FortiGate 中文一本通

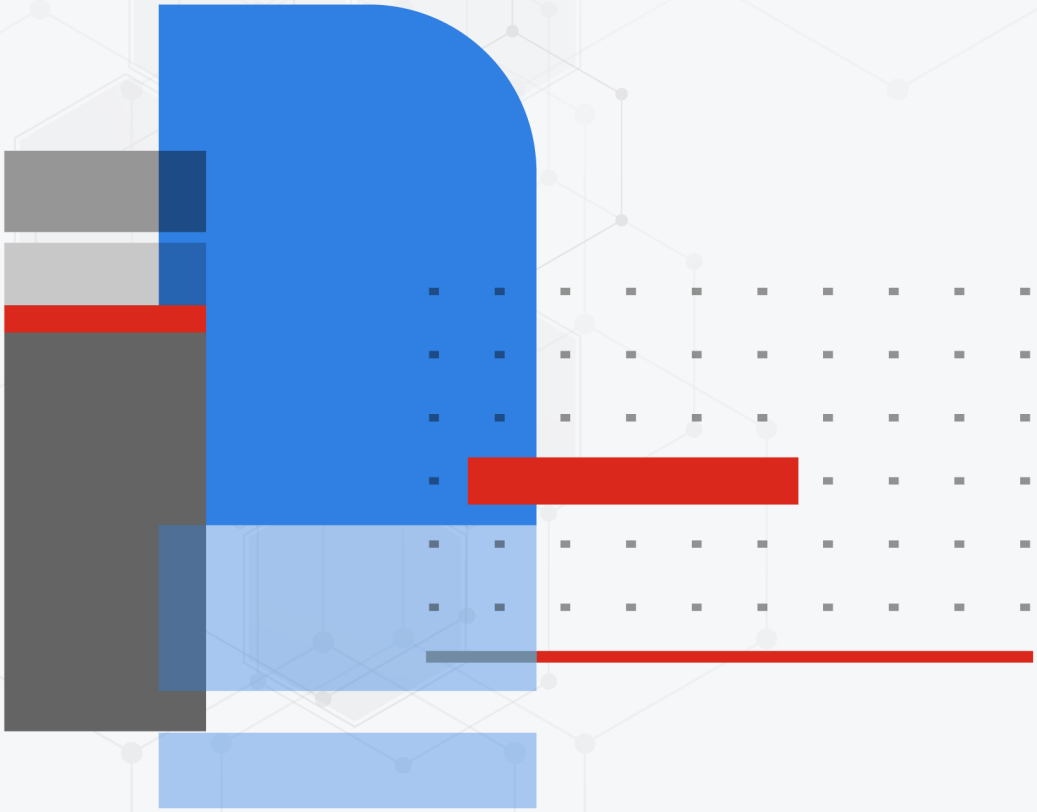
FortiOS 7

35th

Fortinet TAC Team

提示：

通过左侧 PDF 书签浏览文档目录



产品简介

产品介绍

FortiGate 是全新的下一代防火墙，在整个硬件架构和系统上面都有新的设计，在性能和功能上面都有了很大提升，具有性能高、接口丰富、功能齐全、安全路由交换一体化、性价比高等优势。

FortiGate 全新下一代防火墙是面向云计算、数据中心和园区及企业网出口用户开发的新一代高性能防火墙设备。它的功能特性如下：

- 采用多核 CPU + 芯片结构，内置 CP 芯片和 NP 芯片，CP 芯片用于处理内容检测加速，NP芯片用于处理网络层数据转发，具有很高的数据转发性能，大小包线速，最高可达 80Gps 吞吐。
- 具有稳定的防火墙功能，同时具备全面安全防护功能，入侵防御、反病毒、反垃圾邮件、Web 过滤、敏感数据防泄漏等。
- 支持基于用户，五元组、应用层的安全的访问控制。
- 支持 IPSec、SSL 等多种 VPN 业务，可以构建多种形式的 VPN。
- 提供强大的路由能力，静态/RIP/OSPF/BGP 路由、策略路由，路由负载均衡。
  - 高可靠性，支持 VRRP、同时支持更高靠性的 HA 技术，可实现连接状态的同步，支持主主模式，主备模式；支持多心跳冗余，同时可以利用通讯线路做后备心跳线。充分满足各种环境的可靠性需求。

产品型号

桌面设备

桌面设备是保护小型办公、远程办公、零售网络的理想的安全部署选择，同时还可以做为客户端设备（CPE）。Fortinet所提供的桌面级的FortiGate网络安全设备同样具有全面的网络与安全功能，保护远程的用户、应用以及数据。远离APT攻击的威胁。利用AI/ML驱动的安全和创新融合（包括安全 SD-WAN）保护和连接您的分布式边缘。

FortiWiFi设备还提供了一个额外的优势，集成了无线功能，即做为无线胖客户端。FortiWiFi设备使您具备整合无线与有线流量的能力，消除潜在的安全盲点、简化了无线网络部署与维护的复杂性。

```
FortiGate/FortiWiFi-30G
FortiGate/FortiWiFi-40F
FortiGate/FortiWiFi-50G
FortiGate/FortiWiFi-60F
FortiGate-70F
FortiGate/FortiWiFi-70G
FortiGate/FortiWiFi-80F
FortiGate-90G
```

中端设备

FortiGate中端型号安全设备是经过用户验证的高性价比的解决方案。Fortinet能够提供同类厂商中最广的产品线与最先进的安全技术，在不断变化的网络环境中，以有限的部署，提供无限的安全防护。为企业站点获得无与伦比的可见性和保护，以便您在单个仪表板中管理应用程序、用户、设备和访问。

```
FortiGate-100F
FortiGate-120G
FortiGate-200F
FortiGate-200G
FortiGate-400F
FortiGate-600F
FortiGate-900G
```

高端设备

Fortinet业界领先的网络安全平台可提供下一代防火墙安全，同时具有非凡的吞吐量、超低的延迟率与多重威胁防御机制。您可以依赖FortiGate高端设备的扩展性，灵活性，可靠性来实现您网络的需要。部署超大规模安全性，具有一致、协调的保护、丰富的接口和可扩展到任何环境的解密。

FortiGate-6K/7K系列机架和刀片可对高速服务提供商，数据中心和电信运营商的网络提供优越的性能以及可扩展的灵活性。自带的10-GbE支架和高度灵活ATCA兼容的架构使FortiGate-6K/7K系列可服务于下一代网络苛求的环境以及多租户基于云端的Saas与IaaS。

FortiGate-3K/4K系列设备可对大型企业和服务管理提供商提供高性能且集成NGFW的安全解决方案。基于FortiASIC专有芯片加速、高密度端口以及高度的部署灵活性是这一系列产品的显著特点。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate-1000F
FortiGate-1800F
FortiGate-2600F
FortiGate-3000F
FortiGate-3200F
FortiGate-3500F
FortiGate-3700F
FortiGate-4200F
FortiGate-4400F
FortiGate-4800F
FortiGate-6001F
FortiGate-6300F
FortiGate-6500F
FortiGate-7081F
FortiGate-7121F
```

虚拟机VM

通过FortiGate虚拟机， 可实现虚拟架构下威胁的控制与安全防护，同时还可以避免安全盲区以及满足网络的合规性要求。 FortiGate虚拟机具有如同FortiGate物理设备所具有相同的安全与网络服务，自由灵活的集中管控物理设备与虚拟设备混合部署。

```
FortiGate-VM00
Throughput
12 Gbps
vCPU
1x vCPU core, (up to) 2 GB RAM

FortiGate-VM01, -VM01V
Throughput
12 Gbps
vCPU
1x vCPU core, (up to) 2 GB RAM

FortiGate-VM02, -VM02V
Throughput
15 Gbps
vCPU
2x vCPU cores, (up to) 4 GB RAM

FortiGate-VM04, -VM04V
Throughput
28 Gbps
vCPU
4x vCPU cores, (up to) 6 GB RAM

FortiGate-VM08, -VM08V
Throughput
33 Gbps
vCPU
8x vCPU cores, (up to) 12 GB RAM

FortiGate-VM16, -VM16V
Throughput
36 Gbps
vCPU
16x vCPU cores, (up to) 24 GB RAM

FortiGate-VM32, -VM32V
Throughput
50 Gbps
vCPU
32x vCPU cores, (up to) 48 GB RAM

FortiGate-VMUL, -VMULV
vCPU
Unlimited vCPU cores and RAM
```

详细产品参数参考官网：https://www.fortinet.com/cn/products/next-generation-firewall.html#models-specs ↗

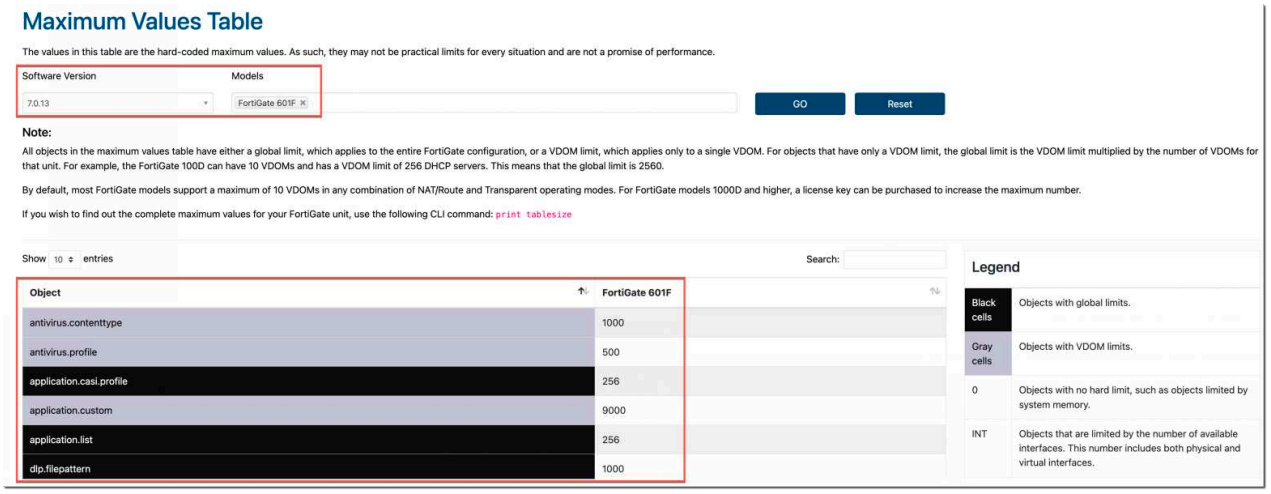
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

产品性能规格

不同产品型号的性能规格请参考Fortinet Product Matrix ↗。

产品功能规格

1. 不同产品型号的功能规格请参考 ↗查询。



2. 也可以在对应型号设备的CLI下执行“print tablesize”命令得到规格显示。

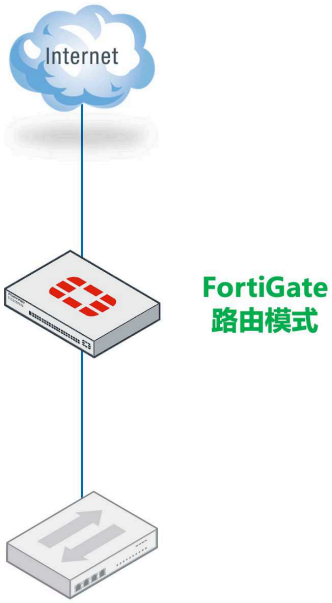
```bash
FortiGate # print tablesize
system.vdom: 0 0 10
system.datasource: 0 0 0
system.accprofile: 0 0 18
system.np6xlite: 0 256 512
system.vdom-link: 0 0 0
system.switch-interface: 0 0 0
system.switch-interface:span-source-port: 0 0 0
system.switch-interface:member: 0 0 0
system.object-tagging: 0 1024 1024
system.object-tagging:tags: 0 0 0
system.interface: 0 0 4096
system.interface:client-options: 0 0 0
system.interface:fail-alert-interfaces: 0 0 0
system.interface:member: 0 0 0
system.interface:security-groups: 0 0 0
system.interface:vrrp: 0 0 0
system.interface:vrrp:proxy-arp: 0 0 0
system.interface:secondaryip: 256 0 0
system.interface:dhcp-snooping-server-list: 255 0 2048
......
```

产品布署模式

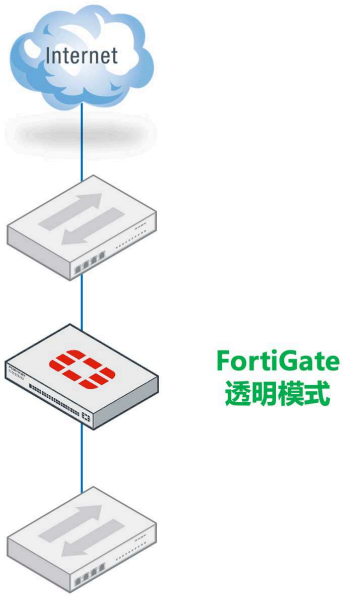
FortiGate有四种工作模式：路由模式、透明模式、旁路模式及混合模式：

1. NAT（路由）模式：把设备当作网络出口，充分使用设备的NAT、路由选路、行为控制、VPN等功能的部署方式。如下图；

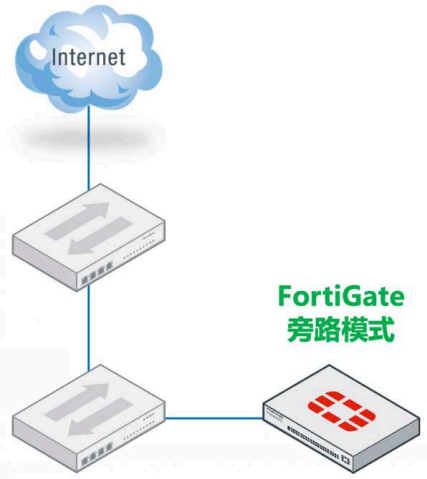
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 透明模式：当用户网络已具备高性能的网络出口，又想使用NGFW的功能，则可以把NGFW串接在内网核心交换机和网络出口设备之间，用户将不必变更网络拓扑和修改路由，就 可使用NGFW的行为控制、VPN等功能。如下图；

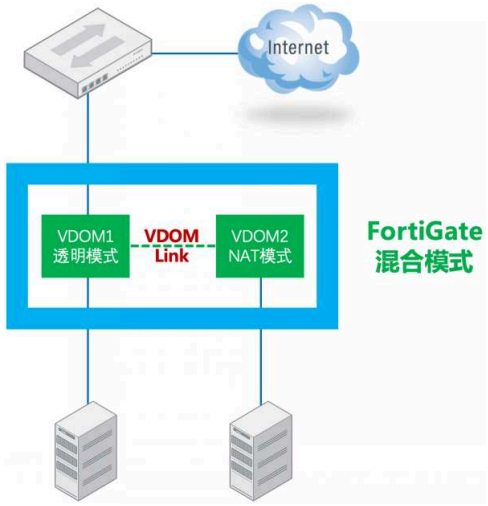


3. 旁路模式：当用户网络已具备高性能的网络出口，也不想把设备串接在内网核心交换机和出口设备之间，又想使用NGFW的VPN、DHCP等功能，则可将设备像一台服务器一样旁挂在核心交换机上，如下图；



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 混合模式（vdom）：指设备同时工作于是路由模式和透明模式，将一个设备分成两个vdom域，一个vdom是透明模式，一个vdom是路由模式，将多个接口划入不同的vdom实现混合模式，如下图。



产品生命周期

Fortinet各个硬件与软件的产品生命周期（Product Life Cycle），请访问 https://support.fortinet.com/support/#/lifecycle ↗ ，使用 Support 账户登录后查看。

产品选型

产品选型请联系Fortinet售前部门：se_china@fortinet.com ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

固件下载

版本推荐

重要

FortiGate版本与FortiManager、FortiAnalyzer产品版本的适应关系可通过如下网站查询：https://docs.fortinet.com/compatibility-tool/fortimanager ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

产品类型	产品名称	推荐版本	是否在支持周期内
入门级	FortiGate-30E	6.2.17	✖
	FortiWiFi-30E	6.2.17	✖
	FortiGate-30G	7.2.12	✅
	FortiGateRugged-35D	6.2.17	✖
	FortiGate-40F/40F-3G4G	7.2.12	✅
	FortiWiFi-40F/40F-3G4G	7.2.12	✅
	FortiGate-50E/51E/52E	6.2.17	✖
	FortiWiFi-50E/51E	6.2.17	✖
	FortiGate-60E	7.2.12	✅
	FortiWifi-60E	7.2.12	✅
	FortiGate-60F/61F	7.2.12	✅
	FortiWiFi-60F/61F	7.2.12	✅
	FortiGateRugged-60F/60F-3G4G	7.2.12	✅
	FortiGate-70F/71F	7.2.12	✅
	FortiGateRugged-70F/70F-3G4G	7.2.12	✅
	FortiGate 70G/71G	7.2.8	✅
	FortiGate-80E/81E	7.2.12	✅
	FortiGate-80F/81F	7.2.12	✅
	FortiGate-90E/91E	7.2.12	✅
	FortiGate-90G/91G	7.2.12	✅
	FortiGate-94D	6.0.18	✖
	FortiGate-98D	6.0.18	✖
中端	FortiGate-100E/101E	7.2.12	✅
	FortiGate-100F/101F	7.2.12	✅
	FortiGate-120G/121G	7.2.12	✅
	FortiGate-140E	7.2.12	✅
	FortiGate-200E/201E	7.2.12	✅
	FortiGate-200F/201F	7.2.12	✅
	FortiGate 200G/201G	7.2.12	✅
	FortiGate-240D	6.0.18	✖
	FortiGate-280D	6.0.18	✖
	FortiGate-300E/301E	7.2.12	✅

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

	FortiGate-400E/401E	7.2.12	✅
	FortiGate-400E-BYPASS	7.2.12	✅
	FortiGate-400F/401F	7.2.12	✅
	FortiGate-500E/501E	7.2.12	✅
	FortiGate-600D	6.4.16	✖
	FortiGate-600E/601E	7.2.12	✅
	FortiGate-600F/601F	7.2.12	✅
	FortiGate-800D	7.2.12	✅
	FortiGate-900D	7.2.12	✅
	FortiGate-900G/901G	7.2.12	✅
高端	FortiGate-1000D	7.2.12	✅
	FortiGate-1100E/1101E	7.2.12	✅
	FortiGate-1000F/1001F	7.2.12	✅
	FortiGate-1200D	7.2.12	✅
	FortiGate-1500D	7.2.12	✅
	FortiGate-1500DT	7.2.12	✅
	FortiGate-1800F/1801F	7.2.12	✅
	FortiGate-2000E	7.2.12	✅
	FortiGate-2200E/2201E	7.2.12	✅
	FortiGate-2500E	7.2.12	✅
	FortiGate-2600F/2601F	7.2.12	✅
	FortiGate-3000D	7.2.12	✅
	FortiGate-3000F/3001F	7.2.12	✅
	FortiGate-3100D	7.2.12	✅
	FortiGate-3200D	7.2.12	✅
	FortiGate-3200F/3201F	7.2.12	✅
	FortiGate-3300E/3301E	7.2.12	✅
	FortiGate-3400E/3401E	7.2.12	✅
	FortiGate-3500F/3501F	7.2.12	✅
	FortiGate-3600E/3601E	7.2.12	✅
	FortiGate-3700D	7.2.12	✅
	FortiGate-3700F/3701F	7.2.12	✅
	FortiGate-3800D	7.2.12	✅
	FortiGate-3810D	6.4.16	✖

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

	FortiGate-3815D	6.4.16	✖
	FortiGate-3960E	7.2.12	✅
	FortiGate-3980E	7.2.12	✅
	FortiGate-4200F/4201F	7.2.12	✅
	FortiGate-4400F/4401F	7.2.12	✅
	FortiGate-4800F/4801F	7.2.12	✅
	FortiGate-5001D	6.4.16	✖
	FortiGate-5001E/5001E1	7.2.12	✅
	FortiGate-6K/7K	7.0.17	✅
虚机VM	FortiGate-VM64	7.2.12	✅

固件版本命名规则

重要

FGT_*A*-*B*-*C*-FORTINET.out

如：FGT_*101F*-*v7.0.13.M*-*build0566*-FORTINET.out

其中：

- *A*部分表示FortiGate型号，不同型号有不同的固件。
- *B*代表版本，有各个不同系列的版本，这里使用x.y.z（如7.0.13）来详细说明：



  - x.y表示大版本号，我们已经发布的大版本有v6.0、v6.2、v6.4、v7.0、v7.2、v7.4等。
  - z表示大版本下持续发布的小版本，对于成熟版本，主要是修复bug，对于新功能版本，主要是推出新功能或者改进原有功能。
- *C*表示内部代码build编号。
- 正在运行的设备版本号，可以在CLI下使用get system status观察到，如下所示。

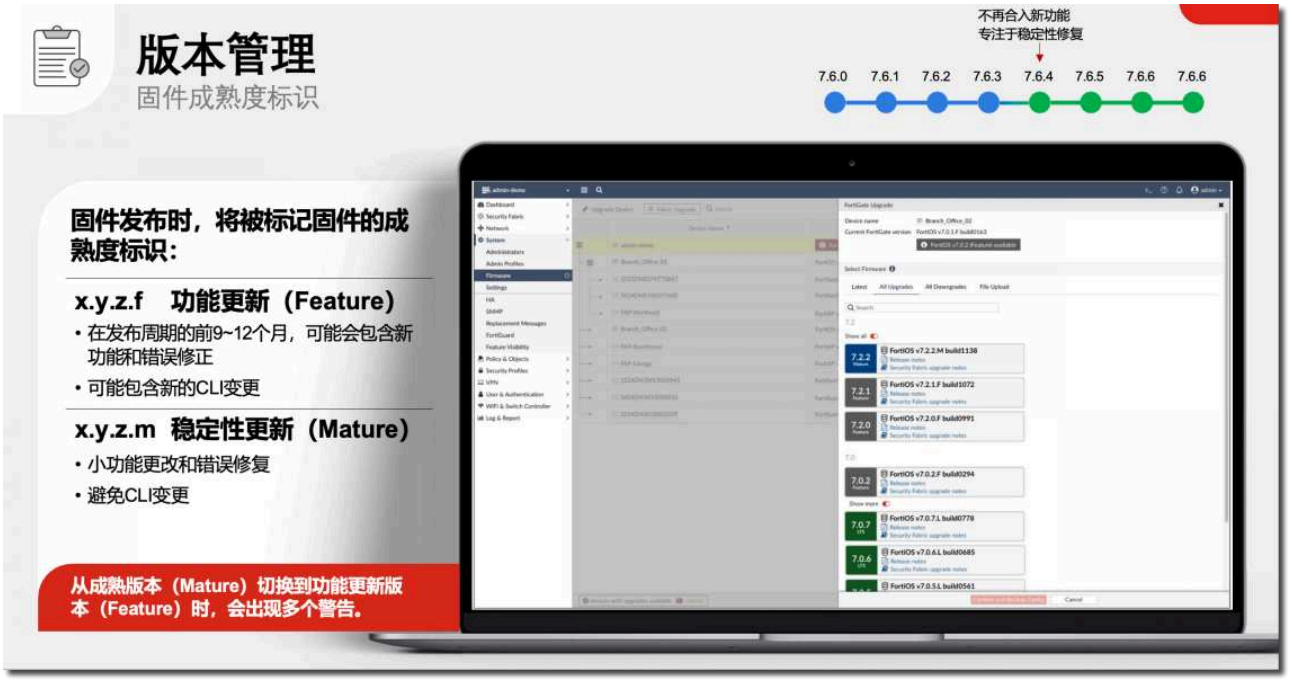
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # get sys status | grep Version:
Version: FortiGate-101F v7.0.13,build0566,231024 (GA.M)
```

选择固件版本的原则

重要

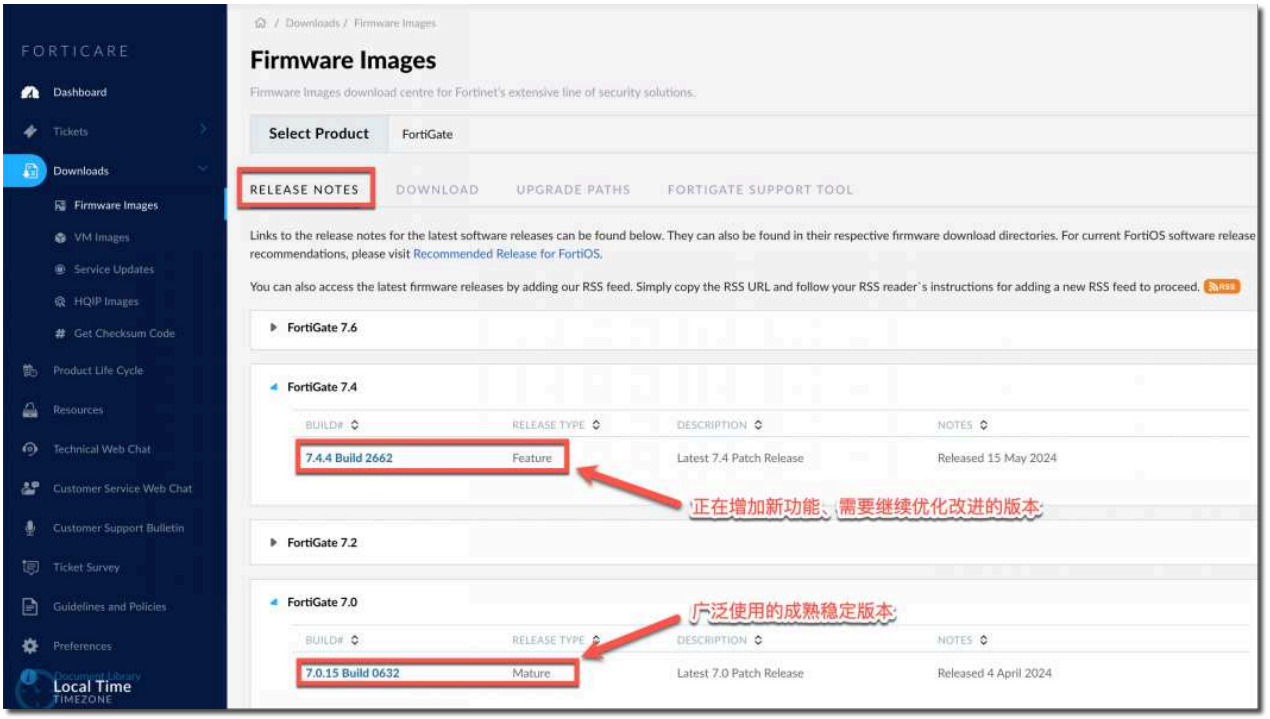
带M标识的版本，B (x.y.z)越大越稳定可靠。



在版本选择上，尽量使用版本数字后为M（Mature）的版本，如“FGT_101F-v7.0.13.M-build0566-FORTINET.out”，该种类型的固件版本较为成熟稳定，尽量不要使用版本数字后为F（Feature）的版本，如“FGT_101F-v7.4.1.F-build2463-FORTINET.out”。

- Mature版本是成熟的版本，是我们主要推荐的稳定版本。该种版本的更新几乎不会引入新功能，以修复Bug为主。对于承载敏感和重要业务的FortiGate，应该部署Mature类型的版本。
- Feature版本属于持续增加新功能、不停优化改进的版本。该种版本的更新以推出新功能为主，只有必须要用到该版本包含的新功能时才应该部署。
- 随着功能的增加改进，Feature版本到一定阶段后会发展成为Mature成熟版本，您在 https://support.fortinet.com/support/#/downloads/firmware ↗ 下载版本时，一定要参考菜单Support→Firmware Download→Release Notes的说明。这部分的说明是经常被更新的。

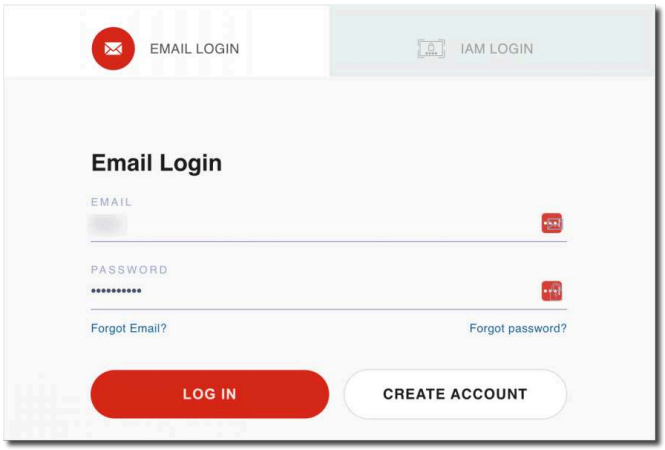
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



固件版本下载

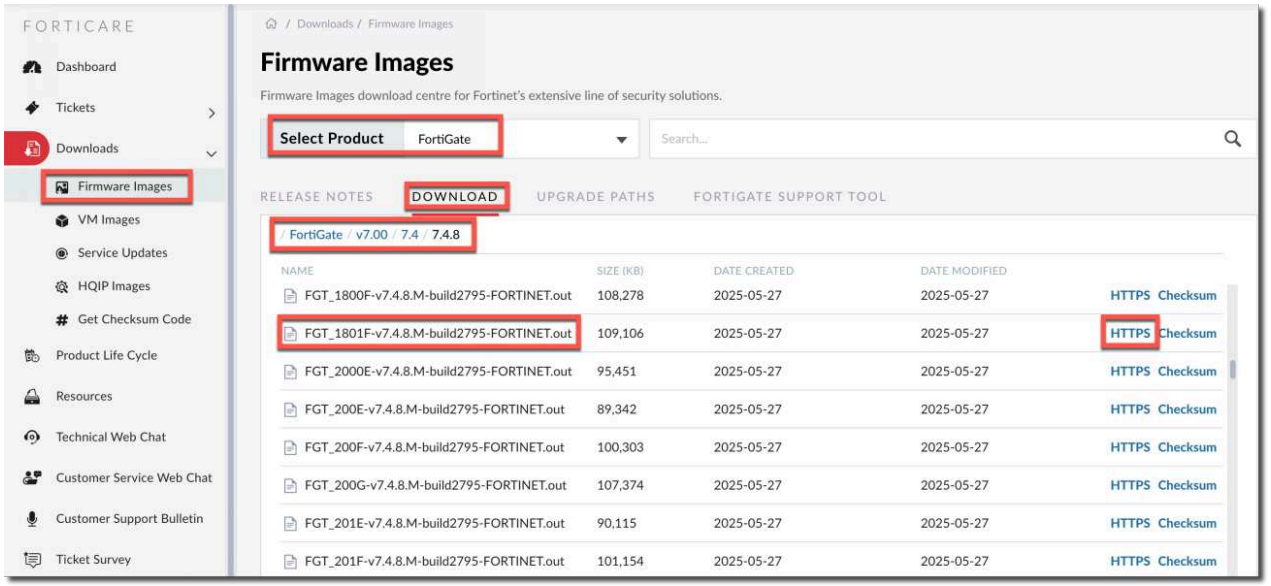
FortiOS固件可以通过Support网站，登录您的FortiCloud账户后进行下载。

1. 使用浏览器直接打开https://support.fortinet.com/support/#/downloads/firmware ↗ ， 登录您的FortiCloud账户（如您忘记了自己的FortiCloud账户或密码或账户被锁定，可联系support_cn@fortinet.com申请恢复）。

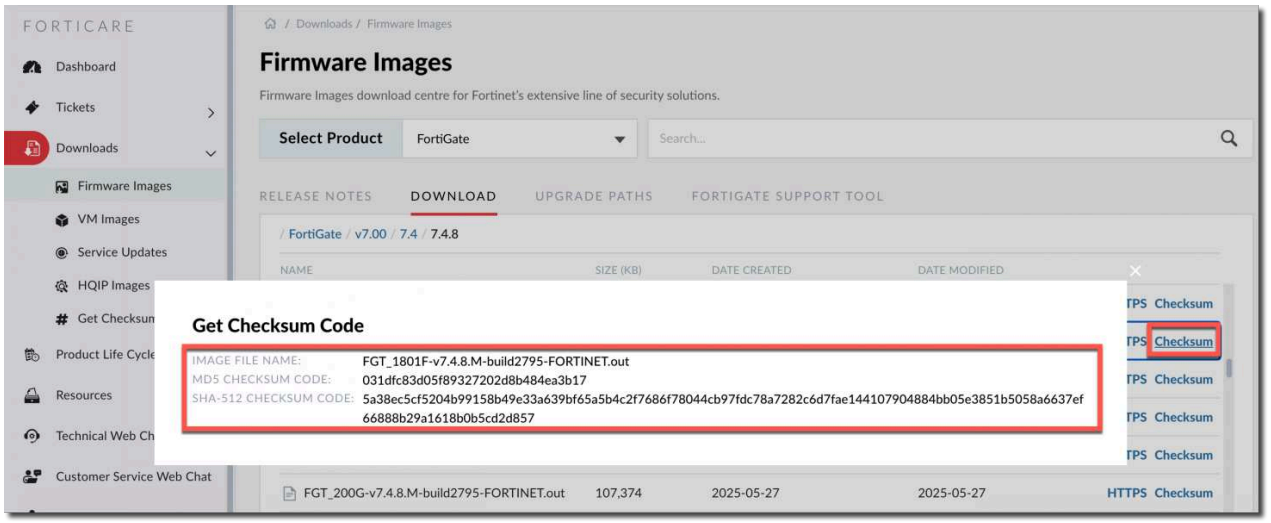


2. 登录后，选择对应的产品：FortiGate，选择Download，进入要下载的版本目录（如下所示为FortiOS 7.4.8），选择您的产品对应的版本（如下图所示为FortiGate-1801F），点击右侧的HTTPS按钮进行下载。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 点击固件名称右侧的Checksum按钮，可以看到该版本文件的Checksum信息，请您下载文件后进行验证。



4. 附Checksum验证工具：Checksum_Tool ↗，也可通过在线Checksum校验（如https://www.md5ma.com/md5-calculator ↗）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

公网接口访问限制

为了提升网络安全性，限制来自互联网对FortiGate的管理访问是至关重要的。通过限制管理接口的访问范围，可以有效防止未经授权的远程登录，降低潜在的安全风险。

为什么要限制FortiGate的互联网访问?

- **防止未经授权的访问**：公开的管理接口可能被恶意用户扫描和利用，导致未经授权的访问。
- **减少攻击面**：限制管理接口的访问范围，可以减少暴露在互联网中的服务，降低被攻击的可能性。
- **遵循安全最佳实践**：网络安全的基本原则之一是最小化暴露面，限制管理接口的访问是实现这一原则的重要措施。

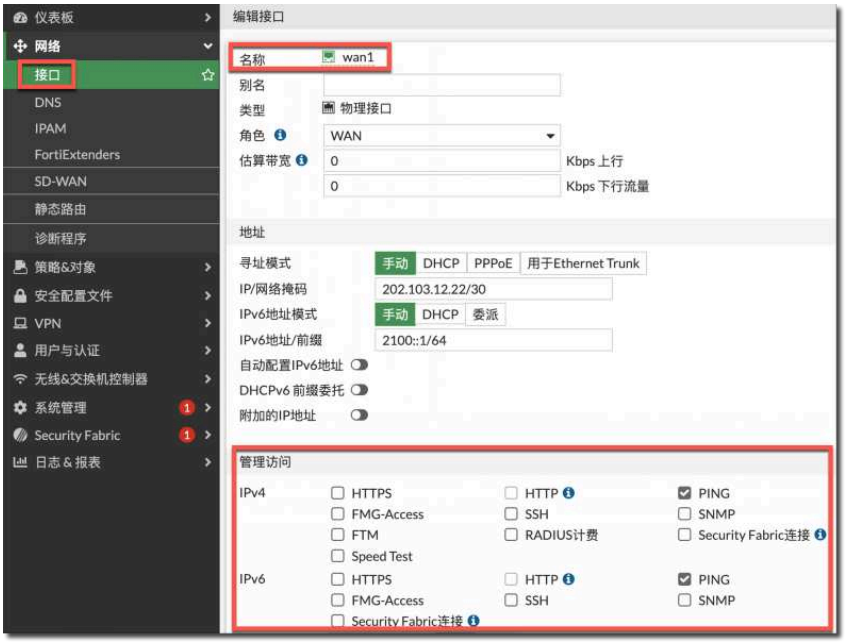
请根据实际网络环境和安全需求，合理应用以下方法，以确保FortiGate的安全管理。

禁用互联网接口管理协议

> **重要**
>
> 通过禁用外部接口（如WAN口）的管理协议（如HTTP、HTTPS、SSH、Telnet、FMG-Access等）访问，仅保留必要的管理协议（如Ping），可以减少暴露在互联网的管理服务，降低被攻击的风险。

1. 进入“网络→接口”页面，编辑FortiGate的互联网网接口（这里以wan1为例），在管理访问中，只开启PING访问，关闭其他协议的管理访问（如果FortiGate启用了互联网接口的IPv6，则需要在IPv6的管理访问中执行相同操作）。

   > **重要**
   >
   > FortiManager通过Internet管理FortiGate时，如果是FortiGate主动注册到FortiManager的模式，不需要开启FMG-Access管理。




```bash
config system interface
    edit "wan1"
        set allowaccess ping
        config ipv6
            set ip6-allowaccess ping
        end
    next
end
```

2. 在内网接口上开启管理协议（如HTTPS、SSH等）通过内网接口或VPN远程连接的方式管理FortiGate。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置Local-in策略

重要

Local-in策略用于控制目标是FortiGate自身地址的流量，可用于限制对接口本身的访问。

关于Local-in策略的更多介绍可参考策略与对象→本地策略→Local-in策略 ↗章节。

1. 如果由于实际需要，FortiGate的外网接口必须开启HTTPS/SSH远程访问（或内网接口限定使用特定跳板机/VPN客户端网段访问），可以通过Local-in策略指定可信任的主机IP地址范围，确保只有来自这些地址的连接才能进行管理访问，从而提高安全性。

```bash
config system interface
    edit "wan1"
        set allowaccess ping https ssh
        config ipv6
            set ip6-allowaccess ping https ssh
        end
    next
end
```

2. 创建允许访问FortiGate的公网接口的源地址对象（请替换内容为您真实环境中的信任公网地址），并使用地址组引用这些地址对象。

```bash
config firewall address
    edit "60.247.121.226/32"
        set subnet 60.247.121.226 255.255.255.255
    next
    edit "123.112.245.11/32"
        set subnet 123.112.245.11 255.255.255.255
    next
    edit "39.105.115.224/29"
        set subnet 39.105.115.224 255.255.255.248
    next
end

config firewall addrgrp
    edit "Internet_Admin_Trust_List4"
        set member "39.105.115.224/29" "60.247.121.226/32" "123.112.245.11/32"
    next
end
```

3. （可选）如果FortiGate启用了互联网接口的IPv6，则需要同时创建IPv6的地址对象/地址组。

```bash
config firewall address6
    edit "240e:88::3/128"
        set ip6 240e:88::3/128
    next
    edit "2001::/96"
        set ip6 2001::/96
    next
end

config firewall addrgrp6
    edit "Internet_Admin_Trust_List6"
        set member "2001::/96" "240e:88::3/128"
    next
end
```

4. 在FortiGate的互联网接口（这里以wan1为例）上配置Local-in策略，禁止除源地址组外的其他地址访问FortiGate互联网接口的HTTP/SSH协议。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

- Local-in策略只会影响目标是FortiGate自身地址的流量，不会影响DNAT策略流量（穿越流量）。
- 此例中的FortiGate使用默认的HTTPS端口443、SSH端口22作为管理端口，如果您修改了默认HTTPS/SSH管理端口，请创建对应端口的服务对象（如下所示），然后在Local-in策略中的 `service` 中引用。

```bash
config firewall service custom
    edit GUI_HTTPS
        set tcp-portrange 4443
    next
    edit Custom_SSH
        set tcp-portrange 2233
    next
end
```

```bash
config firewall local-in-policy
    edit 1
        set intf "wan1"
        set srcaddr "Internet_Admin_Trust_List4"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSH"
        set schedule "always"
    next
    edit 2
        set intf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "HTTPS" "SSH"
        set schedule "always"
    next
end
```

重要

Local-in Policy默认隐含策略的动作为permit all。所以以上配置只会影响HTTPS、SSH的访问，不会影响其他访问FortiGate自身的流量（如IPSec、SSL VPN、BGP、OSPF等）。

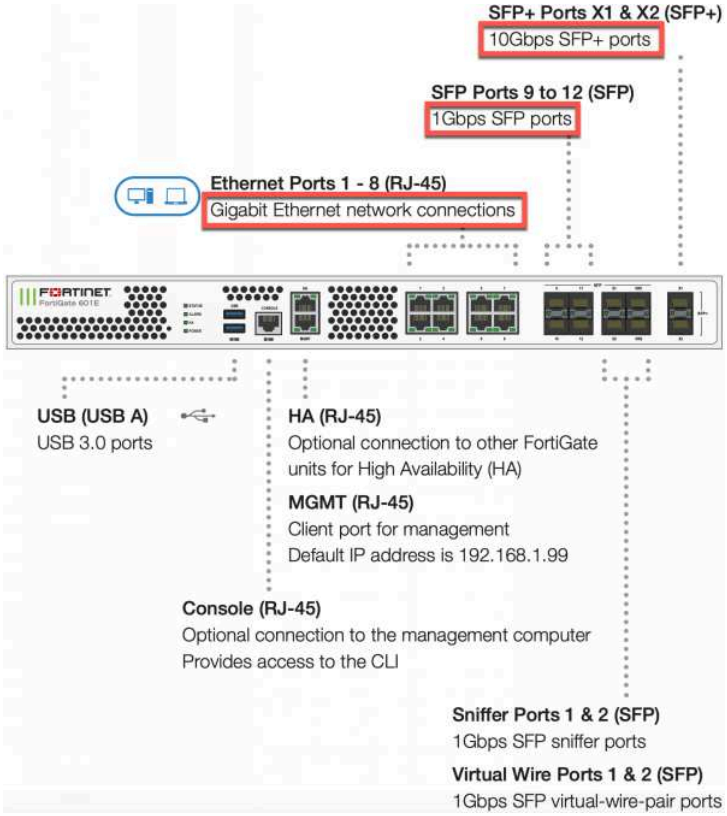
5. （可选）如果FortiGate启用了互联网接口的IPv6，则需要对应创建IPv6的Local-in策略。

```bash
config firewall local-in-policy6
    edit 1
        set intf "wan1"
        set srcaddr "Internet_Admin_Trust_List6"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSH"
        set schedule "always"
    next
    edit 2
        set intf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "HTTPS" "SSH"
        set schedule "always"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

不要将10G与1G接口混用

1. 对于使用NP6芯片（不包含NP6xlite）的设备（如FortiGate 600E），同时具备QSGMII的1G接口和XAUI的10G接口：



2. 如果存在以下情况，容易出现NP层面丢包，这对基于TCP的服务应用很可能造成测速下降的问题现象：

   - 在10G接口→1G接口的方向上存在较高带宽的数据传输
   - 数据传输过程存在突发流量micro bursts
   - 流量可以被NP6加速

3. **实际部署时，尽量避免同时使用1G接口和10G接口进行流量转发。**

4. 如果设备已经部署无法更改接口连线，需要同时保持10G和1G接口在生产环境中使用，可以考虑修改以下配置让上述流量不被NPU加速，以规避这个问题。

```bash
config system npu
  set host-shortcut-mode host-shortcut    //该命令效果是10G→1G方向的流量关闭NPU加速
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

120G/121G HA心跳口问题

问题现象

在使用FortiOS 7.2.9/7.2.10版本的120G/121G设备上配置HA，且HA心跳接口使用“ha”或“mgmt”接口时，会出现如下问题：

1. “系统管理→高可靠性”页面无法正常打开，一直处于加载状态。
2. 两台120G/121G设备的HA状态一直无法成为“Synchronized”（同步）状态，如下所示（在主机FG120GTKXXYYZZ50查看HA状态），备机FortiGate (FG120GTKXXYYZZ59) 的状态在1721194954秒前更新，checksum dump为00。这表明 FortiGate 设备之间存在心跳连接问题。

```bash
FG120GTKXXYYZZ59 # get system ha status
HA Health Status: OK
Model: FortiGate-120G
......
 Configuration Status:
    FG120GTK24001650(updated 1 seconds ago): in-sync
    FG120GTKXXYYZZ50 chksum dump: 29 e0 e4 32 6c 76 99 68 2b ed 8b bc c1 2d 2c 37
    //FG120GTKXXYYZZ59(updated 1721194954 seconds ago): out-of-sync//<———备机无法同步
    //FG120GTKXXYYZZ59 chksum dump: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00//<———checksum dump为00
......
HBDEV stats:
    FG120GTK24001650 (updated 1 seconds ago):
        ha: physical/1000auto, up, rx-bytes/packets/dropped/errors=121750988/234138/0/0, tx=120280738/235391/0/0
    //FG120GTKXXYYZZ59 (updated 1721194954 seconds ago)://<———更新时间异常
Primary : FortiGate-120G , FG120GTK24001650, HA cluster index = 1
Secondary : , FG120GTKXXYYZZ59, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FG120GTK24001650, HA operating index = 0
Secondary: FG120GTKXXYYZZ59, HA operating index = 1
```

问题原因

当使用“ha”或“mgmt”接口用作HA心跳接口时，FortiGate无法正常更新HA逻辑接口 “port_ha”的MAC地址。这是一个FortiOS 7.2.9/7.2.10版本的bug（参考：https://docs.fortinet.com/document/fortigate/7.2.9/fortios-release-notes/236526/known-issues ↗，Bug ID 1056138）。

解决方法

1. Workaround：暂时使用“ha”和“mgmt”以外的接口作为HA心跳接口。
2. 该问题已在FortiOS 7.2.11/7.4.5/7.6.1版本解决。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

PPPoE接口配置

配置说明

需要使用FortiGate PPPoE拨号时，建议通过CLI的方式新建PPPoE虚拟接口，在该接口下配置用户名与密码，并绑定公网物理口。

> **重要**
>
> 在7.4.2及以后版本的硬件设备上，可以在GUI创建PPPoE虚拟接口。

使用该种配置方法有如下优势：

- 传统方式（将普通接口的模式修改为PPPoE），修改接口下与PPPoE拨号无关的参数（如“DNS覆盖”、接口管理协议、MTU、inbandwidth/outbandwidth等），PPPoE会重新拨号，影响业务。而手动创建的PPPoE虚拟接口修改与PPPoE拨号无关的参数，PPPoE不会重新拨号，不会影响业务。
- 传统方式（将普通接口的模式修改为PPPoE）拨号成功后，会动态创建ppp接口，无法指定动态创建的ppp接口的`tcp-mss`。PPPoE虚拟接口可以针对PPPoE虚拟接口设置`tcp-mss`参数（传统方式），这在PPPoE环境下产生的TCP分片丢包问题非常有用。
- PPPoE接口配置更灵活，可以在一个物理口上配置多个PPPoE接口。可独立于物理口配置每个PPPoE接口的属性。在其他模块（如防火墙策略、SD-WAN）引用接口时更加直观和灵活。
- 由于PPPoE接口为动态获取网关，与策略路由配合使用时，策略路由可以正常获取到PPPoE的网关，不需要手动填写网关。
- 可配置按需拨号。

配置步骤

1. 例如配置port2的PPPoE，在CLI（`config system pppoe-interface`）下新建虚拟PPPoE接口，并绑定在port2接口上，配置PPPoE用户名和密码。

```bash
config system pppoe-interface
    edit "pppoe"
        set device "port2"
        set username "bing"
        set password xxxxxxxx
    next
end
```

2. 以上命令执行后，会自动在`config system interface`下创建同名接口，其中包含“从服务器中重新得到网关”的配置。

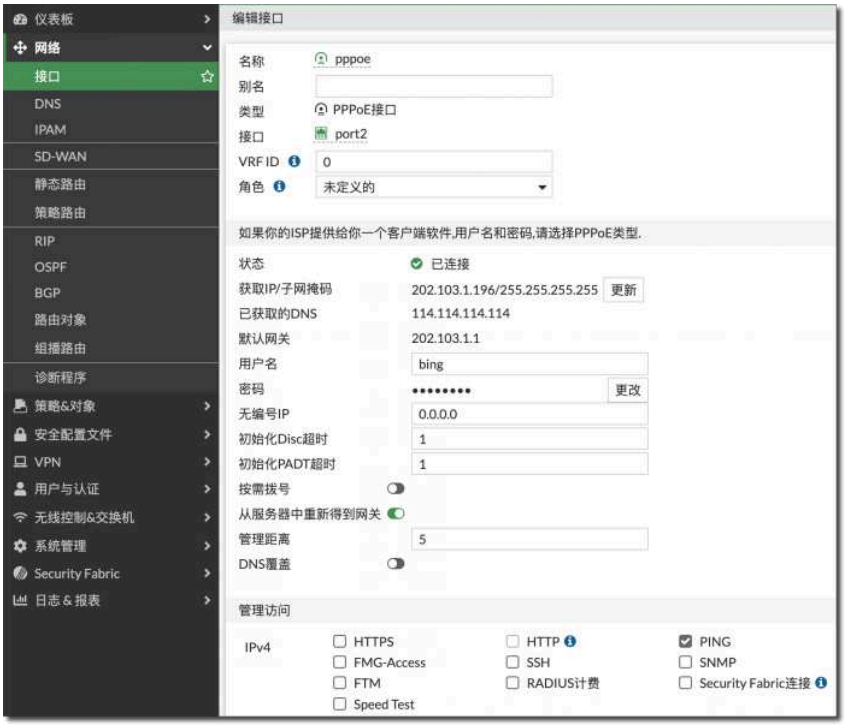
```bash
FortiGate # show full sys int pppoe
config system interface
    edit "pppoe"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set defaultgw enable
        set interface "port2"
    next
end
```

3. 在此接口下，可以配置PPPoE虚拟接口的相关参数，如管理协议、TCP-MSS、DNS覆盖等，在这里修改的参数不会导致PPPoE重新拨号。

```bash
config system interface
    edit "pppoe"
        set allowaccess ping
        set tcp-mss 1400
        set dns-server-override disable
    next
end
```

4. 以上配置完成后，可以在GUI上看到port2下多了一个PPPoE接口，并获取到了运营商分配的IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

TLS探测配置

TLS探测介绍

当FortiGate在检查基于TLS的连接（如开启WebFilter并检测HTTPS连接）时，客户端经过FortiGate的业务VDOM访问某个HTTPS网站，FortiGate会提取客户端PC发送的TLS Client Hello中的SNI，从SNI中提取网站的域名，然后先于客户端去探测网站证书的合法性，这是为了保证后续TLS协商以及业务报文的安全性。TLS探测报文的源地址只会使用FortiGate自身的IP地址。

在多出口、多VDOM、透明模式、SD-WAN、接口配置第二IP等场景下，TLS探测可能会因路由或线路问题导致超时失败。

拓扑信息

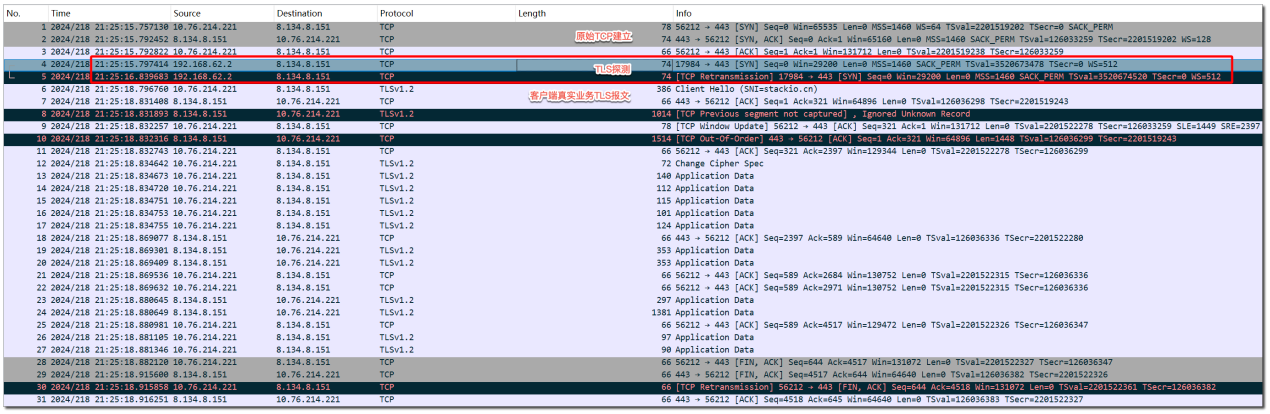
FortiGate如果开启了网页过滤（Web Filter）功能，需要注意如下拓扑环境下的配置。

- FortiGate划分了多个VDOM：
  - 管理VDOM接口（mgmt）可以访问Internet与内网其他设备，用于登录、FortiGuard分类查询、Syslog、SNMP等管理业务。
  - 业务VDOM的所有接口只做业务转发，接口IP无法访问Internet。
  - 通过业务VDOM接口转发的流量可以正常访问Internet。
- FortiGate未开启VDOM：
  - 默认路由中包含多个出接口。
  - 其中一些出接口的IP无法访问Internet。
  - 接口配置了第二地址，只有第二地址可以访问Internet。

问题现象

1. 以FortiGate多VDOM的场景为例。默认配置下，从FortiGate发送的TLS探测报文，只能以防火墙业务VDOM自己的接口IP来发出。

2. 如果业务VDOM的接口IP本身无法访问Internet的，FortiGate去探测网站HTTPS时，TCP是无法建立的，超时3s后，会放弃TLS探测，继续真实客户端的TLS报文的转发。如下所示在FortiGate业务VDOM的外网口抓包。



3. 相关IPS Debug日志显示TLS探测失败。

```bash
diagnose ips filter set "(host x.x.x.x or host x.x.x.x) and port 443"
diagnose ips debug enable all
diagnose debug console timestamp enable
diagnose debug enable

2024-12-27 15:32:49 [10600@-1]ssl_resume_sess: sess 4311: ssl resume
2024-12-27 15:32:49 [10600@-1]ips_urlf_del_query: id:2229, queue:0
2024-12-27 15:32:49 [10600@-1]eng_debug_log: Probe info:
2024-12-27 15:32:49 [10600@-1]eng_debug_log:   Server: 8.134.8.151:443
2024-12-27 15:32:49 [10600@-1]eng_debug_log:   Server name: stackio.cn
2024-12-27 15:32:49 [10600@-1]eng_debug_log:   STARTTLS: no
2024-12-27 15:32:49 [10600@-1]eng_debug_log:   Probe failed: unable to connect    ←——TLS探测失败
2024-12-27 15:32:49 [10600@-1]eng_debug_log: parallel probes: 1
2024-12-27 15:32:49 [10600@-1]eng_debug_log: Memory usage: 276 KiB, errors: 2046
2024-12-27 15:32:49 [10601@-1]probe_finish: probe is finished. id: 1194, sess: 4218
2024-12-27 15:32:49 [10601@-1]ssl_resume_sess: sess 4218: ssl resume
2024-12-27 15:32:49 [10601@-1]ips_eng_log_ssl: ssl log host stackio.cn, CN , type 12
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 对应的SSL安全事件日志（日志子类型为`certificate-probe-failed`）。

```bash
date=2025-10-16 time=14:20:41 eventtime=1760595641888725921 tz="+0800" logid="1700062305" type="utm" subtype="ssl"
eventtype="ssl-anomaly" level="warning" vd="root" action="allow" policyid=1 poluuid="04d852a8-7f02-51f0-65cd-
4c50ca8f3632" policytype="policy" sessionid=6753380 service="HTTPS" profile="test-example" srcip=192.168.100.177
srcport=53784 srccountry="Reserved" dstip=173.243.143.6 dstport=443 dstcountry="United States" srcintf="lan"
srcintfrole="lan" dstintf="wan1" dstintfrole="wan" srcuuid="e2f430d6-7f00-51f0-8d55-e762fbba6612"
dstuuid="e2f430d6-7f00-51f0-8d55-e762fbba6612" proto=6 eventsubtype="certificate-probe-failed"
hostname="173.243.143.6"
```

5. 这是由于默认配置下，TLS探测报文使用当前业务VDOM下的默认路由出接口。但只有管理VDOM的接口可以正常访问Internet，这样就会造成访问延迟。

解决方法1

1. 修改TLS探测使用的VDOM和接口。

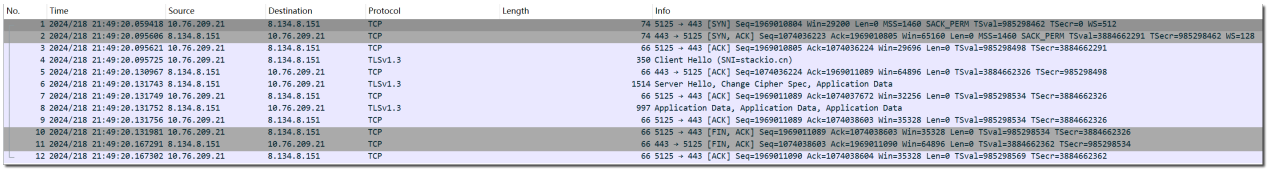
```bash
config ips global
config tls-active-probe
    set interface-selection-method <auto|sdwan|specify>
    set interface <intf name>
    set vdom <vdom name>
    set source-ip <source_ipv4>
    set source-ip6 <source_ipv6>
  end
end
```

- `interface-selection-method`：TLS探测报文选择接口的方式。
  - `auto`：默认配置，根据当前VDOM下的路由表来进行发送（有多个接口负载分担时，可能会发送到错误的接口）；
  - `sdwan`：匹配SD-WAN规则进行发送。
  - `specify`：手工选择需要发送的方式。
- `interface`：指定发送TLS探测报文的接口（当`interface-selection-method`设置为`specify`时可选）。
- `vdom`：指定发送TLS探测报文的VDOM（当`interface-selection-method`设置为`specify`或`sdwan`时可选）。
- `source-ip` / `source-ip6`：指定发送TLS探测报文的源IPv4/IPv6（当`interface-selection-method`设置为`specify`或`sdwan`时可选）。

2. 此例中，在Global下将TLS探测的接口改为root VDOM的mgmt口，可以正常进行TLS探测，不会产生超时现象。

```bash
config global
    config ips global
        config tls-active-probe
            set interface-select-method specify
            set vdom root
            set interface mgmt
        end
    end
end
```

3. 在mgmt接口上抓取的完整的TLS探测报文如下。



No.	Time	Source	Destination	Protocol	Length	Info
1	2024/218 21:49:20.059418	10.76.209.21	8.134.8.151	TCP	74	5125 → 443 [SYN] Seq=1969010804 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=985298462 TSecr=0 WS=512
2	2024/218 21:49:20.095606	8.134.8.151	10.76.209.21	TCP	74	443 → 5125 [SYN, ACK] Seq=1074036223 Ack=1969010805 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3884662291 TSecr=985298462 WS=128
3	2024/218 21:49:20.095621	10.76.209.21	8.134.8.151	TCP	66	5125 → 443 [ACK] Seq=1969010805 Ack=1074036224 Win=29696 Len=0 TSval=985298498 TSecr=3884662291
4	2024/218 21:49:20.095725	10.76.209.21	8.134.8.151	TLSv1.3	350	Client Hello (SNI=stackio.cn)
5	2024/218 21:49:20.130967	8.134.8.151	10.76.209.21	TCP	66	443 → 5125 [ACK] Seq=1074036224 Ack=1969011089 Win=64896 Len=0 TSval=3884662326 TSecr=985298498
6	2024/218 21:49:20.131743	8.134.8.151	10.76.209.21	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
7	2024/218 21:49:20.131749	10.76.209.21	8.134.8.151	TCP	66	5125 → 443 [ACK] Seq=1969011089 Ack=1074037672 Win=32256 Len=0 TSval=985298534 TSecr=3884662326
8	2024/218 21:49:20.131752	8.134.8.151	10.76.209.21	TLSv1.3	997	Application Data, Application Data, Application Data
9	2024/218 21:49:20.131756	10.76.209.21	8.134.8.151	TCP	66	5125 → 443 [ACK] Seq=1969011089 Ack=1074038603 Win=35328 Len=0 TSval=985298534 TSecr=3884662326
10	2024/218 21:49:20.131981	10.76.209.21	8.134.8.151	TCP	66	5125 → 443 [FIN, ACK] Seq=1969011089 Ack=1074038603 Win=35328 Len=0 TSval=985298534 TSecr=3884662326
11	2024/218 21:49:20.167291	8.134.8.151	10.76.209.21	TCP	66	443 → 5125 [FIN, ACK] Seq=1074038603 Ack=1969011090 Win=64896 Len=0 TSval=3884662362 TSecr=985298534
12	2024/218 21:49:20.167302	10.76.209.21	8.134.8.151	TCP	66	5125 → 443 [ACK] Seq=1969011090 Ack=1074038604 Win=35328 Len=0 TSval=985298569 TSecr=3884662362

解决方法2

如果是FortiGate所有接口都不能访问Internet的封闭环境，可以关闭TLS探测，需要配置自定义SSL/SSH配置文件，然后在防火墙策略中引用（出于安全性考虑，不推荐此方法）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall ssl-ssh-profile
    edit "test-example"
        config https
            set sni-server-cert-check disable
        end
    next
end

config firewall policy
    edit 1
        set name "to_Internet"
        set ssl-ssh-profile "test-example"
    next
end
```

TLS探测失败默认动作

上文介绍过，在检查基于TLS的连接（如HTTPS）时，FortiGate需要执行TLS证书探测，以便获取服务器的证书并确定用户试图访问的目标域名/地址。若因某些原因导致此TLS探测失败（例如FortiGate的探测请求无法到达目标Web服务器），则FortiGate需判断该连接应被阻断还是允许通过。

SSL/SSH配置文件中的`cert-probe-failure`选项可以控制此行为：

> **重要**
>
> - 在FortiOS 7.6.0之前版本中，`cert-probe-failure`的默认动作为`block`。
> - 在FortiOS 7.6.0及之后版本中，`cert-probe-failure`的默认动作为`allow`。

```bash
config firewall ssl-ssh-profile
    edit <profile_name>
        config https
            set cert-probe-failure <allow|block>    ←——在7.6.0之前，默认配置为block，在7.6.0及之后，默认动作为allow
        end
    next
end
```

但在不同的FortiOS版本/防火墙策略检测模式（flow/proxy）上，该配置产生的影响存在区别。

- **7.2.11/7.4.5/7.6.1之前版本（动作block）：**
  - **代理（proxy）模式：**若TLS探测失败，则阻断连接。该选项仅对采用代理（proxy）模式的防火墙策略生效。
  - **流（flow）模式：**`cert-probe-failure`选项会被忽略，此时即使探测失败，系统仍会始终允许连接建立（但可能会产生上文提到的访问延迟）。
- **7.2.11/7.4.5/7.6.1及之后版本（动作block）：**
  - **代理（proxy）模式：**若TLS探测失败，则阻断连接。
  - **流（flow）模式：**`cert-probe-failure`选项会被考虑，若TLS探测失败，则阻断连接，与proxy模式保持一致。

产生的问题

如上所述，在7.2.11/7.4.5/7.6.1及之后版本开始，`cert-probe-failure`设置已经对基于流（flow）模式的防火墙策略生效。在常规部署中，通常会使用flow模式（默认配置）作为防火墙的检测模式。

如果防火墙之前已存在TLS探测失败的的情况，在升级到7.2.11/7.4.5后可能会突然出现TLS连接问题。此时，转发流量日志将显示Web会话被UTM阻断。安全事件中的相关SSL日志将记录以下信息（`certificate-probe-failed`、`SSL connection is blocked due to unable to retrieve server's certificate`）：

```bash
↓↓↓TLS探测在初始阶段失败，没有具体原因↓↓↓
date=2025-10-16 time=14:20:41 eventtime=1760595641888725921 tz="+0800" logid="1700062305" type="utm" subtype="ssl"
eventtype="ssl-anomaly" level="warning" vd="root" action="block" policyid=1 poluuid="04d852a8-7f02-51f0-65cd-
4c50ca8f3632" policytype="policy" sessionid=6753380 service="HTTPS" profile="test-example" srcip=192.168.100.177
srcport=53784 srccountry="Reserved" dstip=173.243.143.6 dstport=443 dstcountry="United States" srcintf="lan"
srcintfrole="lan" dstintf="wan1" dstintfrole="wan" srcuuid="e2f430d6-7f00-51f0-8d55-e762fbba6612" dstuuid="e2f430d6-
7f00-51f0-8d55-e762fbba6612" proto=6 eventsubtype="certificate-probe-failed" hostname="173.243.143.6"

↓↓↓TLS探测在与Server交换证书阶段失败，原因是无法获取服务器证书，可能是因为线路MTU等问题↓↓↓
date=2024-10-03 time=16:00:05 id=7421548890156962227 itime="2024-10-03 16:00:05" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=704052702 devid="F2K60FTK21900878" vd="root" type="utm" subtype="ssl" level="warning"
sessionid=1749042461 policyid=1735 srcip=172.16.11.37 dstip=54.177.212.176 srcport=53508 dstport=443 proto=6
logid=1700062305 service="SSL" action="blocked" eventtime=1727964004535181139 srcintfrole="wan" dstintfrole="wan"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
srcintf="port33" dstintf="port19" eventtype="ssl-anomaly" profile="certificate-inspection" hostname="fortinet.com"
msg="SSL connection is blocked due to unable to retrieve server's certificate" tz="+0200" eventsubtype="certificate-
probe-failed" srcuuid="7aaabd7a-7b3b-51ef-043f-65b562658a6d" dstuuid="83807c12-a3df-51ed-6ed9-2e2613693fe8"
sni="fortinet.com" policytype="policy" srccountry="Reserved" dstcountry="United States" poluuid="2df1b1e4-7a4d-51ef-
078f-d42cf99bc294" dtime="2024-10-03 16:00:05" itime_t=1727964005 devname="FortiGate-100F"
```

解决方法1

解决底层TLS探测失败问题。如上个章节所示，在大多数情况下，通过检查FortiGate用于连接远程Web服务器的路由和网络路径，可修复TLS探测失败问题。

解决方法2

如果无法解决TLS探测失败问题，则可以创建自定义SSL/SSH配置文件，修改`cert-probe-failure`的动作为allow（但仍可能会产生上个章节提到的访问延迟），并在相应的防火墙策略中引用该自定义SSL/SSH配置文件。

重要

在FortiOS 7.6.0及之后版本中，`cert-probe-failure`的默认动作已经被设置为`allow`。

bash
```
config firewall ssl-ssh-profile
    edit "test-example"
        config https
            set cert-probe-failure allow
        end
    next
end
config firewall policy
    edit 1
        set name "to_Internet"
        set ssl-ssh-profile "test-example"
    next
end
```

重要

注意：如果在`config ssl`中配置了`inspect-all`（如下所示），则`config https`中的`cert-probe-failure`选项会被禁用。

bash
```
config firewall ssl-ssh-profile
edit "test-example"
config ssl
set inspect-all certificate-inspection
end
next
end
```

解决方法3

创建自定义SSL/SSH配置文件，关闭`sni-server-cert-check`，禁用SNI检查，同时可以禁用TLS探测。并在相应的防火墙策略中引用该自定义SSL/SSH配置文件。出于安全性考虑，不推荐此方法。

bash
```
config firewall ssl-ssh-profile
    edit "test-example"
        config https
            set sni-server-cert-check disable
        end
    next
end

config firewall policy
    edit 1
        set name "to_Internet"
        set ssl-ssh-profile "test-example"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

开启COMLog

COMLog介绍

该功能会将Console下的所有输出记录到Flash卡的一个日志文件（4 MB）中，设备断电、重启、从BIOS格式化Flash或升级FortiOS后，该日志文件不会被擦除。

启用COMLog后，FortiGate会将启用后所有Console输出记录到Flash中，还会每小时写入一个时间戳。

如果设备遇到突然重启或无响应等意外行为，系统日志可能无法记录到有价值的信息，而Console下会产生一些系统日志无法记录的日志信息，COMLog的记录可能会提供一些线索，从而帮助工程师找到问题发生的原因。在设备正式上线前，建议在支持COMLog的设备上开启COMLog记录功能。

COMLog支持列表

- B系列：5001B Gen 2。
- C系列：1000，3240，5001C，5101C。
- D系列：300，400，500，600，800，900，1000，1200，1500，3000，3100，3200，3700，3800，3810，3815，3960，3980，5001。
- E系列：300，500，1100，2000，2200，2500，3300，3400，3600，3960，3980，5001（也包含带硬盘型号）。
- F系列：400，600，1000，1800，2200，2600，3000，3500，3700，4200，4400，4800，6300，6500，7121（也包含带硬盘型号）。
- G系列：900（也包含带硬盘型号）。
- VM与其他型号：不支持。

开启COMLog

1. 开启/关闭COMLog。

```
diagnose debug comlog <enable|disable>
```
bash

2. 查看COMLog开启状态。

```
diagnose debug comlog info
```
bash

3. 清除记录在Flash中的所有COMLog日志。

```
diagnose debug comlog clear
```
bash

查看COMLog

CLI查看

1. 配置Console输出方式为Standard，一次显示所有输出。

```
config system console
    set output standard
end
```
bash

2. 在CLI下查看已记录的COMLog，并复制到文本文件中。

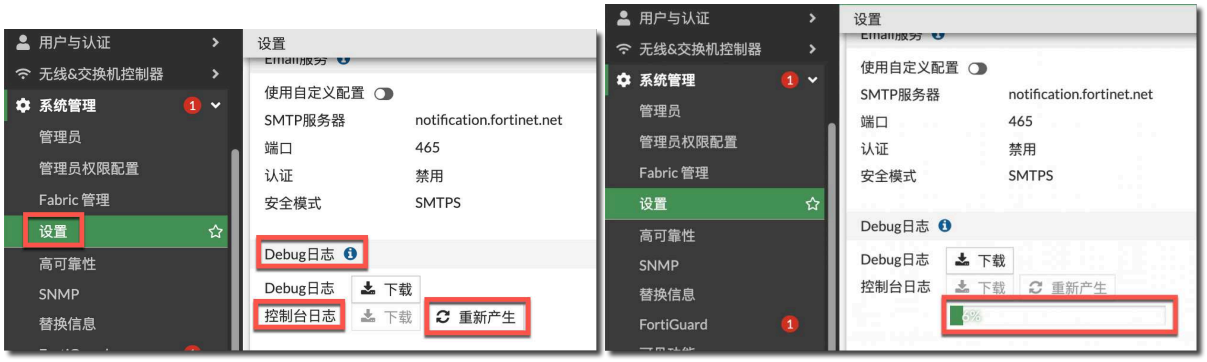
> **重要**
>
> 由于Console的输出速率有限，建议使用SSH或GUI来收集COMLog输出，不要使用Console来输出COMLog。

```
diagnose debug comlog read
```
bash

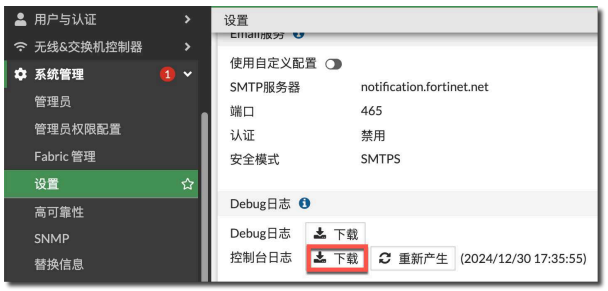
GUI下载

1. 开启COMLog后，进入“系统管理→设置”的“Debug日志”部分，点击“控制台日志”右侧的“重新产生”按钮。FortiGate会开始将Flash中的COMLog复制到GUI缓存中以供下载。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 等待COMLog生成进度完成，点击“下载”按钮。



3. 通过GUI下载到的COMLog文件后缀名为.log，内容为Zlib压缩格式，必须使用Zlib解压工具（如zlib-flate）进行解压，才能看到明文的COMLog。

注意事项

1. 启用COMLog时，请避免配置密码或密钥等机密配置，因为这些密码和密钥会以明文方式记录在COMLog中。可以在配置密码和密钥等配置前禁用COMLog，配置完成后再启用COMLog。

2. 由于Console的输出速率有限，建议使用SSH或GUI来收集COMLog输出，不要使用Console来输出COMLog。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

云部署注意事项

在云平台部署Fortinet相关产品时，请注意您需要承担所使用的资源产生的费用，包括但不限于：CPU、内存、存储卷、快照、数据传输及网络带宽。

当部署的VM正式运行后，系统可能会自动生成临时文件、系统日志或额外的存储卷与快照，这些都可能占用磁盘空间并产生额外费用。

为了帮助您更好地管理成本，建议采取以下措施：

- **定期检查**云环境中运行的收费服务与功能。
- **监控磁盘使用情况**，了解存储卷或快照的生成机制。
- **设置合理的用量限制、配额和预算告警**，以便及时掌握资源消耗情况。
- **配置磁盘空间告警**，并在收到告警后及时调整。

不同云服务提供商提供的管理工具可能有所差异，您可以参考相关云平台官方文档，配置适合的告警、预算及用量控制策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

运维注意事项

请参考运维注意事项↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

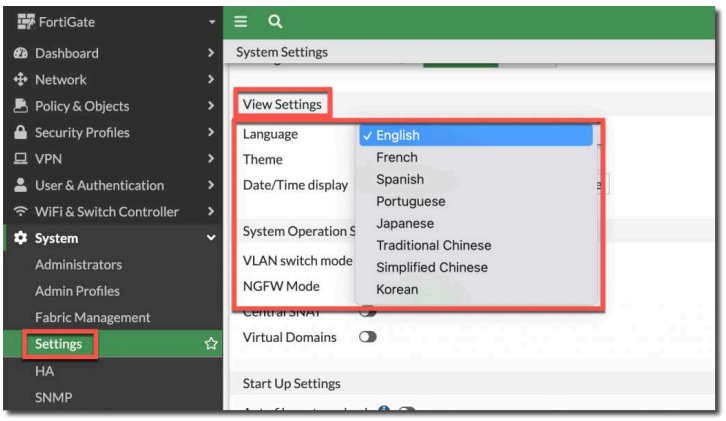
语言/时区切换

简介

- 设备Web界面初始语言为英文，可更改为中文（或其他语言）界面。
- 设备默认时区为`(UTC-12:00) Etc/GMT+12`，可更改为+8区（或其他区）时间。

语言切换

登录Web界面后，进入System→Settings，找到View Settings，修改Language为Chinese即可：

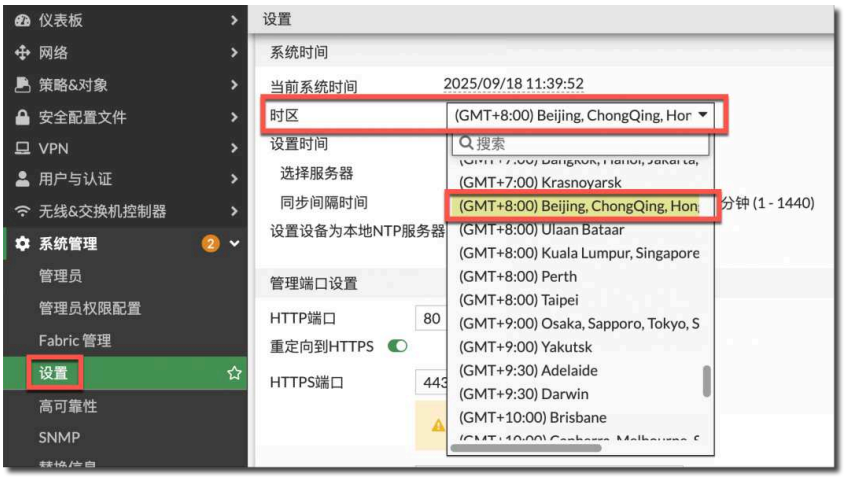



```
FortiGate # config system global
FortiGate (global) # set language ?

english       English.
french        French.
spanish       Spanish.
portuguese    Portuguese.
japanese      Japanese.
trach         Traditional Chinese.
simch         Simplified Chinese.
korean        Korean.
FortiGate (global) # set language simch
FortiGate (global) # end
```

时区切换

FortiOS 7.4之前版本

进入“系统管理→设置”页面，在“系统时间”处修改。

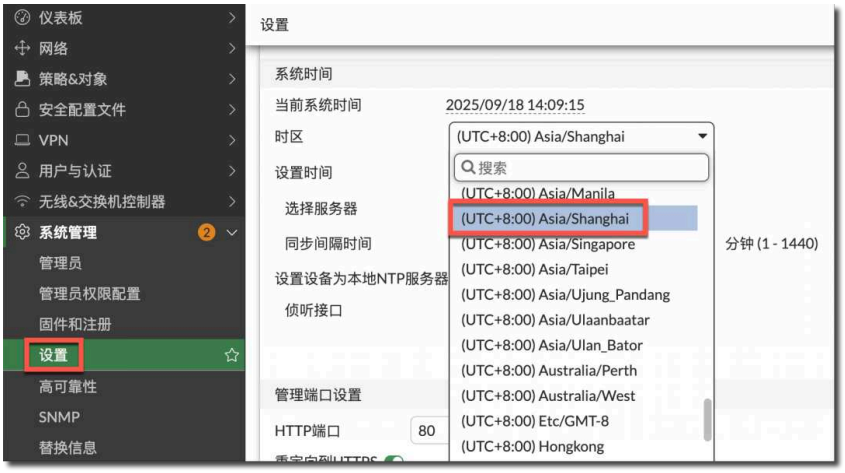


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system global
    set timezone 55
end
```

FortiOS 7.4及之后版本

进入“系统管理→设置”页面，在“系统时间”处修改。




```
config system global
    set timezone "Asia/Shanghai"
end
```

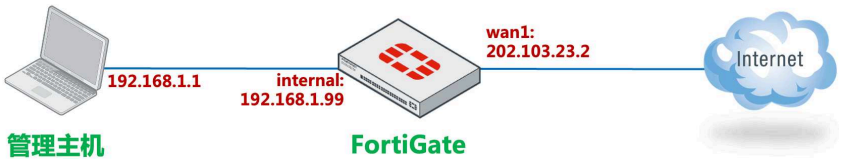

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Web管理

需求

通过web可视化操作界面对防火墙进行配置管理，配置wan1口的管理功能。

组网拓扑



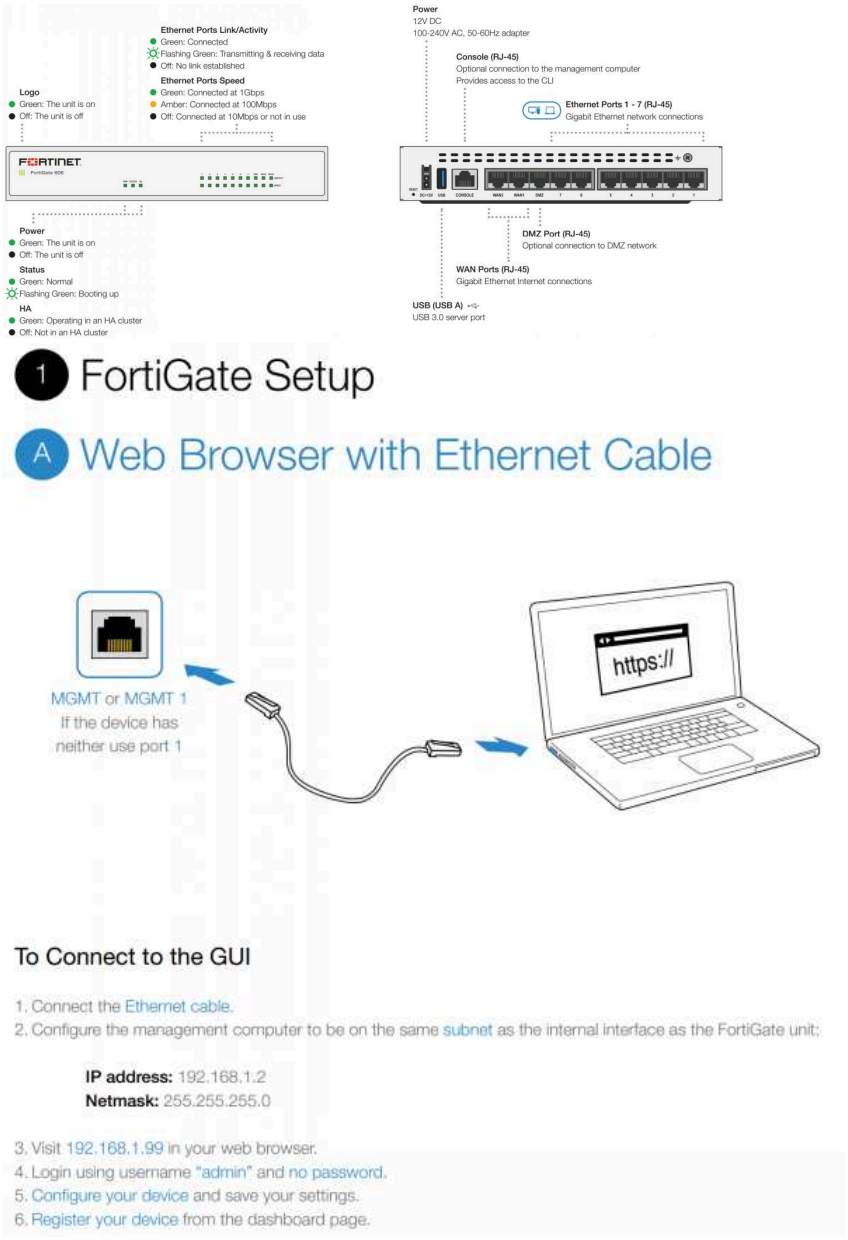
配置要点

1. FortiGate出厂配置默认地址为192.168.1.99，可以通过https的方式进行web管理（默认用户名admin，密码为空），不同型号设备用于管理的接口略有不同。

> **重要**
>
> FortiGate-60F、FortiGate-40F等所有的交换口隶属于三层口internal下，默认配置下，仅有internal接口可以进行三层配置，例如IP配置。
>
> 如需对交换接口（如internal/lan）下的成员接口配置IP，需要将其从交换接口中拿出（取消成员关系）后再单独配置。
>
> 具体的接口管理IP分配需要参考设备出厂包装盒里面的：QuickStart Guide和FortiGate Supplement文档。或者通过docs网站文档搜索获取具体型号的接口信息和登陆管理信息链接：
>
> https://docs.fortinet.com/product/fortigate/hardware ↗
>
> https://docs.fortinet.com/document/fortigate/hardware/fortigate-fortiwifi-60e-poe-qsg-supplement?model=all ↗
>
> https://docs.fortinet.com/document/fortigate/hardware/fortigate-quickstart-guide-high-end?model=all ↗

2. 举例：FortiGate-60E，默认配置下，1、2、3、4、5、6、7均属于internal交换接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 将电脑IP地址设置为192.168.1.2/24（或同网段除192.168.1.99的地址），并连到internal口（举例：FortiGate-60E，默认配置下，1、2、3、4、5、6、7均属于internal交换接口）或者MGMT口，管理主机打开浏览器，输入 `https://192.168.1.99`，用户名：admin，密码：空，进入FortiGate设备页。

> **重要**
>
> 若密码修改后忘记请参照系统管理→管理员配置→密码恢复↗章节进行恢复初始密码。

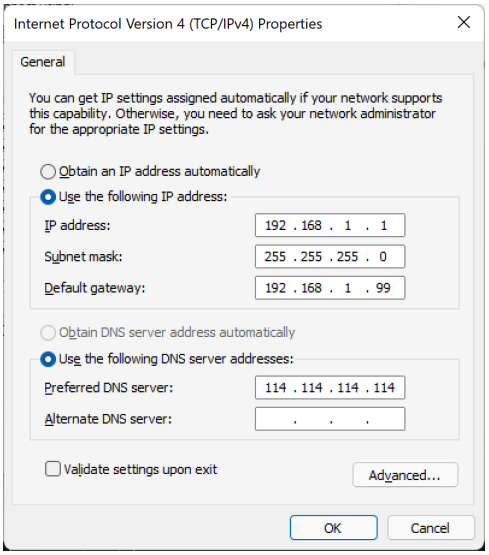
4. 登陆设备后按需配置其他接口的IP和管理功能。默认其他接口是没有IP地址，也未开启HTTPS等其他管理功能。若防火墙接口地址修改过，但忘记相应地址，可进命令行查看当前配置，参考系统管理→常用基础命令↗"章节。

> **重要**
>
> 浏览器建议采用Firefox、Google Chrome、Microsoft Edge。

配置步骤

1. 在FortiGate出厂配置情况下，将电脑设置为192.168.1.1，网关设置为192.168.1.99，如下图：

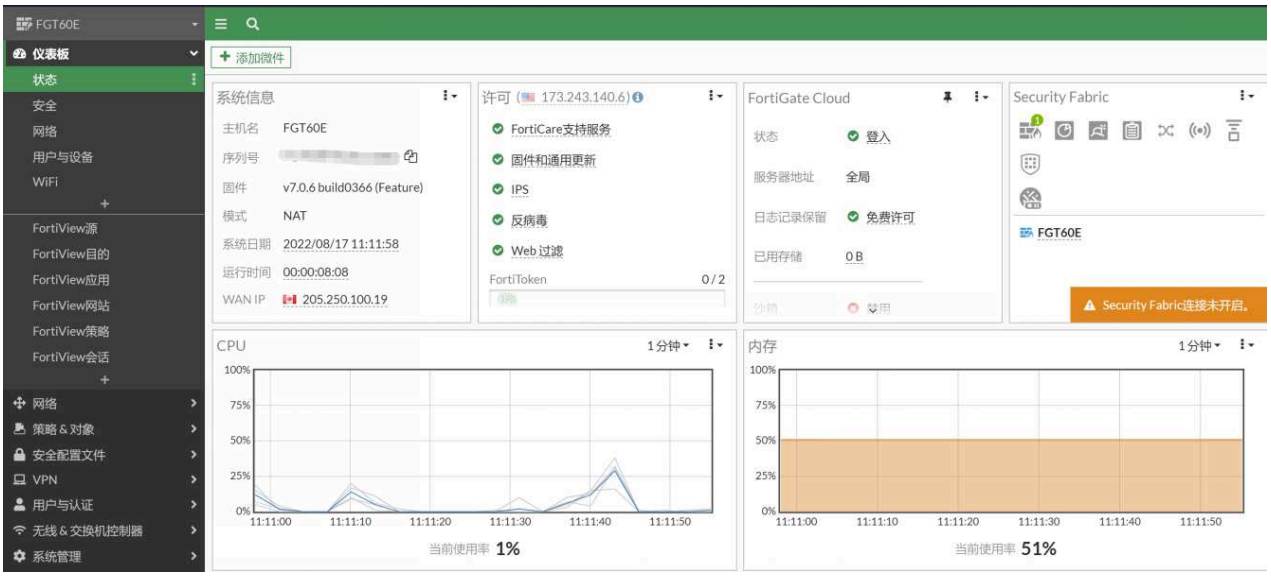
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在IE浏览器里输入`https://192.168.1.99`将出现防火墙登陆的页面。

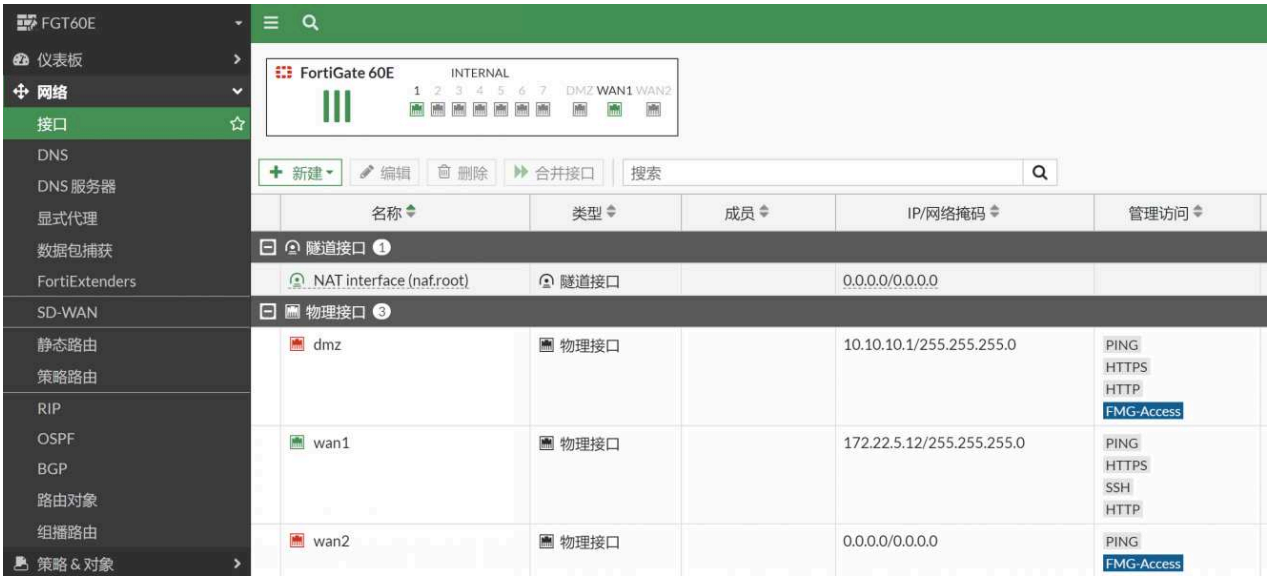


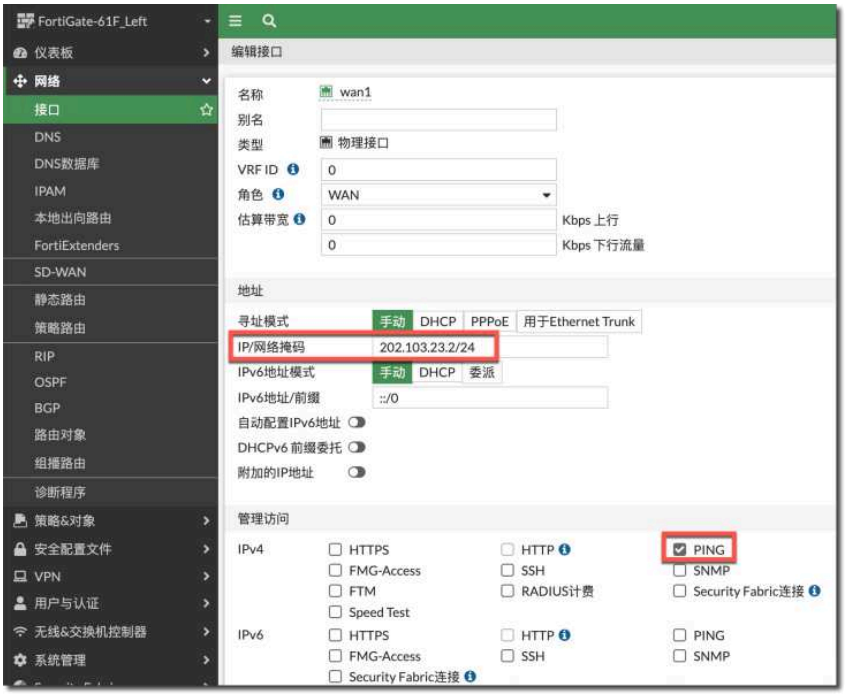
3. 输入用户名admin密码默认空，按照提示设置新的管理员密码后，即可进入防火墙首页。



4. 进入“网络→接口”页面，双击wan1接口进行编辑，配置接口地址为：202.103.23.2/24，管理访问：勾选PING。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





具体各种方式含义如下：

- HTTPS：允许用户用 `https://202.103.23.2` ，进行管理。
- PING：允许用户ping此接口地址，如果不勾选，在路由可达的情况下也Ping不通。
- HTTP：允许用户用 `http://202.103.23.2` ，进行管理。
- SSH：允许用户用用SSH 192.168.0.99方式管理设备。
- SNMP：允许用户通过该接口对设备进行SNMP管理。

验证效果

1. 电脑直连Internal接口的成员接口，电脑网卡IP修改为192.168.1.2，在浏览器里输入： `https://192.168.1.99` ，即可通过internal成员接口登陆管理防火墙。
2. 开启wan1的PING管理协议后，也可以Ping通wan1接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

消除Web证书告警

问题现象

默认配置下，访问FortiGate的Web管理页（GUI）面时，浏览器会弹出告警提示，这是由于FortiGate默认使用的是自签名证书，CA为FortiGate自身，浏览器默认情况下只信任公网权威CA机构颁发的证书，所以自签名的证书会被浏览器认为是不被信任的证书。

> **重要**
>
> 即使用户在管理PC信任了FortiGate Web管理页面证书对应的CA，但由于该证书可能没有SAN（Subject Alternative Name）字段（也可能是SAN属性中没有包含FortiGate的管理IP或域名），访问FortiGate Web管理页面时，浏览器依然会提示告警信息。



解决方法1-使用Fortinet_GUI_Server证书

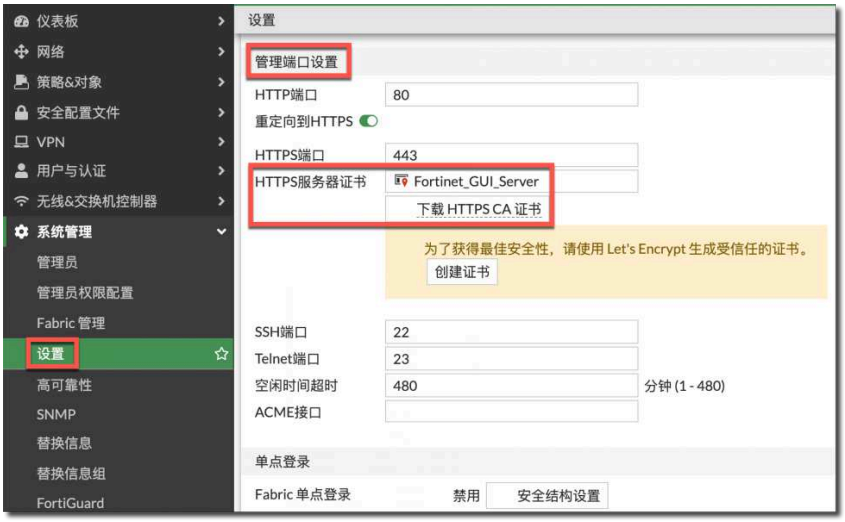
> **重要**
>
> 该方法在FortiOS 7.2.1及以上版本支持。

下载CA证书

1. 在FortiGate的“系统管理→设置”页面的“管理端口设置”部分中，确认“HTTPS服务器证书”选择为“Fortinet_GUI_Server”证书（默认配置会选择此证书）。

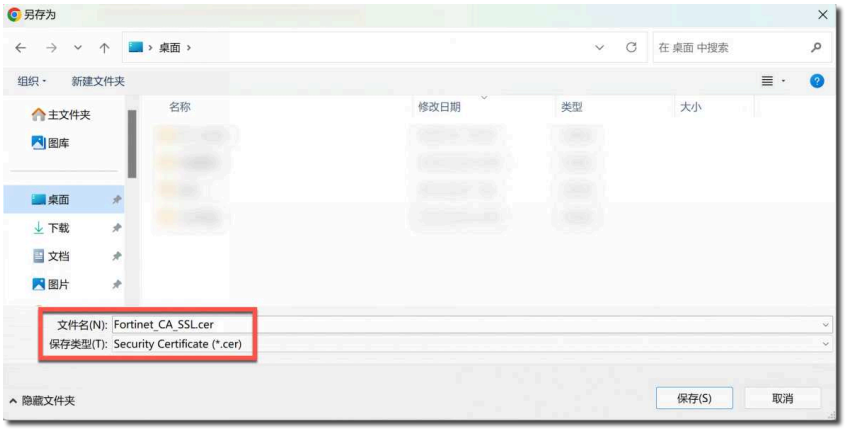
   > **重要**
   >
   > - 如果“HTTPS服务器证书”选择的不是“Fortinet_GUI_Server”证书，请先选择“Fortinet_GUI_Server”证书后点击页面下方的“应用”按钮下发配置。
   > - 如果是HA环境，从所有HA成员下载的CA证书都是一样的，CA证书名称均为第一次成为HA集群主设备的序列号。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

2. 点击“下载HTTPS CA证书”按钮，下载“Fortinet_GUI_Server”证书的CA证书，将CA证书保存在本地磁盘，该CA文件名称一般为“Fortinet_CA_SSL.cer”。



重要

- 当“Fortinet_GUI_Server”证书到期前2天时，FortiGate会重新生成“Fortinet_GUI_Server”证书（客户端PC不需要重新下载并信任Fortinet_CA_SSL）。
- 如果“Fortinet_CA_SSL”证书在FortiGate上过期并重新生成， Fortinet_GUI_Server也会重新生成（客户端PC需要重新下载并信任新的Fortinet_CA_SSL）。

导入和信任CA证书

Windows PC

1. 双击下载的CA证书文件，在安全警告框中点击“打开”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在打开的证书界面点击“安装证书”按钮。



3. 在弹出的“证书导入向导”中选择存储位置（“当前用户仅对此用户生效”，“本地计算机”对所有用户生效），点击下一步按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

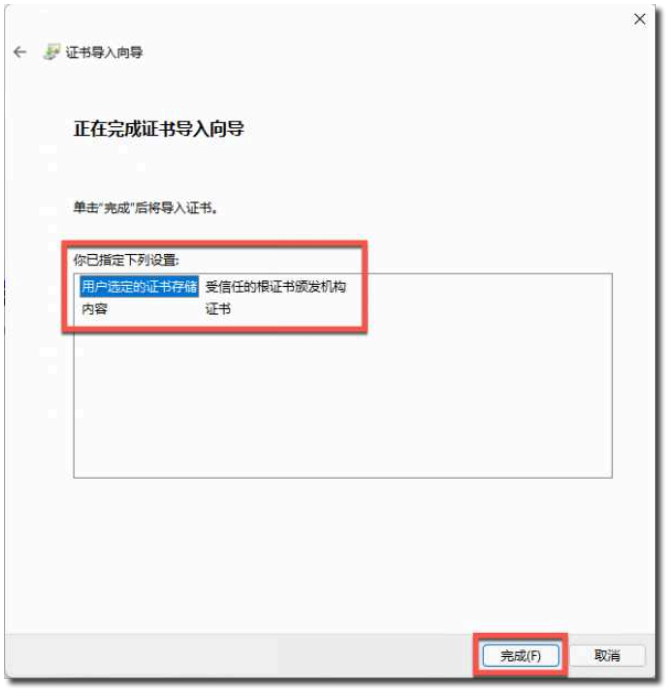


4. “证书存储”选择“将所有的证书都放入下列存储(P)”，点击“浏览”按钮，选择存储到“受信任的根证书颁发机构”中，点击“确定”按钮，随后点击“证书导入向导”的“下一步按钮”。



5. 点击“完成”按钮，完成CA证书的导入向导。

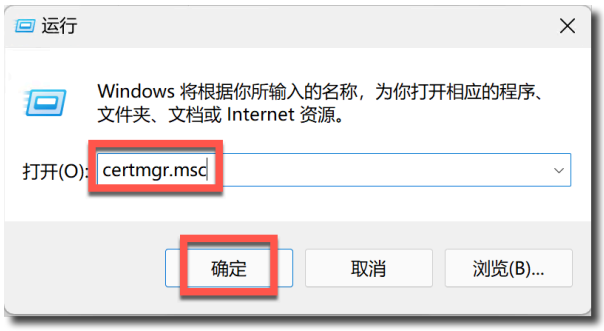
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 随后可能会弹出如下的提示信息，点击“是(Y)”按钮即可成功导入。

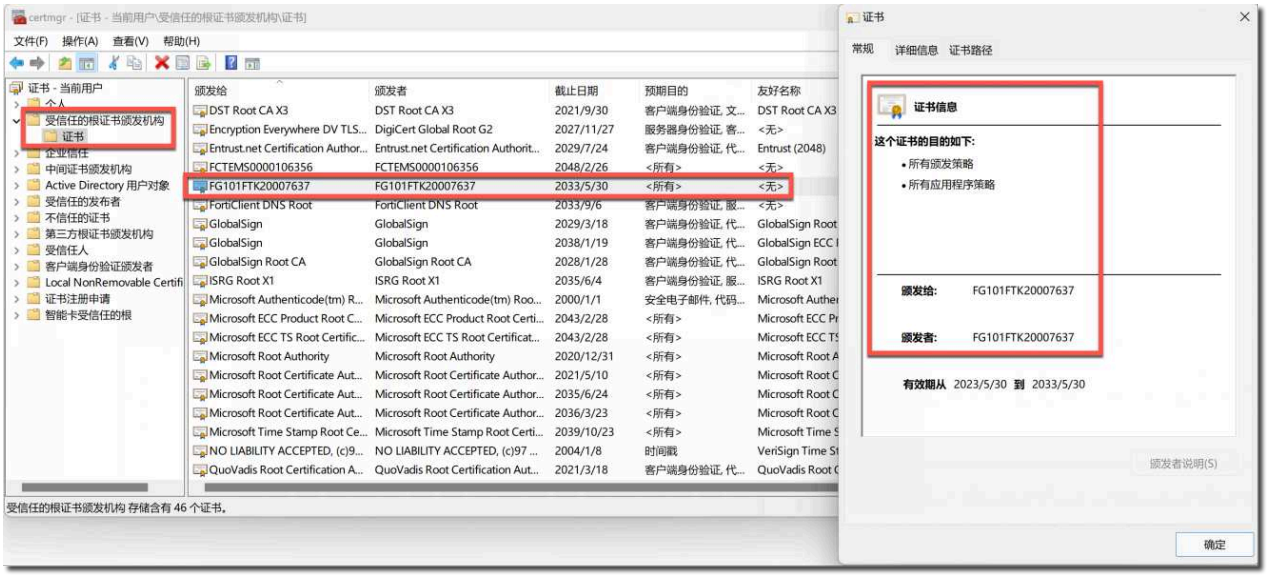


7. 使用Win + R快捷键打开运行窗口，输入“certmgr.msc”，点击确定按钮。



8. 在“受信任的根证书颁发机构”中可以看到以上导入的CA证书，证书的名称为设备的序列号。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



macOS

1. 双击下载的CA证书文件，会弹出“钥匙串访问”窗口（需要系统密码验证），进入“证书”选项页，双击FortiGate的CA证书（或右键点击该CA证书并选择“显示简介”）。

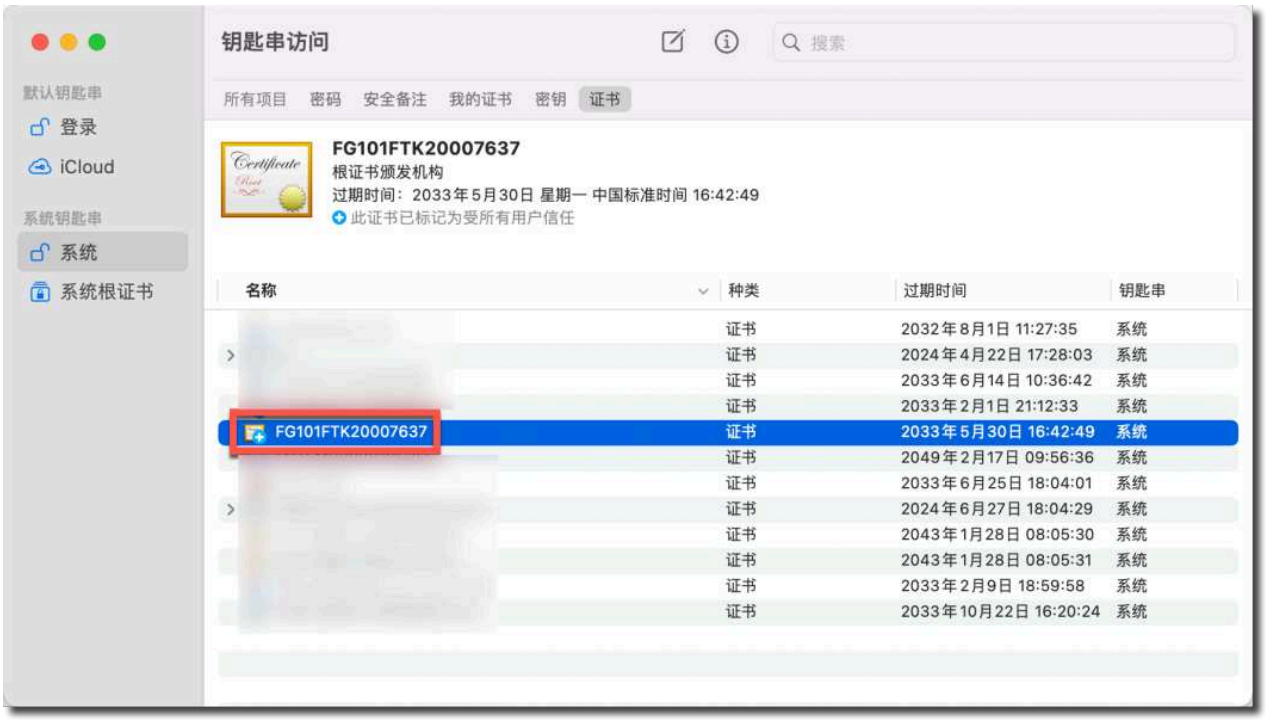


2. 打开该CA证书后，展开“信任”选项卡，修改“安全套接字层 (SSL)”的选项为“始终信任”，然后关闭该窗口（关闭时需要系统密码验证）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 此时证书列表中该CA证书前的✖符号消失，变为✚。



iOS与iPad OS

请参考：https://support.apple.com/zh-cn/102390 ↗

Android

请参考：https://juejin.cn/s/安卓安装根证书 ↗

结果验证

再次使用Chrome/Firefox访问FortiGate的Web管理页面（需要清除该站点的Cookie），不会再产生证书告警，浏览器显示“连接是安全的”。

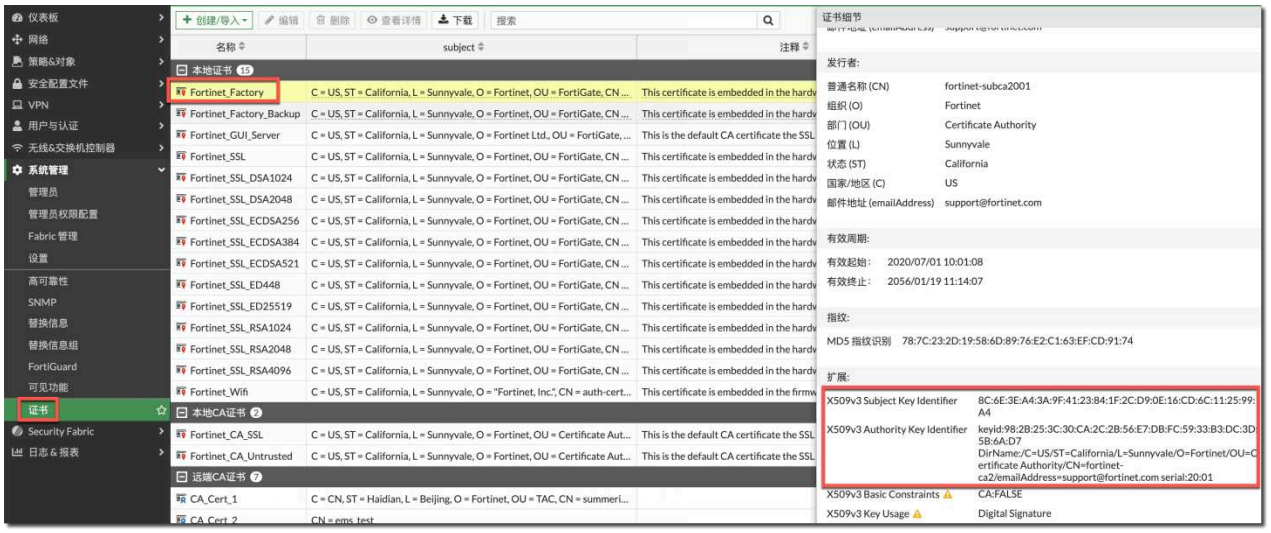
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



实现原理

1. 现在的主流浏览器在验证网站证书时，不仅会检查网站证书的CA证书是否受信任，也会检查网站证书的SAN（Subject Alternative Name）字段是否包含访问该网站时使用的IP或域名。

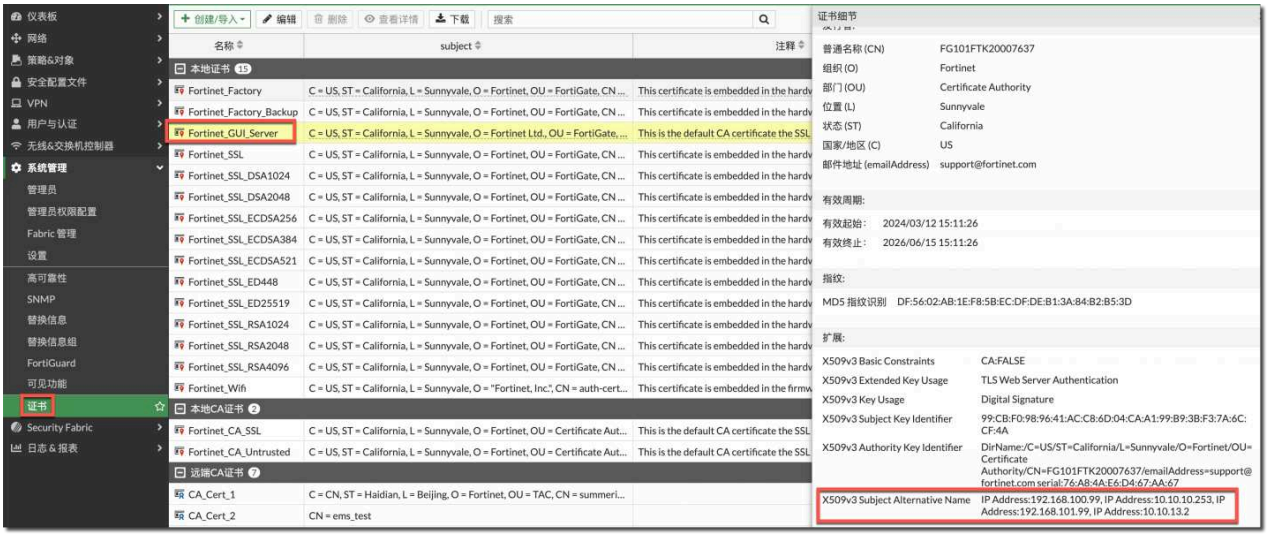
2. 使用其他非“Fortinet_GUI_Server”的内置证书（如Fortinet_Factory）作为Web管理页面的证书时，即使用户在管理PC导入了对应的CA作为“受信任的根证书颁发机构”中的一员，但由于该证书没有SAN字段（如下图所示），访问FortiGate Web管理页面时，浏览器依然会提示告警信息。



3. 当使用“Fortinet_GUI_Server”作为Web管理页面的证书，FortiGate会自动将设备的所有管理IP添加到“Fortinet_GUI_Server”证书的SAN（Subject Alternative Name）属性中（如下图所示），当管理PC导入了对应的CA作为“受信任的根证书颁发机构”中的一员，浏览器检查Web管理页面中的SAN包含页面IP，就认为该证书是受信任的。

> **重要**
>
> 只有开启了HTTPS访问的接口IP会被添加到“Fortinet_GUI_Server”证书的SAN属性中。当接口关闭HTTPS访问后，对应的IP也会从SAN字段中删除。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



解决方法2-导入第三方证书

1. 通过其他证书颁发机构（CA）为FortiGate颁发证书，颁发的证书中的SAN（Subject Alternative Name）字段必须包含FortiGate的管理IP或域名（颁发和导入过程请参考：系统管理→系统设置→证书管理 ↗章节）。

> **重要**
>
> 如果FortiGate的管理IP或域名发生变化，则需要重新为FortiGate颁发包含对应SAN的证书。

> **重要**
>
> 通过CSR的方式配置SAN时，注意CSR配置中请求的SAN的格式，如下举例：
>
> 域名：`DNS:www.fortinet.com.cn`
>
> IP地址：`IP:10.10.12.1`

2. 在FortiGate的“系统管理→设置”页面的“管理端口设置”部分中，将“HTTPS服务器证书”选择为上步导入的证书。

3. 管理PC信任该证书所属的CA（参考上述方法，如果CA为公网公认的权威CA，则不需要手动信任）。

解决方法3-使用Let's Encrypt颁发证书

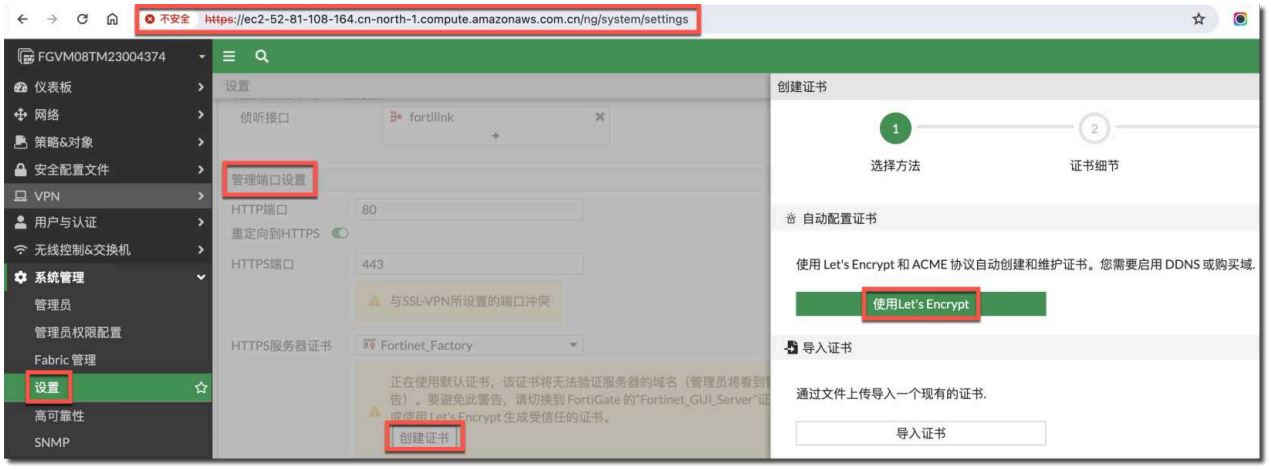
> **重要**
>
> 使用该方法有以下要求：
>
> - FortiGate必须有公网IP和对应的公网域名（或是在Internet设备上将公网IP映射到FortiGate）。
> - FortiGate的公网接口必须面向Internet开放TCP 80和443端口，以便FortiGate能够侦听ACME更新请求。 该接口不能配置任何VIP，也不能在端口80或443上进行端口转发。
> - 颁发的证书中的SAN（Subject Alternative Name）属性会自动填充FortiGate的DNS主机名，无法编辑，不能使用通配符，不能添加多个SAN字段。
> - FortiGate必须能够访问acme-v02.api.letsencrypt.org ↗， 这个域名是证书服务的提供商Let‘s Encrypt的地址（默认）。
> - 此方法创建的FortiGate证书不需要管理PC将CA证书导入本地的“受信任的根证书颁发机构”。
> - FortiGate注册的域名需要在国内备案，否则可能出现注册过程被ISP或云运营商阻断的情况。

配置步骤

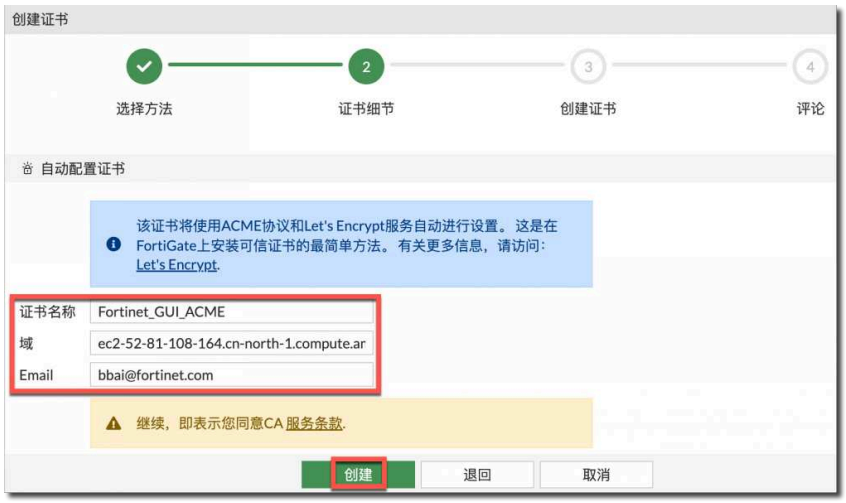
1. 如下图所示，FortiGate的管理域名为`ec2-52-81-108-164.cn-north-1.compute.amazonaws.com.cn`（注意该域名必须在Internet的DNS服务器上可以解析）。

2. 现在使用浏览器访问时，会有“不安全”的标识。在FortiGate的“系统管理→设置”的“管理端口设置”中，点击“创建证书”按钮，在右侧弹出的“创建证书”窗口中，点击“使用Let's Encrypt”，通过向导为FortiGate创建公有CA颁发的证书（该功能免费）。

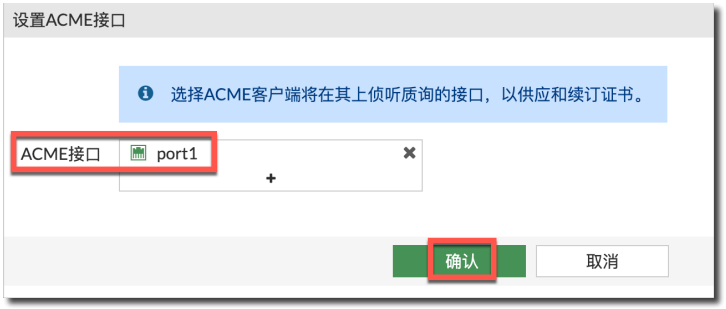
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在右侧弹出的“创建证书”窗口中，填写证书名称，“域”填写FortiGate的管理域名，填写Email信息，点击“创建”按钮。

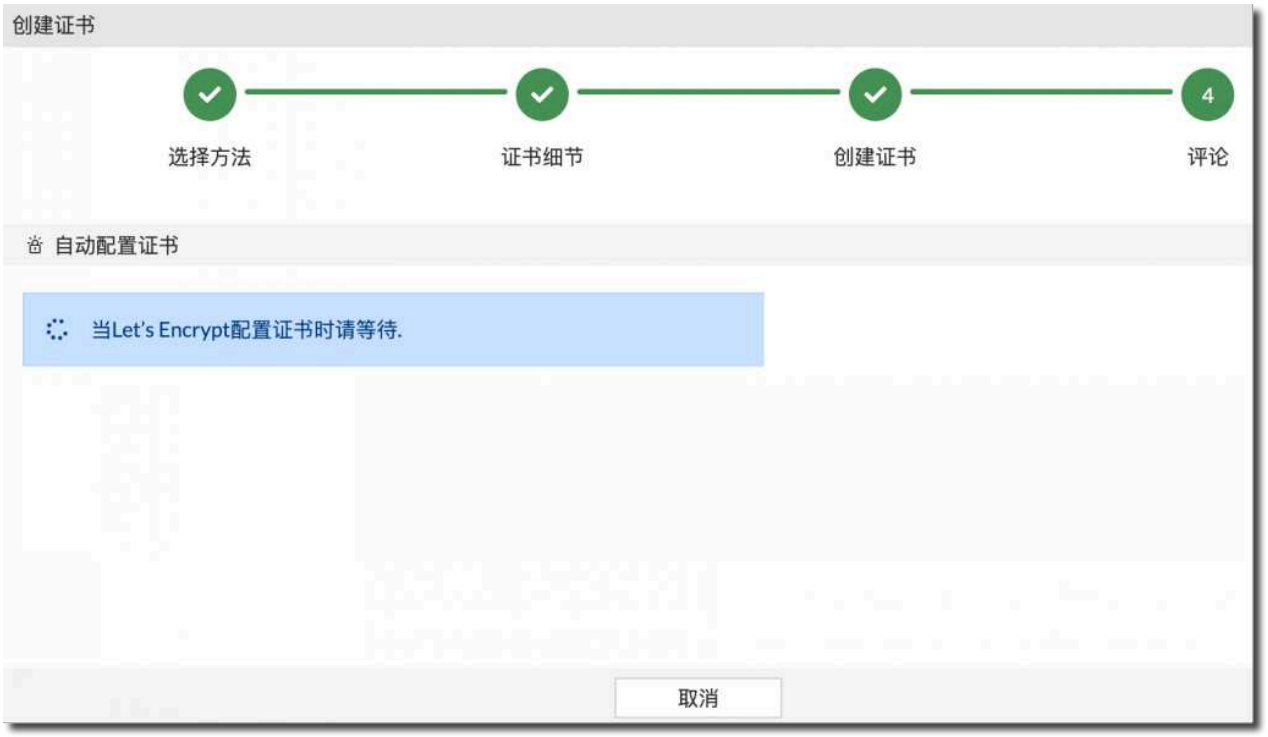


4. 在弹出的“设置ACME”窗口中，选择“ACME接口”为FortiGate的公网接口，点击“确认”按钮。



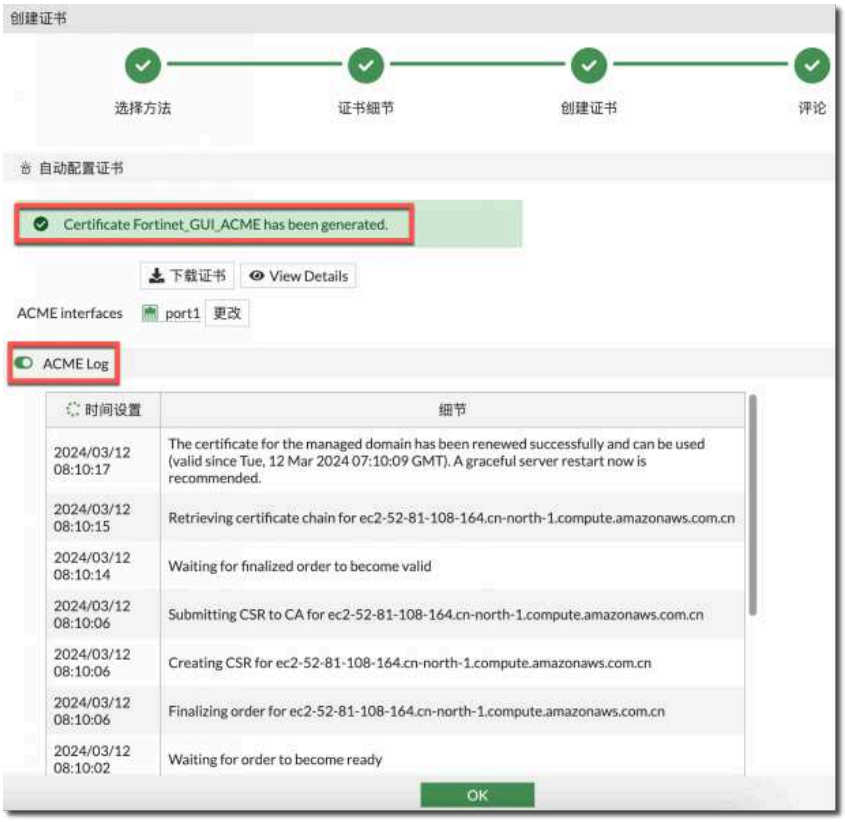
5. 耐心等待证书配置完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



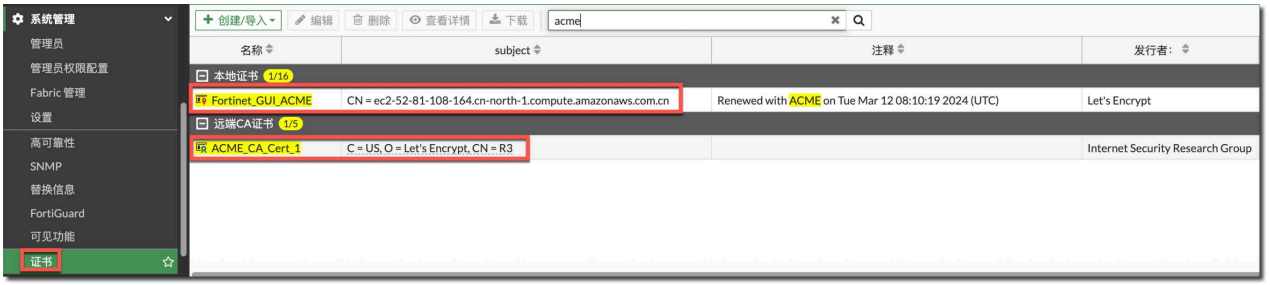
6. Let's Encrypt证书创建完成。

> **重要**
>
> 如果创建失败，可以点击“ACME Log”检查创建过程中的报错信息。



7. 证书的管理界面中除了生成了申请的“Fortinet_GUI_ACME”证书外，还有一张中间CA证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config vpn certificate ca
    edit "ACME_CA_Cert_1"
        set range global
    next
end

config vpn certificate local
    edit "Fortinet_GUI_ACME"
        set password ENC
jWTgiiU41fD+Mi94XyBXAY2ZY2wc+syGDVfIAEXKYRSwX2s30XJuR4sPybF+SNgKrWKDSp4tBxWunSNTMAjloZxtYZY1ieXOPPWQqkLtrZHuPZbRWx
TBzl8hJm4ZeYxnh5xcN0hLjX4PXELjgIcQWv9fDE2B8YyJPzZDeL5FgSYA+tlM9670nfzlO9CbGIpQXqRGHw==
        set comments "Renewed with ACME on Tue Mar 12 08:10:19 2024 (UTC)"
        set range global
        set enroll-protocol acme2
        set acme-domain "ec2-52-81-108-164.cn-north-1.compute.amazonaws.com.cn"
        set acme-email "bbai@fortinet.com"
    next
end
```

8. 在“系统管理→设置”页面的“管理端口设置”部分中，将“HTTPS服务器证书”选择为Let's Encrypt创建的证书“Fortinet_GUI_ACME”。




```bash
config system global
    set admin-server-cert Fortinet_GUI_ACME
end
```

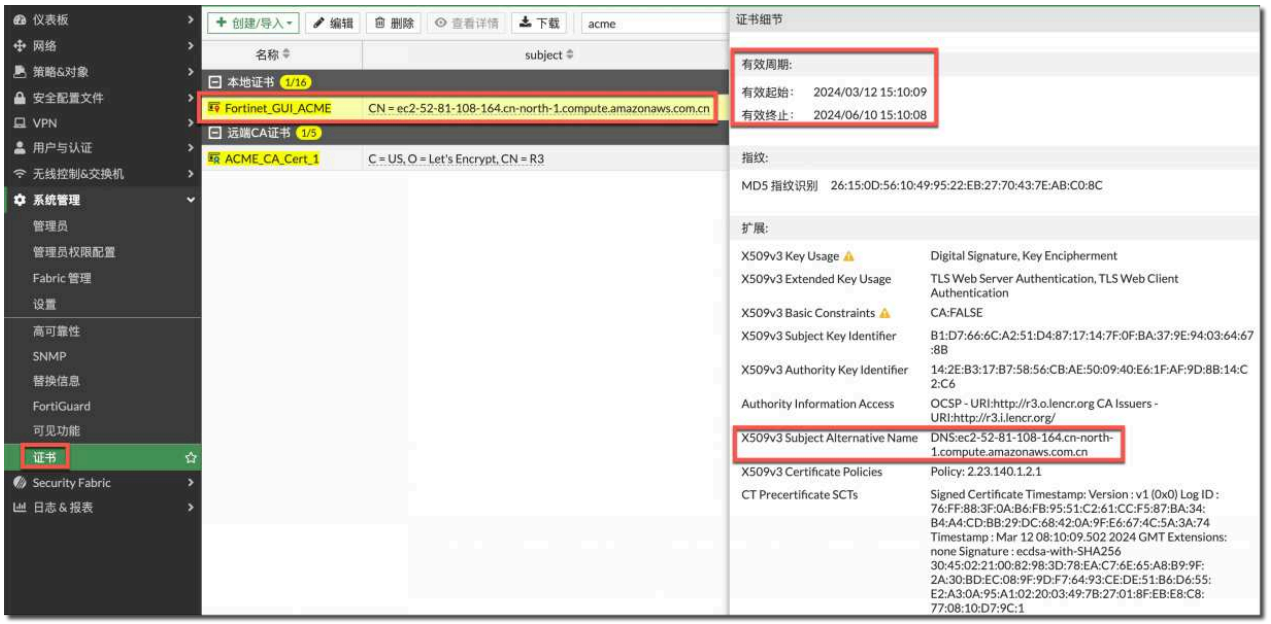
结果验证

1. 再次使用Chrome/Firefox访问FortiGate的Web管理页面（需要清除该站点的Cookie），不会再产生证书告警，浏览器显示“连接是安全的”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 申请到的Let's Encrypt证书中的SAN字段包含FortiGate的管理域名，有效期为90天，到期时间2天前会自动续期。



相关调试CLI

1. 查看FortiGate ACME状态。

> **重要**
>
> ACME hallenge type是根据FortiGate的当前配置自动选择的。 当端口443是可用状态（不被GUI、SSL VPN、Portal等使用）时，它更喜欢使用tls-alpn-01挑战，否则使用TCP端口80上的http-01挑战。 如果GUI在端口80上运行，并且在所选的接口上设置了HTTP访问权限，那么http-01挑战将由节点代理转发，否则Apache将直接监听端口80，只监听ACME。

```bash
FortiGate # get system acme status
Listening on interfaces:        port1
ACME certificates registered:   1    //注册的证书个数//
ACME challenge type:            http-01    //监听80端口//
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose sys tcpsock | grep :80-
172.31.1.91:80→0.0.0.0:0→state=listen err=0 socktype=1 rma=0 wma=0 fma=0 tma=0 inode=59778 process=152/httpsd
```

2. 查看ACME申请记录日志。

```
FortiGate # diagnose sys acme status-full ec2-52-81-108-164.cn-north-1.compute.amazonaws.com.cn
{
  "name": "ec2-52-81-108-164.cn-north-1.compute.amazonaws.com.cn",
  "finished": true,
  "notified": false,
  "last-run": "Tue, 12 Mar 2024 08:09:20 GMT",
  "valid-from": "Tue, 12 Mar 2024 07:10:09 GMT",
  "errors": 0,
  "last": {
    "status": 0,
    "detail": "The certificate for the managed domain has been renewed successfully and can be used (valid since
Tue, 12 Mar 2024 07:10:09 GMT). A graceful server restart now is recommended.",
    "valid-from": "Tue, 12 Mar 2024 07:10:09 GMT"
  }
......
```
bash

3. 重启与Let's Encrypt通信的Apache服务器。

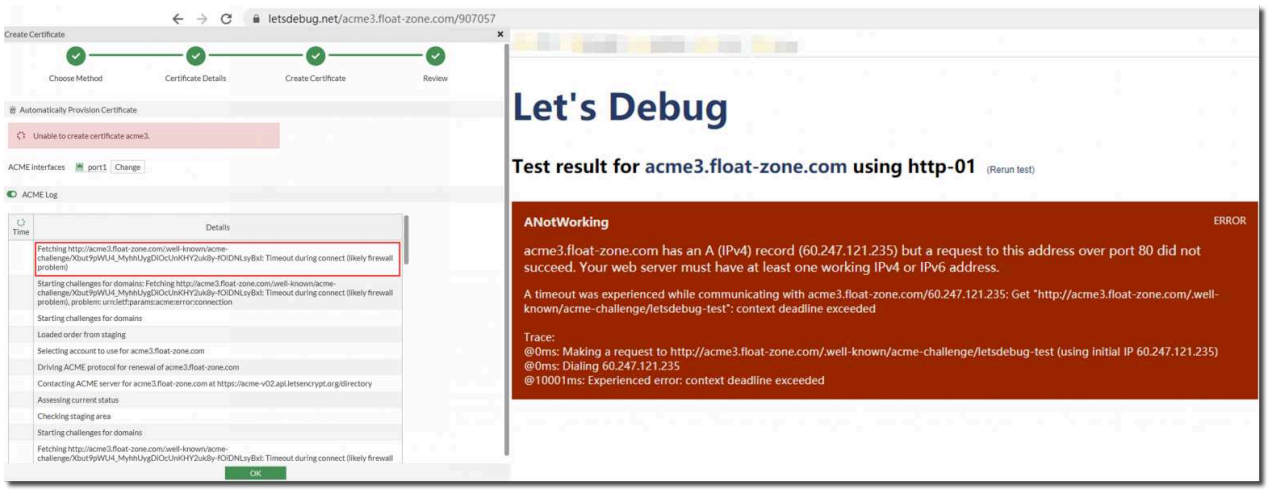
```
FortiGate # diagnose sys acme restart
```
bash

Let's Encrypt申请域名失败举例

检查申请Let's Encrypt证书时页面打印的“ACME Log”。

Let's Encrypt无法主动访问到FortiGate的TCP 80或443端口

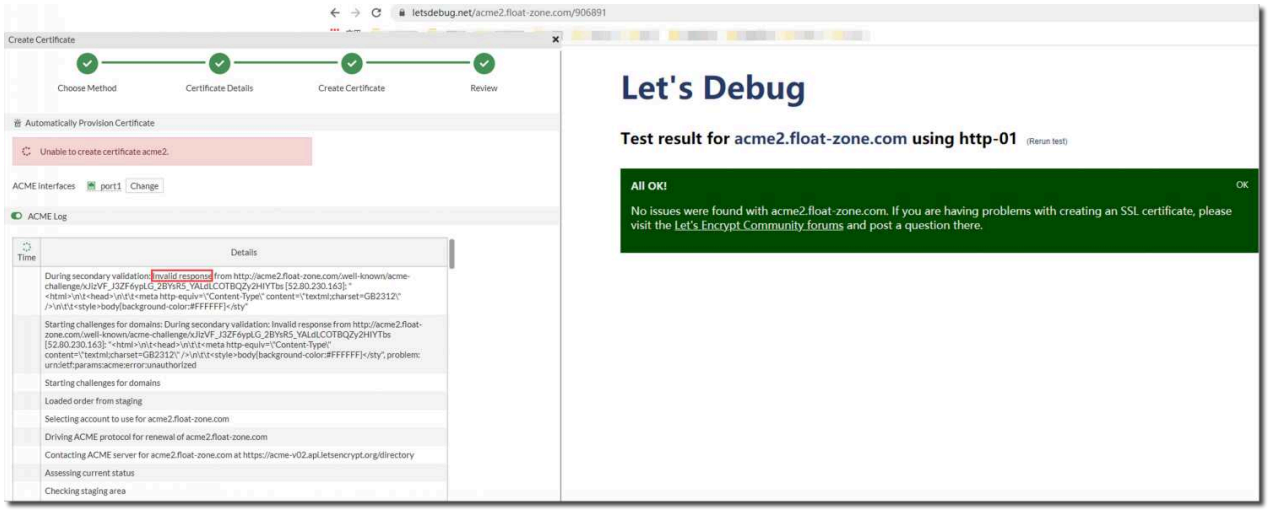
1. 例如使用位于内网的FortiGate（也无无公网IP映射到FortiGate），Let's Encrypt访问不了其TCP 80或443端口，日志提示Timeout during connect（likely firewall problem），通过抓包查看未有Let's Encrypt acme-challenge消息到达FortiGate。
2. Let's Encrypt有一个测试网站https://letsdebug.net/ ↗ ，可以先对FortiGate进行检查。



FortiGate的域名使用了未在国内备案的域名

1. 例如，DDNS域名使用acme2.float-zone.com ↗ ，由于float-zone.com未在国内备案，因此运营商可能会拦截对该域名的请求。FortiGate的ACME Log显示invalid response。
2. 但https://letsdebug.net/ ↗ 检测是正常的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

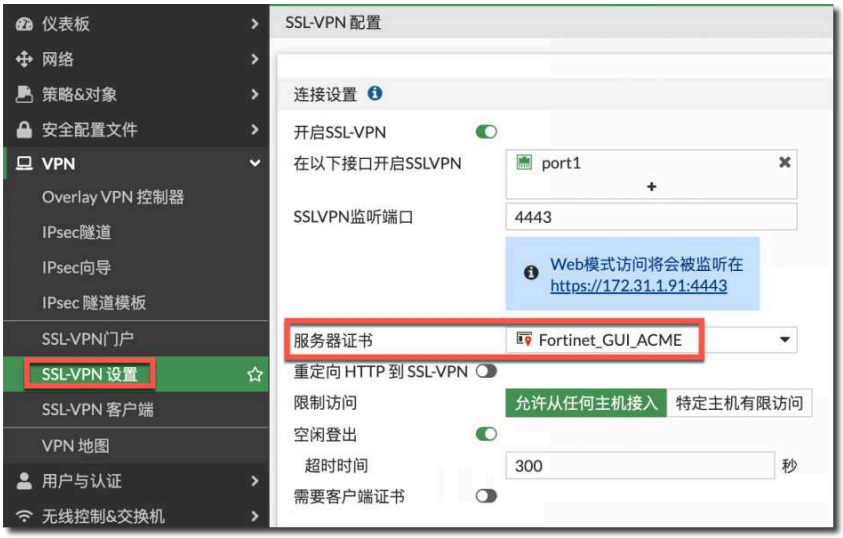


3. 本地使用游览器主动访问FortiGate ACME日志中的域名被拦截。因此ACME日志显示invalid response。



SSL VPN证书

参考方法2或方法3导入设备证书，并在客户端信任对应的CA证书后，在“VPN→SSL VPN→SSL-VPN设置”中选择该证书即可。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config vpn ssl settings
    set servercert "Fortinet_GUI_ACME"
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

关闭Web提示信息

关闭升级提示

当FortiGate有新的固件可以升级时，每次登录页面都会弹出升级固件的提示信息，必须点击“下次再说”才能正常进入管理页面。



通过如下CLI可关闭“升级固件”的提示信息。

```bash
config sys global
    set gui-firmware-upgrade-warning disable
end
```

关闭注册提示

当FortiGate未注册时，每次登录页面都会弹出升级固件的提示信息，必须点击“下次再说”才能正常进入管理页面。



通过如下CLI可关闭“注册FortiCare”的提示信息。

```
config sys global
    set gui-forticare-registration-setup-warning disable
end
```

关闭FortiConverter提示

从FortiOS 7.4开始，登录FortiGate时会提示使用FortiConverter进行配置转换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



通过如下CLI可关闭FortiConverter的提示信息。

```bash
diagnose sys forticonverter set-prompt-visibility hidden
```

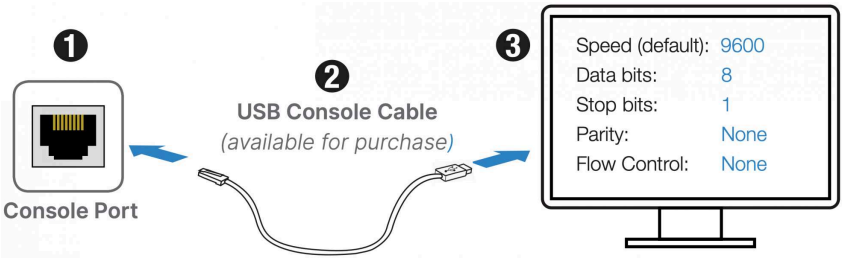

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Console管理

功能需求

若需要进入命令行进行配置管理，可通过Concole线，使用Putty/SecureCRT/XSHELL等终端软件进入CLI界面，防火墙默认允许Concole管理。

组网拓扑

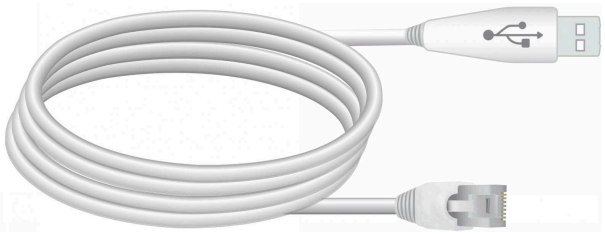


配置要点

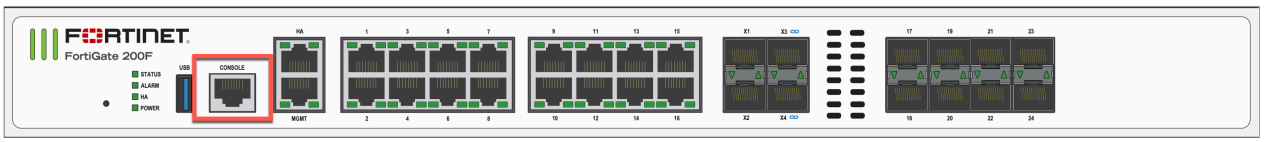
1. 准备配置线及可连Console线的PC（根据不同的Console线种类，可能需要自行安装Console线驱动，部分型号的FortiGate会随箱包含一条USB→Console线缆）。
2. 连接Console线。Console线的水晶头端连到设备的concole口上，另一头连电脑的USB接口。
3. 配置终端软件，如Putty、SecureCRT、XSHELL。

配置步骤

1. 准备Console线及PC。Console线一头类似网线水晶头（接在FortiGate的Console口上），另一头为USB接口，如下图所示。

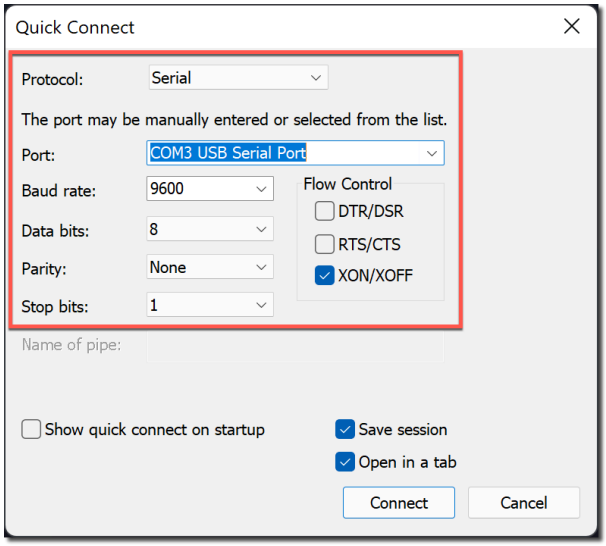


2. 连接配置线，将Console线水晶头一端插入网络设备的Console接口（Console口一般位于网络设备的网络接口旁，其上都会标有字母CONSOLE），然后将Console线的USB接口端连接PC。



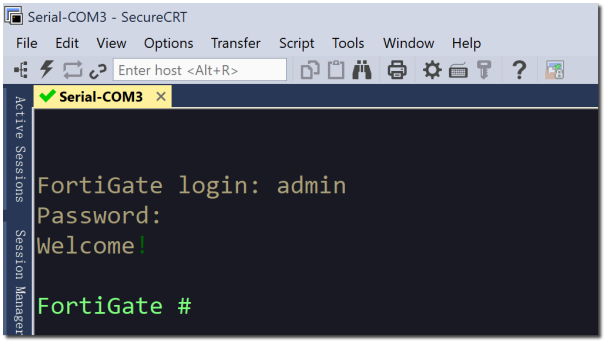
3. 连好配置线后，配置终端软件，Protocol选择“Serial”，Baud rate设置为9600，Data bits设置为8，Stop bits设置为1，这里以SecureCRT为例。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



结果验证

按回车键，则会打印出“FortiGate login：”提示输入用户名及密码（设备出厂默认用户名为admin密码为空，如果密码有改过，且忘记了，可参考"系统管理→管理员配置→密码恢复"恢复密码。



注意事项

若设置后无法进入命令行，请检查：

- Console线是否连接在concole口。
- 终端软件的波特率是否配置为9600，Data bits设置为8，Stop bits设置为1。
- 在“硬件管理器”中检查COM接口是否为“未识别设备”，如果是，可能是缺少驱动程序，需要安装Console线驱动程序（Windows 10/Windows 11一般不需要安装，驱动程序可从Console线经销商处获取）。
- 如果以上操作都对还是无法进入，请尝试更换电脑、Console线及终端软件，或联系Fortinet技术支持。

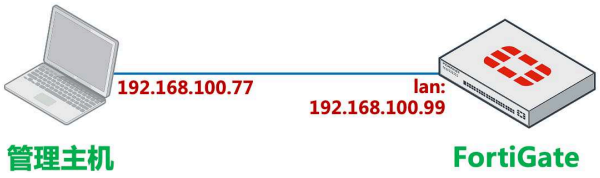
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSH/Telnet管理

功能需求

当需要进设备的命令行进行配置或收集信息，但没有配置线，或不在设备旁边时，可通过远程SSH或Telnet对设备进行管理。

组网拓扑



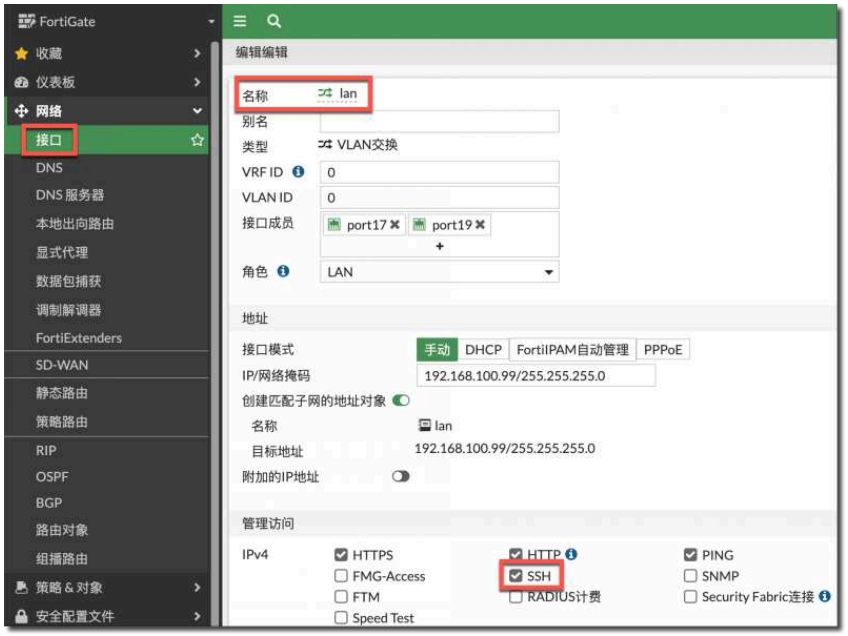
配置要点

使用SSH/Telnet方式管理首先要保证管理主机到设备的接口地址的连通性，可把接口的PING功能勾选，若能PING通管理接口则说明连通性没问题：

1. 开启接口 SSH、TELNET功能。
2. SSH管理设备。
3. TELNET管理设备。

配置步骤

1. 开启接口SSH管理功能，进入“系统管理→网络→接口”， 编辑lan（双击lan接口）接口，在“管理访问”中，勾选SSH。



2. 在7.0以后版本中，Telnet管理必须通过CLI开启，由于Telnet为明文传输，从安全性考虑，建议只开启SSH即可。

> **重要**
>
> 添加Telnet管理协议时，使用append命令将telnet协议附加上去即可（不会改变原有的管理协议），不要使用set命令，使用“set allowaccess telnet”会将原有允许的管理协议清空。

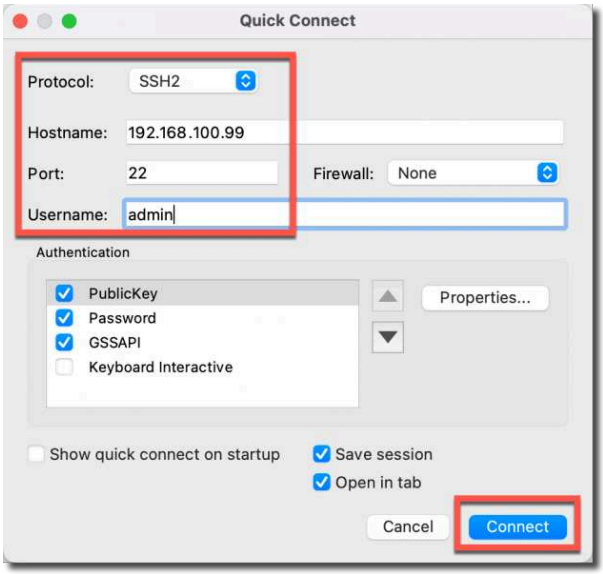
```
FortiGate # config system interface
FortiGate (interface) # edit lan
FortiGate (lan) # append allowaccess telnet
FortiGate (lan) # end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

SSH管理

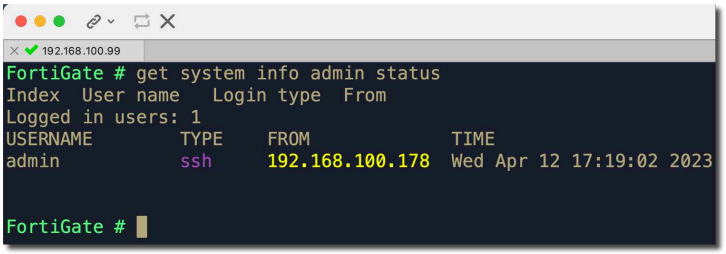
1. 使用终端软件（如SecureCRT）新建一个SSH连接，以下以Secure CRT软件为例。Protocol选择SSH2，Hostname输入设备的管理地址192.168.100.99（即lan口对应的IP地址），端口号22，其他保持默认值，点击Connect。



2. 输入管理员密码（用户名密码与Web登录的一致），点击OK。



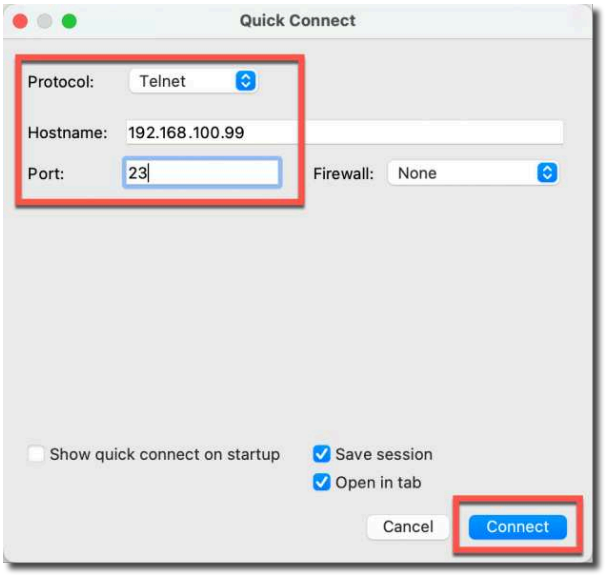
3. 登录设备进行CLI管理。



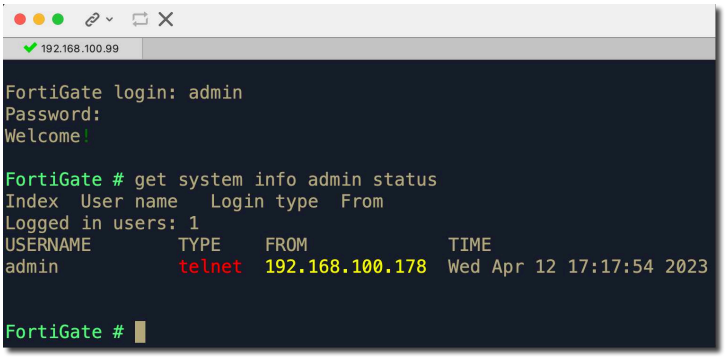
Telnet管理

1. 使用终端软件（如SecureCRT）新建一个SSH连接，以下以Secure CRT软件为例。Protocol选择Telnet，Hostname输入设备的管理地址192.168.100.99（即lan口对应的IP地址），端口号23，其他保持默认值，点击Connect。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 输入用户名和密码（用户名密码与Web登录的一致），登录设备进行CLI管理。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

产品生命周期

产品生命周期简介

Fortinet会定期淘汰旧产品，以支持创新与新技术的发展。本政策适用于以下类别：

- 硬件产品及其相关服务（如FortiCare、FortiGuard）
- 软件产品（包括FortiOS、FortiClient等）
- 设备型订阅服务（如FortiGuard）
- 独立服务（Stand-alone Services），例如高级技术支持（Premium Technical Support）

生命周期阶段

Fortinet的产品生命周期由多个关键节点组成，每个节点定义了产品销售与支持状态的变化：

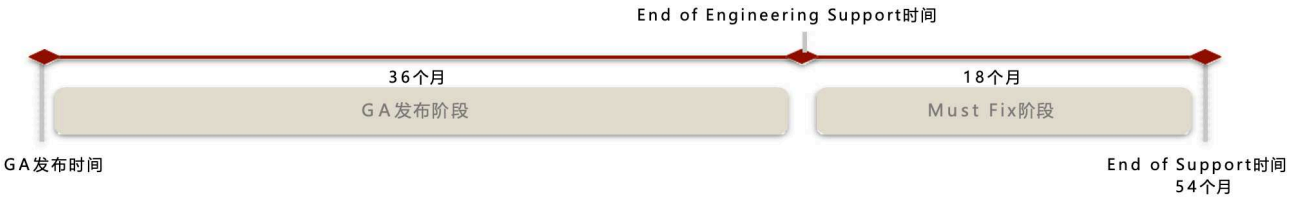
阶段	英文缩写	含义与说明
产品正式发布	GA（General Availability）	产品向公众开放销售，可购买支持合同
终止声明	EOLN（End of Life Notification）	Fortinet发布停止销售与支持的公告，通常包含替代产品建议 对于固件，EOL日期通常在GA发布时即给出
停止订购	EOO（End of Order）	产品最后可下单日期，通常在公告前至少90天通知 对于独立服务，EOO即Last Extension Date
最后服务续约日期	LSED（Last Service Extension Date）	软件/硬件：合同续期不得超过EOS LSED为EOS前12个月 独立服务：LSED为EOL公告后90天
终止工程支持	EOES（End of Engineering Support）	Fortinet不再提供常规软件工程支持 仅对行业级关键问题与PSIRT漏洞进行必要修复（must-fix） 通常为GA后36个月
最终固件版本	FFR（Final Firmware Release）	指定硬件所支持的最后固件版本，维持must-fix状态直到EOS
支持终止	EOS（End of Support）	生命周期最后阶段，Fortinet不再销售、制造或提供支持服务

生命周期时长

产品类型	生命周期主要阶段	持续时间
硬件产品	从EOO起至EOS	60个月（约5年）
软件产品	从GA起至EOS	54个月（约4.5年）
独立服务（Stand-alone Services）	到服务合同终止	按合同期限
工程支持终止（EOES）	从GA起	36个月
服务续约截止（LSED）	EOS前	12个月（独立服务为EOL公告后90天）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

软件与固件



硬件与FortiCare服务



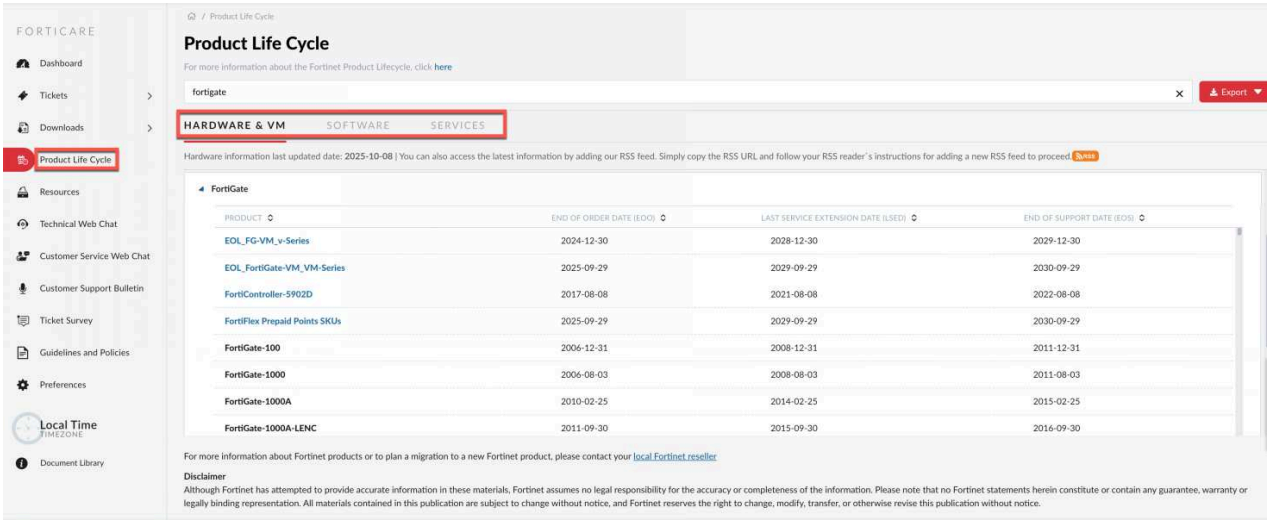
独立服务



查询生命周期

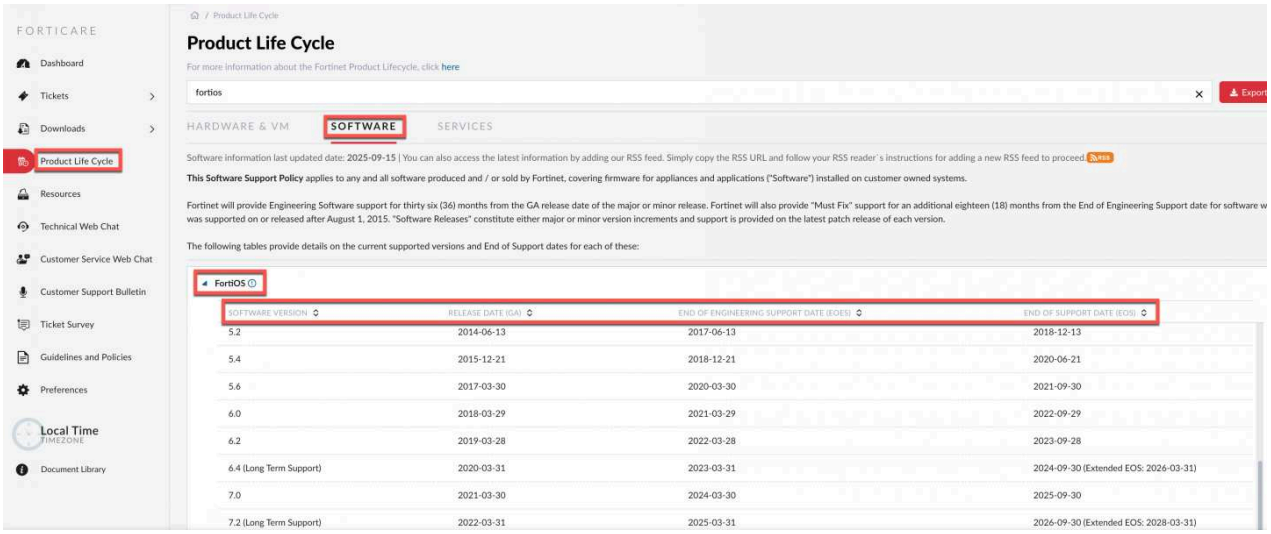
1. 使用设备注册的FortiCloud账户登录https://support.fortinet.com/support/#/lifecycle ↗ 。

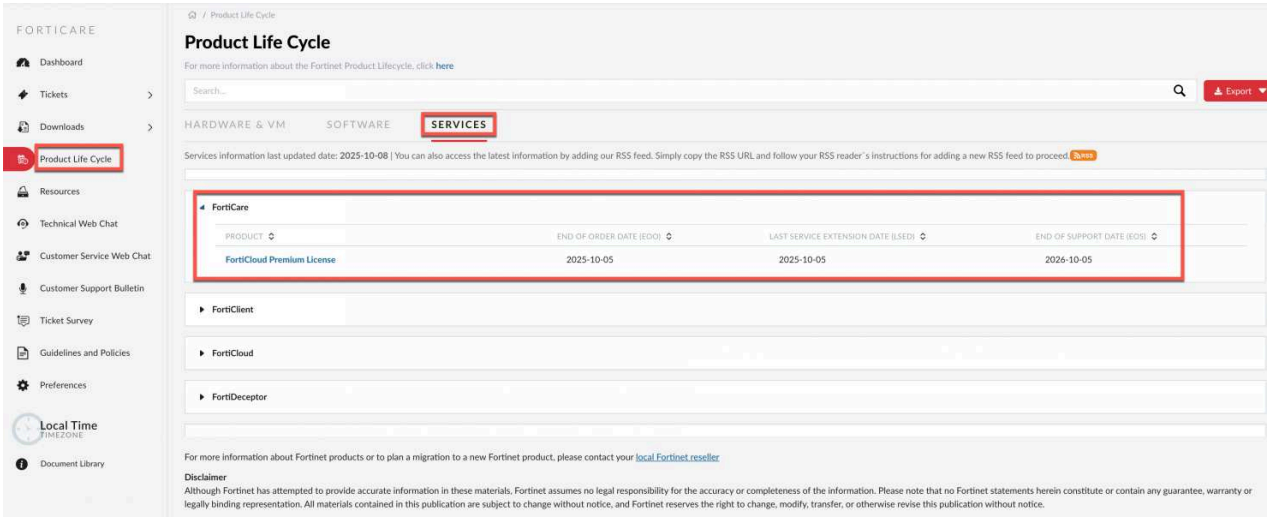
2. 登录后，可以选择不同的分类来查看硬件、软件、服务器的生命周期。



3. 如下所示可以查看FortiOS各个软件版本的生命周期（GA、EOES、EOS）、FortiCare服务的生命周期（EOO、LSED、EOS）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





总结与建议

- 提前规划升级：建议在EOES阶段前（约GA后3年内）规划替换方案。
- 合同管理：关注FortiCare/FortiGuard到期，避免在EOS后尝试续约。
- 风险评估：EOS后继续运行存在安全与合规风险，建议迁移到下一代产品。
- 关注公告：定期检查官方EOL通知，纳入资产与补丁管理流程。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

升级路径

由于不同固件版本之间数据库的差异，FortiGate在升级固件版本时请**务必遵循**升级路径的顺序进行升级，以保证数据库的正确性。

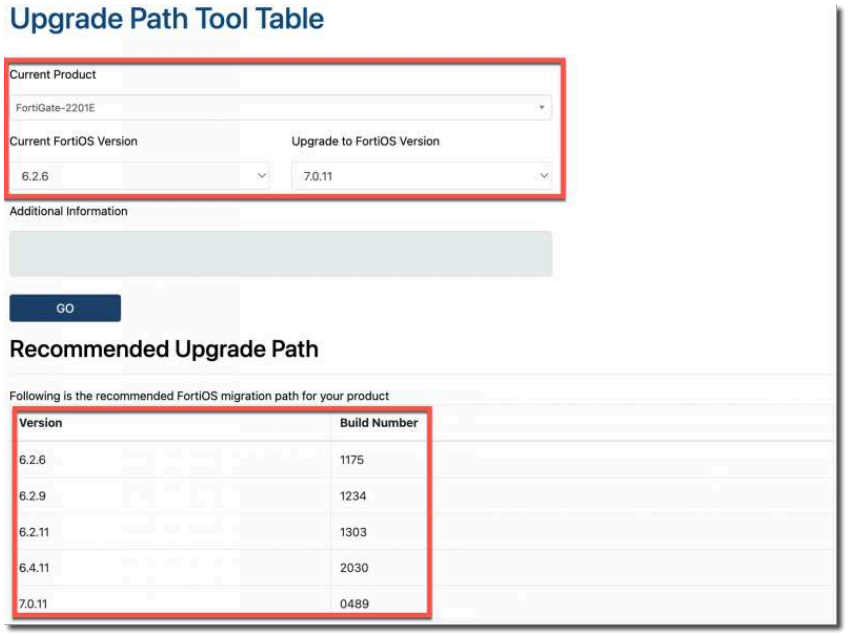
重要

如果不按照升级路径而跨版本升级，可能会导致FortiGate数据库损坏，影响FortiGate的正常运行和功能使用。

FortiGate版本与FortiManager、FortiAnalyzer产品版本的适应关系可通过如下网站查询：https://docs.fortinet.com/compatibility-tool/fortimanager

查询步骤

1. 进入https://docs.fortinet.com/upgrade-tool ，选择要升级的FortiGate型号，选择当前固件版本，和要升级到的目标版本，可以查询到中间的过渡升级版本。



2. 按照查询得出的升级路径，分别下载除当前版本的其他固件版本文件（参考系统管理→固件与配置管理→固件版本管理→固件下载 章节）。
3. 按照查询的升级路径依次升级固件版本，直至升级到目标版本。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Web界面升级

需求

由于当前的软件版本老旧，想要通过web界面升级设备的系统软件版本。

升级要点

重要

- 升级前，务必做好配置备份，参考系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗。
- 升级固件必须遵循升级路径，参考系统管理→固件与配置管理→固件版本管理→升级路径 ↗，前往https://docs.fortinet.com/upgrade-tool ↗ 查询升级路径，否则可能造成配置丢失。

1. FortiGate防火墙的每款型号都有单独的版本文件，升级前务必确认下当前的设备型号。
2. 升级包的后缀名必须为.out，前缀任意。
3. 升级前建议准备配置线，以防在升级失败后能及时处理。
4. 升级过程中请不要切换到其他界面，更不能断电或重启设备，升级过程一般在5分钟以内完成。
5. 版本导入后设备将自动重启，重启才能生效。

升级步骤

1. 登入FortiGate的Web界面，进入系统管理→Fabric管理（7.4为Firmware & Registration页面），右键点击要升级的设备，选择升级按钮。

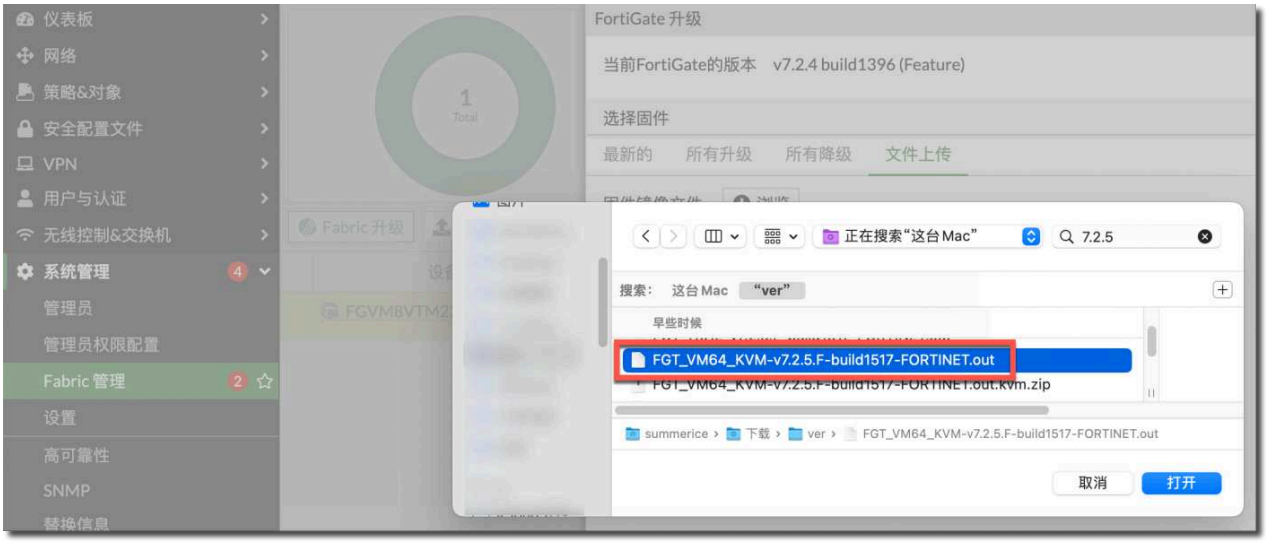


2. 在弹出的页面中，选择文件上传。



3. 点击浏览选择本地固件文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 点击“确认和备份配置”，系统会备份配置文件并自动重启升级。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

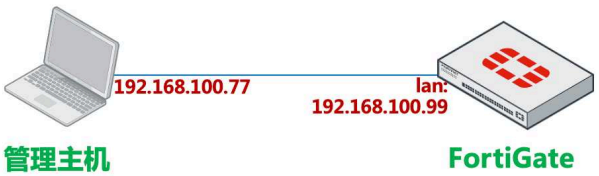
FTP/TFTP/USB方式升级

需求

当不方便通过Web页面管理和升级FortiGate时，可以考虑通过FTP/TFTP/USB等CLI下的方式升级。使用该方法升级同样支持HA不间断升级 ↗。

> **重要**
>
> 升级前，务必做好配置备份，备份步骤请参考：系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗。

拓扑图



配置要点

> **重要**
>
> - 升级前，务必做好配置备份，参考系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗。
> - 升级固件必须遵循升级路径，参考系统管理→固件与配置管理→固件版本管理→升级路径 ↗，前往https://docs.fortinet.com/upgrade-tool ↗ 查询升级路径，否则可能造成配置丢失。

1. 连接网线，保证通讯正常。
2. 搭建好FTP/TFTP服务器，如果使用USB方式升级，需要将包含固件的U盘插入FortiGate的USB接口。
3. 开始升级。

升级方法

FTP/TFTP方式

1. CLI下通过FTP/TFTP的方式升级/导入固件。

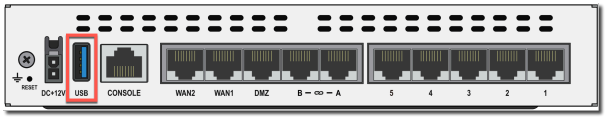
```bash
FTP:
exe restore image ftp <固件文件名称> <FTP服务器IP或域名>[:FTP端口号，标准端口21无需填写] <FTP用户名> <FTP密码>

TFTP:
exe restore image tftp <固件文件名称> <TFTP服务器IP或域名>[:TFTP端口号，标准端口21无需填写]
```

2. 举例如下。

```bash
FTP:
exe restore image ftp FGT_61F-v7.0.11.M-build0489-FORTINET.out 192.168.1.100 user1 Fortinet123#

TFTP:
exe restore image tftp FGT_61F-v7.0.11.M-build0489-FORTINET.out 192.168.1.100
```

USB方式

1. 通过USB方式升级，需要将包含固件的U盘插入FortiGate的USB接口，如下图所示。



2. 升级命令。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
exe restore image usb <固件文件名称>
```

3. 举例如下。

```bash
exe restore image usb FGT_61F-v7.0.11.M-build0489-FORTINET.out
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

通过FortiGuard升级

功能介绍

FortiGate可以通过`execute restore image management-station <version_name>`命令在线下载版本并升级，该功能有以下特点：

- 相比较通过Web方式在线升级，可以看到固件的下载进度，更直观。
- 适用于暂时无法登录FortiCloud下载固件版本文件进行离线升级。
- FortiGate需要可以通过Internet访问FortiGuard。
- FortiGate需要有Firmware & General Updates License。
- 使用该方法升级同样支持HA不间断升级 ↗。

> **重要**
>
> - 升级前，务必做好配置备份，参考系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗。
> - 升级固件必须遵循升级路径，参考系统管理→固件与配置管理→固件版本管理→升级路径 ↗，前往https://docs.fortinet.com/upgrade-tool ↗ 查询升级路径，否则可能造成配置丢失。

升级要点

> **重要**
>
> 升级固件必须遵循升级路径，参考系统管理→固件与配置管理→固件版本管理→升级路径 ↗，前往https://docs.fortinet.com/upgrade-tool ↗ 查询升级路径，否则可能造成配置丢失。

1. 升级前建议准备配置线，以防在升级失败后能及时处理。

2. 升级过程中请不要断电或重启设备，升级过程一般在5分钟以内完成。

3. 版本下载后设备将自动重启，重启才能生效。

升级步骤

举例：FortiGate-VM，7.0.17 GA版本，需要升级至7.4.7版本，查询升级路径为7.0.17→7.2.11→7.4.7。

1. 登入FortiGate的CLI界面，输入命令`execute restore image management-station ?`（最后输入`?`）。

```bash
FortiGate-VM # execute restore image management-station ?
Image-ID    Version
07006000FIMG0013706003  v7.06 MR6-GA-F P3 b3510 (upgrade)
07006000FIMG0013706002  v7.06 MR6-GA-F P2 b3462 (upgrade)
07006000FIMG0013706001  v7.06 MR6-GA-F P1 b3457 (upgrade)
07006000FIMG0013706000  v7.06 MR6-GA-F b3401 (upgrade)
07004000FIMG0013704007  v7.04 MR4-GA-M P7 b2731 (upgrade)
07004000FIMG0013704006  v7.04 MR4-GA-M P6 b2726 (upgrade)
07004000FIMG0013704005  v7.04 MR4-GA-M P5 b2702 (upgrade)
07004000FIMG0013704004  v7.04 MR4-GA-F P4 b2662 (upgrade)
07004000FIMG0013704003  v7.04 MR4-GA-F P3 b2573 (upgrade)
07004000FIMG0013704002  v7.04 MR4-GA-F P2 b2571 (upgrade)
07004000FIMG0013704001  v7.04 MR4-GA-F P1 b2463 (upgrade)
07004000FIMG0013704000  v7.04 MR4-GA-F b2360 (upgrade)
07002000FIMG0013702011  v7.02 MR2-GA-M P11 b1740 (upgrade)
07002000FIMG0013702010  v7.02 MR2-GA-M P10 b1706 (upgrade)
07002000FIMG0013702009  v7.02 MR2-GA-M P9 b1688 (upgrade)
07002000FIMG0013702008  v7.02 MR2-GA-M P8 b1639 (upgrade)
07002000FIMG0013702007  v7.02 MR2-GA-M P7 b1577 (upgrade)
07002000FIMG0013702006  v7.02 MR2-GA-F P6 b1575 (upgrade)
07002000FIMG0013702005  v7.02 MR2-GA-F P5 b1517 (upgrade)
07002000FIMG0013702004  v7.02 MR2-GA-F P4 b1396 (upgrade)
07002000FIMG0013702003  v7.02 MR2-GA-F P3 b1262 (upgrade)
07002000FIMG0013702002  v7.02 MR2-GA-F P2 b1255 (upgrade)
07000000FIMG0013700016  v7.00 GA-M P16 b0667 (downgrade)
07000000FIMG0013700015  v7.00 GA-M P15 b0632 (downgrade)
07000000FIMG0013700014  v7.00 GA-M P14 b0601 (downgrade)
07000000FIMG0013700013  v7.00 GA-M P13 b0566 (downgrade)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
07000000FIMG0013700012  v7.00 GA-M P12 b0523 (downgrade)
07000000FIMG0013700011  v7.00 GA-M P11 b0489 (downgrade)
07000000FIMG0013700010  v7.00 GA-M P10 b0450 (downgrade)
07000000FIMG0013700009  v7.00 GA-M P9 b0444 (downgrade)
07000000FIMG0013700008  v7.00 GA-F P8 b0418 (downgrade)
07000000FIMG0013700007  v7.00 GA-F P7 b0367 (downgrade)
06004000FIMG0013704016  v6.04 MR4-GA-M P16 b2098 (downgrade)
......
```

2. 输出信息中可以看到该设备型号可以升级/降级的所有固件版本，其中“Version”列可以标识具体的版本号，如`v7.04 MR4-GA-M P7 b2731`表示7.4.7，对应的“Image-ID”为`07004000FIMG0013704007`，`v7.02 MR2-GA-M P11 b1740 (upgrade)`表示7.2.11，对应的“Image-ID”为`07002000FIMG0013702011`。

重要

- `v7.02`：表示版本7.2。
- `MR2-GA-F`：F表示功能版本，M表示成熟版本。
- `P11`：表示Patch 11（7.2.11）。
- `b1740`：表示build号。

bash
```
Image-ID    Version
07004000FIMG0013704007  v7.04 MR4-GA-M P7 b2731 (upgrade)
07002000FIMG0013702011  v7.02 MR2-GA-M P11 b1740 (upgrade)
```

3. 首先需要升级到7.2.11版本，执行如下CLI命令，`07002000FIMG0013702011`为7.2.11版本的“Image-ID”，如果FortiGate可以正常通过Internet访问到FortiGuard，会下载对应的版本并显示下载进度，下载完成后，键入`y`确认，随后设备将重启并升级至目标系统版本7.2.11。

bash
```
FortiGate-VM # execute restore image management-station 07002000FIMG0013702011
Please wait ...

Getting image 07002000FIMG0013702011 from Management station ...
################################################################################################################
This operation will replace the current firmware version!
Do you want to continue? (y/n)y

Verifying the signature of the firmware image.
Warning: Upgrading to an image with Mature maturity notation.

Checking new firmware integrity  ... pass

Please wait for system to restart.
```

4. 使用相同的方法升级到7.4.7版本。

bash
```
FortiGate-VM # execute restore image management-station 07004000FIMG0013704007
Please wait ...

Getting image 07004000FIMG0013704007 from Management station ...
################################################################################################################
This operation will replace the current firmware version!
Do you want to continue? (y/n)y

Verifying the signature of the firmware image.
Image verification OK!
Warning: Upgrading to an image with Mature maturity notation.

Checking new firmware integrity  ... pass

Please wait for system to restart.
```

5. 如果升级的目标版本是F（Feature）类型，会有额外的警告信息，并需要多次确认。

bash
```
Verifying the signature of the firmware image.
Warning: Upgrading to an image with Feature maturity notation.
Image file uploaded is marked as a Feature image, are you sure you want to upgrade?
Do you want to continue? (y/n)y

Please confirm again. Are you sure you want to upgrade using uploaded file?
Do you want to continue? (y/n)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

6. 如果是降级或不按照升级路径升级（不推荐），会有额外的警告信息，并需要多次确认。

```bash
Verifying the signature of the firmware image.
Warning: Installing image v7.2.11 from v7.4.7 is not a recommended upgrade path. Continuing with the upgrade may result in loss of configuration. Do you want to proceed?
Do you want to continue? (y/n)y

Warning: Downgrading to an image with Mature maturity notation.
Image file uploaded is marked as a Mature image, are you sure you want to downgrade?
Do you want to continue? (y/n)y

Please confirm again. Are you sure you want to downgrade using uploaded file?
Do you want to continue? (y/n)y

This operation will downgrade the current firmware version.
Do you want to continue? (y/n)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

固件切换

功能介绍

1. 在FortiGate物理设备的Flash闪存中，可以保存两个固件版本及其对应的配置文件，一个为默认运行的固件，另一个为备份固件。

2. 通过如下命令可以看到当前Flash闪存中存在的两个固件版本分区。如下输出中，Active为Yes的分区（2）是当前正在运行的固件版本分区，另外一个是升级到此版本前的上个固件版本分区。

```
FortiGate # diagnose sys flash list
Partition  Image                                  TotalSize(KB)  Used(KB)  Use%  Active
1          FG101F-7.00-FW-build0450-230221                253920    111052   44%  No
2          FG101F-7.00-FW-build0489-230314                253920    110816   44%  Yes
3          ETDB-91.03066                                 3021708    270904    9%  No
Image build at Mar 15 2023 00:12:07 for b0489
```

3. 如果在升级后遇到问题需要回退（降级），我们可以将当前的运行版本切换回升级前的上个版本。

> **重要**
>
> 配置文件也会恢复到升级前上个版本运行的配置文件，如果您在升级后又配置了新的内容，请注意切换后配置上的差异。
>
> 请尽量使用此方法（Flash固件切换）进行无损降级。不要直接在较高版本中上传较低版本的固件进行降级，即使是空配置的状态，也可能导致FortiOS数据库损坏，进而导致降级后部分功能无法正常使用，甚至是无法正常启动！

切换步骤

1. 要恢复到Flash分区中的另一个固件，请通过CLI使用以下命令（该命令只能由具有super_admin权限的管理员执行），并选择下次重新启动时应使用的固件。

```
FortiGate # execute set-next-reboot {primary | secondary}
```

> **重要**
>
> Primary和Secondary分别指分区1和分区2，可以忽略分区3。

2. 在此例中，我们正在运行的是分区2，想要切换的是分区1，所以要执行以下命令。

```
FortiGate # execute set-next-reboot primary
Default image is changed to image# 1.
```

3. 重启FortiGate，FortiGate将会加载分区1中的固件版本及其对应的配置文件。

```
FortiGate # execute reboot
```

4. 重启后，再次查看Flash分区信息，Active的分区已更改为分区1。

```
FortiGate # diagnose sys flash list
Partition  Image                                  TotalSize(KB)  Used(KB)  Use%  Active
1          FG101F-7.00-FW-build0450-230221                253920    111052   44%  Yes
2          FG101F-7.00-FW-build0489-230314                253920    110816   44%  No
3          ETDB-91.03066                                 3021708    270904    9%  No
Image build at Feb 13 2023 00:11:57 for b0450
```

注意事项

1. 每次执行升级后，Flash分区会将较旧的固件版本分区替换为新升级的固件版本。
2. 在HA环境下，该命令不会在集群成员中同步，必须在每个HA成员中执行。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

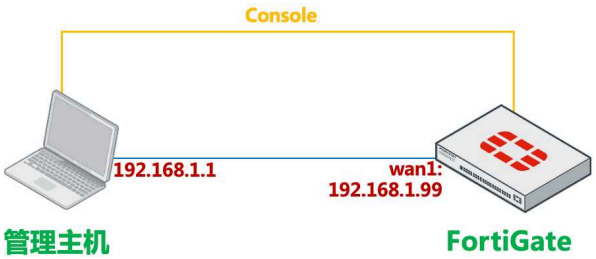
Flash刷机

需求

防火墙无法正常启动时，可以考虑格式化 Flash 闪存盘，传入新的固件，防火墙会使用新的固件与配置文件启动。

> **重要**
>
> 通过此方式将固件刷入Flash卡后，原有固件与配置文件会被清空。
>
> 刷机前，务必做好配置备份，参考系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗。
>
> 如果FortiGate设备运行的BIOS版本为5000100或6000100（或更新版本），用户将无法降级到6.0、6.2或6.4.13、7.0.12、7.2.5、7.4.0以下的FortiOS版本，如果需要降级到这些版本，请参考这里 ↗修改BIOS安全级别。

拓扑图



配置要点

1. 准备好工具，连接好Console线。
2. 连接网线，保证通讯正常。
3. 搭建好TFTP服务器。
4. 开始升级。

配置步骤

1. 准备好工具，准备好Console线，网线，升级文件，TFTP工具，若PC没有com口，需要购买转USB的线缆，并且装好驱动。

2. 连接网线，保证通讯正常。

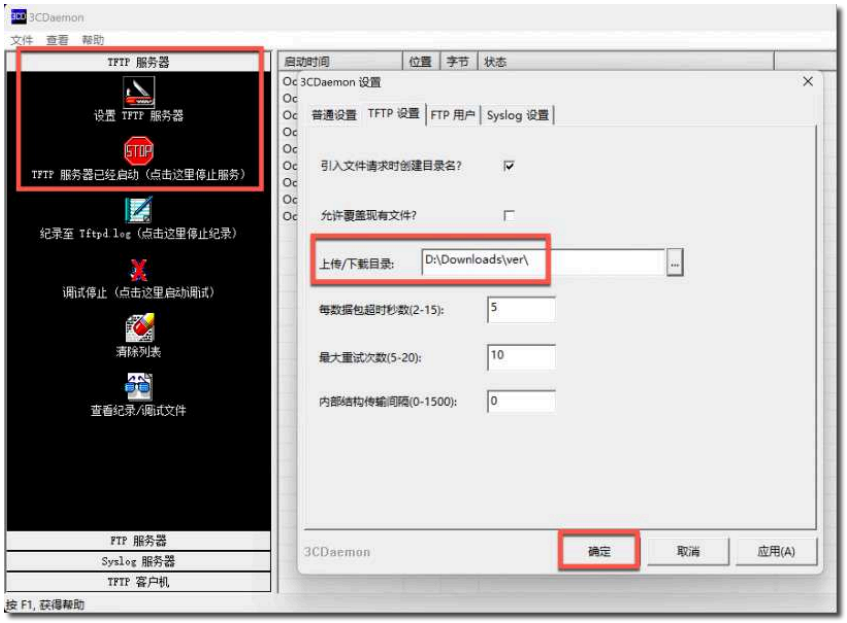
3. 搭建好TFTP服务器，可下载如下附件里的TFTP服务器软件（也可使用其他TFTP Server软件）。

   - Windows：3CDaemon ↗
   - macOS：Transfer ↗

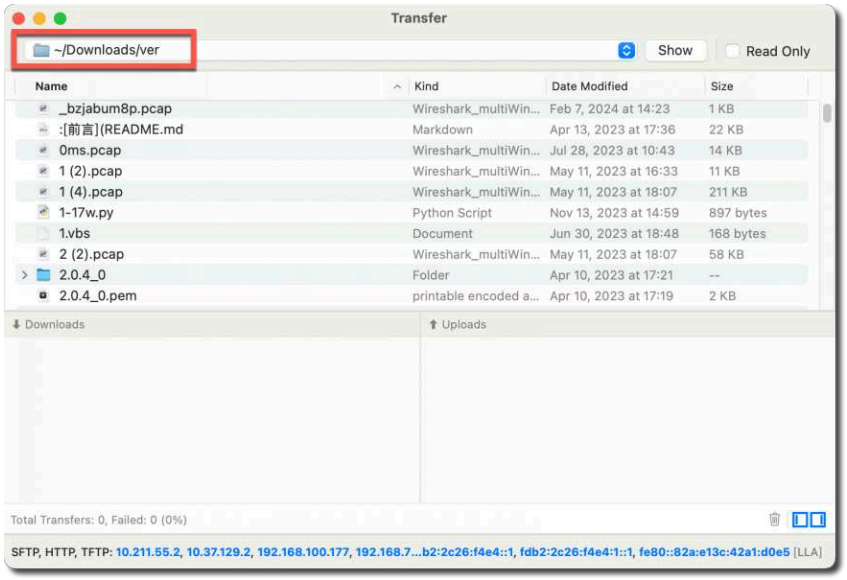
4. 启动TFTP服务器软件（确保TFTP服务器处于开启状态），修改TFTP服务器的文件路径到固件包所在路径，如下所示。

   - Windows（如下图路径为`D:\Downloads\ver\`）：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- macOS（如下图路径为`~/Downloads/ver`）：



5. 开始升级，重新启动设备。

6. 重启开始时将出现"Press any key to display configuration menu..."，此时按任意键进入BIOS菜单（有些型号的BIOS可能需要敲入Ctrl + B进入，请根据提示信息操作）。

```bash
Please wait for OS to boot, or press any key to display configuration menu....

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.
```

7. 键入`F`，格式化Flash卡，提示是否确认格式化，键入`yes`后回车。

> **重要**
>
> 键入F，将flash卡格式化，原有配置文件及OS将会被删除掉。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
Enter C,R,T,F,I,B,Q,or H:f
It will erase data in boot device. Continue? [yes/no]:yes
Formatting.......... Done.
```

8. 格式化完毕后，键入`C`，配置TFTP服务器，看到菜单如下。

```bash
[P]: Set firmware download port.
[D]: Set DHCP mode.
[I]: Set local IP address.
[S]: Set local subnet mask.
[G]: Set local gateway.
[V]: Set local VLAN ID.
[T]: Set remote TFTP server IP address.
[F]: Set firmware file name.
[E]: Reset TFTP parameters to factory defaults.
[R]: Review TFTP parameters.
[N]: Diagnose networking(ping).
[Q]: Quit this menu.
[H]: Display this list of options.
```

9. 键入`P`可以选择FortiGate上传固件使用的接口，这里我们使用WAN1接口为例，键入WAN1的序号8，然后键入回车键。

```
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:8
   [0]:  port 1
   [1]:  port 2
   [2]:  port 3
   [3]:  port 4
   [4]:  port 5
   [5]:  A
   [6]:  B
   [7]:  DMZ
   [8]:  WAN1
   [9]:  WAN2
```

0. 键入`I`，输入防火墙本地IP（中括号[ ]内的IP为上次进入BIOS配置的本地IP），然后键入回车键。

```bash
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:i

Enter local IP address [192.168.91.180]: 192.168.90.176
.done
```

1. 键入`S`，输入防火墙本地IP的掩码（中括号[ ]内的掩码为上次进入BIOS配置的本地IP掩码），然后键入回车键。

```bash
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:s

Enter local subnet mask [255.255.255.0]: 255.255.255.0
.done
```

2. 如果FortiGate与TFTP服务器不在同一网段，键入`G`，输入FortiGate的默认网关，否则跳过此步（中括号[ ]内的网关为上次进入BIOS配置的网关），然后键入回车键。

```bash
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:g

Enter local gateway IP address [192.168.91.254]: 192.168.90.254
.done
```

3. 键入`T`，输入TFTP服务器的IP地址（中括号[ ]内的IP为上次进入BIOS配置的TFTP服务器IP），然后键入回车键。

```bash
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:t

Enter remote TFTP server IP address [192.168.118.26]: 192.168.90.178
.done
```

4. 键入`F`，输入传输的版本镜像名称（中括号`[]`内的文件名称为上次进入BIOS配置的镜像文件名称），然后键入回车键。

```bash
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:f

Enter firmware file name [FGT_61F-v6-build0866-FORTINET.out]: FGT_61F-v7.2.8.M-build1639-FORTINET.out
.done
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

5. 键入 `R` ，检查TFTP配置是否正确，检查无误后，键入 `Q` 返回上一级菜单。

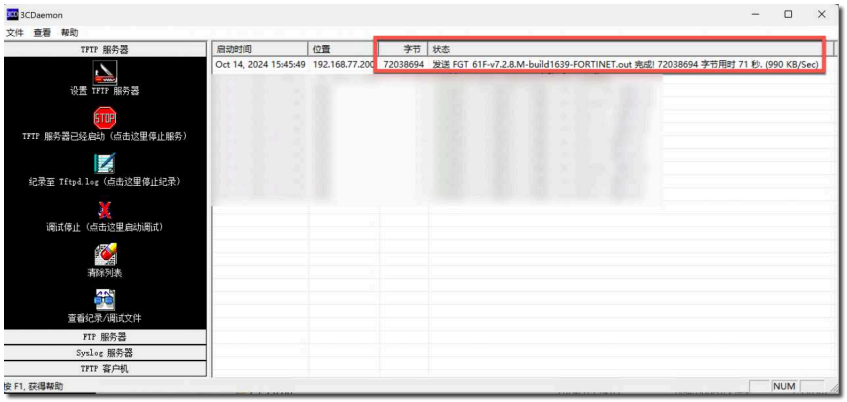
```bash
Enter P,D,I,S,G,V,T,F,E,R,N,Q,or H:r
Image download port:    WAN1
DHCP status:            Disabled
Local VLAN ID:          <NULL>
Local IP address:       192.168.90.176
Local subnet mask:      255.255.255.0
Local gateway:          192.168.90.254
TFTP server IP address: 192.168.90.178
Firmware file name:     FGT_61F-v7.2.8.M-build1639-FORTINET.out
```

6. 键入 `T` ，开始从TFTP服务器传输版本镜像文件，传输完成后，键入 `D` 将该镜像设置为默认启动的主系统版本（也可键入 `B` 设置为备份系统的镜像）。

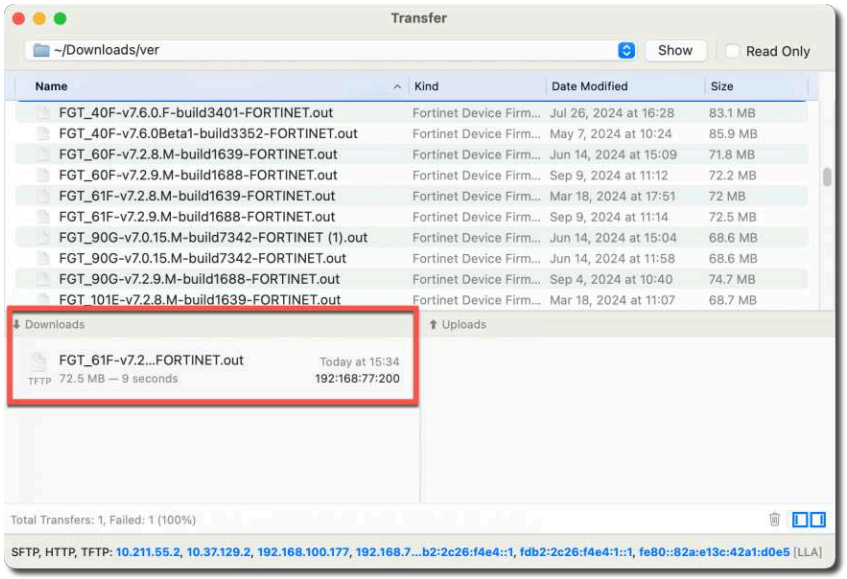
```bash
Enter C,R,T,F,I,B,Q,or H:t

Please connect TFTP server to Ethernet port 'WAN1'.
MAC: 90:6c:ac:f9:18:e8
Connect to tftp server 192.168.90.178 ...

##########################################################################################################################
##############################
Image Received.
Checking image ... OK
Uncompressed size: 268435968 = 0×10000200
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?D
```

7. 同时TFTP服务器也会提示下载成功。

- Windows：



- macOS：



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

8. 随后FortiGate可能会提示重新部署启动分区，键入`Y`（如果没有出现此提示，请忽略此步）。设备将重新格式化启动分区并使用以上步骤刷入的镜像版本启动。

```bash
Programming the boot device now.
The system must re-layout the boot device to install this firmware.
The default and backup firmware will be lost.
Continue:[Y/N]?y
..
Booting OS...
Reading boot image... 2967212 bytes.
Initializing firewall...
System is starting...
Resizing shared data partition...done
Formatting shared data partition  ...  done!
Starting system maintenance...
Scanning /dev/mmcblk0p1... (100%)
Scanning /dev/mmcblk0p3... (100%)

FortiGate-101E login:
```

9. 设备已加载TFTP导入的镜像作为主版本启动。

```bash
FortiGate-61F # get sys status | grep Version
Version: FortiGate-61F v7.2.8,build1639,240313 (GA.M)
Release Version Information: GA
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

软件签名增强

功能简介

“软件签名增强”功能是FortiOS 7推出的新功能，对重要的系统文件和可执行文件实现了BIOS级别签名和文件完整性检查。首先要保证在引导系统时加载的内核版本是经过签名的。系统一旦启动，将在活动系统上运行定期检查，以确认系统内核和进程以及AV/IPS引擎是经过签名的。此功能从6.4.13、7.0.12、7.2.5、7.4.0、7.6.0开始生效。

“软件签名增强”功能主要有三个模块。

启动保护

在设备启动时，会检查版本固件以及AV/IPS的签名合法性，在BIOS中支持3个“启动保护安全级别”设置（FortiGate硬件产品），分别为Level 0、Level 1、Level 2。：

- Level 1：当检测到系统内核文件的错误签名时（如非GA的临时版本），产生告警信息。





- Level 2（大多数设备默认）：当检测到系统内核文件的错误签名时（如非GA的临时版本），将FortiGate关机，FortiOS固件和每个版本的AV/IPS引擎文件将由Fortinet CA和第三方权威CA双重签名。

```bash
Initializing firewall...
System is starting...
System file integrity init check failed!
The system is going down NOW !!
The system is halted.
```

- Level 0：静默检查，当检测到系统内核文件的错误签名时（如非GA的临时版本），不产生告警信息，也不会将设备关闭。

系统安全保障

篡改文件系统或文件的尝试将立即被检测到，会触发设备重新启动，并生成事件日志。

定期检查系统

系统将定期（每6小时）检查进程和文件名、权限，并对它们执行签名检查。这种定期检查每6小时进行一次。如果检测到异常，将触发设备重启，并生成事件日志，相关日志如下所示：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

20230 - LOG_ID_SYS_SECURITY_WRITE_VIOLATION 432
Root filesystem is read only. Any modification triggers this log
20231 - LOG_ID_SYS_SECURITY_HARDLINK_VIOLATION 432
Attacker trying to replace symlink would trigger this log
20232 - LOG_ID_SYS_SECURITY_LOAD_MODULE_VIOLATION 433
Only kernel can load modules any unusual loading of modules triggers this log
20233 - LOG_ID_SYS_SECURITY_FILE_HASH_MISSING 434
File hashes are generated for legitimate files during bootup. If hash cannot be found, file may be suspicious as it could be a new routine inserted by attacker
20234 - LOG_ID_SYS_SECURITY_FILE_HASH_MISMATCH 434
File hashes are generated for legitimate files during bootup. If hash does not match when the file is exercised its an indication that it could have been modified by an attacker

IPS/AV特征库签名

1. AV和IPS包现在由Fortinet CA签名，以确保包的真实性。FortiGate更新时将进行如下检查：

- 自动更新时，只接受经过签名和验证的IPS/AV包。
- 手动更新时，将接受签名和验证的IPS/AV包。如果IPS/AV包未签名，则有以下情况：
  - BIOS Security Level 0：接受新的AV和IPS包，即使它没有签名。
  - BIOS Security Level 1：显示警告并要求用户确认接受。
  - BIOS Security Level 2：显示错误并拒绝AV和IPS包。

2. 对于HA，备设备将在保存签名包的同时从主设备同步签名文件。

3. 在CLI下，可以查看当前的IPS/AV特征库是否通过签名验证。

```bash
FortiGate # diagnose autoupdate signature check-all
aven(7,33) signature is valid.
virdb(2,2) signature is valid.
etdb(2,7) signature is valid.
exdb(2,4) signature is valid.
fcni(9,0) signature N/A.
contract(10,0) signature N/A.
idsen(30,80) signature is valid.
ipscfgscr(30,50) signature is valid.
fldb(34,2) signature is valid.
idsdb(4,24) signature is valid.
idsetdb(4,27) signature is valid.
idsurldb(5,1) signature is valid.
appdb(38,1) signature is valid.
isdb(39,1) signature is valid.
iot_detec(40,1) signature is valid.
geoip(28,0) signature N/A.
certdb(33,0) signature N/A.
update objects signature check finished.

FortiGate # diagnose autoupdate versions
AV Engine
————————
Version: 6.00288 signed
Contract Expiry Date: n/a
Last Updated using manual update on Mon May 15 18:35:00 2023
Last Update Attempt: n/a
Result: Updates Installed

Virus Definitions
————————
Version: 1.00000 signed
Contract Expiry Date: n/a
Last Updated using manual update on Mon Apr  9 19:07:00 2018
Last Update Attempt: n/a
Result: Updates Installed
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
37
38  Extended set
39  ————————
40  Version: 1.00000 signed
41  Contract Expiry Date: n/a
42  Last Updated using manual update on Mon Apr  9 19:07:00 2018
43  Last Update Attempt: n/a
44  Result: Updates Installed
```

4. FortiGate向FortiGuard自动更新时的验证签名Debug如下。

```
1  ...
2  installUpdateObject[321]-Signature verified for obj 9, ret=0, data_len=90, obj_len=90, sig_len=0.
3  installUpdateObject[358]-Step 2:Prepare temp file for obj 9
4  installUpdObjRest[827]-Step 3:Signal parent not to respawn
5  installUpdObjRest[837]-Step 4:Kill daemon(s)
6  installUpdObjRest[871]-Step 5:Backup /etc/fcni.dat→/tmp/update.backup
7  installUpdObjRest[899]-Step 6:Copy new object /tmp/updrbmfhS→/etc/fcni.dat
8  installUpdObjRest[984]-Step 7:Validate object
9  ...
```
bash

功能影响

1. 当版本签名在启动检查失败时（如“临时发布”或“特殊分支”等固件）， BIOS安全级别为2时将强制FortiGate关机，不会重新启动。
2. **当BIOS安全级别为Level 2时，将不能降级到一些较旧的版本（6.0、6.2或是6.4.13、7.0.12、7.2.5、7.4.0以下的版本）。解决方法是将BIOS安全级别从2更改为1或者0。**
3. 在RMA期间，没有BIOS安全级别的设备（6.4.13，7.0.12，7.2.5，7.4.0以下版本）可能被替换为具有安全级别支持的新硬件（默认安全级别为2）。如果客户正在运行非GA版本（如TOP 3版本），则客户应在更换设备之前需将BIOS上的安全级别设置为0。
4. 当FortiGate被攻击时，作为一种保护措施，试图篡改系统文件会导致FortiGate立即重启。修改BIOS安全级别不会影响此行为。
5. 如果系统文件校验和不匹配，在文件系统定期检查期间，FortiGate也会重新启动。修改BIOS安全级别不会影响此行为。

查看BIOS安全级别

```
1  FortiGate # get system status
2  ...
3  Version: FortiGate-601F v7.2.6,build1559,230822 (interim)
4  Security Level: 1
5  Firmware Signature: un-certified
6  ...
```

重要

从7.0.16、7.2.11、7.4.6、7.6.1版本开始，更新了安全级别的命名规则。以前的数字级别0、1和2现在分别表示为low、low和high。

修改BIOS安全级别

重要

请注意，调低该参数将影响设备或网络的整体安全状态。可能允许访问设备的用户在系统中安装或运行修改过的恶意代码。 强烈建议将FortiOS升级到支持BIOS安全检查的版本，最大限度地提高设备的安全等级。

如果FortiGate设备运行的BIOS版本为5000100或6000100（或更新版本），用户将无法降级到6.0、6.2或这些：6.4.13、7.0.12、7.2.5、7.4.0以下的FortiOS版本。

设备将无法正常启动，启动时将显示以下错误信息：

```
1  Booting OS ...
2  Fatal error: Loading FOS fails!
3  Please power cycle. System halted.
```

如果因为特殊要求，需要在已经具备BIOS安全级别功能的FortiOS版本上降级到以上FortiOS版本，请按照以下步骤更改BIOS安全级别。

1. 使用PC已连接设备的Console接口，重启FortiGate。在重启过程中，FortiGate会在Console中打印一条信息 “press any key to display configuration menu”，然后按一个任意键进入BIOS。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate-60F
Ver:05000009
Serial number: FGT60XXXXXXXXXXXX
CPU: 1200MHz
Total RAM: 2 GB
Initializing boot device ...
Initializing MAC ... NP6XLITE#0
Please wait for OS to boot, or press any key to display configuration menu. ⟵ Press any key.
```

2. 键入`I`，进入`System information`。

```bash
[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.    ⟵键入I
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot.
[H]: Display this list of options.
```

3. 键入`U`，进入`Set security level`。

```bash
Enter C,R,T,F,I,B,Q,or H:
[S]: Set serial port baudrate.
[R]: Set restricted mode.
[T]: Set menu timeout.
[U]: Set security level.    ⟵键入U
[I]: Display system information.
[E]: Reset system configuration.
[P]: Normal POST test.
[Q]: Quit this menu.
[H]: Display this list of options.
```

4. 键入安全级别的数字 （0、1或2）。

```bash
Enter S,R,T,U,I,E,P,Q,or H:
[0]: Level 0 - Check image silently
[1]: Level 1 - Check image with result only
[2]: Level 2 - Check image and reinforce validity
Enter security level setting [2]:    ⟵键入安全级别的数字（0、1或2）
```

5. 随后按照说明退出BIOS菜单并启动设备（通常是键入2次`Q`）。

常见问题

1. 哪些硬件支持BIOS安全级别设置?

```bash
FGT_40F, FGT_41F, FGT_41F_3G4G
FGT_60F, FGT_61F, FGR_60F, FGR60F_3G4G
FGT_70F, FGT_71F
FGT_80F, FGT_80F_BP, FGT_80F_POE
FGT_81F, FGT_81F_POE
FGT_100F, FGT_101F
FGT_200F, FGT_201F
FGT_400E_BP, FGT_400E, FGT_401E
FGT_1100E, FGT_1101E
FGT_1800F, FGT_1801F
FGT_2200E, FGT_201E
FGT_2600F, FGT_2601F
FGT_3300E, FGT_3301E
FGT_3400E, FGT_3401E
FGT_3500F, FGT_3501F FGT_3600E, FGT_3601E
FGT_4200F, FGT_4201F
FGT_4400F, FGT_4401F
FGT_600E, FGT601E
```

2. 是否对VM有影响?

- 虚拟机VM上无法修改“BIOS安全级别”。从`get system status`中看到的BIOS安全级别取决于固件版本：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

    - 6.4.16、7.0.16、7.2.9、7.4.4、7.6.0及之后版本：Level 2。
    - 6.4.13 ~ 6.4.15，7.0.12 ~ 7.0.15，7.2.5 ~ 7.2.8，7.4.0 ~ 7.4.3：Level 1。
  - 所以在BIOS安全级别为2的VM镜像中上传非GA的临时版本时，是无法上传的，必须先降级到BIOS安全级别为1的VM版本后，再导入非GA版本。

3. 如果BIOS设置为Level 2，但启动的固件不支持软件签名增强，预期的行为是什么?

   - 在引导时和系统启动时都不执行检查。

4. 如果BIOS设置安全级别为0，在启动时是否还会执行检查?

   - 会执行检查，它是静默地完成的，结果可以在`get system status`中看到。

5. 如果BIOS安全级别设置为0，系统安全保障和定期检查是否会激活。

   - 是的，如果加载的固件支持该特性，仍然会执行系统安全保障和定期检查。

6. 如何查看一个系统文件的MD5校验和?

```bash
FortiGate # diagnose sys csum /bin/init    //该命令需要指定具体的文件//
/bin/init:      df c1 b2 8f d9 a6 82 c5 d2 1e 45 87 e5 ec 98 f6

diagnose sys filesystem hash    //列出所有敏感文件的hash，7.4支持//
12b9377cbe7e5c94e8a70d9d23929523d14afa954793130f8a3959c7b849aca8        /data/etc/fdsm_mgmt_id.dat
00664fbc0fdafced6c4e0f77570f371cf0d0b85e0429c10d1376a81941f17289        /data/etc/cloudinit.log
48bd618e47b0dc185ff512b75c9fc6f7c5437d8aec6d7f3527c41d6687375d59        /data/etc/ips.mudb.rules.x
3af43771ffc8990ed38c7bd10ad37e60391e565c51a133e0acdc63539661ef11        /data/etc/applications.csv
423720df1a74eca781eaa37a388d86f438541d7f0624cd8f0c5781c843a5bded        /data/etc/sample.pac
db057221b788f6ed5c8b629ad83d6f8fca8dc35274bce13be6520595c09f1f65        /data/etc/modem_list_fex.conf
2e29084d86f3925a0fb6bf96c4d83a6d3025fdd9cf8059ebcfc307153b9fd63b        /data/etc/virexdb
0ceb39183d6ce36e7bd6bb5edfe6beacac702be9bfeac3bf0e2066df3643af1d        /data/etc/ips.iot.rules
a38bba93dc8691ca7367d134f575df31ba51c5c591309447338d10d08812910c        /data/etc/geoip_db.gz
2e29084d86f3925a0fb6bf96c4d83a6d3025fdd9cf8059ebcfc307153b9fd63b        /data/etc/virext
0cbf59ea97ced14b3dd844cb4dcd784ddcae7d5ef38c2a6081c9e369c25d5ac6        /data/etc/protocols.csv
896b71b3d9b209d339213f9d4af4088d3addd891cd292e93b5168eddb36b599a        /data/etc/virfldb.x
dbe703c06735797ac86570442b39827ca1844fea6312e48fee8c2d80647392d0        /data/etc/fgt.crt
3e36debe496618432707dc680ef78fc59c2d9ecc38b3f65a2f055dc826492492        /data/etc/fcni.dat
```

7. 如果遇到系统文件被篡改或是误报，我应该怎么办?

   - 如下所示，设备Console打印信息：

```bash
fos_ima: fos_process_appraise 99: Suspicous Executable File(/data2/libcrashpad.so) is missing hash
fos_ima: fos_process_appraise 99: Suspicous Executable File(/data2/flatkc_info) is missing hash
```

   - 如果您看到文件缺失散列值，如以下（但不限于），可能是攻击造成，可以访问此链接联系PSIRT团队：https://www.fortiguard.com/faq/psirt-contact ↗ ，会有Fortinet相关人员与您取得联系，或联系Fortinet技术支持。

```bash
/bin/sh
/bin/toybox
/data2/tftpd
/data2/libvcm.so.gz
/data2/libcrashpad.so
/data2/libpreload.so
/data2/flatkc_info
/data/lib/libvar.so
/tmp/busybox
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

固件自动升级

> **重要**
>
> 自动升级功能的初衷是为了规避已经发现的系统漏洞，防止黑客利用漏洞攻击。但在一些重要的生产环境中，不在维护时间内的更新和重启会造成严重的生产事故，所以在大部分生产环境下，建议关闭自动升级功能。

功能介绍

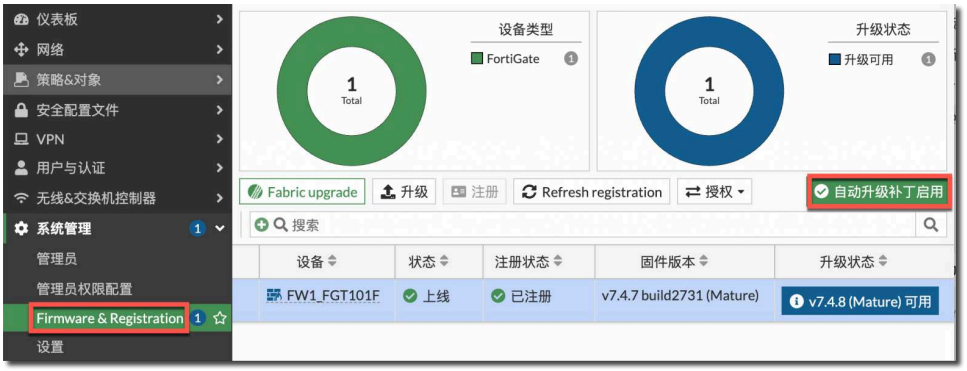
从FortiOS 7.2.1开始，FortiGate支持在线自动升级功能。

- 只能升级相同的次要版本（x.y.z中的y）的小版本（x.y.z中的z），不能在大版本之间自动升级。例如，7.2.5版本只能自动升级到7.2.X，不能自动升级到7.4.X。
- 如果存在Mature类型的新版本，自动升级会按照升级路径的版本顺序进行。
- 如果不存在Mature类型的新版本，则会参考 `diagnose fdsm image-upgrade-matrix` 中的升级路径。
- 每次自动升级只会升级一个版本，如果升级路径中存在多个版本，会产生多次重启。
- 命令 `diagnose test application forticldd 13` 可以查看自动升级的开启状态以及将要自动升级的版本和具体时间。

功能配置

GUI配置

1. 进入设备的管理页面，访问“系统管理→Firmware & Registration”，右上角显示“自动升级补丁启用”，点击该按钮。



2. 在弹出的“自动补丁升级”窗口中，可以禁用补丁自动升级或配置自动升级的相关参数，完成配置后点击“OK”按钮下发配置。

   - 升级时间表：
     - 延迟：当检测到新版本后，延迟升级的时间（默认3天）。
     - Specify days：当检测到新版本后，特定一周中的某一天或几天升级，如果选了多天，则会在最近一天的可用时间升级。
   - Install during specified time：升级当天执行升级动作具体的时间段，会在选定的时间内的随机时间安排升级。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

CLI配置

```bash
config system fortiguard
    set auto-firmware-upgrade { enable | disable* }
    set auto-firmware-upgrade-day {sunday monday tuesday wednesday thursday friday saturday}
    set auto-firmware-upgrade-start-hour <integer>
    set auto-firmware-upgrade-end-hour <integer>
    set auto-firmware-upgrade-delay <integer>
end
```

- `auto-firmware-upgrade-day`：指定某一天或某几天才能执行自动升级，比如只能周末升级版本，缺省是每周7天全选。
- `auto-firmware-upgrade-start-hour` / `auto-firmware-upgrade-end-hour`：指定升级时间点，缺省是2:00~4:00的随机时间点。
- `auto-firmware-upgrade-delay`（7.2.6新增功能）：发现有新版本后延迟多少天再升级（0~14天，缺省3天）。当`set auto-firmware-upgrade-delay`配置为0时，`auto-firmware-upgrade-day`配置才会生效。

自动升级默认状态

在不同的版本/FortiGate型号条件下，自动升级功能的默认开启状态如下所示：

设备版本	FortiGate型号	自动升级默认状态
7.2.1~7.2.5 / 7.4.0~7.4.4 / 7.6.0	所有	关闭
7.2.6~7.2.X	<100	开启
	⩾100	关闭
7.4.5~7.4.X / 7.6.1~7.6.X	所有	开启

查看自动升级状态

通过`diagnose test application forticldd 13`命令可以看到当前设备自动升级的相关状态，常见状态有如下几种。

- FortiGate当前没有检测到新版本，没有升级计划，计划了下次检测新版本的时间为`Wed Jun 4 03:07:58 2025`（计划检查时间也遵从已配置的自动更新时间范围）。

```bash
FortiGate # diagnose test application forticldd 13
Scheduled push image upgrade: no
Scheduled Config Restore: no
Scheduled Script Restore: no
Automatic image upgrade: Enabled.
        Next upgrade check scheduled at (local time) Wed Jun  4 03:07:58 2025
```

- FortiGate检测到新版本7.4.8，并计划了升级时间为`Thu Jun 5 05:13:10 2025`。

```bash
FortiGate # diagnose test application forticldd 13
Scheduled push image upgrade: no
Scheduled Config Restore: no
Scheduled Script Restore: no
Automatic image upgrade: Enabled.
        Next upgrade check scheduled at (local time) Thu Jun  5 02:13:51 2025
        New image 7.4.8b2795(07004000FIMG0023904008) installation is scheduled to
                start at Thu Jun  5 05:13:10 2025
                end by Thu Jun  5 07:00:00 2025
        Last upgrade check executed at (local time) Wed Jun  4 03:07:58 2025
```

- 当FortiGate检测到新版本并计划升级时间后，会向设备注册的邮箱发送一封通知邮件，包含系统计划自动升级的事件日志。

```bash
date=2025-06-04 time=11:07:58 devid="FG101FTK20007637" devname="FW1_FGT101F" eventtime=1749006478360626440
tz="+0800" logid="0100032263" type="event" subtype="system" level="notice" vd="root" logdesc="Automatic firmware
upgrade schedule changed" user="system" msg="System patch-level auto-upgrade new image installation (re)scheduled
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
to between local time Thu Jun  5 12:13:10 2025 and local time Thu Jun  5 14:00:00 2025."
```

- 设备关闭了自动升级功能。

> **重要**
>
> 如果FortiGate被FortiCloud管理，即使这里的状态为 `Disabled` ，仍然可能通过FortiCloud自动升级，详见下方的“关闭自动升级→设备被FortiCloud管理↗”章节。

```bash
FortiGate # diagnose test application forticldd 13
Scheduled push image upgrade: no
Scheduled Config Restore: no
Scheduled Script Restore: no
Automatic image upgrade: Disabled.
```

关闭自动升级

自动升级功能的初衷是为了规避已经发现的系统漏洞，防止黑客利用漏洞攻击。但在一些重要的生产环境中，不在维护时间内的更新和重启会造成严重的生产事故，所以在大部分生产环境下，需要关闭自动升级功能。

如果在自动升级开启的状态下，已经计划了升级时间，用如下方式关闭后，已有的升级计划也会终止。

设备被FortiGate Cloud管理

> **重要**
>
> 如果设备加入了FortiGate Cloud，即使设备自身关闭了自动升级，仍然会通过FortiGate Cloud进行自动升级。

1. 检查设备是否被FortiGate Cloud管理。



2. 如果设备已配置FortiGate Cloud管理，不仅要关闭设备自身的自动升级功能，还需要同时关闭FortiGate Cloud下的自动升级功能。

```bash
config system fortiguard
    set auto-firmware-upgrade disable
end

config system central-management
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
end
```

设备被FMG/Security Fabric管理

只需要关闭设备自身的自动升级功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system fortiguard
    set auto-firmware-upgrade disable
end
```

强制升级

触发条件

在7.4.8、7.6.4、8.0.0及以后版本，以下情况会触发强制自动升级（FortiGate所有型号），**不受以上自动升级设置的影响**：

1. **固件版本支持周期终止**：当设备固件达到官方**工程支持终止**日期（End of Engineering Support，简称EOES，该时间可以登录 https://support.fortinet.com/support/#/lifecycle ↗ 查询）时，系统将强制升级至最新版本（主次版本号保持不变，例如7.2.X会升级到7.2最新的版本，而不会升级到7.4.X）。

   > **重要**
   >
   > 注意EOES时间并非EOS（End of Support）时间，通常比EOS时间要早：
   >
   > - EOES指Fortinet不再对该版本做代码更新（除非是critical级别的问题）。
   > - EOS指Fortinet不再对该版本提供技术支持。
   > - 关于产品生命周期的更多信息请参考系统管理→固件与配置管理→固件版本管理→产品生命周期 ↗章节。

2. **无有效FMGR合同**：若设备未绑定有效的FMGR合同（Firmware & General Updates），系统将强制升级至最新补丁版本（主次版本号保持不变，例如7.2.X会升级到7.2最新的版本，而不会升级到7.4.X）。

例外情况

1. 设备被FortiManager管理。
2. 设备属于Security Fabric中。

延迟强制自动升级

- 强制自动升级可以手动延迟（一周），但无法取消。

```bash
execute auto-upgrade delay-installation
```

- 查看当前强制自动升级的状态。

```
execute auto-upgrade status
```

- GUI的升级页面会显示与常规自动升级相似但不同的提示信息，以便用户明确识别当前为强制自动升级。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置备份及恢复

需求

将防火墙的配置保存并导出备份，在必要时用来恢复之前的配置。

配置要点

1. 保存配置
2. 导出配置
3. 恢复配置

> **重要**
>
> - 导入的配置文件必须是conf格式，否则无法识别。
> - 导入配置后需要重启才会生效。
> - 备份配置设置的密码必须谨记，如遗忘则无法导入恢复。
> - 请使用具有“super_admin”权限的管理员导出配置文件，而不是“prof_admin”，否则导出的配置文件不完整（缺少super_admin账户配置，导入设备后无法再导入其他配置文件）。

操作步骤

保存配置

1. Web：Web上配置完，及时生效，且自动保存配置，无需手工保存。 每次修改配点击确认按钮后，配置自动保存。

2. CLI：命令行下输入next或end后配置生效并自动保存。

导出配置

1. 进入Web页面点击右上方登录账号admin，找到配置，点击"备份"按钮，对配置进行保存。

> **重要**
>
> 请使用具有“super_admin”权限的管理员导出配置文件，而不是“prof_admin”，否则导出的配置文件不完整（缺少super_admin账户配置，导入设备后无法再导入其他配置文件）。

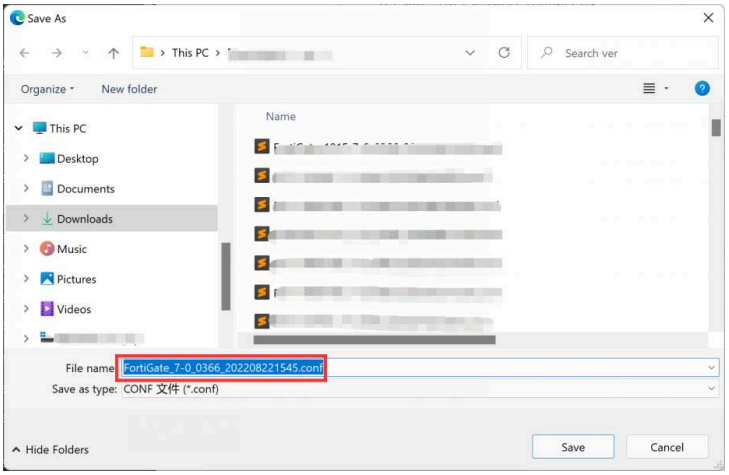


2. 支持选择是否对配置文件进行加密，根据实际情况选择是否加密（加密需设置密码，请牢记该密码），点击确认。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 点击确定并把配置文件备份到本地磁盘上选择的位置，文件格式为*.conf。



4. 同时，FortiGate也支持在CLI下通过FTP/TFTP/SFTP/USB（需将包含配置文件的U盘插入FortiGate的USB接口）等方式将配置文件导出，命令格式如下：

```
FTP:
exe backup config ftp <配置文件名称> <FTP服务器IP或域名>[:FTP端口号，标准端口无需填写] <FTP用户名> <FTP密码> [配置文件加密密码，如果不需要则不填]
举例:
exe backup config ftp FortiGate_7-2_1396_202305121543.conf 192.168.1.100 user1 Fortinet123#

SFTP:
exe backup config sftp <配置文件名称> <SFTP服务器IP或域名>[:SFTP端口号，标准端口无需填写] <SFTP用户名> <SFTP密码> [配置文件加密密码，如果不需要则不填]
举例:
exe backup config ftp FortiGate_7-2_1396_202305121543.conf 192.168.1.100 user1 Fortinet123#

TFTP:
exe backup config tftp <配置文件名称> <TFTP服务器IP或域名>[:TFTP端口号，标准端口无需填写] [配置文件加密密码，如果不需要则不填]
举例:
exe backup config tftp FortiGate_7-2_1396_202305121543.conf 192.168.1.100

USB:
exe backup config usb <配置文件名称> [配置文件加密密码，如果不需要则不填]
举例:
exe backup config usb FortiGate_7-2_1396_202305121543.conf
```

恢复配置

1. 页面右上角点击admin，找到配置，点击"恢复"按钮，用原来存储在本地的配置文件恢复防火墙配置。

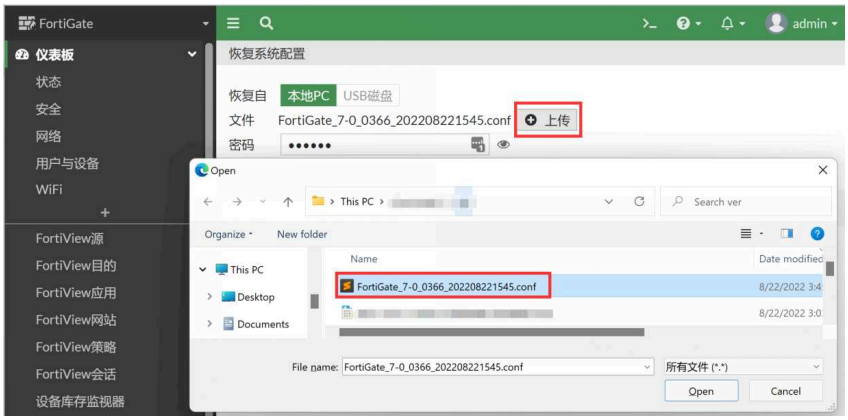
> **重要**
>
> 请使用具有“super_admin”权限的管理员导出配置文件，而不是“prof_admin”，否则导出的配置文件不完整（缺少super_admin账户配置，导入设备后无法再导入其他配置文件）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

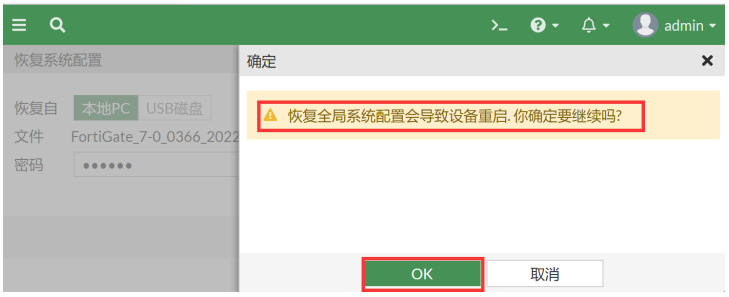


2. 弹出如上恢复界面（如配置文件未加密，则无需输入密码）。

3. 点击浏览，选择之前备份的配置文件，输入之前备份配置文件时设置的密码，点击确认按钮即可。



4. 导入成功后会提示系统重启后生效，故需要重启设备。点击“OK"。



5. 同时，FortiGate也支持在CLI下通过FTP/TFTP/USB（需将包含配置文件的U盘插入FortiGate的USB接口）等方式将配置文件导入，命令格式如下：

```
FTP:
exe restore config ftp <配置文件名称> <FTP服务器IP或域名>[:FTP端口号，标准端口无需填写] <FTP用户名> <FTP密码> [配置文件加密密码，如果导出时未配置则不填]
举例:
exe restore config ftp FortiGate_7-2_1396_202305121543.conf 192.168.1.100 user1 Fortinet123#

TFTP:
exe restore config tftp <配置文件名称> <TFTP服务器IP或域名>[:TFTP端口号，标准端口无需填写] [配置文件加密密码，如果不需要则不填]
举例:
exe restore config tftp FortiGate_7-2_1396_202305121543.conf 192.168.1.100

USB:
exe restore config usb <配置文件名称> [配置文件加密密码，如果不需要则不填]
举例:
exe restore config usb FortiGate_7-2_1396_202305121543.conf
```

重要

如果是HA环境，则导入配置文件后，主备设备均会重启。

验证效果

设备重启后还原为之前的配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

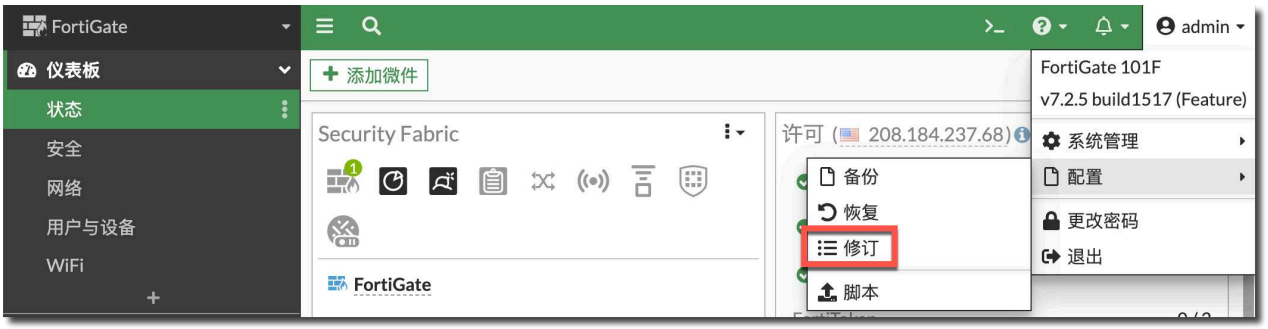
备份配置文件到Flash

功能介绍

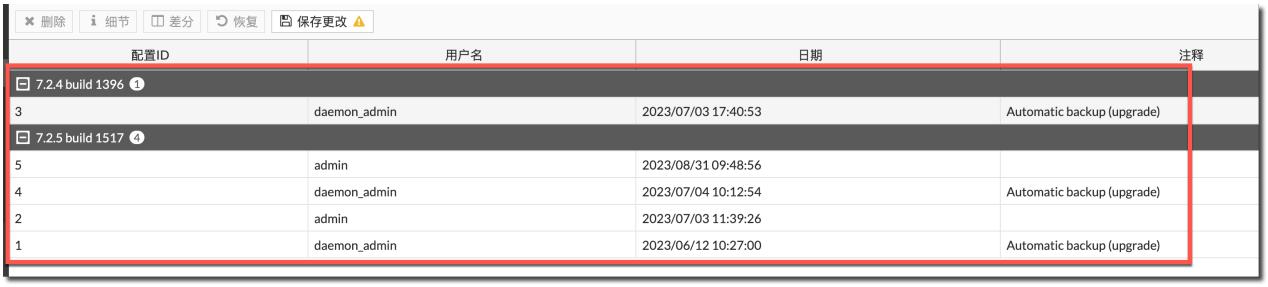
FortiGate可以备份配置文件到Flash闪存中，保存后，可以在多个配置文件间进行切换，以及对比多个配置文件间的差异，重启不会丢失Flash中的所有配置文件。

使用方法

1. 登录FortiGate，点击右上角的管理员账户→配置→修订按钮，进入修订页面。



2. 在修订页面中，可以看到已经备份到Flash中的配置文件及对应版本分类（对应的CLI如下所示）。

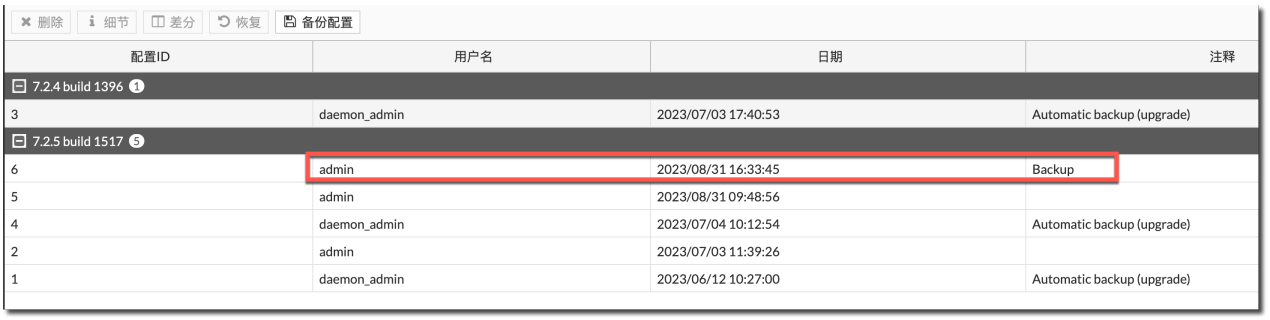



```
FortiGate # execute revision list config
Last Firmware Version: V0.0.0-build000-REL0

ID  TIME                 ADMIN           FIRMWARE VERSION          COMMENT
1   2023-06-12 10:27:00  daemon_admin    V7.2.5-build1517-REL0     Automatic backup (upgrade)
2   2023-07-03 11:39:26  admin           V7.2.5-build1517-REL0
3   2023-07-03 17:40:53  daemon_admin    V7.2.4-build1396-REL0     Automatic backup (upgrade)
4   2023-07-04 10:12:54  daemon_admin    V7.2.5-build1517-REL0     Automatic backup (upgrade)
5   2023-08-31 09:48:56  admin           V7.2.5-build1517-REL0
```

3. 点击页面上的“保存更改”按钮，可以保存当前的版本配置到Flash中，对应的CLI如下所示。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
FortiGate # exe backup config flash Backup
Please wait ...
Config backed up to flash disk done.
```

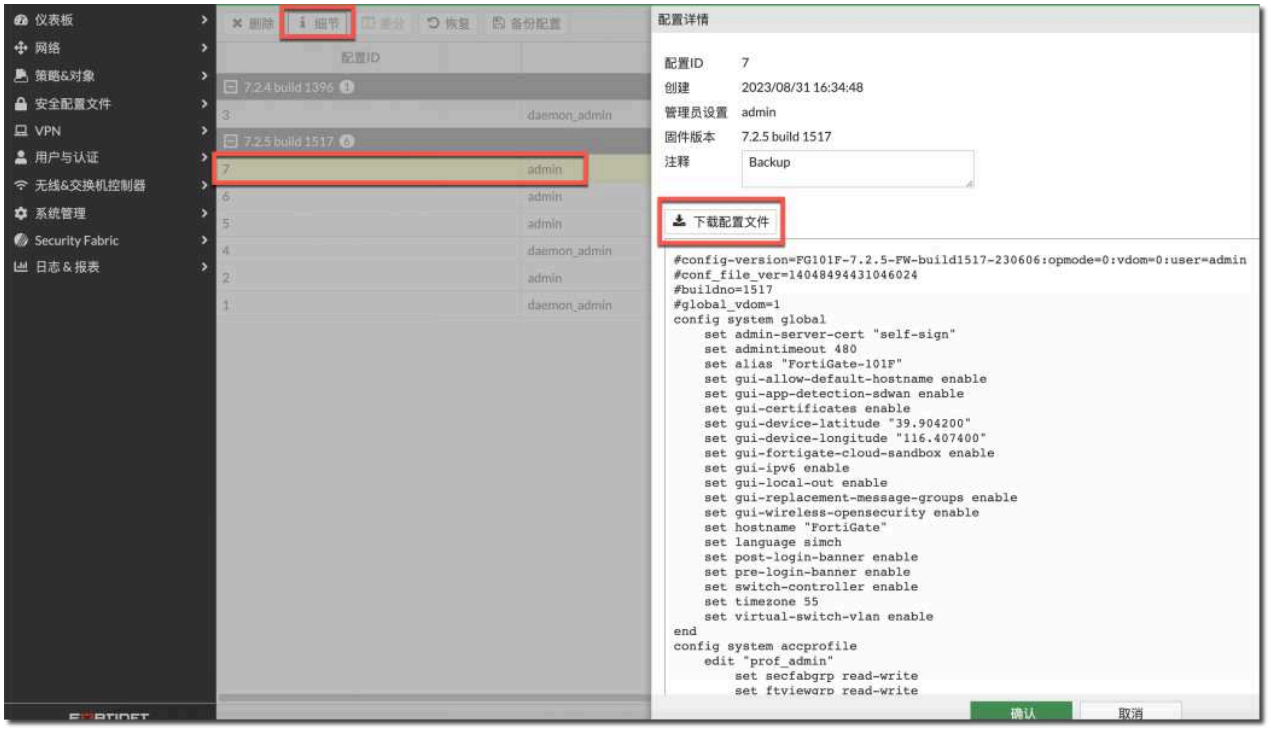
4. 选中某个配置文件，点击“恢复”按钮，可以将此配置恢复到当前FortiGate上，需要重启设备。



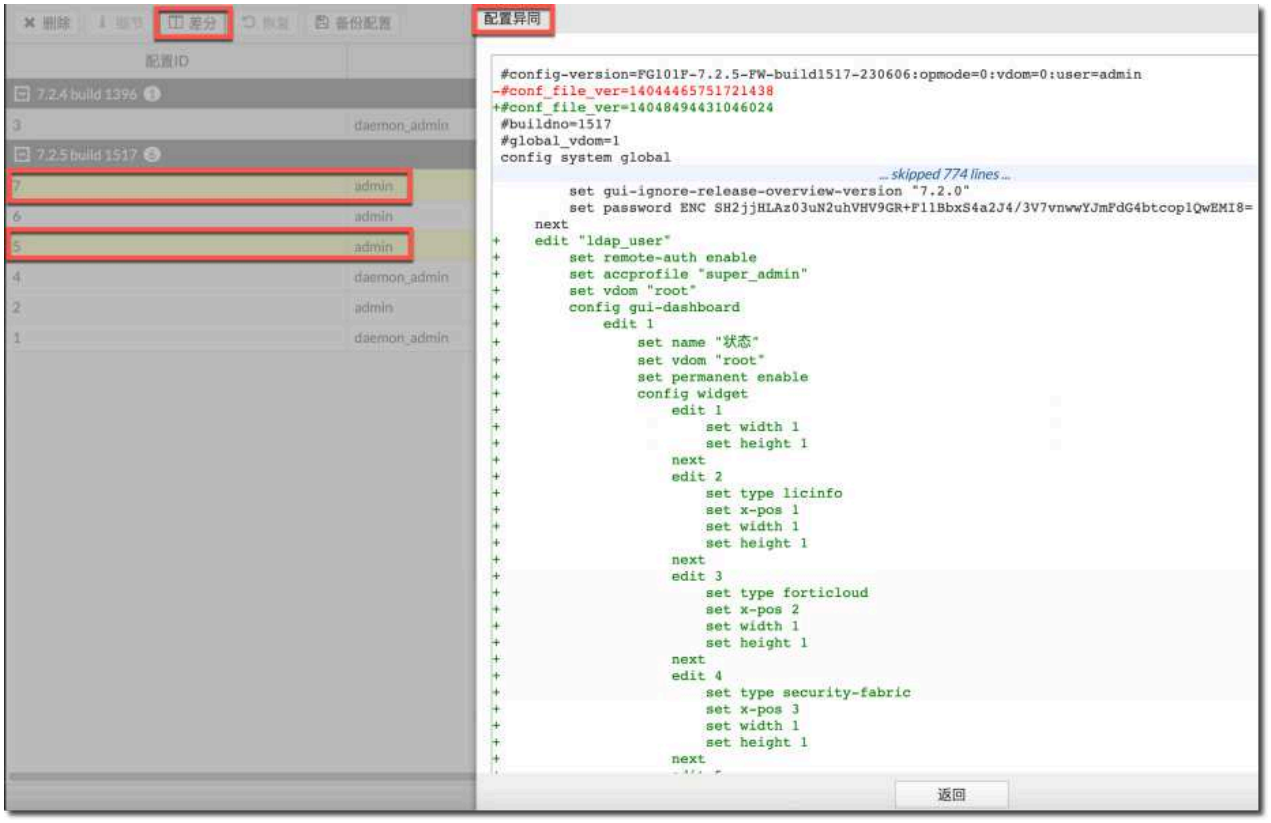

```
FortiGate # execute restore config flash 7
This operation will overwrite the current setting and could possibly reboot the system!
Do you want to continue? (y/n)
```

5. 选中某个配置文件，点击“细节”按钮，可以看到配置文件的信息和具体内容，也可以下载该配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 按住Ctrl（macOS为⌘command键）键使用鼠标，选中两个配置文件，然后点击差分按钮，在弹出的页面中可以看到两个配置文件的差异。



7. 删除备份的配置文件。

```
execute revision delete config <revision>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

自动备份配置

通过系统自动备份

> **重要**
>
> 建议在设备部署前开启这两个全局配置，在误操作导致的设备配置丢失后可以快速恢复历史配置。

```
config system global
    set revision-image-auto-backup enable
    set revision-backup-on-logout enable
end
```

- 在设备固件升级后，自动将配置文件备份到Flash。
- 在设备管理员登出后，自动将配置文件备份到Flash，建议在设备部署前开启。

通过自动化功能备份

1. 使用Security Fabric中的自动化功能，可以自动定期将系统配置文件备份到Flash中，用于配置回溯或恢复。

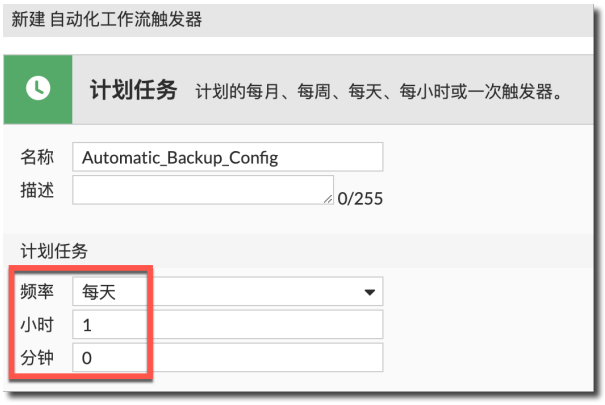
2. 进入FortiGate的Security Fabric→自动化→工作流页面，新建工作流，配置工作流名称，点击添加触发器，在右侧弹出的条目窗口中点击新建按钮。



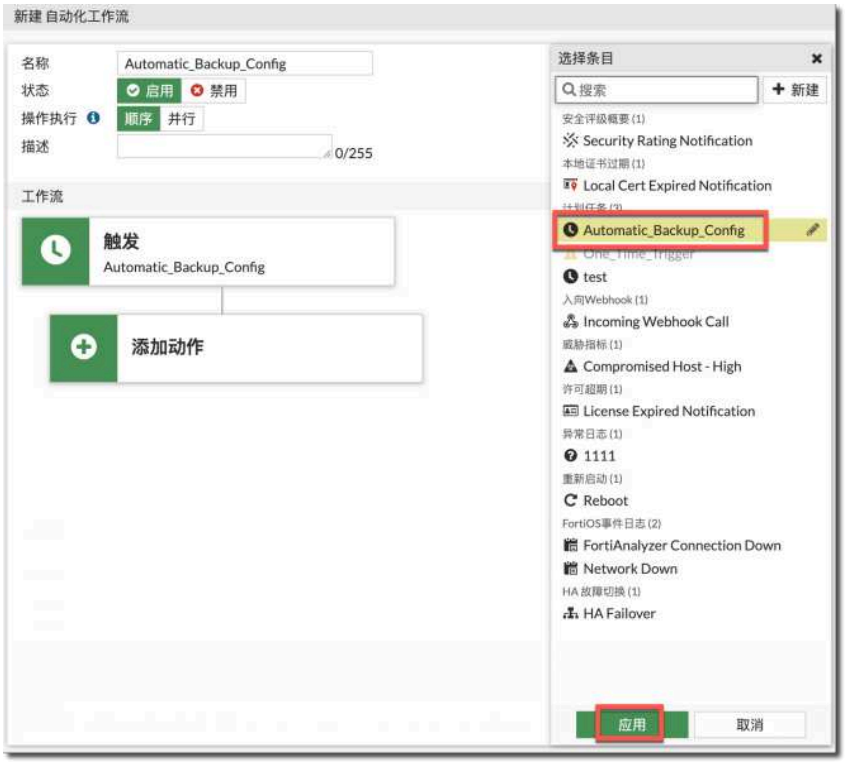
3. 在弹出的新建触发器窗口中选择其他条件中的计划任务触发器，配置触发器的时间为每天凌晨1点，点击确定下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



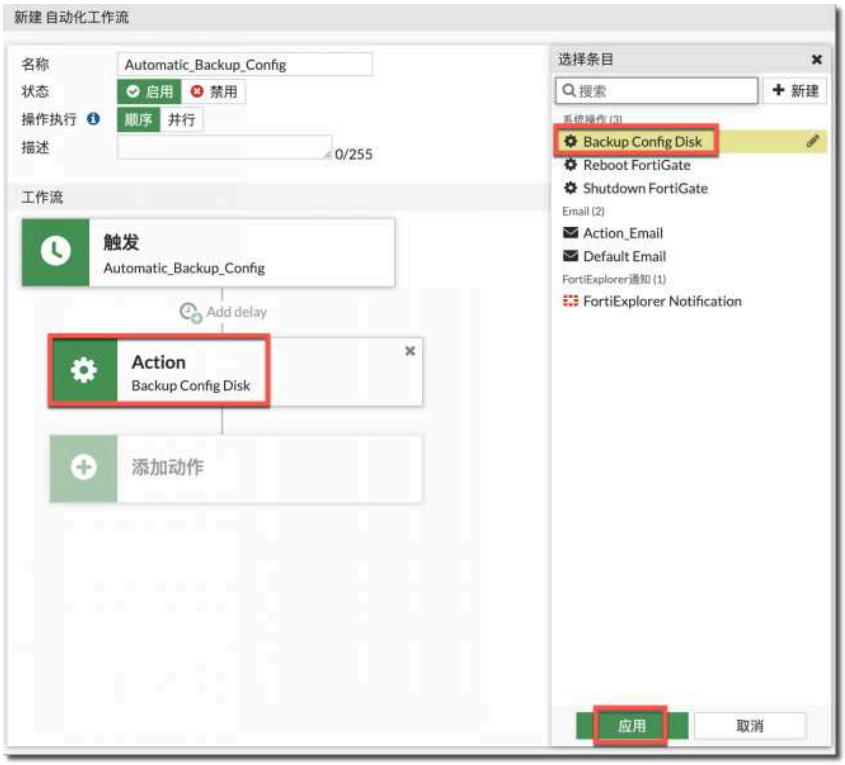


4. 在选择条目中选中上步创建的计划任务，点击下方的应用按钮。

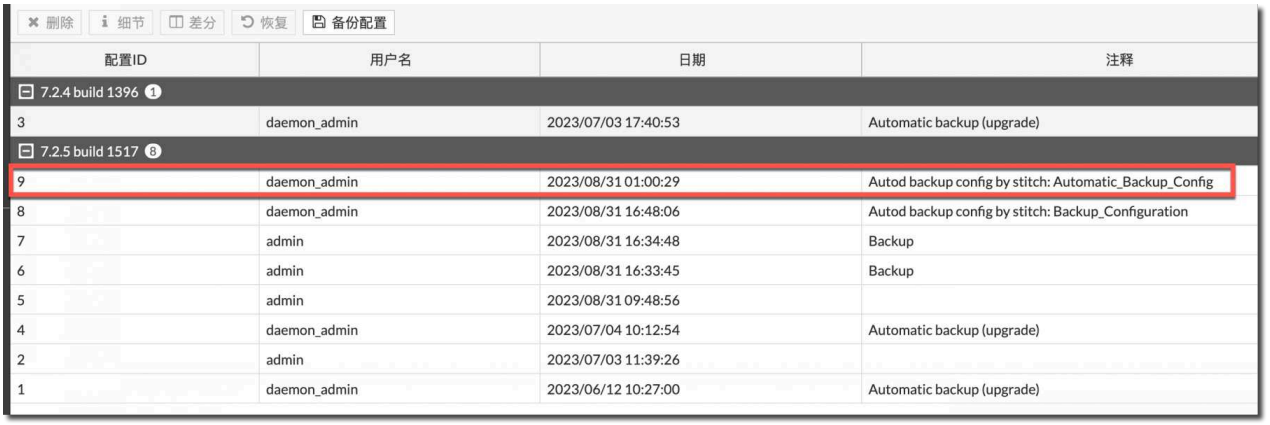


5. 点击Action按钮，在右侧弹出的条目中选择系统预置的“Backup Config Disk”，该动作用于将配置文件保存至Flash中，点击应用按钮，最后点击确认下发该工作流的配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 查看自动化备份的配置文件。



配置ID	用户名	日期	注释
7.2.4 build 1396 1			
3	daemon_admin	2023/07/03 17:40:53	Automatic backup (upgrade)
7.2.5 build 1517 8			
9	daemon_admin	2023/08/31 01:00:29	Autod backup config by stitch: Automatic_Backup_Config
8	daemon_admin	2023/08/31 16:48:06	Autod backup config by stitch: Backup_Configuration
7	admin	2023/08/31 16:34:48	Backup
6	admin	2023/08/31 16:33:45	Backup
5	admin	2023/08/31 09:48:56	
4	daemon_admin	2023/07/04 10:12:54	Automatic backup (upgrade)
2	admin	2023/07/03 11:39:26	
1	daemon_admin	2023/06/12 10:27:00	Automatic backup (upgrade)

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

备份不包含密码的配置文件

重要

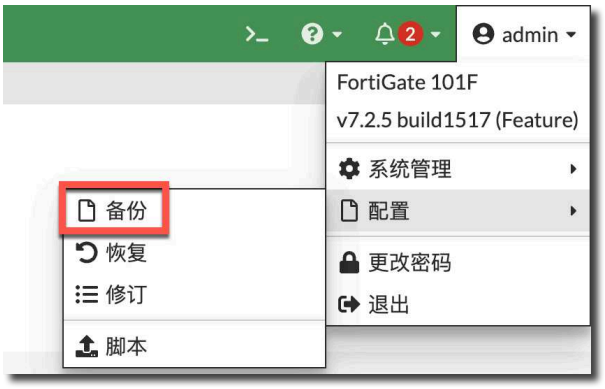
该功能在7.2.0及更新版本上支持。

重要

此方式导出的配置文件仅用于维护或支持人员定位问题，请不要用于日常的配置备份及配置恢复！否则会导致业务异常！

导出方法

1. 点击页面右上角的管理员→配置→备份按钮，跳转到备份系统配置页面。

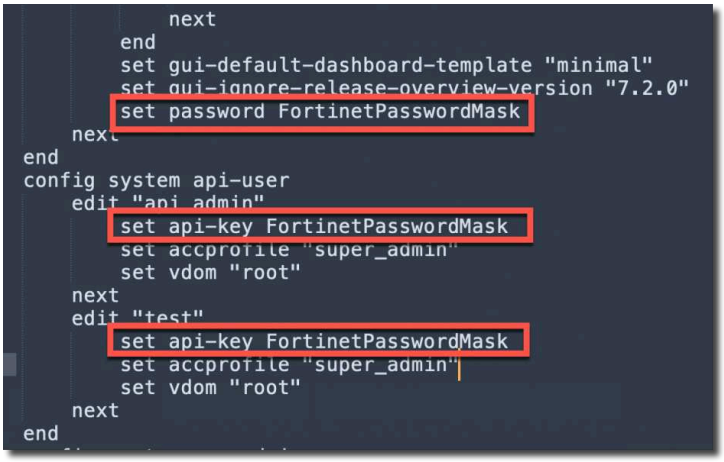


2. 备份系统配置时，选中“密码掩码”，然后点击确认备份配置。



3. 导出的配置中，所有密码字符均被替换为“FortinetPasswordMask”字符（包括管理员密码、用户密码、远程服务器密码、IPSec预共享密钥、证书密码等）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

通过SCP备份配置文件

功能简介

在FortiGate设备上启用SCP管理后，用户可以使用SCP协议（基于SSH）从FortiGate设备下载/上传配置或上传固件版本。本文介绍如何通过常见的SCP客户端来备份或上传FortiGate的配置文件。

SCP传输分为两种认证模式：

- 用户名/密码认证（每次登录都需要输入密码）
- SSH密钥认证（生成密钥对并保存后，每次登录不需要输入密码）

以下是通过SCP备份配置文件的步骤，用户可自行编写Python脚本执行定期配置文件的备份。

FortiGate开启SCP管理

1. 在FortiGate需要用于SCP传输的接口上开启SSH管理协议。

```bash
config system interface
    edit "internal5"
        append allowaccess ssh
    next
end
```

2. 在全局模式下开启SCP管理功能，并确认SSH管理端口号（默认为22）。

```bash
config system global
    set admin-scp enable
    set admin-ssh-port 22
end
```

SCP使用用户名/密码认证

Windows

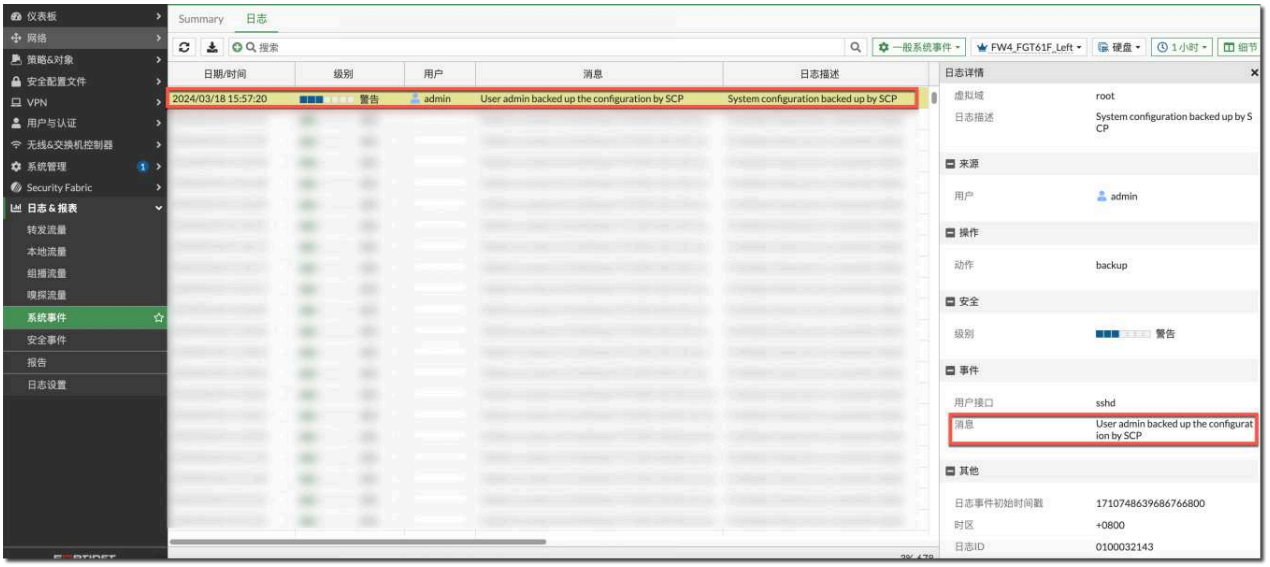
1. 打开CMD终端窗口，执行 `scp admin@<FortiGate_IP>:sys_config <location>` 命令下载配置文件到本地，如下所示，第一次SCP访问FortiGate时会提示是否信任该主机，输入yes后回车。输入password为FortiGate管理员admin的密码（也可使用其他有权限的管理员账户），备份配置成功，配置文件被下载到指定目录。

```bash
scp admin@10.10.12.1:sys_config d:\Downloads\ver
```



2. 在FortiGate上查看系统事件日志，可以看到客户端通过SCP备份配置文件的日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
date=2024-03-18 time=15:57:20 eventtime=1710748639686766920 tz="+0800" logid="0100032143" type="event" subtype="system" level="warning" vd="root" logdesc="System configuration backed up by SCP" user="admin" ui="sshd" action="backup" msg="User admin backed up the configuration by SCP"
```

重要

上传（恢复）配置文件请使用 `scp <path_to_config_file> admin@<FortiGate_IP>:fgt-restore-config` 命令，例如 `scp d:\Downloads\ver\sys_config admin@10.10.12.1:fgt-restore-config` 。

注意上传配置文件后FortiGate会立即重启，如果FortiGate属于HA集群，那么HA集群内的所有FortiGate都会同时重启并恢复此配置（不包含HA不同步的配置）。

macOS/Linux

1. 打开终端窗口，执行 `scp admin@<FortiGate_IP>:sys_config <location>` 命令下载配置文件到本地，如下所示，第一次SCP访问FortiGate时会提示是否信任该主机，输入yes后回车。输入的password为管理员admin的密码，备份配置成功，配置文件被下载到指定目录。

重要

如果客户端openSSH为9.0及以上版本，需要在 `scp` 命令后加上 `-O` 选项， `scp -O admin@<FortiGate_IP>:sys_config <location>` 。

```bash
scp -O admin@10.10.12.1:sys_config ~/Downloads/ver
```



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

上传（恢复）配置文件请使用 `scp <path_to_config_file> admin@<FortiGate_IP>:fgt-restore-config` 命令，例如 `scp ~/Downloads/ver/sys_config admin@10.10.12.1:fgt-restore-config` 。

注意上传配置文件后FortiGate会立即重启，如果FortiGate属于HA集群，那么HA集群内的所有FortiGate都会同时重启并恢复此配置。

2. 在FortiGate上查看系统事件日志，可以看到客户端通过SCP备份配置文件的日志（略，参考Windows SCP备份配置文件FortiGate产生的日志）。

SCP使SSH密钥认证

Windows

1. 打开CMD终端窗口，在默认路径下（一般为 `C:\Users\<username>` ，如此例中的路径为 `C:\Users\cyndi` ），使用 `ssh-keygen -t ed25519` 命令，生成SSH密钥对，推荐使用ed25519算法。

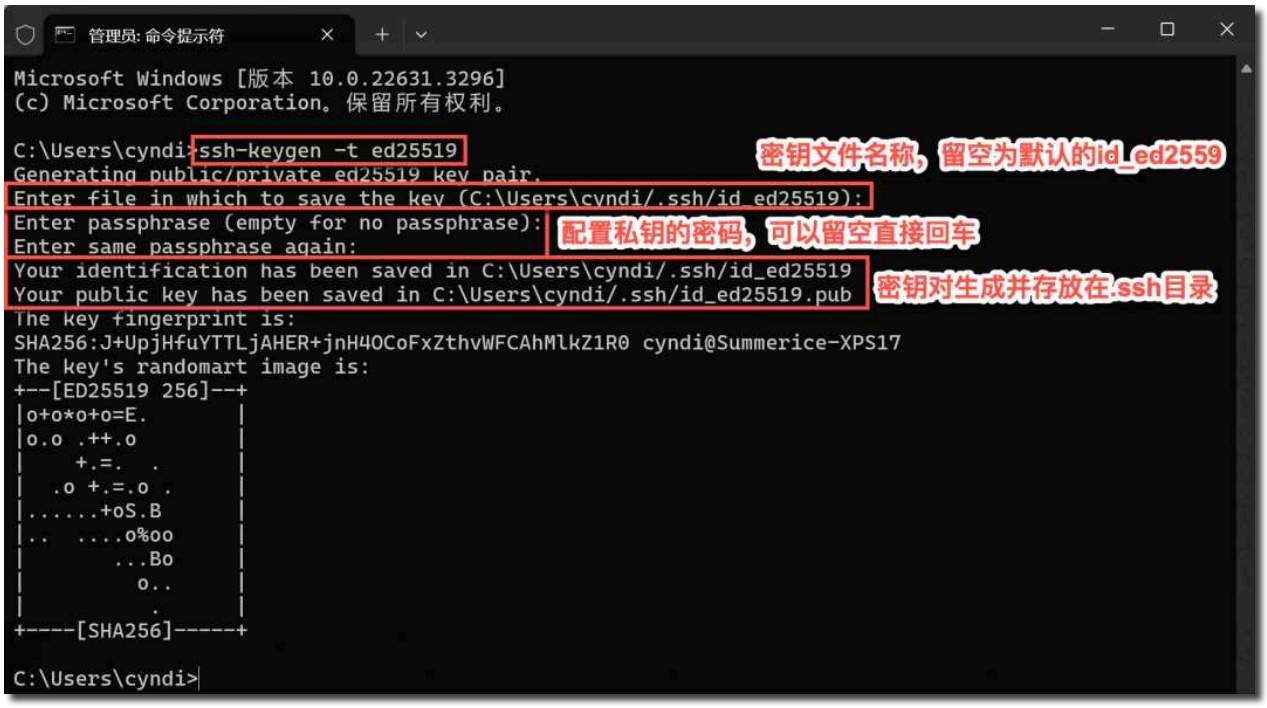
重要

`-t` 后跟随的 `ed25519` 表示SSH密钥算法，在SCP命令中可以使用dsa、ecdsa、ecdsa-sk、ed25519、ed25519-sk、rsa。

FortiGate使用ed25519和rsa作为默认的SSH密钥算法，在FortiOS 7.4.2之前，SSH密钥算法是无法更改的。

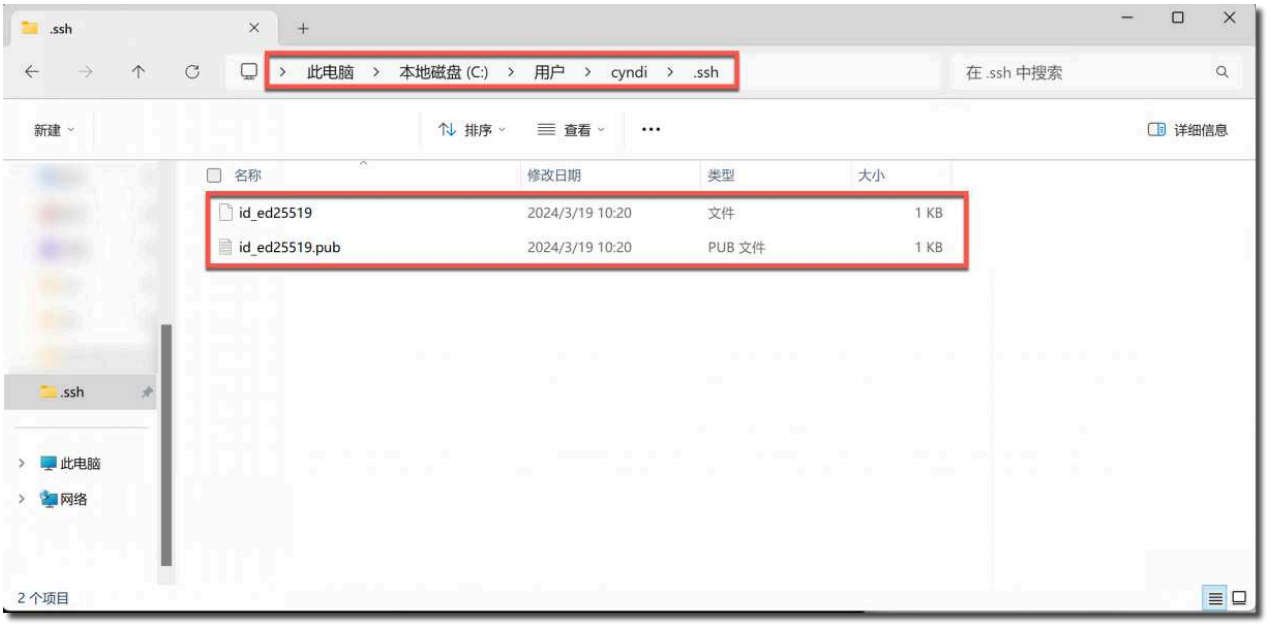
在FortiOS 7.4.2及更新版本中，可以自定义SSH密钥算法：

```bash
FortiGate # config system global
FortiGate (global) # set ssh-hostkey-algo ?
ecdsa-sha2-nistp521    ecdsa-sha2-nistp521
ecdsa-sha2-nistp384    ecdsa-sha2-nistp384
ecdsa-sha2-nistp256    ecdsa-sha2-nistp256
rsa-sha2-256           rsa-sha2-256
rsa-sha2-512           rsa-sha2-512
ssh-ed25519            ssh-ed25519
```



2. 如下所示，客户端在CMD下的默认目录（ `C:\Users\cyndi` ）生成了SSH密钥对的文件夹，该密钥对所属文件夹的名称为 `.ssh` ，由于在生成时没有自定义密钥文件名称，密钥对文件的名称为默认名称。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 使用记事本打开生成的公钥文件（后缀为pub，此例中为`C:\Users\cyndi\.ssh\id_ed25519.pub`），如下所示。

```bash
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIABtVpehNaFSWbOP13OaZKyxFsvAlSW/jtFidqa7l0×D cyndi@Summerice-XPS17
```

重要

可以看到公钥文件id_ed25519.pub由三部分组成，需要收集的为公钥文件中的前两部分：

- `ssh-ed25519`：SSH使用的密钥算法。
- `AAAAC3NzaC1lZDI1NTE5AAAAIABtVpehNaFSWbOP13OaZKyxFsvAlSW/jtFidqa7l0×D`：公钥文本。
- `cyndi@Summerice-XPS17`：用户邮箱，系统根据系统用户名与主机名自动生成，也可在生成密钥对时使用`-C`参数手工指定。

4. 在FortiGate的CLI中，编辑管理员admin的配置，设置`ssh-public-key1`的内容为公钥文件中的前两部分，即SSH使用的密钥算法和公钥文本，中间以空格隔开，前后要加上英文的双引号`""`，如下所示，`"ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIABtVpehNaFSWbOP13OaZKyxFsvAlSW/jtFidqa7l0×D"`。

重要

最多可设置3个`ssh-public-key`），`ssh-public-key`的格式输入正确时，会提示`SSH key is good.`。

```bash
FortiGate # config sys admin
FortiGate (admin) # edit admin
FortiGate (admin) # set ssh-public-key1 "ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIABtVpehNaFSWbOP13OaZKyxFsvAlSW/jtFidqa7l0×D"
SSH key is good.
FortiGate (admin) # end
FortiGate #
```

5. 在Windows下打开CMD终端窗口，执行`scp admin@<FortiGate_IP>:sys_config <location>`命令下载配置文件到本地，如下所示，第一次SCP访问FortiGate时会提示是否信任该主机，输入yes后回车。不需要输入管理员密码，备份配置成功，配置文件被下载到指定目录。

重要

如果`.ssh`文件夹下有多个SSH公钥文件，也可使用`-i <pubkey_location>`参数指定某个公钥文件进行SCP协商。

```bash
scp admin@10.10.12.1:sys_config d:\Downloads\ver
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

上传（恢复）配置文件请使用 `scp <path_to_config_file> admin@<FortiGate_IP>:fgt-restore-config` 命令，例如 `scp d:\Downloads\ver\sys_config admin@10.10.12.1:fgt-restore-config` 。

注意上传配置文件后FortiGate会立即重启，如果FortiGate属于HA集群，那么HA集群内的所有FortiGate都会同时重启并恢复此配置（不包含HA不同步的配置）。

6. 在FortiGate上查看系统事件日志，可以看到客户端通过SCP备份配置文件的日志（略，参考Windows SCP使用管理员账户密码方式备份配置文件FortiGate产生的日志）。

macOS/Linux

1. 以macOS为例，打开终端窗口，在默认路径下（一般为 `/Users/<username>` ，如此例中的路径为 `/Users/summerice` ），使用 `ssh-keygen -t ed25519` 命令，生成SSH密钥对，推荐使用ed25519算法。

重要

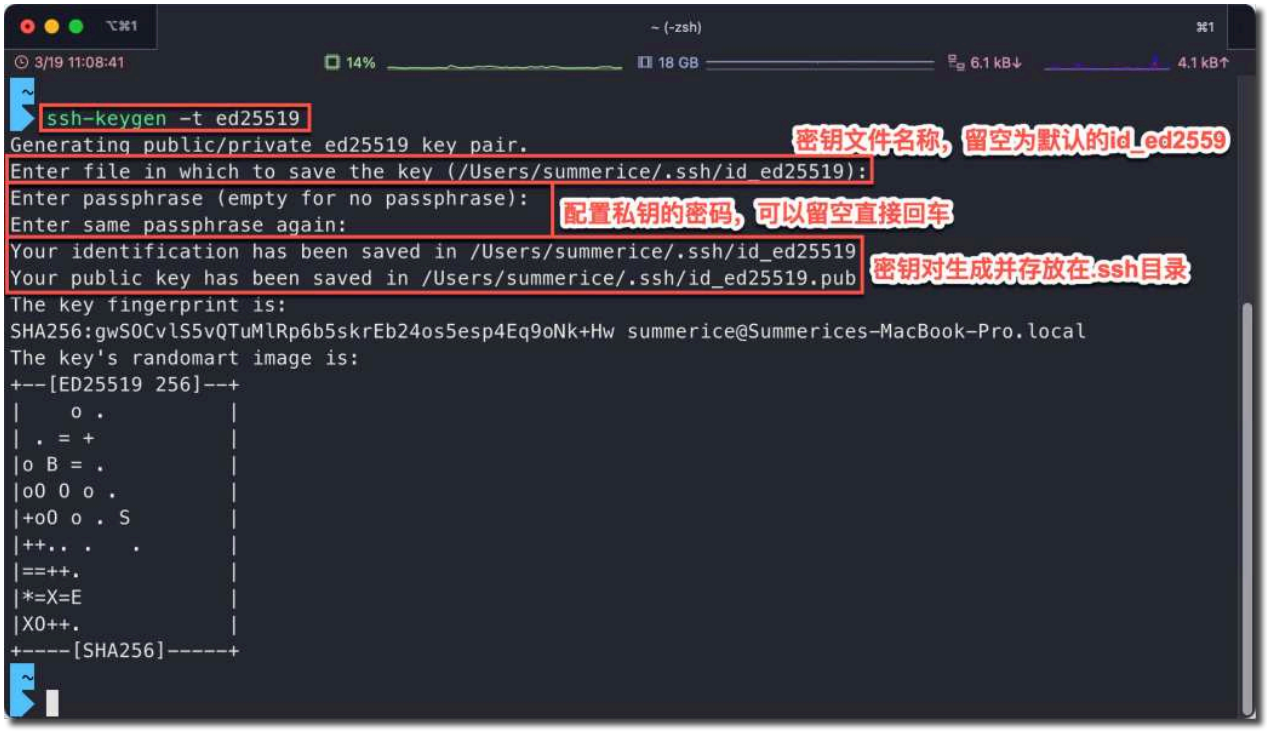
`-t` 后跟随的 `ed25519` 表示SSH密钥算法，在SCP命令中可以使用dsa、ecdsa、ecdsa-sk、ed25519、ed25519-sk、rsa。

FortiGate使用ed25519和rsa作为默认的SSH密钥算法，在FortiOS 7.4.2之前，SSH密钥算法是无法更改的。

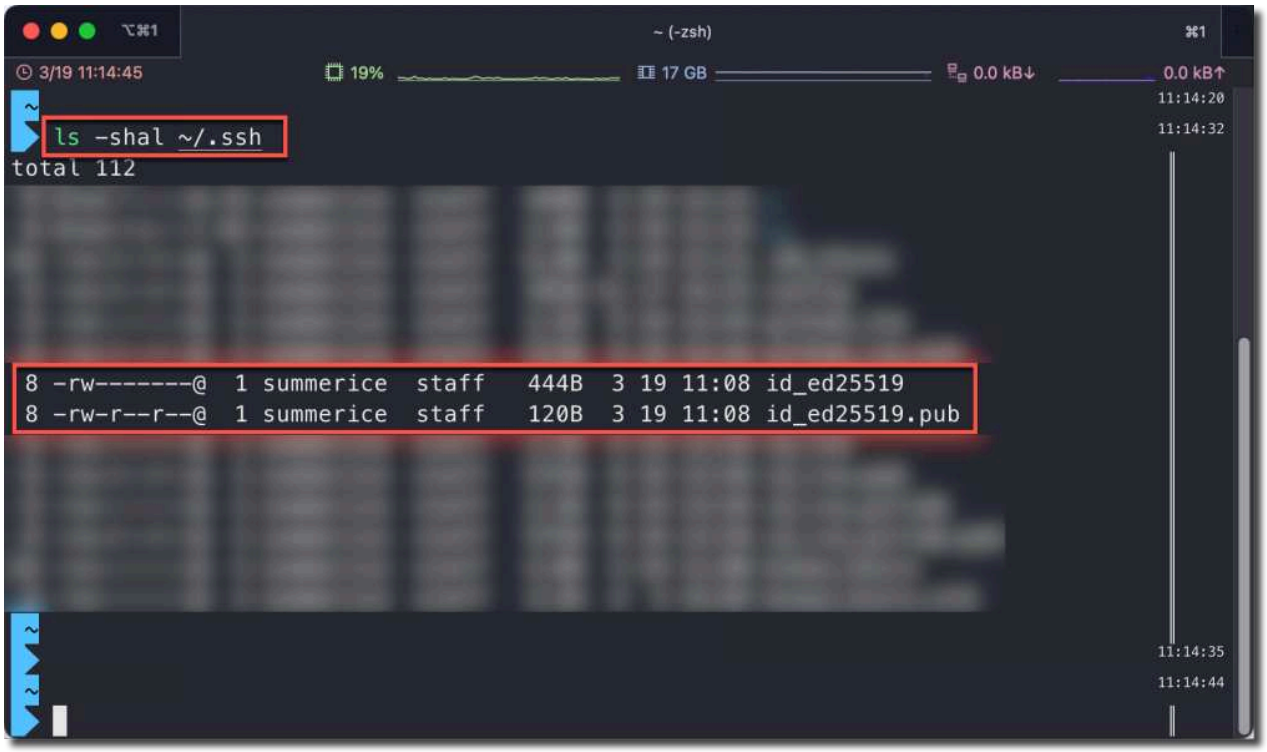
在FortiOS 7.4.2及更新版本中，可以自定义SSH密钥算法：

```bash
FortiGate # config system global
FortiGate (global) # set ssh-hostkey-algo ?
ecdsa-sha2-nistp521    ecdsa-sha2-nistp521
ecdsa-sha2-nistp384    ecdsa-sha2-nistp384
ecdsa-sha2-nistp256    ecdsa-sha2-nistp256
rsa-sha2-256           rsa-sha2-256
rsa-sha2-512           rsa-sha2-512
ssh-ed25519            ssh-ed25519
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 如下所示，客户端在终端下的默认目录（`/Users/summerice`，在macOS或Linux下也可以用`~`表示该目录）生成了SSH密钥对的文件夹，该密钥对所属文件夹的名称为`.ssh`，由于在生成时没有自定义密钥文件名称，密钥对文件的名称为默认名称。



3. 使用`cat`命令查看生成的公钥文件（后缀为pub，此例中为`~/.ssh/id_ed25519.pub`）的内容，如下所示。

```bash
$ cat ~/.ssh/id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGGp5Pv2JGgGjmV+jOeSPwEbJsMAiz7tLJDsZQpCAvwg summerice@Summerices-MacBook-Pro.local
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

可以看到公钥文件id_ed25519.pub由三部分组成，需要收集的为公钥文件中的前两部分：

- `ssh-ed25519`：SSH使用的密钥算法。
- `AAAAC3NzaC1lZDI1NTE5AAAAIGGp5Pv2JGgGjmV+jOeSPwEbJsMAiz7tLJDsZQpCAvwg`：公钥文本。
- `summerice@Summerices-MacBook-Pro.local`：用户邮箱，系统根据系统用户名与主机名自动生成，也可在生成密钥对时使用`-C`参数手工指定。

4. 在FortiGate的CLI中，编辑管理员admin的配置，设置`ssh-public-key2`的内容为公钥文件中的前两部分，即SSH使用的密钥算法和公钥文本，中间以空格隔开，前后要加上英文的双引号`""`，如下所示，`"ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGGp5Pv2JGgGjmV+jOeSPwEbJsMAiz7tLJDsZQpCAvwg"`。

重要

最多可设置3个`ssh-public-key`，`ssh-public-key`的格式输入正确时，会提示`SSH key is good.`。

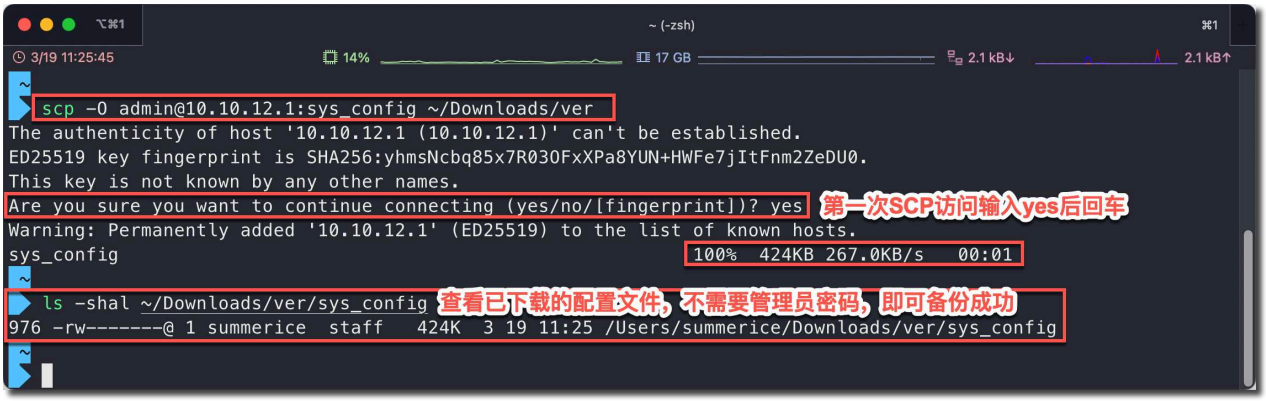
```
FortiGate # config sys admin
FortiGate (admin) # edit admin
FortiGate (admin) # set ssh-public-key2 "ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGGp5Pv2JGgGjmV+jOeSPwEbJsMAiz7tLJDsZQpCAvwg"
SSH key is good.
FortiGate (admin) # end
FortiGate #
```

5. 打开macOS的终端窗口，执行`scp admin@<FortiGate_IP>:sys_config <location>`命令下载配置文件到本地，如下所示，第一次SCP访问FortiGate时会提示是否信任该主机，输入yes后回车。不需要输入管理员密码，备份配置成功，配置文件被下载到指定目录。

重要

如果客户端openSSH为9.0及以上版本，需要在`scp`命令后加上`-O`选项，`scp -O admin@<FortiGate_IP>:sys_config <location>`。

```
scp -O admin@10.10.12.1:sys_config ~/Downloads/ver
```
bash



重要

上传（恢复）配置文件请使用`sudo scp -O <path_to_config_file> admin@<FortiGate_IP>:fgt-restore-config`命令，例如`sudo scp -O ~/Downloads/ver/sys_config admin@10.10.12.1:fgt-restore-config`。

注意上传配置文件后FortiGate会立即重启，如果FortiGate属于HA集群，那么HA集群内的所有FortiGate都会同时重启并恢复此配置。

6. 在FortiGate上查看系统事件日志，可以看到客户端通过SCP备份配置文件的日志（略，参考Windows SCP使用管理员账户密码方式备份配置文件FortiGate产生的日志）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

恢复出厂

需求

当需要把设备的所有配置删除，可进行恢复出厂操作。恢复出厂后所有配置都将丢失，若一定要恢复出厂设置建议前先备份当前的配置；备份配置操作步骤请参考系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗。

> **重要**
>
> 设备的授权信息都在云端，恢复出厂配置后保证设备联网就可重新获取授权信息。

配置要点

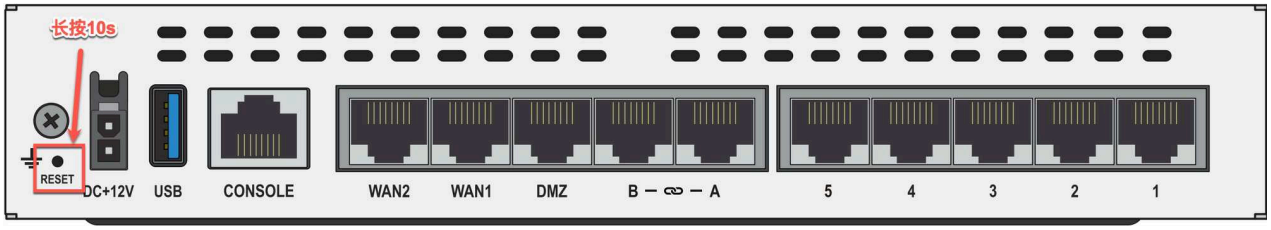
1. 恢复出厂设置会清空所有配置，系统会自动重启。
2. 恢复出厂设置后，internal口或则MGMT口地址恢复为192.168.1.99。

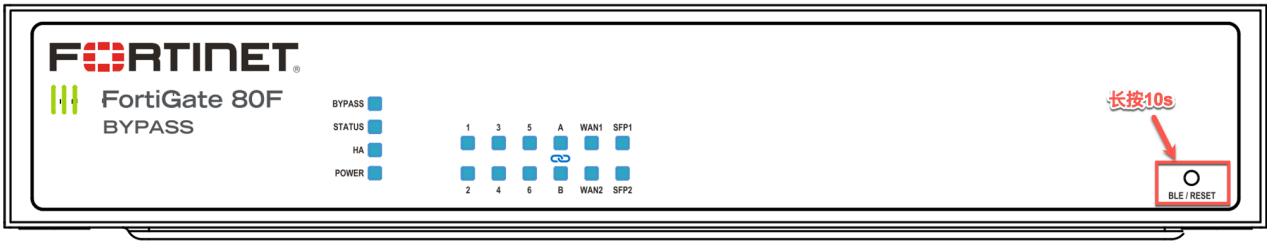
操作步骤

1. 第一种方式：命令行方式：进入命令行，执行execute factoryrest命令，回车后会提示此操作将会恢复出厂配置，是否继续，输入字母"y"即可。

```
FortiGate # execute  factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n) y
```

2. 第二种方式：通过设备上reset复位键（仅部分型号等有reset键，其他型号无法执行此操作）：reset键操作防火墙系统正常启动后（可以ping通或登录管理页面）30S内，长按10S左右，系统将自动重启，届时将恢复为出厂设置。如下所示60F和80F的重置按钮位置。





验证效果

恢复出厂设置后，管理口地址恢复为192.168.1.99，可通过此地址登陆https://192.168.1.99 ↗ 进行管理，用户名和密码分别恢复默认的admin和空。

注意事项

恢复出厂不清空硬盘日志，恢复出厂仅针对配置文件而言。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置回退

网络需求

当网络管理员通过远程方式变更FortiGate配置时，错误的配置可能会造成访问丢失。这种情况下，需要在配置错误并失去访问连接的情况下，自动回退FortiGate配置到错误配置下发前的状态。

配置步骤

> **重要**
>
> 强烈建议在修改设备关键配置（特别是与设备连通性相关的配置时），避免通过远程的方式进行操作。如果必须通过远程的方式进行操作，才考虑使用此方法。

1. 在进行远程配置变更前，将FortiGate的配置保存方式设置为`revert`，`cfg-revert-timeout`默认值为600s。

> **重要**
>
> 在配置变更结束后，请将配置保存模式恢复为“自动”。




```
config system global
    set cfg-save revert
    set cfg-revert-timeout 600
end
```

配置保存模式有以下3种：

- `Automatic`（默认）：配置更改会实时下发到Memory和Flash。
- `manual`：配置更改只会下发到Memory，不下发到Flash，必须手动下发到Flash中（通过GUI或`exe cfg save`），未手动保存到Flash的配置将会在重启后丢失。修改配置后，会显示有配置未保存的提示，点击提示可以查看具体修改的配置内容。
- `revert`：配置更改只会下发到Memory，不下发到Flash。当配置更改后，如果在cfg-revert-timeout时间内未手动保存配置（通过GUI或`exe cfg save`），设备会Reload并恢复Flash中的原有配置文件（重启前GUI会提示相关告警信息提示手动保存配置）。配置文件Reload期间，设备业务会产生中断，所以在配置变更结束后，请将配置保存模式恢复为“自动”。

2. 修改设备配置，例如修改接口IP，查看修改接口前的IP地址如下。

```bash
config system interface
    edit "wan1"
        set ip 3.3.3.3 255.255.255.0
    next
end
```

3. 修改该接口IP到其他IP地址，此时配置会下发到内存中并生效，而不会下发到Flash中。

```bash
config system interface
    edit "wan1"
        set ip 4.3.3.3 255.255.255.0
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end
```

4. 如果GUI仍然可以访问，GUI页面右上角会提示配置已变更，若未在600s内手动点击“保存阶段性更改”（或CLI执行`exe cfg save`）将配置保存到Flash中，设备会Reload并恢复Flash中的原有配置。



5. 假如步骤3为误操作，导致FortiGate无法远程管理，等待600s后，FortiGate会重载（Reload，非重启设备）Flash中的配置文件。可以看到Reload之后，接口IP恢复到修改之前的IP地址。

> **重要**
>
> - Reload期间，设备业务会产生中断，所以在配置变更结束后，请将配置保存模式恢复为“自动”。
> - 在HA环境下，所有HA成员都会同时执行Reload。

```bash
config system interface
    edit "wan1"
        set ip 3.3.3.3 255.255.255.0
    next
end
```

6. 设备Reload期间的Console记录。

```bash
FortiGate #
System will reload in the next 10 seconds ...
System will reload in the next 9 seconds ...
System will reload in the next 8 seconds ...
System will reload in the next 6 seconds ...
System will reload in the next 5 seconds ...
System will reload in the next 4 seconds ...
System will reload in the next 3 seconds ...
System will reload in the next 1 seconds ...
......
FortiGate login:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

管理员设置

功能需求

设备出厂时设备内置的默认账号为admin（拥有所有权限），默认密码：空，现在需求如下：

1. 修改管理员admin的密码为fgt@123, 设置管理员admin账号的管理主机IP为172.18.10.108/32，即只有172.18.10.108这台主机可以用admin账号管理设备。
2. 添加管理员账号monitor，配置密码为123456a!，权限设置为test，管理主机IP不限，即所有主机都能用此账号登陆设备管理，权限为只读。
3. 定义密码规则，对密码的复杂度进行限制。
4. 设置Web页面超时时间：若设置为90分钟，则90分钟内管理员未做任何操作，则自动退出管理页面。

配置要点

1. 修改管理员密码，管理IP。
2. 添加访问内容表readonly。
3. 添加管理员monitor。
4. 定义密码规则，修改设备管理参数。
5. 设置管理登录超时时间。

配置步骤

修改admin管理员密码/管理IP

1. 进入系统管理→管理员页面。



2. 编辑用户名"admin"（双击或者点击编辑按钮）点击"更改密码"。

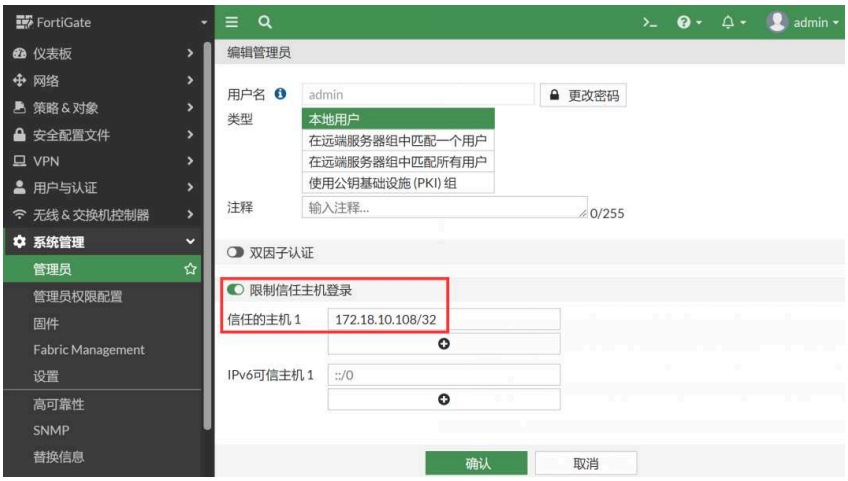


3. 在随后出现的修改密码弹出窗口内，输入新密码fgt@123，点击确定。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 启用"限制信任主机登录"在"信任的主机1"处填写管理IP：172.18.10.108/32，点击"确定"。



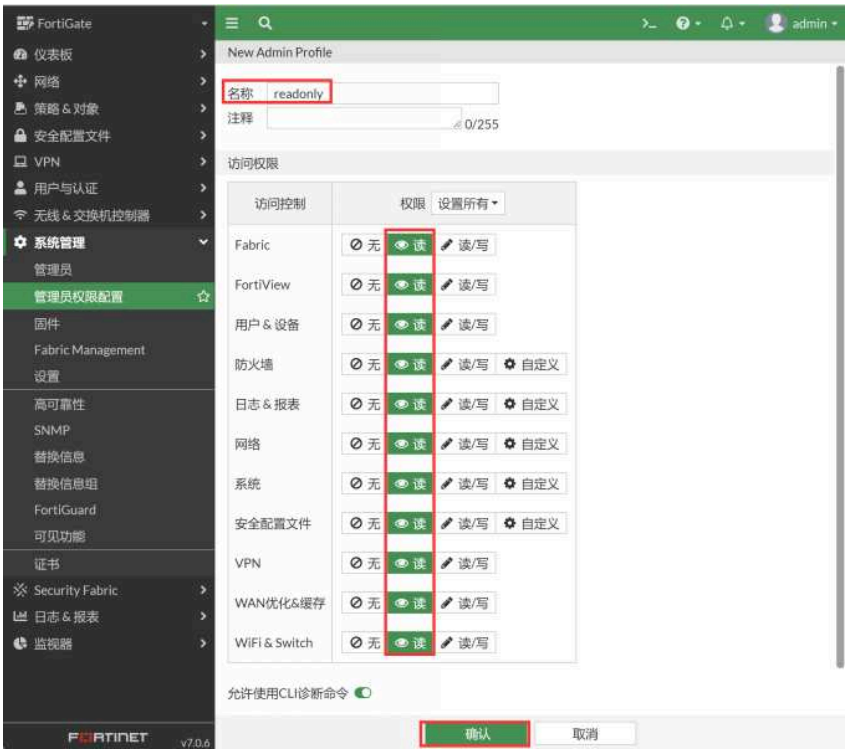
添加访问内容表readonly

1. 进入系统管理→管理员权限配置→新建。



2. 输入名称：readonly，所有勾选只读权限，点击"确认"。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

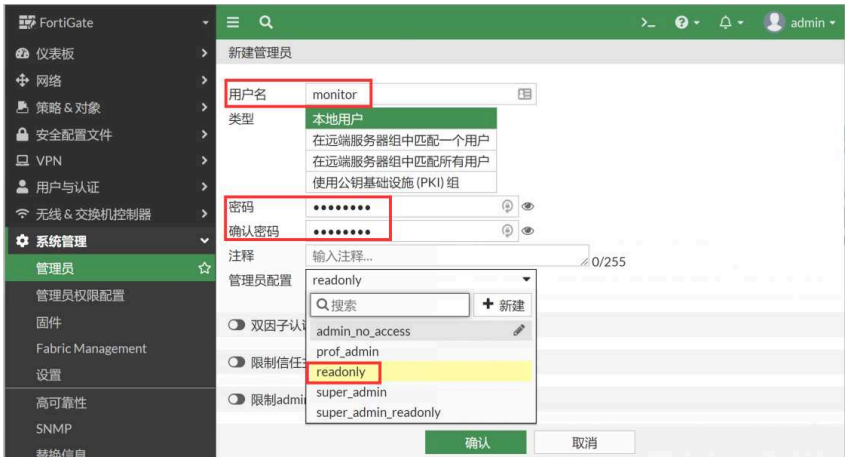


添加管理员monitor

1. 进入系统管理→管理员，点击新建→管理员。



2. 添加管理员monitor，密码：123456a!，权限设置为readonly，管理主机IP不限制，如下图所示。



登录超时时间

1. 默认配置下，管理员在登录FortiGate（GUI/SSH/Console等）5分钟内如果没有任何操作，系统会自动登出该管理员的登录状态。

2. 可以修改管理员的登录超时时间范围为1~480min，如下所示修改管理员的空闲时间为60分钟。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system global
    set admintimeout 60
end
```

结果验证

使用monitor账号登陆设备，修改配置，提示没有权限错误。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

远程认证管理员

除了本地配置的管理员，FortiGate还支持远程认证的管理员登录，如LDAP、Radius、Tacacs+等。

远程认证服务器配置

LDAP服务器配置请参考：用户与认证→LDAP认证→LDAP认证配置与排错 ↗。

Radius服务器配置请参考：用户与认证→Radius认证→Radius认证配置与排错 ↗。

远程认证管理员配置

1. 这里以LDAP用户为例，参考上述配置步骤，已经配置了LDAP远程服务器和远程用户组。

```bash
config user ldap
    edit "LDAP"
        set server "192.168.100.50"
        set cnid "cn"
        set dn "dc=summerice2019,dc=com"
        set type regular
        set username "administrator"
        set password xxxxxxxx
    next
end
config user group
    edit "LDAP_Users"
        set member "LDAP"
        config match
            edit 1
                set server-name "LDAP"
                set group-name "CN=ad_group1,DC=summerice2019,DC=com"
            next
            edit 2
                set server-name "LDAP"
                set group-name "CN=Users,CN=Builtin,DC=summerice2019,DC=com"
            next
        end
    next
end
```

2. 进入FortiGate的“系统管理→管理员”页面，新建管理员。



- 类型：
  - 用户名：管理员用户名，解释如下。
  - 类型：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 在远端服务器组中匹配一个用户：使用配置的用户名匹配远程服务器中的用户，管理员配置的用户名必须属于远程认证服务器中的一个用户，用户登陆时也必须使用这个用户名。
- 在远端服务器组中匹配所有用户：使用管理员登录时输入的用户名匹配远程服务器中的用户，管理员配置的用户名不必属于远程认证服务器中的任何用户（可随意配置），用户登陆时使用LDAP服务器上的用户名输入。

- 备份密码：当远程认证服务器不可用时，可以使用备份密码作为逃生密码（使用“在远端服务器组中匹配所有用户”的类型时，无法配置备份密码）。
- 管理员配置：该管理员所拥有的管理员权限。
- 远端用户组：选择上步中创建的LDAP用户组。

3. 以上配置对应的CLI如下。

```
config system admin
    edit "ldap_user"
        set remote-auth enable
        set accprofile "super_admin"
        set vdom "root"
        set remote-group "LDAP_Users"
        set password ENC SH2Cn+7WDWNOQFNb12zdDAuL/XVDN6ga4qxCtdB9lEV8FwRkSjPQixI/Rm07s8=
    next
end
```

4. 如果使用“在远端服务器组中匹配所有用户”类型，对应的CLI如下。

```
config system admin
    edit "ldap_user"
        set remote-auth enable
        set accprofile "super_admin"
        set vdom "root"
        set wildcard enable
        set remote-group "LDAP_Users"
    next
end
```

注意事项

1. 如果FortiGate的认证用户组中配置了多个远程认证服务器，如下包含了LDAP和Radius两个服务器。




```
config user group
    edit "Remote_Users"
        set member "LDAP" "Radius"
        config match
            edit 1
                set server-name "LDAP"
                set group-name "CN=Users,CN=Builtin,DC=summerice2019,DC=com"
            next
            edit 2
                set server-name "LDAP"
                set group-name "CN=ad_group1,DC=summerice2019,DC=com"
            next
        end
    next
end
```

2. 那么FortiGate会先到哪个认证服务器去认证呢?

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 对于FortiGate来说，两个认证服务器没有优先顺序，认证报文会同时发送至LDAP与Radius，哪个服务器先返回了认证结果，FortiGate就采用哪个服务器返回的认证结果。

4. 排除网络延迟的差异，由于Radius认证采用的是UDP协议，通常会比LDAP更快的返回认证结果，从而导致FortiGate优先采用Radius的认证结果，但这并不代表Radius认证优先于LDAP认证。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

远程认证与本地认证的优先级

配置方法

远程认证与本地认证的优先级由以下命令决定，默认为disable状态。

```
config system global
    set admin-restrict-local ?    //Enable/disable local admin authentication restriction when remote authenticator
is up and running (default = disable).
    enable     Enable local admin authentication restriction.
    disable    Disable local admin authentication restriction.
end
```

默认情况（disable）

```
config system global
    set admin-restrict-local diable
end
```

- 如果远程和本地有相同的用户名，不同的密码，则本地认证有效。
- 如果用户名/密码都一样，也是本地认证有效。
- 使用diagnose debug application fnbamd -1可以观察到，认证直接在本地完成，不会送到远程服务器上。

修改为enable

```
config system global
    set admin-restrict-local enable
end
```

- 当任何一个远程认证服务器可达时，远程认证服务器生效，本地认证无效。
- 只有当FortiGate到远程认证服务器不可达时，本地认证才有效。
- 如果远程服务器和本地有相同的用户名，认证会先到远程服务器上，但是登录会直接显示失败（无论使用远程用户还是本地用户的密码，无论远程用户和本地用户的密码是否相同）。

> **重要**
>
> 在7.6.0版本之前，Console可以使用本地账户登录，不受此功能开启的限制。

多个远程认证服务器的情况（set admin-restrict-local enable）

7.2.0之前

当FortiGate配置了多个远程认证服务器，只配置了一个远程认证服务器与管理员关联，举例：FortiGate同时配置了LDAP与Radius服务器，但只有LDAP服务器与管理员配置了关联，Radius服务器没有与任何管理员配置关联：

- 当任何一个远程认证服务器可达时，远程认证服务器生效，本地认证无效。
- 只有当FortiGate到所有的远程认证服务器（上述举例为LDAP、Radius）不可达时，本地认证才有效，即使Radius认证服务器没有关联任何管理员。

7.2.0及之后

当FortiGate配置了多个远程认证服务器，只配置了一个远程认证服务器与管理员关联，举例：FortiGate同时配置了LDAP与Radius服务器，但只有LDAP服务器的用户组与管理员配置了关联，Radius服务器没有与任何管理员配置关联：

- 只要防火墙管理认证调用的远程认证服务器不可达，本地用户认证就可以生效。

7.6.0新增选项

```
config system global
    set admin-restrict-local {all | non-console-only | disable}
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- `non-console-only`：行为与7.6.0之前的 `enable` 一致（Console登录不受admin-restrict-local影响）。
- `all`：行为与7.6.0之前的 `enable` 一致（Console登录同样受admin-restrict-local影响）。
- `disable`：行为与7.6.0之前的 `disable` 一致。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

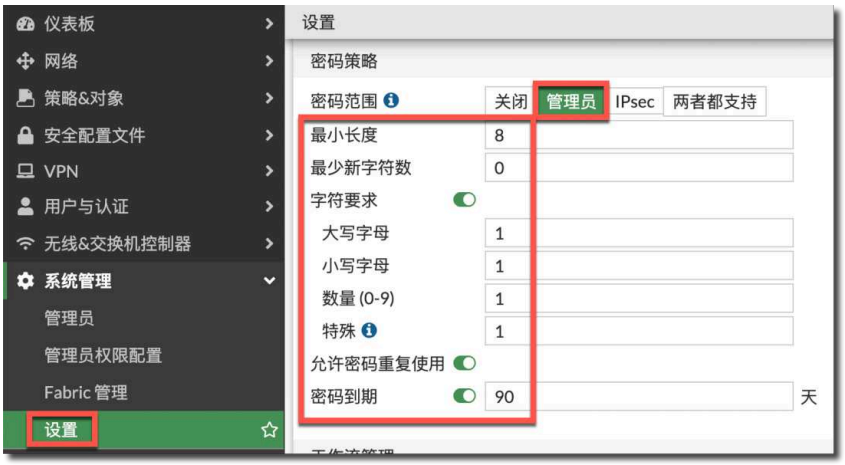
管理员密码策略

功能简介

默认情况下，FortiGate的管理员的密码复杂度没有要求，如果需要对管理员设置密码时的字符复杂度做一定的限制，可以开启密码策略功能。

配置步骤

1. 进入系统管理→设置页面，在密码策略选项中，密码范围选择管理员（也可以配置IPSec预共享密钥的复杂度）：



- 最小长度：密码的最小字符长度
- 最少新字符数：修改密码时，允许新密码有多少个字符是旧密码中包含的
- 字母要求：
  - 大写字母：密码中至少包含的大写字母数量
  - 小写字母：密码中至少包含的小写字母数量
  - 数量：密码中至少包含的数字的数量
  - 特殊：码中至少包含的特殊字符（如_/!@）数量
- 允许密码重复使用：如果关闭，则在修改密码时不允许使用已经使用过的密码
- 密码到期：密码到期后会提示管理员修改密码

2. 相关的CLI配置：

```
config system password-policy
    set status enable
    set min-lower-case-letter 1
    set min-upper-case-letter 1
    set min-non-alphanumeric 1
    set min-number 1
    set expire-status enable
end

config system admin
    edit "admin"
        set accprofile "super_admin"
        set vdom "root"
        set password-expire 2023-11-22 16:21:57
        set password ENC SH2jjHLAz03uN2uhVHV9GR+F11BbxS4a2J4/3V7vnwwYJmFdG4btcop1QwEMI8=
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

密码策略仅支持管理员账户密码和IPSec预共享密钥，不支持防火墙认证用户。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

通过FortiCloud账户登录FortiGate

功能介绍

可以使用FortiGate所注册的FortiCloud账户登陆FortiGate，当用户有多台属于同一FortiCloud账户下的设备时，使用同一个FortiCloud账户登录多台FortiGate，方便用户统一管理设备账户与密码，减少维护成本。

支持FortiCloud主账户登录，也支持FortiCloud下注册的IAM账户登录。

注意事项

1. 账户必须是FortiGate注册到FortiCloud的账户。

2. 开启后登录界面的本地账户密码输入框默认隐藏，点击用户名输入框后可以显示。

3. 权限选择继承模式时，FortiCloud主账户总是拥有Super admin权限，IAM用户可以在FortiCloud中设置Super admin或Readonly权限。

4. 如果FortiCloud主账号开启了双因子认证，则其下面的IAM账户也必须开启双因子认证才能登陆。

> **重要**
>
> 在7.2.4 GA后，可以在FortiGate本地设置覆盖FortiCloud账号的权限。

配置步骤

FortiGate配置

1. 进入设备管理页面的“系统管理→设置”页面中，在单点登录部分开启“FortiCloud单点登录”。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- **继承自FortiCloud**：默认情况下，FortiCloud单点登录账户的权限（Default admin profile）会从FortiCloud的配置中继承，FortiCloud主账户总是拥有Super admin权限，IAM用户可以在FortiCloud中设置Super admin或Readonly权限。
- **指定**：在7.2.4 GA后，可以选择Default admin profile的模式为指定，本地覆盖FortiCloud账户的权限。

2. 对应的CLI如下。

```
config system global
    set admin-forticloud-sso-login enable
    set admin-forticloud-sso-default-profile 'super_admin'    //这里的配置为指定模式，如果为继承模式，则这里为空，即''
end
```

3. 这里我们先配置为默认的继承模式测试。

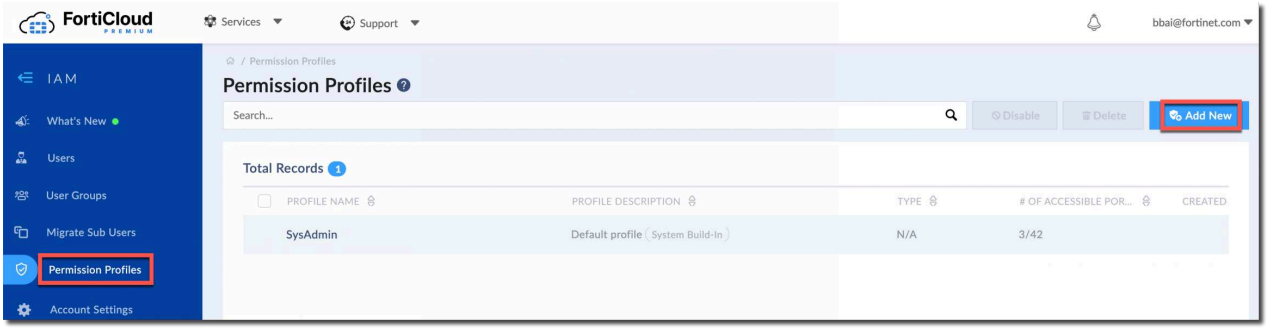
FortiCloud IAM账户配置

重要

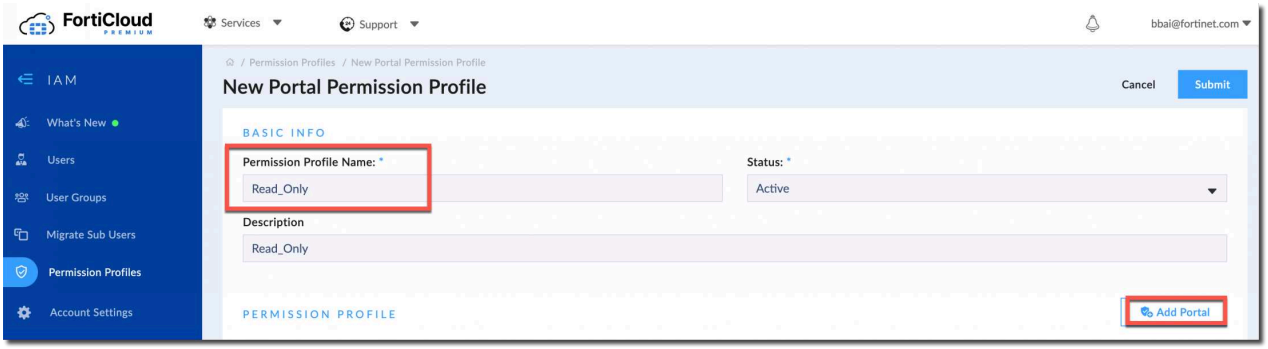
如果需要通过FortiCloud下的IAM子账户登录FortiGate，则需要配置此部分。如果只需要使用FortiCloud主账户登录FortiGate，则不需要配置此部分。

1. 通过https://support.fortinet.com/iam ↗ 使用FortiCloud主账户登录FortiCloud IAM账户管理界面。

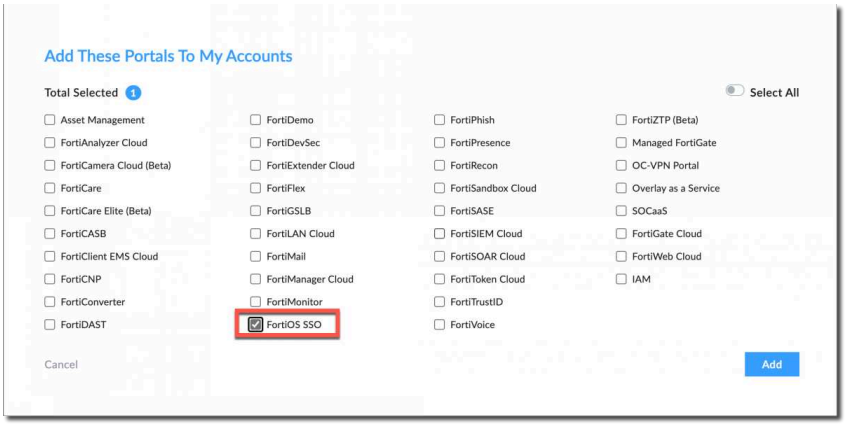
2. 进入Permission Profiles界面，右上角点击新建Permission Profiles。



3. 填写Permission Profiles名称，点击右下角的Add Portal按钮。

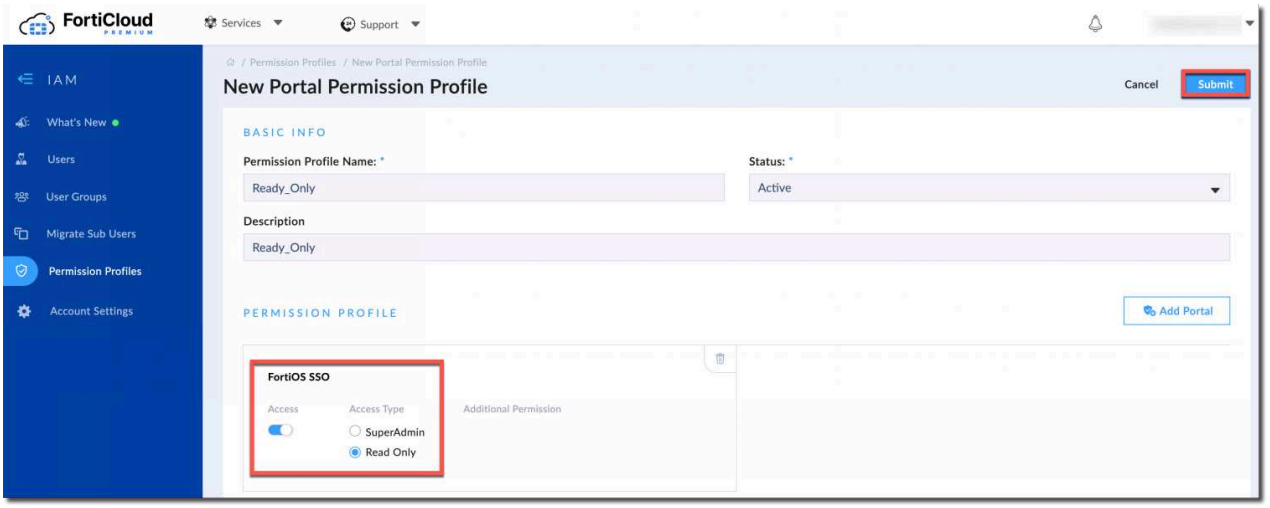


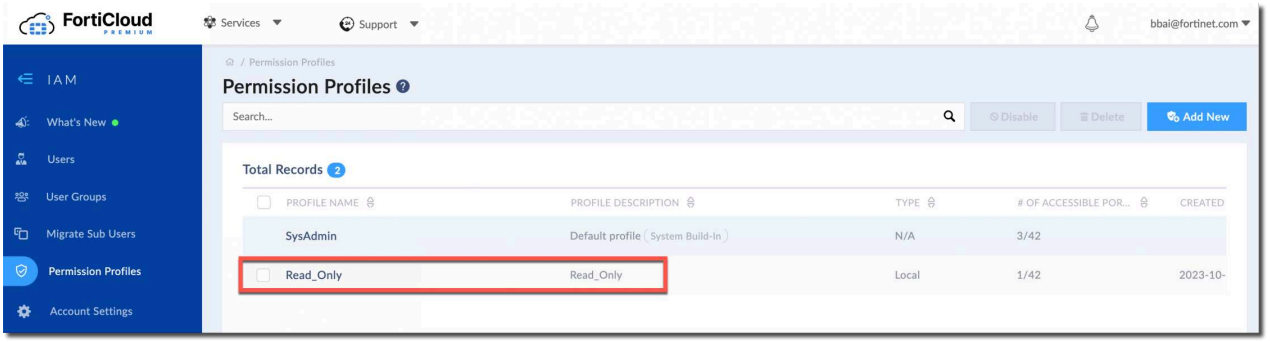
4. 在弹出的页面中选择“FortiOS SSO”，点击Add。



5. 开启Access按钮，右侧选择Access Type为Ready Only，点击右上角的Submit按钮提交配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

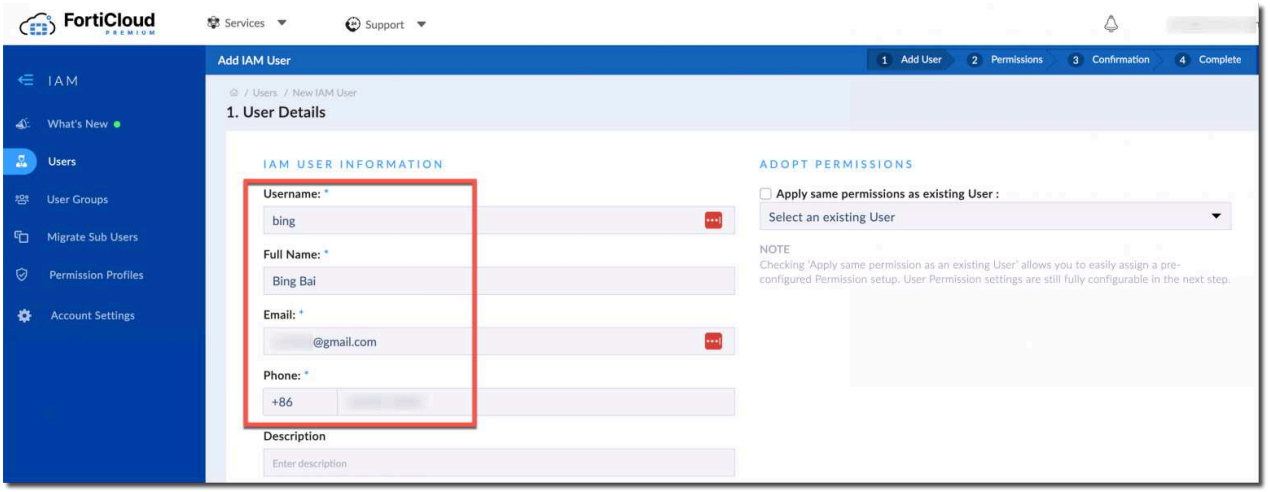




6. 进入Users界面，右上角点击新建IAM User。

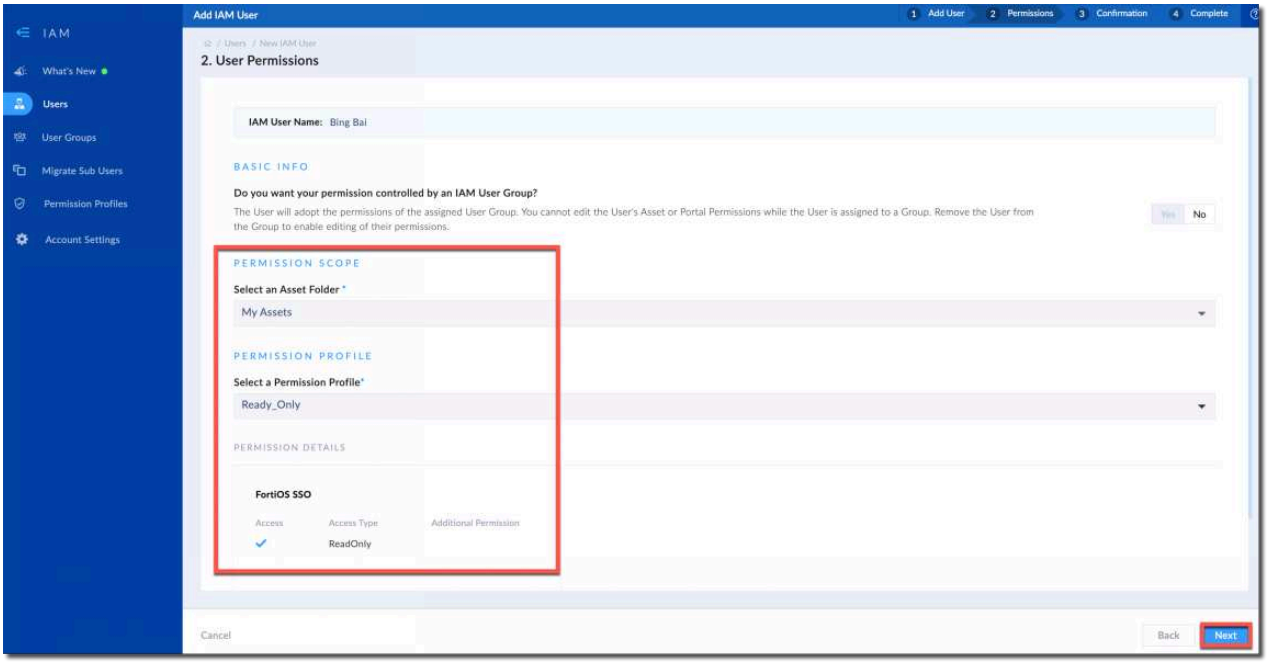


7. 填写用户相关信息，Username用于登录FortiGate，点击Next。

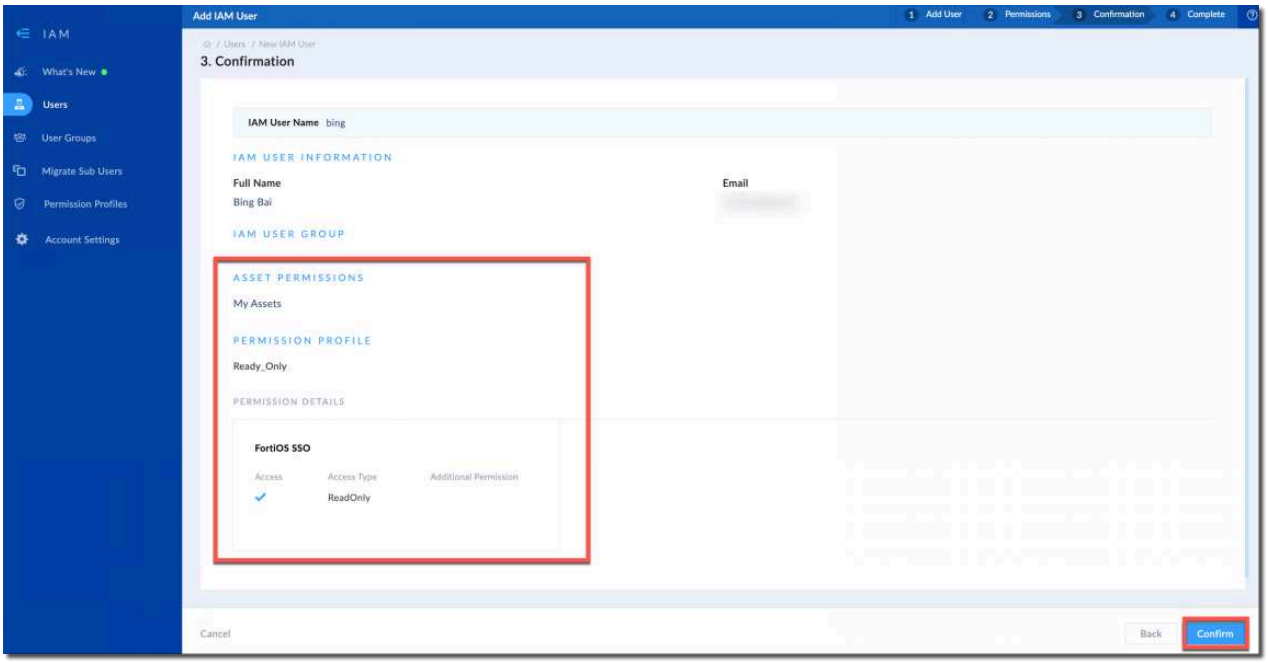


8. 选择该用户的Asset Folder，选择之前创建的Permission Profile Ready_Only，点击Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

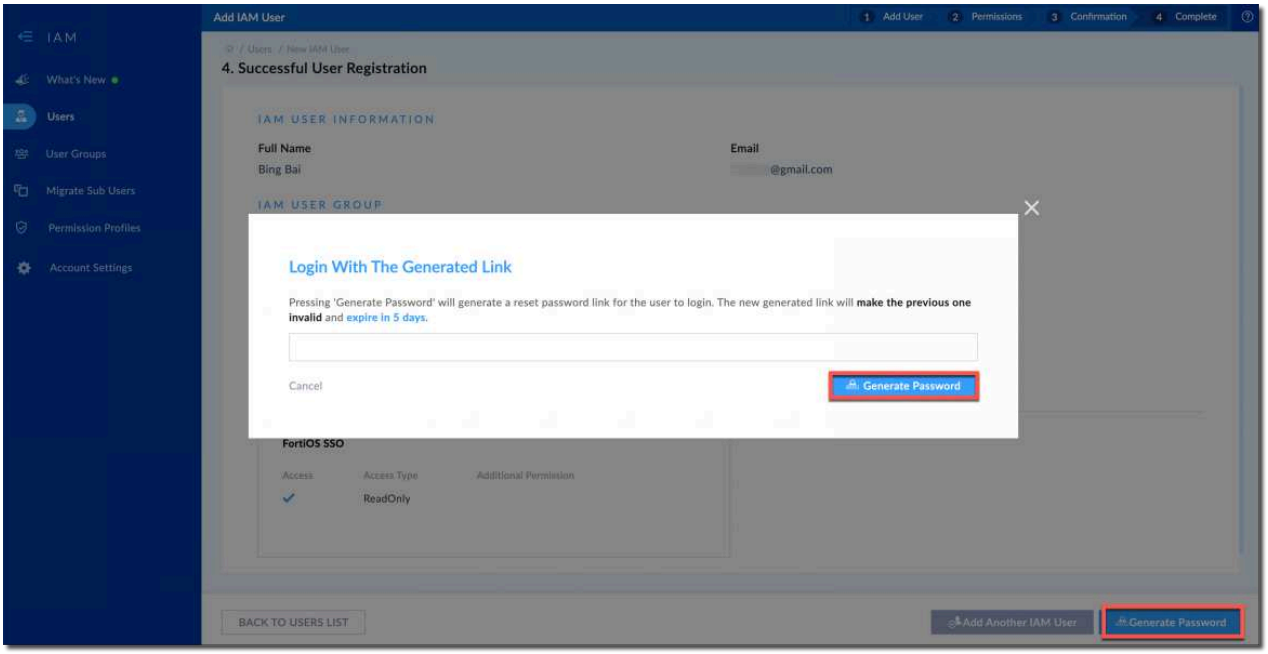


9. 确认信息无误后，点击Confirm创建账户。

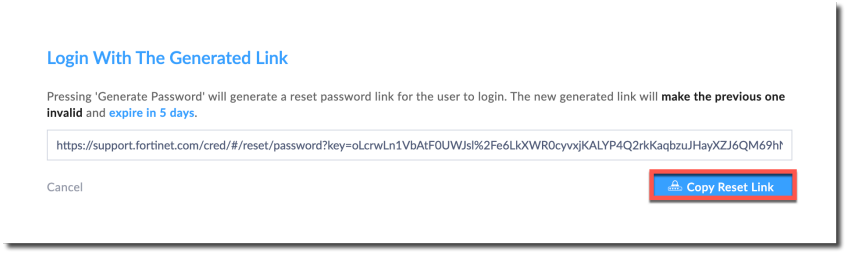


.0. 在后续页面的右下角点击Generate Password按钮，在弹出的窗口中点击Generate Password按钮。

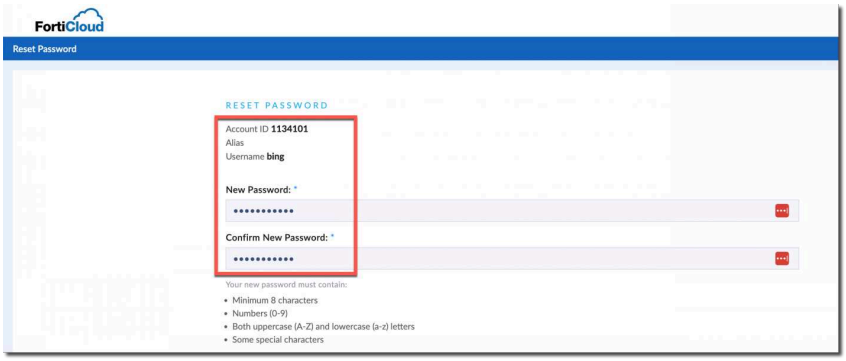
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. 复制生成的URL，并使用浏览器打开。



2. 在该URL下配置IAM用户的密码，记住这里的Account ID，将用于IAM账户登录使用，点击Submit提交密码配置。

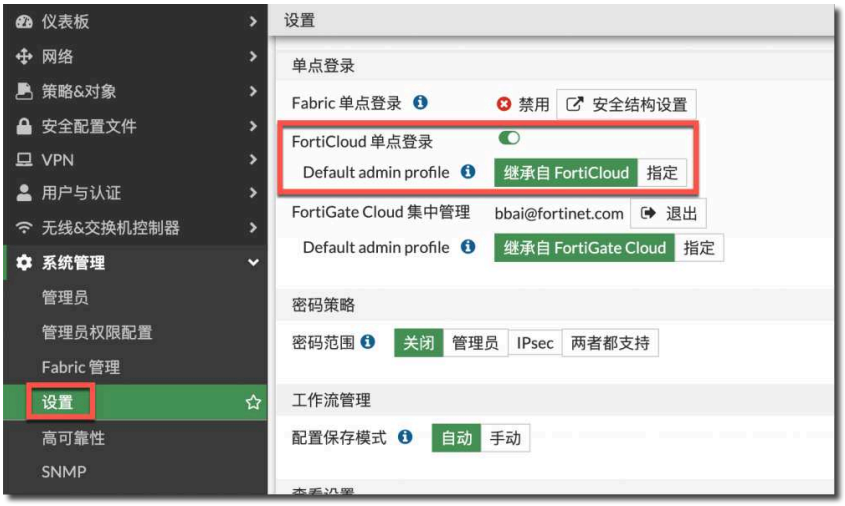


结果验证

FortiCloud主账户登录

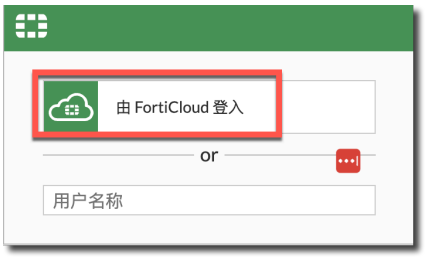
1. Default admin profile为继承自FortiCloud。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

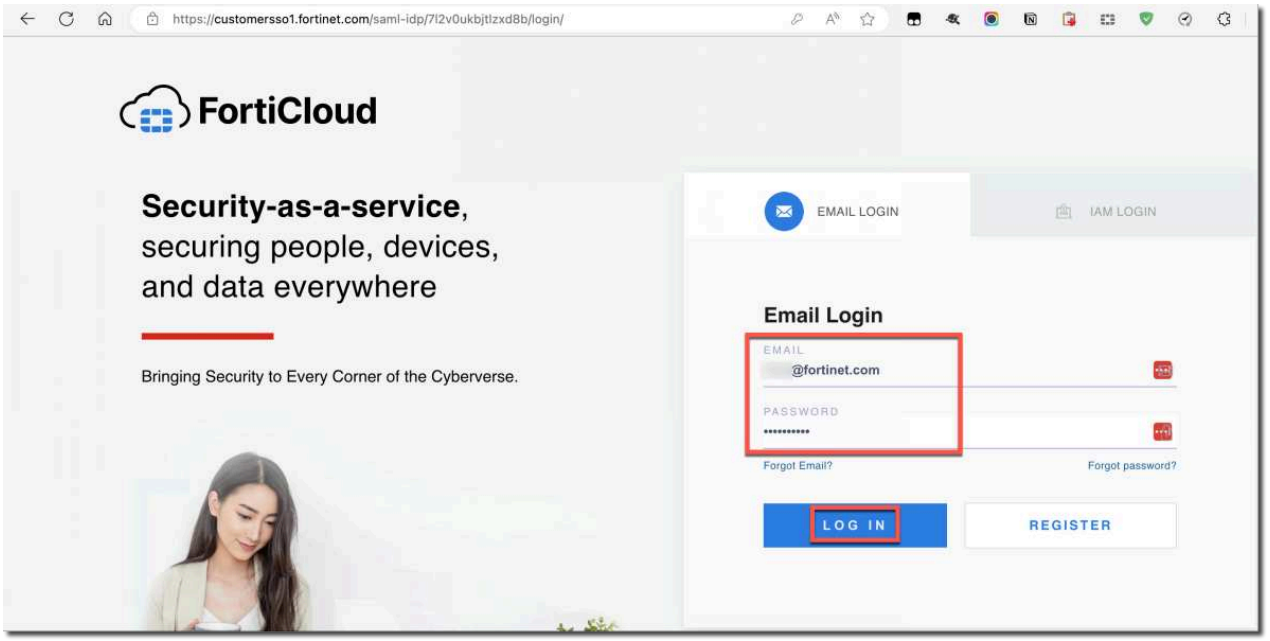



```
config system global
    set admin-forticloud-sso-login enable
    set admin-forticloud-sso-default-profile ''
end
```

2. 访问FortiGate登陆页面，可以看到增加了“由FortiCloud登入”的选项。

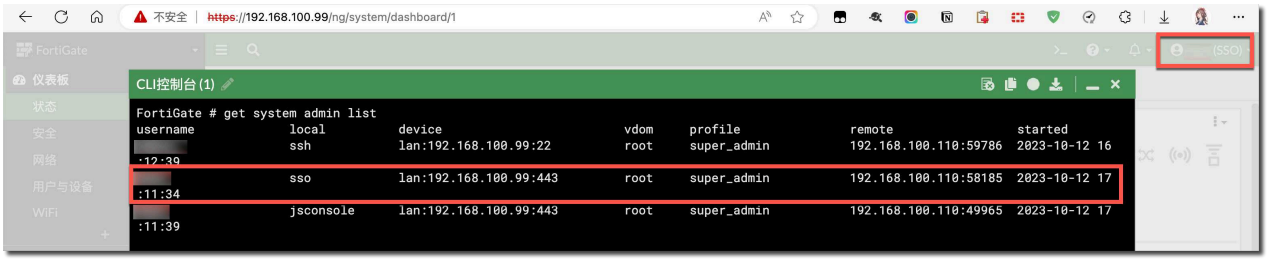


3. 选择Email Login方式，填入设备注册到的FortiCloud主账户和密码，点击Log in按钮。



4. 登录FortiGate成功，登录后的权限为super_admin。

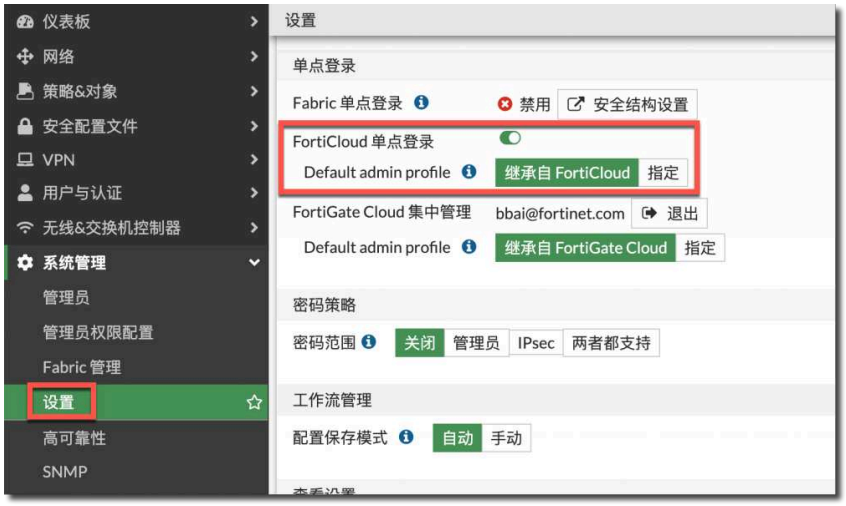
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



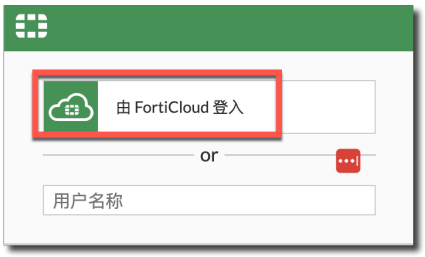

```
1  date=2023-10-12 time=17:11:35 eventtime=1697101894379458919 tz="+0800" logid="0100032001" type="event"
   subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1697101894" user="xxxx"
   ui="sso(192.168.100.110)" method="sso" srcip=192.168.100.110 dstip=192.168.100.99 action="login" status="success"
   reason="none" profile="super_admin" msg="Administrator xxxx logged in successfully from sso(192.168.100.110)"
```

FortiCloud IAM账户登录

1. Default admin profile为继承自FortiCloud。

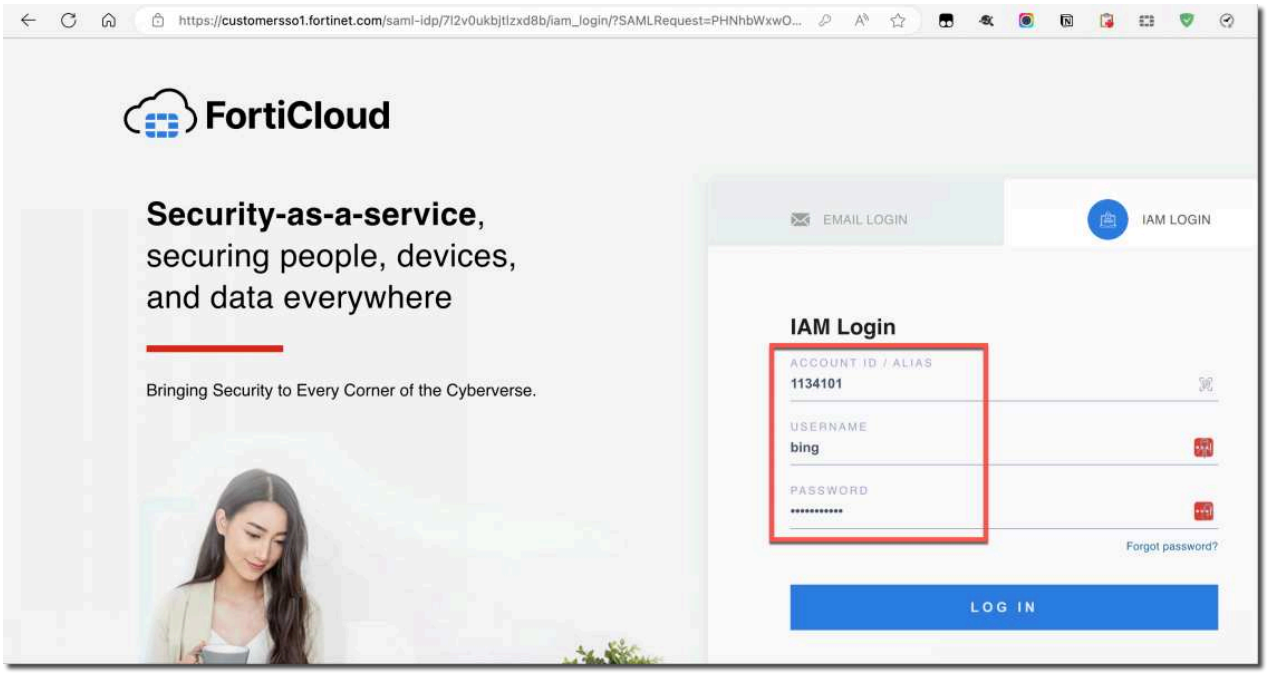


2. 访问FortiGate登陆页面，可以看到增加了“由FortiCloud登入”的选项。

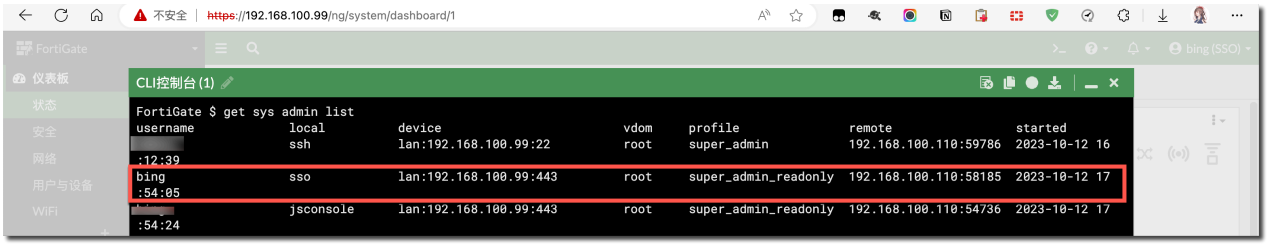


3. 选择IAM Login方式，填入IAM账户的Account ID、用户名和密码，点击Log in按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 登录FortiGate成功，登录后的权限为read_only，且无法修改任何配置。

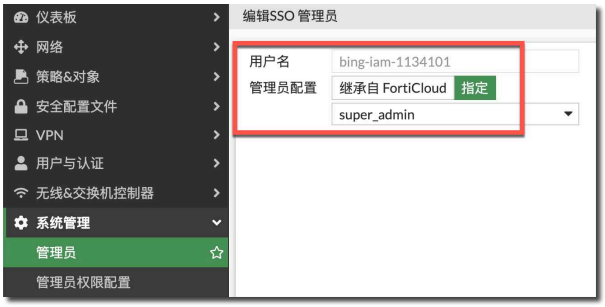



```
1  date=2023-10-12 time=17:54:05 eventtime=1697104445968808759 tz="+0800" logid="0100032001" type="event"
   subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1697104445" user="bing"
   ui="sso(192.168.100.110)" method="sso" srcip=192.168.100.110 dstip=192.168.100.99 action="login" status="success"
   reason="none" profile="super_admin_readonly" msg="Administrator bing logged in successfully from
   sso(192.168.100.110)"
```

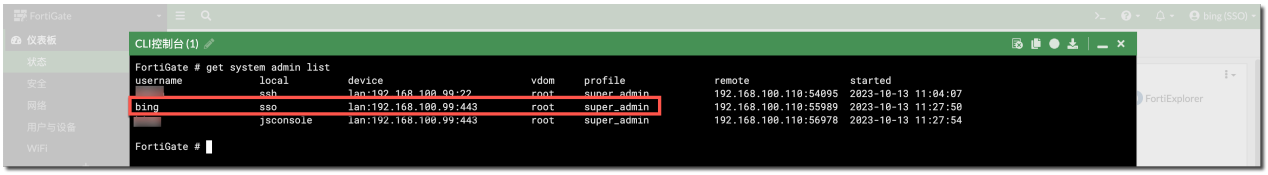
5. 使用本地管理员修改已创建的FortiCloud IAM用户的权限为super_admin（如果是未登陆过的FortiCloud用户，则只需在系统管理→设置中修改Default admin profile为指定super_admin权限，如果是已登录过的FortiCloud账户，必须使用本地管理员在管理员设置中配置权限）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





6. 再次使用FortiCloud IAM用户登录，登录FortiGate成功，登录后的权限为super_admin。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

限制管理员SSH/Telnet跳板

重要

该功能在FortiOS 7.2.1及以上版本支持。

网络需求

默认配置下，管理员登录FortiGate后，可以使用SSH、Telnet功能远程连接到其他主机。

出于安全性的需求，FortiGate可以配置管理员所使用的管理员配置文件，禁止其使用FortiGate的SSH、Telnet功能作为跳板来远程连接到其他主机。

配置方法

此功能仅在CLI下可配置。

重要

内置的`super_admin`管理员配置文件无法开启此功能。默认配置为`enable`。

```bash
config system accprofile
    edit < name >
        set system-execute-ssh < enable | disable >    //开启或关闭SSH权限//
        set system-execute-telnet < enable | disable >    //开启或关闭Telnet权限//
    next
end
```

配置步骤

1. 在FortiGate上新建管理员配置文件，并禁止使用FortiGate的SSH、Telnet功能作为跳板来远程连接到其他主机的功能。

```bash
config system accprofile
    edit "Restrict_SSH_and_Telnet"
        set secfabgrp read-write
        set ftviewgrp read-write
        set authgrp read-write
        set sysgrp read-write
        set netgrp read-write
        set loggrp read-write
        set fwgrp read-write
        set vpngrp read-write
        set utmgrp read-write
        set wanoptgrp read-write
        set wifi read-write
        set system-execute-ssh disable
        set system-execute-telnet disable
    next
end
```

2. 创建管理员引用上步创建的管理员配置文件。

```bash
config system admin
    edit "admin_beijing"
        set accprofile "Restrict_SSH_and_Telnet"
        set vdom "root"
        set password fortinet
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置验证

1. 使用管理员`admin_beijing`登录FortiGate（通过Web CLI或SSH登录），并在FortiGate下使用Telnet、SSH命令访问其他服务器，提示没有权限运行该命令。

```bash
C:\Users\cyndi>ssh admin_beijing@10.10.12.1
admin_beijing@10.10.12.1's password:

FortiGate $ exe telnet 192.168.100.99
You are not entitled to run the command.
Command fail. Return code -37

FortiGate $ exe ssh 192.168.100.99
You are not entitled to run the command.
Command fail. Return code -37
```

2. 使用管理员`admin`登录FortiGate（通过Web CLI或SSH登录），使用Telnet、SSH命令可以正常访问其他服务器。

```bash
C:\Users\cyndi>ssh admin@10.10.12.1
admin@10.10.12.1's password:

FortiGate # exe telnet 192.168.100.99
Trying 192.168.100.99 ...
Connected to 192.168.100.99.
FW1_FGT101F login: admin
Password:
Welcome!
FW1_FGT101F # exit
Connection closed by foreign host.

FortiGate # exe ssh admin@192.168.100.99
admin@192.168.100.99's password:
FW1_FGT101F # exit
Connection to 192.168.100.99 closed.
FortiGate #
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

密码恢复

重要

此功能仅支持7.2.4之前的FortiOS版本。为了安全性考虑，从7.2.4 GA版本开始，FortiOS不再支持密码恢复功能，请务必妥善保存管理员密码以及定期做好配置备份！

功能需求

1. 若设备的密码忘记，需要用配置线进行密码恢复。
2. 密码恢复需要重启设备，并在设备的 底层菜单界面上操作，会造成网络中断，请在方便断网时操作。
3. 密码恢复后 配置不会改变。

配置要点

1. 使用终端软件（如SecureCRT、XSHELL）连接防火墙串口。
2. 断电重启设备，输入使用内置账户maintainer登录。
3. 为管理员用户重新设置新的密码。

配置步骤

1. 连好Console线，设置并连接终端软件（详见系统管理→管理方式→console管理方式 ↗）。

2. 断电重启设备，重启后在15秒内输入用户名maintainer， 密码为bcpb+该设备的SN号，通常是以FGT开头的16字符串，产品序列号见设备的底部或者侧面，如下图所示。



3. 该账户仅在断电重启后15秒内有效，且必须要通过Console口使用。

```
FGT60C3G10000413 login: maintainer
Password:  bcpbFGT60C3G10000413
FGT60C3G10000413 #
```

4. 修改管理员账号密码。

```
FGT60C3G10000413# config system admin
FGT60C3G10000413 (admin) # edit admin
FGT60C3G10000413(admin) # set pass 123455@!@#
FGT60C3G10000413 (admin) # end
```

结果验证

使用刚重置密码的admin账户，通过https或者ssh登陆防火墙。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

API用户

重要

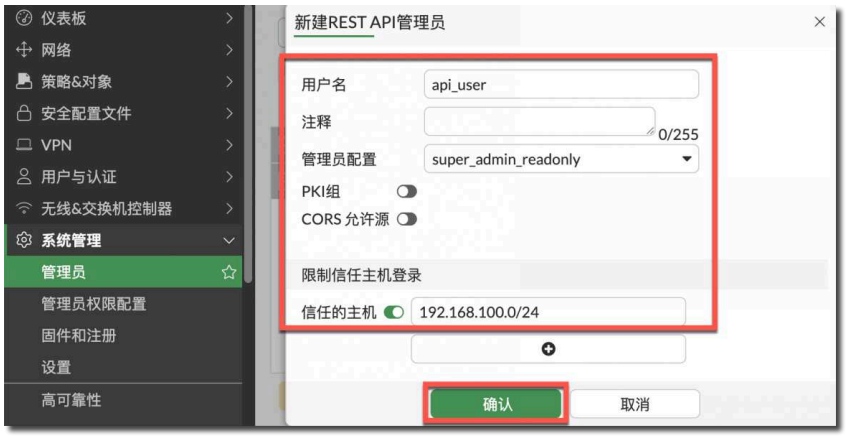
API文档获取方式请参考：系统管理→FortiGuard管理→注册指南→API文档获取↗章节。

用户创建

1. 进入GUI的“系统管理→管理员”页面，点击“新建”按钮，选择“REST API管理员”。

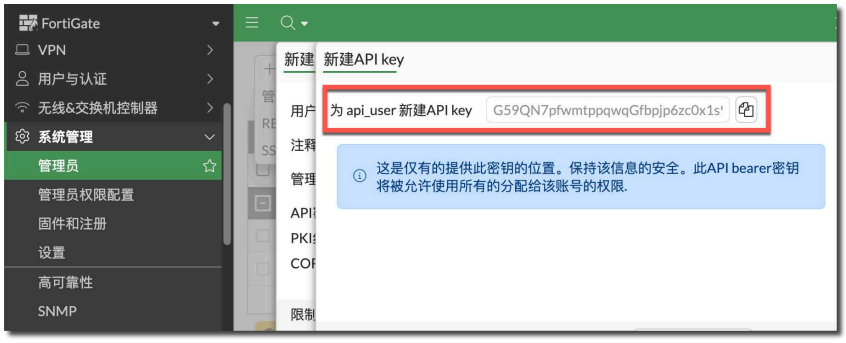


2. 配置API用户名与“管理员配置”，这里以预置的“super_admin_readonly”为例。按需要配置“PKI组”、“CORS允许源”、“信任的主机”配置。



- 管理员配置：选择API用户的管理员权限配置（配置请参考“系统管理→管理员配置→管理员设置↗”章节，在GUI下，只能选择“super_admin_readonly”、“admin_no_access”以及自定义的管理员权限文件。如果需要选择预置的“super_admin”和“prof_admin”，需要在CLI下配置。
- PKI组：在API key认证的基础上开启REST API客户端证书认证，只有此PKI组中的证书用户可以访问API。
- CORS允许源：当REST API客户端是通过跨域请求（CORS）的方式访问FortiGate的API时，需要允许CORS的网站源地址（具体示例请见“系统管理→FortiGuard管理→API文档获取↗”中的“通过FNDN使用API”部分）。
- 信任的主机：限制允许访问的REST API客户端IP。

3. 点击“确认”按钮后，会生成API key。注意该API key只会在这里显示一次，请妥善保存API key。



4. API用户创建完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system api-user
    edit "api_user"
        set api-key ENC SH281AhpqGoK53Cq8e/pcf89amfyatlAMsh3uP0427kvqCNdFFZViV9L6q11ao=
        set accprofile "super_admin_readonly"
        config trusthost
            edit 1
                set ipv4-trusthost 192.168.100.0 255.255.255.0
            next
        end
    next
end
```

其他选项

CLI配置

```bash
config system api-user
    edit <user_name>
        set comments <string>
        set api-key ************    ←——只能系统生成，无法在CLI中指定
        set accprofile <admin_accprofile>
        set schedule <schedule_object>
        set cors-allow-origin "https://fndn.fortinet.net"
        set peer-auth enable
        set peer-group <group>
        config trusthost
            edit 1
                set type ipv4-trusthost
                set ipv4-trusthost <class_ip&net_netmask>
            next
            edit 2
                set type ipv6-trusthost
                set ipv6-trusthost <class_ip&net_netmask>
            next
            ...
        end
    next
end
```

生成API key

- 由系统生成或重新生成API key，该key无法在CLI中指定。

```bash
execute api-user generate-key <API username>

execute api-user generate-key api_user
```

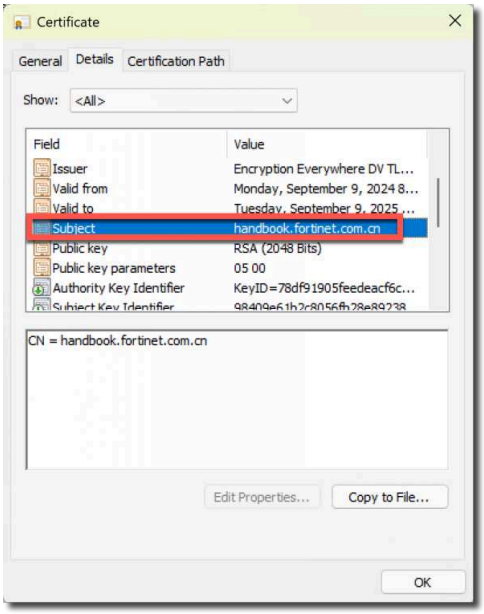
- 从FortiOS 7.6.0版本开始，可以配置API key的过期时间，单位为min。

```bash
execute api-user generate-key <API username> <expiry time>

execute api-user generate-key api_user 480
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

API PKI组认证

1. 配置PKI用户，指定用于REST API客户端认证使用的证书用户，这些信息可以从用于REST API客户端认证的用户证书属性中找到。




```bash
config user peer
    edit "pki_user"
        set mandatory-ca-verify enable     ←——默认开启
        set ca "DigiCertGlobalRootG2"
        set subject "CN = handbook.fortinet.com.cn"
        set cn "handbook.fortinet.com.cn"
    next
end
```

重要

`mandatory-ca-verify` 选项：

- enable：需要将API客户端证书对应的CA证书安装在FortiGate上（导入方法参考：系统管理→系统设置→证书管理 ↗章节），认证时FortiGate会验证客户端证书是否与 `set ca` 指定的CA证书匹配（默认启用）。同时也要验证客户端提供的证书中的字段是否与PKI用户中配置的一致。
- disable：只要API客户端提供的证书中的属性与PKI用户中配置的一致，FortiGate即认为客户端证书有效。
- 验证证书字段有3种方式：Subject、CN或LDAP，所有字符串比较均区分大小写。

2. 创建用户组引用PKI用户。

```bash
config user group
    edit "api_usergrp"
        set member "pki_user"
    next
end
```

3. 在API用户中开启“PKI组”认证，并引用PKI用户组。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system api-user
    edit api_user
        set peer-auth enable
        set peer-group api_usergrp
    next
end
```

4. API客户端可以使用如下命令指定API访问时使用的证书文件以及API key。

```
# curl -k --key ./<user private key> --cert <path of user certificate>
https://<IP/FQDN>/api/v2/cmdb/firewall/address/?access_token=<api_key>

# curl -k --key ./useKeyr.pem --cert ./handbook.fortinet.com.cn.crt
https://192.168.100.99/api/v2/cmdb/firewall/address/?access_token=bbQfw68qrnyN3yyybznGtgGx897qH3
```

5. FortiGate可以正确返回API查询结果。

```bash
* Server certificate:
* subject: C=US; ST=California; L=Sunnyvale; O=Fortinet; OU=FortiGate; CN=FGVM020000158352;
emailAddress=support@fortinet.com
* start date: Oct 23 11:04:36 2019 GMT
* expire date: Jan 19 03:14:07 2056 GMT
* common name: FG101FTK2000XXXX
* issuer: C=US; ST=California; L=Sunnyvale; O=Fortinet; OU=Certificate Authority; CN=fortinet-subca2001;
emailAddress=support@fortinet.com
::: important
GET /api/v2/cmdb/firewall/address/?access_token=bbQfw68qrnyN3yyybznGtgGx897qH3 HTTP/1.1
Host: FG101FTK2000XXXX
User-Agent: curl/8.7.1
Accept: */*

:::
< HTTP/1.1 200 OK
< Date: Wed, 08 Jul 2025 17:19:13 GMT
< Server: Apache
< X-Frame-Options: SAMEORIGIN
< Content-Security-Policy: frame-ancestors 'self'
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=0
< X-UA-Compatible: IE=Edge
< Cache-Control: no-cache, must-revalidate
< ETag: 2a3997e13943e98865004c368a65a8de
< Content-Length: 7940
< Content-Type: application/json
<
{
"http_method":"GET",
"revision":"2a3997e13943e98865004c368a65a8de",
"results":[
{
"name":"FABRIC_DEVICE",
"q_origin_key":"FABRIC_DEVICE",
"uuid":"0f1a2390-525c-51f0-2ad2-b213f4cba84b",
"subnet":"0.0.0.0 0.0.0.0",
"type":"ipmask",
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
"sub-type":"sdn",
"clearpass-spt":"unknown",
"start-mac":"00:00:00:00:00:00",
"end-mac":"00:00:00:00:00:00",
"country":"",
"cache-ttl":0,
"sdn":"",
"fsso-group":[
],
......
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SNMP介绍

简单网络管理协议

简单网络管理协议（SNMP，Simple Network Management Protocol）构成了互联网工程工作小组（IETF，Internet Engineering Task Force）定义的Internet协议族的一部分。该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。它由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模式（database schema），和一组数据对象。

概论和基础观念

在典型的SNMP用法中，有许多系统被管理，而且是有一或多个系统在管理它们。每一个被管理的系统上有运行一个叫做代理者（agent）的软件组件，且透过SNMP对管理系统报告信息。

基本上，SNMP代理者以变量呈现管理数据。管理系统透过GET，GETNEXT和GETBULK协议指令取回信息，或是代理者在没有被询问的情况下，使用TRAP或INFORM发送数据。管理系统也可以发送配置更新或控制的请求，透过SET协议指令达到主动管理系统的目的。配置和控制指令只有当网络基本结构需要改变的时候使用，而监控指令则通常是常态性的工作。

可透过SNMP访问的变量以层次结构的方式结合。这些分层和其他元数据（例如变量的类型和描述）以管理信息库（MIBs）的方式描述。

SNMP协议

SNMP第一版和SMI规格的数据类型SNMP V1

SNMP第一版SMI指定许多SMI规格的数据类型，它们被分为两大类：

1. 简单数据类型
2. 泛应用数据类型

SNMP第二版和管理信息结构SNMP V2

SNMP第二版SMI在RFC 2578之中描述，它在SNMP第一版的SMI规格数据类型上进行增加和强化，例如位串（bit strings）、网络地址（network addresses）和计数器（counters）。

SNMP协议在OSI模型的应用层（第七层）运作，在第一版中指定五种核心PDU：

```
GET REQUEST
GET NEXT REQUEST
GET RESPONSE
SET REQUEST
TRAP
```

其他PDU在SNMP第二版加入，包含：

```
GETBULK REQUEST
INFORM
```

SNMP第二版SMI也指定了信息模块来详细说明一群相关连的定义。有三种SMI信息模块：MIB模块、回应状态、能力状态。

SNMP第三版 SNMP V3

SNMP第三版由RFC 3411-RFC 3418定义，主要增加SNMP在安全性和远程配置方面的强化。SNMP第三版提供重要的安全性功能：

1. 信息完整性：保证数据包在发送中没有被窜改。
2. 认证：检验信息来自正确的来源。
3. 数据包加密：避免被未授权的来源窥探。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

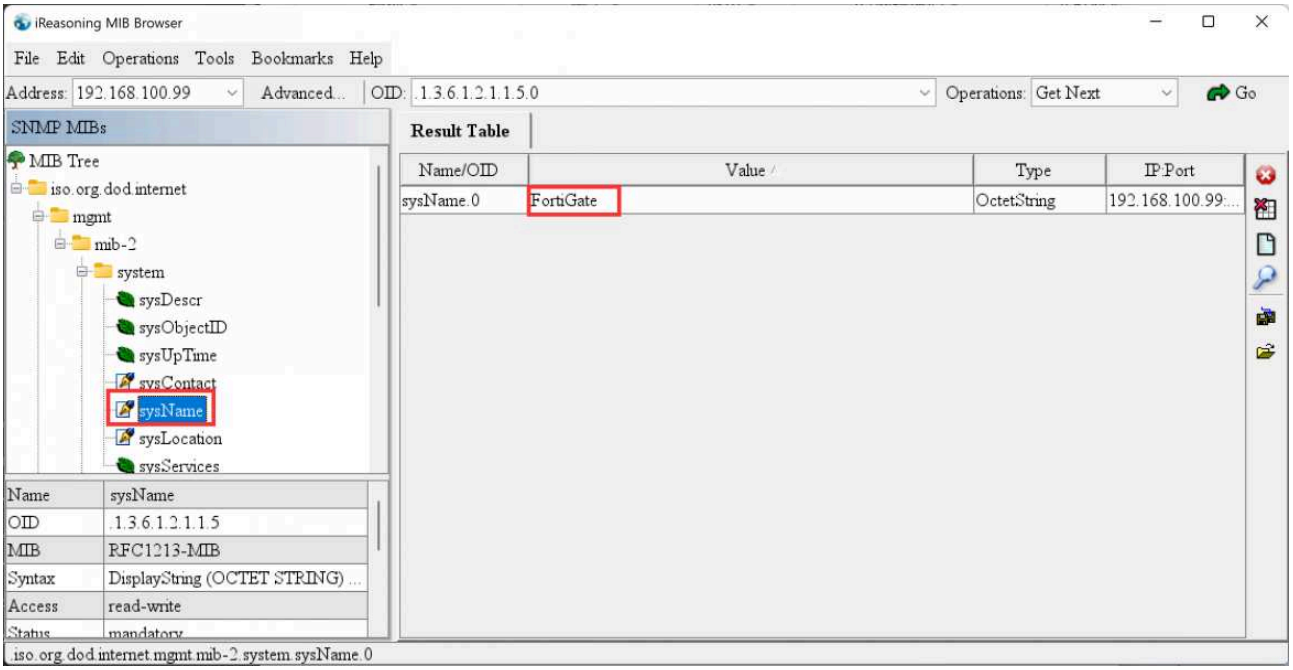
SNMP公共MIB和私有MIB

公共MIB库

公共MIB可以认为是大家共用使用的一些MIB查询节点，比如设备名称、设备运行时间、接口MAC、接口MTU、接口描述、接口收发报文数（接口流量）、路由表等等信息。

举例1：设备名称

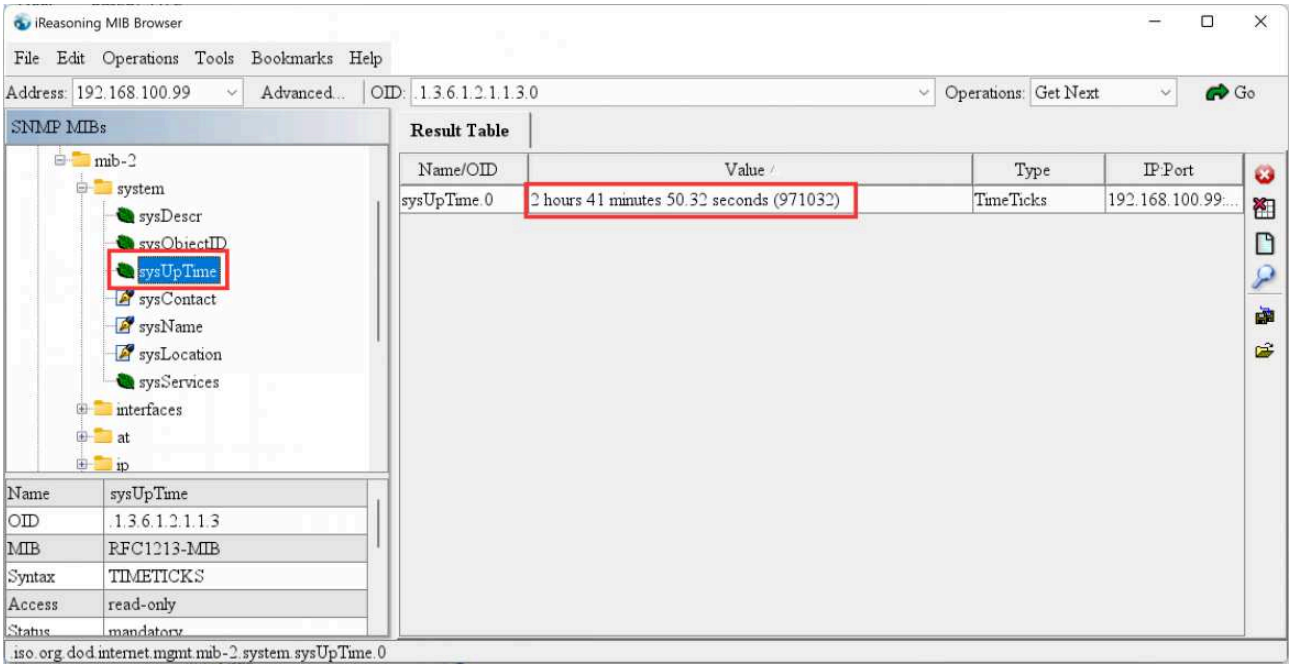
```
Name:         sysName
Type:         OBJECT-TYPE
OID:          1.3.6.1.2.1.1.5
```



举例2：设备启动时间

```
Name:         sysUpTime
Type:         OBJECT-TYPE
OID:          1.3.6.1.2.1.1.3
```

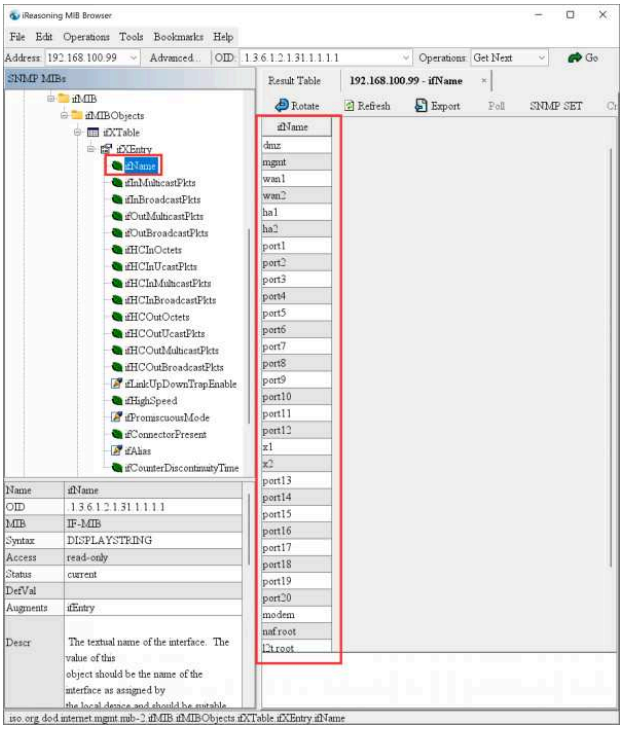

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



举例3：设备接口名称、流量统计、接口描述、接口Alias、等OID

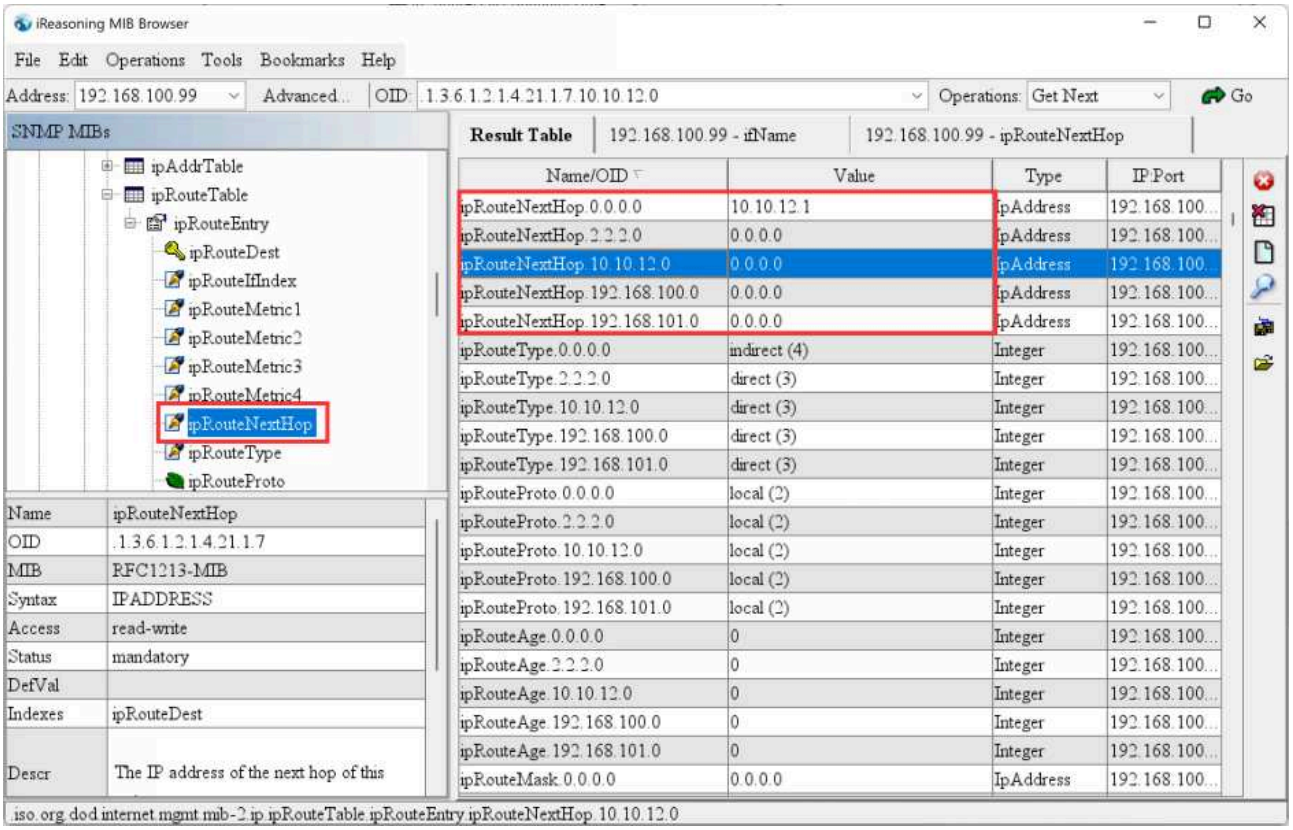
```
Name:        ifXTable
Type:        OBJECT-TYPE
OID:         1.3.6.1.2.1.31.1.1
Full path:       iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ifMIB(31).ifMIBObjects(1).ifXTable(1)
Module:        IF-MIB

Parent:        ifMIBObjects
First child:        ifXEntry
Next sibling:        ifStackTable

Numerical syntax:        Sequence
Base syntax:        SEQUENCE OF IfXEntry
Composed syntax:        SEQUENCE OF IfXEntry
Status:        current
Max access:        not-accessible
Sequences:
       1: ifName - DisplayString(4 - octets)
       2: ifInMulticastPkts - Counter32(65 - counter (32 bit))
       3: ifInBroadcastPkts - Counter32(65 - counter (32 bit))
       4: ifOutMulticastPkts - Counter32(65 - counter (32 bit))
       5: ifOutBroadcastPkts - Counter32(65 - counter (32 bit))
       6: ifHCInOctets - Counter64(70 - counter (64 bit))
       7: ifHCInUcastPkts - Counter64(70 - counter (64 bit))
       8: ifHCInMulticastPkts - Counter64(70 - counter (64 bit))
       9: ifHCInBroadcastPkts - Counter64(70 - counter (64 bit))
       10: ifHCOutOctets - Counter64(70 - counter (64 bit))
       11: ifHCOutUcastPkts - Counter64(70 - counter (64 bit))
       12: ifHCOutMulticastPkts - Counter64(70 - counter (64 bit))
       13: ifHCOutBroadcastPkts - Counter64(70 - counter (64 bit))
       14: ifLinkUpDownTrapEnable - INTEGER(2 - integer (32 bit))
       15: ifHighSpeed - Gauge32(66 - gauge (32 bit))
       16: ifPromiscuousMode - TruthValue(2 - integer (32 bit))
       17: ifConnectorPresent - TruthValue(2 - integer (32 bit))
       18: ifAlias - DisplayString(4 - octets)
       19: ifCounterDiscontinuityTime - TimeStamp(67 - timeticks)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



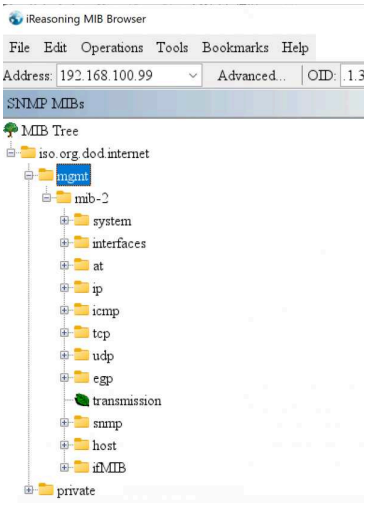
举例4：设备路由表信息

```
Name:        ipRouteNextHop
Type:        OBJECT-TYPE
OID:         1.3.6.1.2.1.4.21.1.7
```



公共的mib 库非常之多，其中有很多有用的OID：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

具体可以通过以下链接查看到公共MIB：

Net-SNMP Distributed MIBs：http://net-snmp.sourceforge.net/docs/mibs/ ↗

UCD-SNMP-MIB：http://net-snmp.sourceforge.net/docs/mibs/ucdavis.html ↗

HOST-RESOURCES-MIB：http://net-snmp.sourceforge.net/docs/mibs/host.html ↗

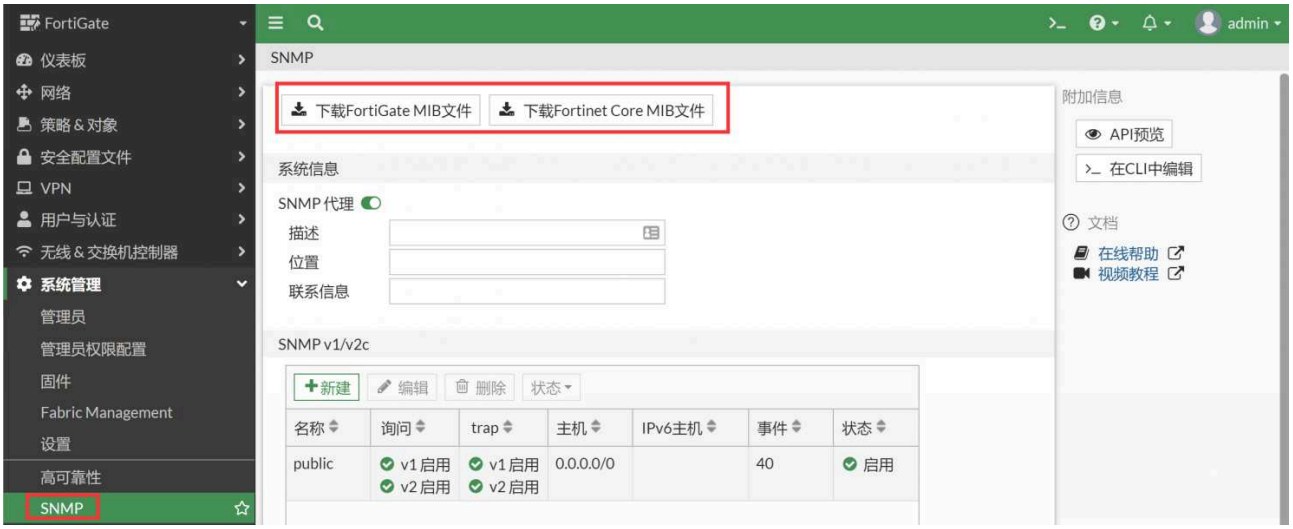
IF-MIB：http://net-snmp.sourceforge.net/docs/mibs/ifMIBObjects.html ↗

mibDepot：http://www.mibdepot.com/index.shtml ↗

私有MIB库

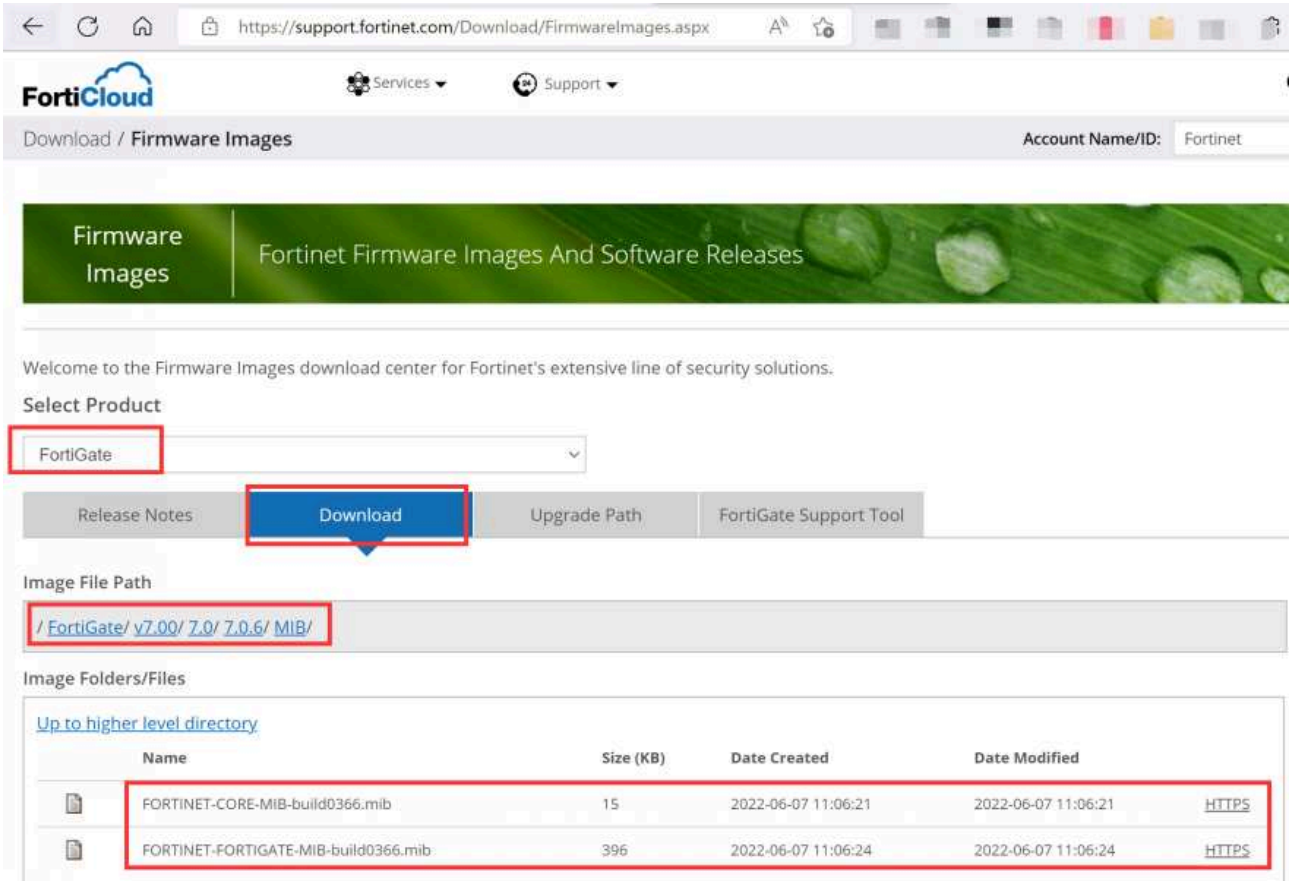
FortiGate的私有mib文件可以在SNMP配置界面处直接下载，或在support网站登录后下载。

FortiGate SNMP配置界面处直接下载



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

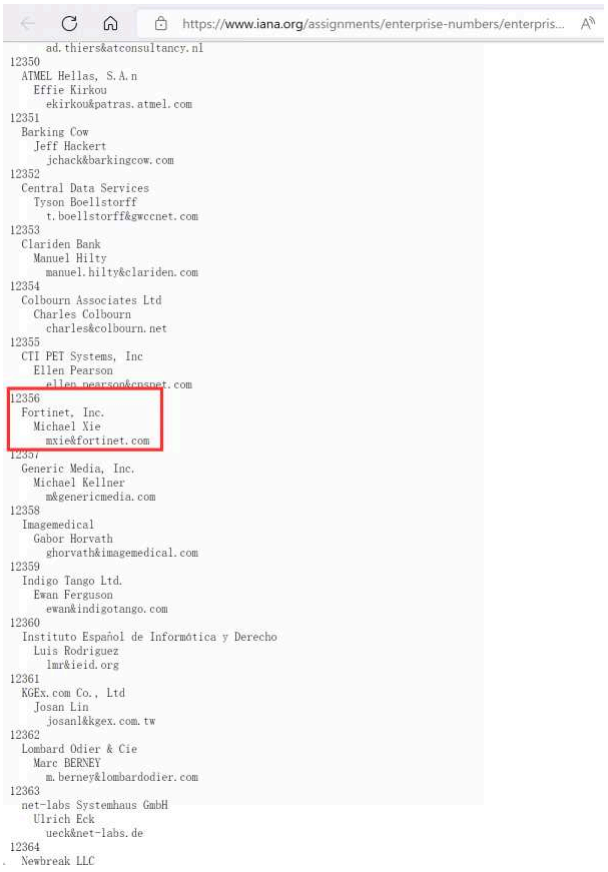
SUPPORT网站下载



注意事项

关于私有mib的oid，Fortinet的私有number是12356，可通过以下链接获取私有厂家的enterprise-numbers：
https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

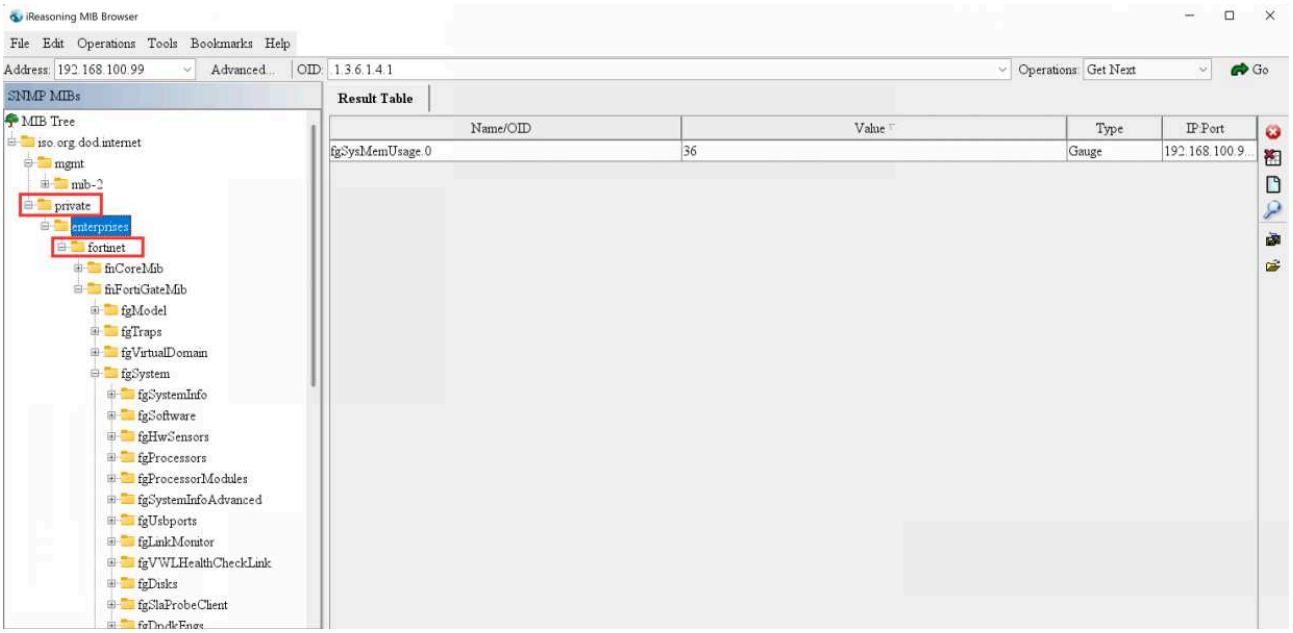


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SNMP建议监控指标

FortiGate私有MIB

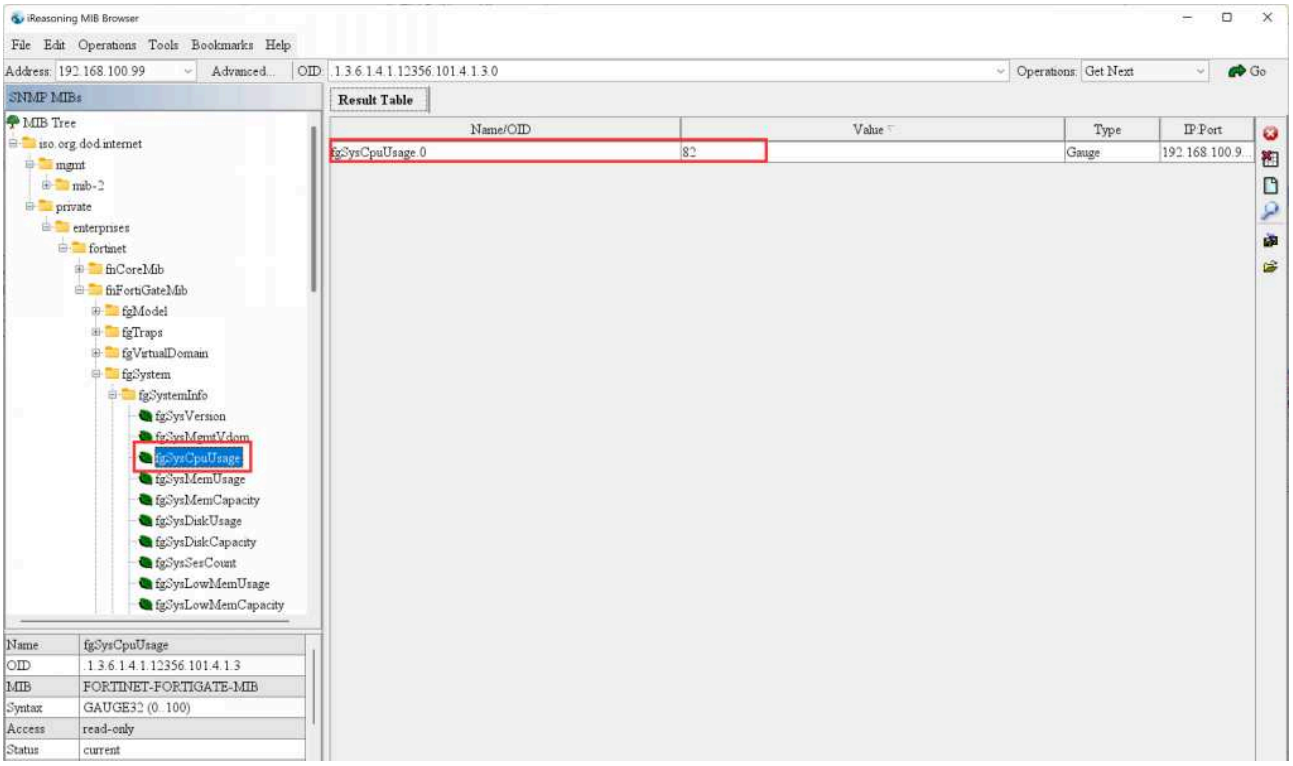
私有MIB库需要手工导入。



最常见的SNMP健康指标：FortiGate的CPU、MEM、新建、并发、接口流量等等。

CPU OID

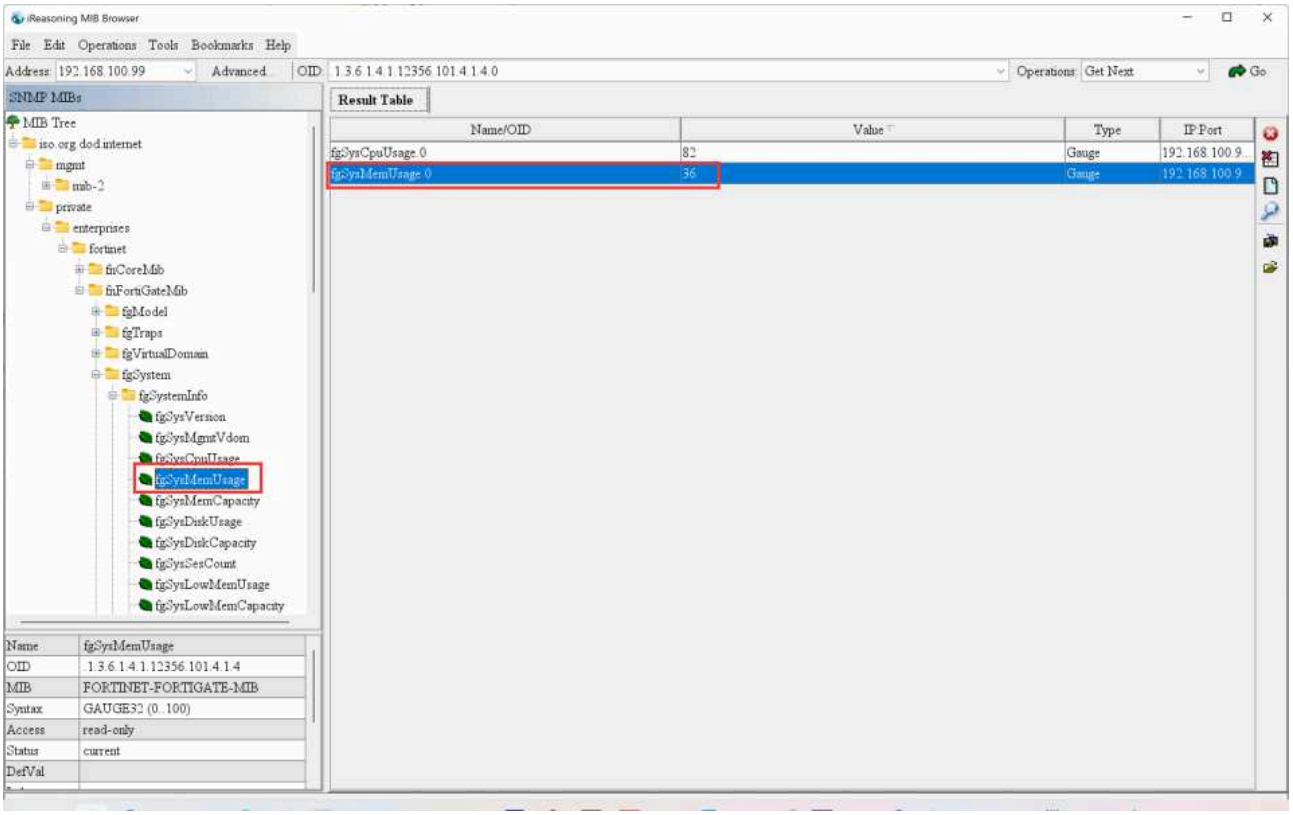
```
Name:        fgSysCpuUsage  OID:        1.3.6.1.4.1.12356.101.4.1.3.0
```



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

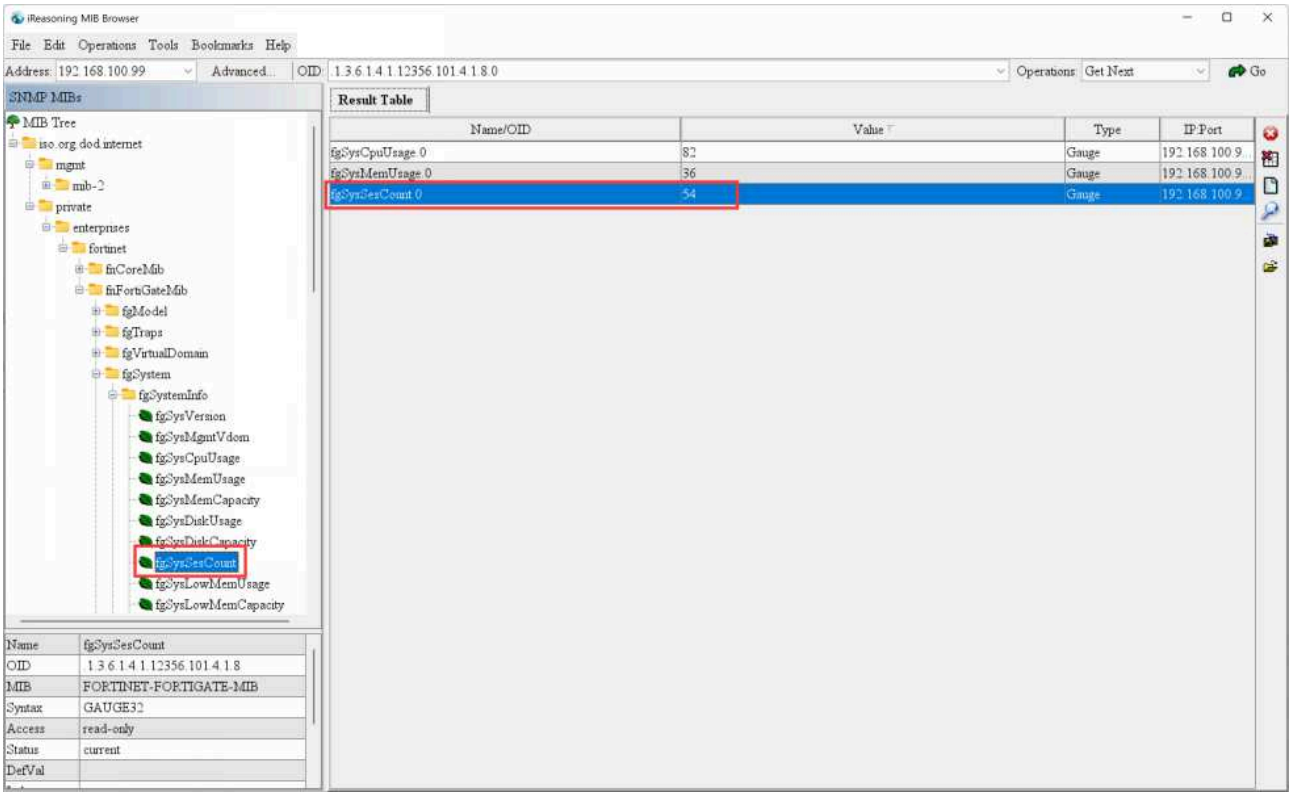
MEM OID

```
Name:        fgSysMemUsage  OID:        1.3.6.1.4.1.12356.101.4.1.4.0
```



并发会话数OID

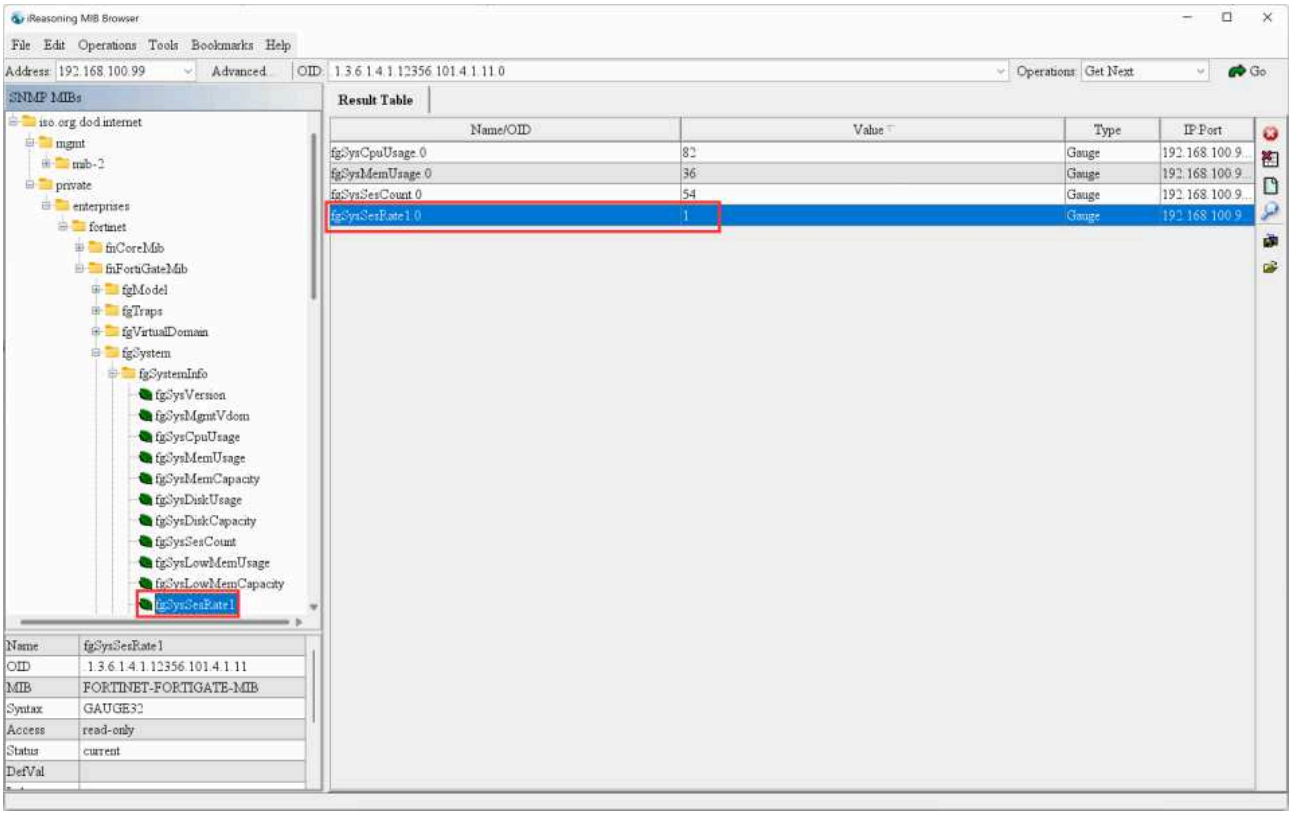
```
Name:        fgSysSesCount    OID:        1.3.6.1.4.1.12356.101.4.1.8.0
```



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

新建会话数OID

```
Name:        fgSysSesRate1  OID:        1.3.6.1.4.1.12356.101.4.1.11.0
```



接口流量OID

重要

这个部分使用的公共的MIB节点通过复合公式计算出来的接口带宽值，不是直接使用MIB值，通过这个计算方法来读取的接口流量。

复合参数	复合表达式	单位	备注
接口bps（in）Inbound Throughput	吞吐量：间隔t秒执行2次获取ifHCInOctets.x (.1.3.6.1.2.1.31.1.1.1.6.x)的值，结果分别为ifHCInOctets.x.time1和ifHCInOctets.x.time2。interface x的in_bps = (ifHCInOctets.x.time2 - ifHCInOctets.x.time1) * 8 / t	bps	吞吐率（Inbound Utilization）=接口吞吐量/接口最大吞吐量=60%
接口bps（out）Outbound Throughput	吞吐量：间隔t秒执行2次获取ifHCOutOctets.x(.1.3.6.1.2.1.31.1.1.1.10.x)的值，结果分别为ifHCOutOctets.x.time1和ifHCOutOctets.x.time2。interface x的out_bps = (ifHCOutOctets.x.time2 - ifHCOutOctets.x.time1) * 8 / t	bps	吞吐率（Outbound Utilization）=接口吞吐量/接口最大吞吐量=60%

```bash
Name:        ifHCInOctets
Type:        OBJECT-TYPE
OID:        1.3.6.1.2.1.31.1.1.1.6

Name:        ifHCOutOctets
Type:        OBJECT-TYPE
OID:        1.3.6.1.2.1.31.1.1.1.10

Type:        OBJECT-TYPE
OID:        1.3.6.1.2.1.31.1.1.1
Full path:        iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ifMIB(31).ifMIBObjects(1).ifXTable(1).ifXEntry(1)
Sequences:
       1: ifName - DisplayString(4 - octets)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        2: ifInMulticastPkts - Counter32(65 - counter (32 bit))
        3: ifInBroadcastPkts - Counter32(65 - counter (32 bit))
        4: ifOutMulticastPkts - Counter32(65 - counter (32 bit))
        5: ifOutBroadcastPkts - Counter32(65 - counter (32 bit))
        6: ifHCInOctets - Counter64(70 - counter (64 bit))
        7: ifHCInUcastPkts - Counter64(70 - counter (64 bit))
        8: ifHCInMulticastPkts - Counter64(70 - counter (64 bit))
        9: ifHCInBroadcastPkts - Counter64(70 - counter (64 bit))
        10: ifHCOutOctets - Counter64(70 - counter (64 bit))
        11: ifHCOutUcastPkts - Counter64(70 - counter (64 bit))
        12: ifHCOutMulticastPkts - Counter64(70 - counter (64 bit))
        13: ifHCOutBroadcastPkts - Counter64(70 - counter (64 bit))
        14: ifLinkUpDownTrapEnable - INTEGER(2 - integer (32 bit))
        15: ifHighSpeed - Gauge32(66 - gauge (32 bit))
        16: ifPromiscuousMode - TruthValue(2 - integer (32 bit))
        17: ifConnectorPresent - TruthValue(2 - integer (32 bit))
        18: ifAlias - DisplayString(4 - octets)
        19: ifCounterDiscontinuityTime - TimeStamp(67 - timeticks)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate防火墙监控指标参数

建议监控内容项

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

监控参数明细	Object	对应OID值	参数类别（单位）	SYSLOG告警	SNMP告警
系统运行时间	sysUpTime.0	.1.3.6.1.2.1.1.3.0	timeTicks (0.01s)		
当前接口状态（对于VPN Tunnel接口只能显示管理状态）	ifOperStatus.x	.1.3.6.1.2.1.2.2.1.8.x	INTEGER {up(1), down(2), testing(3), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7) }	是	是
VPN Tunnel二阶段状态	fgVpnTunEntStatus.x.y	.1.3.6.1.4.1.12356.101.12.2.2.1.20.x.y	INTEGER {down(1), up(2) }	是	是
每个CPU利用率	fgProcessorUsage.x	.1.3.6.1.4.1.12356.101.4.4.2.1.2.*	1-100（%）	是	是
多个CPU的总利用率	fgSysCpuUsage（percentage %）	.1.3.6.1.4.1.12356.101.4.1.3	1-100（%）	是	是
内存利用率	fgSysMemUsage	.1.3.6.1.4.1.12356.101.4.1.4	1-100（%）	是	是
并发连接数	fgSysSesCount.0	.1.3.6.1.4.1.12356.101.4.1.8.0	数字	是	是
每秒新建连接数（1分钟平均）	fgSysSesRate1.0	.1.3.6.1.4.1.12356.101.4.1.11.0	数字	否	是
每秒新建连接数（10分钟平均）	fgSysSesRate10.0	.1.3.6.1.4.1.12356.101.4.1.12.0	数字	否	是
每秒新建连接数（30分钟平均）	fgSysSesRate30.0	.1.3.6.1.4.1.12356.101.4.1.13.0	数字	否	是
每秒新建连接数（60分钟平均	fgSysSesRate60.0	.1.3.6.1.4.1.12356.101.4.1.14.0	数字	否	是
协议错误丢包	ipInHdrErrors.0	.1.3.6.1.2.1.4.4.0	数字，IP包头错误个数，累加	否	是
接口流量（in）	ifHCInOctets.x	.1.3.6.1.2.1.31.1.1.1.6.x	数字，单位bit	否	是
接口流量（out）	ifHCOutOctets.x	.1.3.6.1.2.1.31.1.1.1.10.x	数字，单位bit	否	是
接口包转发数（in）	ifInUcastPkts.x	.1.3.6.1.2.1.2.2.1.11.x	数字：单播数据包数量	否	是
接口包转发数（out）	ifOutUcastPkts.x	.1.3.6.1.2.1.2.2.1.17.x	数字：单播数据包数量	否	是
接口丢包（in）	ifInDiscards.x	.1.3.6.1.2.1.2.2.1.13.x	数字：单播数据包数量	否	是
接口丢包（out）	ifOutDiscards.x	.1.3.6.1.2.1.2.2.1.19.x	数字：单播数据包数量	否	是
接口错包（in）	ifInErrors.x	.1.3.6.1.2.1.2.2.1.14.x	数字	否	是
接口错包（out）	ifOutErrors.x	.1.3.6.1.2.1.2.2.1.20.x	数字	否	是

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

系统状态监控项

监控参数明细	Object	对应OID值	参数类别（单位）	SYSLOG告警	SNMP告警
主机名称	sysName.0	.1.3.6.1.2.1.1.5.0	字符串		
设备序列号	fnSysSerial.0	.1.3.6.1.4.1.12356.100.1.1.1.0	字符串		
系统运行时间	sysUpTime.0	.1.3.6.1.2.1.1.3.0	timeTicks (0.01s)		
系统版本	fgsSysVersion	.1.3.6.1.4.1.12356.101.4.1.1.0	字符串		
系统CPU数量	fgProcModProcessorCount.1	.1.3.6.1.4.1.12356.101.4.5.3.1.5.1	正整数		
每个CPU利用率(1分钟)	fgProcessorUsage.x	.1.3.6.1.4.1.12356.101.4.4.2.1.2.X	1-100（%）	是	是
每个CPU利用率(5秒钟)	fgProcessorUsage5sec.x	.1.3.6.1.4.1.12356.101.4.4.2.1.3.x	1-100（%）		
多个CPU的总利用率	fgSysCpuUsage.0	.1.3.6.1.4.1.12356.101.4.1.3.0	1-100（%）	是	是
内存利用率	fgSysMemUsage.0	.1.3.6.1.4.1.12356.101.4.1.4.0	1-100（%）	是	是
总内存大小	fgSysMemCapacity.0	.1.3.6.1.4.1.12356.101.4.1.5.0	单位（kb）		
并发连接数	fgSysSesCount.0	.1.3.6.1.4.1.12356.101.4.1.8.0	数字	是	是
每秒新建连接数（1分钟平均）	fgSysSesRate1.0	.1.3.6.1.4.1.12356.101.4.1.11.0	数字	否	是
每秒新建连接数（10分钟平均）	fgSysSesRate10.0	.1.3.6.1.4.1.12356.101.4.1.12.0	数字	否	是
每秒新建连接数（30分钟平均）	fgSysSesRate30.0	.1.3.6.1.4.1.12356.101.4.1.13.0	数字	否	是
每秒新建连接数（60分钟平均）	fgSysSesRate60.0	.1.3.6.1.4.1.12356.101.4.1.14.0	数字	否	是
设备License状态(table view)	FgLicContractEntry	.1.3.6.1.4.1.12356.101.4.6.3.1.2.1	字符串		
设备Licence名称	fgLicContractDesc	.1.3.6.1.4.1.12356.101.4.6.3.1.2.1.1	字符串		
设备Licence到期时间	fgLicContractExpiry	.1.3.6.1.4.1.12356.101.4.6.3.1.2.1.2	字符串		

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

接口状态监控项

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

监控参数明细	Object	对应OID值.x （x为接口ID）	参数类别（单位）	SYSLOG告警	SNMP告警
IfEntry(基础表)					
系统接口数量	ifNumber.0	.1.3.6.1.2.1.2.1.0	正整数		
接口ID	ifIndex	.1.3.6.1.2.1.2.2.1.1	1.2.3….自然数		
接口MTU	ifMtu.x	.1.3.6.1.2.1.2.2.1.4.x	正整数		
接口速率	ifSpeed.x	.1.3.6.1.2.1.2.2.1.5.x	正整数,单位:bit		
接口管理状态	ifAdminStatus.x	.1.3.6.1.2.1.2.2.1.7.x	INTEGER {up(1), down(2)}		
接口工作状态（对于VPN Tunnel接口只能显示管理状态）	ifOperStatus.x	.1.3.6.1.2.1.2.2.1.8.x	INTEGER {up(1), down(2), testing(3), unknown(4), dormant(5), notPresent(6), lowerLayerDown(7) }	是	是
VPN Tunnel二阶段状态	fgVpnTunEntStatus.x.y	.1.3.6.1.4.1.12356.101.12.2.2.1.20.x.y	INTEGER {down(1), up(2) }	是	是
接口流量（in）	ifInOctets.x	.1.3.6.1.2.1.2.2.1.10.x	数字(32位)，字节	否	是
接口单播包转发数（in）	ifInUcastPkts.x	.1.3.6.1.2.1.2.2.1.11.x	数字(32位)，个	否	是
接口非单播包转发数（in）	ifInNUcastPkts.x	.1.3.6.1.2.1.2.2.1.12.x	数字(32位)，个		
接口丢包（in）	ifInDiscards.x	.1.3.6.1.2.1.2.2.1.13.x	数字(32位)，个	否	是
接口错包（in）	ifInErrors.x	.1.3.6.1.2.1.2.2.1.14.x	数字(32位)，个	否	是
丢弃的未知协议包	ifInUnknownProtos.x	.1.3.6.1.2.1.2.2.1.15.x	数字(32位)，个	否	是
接口流量（out）	ifOutOctets.x	.1.3.6.1.2.1.2.2.1.16.x	数字(32位)，字节	否	是
接口单播包转发数（out）	ifOutUcastPkts.x	.1.3.6.1.2.1.2.2.1.17.x	数字(32位)，个	否	是
接口非单播包转发数（out）	ifOutNUcastPkts.x	.1.3.6.1.2.1.2.2.1.18.x	数字(32位)，个	否	是
接口丢包（out）	ifOutDiscards.x	.1.3.6.1.2.1.2.2.1.19.x	数字(32位)，个	否	是
接口错包（out）	ifOutErrors.x	.1.3.6.1.2.1.2.2.1.20.x	数字(32位)，个	否	是
IfXEntry (增强表)					
接口名字	ifName.x	.1.3.6.1.2.1.31.1.1.1.1.x	字符串		
接口多播包转发数（in）	ifInMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.2.x	数字(32位)，个	否	是

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

接口广播包转发数（in）	ifInBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.3.x	数字(32位)，个	否	是
接口多播包转发数（out）	ifOutMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.4.x	数字(32位)，个	否	是
接口广播包转发数（out）	ifOutBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.5.x	数字(32位)，个	否	是
接口流量（in）64位	ifHCInOctets.x	.1.3.6.1.2.1.31.1.1.1.6.x	数字(64位)，字节	否	是
接口单播包转发数（in）64位	ifHCInUcastPkts.x	.1.3.6.1.2.1.31.1.1.1.7.x	数字(64位)，个	否	是
接口多播包转发数（in）64位	ifHCInMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.8.x	数字(64位)，个	否	是
接口广播包转发数（in）64位	ifHCInBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.9.x	数字(64位)，个	否	是
接口流量（out）64位	ifHCOutOctets.x	.1.3.6.1.2.1.31.1.1.1.10.x	数字(64位)，字节	否	是
接口单播包转发数（out）64位	ifHCOutUcastPkts.x	.1.3.6.1.2.1.31.1.1.1.11.x	数字(64位)，个	否	是
接口多播包转发数（out）64位	ifHCOutMulticastPkts.x	.1.3.6.1.2.1.31.1.1.1.12.x	数字(64位)，个	否	是
接口广播包转发数（out）64位	ifHCOutBroadcastPkts.x	.1.3.6.1.2.1.31.1.1.1.13.x	数字(64位)，个	否	是
接口updown状态变化是否发送trap	ifLinkUpDownTrapEnable.x	.1.3.6.1.2.1.31.1.1.1.14.x	1：enable, 2:其他	否	是
接口速率	ifHighSpeed.x	.1.3.6.1.2.1.31.1.1.1.15.x	正整数,单位:Mbit		
复合参数					
接口bps（in）Inbound Throughput	使用复合表达式	吞吐量：间隔t秒执行2次获取ifHCInOctets.x (.1.3.6.1.2.1.31.1.1.1.6.x)的值，结果分别为ifHCInOctets.x.time1和ifHCInOctets.x.time2。interface x的in_bps = (ifHCInOctets.x.time2 - ifHCInOctets.x.time1) * 8 / t	吞吐量：数字,bps	否	是
接口bps（out）Outbound Throughput	使用复合表达式	吞吐量：间隔t秒执行2次获取ifHCOutOctets.x的值，结果分别为ifHCOutOctets.x.time1和ifHCOutOctets.x.time2。interface x的out_bps = (ifHCOutOctets.x.time2 - ifHCOutOctets.x.time1) * 8 / t	吞吐量：数字,bps	否	是

TCP/IP/策略监控项

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

监控参数明细	Object	对应OID值	参数类别（单位）	SYSLOG告警	SNMP告警
IP					
端口接收到的ip报文总数	ipInReceives.0	.1.3.6.1.2.1.4.3.0	数字（32位），个	否	是
IP头部错误丢包	ipInHdrErrors.0	.1.3.6.1.2.1.4.4.0	数字（32位），个	否	是
IP目标地址错误丢弃包	ipInAddrErrors.0	.1.3.6.1.2.1.4.5.0	数字（32位），个	否	是
未知协议数据包	ipInUnknownProtos	.1.3.6.1.2.1.4.7.0	数字（32位），个	否	是
被丢弃的IP包（如缓冲区不够）	ipInDiscards.0	.1.3.6.1.2.1.4.8.0	数字（32位），个	否	是
被转发包的IP包，包括ICMP	ipInDelivers.0	.1.3.6.1.2.1.4.9.0	数字（32位），个	否	是
需重组数据包	ipReasmReqds.0	.1.3.6.1.2.1.4.14.0	数字（32位），个	否	是
重组成功数据包	ipReasmOKs.0	.1.3.6.1.2.1.4.15.0	数字（32位），个	否	是
重组失败数据包	ipReasmFails.0	.1.3.6.1.2.1.4.16.0	数字（32位），个	否	是
分片成功数据包	ipFragOKs.0	.1.3.6.1.2.1.4.17.0	数字（32位），个	否	是
分片失败数据包	ipFragFails.0	.1.3.6.1.2.1.4.18.0	数字（32位），个	否	是
TCP					
TCP数据分组（in）	tcpInSegs.0	.1.3.6.1.2.1.6.10.0	数字（32位），个	否	是
TCP数据分组（out）	tcpOutSegs.0	.1.3.6.1.2.1.6.11.0	数字（32位），个	否	是
重传的数据分组	tcpRetransSegs.0	.1.3.6.1.2.1.6.12.0	数字（32位），个	否	是
接收到的TCP错包	tcpInErrs.0	.1.3.6.1.2.1.6.14.0	数字（32位），个	否	是
发送的RST数据包	tcpOutRsts.0	.1.3.6.1.2.1.6.15.0	数字（32位），个	否	是
Policy					
策略命中包数	fgFwPolPktCount.1.x（x为策略ID）	.1.3.6.1.4.1.12356.101.5.1.2.1.1.2.1.x	数字（32位），次		
策略命中字节数	fgFwPolByteCount.1.x（x为策略ID）	.1.3.6.1.4.1.12356.101.5.1.2.1.1.3.x	数字（32位），byte		

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SNMP的常用工具

Net-SNMP

网址链接：http://www.net-snmp.org/ ↗

Download：http://www.net-snmp.org/download.html ↗

1. CentOS 7 安装Net-SNMP和SNMP V2：

```
[Wed Aug 05 10:07:33 root@centos7~#yum install -y net-snmp*
Loaded plugins: fastestmirror, langpacks
Determining fastest mirrors
 * base: mirror2.totbb.net
 * extras: mirror.hostlink.com.hk
 * updates: mirror01.idc.hinet.net
base                                                                                                |
3.6 kB  00:00:00
extras                                                                                              |
2.9 kB  00:00:00
updates                                                                                             |
2.9 kB  00:00:00
(1/2): extras/7/x86_64/primary_db                                                                   |
205 kB  00:00:00
(2/2): updates/7/x86_64/primary_db
|3.7 MB   00:00:11
......

Installed:
  net-snmp.x86_64 1:5.7.2-48.el7_8.1           net-snmp-agent-libs.x86_64 1:5.7.2-48.el7_8.1  net-snmp-
devel.x86_64 1:5.7.2-48.el7_8.1
  net-snmp-gui.x86_64 1:5.7.2-48.el7_8.1       net-snmp-perl.x86_64 1:5.7.2-48.el7_8.1        net-snmp-
python.x86_64 1:5.7.2-48.el7_8.1
  net-snmp-sysvinit.x86_64 1:5.7.2-48.el7_8.1  net-snmp-utils.x86_64 1:5.7.2-48.el7_8.1

Dependency Installed:
  elfutils-devel.x86_64 0:0.176-4.el7                          elfutils-libelf-devel.x86_64 0:0.176-4.el7
  libdb-devel.x86_64 0:5.3.21-25.el7                           lm_sensors-devel.x86_64 0:3.4.0-
8.20160601gitf9185e5.el7
  perl-ExtUtils-Install.noarch 0:1.58-295.el7                  perl-ExtUtils-MakeMaker.noarch 0:6.68-3.el7
  perl-ExtUtils-Manifest.noarch 0:1.61-244.el7                 perl-ExtUtils-ParseXS.noarch 1:3.18-3.el7
  perl-Tk.x86_64 0:804.030-6.el7                               perl-devel.x86_64 4:5.16.3-295.el7
  popt-devel.x86_64 0:1.13-16.el7                              rpm-devel.x86_64 0:4.11.3-43.el7
  systemtap-sdt-devel.x86_64 0:4.0-11.el7                      tcp_wrappers-devel.x86_64 0:7.6-77.el7

Updated:
  net-snmp-libs.x86_64 1:5.7.2-48.el7_8.1

Dependency Updated:
  elfutils.x86_64 0:0.176-4.el7            elfutils-libelf.x86_64 0:0.176-4.el7            elfutils-libs.x86_64
0:0.176-4.el7

Complete!
[Thu Aug 06 09:56:37 root@centos7~#
[Thu Aug 06 10:09:13 root@centos7~# snmpd -v

NET-SNMP version:  5.7.2
Web:               http://www.net-snmp.org/
Email:             net-snmp-coders@lists.sourceforge.net

[Thu Aug 06 10:09:18 root@centos7~#
[Thu Aug 06 10:09:46 root@centos7~#systemctl start snmpd.service
[Thu Aug 06 10:09:49 root@centos7~#
[Thu Aug 06 10:10:17 root@centos7~#snmpwalk -v 1 -c public 127.0.0.1 .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = STRING: Linux centos7.lab.fortinet.com 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02
UTC 2019 x86_64
[Thu Aug 06 10:10:19 root@centos7~#
[Thu Aug 06 10:24:55 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.90.3 .1.3.6.1.2.1.1.5.0
SNMPv2-MIB::sysName.0 = STRING: HUB2-ShangHai
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[Thu Aug 06 10:24:59 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.90.3 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM04TM20003482"
[Thu Aug 06 10:25:01 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.90.3 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v6.4.1,build1637,200604 (GA)"
[Thu Aug 06 10:25:21 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.90.3 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (301149616) 34 days, 20:31:36.16
[Thu Aug 06 10:25:55 root@centos7~#
```

2. Net-SNMP SNMP V3

```
[Thu Aug 06 11:56:06 root@centos7~#service snmpd  stop
Stopping snmpd (via systemctl):                            [  OK  ]
[Thu Aug 06 11:56:20 root@centos7~#
[Thu Aug 06 12:00:52 root@centos7~#
[Thu Aug 06 12:01:01 root@centos7~#net-snmp-config --create-snmpv3-user -ro -a SHA -A forti3389 -x AES -X
forti5566 fortinet
adding the following line to /var/lib/net-snmp/snmpd.conf:
   createUser fortinet SHA "forti3389" AES forti5566
adding the following line to /etc/snmp/snmpd.conf:
   rouser fortinet
[Thu Aug 06 12:01:09 root@centos7~#
[Thu Aug 06 12:01:10 root@centos7~#chkconfig snmpd on
Note: Forwarding request to 'systemctl enable snmpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/snmpd.service to
/usr/lib/systemd/system/snmpd.service.
[Thu Aug 06 12:01:30 root@centos7~#service snmpd start
Starting snmpd (via systemctl):                            [  OK  ]
[Thu Aug 06 12:01:36 root@centos7~#
[Thu Aug 06 12:06:29 root@centos7~#
[Thu Aug 06 12:06:38 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.90.3
SNMPv2-MIB::sysDescr.0 = STRING: Fortinet_BeiJing_LAB_FGT-KVM
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.12356.101.1.60
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (301754102) 34 days, 22:12:21.02
SNMPv2-MIB::sysContact.0 = STRING: kmliu@fortinet.com
SNMPv2-MIB::sysName.0 = STRING: HUB2-ShangHai
SNMPv2-MIB::sysLocation.0 = STRING: China_BeiJing_Lab
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORIndex.1 = INTEGER: 1
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-SMI::zeroDotZero.0
SNMPv2-MIB::sysORDescr.1 = STRING:
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 19
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
^C
[Thu Aug 06 12:06:41 root@centos7~#
[Thu Aug 06 12:06:45 root@centos7~#
[Thu Aug 06 12:10:23 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.90.3 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM04TM20003482"
[Thu Aug 06 12:10:45 root@centos7~#
[Thu Aug 06 12:10:46 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.90.3 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (301780209) 34 days, 22:16:42.09
[Thu Aug 06 12:11:00 root@centos7~#
[Thu Aug 06 12:11:12 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.90.3 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v6.4.1,build1637,200604 (GA)"
[Thu Aug 06 12:11:19 root@centos7~#
```

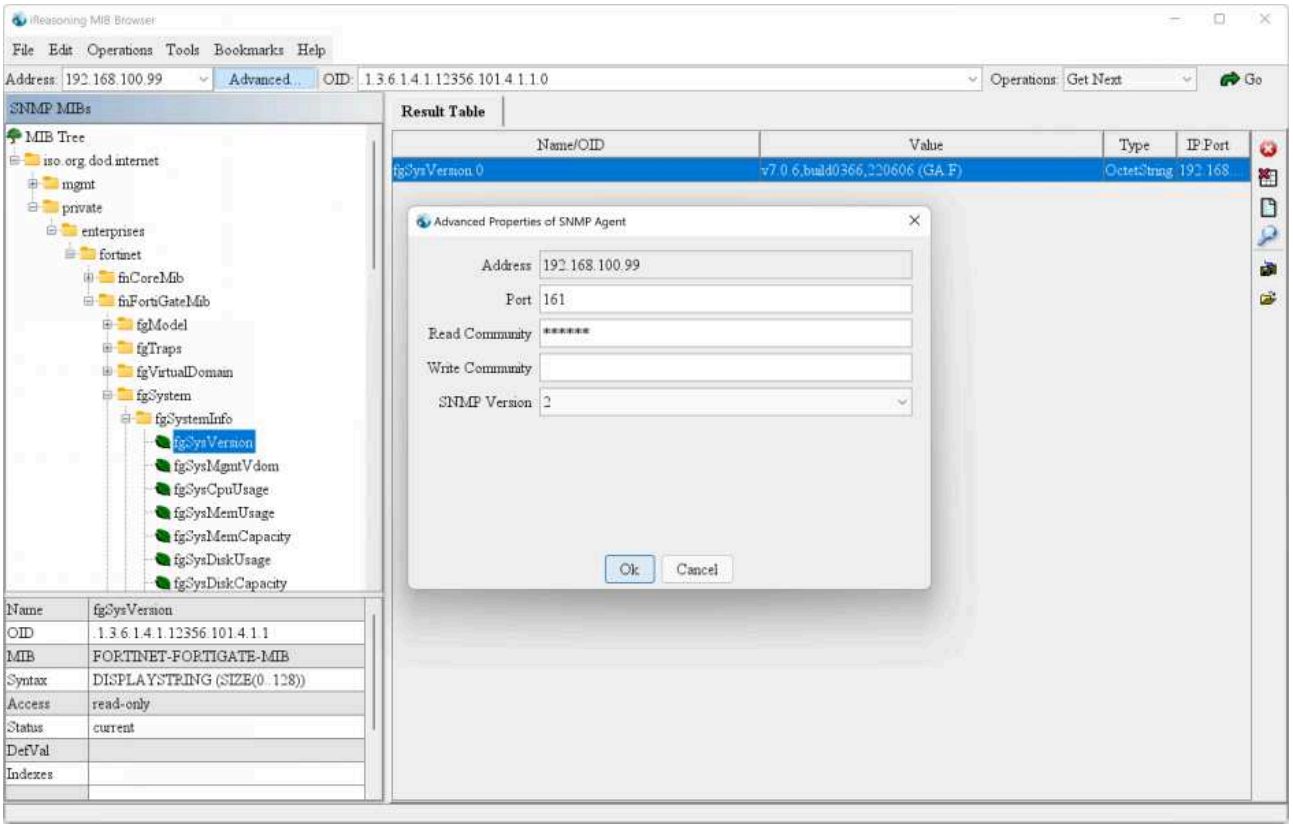
Net-SNMP v3参考链接：https://www.thegeekdiary.com/centos-rhel-6-install-and-configure-snmpv3/ ↗

iReasoning MIB browser（提供免费版本）

网址链接：https://www.ireasoning.com/ ↗

Download：https://www.ireasoning.com/downloadmibbrowserfree.php ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



PRTG（提供100个传感器的免费版本）

网址链接：https://www.cn.paessler.com/

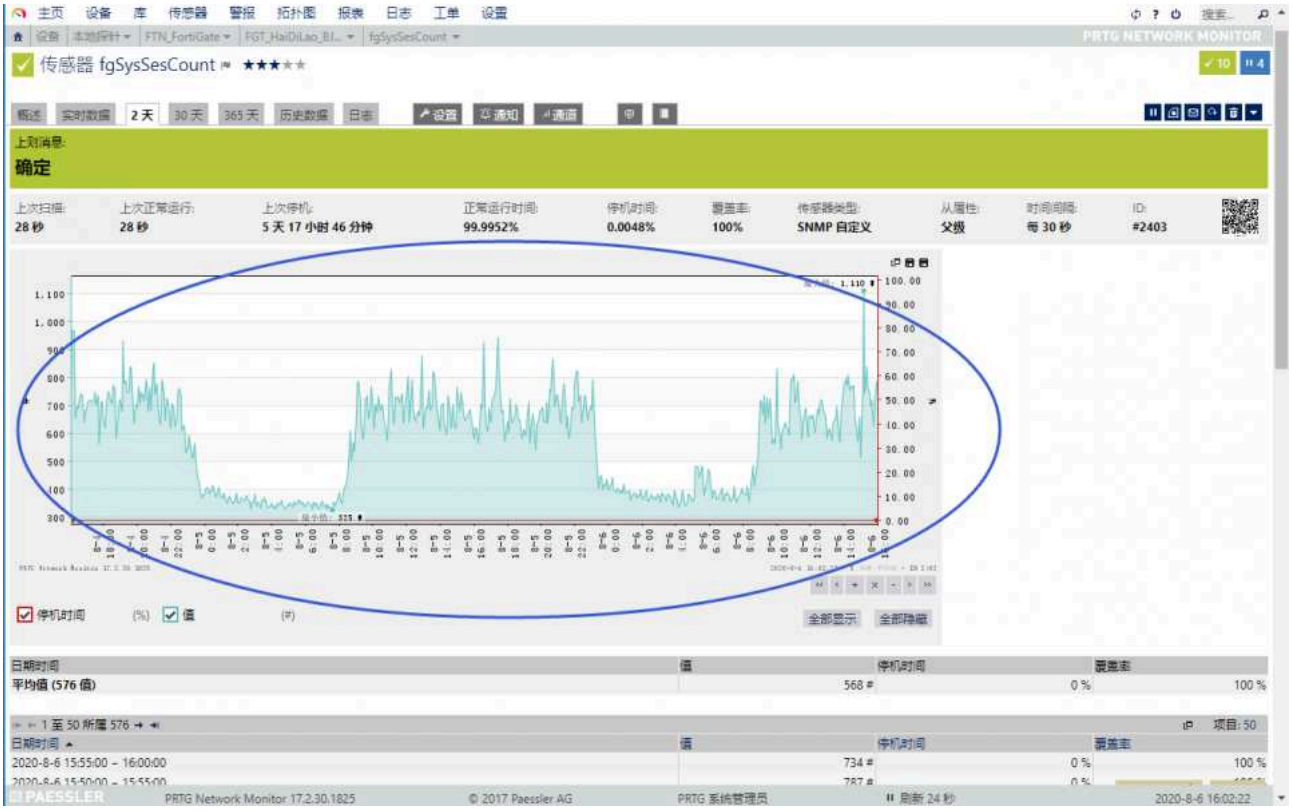
Download：https://www.cn.paessler.com/download/prtg-download/

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



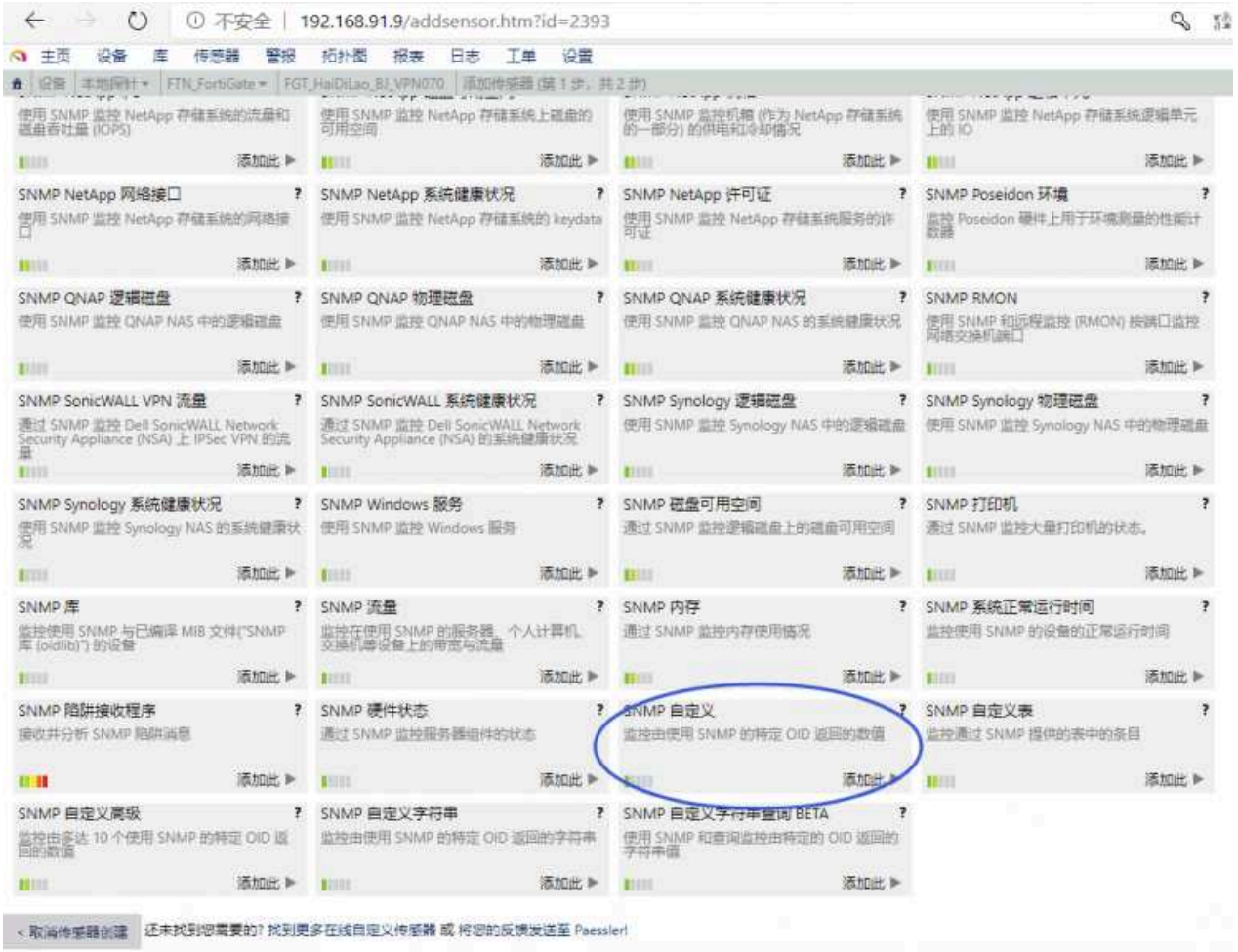


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

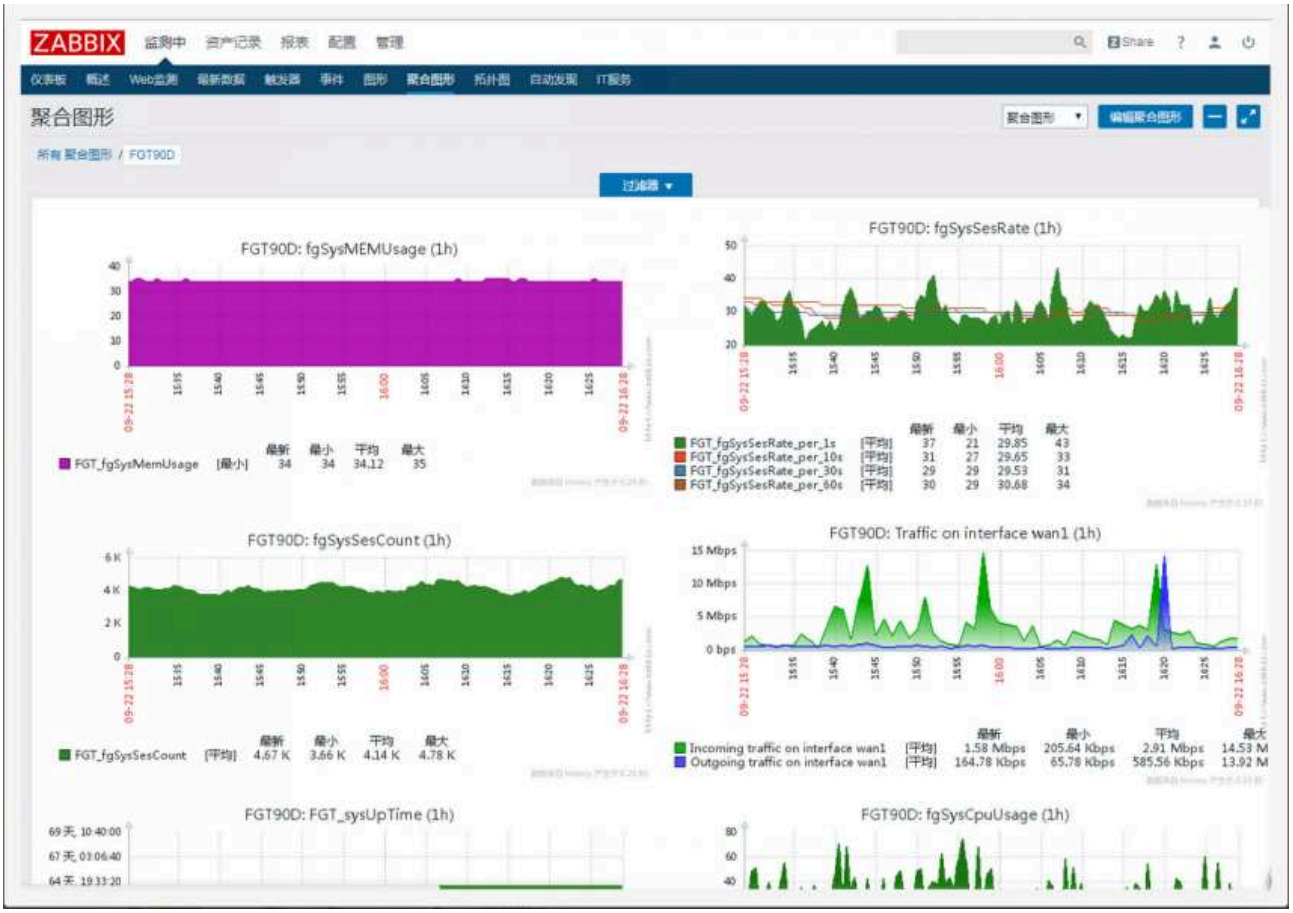


Zabbix（开源免费）

网址链接：https://www.zabbix.com/cn ↗

针对FortiGate的监控模板下载：https://git.zabbix.com/projects/ZBX/repos/zabbix/browse/templates/net/fortinet/fortigate_snmp?at=release/6.4 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

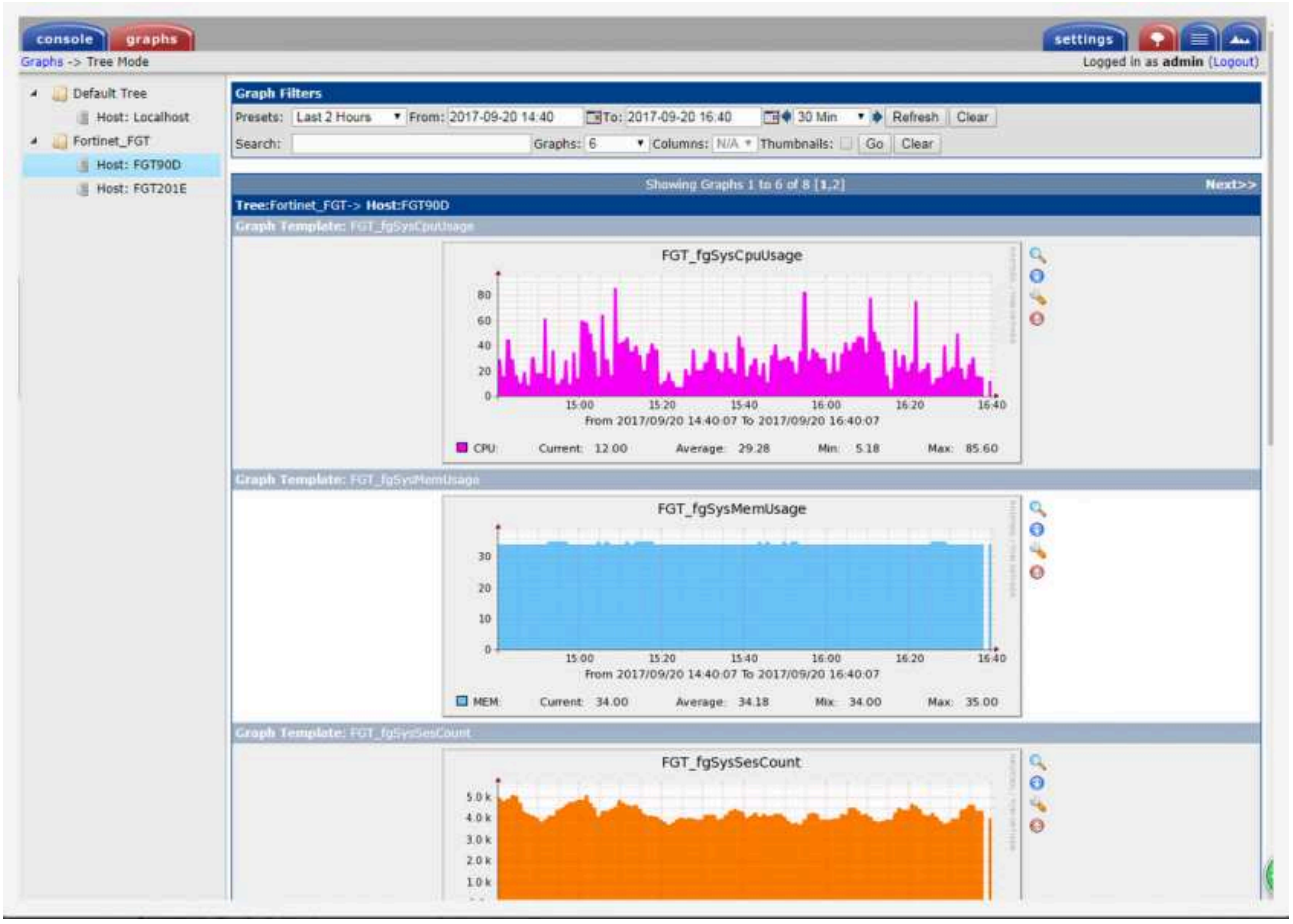


Cacti（开源免费）

网址链接：https://www.cacti.net/ ↗

download网址：https://www.cacti.net/download_cacti.php ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



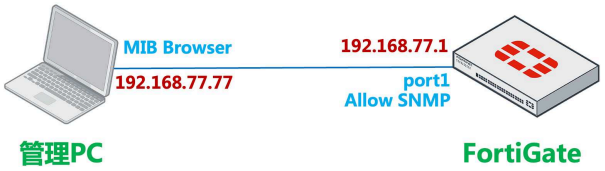
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SNMP的设置

网络需求

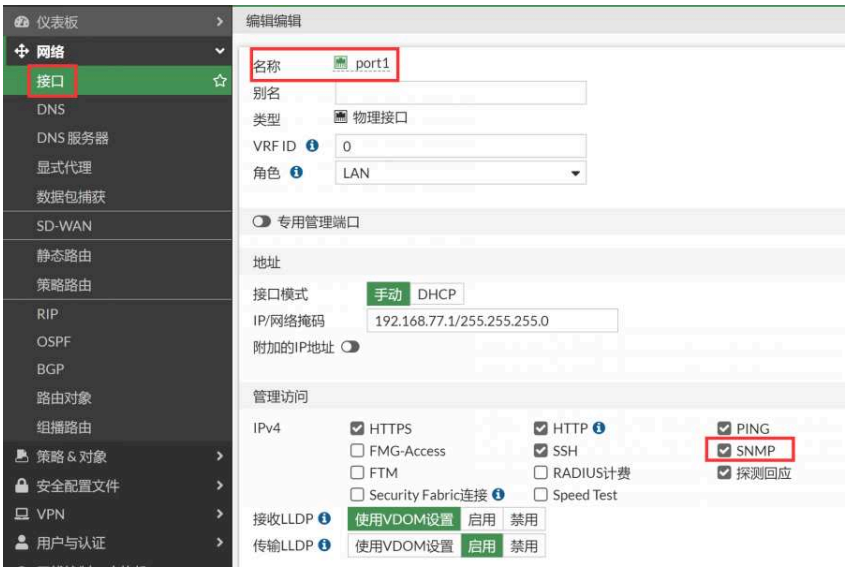
配置FortiGate的SNMP。

网络拓扑

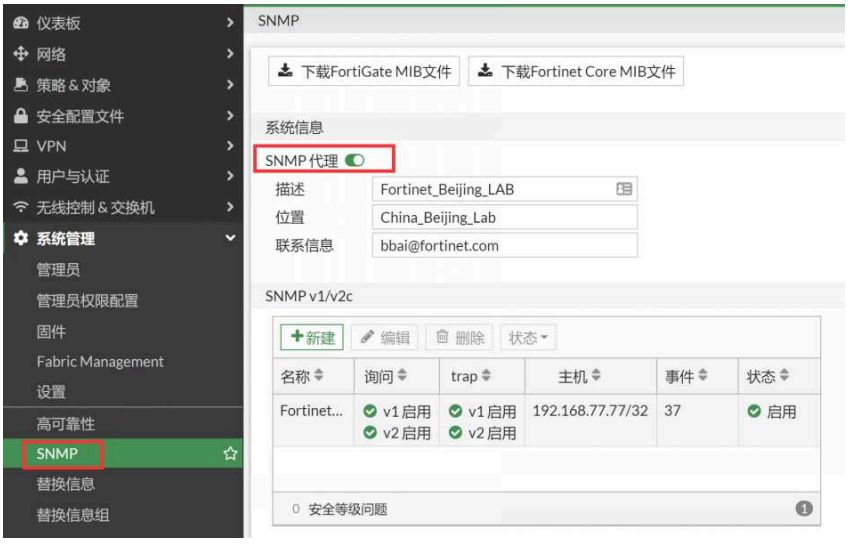


配置步骤

1. 接口上开启SNMP的允许访问。



2. 开启SNMP的总开关。

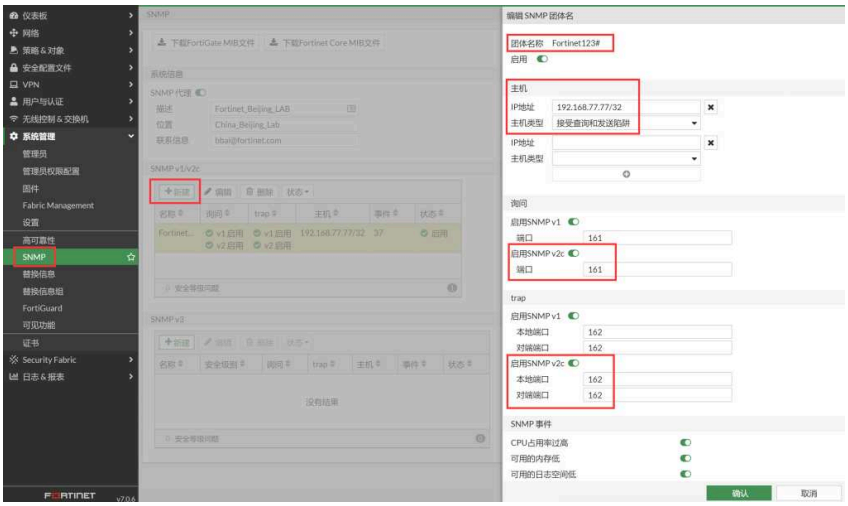


3. 配置SNMP v2的属性，比如配置SNMPv2的SNMP属性为Fortinet123#，建议不要使用通用的public，容易被探测和攻击。需要添加SNMP客户端的主机IP（192.168.77.77）的SNMP权限，把主机的IP地址（192.168.77.77）添加到SNMPv2的配置里面。

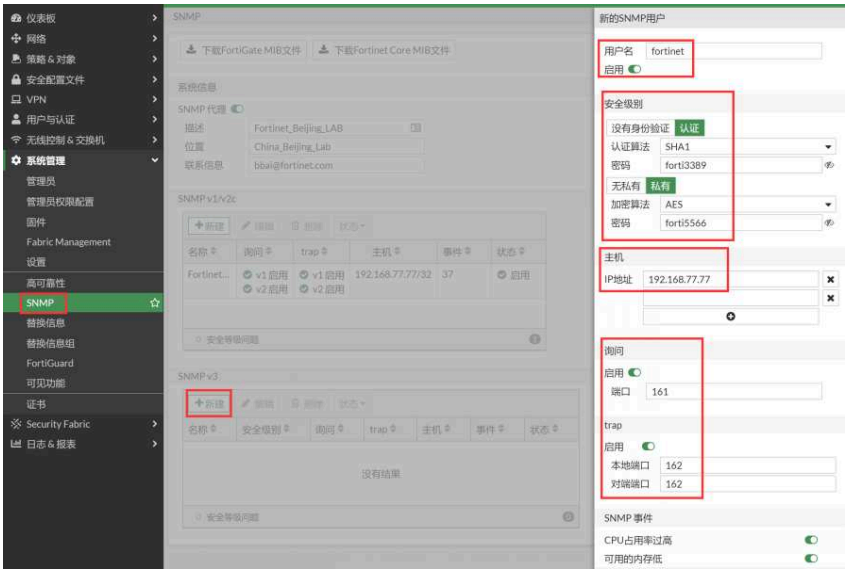
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

团体名称（Community）中不能包含字符 `$`，否则配置后读取SNMP会失败。



4. 配置SNMPv3，配置SNMPv3的用户名为fortinet，认证算法选择SHA1，密码为forti3389，加密算法选择为AES，密码为forti5566。需要添加SNMP客户端的主机IP（192.168.77.77）的SNMP权限，把主机的IP地址（192.168.77.77）添加到SNMPv2的配置里面。



5. SNMP命令行配置汇总。

```
config system interface
    edit "port1"
        set allowaccess ping https ssh snmp http probe-response
    next
end

config system snmp sysinfo
    set status enable
    set description "Fortinet_Beijing_LAB"
    set contact-info "bbai@fortinet.com"
    set location "China_Beijing_Lab"
end

config system snmp community
    edit 1
        set name "Fortinet123#"
        config hosts
            edit 1
                set ip 192.168.77.77 255.255.255.255
            next
        end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    next
end

config system snmp user
    edit "fortinet"
        set notify-hosts 192.168.77.77
        set security-level auth-priv
        set auth-pwd ENC
MTAwNG2U70/eePNhi1N3/u4q6FSRuv2ebcPGgqV+yxRuFtKxFilE6SmYZfpMvYOQBU4InxdTXnlIeYdMguMT8×7Hsqz/Q+3G2DWXlmtJohv0RukHWQ
K4nkY/aYKCnujZkKGGyPxDKysAj4LDkR1CazeJkMKtVgGyoPF2WEjbPEt6PijsUZ67cDptDDzqnABzQFUemw==
        set priv-pwd ENC
MTAwNFIePySDQu7hqz+SFic3AUQ+1G4HX5er9qOeMxFTkZ8I7DnW+rw3XYNwgSfQtHuWEwTZGmztt6kUYUaT+oxLSdLG/RqU/3wbbE1/m4MH64bSYZ
gd+c+Pks8S44UPmGBdQeewwpwQi7xHmL/y9Gyv+t7Wb6ge0WS3dQFe971Vp7n4evJgU51EK90Cnt7TjNX0lQ==
    next
end
```

重要

有一个特别的场景需要特别注意，那就是HA独立管理口的场景，需要一些特殊的配置才可以搞定。后边的章节：

系统管理→SNMP→SNMP有HA独立管理的设置 ↗

会描述这种情况。其他情况下都是以上类似的配置即可开启FortiGate的SNMP。

结果验证

1. Net-SNMP SNMP V2结果验证。

```
[Thu Aug 06 11:46:54 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.6,build0366,220606 (GA.F)"
[Thu Aug 06 11:46:55 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (301635896) 34 days, 21:52:38.96
[Thu Aug 06 11:46:58 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM08TM22000173"
[Thu Aug 06 11:47:46 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 1.3.6.1.2.1.31.1.1.1.1.1
IF-MIB::ifName.1 = STRING: port1
[Thu Aug 06 11:47:47 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 1.3.6.1.2.1.31.1.1.1.1.2
IF-MIB::ifName.2 = STRING: port2
[Thu Aug 06 11:47:51 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 1.3.6.1.4.1.12356.101.4.1.8.0
SNMPv2-SMI::enterprises.12356.101.4.1.8.0 = Gauge32: 77
```

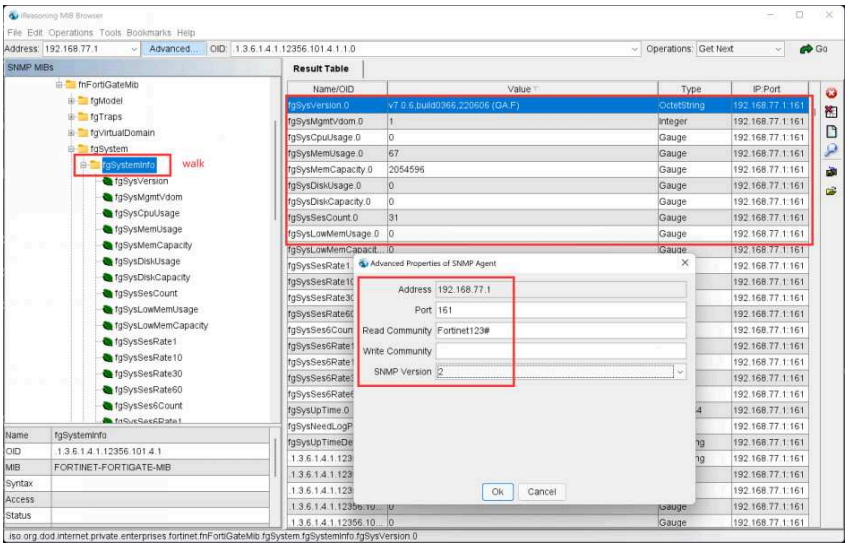
2. Net-SNMP SNMPv3结果验证。

```
[Thu Aug 06 12:01:01 root@centos7~#net-snmp-config --create-snmpv3-user -ro -a SHA -A forti3389 -x AES -X
forti5566 fortinet
adding the following line to /var/lib/net-snmp/snmpd.conf:
   createUser fortinet SHA "forti3389" AES forti5566
adding the following line to /etc/snmp/snmpd.conf:
   rouser fortinet
[Thu Aug 06 12:01:10 root@centos7~#chkconfig snmpd on
Note: Forwarding request to 'systemctl enable snmpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/snmpd.service to
/usr/lib/systemd/system/snmpd.service.
[Thu Aug 06 12:01:30 root@centos7~#service snmpd start
Starting snmpd (via systemctl):                            [  OK  ]
[Thu Aug 06 12:06:38 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.77.1
SNMPv2-MIB::sysDescr.0 = STRING: Fortinet_Beijing_LAB
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.12356.101.1.60
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (301754102) 34 days, 22:12:21.02
SNMPv2-MIB::sysContact.0 = STRING: bbai@fortinet.com
SNMPv2-MIB::sysName.0 = STRING: FortiGate
SNMPv2-MIB::sysLocation.0 = STRING: China_Beijing_Lab
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysORIndex.1 = INTEGER: 1
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-SMI::zeroDotZero.0
SNMPv2-MIB::sysORDescr.1 = STRING:
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (0) 0:00:00.00
IF-MIB::ifNumber.0 = INTEGER: 19
```

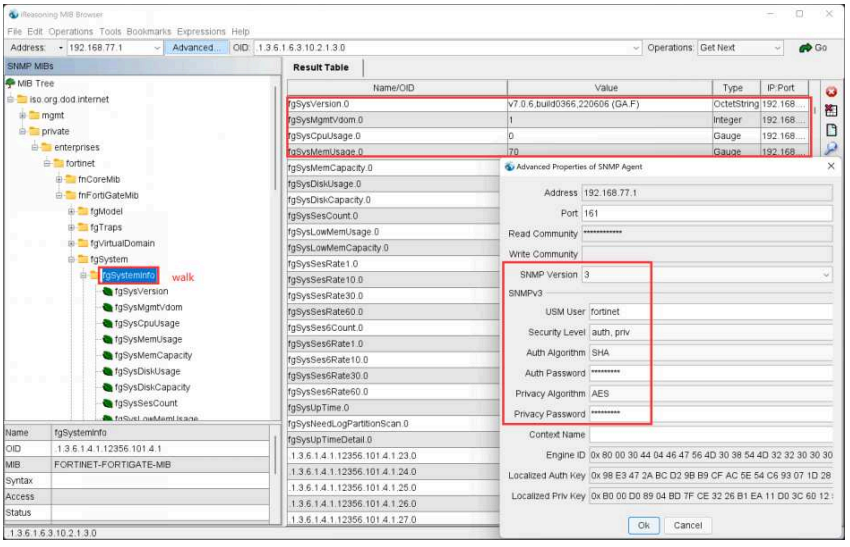

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
IF-MIB::ifIndex.1 = INTEGER: 1
IF-MIB::ifIndex.2 = INTEGER: 2
[Thu Aug 06 12:10:23 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.77.1 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM08TM22000173"
[Thu Aug 06 12:10:45 root@centos7~#
[Thu Aug 06 12:10:46 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.77.1 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (301780209) 34 days, 22:16:42.09
[Thu Aug 06 12:11:00 root@centos7~#
[Thu Aug 06 12:11:12 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.77.1 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.6,build0366,220606 (GA.F)"
```

3. iReasoning MIB Browser SNMPv2验证。

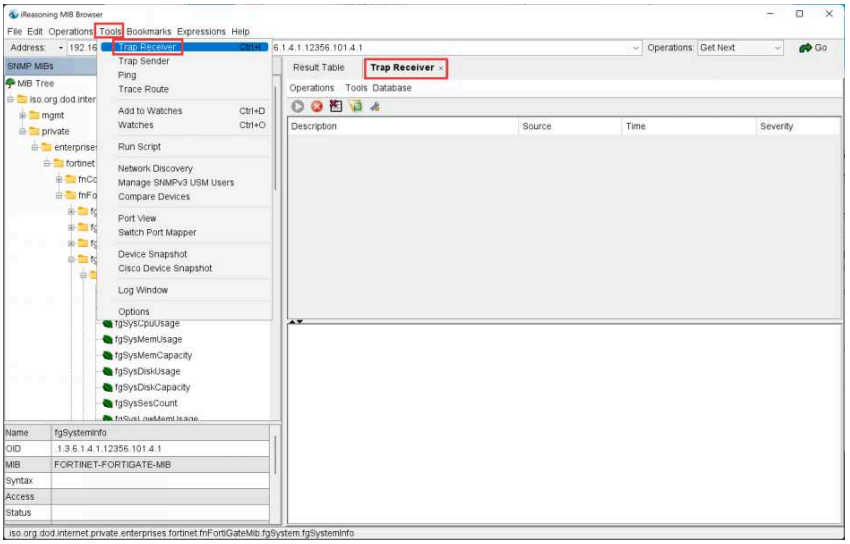


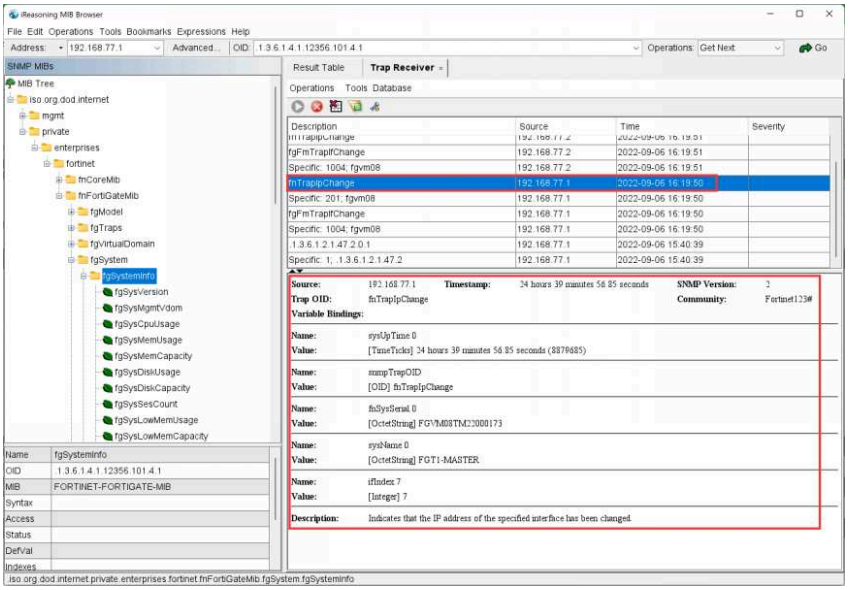
4. MIB Browser SNMP V3验证。

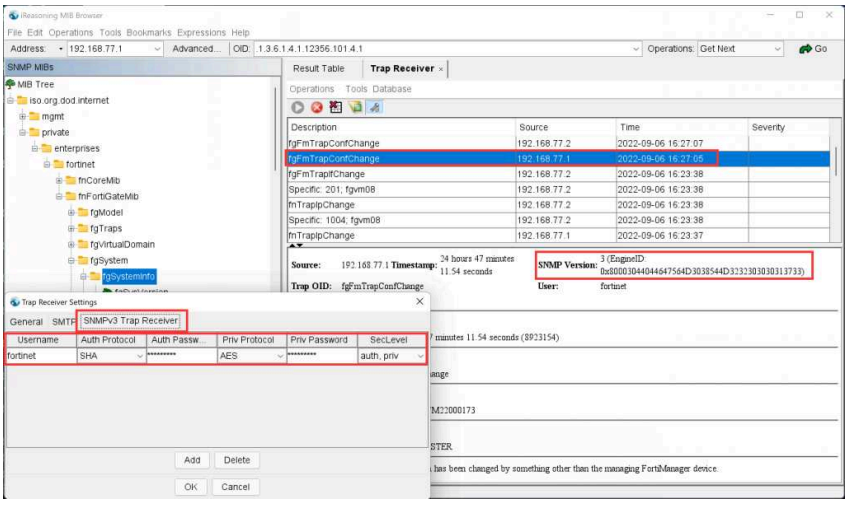


5. iReasoning MIB Browser SNMP Trap验证，SNMPv2和SNMPv3均可以正常接收Trap消息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







SNMP排错

1. 抓包，确认SNMP UDP 161、162的通信是正常的，正常SNMP是有去有回的。

```
# diagnose sniffer packet any "port 161 and host 192.168.77.1" 4
```

2. 通过第一步抓包看到SNMP流量有去有回了，但是SNMP还是失败，则开启SNMP进程的debug，查看具体原因。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

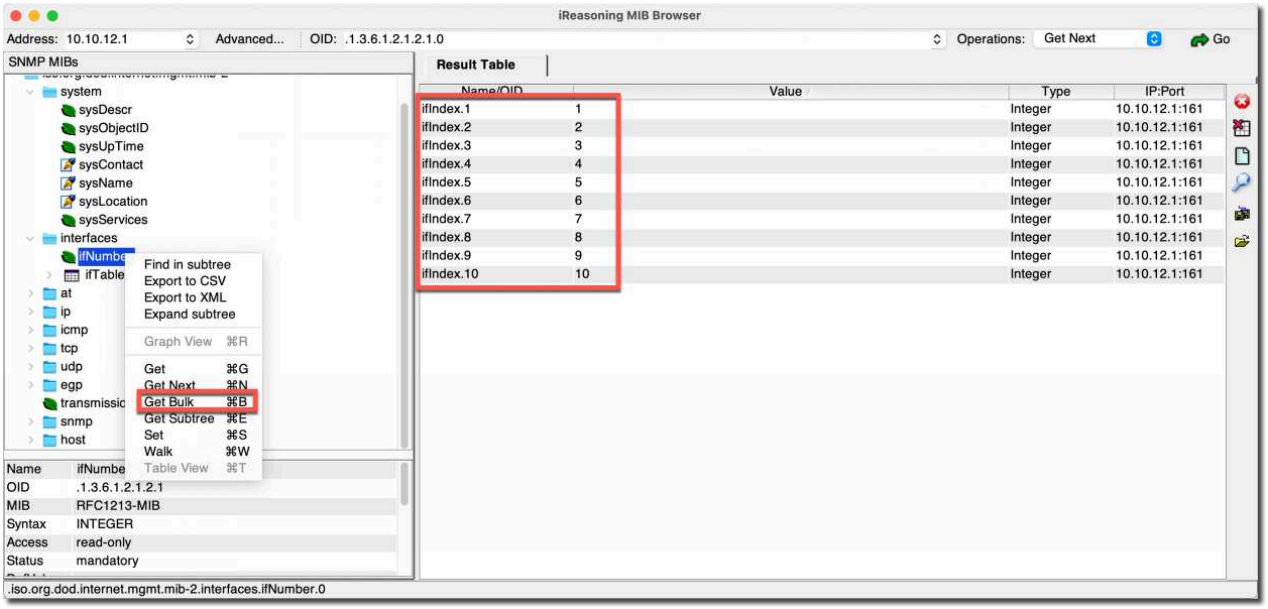
```
# diagnose debug application snmpd -1
# diagnose debug enable
```

比如，最常见的错误“community”不匹配、管理员配置了可信任主机，但是没有包括SNMP的IP地址等等...

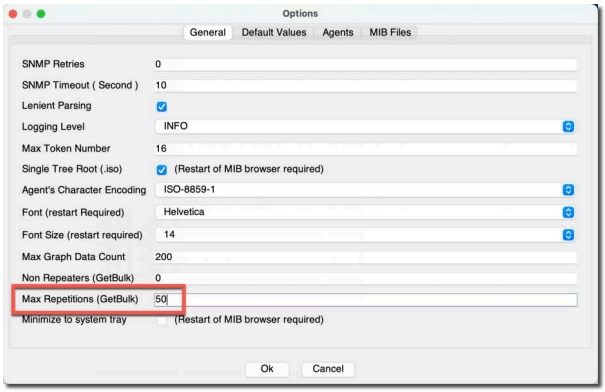
```
HUB2-ShangHai # snmpd: updating cache: idx_cache
snmpd: <msg> 47 bytes 192.168.90.254:44539 → 200.1.1.1/200.1.1.1:161 (itf 3.3)
snmpd: checking if community "Fortinet123#2" is valid
snmpd: updating cache: vdom_idx_map_cache
snmpd: updating vdom idx mapping
snmpd: Creating vdom_idx_cache for root
snmpd: Vdom created kernel-index=0, snmp-index=1, name=root
snmpd: checking against community "Fortinet123#"
snmpd: vdom name mismatch
snmpd: checking against community "FortiManager"
snmpd: name mismatch.
snmpd: failed to match community "Fortinet123#2"
snmpd: </msg> 0
```

注意事项

1. 使用iReasoning MIB Browser的“get bulk”方式去get FortiGate某节点的多个子节点时，默认情况下最多只能读取10个，如下所示读取FortiGate的接口列表时，使用get bulk方式只能读取10个接口信息：

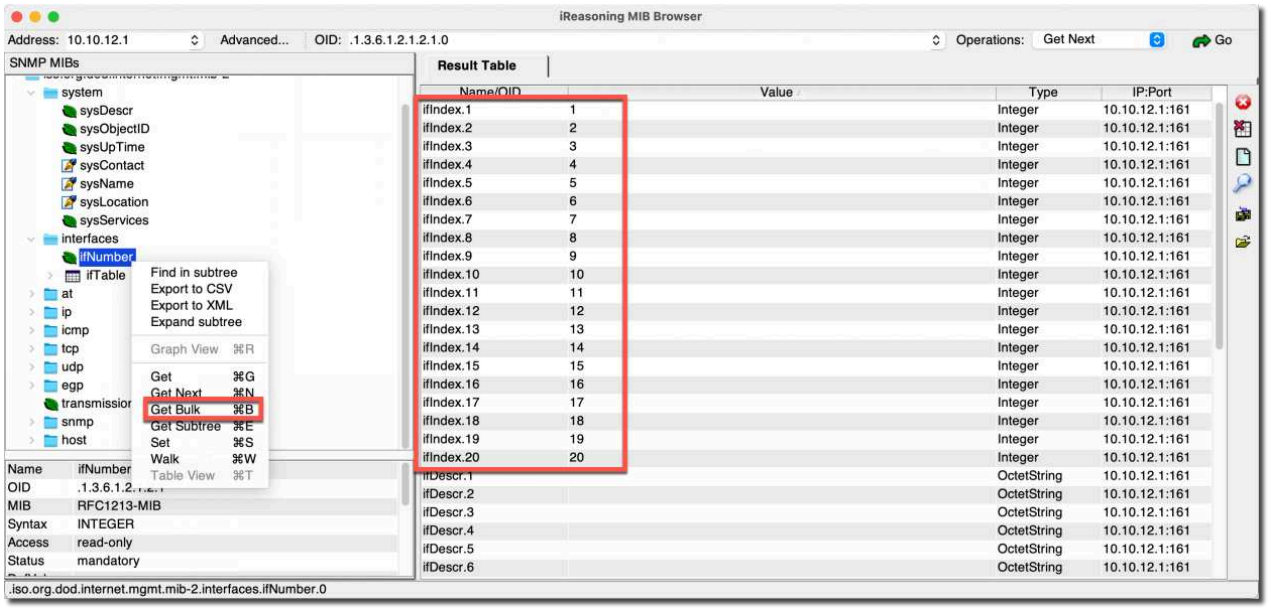


2. 此时读取的接口信息是不全的，需要在iReasoning MIB Browser的软件配置中，修改“get bulk”的最大值，



3. 再次执行“get bulk”，所有的接口信息都可以get到：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 也可以使用walk方式代替get bulk遍历节点。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SNMP与管理员可信主机

网络需求

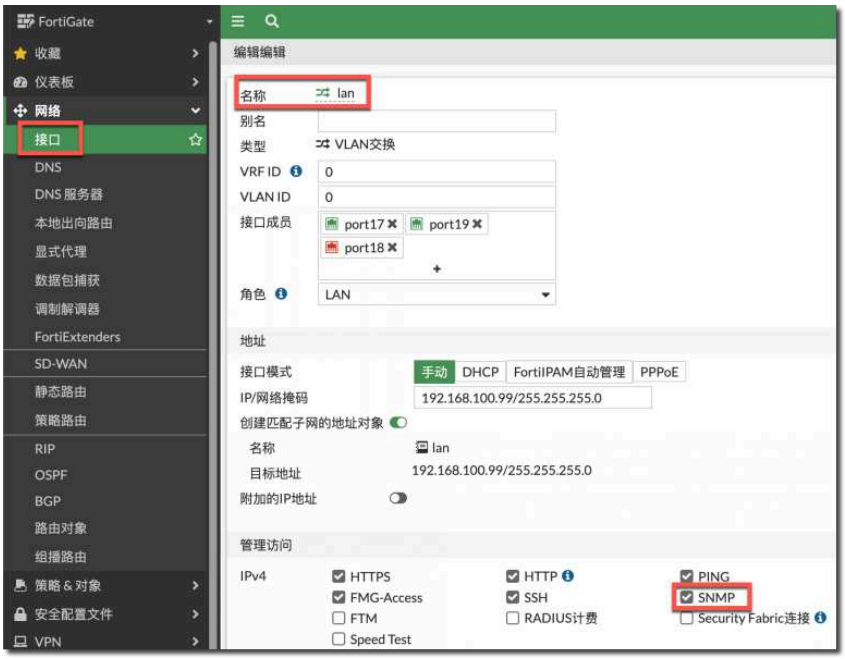
通过管理PC通过FortiGate的lan口访问SNMP，同时FortiGate配置了管理员可信主机。

网络拓扑



配置步骤

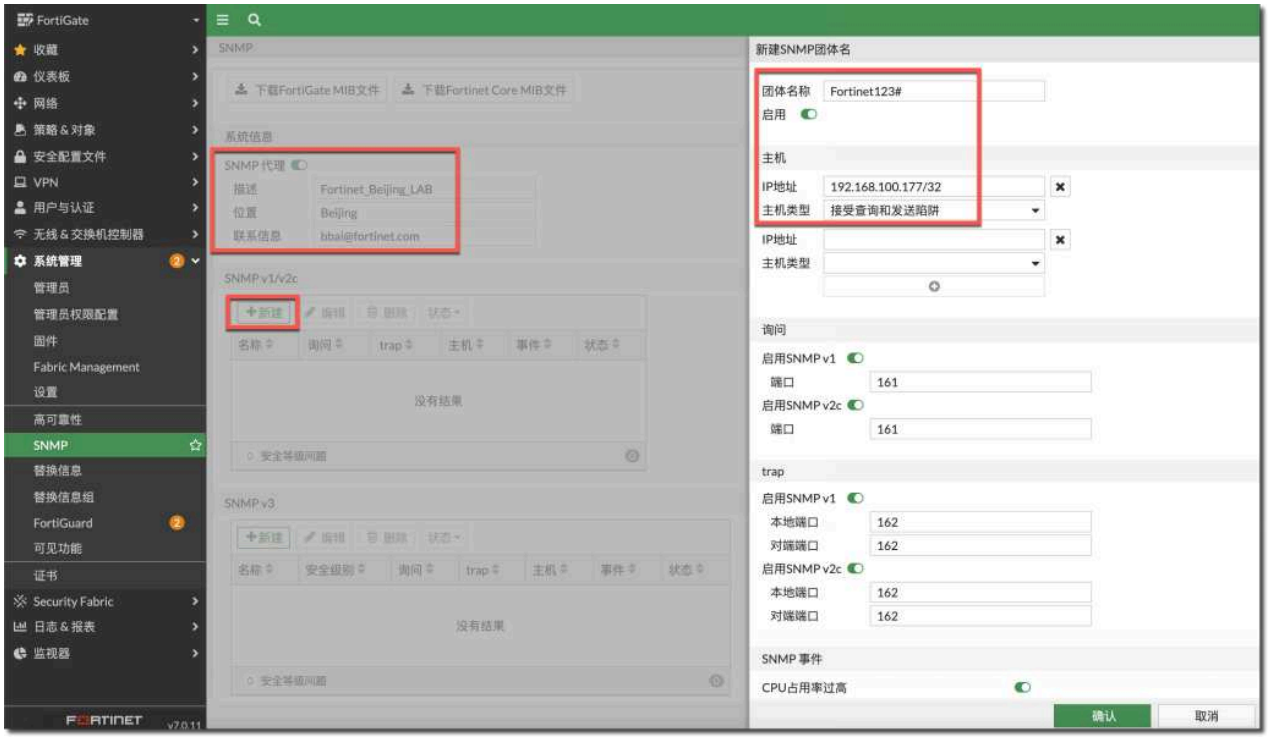
1. 在FortiGate的lan接口上开启SNMP的允许访问。

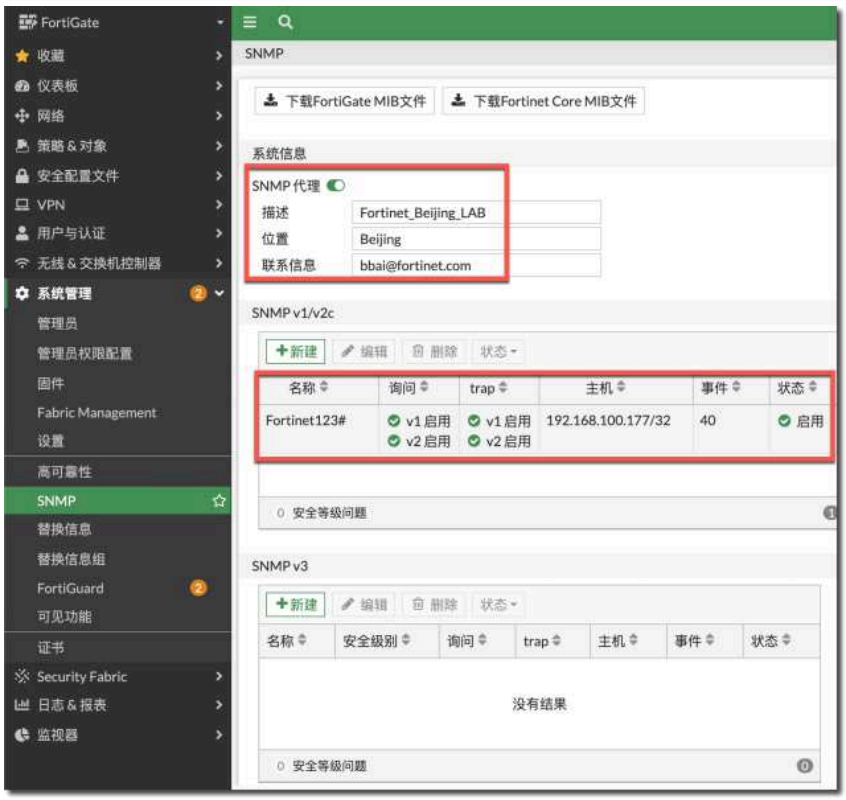



```
config system interface
    edit "lan"
        append allowaccess snmp
    next
end
```

2. 开启SNMP代理的总开关，并填写代理信息。新建并配置SNMP v1和v2的属性，例如配置SNMP团体名称为Fortinet123#，建议不要使用通用的public，容易被探测和攻击。配置SNMP主机为192.168.100.177/32。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
config system snmp sysinfo
    set status enable
    set description "Fortinet_Beijing_LAB"
    set contact-info "bbai@fortinet.com"
    set location "Beijing"
end

config system snmp community
    edit 2
        set name "Fortinet123#"
        config hosts
            edit 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

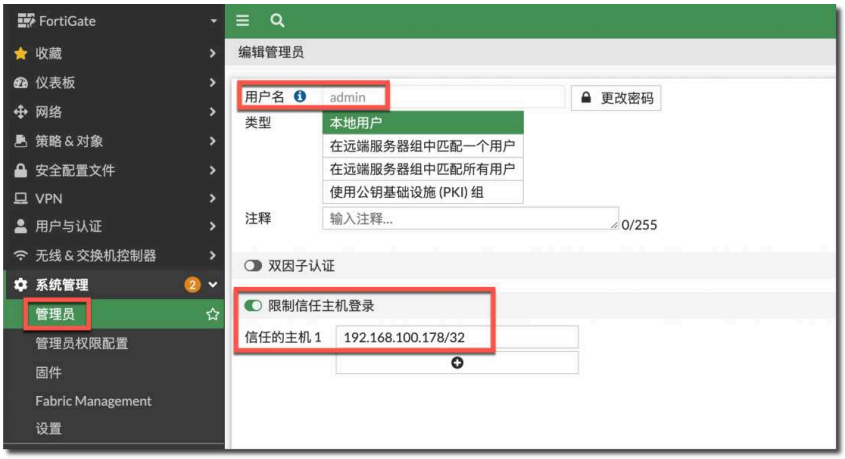
```
                set ip 192.168.100.177 255.255.255.255
            next
        end
    next
end
```

结果验证

1. 使用客户端PC 192.168.100.177对FortiGate进行SNMP读取，在没有配置管理员信任主机之前，SNMP可以正常读取。

```
~ > ifconfig en7
...
    inet 192.168.100.177 netmask 0xffffff00 broadcast 192.168.100.255
...

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.11,build0489,230314 (GA.M)"

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (11060652) 1 day, 6:43:26.52

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FG101FTK20007637"
```

2. 配置管理员信任主机为192.168.100.178/32，不包含192.168.100.177/32。






```
config system admin
    edit "admin"
        set trusthost1 192.168.100.178 255.255.255.255
    next
end
```

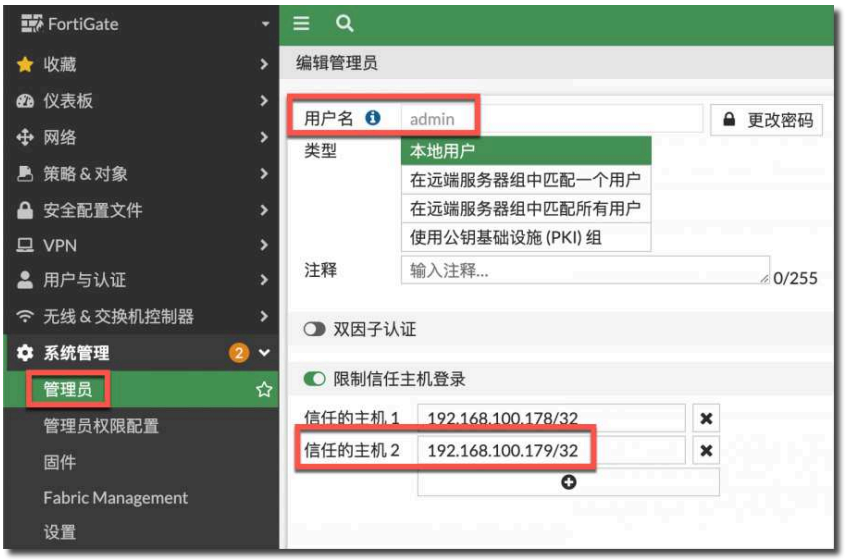
3. 再次使用客户端PC 192.168.100.177对FortiGate进行SNMP读取，全部超时失败。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
~ > ifconfig en7
...
    inet 192.168.100.177 netmask 0xffffff00 broadcast 192.168.100.255
...

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.101.4.1.1.0
Timeout: No Response from 192.168.100.99

✘ ~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 1.3.6.1.2.1.1.3.0
Timeout: No Response from 192.168.100.99

✘ ~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.100.1.1.1.0
Timeout: No Response from 192.168.100.99
```

4. 很明显管理员信任主机是对接口下面的所有访问协议起作用的，包括所有的管理协议（除了PING），自然也包括了SNMP协议。所以即使接口下开启了SNMP协议，但配置了管理主机后，也只有管理主机可以访问该接口的SNMP服务。

5. 开启管理员可信主机后要解决这个问题，需要将SNMP管理主机的IP地址也加入到管理员的可信任主机中，这样SNMP才可以正常获取信息。




```
config system admin
    edit "admin"
        set trusthost1 192.168.100.178 255.255.255.255
        set trusthost2 192.168.100.179 255.255.255.255
    next
end
```

6. 再次使用客户端PC 192.168.100.177对FortiGate进行SNMP读取，读取成功。

```
~ > ifconfig en7
...
    inet 192.168.100.177 netmask 0xffffff00 broadcast 192.168.100.255
...

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.11,build0489,230314 (GA.M)"

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (11060652) 1 day, 6:43:26.52

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FG101FTK20007637"
```

注意事项

1. 以上情况中，FortiGate只存在一个管理员账户admin，所以当配置了管理员可信主机后，即使接口下开启了管理协议，可信主机外的IP也无法正常访问接口下的管理协议（除了PING）。

2. 但如果存在多个管理员账户，而其中有管理员配置了可信主机，但有管理员没有配置可信主机（如下图所示），且接口下开启了各种管理协议。那么对于像SNMP这种不需要FortiGate管理员认证的协议，则可以通过可信主机外的IP正常访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
~ > ifconfig en7
 ...
    inet 192.168.100.179 netmask 0xffffff00 broadcast 192.168.100.255
 ...

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.101.4.1.1.0
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.11,build0489,230314 (GA.M)"

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (11060652) 1 day, 6:43:26.52

~ > snmpwalk -v2c -c Fortinet123# 192.168.100.99 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FG101FTK20007637"
```

3. 对于HTTPS、SSH、Telnet这类需要认证FortiGate管理员账号的协议来说：
   - 当只有一个管理员并且配置了可信主机后，非可信主机访问HTTPS、SSH、Telnet服务会被直接拒绝（无法打开HTTPS登录页面和SSH/Telnet连接）。
   - 当像2中那样配置了多个管理员，有的管理员配置了可信主机，有的管理员没有配置可信主机，那么使用非可信主机访问HTTPS的登录页面是可以正常打开登录页面的，SSH/Telnet登录信息也是可以显示的，会在登陆时检查是否为对应管理员的可信主机。

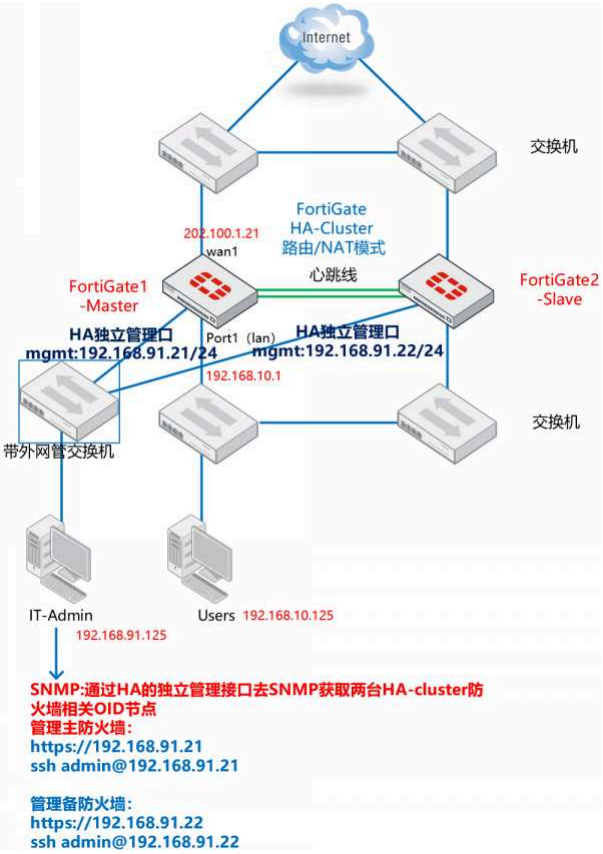
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SNMP的HA独立管理

需求

在HA环境下配置FortiGate的SNMP，并且通过HA成员的独立管理接口进行SNMP操作。

组网拓扑



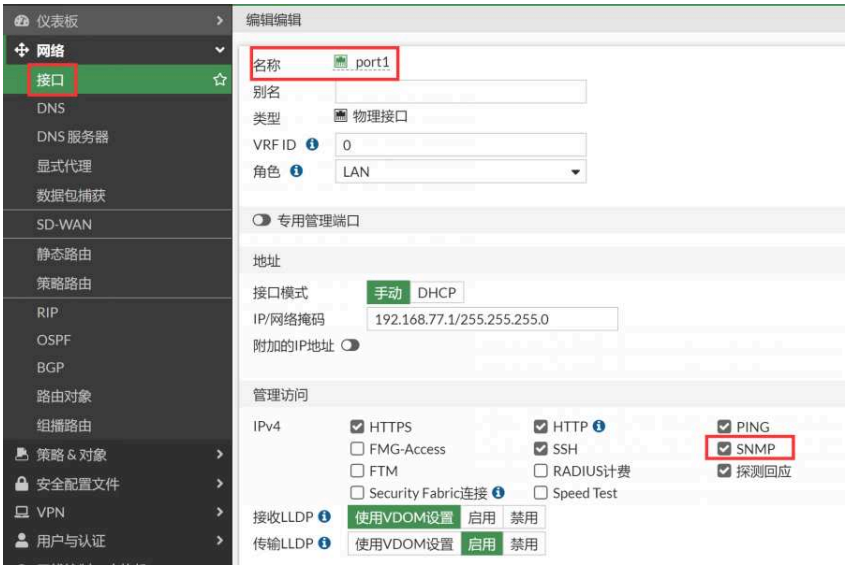
操作步骤

重要

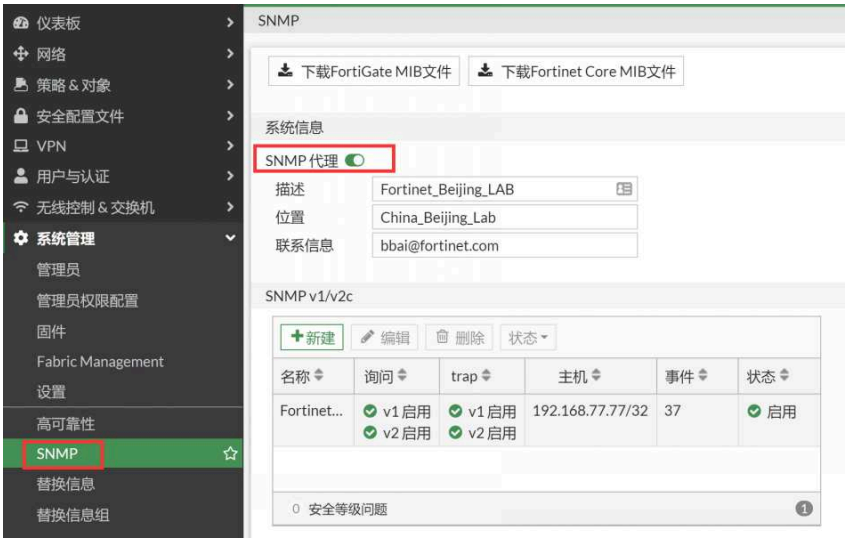
HA独立管理口的配置，请参考：HA双机热备→HA-Cluster的网管→HA集群带外独立管理-独立管理接口↗章节，使用的同样的一个拓扑图。本章节将关注点放置于如何配置和使用SNMP上。

1. 在HA独立管理接口上开启SNMP的允许访问（包括主防火墙的HA独立管理口port1和备防火墙的HA独立管理口port1）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

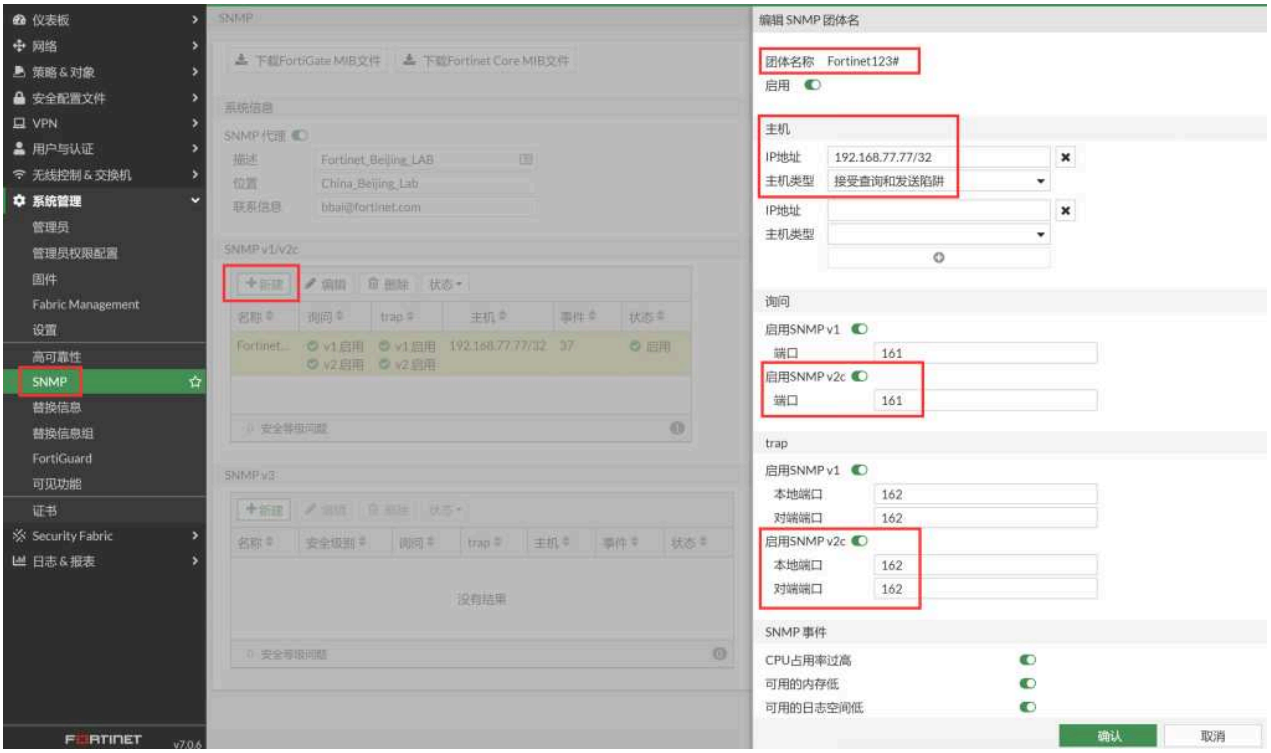


2. 开启SNMP的总开关。

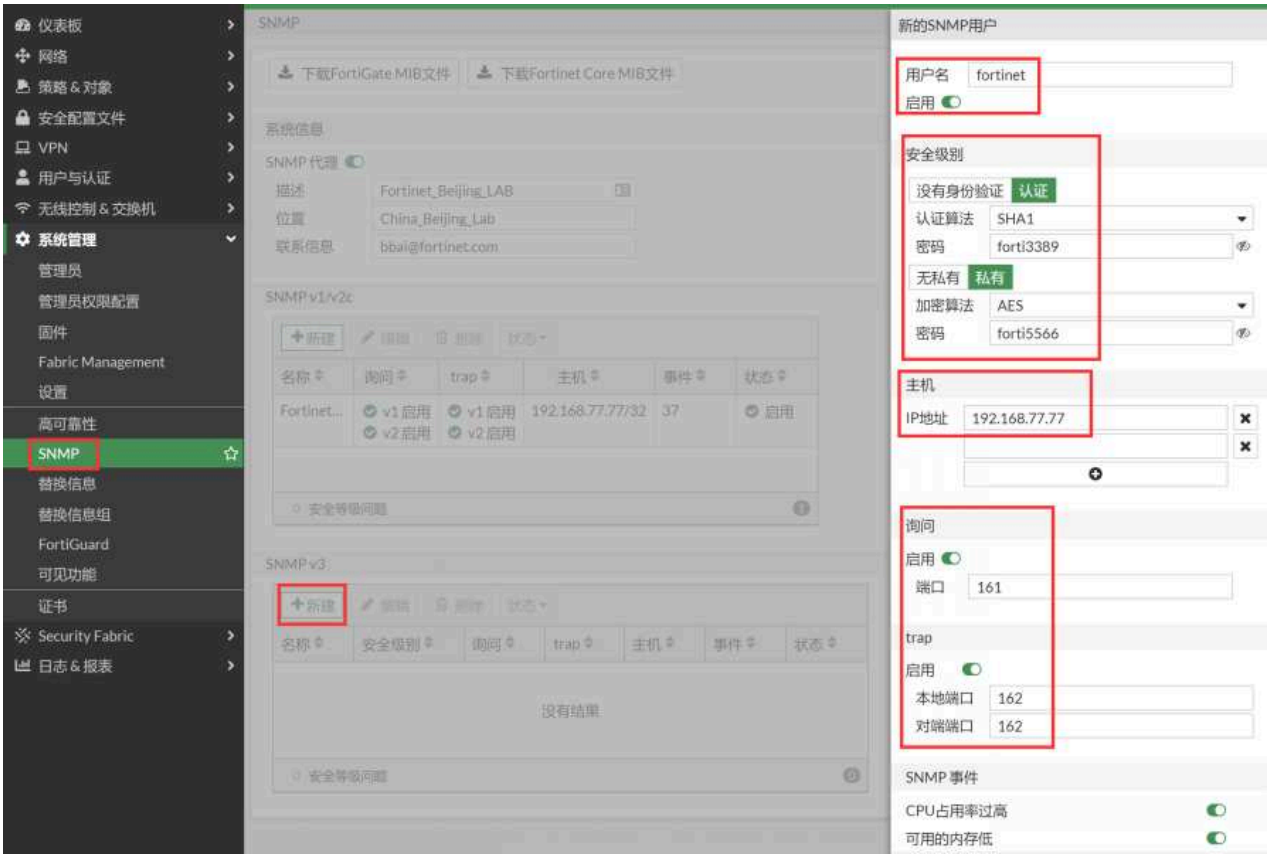


3. 配置SNMP v2的属性，比如配置SNMPv2的SNMP属性为Fortinet123#，建议不要使用通用的public，容易被探测和攻击。需要添加SNMP客户端的主机IP（192.168.77.77）的SNMP权限，把主机的IP地址（192.168.77.77）添加到SNMPv2的配置里面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

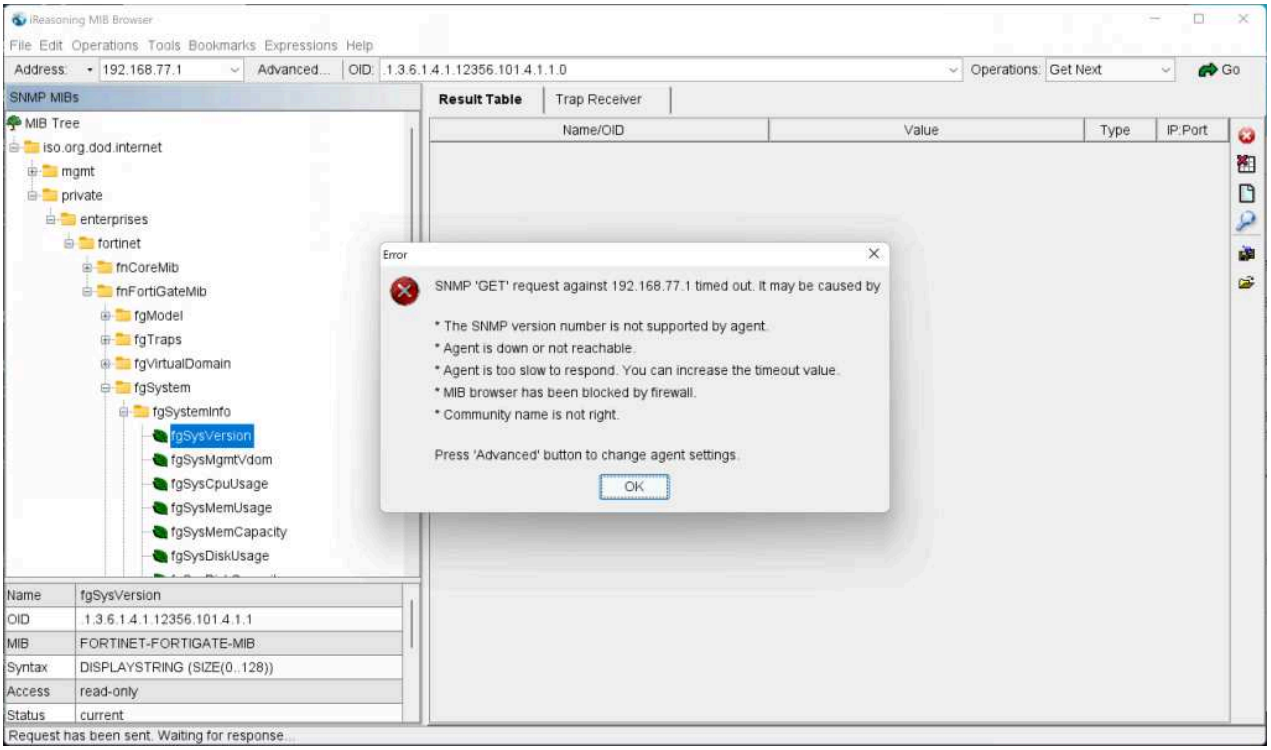


4. 配置SNMPv3，配置SNMPv3的用户名为fortinet，认证算法选择SHA1，密码为forti3389，加密算法选择为AES，密码为forti5566。需要添加SNMP客户端的主机IP（192.168.77.77）的SNMP权限，把主机的IP地址（192.168.77.77）添加到SNMPv2的配置里面。



5. 这个时候去测试SNMP会发现SNMP是无法成功获取到的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 在FortiGate上进行抓包，可以看到SNMP查询没有任何回应，debug flow显示SNMP请求在vd-vsys_hamgmt里面被丢弃的。

```
FGT1-MASTER # diagnose sniffer packet any "host 192.168.77.77 and port 161" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.77.77 and port 161]
7.576093 port1 in 192.168.77.77.53750 → 192.168.77.1.161: udp 53
7.576474 port1 in 192.168.77.77.53750 → 192.168.77.1.161: udp 53
15.795977 port1 in 192.168.77.77.53751 → 192.168.77.1.161: udp 53
15.796132 port1 in 192.168.77.77.53751 → 192.168.77.1.161: udp 53

FGT1-MASTER # diagnose debug flow filter port 161
FGT1-MASTER # diagnose debug flow filter addr 192.168.77.77
FGT1-MASTER # diagnose debug flow show function-name enable
show function name
FGT1-MASTER # diagnose debug flow trace start 10
FGT1-MASTER # diagnose debug enable
FGT1-MASTER # id=20085 trace_id=1 func=print_pkt_detail line=5863 msg="vd-vsys_hamgmt:0 received a
packet(proto=17, 192.168.77.77:53831→192.168.77.1:161) tun_id=0.0.0.0 from port1. "
id=20085 trace_id=1 func=init_ip_session_common line=6042 msg="allocate a new session-00014576, tun_id=0.0.0.0"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2605 msg="find a route: flag=84000000 gw-192.168.77.1 via
vsys_hamgmt"
id=20085 trace_id=2 func=print_pkt_detail line=5863 msg="vd-vsys_hamgmt:0 received a packet(proto=17,
192.168.77.77:53831→192.168.77.1:161) tun_id=0.0.0.0 from port1. "
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5949 msg="Find an existing session, id-00014576, original
direction"
```

7. 查看SNMP的debug信息，显示无法在vsys_hamgmt VDOM下查找到对应的community。

```
FGT1-MASTER # diagnose debug application snmpd -1
Debug messages will be on for 28 minutes.
FGT1-MASTER # diagnose debug enable
FGT1-MASTER # snmpd: <msg> 53 bytes 192.168.77.77:34002 → 192.168.77.1/192.168.77.1:161 (itf 3.3)
snmpd: checking if community "Fortinet123#" is valid
snmpd: updating cache: vdom_idx_map_cache
snmpd: updating vdom idx mapping
snmpd: Creating vdom_idx_cache for root
snmpd: Vdom created kernel-index=0, snmp-index=1, name=root
snmpd: cannot locate vdom with name vsys_hamgmt
snmpd: checking against community "Fortinet123#"
snmpd: request 2(vsys_hamgmt)/3/192.168.77.77 ≠ comm 1/0/192.168.77.77/255.255.255.255
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
snmpd: host or intf mismatch
snmpd: checking against community "FortiManager"
snmpd: full name mismatch
snmpd: failed to match community "Fortinet123#"
snmpd: </msg> 0
```

重要

SNMP获取失败的原因是什么呢?

原因就是因为存在HA独立管理口，HA独立管理口其实认为是一个独立的VDOM，vsys_hamgmt，默认的SNMP处理是root这个VDOM进行处理的，而不是vsys_hamgmt，因此SNMP请求HA的独立管理口是不行的。

这个时候如果是请求的是root vdom里面的业务接口，非HA独立管理口的话，就没啥问题的，此问题仅仅出现在请求HA独立管理口的SNMP的情况下。

因此为了满足这种场景下的SNMP使用需求，在SNMP的配置下有一个命令来适配HA独立管理口的使用，具体可以参考Fortinet Community文档的说明：

https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-SNMP-polling-via-the-dedicated-HA/ta-p/196034 ↗

https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-SNMP-Community-over-Cluster/ta-p/192507 ↗

8. **关键的一步，配置snmp主机的ha-direct enable**，这样SNMP才可以通过HA独立管理口获取到数据（只支持命令行配置）。以下分别是SNMPv2和SNMPv3下的配置方法。（如果只是需要SNMP相关流量从每台HA成员的独立管理口收发，则不需要在config system ha下开启ha-direct）

```
config system snmp community
    edit 1
        set name "Fortinet123#"
        config hosts
            edit 1
                set ip 192.168.77.77 255.255.255.255
                set ha-direct enable
            next
    next
end
```

```
config system snmp user
    edit "fortinet"
        set notify-hosts 192.168.77.77
        set ha-direct enable
    next
end
```

重要

开启SNMP配置下的“HA-direct”后，主机和备机的SNMP Trap报文也会通过各自的独立管理口分别发出，而不是通过主机的业务口发出。

结果验证

1. Net-SNMP SNMPv2结果验证。

```
[Tue Aug 11 15:28:55 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 .1.3.6.1.4.1.12356.101.4.1.1.0  // 主防火墙结果验证
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.6,build0366,220606 (GA.F)"
[Tue Aug 11 15:28:57 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (94369138) 10 days, 22:08:11.38
[Tue Aug 11 15:29:02 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.1 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM08TM22000173"
[Tue Aug 11 15:29:15 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.2 .1.3.6.1.4.1.12356.101.4.1.1.0  // 备防火墙结果验证
SNMPv2-SMI::enterprises.12356.101.4.1.1.0 = STRING: "v7.0.6,build0366,220606 (GA.F)"
[Tue Aug 11 15:29:17 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.2 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (93667021) 10 days, 20:11:10.21
[Tue Aug 11 15:29:21 root@centos7~#snmpwalk -v2c -c Fortinet123# 192.168.77.2 .1.3.6.1.4.1.12356.100.1.1.1.0
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM08TM22000174"
```

2. Net-SNMP SNMP V3结果验证。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
[Thu Aug 06 12:01:01 root@centos7~# net-snmp-config --create-snmpv3-user -ro -a SHA -A forti3389 -x AES -X forti5566 fortinet
adding the following line to /var/lib/net-snmp/snmpd.conf:
   createUser fortinet SHA "forti3389" AES forti5566
adding the following line to /etc/snmp/snmpd.conf:
   rouser fortinet
[Thu Aug 06 12:01:10 root@centos7~#chkconfig snmpd on
Note: Forwarding request to 'systemctl enable snmpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/snmpd.service to
/usr/lib/systemd/system/snmpd.service.
[Thu Aug 06 12:01:30 root@centos7~#service snmpd start
Starting snmpd (via systemctl):                            [  OK  ]
[Tue Aug 11 15:37:22 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.77.1 .1.3.6.1.4.1.12356.100.1.1.1.0 // 主防火墙
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM08TM22000173"
[Tue Aug 11 15:37:23 root@centos7~#snmpwalk -v3 -u fortinet -l authPriv -a SHA -A forti3389 -x AES -X forti5566
192.168.77.2 .1.3.6.1.4.1.12356.100.1.1.1.0 // 备防火墙
SNMPv2-SMI::enterprises.12356.100.1.1.1.0 = STRING: "FGVM08TM22000174"
```

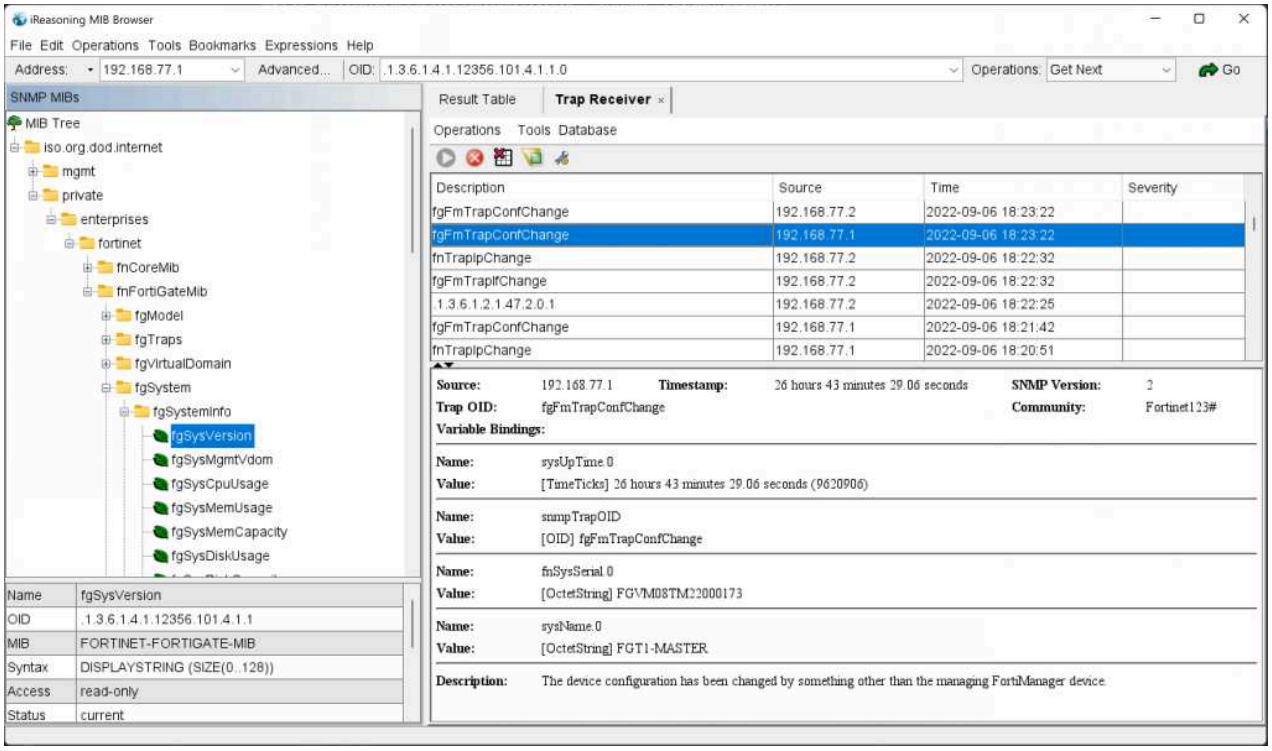
重要

Net-SNMP v3参考链接：https://www.thegeekdiary.com/centos-rhel-6-install-and-configure-snmpv3/

3. SNMPv2和SNMPv3的SNMP查询都正常，这个时候SNMP的查询就OK了，那么现在考虑另外一个问题，SNMP的Trap是否也OK呢？我们抓包看一下SNMP Trap的情况，可以看到SNMP Trap仍然可以通过HA独立管理口发送，并不需要在HA下开启ha-direct。

```bash
FGT2-SLAVE # diagnose sniffer packet any 'port 162' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 162]
15.428042 port1 out 192.168.77.2.162 → 192.168.77.77.162: udp 138
18.958515 port1 out 192.168.77.2.162 → 192.168.77.77.162: udp 253
133.104369 port1 out 192.168.77.2.162 → 192.168.77.77.162: udp 138
```

4. 查看IReasoning MIB Browser上的Trap Receiver，可以看到主机和备机分别发送的SNMP Trap。



监控BGP/OSPF的注意事项

1. 在SNMP启用ha-direct的情况下，查询BGP/OSPF相关OID时请使用“community-vdom”格式。例如，在root VDOM中SNMP配置的community为public，查询root VDOM的BGP/OSPF相关OID需要使用public-root来作为community（如果未开启VDOM功能，默认的VDOM就是root）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

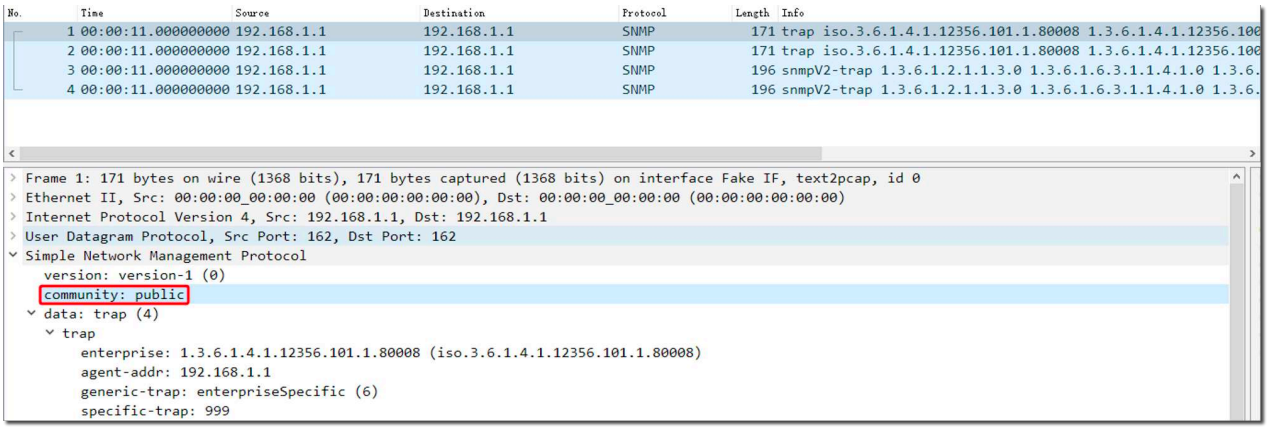
未启用SNMP的ha-direct，通过业务口查询BGP/OSPF相关OID，直接使用配置的community即可。

```bash
config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ha-direct enable
            next
        end
    next
end

root@centos7~# snmpwalk -v 2c -c public-root 192.168.88.87 .1.3.6.1.2.1.15.3.1.2
SNMPv2-SMI::mib-2.15.3.1.2.192.168.90.247 = INTEGER: 6
SNMPv2-SMI::mib-2.15.3.1.2.192.168.168.130 = INTEGER: 1
```

2. SNMPv3也要使用一样的格式，如下FortiGate配置的SNMPv3 community为user1，查询root VDOM的BGP/OSPF OID需要使用public-user1来作为community（如果未开启VDOM功能，默认的VDOM就是root）。

```bash
config system snmp user
    edit "public"
        set ha-direct enable
        set security-level auth-priv
        set auth-pwd fortinet
        set priv-pwd fortinet
    next
end

root@centos7~# snmpwalk -v3 -u public-root -l authPriv -a sha -A fortinet -x aes -X fortinet 192.168.88.87
.1.3.6.1.2.1.15.3.1.2
SNMPv2-SMI::mib-2.15.3.1.2.192.168.90.247 = INTEGER: 6
SNMPv2-SMI::mib-2.15.3.1.2.192.168.168.130 = INTEGER: 1
```

3. 针对SNMP Trap，在SNMP启用ha-direct的情况下，FortiGate主动发送的BGP/OSPF相关Trap报文中的community不会使用“community-vdom”格式，而是直接使用community，如下报文所示。



4. 这样SNMP分析软件（如Zabbix、SolarWinds等）使用“community-vdom”格式作为community时，会由于团体子不匹配而报错。

5. 解决方法是在FortiGate上配置两个Community，格式如下：

- 一个Community使用“community”格式（如public），host-type为query，用于OID的读取。
- 另一个Community使用“community-vdom”格式（如public-root），host-type为trap，用于发送BGP/OSPF相关Trap。
- SNMP分析软件配置的监控Community为“community-vdom”格式（如public-root）。

```bash
config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ip 192.168.1.1 255.255.255.255
                set host-type query
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            next
        end
    next
    edit 2
        set name "public-root"
        config hosts
            edit 1
                set ip 192.168.1.1 255.255.255.255
                set host-type trap
            next
        end
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGuard服务介绍

服务介绍

1. 设备服务是需要注册才会生效的（当然有特例，就是设备购买的前三个月，可以免费的试用所有的服务，而通常这些服务都是需要购买并且注册才生效的）。
2. 注册分为设备注册、服务注册（将服务绑定到固定的设备上，详细可见后续的设备注册、服务注册章节）。
3. 注册地址：https://support.fortinet.com ↗
4. 注册指南（点击查看） ↗。

服务分类

1. FortiCare支持服务
   - RMA硬件返修服务
   - 400电话/邮件等等技术支持服务
2. 固件和通用更新
   - 设备固件下载与更新服务
   - APP Control特征库更新
   - 设备识别库更新
   - Internet service DateBase库更新

   重要

   只需要有基础的FortiCare服务即可得到以上服务更新。
3. 入侵防御（IPS特征库更新）
   - IPS特征库
   - IPS引擎
   - 恶意URL
   - 僵尸网络IP库
   - 僵尸网络域名库
4. 反病毒（AV特征库更新）
   - AV特征库
   - AV引擎
   - 移动端恶意软件
5. Web过滤（URL分类过滤）
   - FortiGuard URL分类
   - 列入黑名单的网址数字证书
6. 工业安全数据库（Industrial DB）
7. FortiGate Cloud/FortiSandbox Cloud（有一定空间的免费许可）
8. Anti-Spam过滤

重要

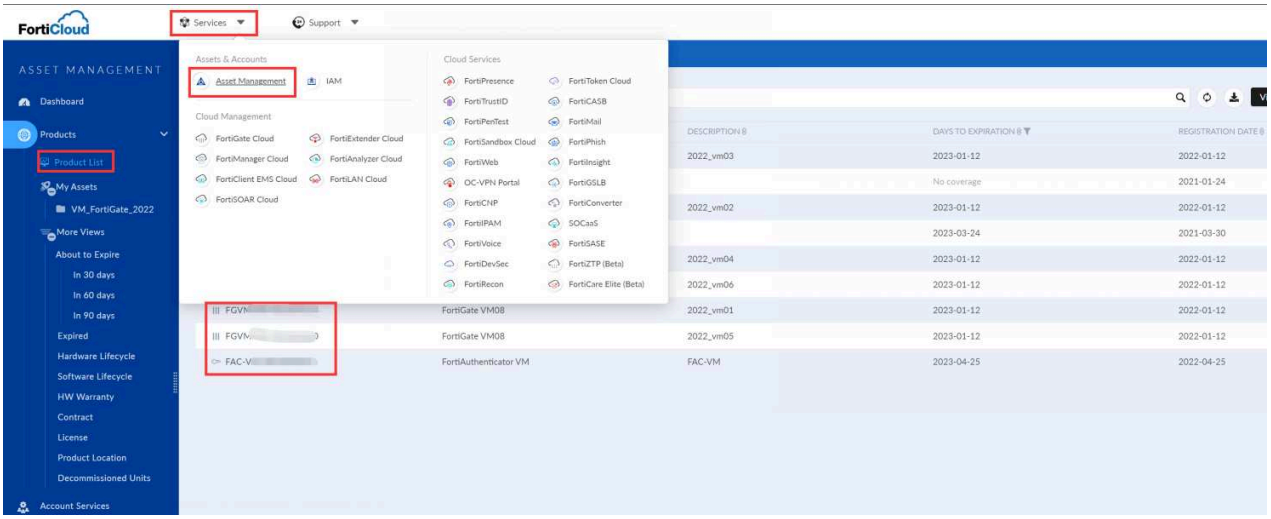
以上的NGFW类的特征服务，需要购买相应的license服务许可才可以正常的使用（设备开箱启动可以免费全功能使用3个月试用），具体的Bondle价格等等需要通过供应商处获取。关于特征库的更新和研究的网站：http://www.fortiguard.com/ ↗

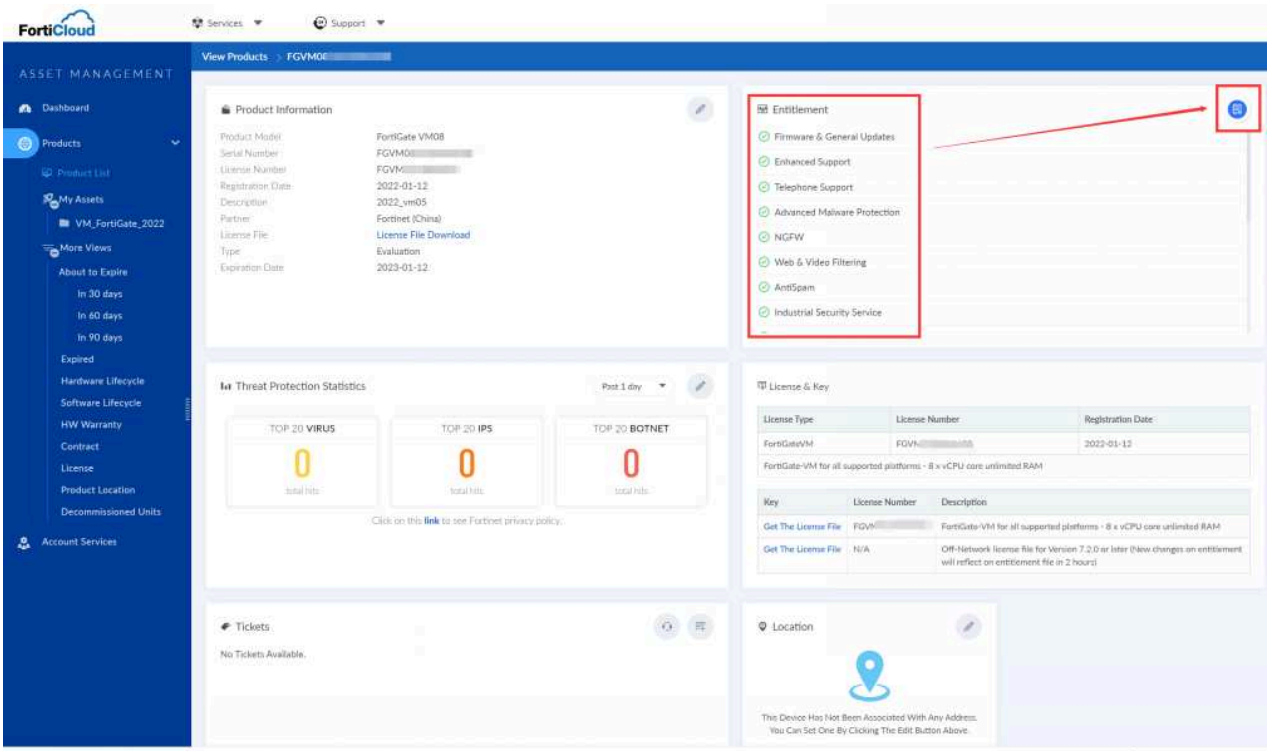
9. 虚拟域许可（默认有10个VDOM的license许可）
0. 其他许可，不同的软件版本，以上内容不尽相同，但是都大致有上述的模块和内容，具体不一样的版本可能存在一些差异，以上基于FortiOS 7.0.6进行的说明。

服务查看

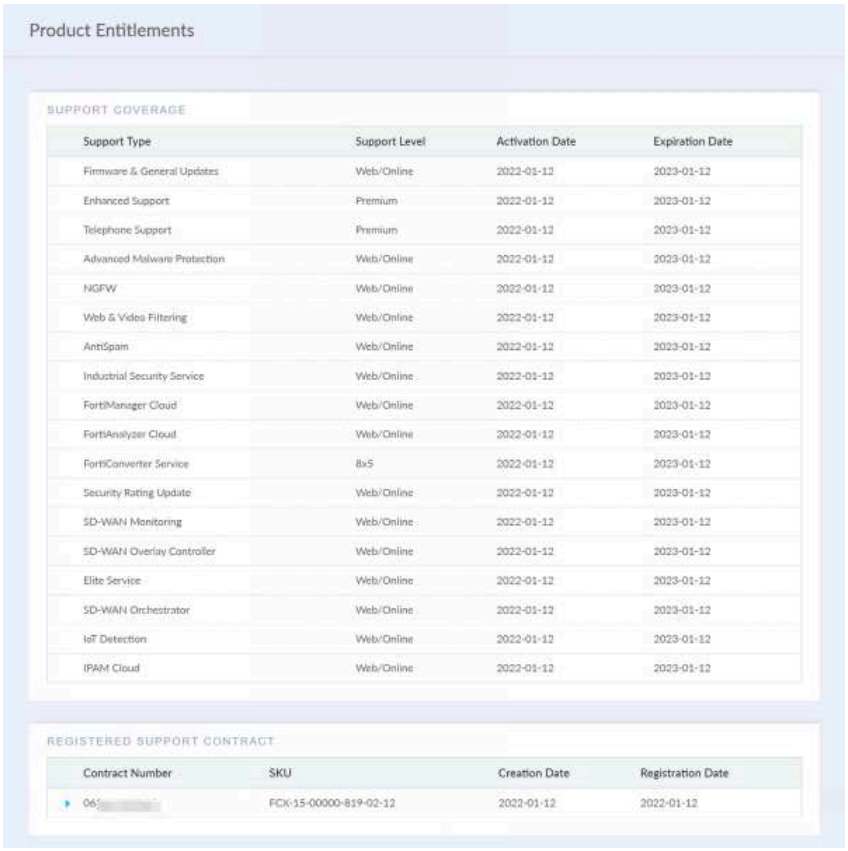
1. 通过Support网站登陆后查看：https://support.fortinet.com/asset/#/views/products ↗ 查看设备服务状态，注册设备之后才可以查看。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

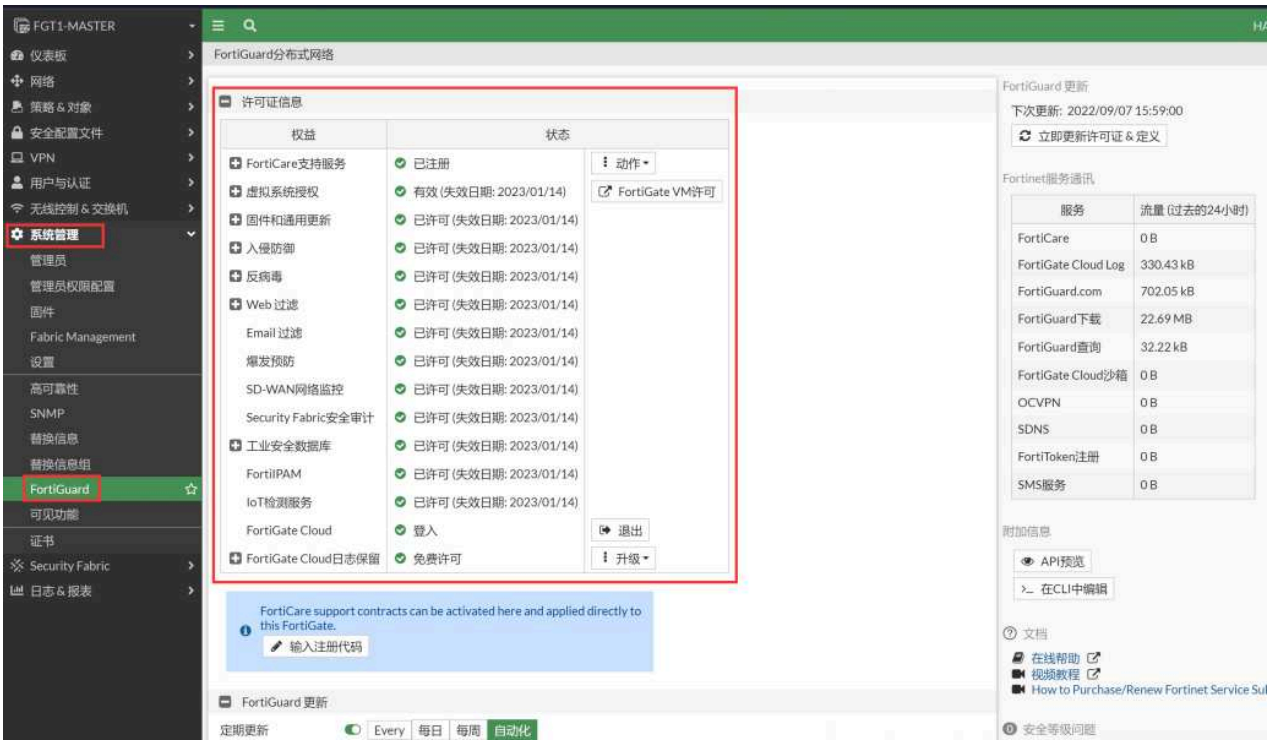




Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 通过FortiGate管理页面查看（FortiGate的服务是通过互联网进行更新，因此FortiGate需要可以连接到互联网，才可以正常的自动更新），正常情况下，网站的服务和设备上的服务将会是同步的状态。



常见问题

1. FortiGate设备服务无法正常更新。
   - FGT无法连接到互联网，包括FGT无法上网、DNS异常解析、运营商阻止了FortiGuard更新的目的端口，FGT的某些源端口工作异常。
   - 修改了FGT的DNS为内部DNS，不是FortiGuard默认的DNS，这样可能引起DNS解析FortiGuard的相关域名存在异常（服务器在国外）。
   - 服务没有在网站上注册，先到网站上确认设备服务状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 有HA的环境下，只会显示服务到期时间最近的那台设备的服务时间，如果其中有一台设备过期，那么HA中的其他设备均会显示过期。
- FortiGate默认为2小时更新一次，有时候不是立即就生效的，需要等一等，或者手工更新一下，手工命令如下：execute update-now。
- 拥有多个VDOM，而可以上互联网的不是管理VDOM（默认是管理VDOM是root），这样也会导致更新失败，修改管理VDOM为可以上网的VDOM，或者让root VDOM可以上互联网。

2. 排错思路和方法：
   - Troubleshooting Tip: Diagnosing FortiGuard problems of Antivirus, Intrusion Prevention, Web Filtering, Spam Filtering: https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-Diagnosing-FortiGuard-problems-of-Antivirus/ta-p/194121 ↗
   - Technical Tip: Verifying and troubleshooting FortiGuard updates status and versions: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verifying-and-troubleshooting-FortiGuard-updates/ta-p/194931 ↗
   - Technical Note: FortiGuard Support licenses show as expired: https://community.fortinet.com/t5/FortiGate/Technical-Note-FortiGuard-Support-licenses-show-as-expired/ta-p/194093 ↗
3. FGT无法连接互联网的情况下，如何更新特征库?
   - 手工导入特征库，GUI导入特征库或者命令行导入特征库，特征库可以在https://support.fortinet.com/Download/AvNidsDownload.aspx ↗ 下载离线版本特征库（需要登陆Support帐号）。
   - 统一通过FortiManger作为FortiGuard的中转站，需要FortiManger可以上互联网即可（可以使用代理方式），FortiGate无需上互联网，FGT将会通过FMG更新服务和特征库。
4. FortiGuard服务过期后会发生什么?
   - 基于特征库的服务到期，如AV、IPS、应用控制、IPS，相关特征库将无法继续更新，但可以继续使用旧的特征库。
   - 基于FortiGuard实时查询的服务到期，如WebFilter、DNS Filter，实时分类查询功能将无法使用，请注意可能导致开启WebFilter或DNS Filter的安全策略匹配的流量被阻断，但基于静态URL Filter的Web Filter可以继续使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiCare服务介绍

请参考FortiCare服务介绍 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

设备注册步骤

请参考设备注册指南↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

服务注册步骤

请参考服务注册指南↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

PRMA高级服务注册步骤

请参考PRMA高级服务注册指南 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

产品服务续费

请参考产品服务续费指南 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

RMA服务迁移

请参考以旧换新服务迁移步骤 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

RMA/DOA硬件保修政策

请参考RMA/DOA硬件保修政策 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

产品注册信息变更

1. 参考FortiCare创建Ticket步骤 ↗提交Ticket处理（响应较快）。

2. 联系400-600-5255提交变更请求。

3. 发送邮件至support_cn@fortinet.com提交变更请求。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

API文档获取

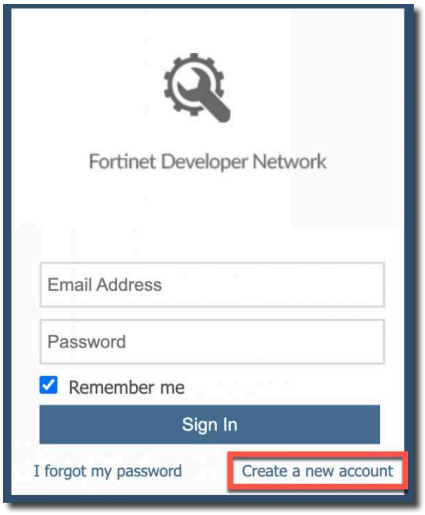
Fortinet Developer Network（FNDN）是一个基于订阅的社区，可帮助管理员提升和增强Fortinet产品的效能。您可以访问FNDN中的FortiAPI模块，以获取FortiOS各个版本的API列表与API Demo。

要访问FNDN，您需要先使用邮箱账户注册FNDN，所有FNDN用户必须由两名Fortinet员工进行担保。担保人必须能够确认用户的身份以及访问需求，创建新的FNDN账户需要提供两位担保人的电子邮件地址。

账号创建

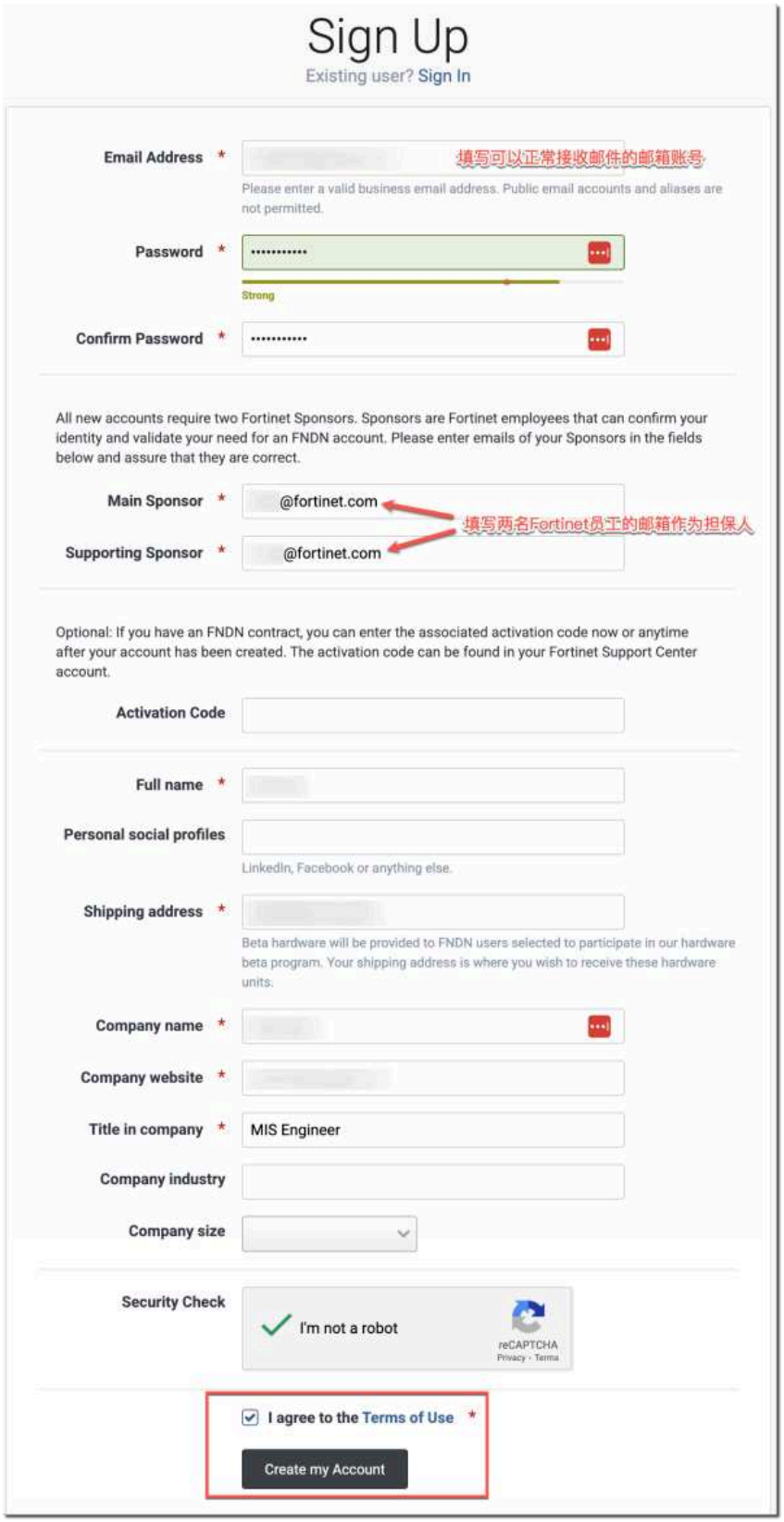
1. 首先需要获得两名Fortinet员工的担保，您可以向您的销售或售前人员咨询，并获得两名担保人的邮箱。

2. 访问FNDN网站，https://fndn.fortinet.net/ ↗ ，点击“Create a new account”。



3. 在注册页面填写必填项，填写两名Fortinet员工的邮箱作为担保人，同意使用条款并创建账户。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 随后在两位Fortinet担保人都批准申请后，若满足要求，FNDN管理员将审核该申请，并在大约一个工作日内批准账户访问权限，您将会在注册邮箱中收到审核结果的通知邮件。

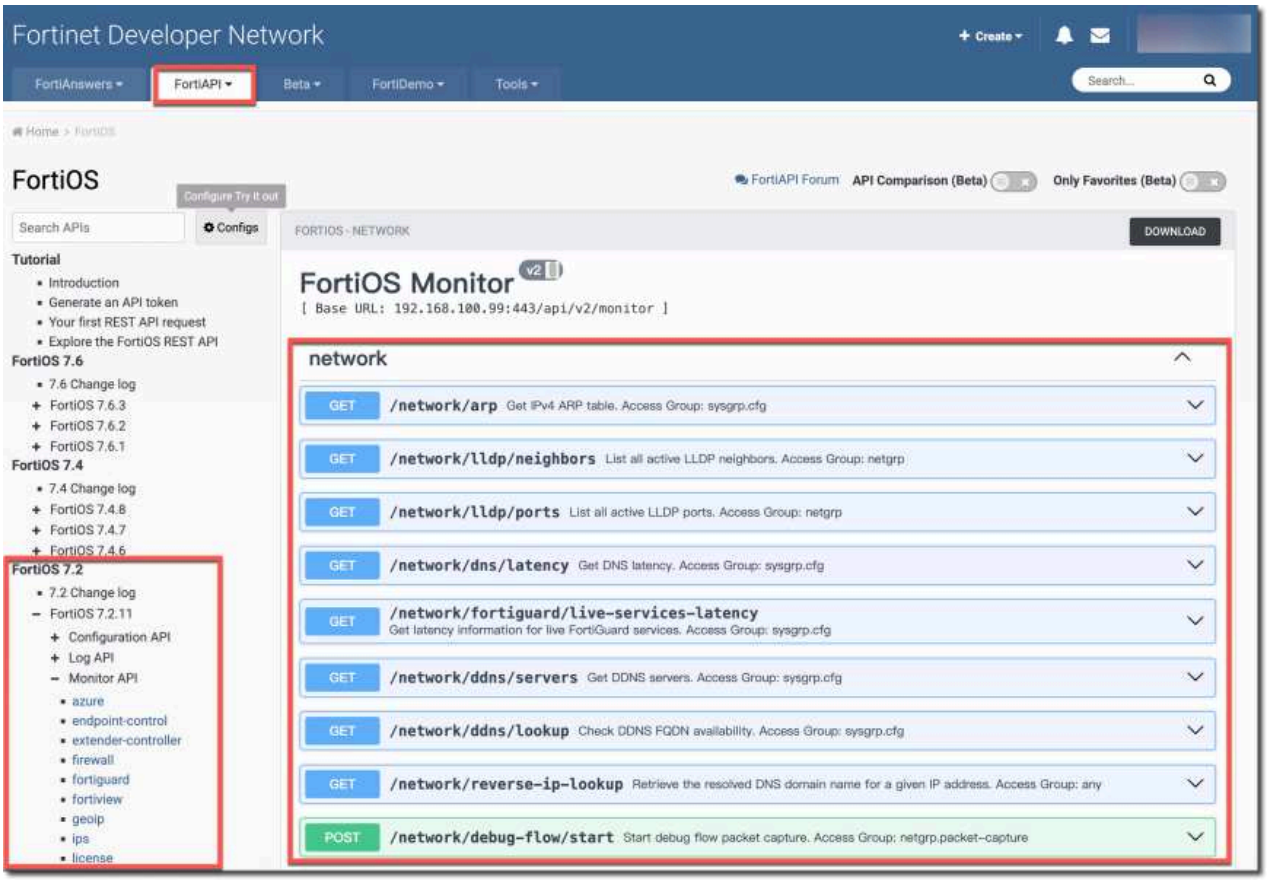
通过FNDN使用API

重要

FortiGate API用户的配置方法请参考：系统管理→管理员配置→API用户 ↗章节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

1. FNDN账号审核通过后，登录到https://fndn.fortinet.net/index.php?/fortiapi/1-fortios/ ↗ ，可以浏览对应FortiOS版本的API列表。

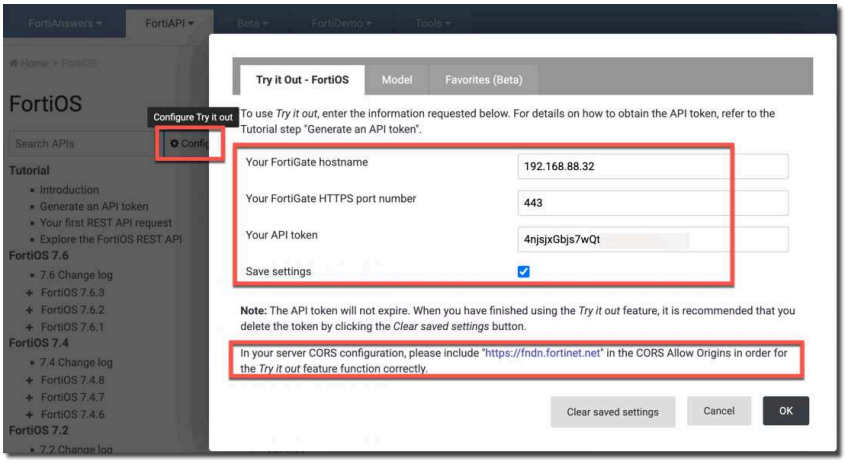


2. 点击左侧的“Config”按钮，填写本地FortiGate的API访问信息，可以在FNDN上通过本地网络访问目标设备的API。

重要

需要FortiGate的API用户允许 `https://fndn.fortinet.net` 的CORS访问：

```bash
config system api-user
    edit "api_user"
        set cors-allow-origin "https://fndn.fortinet.net"
    next
end
```

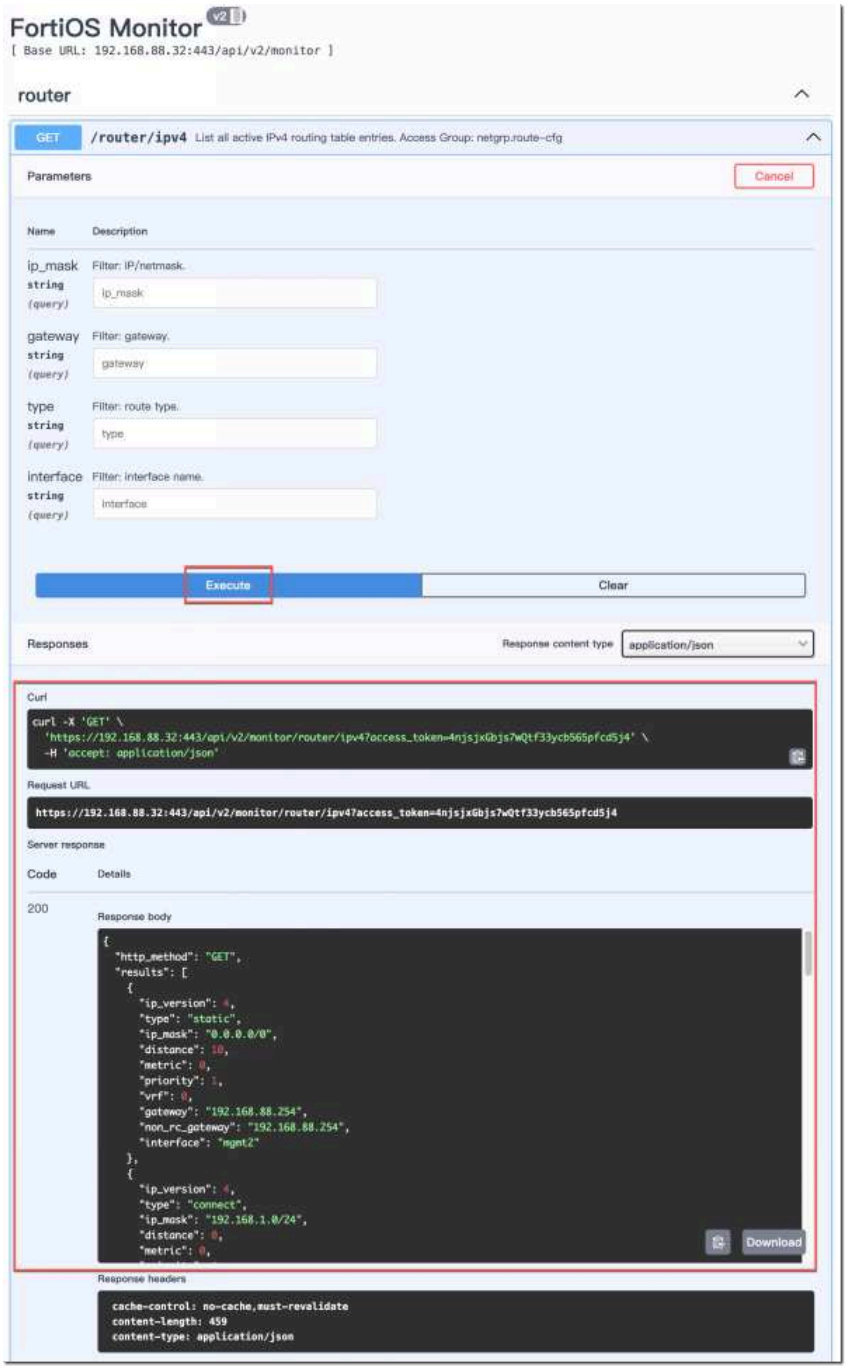


3. 例如需要通过API获取FortiGate当前的IPv4路由表，在该API条目中点击“Try it out”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 可以根据需要配置过滤器，点击“Execute”按钮执行API查询动作，可以看到FortiGate返回了当前的IPv4路由表信息。另外也可以看到API具体执行的Curl格式与请求的URL。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

远程技术支持

由于当今网络的复杂性，很多时候需要在客户和Fortinet TAC工程师之间安排远程会话，以便有效地解决技术问题。

在向Fortinet TAC请求远程会话之前，请您确保遵守以下要求：

- 提供问题相关的日志文件、设备运行状态输出（如`exe tac report`）、FortiGate配置文件、网络拓扑、问题的详细描述以及问题的出现条件。
- 尝试在已有的FortiGate文档的帮助下独立解决该问题，并向TAC工程师详细描述解决该问题已经做过的尝试。
- 已考虑TAC工程师提出的建议，其中包括Workaround或版本升级，以缓解当前问题。
- **Fortinet TAC支持的重点是故障排查，而不是配置协助。如果需要配置协助，请您先参考已有的FortiGate配置文档或联系您的代理商进行配置。**

如果确认满足以上要求，请遵循以下步骤，以实现高效的远程会话：

- 在加入远程之前，准备好排查环境。包括打开问题防火墙页面、终端工具等，以减少客户和工程师的时间浪费。
- 准备在TAC工程师远程期间明确解释并重现问题。
- 除非必要，请勿与其他同事共享会议链接，以避免给各方带来不必要的干扰。

创建Ticket的步骤请参考Fortinet售后支持平台FortiCare系统 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

在线更新特征库

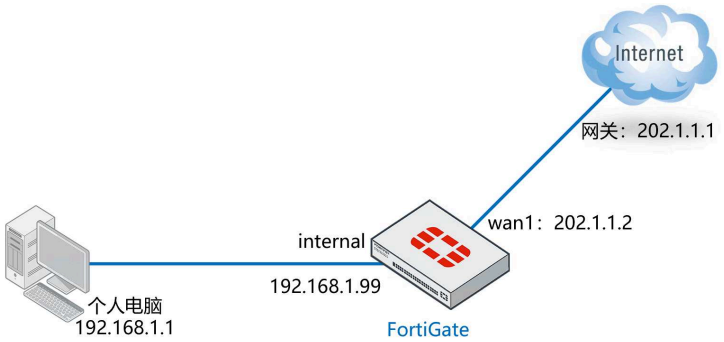
重要

- Web分类过滤、垃圾邮件库说明：Web分类过滤、垃圾邮件是存放在云端，其它库是下载在防火墙本地。
- 只有被防火墙策略引用的UTM功能的特征库才会自动更新，没有被引用的UTM功能特征库（或策略引用了UTM功能，但处于disable状态），不会自动更新（版本号会一直保持在旧版本或0.000）。
- IoT与OT特征库存在于在应用控制特征库中，需要防火墙策略引用应用控制配置文件后才会更新。
- ISDB以及地理位置等非UTM特征库默认就会自动更新。

需求

防火墙需要每隔两个小时就升级更新病毒库、应用特征库、入侵防御特征库。同时能够离线升级更新特征库。

组网拓扑



配置要点

1. 配置防火墙联通互联网。
2. 在线自动升级后有效的前提是已经购买过相关的授权许可，且已经注册服务，更新授权的操作方式请参考系统管理→FortiGuard管理→注册指南→服务注册步骤 ↗ 章节。
3. 由于升级过程中，防火墙需要从外网下载升级包，会占用网络带宽，且会影响设备的数据转发，所以建议将自动升级时间设置在在上网低峰的时候。

重要

自动升级必须保证防火墙联网，且配置正确的DNS地址；可是使用FortiGuard服务器，也可以手动设定DNS服务器（尽量为国外的DNS地址）。

配置步骤

1. 配置防火墙联通互联网，需要配置好接口地址，路由及DNS，详细步骤请参考网络管理→路由模式→静态地址线路上网配置 ↗。
2. 定期及自动升级，进入系统管理→FortiGuard，勾选“定期更新”，并设置每天凌晨3点更新。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

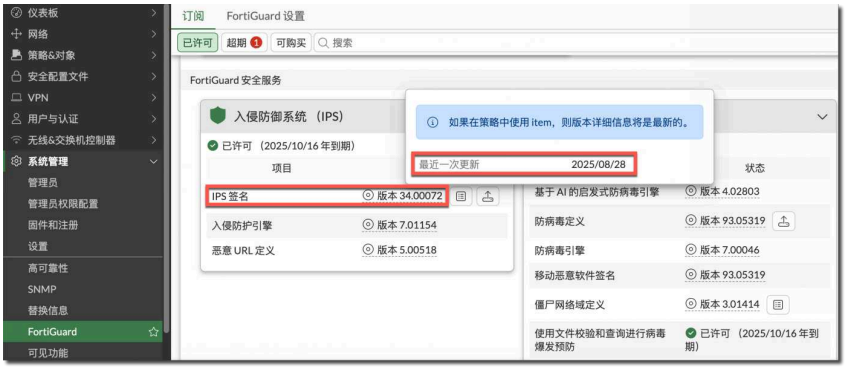



```bash
config system autoupdate schedule
    set frequency daily
    set time 03:60
end
```

重要

推荐将自动更新的周期设置为1天或1天以上，以节省性能消耗。

3. 确认自动升级成功，进入系统管理→FortiGuard确认所有的特征库均已升级成功，确认更新日期。



4. 也可以点击系统管理→FortiGuard页面右上方的更新按钮进行手动更新（或在CLI下执行`execute update-now`）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

离线手工更新特征库

需求

防火墙无法联网或授权过期的情况下，技术支持 中心可以临时提供入侵（IPS）、应用（APP）和病毒（AV）的离线特征库进行手工升级。建议尽快购买授权，实现在线自动升级，确保库文件及时更新，提升安全性。

> **重要**
>
> Web Filter分类过滤/DNS Filter分类过滤/基于FortiGuard的DLP/视频分类过滤等基于FortiGuard分类的服务，需购买相关授权并连接FortiGuard实时查询（设备需要能够连接Internet）。

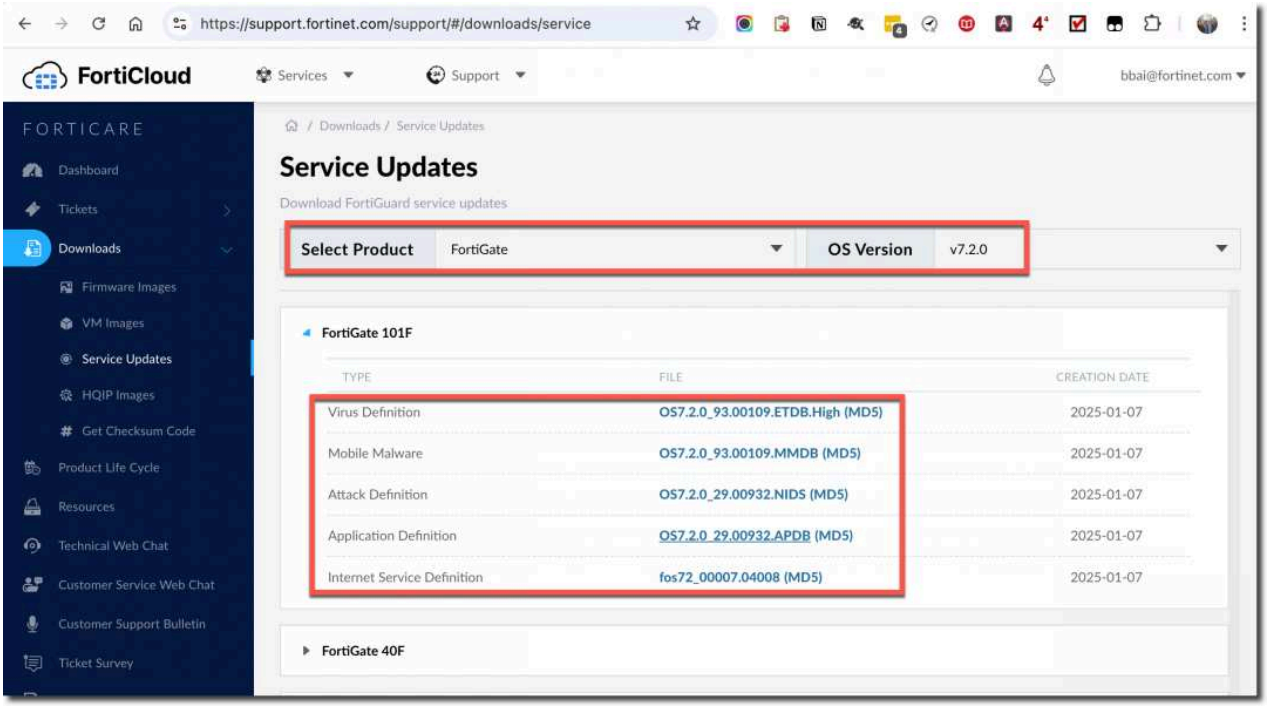
配置要点

1. 获取离线特征库。
2. 手工更新。
3. 确认升级成功。

配置步骤

Web方式离线升级

1. 获取离线特征库，访问并登录https://support.fortinet.com/support/#/downloads/service ↗ 网站离线获取特征库文件。有服务的设备才有权限下载特征库。IPS和AV的引擎是不能从这里下载的，如果需要最新的引擎，需要从技术支持处获取。



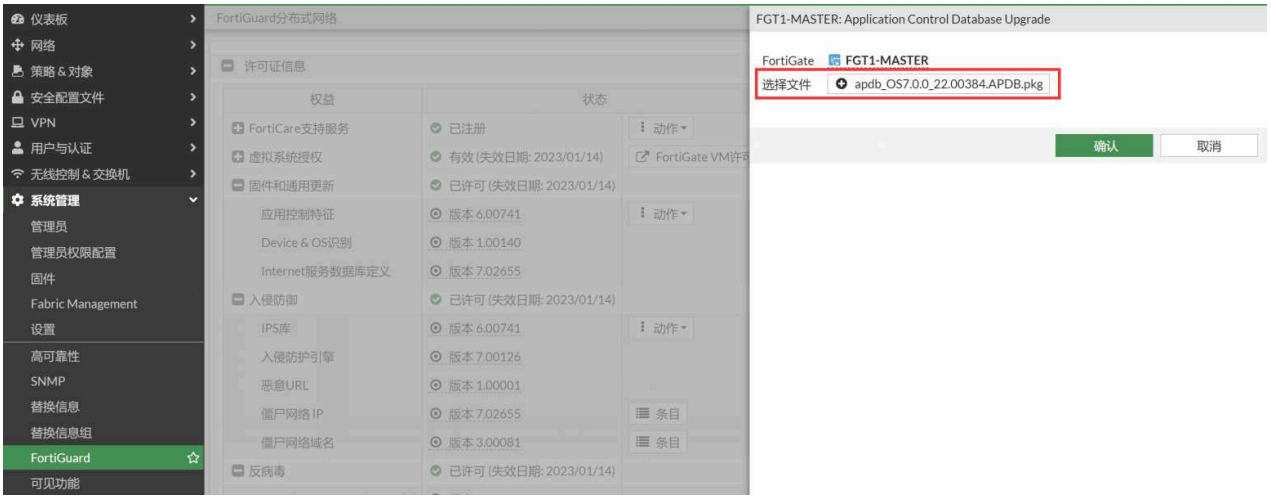
   - vsigupdate-OS7.0.0_90.05756.ETDB.High.pkg：AV特征库
   - nids_OS7.0.0_22.00386.NIDS.pkg：IPS特征库
   - apdb_OS7.0.0_22.00384.APDB.pkg：应用控制特征库
   - ffdb_fos70_00007.02656.pkg：ISDB特征库

2. 下载对应的特征库定义后，进入系统管理→FortiGuard，点击右侧的动作→升级数据库按钮，分别升级ISDB、应用控制、病毒特征库、IPS特征库。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 点击相应特征库后面的升级数据库，点击“上传”选择本地的离线特征库文件，确定即可。



4. 分别导入到防火墙里升级完后，不需要重启防火墙，升级完毕之后页面会提示升级成功。不会更新特征库和引擎都不会影响到业务的正常运行。

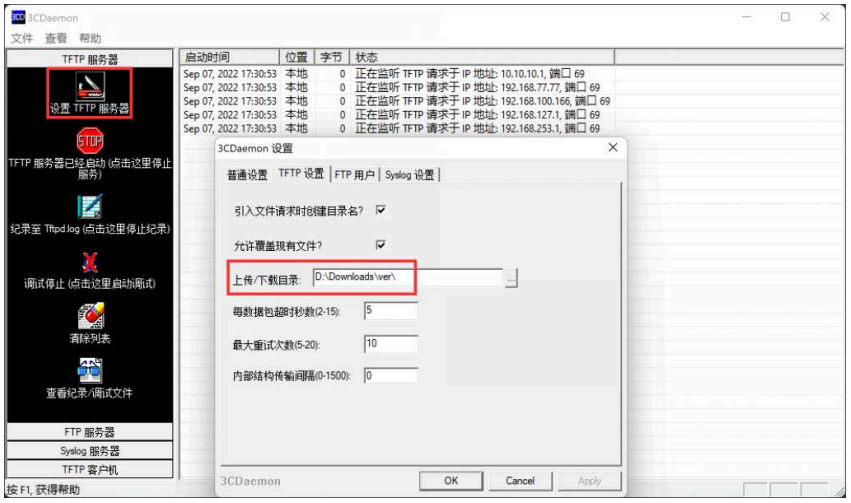


CLI方式TFTP/FTP升级

1. 也可以通过TFTP/FTP的方式进行升级，我们这里以TFTP升级IPS数据库为例。

2. 配置TFTP服务器，这里以3CDaemon为例，配置TFTP服务器的路径为特征库所在路径。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在FortiGate的CLI下执行更新IPS特征库命令。

```
FortiGate # exe restore ?
av                av
config            Restore config.
image             image
ips               ips
ipsuserdefsig     ipsuserdefsig
other-objects     other-objects
script            script
secondary-image   secondary-image

FortiGate #  execute restore ips tftp nids_OS7.0.0_22.00386.NIDS.pkg 192.168.100.166
This operation will overwrite the current IPS package!
Do you want to continue? (y/n)y
Please wait ...
Connect to tftp server 192.168.100.166 ...
##
Get IPS database from tftp server OK.
```

4. 提示更新成功后，使用diagnose autoupdate versions查看“Attack Definitions”的信息，显示上次更新为Manual模式，版本号与特征库文件一致。

```
# diagnose autoupdate versions
...
Attack Definitions
————————
Version: 22.00386
Contract Expiry Date: Sun Mar 26 2023
Last Updated using manual update on Wed Sep  7 17:56:43 2022
Last Update Attempt: Tue Aug 30 19:01:35 2022
...
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

离线导入设备License

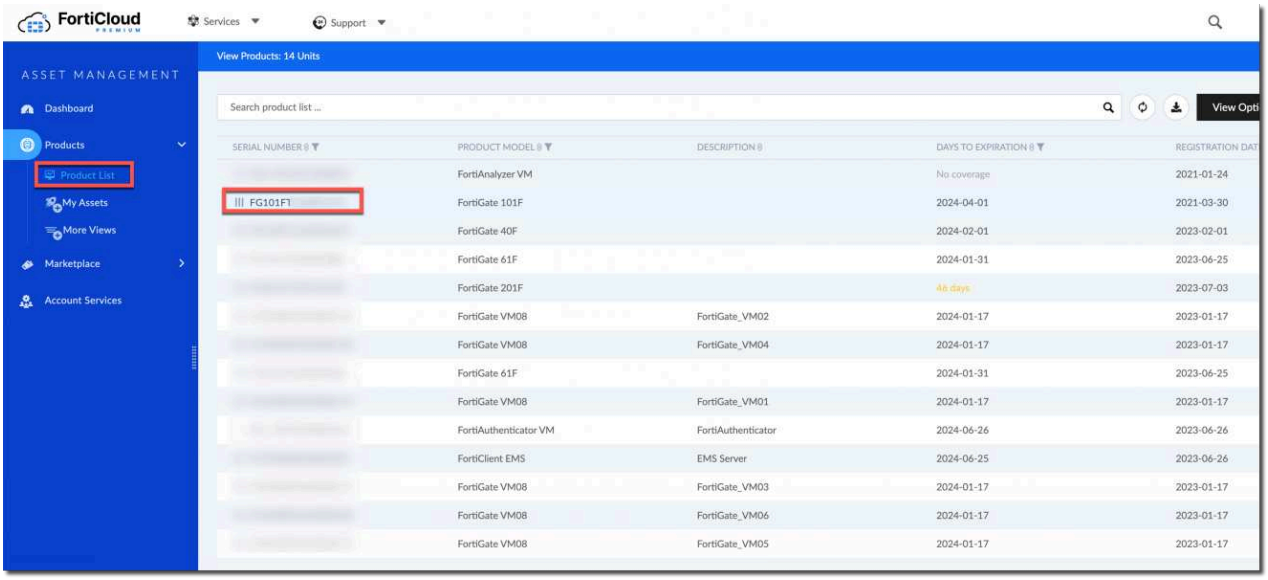
重要

该功能在FortiOS 7.2.0及以上版本上支持。

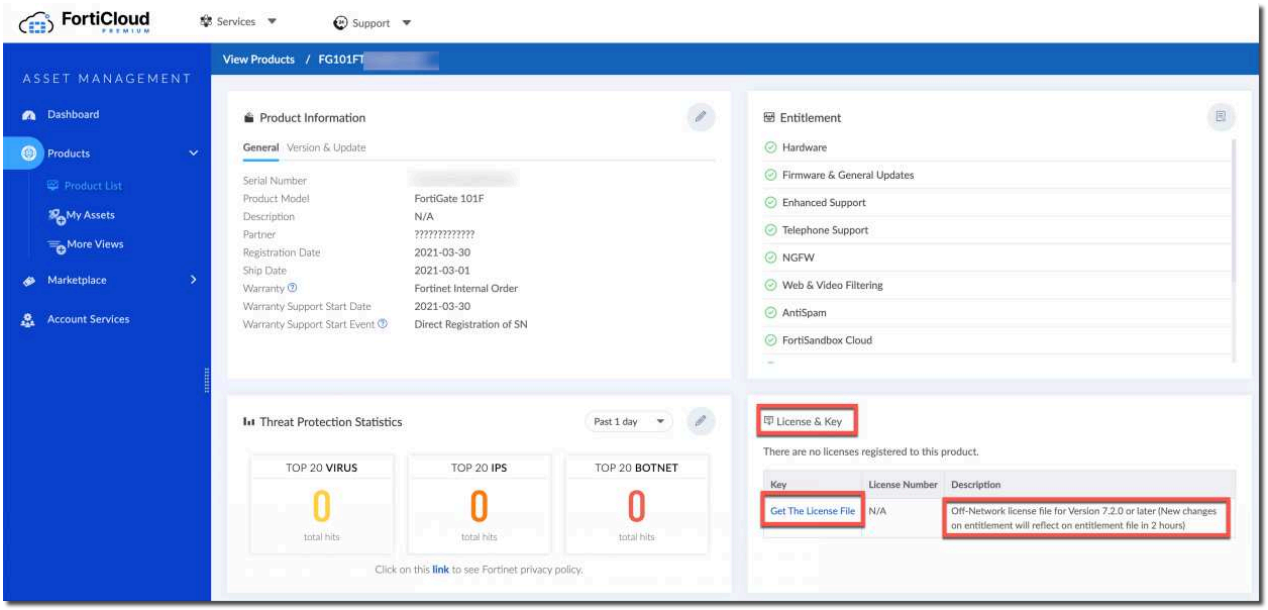
当由于安全性需要，用户的设备（硬件FortiGate或VM FortiGate）不能连接Internet，也没有FortiManager可以代理更新，无法通过FortiGuard/FortiManager同步服务License信息时，可以通过离线导入服务License的方式将License信息同步到FortiGate上。

导入过程

1. 设备与相关服务注册完成后，登录https://support.fortinet.com/ ↗ 网站（使用设备注册时的账户），进入Product List，点击要离线导入License的设备：



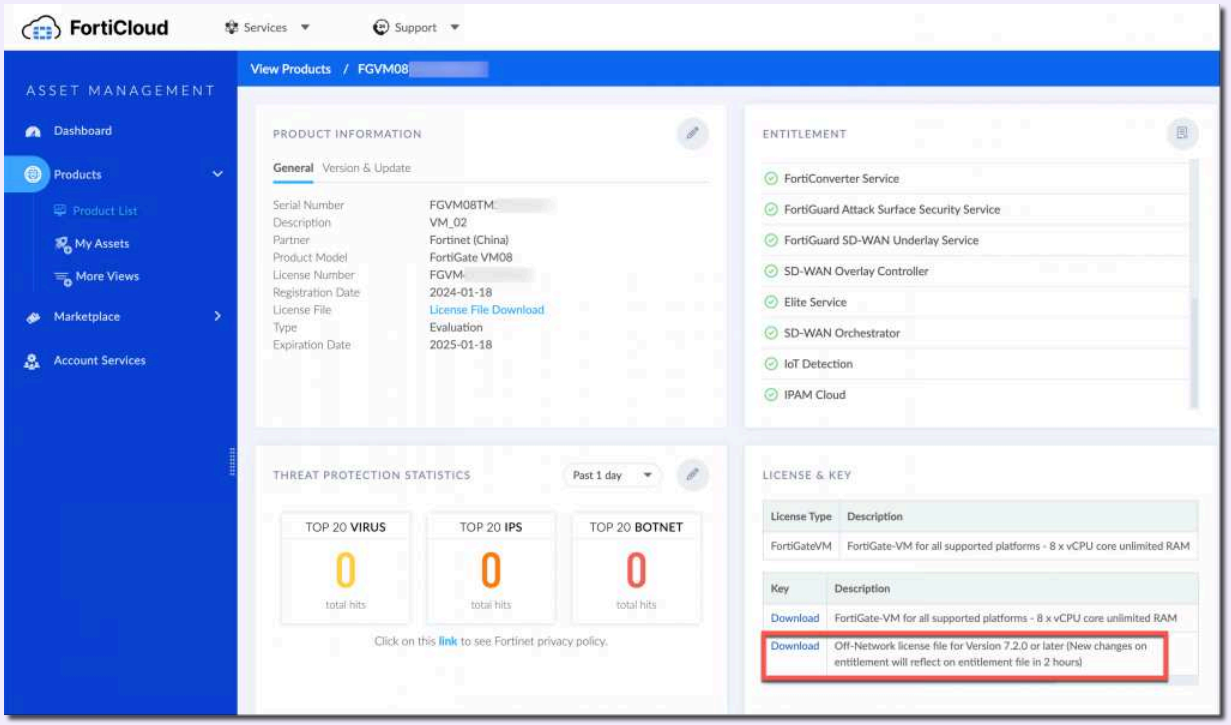
2. 在License & Key模块中，点击“Get the License File”按钮，下载设备的License文件（注意右侧的说明，已经注册的服务需要最多2小时才能更新到离线License文件中，该功能仅支持FortiOS 7.2及以上版本），下载的文件格式为FG101FTKxxxxxxxxOff-NetworkLicenseFile.lic：



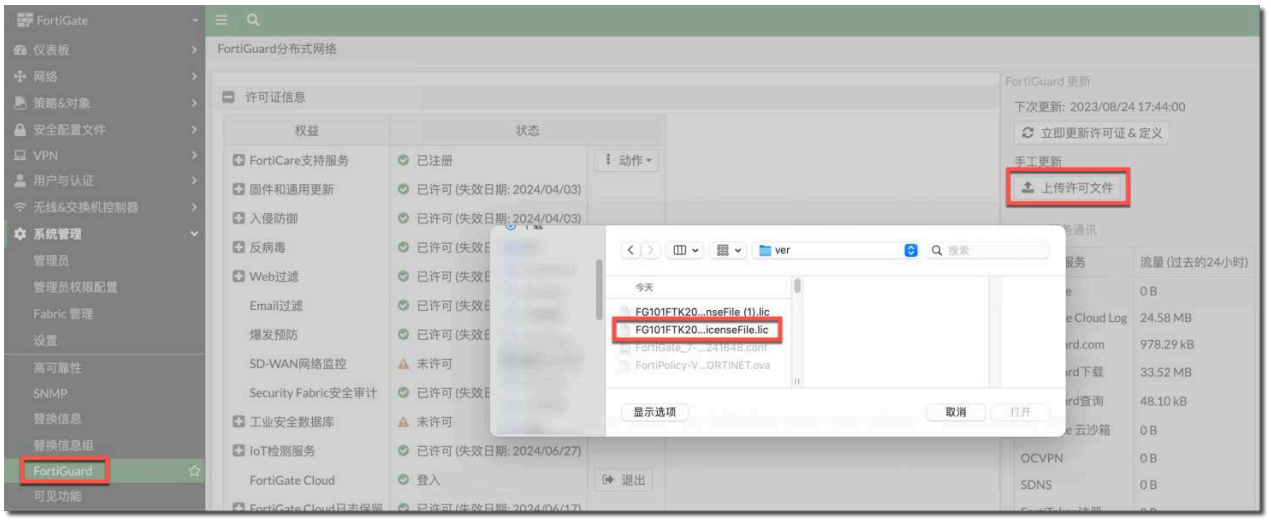
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

如果是VM FortiGate，请下载“Off-Network”类型的License（注意右侧的说明，已经注册的服务需要最多2小时才能更新到离线License文件中，该功能仅支持FortiOS 7.2及以上版本）。下载的文件格式为FGVMxxxxxxxxxxxxOff-NetworkLicenseFile.lic。



3. 登录设备的管理页面，进入系统管理→FortiGuard页面，在页面右侧点击“上传许可文件”按钮，选择要上传的离线License文件：



重要

VM FortiGate需要先通过Internet或FortiManager激活一次后，才能离线更新服务License，否则无法正常访问GUI页面。

4. 上传完成后，FortiGate即可离线更新到在Support网站已注册的服务内容。

5. 也可以通过CLI通过FTP/TFTP离线更新License文件。

```
FortiGate # execute restore manual-license {ftp | tftp} <license file name> <server> [args]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

禁用云通信

FortiGate 设备会与多个云端服务进行通信，例如 FortiGuard 下载与查询服务、FortiCloud 及其他云相关服务，用于下载服务包、执行实时安全过滤、日志上报及同步任务。

在某些安全或隔离网络（Air-Gap）环境下，管理员可能希望完全关闭这类外部通信。

云通信统计信息

GUI 查看

进入“系统管理 → FortiGuard → FortiGuard 设置”查看云通信统计计数。



CLI 查看

```bash
FortiGate # diagnose sys service-communication
FortiCare:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
FortiGuard Download:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
FortiGuard Query:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
FortiCloud Log:
The last 1 hour(in bytes):  35541766 1103963 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  36645729 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  36645729 0 0 0 0 0 0
FortiSandbox Cloud:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
FortiGuard.com:
The last 1 hour(in bytes):  4851531 101213748 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  106065279 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  106065279 0 0 0 0 0 0
SDNS Service:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiToken Registration:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
SMS Service:
The last 1 hour(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0
The last 24 hours(in bytes):  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
The last 7 days(in bytes):  0 0 0 0 0 0 0
```

禁用云通信

执行以下 CLI 命令即可关闭所有云通信，当 `cloud-communication` 被禁用后，系统会自动关闭 `forticldd` 和 `updated` 守护进程，并同步禁用多项与云服务相关的功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

提示

- 禁用云通信后，FortiGuard 实时威胁防护（例如 Web 过滤、反垃圾邮件、病毒库更新等）将不可用。
- FortiAnalyzer、FortiCloud 日志上传及 NTP 同步也会被同时关闭。
- 此操作建议仅用于离线或高安全隔离环境。

:::

```bash
config system global
    set cloud-communication disable
end
```

自动修改项

执行以上 CLI 命令禁用云通信后，以下配置会被系统自动更改：

```bash
config system global
    set fds-statistics disable
end

config system central-management
    set type none
    set include-default-servers disable
end

config system fortiguard
    set antispam-force-off enable
    set outbreak-prevention-force-off enable
    set webfilter-force-off enable
end

config system email-server
    set server ''
end

config system ntp
    set ntpsync disable
end

config system autoupdate schedule
    set status disable
end

config system autoupdate tunneling
    set status disable
end

config log fortiguard setting
    set status disable
end
```

重新启用云通信

1. 若需恢复云通信，请首先重新启用全局选项：

```bash
config system global
    set cloud-communication enable
end
```

2. 根据需要逐项恢复相应功能。
   - 重新启用 FortiCloud 自动登录：

```bash
config system fortiguard
    set auto-join-forticloud enable
end
```

   - 重新启用邮件服务器：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system email-server
    set server "fortinet-notifications.com"
    set port 465
    set security smtps
end
```

- 重新启用 NTP 同步：

```bash
config system ntp
    set ntpsync enable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

特征库误报/缺失上报

如果在使用IPS、AV、Application等特征库时，出现误报、缺少应用特征等问题时，您可自行联系FortiGuard团队进行相关信息的报告。

- 应用控制特征库缺失：https://www.fortiguard.com/faq/appctrlsubmit ↗
- 申诉应用控制特征库误报：https://www.fortiguard.com/faq/classificationdispute ↗
- 申诉被封的垃圾邮件IP、URL或电子邮件地址：https://www.fortiguard.com/faq/antispam/blocklist ↗
- 申诉网页过滤错误分类：https://www.fortiguard.com/faq/wfratingsubmit ↗
- 提交或申诉病毒文件：https://www.fortiguard.com/faq/antivirus-contact ↗
- 提交病毒文件并在线扫描：https://www.fortiguard.com/faq/onlinescanner ↗
- 报告IPS漏洞或IPS服务问题：https://www.fortiguard.com/faq/ips-contact ↗
- 报告终端系统漏洞问题：https://www.fortiguard.com/faq/ev-contact ↗
- 报告ISDB问题：https://www.fortiguard.com/faq/isdb-contact ↗
- 报告Fortinet产品漏洞：https://www.fortiguard.com/faq/psirt-contact ↗
- 报告IOC（Indicators of Compromise）分类问题：https://www.fortiguard.com/faq/ioc ↗
- 报告IP地理分类问题：https://www.fortiguard.com/faq/ipge ↗
- 报告恶意URL分类问题：https://www.fortiguard.com/faq/malurl ↗
- 报告安全URL分类问题：https://www.fortiguard.com/faq/wlurl ↗
- 报告IoT（Internet of Things）分类问题：https://www.fortiguard.com/faq/iotdispute ↗
- 报告FortiWeb应用程序分类问题：https://www.fortiguard.com/faq/contact-web-security ↗
- 报告SSL证书黑名单问题：https://www.fortiguard.com/faq/bad-cert ↗
- 报告应用控制功能问题：https://www.fortiguard.com/faq/appcontrol-contact ↗
- 报告网页过滤服务问题：https://www.fortiguard.com/faq/webfilter-contact ↗
- 报告反垃圾邮件服务问题：https://www.fortiguard.com/faq/antispam-contact ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiManger功能简介

FortiManger是FortiGate的统一网管系统

- 统一的集中管理防火墙的平台
- 最大限度的减少大型部署的初始成本和后续的运维成本
- 可以统一下发CLI脚本方便的保持所有FGT设备的合规性
- 可以作为本地的FortiGuard缓存服务器，FGT无需去互联网更新FortiGuard
- 自动化备份设备配置和策略模块维护
- SD-WAN集中管理
- VPN模块集中管理
- 日志收集和报告

什么时候应该在你的网络中使用FortiManager?

在大型企业和托管安全服务提供商（MSSP）中，网络规模带来了小型网络所没有的挑战，通过FortiManager集中管理可以帮助客户更轻松地管理多种设备的不同部署类型，并降低操作成本：

- 批量部署
- 计划配置更改及下发
- 对许多变化进行维护
- 跟踪和审计

FortiManager的主要功能是什么?

- 集中管理：您可以使用FortiManager从单个控制台管理所有FortiGate，而不是单独登录数百个FortiGate。
- 管理域（ADOM）：FortiManager可以将设备分为地理或功能ADOM，如果您拥有大型网络安全管理员团队，则更加适应ADOM。
- 配置修订控制：您的FortiManager保存所有配置更改的历史记录。您可以安排FortiManager部署新的配置或将受管设备恢复到之前的配置。
- 本地FortiGuard服务供应：为了减少网络延迟并尽量减少互联网带宽使用，您的受管设备可以使用FortiManager作为专用的FortiGuard分布式网络（FDN）服务器。
- 固件管理：FortiManager可以为受管设备安排固件升级。
- 脚本：FortiManager支持基于CLI和基于TCL语言的脚本。
- 记录和报告：托管设备可以在FortiManager上存储日志。从该日志数据中，您可以生成基于SQL的报告，因为FortiManager具有与FortiAnalyzer相同的日志记录和报告功能。

FortiManager能做什么?

- 在您的网络中配置防火墙策略
- 充当配置版本控制和安全审计的中央资料库（日志存档）
- 部署和管理复杂的网状和星型IPsec VPN
- 充当受管设备和FortiClient安装的专用FortiGuard分发服务器（FDS）
- 使用JSON API脚本和自动化设备配置，策略更改等
- SD-WAN集中管理中心

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiManger产品介绍

主要产品

硬件盒式设备
FMG 1000D
FMG 1000F
FMG 2000E
FMG 200F
FMG 200D
FMG 3000F
FMG 300D
FMG 300E
FMG 300F
FMG 3700F
FMG 3900E
FMG 4000D
FMG 4000E
FMG 400E

当然更多的我们会用的VM的方式部署FortiManger，包括公有云和私有云平台：

VM平台
Aliyun
AWS
Azure
Google GCP
Hyper-V
KVM
Oracle
VMware ESXi
Xen

重要

更多型号参考：https://www.fortinet.com/products/management/fortimanager#models-specs ↗

产品规格参考：https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortimanager.pdf ↗

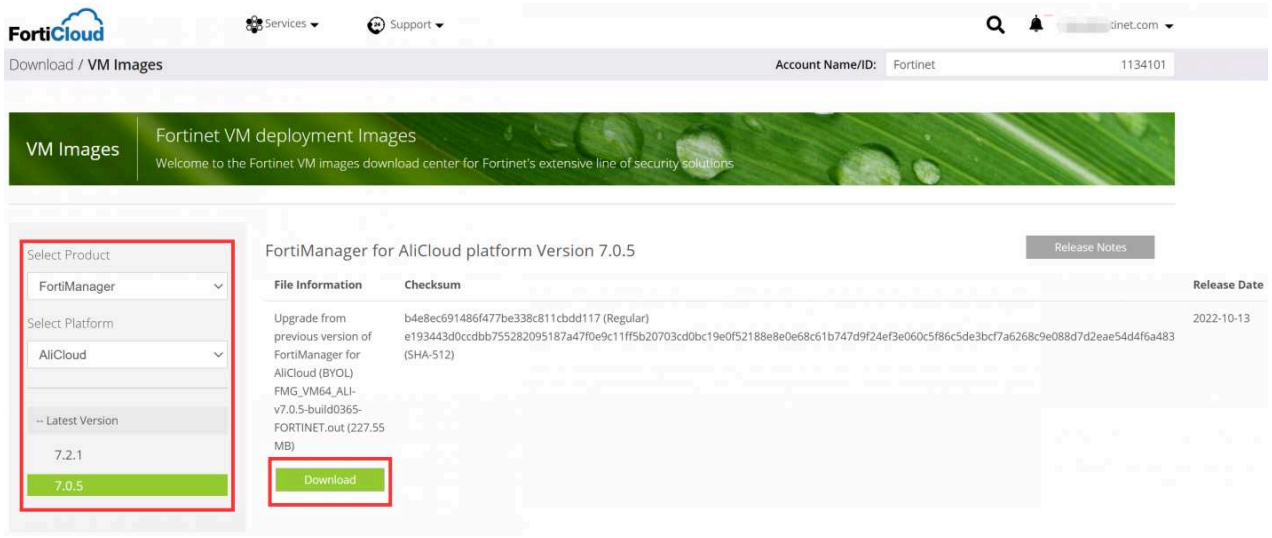
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VM安装手册

https://docs.fortinet.com/cloud-solutions

VM版本下载

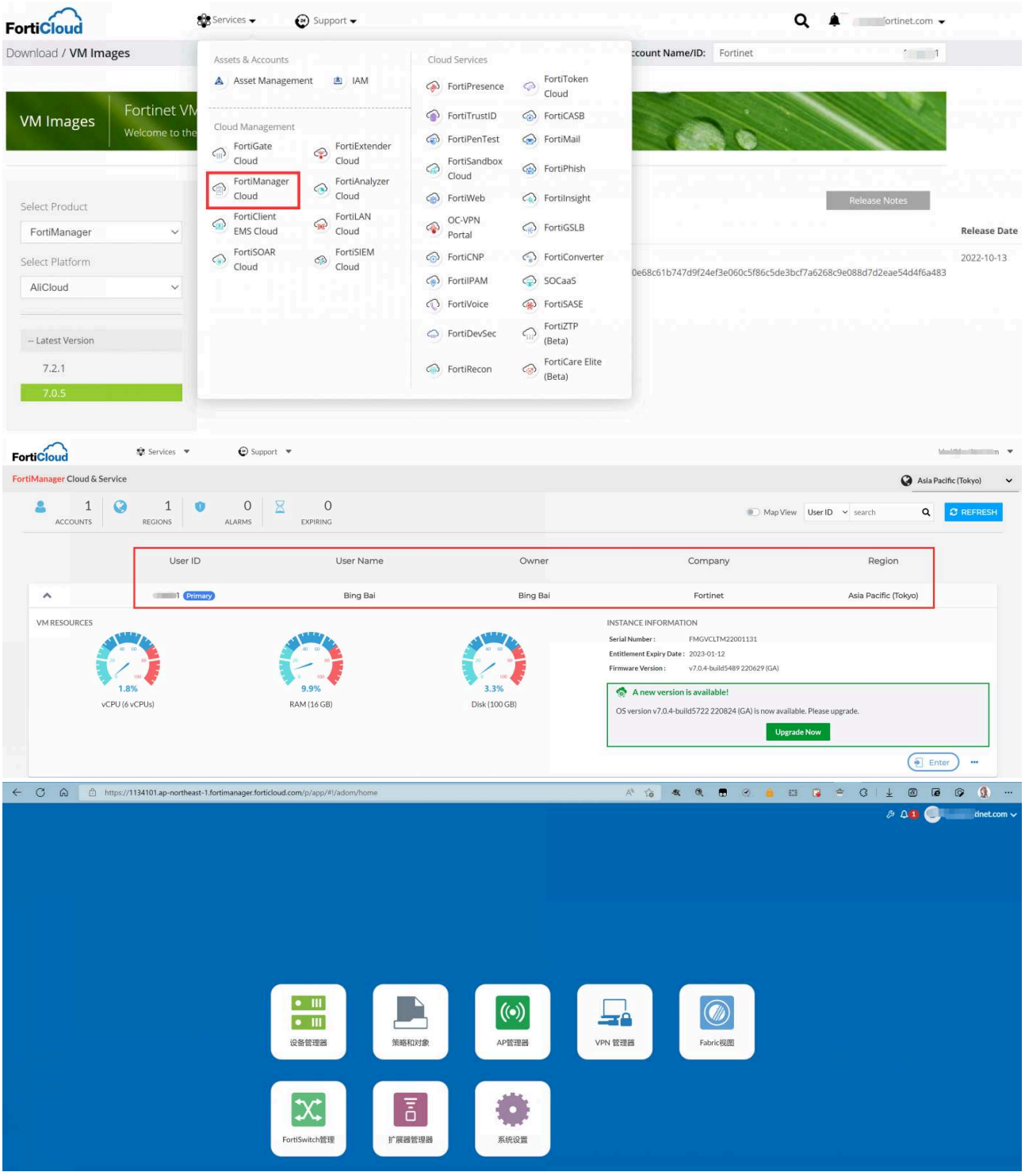
1. 进入https://support.fortinet.com/Download/VMImages.aspx 并登陆。
2. 选择产品为FortiManager，并选择想要下载的虚拟化平台和对应版本。



FortiManagerCloud

https://fortimanager.forticloud.com/ ，通过FortiCloud访问FortiManager，服务器不在国内，相对比较慢。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiManger版本推荐

重要

FortiGate版本与FortiManager、FortiAnalyzer产品版本的适应关系可通过如下网站查询：https://docs.fortinet.com/compatibility-tool/fortimanager ↗

固件命名规则

重要

FMG_*A*-*B*-*C*-FORTINET.out

如：*FMG_VM64-v7.0.12-build0623*-FORTINET.out

其中：

- *A*部分表示FortiManager型号，不同型号有不同的固件。
- *B*代表版本，有各个不同系列的版本，这里使用x.y.z（如7.0.12）来详细说明：
  - x.y表示大版本号，我们已经发布的大版本有v6.0、v6.2、v6.4、v7.0、v7.2和v7.4。
  - z表示大版本下持续发布的小版本，z越大，表示该版本越稳定。
- *C*表示内部代码编号。
- 正在运行的设备版本号，可以在CLI下使用get system status观察到，如下所示。

```bash
FortiManager # get sys status
Platform Type                    : FMG-VM64
Platform Full Name               : FortiManager-VM64
Version                          : v7.2.5-build1574 240313 (GA)
Serial Number                    : FMG-VMTM23011097
BIOS version                     : 04000002
Hostname                         : FMG-VM64
Max Number of Admin Domains      : 10000
Max Number of Device Groups      : 10000
Admin Domain Configuration       : Enabled
FIPS Mode                        : Disabled
HA Mode                          : Stand Alone
Branch Point                     : 1574
Release Version Information      : GA
Current Time                     : Wed Apr 24 17:19:20 HKT 2024
Daylight Time Saving             : Yes
Time Zone                        : (GMT+8:00) Beijing, ChongQing, HongKong, Urumqi.
x86-64 Applications              : Yes
Disk Usage                       : Free 476.43GB, Total 491.15GB
File System                      : Ext4
License Status                   : Valid
```

选择固件的原则

重要

B (x.y.z) 中的z越大越稳定可靠。

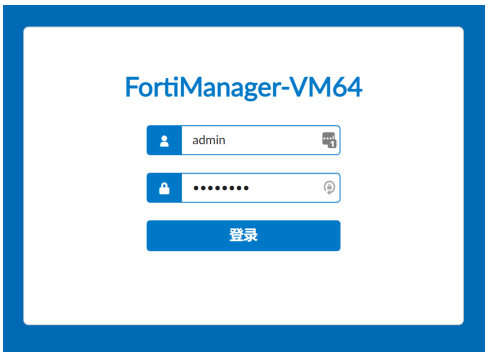
1. 首先确认被FortiManager管理的FortiGate的版本（FortiOS推荐版本请参考系统管理→固件与配置管理→固件版本管理→固件下载 ↗章节），FortiManager的版本可以向下兼容2个版本。例如FortiGate的版本为FortiOS 7.0.15，那么FortiManager的版本可以使用的版本为7.0、7.2或7.4。
2. 选定了大版本（x.y）后，小版本（z）尽量选择当前最新版本。例如选择了FortiManager 7.0版本，那么就使用该大版本（7.0）下的已发布的最新小版本（12，截止到2024年4月24日）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiManger网管登陆

默认的FortiManger和FortiGate的默认网管类似，默认情况下都可以通过GUI和CLI进行网管FortiManger。

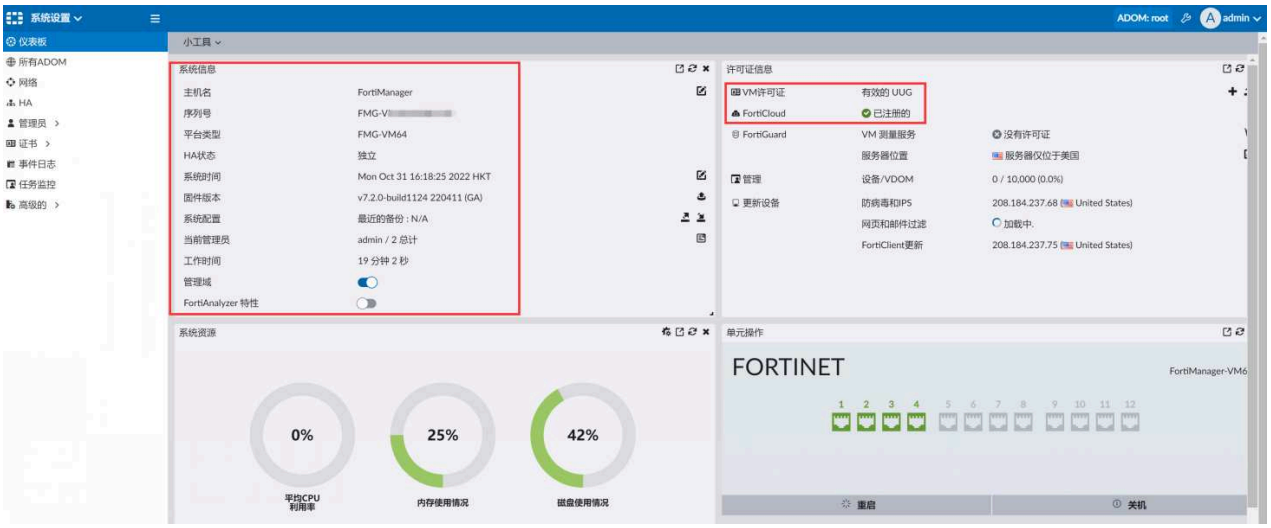
1. FortiManger的管理口（mgmt1或port1）IP地址默认为192.168.1.99，可以进入FortiManager管理页面或Console CLI下修改。



2. 登陆成功，可以看到管理界面。

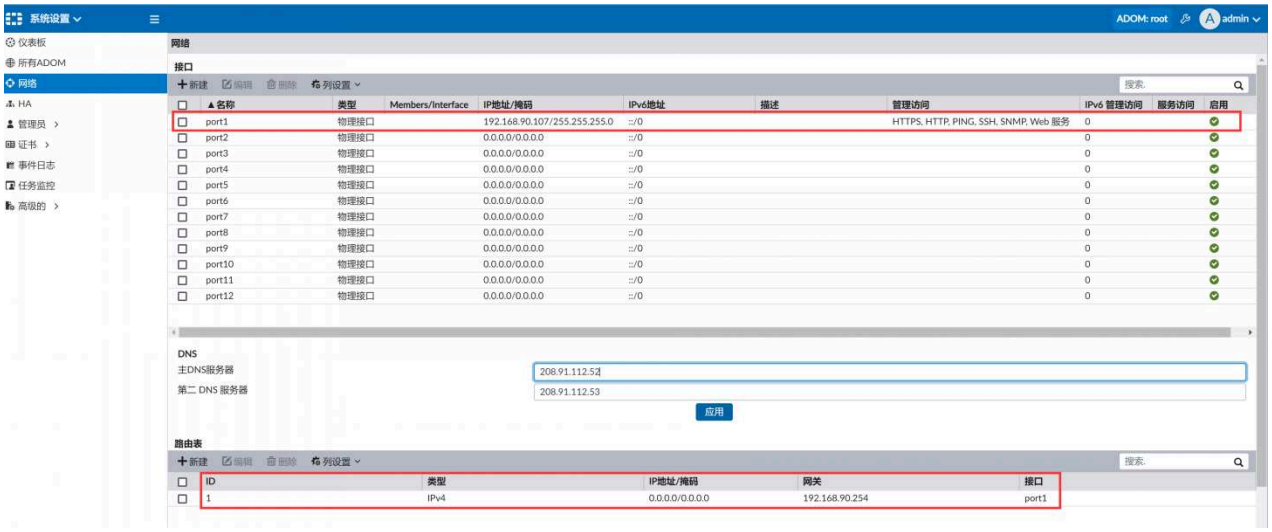


3. 进入系统设置视图，可以看到系统信息与License信息。



4. 在网络页面，可以配置设备接口的IP地址及路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ADOM简介

FortiManger的ADOM和FortiGate的VDOM类似，是一个独立的虚拟管理空间，多个ADOM之间彼此独立，一台FMG可以划分多个ADOM。

什么时候需要用到ADOM?

- 被管理的设备拥有不同的固件版本，如FortiOS 6.4/7.0/7.2，因为不同版本的有效命令行语法有一定区别，因此必须以版本进行区分ADOM，每一个版本平台拥有独立的空间。
- 管理员管理权限和区域划分，比如南区的管理员只能管理南区的设备，北区的管理员只能管理北区的设备，东区的管理员只能管理东区的设备，超级管理员可以管理所有的设备，那么这样的情况下就需要划分南区、北区、东区三个VDOM，分别指派给三个区域的管理员。
- MSSP业务情景，每一个租户拥有一个独立的ADOM，管理自己独立的设备。
- 拥有不同的设备类型，同时拥有多种设备类型，比如FortiGate, FortiMail, FortiWeb，那么则需要针对FortiMail和FortiWeb再分别创建两个VDOM。
- 业务规划或测试隔离，根据业务或者部门来划分ADOM，生产网络和测试网络等，拥有不同的ADOM，彼此隔离，互不影响。
- ADOM最大数目取决于设备型号，就和FortiGate类似的，如果开启VDOM功能的话，那么默认的那个防火墙就叫做root，FortiManger也是这样的，默认的那个FortiManger也叫做root。其他的ADOM自己手工命名并创建。

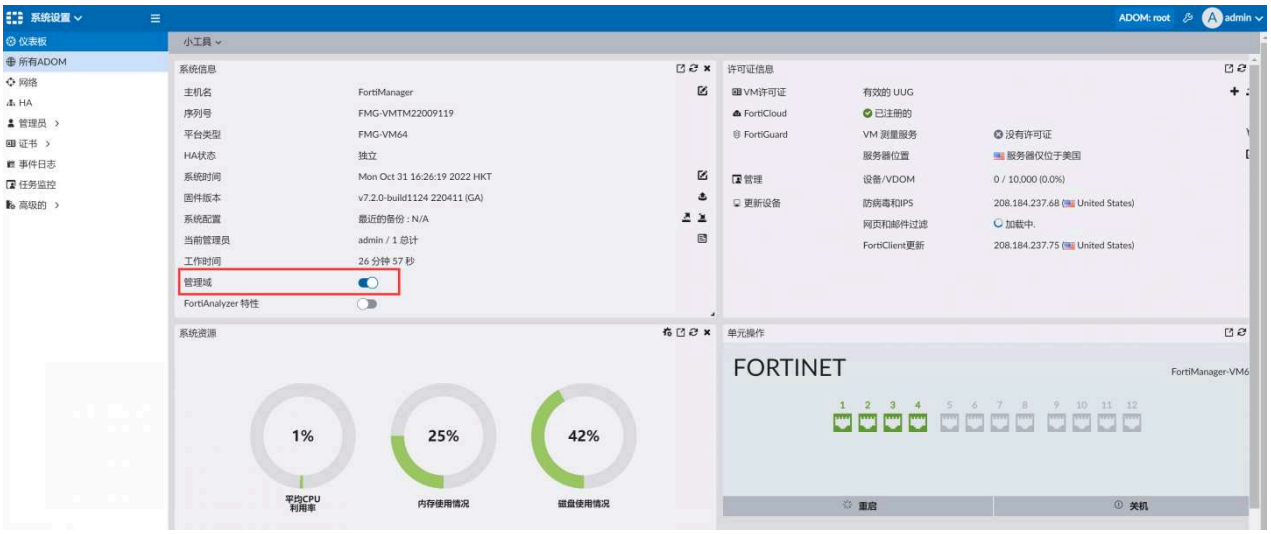
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

开启ADOM

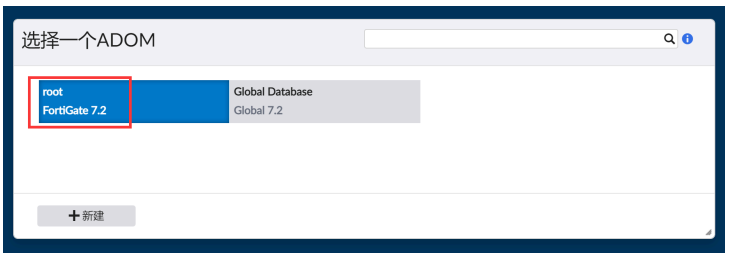
1. 进入系统设置。



2. 开启管理域功能。

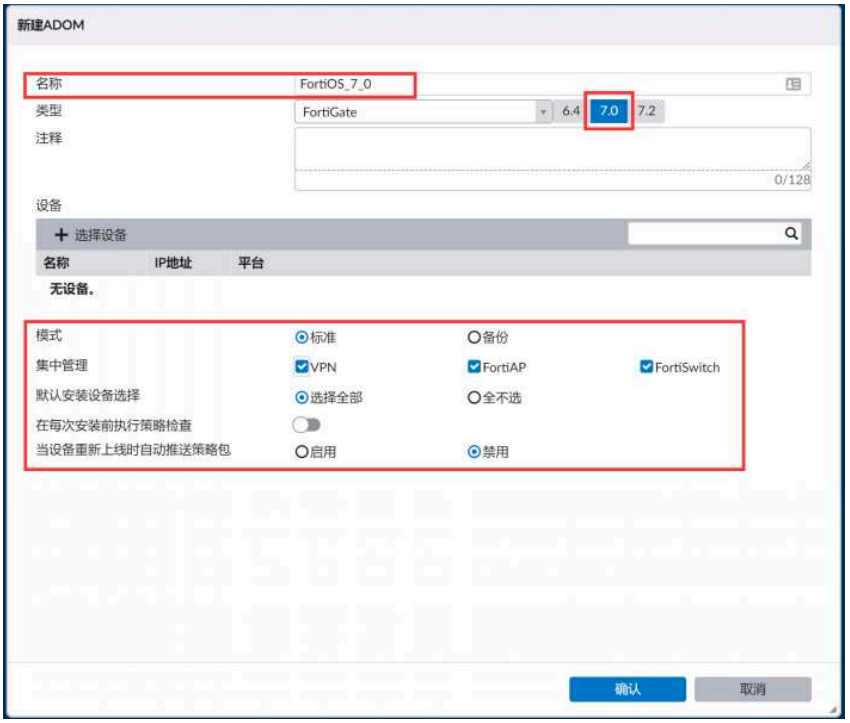


3. 再次登录FortiManger管理界面，原来的FortiManger变成了root ADOM。

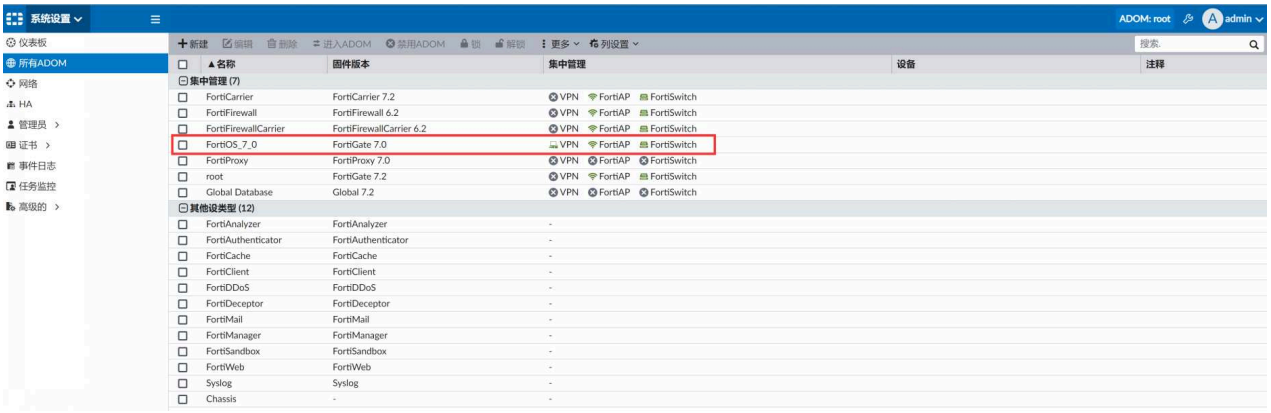


4. 点击新建按钮，新建一个7.0版本的ADOM。

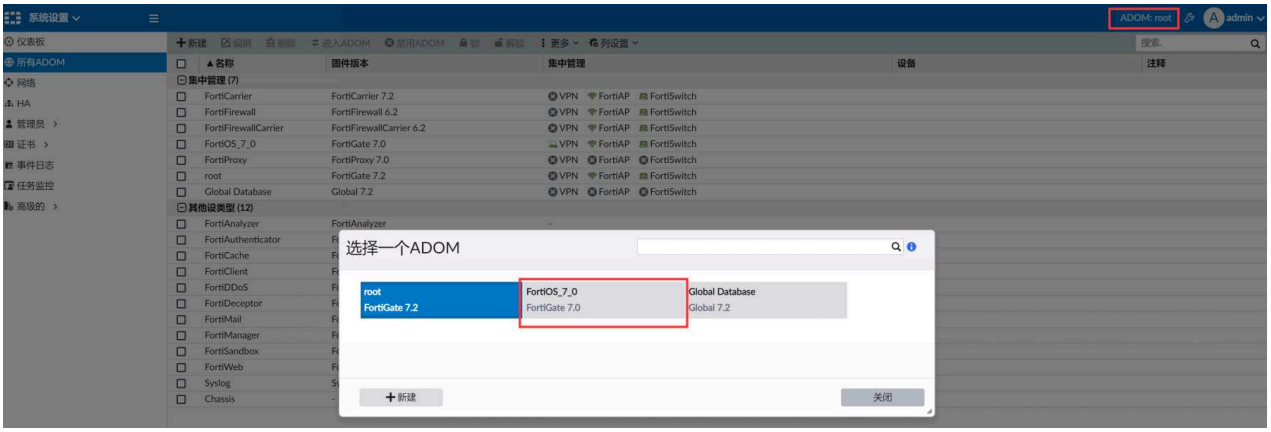
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 创建完成后，在系统设置中可以看到新建的ADOM。



6. 点击页面右上角的ADOM选择器，可以看到新建的ADOM，点击可进入该ADOM。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ADOM的高级特性

ADOM运行模式



标准模式

提供从FortiManager到ADOM和受管设备的配置更改的完全访问权限。

- 默认的模式
- ADOM读写权限
- 所有管理面板可用
- 能通过FortiManager的界面对被管理的设备配置变更
- 直接在受管设备上进行的更改能自动更新到FortiManager

> **重要**
>
> 通过FGFM协议，被管理的设备每5秒会对配置进行差异检查，并且会将差异修订发送到FortiManager。

标准模式面板截图：



备份模式

直接在受管设备上进行备份配置更改，主要目的是备份直接在受管设备上进行的配置更改。

- ADOM 是只读的
- 更少的可用管理面板
- 只能通过脚本的方式来对被管理的设备进行配置变更
- 可以直接在被管理的设备上进行配置变更
- 必须满足配置修订要在FortiManager上备份的特定条件：
  - 配置变更然后管理员会话超时
  - 配置变更然后登出
  - 配置变更然后重启
  - 从被管理设备上手动备份配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

标准模式面板截图：



ADOM高级模式

一台防火墙的不同VDOM可以加入到不同的FortiManger的ADOM里，默认不可以。



标准

FortiGate 设备仅能被添加到一个ADOM，默认模式。

高级

一台FortiGate的不同VDOM能被指派到不同的ADOM，全局应用到全部ADOM，这个适合高级用户开启，相对比较复杂。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

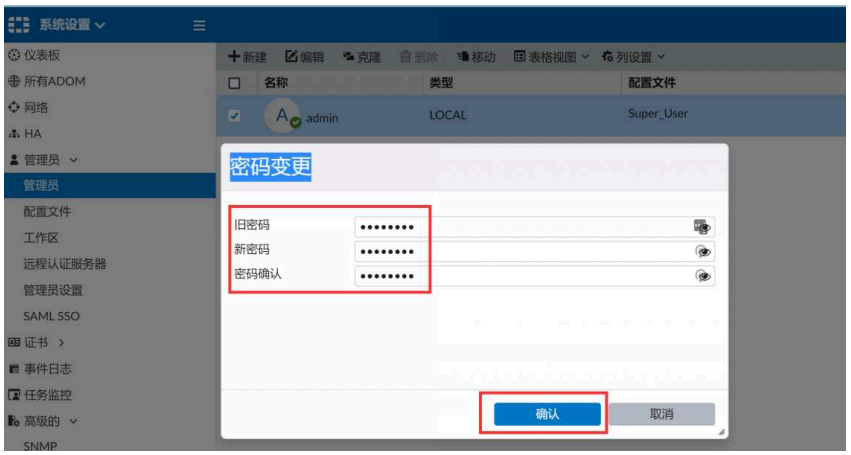
管理员账号管理

修改管理员密码

1. 进入系统设置→管理员界面，邮件点击管理员，选择密码变更。



2. 输入旧密码和新密码，并点击确认。



重要

第一次登陆防火墙的时候也会提示让我们设置一个新的密码。这个位置是手工修改管理员的密码位置。

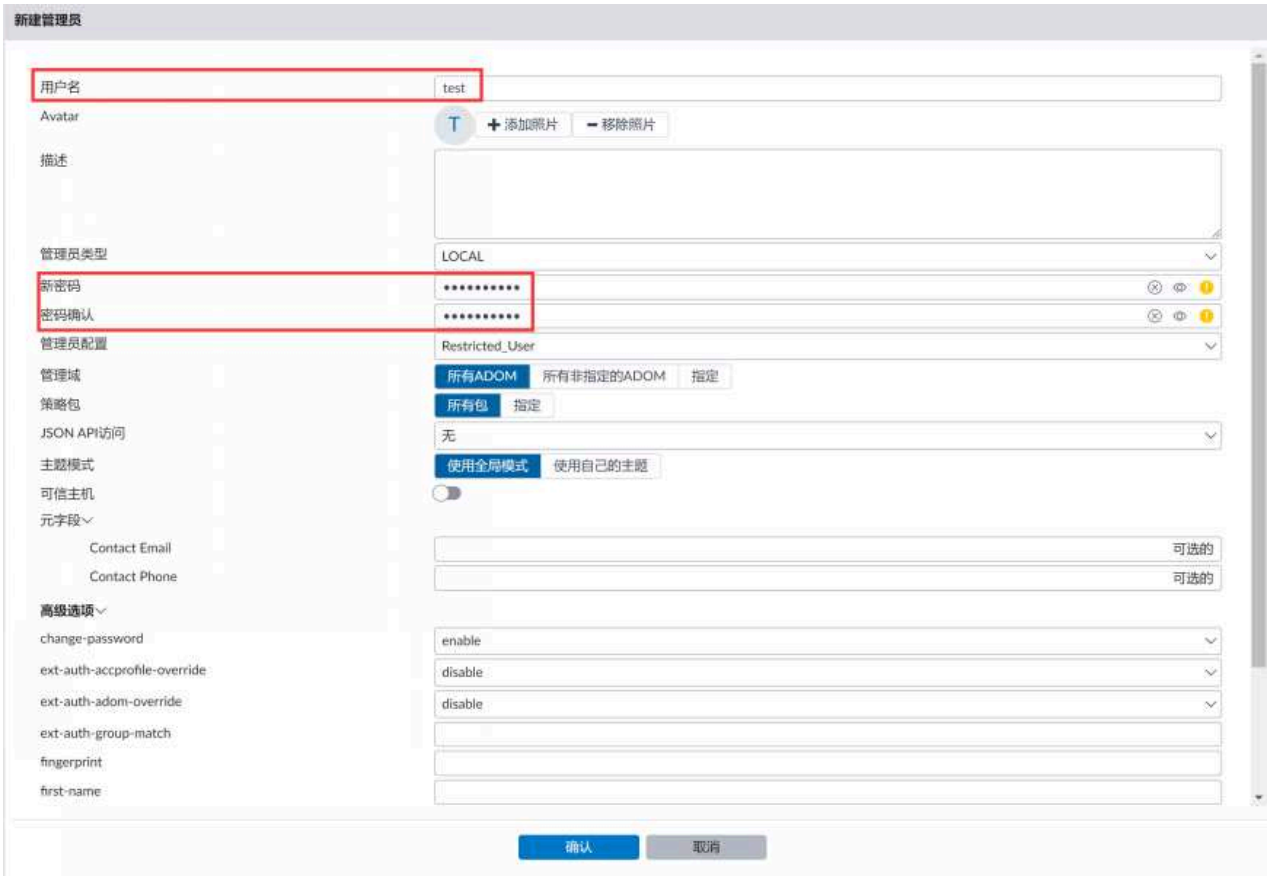
新建管理员

1. 进入管理员页面，点击新建按钮。

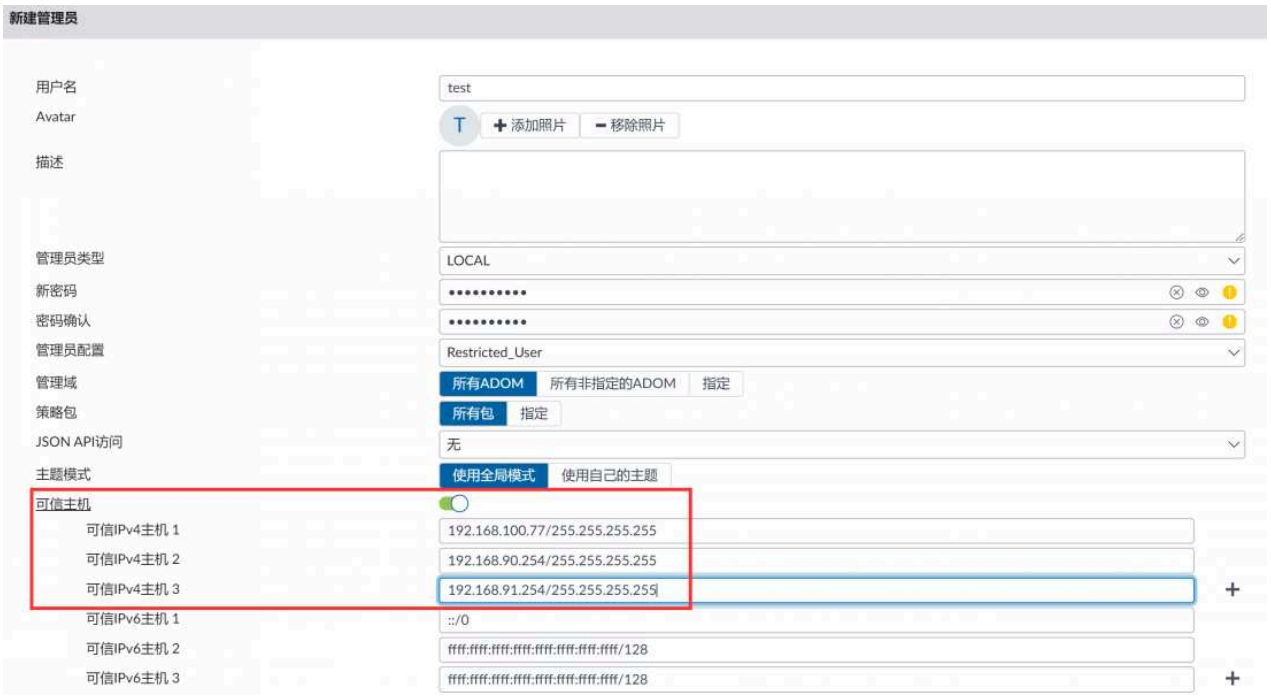


2. 在弹出的新建管理员页面中，填写管理员名称与密码。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

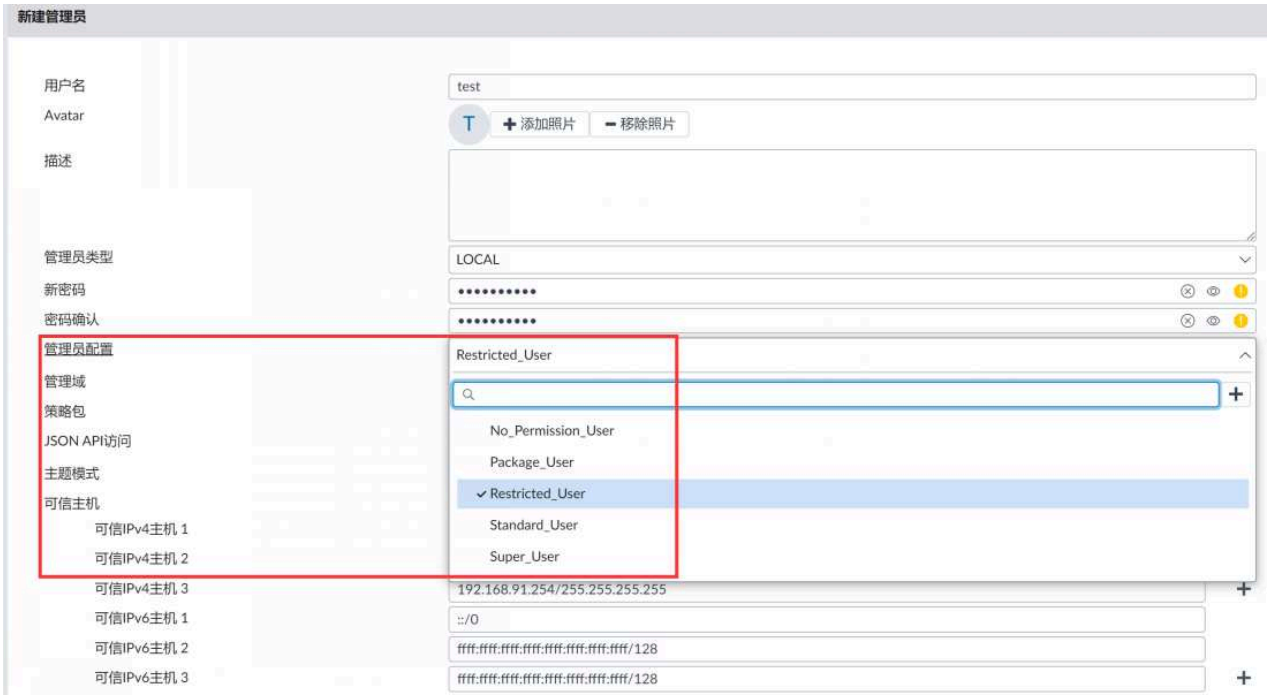


3. 配置可信主机，只有在可信性主机范围内的IP地址可以管理FortiManeger。



4. 配置管理员权限。

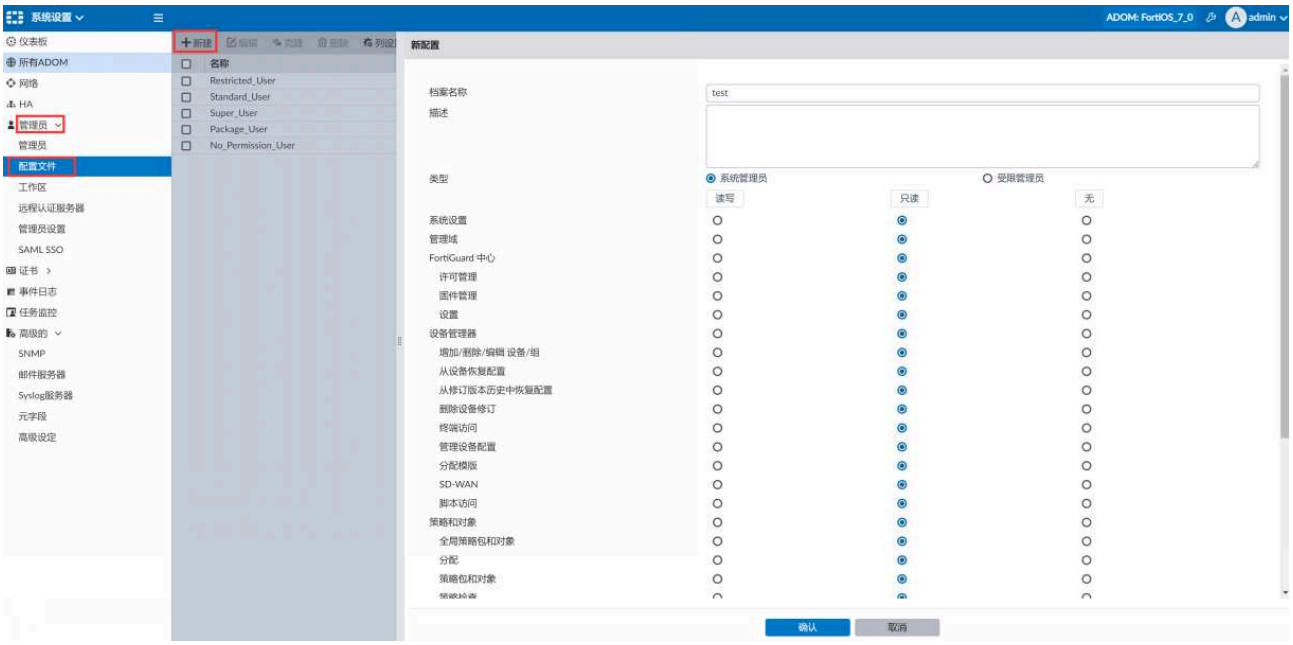
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- Restricted_User：未启用系统权限，并且对所有设备权限具有只读访问权限。
- Standard_User：未启用系统权限，但对所有设备权限具有读/写访问权限。
- Super_User：已启用所有系统和设备权限。
- Package_User：已启用读/写策略包和对象权限，并具有系统和其他内容的只读访问权限。

管理员配置文件

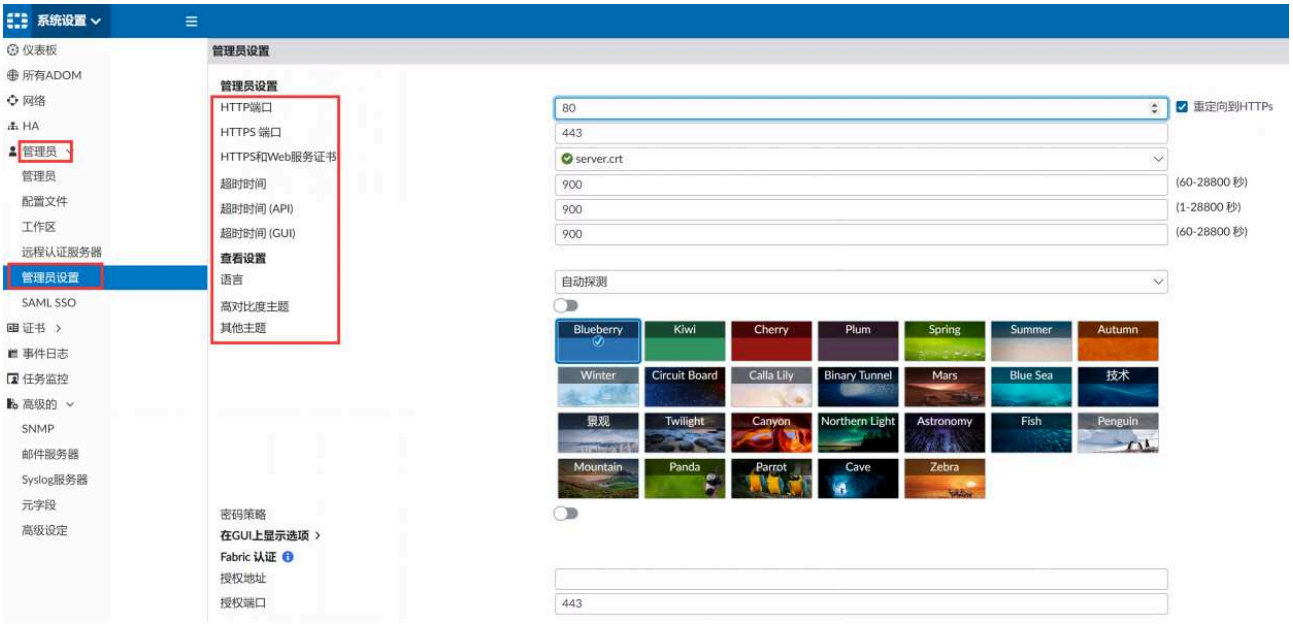
可以针对自己的需求进行新建管理员配置文件。



管理员高级配置

可修改管理端口、调整管理员超时时间、调整管理FMG的数字证书、语言、主题等等。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



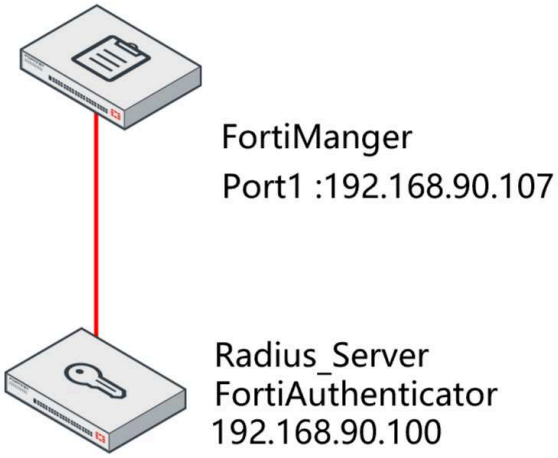
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置远程管理员

需求

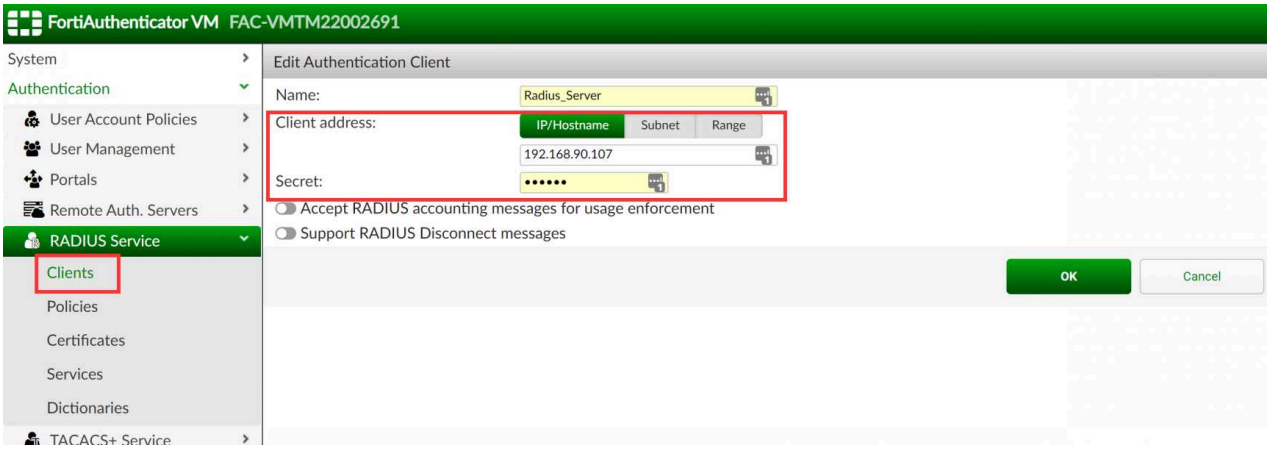
要求使用test这个远程账号登陆FortiManger，如果远程认证服务器失效，则使用test这个账号的逃生密码test进行登陆，另外其他的远程用户也需要可以登陆到FortiManger。

拓扑



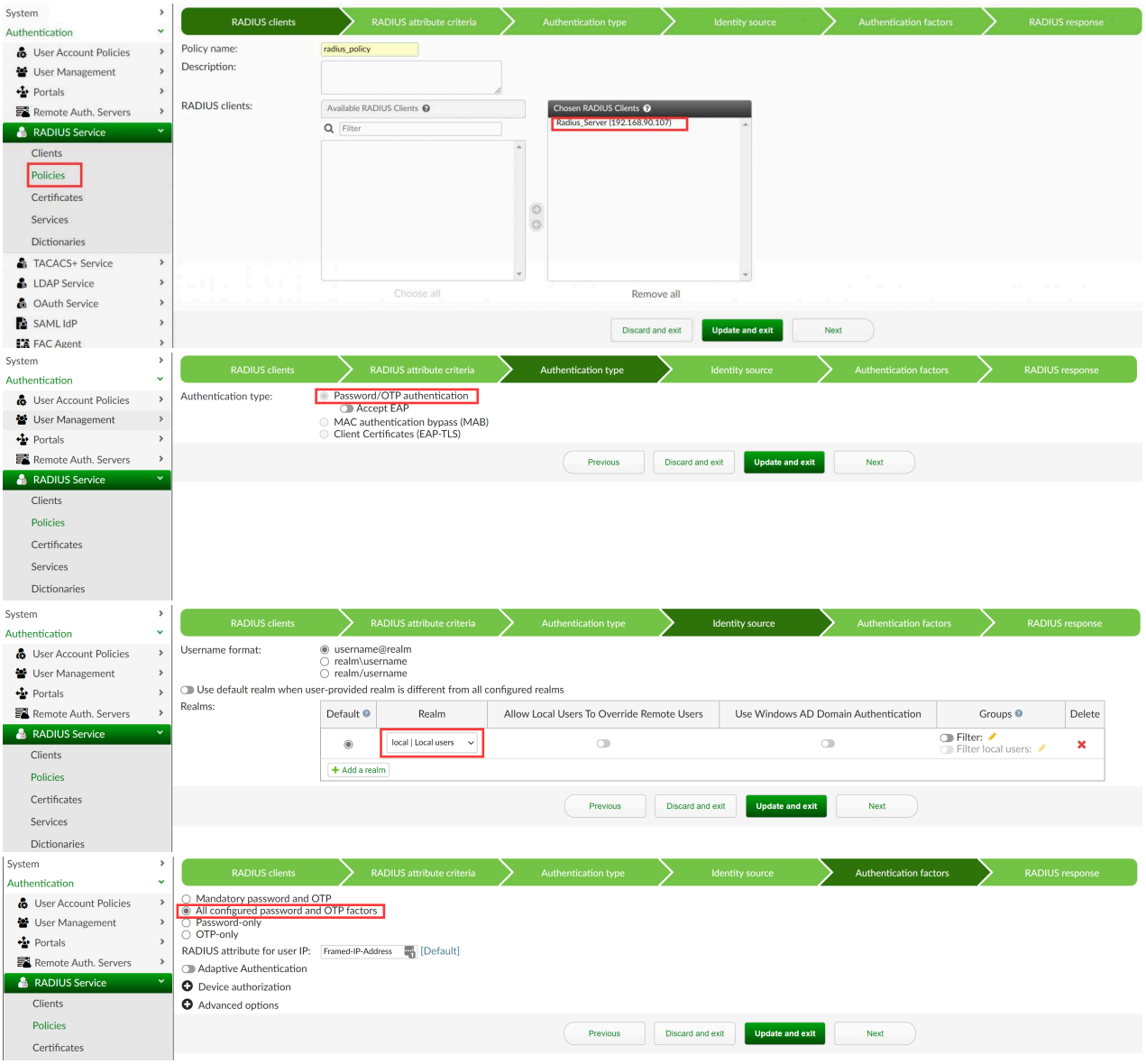
配置步骤

1. FortiAuthenticator上配置Radius认证client，IP地址需要保函FortiManger的管理IP地址。

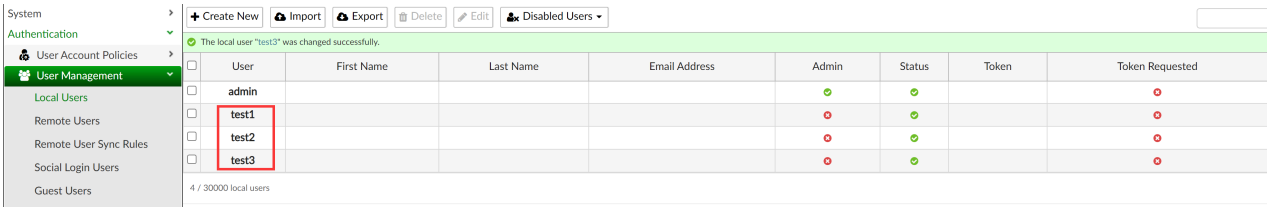


2. 配置Radius Profile，认证方式为本地密码认证。

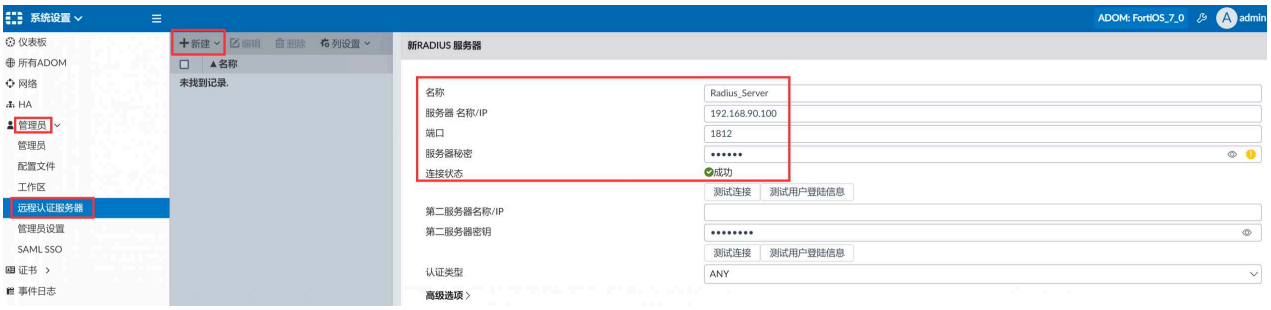
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置本地Radius账户test1、test2、test3（密码均为11111111）。

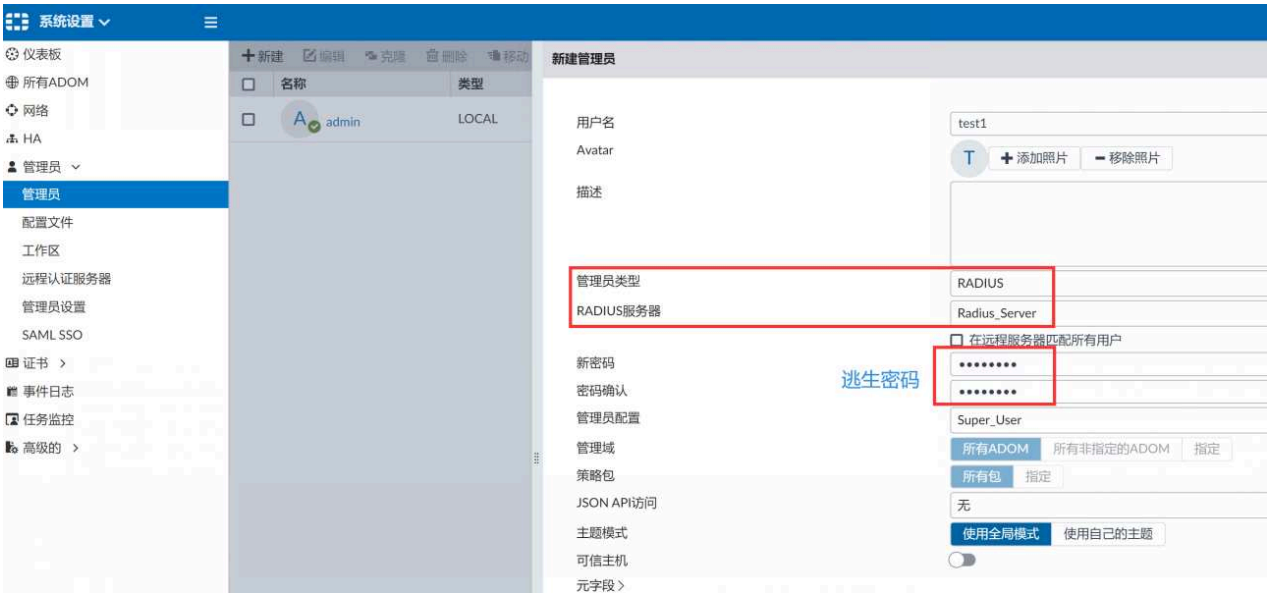


4. 在FortiManager上创建远程Radius认证服务器，并测试成功。



5. 新建Radius管理员账户test1（密码Fortinet123#），不勾选“在远程服务器匹配所有用户”，这个账号必须先去Radius认证，认证通过可以登陆，如果Radius服务器出现了故障，则使用逃生账户密码（Fortinet123#）也可以登陆FortiManger。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 新建Radius管理员账户test2，勾选“在远程服务器匹配所有用户”，这个帐号必须在Radius服务器认证，无本地逃生密码。



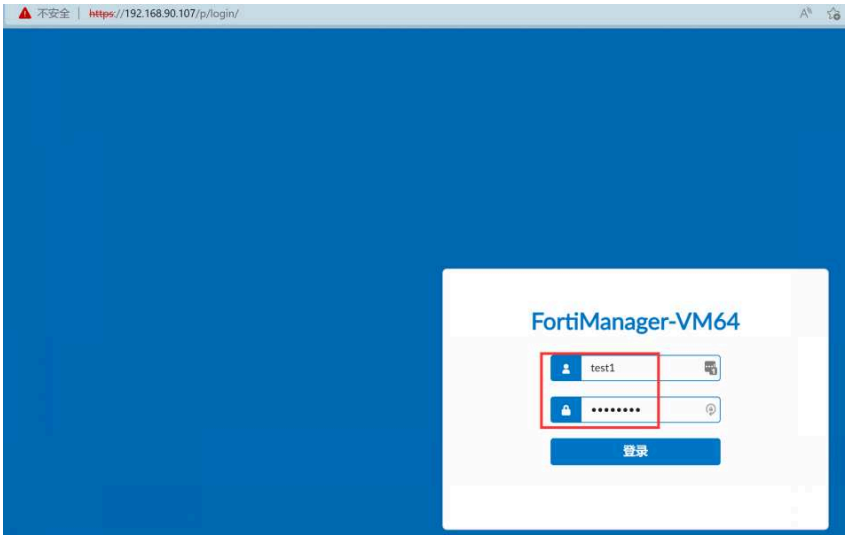
重要

关于存在于FMG本地的admin账号，通常如果对于账号管理不是特别的严格的话，我们都是建议保留这个admin账号，这样比较好，防止没有配置test1这样的明细的具备逃生密码的账号且Radius服务器故障的时候，无法登陆到FMG。本地的admin相当于是另外一个逃生账号，当然密码需要保存好，另外平时尽量不要使用到本地的admin账号，只有当Radius服务器故障，且没有test1这样的逃生账号的时候，这个时候本地的admin才用来作为逃生账号使用。

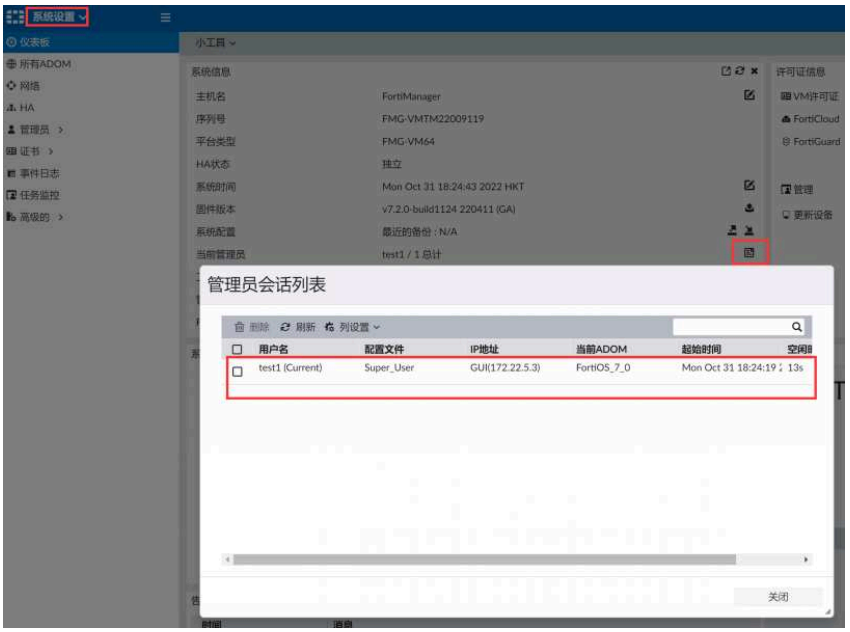
结果验证

1. 使用test1用户的Radius密码11111111登陆FortiManager。

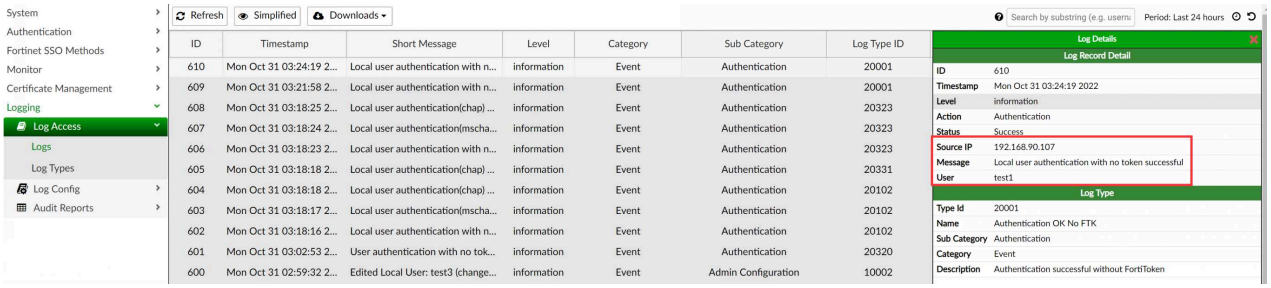
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 登陆成功后，在系统设置中可以看到在线用户。

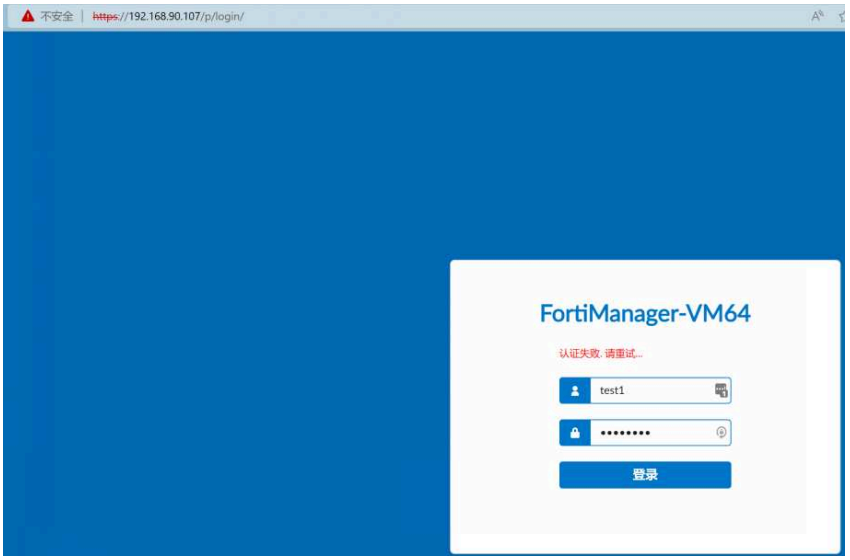


3. FAC上Radius的登陆成功日志。

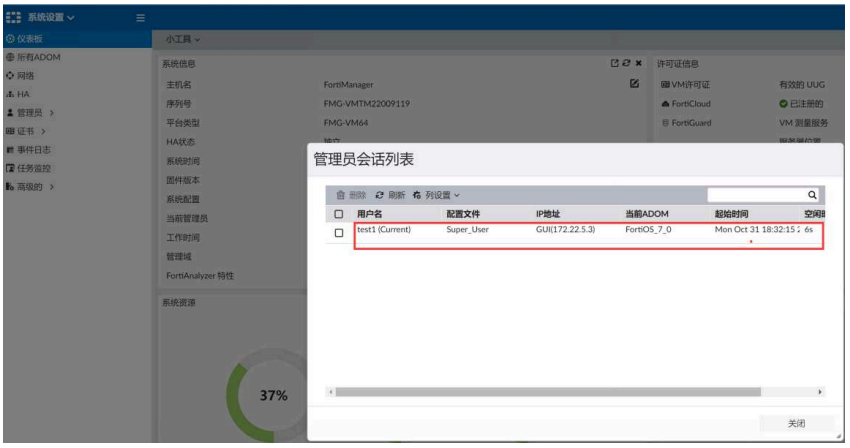


4. 将Radius服务器关闭，再次使用test1和他的Radius密码11111111登陆FortiManager，登陆失败。

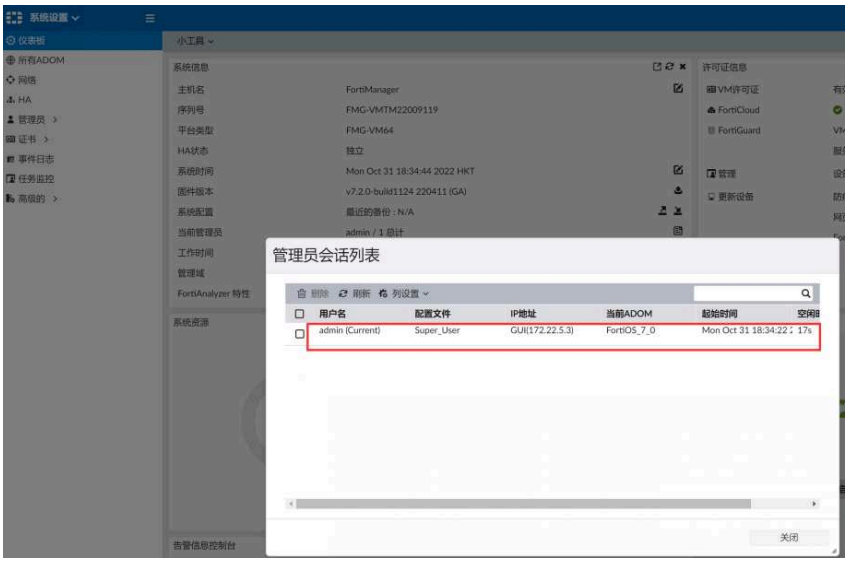
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 这个时候就需要使用我们为test1设置的本地逃生密码Fortinet123#了，继续使用zhangsan账号和逃生密码登陆FortiManger。



6. 当然此时使用本地的admin账号也是可以登陆FortiManger的另外一个逃生账号。

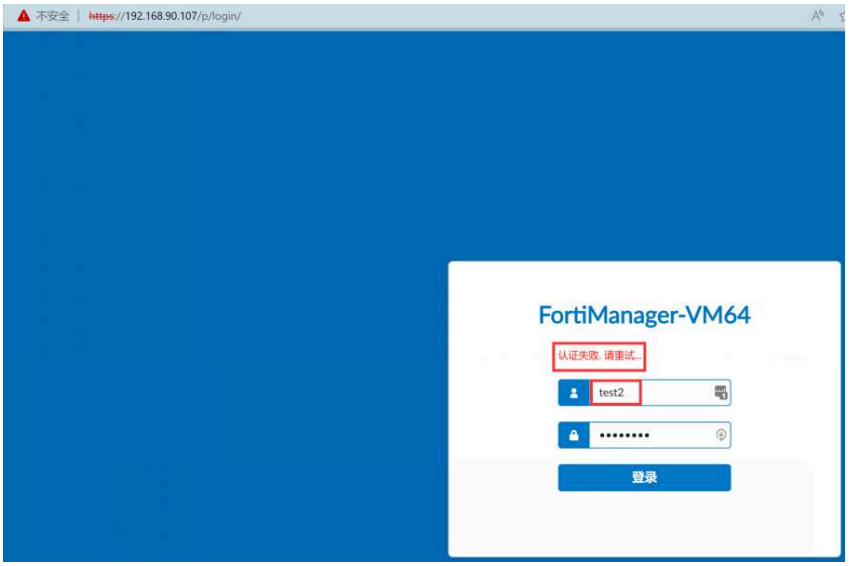


重要

假如将FMG本地的admin账号删除了，这个情况下admin是没办法通过Radius认证成功的（Radius故障了，不可达了），这个时候只能用test1的逃生密码登陆FortiManger。而现在模拟的是我们没有删除本地的admin账号，因此这个情况下我们可以使用admin账号继续登陆FortiManger，相当于另外的一个逃生账号。

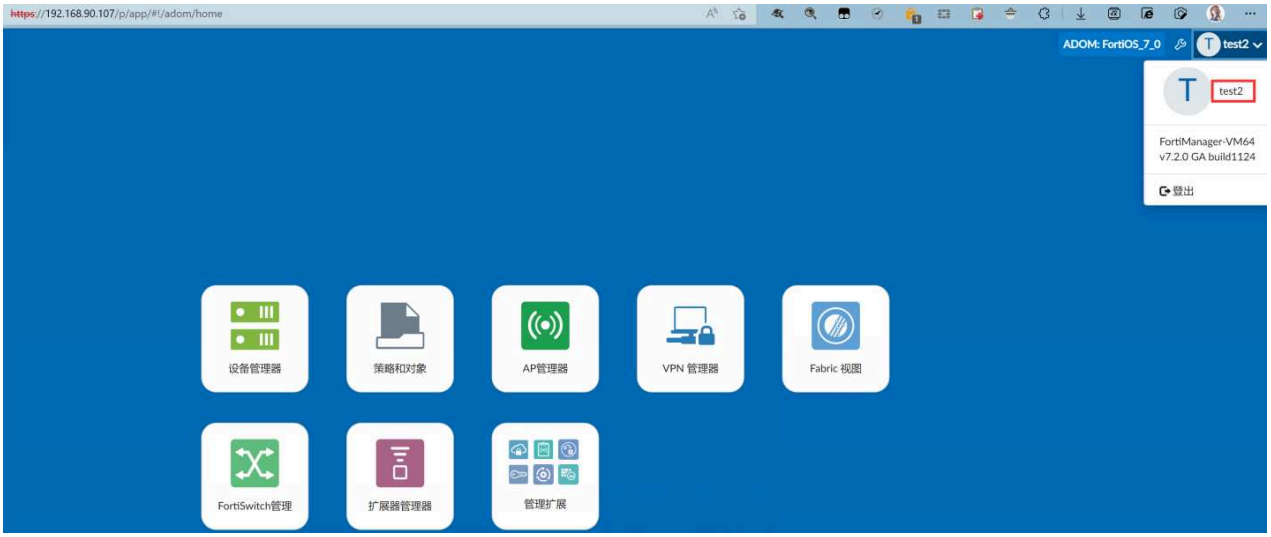
7. 使用test2账户（Radius用户密码11111111）登陆，该账户只允许Radius认证，没有逃生密码，由于FAC Radius服务器已经关闭，该用户登录失败。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 恢复FAC的Radius服务状态。

9. 再次使用test2（密码11111111）用户登陆，使用Radius认证登陆成功。



> **重要**
>
> test2配置的是标准管理员，不是超级管理员，因此看到的FortiManger内容有限。

.0. 查看FAC Radius认证成功的日志。

ID	Timestamp	Short Message	Level	Category	Sub Category	Log Type ID
620	Mon Oct 31 20:06:32 2...	Web access granted to 'admin'	information	Event	Authentication	20994
619	Mon Oct 31 20:06:32 2...	Administrator 'admin' logged in	information	Event	Authentication	20994
618	Mon Oct 31 20:06:32 2...	Local administrator authenticati...	information	Event	Authentication	20994
617	Mon Oct 31 20:05:03 2...	Local user authentication with n...	information	Event	Authentication	20001
616	Mon Oct 31 20:04:06 2...	Local user authentication with n...	information	Event	Authentication	20001
615	Mon Oct 31 20:02:42 2...	FortiAuthenticator booted up a...	notice	Event	System	30901
614	Mon Oct 31 20:02:41 2...	NTPD adjusted time from Mon ...	information	Event	System	30905
613	Mon Oct 31 20:02:03 2...	RADIUS server running in full ed...	information	Event	System	30101
612	Mon Oct 31 03:27:31 2...	Shutdown process is initiated.	notice	Event	System	30902
611	Mon Oct 31 03:27:28 2...	Shutdown process is initiated. R...	notice	Event	System	30902
610	Mon Oct 31 03:24:19 2...	Local user authentication with n...	information	Event	Authentication	20001

Log Details

Log Record Detail

ID	617
Timestamp	Mon Oct 31 20:05:03 2022
Level	information
Action	Authentication
Status	Success
Source IP	192.168.90.107
Message	Local user authentication with no token successful
User	test2

Log Type

Type Id	20001
Name	Authentication OK No FTK
Sub Category	Authentication
Category	Event
Description	Authentication successful without FortiToken

总结

推荐方式1（以上配置举例）

- 配置一个明细的test1账号+逃生密码

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 配置另外一个匹配远程Radius所有用户test2
- 保留本地admin账号（作为另外一个远程Radius的本地逃生账号）
- 远程用户全部可以登录，如果Radius服务器故障，可以使用test1的账号和逃生密码登陆，另外还可以使用本地的admin账号逃生登陆



推荐方式2

- 保留本地admin账号（作为远程Radius的本地逃生账号）
- 配置一个匹配远程Radius所有用户的账户
- 远程用户全部可以登录，如果Radius服务器故障，可以使用本地的admin账号逃生登陆



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

管理员和ADOM关联

需求

对于分区管理的需求，我们通常建议将管理员与ADOM进行绑定，每个区域的管理员只可以看到属于自己区域的管理设备，对于其他区域的设备不可见，这样可以实现管理员和设备的分区独立管理。

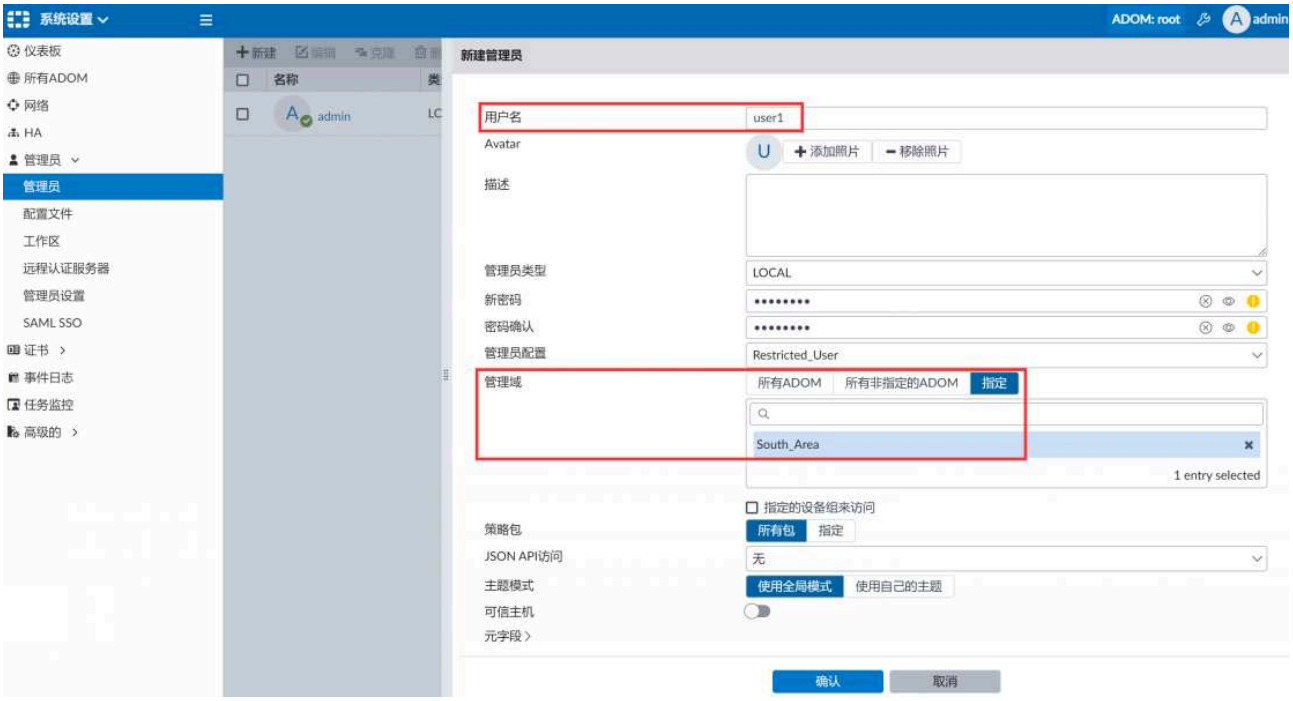
举例：有三个ADOM，South_Area、North_Area、East_Area，三个区域的管理员分别管理各自的FortiGate，相互之间独立彼此独立，管理员user1需要管理ADOM South_Area，管理员user2需要管理ADOM North_Area，管理员user3需要管理ADOM East_Area，而超级管理员admin则可以管理所有区域的所有防火墙。

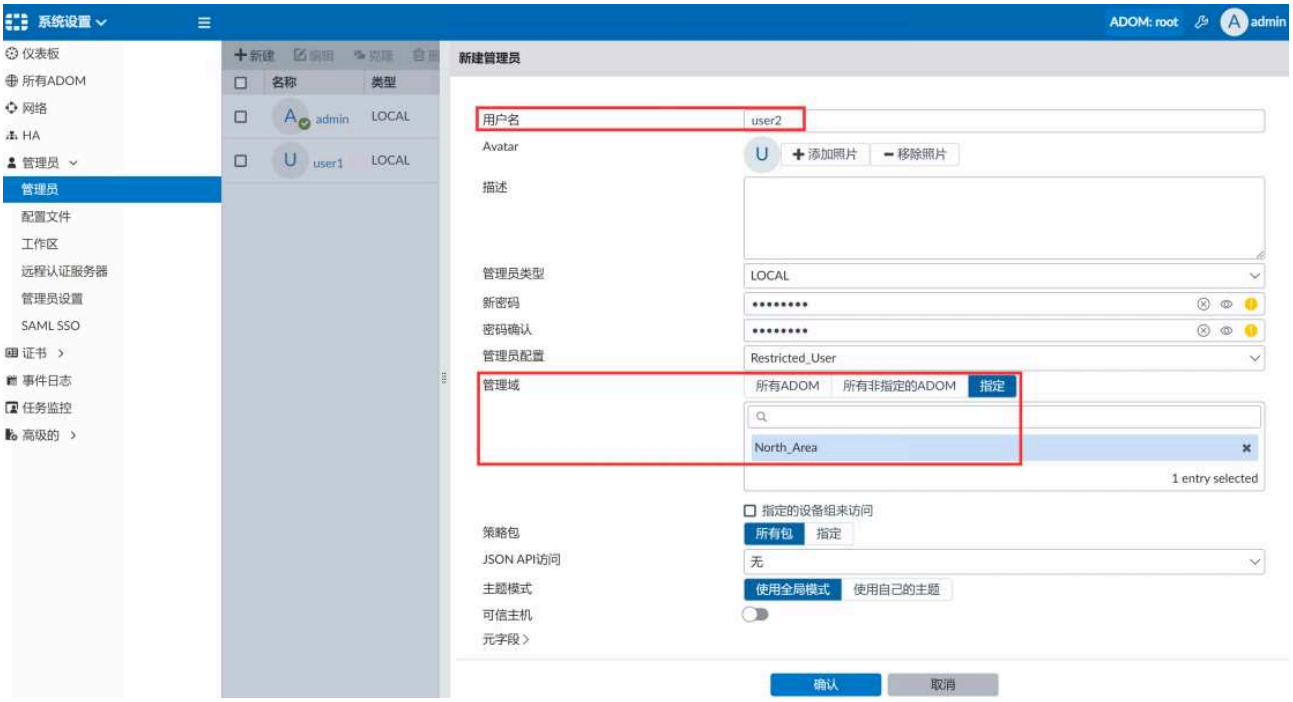


配置步骤

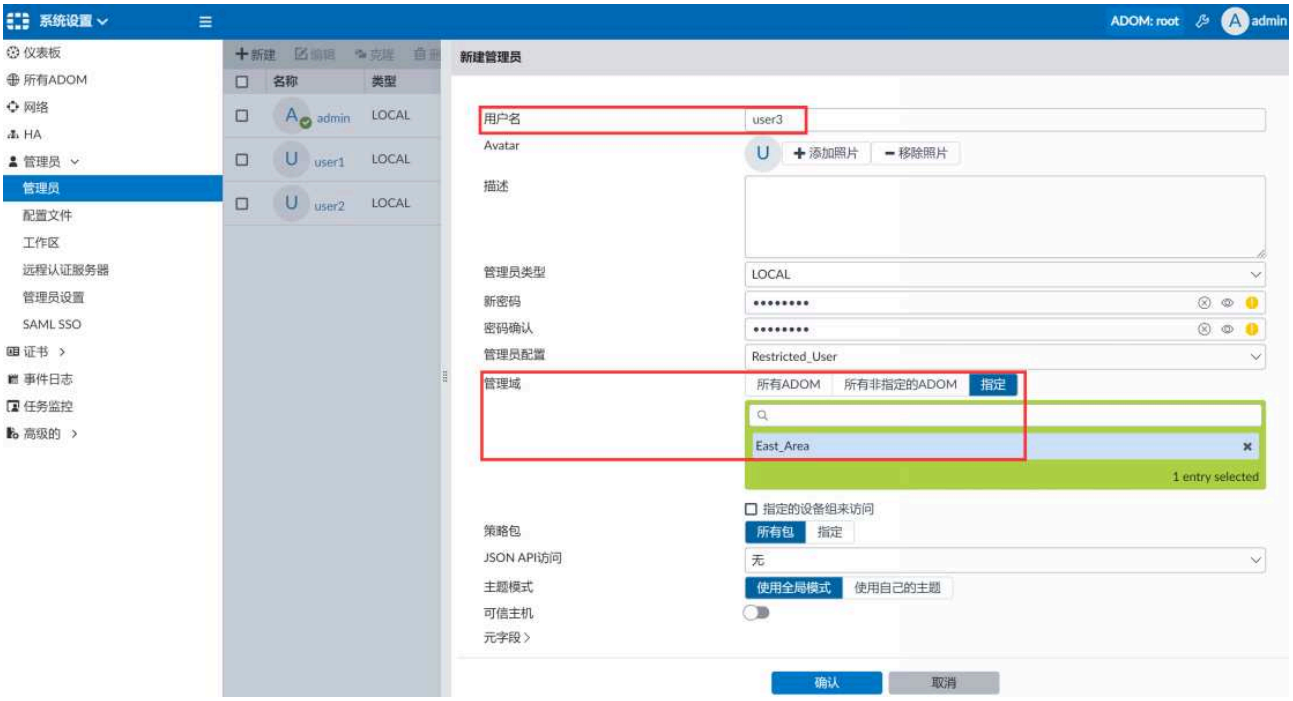
新建user1、user2、user3三个本地账号并绑定到相应的ADOM上。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





结果验证

1. 使用user1登陆FortiManager，可以看到user1只能访问South_Area ADOM。



2. 使用user2登陆FortiManager，可以看到user2只能访问North_Area ADOM。

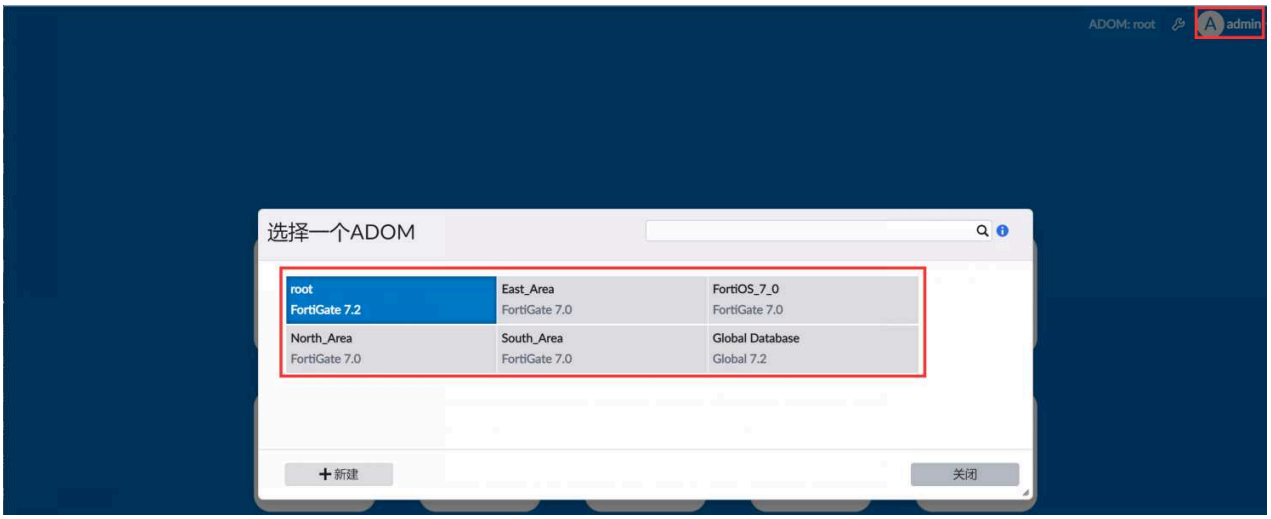
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 使用user3登陆FortiManager，可以看到user3只能访问East_Area ADOM。



4. 使用admin登陆FortiManager，可以看到admin能访问所有ADOM。

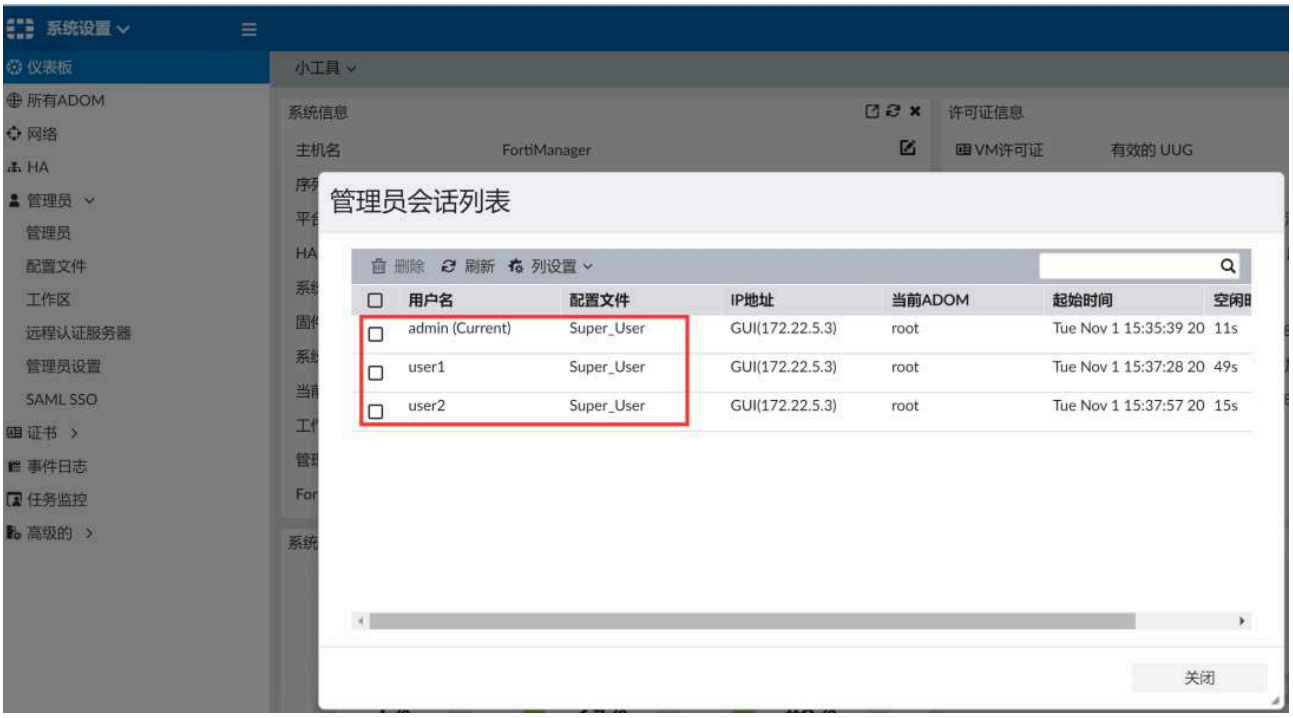


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ADOM的Workspace模式

需求

当多个管理员同时登陆到同一个ADOM，如果多个管理员试图同时更改相同的ADOM，则会导致小概率配置冲突。



为了避免这种情况，我们可以在CLI下开启workspace模式。禁用并发管理员对ADOM的配置访问，添加ADOM锁定，同时只能有一个管理员具备读/写访问权限，所有其他管理员都只具有读访问权限。

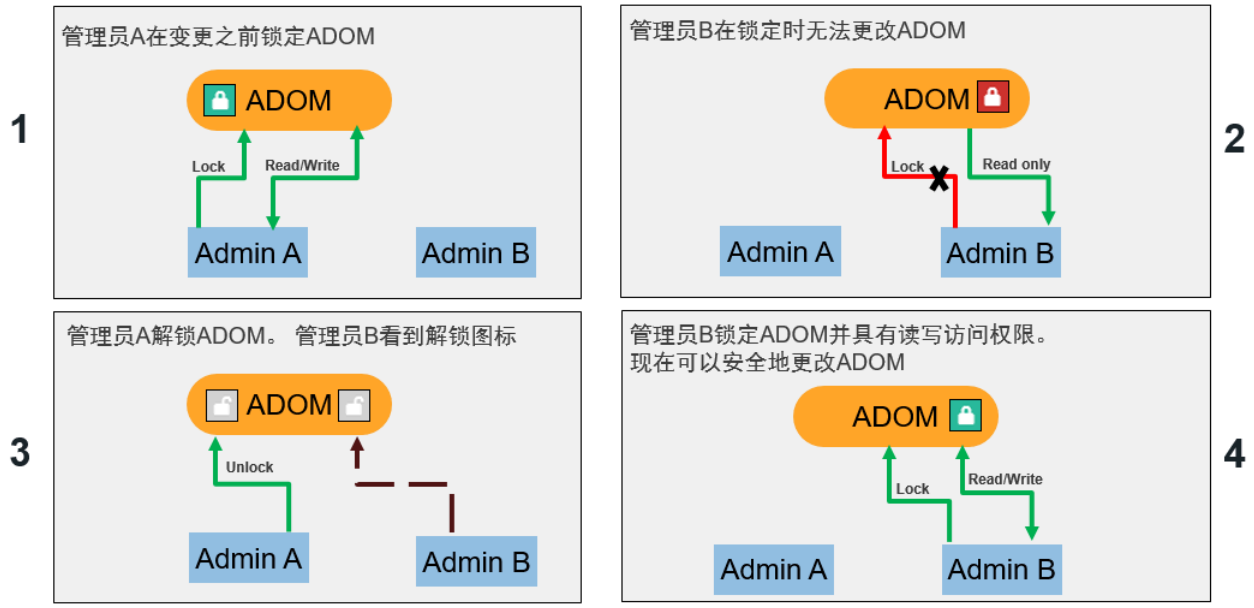
```
config system global
  set workspace-mode normal
end
```

重要

在启用Workspace模式以保存其工作之前，必须通知其他管理员，否则可能会导致一些登录用户丢失未保存的数据。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

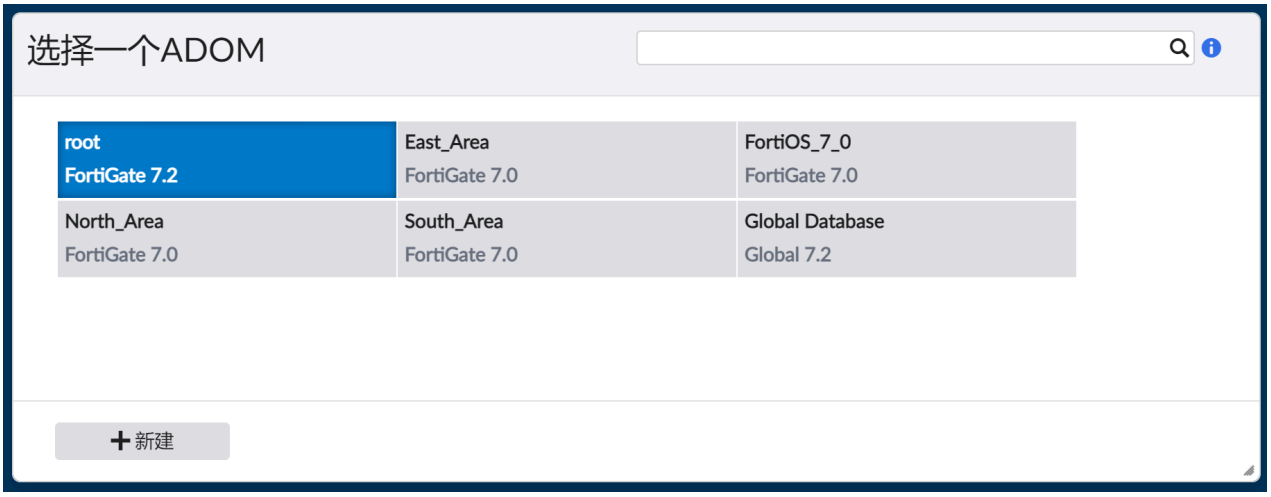
功能简介



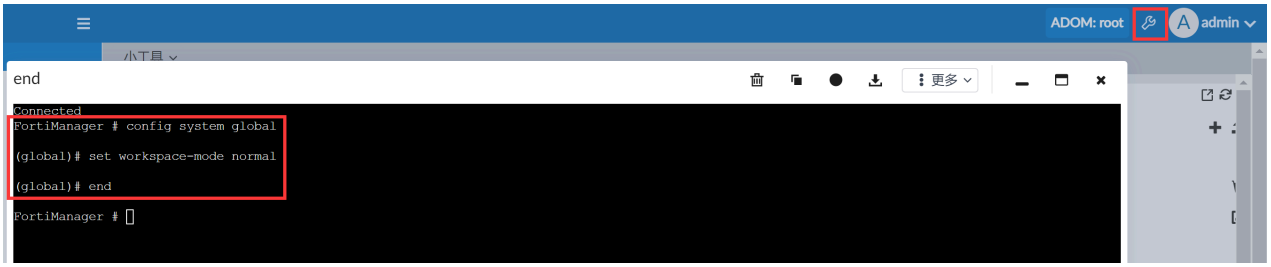
以此避免多个管理员同时修改同一配置的冲突风险。

配置步骤

1. 使用admin账户登陆FortiManager，默认情况下，workspace-mode是“set workspace-mode disabled”，因此没有任何的锁定标志。

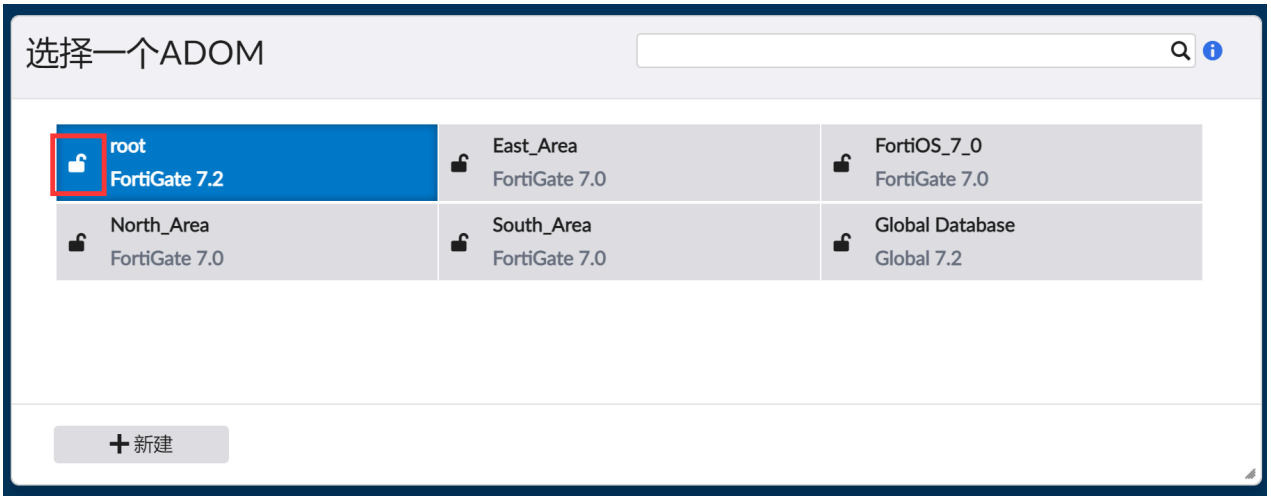


2. 进入Web CLI，在“config system global”下开启“set workspace-mode normal”。

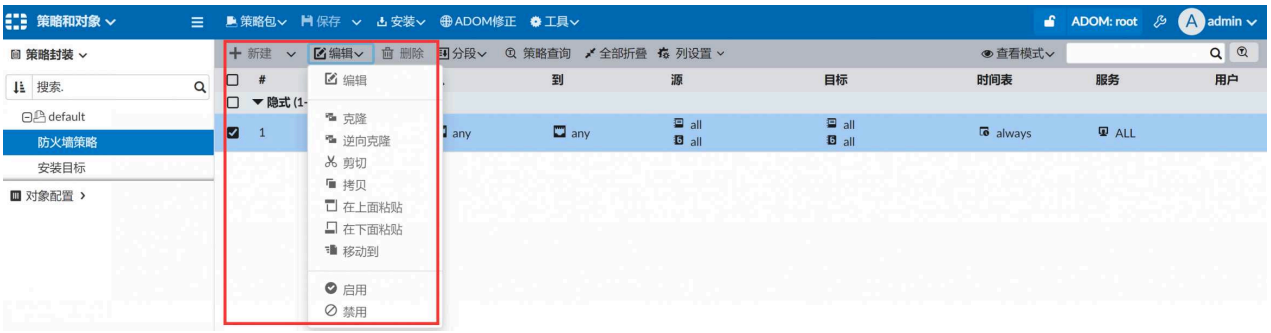


3. 再次登录FortiManger，每一个ADOM都多了一把锁的标志，在没有锁定之前都仅仅拥有只读权限。

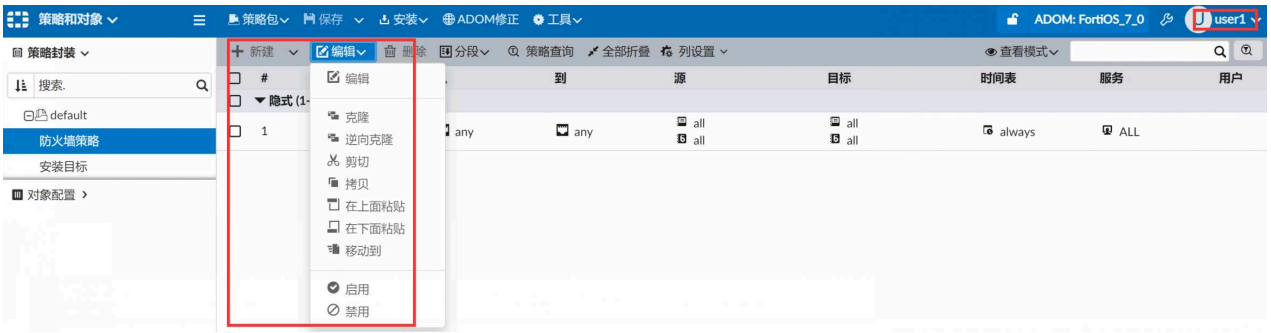
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 在这个情况下，针对管理设备所有的配置按钮都是灰色的，都是只读权限。



5. 使用另外一个管理员user1登陆查看，和admin一样的结果，仅仅具有只读权限。

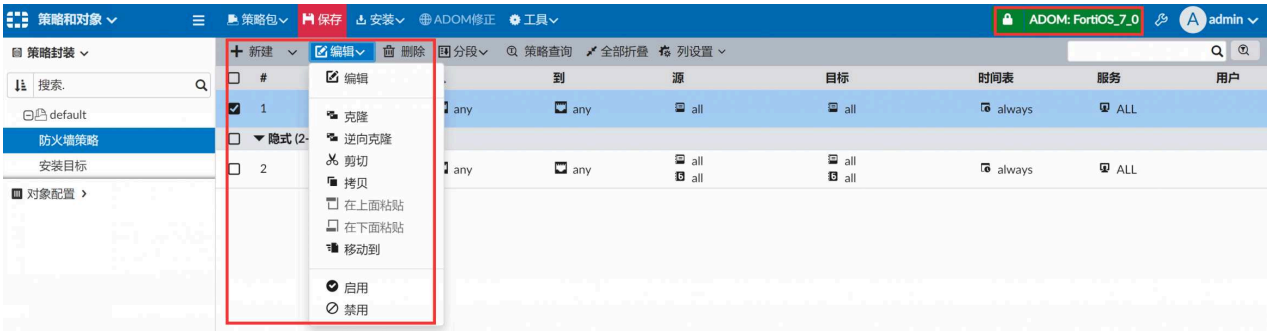


6. 此时admin账号想要在策略包里面添加一条策略（需要写的权限），这个时候我们就需要使用admin账户将这个root ADOM进行锁定了，只有锁定了ADOM的账户才会拥有读/写的操作权限。点击页面右上角的锁定按钮，锁定当前ADOM。



7. 新建或编辑策略，可以看到针对该ADOM，admin账户已经具备写权限。

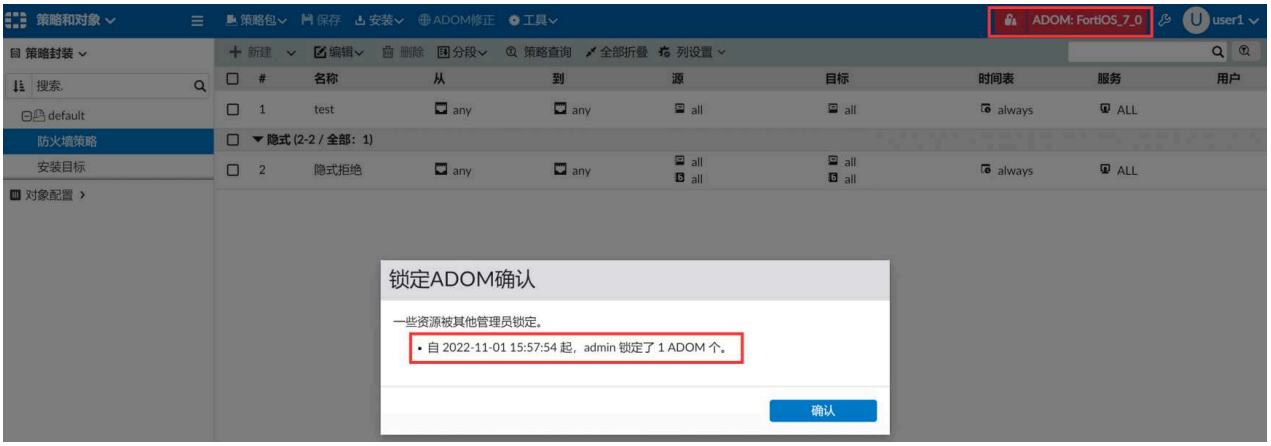
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 新建完成后，注意点击页面左上角的“保存”按钮，配置才会被下发到启动配置文件中。



9. 此时FortiOS_7_0这个ADOM已经被admin账户锁定了，使用user1账户同时登陆后查看该ADOM的权限。可以看到由于admin已经锁定了该ADOM，user1无法针对该ADOM进行任何写操作。



0. 针对ADOM锁定图标颜色的说明。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

证书管理

数字证书是一个经证书授权中心（CA）数字签名的、包含公钥拥有者信息以及公钥，并且在特定的时间段内有效的文件。

FortiGate证书类型

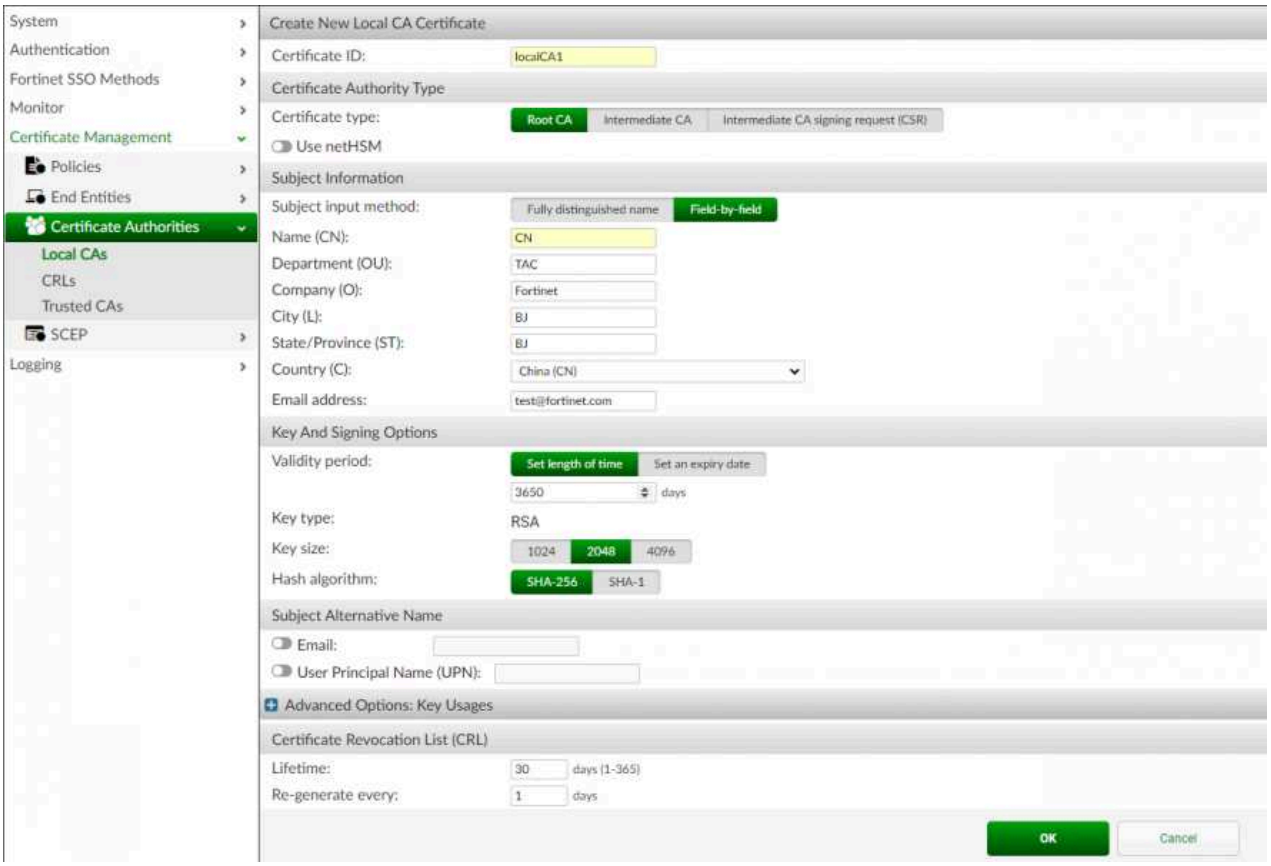
这里使用**FortiAuthenticator**作为证书服务器，生成证书并导入FortiGate。

远端CA证书

远程CA证书是只有CA的公钥，用于验证证书的有效性，如SSLVPN中验证终端的证书。

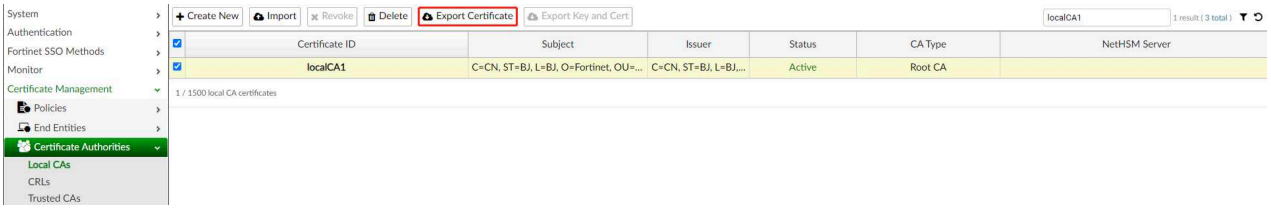
1. **FortiAuthenticator生成根CA证书**

   选择“Certicate Managerment”-->”Certificate Authorities“-->“Local CAs”，点击“Create New”，输入CA名称及证书信息，并点击“确认”。



2. **导出CA证书**

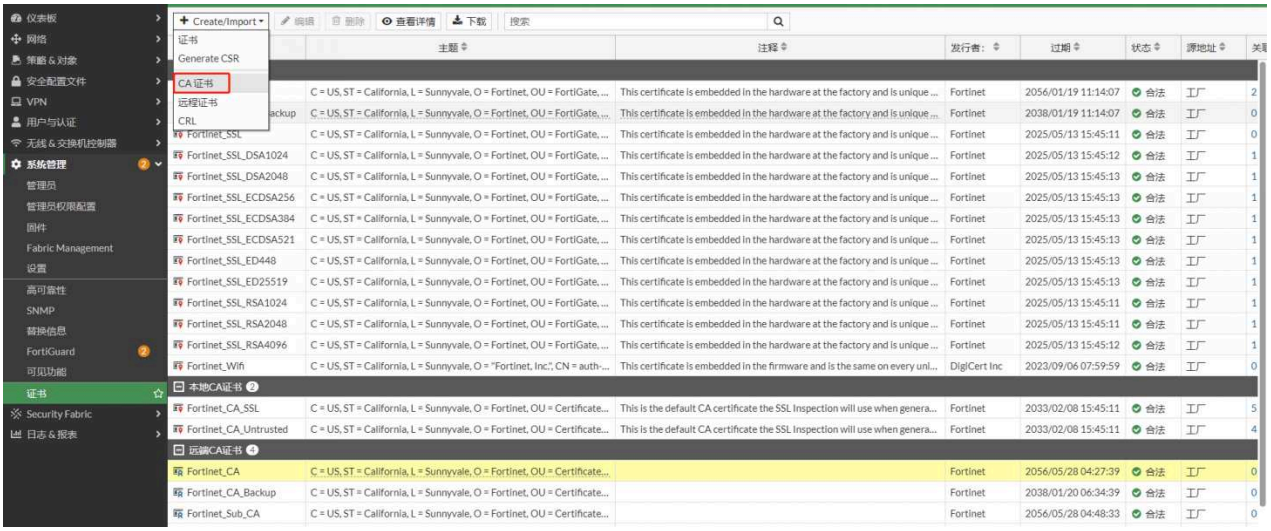
   导出的文件为localCA1.crt



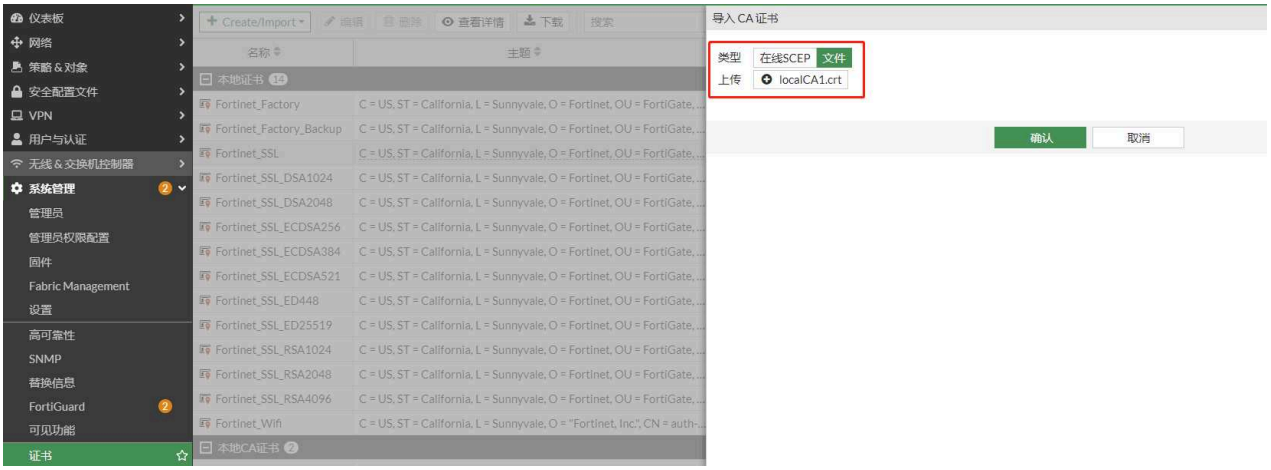
3. **导入FortiGate**

   选择“系统管理”-->“证书”，点击“Create/Import”，选择“CA证书”。

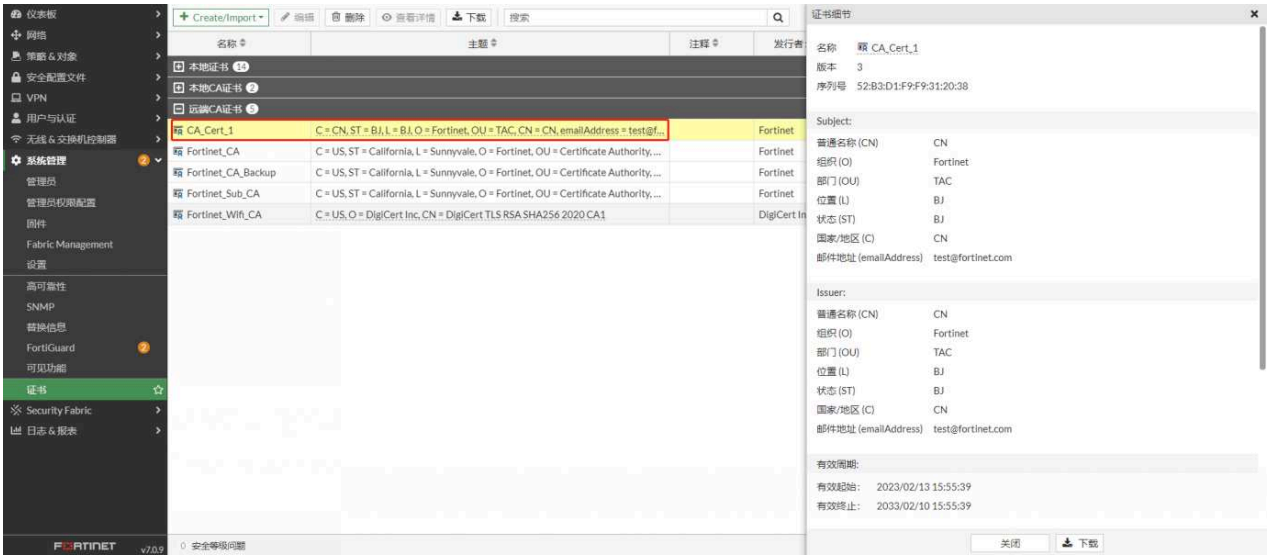
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



选择“文件”，上传CA“localCA1.crt”。



4. 查看导入的证书



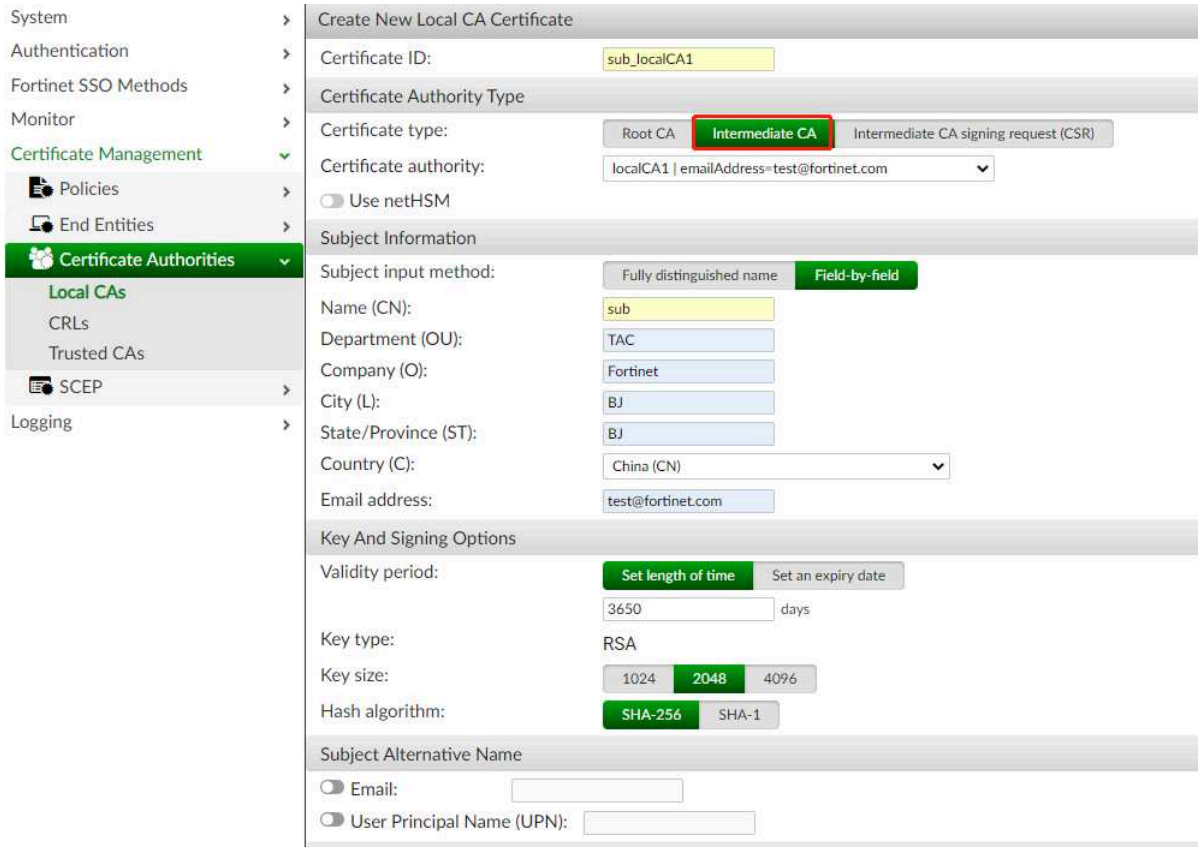
本地CA证书

本地CA证书是具有CA的公钥和私钥，具有签发能力的CA证书，如重签发portal认证的证书。

1. **FortiAuthenticator生成中间CA证书**

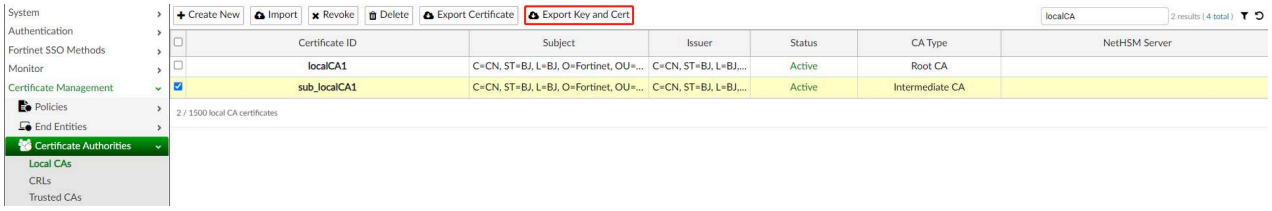
选择“Certicate Managerment”-->”Certificate Authorities“-->“Local CAs”，点击“Create New”，输入CA名称及证书信息，证书类型选择“Intermediate CA“，指定签发的根CA，并点击“确认”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

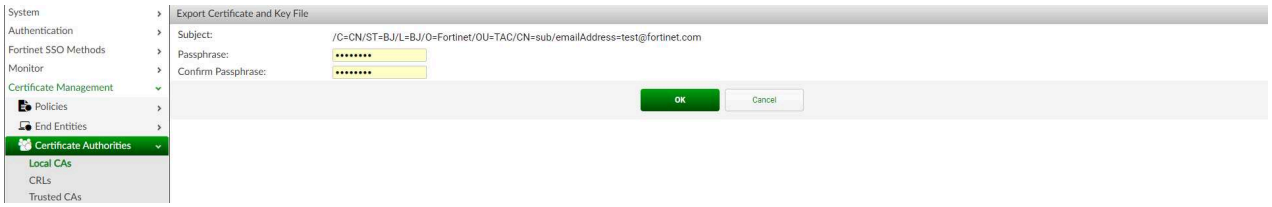


2. 导出CA公钥和私钥

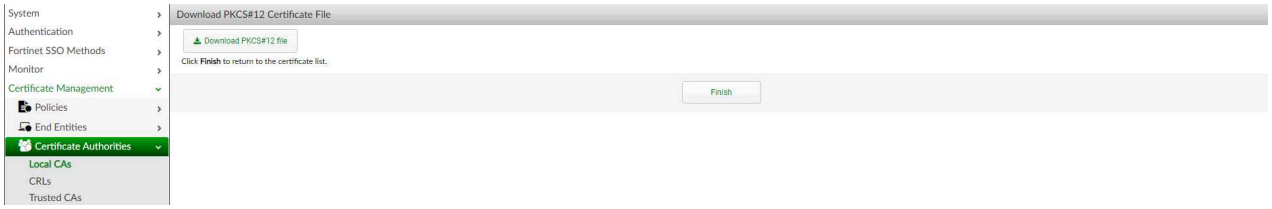
点击”Export Key and Cert“。



输入用于保护证书的密码。



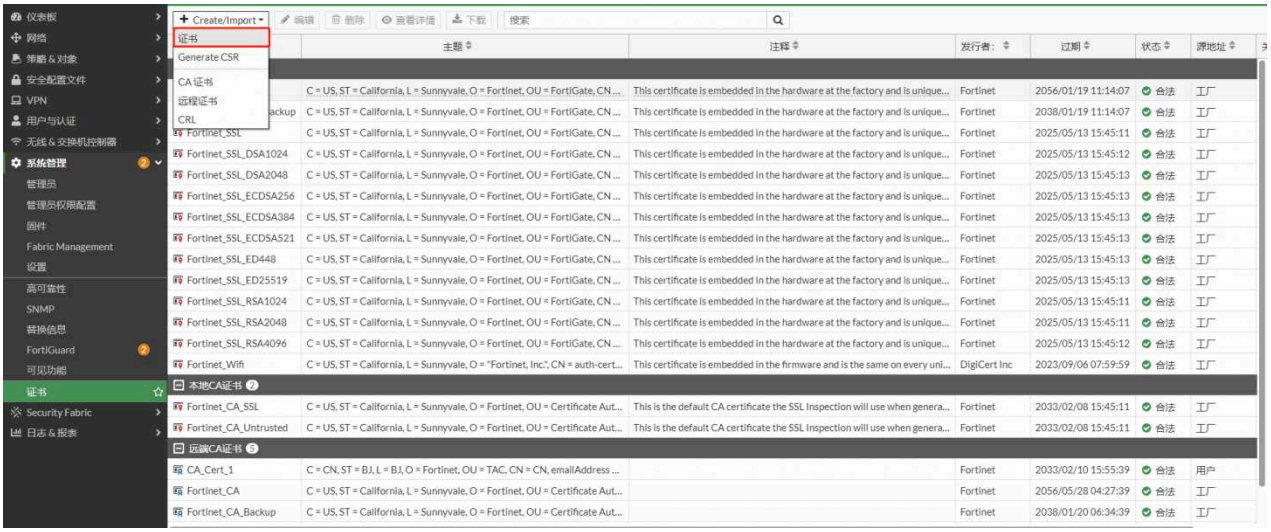
下载证书，文件名是sub_localCA1..p12



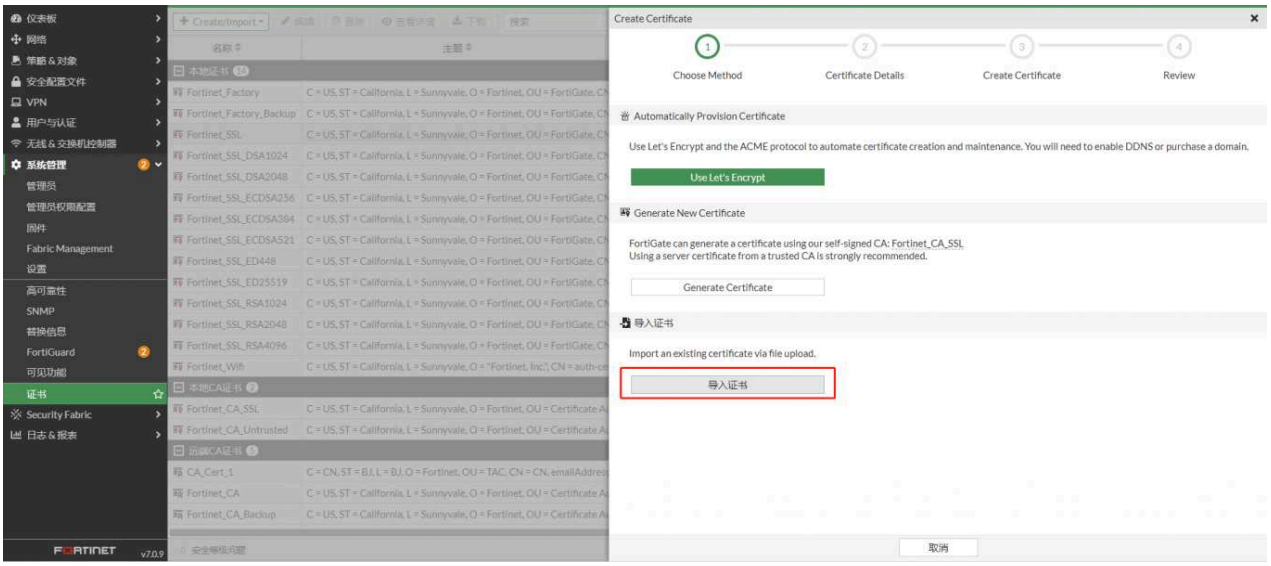
3. 导入FortiGate

选择“系统管理”-->“证书”，点击“Create/Import”，选择“证书”。

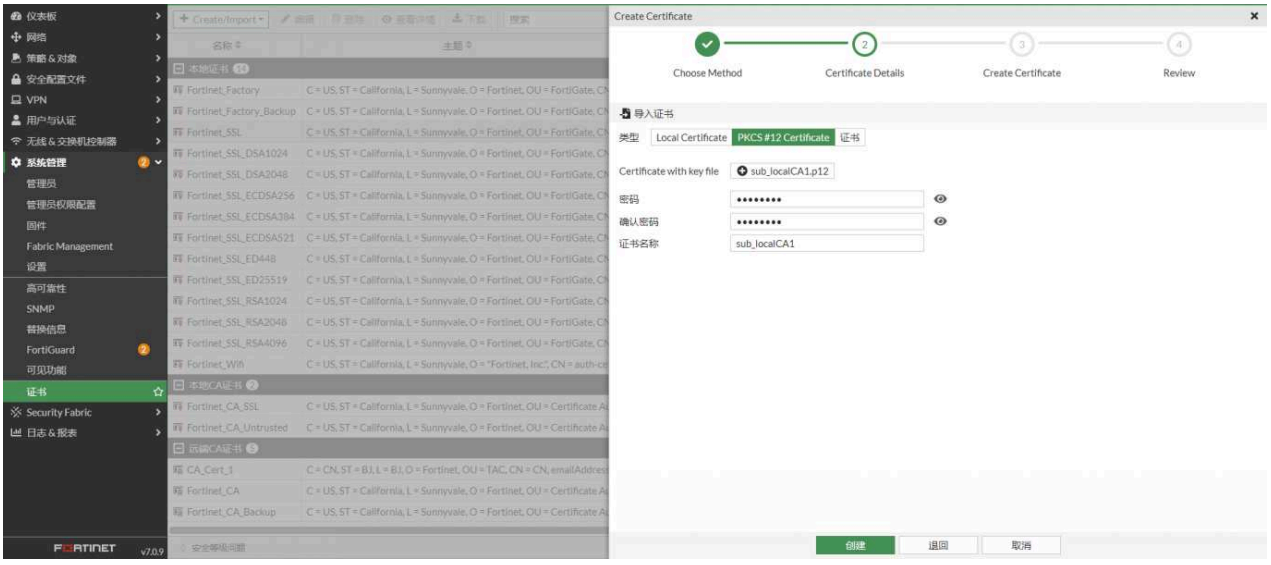
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击”导入证书“。

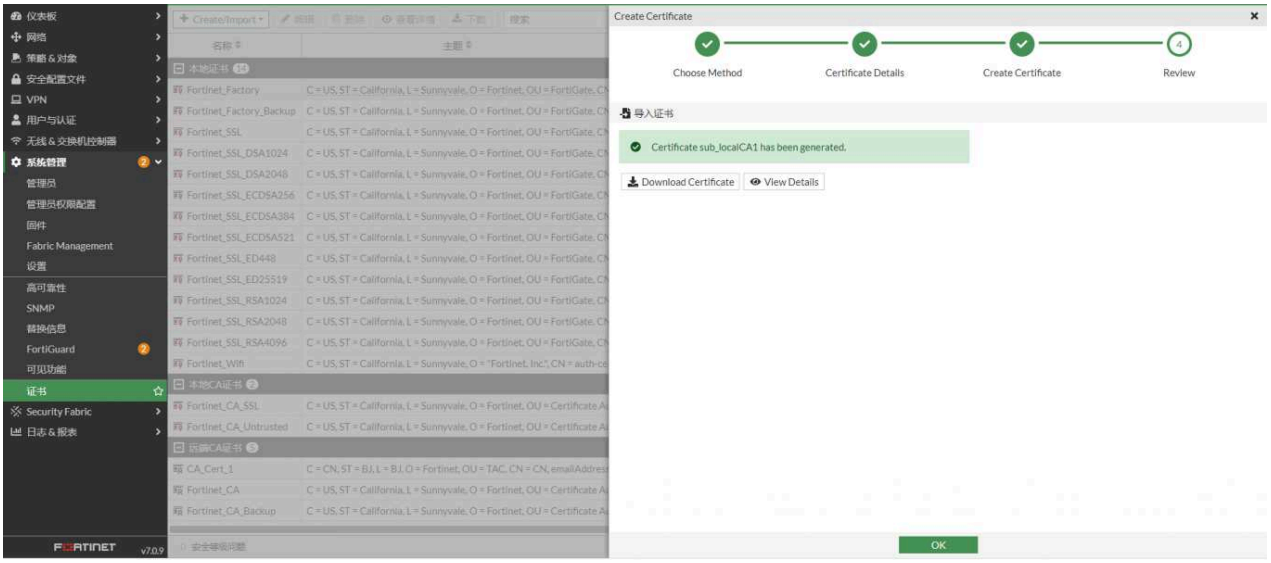


选择”PKCS#12 Certificate“，输入证书的密码，点击”创建“。



导入成功

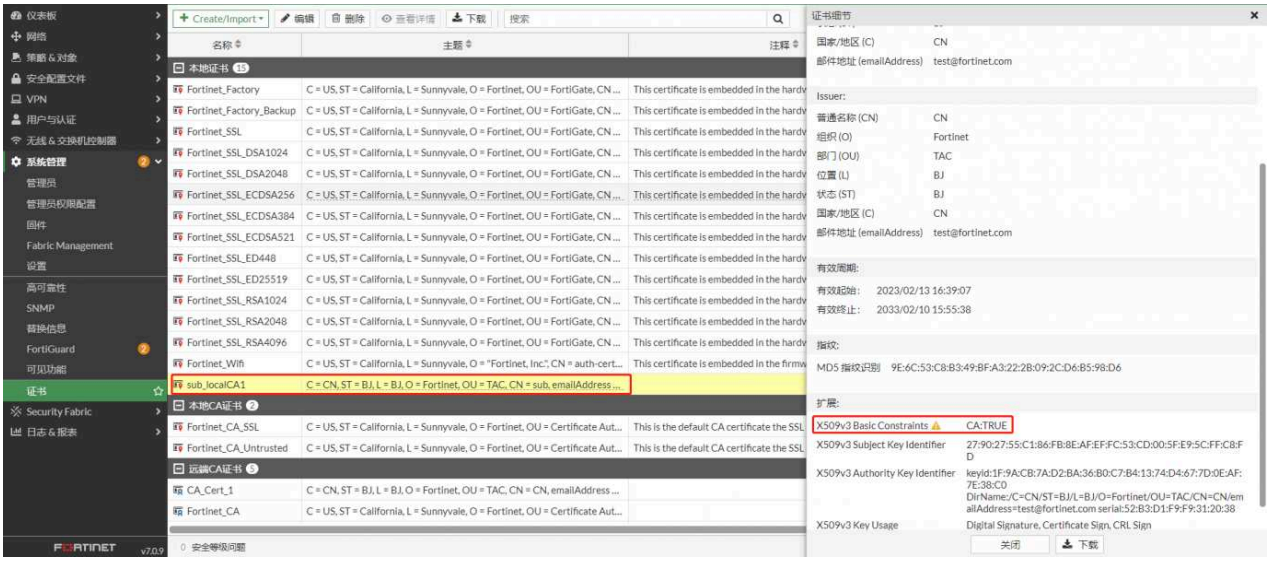
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



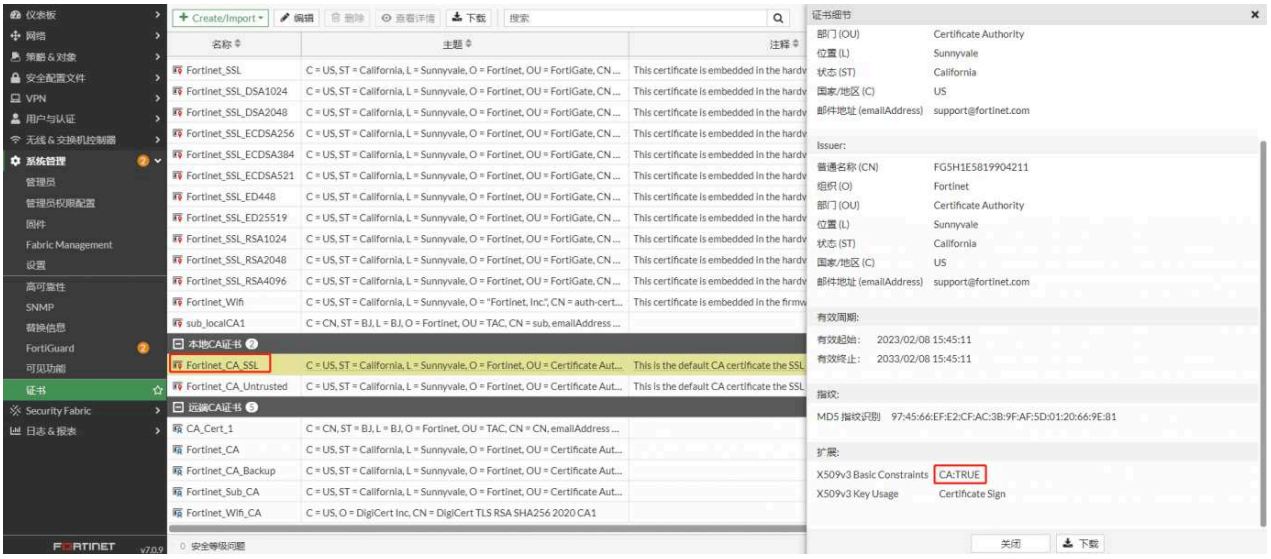
4. 查看导入的证书

可以看到sub_localCA1的具有CA:TRUE，是具有签发能力的CA证书。

sub_localCA1作为本地证书导入，位于本地证书菜单下，但和本地CA证书Fortinet_CA_SSL的作用是一样的。



Fortinet_CA_SSL是具有签发能力的CA证书



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

本地证书

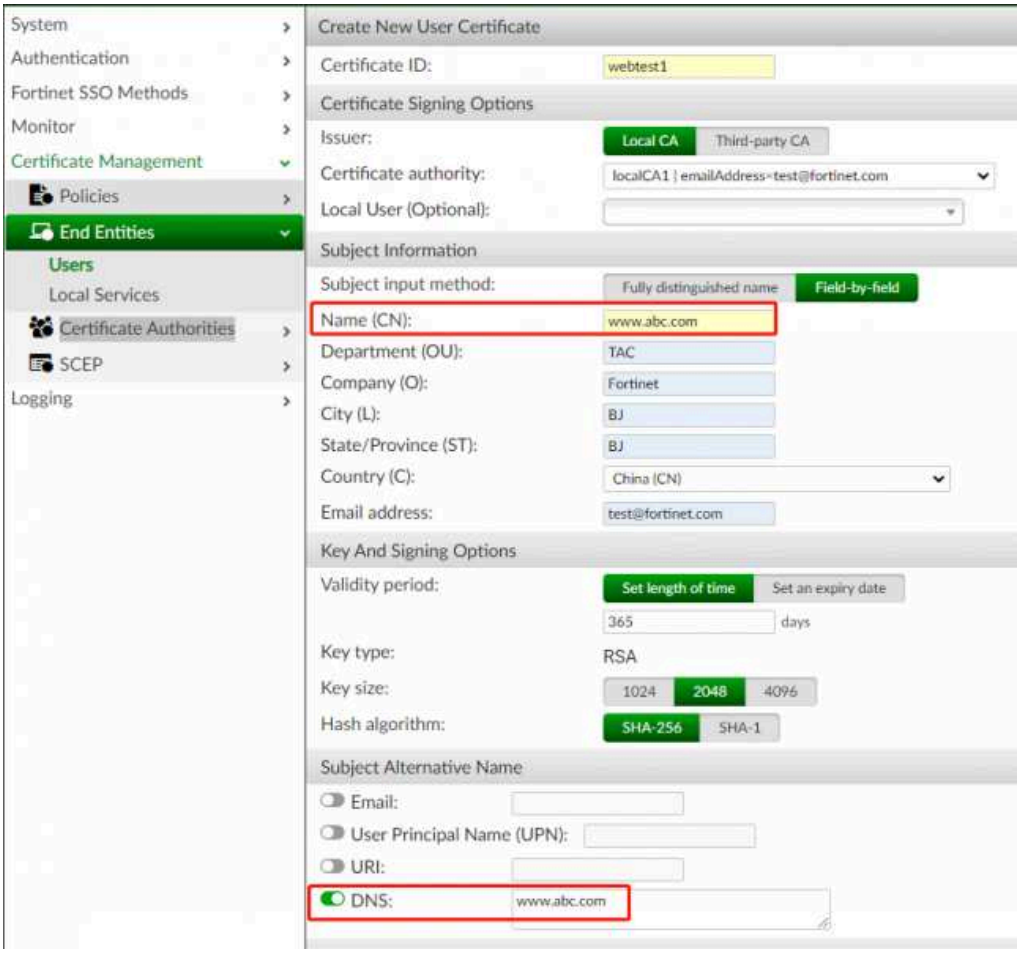
本地证书是具有公钥和私钥，为特定的服务颁发的证书，如FortiGate GUI，SSLVPN，IPSEC VPN证书。

1. **FortiAuthenticator生成用户证书**

选择“Certicate Managerment”-->“End Entities”-->”Users“，点击“Create New”，输入证书名称及证书信息，指定签发的根CA，点击“确认”。

CN：当浏览器尝试连接到远程服务器(例如HTTPS服务器)时，它将首先获取该服务器的SSL证书。 然后将要连接的域名与SSL证书中的CN进行比较。 如果它们相同，它将使用SSL证书来加密连接，否则将告警。

SAN：单个SSL证书只能使用单个Common Name，意味着SSL证书可用于单个主机名+域名。 为了解决此限制，创建了Subject Alternative Name 。 SAN用于在SSL证书中定义多名称或多通用名称。这里SAN和CN配置为一样即可。



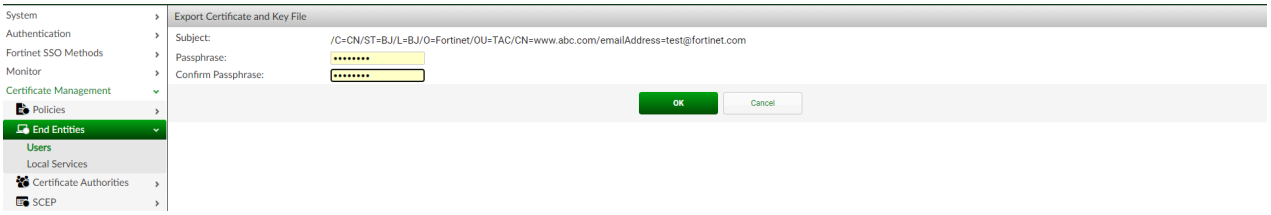
2. **导出用户证书公钥和私钥**

点击”Export Key and Cert“。



输入证书保护的密码。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

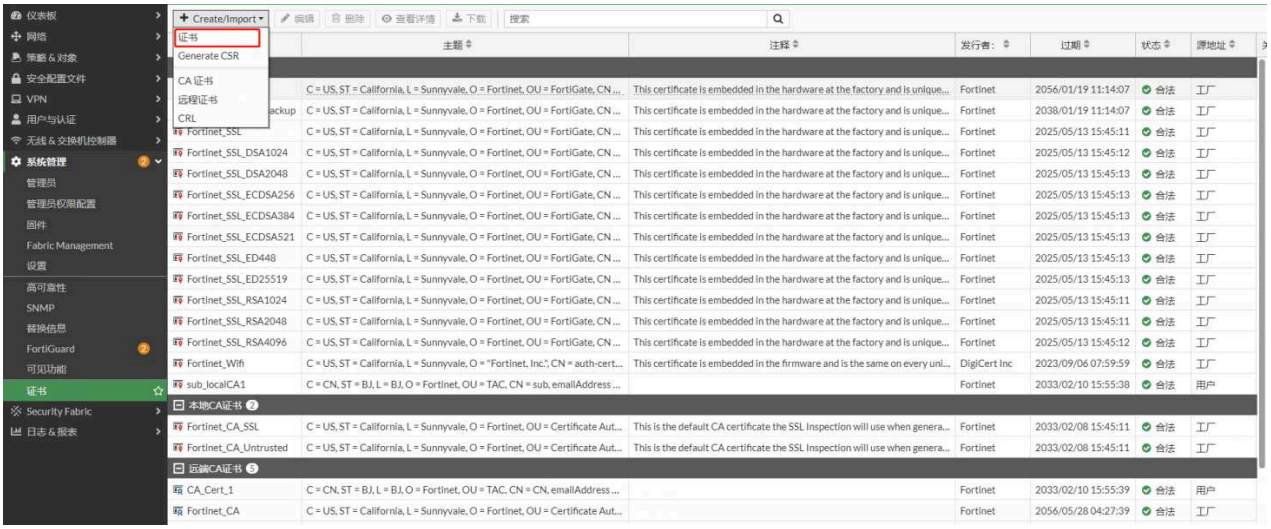


导出证书，名称是webtest1.p12。

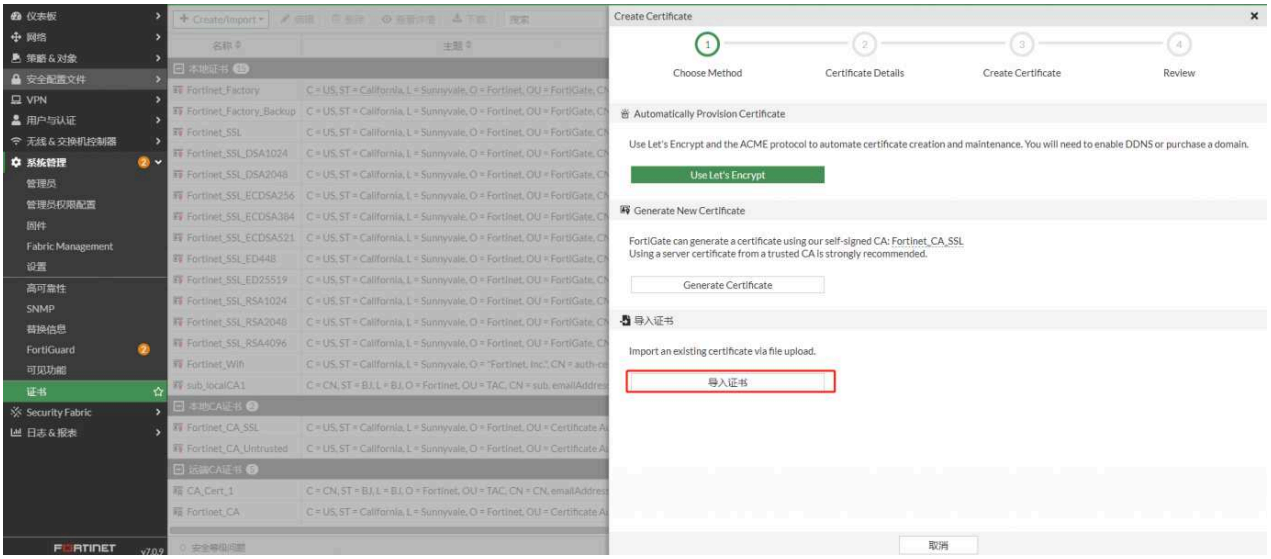


3. 导入FortiGate

选择“系统管理”-->“证书”，点击“Create/Import”，选择“证书”。

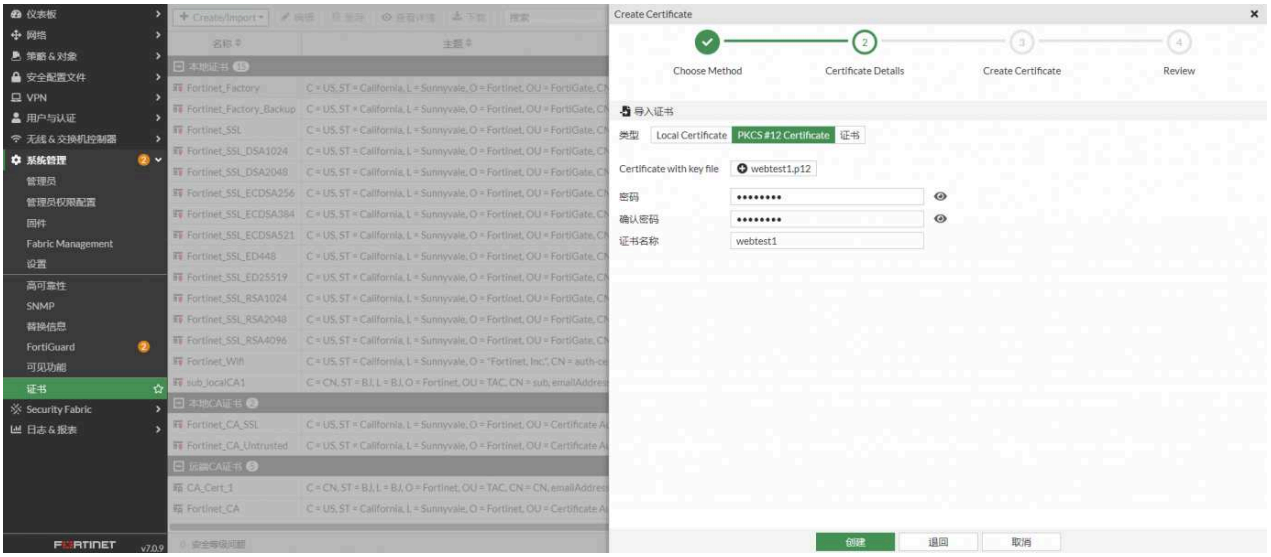


选择”导入证书“。

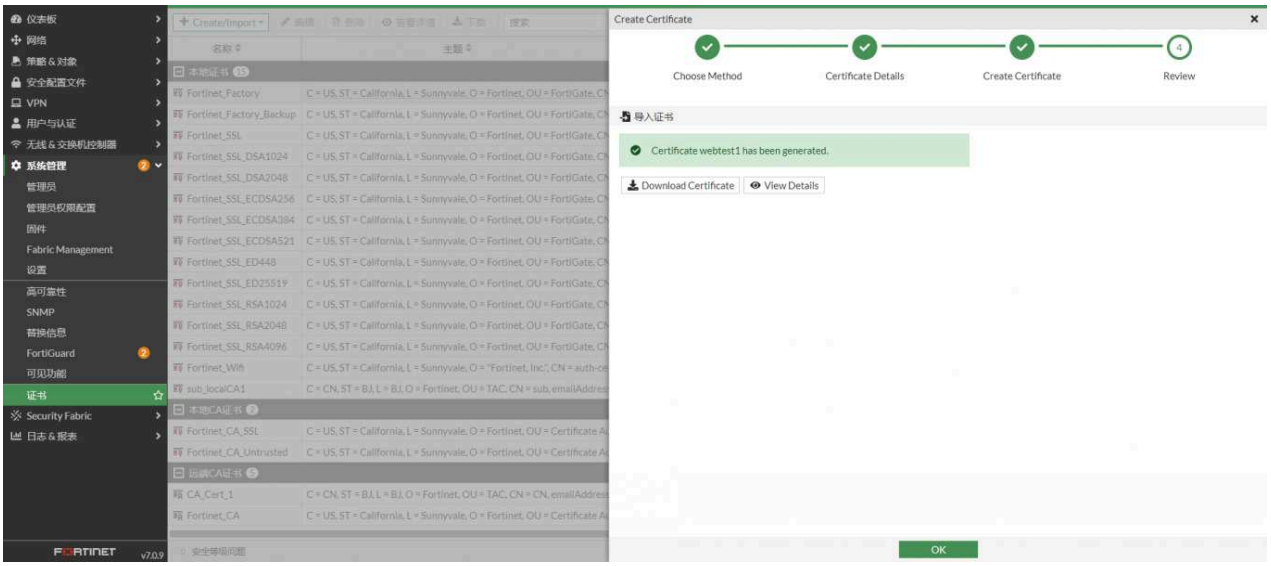


选择”PKCS#12 Certificate“，输入证书的密码，点击”创建“。

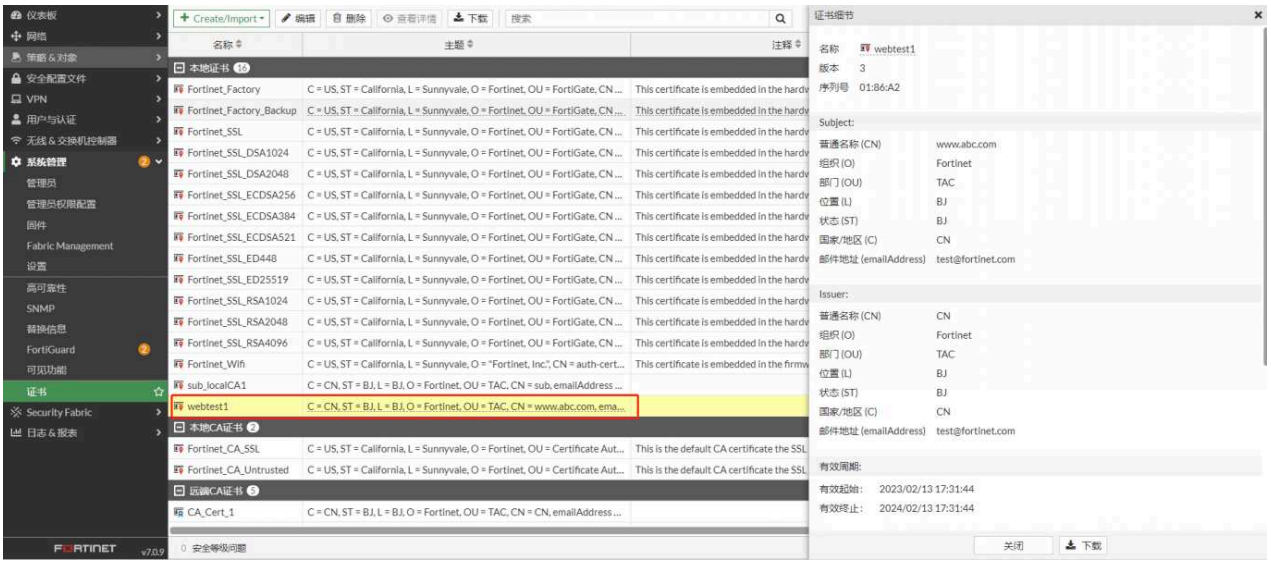
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



导入成功。y



4. 查看证书



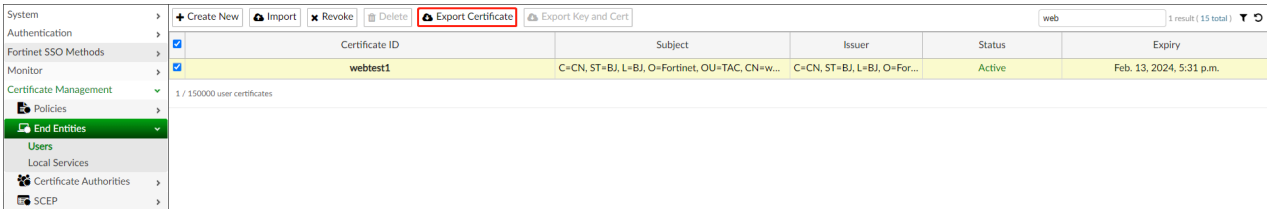
远程证书

远程是没有私钥的证书，用于验证私钥的签名，如SAML证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

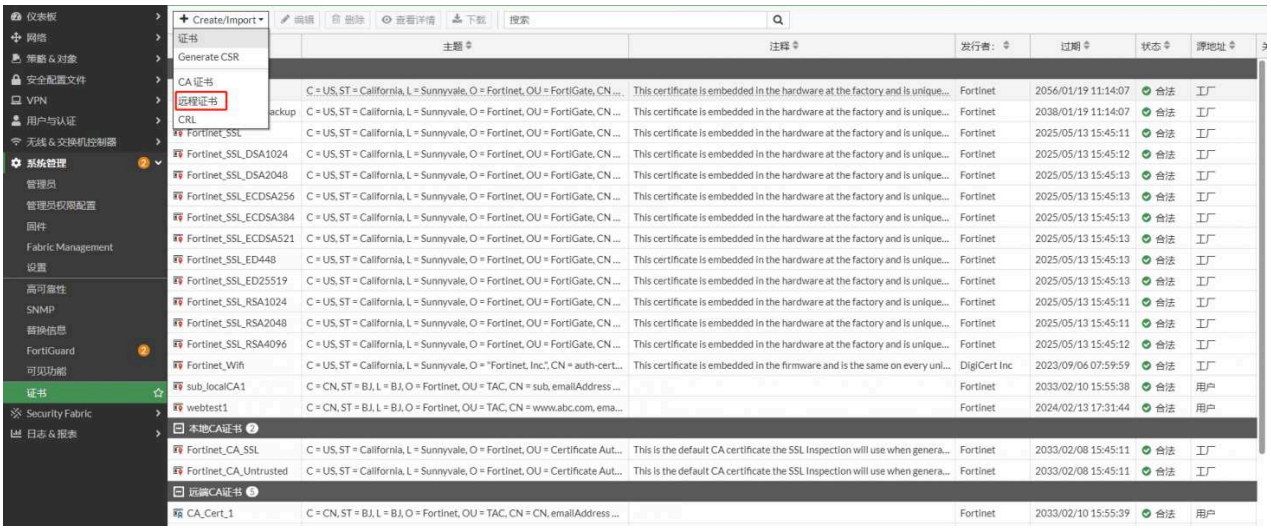
1. 导出证书

以webtest1证书为例。点击”Export Certificate“导出证书，文件名为webtest1.cer。

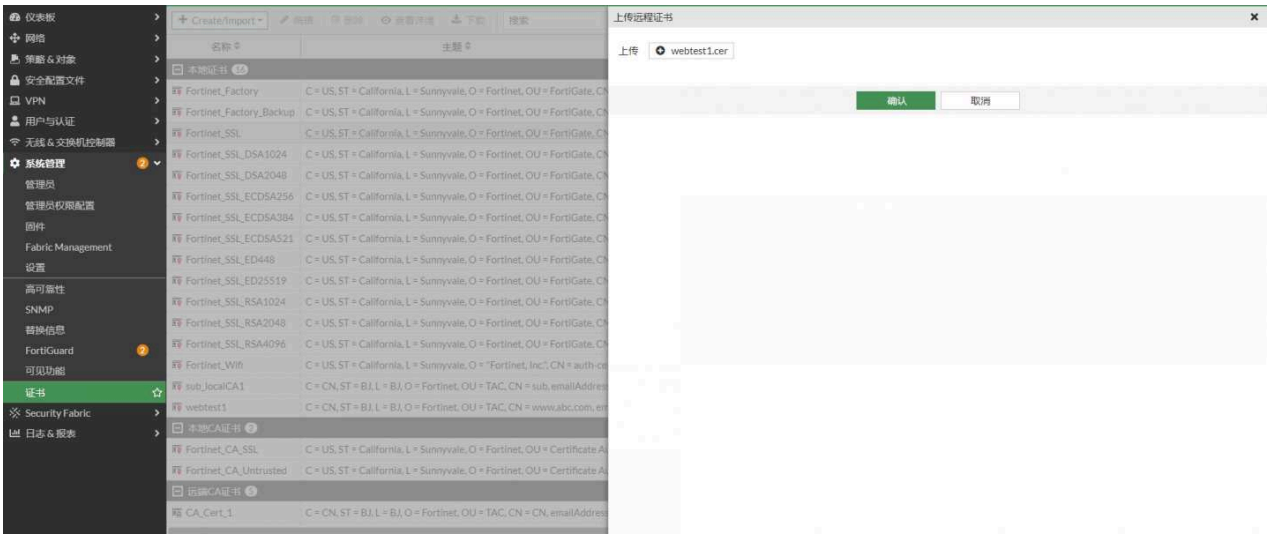


2. 导入FortiGate

选择“系统管理”-->“证书”，点击“Create/Import”，选择“远程证书”。

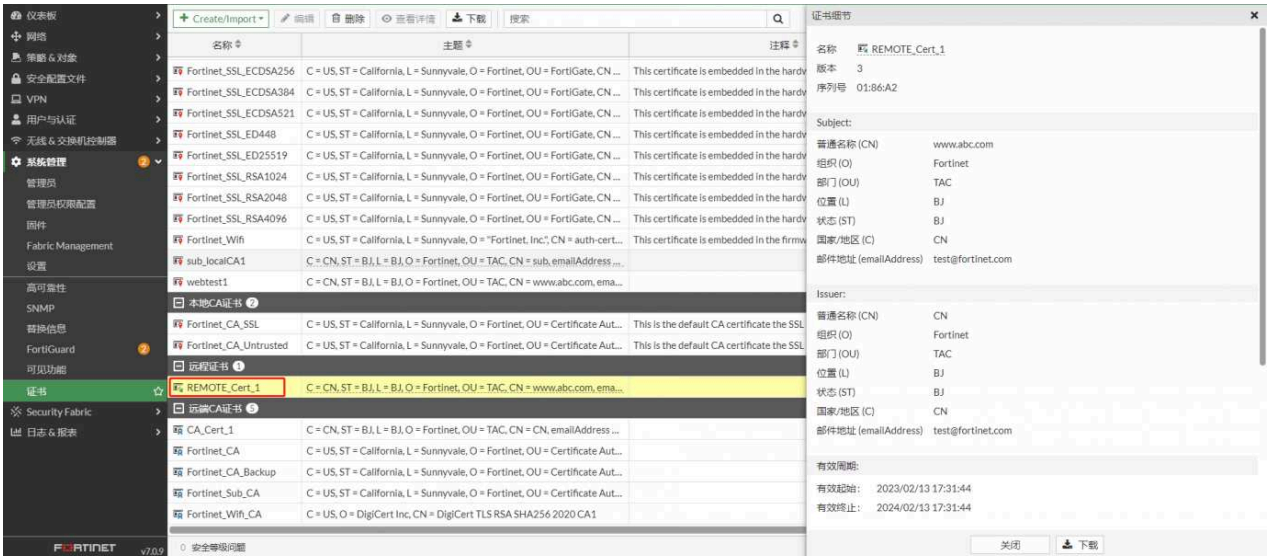


上传”webtest1.cer“。



3. 查看证书

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Email服务

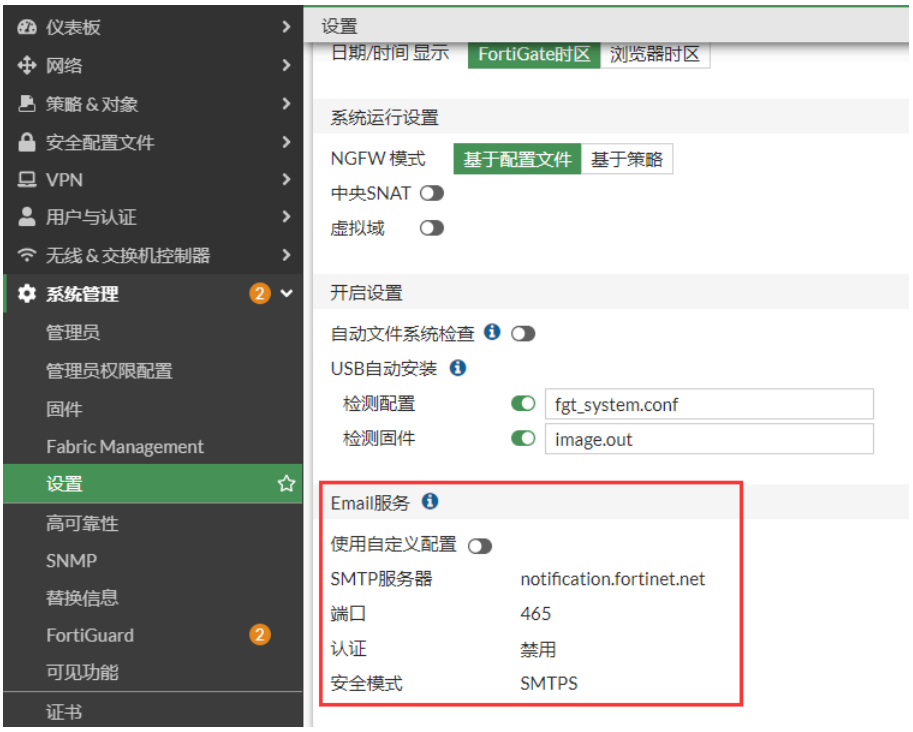
简介

Email服务用于FortiGate发送的电子邮件，包括警报电子邮件，FortiToken激活以及automation stitch邮件。FortiGate有一个默认的SMTP服务器notifation.fortinet.net ↗，用于提供安全的SMTP邮件服务，也支持自定义的邮件服务。

默认的SMTP服务器

FortiGate默认的SMTP服务器配置如下图，无需修改，确保FortiGate能够连接STMP服务器，即FortiGate能够上网。

在6.4.12，7.0.10，7.2.4中，FortiGate发件箱地址是DoNotReply@notification.fortinet.net，“缺省回复至”选项已移除，该选项与发件箱一致，这样是为了避免被对端邮件服务器当成垃圾邮件给丢弃。

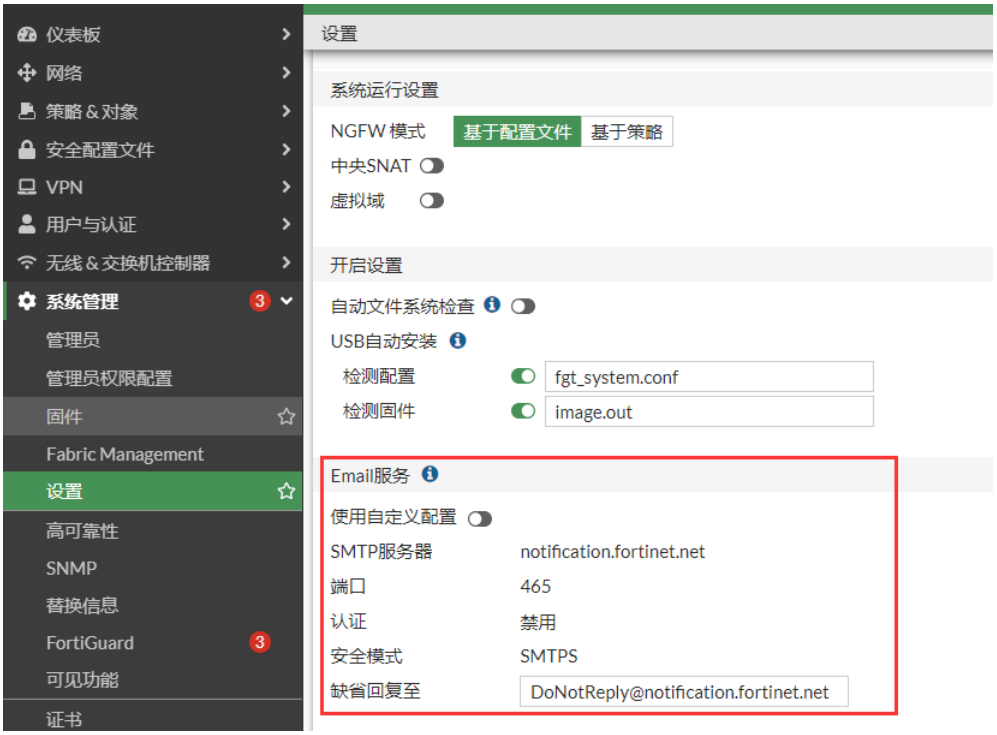


邮件发送的明细如下：

```
Date: Fri, 2 Dec 2022 11:35:33 +0800
From: DoNotReply@notification.fortinet.net
Message-Id: <1669952133.28@notification.fortinet.net>
Reply-To: "DoNotReply" <DoNotReply@notification.fortinet.net>
To: xxxxxx@test.com
Subject: Test
```

在之前的版本中，“缺省回复至”选项需要单独填写，请设置为“DoNotReply@notification.fortinet.net”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



自定义的STMP服务器

163邮件服务器

1. 在163邮件中，开启POP3/SMTP服务，点击“开启”。



在弹出框中点击“继续开启”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



手机微信扫码发送短信，当发完后，点击“我已发送”。



然后就可以获取到“授权码”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



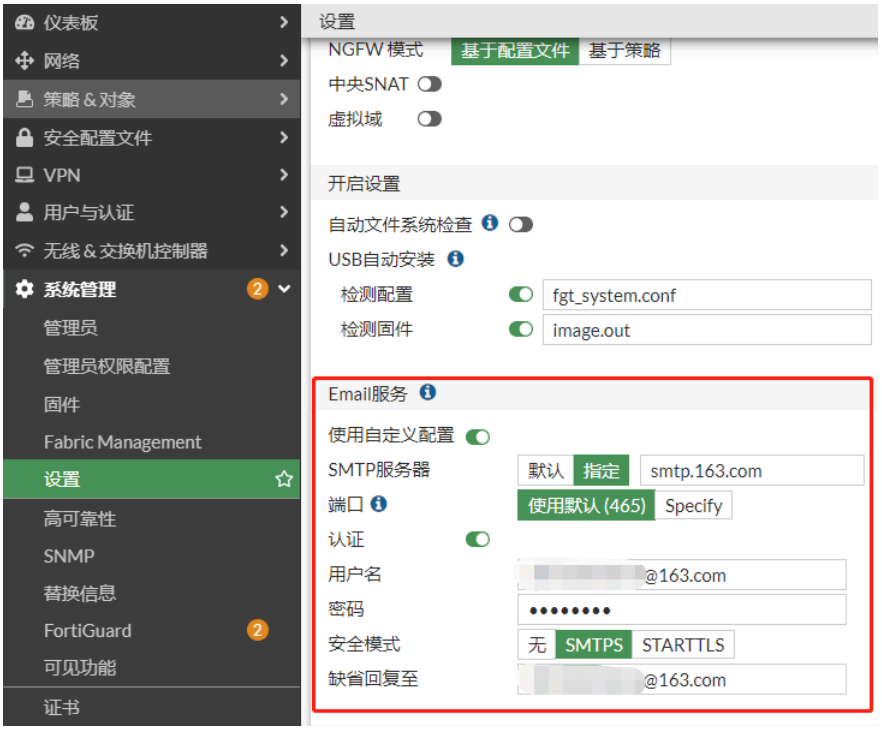
POP3/SMTP服务开启成功。



2. Email服务设置

163的SMTP服务器是smtp.163.com ↗，用户名是163的邮箱账号，密码是授权码（不是163邮箱密码），安全模式为SMTPS，缺省回复至是163的邮箱账号。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



QQ邮件服务器

1. 在QQ邮箱中，点击“账户”，开启“POP3/SMTP服务”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



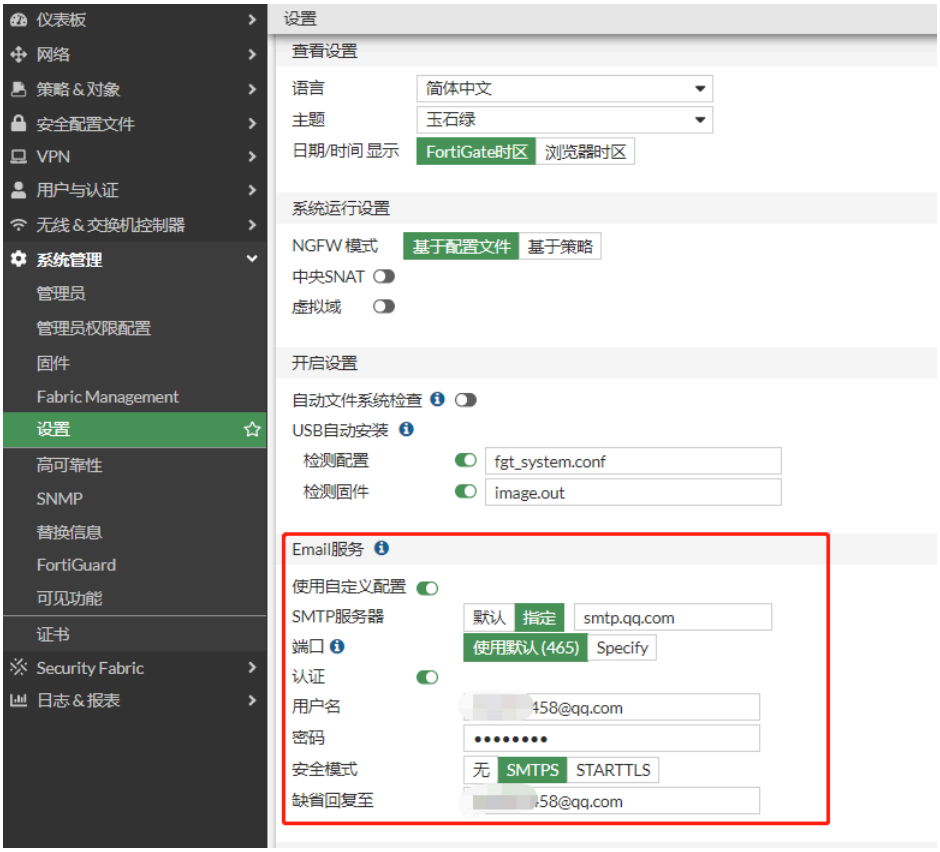
然后点击“生成授权码”，按照提示的步骤拿到授权码。



2. Email服务设置

QQ的SMTP服务器是smtp.qq.com ↗，用户名是qq的邮箱账号，密码是授权码（不是qq密码），安全模式为SMTPS，缺省回复至是qq的邮箱账号。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



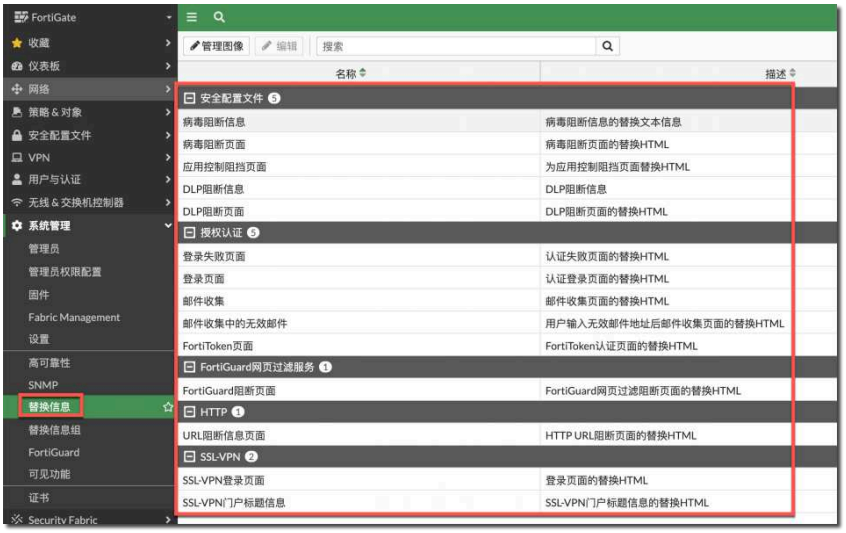
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

页面替换

功能介绍

FortiOS可以自定义部分用户页面样式，以满足用户的个性化需求。可以修改内容的内容包括HTML、文本信息和图片Logo。

可替换资源的页面如下：



修改替换信息

> **重要**
>
> “替换消息”页面有两个视图。简单查看视图（默认）显示最常用的替换消息。扩展查看视图显示所有替换消息类别。

在GUI修改

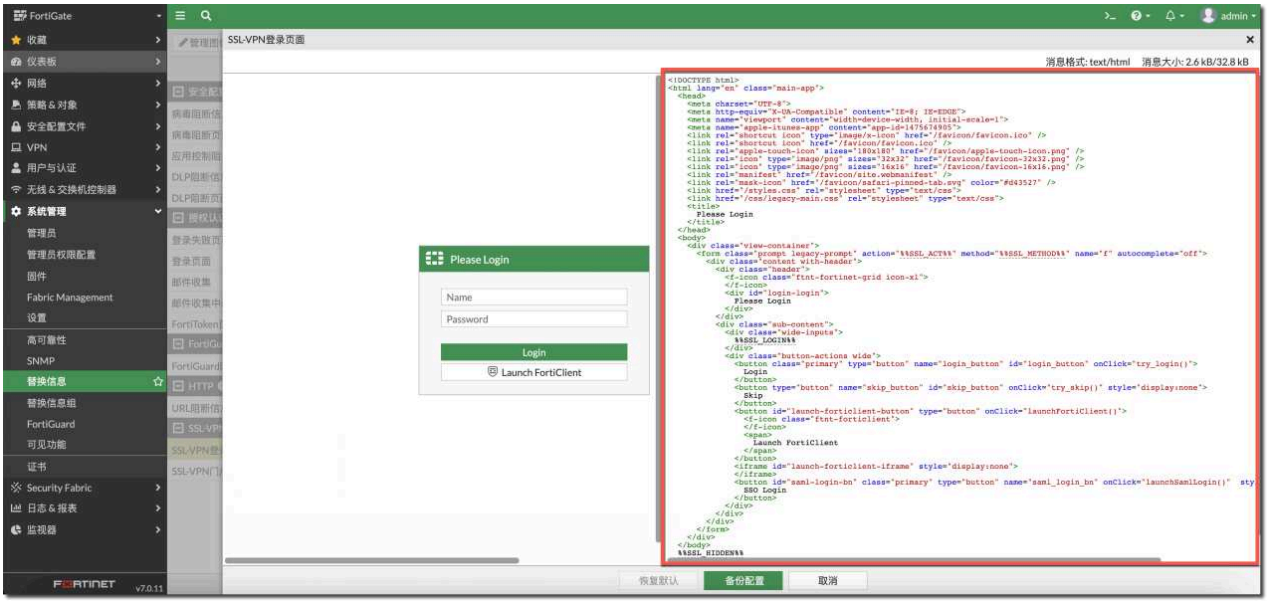
1. 进入“系统管理→替换信息”页面， 编辑某个替换信息。

> **重要**
>
> 如果没有找到要编辑的替换消息条目，请单击右上角的扩展查看视图。



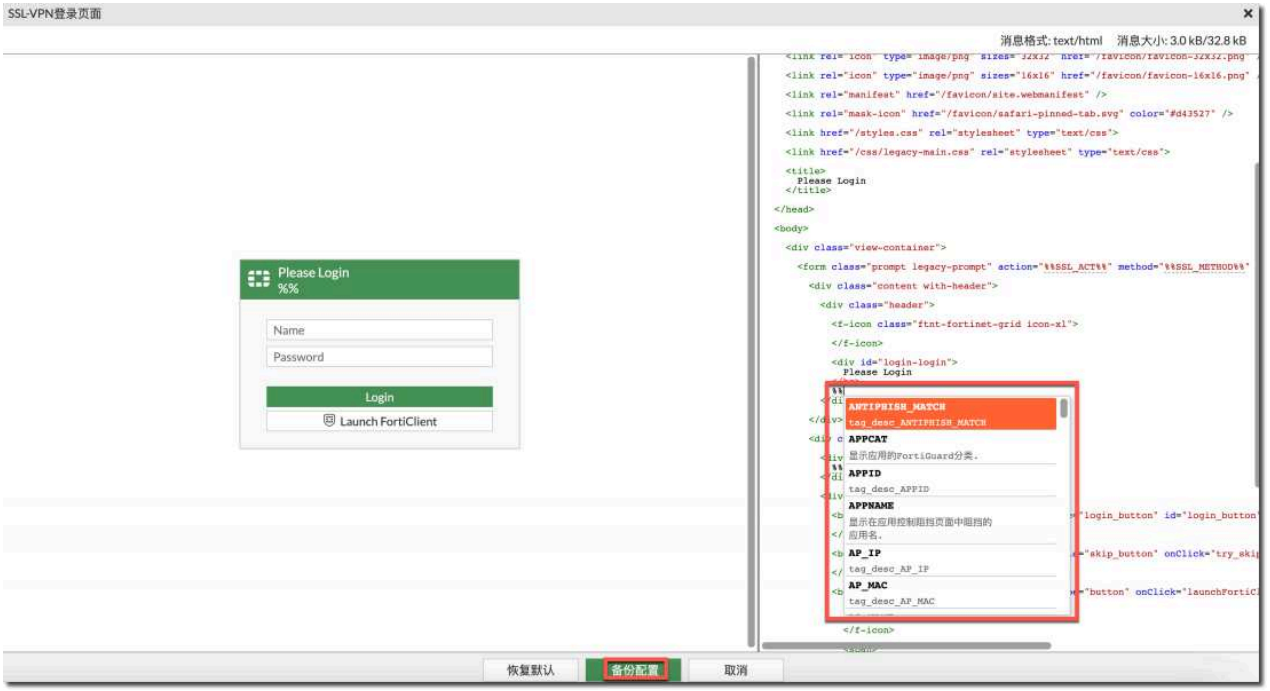
2. 在右侧修改HTML内容，左侧可以实时预览修改结果。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 需要将变量添加到代码时，右键单击并选择插入标记，或键入%%查看可用变量列表，也可以键入变量名称然后按Enter或Tab键自动完成变量名称，修改完成后，点击“备份配置”按钮下发配置。

> **重要**
>
> 点击“恢复默认”按钮可以将HTML恢复为出厂状态。



CLI替换

例如想要修改“流量限制超限页面”（限速超速）的HTML内容，使用如下命令：

```
config system replacemsg traffic-quota "per-ip-shaper-block"
    set buffer "<html>
  <head>
    <title>
      Traffic Quota Control
    </title>
  </head>
  <body>
    <font size=2>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
      <table width=\"100%\">
        <tr>
          <td bgcolor=#3300cc align=\"center\" colspan=2>
            <font color=#ffffff>
              <b>
                Traffic blocked because exceeded session quota
              </b>
            </font>
          </td>
        </tr>
      </table>
      <br>
      <br>
      Traffic blocked because it exceeded the per IP shaper session quota. Please contact the system administrator.
      <br>
      %%QUOTA_INFO%%
      <br>
      <br>
      <hr>
    </font>
  </body>
</html>"
    set header http
    set format html
end
```

修改替换图片

可以替换以下位置的图片：

- 免责声明页面（Disclaimer page）
- 拒绝免责声明页面（Declined disclaimer page）
- 登录页面（Login page）
- 登录失败页面（Login failed page）
- 登录要求页面（Login Challenge Page）
- 保持存活页面（Keepalive page）

GUI替换

1. 进入“系统管理→替换信息”页面，点击“管理图像”按钮。



2. 在弹出的图片管理中，点击新建按钮。

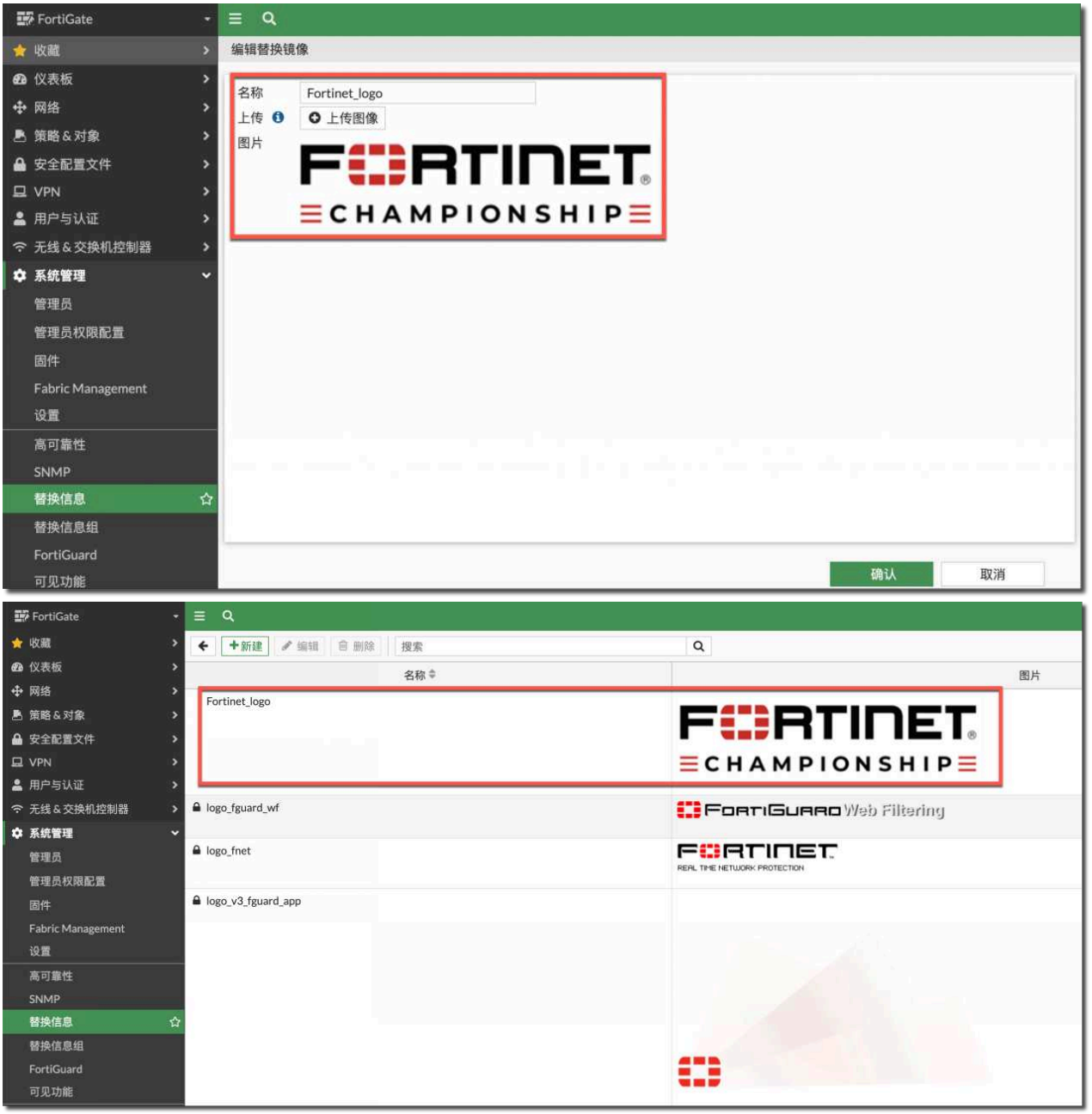
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置图片名称，并上传图片。

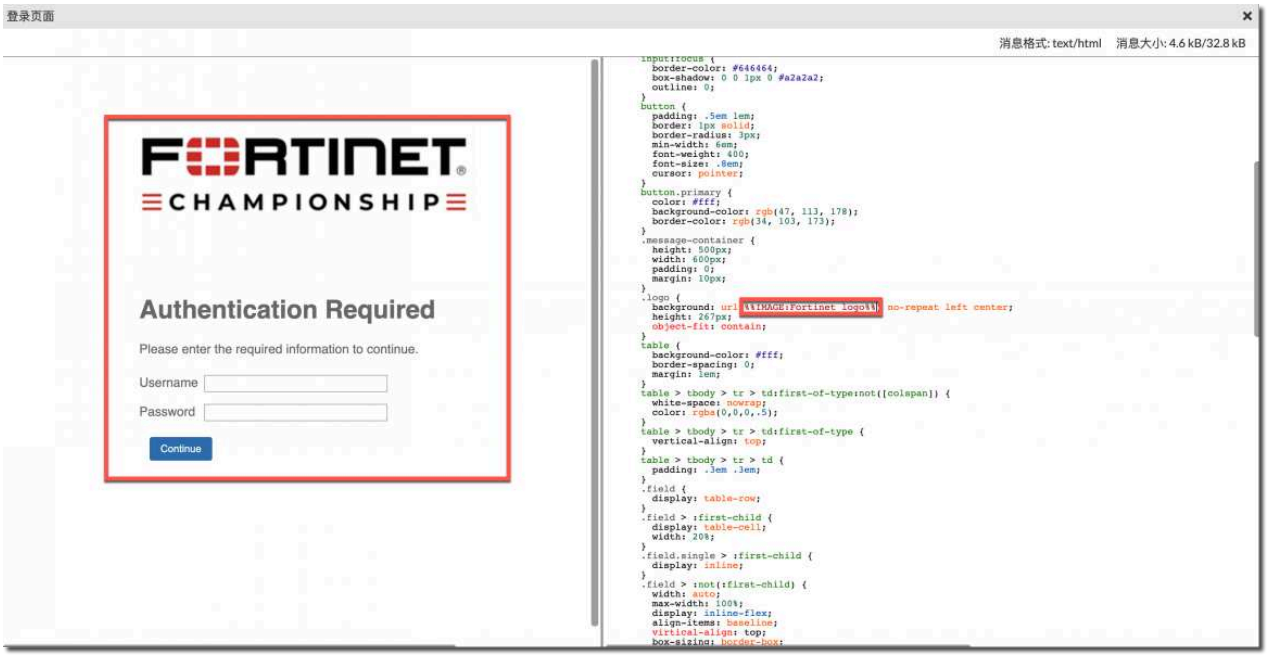
> **重要**
>
> 支持的图像格式为GIF、JPEG、TIFF和PNG，支持的最大文件大小为24 KB。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 进入“系统管理→替换信息”页面，编辑要替换图片的替换信息，右键单击要添加图像的消息代码，然后选择“插入图像”，选择上步上传的图片，并双击选择，左侧的预览可以看到替换的Logo。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



CLI替换

使用图片的Base64编码通过CLI替换图片，图片的Base64信息可以通过在线转换方式获取（如https://tool.chinaz.com/tools/imgtobase ↗ ）。

```
config system replacemsg-image
    edit <image_name>
        set image-type {gif | jpg | tiff | png}
        set image-base64 <string>
    next
end
```

替换信息组

使用上述替换信息可以对所有的相关页面资源进行内容替换，但无法基于每个认证策略、UTM profile、自动化邮件等配置进行个性化定制，而替换信息组可以实现此需求。当认证策略、UTM profile等配置引用策略信息组时，“替换信息组”中的替换内容优先于“替换信息”功能中配置的替换内容。

替换信息组类型	用途	替换资源
安全（utm）	在防火墙策略中引用的UTM配置文件、SSL VPN等页面	admin alertmail custom-message fortiguard-wf ftp http icap mail nac-quar spam sslvpn traffic-quota utm webproxy
认证（auth）	防火墙策略中开启的认证页面	auth webproxy

配置举例

1. 在GUI界面开启“替换信息组”功能的显示。

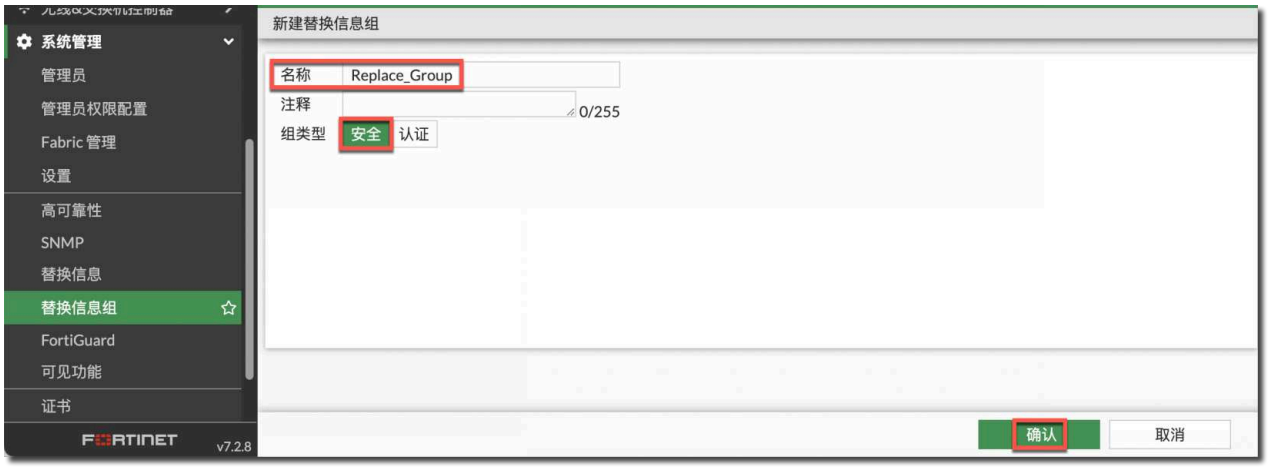
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system settings
    set gui-replacement-message-groups enable
end
```

2. 进入FortiGate的“系统管理→替换信息组”页面，点击“新建”按钮。



3. 配置替换信息组名称，“组类型”选择“安全”，点击“确认”按钮下发配置。



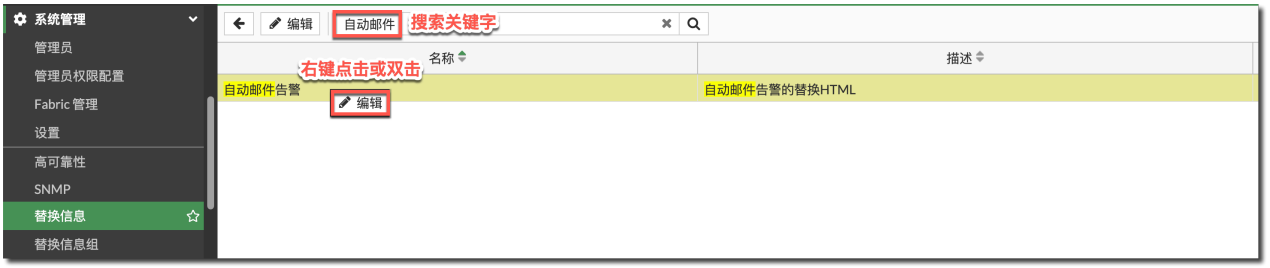
4. 右键点击新建的替换信息组，点击“编辑”按钮（或双击编辑）。



5. 搜索关键字“自动邮件”，找到“自动邮件告警”条目，右键或双击编辑该条目。

> **重要**
>
> 替换信息组中也包含其他功能模块页面的替换信息，当用户需要替换多个功能模块的页面信息时，可以使用此功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 在HTML编辑页面，将想要添加的告警图片URL添加到`message-container`部分，如下图所示（`<img src="https://www.fortinet.com/content/dam/fortinet/images/icons/benefits/icon-wireless-fortinet-ips.svg" alt="Fortinet Logo"/>`），左侧的预览可以正常显示该图片，点击“备份配置”按钮保存配置。

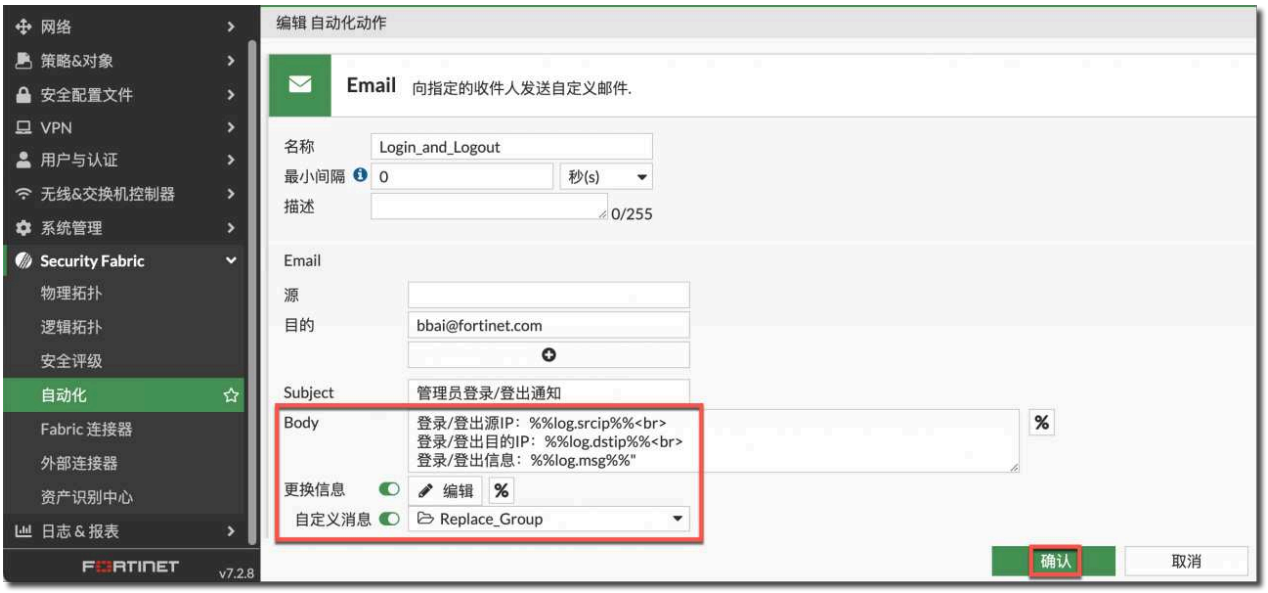



```bash
config system replacemsg-group
    edit "Replace_Group"
        set comment ''
        set group-type utm
        config automation
            edit "automation-email"
                set buffer "<!DOCTYPE html>
<html lang=\"en\">
 <head>
 <meta charset=\"UTF-8\">
 <meta http-equiv=\"X-UA-Compatible\" content=\"IE=8; IE=EDGE\">
 <meta name=\"viewport\" content=\"width=device-width, initial-scale=1\">
 <link href=\"https://fonts.googleapis.com/css?family=Roboto&display=swap\" rel=\"stylesheet\">
 <style>
 body {
 height: 100%;
 font-family: Roboto, Helvetica, Arial, sans-serif;
 margin: 0;
 display: flex;
 align-items: center;
 justify-content: center;
 }
 .message-container{
 margin: 0 auto;
 max-width: 580px;
 }
 .email-body {
 line-height: 1.5em;
 }
 </style>
 </head>
 <body>
 <div class=\"message-container\">
 <img src=\"https://www.fortinet.com/content/dam/fortinet/images/icons/benefits/icon-wireless-fortinet-ips.svg\"
alt=\"Fortinet Logo\"/>
 <h1>
 Security Fabric Automation
 </h1>
 <h3>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
 %%AUTOMATION_FGT_SERIAL%%: %%AUTOMATION_STITCH_NAME%%
 </h3>
 <div class=\"email-body\">
 %%AUTOMATION_EMAIL_BODY%%
 </div>
 </div>
 </body>
</html>
"
                set header http
                set format html
            next
        end
    next
end
```

7. 进入FortiGate的“Security Fabric→自动化→操作”页面，编辑自动邮件动作。开启“更换信息”选项，然后开启“自定义消息”选项，并选择上步创建的替换信息组。注意由于调用了替换信息组（HTML格式），所以需要在“Body”中每行加入HTML换行符 `<br>` 。点击“确认”按钮下发配置。




```
config system automation-action
    edit "Login_and_Logout"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "管理员登录/登出通知"
        set message "登录/登出源IP：%%log.srcip%%<br>
登录/登出目的IP：%%log.dstip%%<br>
登录/登出信息：%%log.msg%%\""
        set replacement-message enable
        set replacemsg-group "Replace_Group"
    next
end
```

bash

其他功能引用

1. 在WebFilter配置文件中引用，所有被此WebFilter阻断返回的页面会被替换为替换信息组newutm中配置的内容。

```
config webfilter profile
    edit "default"
        set replacemsg-group "newutm"
    next
end
```

bash

2. 在防火墙策略中引用，所有匹配该策略的认证用户的页面会被替换为替换信息组newauth中配置的内容。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall policy
    edit 1
        ...
        set replacemsg-override-group "newauth"
        ...
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

登录提示信息

在Web/SSH管理用户登录前和登录后都可以弹出提示信息，以展示警告信息，这些提示信息可以在替换信息页面进行自定义。

配置步骤

1. 在CLI下开启登录前或登录后的的提示信息。

```
config system global
    set pre-login-banner enable
    set post-login-banner enable
end
```

2. 默认情况下，登录前和登录后提示信息均为英文。





3. 可以在替换信息页面对这两种提示信息进行自定义，进入“系统管理→替换信息”页面，右上角切换到拓展查看，搜索“登录”，找到管理员设置中的登录前免责信息和登录后免责信息。



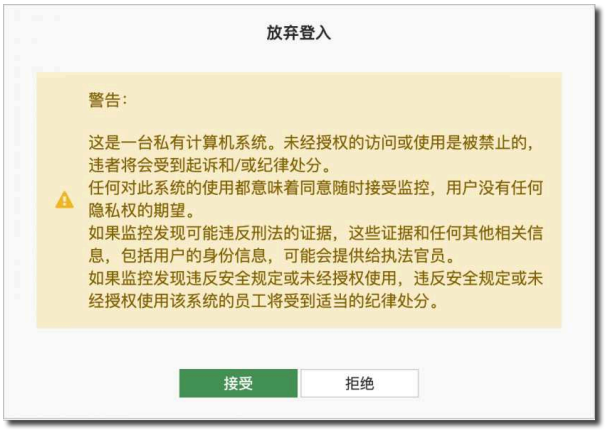
4. 编辑登录前或登录后免责信息配置，右侧填写自定义的提示内容，左侧显示预览信息，填写完成后点击备份配置按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



结果验证

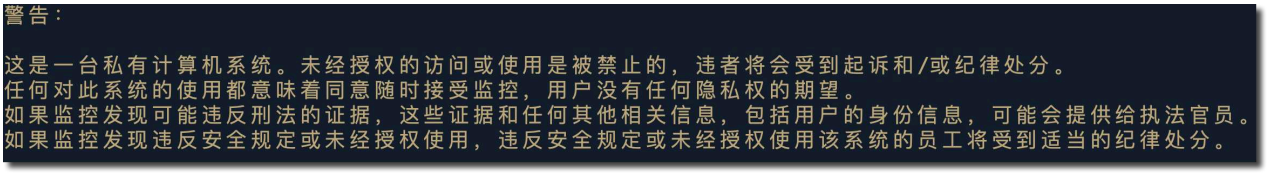
1. 使用Web方式登录FortiGate，在登录前，就会弹出告警信息。



2. 点击接受继续登录，登录完成后，弹出登录后的告警信息。



3. 使用SSH登录FortiGate，在登录前，就会弹出告警信息。



4. 登录完成后，提示登录后的告警信息，键盘键入a后登录成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
警告：

设备承载重要业务，请勿随意修改设备配置，重大操作前请务必备份配置文件！

(Press 'a' to accept):

FortiGate #
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

常用基础命令

命令结构

```
config      Configure object.                          对策略，对象等进行配置
get         Get dynamic and system information.        查看相关关对象的参数信息
show        Show configuration.                        查看配置文件
diagnose    Diagnose facility.                         诊断命令
execute     Execute static commands.                   常用的工具命令，如 ping
exit        Exit the CLI.                              退出
```

常用命令

常用配置命令

1. 配置接口地址

```
FortiGate # config system interface
FortiGate (interface) # edit lan
FortiGate (lan) # set ip 192.168.100.99/24
FortiGate (lan) # end
```

2. 配置静态路由

```
FortiGate # config router static
FortiGate (static) # edit 0                   //“ 0 ”系统自动分配路由条目的序号
FortiGate (0) # set device wan1               //出接口
FortiGate (0) # set dst 10.0.0.0 255.0.0.0    //目的网段
FortiGate (0) # set gateway 192.168.57.1      //网关IP
FortiGate (0) # end
```

3. 配置默认路由

```
FortiGate # config router static
FortiGate (static) # edit 0
FortiGate (0) # set gateway 192.168.57.1
FortiGate (0) # set device wan1
FortiGate (0) # end
```

4. 添加IP地址对象

```
FortiGate # config firewall address
FortiGate (address) # edit clientnet
new entry 'clientnet' added
FortiGate (clientnet) # set subnet 192.168.1.0 255.255.255.0
FortiGate (clientnet) # end
```

5. 添加IP池

```
FortiGate# config firewall ippool
FortiGate (ippool) # edit nat-pool
new entry 'nat-pool' added
FortiGate (nat-pool) # set startip 100.100.100.1
FortiGate (nat-pool) # set endip 100.100.100.100
FortiGate (nat-pool) # end
```

6. 添加虚拟IP

```
FortiGate # config firewall vip
FortiGate (vip) # edit webserver
new entry 'webserver' added
FortiGate (webserver) # set extip 202.0.0.167
FortiGate (webserver) # set extintf wan1

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate (webserver) # set mappedip 192.168.0.168
FortiGate (webserver) # end
```

7. 配置上网策略

```
FortiGate # config firewall policy
FortiGate (policy) # edit 1
FortiGate (1)#set srcintf internal     //源接口
FortiGate (1)#set dstintf wan1         //目的接口
FortiGate (1)#set srcaddr all          //源地址
FortiGate (1)#set dstaddr all          //目的地址
FortiGate (1)#set action accept        //动作
FortiGate (1)#set schedule always      //时间
FortiGate (1)#set service ALL          //服务
FortiGate (1)#set logtraffic disable   //日志开关
FortiGate (1)#set nat enable           //开启nat
FortiGate (1)#end
```

8. 配置VIP映射策略

```
FortiGate # config firewall policy
FortiGate (policy) #edit 2
FortiGate (2)#set srcintf wan1      //源接口
FortiGate (2)#set dstintf internal  //目的接口
FortiGate (2)#set srcaddr all       //源地址
FortiGate (2)#set dstaddr ngfw1     //目的地址，虚拟VIP映射，需要先配置好VIP条目才可以被调用
FortiGate (2)#set action accept     //动作
FortiGate (2)#set schedule always   //时间
FortiGate (2)#set service ALL       //服务
FortiGate (2)#set logtraffic all    //日志开关
end
```

常用show命令

1. 查看设备信息、主机名，管理端口

```
FortiGate # show system global
```

2. 查看系统状态信息和当前资源信息

```
FortiGate # get system status
FortiGate # get system performance status
```

3. 查看应用流量统计

```
FortiGate # get system performance firewall statistics
```

4. 查看ARP表

```
FortiGate # get system arp
```

5. 查看arp丰富信息

```
FortiGate # diagnose ip arp list
```

6. 清除ARP缓存

```
FortiGate # execute clear system arp table
```

7. 查看当前会话表

```
FortiGate # diagnose sys session stat
FortiGate # diagnose sys session full-stat
```

8. 查看会话列表

```
FortiGate # diagnose sys session list
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

9. 查看物理接口状态

```
FortiGate # get system interface physical
```

0. 查看默认路由配置

```
FortiGate # show router static
```

1. 查看路由表中的静态路由

```
FortiGate # get router info routing-table static
```

2. 查看OSPF相关配置

```
FortiGate # show router ospf
```

3. 查看全局路由表

```
FortiGate # get router info routing-table all
```

4. 查看HA状态

```
FortiGate # get system ha status
```

5. 查看主备机是否同步

```
FortiGate # diagnose sys ha checksum
```

常用诊断命令

1. IPSec IKE

```
FortiGate # diagnose debug application ike -1
FortiGate # diagnose debug enable
```

常用execute命令

```
FortiGate #execute  ping  8.8.8.8                          //常规ping操作
FortiGate #execute  ping-options source  192.168.1.200    //指定ping数据包的源地址 192.168.1.200
FortiGate #execute  ping  8.8.8.8                          //继续输入ping的目标地址，即可通过192.168.1.200的源地址执行ping操
作
FortiGate #execute  traceroute   8.8.8.8
FortiGate #execute  telnet 2.2.2.2      //进行telnet访问
FortiGate #execute  ssh  2.2.2.2        //进行ssh 访问
FortiGate #execute  factoryreset        //恢复出厂设置
FortiGate #execute  reboot              //重启设备
FortiGate #execute  shutdown            //关闭设备
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

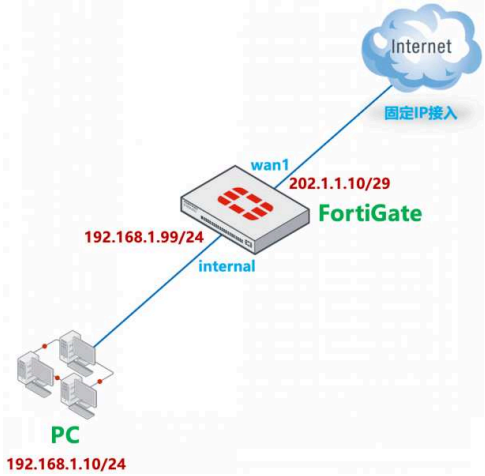
静态地址上网配置

网络需求

外网接口使用静态IP，由运营商分配指定的静态地址，内网为192.168.1.0/24网段，实现基本上网功能。

网络拓扑

假设运营商分配的地址如下，网段：202.1.1.8/29，分配IP地址：202.1.1.10，网关地址：202.1.1.9，DNS：202.106.196.115。

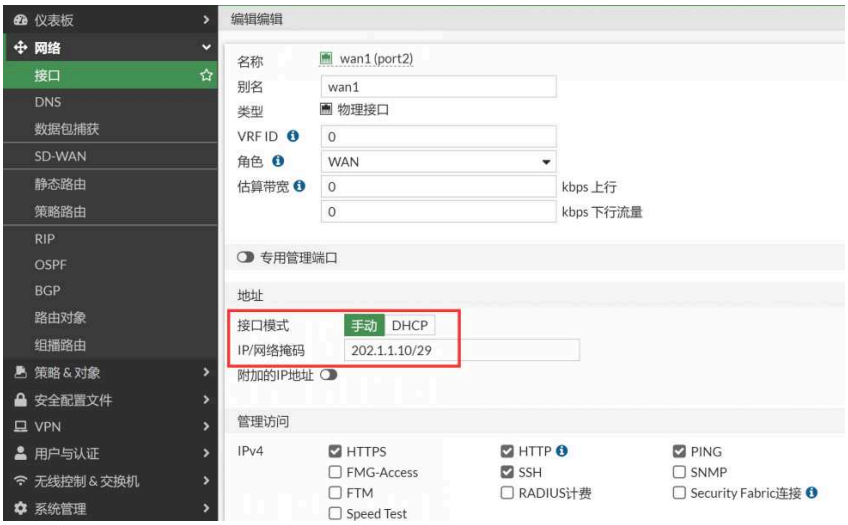


配置要点

- 配置接口IP
- wan1口: IP地址配置为互联网运营商所提供的地址
- internal口: IP地址设置格式为：192.168.1.99/24，可选择性地开启接口的管理功能
- 配置静态路由表
- 配置地址对象"lan"，内容为192.168.1.0/24
- 配置从internal到wan1口的策略，并开启NAT

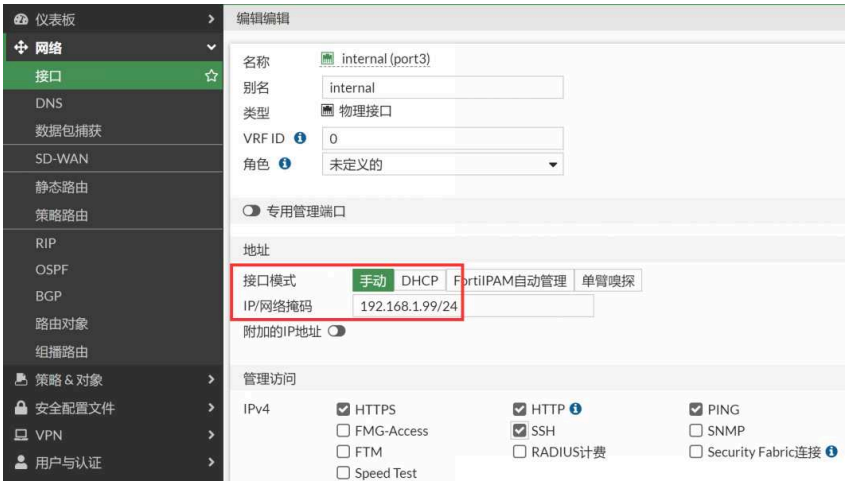
操作步骤

1. 配置接口IP，进入网络→接口→编辑wan1，对于202.1.1.8/29网段，202.1.1.8为网络地址和202.1.1.15广播地址均不可用，202.1.1.9为运营商网关所用，202.1.1.9~202.1.1.14为可用IP地址范围。所以配置给wan1接口的地址我们选择为202.1.1.10。



2. 编辑internal，该接口的默认地址为192.168.1.99/24，根据实际情况更改即可。可选择性地开启接口的管理功能。建议内部开启HTTPS、SSH、PING服务。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置静态路由，进入网络→静态路由，点击新建。



4. 新建静态路由。

- 目的地址：由于是默认网关，使用默认的0.0.0.0/0.0.0.0即可
- 接口：该路由所关联的接口，wan1口，必须正确填写，否则该路由无法工作
- 网关：下一跳IP地址，即wan1口对端运营商设备接口的IP地址
- 管理距离：默认10
- 高级选项-优先级：默认1



5. 配置地址资源，进入策略&对象→地址，新建地址，名称配置为"lan"，地址节点选择子网"192.168.1.0/24"，点击确认。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



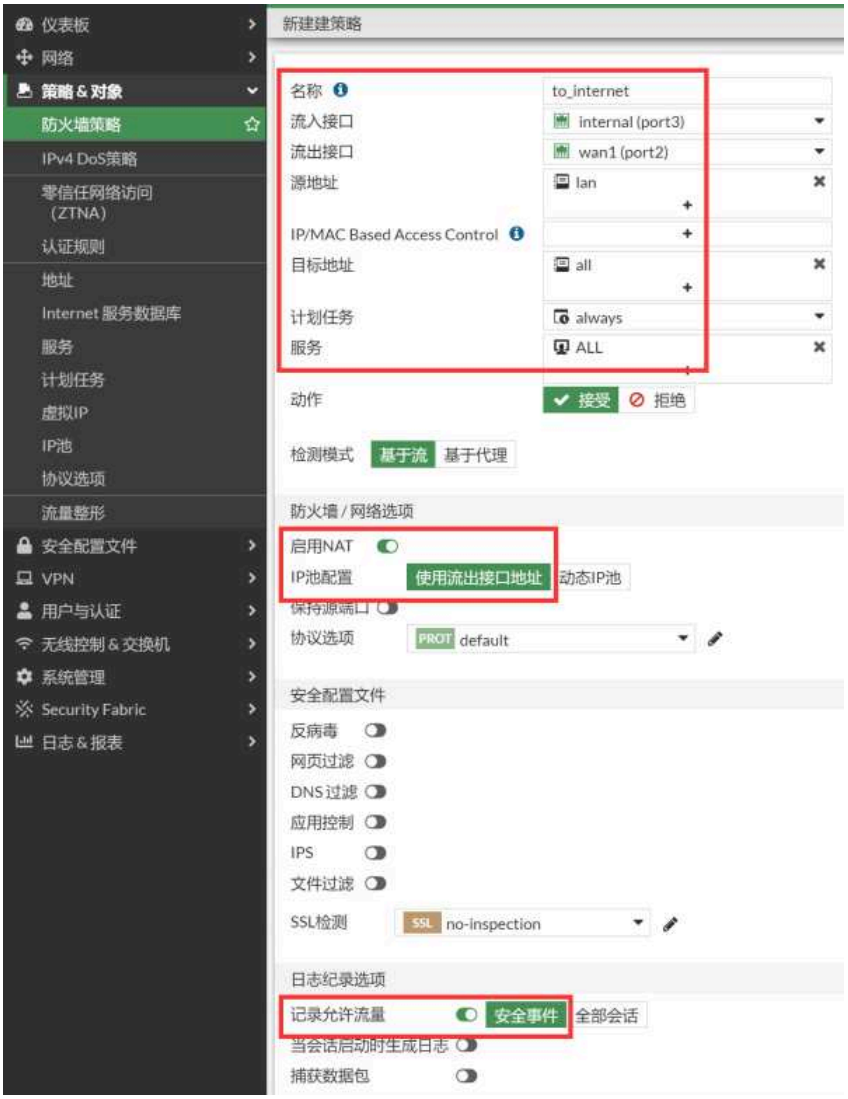
6. 配置防火墙策略（对于某些低端型号，系统会默认配置一条从internal到wan1的NAT策略），进入策略&对象→防火墙策略，点击新建按钮。



7. 在新建页面中，按照如下方式配置策略，点击确定按钮后，系统自动保存配置，策略生效。

- 流入接口：internal
- 源地址：选择刚才定义的地址对象“lan”
- 流出接口：wan1
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为wan1接口地址，进行互联网访问
- 注意： 启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



结果验证

将电脑IP地址设置为192.168.1.10/24，网关设置地为192.168.1.99，DNS配置为当地的DNS，电脑可正常上网。

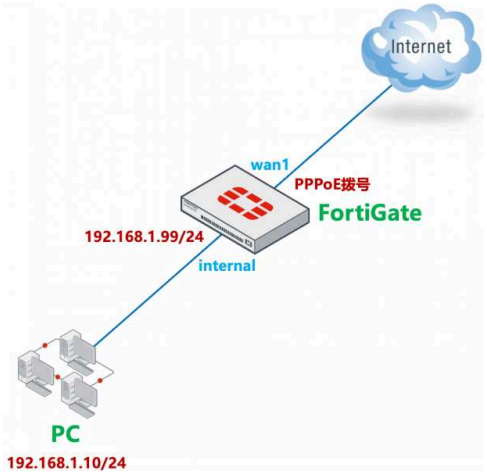
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ADSL线路上网配置

网络需求

外网接口使用ADSL拨号，内网为192.168.1.0/24网段，实现基本上网功能。

网络拓扑



配置要点

- wan1（port2）口: 接ADSL的接口，务必开启自动获取网关，这样ADSL拨号成功后设备会自动生成默认路由，无需手动配置默认路由
- internal（port3）口: IP地址设置格式为：192.168.1.99/24，可选择性地开启接口的管理功能
- 配置地址对象“lan”，内容为192.168.1.0/24
- 配置从internal（port3）到pppoe口的策略，并开启NAT

配置步骤

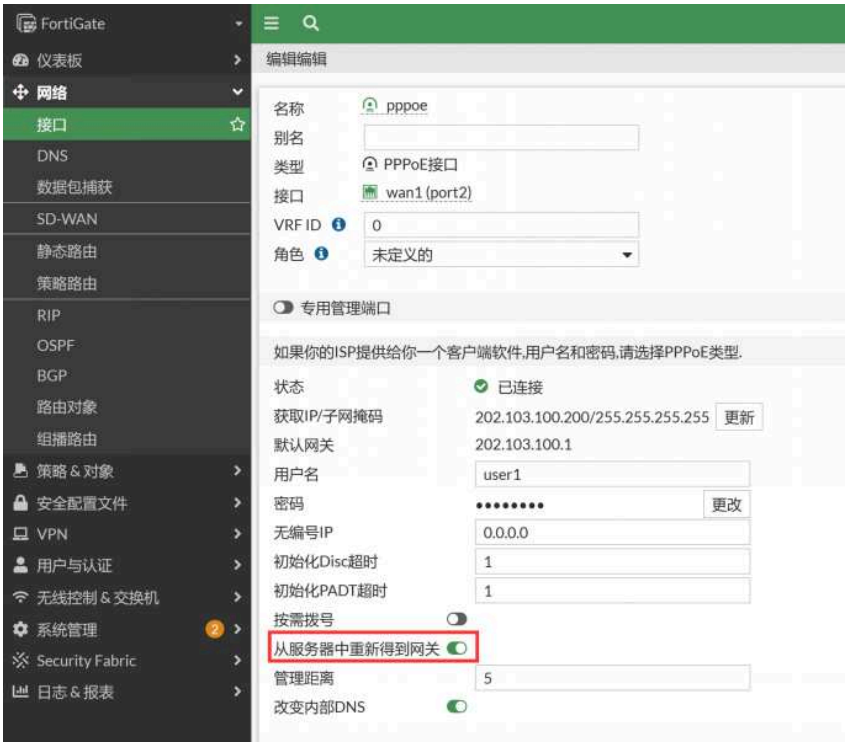
1. 配置wan1口的PPPoE，建议在CLI下配置PPPoE接口，使用此方式配置获取到IP后会自动添加默认路由到运营商。

> **重要**
>
> 建议通过CLI的方式新建PPPoE虚拟接口，参考：部署前注意事项→PPPoE接口 ↗配置章节。

```
config system pppoe-interface
    edit "pppoe"
        set device "port2"
        set username "user1"
        set password xxxxxxxx
    next
end

以上命令执行后，会自动在system interface下创建同名接口，其中包含“从服务器中重新得到网关”的配置
FortiGate # show full sys int pppoe
config system interface
    edit "pppoe"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set defaultgw enable
        set interface "port2"
    next
end
```

2. 以上配置完成后，可以在GUI上看到wan1（port2）下多了一个PPPoE接口，并获取到了运营商的IP。可以看到“从服务器中重新得到网关”已开启。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



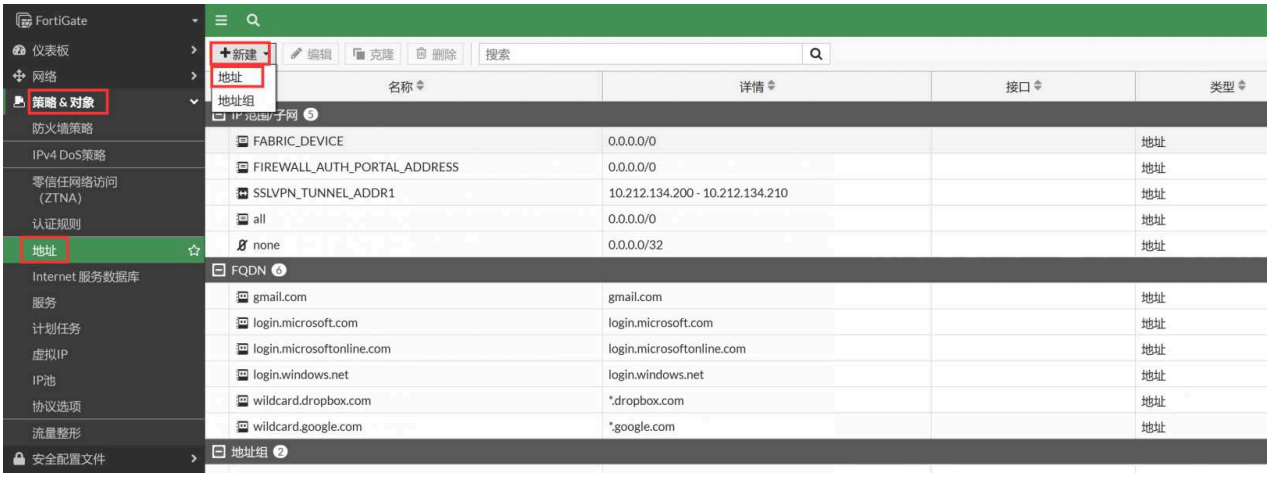

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 202.103.100.1, pppoe, [1/0]
C       192.168.1.0/24 is directly connected, port3
C       202.103.100.1/32 is directly connected, pppoe
C       202.103.100.200/32 is directly connected, pppoe
```

3. 配置internal（port3）接口的IP为192.168.1.99/24。选择性地开启接口的管理功能，建议内部开启https ,ssh, ping服务。

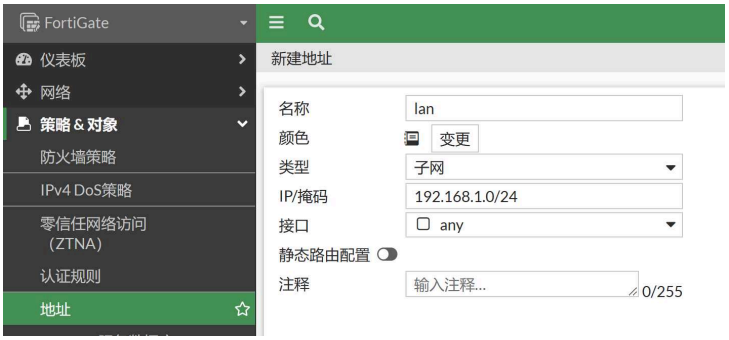


4. 配置地址资源，进入防火墙&对象→地址，点击新建地址按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

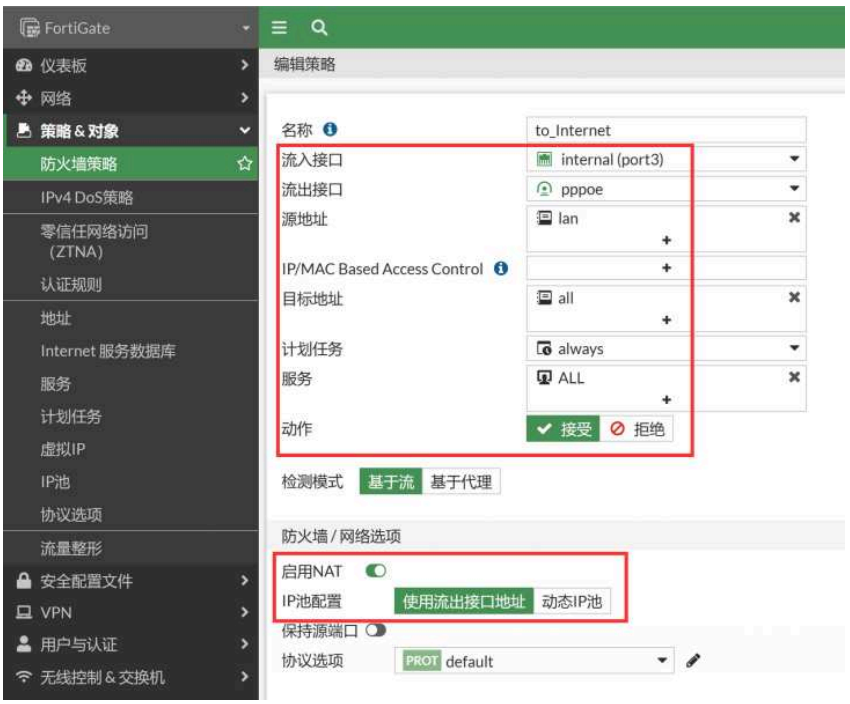


5. 名称配置为lan，地址节点选择子网：192.168.1.0/24，点击确认。




```
config firewall address
    edit "lan"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，放通内网到Internet的流量，并开启NAT，点击确定按钮后，系统自动保存配置，策略生效。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port3"
        set dstintf "port2"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

- 流入接口：internal（port3）
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：pppoe接口
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为wan1接口地址，进行互联网访问
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

结果验证

将电脑IP地址设置为192.168.1.10/24，网关设置地为192.168.1.99，DNS一般设置为当地的DNS即可，电脑可正常上网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

虚拟接口对介绍

简介

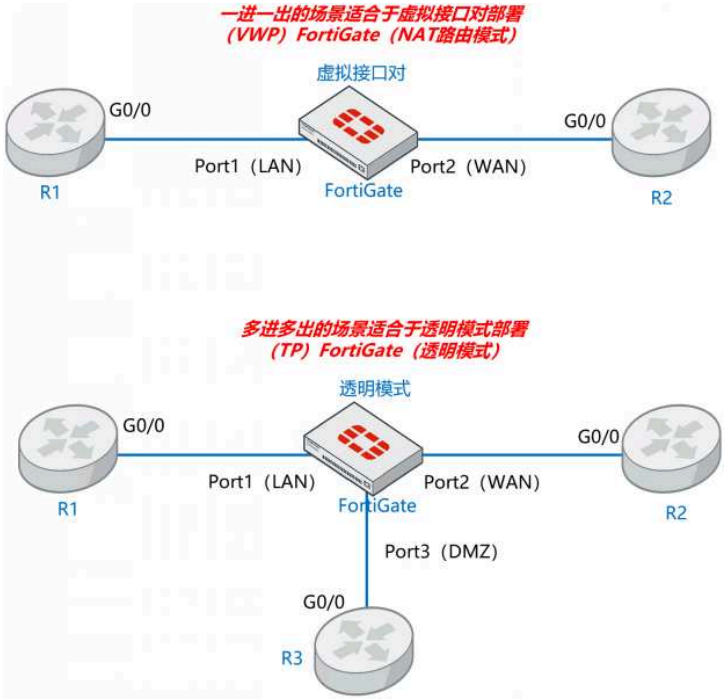
“Virtual Wire Pair”（虚拟接口对）功能提供了一种简便且灵活的类似于FortiGate透明模式的部署方式，“虚拟接口对”顾名思义包括了两个接口（一对接口，无IP地址），流量从一个接口进只能从另外一个接口出，无需查询二层表项，同时通过“虚拟接口对”转发的流量会走NP芯片进行offload，具备很高的转发性能，当然转发流量是否通过最终还是由FortiGate的策略来控制的。由于“虚拟接口对”无需任何IP地址，因此“虚拟接口对”可以方便的插入现有网络中进行部署，和传统的FortiGate透明部署一样不需要改变现有组网的任何配置。

优势

- VWP是直接运行在路由模式下的，FGT无需切换到透明模式，无需配置IP地址，使用起来简单方便。
- 从一个接口进一定从另一个接口出，无需查询MAC表项，有更高的转发效率。
- 存在多VLAN的情况下，无需配置VLAN接口，无需配置Forward-Domain，无需配置更多的策略，VWP对于VLAN业务处理的设计和配置要比传统透明模式简洁很多。
- 一些简单的透明场景VWP更加合适，整个VWP的设计就是如此，部署起来比传统透明模式要简单很多。

劣势

只能一进一出两个接口部署，不能支持多接口的复杂透明模式场景，多进多出的透明部署场景需要使用到传统的透明模式部署。



总结

一进一出的透明模式场景，强烈推荐使用虚拟接口对部署（VWP），又简单又好用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

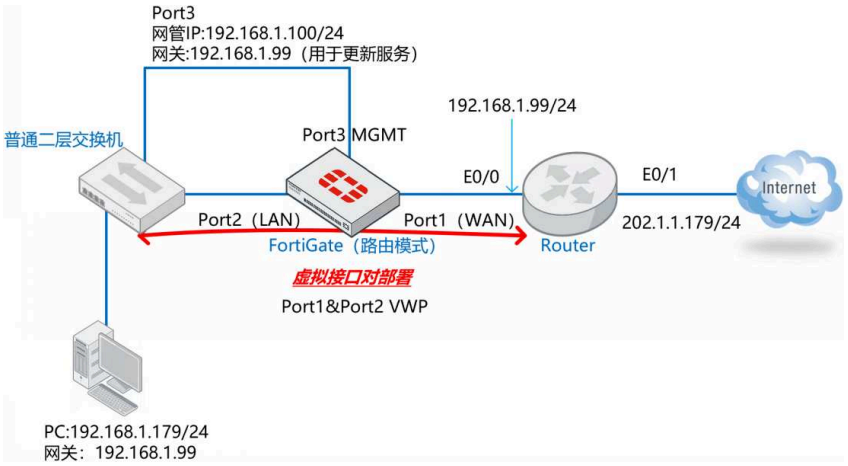
开启虚拟接口对并保护上网流量

网络需求

在不改变现有网络拓扑前提下，将防火墙路由模式部署到网络中，放在路由器和交换机之间，在此基础上开启虚拟接口对（VWP），对内网网段192.168.1.0/24的上网数据进行4~7层的安全防护。

虚拟接口对的策略和透明模式的策略/路由模式的策略使用起来几乎一样，没有太多的特别之处。

网络拓扑



配置要点

- Internet_R路由器的基础配置
- 配置虚拟接口对（Port1&Port2）
- 配置虚拟接口对安全策略允许内网PC访问互联网

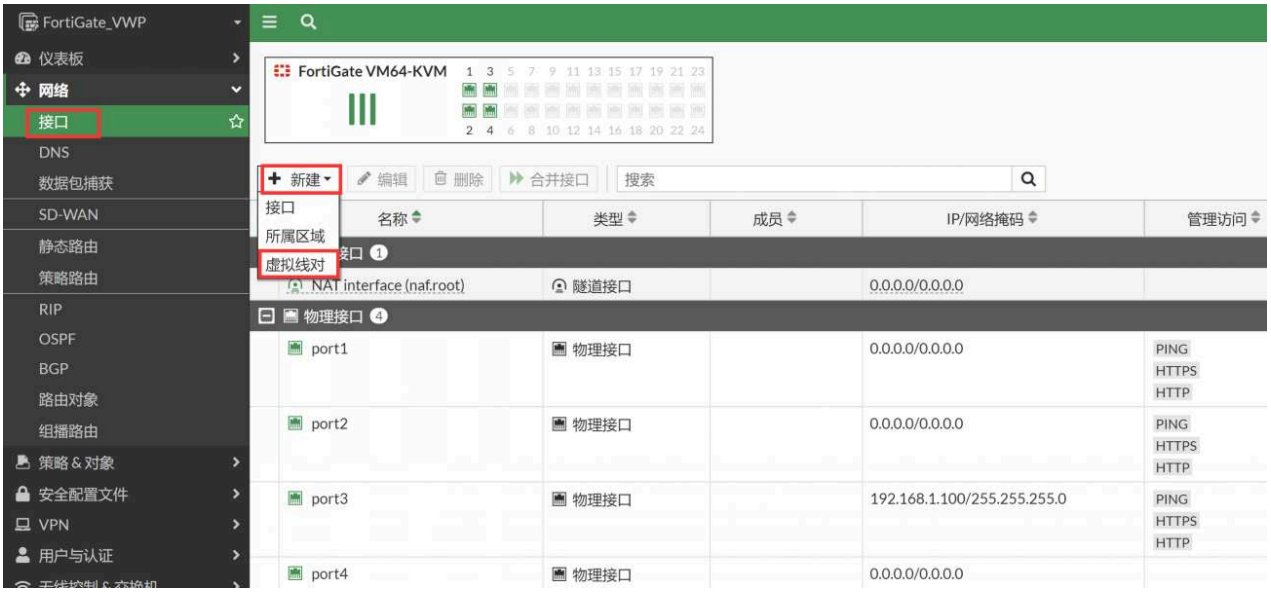
配置步骤

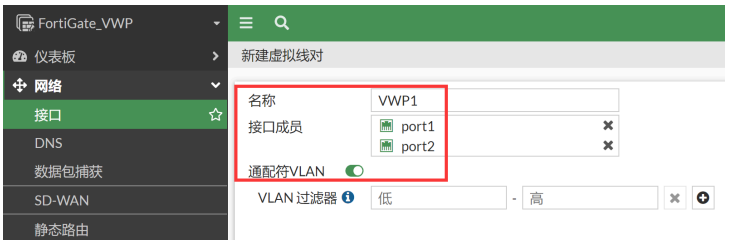
1. Internet_R路由器的基础配置。

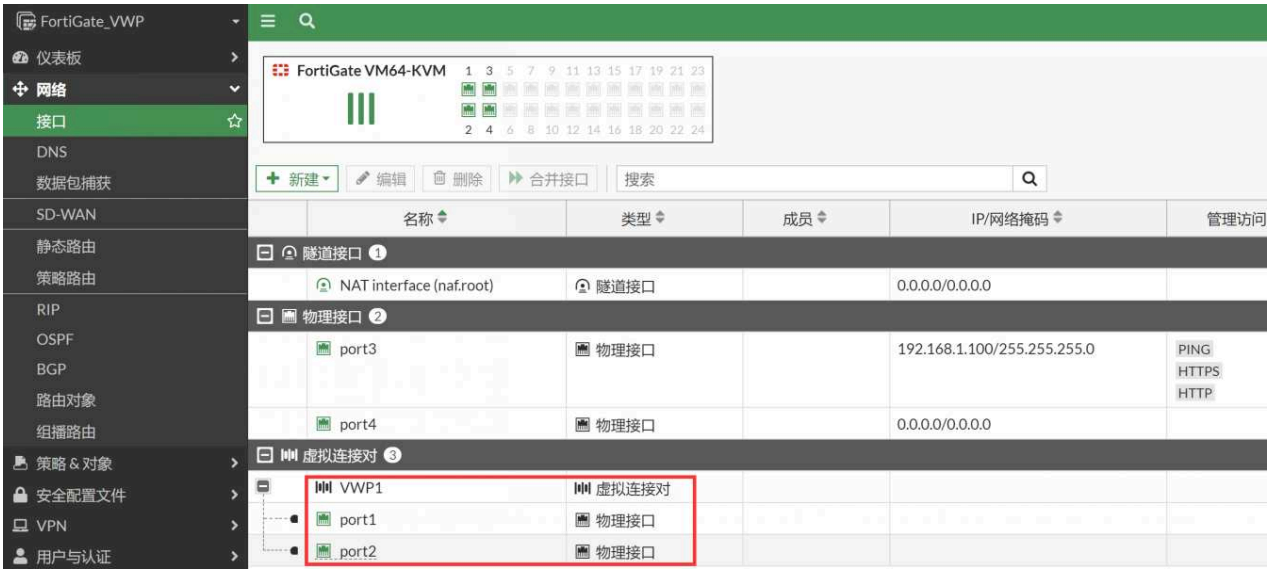
```
hostname Internet_R
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

2. 配置虚拟接口对（Port1&Port2），防火墙处于路由模式的情况下，直接创建虚拟接口对：将port1和port2加入到虚拟接口对中并开启通配符VLAN，识别VLAN-Tag的数据。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





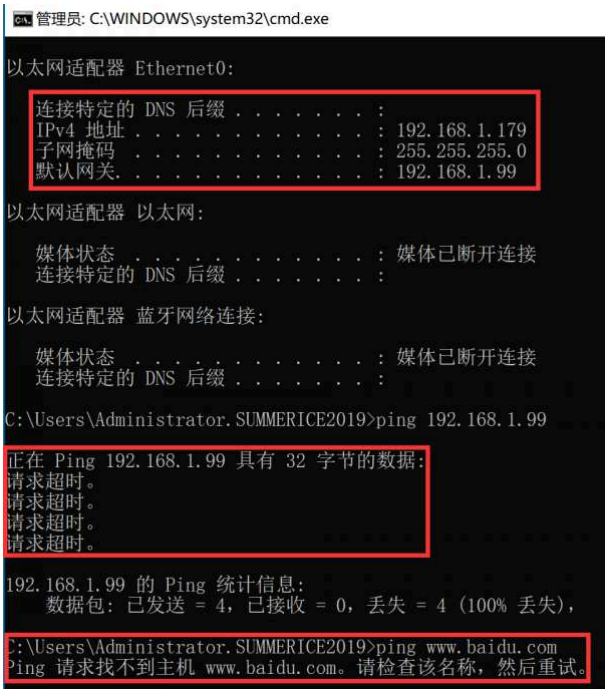


3. 虚拟接口对通道正式打通，可以认为port1和port2之间可以透明的传输数据了（需要防火墙策略放通），对应的CLI如下：

```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enable
    next
end
```

4. 配置虚拟接口对安全策略允许内网PC访问互联网，默认情况下FortiGate没有开启任何策略，此时TCP/UDP/ICMP的流量是全部不通的，例如默认FGT没有策略的情况下，内网PC访问网关和互联网资源都是被Drop的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

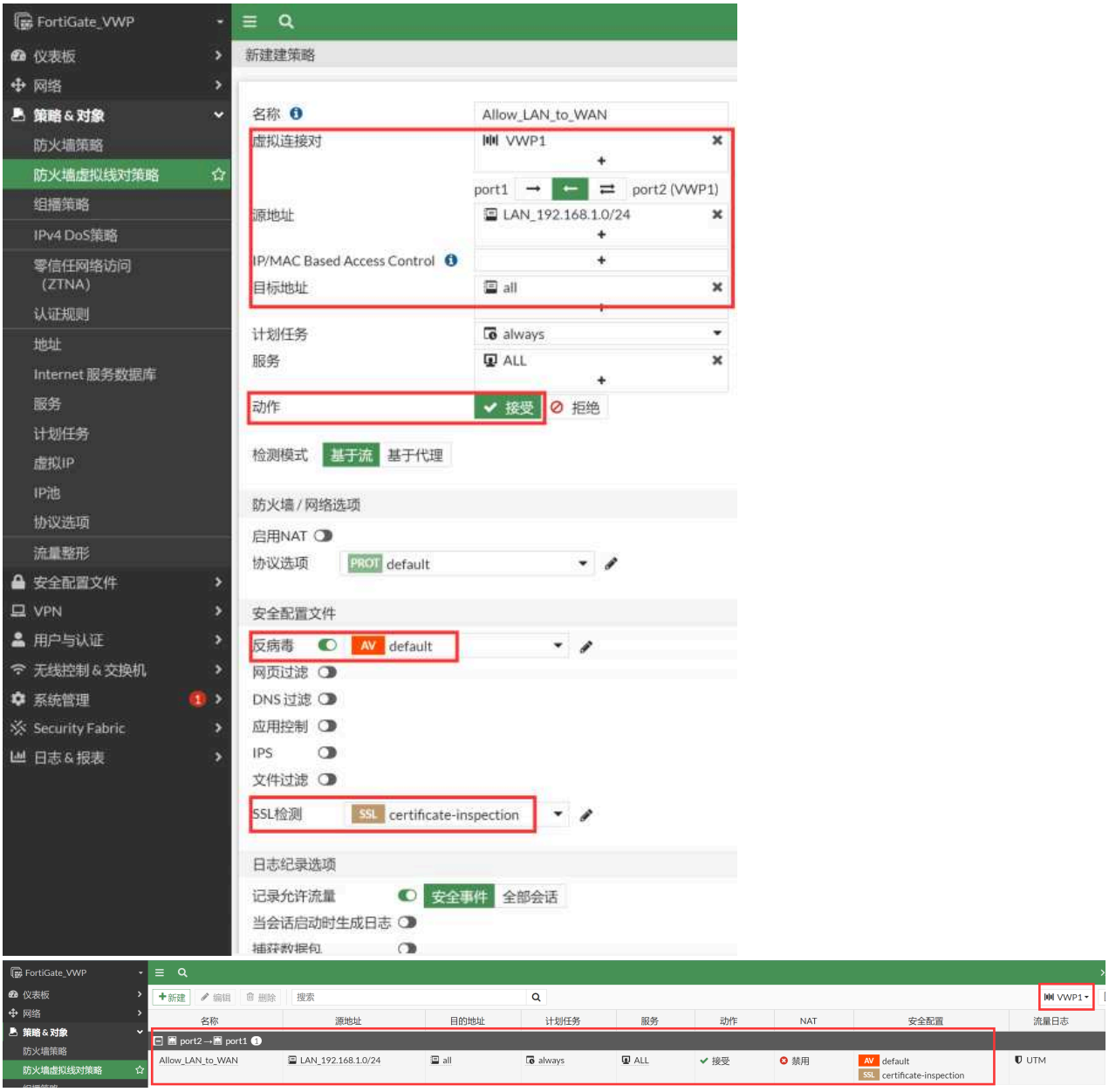


5. 如果需要想要IPV4业务可以通的话，则需要配置相应的安全策略。配置虚拟接口对的策略：允许LAN（port2）到WAN（port1）的上网流量穿过FGT，策略&对象的位置会多出“防火墙虚拟线对策略”（如果没有看到，则刷新页面或注销管理登陆，重新登陆FGT即可看到）。



6. 右上角选择VWP1线对，方向选择port2→port1（也可选择双向的方向），新建VWP策略，开启AV功能并引用默认的AV Profile（虚拟连接对可以选择多个，在同一条相同动作的策略中进行多接口控制）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



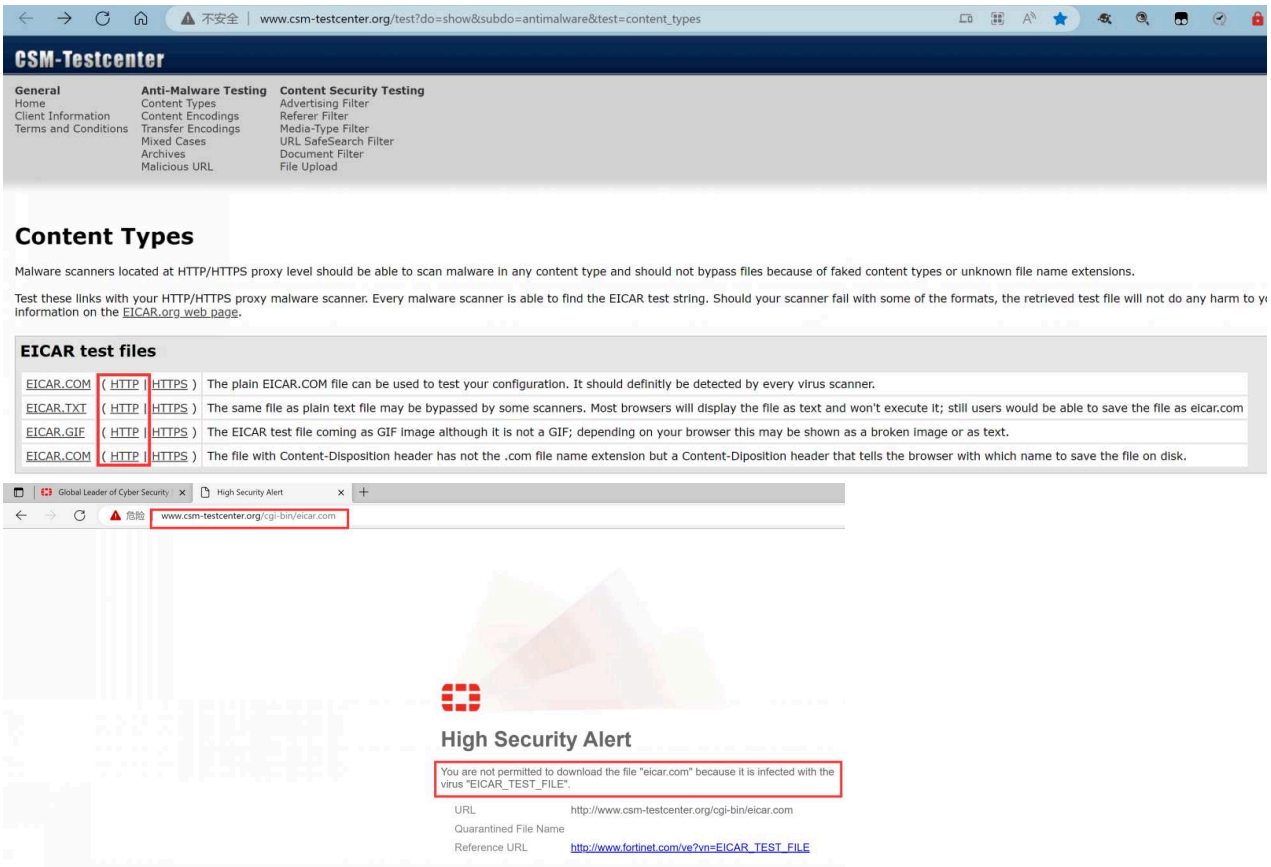
结果验证

1. 使用内网PC访问外部网络，可以正常访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

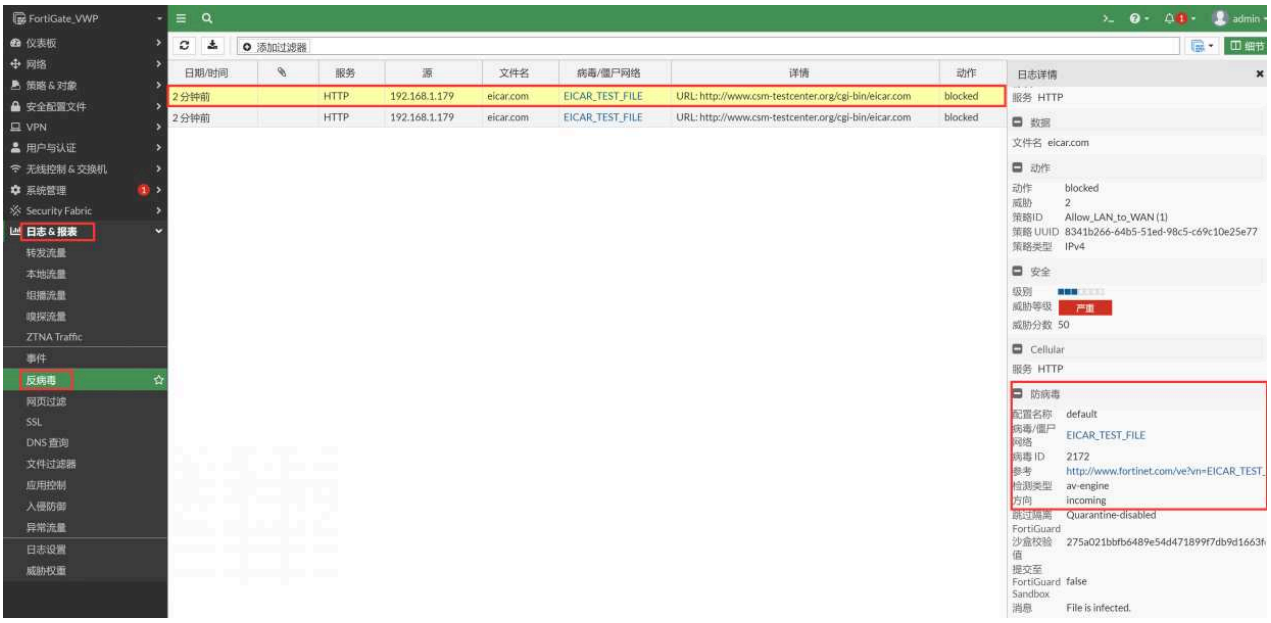


2. 测试通过HTTP下载病毒文件（http://www.csm-testcenter.org/test?do=show&subdo=antimalware&test=content_types ↗），被FortiGate阻断。

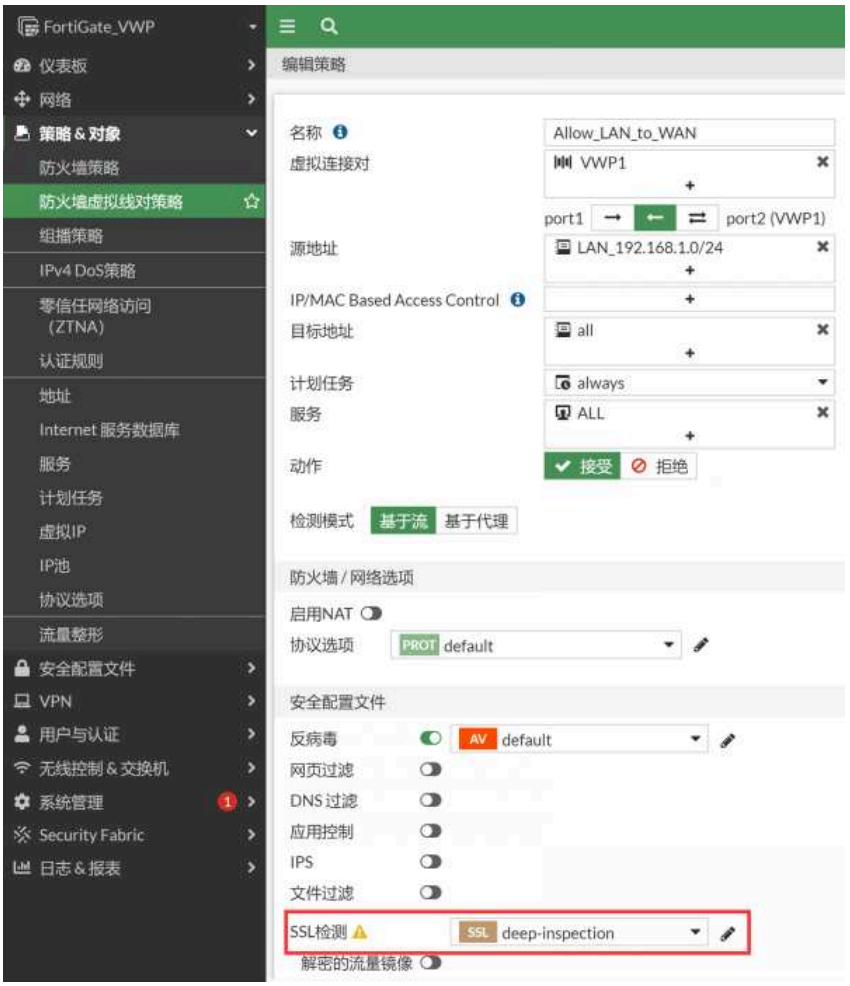


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在FortiGate上查看相应的AV日志。

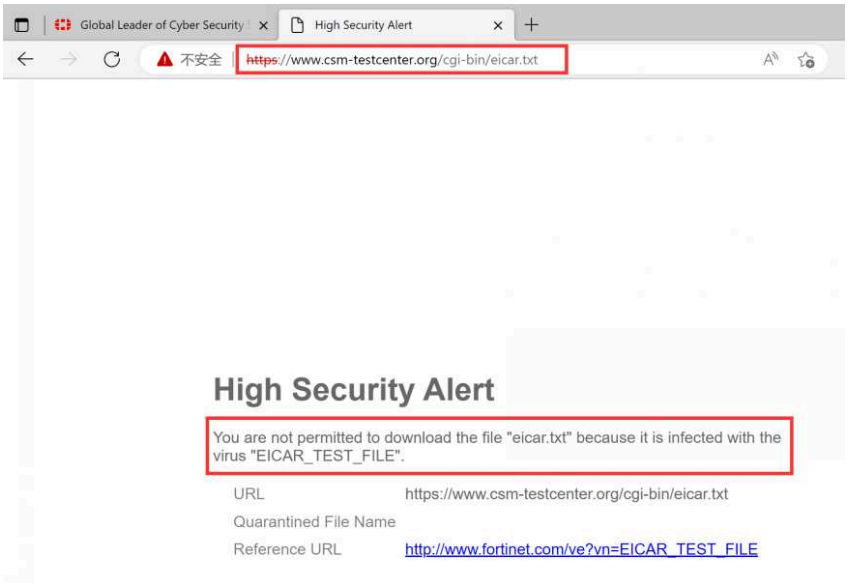


4. 如果是通过HTTPS下载病毒，由于数据被HTTPS加密，如需要检测需要开启SSL深度检测，需要在虚拟接口对策略中调用SSL深度检测。

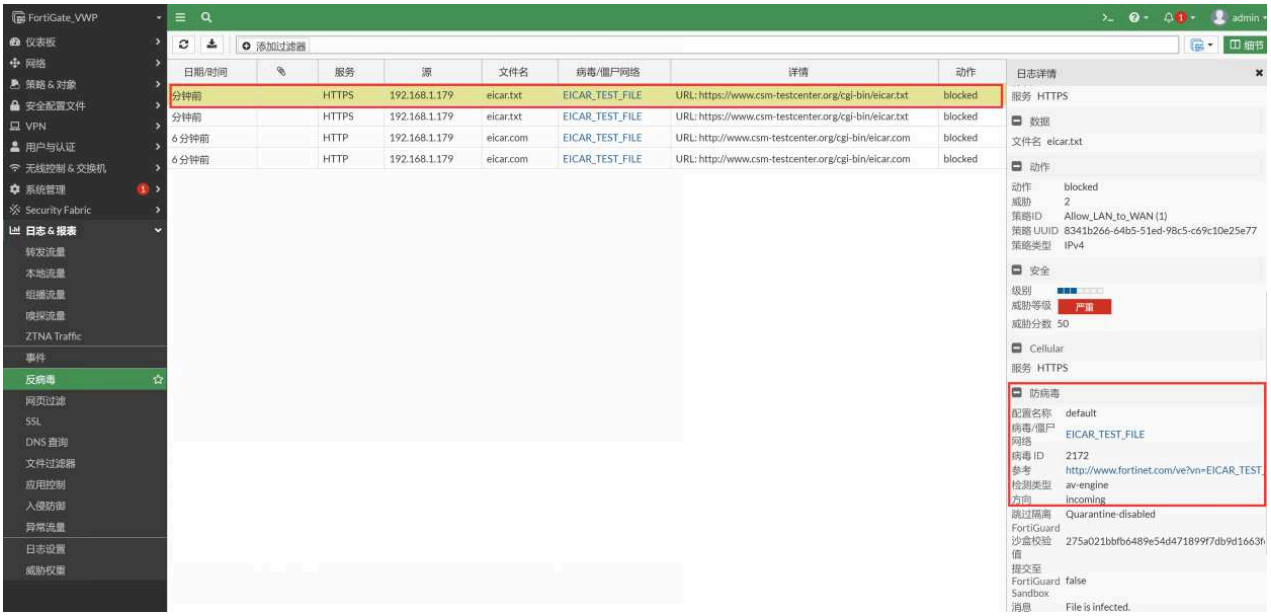


5. 测试通过HTTPS下载病毒文件（http://www.csm-testcenter.org/test?do=show&subdo=antimalware&test=content_types ↗），被FortiGate阻断。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 在FortiGate上查看相应的AV日志。



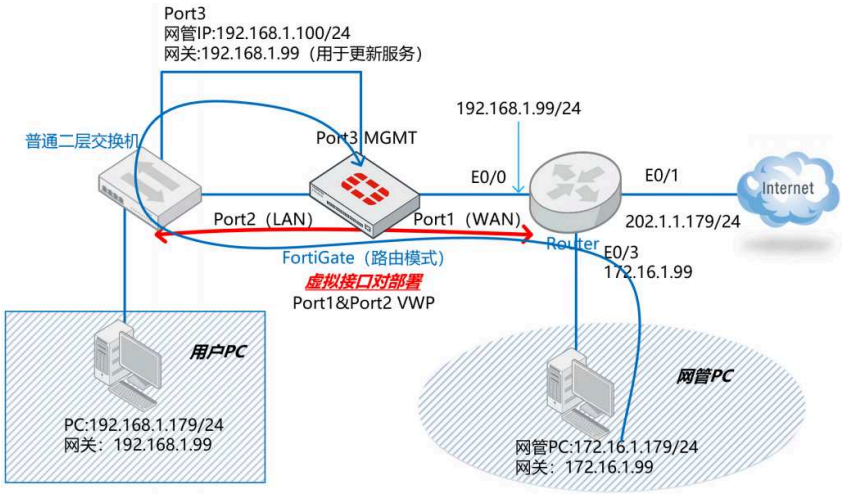
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

虚拟接口对的网络管理问题

网络需求

有一个特别的网管情况：防火墙是运行在路由模式下的，一旦开启了VWP，VWP相当于一个透明的接口对，可以透传流量，但是由于FortiGate本身需要被网管，而一旦网管的流量需要穿过VWP被网管的话，则就会遇到网管不了的情况，因为网管数据穿过VWP访问FortiGate的本机IP，这样会话存在混乱，内核和转发将判断会话存在异常，会该网管的导致数据不通。

网络拓扑



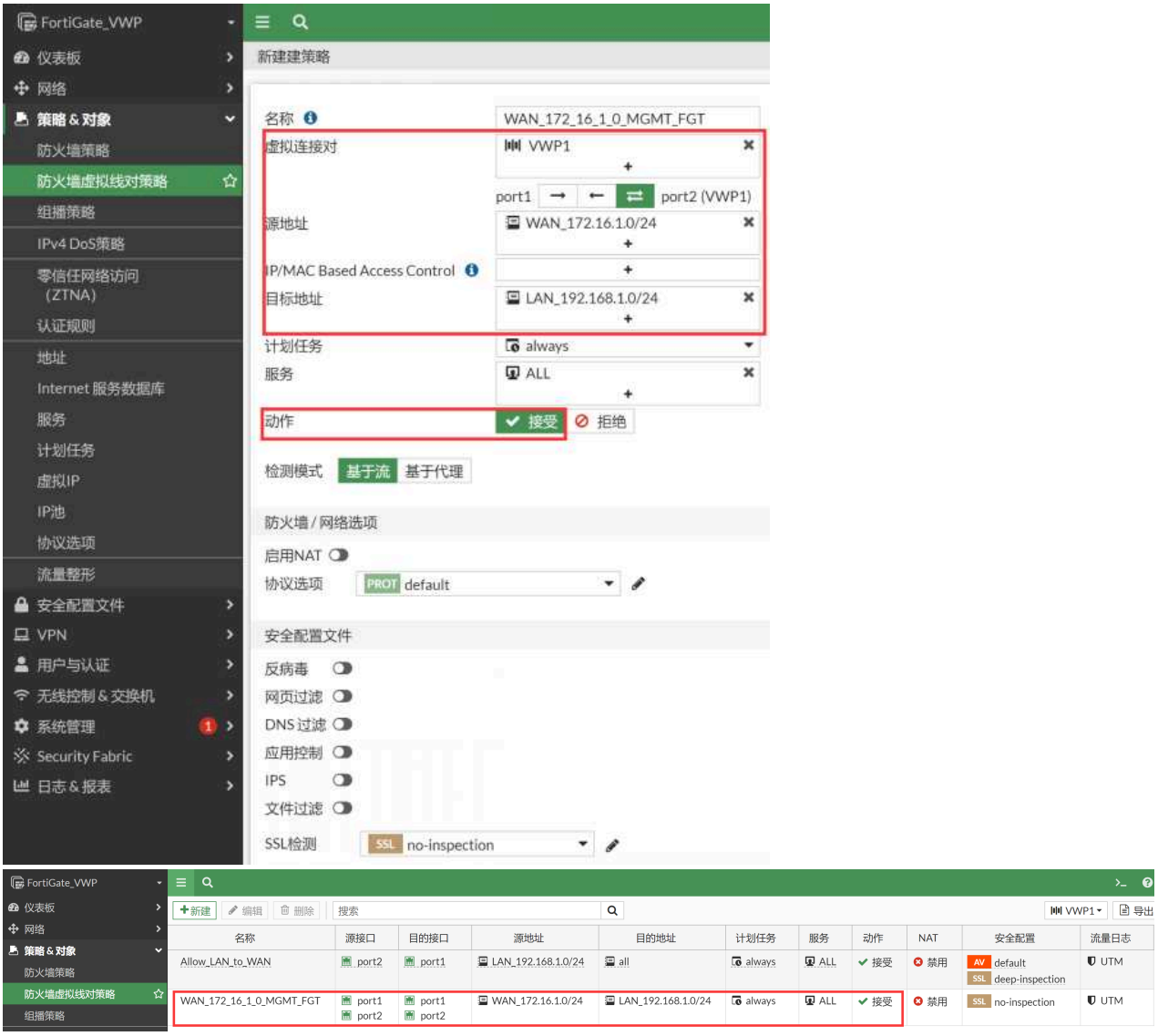
网管区域在WAN侧，而FortiGate的网管接口Port3在LAN侧，这种拓扑环境下网管有两种情况：

- 用户PC可以正常网管FortiGate：用户PC 192.168.1.179由于和FGT的Port3网管接口同属于LAN侧流量，流量无需穿越VWP，因此可以正常网管（推荐的网管规划和部署）。
- 网管PC无法网管FortiGate：网管PC 172.16.1.179在FortiGate的WAN侧，发起去FGT的Port3网管接口的流量时候，正常流量会穿越VWP然后再达到Port3接口上，由于穿过VWP的时候发现目的IP是Port3，这是一个访问FGT本机的报文，这样FGT在处理管理流量会存在问题。

问题复现

1. 我们来分析一下上述第二种异常的情况，为测试WAN的网管PC穿越VWP管理FGT，需要新增一条允许WAN 172.16.1.0/24到LAN 192.168.1.0/24的策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 使用网管PC 172.16.1.179访问FortiGate的Port3 192.168.1.100，在FortiGate上抓包查看，网管的数据在Port3接口IN之后就被丢弃了，PING/SSH/HTTPS网管全部失败。

```
FortiGate_VWP # diagnose sniffer packet any "host 172.16.1.179" 4
interfaces=[any]
filters=[host 172.16.1.179]
1.216456 port1 in 172.16.1.179.51524 → 192.168.1.100.443: syn 3746720489
1.216496 port2 out 172.16.1.179.51524 → 192.168.1.100.443: syn 3746720489
1.259983 port3 in 172.16.1.179.51524 → 192.168.1.100.443: syn 3746720489

3.241235 port1 in 172.16.1.179 → 192.168.1.100: icmp: echo request
3.241320 port2 out 172.16.1.179 → 192.168.1.100: icmp: echo request
3.244140 port3 in 172.16.1.179 → 192.168.1.100: icmp: echo request

26.005468 port1 in 172.16.1.179.51533 → 192.168.1.100.22: syn 2838383157
26.005514 port2 out 172.16.1.179.51533 → 192.168.1.100.22: syn 2838383157
26.050901 port3 in 172.16.1.179.51533 → 192.168.1.100.22: syn 2838383157
```

3. debug flow查看原因，由于数据从port2 in→port1 out穿越过VWP一次（创建了一个会话），然后又从port3（root）发出一个回复报文，这个回复报文会匹配到之前创建会话，这样的会话接口存在混乱，会引起重放检测失败丢包。

```
diagnose debug flow filter addr 172.16.1.179
diagnose debug flow show function-name enable
diagnose debug flow trace start 100
diagnose debug enable

id=20085 trace_id=10 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=6, 172.16.1.179:51565->192.168.1.100:443) from port1. flag [S], seq 1925780389, ack 0, win 8192"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
id=20085 trace_id=10 func=init_ip_session_common line=5654 msg="allocate a new session-000005b1"
id=20085 trace_id=10 func=br_fw_forward_handler line=539 msg="Allowed by Policy-2:"
id=20085 trace_id=10 func=__if_queue_push_xmit line=417 msg="send out via dev-port2, dst-mac-50:00:00:03:00:02"

id=20085 trace_id=11 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=6, 172.16.1.179:51565->192.168.1.100:443) from port3. flag [S], seq 1925780389, ack 0, win 8192"
id=20085 trace_id=11 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000005b1, original direction"
id=20085 trace_id=11 func=vf_ip_route_input_common line=2591 msg="find a route: flag=80000000 gw-192.168.1.100 via root"

id=20085 trace_id=12 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=6, 192.168.1.100:443->172.16.1.179:51565) from local. flag [S.], seq 2874972251, ack 1925780390, win 14600"
id=20085 trace_id=12 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000005b1, reply direction"
id=20085 trace_id=12 func=ip_session_core_in line=6222 msg="outgoing dev changed:3→5 dir=reply, drop"

id=20085 trace_id=49 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 172.16.1.179:1->192.168.1.100:2048) from port1. type=8, code=0, id=1, seq=47."
id=20085 trace_id=49 func=init_ip_session_common line=5654 msg="allocate a new session-000005cc"
id=20085 trace_id=49 func=br_fw_forward_handler line=539 msg="Allowed by Policy-2:"
id=20085 trace_id=49 func=__if_queue_push_xmit line=417 msg="send out via dev-port2, dst-mac-50:00:00:03:00:02"

id=20085 trace_id=50 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 172.16.1.179:1->192.168.1.100:2048) from port3. type=8, code=0, id=1, seq=47."
id=20085 trace_id=50 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000005cc, original direction"
id=20085 trace_id=50 func=vf_ip_route_input_common line=2591 msg="find a route: flag=80000000 gw-192.168.1.100 via root"

id=20085 trace_id=51 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 192.168.1.100:1->172.16.1.179:0) from local. type=0, code=0, id=1, seq=47."
id=20085 trace_id=51 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000005cc, reply direction"
id=20085 trace_id=51 func=ip_session_core_in line=6222 msg="outgoing dev changed:3→5 dir=reply, drop"
```

4. 值得注意的是，FGT（192.168.1.100）是可以主动去ping通172.16.1.179的，也就是说FGT是可以正常的更新Fortiguard服务和上互联网的。

```
FortiGate_VWP # execute ping 172.16.1.179
PING 172.16.1.179 (172.16.1.179): 56 data bytes
64 bytes from 172.16.1.179: icmp_seq=0 ttl=127 time=7.8 ms
64 bytes from 172.16.1.179: icmp_seq=1 ttl=127 time=8.0 ms
64 bytes from 172.16.1.179: icmp_seq=2 ttl=127 time=7.4 ms
64 bytes from 172.16.1.179: icmp_seq=3 ttl=127 time=6.0 ms
64 bytes from 172.16.1.179: icmp_seq=4 ttl=127 time=8.8 ms

FortiGate_VWP # diagnose sniffer packet any "icmp" 4
interfaces=[any]
filters=[icmp]
55.845400 port3 out 192.168.1.100 → 172.16.1.179: icmp: echo request
55.848682 port2 in 192.168.1.100 → 172.16.1.179: icmp: echo request
55.848706 port1 out 192.168.1.100 → 172.16.1.179: icmp: echo request
55.851016 port1 in 172.16.1.179 → 192.168.1.100: icmp: echo reply
55.851030 port2 out 172.16.1.179 → 192.168.1.100: icmp: echo reply
55.855936 port3 in 172.16.1.179 → 192.168.1.100: icmp: echo reply
56.857317 port3 out 192.168.1.100 → 172.16.1.179: icmp: echo request
56.863493 port2 in 192.168.1.100 → 172.16.1.179: icmp: echo request
56.863515 port1 out 192.168.1.100 → 172.16.1.179: icmp: echo request
56.870026 port1 in 172.16.1.179 → 192.168.1.100: icmp: echo reply
56.870039 port2 out 172.16.1.179 → 192.168.1.100: icmp: echo reply
56.876321 port3 in 172.16.1.179 → 192.168.1.100: icmp: echo reply

id=20085 trace_id=93 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 192.168.1.100:2816->172.16.1.179:2048) from local. type=8, code=0, id=2816, seq=0."
id=20085 trace_id=93 func=init_ip_session_common line=5654 msg="allocate a new session-000013a5"

id=20085 trace_id=94 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 192.168.1.100:2816->172.16.1.179:2048) from port2. type=8, code=0, id=2816, seq=0."
id=20085 trace_id=94 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000013a5, original direction"
id=20085 trace_id=94 func=br_fw_forward_dirty_handler line=318 msg="Found a reflect session: pro=1, 192.168.1.100/2816⇒172.16.1.179/8, dev=4→3"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

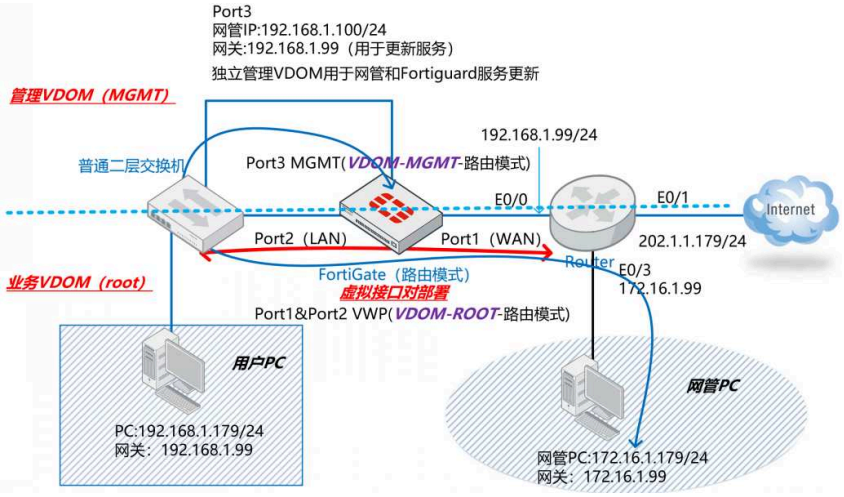
```
id=20085 trace_id=94 func=__if_queue_push_xmit line=417 msg="send out via dev-port1, dst-mac-aa:bb:cc:00:20:00"

id=20085 trace_id=95 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 172.16.1.179:2816->192.168.1.100:0) from port1. type=0, code=0, id=2816, seq=0."
id=20085 trace_id=95 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000013a5, reply direction"
id=20085 trace_id=95 func=__if_queue_push_xmit line=417 msg="send out via dev-port2, dst-mac-50:00:00:03:00:02"

id=20085 trace_id=96 func=print_pkt_detail line=5494 msg="vd-root:0 received a packet(proto=1, 172.16.1.179:2816->192.168.1.100:0) from port3. type=0, code=0, id=2816, seq=0."
id=20085 trace_id=96 func=resolve_ip_tuple_fast line=5569 msg="Find an existing session, id-000013a5, reply direction"
id=20085 trace_id=96 func=vf_ip_route_input_common line=2591 msg="find a route: flag=80000000 gw-192.168.1.100 via root"
```

5. 以上就是VWP环境下的网管问题的故障现象，单向通信，跨VWP的网管流量无法正常通信。

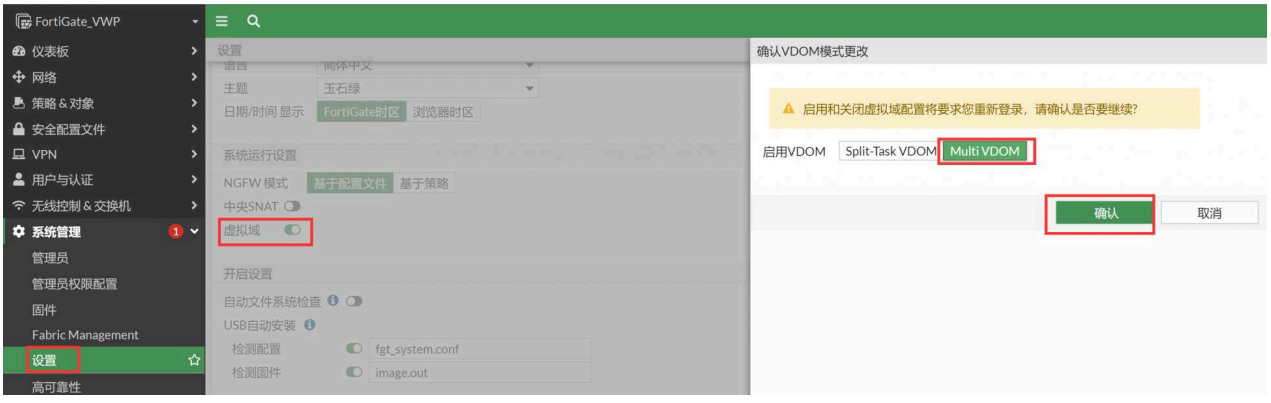
解决办法

1. 从设计上避免这种跨VWP的网管FGT自身的流量，不跨VWP的网管是正常的。

2. 如果无法避免这样的流量，则使用VDOM技术将网管和业务二者独立开来，创建一个管理的VDOM（MGMT）专门用于MGMT，与VWP的所属的VDOM（ROOT）完全独立运行即可，如下图所示。



3. 开启FortiGate的VDOM功能。



对应命令行：

```
FortiGate_VWP # config system global
FortiGate_VWP (global) # set vdom-mode multi-vdom
FortiGate_VWP (global) # end
You will be logged out for the operation to take effect
Do you want to continue? (y/n) y
exit
```

4. 创建MGMT VDOM。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



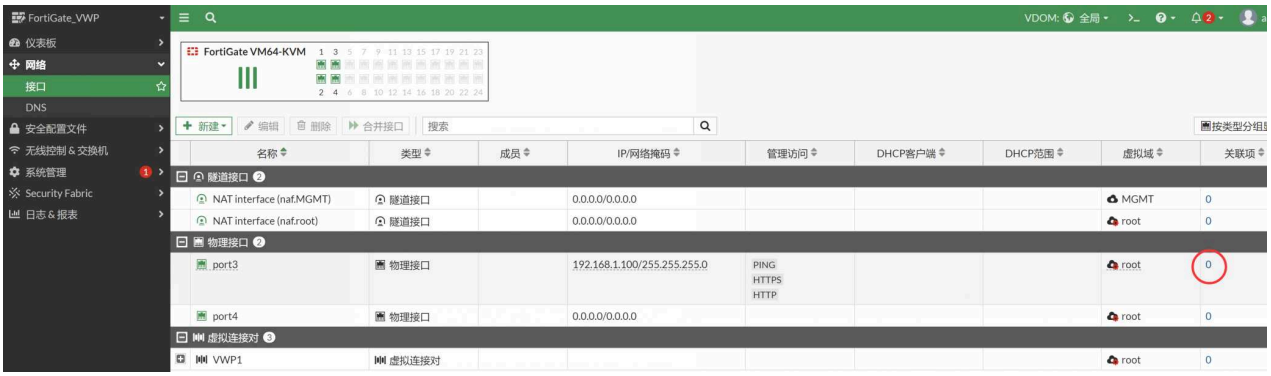




5. 准备将port3加入MGMT VDOM中，将port3加入MGMT VDOM之前需要去掉相关的配置关联项，也就是说port3不能在root下有相关的配置，比如此时有静态路由的配置，则需要删掉该路由。

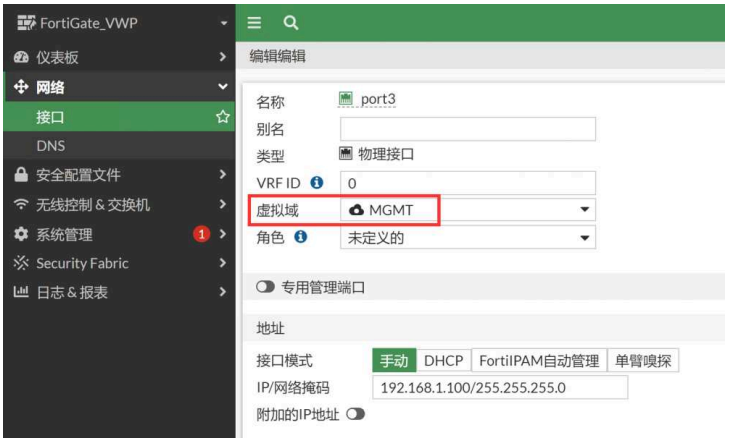




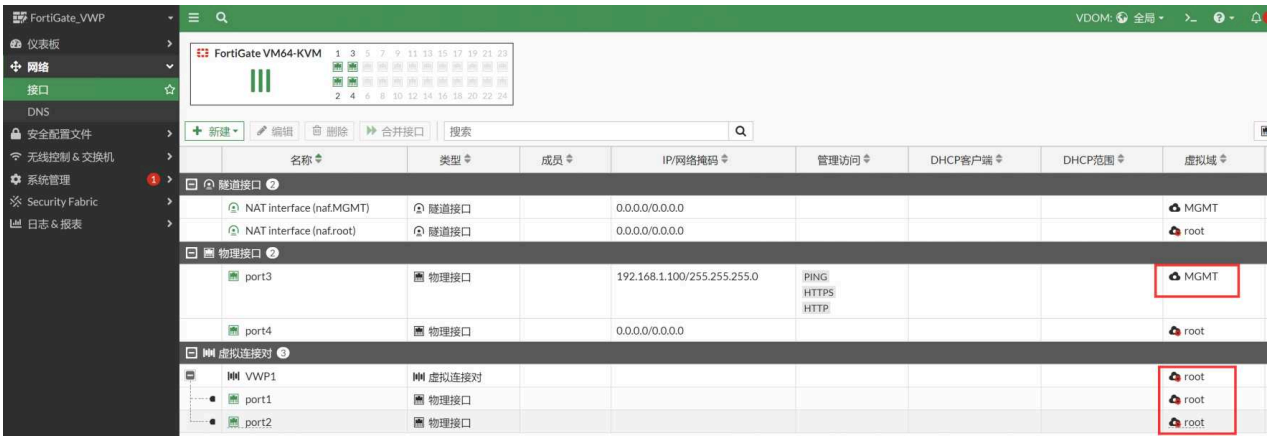


6. 此时可以将port3加入MGMT VDOM。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 这样相当于port3属于VDOM MGMT，而port1和port2属于 VDOM ROOT，二者完全独立，这样就可以解决会话混乱的问题了。



8. 再进入MGMT VDOM，将管理接口的默认路由加上去。



9. 将MGMT VDOM设置为管理VDOM，用于更新Fortiguard（这一项很重要，如果管理VDOM是root则不需要此操作，默认的管理VDOM是root）。

```
FortiGate_VWP # config global
FortiGate_VWP (global) # config system global
FortiGate_VWP (global) # set management-vdom MGMT
FortiGate_VWP (global) # end
FortiGate_VWP (global) # end
```

效果验证

1. 再次抓取网管PC跨VWP去管理FGT的网管流量。

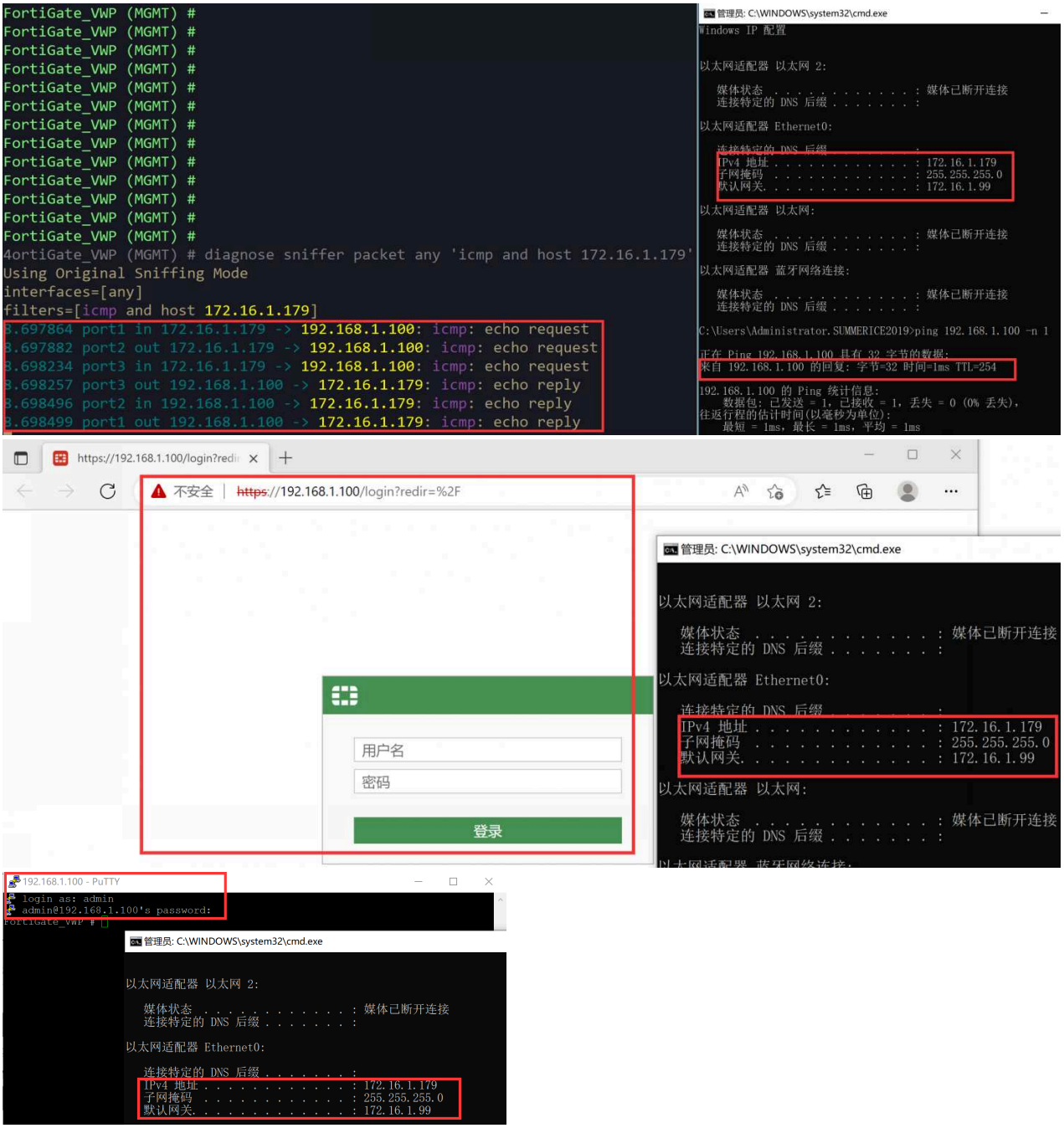
```
FortiGate_VWP (root) # diagnose sniffer packet any "host 172.16.1.179" 4
interfaces=[any]
filters=[host 172.16.1.179]
6.911052 port1 in 172.16.1.179 → 192.168.1.100: icmp: echo request
6.911092 port2 out 172.16.1.179 → 192.168.1.100: icmp: echo request
6.914638 port3 in 172.16.1.179 → 192.168.1.100: icmp: echo request
6.914682 port3 out 192.168.1.100 → 172.16.1.179: icmp: echo reply
6.918603 port2 in 192.168.1.100 → 172.16.1.179: icmp: echo reply
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
6.918621 port1 out 192.168.1.100 → 172.16.1.179: icmp: echo reply

48.683279 port1 in 172.16.1.179.49159 → 192.168.1.100.80: syn 3128124765
48.683385 port2 out 172.16.1.179.49159 → 192.168.1.100.80: syn 3128124765
48.684797 port1 in 172.16.1.179.49160 → 192.168.1.100.80: syn 2745446281
48.684845 port2 out 172.16.1.179.49160 → 192.168.1.100.80: syn 2745446281
48.686611 port1 in 172.16.1.179.49161 → 192.168.1.100.443: syn 2797650417
48.686655 port2 out 172.16.1.179.49161 → 192.168.1.100.443: syn 2797650417
48.712056 port3 in 172.16.1.179.49159 → 192.168.1.100.80: syn 3128124765
48.712230 port3 out 192.168.1.100.80 → 172.16.1.179.49159: syn 1287655075 ack 3128124766
48.713907 port3 in 172.16.1.179.49160 → 192.168.1.100.80: syn 2745446281
48.713951 port3 out 192.168.1.100.80 → 172.16.1.179.49160: syn 1003036694 ack 2745446282
48.715772 port2 in 192.168.1.100.80 → 172.16.1.179.49159: syn 1287655075 ack 3128124766
48.715790 port1 out 192.168.1.100.80 → 172.16.1.179.49159: syn 1287655075 ack 3128124766
48.717463 port2 in 192.168.1.100.80 → 172.16.1.179.49160: syn 1003036694 ack 2745446282
48.717478 port1 out 192.168.1.100.80 → 172.16.1.179.49160: syn 1003036694 ack 2745446282
48.717537 port1 in 172.16.1.179.49159 → 192.168.1.100.80: ack 1287655076
48.717547 port2 out 172.16.1.179.49159 → 192.168.1.100.80: ack 1287655076
48.719277 port1 in 172.16.1.179.49160 → 192.168.1.100.80: ack 1003036695
48.719291 port2 out 172.16.1.179.49160 → 192.168.1.100.80: ack 1003036695

232.060671 port1 in 172.16.1.179.49158 → 192.168.1.100.22: syn 446444854
232.060794 port2 out 172.16.1.179.49158 → 192.168.1.100.22: syn 446444854
232.069282 port3 in 172.16.1.179.49158 → 192.168.1.100.22: syn 446444854
232.069473 port3 out 192.168.1.100.22 → 172.16.1.179.49158: syn 1275691481 ack 446444855
232.072262 port2 in 192.168.1.100.22 → 172.16.1.179.49158: syn 1275691481 ack 446444855
232.072278 port1 out 192.168.1.100.22 → 172.16.1.179.49158: syn 1275691481 ack 446444855
232.074496 port1 in 172.16.1.179.49158 → 192.168.1.100.22: ack 1275691482
232.074512 port2 out 172.16.1.179.49158 → 192.168.1.100.22: ack 1275691482
232.084068 port3 in 172.16.1.179.49158 → 192.168.1.100.22: ack 1275691482
232.106501 port3 out 192.168.1.100.22 → 172.16.1.179.49158: psh 1275691482 ack 446444855
232.111292 port2 in 192.168.1.100.22 → 172.16.1.179.49158: psh 1275691482 ack 446444855
232.111311 port1 out 192.168.1.100.22 → 172.16.1.179.49158: psh 1275691482 ack 446444855
232.129332 port1 in 172.16.1.179.49158 → 192.168.1.100.22: psh 446444855 ack 1275691499
232.129361 port2 out 172.16.1.179.49158 → 192.168.1.100.22: psh 446444855 ack 1275691499
232.132511 port3 in 172.16.1.179.49158 → 192.168.1.100.22: psh 446444855 ack 1275691499
```

2. 跨VWP的网管工作正常。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



总结

开启了VWP的FGT网管尽量不要跨VWP进行网管，如果不能避免这样的部署就通过上述所示的VDOM去解决。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

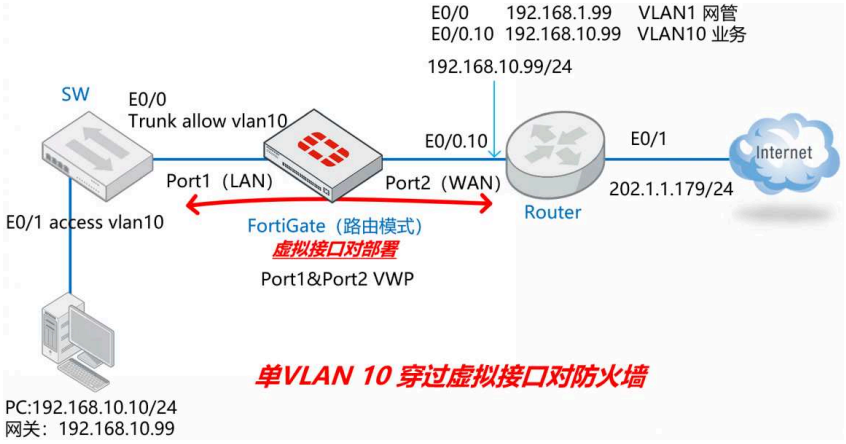
VLAN与虚拟接口对

网络需求

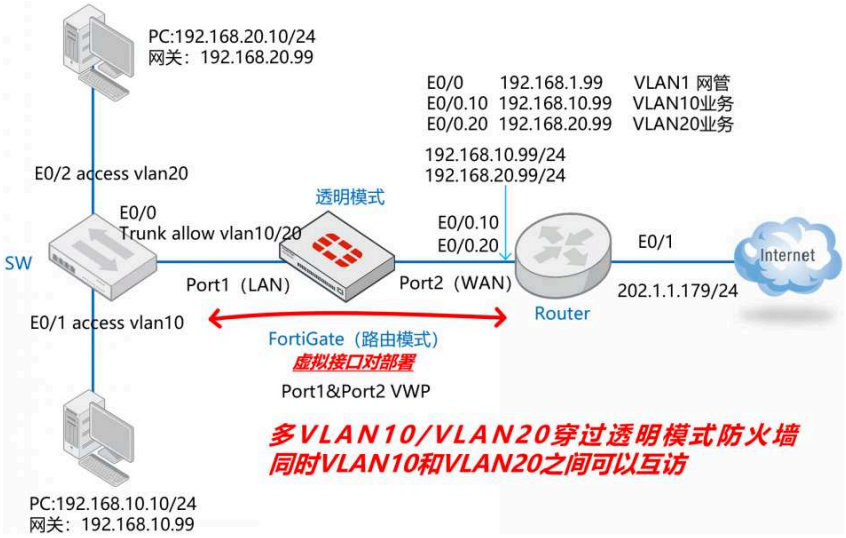
内部有两个VLAN（trunk环境），网关在路由器上，防火墙工作在虚拟接口对方式部署在核心交换与核心路由之间，允许两个VLAN访问外网，同时两个VLAN之间需要互访，并且对这两个VLAN进行保护，开启反病毒过滤。

网络拓扑

拓扑1：单VLAN透传



拓扑2：多VLAN透传，VLAN之间互访



配置要点

拓扑1：单VLAN透传

- SW交换机/Internet_R路由器的基础配置
- 配置虚拟接口对（Port1&Port2）
- 配置安全策略允许内网PC（VLAN10内主机）访问互联网

拓扑2：多VLAN透传，VLAN之间互访

- SW交换机/Internet_R路由器的基础配置
- 配置虚拟接口对（Port1&Port2）
- 配置安全策略允许内网PC（VLAN10和VLAN20内主机）访问互联网

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置步骤

拓扑1：单VLAN透传

1. SW交换机/Internet_R路由器的基础配置。

   SW：

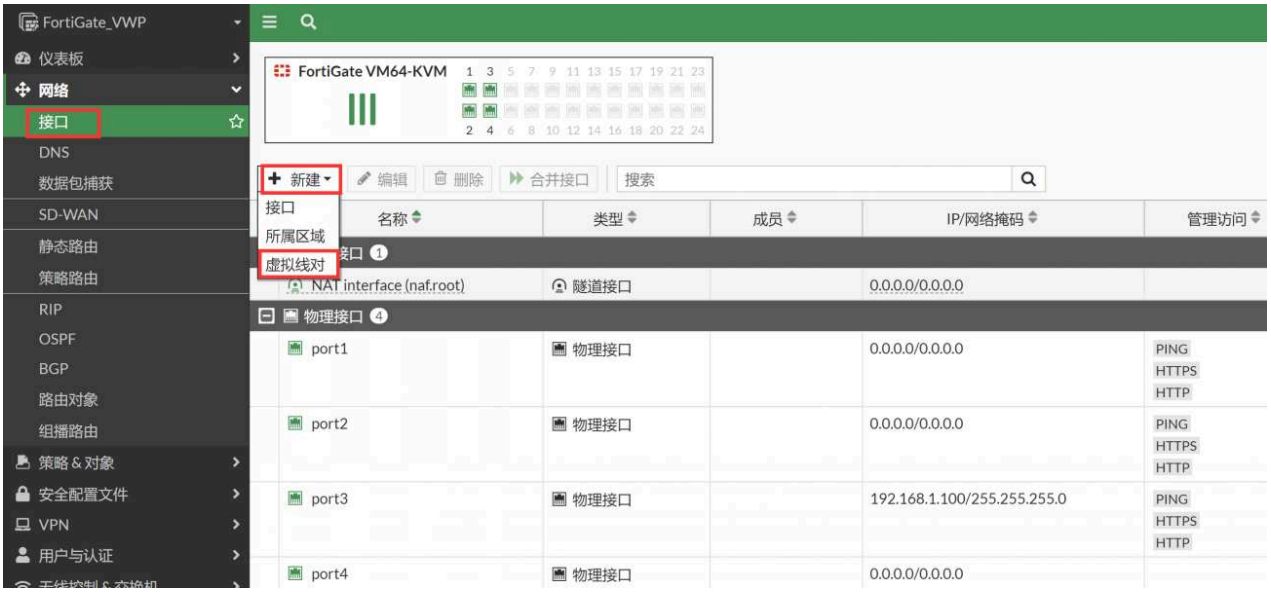
```
interface Ethernet0/0
switchport trunk allowed vlan 1,10
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
```

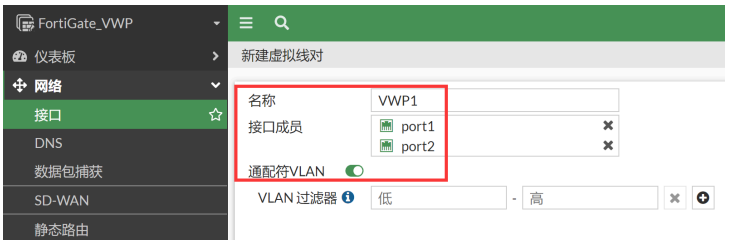
   Internet_R：

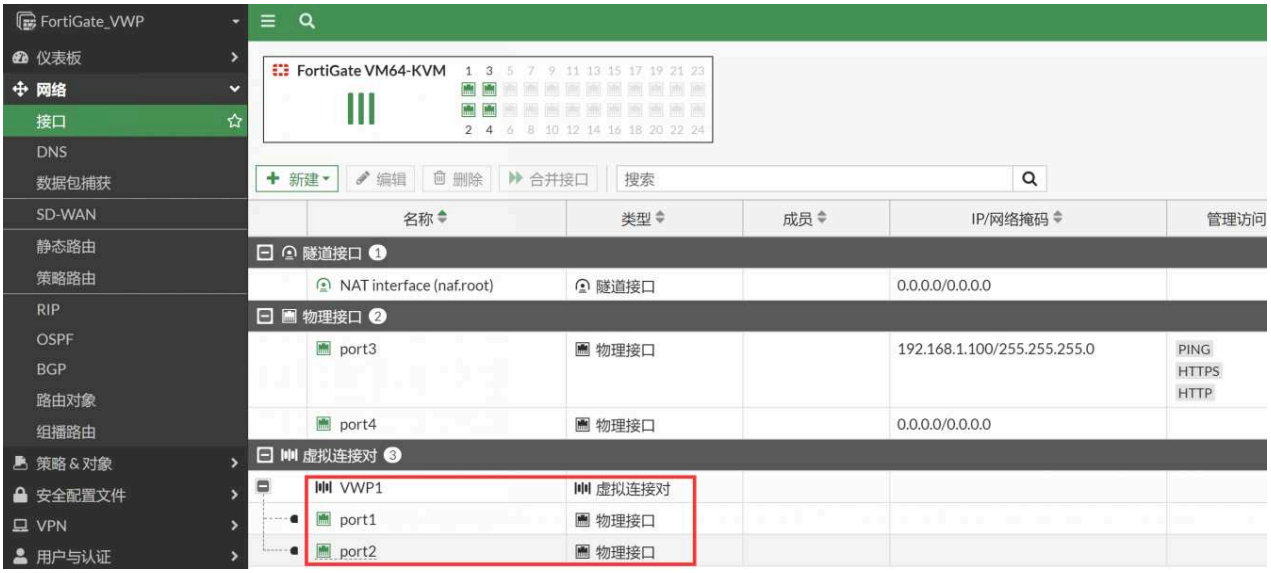
```
hostname Internet_R
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

2. 配置虚拟接口对（Port1&Port2），防火墙处于路由模式的情况下，直接创建虚拟接口对，将port1和port2加入到虚拟接口对中并开启通配符VLAN，识别VLAN-Tag的数据。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







3. 虚拟接口对通道正式打通，可以认为port1和port2之间可以透明的传输数据了（需要防火墙策略放通），对应的CLI如下。

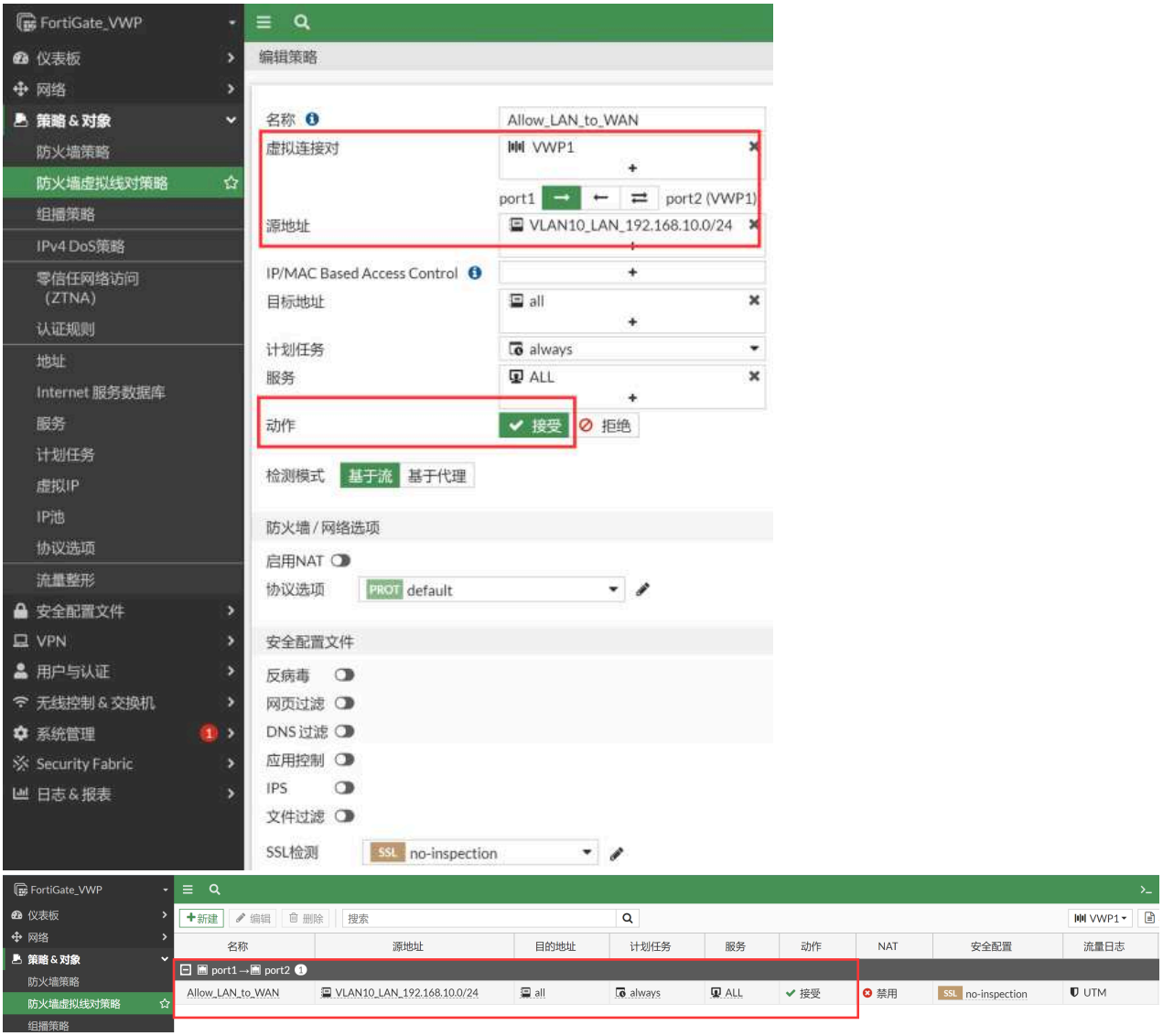
```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enable    //这个命令很关键，识别VLAN-TAG，VWP模式下无需再到本地创建对应的VLAN接口和Forwar-Domain了，大大的简化了策略的配置量
    next
end
```

4. 配置虚拟接口对的策略：允许LAN（Port2，VLAN10内网主机）到WAN（port1）的上网流量穿过FGT，策略&对象的位置会多出“防火墙虚拟线对策略”（如果没有看到，则刷新页面或注销管理登陆，重新登陆FGT即可看到）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 右上角选择VWP1线对，方向选择port1→port2（也可选择双向的方向），新建VWP策略（虚拟连接对可以选择多个，在同一条相同动作的策略中进行多接口控制）。



> **重要**
>
> 只需要配置VALN10网段到WAN的策略即可实现，配置很简单，可以忽略VLAN-TAG接口和Forward-Domain等透明模式下需要考虑的因素。

拓扑2：多VLAN透传，VLAN之间互访

1. SW交换机/Internet_R路由器的基础配置。

SW：

```
interface Ethernet0/0
switchport trunk allowed vlan 1,10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
```

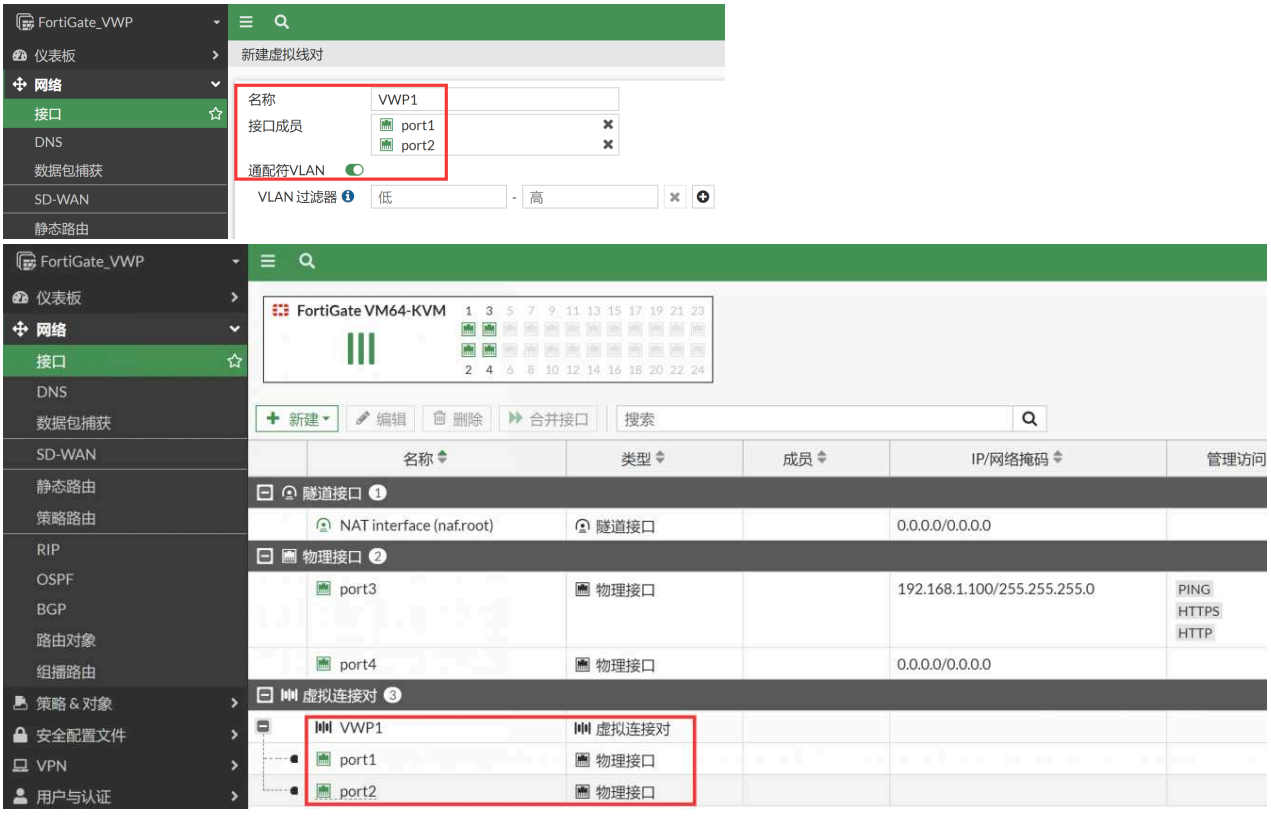

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
switchport access vlan 10
switchport mode access
!
interface Ethernet0/2
switchport access vlan 20
switchport mode access
```

Internet_R:

```
hostname Internet_R
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

2. 配置虚拟接口对（Port1&Port2），防火墙处于路由模式的情况下，直接创建虚拟接口对，将port1和port2加入到虚拟接口对中并开启通配符VLAN，识别VLAN-Tag的数据。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

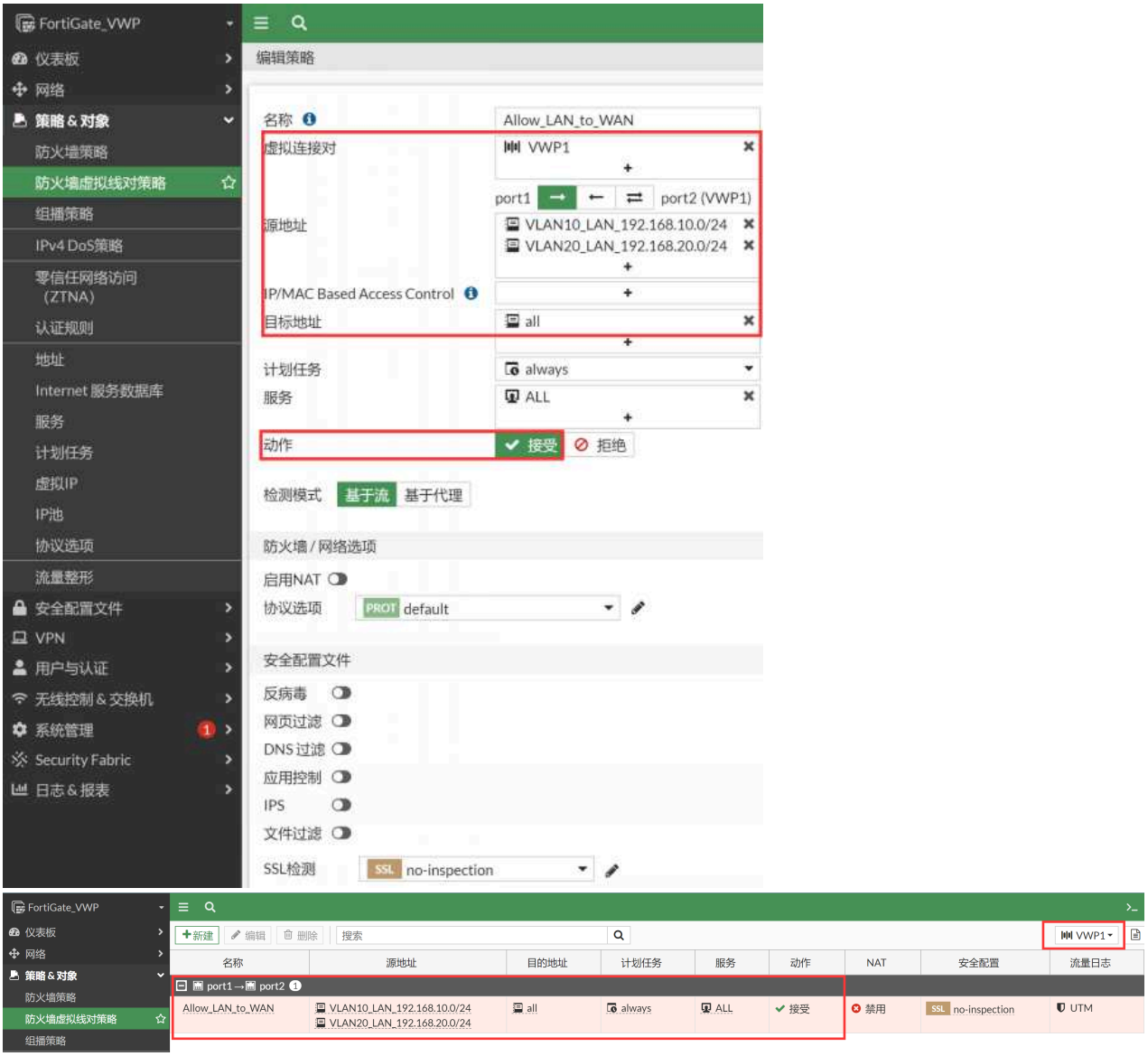
3. 虚拟接口对通道正式打通，可以认为port1和port2之间可以透明的传输数据了（需要防火墙策略放通），对应的CLI如下。

```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enable     //这个命令很关键，识别VLAN-TAG，VWP模式下无需再到本地创建对应的VLAN接口和Forwar-Domain
了，大大的简化了策略的配置量
    next
end
```

4. 配置虚拟接口对的策略：允许LAN（port1）到WAN（port2）的上网流量穿过FGT，策略&对象的位置会多出“防火墙虚拟线对策略”（如果没有看到，则刷新页面或注销管理登陆，重新登陆FGT即可看到）。



5. 右上角选择VWP1线对，方向选择port1→port2（也可选择双向的方向），新建VWP策略（虚拟连接对可以选择多个，在同一条相同动作的策略中进行多接口控制）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

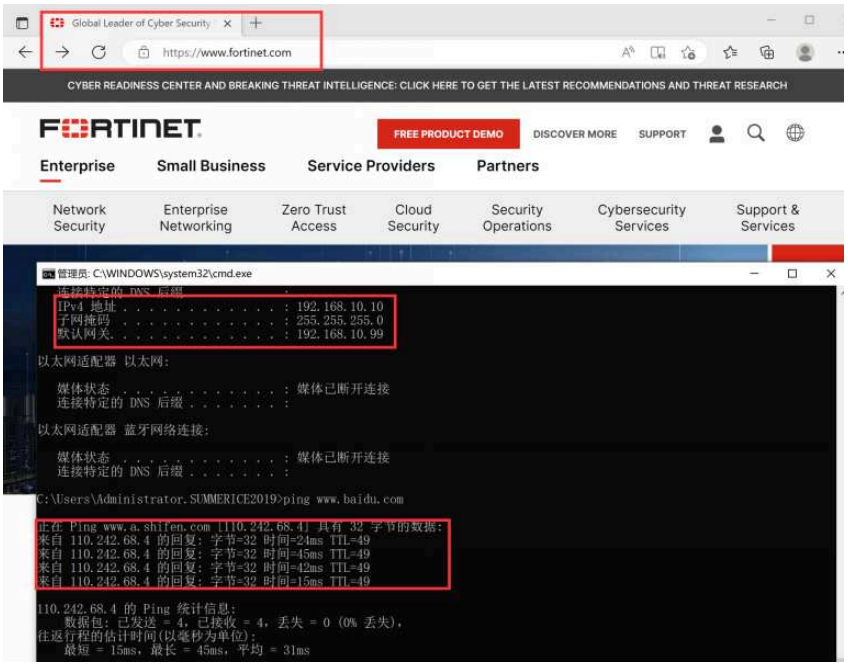
其实配置上上述两条策略数据就已经通了，因为两条策略的目的IP都是any，包括了192.168.20.0/24和192.168.10.0/24，如果要明细配置策略则需要将策略中的目标地址改为明细的地址对象，并放置到策略的最前面，以便优先匹配。

6. 只需要配置VALN10/VLAN20网段相互之间的策略即可，配置很简单，可以忽略VLAN-TAG接口和Forward-Domain等透明模式下需要考虑的因素。配置相对很简单。

效果验证

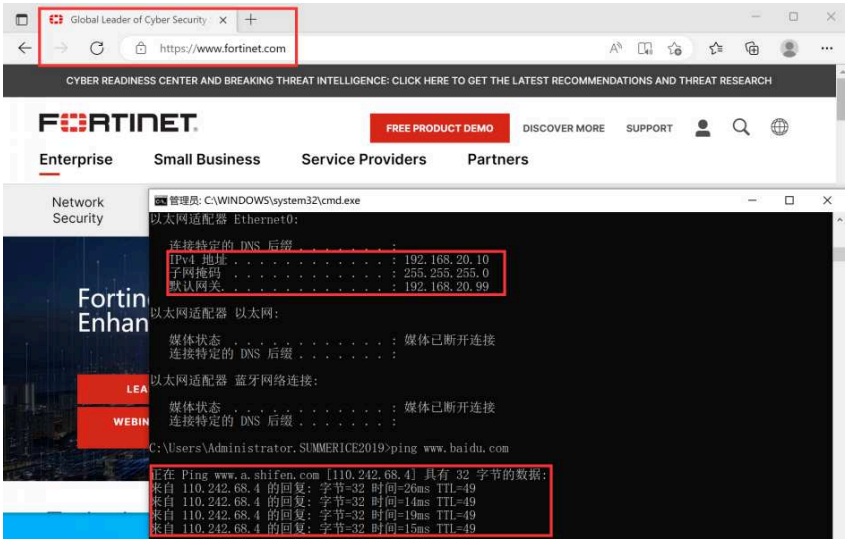
拓扑1：单VLAN透传

VLAN10内的PC通过透明模式的FortiGate访问互联网，可以正常访问。



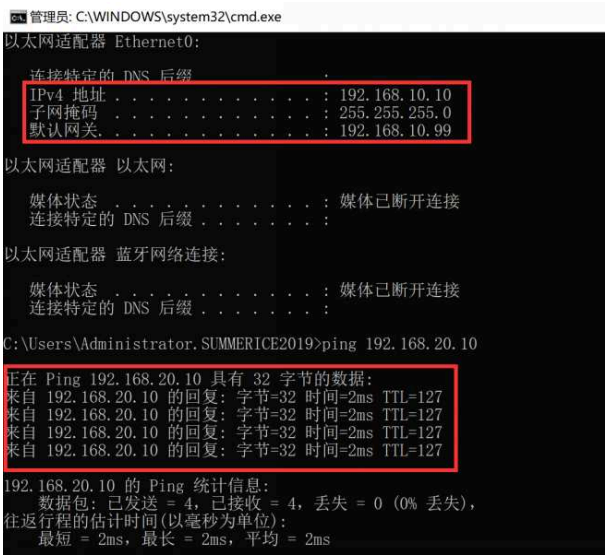
拓扑2：多VLAN10/20透传，VLAN之间互访

1. VLAN20内的PC访问互联网，可以正常访问。



2. VLAN10内的PC访问VLAN20的PC，可以正常访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 抓包查看VLAN10内的PC访问VLAN20的PC的流量，注意入方向携带VLAN-TAG的数据sniffer无法正常的显示明细数据。

```
FortiGate_VWP # diagnose sniffer packet any 'none' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[none]
21.060512 port1 in 802.1Q vlan#10 P0
21.060542 port2 out 192.168.10.10 → 192.168.20.10: icmp: echo request
21.062168 port2 in 802.1Q vlan#20 P0
21.062178 port1 out 192.168.10.10 → 192.168.20.10: icmp: echo request
21.065095 port1 in 802.1Q vlan#20 P0
21.065106 port2 out 192.168.20.10 → 192.168.10.10: icmp: echo reply
21.065540 port2 in 802.1Q vlan#10 P0
21.065546 port1 out 192.168.20.10 → 192.168.10.10: icmp: echo reply
```

4. debug flow以上流量。

```
id=20085 trace_id=1 func=print_pkt_detail line=5871 msg="vd-root:0 received a packet(proto=1, 192.168.10.10:1->192.168.20"
id=20085 trace_id=1 func=init_ip_session_common line=6050 msg="allocate a new session-00000821, tun_id=0.0.0.0"
id=20085 trace_id=1 func=br_fw_forward_handler line=573 msg="Allowed by Policy-1:"
id=20085 trace_id=1 func=__if_queue_push_xmit line=391 msg="send out via dev-port2, dst-mac-aa:bb:cc:00:20:00"
id=20085 trace_id=2 func=print_pkt_detail line=5871 msg="vd-root:0 received a packet(proto=1, 192.168.10.10:1->192.168.20.10:2048) tun_id"
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5957 msg="Find an existing session, id-00000821, original direction"
id=20085 trace_id=2 func=br_fw_forward_dirty_handler line=274 msg="auxiliary ses proto=1 dev=4→3 192.168.10.10/1⇒192.168.20.10/8"
id=20085 trace_id=2 func=npu_handle_session44 line=1183 msg="Trying to offloading session from port2 to port1, skb.npu_flag=00000400 ses."
id=20085 trace_id=2 func=br_fw_forward_dirty_handler line=297 msg="state=00008200, state2=00000000, npu_state=00000100"
id=20085 trace_id=2 func=__if_queue_push_xmit line=391 msg="send out via dev-port1, dst-mac-00:0c:29:ae:55:70"
id=20085 trace_id=3 func=print_pkt_detail line=5871 msg="vd-root:0 received a packet(proto=1, 192.168.20.10:1->192.168.10.10:0) tun_id=0."
id=20085 trace_id=3 func=resolve_ip_tuple_fast line=5957 msg="Find an existing session, id-00000821, reply direction"
id=20085 trace_id=3 func=br_fw_forward_dirty_handler line=274 msg="auxiliary ses proto=1 dev=4→3 192.168.10.10/1⇒192.168.20.10/8"
id=20085 trace_id=3 func=npu_handle_session44 line=1183 msg="Trying to offloading session from port1 to port2, skb.npu_flag=00000000 ses."
id=20085 trace_id=3 func=br_fw_forward_dirty_handler line=297 msg="state=00008200, state2=00000000, npu_state=00000100"
id=20085 trace_id=3 func=__if_queue_push_xmit line=391 msg="send out via dev-port2, dst-mac-aa:bb:cc:00:20:00"
id=20085 trace_id=4 func=print_pkt_detail line=5871 msg="vd-root:0 received a packet(proto=1, 192.168.20.10:1->192.168.10.10:0) tun_id=0."
id=20085 trace_id=4 func=resolve_ip_tuple_fast line=5957 msg="Find an existing session, id-00000821, reply direction"
```

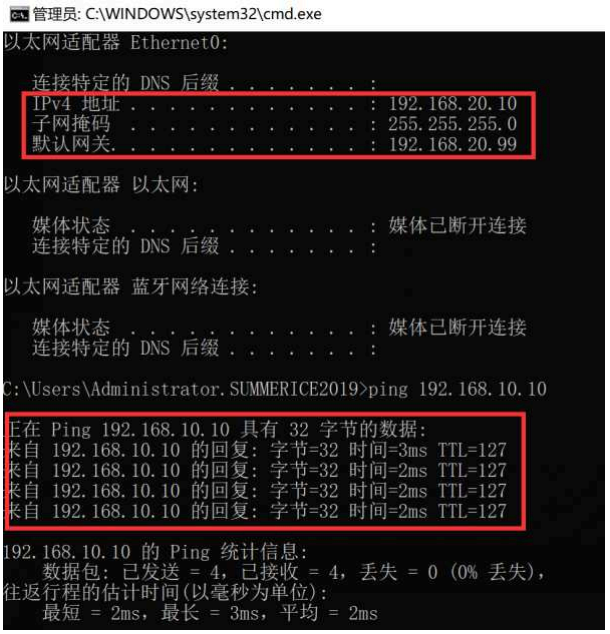

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
id=20085 trace_id=4 func=npu_handle_session44 line=1183 msg="Trying to offloading session from port2 to port1,
skb.npu_flag=00000400 ses."
id=20085 trace_id=4 func=br_fw_forward_dirty_handler line=297 msg="state=00008200, state2=00000000,
npu_state=00000100"
id=20085 trace_id=4 func=__if_queue_push_xmit line=391 msg="send out via dev-port1, dst-mac-00:0c:29:57:97:29"
```

5. 相关会话信息，可以看到reflect session的数量为1，为反向流量会话。

```
session info: proto=1 proto_state=00 duration=2 expire=57 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty br
statistic(bytes/packets/allow_err): org=120/2/1 reply=120/2/1 tuples=2
tx speed(Bps/kbps): 50/0 rx speed(Bps/kbps): 50/0
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.10.10:1->192.168.20.10:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.20.10:1->192.168.10.10:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=14730 auth_info=0 chk_client_info=0 vd=0
serial=0000096d tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
vlanid=10 npu_state=0x000100
no_ofld_reason:  npu-flag-off
ext_header_type=0x22:0x22
reflect info 0:
dev=4->3/3->4
npu_state=0x000100
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
total reflect session num: 1
total session 1
```

6. 使用VLAN20内网PC访问VLAN10内网PC，也可以正常访问（具体抓包和debug过程和上述一致）。



补充说明

1. 关于VLAN-forward参数，默认在VWP的环境下，成员接口的vlanforward是打开的。

```
onfig system interface
    edit "port1"
        set vdom "root"
        set vlanforward enable    //默认开启
        set type physical
        set alias "WAN"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set snmp-index 1
    next
end
FortiGate_VWP (port1) # next
FortiGate_VWP (interface) # edit port2
FortiGate_VWP (port2) # show
config system interface
    edit "port2"
        set vdom "root"
        set vlanforward enable    //默认开启
        set type physical
        set alias "LAN"
        set snmp-index 2
    next
end
```

2. 但是如果已经开启了set wildcard-vlan enable的情况下，set vlanforward enable是不生效的。set wildcard-vlan enable的优先级比vlanforward要高，都开启的情况下，FortiGate会优先使用set wildcard-vlan enable。

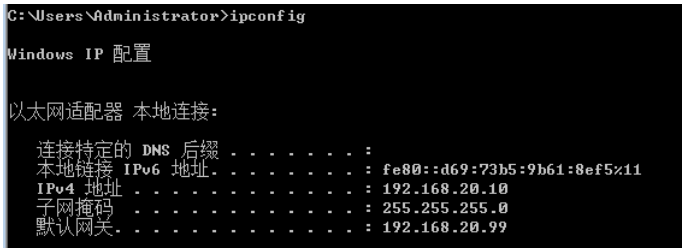
总结

1. 开启了wildcard-vlan enable，vlanforward不生效，wildcard-vlan优先，识别VLAN-TAG，并上送到FGT的CPU上去策略处理。这是推荐的配置。
2. 如果关闭了wildcard-vlan disable，则vlanforward生效，则携带了vlan-tag的数据会直接穿透VWP接口，不再匹配策略，直接bypass可通（不推荐这样使用，流量不可见也不可控，这不是安全设备想要的结果，具体参考网络管理→透明模式→传统透明模式→VLAN与透明模式→vlanforward ↗章节）。
3. 具体现象可以尝试关闭wildcard-vlan，清空VWP策略。

```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan disable  //关闭wildcard
    next
end
config system interface
    edit "port1"
        set vdom "root"
        set vlanforward enable
        set type physical
        set alias "WAN"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set vlanforward enable
        set type physical
        set alias "LAN"
        set snmp-index 2
    next
end

FortiGate_VWP # config firewall policy
FortiGate_VWP (policy) # purge    （清除策略，让设备没有任何策略）
This operation will clear all table!
Do you want to continue? (y/n)y
FortiGate_VWP (policy) # end
```

4. 具体的数据转发现象呢？我们会发现，所有的携带了VLAN-TAG的数据都是通的，VLAN10/20的PC可以上网，VLAN10和VLAN20的PC相互可通信。但是在FGT上看不到任何的信息，抓不到任何的包，直接bypass掉携带了VLAN-TAG的数据。VWP不处理携带了VLAN-TAG的数据。而不携带VLAN-TAG的数据（VLAN1）将会上送到FGT的CPU进行策略匹配处理。携带了VLAN-TAG的数据被bypass掉了，直接可通。（vlan1的不携带vlan-tag的数据会上送到CPU进行处理，需要策略放通才可以正常通信。）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





5. 抓不到相应的报文。但是数据是可通的。

```
FortiGate_VWP # diagnose sniffer packet any "host 192.168.20.10" 4
interfaces=[any]
filters=[host 192.168.20.10]
```

6. 实际上可以抓到VLAN-TAG的数据，只是FGT由于开启了vlanforward，不处理携带了VLAN-TAG的数据，直接bypass掉了（不推荐这样的部署）。

```
FortiGate_VWP # diagnose sniffer packet any "none" 4
interfaces=[any]
filters=[none]
1.189503 port2 in 802.1Q vlan#20 P0
1.475067 port2 in 802.1Q vlan#20 P0
1.475081 port1 out 802.1Q vlan#20 P0
1.475749 port1 in 802.1Q vlan#20 P0
1.475756 port2 out 802.1Q vlan#20 P0
1.568623 port2 in 802.1Q vlan#10 P0
1.568668 port1 out 802.1Q vlan#10 P0
2.211987 port2 in 802.1Q vlan#10 P0
2.226707 port2 in 802.1Q vlan#10 P0
2.226719 port1 out 802.1Q vlan#10 P0
2.246979 port2 in 802.1Q vlan#10 P0
2.246985 port1 out 802.1Q vlan#10 P0
2.248370 port2 in 802.1Q vlan#10 P0
2.248377 port1 out 802.1Q vlan#10 P0
2.356281 port2 in 802.1Q vlan#10 P0
2.356287 port1 out 802.1Q vlan#10 P0
2.357778 port2 in 802.1Q vlan#10 P0
2.357784 port1 out 802.1Q vlan#10 P0
2.468629 port2 in 802.1Q vlan#10 P0
2.468643 port1 out 802.1Q vlan#10 P0
2.489493 port2 in 802.1Q vlan#20 P0
2.489500 port1 out 802.1Q vlan#20 P0
2.490062 port1 in 802.1Q vlan#20 P0
2.490067 port2 out 802.1Q vlan#20 P0
3.290091 port2 in 802.1Q vlan#20 P0
3.502555 port2 in 802.1Q vlan#20 P0
3.502570 port1 out 802.1Q vlan#20 P0
3.503316 port1 in 802.1Q vlan#20 P0
3.503322 port2 out 802.1Q vlan#20 P0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

7. 推荐开启 wildcard-vlan （set wildcard-vlan enable），让FGT可以识别VLAN-TAG的数据，然后使用策略控制所有的携带和不携带VLAN-TAG的数据流。

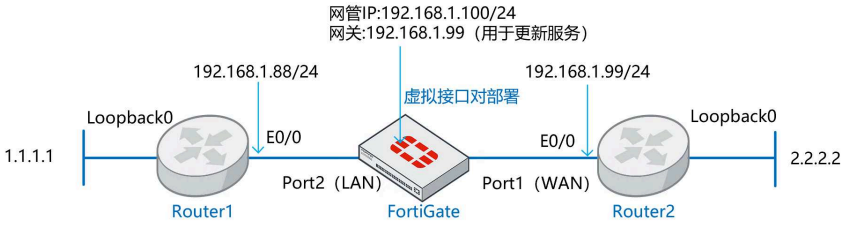
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

组播(OSPF)与虚拟接口对

网络需求

路由器1和路由器2之间运行了动态路由协议，防火墙以虚拟接口对的方式运行在两台路由器之间，需要确保两台路由器之间的动态路由协议运行正常，并且数据可通。

网络拓扑



R1和R2之间运行了RIP/OSPF/EIGRP协议

配置要点

- Router1/Router2路由器的基础配置
- 将防火墙的port1和port2配置为虚拟接口对
- 默认不配置策略情况下，观察动态路由协议的情况
- 配置安全策略解决OSPF/EIGRP邻居关系异常

配置步骤与结果验证

1. Router1/Router2路由器的基础配置。

Router1：

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.1.88 255.255.255.0
no shutdown
!
router ospf 10
network 1.1.1.1 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
router rip
version 2
network 1.0.0.0
network 192.168.1.0
no auto-summary
!
router eigrp 10
network 1.1.1.1 0.0.0.0
network 192.168.1.0
```

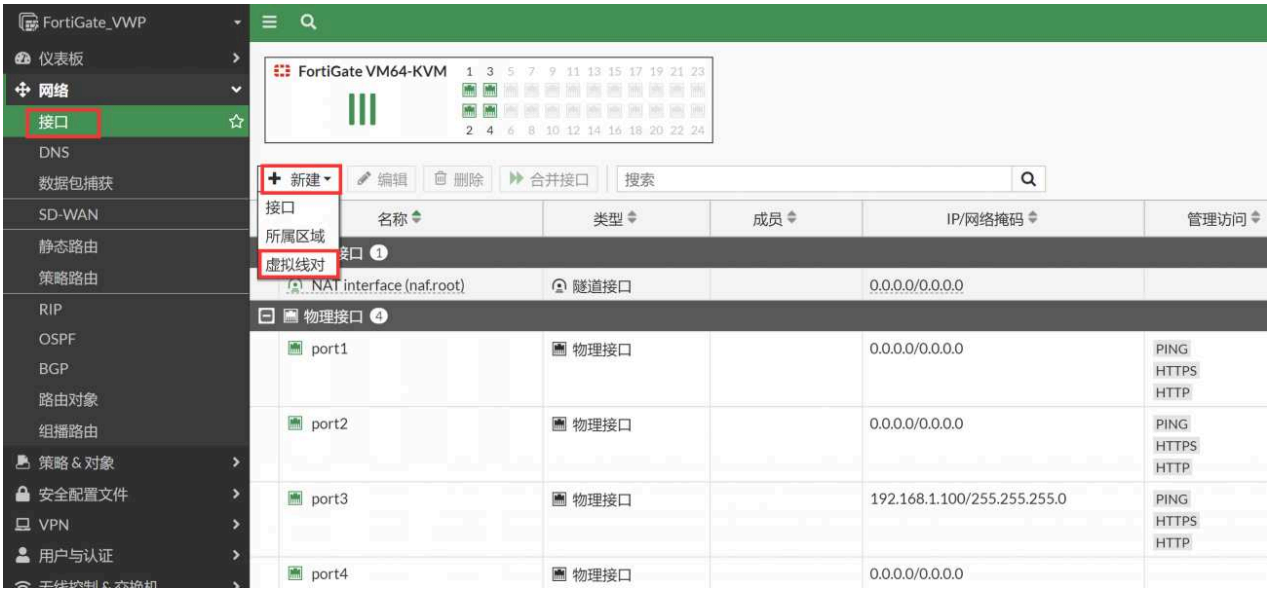
Router2：

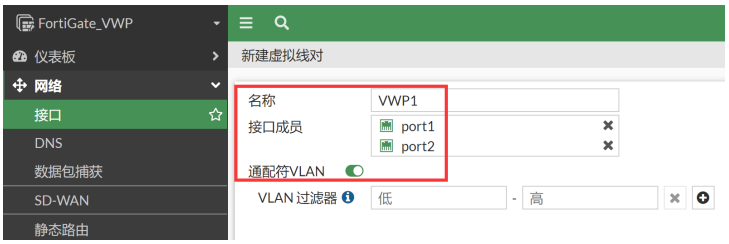
```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
!
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
router ospf 10
network 2.2.2.2 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
router rip
version 2
network 2.0.0.0
network 192.168.1.0
no auto-summary
!
router eigrp 10
network 2.2.2.2 0.0.0.0
network 192.168.1.0

```

2. 将防火墙的port1和port2配置为虚拟接口对，防火墙处于路由模式的情况下，直接创建虚拟接口对，将port1和port2加入到虚拟接口对中并开启通配符VLAN，识别VLAN-Tag的数据（推荐开启通配符VLAN）。







3. 虚拟接口对通道正式打通，可以认为port1和port2之间可以透明的传输数据了（需要防火墙策略放通），对应的CLI如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enable    //这个命令很关键，识别VLAN-TAG，VWP模式下无需再到本地创建对应的VLAN接口和Forwar-Domain了，大大的简化了策略的配置量
    next
end
```

4. 默认不配置任何策略情况下，观察动态路由协议的情况，RIP 邻居是不正常的（无邻居，无路由），OSPF邻居无法建立成功，EIGRP邻居无法建立成功。

```
Router1#show ip rip database
1.0.0.0/8    auto-summary
1.1.1.1/32    directly connected, Loopback0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, Ethernet0/0

Router1#show ip route
 ...
Gateway of last resort is not set
      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/0
L        192.168.1.88/32 is directly connected, Ethernet0/0

Router1#show ip ospf  neighbor

Router1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
```

原因分析

1. 我们知道RIP/OSPF/EIGRP都是用组播IP来建立邻居关系，同时OSPF和RIGRP也有单播报文的交互：

```
RIP:  UDP 520  ||  组播 224.0.0.9
OSPF: IP 89   ||  组播 224.0.0.5/224.0.0.6  ||  单播 DBD报文使用单独发送
EIGRP: IP 88  ||  组播 224.0.0.10   ||  单播 UPDATE报文使用单播传递我们会发现在VWP环境中，RIP/OSPF/EIGRP路由协议统统失败。这和透明模式下的现象是不一样的。
```

2. 我们会发现在VWP环境中，RIP/OSPF/EIGRP路由协议统统失败。这和透明模式下的现象是不一样的。

   - 透明模式下：RIP是正常的，OSPF的邻居虽然无法建立但组播交互是正常的，EIRGP的邻居虽然失败但是组播交互也是正常的。
   - VWP模式下：RIP/OSPF/EIGRP都不行，组播单播都无法通信。

3. 我们再VWP模式下抓包查看，邻居交互的组播报文都只有IN，没有OUT，组播报文默认都被丢弃了。这是透明模式的VWP模式最大的一个区别，透明模式下组播默认存在一条any到any允许可以通的组播策略，而VWP实际上是运行在路由模式下的，而路由模式下的组播默认是被隐藏丢弃的。这是二者现象不一样的最关键原因，因此RIP/OSPF/EIGRP三者全挂。

```
FortiGate_VWP # diagnose sniffer packet any "host 192.168.1.88" 4
interfaces=[any]
filters=[host 192.168.1.88]
1501.278671 port2 in 192.168.1.88.520 → 224.0.0.9.520: udp 24
1501.278765 port3 in 192.168.1.88.520 → 224.0.0.9.520: udp 24

1502.138508 port2 in 192.168.1.88 → 224.0.0.5:  ip-proto-89 56
1502.138837 port3 in 192.168.1.88 → 224.0.0.5:  ip-proto-89 56

1511.257832 port2 in 192.168.1.88 → 224.0.0.10:  ip-proto-88 40
1511.258000 port3 in 192.168.1.88 → 224.0.0.10:  ip-proto-88 40

1512.054185 port2 in 192.168.1.88 → 224.0.0.5:  ip-proto-89 56
1512.054332 port3 in 192.168.1.88 → 224.0.0.5:  ip-proto-89 56

1520.487732 port2 in 192.168.1.88 → 224.0.0.10:  ip-proto-88 40
1520.487883 port3 in 192.168.1.88 → 224.0.0.10:  ip-proto-88 40

1527.402323 port2 in 192.168.1.88.520 → 224.0.0.9.520: udp 24
1527.402499 port3 in 192.168.1.88.520 → 224.0.0.9.520: udp 24
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

解决办法

1. 既然知道问题的原因，那么解决办法就很简单了，只需要放通组播的策略，然后再放通单播的策略即可。

2. 首先在系统管理→可见功能，打开组播策略GUI的显示。

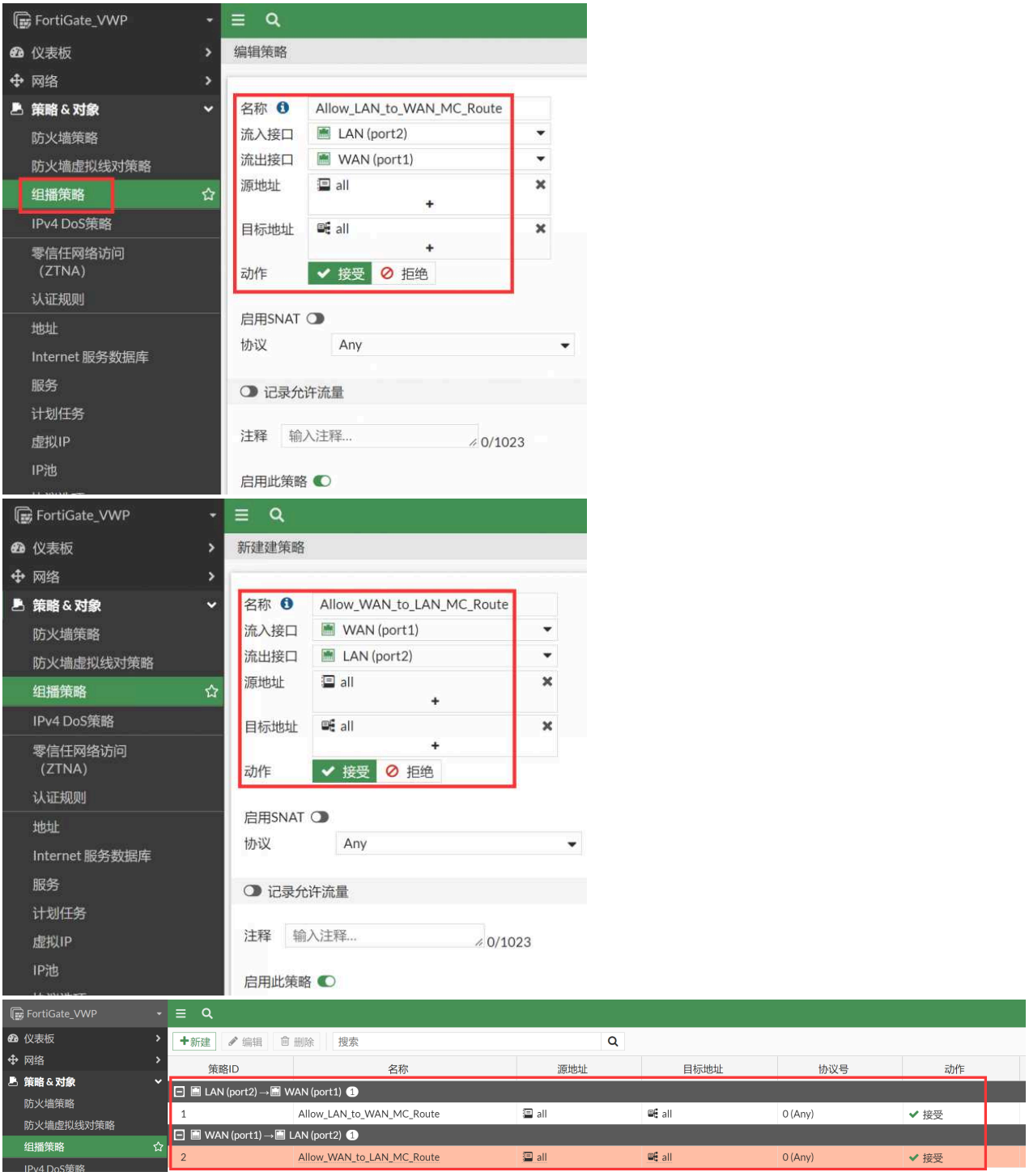


3. 进入策略&对象→组播策略中，可以看到默认的丢弃策略是隐藏的。



4. 新增组播策略允许路由组播通过。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 组播策略配置完毕，RIP协议就工作正常了。

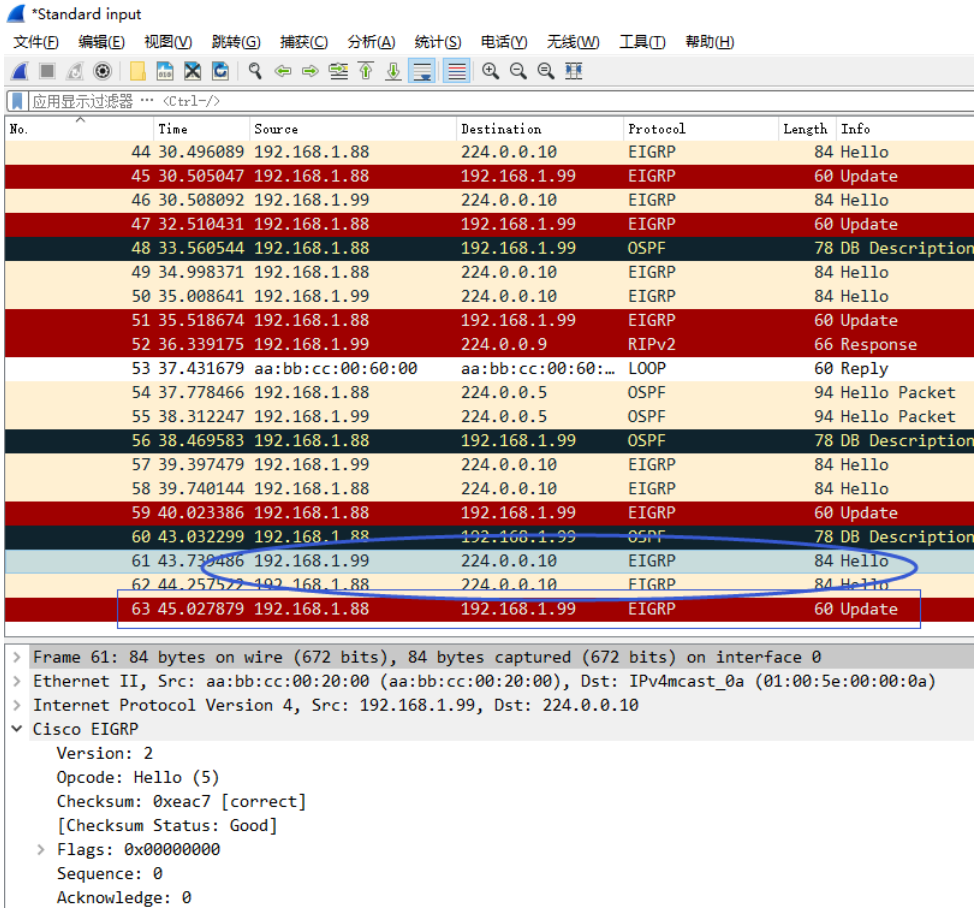
```
Router1#show ip rip database
1.0.0.0/8    auto-summary
1.1.1.1/32    directly connected, Loopback0
2.0.0.0/8    auto-summary
2.2.2.2/32
    [1] via 192.168.1.99, 00:00:01, Ethernet0/0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, Ethernet0/0

Router1#show ip route
 ...
R        2.2.2.2 [120/1] via 192.168.1.99, 00:00:03, Ethernet0/0
 ...
```

6. RIP协议只涉及到组播报文发送，但是OSFP和EIGRP邻居还是失败的，因为OSPF和EIGRP的邻居建立过程中需要单播的通信，我们来看现象。

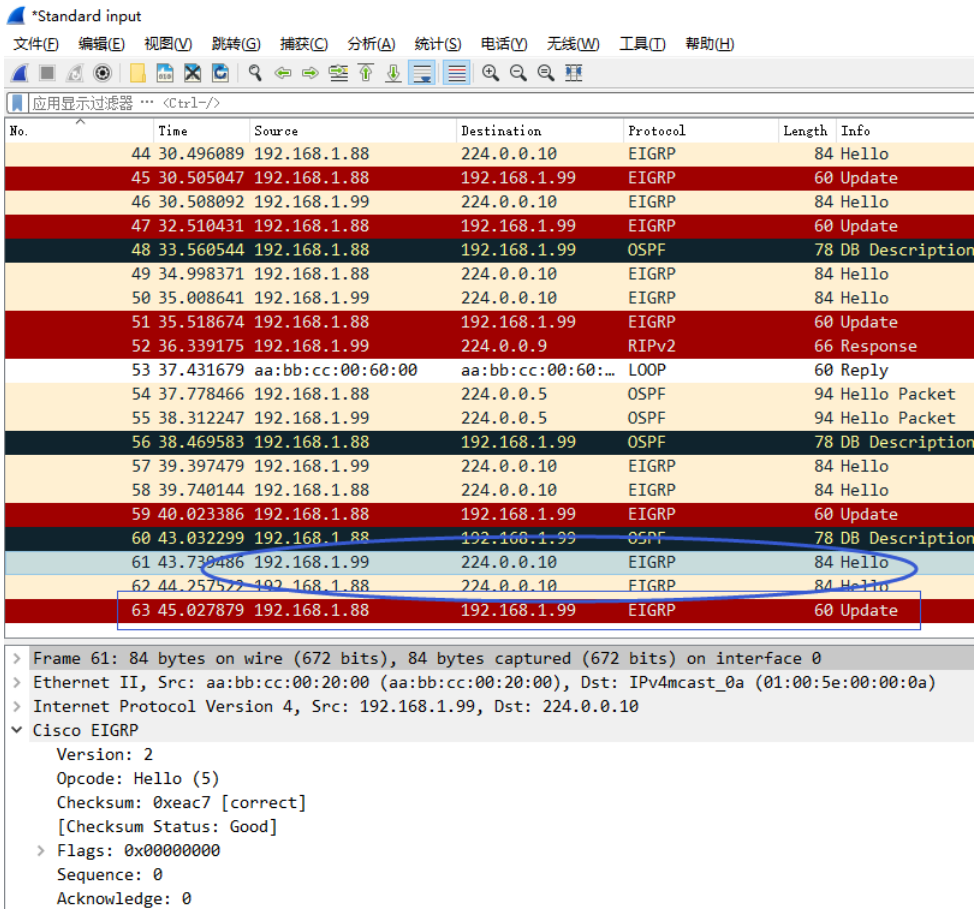
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Router1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 10)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         274         0×80000003 0×00F9A5 2

Router1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   INIT/DROTHER    00:00:37    192.168.1.99    Ethernet0/0

Router1#
*Jul  2 07:55:15.999: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Ethernet0/0 from EXSTART to DOWN, Neighbor Down:
Too many retransmissions
*Jul  2 07:56:16.002: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Ethernet0/0 from DOWN to DOWN, Neighbor Down:
Ignore timer expired
```

7. 这就和透明模式的现象完全一致了，进一步分析原因，OSPF和EIGRP的组播其实是正常转发的，但是OSPF和EIGRP建立邻居关系不仅仅只使用了组播，而且还使用单播，默认情况下没有任何策略情况下，单播的数据会被默认丢弃，因此邻居关系异常。OSPF的DB Description报文使用单播，EIGRP的Update报文使用单播。这是OSPF和EIGRP邻居关系还是异常的原因。如下抓包所示，OSPF和EIGRP邻居建立过程中的单播报文被FGT丢弃了。



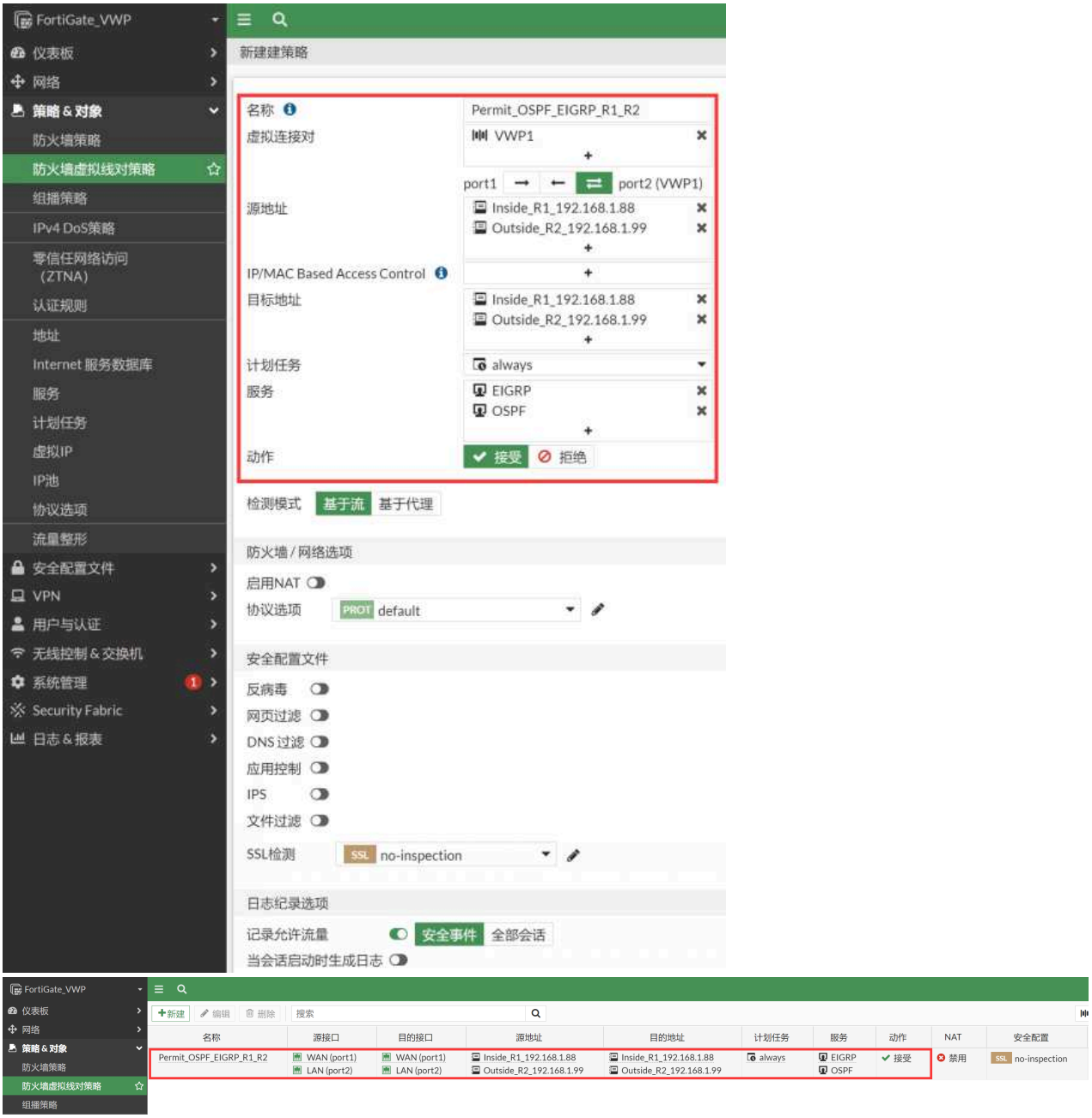
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
FortiGate_VWP # diagnose sniffer packet any "host 192.168.1.88" 4
interfaces=[any]
filters=[host 192.168.1.88]
1.720001 port1 in 192.168.1.99 → 192.168.1.88:  ip-proto-88 20   //EIGRP单播数据只有IN没有OUT，被策略丢弃
1.747272 port2 in 192.168.1.88 → 192.168.1.99:  ip-proto-88 20

3.144458 port2 in 192.168.1.88 → 224.0.0.10:  ip-proto-88 40   //EIGRP组播数据有IN有OUT
3.144472 port1 out 192.168.1.88 → 224.0.0.10:  ip-proto-88 40

21.561302 port2 in 192.168.1.88 → 224.0.0.5:  ip-proto-89 56   //OSPF组播数据有IN有OUT
21.561320 port1 out 192.168.1.88 → 224.0.0.5:  ip-proto-89 56

22.021894 port2 in 192.168.1.88 → 192.168.1.99:  ip-proto-89 44  //OSPF单播数据只有IN没有OUT，被策略丢弃
22.023435 port2 in 192.168.1.88 → 192.168.1.99:  ip-proto-89 60
```

8. 既然OSPF和EIGRP邻居建立不起来的原因清楚了，那么要解决这个问题就很简单了。只需要增加普通的IPv4单播策略即可。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



9. 上述策略配置完毕，会发现RIP/OSPF/EIGRP的三者的邻居关系都已经正常建立，路由学习也正常。

```
*Oct 15 09:20:13.561: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.1.99 (Ethernet0/0) is up: new adjacency
*Oct 15 09:20:39.923: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Ethernet0/0 from LOADING to FULL, Loading Done
Router1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:34    192.168.1.99    Ethernet0/0

Router1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.1.99            Et0/0                    13 00:03:06   23   138  0  35

Router1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 192.168.1.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 2.2.2.2/32, 1 successors, FD is 409600
        via 192.168.1.99 (409600/128256), Ethernet0/0
P 1.1.1.1/32, 1 successors, FD is 128256
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
         via Connected, Loopback0

Router1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 10)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         252         0×80000005 0×0098DF 2
2.2.2.2         2.2.2.2         253         0×80000005 0×008DD3 2
                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.99    2.2.2.2         253         0×80000001 0×003B1D

Router1#show ip rip database
1.0.0.0/8    auto-summary
1.1.1.1/32    directly connected, Loopback0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, Ethernet0/0

Router1#show ip route
 ...
D        2.2.2.2 [90/409600] via 192.168.1.99, 00:02:51, Ethernet0/0
 ...
```

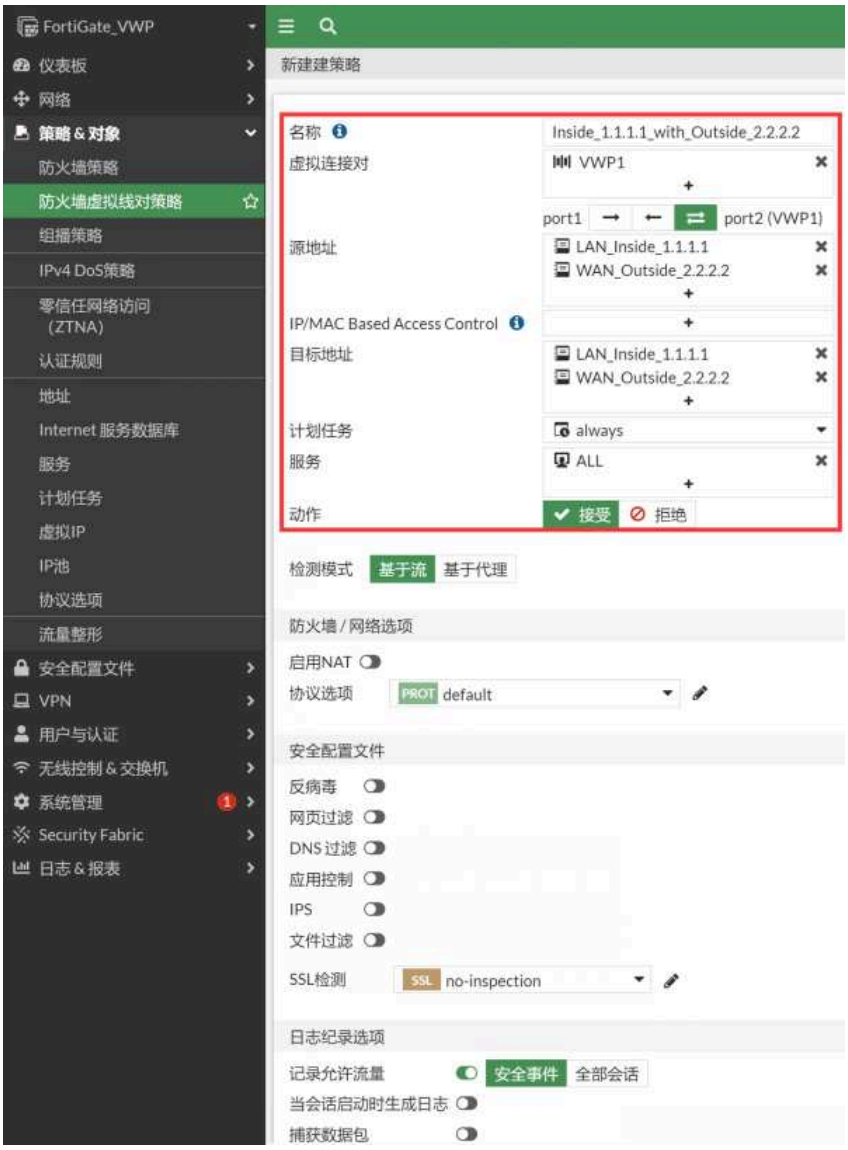
0. 需要配置业务策略允许Router1的1.1.1.1访问Router2的2.2.2.2，没配置策略之前是不通的。

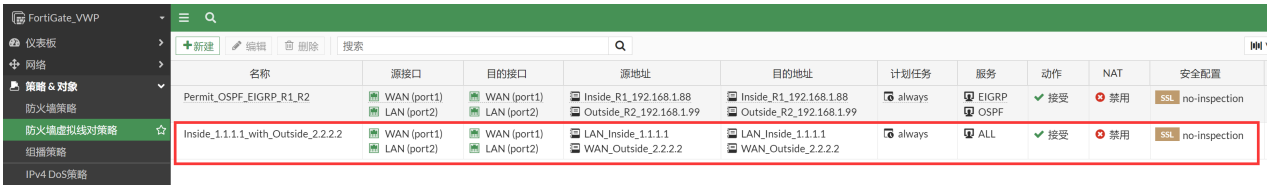
```
Router1#ping 2.2.2.2 source  1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)
```

1. 配置VWP策略允许 Router1的1.1.1.1访问Router2的2.2.2.2。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







2. 测试Router1的1.1.1.1访问Router2的2.2.2.2，可以正常访问。

```
Router1#ping 2.2.2.2 source  1.1.1.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/9 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate_VWP # diagnose sniffer packet any "icmp" 4
interfaces=[any]
filters=[icmp]
5.551382 port2 in 1.1.1.1 → 2.2.2.2: icmp: echo request
5.551455 port1 out 1.1.1.1 → 2.2.2.2: icmp: echo request
5.552281 port1 in 2.2.2.2 → 1.1.1.1: icmp: echo reply
5.552292 port2 out 2.2.2.2 → 1.1.1.1: icmp: echo reply
```

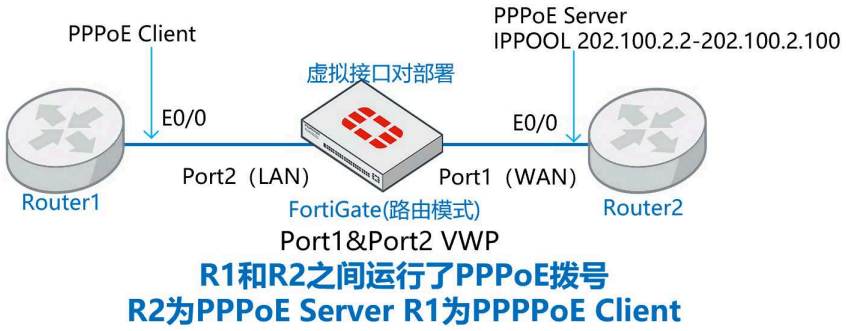

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

非IP流量(PPPOE)与虚拟接口对

网络需求

路由器1和路由器2之间运行了PPPOE协议（非IP协议），防火墙以虚拟接口对运行在两台路由器之间，需要确保路由器1的PPPOE拨号正常。

网络拓扑



配置要点

- Router1/Router2路由器的基础配置
- 将防火墙的port1和port2配置为虚拟接口对
- 默认情况下，观察PPPOE拨号的情况
- 配置l2forward解决非IP流量转发问题

配置步骤与结果验证

1. Router1/Router2路由器的基础配置。

Router1：

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
no ip address
no shutdown
pppoe enable group global
pppoe-client dial-pool-number 1
!
interface Dialer1
mtu 1492
ip address negotiated
encapsulation ppp
dialer pool 1
ppp pap sent-username pppoeuser1 password 0 fortinet
ppp ipcp route default
```

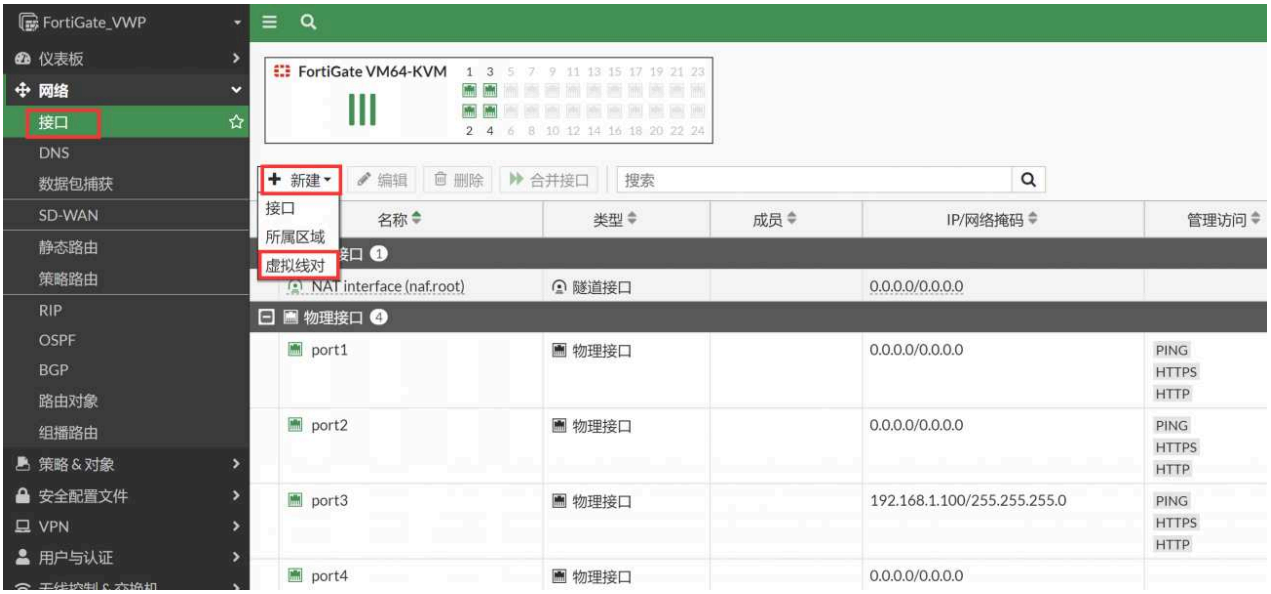
Router2：

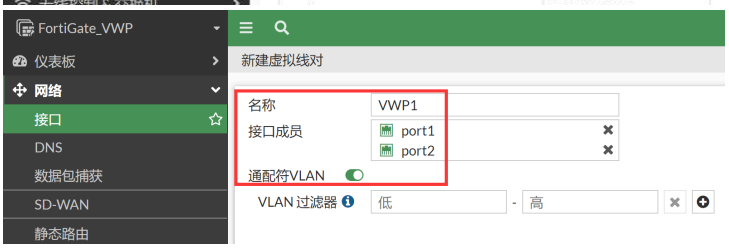
```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
username pppoeuser1 password 0 fortinet
!
bba-group pppoe bba1
virtual-template 1
!
interface Loopback1
ip address 202.100.2.1 255.255.255.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
!
interface Ethernet0/0
no ip address
no shutdown
pppoe enable group bba1
!
interface Virtual-Template1
description PPPOE bba1
mtu 1492
ip unnumbered Loopback1
peer default ip address pool pool1
ppp authentication pap
!
ip local pool pool1 202.100.2.2 202.100.2.100

```

2. 将防火墙的port1和port2配置为虚拟接口对，防火墙处于路由模式的情况下，直接创建虚拟接口对：将port1和port2加入到虚拟接口对中并开启通配符VLAN，识别VLAN-Tag的数据（推荐开启通配符VLAN）。







3. 虚拟接口对通道正式打通，可以认为port1和port2之间可以透明的传输数据了（需策略放通），对应的命令行如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

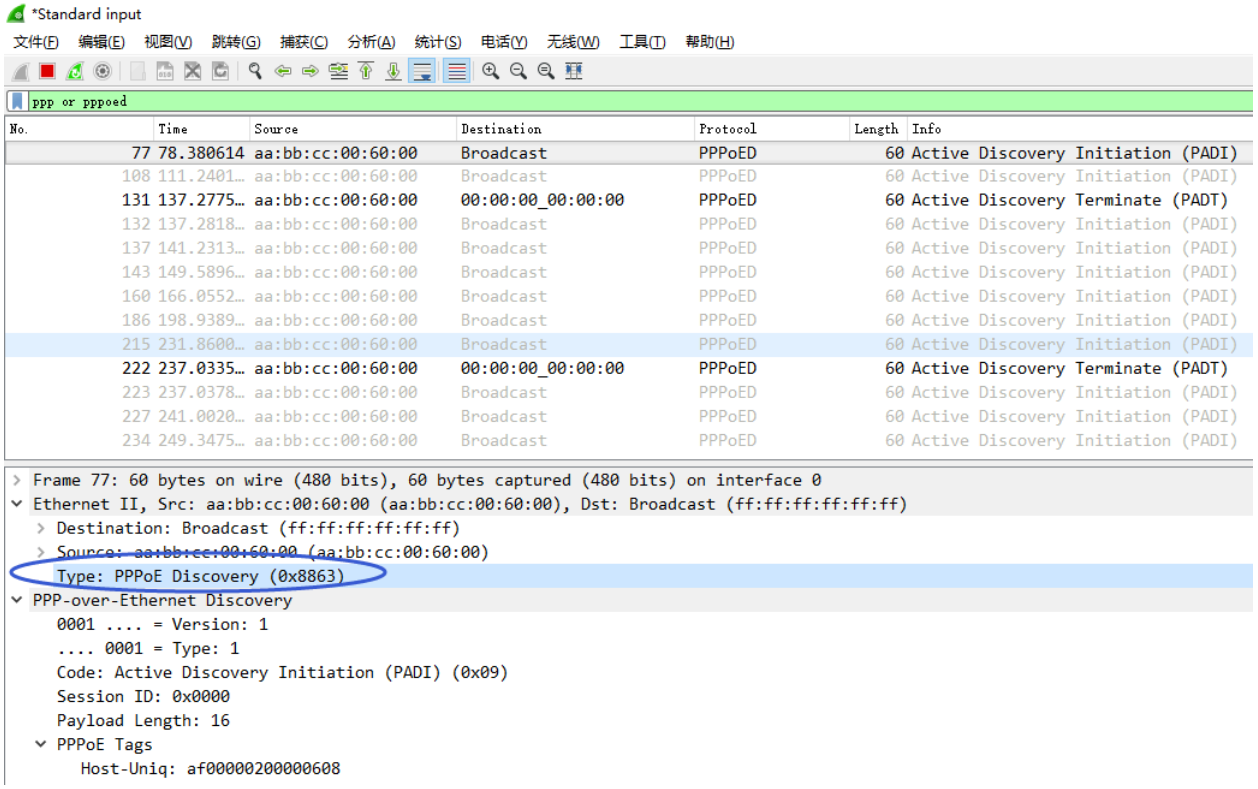
```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enable
    next
end
```

4. 默认情况下，观察PPPOE拨号的情况，Router1（PPPOE Client）无法PPPPOE拨号成功。

```
Router1#show ip route
 ...
Gateway of last resort is not set
      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0

Router1#show ip int brief
 ...
Dialer1                    unassigned      YES IPCP   up                    up
 ...
```

5. 通过在FGT上抓包可以看到FGT并不转发PPPOE的报文，非IP的PPPOE数据默认不会被FGT所转发。

```
FortiGate_VWP # diagnose sniffer packet any "pppoed" 4
interfaces=[any]
filters=[pppoed]
4.124126 port1 in pppoe printer hasn't been added to sniffer
37.014209 port1 in pppoe printer hasn't been added to sniffer
69.908430 port1 in pppoe printer hasn't been added to sniffer
102.798634 port1 in pppoe printer hasn't been added to sniffer
135.705063 port1 in pppoe printer hasn't been added to sniffer
```



6. 那么要如何解决此情况呢？在FGT的虚拟接口对的具体接口下配置set l2forward enable即可！

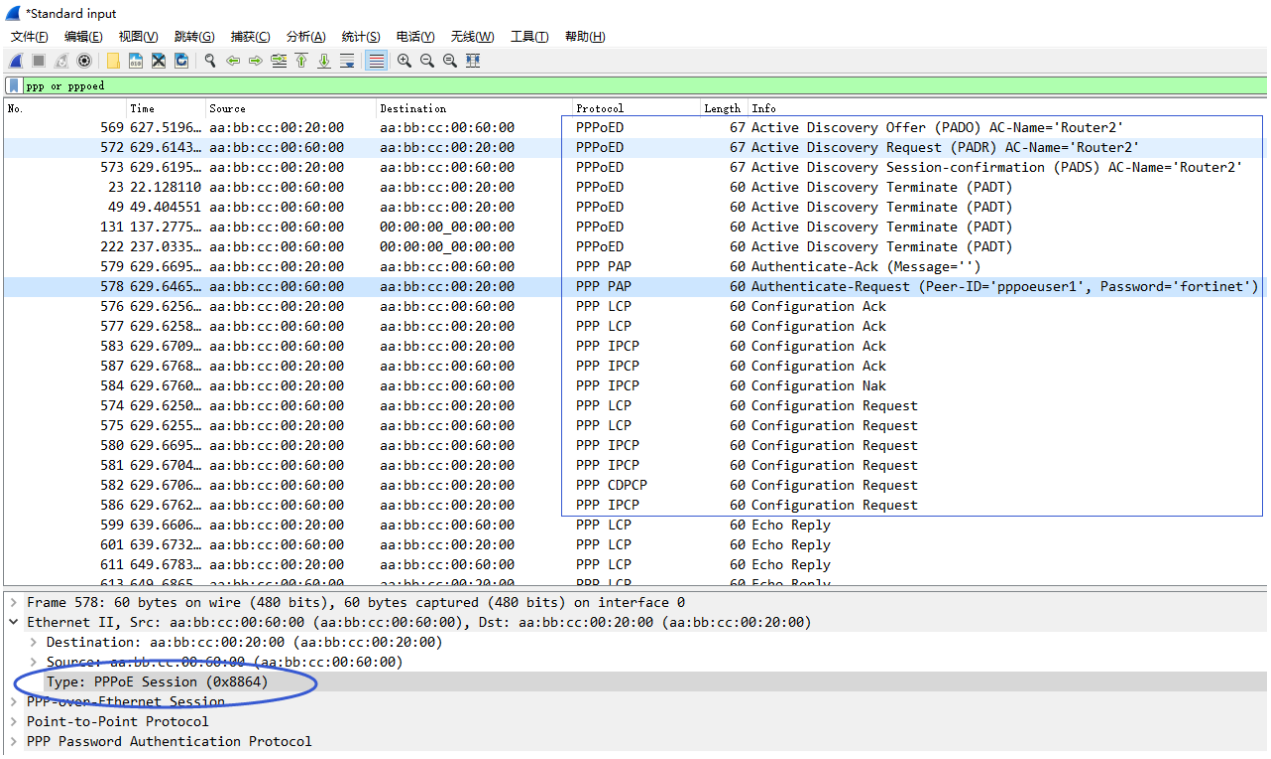
```
FortiGate_VWP # config system interface
FortiGate_VWP (interface) # edit port1
FortiGate_VWP (port1) # set l2forward enable

FortiGate_VWP (port1) # next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate_VWP (interface) # edit port2
FortiGate_VWP (port2) # set l2forward enable
FortiGate_VWP (port2) # end
```

7. 再次抓包查看，此时FGT可以转发PPPOE请求了。

```
FortiGate_VWP # diagnose sniffer packet any "pppoed" 4
interfaces=[any]
filters=[pppoed]
5.324865 port2 in pppoe printer hasn't been added to sniffer
5.324880 port1 out pppoe printer hasn't been added to sniffer
5.325468 port1 in pppoe printer hasn't been added to sniffer
5.325474 port2 out pppoe printer hasn't been added to sniffer
7.420329 port2 in pppoe printer hasn't been added to sniffer
7.420342 port1 out pppoe printer hasn't been added to sniffer
7.425307 port1 in pppoe printer hasn't been added to sniffer
7.425313 port2 out pppoe printer hasn't been added to sniffer
```



8. 路由器1 PPPOE拨号成功。

```
Router1#show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ ------------------- -------- --------------- --------------------
Vi2          LCP+ IPCP+ CDPCP-     LocalT   202.100.2.1

Router1#show pppoe session
     1 client session
Uniq ID  PPPoE  RemMAC          Port                   VT  VA         State
           SID  LocMAC                                     VA-st      Type
    N/A      2  aabb.cc00.2000  Et0/0                  Di1 Vi2        UP
                aabb.cc00.6000                             UP

Router1#show ip route
 ...
Gateway of last resort is 202.100.2.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 202.100.2.1
 ...

Router1#
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Router1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
 ...
Dialer1                    202.100.2.3     YES IPCP   up                    up
 ...
```

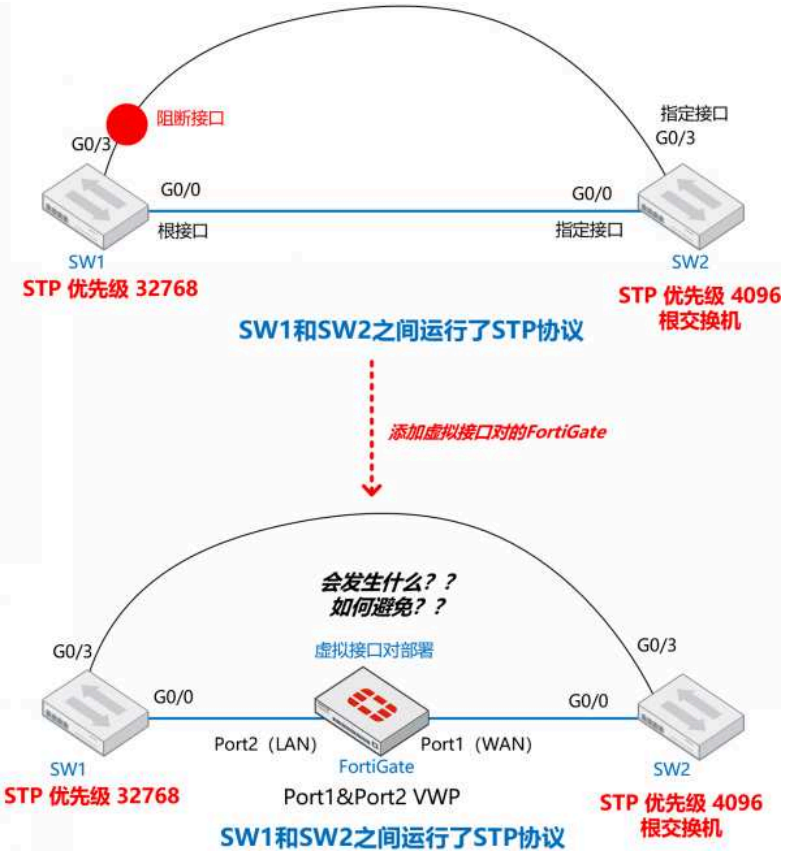

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

生成树(STP)与虚拟接口对

网络需求

SW1和SW2之间运行了STP协议，防火墙以虚拟接口对方式运行在两台SW之间，SW和SW之间原本存在环路，通过STP进行隔离阻断了环路接口，在加入虚拟接口对的FGT之后，需要继续确保STP工作正常。

网络拓扑



配置要点

- Router1/Router2路由器的基础配置
- 将防火墙配置为虚拟接口对并开启网管
- 默认情况下，观察STP BPDU报文与收敛情况
- 配置stpforward解决STP流量转发问题

配置步骤与结果验证

1. SW1/SW2交换机的基础配置和STP状态确认。

SW1:

```
hostname SW1
spanning-tree vlan 1 priority 32768
```

SW2:

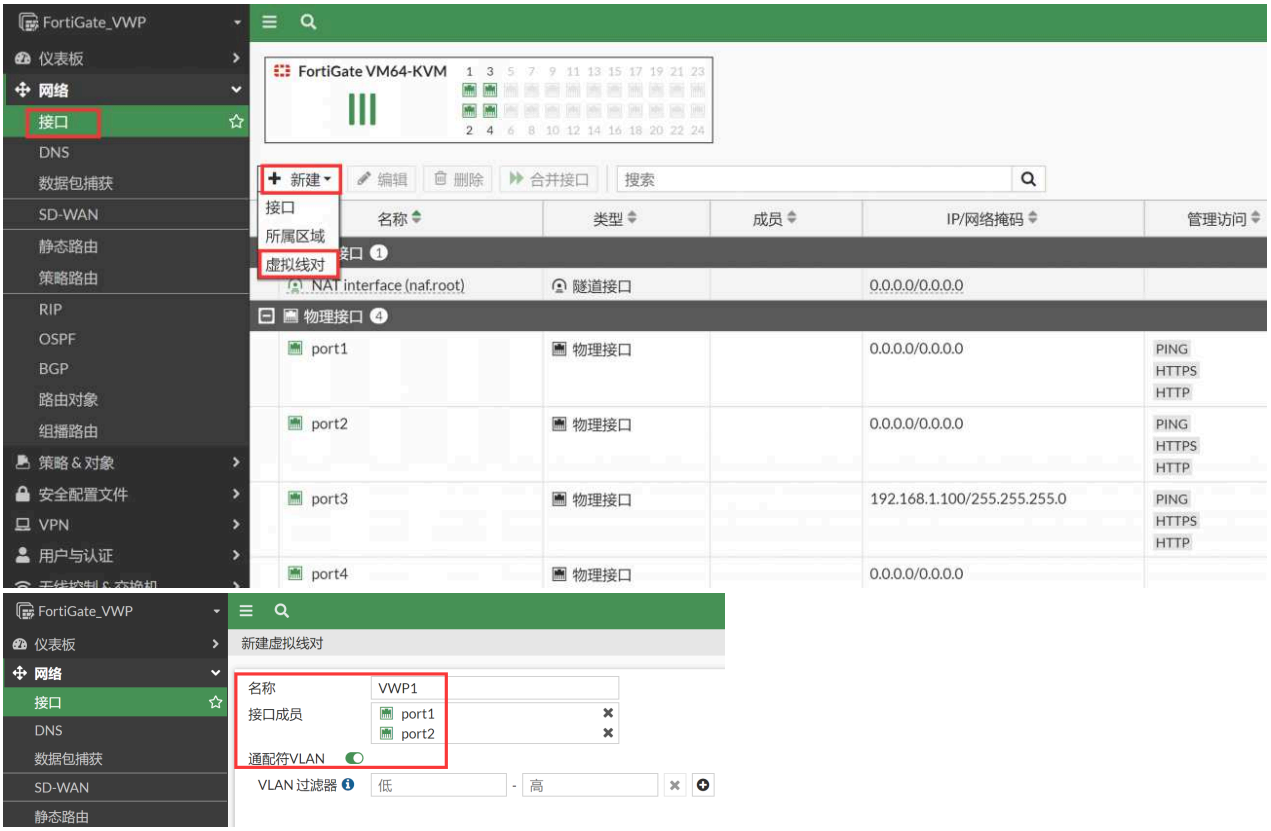
```
hostname SW2
!
spanning-tree vlan 1 priority 4096
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

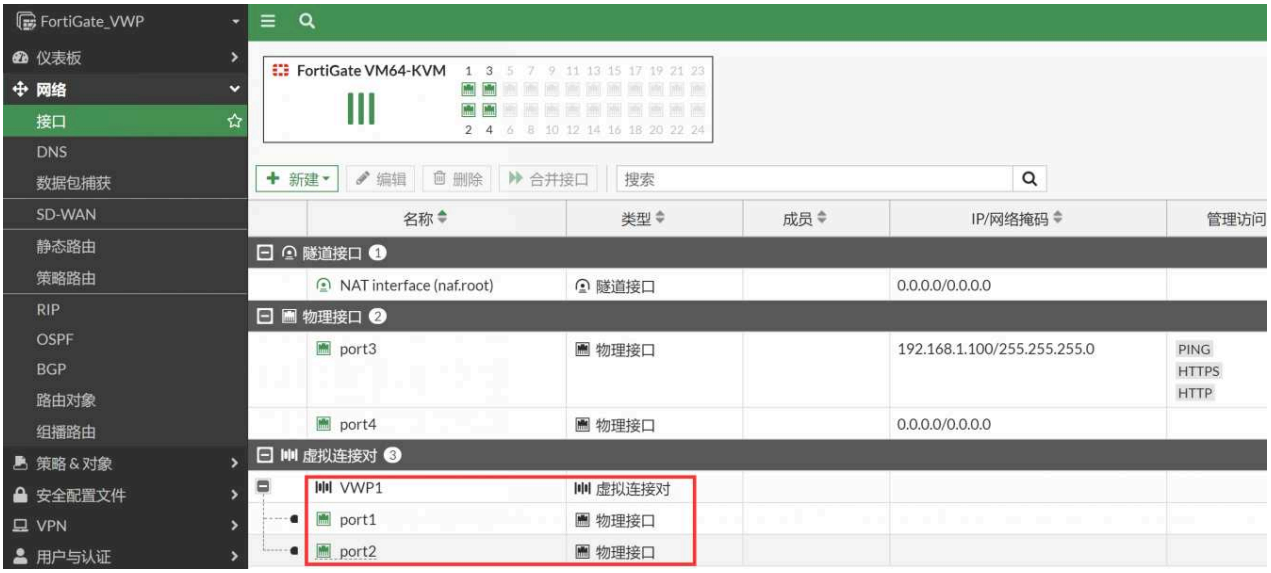
没有加入虚拟接口对的FortiGate之前STP状态：

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             Cost        4
             Port        1 (GigabitEthernet0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5000.0007.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    Shr
Gi0/3               Altn BLK 4         128.4    Shr     // G0/3 被阻断，STP工作正常

SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     5000.0008.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Desg FWD 4         128.4    Shr
```

2. 将防火墙的port1和port2配置为虚拟接口对并加入到SW1和SW2之间，防火墙处于路由模式的情况下，直接创建虚拟接口对：将port1和port2加入到虚拟接口对中并开启通配符VLAN，识别VLAN-Tag的数据（推荐开启通配符VLAN）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 虚拟接口对通道正式打通，可以认为port1和port2之间可以透明的传输数据了（需策略放通），对应的命令行如下。

```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enable
    next
end
```

4. 加入FGT在没有任何配置的情况下，观察STP的运行情况，一旦FGT加入到SW1和SW2之间，很明显网络中出现了环路，设备操作很卡顿，SW1和SW2基本上不再响应请求，三台设备均出现了异常情况（默认情况下虚拟接口对的FGT只转发ARP报文，因此只需要一个arp报文就会产生广播风暴，引起环路导致设备、业务中断）。

```
FortiGate_VWP # diagnose sniffer packet any "none" 4
interfaces=[any]
filters=[none]
0.814720 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.814733 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.817141 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.817148 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.818761 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.818771 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.819709 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.819720 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.821533 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.821544 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.825484 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.825492 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.827856 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.827866 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.828752 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.828762 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.829235 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.829244 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.831930 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.831947 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.834842 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.834853 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.836686 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.836694 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.838965 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.838972 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.841965 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.841974 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.843858 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.843866 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
```

5. SW1/SW2的 STP状态均异常，所有接口都处于转发状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             Cost        4
             Port        4 (GigabitEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5000.0007.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Root FWD 4         128.4    Shr     //SW1的两个接口都处于转发状态

SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     5000.0008.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Desg FWD 4         128.4    Shr  //SW2的两个接口都处于转发状态
```

6. 在FGT上抓包可以看到STP的BPDU报文没有被转发，而是被默认丢弃，这是引起环路的根本原因。STP BPDU数据默认不会被虚拟接口对的FGT所转发，因此STP计算不正确，会计算不出网络中的环路，从而引起广播风暴。

```
FortiGate_VWP # diagnose sniffer packet any "none" 4
interfaces=[any]
filters=[none]
1.234590 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
2.182694 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
3.247650 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
4.193908 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
5.260154 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
6.204003 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
7.278226 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
8.210732 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
9.294582 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
10.223021 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
11.302829 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
12.232585 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
13.310023 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
14.242616 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
```

7. 那么要如何解决此情况呢？在FGT的二层接口下配置set stpforward enable即可！

```
FortiGate_VWP # config system interface
FortiGate_VWP (interface) # edit port1
FortiGate_VWP (port1) # set stpforward enable

FortiGate_VWP (port1) # next
FortiGate_VWP (interface) # edit port2
FortiGate_VWP (port2) # set stpforward enable
FortiGate_VWP (port2) # end
```

8. 再次抓包查看，此时FGT可以转发STP BPDU报文了。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate_VWP # diagnose sniffer packet any "stp" 4
interfaces=[any]
filters=[stp]
2.070782 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
2.070797 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001

4.085338 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
4.085355 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001

6.097429 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
6.097444 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001

8.107806 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
8.107822 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001

10.114977 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
10.114993 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001

12.123637 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
12.123651 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001

14.131744 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
14.131757 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
```

9. 此时再次查看STP的状态，恢复正常选举状态。

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             Cost        4
             Port        1 (GigabitEthernet0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5000.0007.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    Shr
Gi0/3               Altn BLK 4         128.4    Shr    // G0/3 被阻断，STP工作正常

SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     5000.0008.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Desg FWD 4         128.4    Shr
```

重要

要特别注意此情况！避免虚拟接口对的FGT一上线引起STP计算异常，引起广播风暴，造成重大业务故障。

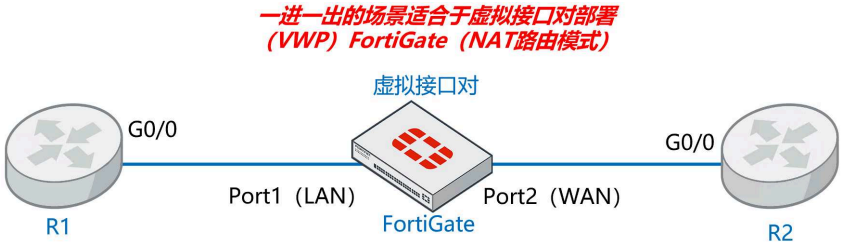
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

虚拟接口对最佳配置实践

网络需求

一进一出的这样的透明需求的组网推荐使用虚拟接口对（virtual-wire-pair）。

网络拓扑



推荐配置

1. 无论网络中是否存在VLAN都推荐开启 wildcard-vlan （set wildcard-vlan enable），让FGT可以识别VLAN-TAG的数据，然后使用策略控制所有的携带和不携带VLAN-TAG的数据流。

2. 开启了wildcard-vlan enable，vlanforward不生效，wildcard-vlan优先，识别VLAN-TAG，并上送到FGT的CPU上去策略处理。这是推荐的配置（推荐）。

3. 如果关闭了wildcard-vlan disable，则vlanforward生效，则携带了vlan-tag的数据会直接穿透VWP接口，不再匹配策略，直接bypass可通。（不推荐这样使用，流量不可见也不可控，这不是安全设备想要的结果）。

```
config system virtual-wire-pair
    edit "VWP1"
        set member "port1" "port2"
        set wildcard-vlan enbale  //手工开启wildcard
    next
end

config system interface
    edit "port1"
        set vdom "root"
        set vlanforward enable   //保持默认enable状态
        set type physical
        set alias "WAN"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set vlanforward enable  //保持默认enable状态
        set type physical
        set alias "LAN"
        set snmp-index 2
    next
end
```

4. 虚拟接口对的FortiGate其实默认只转发IPv4 ARP广播和IPv6 ND组播报文，其他的流量通通会被丢弃。如果你想让虚拟接口对更像一个SW一样的存在，那么在使用的接口下应该这样去修改，这样FortiGate对接入的网络环境影响应该来说是更小的，对于那种不是很清楚网络中有一些什么流量的环境，建议按照上述建议进行配置优化，让FortiGate更加接近于一个SW的存在。

```
config system interface
    edit "port1"
        set broadcast-forward enable   //开启广播转发
        set l2forward enable          //开启非IP流量转发
        set stpforward enable        //开启STP转发
    next
    edit "port2"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set broadcast-forward enable
        set l2forward enable
        set stpforward enable
    next
end
```

5. 使用一个独立的的VDOM用来保护二层（虚拟接口对）的业务流量，然后再使用一个独立管理VDOM（NAT路由模式）用于设备的管理和fortiguard升级等，利用VDOM功能将管理（NAT路由模式）和业务（虚拟接口对）分离。

故障排错

1. 先检查FortiGate的二层MAC地址表，下面的命令能导出每一个虚拟接口对的二层转发表，在转发表里可以单独看到HOST与接口的对应MAC地址关系。

```
FortiGate_VWP # diag netlink brctl list
list bridge information
1. VWP1_v.b         fdb: size=2048 used=2    num=2    depth=1
Total 1 bridges
diag netlink brctl name host <VWP_name_v>.b

虚拟接口对名字VWP1的查看二层转发表的例子：
FortiGate_VWP # diag netlink brctl name host VWP1_v.b
show bridge control interface VWP1_v.b host.
fdb: size=2048, used=2, num=2, depth=1
Bridge VWP1_v.b host table
port no device  devname mac addr                ttl     attributes
  2     4       port2   50:00:00:03:00:01       0       Local Static
  1     3       port1   50:00:00:03:00:00       0       Local Static
```

2. 使用sniffer验证数据包是否到达防火墙，通过以下命令使用sniffer抓取相应信息；通过使用ping在FortiGate两端进行测试可以初步分析问题。这个能看到在FortiGate上面流入以及流出的数据包。

```
进行抓取目的地址是114.114.119.119的数据：
diagnose sniffer packet any "host 114.114.119.119" 4 0 l            按CTRL+C进行停止

基于端口进行数所包抓取
diagnose sniffer packet portA  "host 114.114.119.119" 4 0  l
diagnose sniffer packet portB  "host 114.114.119.119" 4 0  l

如有需要，可以通过每个vlan进行获取更明细内容
diagnose sniffer packet <each_vlan_interface> "" 6 0 l

参数4和6的区别（用于显示输出抓取数据参数）：
1: print header of packets (只有IP头部)
2: print header and data from ip of packets (有ip头部和数据内容)
3: print header and data from ethernet of packets  (if available)
4: print header of packets with interface name (只有IP头部和端口)
5: print header and data from ip of packets with interface name (有ip头部和数据内容以及端口)
6: print header and data from ethernet of packets (if available) with intf name

参数0的用处：输出个数

参数l的用处(用于输出时候显示的时间格式)：
a：absolute UTC time, yyyy-mm-dd hh:mm:ss.ms
l：absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms
```

3. 使用debug flow验证数据包是否穿越防火墙（vlanforward无效），在每一个VDOM使用"debug flow"命令进行跟踪流量，通过使用ping在FortiGate两端进行测试可以初步分析问题。这种排障的方法能够查看到流量是否因为某条策略导致数据包不通或者通过设备。

```
以源地址为抓取条件
═══════════════════════════════════════════════════════════
diag debug flow filter add <IP_address_of_source_device>
diag debug flow show function-name enable
diag debug flow show console enable
diag debug flow show iprope enable
diag debug flow trace start 100
diag debug enable
═══════════════════════════════════════════════════════════
如需要停止，可以敲"diag debug flow trace stop"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
以目标地址为抓取条件
═══════════════════════════════════════════════════════
diag debug flow filter add <IP_address_of_destination_device>
diag debug flow show function-name enable
diag debug flow show console enable
diag debug flow show iprope enable
diag debug flow trace start 100
diag debug enable
═══════════════════════════════════════════════════════
如需要停止，可以敲"diag debug flow trace stop"

当有触发排障的流,输出如下:
id=20085 trace_id=113 msg="vd-tp_mode received a packet(proto=6,10.160.0.160:4370→10.160.0.152:23) from
internal."
id=20085 trace_id=113 msg="Find an existing session, id-00000a40, original direction"
id=20085 trace_id=113 msg="enter fast path"
id=20085 trace_id=113 msg="send out via dev-dmz1, dst-mac-00:01:02:03:04:05"
```

4. 查看数据包在防火墙上创建的session。在每一个VDOM使用"diag sys session"命令进行防火墙会话检查，通过使用ping在FortiGate两端进行测试可以初步分析问题，这种排障的方法能够查看防火墙是否会为流量创建会话，以及是否硬件加速以及命中哪一条策略。

```
以源地址为抓取条件（单播）
═══════════════════════════════════════════════════════
diag sys session filter src <IP_address_of_source_device>
diag sys session list
═══════════════════════════════════════════════════════
当有触发排障的会话,输出如下:
session info: proto=1 proto_state=00 duration=2 expire=58 timeout=0 flags=00000000 sockflag=00000000 sockport=0
av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty br
statistic(bytes/packets/allow_err): org=500/5/1 reply=500/5/1 tuples=2
tx speed(Bps/kbps): 248/1 rx speed(Bps/kbps): 248/1
orgin→sink: org pre→post, reply pre→post dev=9→10/10→9 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.1.1:64→192.168.2.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.1:64→192.168.1.1:0(0.0.0.0:0)
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=1
serial=00000512 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
vlanid=100 dd_type=0 dd_mode=0
total session 1

以源地址为抓取条件（多播）
═══════════════════════════════════════════════════════
diagnose sys mcast-session list
═══════════════════════════════════════════════════════
当有触发排障的会话,输出如下:
session info: id=123 vf=1 proto=112 192.168.1.2.0→224.0.0.18.0
used=2 path=1 duration=1353 expire=179 indev=10 pkts=1360 bytes=54400
state=00000002:tp
path: policy=0, outdev=9

session info: id=124 vf=1 proto=112 192.168.2.99.0→224.0.0.18.0
used=2 path=1 duration=1353 expire=179 indev=10 pkts=1360 bytes=54400
state=00000002:tp
path: policy=0, outdev=9
Total 2 sessions
diag sys session list
```

参考文档

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Troubleshoot-and-verify-if-traffic-is-hitting-a/ta-p/197261 ↗

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-First-steps-to-troubleshoot-connectivity/ta-p/192560 ↗

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/196988 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-a-FortiGate-in-Transparent-mode-to/ta-p/197611 ↗

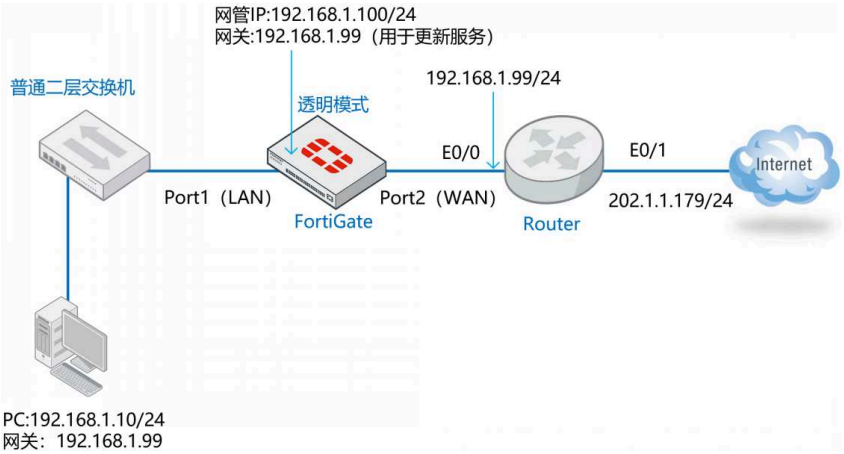
https://community.fortinet.com/t5/FortiGate/Technical-Note-FortiGate-and-Gratuitous-ARP-GARP/ta-p/192962 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

开启透明模式防火墙并保护上网流量

网络需求

在不改变现有网络拓扑前提下，将防火墙NGFW以透明模式部署到网络中，放在路由器和交换机之间，防火墙为透明模式，对内网网段192.168.1.0/24的上网进行4~7层的安全防护。



配置要点

- Internet_R路由器的基础配置
- 将防火墙配置为透明模式并开启网管
- 配置安全策略允许内网PC访问互联网

配置步骤

1. Internet_R路由器的基础配置（以思科为例）。

```
hostname Internet_R
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

2. 将防火墙配置为透明模式，进入设备命令行（CLI）中进行配置，修改FGT的运行模式为透明模式（默认为NAT路由模式）。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。配置可以管理防火墙的本地IP和网关。

```bash
config system global
    set hostname FortiGate_Transparent
end
config system settings
    set opmode transparent
    set manageip 192.168.1.100 255.255.255.0
    set gateway 192.168.1.99
end
```

3. 查看当前设备的状态已变为透明模式。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

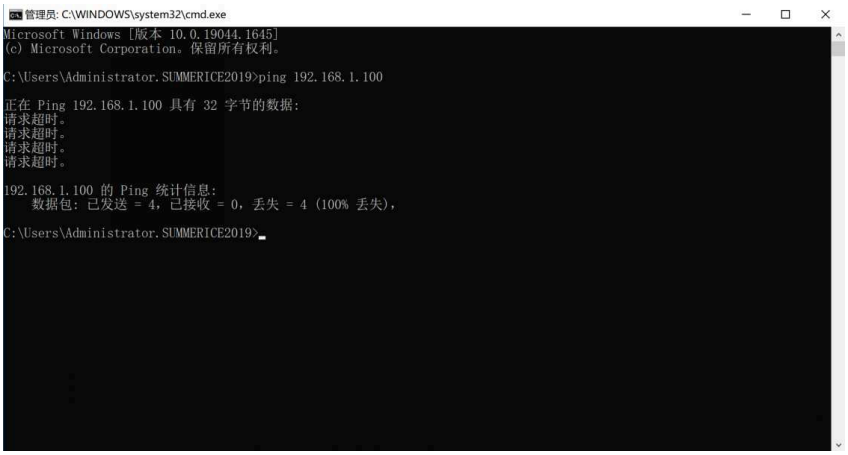
```
FortiGate_Transparent # get system status
Version: FortiGate-VM64-KVM v7.0.8,build0418,221012 (GA.F)
...
Operation Mode: Transparent
...
Virtual domains status: 0 in NAT mode, 1 in TP mode
...
```

重要

透明模式下，所有的接口都无法写入IP地址，整机只有一个设备IP地址。当需要从某个接口管理设备时，需在命令行下开启相应接口的管理权限。

开启透明模式前，需要删除系统自带的fortilink接口（需要先删除fortilink接口关联的DHCP与NTP配置）。

4. 通过内网PC尝试登陆FortiGate的Manage IP：192.168.1.100，此时FortiGate的port1未开启HTTP/HTTPS/PING，所以是无法访问的。

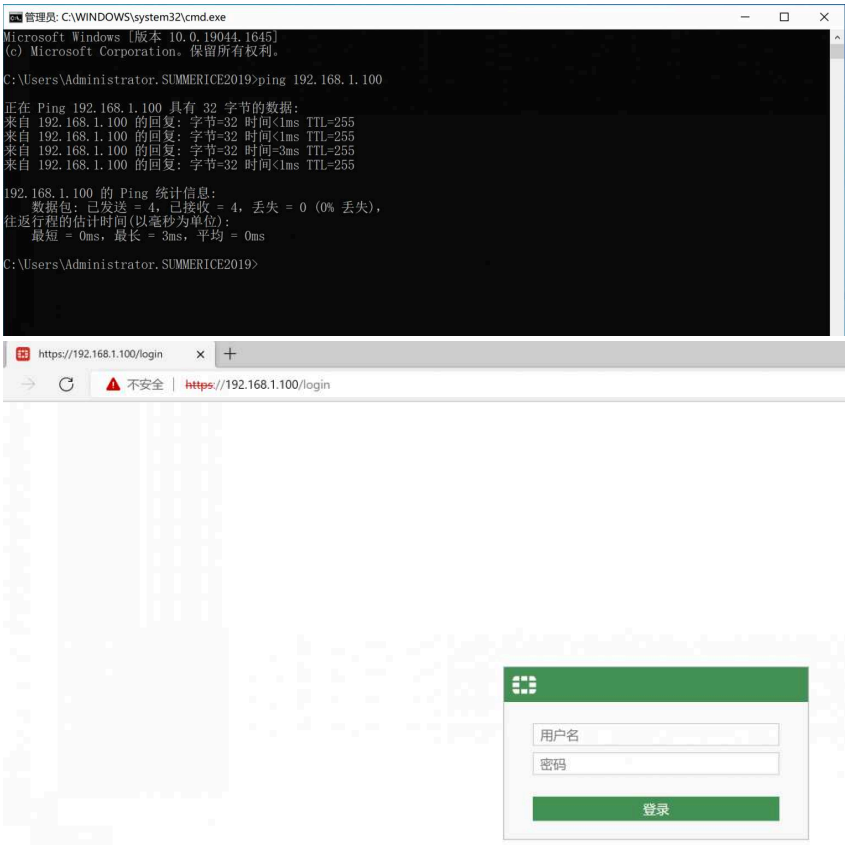


5. MGMT口默认有管理权限，要通过port1（LAN）接口管理设备为例，开启port1（LAN）管理FGT的命令如下。允许网管协议从Port1接口通过https/http/SSH/Ping访问透明模式的FortiGate。

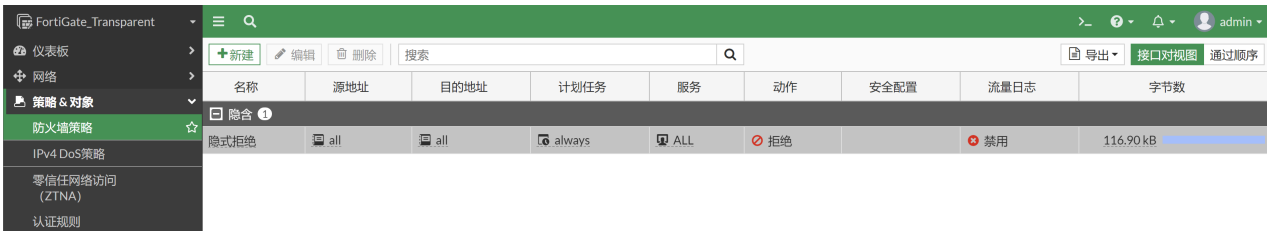
```bash
config system interface
    edit port1
        set allowaccess https http ping ssh
    next
end
```

6. 使用PC PING FortiGate的管理IP，并使用HTTPS登陆管理页面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 配置安全策略允许内网PC访问互联网，默认情况下透明模式的FortiGate没有开启任何策略，此时TCP/UDP/ICMP的流量是全部不通的。



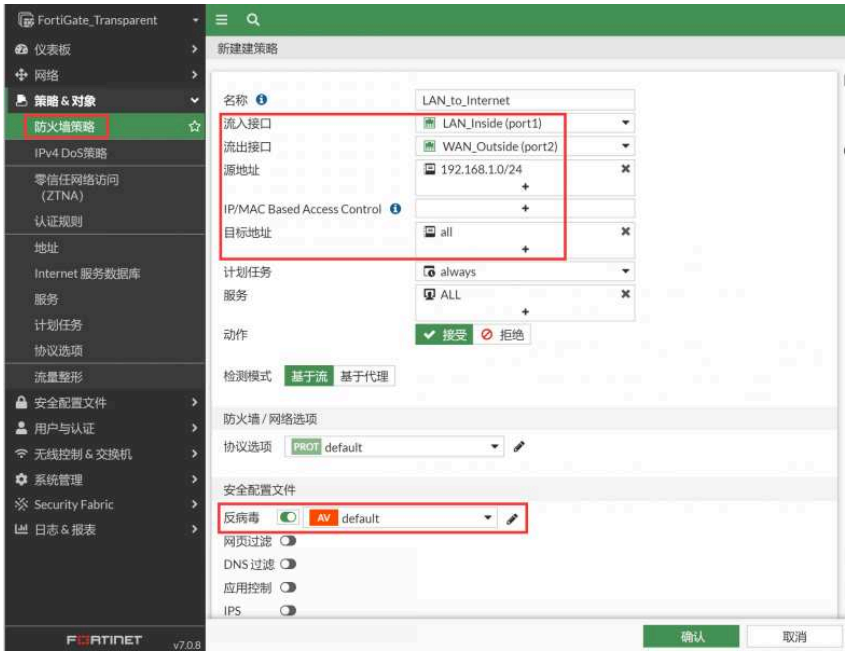

```
C:\Users\Administrator.SUMMERICE2019>ping www.baidu.com
Ping 请求找不到主机 www.baidu.com。请检查该名称，然后重试。

C:\Users\Administrator.SUMMERICE2019>ping 114.114.114.114

正在 Ping 114.114.114.114 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

114.114.114.114 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

8. 建议先给接口一个别名，这样配置策略的时候可以很清楚的知道接口的位置和功能。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

9. 进入策略&对象→防火墙策略，新建防火墙策略，放通port1到port2的流量，源地址创建LAN网段的地址对象并引用，开启防病毒功能，这里使用默认的防病毒配置文件。



重要

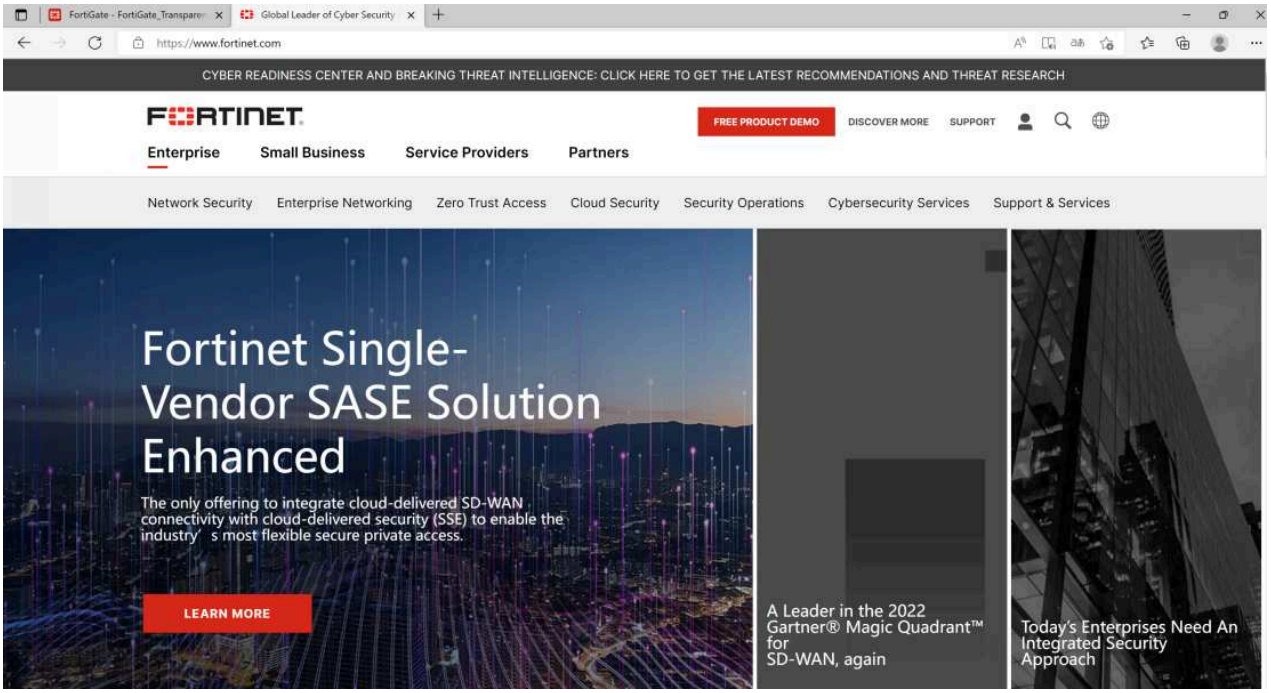
建议在不需要的情况下关闭接口配置下的“设备探测”（Device detection）功能，该功能用于MAC地址厂商设备信息识别及MAC地址过滤，会消耗较多的设备资源。

结果验证

1. 使用内网PC测试Internet业务。

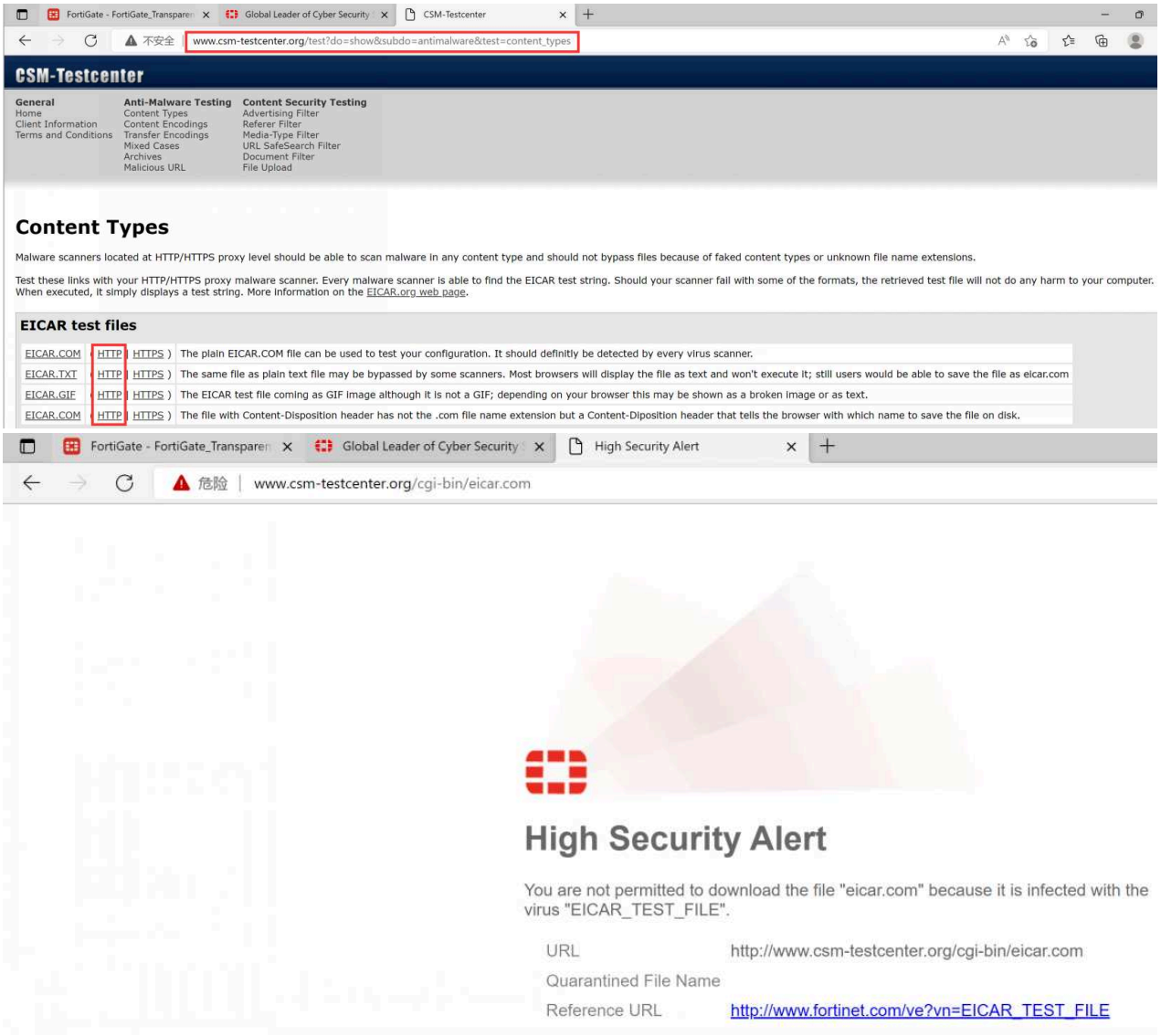
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
C:\Users\Administrator.SUMMERICE2019>ping 114.114.114.114

正在 Ping 114.114.114.114 具有 32 字节的数据:
来自 114.114.114.114 的回复: 字节=32 时间=21ms TTL=84
来自 114.114.114.114 的回复: 字节=32 时间=19ms TTL=76
来自 114.114.114.114 的回复: 字节=32 时间=23ms TTL=69
来自 114.114.114.114 的回复: 字节=32 时间=19ms TTL=85

114.114.114.114 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 19ms, 最长 = 23ms, 平均 = 20ms

C:\Users\Administrator.SUMMERICE2019>ping www.baidu.com

正在 Ping www.a.shifen.com [110.242.68.4] 具有 32 字节的数据:
来自 110.242.68.4 的回复: 字节=32 时间=14ms TTL=48
来自 110.242.68.4 的回复: 字节=32 时间=13ms TTL=48
来自 110.242.68.4 的回复: 字节=32 时间=12ms TTL=48
来自 110.242.68.4 的回复: 字节=32 时间=12ms TTL=48

110.242.68.4 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 12ms, 最长 = 14ms, 平均 = 12ms
```

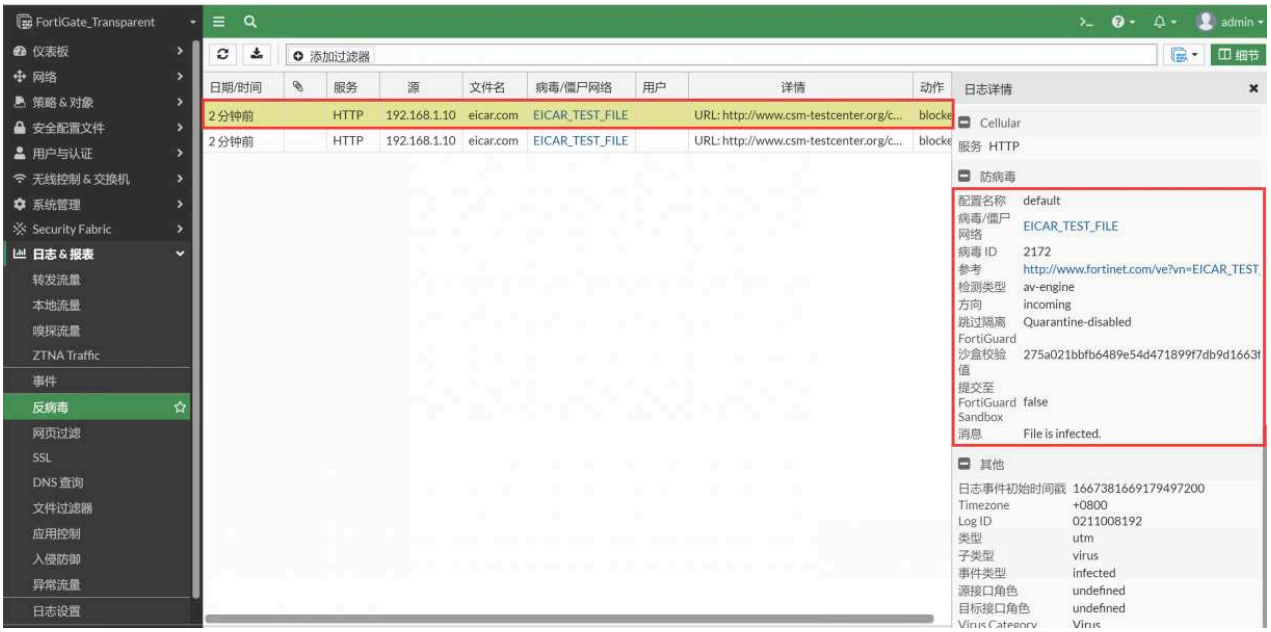


2. 使用PC测试通过HTTP协议下载病毒测试文件，可以看到下载动作被FortiGate拦截。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

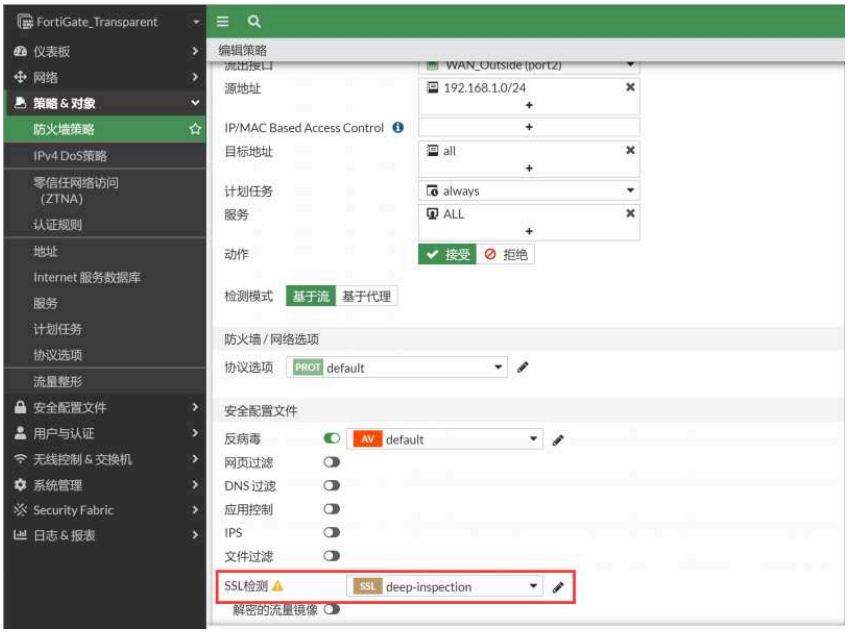


3. 在日志&报表→反病毒中可以看到相关拦截日志，协议为HTTP。

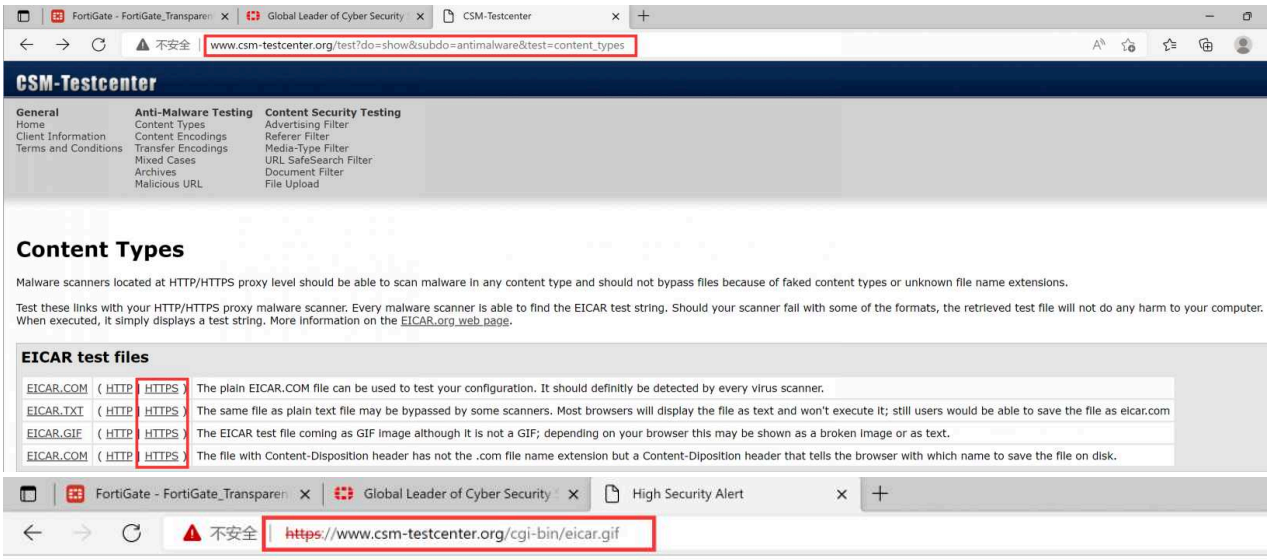


4. 如果是通过HTTPS协议下载病毒文件，由于数据被HTTPS加密，需要在策略中调用SSL深度检测。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

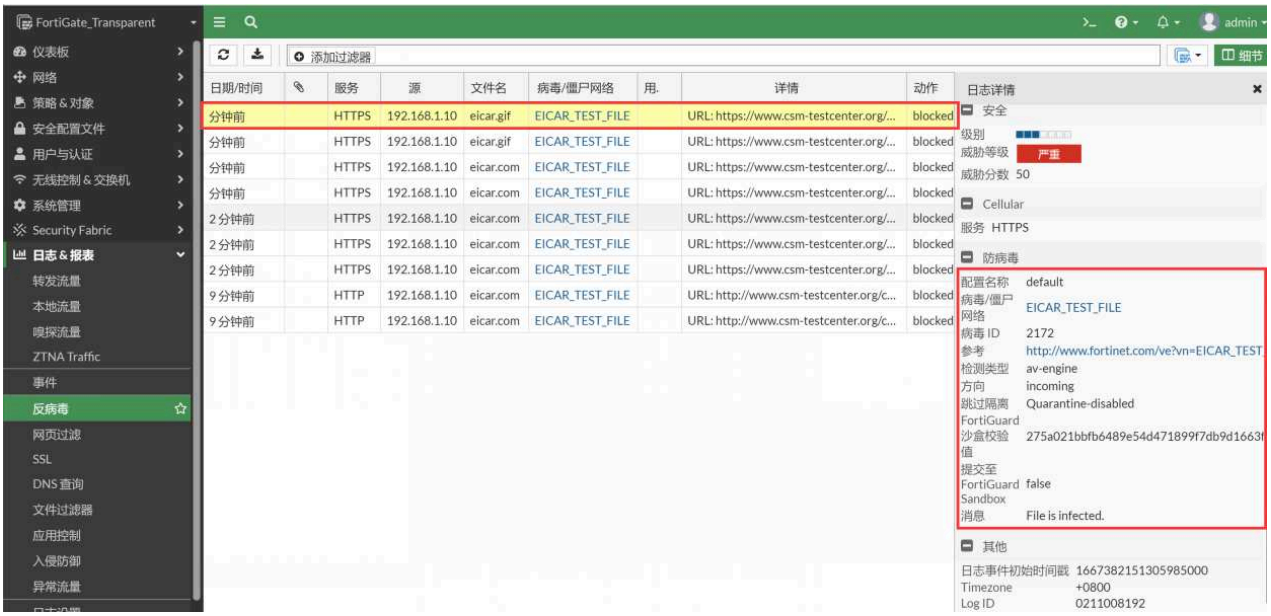


5. 使用PC测试通过HTTP协议下载病毒测试文件，可以看到下载动作被FortiGate拦截。



6. 在日志&报表→反病毒中可以看到相关拦截日志，协议为HTTPS。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Forward-Domain

> **重要**
>
> 有VLAN的场景建议配置。

网络需求

内部网络有两个vlan（trunk环境），网关在路由器上，防火墙工作在透明模式，部署在核心交换与核心路由之间，允许两个vlan访问外网，同时两个vlan之间需要互访，并且对这两个vlan进行保护，开启反病毒过滤。

网络拓扑

拓扑1：单VLAN透传



拓扑2：多VLAN透传，VLAN之间互访



配置要点

拓扑1：单VLAN透传

- SW交换机/Internet_R路由器的基础配置
- 将防火墙配置为透明模式并开启网管
- 配置LAN和WAN接口的VLAN子接口并加入到forward-domain
- 配置安全策略允许内网PC（VLAN10内主机）访问互联网

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

拓扑2：多VLAN透传，以及VLAN之间互访

- SW交换机/Internet_R路由器的基础配置
- 新增Inside和Outside关于VLAN20的子接口并加入到Forward-domain
- 配置Inside_VLAN20 到 Outside_VLAN20的安全策略允许内网PC（VLAN20内主机）访问互联网
- 配置VLAN10与VLAN20之间互访的策略

配置步骤

拓扑1：单VLAN透传

1. SW交换机/Internet_R路由器的基础配置（以思科为例）。

SW:

```bash
SW:
interface Ethernet0/0
switchport trunk allowed vlan 1,10
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
!
```

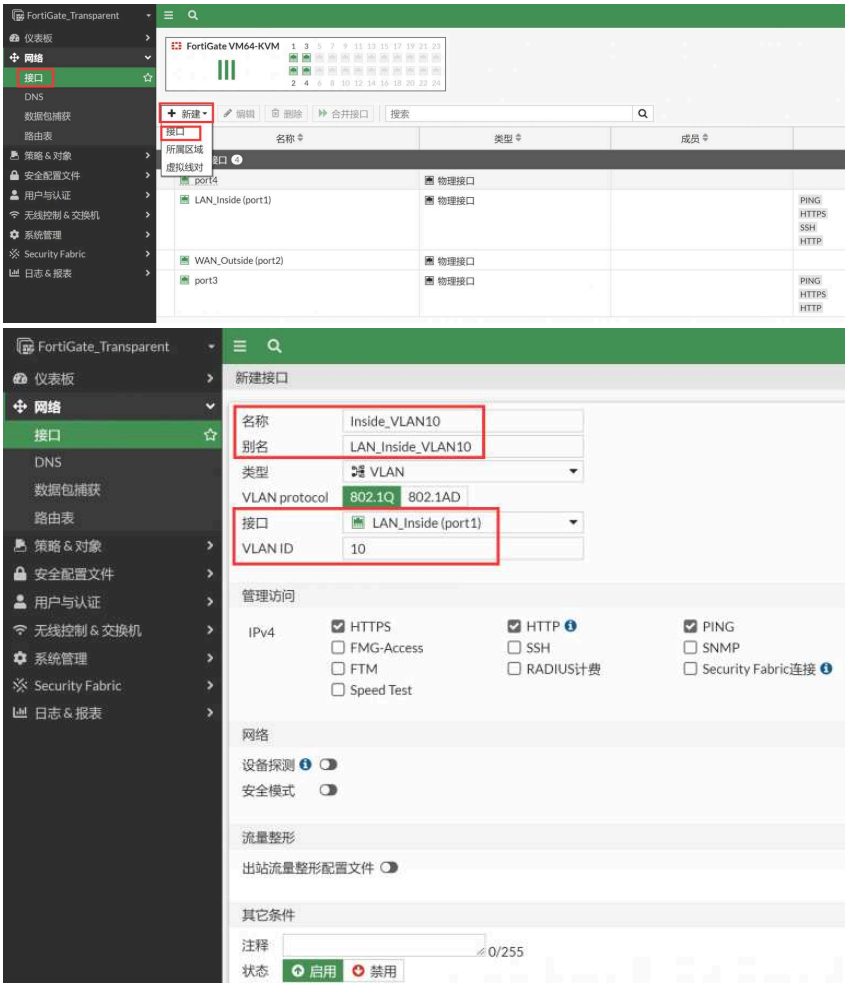
Router:

```bash
Router:
hostname Internet_R
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

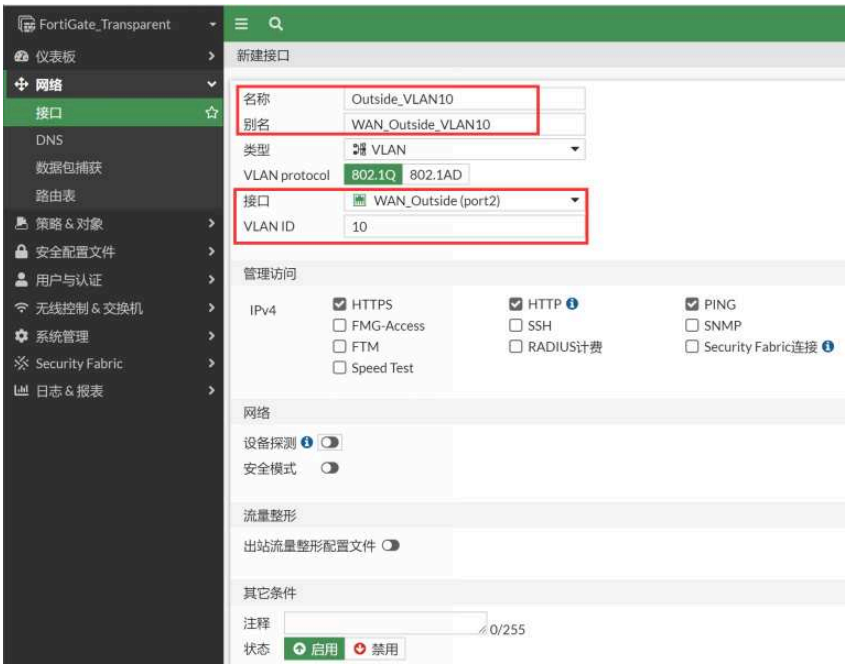
2. 将防火墙配置为透明模式并开启网管（参考网络管理→透明模式→传统透明模式→开启透明模式防火墙并保护上网流量 ↗）。

3. 新建LAN和WAN接口的VLAN10子接口并加入到forward-domain。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```bash
config system interface
    edit "Inside_VLAN10"
        set vdom "root"
        set alias "LAN_Inside_VLAN10"
        set interface "port1"
        set vlanid 10
    next
    edit "Outside_VLAN10"
        set vdom "root"
        set alias "WAN_Outside_VLAN10"
        set interface "port2"
        set vlanid 10
    next
end
```

重要

建议在不需要的情况下关闭接口配置下的“设备探测”（Device detection）功能，该功能用于MAC地址厂商设备信息识别及MAC地址过滤，会消耗较多的设备资源。

4. 为Inside_VLAN10和Outside_VLAN10接口配置forward-domain。

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit Inside_VLAN10
FortiGate_Transparent (Inside_VLAN10) # set forward-domain 10
FortiGate_Transparent (Inside_VLAN10) # next

FortiGate_Transparent (interface) # edit Outside_VLAN10
FortiGate_Transparent (Outside_VLAN10) # set forward-domain 10
FortiGate_Transparent (Outside_VLAN10) # end
```

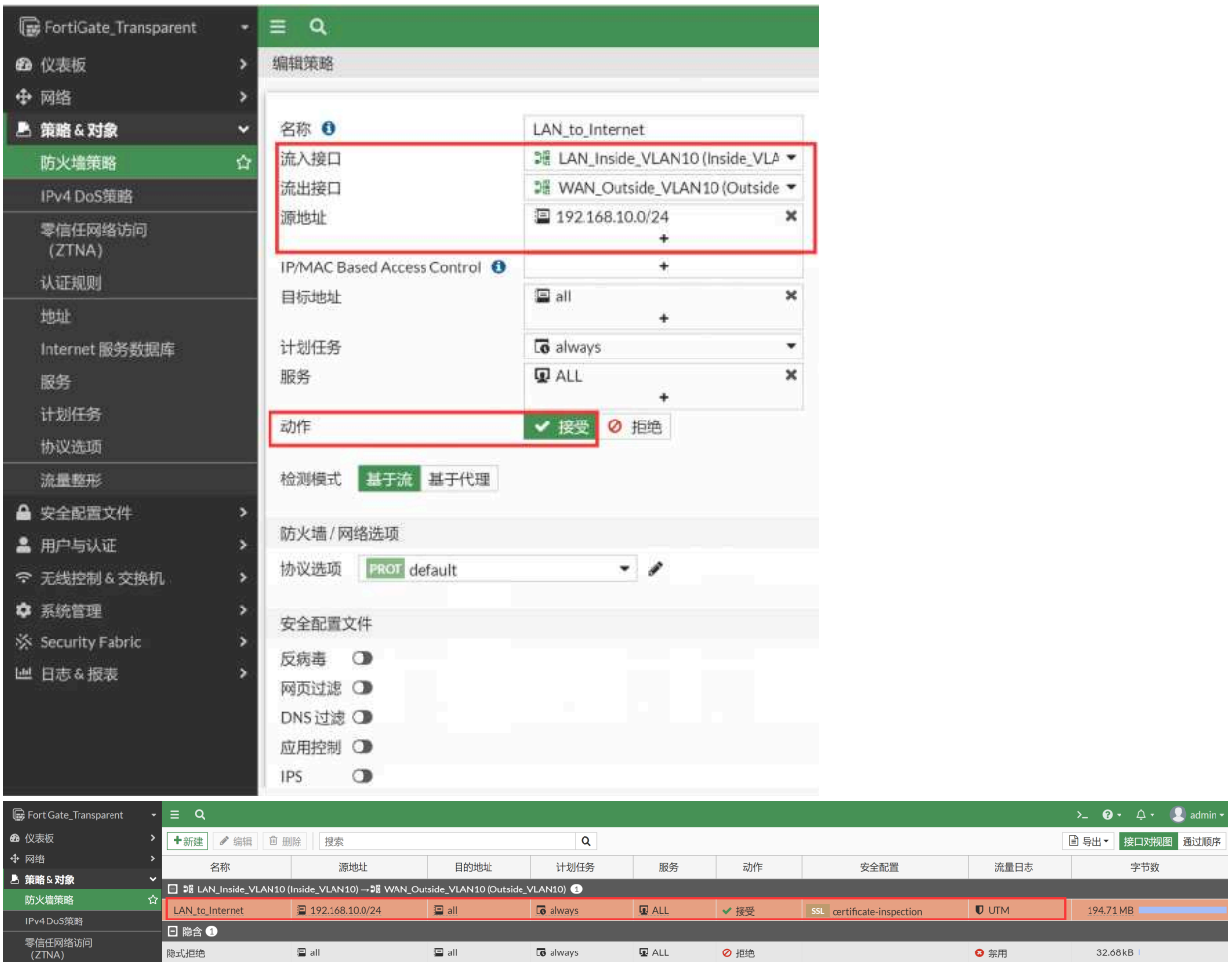

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

Forward-Domain说明：

默认所有的接口都属于Forward-Domain 0，可以理解为同一个广播域，在FortiGate的概念中，Forward-Domain才代表真正的广播域，并非VLAN，而一般的理解交换机的常识都是VLAN隔离广播域，因此如果需要使用VLAN则务必将VLAN-ID和Fortiward-Domain ID关联起来，这样就可以以正常的交换机VLAN隔离广播域的思维去考虑FortiGate的透明模式。Forward-Domain是一个FGT透明模式下比较特别的东西，记住：只要有VLAN-ID的场景就需要配置对应的Forward-Domain ID这样就不会出现什么问题。

5. 配置防火墙策略允许内网PC（VLAN10内主机）访问互联网，注意这里要选择VLAN接口。



拓扑2：多VLAN透传，VLAN之间互访

1. SW交换机/Internet_R路由器的基础配置（以思科为例）。

SW:

```bash
interface Ethernet0/0
switchport trunk allowed vlan 1,10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
!
interface Ethernet0/2
switchport access vlan 20
switchport mode access
!
```

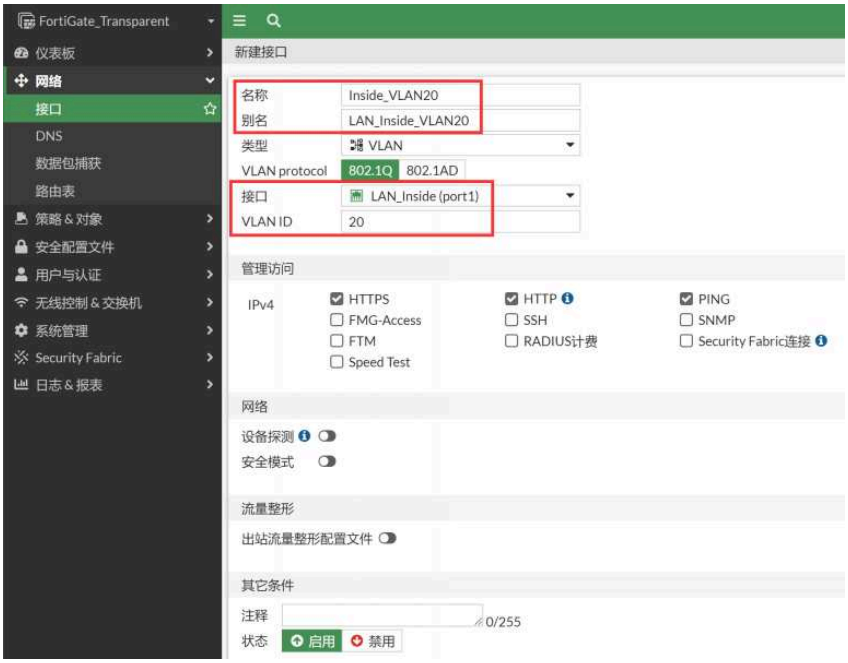
Router:

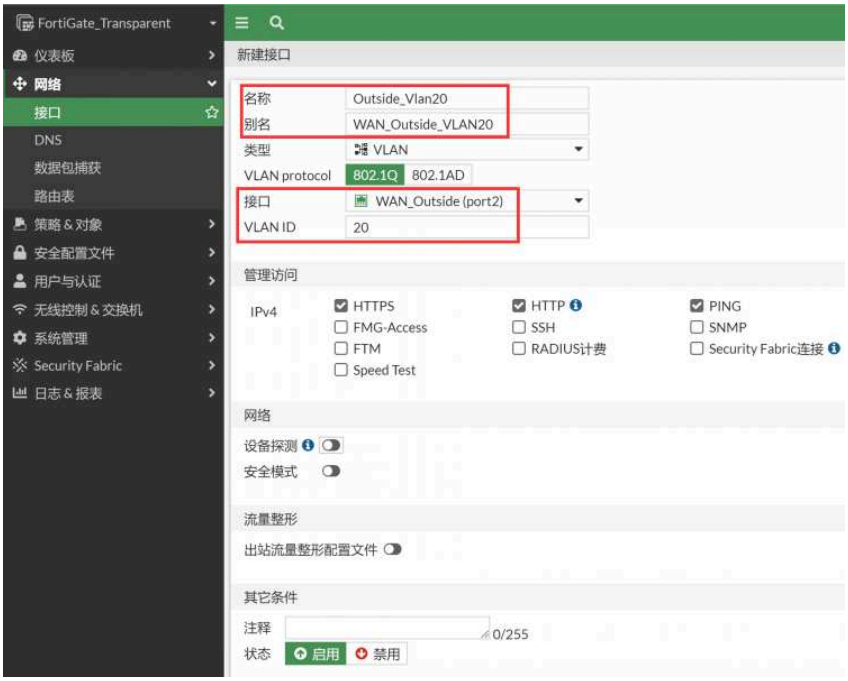
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
hostname Internet_R
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.99 255.255.255.0
no shutdown
ip nat inside
!
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

2. 新增Inside和Outside关于VLAN20的子接口并加入到Forward-domain。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







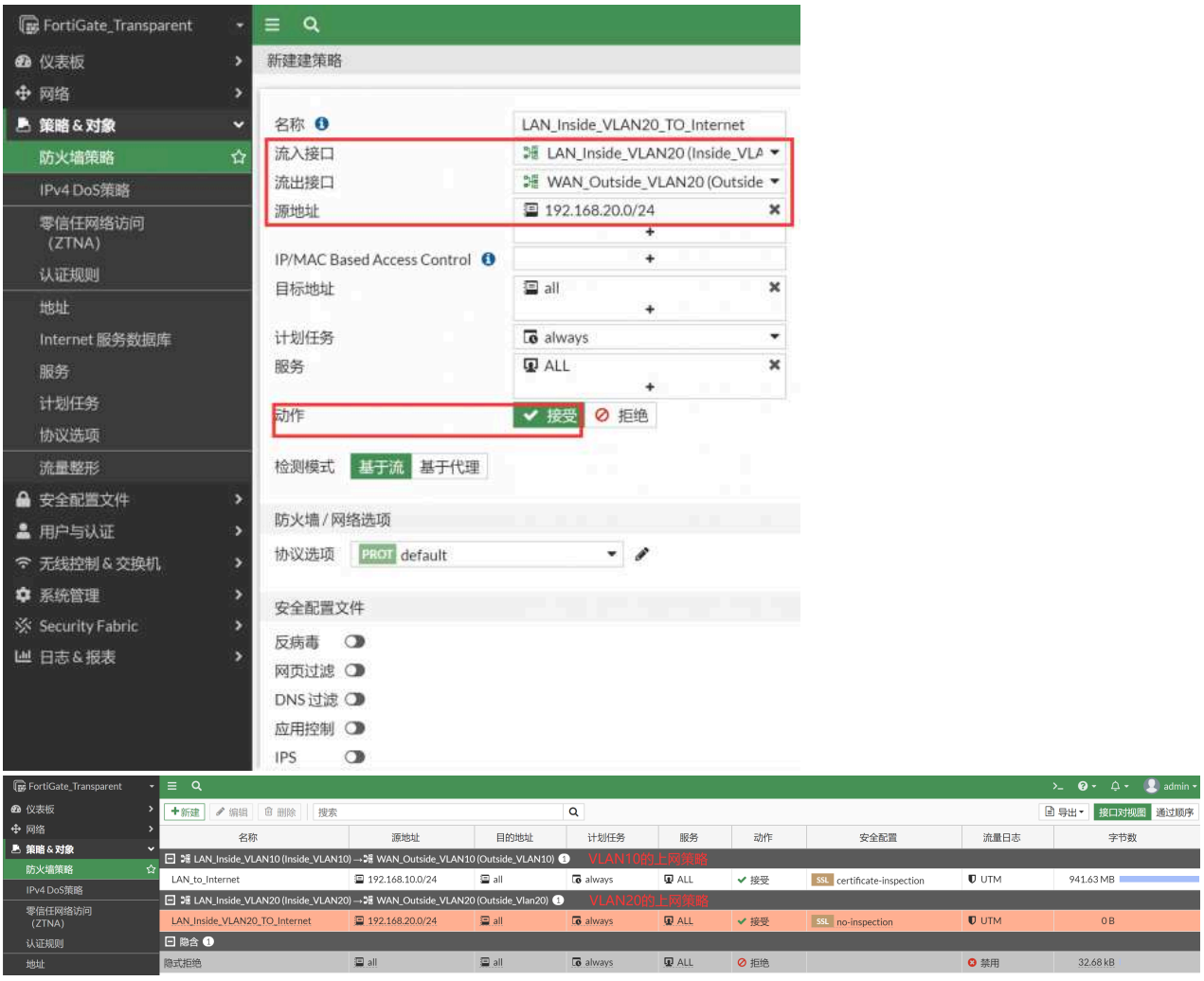
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system interface
    edit "Inside_VLAN20"
        set vdom "root"
        set alias "LAN_Inside_VLAN20"
        set interface "port1"
        set vlanid 20
    next
    edit "Outside_VLAN20"
        set vdom "root"
        set alias "WAN_Outside_VLAN20"
        set interface "port2"
        set vlanid 20
    next
end
```

3. 为Inside_VLAN20和Outside_VLAN20接口配置forward-domain。

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit Inside_VLAN20
FortiGate_Transparent (Inside_VLAN20) # set forward-domain 20
FortiGate_Transparent (Inside_VLAN20) # next

FortiGate_Transparent (interface) # edit Outside_Vlan20
FortiGate_Transparent (Outside_VLAN20) # set forward-domain 20
FortiGate_Transparent (Outside_VLAN20) # end
```

4. 配置Inside_VLAN20到Outside_VLAN20的上网安全策略，允许VLAN20内的主机访问Internet。



5. 此时VLAN 10下的PC已经可以和VLAN 20下的PC互访，不需要配置其他策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

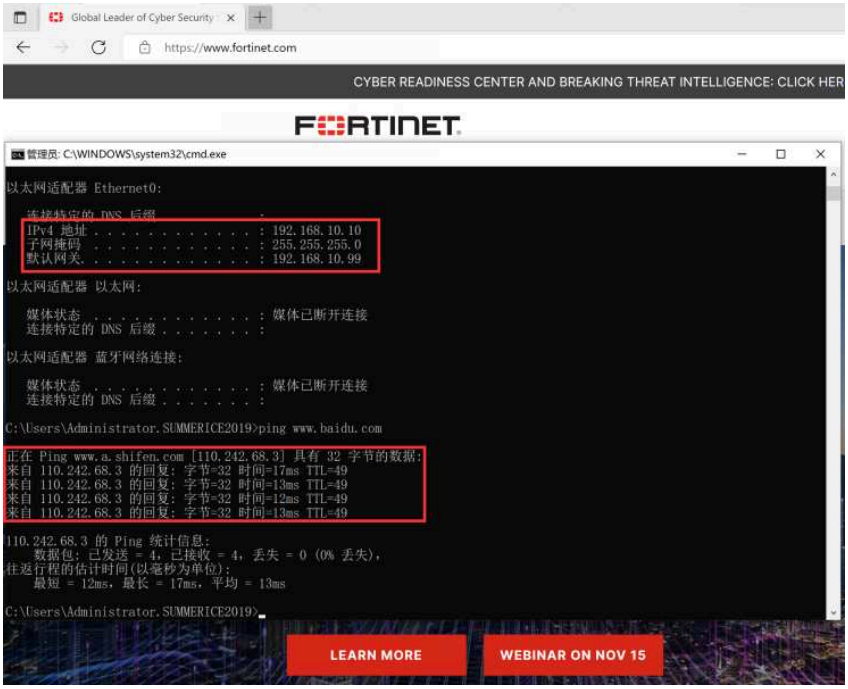
不同Forward-Domain下的VLAN接口是不能配置在同一条安全策略的源目接口中的。在VLAN 10下的PC访问VLAN 20下的PC（192.168.10.10→192.168.20.10）时，流量会经过2次FortiGate：

- 流量先从Inside_VLAN10送到Outside_VLAN10（匹配VLAN 10的上网策略）。此时FortiGate创建192.168.10.10→192.168.20.10（Inside_VLAN10→Outside_VLAN10）的会话。
- 同时，FortiGate会自动创建192.168.10.10→192.168.20.10（Outside_VLAN20→Inside_VLAN20）的辅助会话（上述创建会话的Reflect会话），流量第二次经过FortiGate时，从Outside_VLAN20进入并送到Inside_VLAN20，匹配辅助会话送到VLAN 20下的PC。

结果验证

拓扑1：单VLAN10透传

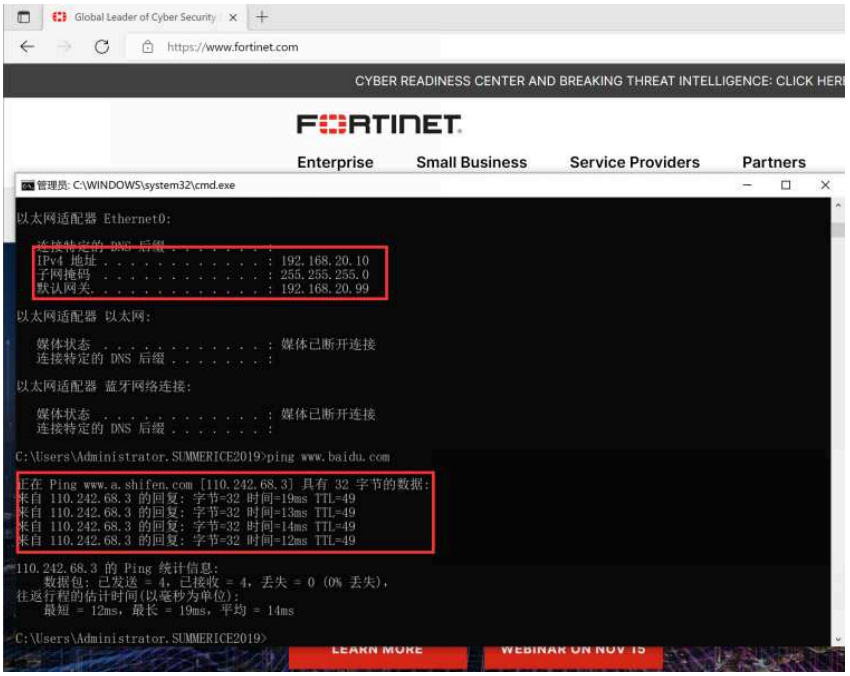
1. VLAN10内的PC通过透明模式的FortiGate访问互联网。



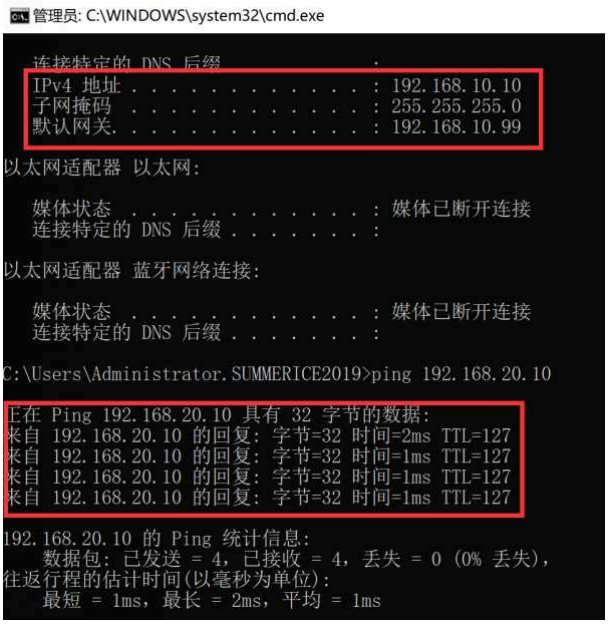
拓扑2：多VLAN透传，VLAN之间互访

1. VLAN20内的PC访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. VLAN10内的PC访问VLAN20的PC。



3. 查看对应sniffer抓包，VLAN 10主机访问VLAN 20主机的Ping Request从Inside_VLAN10进，从Outside_VLAN10出，随后从Outside_Vlan20进，从Inside_VLAN20出。

```bash
FortiGate_Transparent # diagnose sniffer packet any "host 192.168.20.10 and icmp" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.20.10 and icmp]
3.530807 Inside_VLAN10 in 192.168.10.10 → 192.168.20.10: icmp: echo request
3.530823 Outside_VLAN10 out 192.168.10.10 → 192.168.20.10: icmp: echo request
3.530826 port2 out 192.168.10.10 → 192.168.20.10: icmp: echo request
3.531120 Outside_Vlan20 in 192.168.10.10 → 192.168.20.10: icmp: echo request
3.531129 Inside_VLAN20 out 192.168.10.10 → 192.168.20.10: icmp: echo request
3.531130 port1 out 192.168.10.10 → 192.168.20.10: icmp: echo request

3.531696 Inside_VLAN20 in 192.168.20.10 → 192.168.10.10: icmp: echo reply
3.531703 Outside_Vlan20 out 192.168.20.10 → 192.168.10.10: icmp: echo reply
3.531703 port2 out 192.168.20.10 → 192.168.10.10: icmp: echo reply
3.531856 Outside_VLAN10 in 192.168.20.10 → 192.168.10.10: icmp: echo reply
3.531859 Inside_VLAN10 out 192.168.20.10 → 192.168.10.10: icmp: echo reply
3.531859 port1 out 192.168.20.10 → 192.168.10.10: icmp: echo reply
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 查看Request方向与Reply方向对应的debug flow。

   - Ping Request第1次从Inside_VLAN10送到Outside_VLAN10（匹配VLAN 10的上网策略）。此时FortiGate创建192.168.10.10→192.168.20.10（Inside_VLAN10→Outside_VLAN10）的会话。

```bash
Request方向第1次过FortiGate:
id=65308 trace_id=10 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=1, 192.168.10.10:2->192.168.20.10:2048) tun_id=0.0.0.0 from Inside_VLAN10. type=8, code=0, id=2, seq=2879."
id=65308 trace_id=10 func=init_ip_session_common line=6043 msg="allocate a new session-00000386, tun_id=0.0.0.0"
id=65308 trace_id=10 func=br_fw_forward_handler line=578 msg="Allowed by Policy-1:"
id=65308 trace_id=10 func=__if_queue_push_xmit line=392 msg="send out via dev-Outside_VLAN10, dst-mac-aa:bb:cc:00:30:00"
```

   - 同时，FortiGate会自动创建192.168.10.10→192.168.20.10（Outside_VLAN20→Inside_VLAN20）的辅助会话（上述创建会话的Reflect会话），流量第二次经过FortiGate时，从Outside_VLAN20进入并送到Inside_VLAN20，匹配辅助会话送到VLAN 20下的PC。

```bash
Request方向第2次过FortiGate:
id=65308 trace_id=11 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=1, 192.168.10.10:2->192.168.20.10:2048) tun_id=0.0.0.0 from Outside_VLAN20. type=8, code=0, id=2, seq=2879."
id=65308 trace_id=11 func=resolve_ip_tuple_fast line=5945 msg="Find an existing session, id-00000386, original direction"
id=65308 trace_id=11 func=br_fw_forward_dirty_handler line=282 msg="auxiliary ses proto=1 dev=19→18 192.168.10.10/2⇒192.168.20.10/8"
id=65308 trace_id=11 func=npu_handle_session44 line=1322 msg="Trying to offloading session from Outside_VLAN20 to Inside_VLAN20, skb.npu_flag=00000400 ses.state=00008200 ses.npu_state=0×00000100"
id=65308 trace_id=11 func=__if_queue_push_xmit line=392 msg="send out via dev-Inside_VLAN20, dst-mac-00:0c:29:39:f3:ac"
```

   - Reply方向的流量匹配辅助会话和主会话返回。

```bash
Reply方向:
id=65308 trace_id=12 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=1, 192.168.20.10:2->192.168.10.10:0) tun_id=0.0.0.0 from Inside_VLAN20. type=0, code=0, id=2, seq=2879."
id=65308 trace_id=12 func=resolve_ip_tuple_fast line=5945 msg="Find an existing session, id-00000386, reply direction"
id=65308 trace_id=12 func=br_fw_forward_dirty_handler line=282 msg="auxiliary ses proto=1 dev=19→18 192.168.10.10/2⇒192.168.20.10/8"
id=65308 trace_id=12 func=npu_handle_session44 line=1322 msg="Trying to offloading session from Inside_VLAN20 to Outside_VLAN20, skb.npu_flag=00000000 ses.state=00008200 ses.npu_state=0×00000100"
id=65308 trace_id=12 func=__if_queue_push_xmit line=392 msg="send out via dev-Outside_VLAN20, dst-mac-aa:bb:cc:00:30:00"
id=65308 trace_id=13 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=1, 192.168.20.10:2->192.168.10.10:0) tun_id=0.0.0.0 from Outside_VLAN10. type=0, code=0, id=2, seq=2879."
id=65308 trace_id=13 func=resolve_ip_tuple_fast line=5945 msg="Find an existing session, id-00000386, reply direction"
id=65308 trace_id=13 func=__if_queue_push_xmit line=392 msg="send out via dev-Inside_VLAN10, dst-mac-00:0c:29:ae:55:70"
```

5. 查看对应会话，可以看到主会话为192.168.10.10→192.168.20.10（Inside_VLAN10→Outside_VLAN10），辅助会话有reflect标记，Outside_VLAN20→ Inside_VLAN20。

```bash
session info: proto=1 proto_state=00 duration=38 expire=21 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty br
statistic(bytes/packets/allow_err): org=120/2/1 reply=120/2/1 tuples=2
tx speed(Bps/kbps): 3/0 rx speed(Bps/kbps): 3/0
orgin→sink: org pre→post, reply pre→post dev=16→17/17→16 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.10.10:2→192.168.20.10:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.20.10:2→192.168.10.10:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=15744 auth_info=0 chk_client_info=0 vd=0
serial=00000386 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×000100
no_ofld_reason:  npu-flag-off
reflect info 0:
dev=19→18/18→19
```

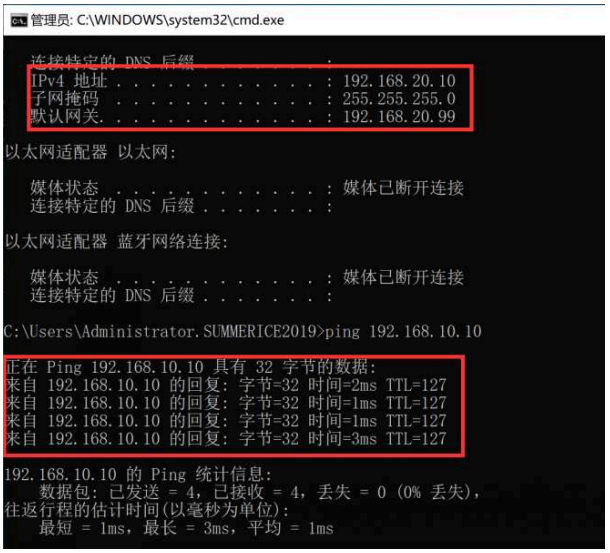

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
npu_state=0×000100
npu info: flag=0×00/0×00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0×0000/0×0000
vlifid=0/0, vtag_in=0×0000/0×0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
total reflect session num: 1
total session 1
```

6. 查看当前接口列表，可以看到4个VLAN接口的index，与会话中的dev对应。

```bash
FortiGate # diagnose netlink interface list | grep VLAN
if=Inside_VLAN10 family=00 type=1 index=16 mtu=1500 link=0 master=0
if=Outside_VLAN10 family=00 type=1 index=17 mtu=1500 link=0 master=0
if=Inside_VLAN20 family=00 type=1 index=18 mtu=1500 link=0 master=0
if=Outside_VLAN20 family=00 type=1 index=19 mtu=1500 link=0 master=0
```

7. 使用VLAN20下的PC访问VLAN 10下的PC，也可以正常访问。



重要

Forward-Domain参考文档：https://community.fortinet.com/t5/FortiGate/Technical-Note-Configure-a-FortiGate-unit-in-Transparent-mode/tap/194458

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

vlanforward

重要

默认关闭，谨慎使用。

功能简介

FortiGate在不配置VLAN接口的情况下，默认不转发那些携带了VLAN-TAG的数据，携带了VLAN-TAG的数据会被认为是非IP数据，直接全部丢弃（set vlanforward disable）——默认disable。

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit port1
FortiGate_Transparent (port1) # show full-configuration | grep vlanforward
set vlanforward disable    //默认即为disable
```

假如FortiGate在不配置VLAN接口的情况下，默认转发那些携带了VLAN-TAG的数据（set vlanforward enable），也就是说FortiGate（透明）上线一个新的环境，不清楚网络中是否跑了VLAN，为了不影响那些不知道的VLAN的业务，于是开启vlanforward，以便那些未知VLAN的业务可以正常通信。

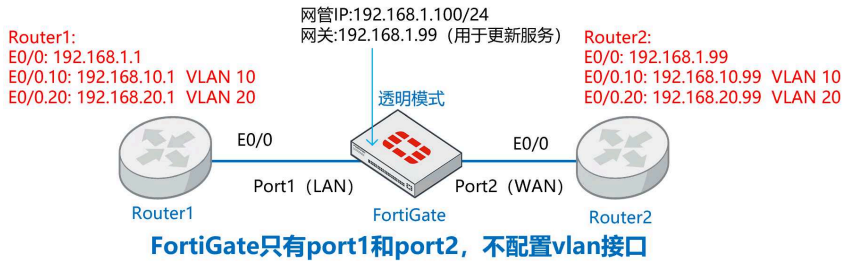
听起来美好，但是实际上问题很大，考虑到FortiGate默认所有接口都是一个forward-domain 0，如此的情况很容易引起广播风暴。因此在目前版本中vlanforward默认就为disable的状态。

通常来说我们上线FortiGate透明的时候需要详细的了解客户的业务情况，网络中是否有VLAN和VLAN-ID多少这些信息都是必须要去了解的，vlanforward enable这种省事的方法不可取，非特别特别的情况下尽量不要使用，同时也是为了避免忘记配置forward-domain而引起广播风暴的风险。通常来说vlanforward保持在disable的状态就好了，不要enable。

重要

详情参考：https://community.fortinet.com/t5/FortiGate/Technical-Note-vlanforward-interface-parameter/ta-p/198171 ↗

网络拓扑



场景一：关闭vlanforward

基本配置

Router1和Router2运行了子接口 E0/0.10和E0/0.20，FortiGate透明模式运行与Router1和Router2之间，三者的基础配置如下：

Router1：

```
hostname Router1
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Ethernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
!
interface Ethernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Router2：

```
hostname Router2
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
!
interface Ethernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.99 255.255.255.0
!
interface Ethernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.99 255.255.255.0
```

FortiGate：

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FortiGate_Transparent
FortiGate_Transparent (global) # set timezone 55
FortiGate_Transparent (global) # set language simch
FortiGate-VM64-KVM (global) # end
FortiGate_Transparent #
FortiGate_Transparent # config system settings

FortiGate_Transparent (settings) # set opmode transparent    // 修改FGT的运行模式为透明模式，默认为NAT路由模式。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。
FortiGate_Transparent (settings) # set manageip 192.168.1.100 255.255.255.0  // 配置可以管理防火墙的本地IP和网关，以便HTTP/SSH管理防火墙及防火墙的服务更新
FortiGate_Transparent (settings) # set gateway 192.168.1.99
FortiGate_Transparent (settings) # end
Changing to TP mode

（MGMT1或MGMT2口默认有管理权限），以要通过port1（LAN）接口管理设备为例，开启port1（LAN）管理FGT的命令如下：
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit port1
FortiGate_Transparent (port1) # set allowaccess https http ping ssh    //允许网管协议从Port1接口通过https/http/SSH/Ping访问透明模式的FortiGate
FortiGate_Transparent (port1) # end

port1和port2都是默认配置，同时也没有配置任何安全策略，纯透明防火墙初始化空配置。
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit port1
FortiGate_Transparent (port1) # show full-configuration | grep vlanforward
        set vlanforward disable    //默认vlanforward是disable的
```

实验步骤

1. 首先测试Router1的e0/0 192.168.1.1到192.168.1.99类似于不带vlan-tag的本地vlan vlan1的业务。

```
Router1#ping 192.168.1.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

2. 结果不通，在FortiGate上抓包，

```
FortiGate_Transparent # diagnose sniffer packet any "arp or icmp" 4 0 l
interfaces=[any]
filters=[arp or icmp]
2019-07-03 18:05:12.481488 port1 in arp who-has 192.168.1.99 (aa:bb:cc:0:20:0) tell 192.168.1.1
2019-07-03 18:05:12.481508 port2 out arp who-has 192.168.1.99 (aa:bb:cc:0:20:0) tell 192.168.1.1
2019-07-03 18:05:12.486286 port2 in arp reply 192.168.1.99 is-at aa:bb:cc:0:20:0
2019-07-03 18:05:12.486295 port1 out arp reply 192.168.1.99 is-at aa:bb:cc:0:20:0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
2019-07-03 18:05:15.442315 port1 in 192.168.1.1 → 192.168.1.99: icmp: echo request
2019-07-03 18:05:17.444526 port1 in 192.168.1.1 → 192.168.1.99: icmp: echo request
2019-07-03 18:05:19.444349 port1 in 192.168.1.1 → 192.168.1.99: icmp: echo request
2019-07-03 18:05:21.444162 port1 in 192.168.1.1 → 192.168.1.99: icmp: echo request
2019-07-03 18:05:23.444217 port1 in 192.168.1.1 → 192.168.1.99: icmp: echo request
```

3. ARP解析正常，但是icmp请求被防火墙丢弃，deubug flow分析不通的原因。

```
diagnose debug flow filter addr 192.168.1.1
diagnose debug flow filter  proto 1
diagnose debug flow show function-name enable
diagnose debug flow trace start 10
diagnose debug enable

id=20085 trace_id=1 func=print_pkt_detail line=5428 msg="vd-root:0 received a packet(proto=1, 192.168.1.1:10->192.168.1.99:2048) from port1. type=8, code=0, id=10, seq=0."
id=20085 trace_id=1 func=init_ip_session_common line=5593 msg="allocate a new session-0000007d"
id=20085 trace_id=1 func=br_fw_forward_handler line=565 msg="Denied by forward policy check"    //没有配置安全策略允许，自然是会丢弃的。
```

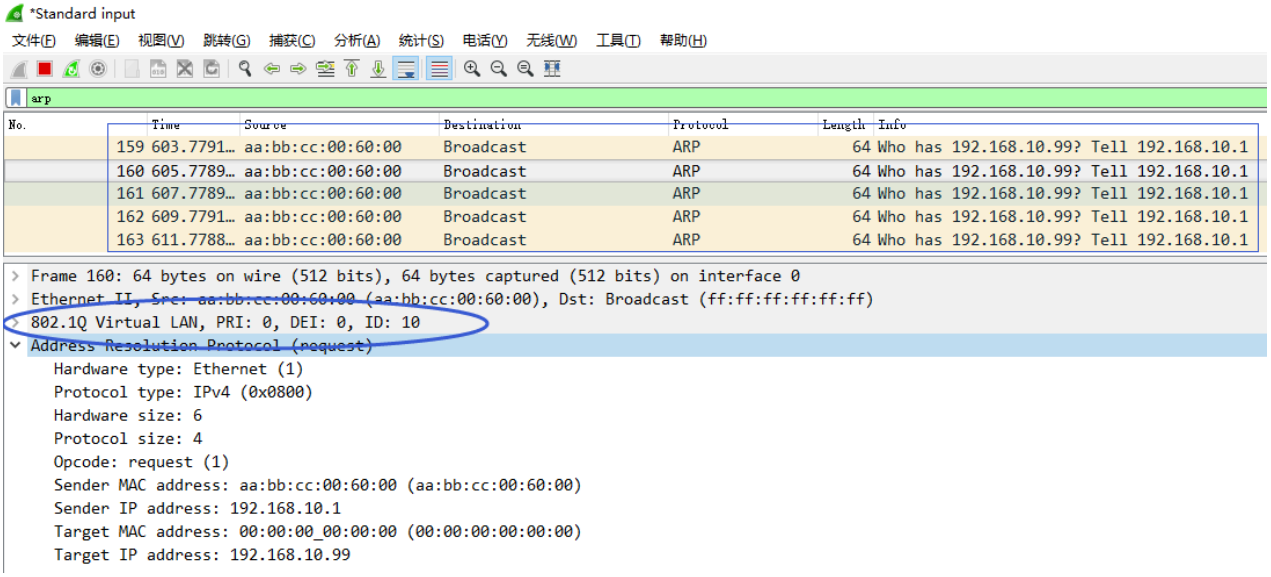
4. 测试Router1的E0/0.10 192.168.10.1→192.168.10.99的业务，此业务携带了VLAN-TAG 10。

```
Router1#ping 192.168.10.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

5. 结果不通，在FGT上抓包。

```
FortiGate_Transparent # diagnose sniffer packet any "arp or icmp" 4 0 l
interfaces=[any]
filters=[arp or icmp]
```

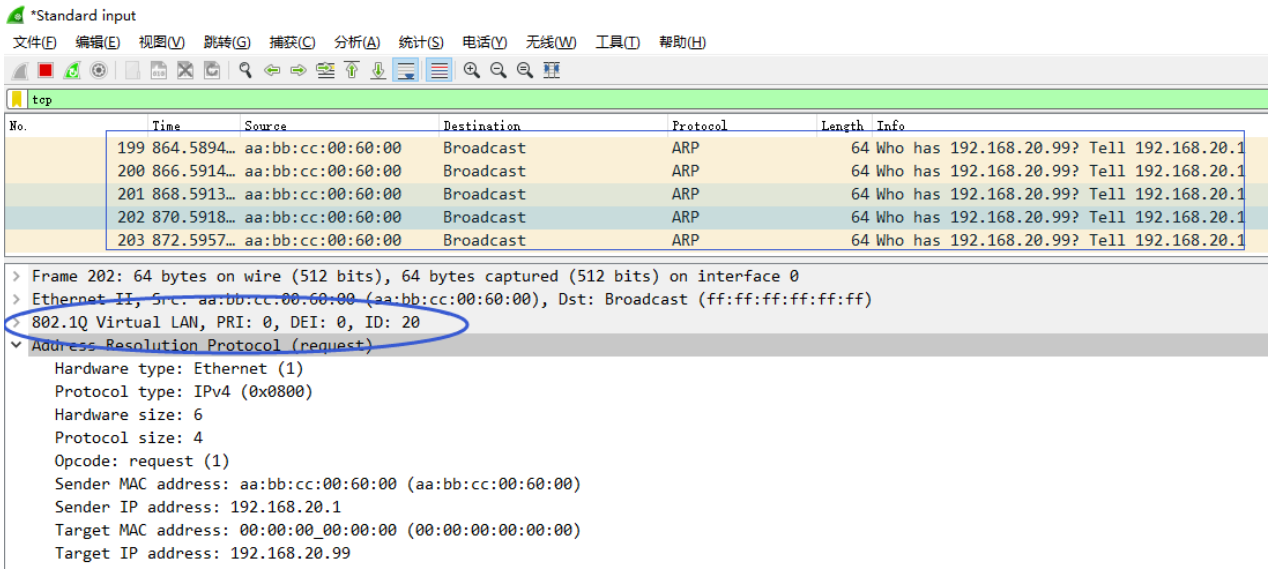
6. 什么都抓不到，通过镜像抓包查看，发现携带了vlan-tag 10的ARP报文都无法被转发，也就是说接口下的这条命令：set vlanforward disable，且FGT本地没有对应vlan-tag 10的接口，会丢弃携带了vlan-tag 10的任何报文，包括ARP报文，甚至数据报文CPU都不上送，携带了VLAN-TAG的数据会被当做非IP流量数据直接丢弃。



7. 测试VLAN20的数据和vlan10同样的效果。

```
Router1#ping 192.168.20.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

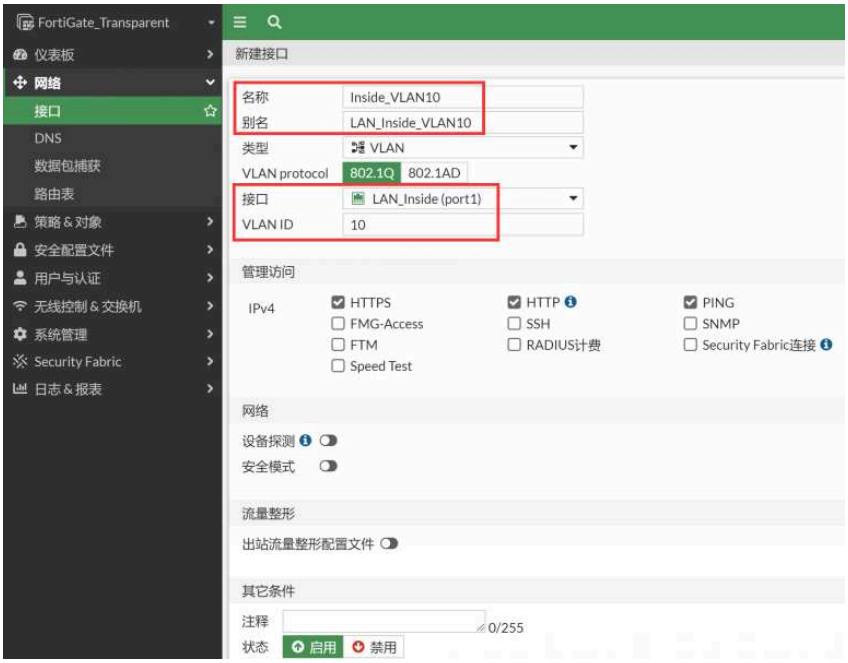


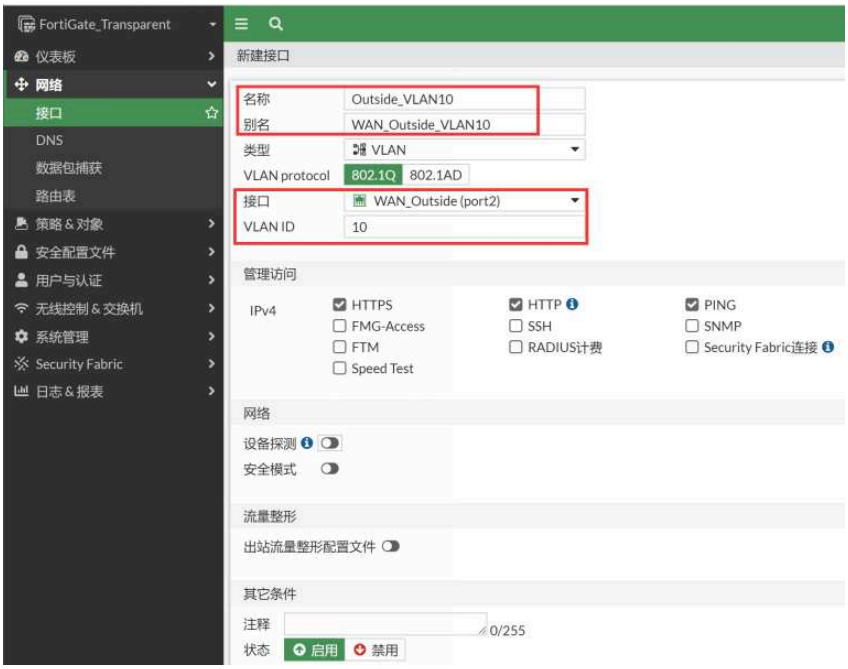
8. 查看Router1的ARP表，发现无法学习到相关的ARP条目。

```
Router1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
 …
Internet  192.168.10.99           0   Incomplete      ARPA
Internet  192.168.20.99           0   Incomplete      ARPA
 …
```

9. 在FGT的Port1和Port2上增加Inside_VLAN10和Outside_VLAN10的两个VLAN 10的接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







.0. 将两个VLAN接口加入到forward-domain 10里。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit Inside_VLAN10
FortiGate_Transparent (Inside_VLAN10) # set forward-domain 10
FortiGate_Transparent (Inside_VLAN10) # next
FortiGate_Transparent (interface) # edit Outside_VLAN10
FortiGate_Transparent (Outside_VLAN10) # set forward-domain 10
FortiGate_Transparent (Outside_VLAN10) # end
```

重要

配置VLAN-ID的场景下则必须配置“forward-domain” 否则FGT的MAC地址表项会错乱翻转，业务不通，甚至存在广播风暴的风险。

重要

假设不配置forward-domain，由于port2、port2.10（Outside_VLAN10）都是属于同一个广播域，那么192.168.10.1请求192.168.10.99的ARP广播请求会被发送到port2、port2.10（Outside_VLAN10）甚至port1都会被广播出去，同时由于Router2的E0/0（192.168.1.99）和E0/0.10（192.168.10.99）的MAC地址一样都是：aa:bb:cc:00:20:00，由于在同一个广播域中的不同接口不能存在相同的MAC地址，此时port2也可以学习到aa:bb:cc:00:20:00,同时port2.10（Outside_VLAN10）也可以学习到aa:bb:cc:00:20:00，这样会造成MAC地址表冲突，同时MAC表中只能存在一个MAC表项，会操作MAC表翻转，如果配置全通策略，甚至可能引起环路的风险。因此配置VLAN-ID务必将forward-domain配置上，这是一个很必要的配置操作。

1. 查看配置了forward-domain的FortiGate的MAC表和Router1的arp表。

```
FortiGate_Transparent # diag netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=6, num=10, depth=2
Bridge root.b host table
port no device  devname mac addr                ttl     attributes
...
  6     14      Outside_VLAN10  aa:bb:cc:00:20:00       5        Hit(5)
  2     4       port2   aa:bb:cc:00:20:00       0        Hit(0)
...
```

```
Router1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
...
Internet  192.168.1.99           0   aabb.cc00.2000  ARPA   Ethernet0/0
Internet  192.168.10.99          0   aabb.cc00.2000  ARPA   Ethernet0/0.10
...
```

2. 此时再看VLAN10的业务，在Router1上使用192.168.10.1 ping 192.168.10.99。

```
Router1#ping 192.168.10.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.99, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

3. 虽然还是不通，但是情况已经不一样了，明显VLAN10的数据全部上送到了CPU进行处理，ARP可正常学习，只是ping不通，原因是防火墙没有配置策略，所以匹配了默认的drop策略。

```
FortiGate_Transparent # diagnose sniffer packet any "arp or icmp" 4 0 l
interfaces=[any]
filters=[arp or icmp]
2019-07-03 18:24:49.697190 Inside_VLAN10 in arp who-has 192.168.10.99 tell 192.168.10.1
2019-07-03 18:24:49.697218 Outside_VLAN10 out arp who-has 192.168.10.99 tell 192.168.10.1
2019-07-03 18:24:49.698089 Outside_VLAN10 in arp reply 192.168.10.99 is-at aa:bb:cc:0:20:0
2019-07-03 18:24:49.698102 Inside_VLAN10 out arp reply 192.168.10.99 is-at aa:bb:cc:0:20:
2019-07-03 18:24:51.700405 Inside_VLAN10 in 192.168.10.1 → 192.168.10.99: icmp: echo request
2019-07-03 18:24:53.700372 Inside_VLAN10 in 192.168.10.1 → 192.168.10.99: icmp: echo request
2019-07-03 18:24:55.704350 Inside_VLAN10 in 192.168.10.1 → 192.168.10.99: icmp: echo request
2019-07-03 18:24:57.704314 Inside_VLAN10 in 192.168.10.1 → 192.168.10.99: icmp: echo request
```

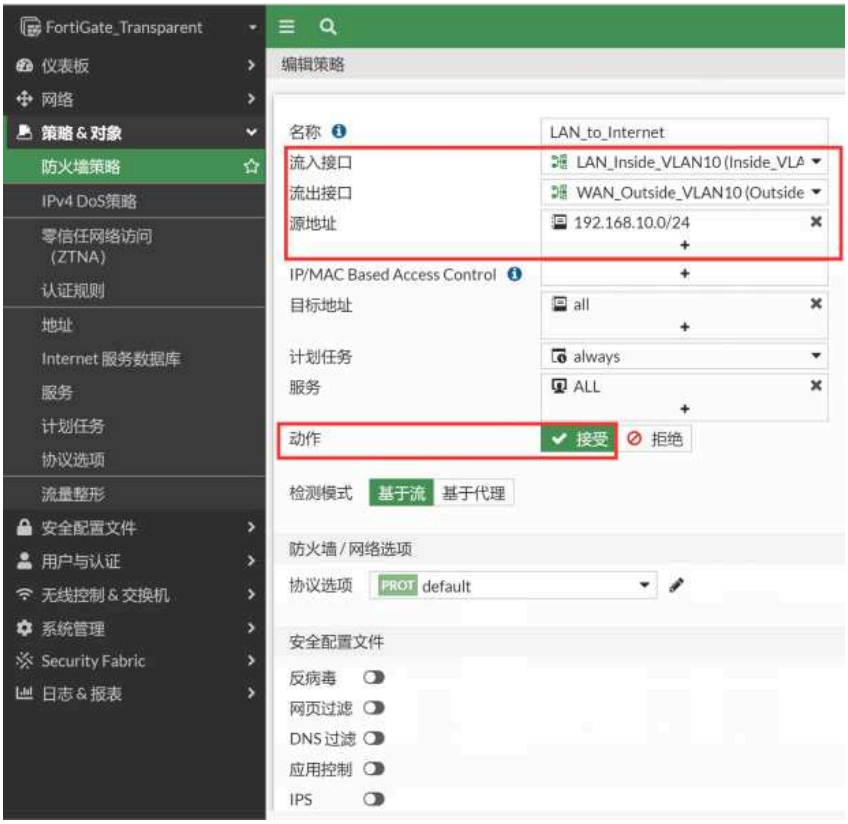
```
Router1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   aabb.cc00.6000  ARPA   Ethernet0/0
Internet  192.168.1.99           5   aabb.cc00.2000  ARPA   Ethernet0/0
Internet  192.168.10.1           -   aabb.cc00.6000  ARPA   Ethernet0/0.10
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Internet  192.168.10.99          0   aabb.cc00.2000  ARPA   Ethernet0/0.10  // arp可以学习到
Internet  192.168.20.1           -   aabb.cc00.6000  ARPA   Ethernet0/0.20
```

```
diagnose debug flow filter addr 192.168.10.1
diagnose debug flow filter  proto 1
diagnose debug flow show function-name enable
diagnose debug flow trace start 10
diagnose debug enable

id=20085 trace_id=2 func=print_pkt_detail line=5428 msg="vd-root:0 received a packet(proto=1, 192.168.10.1:17->192.168.10.99:2048) from Inside_VLAN10. type=8, code=0, id=17, seq=0."
id=20085 trace_id=2 func=init_ip_session_common line=5593 msg="allocate a new session-00000244"
id=20085 trace_id=2 func=br_fw_forward_handler line=565 msg="Denied by forward policy check"
```

4. 此时在FortiGate上配置VLAN 10的放通安全策略。



5. VLAN10的数据可以正常通信。

```
Router1#ping 192.168.10.99 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.10.99, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/2 ms
```

```
FortiGate_Transparent # diagnose sniffer packet any "icmp or arp" 4 0 l
interfaces=[any]
filters=[icmp or arp]
2019-07-03 18:57:39.090299 Inside_VLAN10 in 192.168.10.1 → 192.168.10.99: icmp: echo request
2019-07-03 18:57:39.090376 Outside_VLAN10 out 192.168.10.1 → 192.168.10.99: icmp: echo request
2019-07-03 18:57:39.090379 port2 out 192.168.10.1 → 192.168.10.99: icmp: echo request
2019-07-03 18:57:39.091154 Outside_VLAN10 in 192.168.10.99 → 192.168.10.1: icmp: echo reply
2019-07-03 18:57:39.091166 Inside_VLAN10 out 192.168.10.99 → 192.168.10.1: icmp: echo reply
2019-07-03 18:57:39.091168 port1 out 192.168.10.99 → 192.168.10.1: icmp: echo reply
```

总结

在默认的“set vlanforward disable”的情况下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

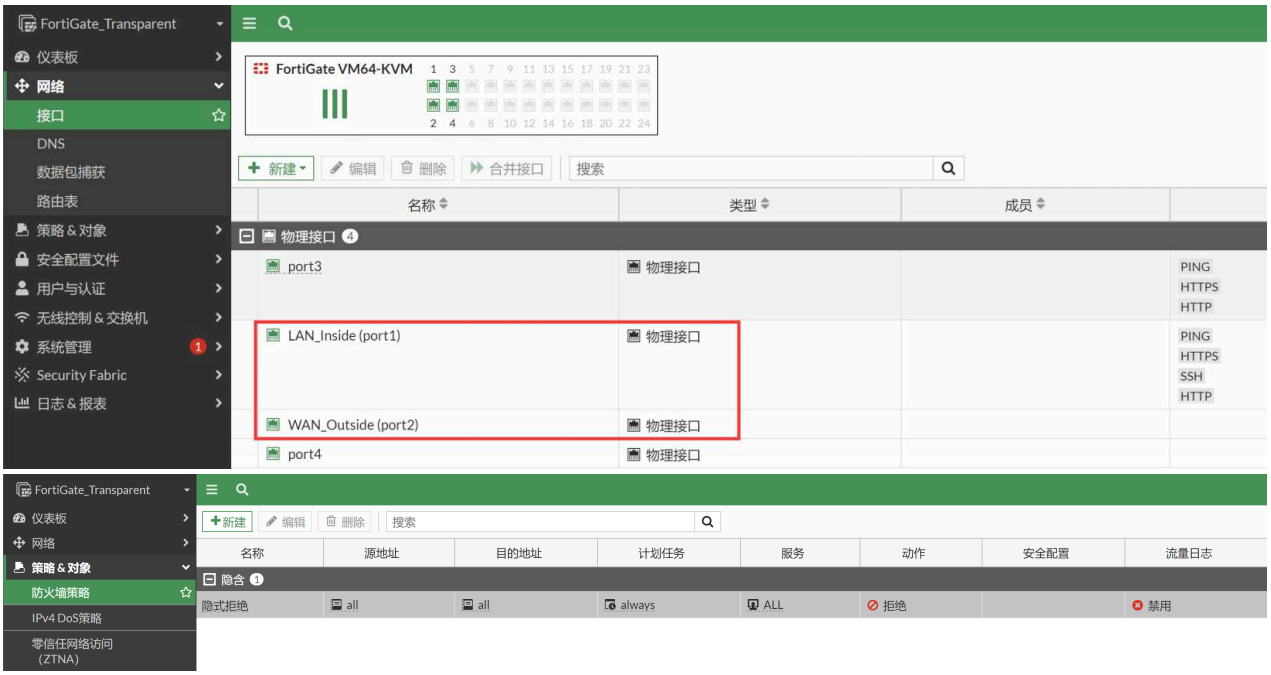
- 如果FGT本地存在VLAN-ID接口（此处为类似VLAN1的接口 port1）则数据会上送CPU处理，如果配置VLAN10的接口，则接收到了VLAN-TAG10的VLAN数据也会上送CPU处理，那么通不通就完全看安全策略是否放通了。
- 如果FGT本地不存在VLAN-ID的接口，收到了VLAN-TAG的数据，且本地并没有相应的VLAN接口，那么这样的数据将会被FGT底层当做非IP数据丢弃，上送CPU的机会都没有，直接丢弃，连arp都不处理，直接丢弃。

场景二：开启vlanforward

实验步骤

1. 在port1和port2上开启vlanforward（不配置任何VLAN接口和安全策略）。

```
config system interface
    edit "port1"
        set vdom "root"
        set allowaccess ping https ssh http
        set vlanforward enable
        set type physical
        set alias "LAN_Inside"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set allowaccess ping https ssh http
        set vlanforward enable
        set type physical
        set alias "WAN_Outside"
        set snmp-index 2
    next
end
```



2. 再次测试一下Router1到Router2的VLAN 20的业务，VLAN 20的数据是通的。

```
Router1#ping 192.168.20.99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

3. 但是在FGT上抓取不到任何的VLAN20相关的数据，数据没有上送到CPU处理，直接被bypass掉了。

```
FortiGate_Transparent # diagnose sniffer packet any "icmp or arp" 4 0 l
interfaces=[any]
filters=[icmp or arp]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

总结

如果FGT上没有创建VLAN20的这个接口，同时接口开启了vlanforward，那么相当于这些未知的携带了VLAN-TAG的数据，将会统统bypass掉，不上CPU处理直接转发走。

如果不熟悉vlanforward和forward-domain的工作原理，这样的bypass流量风险比较大，因为那些bypass的流量FGT完全不可控，也不可见，一旦出问题完全无法掌控，因此vlanforward不建议开启，保持默认disable即可。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Remapping VLAN ID(VLAN NAT，特殊场景使用)

重要

VLAN NAT，特殊场景使用。

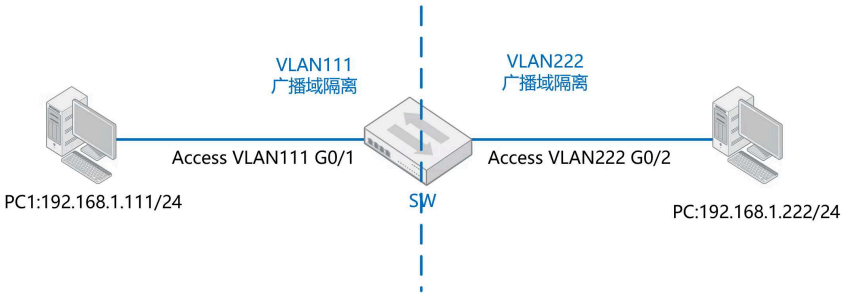
简介

Remapping VLAN简单的可以理解为，透明模式下VLAN ID的NAT转换。比如数据本来在VLAN104中，一旦需要透明穿过VLAN105去访问目的主机，这个时候FGT可以将原本携带了VLAN-Tag 104的数据转换为携带VLAN-Tag 105的数据，进行了一个VLAN-Tag的替换，以便数据可以在两个VLAN之间通信。

重要

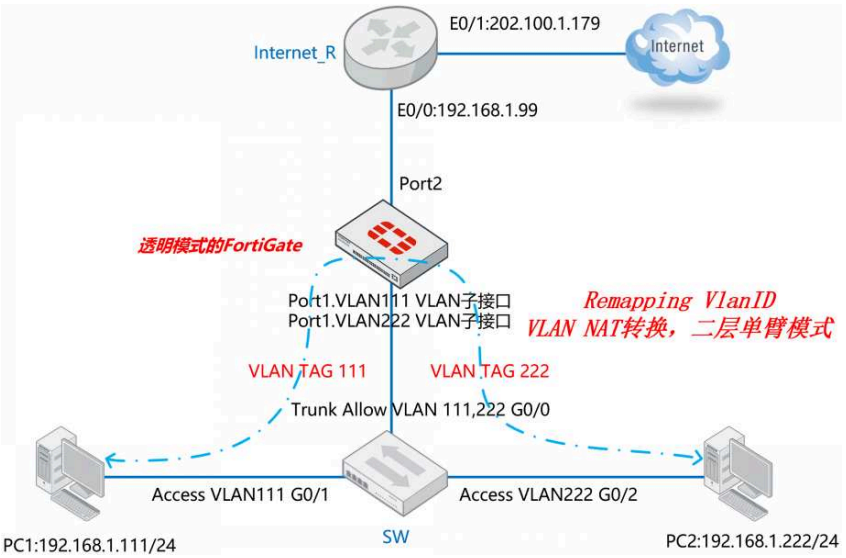
谁说的跨VLAN之间通信的数据必须经过路由器（三层设备），不，Fortigate二层也可以！但是这个技术使用场景有限，一般用在私有云环境中的东西向流量的控制和过滤，用的比较少，了解即可。

原始网络拓扑和需求



需求：要求PC1和PC2之间虽然是相同的网段，但是要相互隔离，同时要求防火墙策略对二者进行访问控制，PC1可以访问PC2，但是PC2不能访问PC1，同时要求PC1和PC2都可以正常的访问互联网。

解决方案拓扑



基础配置

SW:

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/1
switchport access vlan 111
switchport mode access
no shutdown
spanning-tree portfast edge
!
interface GigabitEthernet0/2
switchport access vlan 222
switchport mode access
no shutdown
spanning-tree portfast edge
```

Internet_R:

```
interface Ethernet0/1
ip address 202.100.1.179 255.255.255.0
no shutdown
ip nat outside
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 202.100.1.192
!
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/1 overload
```

FortiGate:

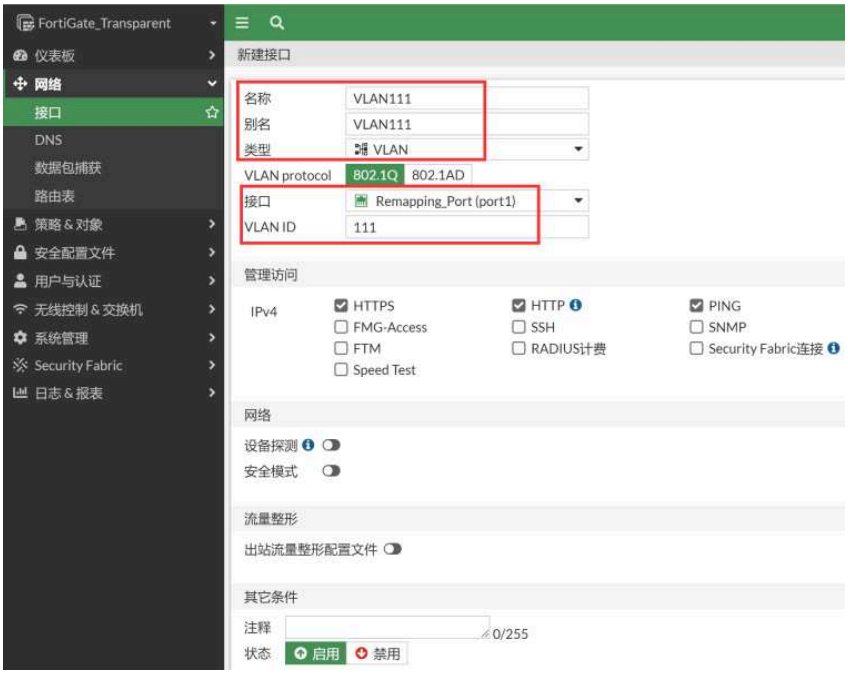
```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FortiGate_Transparent
FortiGate_Transparent (global) # set timezone 55
FortiGate_Transparent (global) # set language simch
FortiGate-VM64-KVM (global) # end
FortiGate_Transparent # config system settings
FortiGate_Transparent (settings) # set opmode transparent    //修改FGT的运行模式为透明模式，默认为NAT路由模式。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。
FortiGate_Transparent (settings) # set manageip 192.168.1.100 255.255.255.0    //配置可以管理防火墙的本地IP和网关，以便HTTP/SSH管理防火墙及防火墙的服务更新。
FortiGate_Transparent (settings) # set gateway 192.168.1.99
FortiGate_Transparent (settings) # end
Changing to TP mode

MGMT1或MGMT2口默认有管理权限，以要通过port2 接口管理设备为例，开启port2管理FGT的命令如下：
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit port2
FortiGate_Transparent (port1) # set allowaccess https http ping ssh    //允许网管协议从Port2接口通过https/http/SSH/Ping访问透明模式的FortiGate
FortiGate_Transparent (port1) # end
```

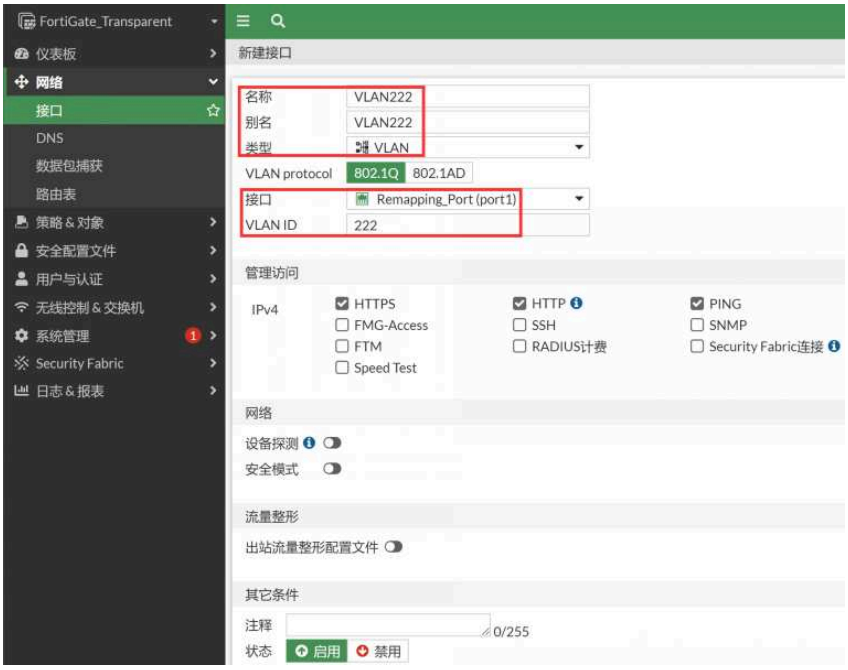
配置步骤

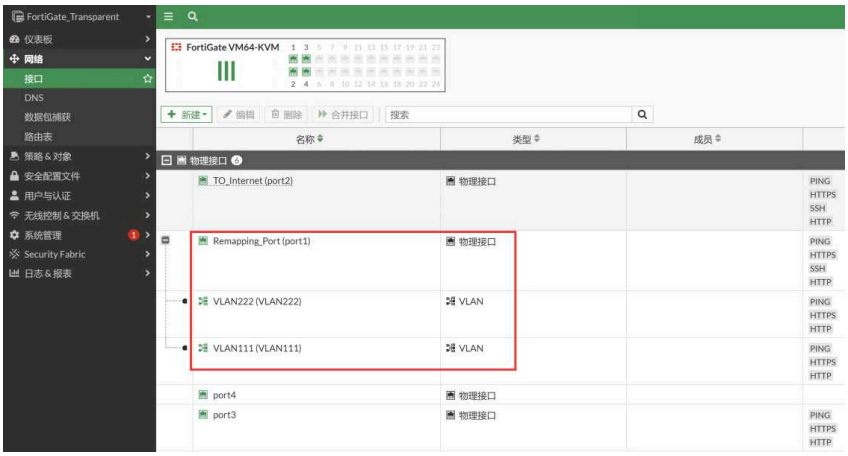
1. 在FortiGate上创建VLAN子接口，VLAN111和VLAN222，分别绑定在port1和port2下。

> **重要**
>
> 建议在不需要的情况下关闭接口配置下的“设备探测”（Device detection）功能，该功能用于MAC地址厂商设备信息识别及MAC地址过滤，会消耗较多的设备资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







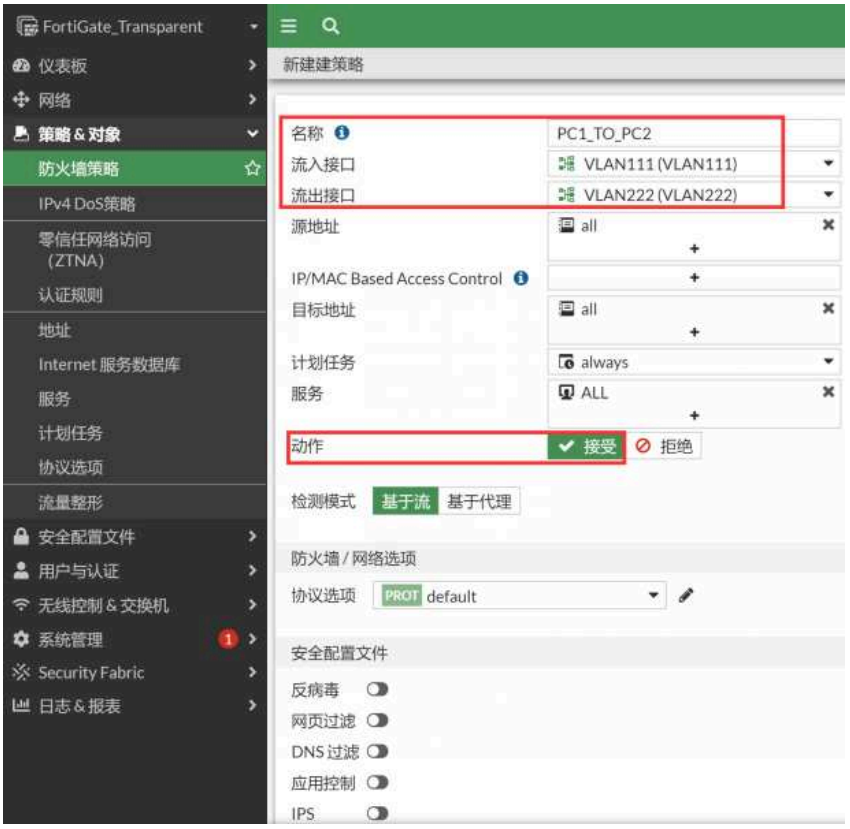
2. 页面右上角打开Web CLI，将VLAN111、VLAN222、port2三个接口划入到同一个Forward-Domain里。这样就将VLAN111和VLAN222之间的广播域打通了，VLAN111去访问VLAN222，则VLAN TAG 111就会被替换成 VLAN TAG222，反过来也一样的效果。同时VLAN111和VLAN222和Port2也是一个广播域，这样VLAN111和VLAN222配置策略后，可以通过Port2上互联网。

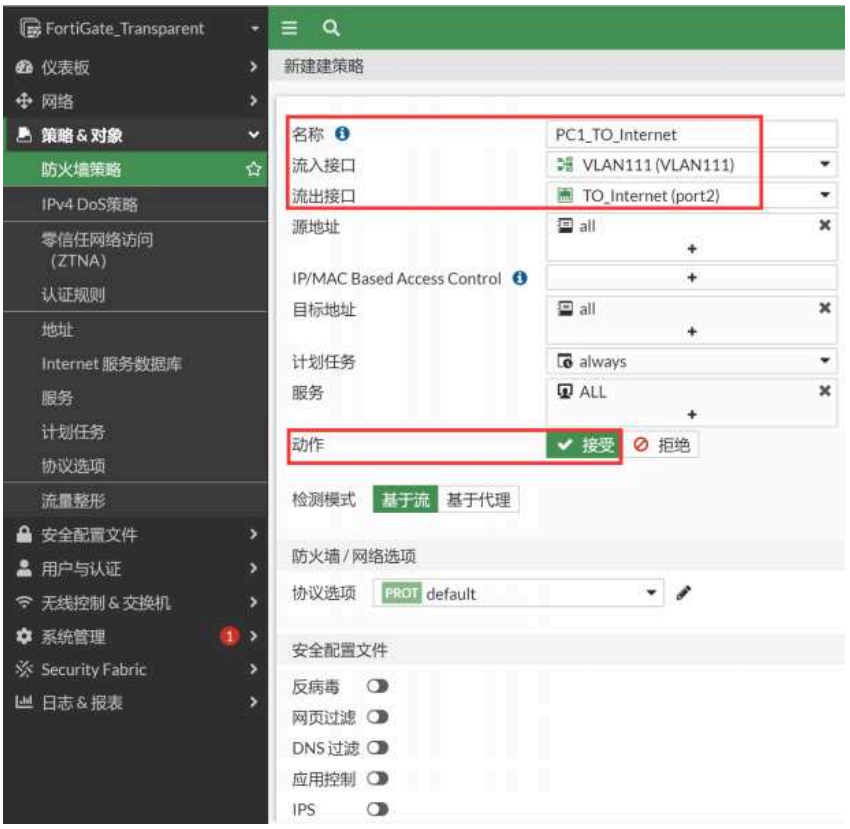
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
切换到命令行，将三个接口划入到同一个Forward-Domain里：
config system interface
    edit "VLAN111"
        set forward-domain 111222
        set alias "VLAN111"
        set interface "port1"
        set vlanid 111
    next
    edit "VLAN222"
        set forward-domain 111222
        set alias "VLAN222"
        set interface "port1"
        set vlanid 222
    next
    edit "port2"
        set allowaccess ping https ssh http
        set forward-domain 111222
        set alias "TO_Internet"
    next
end
```

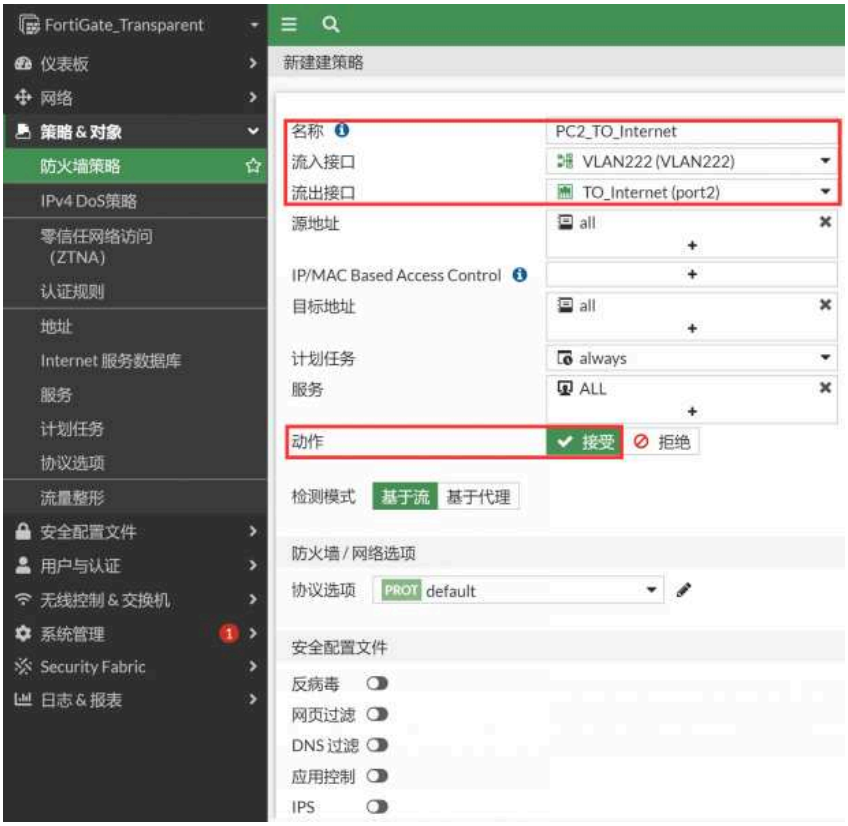
3. 这样流量是通过防火墙策略控制的，因此接下来需要配置防火墙策略，实现：PC1和访问PC2，但是PC2不能访问PC1，同时要求PC1和PC2都可以正常的访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

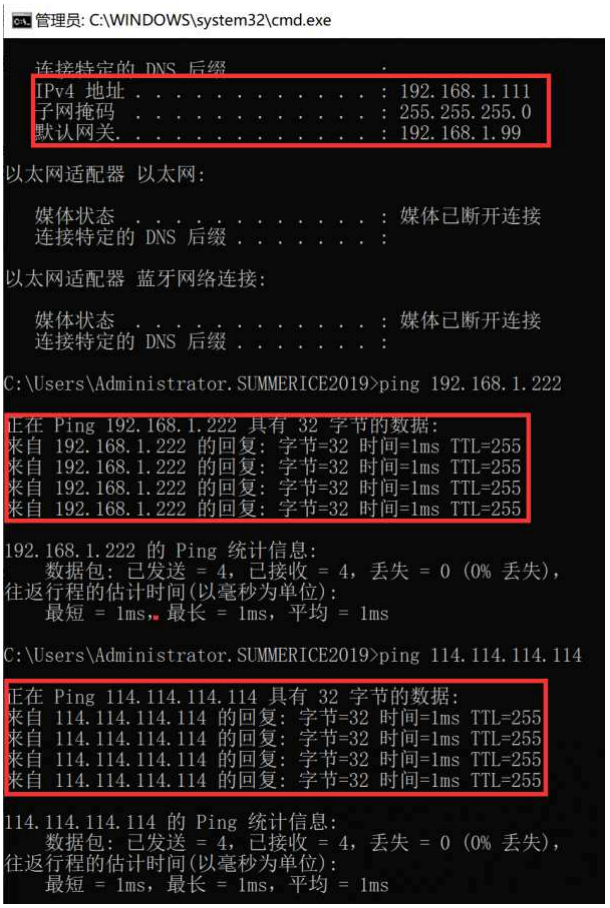




结果验证

1. PC1访问PC2和Internet，访问成功。

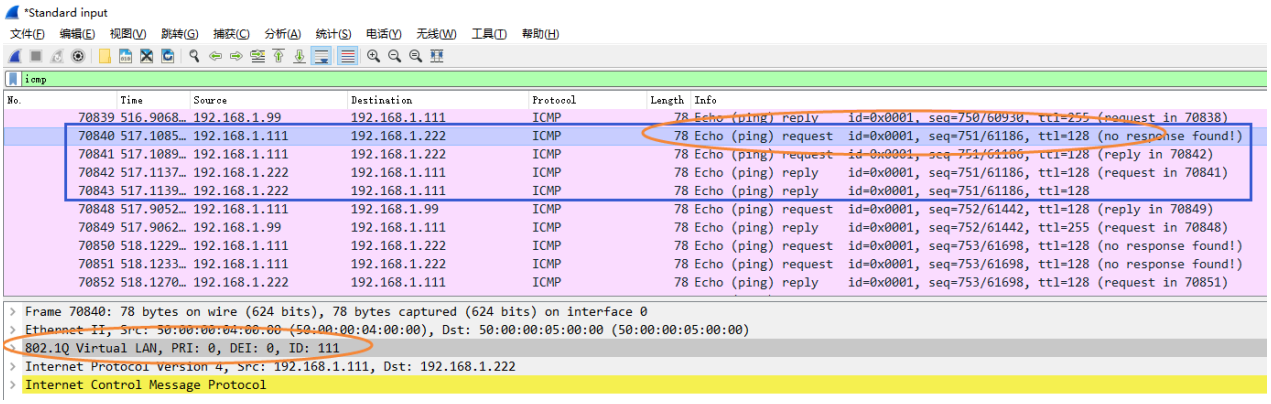
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



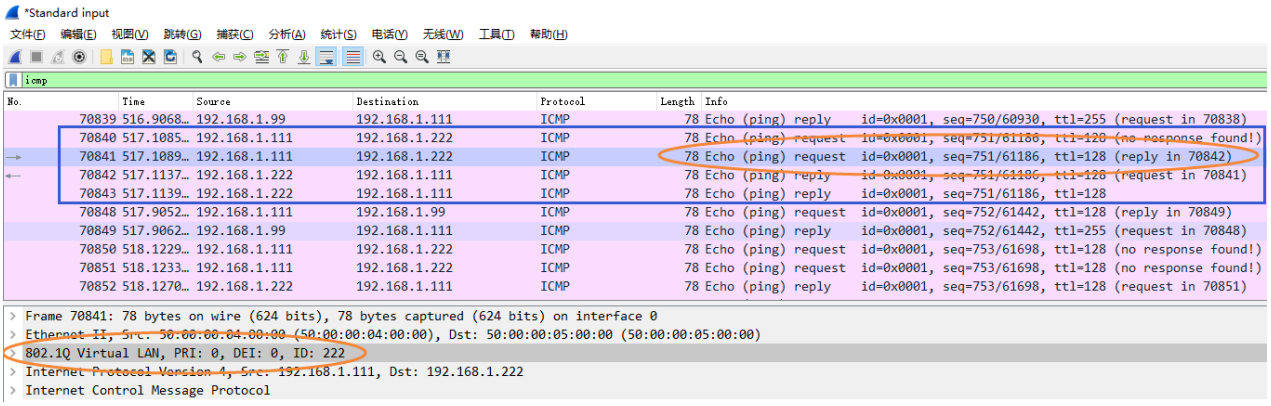
2. 抓包查看PC1访问PC2。

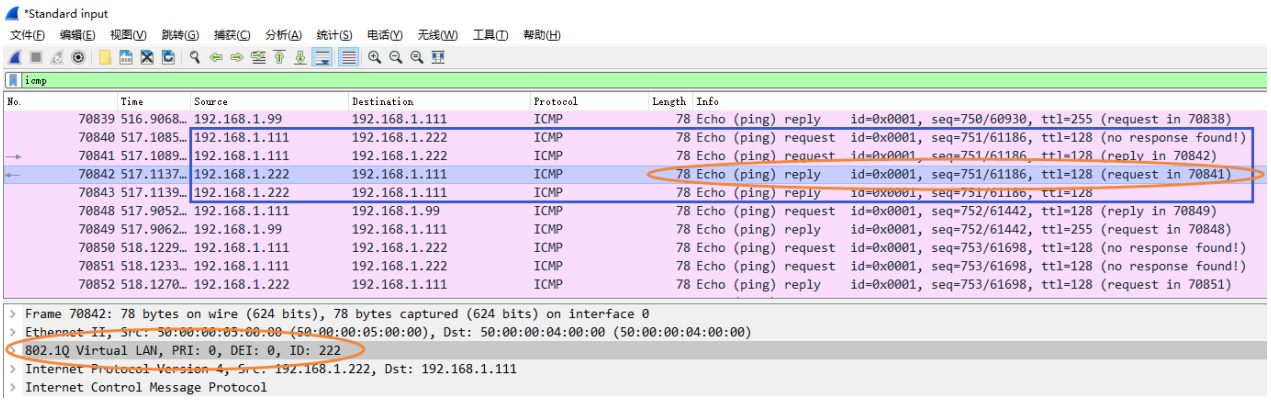
```
FortiGate_Transparent # dia sni pac any "host 192.168.1.222 and icmp" 4
interfaces=[any]
filters=[host 192.168.1.222 and icmp]
0.765120 VLAN111 in 192.168.1.111 → 192.168.1.222: icmp: echo request
0.765133 VLAN222 out 192.168.1.111 → 192.168.1.222: icmp: echo request
0.765136 port1 out 192.168.1.111 → 192.168.1.222: icmp: echo request
0.769002 VLAN222 in 192.168.1.222 → 192.168.1.111: icmp: echo reply
0.769012 VLAN111 out 192.168.1.222 → 192.168.1.111: icmp: echo reply
0.769014 port1 out 192.168.1.222 → 192.168.1.111: icmp: echo reply
```

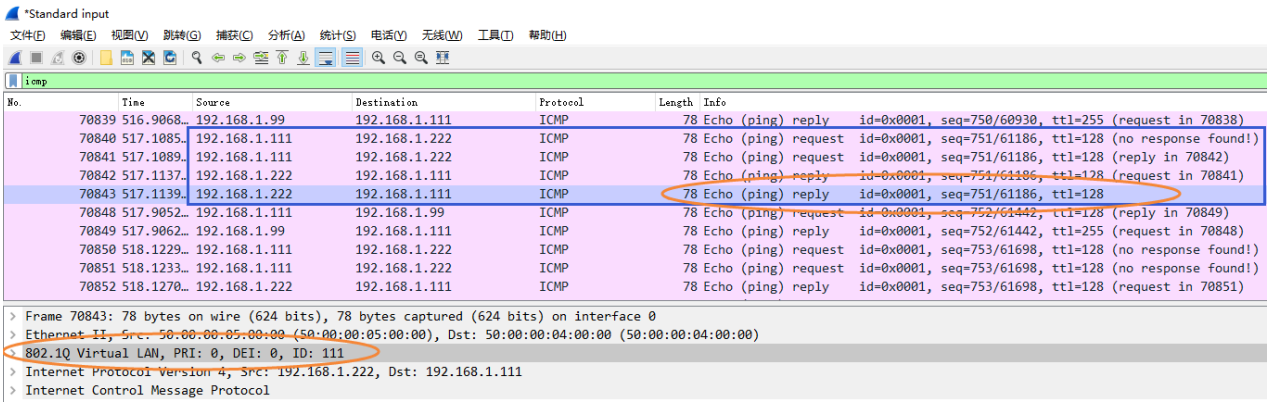
3. 在FortiGate上镜像port1的报文。分析一个PC1 ping PC2的过程 VLAN TAG的变化，非常直接的可以看到请求报文的VLAN-TAG从111变成了222，回复报文的VLAN-TAG从222变成了111，实现了remapping VlanID的功能。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







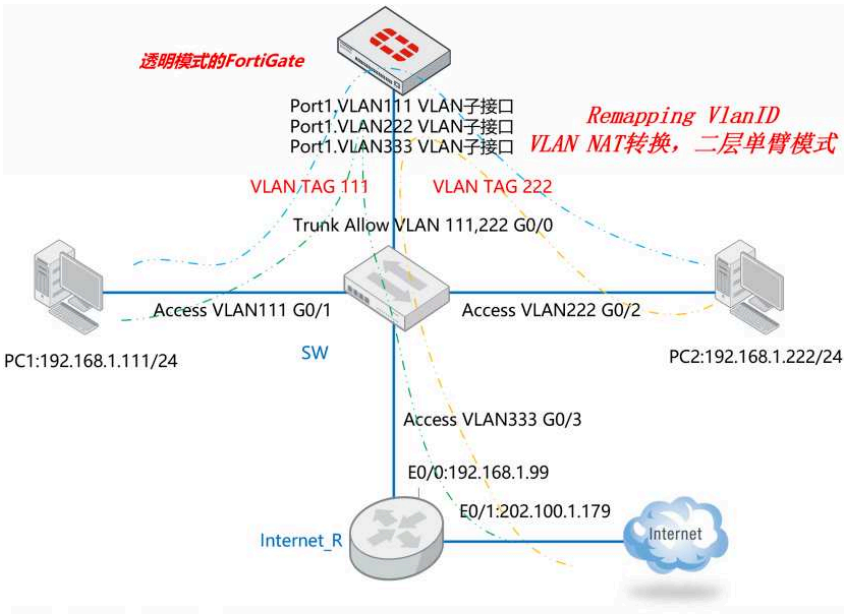
补充

当然组网可以调整为：防火墙完全单臂部署，PC1属于VLAN111、PC2属于VLAN222、Internet_R属于VLAN333，默认情况下相互隔离。

FGT配置remapping VlanID，可以让Port1子接口VLAN111、VLAN222、VLAN333加入到同一个Forward-Domain中，让三者广播域互通，同时FGT可以通过策略控制三者的流量。

这种方案可以用来作为内网相同网段主机的安全隔离，针对二层环境下东西向流量进行安全控制。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



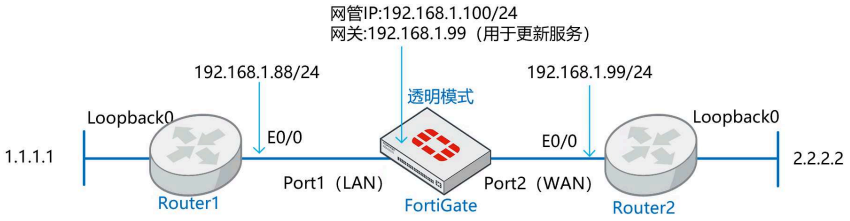
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

组播(OSPF)与透明模式

网络需求

路由器1和路由器2之间运行了动态路由协议，防火墙以透明模式运行在两台路由器之间，需要确保两台路由器之间的动态路由协议运行正常，并且数据可通。

网络拓扑



R1和R2之间运行了RIP/OSPF/EIGRP协议

配置要点

- Router1/Router2路由器的基础配置
- 将防火墙配置为透明模式并开启网管
- 默认不配置策略情况下，观察动态路由协议的情况
- 配置安全策略解决OSPF/EIGRP邻居关系异常

配置步骤和结果验证

1. Router1/Router2路由器的基础配置。

Router1：

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.1.88 255.255.255.0
no shutdown
!
router ospf 10
network 1.1.1.1 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
router rip
version 2
network 1.0.0.0
network 192.168.1.0
no auto-summary
!
router eigrp 10
network 1.1.1.1 0.0.0.0
network 192.168.1.0
```

Router2：

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.1.99 255.255.255.0
no shutdown
!
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
router ospf 10
network 2.2.2.2 0.0.0.0 area 0
network 192.168.1.0 0.0.0.255 area 0
!
router rip
version 2
network 2.0.0.0
network 192.168.1.0
no auto-summary
!
router eigrp 10
network 2.2.2.2 0.0.0.0
network 192.168.1.0

```

2. 将防火墙配置为透明模式，进入设备命令行（CLI）中进行配置，修改FGT的运行模式为透明模式（默认为NAT路由模式）。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。配置可以管理防火墙的本地IP和网关。

```bash
config system global
    set hostname FortiGate_Transparent
end
config system settings
    set opmode transparent
    set manageip 192.168.1.100 255.255.255.0
    set gateway 192.168.1.99
end
```

3. MGMT口默认有管理权限，要通过port1（LAN）接口管理设备为例，开启port1（LAN）管理FGT的命令如下。允许网管协议从Port1接口通过https/http/SSH/Ping访问透明模式的FortiGate。

```bash
config system interface
    edit port1
    edit allowaccess https http ping ssh
end
```

4. 默认不配置策略情况下，观察动态路由协议的情况，RIP 邻居是正常的，但是OSPF邻居无法建立成功，EIGRP邻居路由学习异常，邻居反复的震荡。

```
Router1#show ip rip database
1.0.0.0/8    auto-summary
1.1.1.1/32    directly connected, Loopback0
2.0.0.0/8    auto-summary
2.2.2.2/32
    [1] via 192.168.1.99, 00:00:01, Ethernet0/0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, Ethernet0/0

Router1#show ip route
 ...
R        2.2.2.2 [120/1] via 192.168.1.99, 00:00:03, Ethernet0/0
 ...
```

```
Router1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 10)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         274         0×80000003 0×00F9A5 2

Router1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   EXSTART/DR      00:00:31    192.168.1.99    Ethernet0/0

Router1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   INIT/DROTHER    00:00:37    192.168.1.99    Ethernet0/0

*Jul  2 07:55:15.999: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Ethernet0/0 from EXSTART to DOWN, Neighbor Down:
Too many retransmissions
*Jul  2 07:56:16.002: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Ethernet0/0 from DOWN to DOWN, Neighbor Down:
Ignore timer expired
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Router1#
*Jul  2 07:55:24.200: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.1.99 (Ethernet0/0) is down: retry limit
exceeded
*Jul  2 07:55:28.663: %DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.1.99 (Ethernet0/0) is up: new adjacency
```

重要

原因分析：

我们知道RIP/OSPF/EIGRP都是用组播IP来建立邻居关系：RIP:224.0.0.9，OSPF:224.0.0.5/224.0.0.6，EIGRP:224.0.0.10。

对应FGT来说默认情况下：

如果组播是不通，为何RIP协议又可以正常使用?

如果组播是通的，为何OSPF/EIGRP邻居关系异常呢?

怎么看都是有点矛盾的!

5. 让我们带着这个疑惑来分析一下原因，首先，我们来看FortiGate透明模式下组播到底通还是不通，答案是：通的。原因是默认情况下有两个系统默认的设置允许组播通过FortiGate的。

配置1：系统设置：

```
FortiGate_Transparent # config system settings
FortiGate_Transparent (settings) # show full-configuration | grep multicast
    set multicast-skip-policy disable    //默认为disable，组播流量默认需要查询策略。如果修改为enable，则会bypass掉组播流量，
组播流量也是可以通的，但是FGT上不会建立组播的会话
    set gui-multicast-policy enable
```

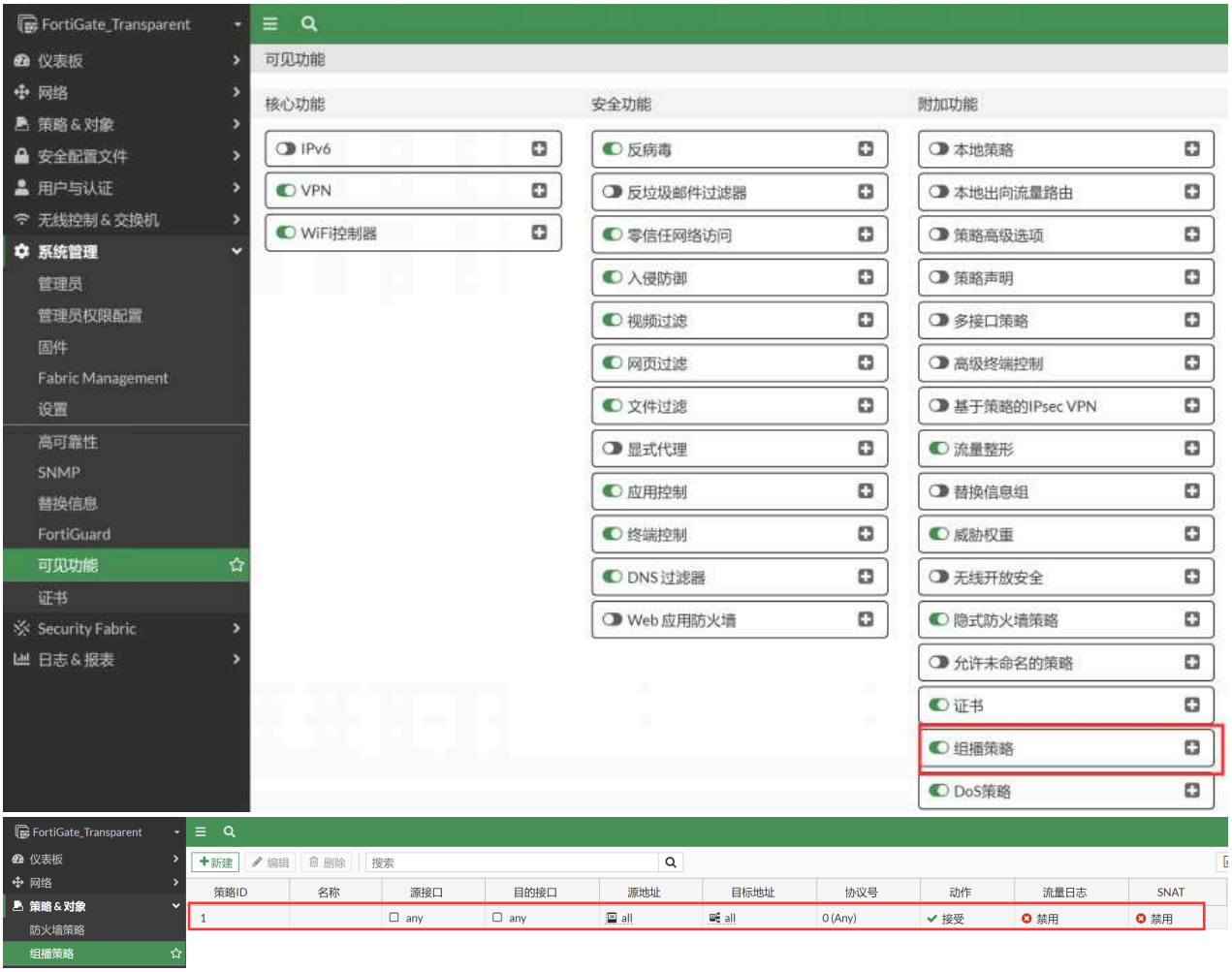
配置2:组播策略：

透明模式下的FortiGate默认存在有一条permit any到any全通的组播策略。

```
FortiGate_Transparent # config firewall multicast-policy
FortiGate_Transparent (multicast-policy) # show
config firewall multicast-policy
    edit 1
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

6. 在GUI中查看组播策略（需要在系统管理→可见功能中打开组播策略显示），可以看到这条默认放通的组播策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

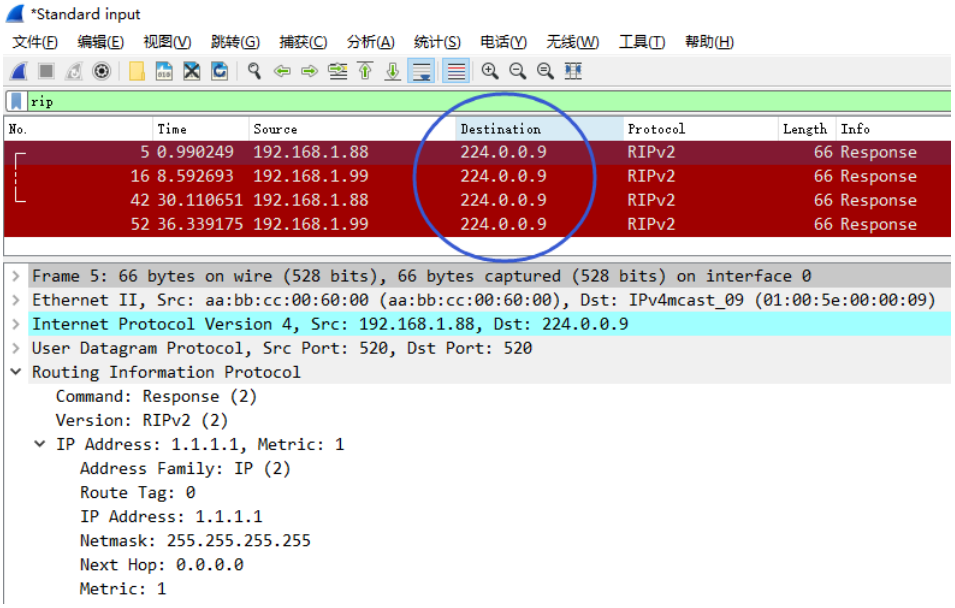


7. 通过上述两个默认的配置，可以看出FGT的组播默认就是通的。在FGT查看组播会话，这样就可以解释通为什么RIP路由协议是OK的了，抓包可以看到RIP协议只有224.0.0.9的组播报文。

```
FortiGate_Transparent # diagnose sys mcast-session list
session info: id=6 vf=0 proto=17 192.168.1.1.520→224.0.0.9.520    //RIP会话
used=2 path=3 duration=137 expire=177 indev=3 pkts=6 bytes=312
state=00000002:tp
path: policy=1, outdev=4

session info: id=4 vf=0 proto=17 192.168.1.99.520→224.0.0.9.520    //RIP会话
used=2 path=3 duration=1035 expire=174 indev=4 pkts=38 bytes=1976
state=00000002:tp
path: policy=1, outdev=3
Total 6 sessions

session info: id=3 vf=0 proto=89 192.168.1.1.0→224.0.0.5.0    //OSPF会话
used=2 path=3 duration=1037 expire=179 indev=3 pkts=110 bytes=8720
state=00000002:tp
path: policy=1, outdev=4

session info: id=5 vf=0 proto=89 192.168.1.99.0→224.0.0.5.0    //OSPF会话
used=2 path=3 duration=1034 expire=176 indev=4 pkts=110 bytes=8688
state=00000002:tp
path: policy=1, outdev=3

session info: id=7 vf=0 proto=88 192.168.1.1.0→224.0.0.10.0    //EIGRP会话
used=2 path=3 duration=22 expire=175 indev=3 pkts=6 bytes=410
state=00000002:tp
path: policy=1, outdev=4
```

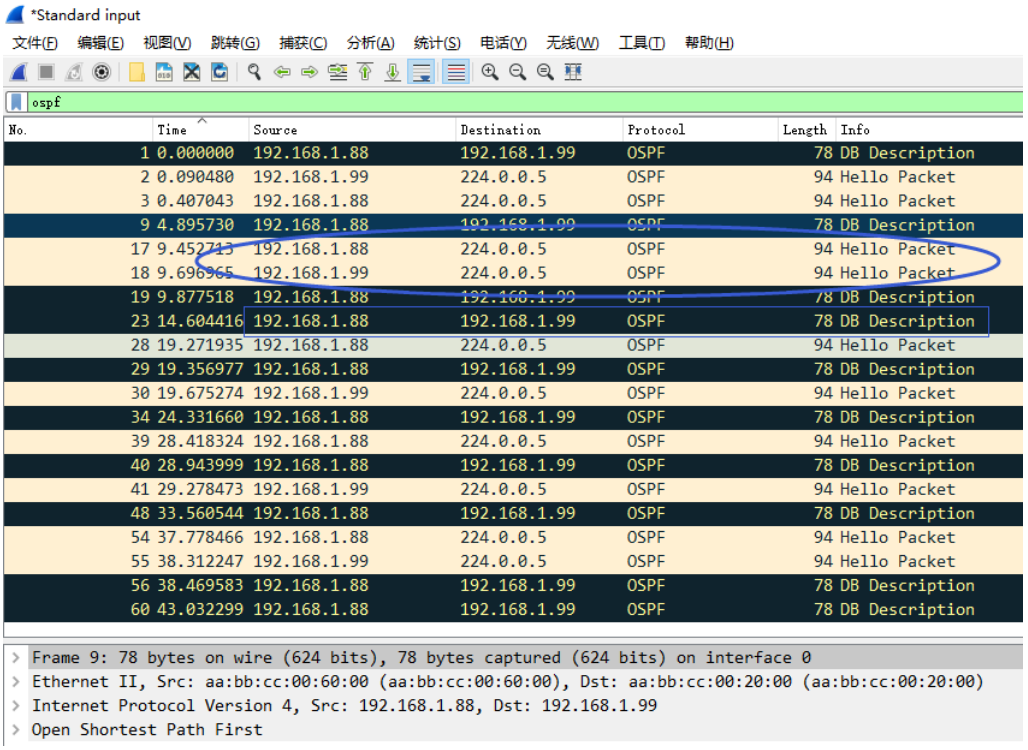

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
session info: id=2 vf=0 proto=88 192.168.1.99.0→224.0.0.10.0    //EIGRP会话
used=2 path=3 duration=1041 expire=176 indev=4 pkts=226 bytes=13610
state=00000002:tp
path: policy=1, outdev=3
```

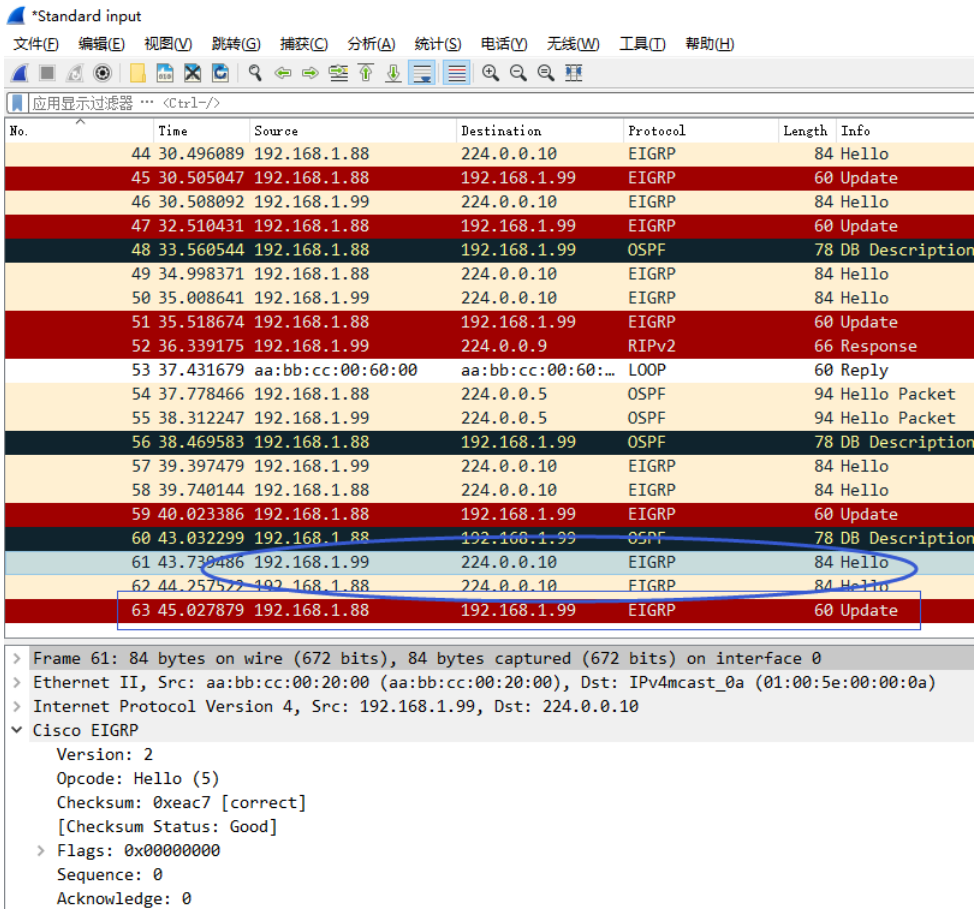


8. 既然RIP路由协议可以正常使用，那为什么OSPF和EIGRP却不行呢？进一步的分析你会发现，OSPF和EIGRP的组播其实是正常转发的，但是OSPF和EIGRP建立邻居关系不仅仅只使用了组播，而且还使用单播，默认情况下没有任何策略情况下，单播的数据会被默认丢弃，因此邻居关系异常。

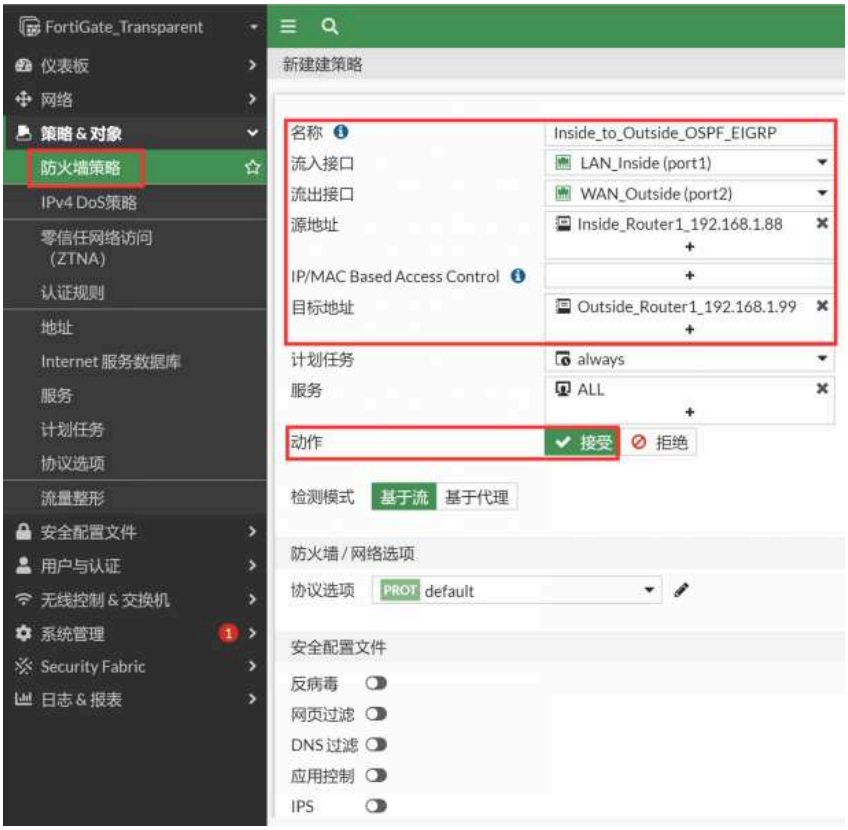
> **重要**
>
> OSPF的DB Description报文使用单播，EIGRP的Update报文使用单播。这是OSPF和EIGRP邻居关系异常的真正原因。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

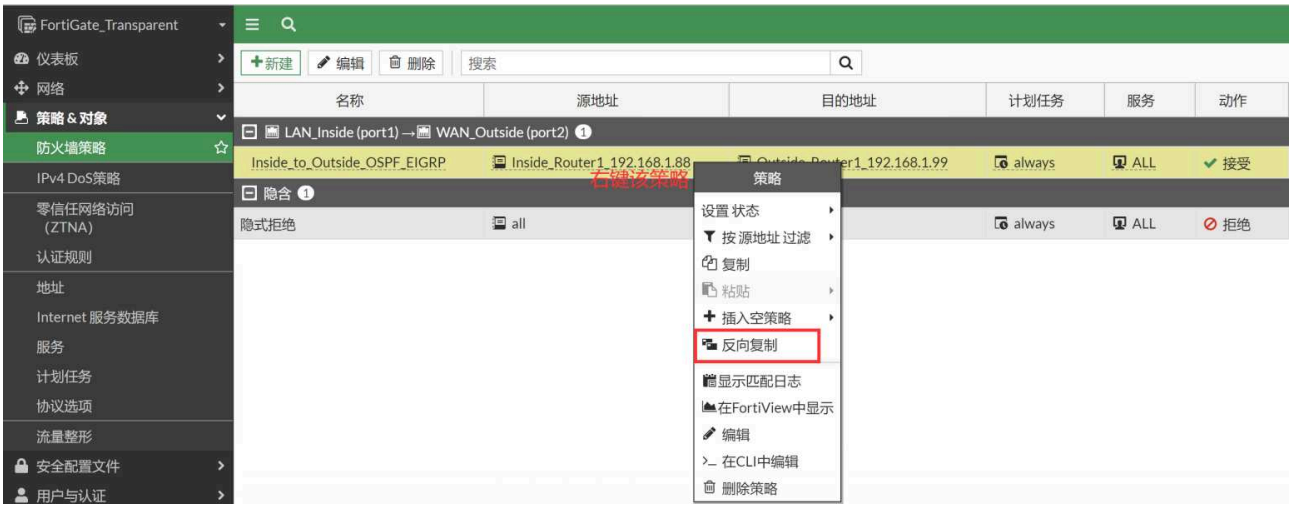


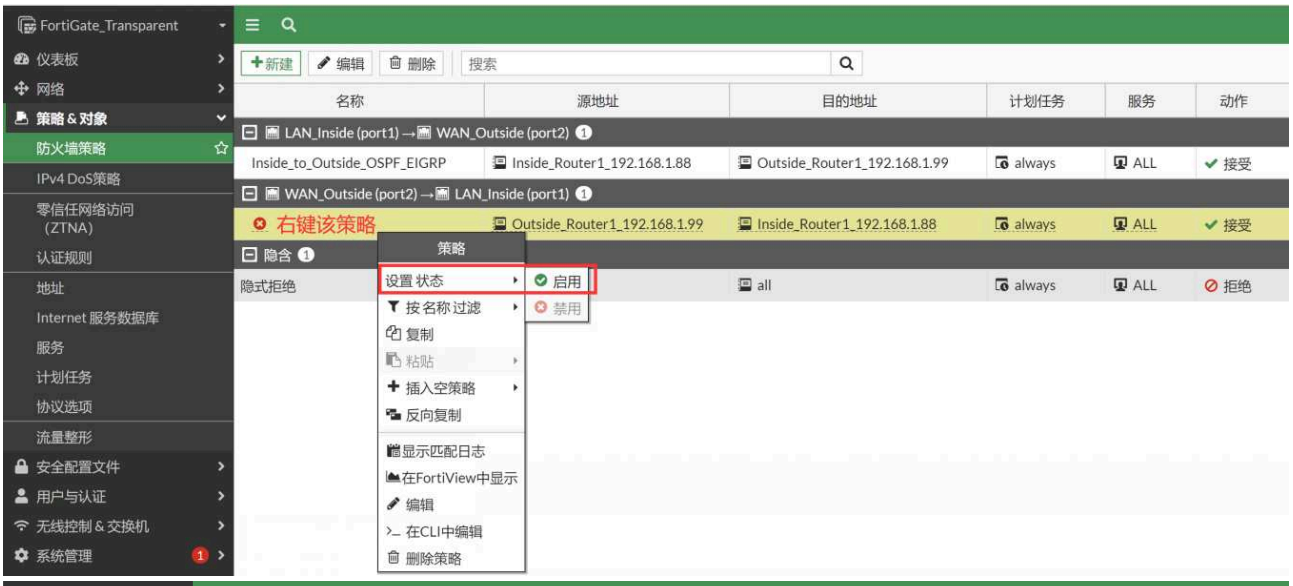
9. 既然原因清楚了，那么要解决这个问题就很简单了。只需要配置单播安全策略解决OSPF/EIGRP邻居关系异常即可。首先创建port1→port2的单播放通策略，源目为Router1和Router2的IP地址。



0. 创建完成后，右键点击该策略，选择创建反向策略，放通Router2到Router1的单播流量，并启用该策略（自行修改名称）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







1. 上述两条策略配置完毕，会发现RIP/OSPF/EIGRP的邻居关系都已经正常建立，路由学习也正常。

```
Router1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:34    192.168.1.99    Ethernet0/0

Router1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   192.168.1.99            Et0/0                    13 00:03:06   23   138  0  35

Router1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(1.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 192.168.1.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 2.2.2.2/32, 1 successors, FD is 409600
        via 192.168.1.99 (409600/128256), Ethernet0/0
P 1.1.1.1/32, 1 successors, FD is 128256
```

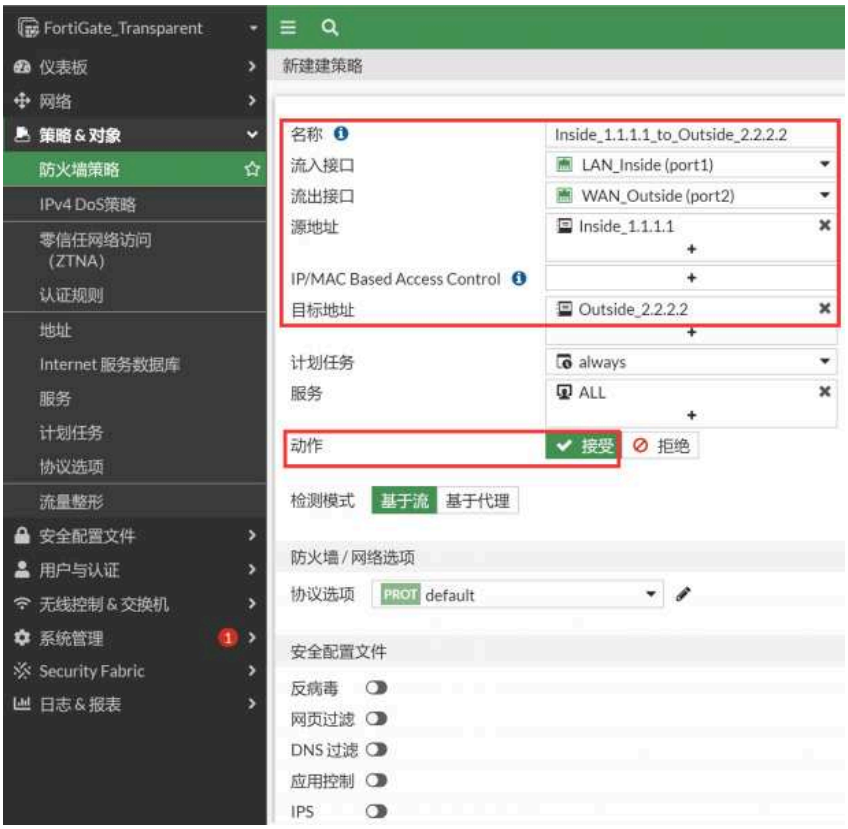

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        via Connected, Loopback0

Router1#show ip ospf database
            OSPF Router with ID (1.1.1.1) (Process ID 10)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         252         0×80000005 0×0098DF 2
2.2.2.2         2.2.2.2         253         0×80000005 0×008DD3 2
                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.1.99    2.2.2.2         253         0×80000001 0×003B1D

Router1#show ip rip  database
1.0.0.0/8    auto-summary
1.1.1.1/32    directly connected, Loopback0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, Ethernet0/0

Router1#show ip route
 ...
D        2.2.2.2 [90/409600] via 192.168.1.99, 00:02:51, Ethernet0/0
 ...
```

2. 此时使用Router1的1.1.1.1 Ping Router2的2.2.2.2，是不通的，因为FortiGate还未放通1.1.1.1和2.2.2.2之间的单播流量。

```
Router1#ping 2.2.2.2 source  1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.....
Success rate is 0 percent (0/5)
```

3. 配置单播安全策略允许Router1的1.1.1.1访问Router2的2.2.2.2。



4. 再次测试Router1的1.1.1.1 Ping Router2的2.2.2.2。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Router1#ping 2.2.2.2 source  1.1.1.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/9 ms

FortiGate抓包:
FortiGate_Transparent # diagnose sniffer packet any "icmp" 4
interfaces=[any]
filters=[icmp]
5.551382 port1 in 1.1.1.1 → 2.2.2.2: icmp: echo request
5.551455 port2 out 1.1.1.1 → 2.2.2.2: icmp: echo request
5.552281 port2 in 2.2.2.2 → 1.1.1.1: icmp: echo reply
5.552292 port1 out 2.2.2.2 → 1.1.1.1: icmp: echo reply
```

补充1

如果组播不希望默认全通，而需要策略明确的策略控制，怎么操作?

1. 进入FortiGate的组播策略页面，删除组播策略的默认放通策略。



2. 配置明细的组播策略代替any到any全通的默认组播策略即可。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



补充2

如果不想配置组播策略，可以全局系统设置中bypass组播流量。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate_Transparent # config system settings
FortiGate_Transparent (settings) # set multicast-skip-policy
enable     Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.
disable    Require a multicast policy to allow multicast traffic to pass through the FortiGate.    //默认是disable
FortiGate_Transparent (settings) # set multicast-skip-policy enable
FortiGate_Transparent (settings) # end
```

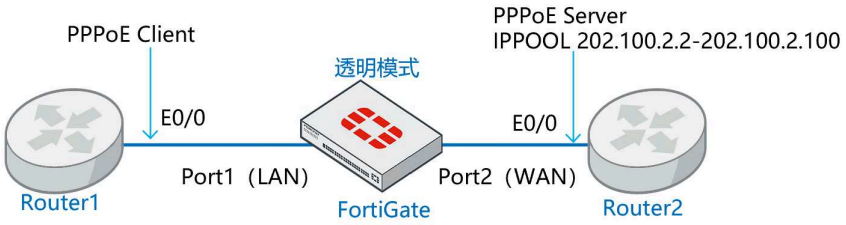

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

非IP流量(PPPOE)与透明模式

网络需求

路由器1和路由器2之间运行了PPPOE协议（非IP协议），防火墙以透明模式运行在两台路由器之间，需要确保路由器1的PPPOE拨号正常。

网络拓扑



R1和R2之间运行了PPPoE拨号
R2为PPPoE Server R1为PPPPoE Client

配置要点

- Router1/Router2路由器的基础配置
- 将防火墙配置为透明模式并开启网管
- 默认情况下，观察PPPOE拨号的情况
- 配置l2forward解决非IP流量转发问题

配置步骤与结果验证

1. Router1/Router2路由器的基础配置。

Router1 (PPPOE Client):

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Ethernet0/0
no ip address
no shutdown
pppoe enable group global
pppoe-client dial-pool-number 1
!
interface Dialer1
mtu 1492
ip address negotiated
encapsulation ppp
dialer pool 1
ppp pap sent-username pppoeuser1 password 0 fortinet
ppp ipcp route default
```

Router2 (PPPOE Server):

```
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!
username pppoeuser1 password 0 fortinet
!
bba-group pppoe bba1
virtual-template 1
!
interface Loopback1
ip address 202.100.2.1 255.255.255.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
!
interface Ethernet0/0
no ip address
no shutdown
pppoe enable group bba1
!
interface Virtual-Template1
description PPPOE bba1
mtu 1492
ip unnumbered Loopback1
peer default ip address pool pool1
ppp authentication pap
!
ip local pool pool1 202.100.2.2 202.100.2.100
```

2. 将防火墙配置为透明模式，进入设备命令行（CLI）中进行配置，修改FGT的运行模式为透明模式（默认为NAT路由模式）。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。配置可以管理防火墙的本地IP和网关。

```bash
config system global
    set hostname FortiGate_Transparent
end
config system settings
    set opmode transparent
    set manageip 192.168.1.100 255.255.255.0
    set gateway 192.168.1.99
end
```

3. MGMT口默认有管理权限，要通过port1（LAN）接口管理设备为例，开启port1（LAN）管理FGT的命令如下。允许网管协议从Port1接口通过https/http/SSH/Ping访问透明模式的FortiGate。

```bash
config system interface
    edit port1
    edit allowaccess https http ping ssh
end
```

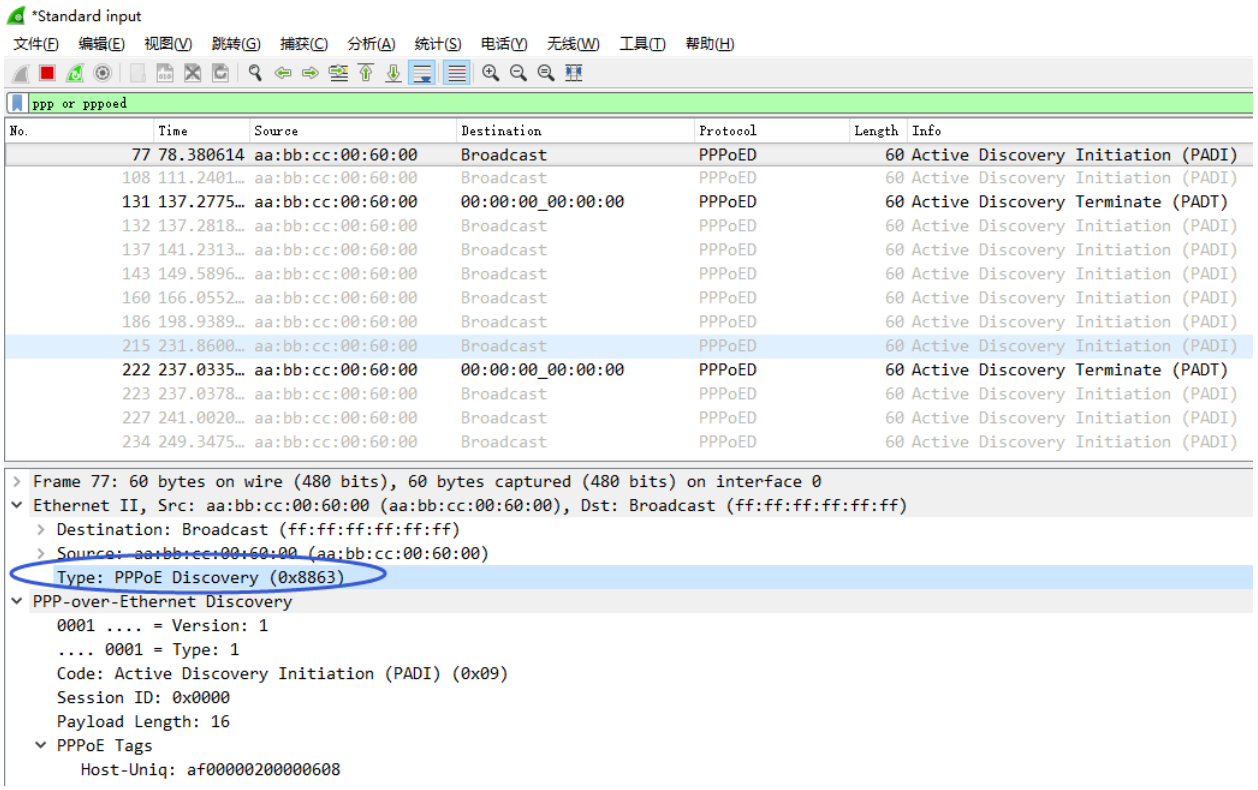
4. 默认情况下，观察PPPOE拨号的情况，Router1（PPPOE Client）无法PPPPOE拨号成功。

```
Router1#show ip route
 ...
      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
 ...
Router1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES manual up                    up
Ethernet0/1                unassigned      YES unset  administratively down down
Ethernet0/2                unassigned      YES unset  administratively down down
Ethernet0/3                unassigned      YES unset  administratively down down
Dialer1                    unassigned      YES IPCP   up                    up
Loopback0                  1.1.1.1         YES manual up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
```

5. 通过在FGT上抓包可以看到FGT并不转发PPPOE的报文，非IP的PPPOE数据默认不会被FGT所转发。

```
FortiGate_Transparent # diagnose sniffer packet any "pppoed" 4
interfaces=[any]
filters=[pppoed]
4.124126 port1 in pppoe printer hasn't been added to sniffer
37.014209 port1 in pppoe printer hasn't been added to sniffer
69.908430 port1 in pppoe printer hasn't been added to sniffer
102.798634 port1 in pppoe printer hasn't been added to sniffer
135.705063 port1 in pppoe printer hasn't been added to sniffer
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



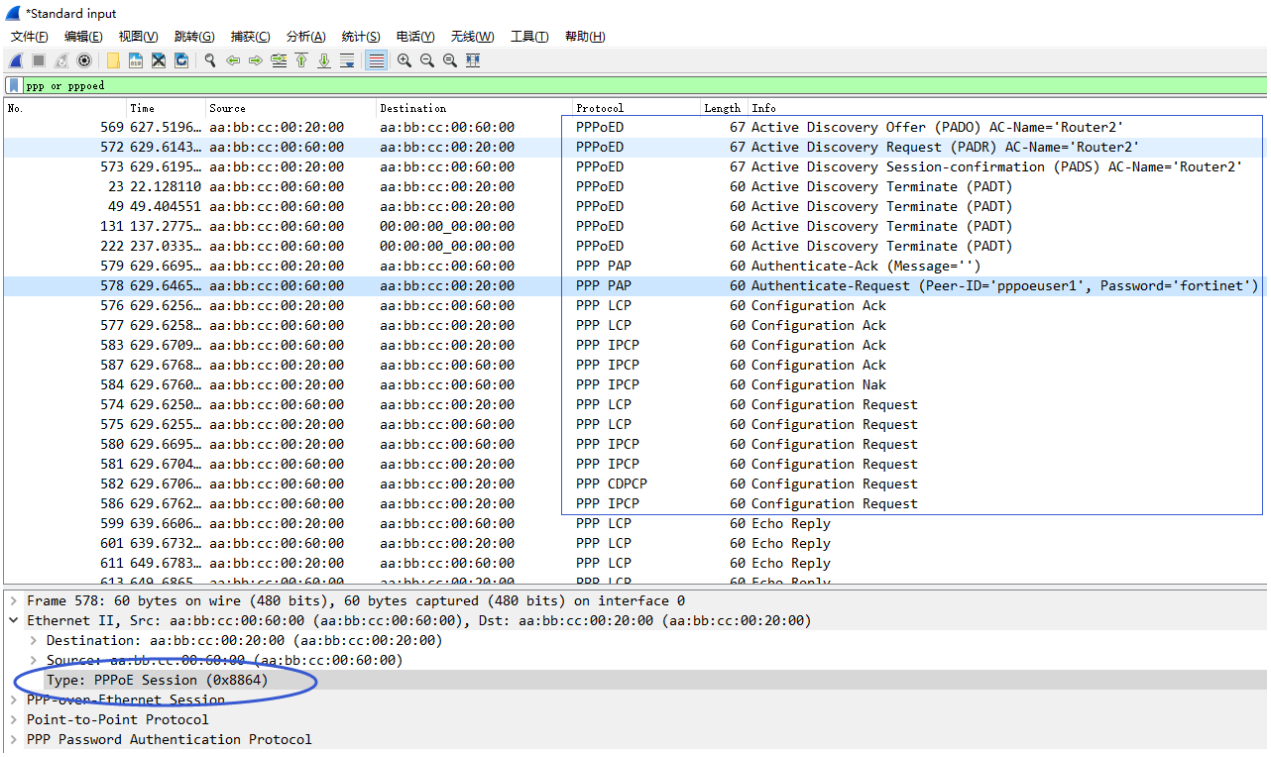
6. 解决非IP流量转发问题，在FGT的二层接口下配置set l2forward enable即可！

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit port1
FortiGate_Transparent (port1) # set l2forward enable

FortiGate_Transparent (port1) # next
FortiGate_Transparent (interface) # edit port2
FortiGate_Transparent (port2) # set l2forward enable
FortiGate_Transparent (port2) # end
```

7. 再次抓包查看，此时FGT可以转发PPPOE请求了。

```
FortiGate_Transparent # diagnose sniffer packet any "pppoed" 4
interfaces=[any]
filters=[pppoed]
5.324865 port1 in pppoe printer hasn't been added to sniffer
5.324880 port2 out pppoe printer hasn't been added to sniffer
5.325468 port2 in pppoe printer hasn't been added to sniffer
5.325474 port1 out pppoe printer hasn't been added to sniffer
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 查看Router1的Router1 PPPOE拨号情况，可以看到拨号成功了。

```
Router1#show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ ------------------- -------- --------------- ------------------
Vi2          LCP+ IPCP+ CDPCP-     LocalT   202.100.2.1

Router1#show pppoe session
     1 client session
Uniq ID  PPPoE  RemMAC          Port                   VT  VA         State
           SID  LocMAC                                    VA-st      Type
    N/A      2  aabb.cc00.2000  Et0/0                  Di1 Vi2        UP
                aabb.cc00.6000                             UP

Router1#show  ip route
 ...
Gateway of last resort is 202.100.2.1 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 202.100.2.1
 ...
C        202.100.2.1 is directly connected, Dialer1
C        202.100.2.3 is directly connected, Dialer1

Router1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
 ...
Dialer1                    202.100.2.3     YES IPCP   up                    up
 ...
```

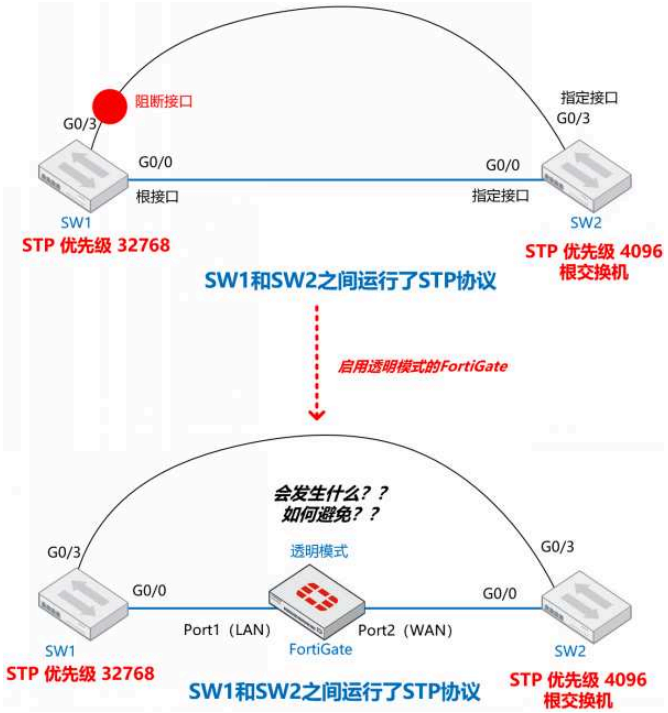

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

生成树(STP)与透明模式

网络需求

SW1和SW2之间运行了STP协议，防火墙以透明模式运行在两台SW之间，SW和SW之间原本存在环路，通过STP进行隔离阻断了环路接口，在加入透明模式的FGT之后，需要继续确保STP工作正常。

网络拓扑



配置要点

- SW1/SW2交换机的基础配置
- 将防火墙配置为透明模式并开启网管
- 默认情况下，观察STP报文的情况
- 配置l2forward解决STP流量转发问题

配置步骤与结果验证

1. SW1/SW2交换机的基础配置。

SW1：

```
hostname SW1
spanning-tree vlan 1 priority 32768
```

SW2：

```
hostname SW2
!
spanning-tree vlan 1 priority 4096
```

2. 查看没有加入透明模式的FortiGate之前STP状态，STP选举和接口状态正常。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SW1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             Cost        4
             Port        1 (GigabitEthernet0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5000.0007.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    Shr
Gi0/3               Altn BLK 4         128.4    Shr     //G0/3被阻断，STP工作正常

SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     5000.0008.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Desg FWD 4         128.4    Shr
```

3. 将防火墙配置为透明模式，进入设备命令行（CLI）中进行配置，修改FGT的运行模式为透明模式（默认为NAT路由模式）。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。配置可以管理防火墙的本地IP和网关。

```bash
config system global
    set hostname FortiGate_Transparent
end
config system settings
    set opmode transparent
    set manageip 192.168.1.100 255.255.255.0
    set gateway 192.168.1.99
end
```

4. MGMT口默认有管理权限，要通过port1（LAN）接口管理设备为例，开启port1（LAN）管理FGT的命令如下。允许网管协议从Port1接口通过https/http/SSH/Ping访问透明模式的FortiGate。

```bash
config system interface
    edit port1
    edit allowaccess https http ping ssh
end
```

5. 加入FGT在没有任何配置的情况下，观察STP的运行情况，一旦FGT加入到SW1和SW2之间，很明显网络中出现了环路，设备操作很卡顿，SW1和SW2基本上不再响应请求，三台设备均出现了异常情况（默认情况下透明模式的FGT只转发ARP报文，因此只需要一个ARP报文就会产生广播风暴，引起环路导致设备、业务中断）。

```
FortiGate_Transparent # diagnose sniffer packet any "" 4
interfaces=[any]
filters=[none]
0.814720 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.814733 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.817141 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.817148 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.818761 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.818771 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.819709 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
0.819720 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.821533 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.821544 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.825484 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.825492 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.827856 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.827866 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.828752 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.828762 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.829235 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.829244 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.831930 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.831947 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.834842 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.834853 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.836686 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.836694 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
0.838965 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.838972 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.841965 port1 in arp who-has 192.168.1.99 tell 192.168.1.100
0.841974 port2 out arp who-has 192.168.1.99 tell 192.168.1.100
0.843858 port2 in arp who-has 192.168.1.99 tell 192.168.1.100
0.843866 port1 out arp who-has 192.168.1.99 tell 192.168.1.100
```

6. 查看SW1/SW2的 STP状态均异常，所有接口都处于转发状态。

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             Cost        4
             Port        4 (GigabitEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5000.0007.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Root FWD 4         128.4    Shr     //SW1的两个接口都处于转发状态

SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     5000.0008.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Desg FWD 4         128.4    Shr  //SW2的两个接口都处于转发状态
```

7. 在FGT上抓包可以看到STP的BPDU报文没有被转发，而是被默认丢弃，这是引起环路的根本原因。STP BPDU数据默认不会被透明模式的FGT所转发，因此STP计算不正确，会计算不出网络中的环路，从而引起广播风暴。

```
FortiGate_Transparent # diagnose sniffer packet any "none" 4
interfaces=[any]
filters=[none]
1.234590 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
2.182694 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
3.247650 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
4.193908 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
5.260154 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
6.204003 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
7.278226 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
8.210732 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
9.294582 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
10.223021 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
11.302829 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
12.232585 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
13.310023 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
14.242616 port1 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 8001.50:00:00:07:00:00.8001
```

8. 那么要如何解决此情况呢？在FGT的二层接口下配置set stpforward enable即可！

> **重要**
>
> 要特别注意此情况！避免透明模式的FortiGate一上线引起STP计算异常，引起广播风暴，造成重大业务故障。

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit port1
FortiGate_Transparent (port1) # set stpforward enable

FortiGate_Transparent (port1) # next
FortiGate_Transparent (interface) # edit port2
FortiGate_Transparent (port2) # set stpforward enable
FortiGate_Transparent (port2) # end
```

9. 再次抓包查看，此时FGT可以转发STP BPDU报文了。

```
FortiGate_Transparent # diagnose sniffer packet any "stp" 4
interfaces=[any]
filters=[stp]
2.070782 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
2.070797 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
4.085338 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
4.085355 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
6.097429 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
6.097444 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
8.107806 port2 in stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
8.107822 port1 out stp 802.1w, rapid stp, flags [learn, forward], bridge-id 1001.50:00:00:08:00:00.8001
```

.0. 此时再次查看STP的状态。

```
SW1#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             Cost        4
             Port        1 (GigabitEthernet0/0)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     5000.0007.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Root FWD 4         128.1    Shr
Gi0/3               Altn BLK 4         128.4    Shr    //G0/3 被阻断，STP工作正常

SW2#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    4097
             Address     5000.0008.0000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4097   (priority 4096 sys-id-ext 1)
             Address     5000.0008.0000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
              Aging Time  300 sec
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/0               Desg FWD 4         128.1    Shr
Gi0/3               Desg FWD 4         128.4    Shr
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

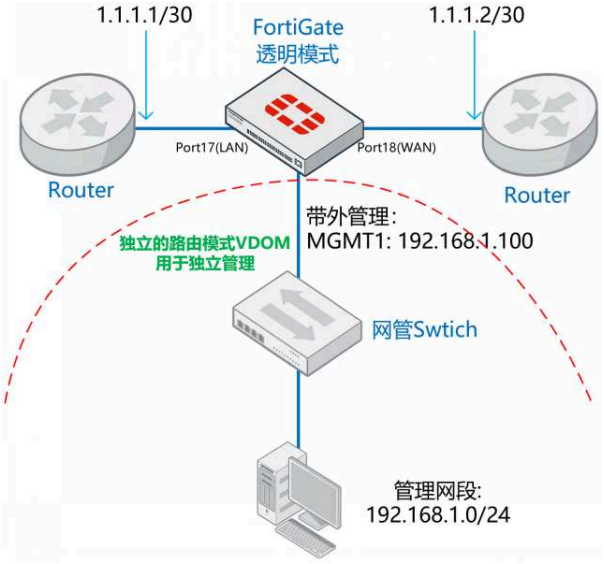
透明模式的带外管理

网络需求

透明模式部署下的防火墙，需实现带外管理：

- 防火墙上须配置一个与管理网段相同的IP地址进行管理
- 添加的管理IP产生的本地路由，不会对正常业务数据传输造成异步路由等冲突

网络拓扑



配置要点

- 将防火墙配置为透明模式
- 配置VDOM
- 将MGMT1加入到独立管理的VDOM中

配置步骤

1. 将防火墙配置为透明模式，进入设备命令行（CLI）中进行配置，修改FGT的运行模式为透明模式（默认为NAT路由模式）。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置。配置可以管理防火墙的本地IP和网关。

```bash
config system global
    set hostname FortiGate_Transparent
end
config system settings
    set opmode transparent
    set manageip 1.1.1.3 255.255.255.0
    set gateway 1.1.1.2
end
```

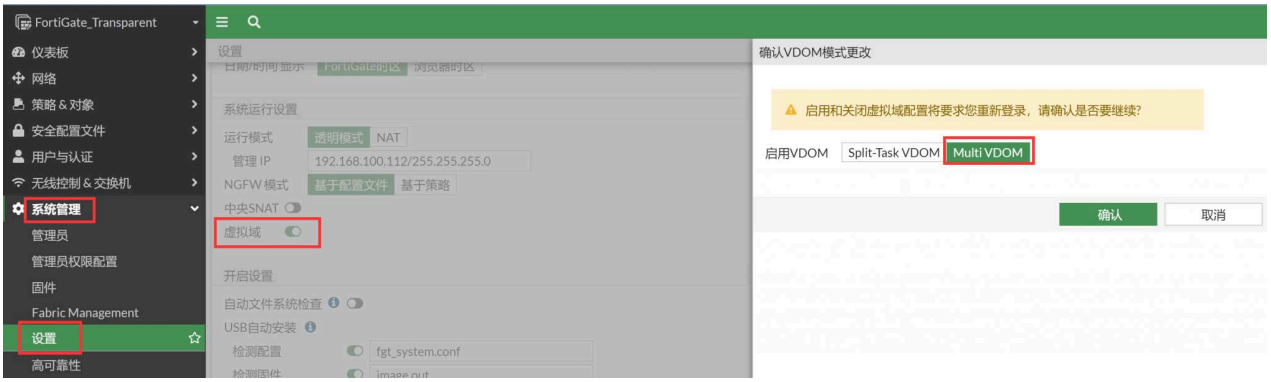
2. MGMT口默认有管理权限，要通过port17（LAN）接口管理设备为例，开启port17（LAN）管理FGT的命令如下。允许网管协议从Port1接口通过https/http/SSH/Ping访问透明模式的FortiGate。

```bash
config system interface
    edit port17
    edit allowaccess https http ping ssh
end
```

3. 当前的配置只能通过1.1.1.3去管理FGT，如果需要独立管理FortiGate需要开启VDOM功能，并且划分独立的网段和路由给到FGT进行网管。

4. 在GUI或命令行下开启VDOM功能，开启后当前管理员会退出登陆。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

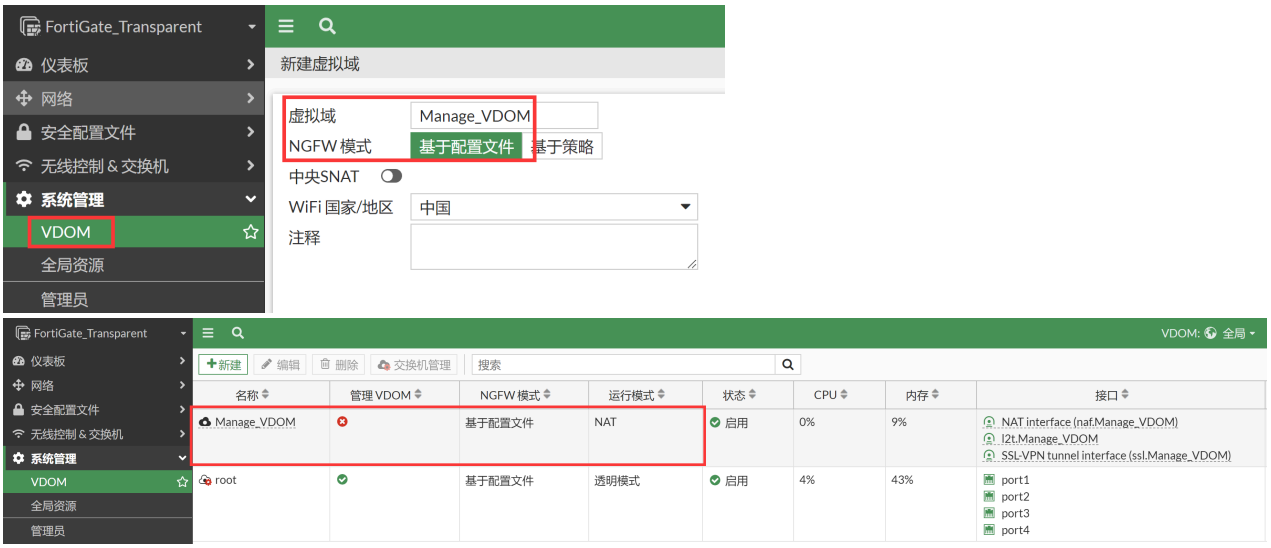



```bash
FortiGate_Transparent # config system global
FortiGate_Transparent (global) # set vdom-mode multi-vdom
FortiGate_Transparent (global) # end
You will be logged out for the operation to take effect.
Do you want to continue? (y/n)y
exit
FortiGate_Transparent login:
```

5. 开启VDOM之后WEB页面系统管理下出现VDOM的配置模块。

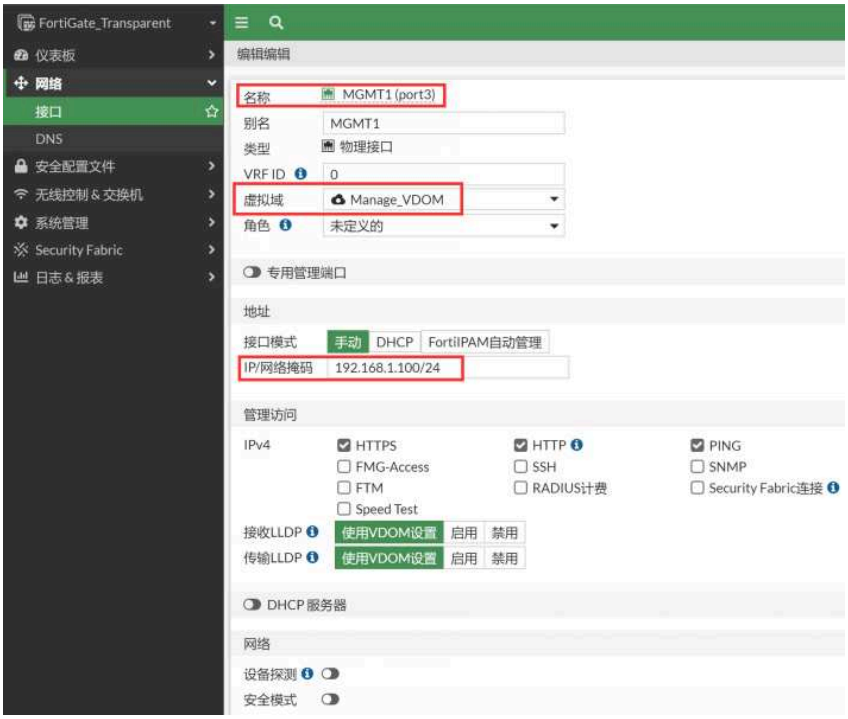


6. 新建一个MGMT的VDOM，默认的root已经是透明模式的状态了。



7. 编辑MGMT1接口，将FortiGate用于独立管理的接口加入Manage_VDOM，并配置独立管理IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 进入Mange_VDOM，为MGMT1配置默认路由。



9. 注意：如果需要服务更新、syslog、SNMP网管等等都需要从MGMT1发出，需要将管理VDOM切换到Mange_VDOM。

```bash
config global
    config system global
        set management-vdom Mange_VDOM
    end
end
```



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

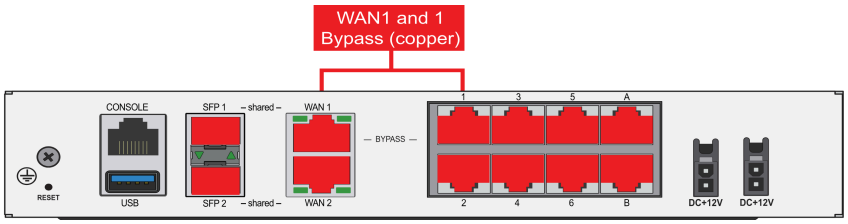
1. 当不需要带外管理端口，对处于透明模式的防火墙直接进行管理时（如此例中的port17口或port18口），需注意：
   - manage IP是整个防火墙本身的IP地址，不针对某个接口，根据配置此处FGT本机管理IP为1.1.1.3。
   - 需通过某个接口对桥模式防火墙进行管理时，需开启相应接口下的如ping，https，ssh等管理功能，如此例中，当要通过port17或者port18来对防火墙进行管理时，需开启port17和port18接口下的ping、https、ssh等管理服务。
2. 而独立管理的VDOM，则是完全由另外一个VDOM（Mange_VDOM）来充当管理功能的防火墙，而原本的root只用来转发业务数据，将管理和业务分离出来。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Bypass部署

模式说明

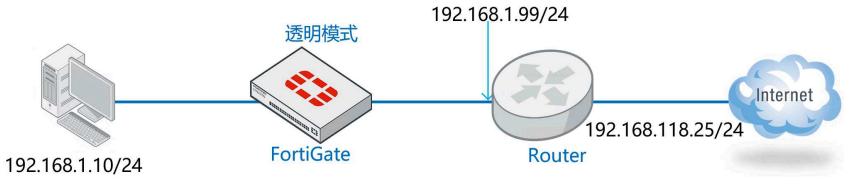
FortiGate部分型号支持Bypass接口，即设备断电后或者重启，依然能够通讯（只能在透明模式下工作）。如下举例设备（80F Bypass），WAN1和internal1接口形成一个Bypass Pair（接口internal1是名为internal的硬件交换接口的一部分。要启用Bypass模式，必须从internal接口中删除internal1）。



重要

目前支持Bypass的FortiGate型号包含：FortiGate 2500E、FortiGate 400E Bypass、FortiGate 800D、FortiGate 80F Bypass、FortiGateRugged 60F 3G4G、FortiGateRugged 60F、FortiGateRugged 70F 3G4G、FortiGateRugged 70F等。具体可参考：
https://docs.fortinet.com/document/fortigate/7.0.99/cli-reference/530620/config-system-bypass ↗

网络拓扑



防火墙工作在透明模式下，开启防病毒功能。使用bypass口，当防火墙故障后，确保链路工作正常。

配置要点

- 将防火墙配置为透明模式
- 配置防火墙策略
- 开启Bypass模式

配置步骤

1. 将防火墙配置为透明模式，进入设备命令行（CLI）中进行配置，修改FGT的运行模式为透明模式（默认为NAT路由模式）。注意切换透明模式防火墙需要防火墙没有相关接口、策略、路由等配置，配置可以管理防火墙的本地IP和网关。

```bash
config system global
    set hostname FortiGate_Transparent
end
config system settings
    set opmode transparent
    set manageip 1.1.1.3 255.255.255.0
    set gateway 1.1.1.2
end
```

2. MGMT口默认有管理权限，要通过port17（LAN）接口管理设备为例，开启port17（LAN）管理FGT的命令如下。

```bash
config system interface
    edit port17
    edit allowaccess https http ping ssh
end
```

3. 配置防火墙策略，保证流量可以正常通过FortiGate。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 开Bypass模式。

```
config system bypass
    set bypass-watchdog enable
    set poweroff-bypass enable
end
```

结果验证

将系统断电或重启设备，客户业务不中断。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

透明模式注意事项与排错

注意事项

1. 默认情况下全新FortiGate不转发BPDU报文，这样可能会导致STP问题从而引起网络出现二层环路，可以登陆到全新FortiGate命令行下，进入到接口编辑下面，执行命令启用BPDU转发：set stpforward enable。

```
 FGT # config system interface
 FGT (interface) #edit port1
 FGT (port1) #set stpforwad enable        #默认为关闭
 FGT (port1) #next
 然后依次进入各接口启用stpforward功能
```

2. 可以使用forward domain来控制指定的接口间数据转发，具有相同的forward domain号不同的接口间数据包可转发。

```
FGT # config system interface
FGT (interface) # edit wan1
FGT (wan1) # set forward-domain 10
FGT (wan1) # next
FGT (interface) # edit wan2
FGT (wan2) # set forward-domain 10
FGT (wan2) # end
```

> **重要**
>
> forward-domain无需提前定义，直接配置生效；forward-domain如同转发域的概念，广播包只会在同个转发域进行广播。

3. 只有Ethernet II类型帧可以被转发，在默认的配置下，所有的其他类型的二层协议都不能被转发。需要转发这些帧请在接口下面启用l2forward功能。

```
FGT # config system interface
FGT (interface) #edit port1
FGT (port1) #set l2forward enable       #默认为关闭
FGT (port1) #next
然后依次登陆各接口启用l2forward功能
```

4. 多播包默认情况下是转发的，所以如果部署透明模式的防火墙接入到多播环境中如果不通，要注意下面的两个参数值，默认是转发的状态。

```
FGT # config system settings
FGT (settings)set multicast-skip-policy disable   #默认为关闭
FGT (settings)end

另外多播策略存在一条默认的any到any的全通策略：
config firewall multicast-policy
    edit 1
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

5. 缺省情况下广播是不受策略控制的，除了ARP广播是允许的，其他的广播流量全部是被禁止转发的，看默认配置如下，如需开启广播转发需要在接口开启broadcast-forward。

```
config system interface
    edit "port1"
        set allowaccess ping https ssh http fgfm
        set broadcast-forward enable   //默认为关闭
    next
end
然后依次进入各接口启用broadcast-forward功能
```

6. 如果明确需要带外管理功能的话，请设置多VDOM，其中VDOM root仅用来管理其他相关的透明VDOM使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate_Transparent # config system global
FortiGate_Transparent (global) # set vdom-mode
no-vdom       Disable split/multiple VDOMs mode.
split-vdom    Enable split VDOMs mode.
multi-vdom    Enable multiple VDOMs mode.
FortiGate_Transparent (global) # set vdom-mode multi-vdom    //开启多VDOM模式
FortiGate_Transparent (global) # end
You will be logged out for the operation to take effect.
Do you want to continue? (y/n)y
exit
FortiGate_Transparent login: admin
Password:
Welcome !
```

7. 如果部署透明模式的全新FortiGate到路由器和主机直连的时候，请注意在这段线路中是否会出现相同的源目的IP地址数据流在防火墙不同方向上时的MAC地址不一致的情况，简单的应用如VRRP之类的主机路由备份协议，这种流量的数据流源目MAC，正向和反向是不一样的，这种情况下请尽量在防火墙上面设置静态IP/MAC以告诉全新FortiGate指定的虚拟MAC地址属于某个VRRP组。

> **重要**
>
> 一个forward_domain里面只能指定一个相同MAC地址对。

8. 透明模式下查查看MAC表，使用diag netlink brctl name host VDOM_name.b查看，以下以root的vdom为例：

```
FGT# diag netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table
port no device devname mac addr ttl attributes
2 7 wan2 02:09:0f:78:69:00 0 Local Static
5 6 trunk_1 02:09:0f:78:69:01 0 Local Static
3 8 dmz 02:09:0f:78:69:01 0 Local Static
4 9 internal 02:09:0f:78:69:02 0 Local Static
3 8 dmz 00:80:c8:39:87:5a 194
4 9 internal 02:09:0f:78:67:68 8
1 3 wan1 00:09:0f:78:69:fe 0 Local Static
```

9. 透明模式的功能限制：

   - 只支持策略模式的IPSec，支持用户认证。
   - 不支持接口模式IPSec，不支持SSL VPN，不支持动态路由和策略路由、不支持DHCP。

总结

透明模式的FortiGate其实默认只转发ARP广播和组播报文（默认存在一条全通的组播策略，如果删除了这条默认的组播全通策略，仍然会放通IPv6 ND的组播流量，而丢弃其他的组播流量），其他的流量通通会被丢弃。如果你想让防火墙更像一个SW一样的存在，那么在使用的二层接口下应该这样去修改。

```
config system interface
    edit "port1"
        set broadcast-forward enable    //开启广播转发
        set l2forward enable            //开启非IP流量转发
        set stpforward enable           //开启STP转发
    next
    edit "port2"
        set broadcast-forward enable
        set l2forward enable
        set stpforward enable
    next
end
```

这样FortiGate对接入的网络环境影响应该来说是更小的，对于那种不是很清楚网络中有一些什么流量的环境，建议按照上述建议进行配置优化，让FortiGate更加接近于一个SW的存在。

> **重要**
>
> 接口下的vlanforward保持为默认的disable，不要去动，不要去动，可能会引起环路！

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

最佳实践

1. 不要将透明模式的两个物理接口连接到同一个VLAN或同一个SW/HUB(相同广播域)，SW一旦检测到相同的MAC地址出现在不同的接口，大部分的二层交换机会出现MAC地址表翻转，会让网络非常的不稳定或环路。

2. 如果网络中存在VLAN，需要在FGT上创建了多个VLAN，要确保给每一个VLAN-ID分配一个独立的Forwarding Domain ID确保广播在VLAN之间被隔离（透明模式下VLAN之间不隔离广播，Fortiward-Domain才隔离广播）。

```
FortiGate_Transparent # config system interface
FortiGate_Transparent (interface) # edit Inside_VLAN10
FortiGate_Transparent (Inside_VLAN10) # set forward-domain 10
FortiGate_Transparent (Inside_VLAN10) # next
```

3. 在所有接口上开启 stpforward enable（开启二层转发的一些特性，防止误丢一些二层数据帧）。

```
config system interface
    edit "portX"
        set broadcast-forward enable
        set l2forward enable
        set stpforward enable
    next
end
```

4. 使用一个独立的透明模式的VDOM用来保护二层的业务流量，然后再使用一个独立管理VDOM（NAT路由模式）用于设备的管理和fortiguard升级等，利用VDOM功能将管理（NAT路由模式）和业务（透明模式）分离。

5. 仅将用于生产的业务接口置于透明模式VDOM中。将所有其他接口置于NAT路由模式VDOM中，这可以防止潜在的第2层环路。

故障排错

1. 先检查FortiGate的二层MAC地址表。注意，在透明模式下，FortiGate是根据二层转发数据库进行转发二层数据，该数据库只能在Global通过命令”diag netlink brctl name host root.b”进行导出，ARP表只能在有IP访问FortiGate的情况下出现。外部设备发送的ARP/GARP会映射到二层转发表，并且当MAC地址变更的时候会在会话同步更改目标MAC地址。下面的命令能导出每一个VDOM桥实例的二层转发表，在转发表里可以单独看到VLAN/VDOM里的MAC地址。

```
diag netlink brctl list
diag netlink brctl name host <VDOM_name>.b

trans VDOM查看二层转发表的例子：
diag netlink brctl name host trans.b

输出如下：
diagnose netlink brctl name host trans.b
show bridge control interface trans.b host.
fdb: size=2048, used=4, num=8, depth=3
Bridge trans.b host table
port no device  devname mac addr                ttl     attributes
  7     21      port3vlan200    00:50:79:66:68:01       0        Static
  1     3        port1   52:c9:fd:91:54:00       0       Local Static
  6     20      port2vlan200    52:c9:fd:91:54:01       0       Local Static
  3     17      port2vlan100    52:c9:fd:91:54:01       0       Local Static
  2     4        port2   52:c9:fd:91:54:01       0       Local Static
  8     5        port3   52:c9:fd:91:54:02       0       Local Static
  7     21      port3vlan200    52:c9:fd:91:54:02       0       Local Static
  5     19      port3vlan100    52:c9:fd:91:54:02       0       Local Static
```

2. 使用sniffer验证数据包是否到达防火墙，通过以下命令使用sniffer抓取相应信息。同时通过使用ping在FortiGate两端进行测试可以初步分析问题。这个能看到在FortiGate上面流入以及流出的数据包。

```
进行抓取目的地址是114.114.119.119的数据：
diagnose sniffer packet any "host 114.114.119.119" 4 0 l    //按CTRL+C进行停止

基于端口进行数所包抓取
diagnose sniffer packet portA  "host 114.114.119.119" 4 0  l
diagnose sniffer packet portB  "host 114.114.119.119" 4 0  l
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
如有需要，可以通过每个vlan进行获取更明细内容
diagnose sniffer packet <each_vlan_interface> "" 6 0 l

参数4和6的区别（用于显示输出抓取数据参数）:
1: print header of packets (只有IP头部)
2: print header and data from ip of packets (有ip头部和数据内容)
3: print header and data from ethernet of packets  (if available)
4: print header of packets with interface name (只有IP头部和端口)
5: print header and data from ip of packets with interface name (有ip头部和数据内容以及端口)
6: print header and data from ethernet of packets (if available) with intf name

参数0的用处：输出个数

参数l的用处(用于输出时候显示的时间格式):
a: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms
l: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms
```

3. 使用debug flow验证数据包是否穿越防火墙（vlanforward无效）。在每一个VDOM使用"debug flow"命令进行跟踪流量，通过使用ping在FortiGate两端进行测试可以初步分析问题，这种排障的方法能够查看到流量是否因为某条策略导致数据包不通或者通过设备。

```
以源地址为抓取条件
═══════════════════════════════════════════════════════════
diag debug flow filter add <IP_address_of_source_device>
diag debug flow show function-name enable
diag debug flow show console enable
diag debug flow show iprope enable
diag debug flow trace start 100
diag debug enable
═══════════════════════════════════════════════════════════
如需要停止，可以敲"diag debug flow trace stop"

以目标地址为抓取条件
═══════════════════════════════════════════════════════════
diag debug flow filter add <IP_address_of_destination_device>
diag debug flow show function-name enable
diag debug flow show console enable
diag debug flow show iprope enable
diag debug flow trace start 100
diag debug enable
═══════════════════════════════════════════════════════════
如需要停止，可以敲"diag debug flow trace stop"

当有触发排障的流，输出如下:
id=20085 trace_id=113 msg="vd-tp_mode received a packet(proto=6,10.160.0.160:4370→10.160.0.152:23) from
internal."
id=20085 trace_id=113 msg="Find an existing session, id-00000a40, original direction"
id=20085 trace_id=113 msg="enter fast path"
id=20085 trace_id=113 msg="send out via dev-dmz1, dst-mac-00:01:02:03:04:05"
```

4. 查看数据包在防火墙上创建的session。在每一个VDOM使用"diag sys session"命令进行防火墙会话检查，通过使用ping在FortiGate两端进行测试可以初步分析问题，这种排障的方法能够查看防火墙是否会为流量创建会话，以及是否硬件加速以及命中哪一条策略。

```
以源地址为抓取条件（单播）
═══════════════════════════════════════════════════════════
diag sys session filter src <IP_address_of_source_device>
diag sys session list
═══════════════════════════════════════════════════════════
当有触发排障的会话,输出如下:
session info: proto=1 proto_state=00 duration=2 expire=58 timeout=0 flags=00000000 sockflag=00000000 sockport=0
av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty br
statistic(bytes/packets/allow_err): org=500/5/1 reply=500/5/1 tuples=2
tx speed(Bps/kbps): 248/1 rx speed(Bps/kbps): 248/1
orgin→sink: org pre→post, reply pre→post dev=9→10/10→9 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.1.1:64→192.168.2.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.1:64→192.168.1.1:0(0.0.0.0:0)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=1
serial=00000512 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
vlanid=100 dd_type=0 dd_mode=0
total session 1

以源地址为抓取条件（多播）
═══════════════════════════════════════════════════════
diagnose sys mcast-session list
═══════════════════════════════════════════════════════
当有触发排障的会话,输出如下:
session info: id=123 vf=1 proto=112 192.168.1.2.0→224.0.0.18.0
used=2 path=1 duration=1353 expire=179 indev=10 pkts=1360 bytes=54400
state=00000002:tp
path: policy=0, outdev=9

session info: id=124 vf=1 proto=112 192.168.2.99.0→224.0.0.18.0
used=2 path=1 duration=1353 expire=179 indev=10 pkts=1360 bytes=54400
state=00000002:tp
path: policy=0, outdev=9
Total 2 sessions
```

参考文档

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Troubleshoot-and-verify-if-traffic-is-hitting-a/ta-p/197261 ↗

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-First-steps-to-troubleshoot-connectivity/ta-p/192560 ↗

https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-session-table-information/ta-p/196988 ↗

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-a-FortiGate-in-Transparent-mode-to/ta-p/197611 ↗

https://community.fortinet.com/t5/FortiGate/Technical-Note-FortiGate-and-Gratuitous-ARP-GARP/ta-p/192962 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

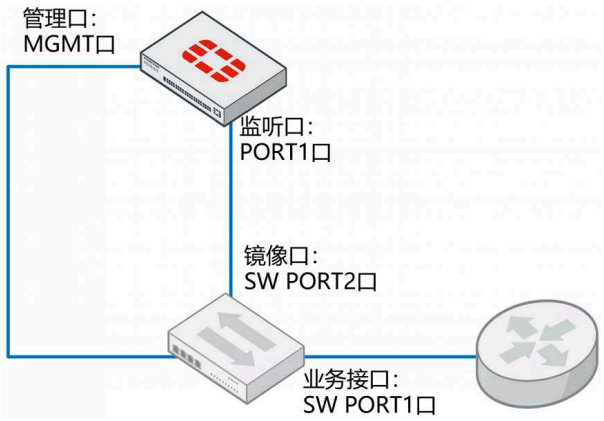
旁路模式典型案例

网络需求

有时客户为了保证重要业务连续不中断，且避免引入新的单点故障点：

- 需采用旁路部署的方式部署防火墙
- 启用防火墙的UTM功能，对防病毒、IPS等安全事件进行检测及记录

网络拓扑



配置要点

- 交换机配置（根据实际情况进行配置，建议由客户方维护人员进行配置）：配置sw G1/0为镜像口，将sw1口上下行流量镜像到sw2口
- 防火墙配置：
  - 配置接口，开启port1的sniffer模式，让port1口可以对收到的数据包进行分析
  - 编辑IPS、防病毒 规则参数（本文中均以default规则为例）
  - 配置防火墙策略，将IPS、防病毒等规则应用于port1口
  - 开启IPS、防病毒等日志

配置步骤

1. 接口启用sniffer模式。

```
FGT #config system interface
FGT (interface) #edit port1
FGT (port1) #set ips-sniffer-mode enable
FGT (port1) #end
```

2. 根据实际情况，编辑相应的UTM规则参数，例如IPS（如default规则）、防病毒（default规则）以及UTM功能日志记录等，具体参数设置，详见UTM安全应用章节。

3. 配置防火墙sniffer策略，将UTM安全策略加载与port1口。

```
FGT # config firewall sniffer
FGT (sniffer) # edit 1
FGT (1) # set logtraffic utm                          //记录UTM日志
FGT (1) set interface "port1"                         //指定port1接口
FGT (1) set application-list-status enable            //开启应用控制监控
FGT (1) set application-list "default"                //根据应用控制规则"default"进行记录
FGT (1) set ips-sensor-status enable                  //开启IPS监控
FGT (1) set ips-sensor "default"                      //根据IPS规则"default"进行记录
FGT (1) set av-profile-status enable                  //开启防病毒监控
FGT (1) set av-profile "AV-flow"                      //根据防病毒规则"AV-flow"进行记录
FGT (1) set webfilter-profile-status enable           //开启web过滤监控
FGT (1) set webfilter-profile "flow-monitor-all "     //根据web过滤规则"default"进行记录
FGT (1) end
```

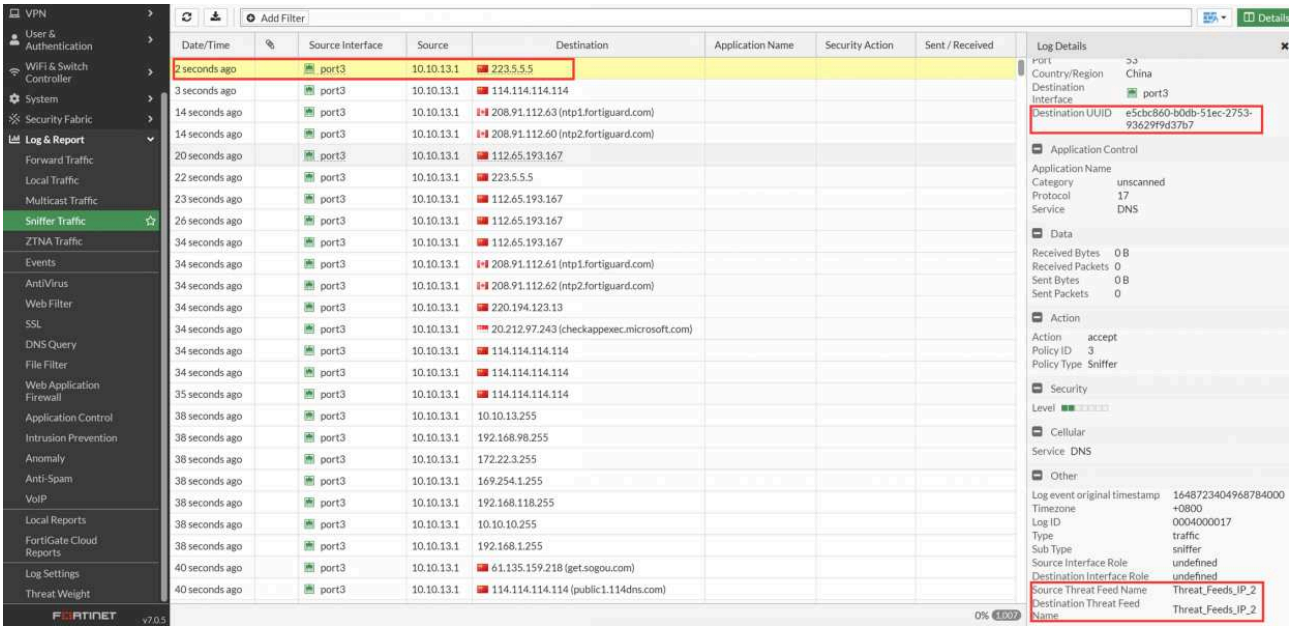

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 查看配置。

```
FGT # config firewall sniffer
FGT (sniffer) # get
== [ 1 ]
FGT (sniffer) # edit 1
FGT (1) # get
id                  : 1
status              : enable
logtraffic          : utm
ipv6                : disable
non-ip              : disable
interface           : port1
host                :
port                :
protocol            :
vlan                :
application-list-status: enable
application-list    : default
ips-sensor-status   : enable
ips-sensor          : default
av-profile-status   : enable
av-profile          : default
webfilter-profile-status: enable
webfilter-profile   : flow-monitor-all
spamfilter-profile-status: disable
dlp-sensor-status   : disable
ips-dos-status      : disable
max-packet-count    : 4000
```

结果验证

进入日志&报表→嗅探流量，进行查看。

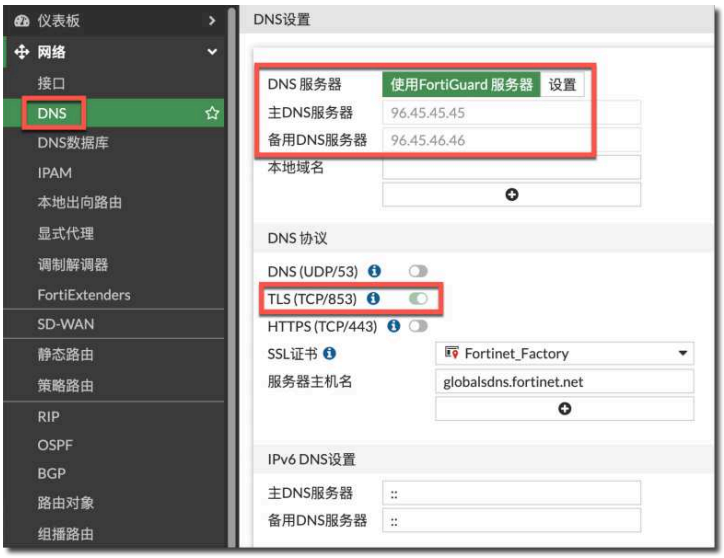


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DNS配置

功能介绍

FortiGate在需要将域名解析为IP地址（如被域名定义的NTP服务器、FortiGuard更新服务器、FQDN地址对象、FortiGate作为DNS服务器、SD-WAN SLA使用域名作为探测服务器等场景）时会查询已配置的DNS服务器。默认配置下，FortiGate使用FortiGuard的DoT（DNS over TLS）作为自身的IPv4 DNS服务器。



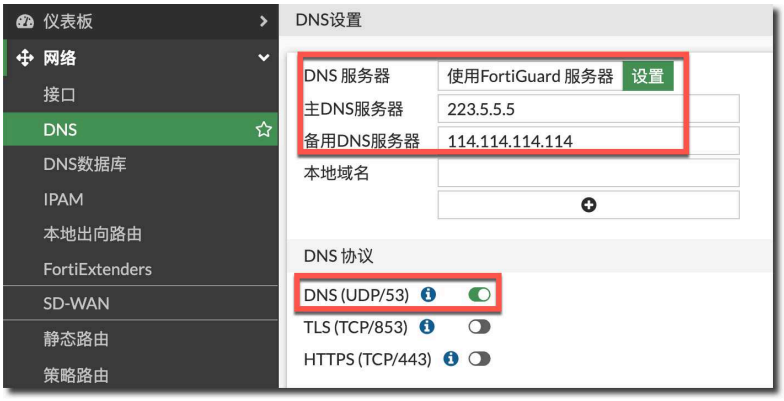

```bash
config system dns
    set primary 96.45.45.45
    set secondary 96.45.46.46
    set protocol dot
    set server-hostname "globalsdns.fortinet.net"
end
```

自定义DNS服务器

如果需要修改为自定义的DNS服务器，需要点击“设置”按钮，然后填入自定义的DNS服务器并选择DNS协议。

重要

在取消使用FortiGuard服务器后，DNS协议默认会选择“TLS(TCP/853)”，需要手动修改为自定义DNS服务器使用的DNS协议。




```bash
config system dns
    set primary 223.5.5.5
    set secondary 114.114.114.114
end
```

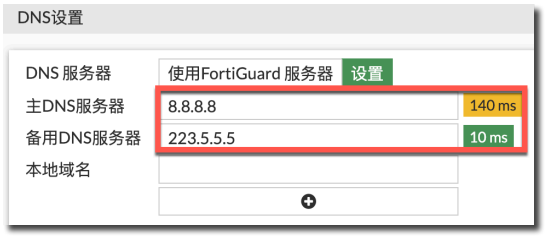

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DNS服务器主备模式

1. DNS服务器在主备的选择上有两种模式：
   - **least-rtt（默认配置）**：根据最后一次往返时间（RTT）最短的作为当前DNS服务器。
   - **failover**：根据服务器的配置顺序选择服务器，首先选择主DNS服务器进行解析，主DNS服务器无法访问或出现问题时裁切换到备用DNS服务器。
2. 该选项只能通过CLI进行更改。

```bash
config system dns
    set server-select-method {least-rtt | failover}
end
```

3. 通过 `diagnose test application dnsproxy 2` 命令可以看到两个服务器的延迟差距，如下所示，使用 `least-rtt` 模式时，FortiGate会选择223.5.5.5作为DNS服务器，使用 `failover` 模式时，FortiGate会选择8.8.8.8作为DNS服务器。




```bash
FortiGate # diagnose test application dnsproxy 2
......
DNS latency info:
vfid=0 server=8.8.8.8 latency=14 updated=126
vfid=0 server=223.5.5.5 latency=1 updated=41
......
```

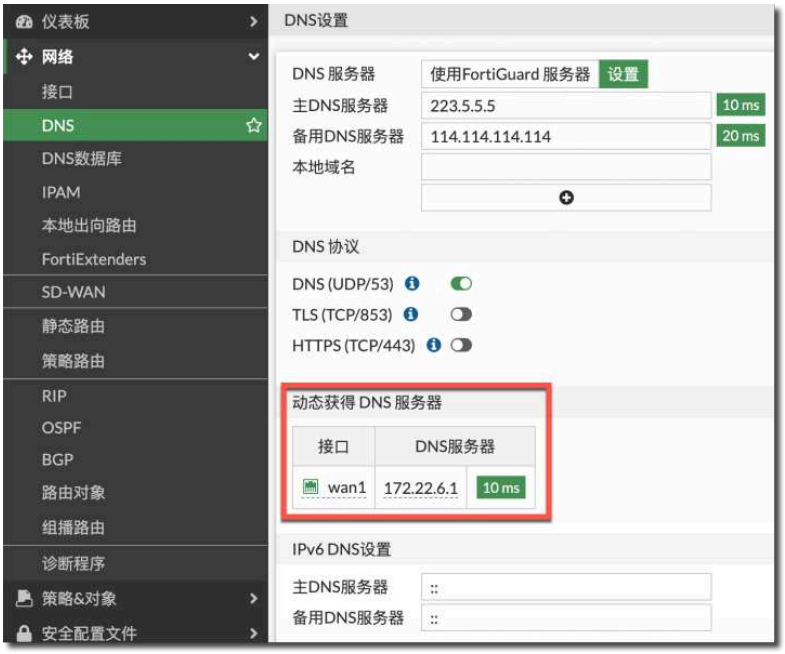
4. 当其中一个DNS服务器无法访问时，会使用另一个DNS服务器进行解析，`diagnose test application dnsproxy 3` 命令可以看到服务器的探测失败的次数（`failure`）以及距离上次探测失败过去的时间（`last_failed`）。

```bash
FortiGate # diagnose test application dnsproxy 3
......
DNS servers:
8.8.8.8:53 vrf=0 tz=0 encrypt=none req=4 to=4 res=0 rt=0 ready=1 timer=0 probe=0 failure=5 last_failed=1215
223.5.5.5:53 vrf=0 tz=0 encrypt=none req=5 to=0 res=5 rt=1 ready=1 timer=0 probe=0 failure=0 last_failed=0
......
```

DNS服务器覆盖

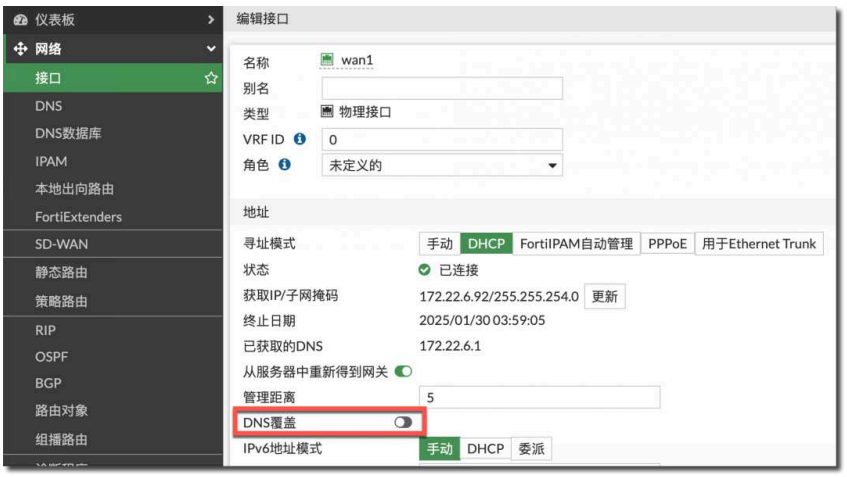
1. 要特别注意，如果配置了PPPoE或DHCP，并从ISP侧获取了IP地址与DNS服务器。默认配置下，从ISP获取的DNS服务器会覆盖手动配置的DNS服务器。如下所示，wan1接口DHCP获取的DNS服务器172.22.6.1覆盖了手工配置的223.5.5.5/114.114.114.114。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 如果需要手工配置的DNS服务器生效，需要在相关PPPoE/DHCP接口下关闭“DNS覆盖”功能。

> **重要**
>
> 如果使用的是将普通接口修改为PPPoE的模式，在接口上关闭“DNS覆盖”功能，会导致接口重新拨号，请务必在窗口期进行操作。
>
> 所以强烈建议新建PPPoE接口来作为拨号接口，而不要使用普通接口上的PPPoE模式（参考：部署前注意事项→PPPoE接口配置 ↗。




```bash
config system interface
    edit "wan1"
        set dns-server-override disable
    next
end
```

VDOM DNS

当 FortiGate 处于多VDOM模式时，DNS解析由管理VDOM（默认为root VDOM）处理。但在某些情况下，用户可能希望在非管理VDOM上配置自定义DNS设置。例如在多租户情况下，每个VDOM可能被不同的租户占用，每个租户可能需要自己的DNS服务器。

```bash
config vdom
    edit <vdom>
        config system vdom-dns
            set vdom-dns enable
            set primary <primary_DNS>
            set secondary <secondary_DNS>
            set protocol {cleartext dot doh}
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set ip6-primary <primary_IPv6_DNS>
            set ip6-secondary <secondary_IPv6_DNS>
            set source-ip <IP_address>
            set interface-select-method {auto | sdwan | specify}
        end
    next
end
```

DNS CLI配置

interface-select-method

当有多个线路可以访问DNS服务器时，可以配置DNS请求的选路方式（默认为`auto`），选择`specify`模式时，可以选择具体的接口。

```bash
config system dns
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
end
```

source-ip

设置DNS请求报文使用的源IP地址。

```bash
config system dns
    set source-ip <class_ip>
end
```

dns-cache-limit

FortiGate会将DNS服务器返回的解析结果缓存起来，需要再次解析缓存中的相同域名时，FortiGate会根据缓存条目快速返回结果，避免每次都需通过互联网重新获取相同的解析结果。此参数可以设置缓存中可以存储的最大DNS条目数（0~4294967295，默认值为5000）。

```bash
config system dns
    set dns-cache-limit <integer>
end
```

1. 通过`diagnose test application dnsproxy 7`可以查看已有的DNS缓存条目。

```bash
FortiGate # diagnose test application dnsproxy 7
worker idx: 0
vfid=0, name=docs.fortinet.com, ttl=360:36:1476
         154.52.22.201 (ttl=360)
vfid=0, name=api.forticonverter.com, ttl=300:0:1455
         3.223.208.97 (ttl=300)
vfid=0, name=ntp2.fortiguard.com, ttl=5382:4934:1352
         208.91.112.62 (ttl=5382) 208.91.112.60 (ttl=5382)
vfid=0, name=ntp1.fortiguard.com, ttl=18545:17755:1010
         208.91.112.61 (ttl=18704) 208.91.112.63 (ttl=18704)
vfid=0, name=globalmsgctrl.fortinet.net, ttl=51:0:948
         38.21.192.4 (ttl=51)
vfid=0, name=globalfctupdate.fortinet.net, ttl=18608:17585:777
         173.243.143.6 (ttl=18608)
vfid=0, name=globalfctupdate.fortinet.net, ttl=14975:13947:772
         2620:101:9000:143:173:243:143:6 (ttl=14975)
vfid=0, name=globalupdate.fortinet.net, ttl=16397:15288:691
         173.243.129.6 (ttl=21498) 173.243.140.6 (ttl=21498)
vfid=0, name=globalupdate.fortinet.net, ttl=11075:9966:691
         2620:101:9000:140:173:243:140:6 (ttl=11075)
vfid=0, name=globaldevquery.fortinet.net, ttl=19376:18265:689
         173.243.140.16 (ttl=19376)
CACHE num=10
```

2. 通过`diagnose test application dnsproxy 1`可以清空DNS缓存条目。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

dns-cache-ttl

DNS缓存条目保留的时间（单位为s，60~86400，默认值为1800）。

```bash
config system dns
    set dns-cache-limit <integer>
end
```

fqdn-cache-ttl

配置FQDN类型的地址对象后，FQDN地址对象会用2种方式学习域名对应的IP地址：

- FortiGate会主动定期去FortiGate配置的DNS服务器查询FQDN对应的解析结果（适用于明确的FQDN，如`www.fortinet.com`，不适用于通配符FQDN，如`*.fortinet.com`）。
- 只要穿过防火墙的DNS请求与响应（A/AAAA记录），匹配上了FQDN中的域名，FortiGate就会记录该IP地址到FQDN地址对象中（同时适用于明确的FQDN，如`www.fortinet.com`，也适用于通配符FQDN，如`*.fortinet.com`）。

FQDN地址对象会将解析结果缓存在FortiGate中。以下选项可以配置FQDN地址对象每个解析结果缓存的最大存活时间 （TTL，单位为s，0~86400，默认值为0，即使用DNS服务器返回的解析结果中的TTL）。这是FQDN地址对象在没有主动刷新的情况下的最大TTL。

```bash
config system dns
    set fqdn-cache-ttl 2000
end
```

1. 通过`diagnose test application dnsproxy 6`可以看到所有FQDN类型的地址对象已解析到的缓存条目，其中`cache_ttl`字段表示FQDN地址对象每个缓存IP条目的最大TTL。

```bash
FortiGate # diagnose test application dnsproxy 6
worker idx: 0
vfid=0 name=handbook.fortinet.com.cn ver=IPv4 wait_list=0 timer=590 min_ttl=600 cache_ttl=2000 slot=-1 num=1
wildcard=0
         39.105.115.226 (ttl=600:596:1996)
vfid=0 name=www.baidu.com ver=IPv4 wait_list=0 timer=50 min_ttl=32 cache_ttl=2000 slot=-1 num=2 wildcard=0
         220.181.111.1 (ttl=32:28:1996) 220.181.111.232 (ttl=32:28:1996)
```

> **重要**
>
> **TTL的3个数字解释（如上所示的ttl=600:596:1996）：**
>
> 第1个数字（600）：DNS服务器返回的解析结果中的最大TTL。
>
> 第2个数字（596）：DNS服务器返回的解析结果中的剩余TTL。
>
> 第3个数字（1996）：DNS缓存条目的剩余TTL。

2. `fqdn-cache-ttl`为全局设置。如果为某个FQDN 地址单独配置了`cache-ttl`值，它将取代该地址的全局`fqdn-cache-ttl`设置。如下所示，单独配置FQDN地址对象`www.baidu.com`的`cache-ttl`为800，`diagnose test application dnsproxy 6`命令的结果中显示`www.baidu.com`的`cache_ttl`为800，而`handbook.fortinet.com.cn`的`cache_ttl`仍为全局配置`fqdn-cache-ttl`中配置的2000。

```bash
config firewall address
    edit "www.baidu.com"
        set type fqdn
        set fqdn "www.baidu.com"
        set cache-ttl 800
    next
end
```

```bash
FortiGate # diagnose test application dnsproxy 6
worker idx: 0
vfid=0 name=handbook.fortinet.com.cn ver=IPv4 wait_list=0 timer=370 min_ttl=600 cache_ttl=2000 slot=-1 num=1
wildcard=0
         39.105.115.226 (ttl=600:376:1776)
vfid=0 name=www.baidu.com ver=IPv4 wait_list=0 timer=17 min_ttl=11 cache_ttl=800 slot=-1 num=4 wildcard=0
         103.235.47.188 (ttl=247:155:708) 103.235.46.96 (ttl=247:155:708) 220.181.111.232 (ttl=11:0:763)
220.181.111.1 (ttl=11:0:763)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 使用 `diagnose test application dnsproxy 4` 可以清空当前的FQDN缓存。

fqdn-min-refresh

FQDN缓存最小刷新时间（单位s，10~3600，默认为60s）。FQDN根据DNS服务器返回的所有该条目解析结果中最小的TTL间隔重新获取更新。默认配置下（`fqdn-min-refresh` =60，`fqdn-cache-ttl` =0），如果DNS服务器返回的解析结果中的最小TTL小于60s，FortiGate仍需要至少60s来重新查询FQDN。如果DNS服务器返回的解析结果中的最小TTL大于60s，FQDN根据DNS服务器返回的所有该条目解析结果中最小的TTL间隔重新获取更新。刷新动作不会删除已有的FQDN缓存IP条目。

> **重要**
>
> 实际的FQDN刷新动作会在 `fqdn-min-refresh` 时间到期前5s执行。

1. 默认配置（`fqdn-min-refresh` =60，`fqdn-cache-ttl` =0）下，使用 `diagnose test application dnsproxy 3` 查看当前 `fqdn-min-refresh` 配置。

```bash
FortiGate # diagnose test application dnsproxy 3
......
FQDN: min_refresh=60 max_refresh=3600
......
```

2. 执行 `diagnose test application dnsproxy 6` 命令，如下所示 `www.baidu.com` 的解析结果有4个，DNS服务器返回的所有该条目解析结果中最小的TTL（`min_ttl`）为48，但重新查询域名的等待时间（`timer`）仍然按照 `fqdn-min-refresh` 的默认配置60s进行倒计时。

```bash
FortiGate # diagnose test application dnsproxy 6
worker idx: 0
vfid=0 name=www.baidu.com ver=IPv4 wait_list=0 timer=56 min_ttl=48 cache_ttl=0 slot=-1 num=4 wildcard=0
        220.181.111.1 (ttl=69:54:54) 220.181.111.232 (ttl=69:54:54) 110.242.70.57 (ttl=48:47:47) 110.242.69.21
(ttl=48:47:47)

FQDN num=2
```

- `min_ttl`：DNS服务器返回的所有该条目解析结果中最小的TTL。
- `timer`：重新查询域名的等待时间计时器。

3. 将 `fqdn-min-refresh` 设置为20，小于 `min_ttl`。

```bash
config system dns
    set fqdn-min-refresh 20
end
```

4. 执行 `diagnose test application dnsproxy 6` 命令，如下所示 `www.baidu.com` 的解析结果有2个，DNS服务器返回的所有该条目解析结果中最小的TTL（`min_ttl`）为54，重新查询域名的等待时间（`timer`）按照 `min_ttl` 的54s进行倒计时。

```bash
FortiGate # diagnose test application dnsproxy 6
worker idx: 0
......
vfid=0 name=www.baidu.com ver=IPv4 wait_list=0 timer=52 min_ttl=54 cache_ttl=0 slot=-1 num=2 wildcard=0
        110.242.70.57 (ttl=54:52:52) 110.242.69.21 (ttl=54:52:52)

FQDN num=2
```

5. `fqdn-min-refresh` 可与 `fqdn-cache-ttl`、`cache-ttl` 结合使用，以发送更频繁的查询并在缓存中存储更多已解析的地址。这在FQDN有较多解析结果且变化非常频繁的情况下非常有用。

6. 总结如下：

- `min_ttl` < `fqdn-min-refresh`：使用 `fqdn-min-refresh` 作为重新请求FQDN的计时器（`timer`）。
- `min_ttl` > `fqdn-min-refresh`：使用 `min_ttl` 作为重新请求FQDN的计时器（`timer`）。
- `fqdn-min-refresh/min_ttl` < `fqdn-cache-ttl/cache-ttl`：使用 `fqdn-min-refresh/min_ttl` 作为重新请求FQDN的计时器（`timer`）。
- `fqdn-min-refresh/min_ttl` > `fqdn-cache-ttl/cache-ttl`：使用 `fqdn-cache-ttl/cache-ttl` 作为重新请求FQDN的计时器（`timer`）。

fqdn-max-refresh

FQDN缓存最大刷新时间（单位为s，3600~86400，默认值为3600）。`fqdn-max-refresh` 用于控制FQDN刷新计时器的全局上限。最小TTL大于fqdn-max-refresh值的FQDN条目，其刷新定时器将减少到该上限。最小TTL小于fqdn-max-refresh值的FQDN条目，其刷新定时器将取决于该条目所有解析结果中最小的TTL值。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

`fqdn-max-refresh`的测试结果与`fqdn-min-refresh`类似，这里就不再赘述。

dnsproxy-worker-count

对于有多个逻辑CPU核心的FortiGate，可以设置用于运行dnsproxy进程的CPU核心数，默认配置为1。

```bash
config system global
    set dnsproxy-worker-count <integer>
end
```

在有大量FDQN地址对象的情况下，编辑DNS相关配置时，dnsproxy进程可能会消耗大量CPU资源，它会同时处理DNS相关配置更改和DNS解析任务。当`dnsproxy-worker-count`从1增加到2时：

- dnsproxy-worker-1：处理DNS相关配置更改。
- dnsproxy-worker-2：处理DNS解析任务。

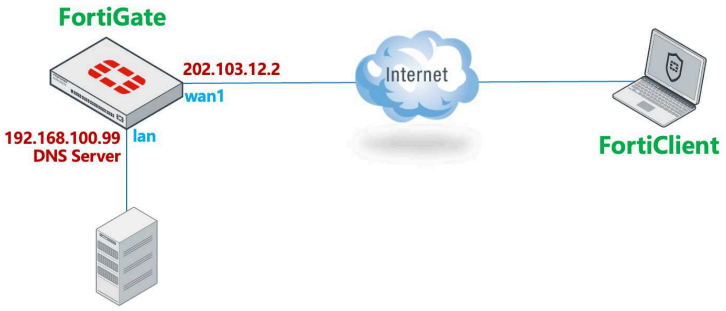
其他CLI配置

```bash
config system dns
    set primary <ip_address>
    set secondary <ip_address>
    set protocol {cleartext dot doh}
    set ssl-certificate <string>
    set server-hostname <hostname>
    set domain <domains>
    set ip6-primary <ip6_address>
    set ip6-secondary <ip6_address>
    set timeout <integer>
    set retry <integer>
    set dns-cache-limit <integer>
    set dns-cache-ttl <integer>
    set cache-notfound-responses {enable | disable}
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
    set source-ip <class_ip>
    set root-servers <DNS root name server IP address>
    set server-select-method {least-rtt | failover}
    set alt-primary <ip_address>
    set alt-secondary <ip_address>
    set log {disable |error | all}
    set fqdn-cache-ttl <integer>
    set fqdn-min-refresh <integer>
    set fqdn-max-refresh <integer>
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

穿越接口的DNS服务

网络需求



FortiGate内网口（lan）开启DNS服务器，作为内部网络和SSL VPN/IPSec VPN客户端的DNS服务器。SSL VPN客户端连接后，使用FortiGate内网口上提供的DNS服务进行域名解析。

1. 在FortiGate上的“主DNS服务器”和“备用DNS服务器”均为公网的DNS服务器，如下所示。

```bash
config system dns
    set primary 223.5.5.5
    set secondary 114.114.114.114
end
```

2. FortiGate仅在内网口上启用DNS服务器（递归方式）。

```bash
config system interface
    edit "lan"
        set ip 192.168.100.99 255.255.255.0
    next
end

config system dns-server
    edit "lan"
        set mode recursive
    next
end
```

3. SSL VPN配置分配的DNS服务器为FortiGate内网接口IP 192.168.100.99。

```bash
config vpn ssl settings
    set servercert "Fortinet_Factory"
    set tunnel-ip-pools "sslvpn_pool"
    set dns-server1 192.168.100.99     ←——设置分配的DNS服务器为FortiGate内网口地址
    set source-interface "wan1"
    set default-portal "web-access"
    config authentication-rule
        edit 2
            set groups "VPN"
            set portal "full-access"
        next
    end
end
```

4. 防火墙策略、SSL VPN门户、用户等配置略。

问题现象

1. FortiClient客户端连接FortiGate的SSL VPN后，使用FortiGate内网口上提供的DNS服务器（192.168.100.99）无法进行域名解析。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
::: important
nslookup www.baidu.com
:::
Server:     192.168.100.99
Address:    192.168.100.99#53
;; connection timed out; no servers could be reached
```

2. 在FortiGate上抓包查看FortiClient（3.3.3.9）发送的DNS请求，只有从`ssl.root`接口进的流量，没有返回的流量。

```bash
FortiGate # diagnose sniffer packet any 'host 3.3.3.9 and port 53' 4
interfaces=[any]
filters=[host 3.3.3.9 and port 53]
0.614261 ssl.root in 3.3.3.9.65295 → 192.168.100.99.53: udp 47
0.614514 ssl.root in 3.3.3.9.53355 → 192.168.100.99.53: udp 47
1.660982 ssl.root in 3.3.3.9.65295 → 192.168.100.99.53: udp 47
1.661521 ssl.root in 3.3.3.9.53355 → 192.168.100.99.53: udp 47
1.793631 ssl.root in 3.3.3.9.56286 → 192.168.100.99.53: udp 31
```

3. 在FortiGate上查看对应的dnsproxy debug信息，提示解析结果为`non-active`。

```bash
diagnose debug application dnsproxy -1
diagnose debug enable

[worker 0] udp_receive_request()-3194: vd=0, vrf=0, intf=39, len=31, alen=16, 3.3.3.9:59503⇒192.168.100.99
[worker 0] handle_dns_request()-2489: vfid=0 real_vfid=0 id=0×1aec pktlen=31 qr=0 req_type=3
[worker 0] dns_parse_message()-603
[worker 0] dns_nat64_ptr_lookup()-272
[worker 0] dns_nat64_ptr_lookup()-285: vdname:root request:256

[worker 0] dns_nat64_update_request()-305
[worker 0] dns_nat64_update_request()-319: vdname:root request:1

[worker 0] get_intf_policy()-1469: ifindex=39
[worker 0] dns_query_delete()-585: orig id:0×1aec local id:0×0000 domain=www.baidu.com use=5 non-active    ←——提示解析结果为non-active
```

解决方法

1. 对于这种穿越接口之间提供DNS服务的场景，DNS服务器接口的配置除了要添加提供DNS服务的接口（此例中为内网口`lan`），还要添加DNS请求流量的入接口（此例中为内网口`ssl.root`）。

```bash
config system dns-server
    edit "lan"
        set mode recursive
    next
    edit "ssl.root"
        set mode recursive
    next
end
```

2. FortiClient客户端再次使用FortiGate内网口上提供的DNS服务器（192.168.100.99）进行域名解析，可以正常获取解析结果。

```bash
::: important
nslookup www.baidu.com
:::
Server:     192.168.100.99
Address:    192.168.100.99#53

Non-authoritative answer:
Name:   www.baidu.com
Address: 110.242.70.57
Name:   www.baidu.com
Address: 110.242.69.21
```

3. 在FortiGate上查看对应的dnsproxy debug信息，显示FortiGate的内网口`lan`收到FortiClient（3.3.3.9）的DNS请求后，递归到公网DNS服务器114.114.114.114进行查询，并将DNS解析结果返回给FortiClient（3.3.3.9）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
diagnose debug application dnsproxy -1
diagnose debug enable

[worker 0] udp_receive_request()-3194: vd=0, vrf=0, intf=39, len=31, alen=16, 3.3.3.9:59143⇒192.168.100.99

[worker 0] get_intf_policy()-1469: ifindex=39
[worker 0] dns_local_lookup_common()-2553: vfid=0, real_vfid=0, view=2, qname=www.baidu.com, qtype=1, qclass=1,
offset=31, map#=3 max_sz=512
[worker 0] dns_lookup_aa_zone()-608: vfid=0, fqdn=www.baidu.com
[worker 0] dns_send_request()-1490
[worker 0] dns_send_resol_request()-1344: orig id: 0×95f3 local id: 0×95f3 domain=www.baidu.com
[worker 0] dns_find_best_server()-652: found server: 114.114.114.114 (vfid=0 vrf=0)
[worker 0] dns_udp_forward_request()-1089: vdom=root req_type=3 domain=www.baidu.com oif=0
[worker 0] dns_udp_forward_request()-1210: Send 31B to [114.114.114.114]:53 via fd=20 request:1
[worker 0] udp_receive_request()-3144
[worker 0] batch_on_read()-3555
[worker 0] _udp_receive_response()-3406: vd-0: len=63, addr=114.114.114.114:53, rating=0
[worker 0] dns_query_handle_response()-2743: vfid=0 real_vfid=0 vrf=0 id=0×95f3 domain=www.baidu.com pktlen=63
[worker 0] dns_query_save_response()-2724: domain=www.baidu.com pktlen=63
[worker 0] dns_set_min_ttl()-190: QR: www.baidu.com
[worker 0] dns_set_min_ttl()-197: Offset of 1st RR: 31 Number of RR's: 2
[worker 0] dns_set_min_ttl()-218: RR TTL: 78, RR type: 1
[worker 0] dns_set_min_ttl()-218: RR TTL: 78, RR type: 1
[worker 0] dns_cache_response()-329: Min ttl = 78
[worker 0] dns_forward_response()-1720
[worker 0] dns_secure_forward_response()-1676: category=255 profile=none
[worker 0] dns_visibility_log_hostname()-241: vd=0 pktlen=63
[worker 0] wildcard_fqdn_response_cb()-965: vd=0 pktlen=63
[worker 0] hostname_entry_insert()-143: af=2 domain=www.baidu.com
[worker 0] hostname_entry_insert()-143: af=2 domain=www.baidu.com
[worker 0] dns_send_response()-1645: domain=www.baidu.com reslen=63
[worker 0] __dns_udp_forward_response()-1522
[worker 0] __dns_udp_forward_response()-1533: vd-0 Send 63B via fd=7, family=2
[worker 0] __dns_udp_forward_response()-1537: set svf of fd to 0
[worker 0] __dns_udp_forward_response()-1587: vd=0 send 63B response 192.168.100.99:53⇒3.3.3.9:59143
[worker 0] dns_query_delete()-585: orig id:0×95f3 local id:0×95f3 domain=www.baidu.com use=7 active
[worker 0] dns_query_cleanup()-564: use=2
```

总结

1. 对于这种穿越接口之间提供DNS服务的场景，如FortiGate不同VLAN之间、不同物理口之间、VPN接口到内网口的DNS访问，均需要在DNS服务器接口配置中增加DNS请求流量的入接口。
2. 从FortiOS 7.6.1开始，这种场景不再需要在DNS服务器上配置DNS请求的入接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

可选DNS服务器

网络需求

FortiGate配置DNS为公网的DNS服务器，同时FortiGate作为内网PC的DNS服务器。客户端PC无法通过FortiGate解析内网服务器的域名，只有内网的DNS服务器可以解析内网域名。需要FortiGate能够解析公共DNS服务器无法解析的内部域名。

1. 在FortiGate上的“主DNS服务器”和“备用DNS服务器”均为公网的DNS服务器，如下所示。

```bash
config system dns
    set primary 223.5.5.5
    set secondary 114.114.114.114
end
```

2. FortiGate作为内部网络的DNS服务器（递归方式），未配置DNS数据库。内网PC的DNS服务器均设定为FortiGate的内网口IP 192.168.100.99，通过FortiGate来解析域名。

```bash
config system interface
    edit "lan"
        set ip 192.168.100.99 255.255.255.0
    next
end

config system dns-server
    edit "lan"
    next
end
```

3. 在此配置下，客户端PC访问域名时，会向FortiGate的内网口192.168.100.99发起DNS解析请求，默认配置（`set server-select-method`）下，FortiGate会选择延迟最小的服务器转发DNS请求，此例中223.5.5.5的延迟更低。

4. 客户端PC有访问内网服务器域名的需求，如`www.fortidocs.com`，这种域名通过公网的DNS服务器是无法解析的，会直接返回DNS NXDOMAIN，导致客户端PC无法通过域名访问内网服务器。

```bash
::: important
nslookup www.fortidocs.com 192.168.100.99
:::
Server:     192.168.100.99
Address:    192.168.100.99#53

** server can't find www.fortidocs.com: NXDOMAIN
```

5. 只有内网的DNS服务器可以解析这些内网服务器的域名，需要FortiGate在解析域名失败后，将解析请求转发至内网DNS服务器。

6. 内网DNS服务器中的DNS条目较多或没有权限访问，无法通过在FortiGate上配置DNS Database来解决此问题。

解决方法

1. 配置可选DNS（Alt-DNS）服务器。当FortiGate的主DNS服务器/备用DNS服务器返回DNS的名称解析错误（NXDOMAIN）时，FortiGate会查询配置的Alt-DNS服务器。可选DNS服务器的常见用途是解析公共DNS服务器无法解析的内部域名。

2. 配置方法（只能通过CLI配置），与DNS服务器一样，可以配置主Alt-DNS和备用Alt-DNS，默认配置（`set server-select-method`）下，FortiGate会选择延迟最小的Alt-DNS服务器转发DNS请求：

> **重要**
>
> 使用条件：
>
> - FortiGate的主DNS服务器/备用DNS服务器返回DNS的错误类型为NXDOMAIN时，FortiGate才会查询配置的Alt-DNS服务器。
> - 没有在DNS Database中配置对应内网域名的条目。

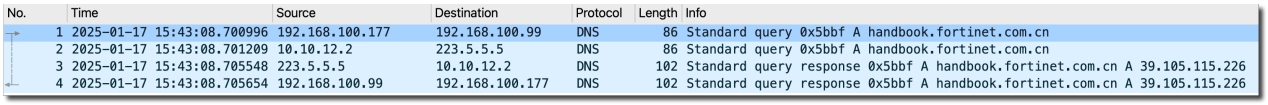
```bash
config system dns
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在以上场景的配置基础上，增加Alt-DNS服务器的配置10.10.12.1和10.10.12.3。

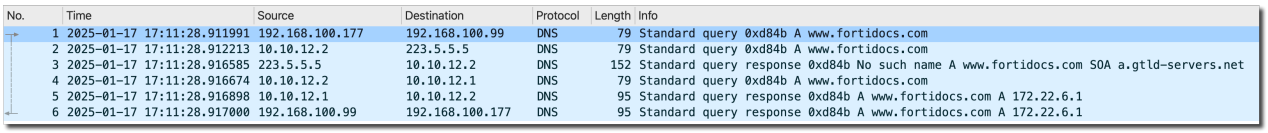
```bash
config system dns
    set primary 223.5.5.5
    set secondary 114.114.114.114
    set alt-primary 10.10.12.1
    set alt-secondary 10.10.12.3
end
```

4. 使用PC客户端指定FortiGate内网口来解析公网DNS服务器可以解析的域名（这里以`handbook.fortinet.com.cn`为例），FortiGate将DNS请求递归到主DNS服务器查询，主DNS服务器返回解析结果（A记录），FortiGate将解析结果以自身内网口为源IP返回给PC客户端。



No.	Time	Source	Destination	Protocol	Length	Info
1	2025-01-17 15:43:08.700996	192.168.100.177	192.168.100.99	DNS	86	Standard query 0x5bbf A handbook.fortinet.com.cn
2	2025-01-17 15:43:08.701209	10.10.12.2	223.5.5.5	DNS	86	Standard query 0x5bbf A handbook.fortinet.com.cn
3	2025-01-17 15:43:08.705548	223.5.5.5	10.10.12.2	DNS	102	Standard query response 0x5bbf A handbook.fortinet.com.cn A 39.105.115.226
4	2025-01-17 15:43:08.705654	192.168.100.99	192.168.100.177	DNS	102	Standard query response 0x5bbf A handbook.fortinet.com.cn A 39.105.115.226

5. 使用PC客户端指定FortiGate内网口来解析公网DNS服务器无法解析的域名（这里以`www.fortidocs.com`为例），FortiGate将DNS请求递归到主DNS服务器查询，主DNS服务器返回无法解析的结果（NXDOMAIN），FortiGate不会将此DNS NXDOMAIN返回给客户端PC，随后使用位于内网的主Alt-DNS服务器（10.10.12.1）进行查询，主Alt-DNS服务器（10.10.12.1）返回解析结果（A记录）给FortiGate，FortiGate将解析结果返回给PC客户端。



No.	Time	Source	Destination	Protocol	Length	Info
1	2025-01-17 17:11:28.911991	192.168.100.177	192.168.100.99	DNS	79	Standard query 0xd84b A www.fortidocs.com
2	2025-01-17 17:11:28.912213	10.10.12.2	223.5.5.5	DNS	79	Standard query 0xd84b A www.fortidocs.com
3	2025-01-17 17:11:28.916585	223.5.5.5	10.10.12.2	DNS	152	Standard query response 0xd84b No such name A www.fortidocs.com SOA a.gtld-servers.net
4	2025-01-17 17:11:28.916674	10.10.12.2	10.10.12.1	DNS	79	Standard query 0xd84b A www.fortidocs.com
5	2025-01-17 17:11:28.916898	10.10.12.1	10.10.12.2	DNS	95	Standard query response 0xd84b A www.fortidocs.com A 172.22.6.1
6	2025-01-17 17:11:28.917000	192.168.100.99	192.168.100.177	DNS	95	Standard query response 0xd84b A www.fortidocs.com A 172.22.6.1

```bash
::: important
nslookup www.fortidocs.com 192.168.100.99
:::
Server:     192.168.100.99
Address:    192.168.100.99#53

Non-authoritative answer:
Name:   www.fortidocs.com
Address: 172.22.6.1
```

6. 查看Alt-DNS整个过程的dnsproxy debug信息。

```bash
diagnose debug application dnsproxy -1
diagnose debug enable

[worker 0] udp_receive_request()-3144
[worker 0] udp_receive_request()-3194: vd=0, vrf=0, intf=46, len=35, alen=16,
192.168.100.177:64454=>192.168.100.99
[worker 0] handle_dns_request()-2489: vfid=0 real_vfid=0 id=0xe5ae pktlen=35 qr=0 req_type=3
[worker 0] get_intf_policy()-1469: ifindex=46
[worker 0] dns_local_lookup_common()-2553: vfid=0, real_vfid=0, view=2, qname=www.fortidocs.com, qtype=1,
qclass=1, offset=35, map#=3 max_sz=512
[worker 0] dns_lookup_aa_zone()-608: vfid=0, fqdn=www.fortidocs.com
[worker 0] dns_send_request()-1490
[worker 0] dns_send_resol_request()-1344: orig id: 0xe5ae local id: 0xe5ae domain=www.fortidocs.com
[worker 0] dns_find_best_server()-652: found server: 223.5.5.5 (vfid=0 vrf=0)
[worker 0] dns_udp_forward_request()-1089: vdom=root req_type=3 domain=www.fortidocs.com oif=0
[worker 0] dns_udp_forward_request()-1210: Send 35B to [223.5.5.5]:53 via fd=20 request:1
[worker 0] udp_receive_request()-3144
[worker 0] batch_on_read()-3555
[worker 0] _udp_receive_response()-3406: vd-0: len=108, addr=223.5.5.5:53, rating=0
[worker 0] dns_query_handle_response()-2743: vfid=0 real_vfid=0 vrf=0 id=0xe5ae domain=www.fortidocs.com
pktlen=108
[worker 0] dns_retransmit_func()-1763: jiffies=183874965 created=183874965 wait_cat=0 wait_res=1 profile=
last_tx=183874964 ftg_last_tx=0 domain=www.fortidocs.com (orig id: 0xe5ae local id:0xe5ae active)
[worker 0] dns_send_request()-1490
[worker 0] dns_send_resol_request()-1344: orig id: 0xe5ae local id: 0xe5ae domain=www.fortidocs.com
[worker 0] dns_find_best_server()-652: found server: 10.10.12.1 (vfid=0 vrf=0)
[worker 0] dns_udp_forward_request()-1089: vdom=root req_type=3 domain=www.fortidocs.com oif=0
[worker 0] dns_udp_forward_request()-1210: Send 35B to [10.10.12.1]:53 via fd=20 request:1
[worker 0] batch_on_read()-3555
[worker 0] _udp_receive_response()-3406: vd-0: len=51, addr=10.10.12.1:53, rating=0
[worker 0] dns_query_handle_response()-2743: vfid=0 real_vfid=0 vrf=0 id=0xe5ae domain=www.fortidocs.com pktlen=51
[worker 0] dns_query_save_response()-2724: domain=www.fortidocs.com pktlen=51
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[worker 0] dns_set_min_ttl()-190: QR: www.fortidocs.com
[worker 0] dns_set_min_ttl()-197: Offset of 1st RR: 35 Number of RR's: 1
[worker 0] dns_set_min_ttl()-218: RR TTL: 86400, RR type: 1
[worker 0] dns_cache_response()-329: Min ttl = 86400
[worker 0] dns_forward_response()-1720
[worker 0] dns_secure_forward_response()-1676: category=255 profile=none
[worker 0] dns_visibility_log_hostname()-241: vd=0 pktlen=51
[worker 0] wildcard_fqdn_response_cb()-965: vd=0 pktlen=51
[worker 0] hostname_entry_insert()-143: af=2 domain=www.fortidocs.com
[worker 0] dns_send_response()-1645: domain=www.fortidocs.com reslen=51
[worker 0] __dns_udp_forward_response()-1522
[worker 0] __dns_udp_forward_response()-1533: vd-0 Send 51B via fd=7, family=2
[worker 0] __dns_udp_forward_response()-1537: set svf of fd to 0
[worker 0] __dns_udp_forward_response()-1587: vd=0 send 51B response 192.168.100.99:53⇒192.168.100.177:64454
[worker 0] dns_query_delete()-585: orig id:0×e5ae local id:0×e5ae domain=www.fortidocs.com use=7 active
```

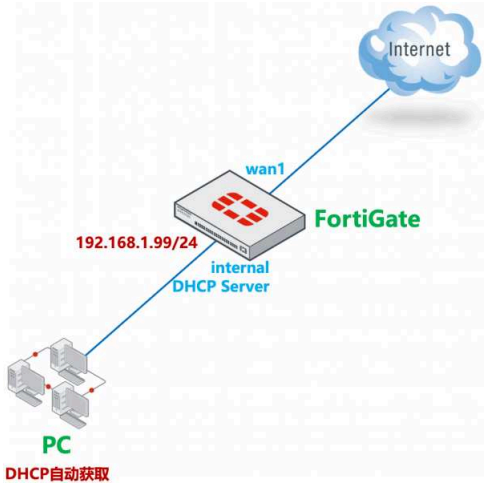

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DHCP服务器配置

网络需求

开启FortiGate的DHCP服务器功能，内网电脑可通过自动获取地址的方式上网。内网用户网段为192.168.1.0/24，网关为192.168.1.99。

网络拓扑



配置要点

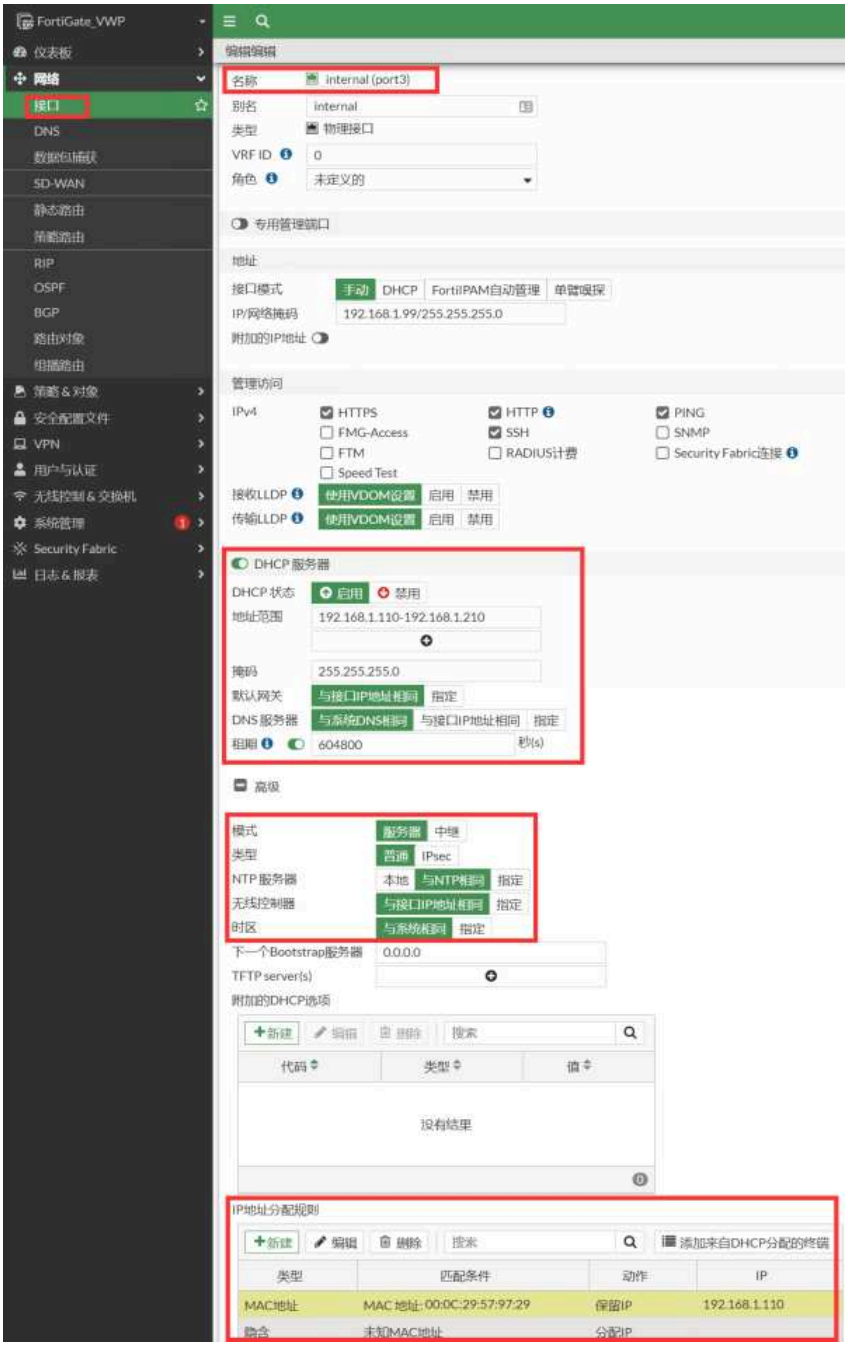
- 基本上网配置
- 配置DHCP服务器

配置步骤

1. 基本上网配置，请参考策略与对象→单线路上网配置→静态地址线路上网配置↗章节。

2. 开启DHCP服务，进入网络→接口，选择需要开启DHCP服务的接口，启用DHCP服务器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

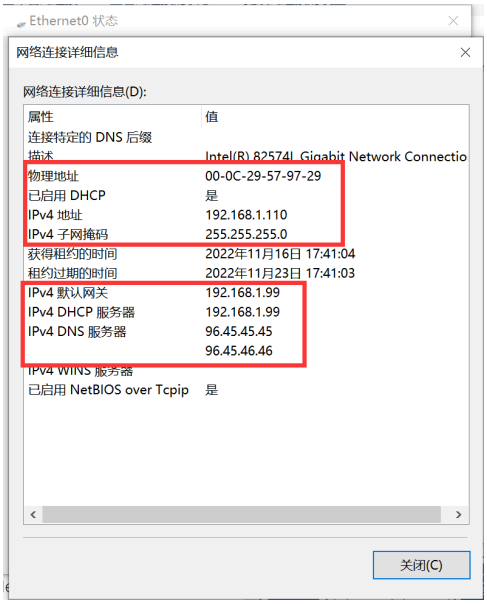


- 地址范围：用于为用户分配的IP地址范围
- 掩码：分配的地址池地址掩码
- 默认网关：一般为 DHCP所在接口的ip地址，也可以手工指定
- DNS服务器：直接使用系统的DNS配置，也可以手工指定
- 模式：选择“DHCP服务器模式”
- IP地址分配规则：可指定固定的MAC地址分配固定的IP地址，也可以针对固定的MAC地址进行阻断过滤的策略控制（不需要控制IP分配到具体的主机时不需要配置）
- 类型：普通（或IPsec，用于为IPsec用户分配IP地址）

结果验证

将电脑配置为自动获取IP地址模式，会获取配置的MAC地址对应的IP地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



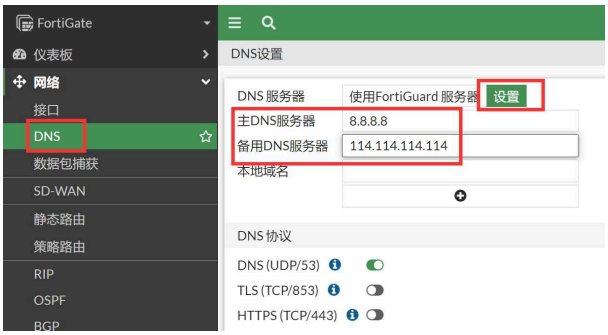
注意事项

1. DHCP配置中，利用系统DNS，为防火墙自身系统的DNS配置。当执行命令set dns-service default时，PC终端获取到防火墙自身系统配置的DNS。

```
FortiGate# config system dhcp server
FortiGate(server) #edit 1
FortiGate(1)#set dns-service default     //默认参数
default    Use system DNS settings.      //防火墙上配置的系统DNS服务器,
local      Use this RGT as DNS server.   //防火墙接口的IP地址,
specify    Specify DNS servers.          //指定DNS
```

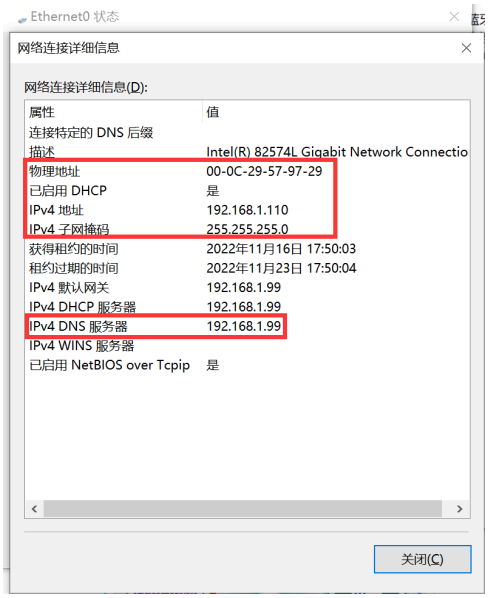
2. 可以自定义设置防火墙自身系统DNS。

```
FortiGate#config system dns      //防火墙上配置的dns
FortiGate(dns) #set primary 8.8.8.8
FortiGate(dns) #end
```



3. 当FortiGate执行命令set dns-service local时，PC终端获取到防火墙启用DHCP接口的IP日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



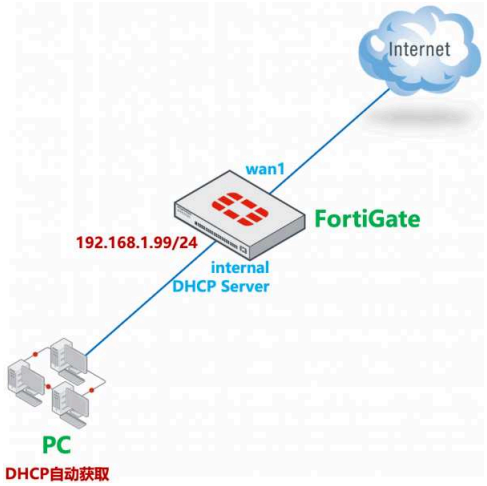
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DHCP静态绑定

网络需求

开启FortiGate的DHCP服务器功能，内网电脑可通过自动获取地址的方式上网。内网用户网段为192.168.1.0/24，网关为192.168.1.99。为MAC地址00:0c:29:57:97:29的主机保留ip地址192.168.1.110。

网络拓扑



配置要点

- 基本上网配置
- 配置DHCP服务器

配置步骤

1. 基本上网配置，请参考策略与对象→单线路上网配置→静态地址线路上网配置↗章节。

2. 配置DHCP服务，请参考网络管理→DHCP配置→DHCP服务器配置↗章节。

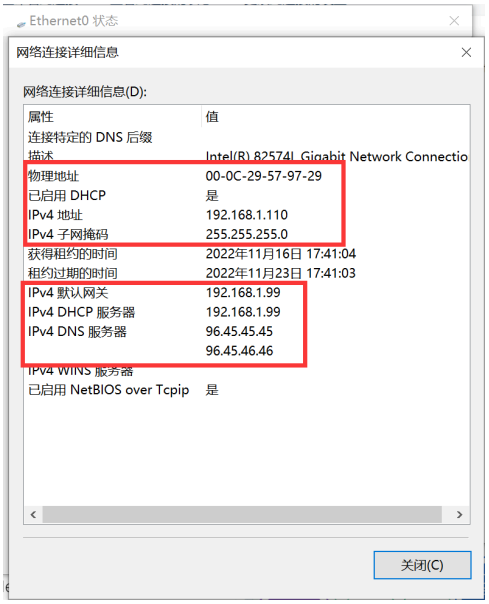
3. 配置保留IP，也可参考网络管理→DHCP配置→DHCP服务器配置↗中的GUI方式配置。

```
FortiGate# config system dhcp server
FortiGate(server) # edit 1                          //DHCP基础配置
FortiGate(1)#set dns-service default
FortiGate(1)#set default-gateway 192.168.1.99
FortiGate(1)#set netmask 255.255.255.0
FortiGate(1)#set interface internal
FortiGate(1) # config ip-range
FortiGate(ip-range) #edit 1
FortiGate(1)set start-ip 192.168.1.110
FortiGate(1)set end-ip 192.168.1.210
FortiGate(1) # next
FortiGate(ip-range) # end                           //DHCP基础配置
FortiGate(1)#config reserved-address                //配置保留ＩＰ
FortiGate(reserved-address)#edit 1                 //条目：1，2，3，仅做为标识作用，可以写多个条目。
FortiGate(1) # set ip 192.168.1.110                 //为指定MAC地址分配该IP地址
FortiGate(1) # set mac 00:0c:29:57:97:29            //指定MAC地址
FortiGate(1) # next
FortiGate(reserved-address) # end
FortiGate(1) # next
FortiGate(server) #end
```

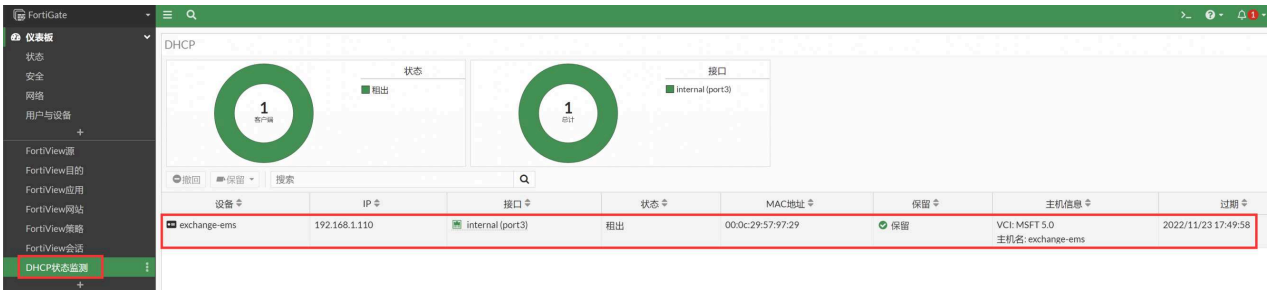

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

1. 将电脑配置为自动获取IP地址模式，MAC地址为00:0c:29:57:97:29的主机会获取192.168.1.110。



2. 查看防火墙上dhcp地址池分配情况。



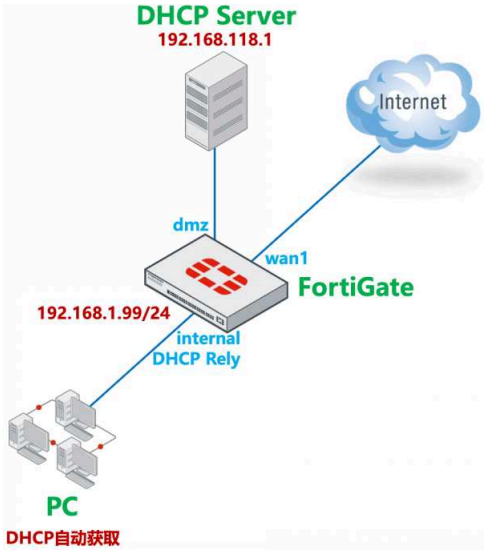
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DHCP中继配置

网络需求

在FortiGate上开启DHCP中继，让内网电脑能获取来自DHCP服务器分配的地址。

网络拓扑



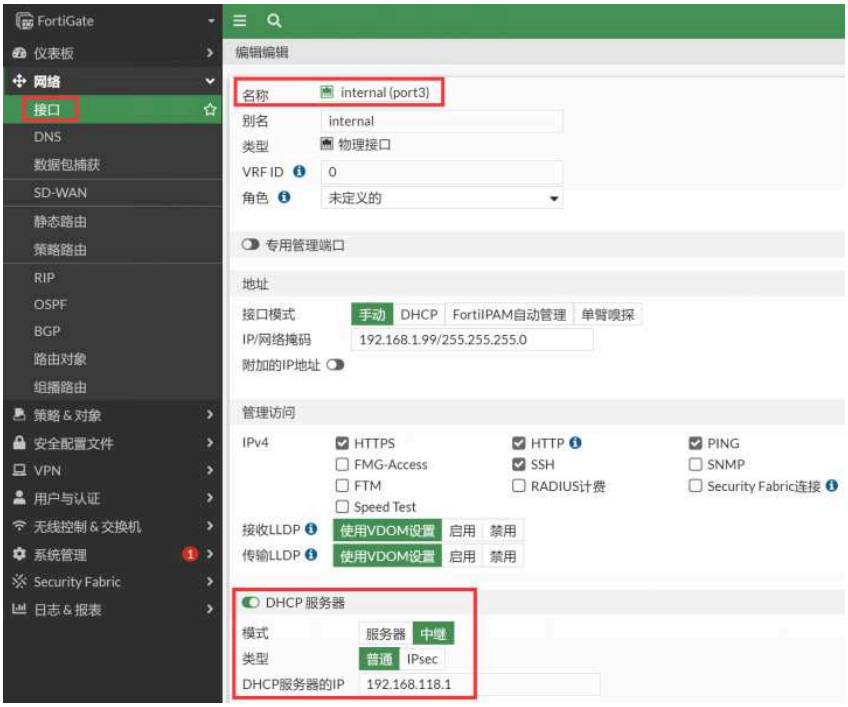
配置要点

- 基础上网配置
- 开启DHCP中继功能，并填写DHCP服务器地址

配置步骤

1. 基本上网配置，请参考策略与对象→单线路上网配置→静态地址线路上网配置↗章节。
2. 开启DHCP中继功能，并填写DHCP服务器地址。进入网络→接口，编辑需要开启DHCP服务的接口，开启DHCP服务器，打开高级选项，模式选择中继。

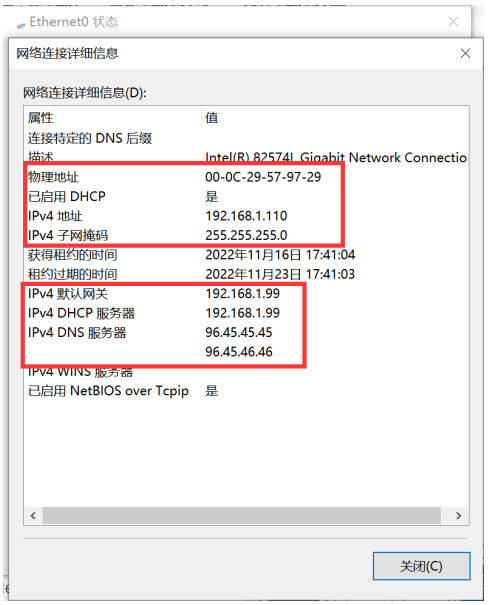
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- DHCP服务器：开启
- DHCP服务器的IP：填写真实DHCP服务器的IP地址，需要防火墙进行中继的DHCP服务器地址
- Mode：中继
- 类型： 普通（或IPsec，用于为IPsec用户分配IP地址）

结果验证

将电脑配置为自动获取IP地址模式，会获取相应的IP地址。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

端口聚合配置

LACP应用场景

1. 在带宽比较紧张的情况下，可以通过逻辑聚合可以扩展带宽到原链路的n倍。
2. 在需要对链路进行动态备份的情况下，可以通过配置链路聚合实现同一聚合组各个成员端口之间彼此动态备份。

LACP模式

LACP的端口可以支持如下几种模式：static（静态），passive，和active：

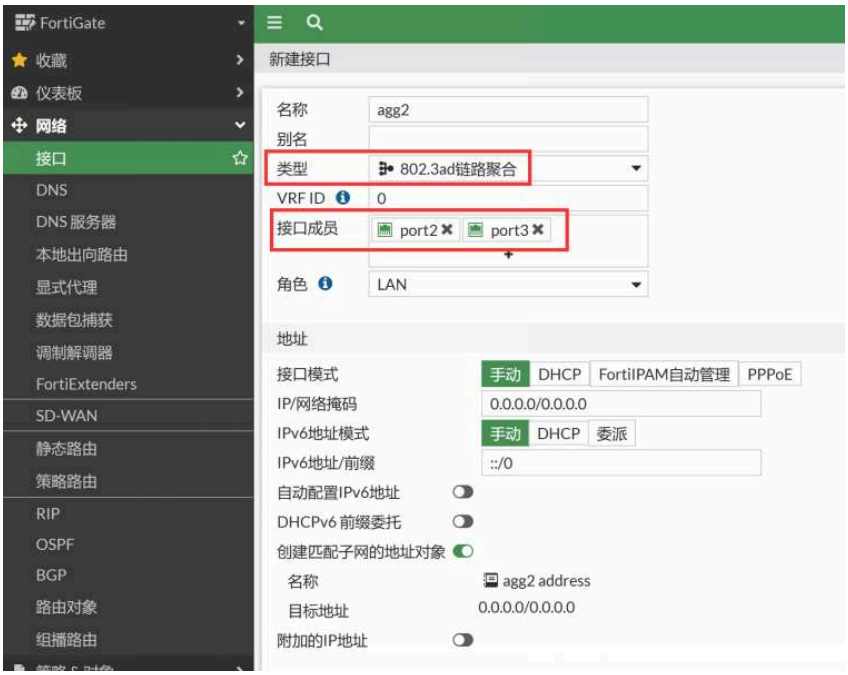
- 静态：人为配置的聚合组，不允许系统自动添加或删除手工或静态聚合端口。
- passive：被动模式，该模式下端口不会主动发送LACPDU报文，在接收到对端发送的LACP报文后，该端口进入协议计算状态。
- Active：主动模式，该模式下端口会主动向对端发送LACPDU报文，进行LACP协议的计算。

LACP配置

1. 添加聚合接口，进入网络→接口，新建接口。



2. 类型选择802.3ad聚合，选择物理接口成员。



重要

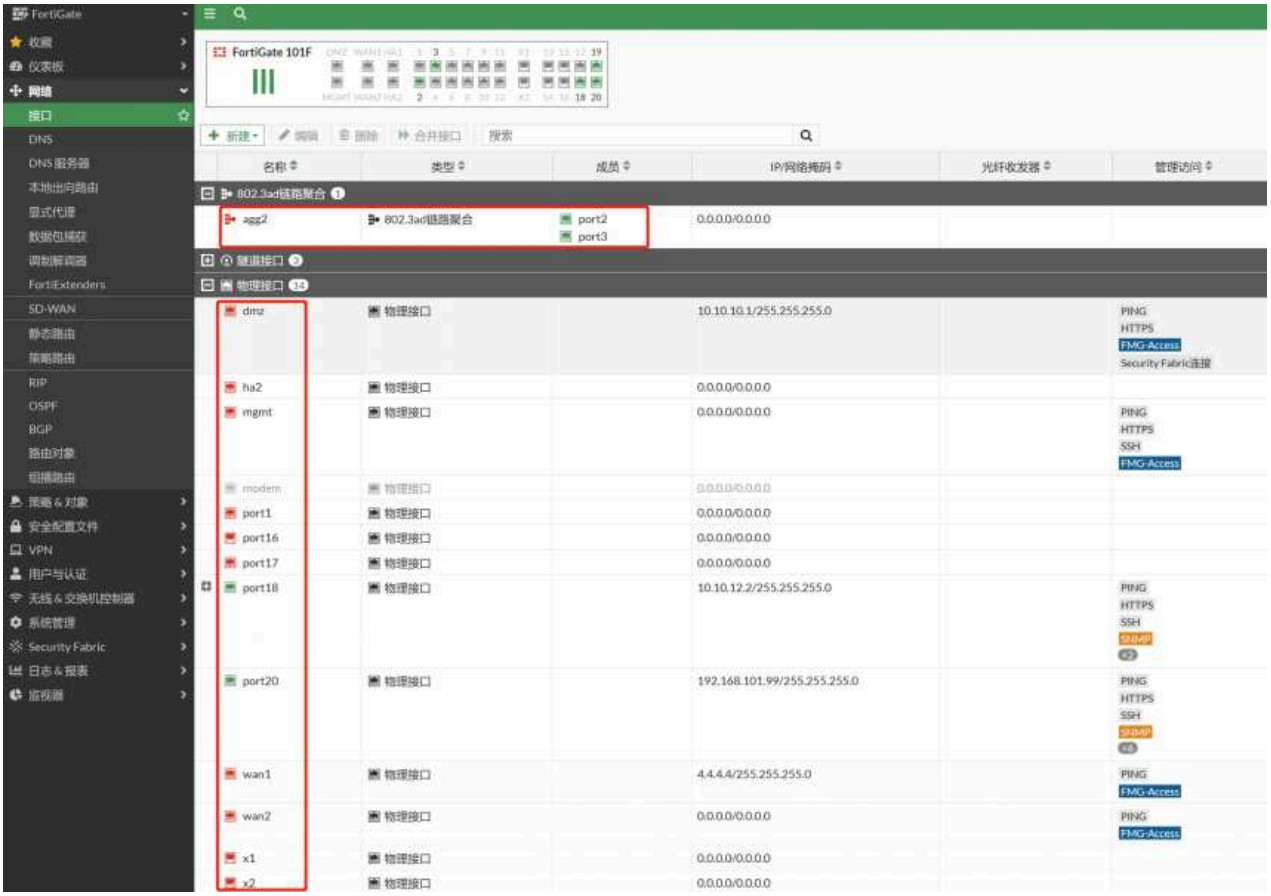
建议在不需要的情况下关闭接口配置下的“设备探测”（Device detection）功能，该功能用于MAC地址厂商设备信息识别及MAC地址过滤，会消耗较多的设备资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 修改LACP的配置（可选）。

```
FortiGate # config system interface
FortiGate (interface) # edit agg2
FortiGate (lacp) # set lacp-mode active          //配置LACP协商模式：主动，被动或者静态，默认为动态
FortiGate (lacp) # set algorithm L3              //负载均衡算法：L3基于IP地址进行哈希，L4基于四层进行哈希
FortiGate (lacp) # end
```

4. 配置完成后查看配置聚合口配置，对应的物理口在WEB/CLI界面上将消失，不可配置。



5. 查看接口的命令行配置。

```
config system interface
    edit "agg2"
        set vdom "root"
        set type aggregate
        set member "port2" "port3"
        set lldp-transmission enable
        set role lan
        set snmp-index 40
        set algorithm L3
    next
end
```

6. 查看LACP接口状态。

```
FGT1-MASTER # diagnose netlink aggregate name agg2
LACP flags: (A|P)(S|F)(A|I)(I|O)(E|D)(E|D)
(A|P) - LACP mode is Active or Passive
(S|F) - LACP speed is Slow or Fast
(A|I) - Aggregatable or Individual
(I|O) - Port In sync or Out of sync
(E|D) - Frame collection is Enabled or Disabled
(E|D) - Frame distribution is Enabled or Disabled

status: up
npu: n
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
flush: n
asic helper: y
ports: 2
link-up-delay: 50ms
min-links: 1
ha: master
distribution algorithm: L4
LACP mode: active
LACP speed: slow
LACP HA: enable
aggregator ID: 1
actor key: 33
actor MAC address: 50:00:00:03:00:01
partner key: 1
partner MAC address: aa:bb:cc:80:a0:00

slave: port9
  index: 0
  link status: up
  link failure count: 0
  permanent MAC addr: 50:00:00:03:00:01
  LACP state: established
  actor state: ASAIEE
  actor port number/key/priority: 1 33 255
  partner state: ASAIEE
  partner port number/key/priority: 1 1 32768
  partner system: 36864 aa:bb:cc:80:a0:00
  aggregator ID: 1
  speed/duplex: 10000 1
  RX state: CURRENT 6
  MUX state: COLLECTING_DISTRIBUTING 4

slave: port10
  index: 1
  link status: up
  link failure count: 0
  permanent MAC addr: 50:00:00:03:00:03
  LACP state: established
  actor state: ASAIEE
  actor port number/key/priority: 2 33 255
  partner state: ASAIEE
  partner port number/key/priority: 2 1 32768
  partner system: 36864 aa:bb:cc:80:a0:00
  aggregator ID: 1
  speed/duplex: 10000 1
  RX state: CURRENT 6
  MUX state: COLLECTING_DISTRIBUTING 4
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

软交换配置

功能说明

软交换口是将防火墙的多个3层接口，通过软件的方式，组成一个2层交换接口。 当FortiGate的每个口都为3层路由接口时，可以将其中的接口组成软件交换接口。

VLAN/Hardware与Software Switch的区别

功能	VLAN/Hardware switch	Software switch
转发	数据包由设备硬件交换机或SPU在硬件层面处理	数据包由CPU处理
STP	支持	不支持
无线SSIDs	不支持	支持
交换接口互访	默认允许	默认允许，可以通过策略控制

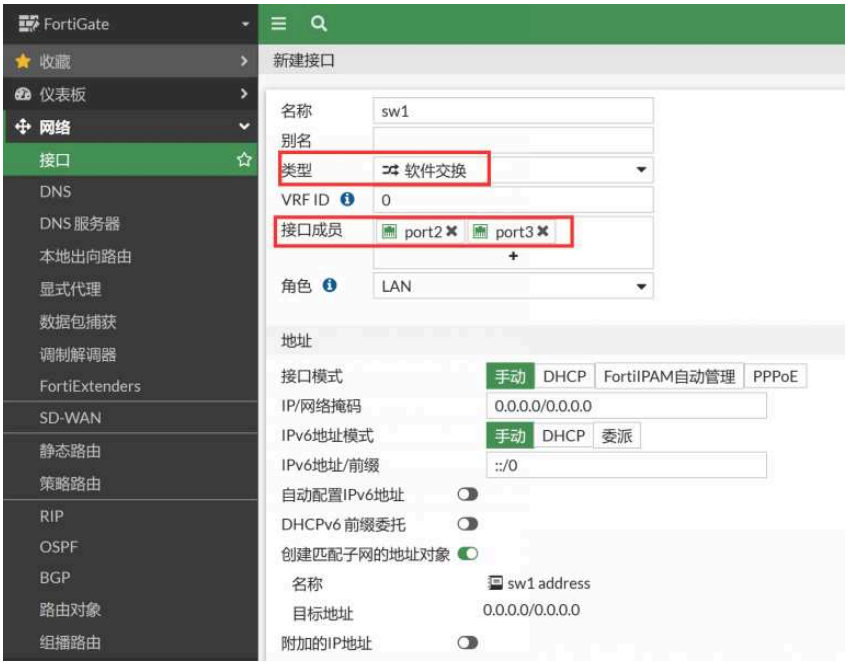
功能配置

1. 添加聚合接口，进入网络→接口，新建接口。



2. 类型选择软件交换，选择物理接口成员。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

建议在不需要的情况下关闭接口配置下的“设备探测”（Device detection）功能，该功能用于MAC地址厂商设备信息识别及MAC地址过滤，会消耗较多的设备资源，可能导致流量无法被芯片加速。

3. 接口配置页面查看建立的软交换口。



4. 在命令行查看软交换接口的配置。

```
FortiGate # show full-configuration system switch-interface sw1
config system switch-interface
    edit "sw1"
        set vdom "root"
        set member "port2" "port3"
        set type switch
        set intra-switch-policy implicit
        set mac-ttl 300
        set span disable
    next
end
```

注意事项

1. 软交换口是通过软件的方式模拟出的，需要由CPU处理，无法被芯片加速，会影响系统的性能，谨慎使用。（部分型号的设备自带硬交换接口，支持硬件加速，如100F）。

2. 默认配置下，交换机内部的成员接口之间通信是放通的，可以通过如下命令修改为必须匹配防火墙策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # config sys switch-interface
FortiGate (switch-interface) # edit sw1
FortiGate (test) # set intra-switch-policy ?
implicit    Traffic between switch members is implicitly allowed.    //默认配置，成员之间的流量全部放通
explicit    Traffic between switch members must match firewall policies.    //根据配置的防火墙策略执行放通或拒绝动作
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VLAN/Hardware Switch

功能介绍

VLAN/Hardware Switch是一个虚拟交换机接口，它将不同的物理接口组合在一起，以便FortiGate可以将这些成员接口组合成单个接口。部分支持此接口的FortiGate型号有一个默认的硬件交换接口，称为internal或lan，VLAN/Hardware Switch可以被硬件级别的芯片支持。

连接到同一VLAN/Hardware Switch的接口，类似于位于同一广播域中的同一物理交换机上一样。接口成员可以从VLAN/Hardware Switch中移除并分配给另一个交换机或用作独立物理接口。

VLAN/Hardware与Software Switch的区别

功能	VLAN/Hardware switch	Software switch
转发	数据包由设备硬件交换机或SPU在硬件层面处理	数据包由CPU处理
STP	支持	不支持
无线SSIDs	不支持	支持
交换接口互访	默认允许	默认允许，可以通过策略控制

VLAN Switch与Hardware Switch的区别

1. 60F、80F、100F、200F等具有硬件交换模块的型号，通过内部硬件交换机创建的交换接口为VLAN Switch。这些型号的设备一般在默认配置下会存在一个名称为lan或Internal的VLAN Switch接口，交换接口成员默认包含硬件交换模块中的成员接口，这些接口可以从预置的交换接口中取出，变为普通物理口。

   重要

   具体型号与硬件结构请参考：

   https://docs.fortinet.com/document/fortigate/7.99.99/hardware-acceleration/366011/fortigate-np6xlite-architectures ↗

   https://docs.fortinet.com/document/fortigate/7.99.99/hardware-acceleration/112876/fortigate-np6-architectures ↗

2. 40F、300E、400E、1100E、2200E、3600E、3980E、400F、600F、1800F、2600F、3000F、4400F等具有硬件交换模块的型号，通过内部硬件交换机创建的交换接口为Hardware Switch。

   重要

   具体型号与硬件结构请参考：

   https://docs.fortinet.com/document/fortigate/7.99.99/hardware-acceleration/46115/fortigate-np7-architectures ↗

3. VLAN Switch接口可以直接在接口下配置VLAN ID，同时配置IP后，可以直接将VLAN Switch配置为VLAN Interface（携带VLAN Tag），实现接口成员同属于该VLAN Interface的效果，而无需在VLAN Switch接口上再配置VLAN接口，而Hardware Switch无法配置VLAN ID，想实现上述效果，必须在Hardware Switch上配置VLAN Interface。

4. 除此之外，VLAN Switch与Hardware Switch这两种交换接口在功能使用上没有差别。

配置VLAN/Hardware Switch

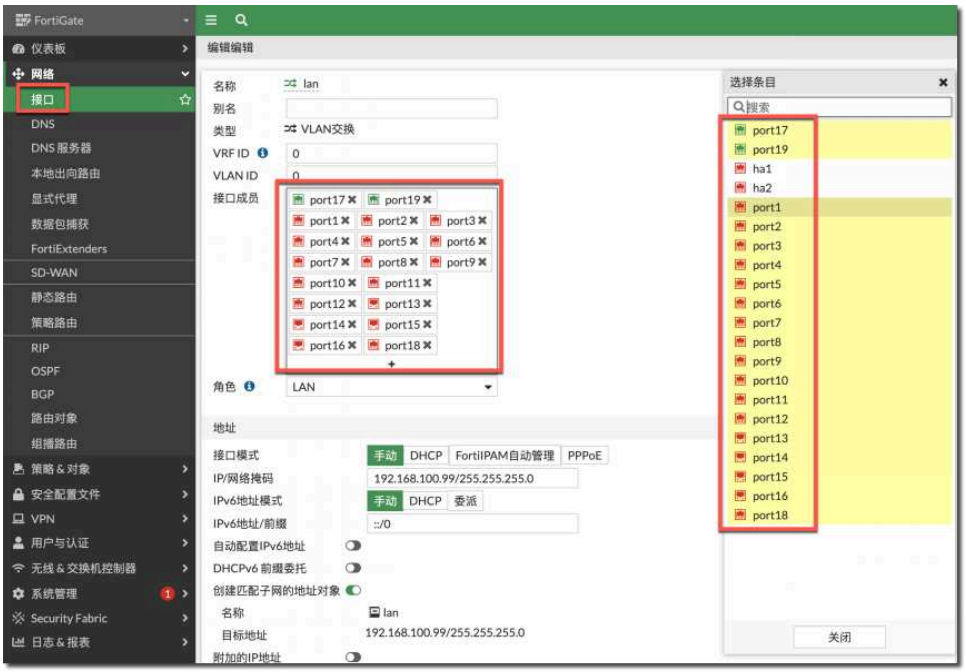
创建/编辑接口

1. 在SoC平台（如40F、60F、80F、100F、200F等）默认配置下会存在一个名称为lan或Internal的VLAN Switch接口，编辑该接口，交换接口成员默认包含硬件交换模块中的成员接口，这些接口可以从预置的交换接口中取出，变为普通物理口，也可将硬件交换模块的接口加入该交换接口，如下FortiGate101F所示。

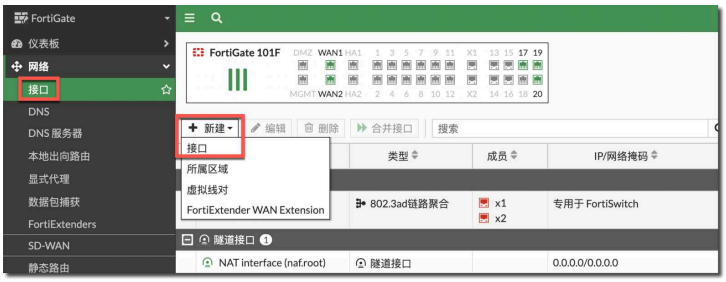
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

将物理口加入Switch接口时，接口需要清除IP地址（配置为0.0.0.0/0），且不能被其他功能引用。

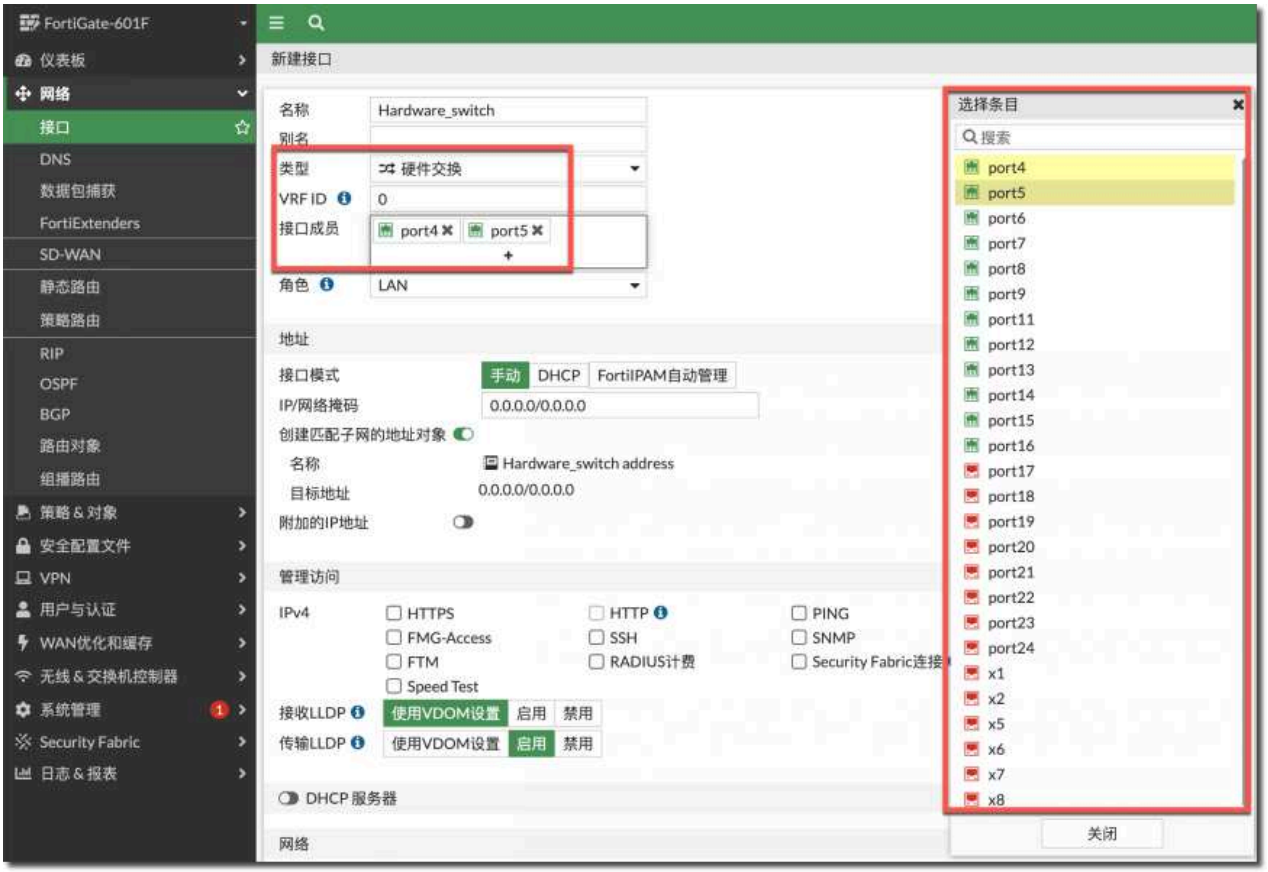


2. 创建新的VLAN/Hardware Switch，进入“网络→接口”页面，新建接口。



3. 选择类型为“VLAN交换/硬件交换”，如下图所示为FortiGate601F，交换接口为“硬件交换”，并添加或删除接口成员。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 通过CLI删除VLAN/Hardware Switch接口。

```
config system virtual-switch
    edit "internal"
        config port
            delete internal2
            delete internal7
            ...
        end
    next
end
```

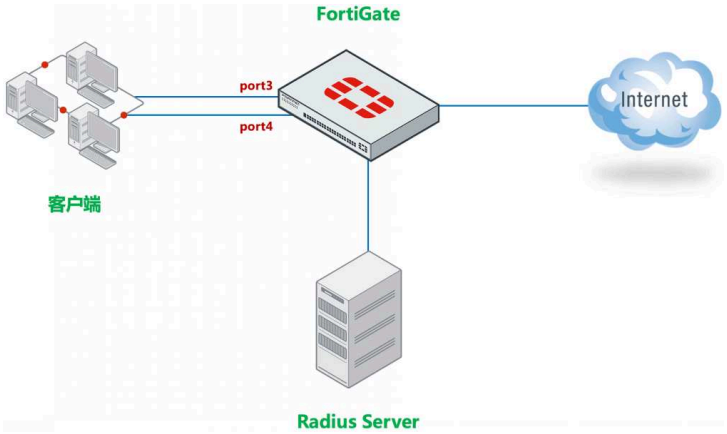
5. 通过CLI添加VLAN/Hardware Switch接口。

```
config system virtual-switch
    edit "internal"
        set physical-switch "sw0"
        config port
            edit "internal3"
            next
            edit "internal5"
            next
            edit "internal4"
            next
            edit "internal6"
            next
        end
    next
end
```

在VLAN/Hardware Switch上使用802.1X

网络拓扑

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



port3和port4是硬件交换模块的一部分，配置Hardware Switch，并将port3和port4加入，在该接口上执行802.1X身份验证。

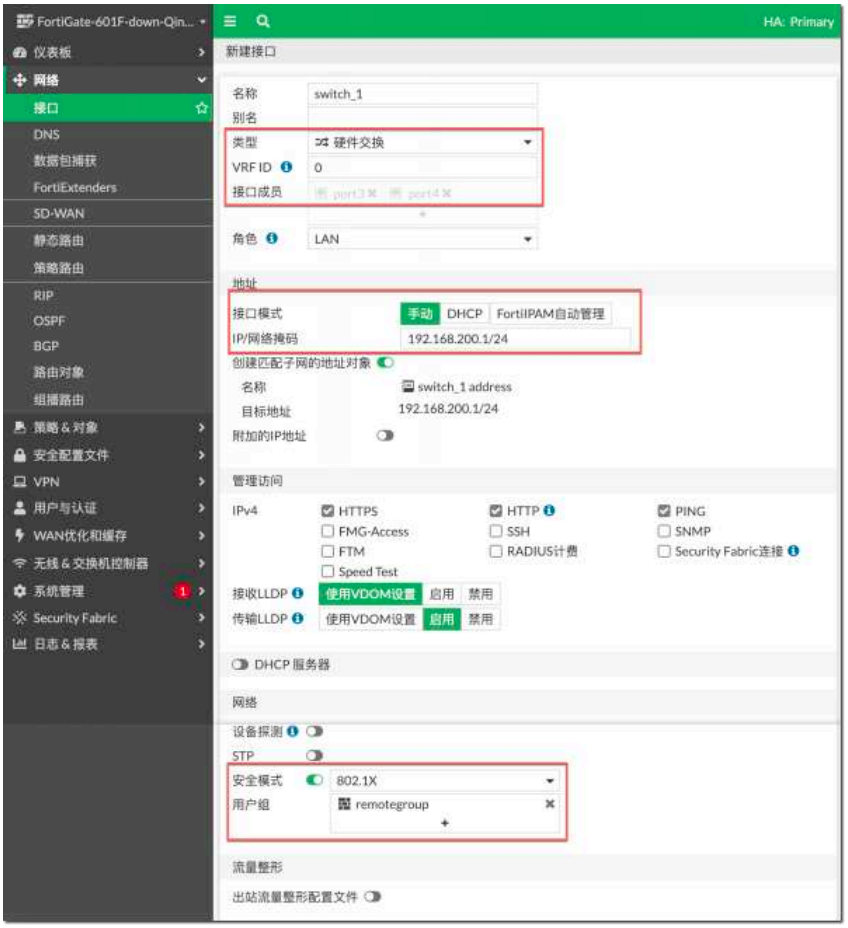
配置步骤

1. 在FortiGate上配置Radius服务器（配置方法参考用户与认证→Radius认证→Radius认证配置与排错↗章节）。
2. 在FortiGate上配置用于802.1X远程Radius认证的用户组（配置方法参考用户与认证→Radius认证→Radius认证配置与排错↗章节）。
3. 在FortiGate的“网络→接口”页面新建Hardware/VLAN Switch接口，将port3和port4加入该接口，对应CLI如下。

```
config system virtual-switch
    edit "switch_1"
        set physical-switch "sw0"
        config port
            edit "port3"
            next
            edit "port4"
            next
        end
    next
end
```

4. 在FortiGate上配置防火墙策略允许新建的Hardware/VLAN Switch下的流量访问Internet。
5. 在Hardware/VLAN Switch上开启802.1X认证，选择创建的Radius认证用户组。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "switch_1"
        set vdom "vdom1"
        set ip 192.168.200.1 255.255.255.0
        set allowaccess ping http https
        set type hard-switch
        set security-mode 802.1X
        set security-groups "remotegroup"
        set device-identification disable
        set role lan
    next
end
```

结果验证

1. 客户端通过port3或port4连接，并通过802.1X认证后，可以正常访问Internet。

2. 在FortiGate上查看802.1X认证端口状态。

```
FortiGate # diagnose sys 802-1x status

Virtual switch 'switch_1' (default mode) 802.1x member status:
  port3: Link up, 802.1X state: authorized
  port4: Link up, 802.1X state: unauthorized
```

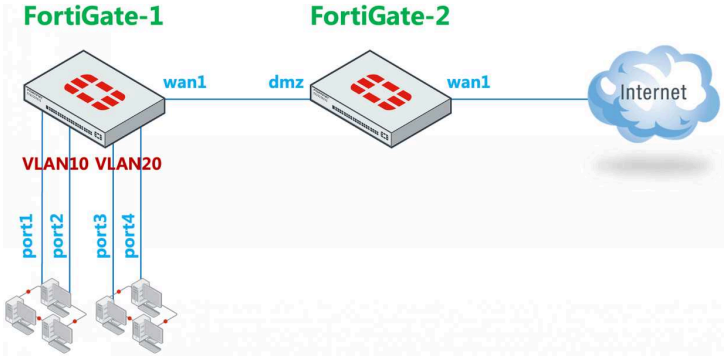
在VLAN/Hardware Switch传输带VLAN Tag的流量

网络需求

VLAN/Hardware Switch也可以让FortiGate像二层VLAN交换机一样工作，进行VLAN交换，并可以设置一个物理口作为Trunk接口。支持的型号如：60F、80F、100E、100F、140E、200F、300E、400E、1100E、1800F、2600F、3500F、4200F、4400F。

网络拓扑

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- FortiGate-1上有两个硬件交换机接口（port1、port2）被分配了VLAN 10，两个接口（port3、port4）被分配了VLAN 20。wan1接口被指定为Trunk端口，与上游的FortiGate-2相连。
- 上游FortiGate-2的子接口VLAN10和VLAN20允许FortiGate-1过来的带VLAN Tag 10和20的流量访问Internet。

配置步骤

基础配置

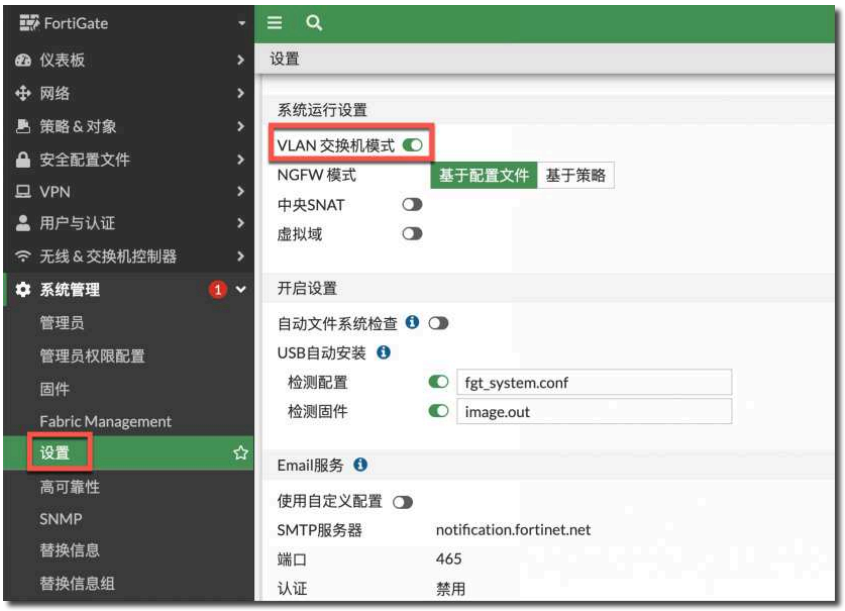
需要确保在“config sys global”下，“virtual-switch-vlan”选项处于“enable”状态。

```
config sys global
    set virtual-switch-vlan enable
end
```

FortiGate-1

1. 需要确保在“config sys global”下，“virtual-switch-vlan”选项处于“enable”状态；或在设备管理页面的“系统管理→设置→系统运行设置”中，“VLAN 交换机模式”选项处于开启状态。

```
config sys global
    set virtual-switch-vlan enable
end
```



2. 新建两个VLAN/Hardware Switch，分别配置VLAN ID为10和20，分别添加成员port1、port2和port3、port4。

```
config system virtual-switch
    edit "VLAN10"
        set physical-switch "sw0"
        set vlan 10
        config port
            edit "port1"
            next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            edit "port2"
            next
        end
    next
    edit "VLAN20"
        set physical-switch "sw0"
        set vlan 20
        config port
            edit "port3"
            next
            edit "port4"
            next
        end
    next
end
```

3. 配置两个VLAN/Hardware Switch接口的IP地址。

```
config system interface
    edit "VLAN10"
        set vdom "root"
        set ip 192.168.10.99 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type hard-switch
    next
    edit "VLAN20"
        set vdom "root"
        set ip 192.168.20.99 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type hard-switch
    next
end
```

4. 配置wan1接口为Trunk口，承载VLAN10和VLAN20的流量。

```
config system interface
    edit wan1
        set trunk enable
    next
end
```

FortiGate-2

1. 新建VLAN子接口VLAN10和VLAN20，并配置IP地址。

```
config system interface
    edit "VLAN10"
        set ip 192.168.10.98 255.255.255.0
        set allowaccess ping https ssh
        set role lan
        set interface "dmz"
        set vlanid 10
    next
    edit "VLAN20"
        set ip 192.168.20.98 255.255.255.0
        set allowaccess ping https ssh
        set role lan
        set interface "dmz"
        set vlanid 20
    next
end
```

2. 在VLAN10和VLAN20接口上分别配置DHCP服务器，分别为VLAN10和VLAN20的客户端分配IP地址。

```
config system dhcp server
    edit 0
        set dns-service default
        set default-gateway 192.168.10.98
        set netmask 255.255.255.0
        set interface "VLAN10"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        config ip-range
            edit 1
                set start-ip 192.168.10.100
                set end-ip 192.168.10.254
            next
        end
        set timezone-option default
    next
        edit 0
        set dns-service default
        set default-gateway 192.168.20.98
        set netmask 255.255.255.0
        set interface "VLAN20"
        config ip-range
            edit 1
                set start-ip 192.168.20.100
                set end-ip 192.168.20.254
            next
        end
        set timezone-option default
    next
end
```

3. 配置防火墙策略允许VLAN10和VLAN20的流量访问Internet。

```
config firewall policy
    edit 0
        set name "VLAN10-out"
        set srcintf "VLAN10"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 0
        set name "VLAN20-out"
        set srcintf "VLAN20"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

结果验证

1. FortiGate-1下VLAN 10和VLAN 20的PC均可以通过FortiGate-2分别获取到VLAN10和VLAN20分配的IP地址。
2. FortiGate-1下VLAN 10和VLAN 20的PC均可以Ping通FortiGate-1的VLAN/Hardware Switch接口IP。
3. FortiGate-1下VLAN 10和VLAN 20的PC均可以Ping通FortiGate-2的VLAN子接口IP。
4. FortiGate-1下VLAN 10和VLAN 20的PC均可以正常访问Internet，流量在FortiGate-1和FortiGate-2之间携带对应的VLAN Tag。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

交换接口的MAC地址表

网络需求

通过执行ARP表项显示命令可以查看与FortiGate相邻的所有设备的MAC地址表。

```bash
FortiGate # get system arp
Address           Age(min)   Hardware Addr      Interface
10.10.12.1        0          00:09:0f:09:07:07 wan1
192.168.100.77    0          00:e0:4c:b9:97:7c LAN
192.168.100.177   0          0c:37:96:06:d7:5d LAN
```

但该命令无法显示设备连接到交换接口的具体哪个成员接口，此时需要查看Hardware/Software交换接口的成员接口所连接设备的MAC表。

查看方法

1. 例如一个软交换接口的配置如下，名称为LAN。

```bash
config system switch-interface
    edit "LAN"
        set vdom "root"
        set member "port2" "port3" "port4" "port5"
    next
end
```

2. 如果想知道连接到了这个软交换接口的成员接口的设备MAC，可执行如下命令，可以看到00:41:72:74:1e:01（192.168.120.2）连接到软件交换接口的port2，00:41:74:6c:11:01（192.168.120.3）连接到port3。

> **重要**
>
> 只支持Hardware/Software交换接口，VLAN交换接口无法查看。

```bash
FortiGate # diagnose netlink brctl name host LAN
show bridge control interface LAN host.
fdb: hash size=32768, used=6, num=6, depth=1, gc_time=4, ageing_time=3, simple=switch
Bridge LAN host table
port  no     device  devname mac addr      ttl     attributes
  1    4      port2   00:41:72:74:1e:01     30      Hit(30)
  2    5      port3   00:41:74:6c:11:01      7      Hit(7)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

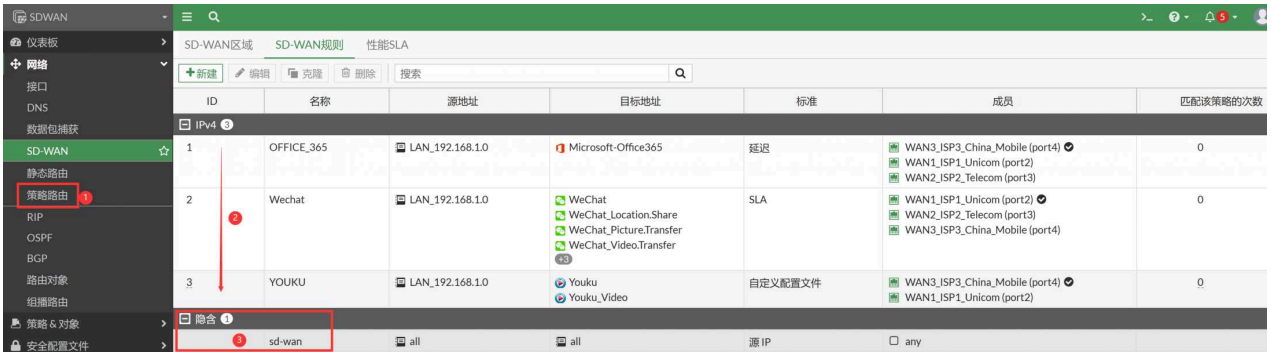
SD-WAN数据转发逻辑

SD-WAN规则介绍

1. SD-WAN 规则 = 策略路由 (PBR)，但是同时SD-WAN rule规则又比策略路由的优先级低一些。



2. SD-WAN 规则和策略路由一样，也是从上往下按照顺序匹配，可以按照特定的算法将指定的数据流转发到相应的出接口上。



3. 在命令行下查看SDWAN规则在策略路由中的条目，SD-WAN规则本质为策略路由（ID>7f000001），优先级高于普通FIB路由。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2131230721(0x7f080001) vwl_service=1(OFFICE_365) vwl_mbr_seq=3 1 2 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=6(port4) oif=4(port2) oif=5(port3)
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Office365(327782,0,0,0)
hit_count=0 last_used=2023-01-02 22:15:18

id=2131230722(0x7f080002) vwl_service=2(Wechat) vwl_mbr_seq=1 2 3 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=4(port2) oif=5(port3) oif=6(port4)
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(7): WeChat(4294838375,0,0,0, 33760) WeChat_Location.Share(4294838376,0,0,0, 36743)
WeChat_Picture.Transfer(4294838377,0,0,0, 36730) WeChat_Video.Transfer(4294838378,0,0,0, 36741)
WeChat_Voice.Chat(4294838379,0,0,0, 36742) WeChat_Voip.Call(4294838380,0,0,0, 36648) WeChat_Web(4294838381,0,0,0,
39523)
hit_count=0 last_used=2023-01-02 22:17:55

id=2131230723(0x7f080003) vwl_service=3(YOUKU) vwl_mbr_seq=3 1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00
protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(2) oif=6(port4) oif=4(port2)
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(2): Youku(4294838550,0,0,0, 16531) Youku_Video(4294838551,0,0,0, 35285)
hit_count=0 last_used=2023-01-02 22:20:41
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. SD-WAN规则的最后面存在一条垫底的默认隐含规则，实际的作用就是当没有匹配到上面SD-WAN规则的数据时，最终将会匹配到这条隐含的规则，隐含规则的本质就是普通的FIB路由表。也就说没有匹配SD-WAN规则的数据将会匹配普通路由表进行转发。

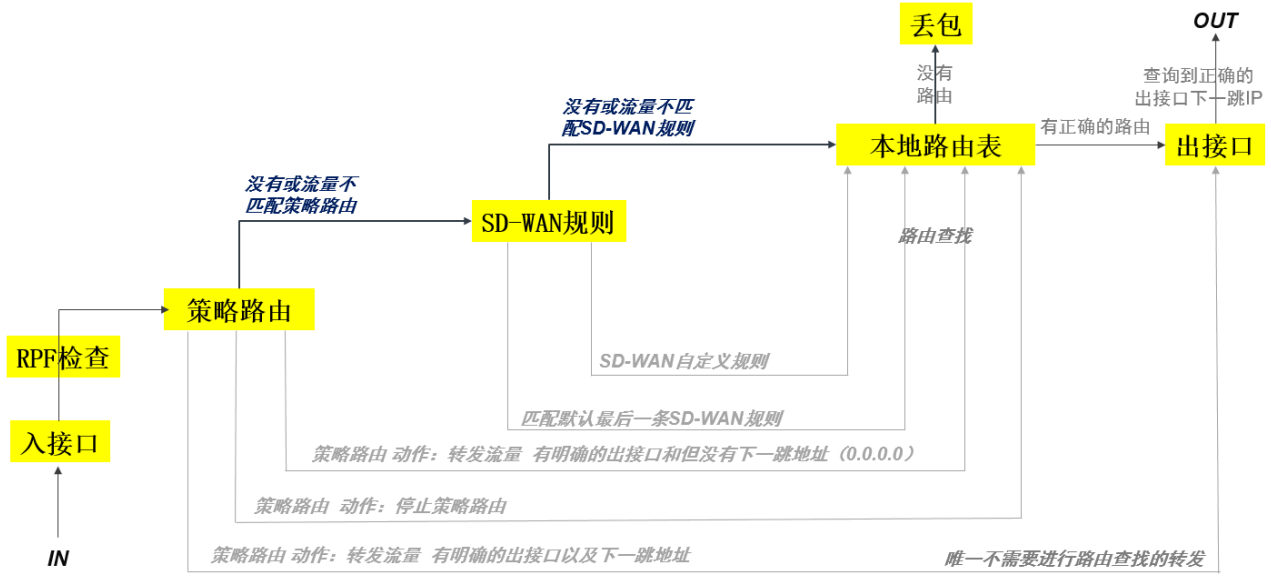


5. 没有匹配SD-WAN规则的数据流将查询路由表，在port2/port3/Port13三条默认路由出口上进行负载均衡（默认按源IP方式负载流量）。

```
SDWAN # get router info kernel
 ...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→0.0.0.0/0 pref=0.0.0.0
        gwy=101.100.1.192 flag=04 hops=0 oif=5(port3)
        gwy=111.100.1.192 flag=04 hops=0 oif=6(port4)
        gwy=202.100.1.192 flag=04 hops=0 oif=4(port2)
 ...

SDWAN # get router info routing-table  all
 ...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
 ...
```

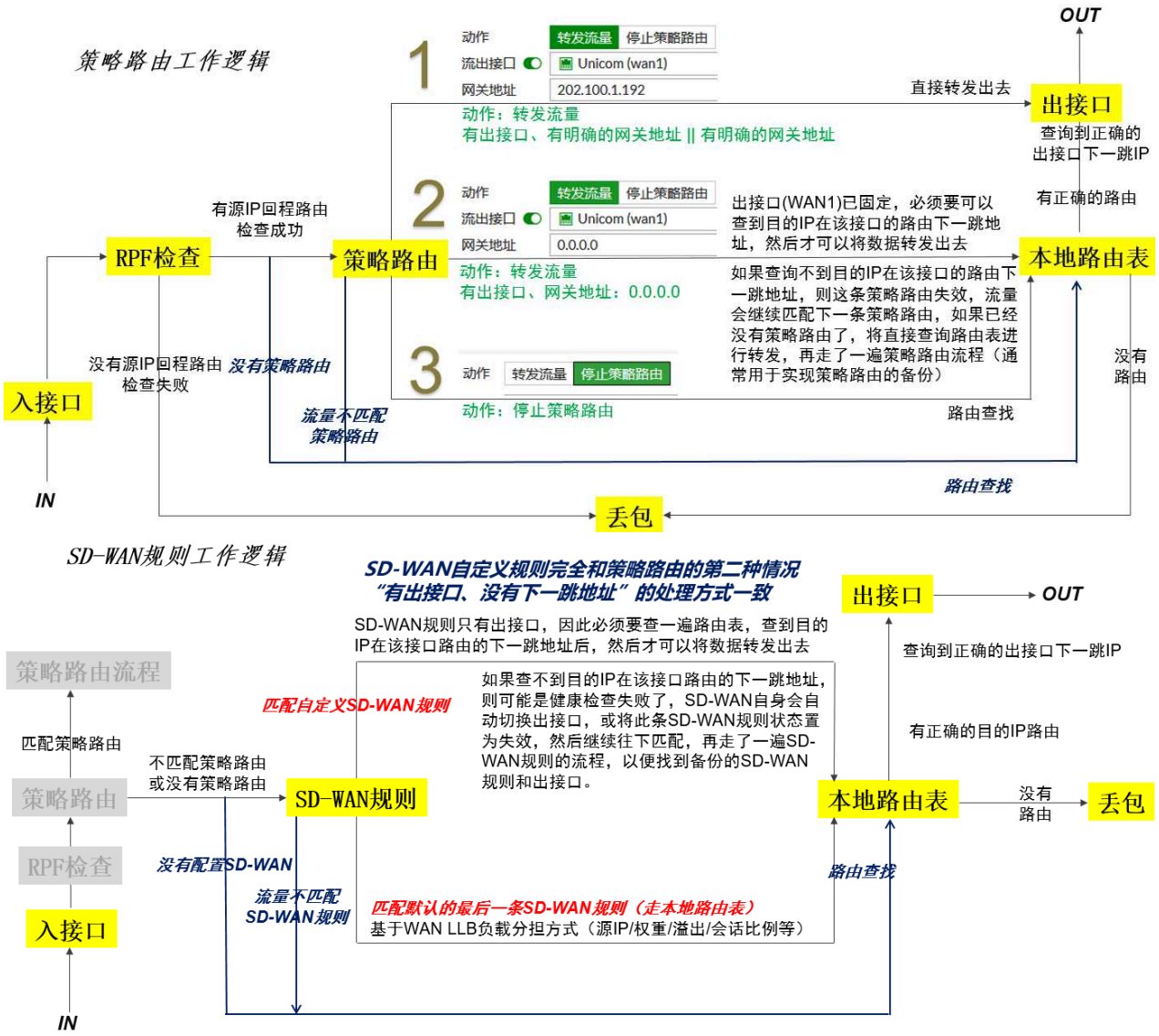
SDWAN工作流程

1. 策略路由、SD-WAN规则、本地路由表的查找与转发逻辑关系：策略路由→SD-WAN规则→本地路由。



2. 对比策略路由和SD-WAN规则的工作过程（二者有细微的差别，大部分情况下很相似）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

- 默认配置下（在config system sdwan → config service → edit X下，set gateway disable + set default disable），在流量匹配SD-WAN规则后，被SD-WAN规则执行动作前，会查找FIB表项（get router info kernel）：
- 如果最佳路由的出接口不是SD-WAN成员，则忽略SD-WAN规则，直接路由转发。
- 如果目标地址属于直连路由，则忽略SD-WAN规则，直接路由转发。
- 如果最佳路由出接口是SD-WAN成员，则通过该SD-WAN规则找到最佳的出接口转发。
- 开启gateway和default后（在config system sdwan → config service → edit X下，set gateway enable + set default enable），则跳过FIB路由查找，直接被SD-WAN规则转发。

SDWAN规则

1. SD-WAN规则分成两种：
   - 手动自定义的SD-WAN规则：低优先级的策略路由（优先级比普通策略路由低），手工添加的SD-WAN规则则类似支持多出口的动态选择、支持应用控制、支持路由属性等的增强版策略路由，其转发优先级比普通策略路由低，比普通路由优先级高。
   - 最后一条默认的SD-WAN规则：依据LLB的负载方式查询本地静态路由（默认源IP负载），LLB负载支持源IP负载、溢出、会话权重负载、源目IP负载等多种方式，就是旧版本中的WAN LLB功能。
2. 手工自定义配置的SD-WAN规则相当于是一条只配置了出接口但没有配置下一跳地址（下一跳地址为0.0.0.0）的策略路由，因此必须要再次查询一遍路由表才可以找到正确的下一跳地址，如果无法查找到该接口的下一跳地址，自定义的SD-WAN规则也将失效，由此可见SD-WAN规则十分依赖FIB路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Debug Flow自定义SD-WAN规则的流量转发过程：

```
diagnose sys session filter proto 1
diagnose sys session filter dst 114.114.114.114
diagnose sys session clear
diagnose debug flow filter addr 114.114.114.114
diagnose debug flow filter proto 1
diagnose debug flow show function-name enable
diagnose debug flow trace start 10
diagnose debug enable
```

```
config system virtual-wan-link
    config service
        edit 2
            set name "114.114.114.114_OUT"
            set mode priority
            set dst "HOST_114.114.114.114"
            set health-check "Unicom"
            set priority-members 1 (WAN1)
        next
```

先match policy routing 找到出接口 via ifindex-7（WAN1）

然后再 find a route 找到下一跳地址 gw-202.100.1.192

```
# id=20085 trace_id=11 func=print_pkt_detail line=5320 msg="vd-root:0 received a packet(proto=1, 10.193.1.79:512-
>114.114.114.114:2048) from lan. type=8, code=0, id=512, seq=49585."
id=20085 trace_id=11 func=init_ip_session_common line=5480 msg="allocate a new session-00382b05"
id=20085 trace_id=11 func=vf_ip_route_input_common line=2578 msg="Match policy routing: to 114.114.114.114 via ifindex-7"
id=20085 trace_id=11 func=vf_ip_route_input_common line=2590 msg="find a route: flag=04000000 gw-202.100.1.192 via wan1"
id=20085 trace_id=11 func=fw_forward_handler line=749 msg="Allowed by Policy-1: SNAT"
id=20085 trace_id=11 func=ids_receive line=282 msg="send to ips"
id=20085 trace_id=11 func=__ip_session_run_tuple line=3226 msg="SNAT 10.193.1.79->202.100.1.25:60928"
id=20085 trace_id=12 func=print_pkt_detail line=5320 msg="vd-root:0 received a packet(proto=1, 114.114.114.114:60928-
>202.100.1.25:0) from wan1. type=0, code=0, id=60928, seq=49585."
id=20085 trace_id=12 func=resolve_ip_tuple_fast line=5395 msg="Find an existing session, id-00382b05, reply direction"
id=20085 trace_id=12 func=__ip_session_run_tuple line=3240 msg="DNAT 202.100.1.25:0->10.193.1.79:512"
id=20085 trace_id=12 func=vf_ip_route_input_common line=2590 msg="find a route: flag=00000000 gw-10.193.1.79 via lan"
id=20085 trace_id=12 func=ids_receive line=282 msg="send to ips"
```

3. SD-WAN规则这样的处理方式，带来的最大的好处是可以实现SD-WAN出口故障的快速切换，SD-WAN的健康检查完全依赖于这种处理方式。一旦健康检查失败，出接口的静态路由将会消失，SD-WAN将无法在路由表中查找到下一跳地址，因此相应的SD-WAN规则也跟随着会失效，从而实现了SD-WAN的多出口故障的自动切换。

> **重要**
>
> SD-WAN的路由必不可少，否则SD-WAN规则将无法使用。

4. 必须要配置的内容：手工配置默认路由或明细路由指向SD-WAN出口（默认源IP负载），或者使用动态路由协议（OSPF/BGP/RIP）学习到相应的路由，总之路由表中一定要有去往SD-WAN规则中的目的IP的路由才可以。

5. 可以根据需要配置到具体port2/port3/port4分别的路由，也可以直接配置指向SD-WAN接口的路由。



（网关在静态路由中配置）

或：



（网关在SDWAN成员中配置）

6. 如果SD-WAN是针对去往Internet的负载：则必须配置默认路由指向SD-WAN；如果SD-WAN是针对去往VPN业务网段的负载：则必须配置VPN明细路由指向SD-WAN。默认情况下路由表中需要存在SD-WAN接口的路由，这样SD-WAN规则才可以生效。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 总结来看：默认情况下， SD-WAN规则由于只能选择出接口而无法直接配置下一跳的IP地址（策略路由可以配置出接口和下一跳IP），因此需要继续通过FIB路由表的查询以便找到正确的下一跳IP地址，才可以将数据转发出去，可以看出SD-WAN规则十分的依赖路由转发表，几乎SD-WAN规则就是依赖FIB路由表而工作的，二者是相互依存的关系。

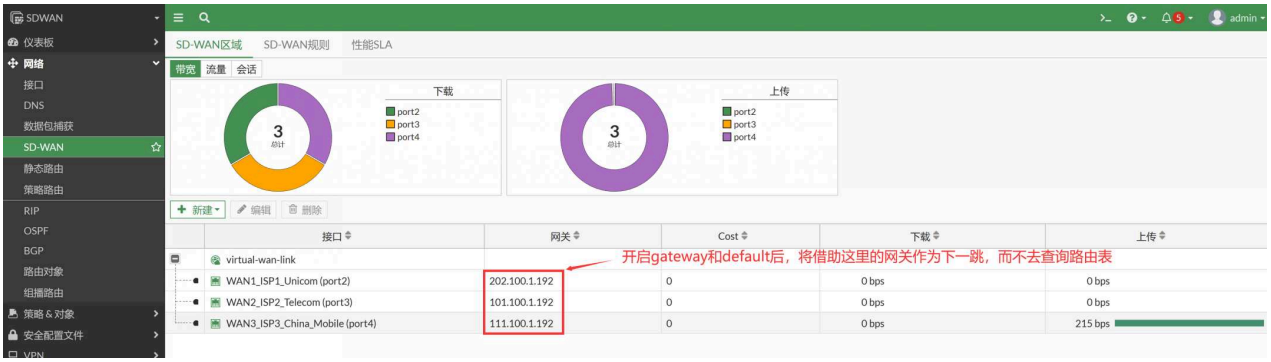
8. 那么是否可以打破这样的依赖关系呢？是否可以和策略路由一样，SD-WAN规则也可以有一个明确的出接口和下一跳IP，而不需要依赖FIB路由表而找到下一跳IP呢？答案是：有的，虽然我们不推荐这样做，这样不利于多出接口的快速切换。具体的做法如下：

```
SDWAN # config system sdwan
SDWAN (sdwan) # config members
SDWAN (members) # show
config members
    edit 1
        set interface "port2"
        set gateway 202.100.1.192
    next
    edit 2
        set interface "port3"
        set gateway 101.100.1.192
    next
    edit 3
        set interface "port4"
        set gateway 111.100.1.192
    next
end
SDWAN (members) # end

SDWAN (sdwan) # config service
SDWAN (service) # edit 1
SDWAN (1) # show full-configuration
config service
    edit 1
        set name "OFFICE_365"
        set addr-mode ipv4
        set input-device-negate disable
        set mode priority
        set role standalone
        set standalone-action disable
        set tos 0x00
        set tos-mask 0x00
        set src "LAN_192.168.1.0"
        set src-negate disable
        set internet-service enable
        set internet-service-name "Microsoft-Office365"
        set health-check "Default_DNS"
        set link-cost-factor latency
        set link-cost-threshold 10
        set hold-down-time 0
        set dscp-forward disable
        set dscp-reverse disable
        set priority-members 3 1 2
        set status enable
        **set gateway disable**
        **set default disable**
        set tie-break zone
        set use-shortcut-sla enable
        set passive-measurement disable
    next
end
```

如果将SD-WAN规则下面的gateway和default默认状态有disable改成enable，则SD-WAN规则将跳过FIB的查询，直接选择members接口里面配置的下一跳IP作为SDWAN规则（策略路由）的下一跳IP，直接转发流量，而不再查询FIB路由表了。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # config system sdwan
SDWAN (sdwan) # config service
SDWAN (service) # edit 1
SDWAN (1) # set gateway enable
SDWAN (1) # set default enable
SDWAN (1) # end
SDWAN (sdwan) # end
```



重要

这种使用场景比较特别，需要将SD-WAN流量固定地从某个出口和下一跳IP转发，而不受到底层FIB路由表路由切换的影响（健康检查切换/link-monitor等等），这种使用场景比较少用到。

9. 默认配置下，本机发出的报文不受SDWAN规则的影响。

总结

1. SD-WAN规则可以认为是调用了多个有序出接口（oif）列表的策略路由，但是优先级比普通的策略路由要低一些，oif在策略路由中从左（最优先）到右（最不优先）进行排序。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2098397185(0x7d130001) vwl_service=1(OFFICE_365) vwl_mbr_seq=3 1 2 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=6(port4) gwy=111.100.1.192
oif=4(port2) gwy=202.100.1.192 oif=5(port3) gwy=101.100.1.192 default
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Office365(327782,0,0,0)
hit_count=0 last_used=2023-01-02 23:10:21
```

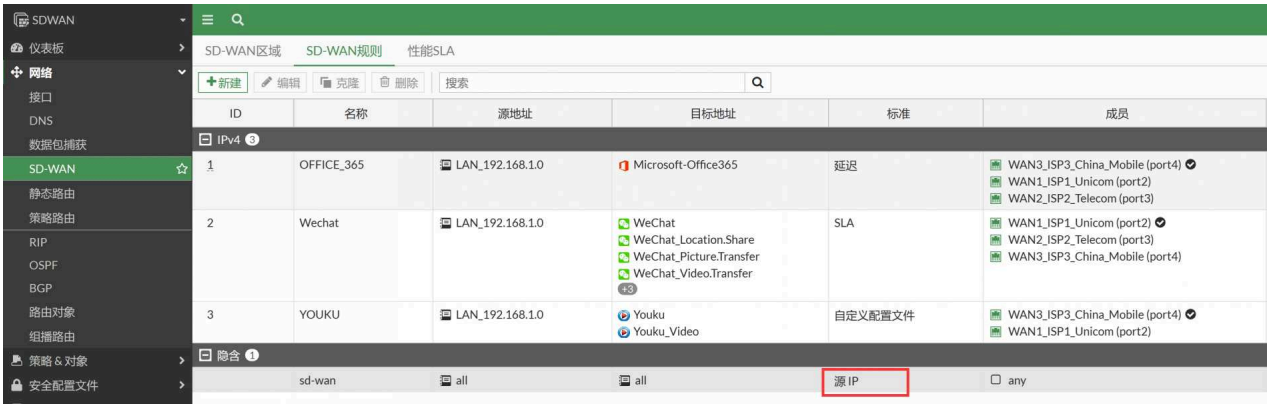
2. SD-WAN规则的类别（Best Quality, Lowest Cost, Maximize Bandwidth）决定了当SLA检查值（延迟、抖动、丢失）发生变化时，接口列表中的出接口（oif）顺序是如何变化的。

3. 默认情况下，FIB路由表中必须有去往目的IP的路由，这样SD-WAN规则才可以生效，SD-WAN规则的出接口的下一跳是通过FIB路由表查询获取的，因此SD-WAN目的网段的路由非常重要。

```
SDWAN # get router info routing-table  all
 ...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
 ...
```

4. 如果没有匹配的SD-WAN的策略路由，则路由的决策会基于FIB进行查找（默认是源IP方式的ECMP）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
# config system sdwan
# set load-balance-mode ?
source-ip-based          Source IP load balancing. All traffic from a source IP is sent to the same interface.

weight-based             Weight-based load balancing. Interfaces with higher weights have higher priority and get
more traffic.

usage-based              Usage-based load balancing. All traffic is sent to the first interface on the list. When
the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.

source-dest-ip-based     Source and destination IP load balancing. All traffic from a source IP to a destination
IP is sent to the same interface.

measured-volume-based    Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes).
More traffic is sent to interfaces with higher volume ratios.
```

5. 路由（或SD-WAN转发顺序）发生改变后（比如出接口列表重新排序、健康检查失败触发、动态路由协议更新），会话将重新上送CPU进行匹配处理，重新查询策略和路由，这样流量可能会迁移到另一个SD-WAN成员接口上（具体详见网络管理→SD-WAN→SD-WAN介绍→SD-WAN健康状态检查↗章节）。

6. 有NAT的会话的流量不会随着路由的变化而改变流量的出接口（默认情况下），只有纯三层的流量转发才会正常的进行出接口切换，如下命令行决定了以上特性。

> **重要**
>
> 默认配置下的SNAT场景，即使转发流量的SD-WAN成员的健康检查变为dead，只要该线路仍然存在路由（可能关闭了`update-static-route`），已有的旧会话仍然不会切换到其他线路。

```
SDWAN # config system global
SDWAN (global) # show full-configuration | grep snat
    set snat-route-change disable
```

7. 没有NAT的流量，在接口下设置会话保持（preserve-session-route）可以允许在路由更改后强制将会话保持在同一个sd-wan成员上，不跟随这出接口的变化而变化已有流量会话的出接口信息。

```
SDWAN # config system interface
SDWAN (interface) # edit port2
SDWAN (port2) # set preserve-session-route enable
SDWAN (port2) # end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SD-WAN接口成员组

静态IP接口成员配置

1. 进入网络→SD-WAN→SD-WAN区域，选择默认的SD-WAN区域（virtual-wan-link）或新建SD-WAN区域。

2. 点击新建→SD-WAN成员，将想要加入SD-WAN成员的接口依次加入SD-WAN区域。



3. 对应CLI：

```
SDWAN # config system sdwan
SDWAN (sdwan) # config members
SDWAN (members) # show
config members
    edit 1
        set interface "port2"
        set zone "virtual-wan-link"
        set gateway 202.100.1.192
        set source 0.0.0.0
        set gateway6 ::
        set source6 ::
        set cost 0
        set priority 1
        set priority6 1024
        set status enable
        set comment ''
    next
    edit 2
        set interface "port3"
        set zone "virtual-wan-link"
        set gateway 101.100.1.192
        set source 0.0.0.0
        set gateway6 ::
        set source6 ::
        set cost 0
        set priority 1
        set priority6 1024
        set status enable
        set comment ''
    next
    edit 3
        set interface "port4"
        set zone "virtual-wan-link"
        set gateway 111.100.1.192
        set source 0.0.0.0
        set gateway6 ::
        set source6 ::
        set cost 0
        set priority 1
```

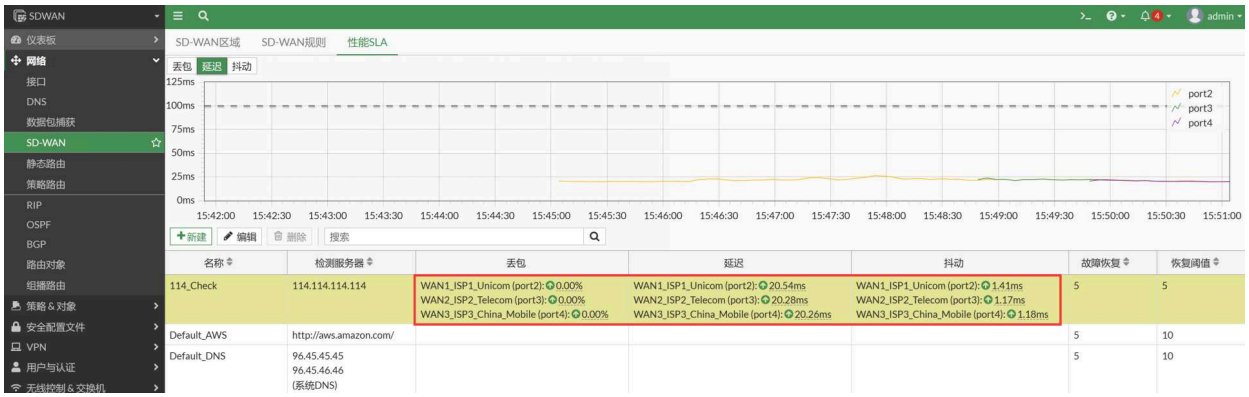

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set priority6 1024
        set status enable
        set comment ''
    next
end
```

参数说明

1. set gateway 202.100.1.192：

- 作用1：这个参数会被用在SD-WAN健康检查目的IP的下一跳地址，比如我们检测114.114.114.114的SD-WAN健康检查，实际后台会在内核下发去往114.114.114.114的明细路由，以便port2/port3/Port13可以各自发起去往114.114.114.114的探测报文。




```
SDWAN # get router info kernel | grep 114.114.114.114
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 111.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=111.100.1.192 dev=6(port4)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 101.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=101.100.1.192 dev=5(port3)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 202.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=202.100.1.192 dev=4(port2)

# get router info routing-table  all | grep 114.114.114.114
```

路由表是看不到114.114.114.114的路由的，而这个kernel路由的gwy地址就是在sd-wan接口成员组中所配置的gateway所得来的。

- 作用2：配置SD-WAN的路由的时候，也会借用SD-WAN接口组的网关作为SD-WAN路由的下一跳IP。



对应CLI：

```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

静态路由借用下一跳SD-WAN接口成员组里下一跳IP的效果：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
...
```

动态IP接口成员配置

1. 如果是PPPOE/DHCP这种动态接口，在SD-WAN接口组的时候，通常需要保持set gateway 0.0.0.0，SD-WAN的路由会自动去查找到PPPOE/DHCP接口的动态的默认网关IP地址。



2. SD-WAN接口成员中的PPPOE接口网关配置为动态，由于PPPOE接口下面的默认参数：defaultgw为enable状态，因此SD-WAN接口成员里面会自动去迭代查询到PPPOE默认路由的真实下一跳IP地址。

```
SDWAN # config system interface
SDWAN (interface) # edit PPPOE1_DR_PENG
SDWAN (PPPOE1_DR_PENG) # show
config system interface
    edit "PPPOE1_DR_PENG"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set snmp-index 13
        set interface "port5"
    next
end

SDWAN (PPPOE1_DR_PENG) # show full-configuration | grep default
        set defaultgw enable    //默认为enable状态
```

3. 效果：SD-WAN健康检查的内核路由下发会找到PPP接口默认路由的真实下一跳IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # get router info kernel  | grep 114.114.114.114
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 114.100.1.204/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=114.100.1.196 dev=19(PPP)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 111.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=111.100.1.192 dev=6(port4)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 101.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=101.100.1.192 dev=5(port3)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 202.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=202.100.1.192 dev=4(port2)
```

4. SD-WAN PPPOE接口的静态路由也会自动找到PPP接口默认路由的真实下一跳IP。

```
SDWAN # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
...
```

5. 补充：PPPOE接口的推荐配置方式（只能命令行配置）。

```
config system pppoe-interface
    edit "PPPOE1_DR_PENG"
        set device "port5"
        set username "test"
        set password ENC
yPSGPPFbTeo7o9/FjjzgRe9vBUUkYXXXHxKlvsLj3Gk9cgS88ik8ifl5yhclIvjJ0XRAJGW5A4PqL3nczbmg/FgLTJCad4OmtjBuly1fjdwcdODr=
    next
end
```

然后会自动产生“PPPOE1_DR_PENG”接口：

```
config system interface
    edit "PPPOE1_DR_PENG"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set snmp-index 13
        set interface "port5"
    next
end

SDWAN (PPPOE1_DR_PENG) # show full-configuration | grep def
        set defaultgw enable
```



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

参数说明

1. `set source 0.0.0.0`：SD-WAN健康监控的源IP会借用set source里面设置的IP，默认为0.0.0.0，则是选择SD-WAN接口的主IP作为源IP进行发送健康检查探测报文。

> **重要**
>
> IPsec VPN隧道、GRE隧道等VPN接口默认情况下接口是没有IP地址的，进行SD-WAN健康监控探测的时候默认是没有办法发送探测报文的，这种情况下监控检测会失败的。
>
> 解决办法：
>
> - 给VPN隧道接口配置上IP地址（推荐）。
> - 在SD-WAN接口成员配置的时候，命令行添加 set source ip，手工给没有IP的隧道指定一个IP地址，用于sd-wan监控检测发送探测包的源IP地址。

2. `set cost 0`：用在 “Lowest Cost & Maximize Bandwidth (SLA) rules”里面。用于SD-WAN算法中的出接口选择使用。具体可见网络管理→SD-WAN→SD-WAN介绍→SD-WAN健康状态检查章节。

3. `set priority 0`：和静态路由中的priority参数一致，用于浮动静态路由时候，让备份的路由也存在于路由表，但是不用于出接口流量的路由转发，效果如下：

```
SDWAN # config system sdwan
SDWAN (sdwan) # config members
SDWAN (members) # show
config members
    edit 1
        set interface "port2"
        set gateway 202.100.1.192
    next
    edit 2
        set interface "port3"
        set gateway 101.100.1.192
    next
    edit 3
        set interface "port4"
        set gateway 111.100.1.192
    next
    edit 4
        set interface "PPPOE1_DR_PENG"
    next
end

SDWAN (members) # edit 2
SDWAN (2) # set priority 100
SDWAN (2) # next

SDWAN (members) # show
config members
    edit 1
        set interface "port2"
        set gateway 202.100.1.192
    next
    edit 2
        set interface "port3"
        set gateway 101.100.1.192
        set priority 100
    next
    edit 3
        set interface "port4"
        set gateway 111.100.1.192
    next
    edit 4
        set interface "PPPOE1_DR_PENG"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

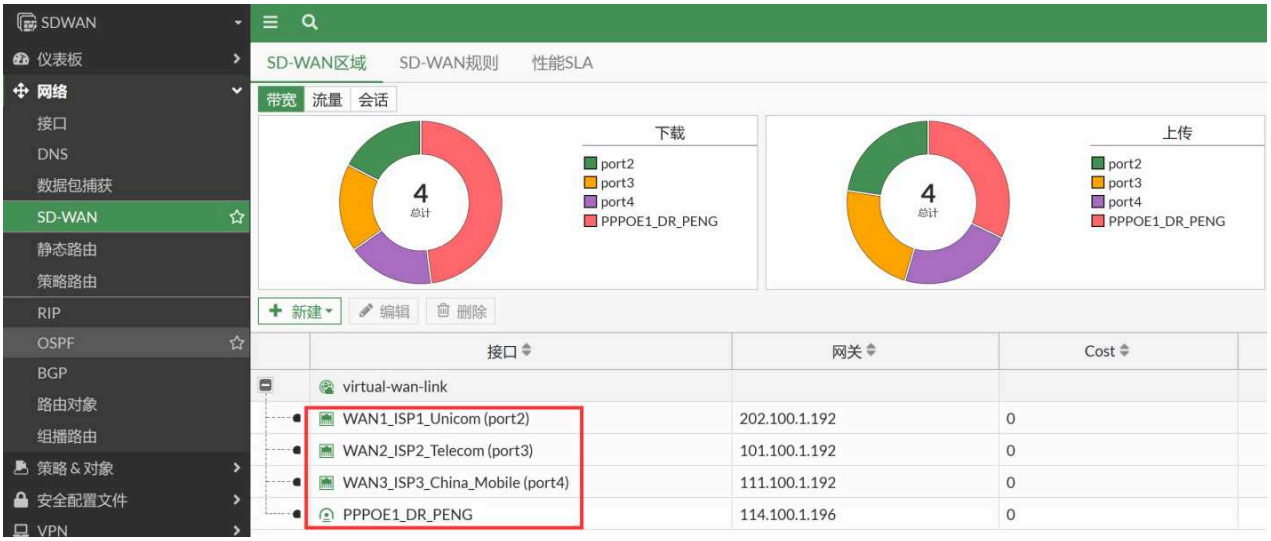
```
    next
end

SDWAN (members) # end
SDWAN (sdwan) # end
```

当没匹配到SD-WAN自定义规则（策略路由），同时有存在SD-WAN的默认路由的时候，就会去匹配SD-WAN的负载路由（最后一条隐藏默认SD-WAN规则），这时候priority参数会生效（priority效果和普通路由一致）。port3的路由priority是100，此路由存在于路由表中，但是不用于出方向的路由转发（策略路由可以使用此路由），仅仅存在路由表中，以便入方向的RPF（反向路径检测）可以正常工作。

```
SDWAN # get router info routing-table all
 ...
S*      0.0.0.0/0 [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
                  [1/0] via 101.100.1.192, port3, [100/0]     //priority为100，对于出方向的策略路由是生效的，不用于出方向的FIB路由的转发。可以解决入方向的RPF问题
 ...
```

成员序号与接口index的关系

1. 查看SD-WAN成员的序号。




```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "port2"
            set gateway 202.100.1.192
        next
        edit 2
            set interface "port3"
            set gateway 101.100.1.192
            set priority 100
        next
        edit 3
            set interface "port4"
            set gateway 111.100.1.192
        next
        edit 4
            set interface "PPPOE1_DR_PENG"
        next
    end


```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # diagnose sys sdwan member    //SD-WAN接口组成员
Member(1): interface: port2, flags=0×0 , gateway: 202.100.1.192, priority: 1 1024, weight: 0
Member(2): interface: port3, flags=0×0 , gateway: 101.100.1.192, priority: 100 1024, weight: 0
Member(3): interface: port4, flags=0×0 , gateway: 111.100.1.192, priority: 1 1024, weight: 0
Member(4): interface: PPPOE1_DR_PENG, flags=0×8 , gateway: 114.100.1.196, priority: 1 1024, weight: 0
```

2. 在SD-WAN SLA监控中查看SD-WAN成员序号。

```
SDWAN # diagnose sys sdwan health-check status    //SD-WAN健康检查
Health Check(114_Check):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(20.472), jitter(0.790), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(20.289), jitter(0.750), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(20.199), jitter(0.746), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(4 PPPOE1_DR_PENG): state(alive), packet-loss(0.000%) latency(20.371), jitter(0.861), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0×1
```

3. 在SD-WAN规则中查看SD-WAN成员序号。

```
SDWAN # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0×260 use-shortcut-sla
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10), heath-check(114_Check)
  Members(4):
    1: Seq_num(1 port2), alive, latency: 21.736, selected
    2: Seq_num(4 PPPOE1_DR_PENG), alive, latency: 21.599, selected
    3: Seq_num(2 port3), alive, latency: 21.524, selected
    4: Seq_num(3 port4), alive, latency: 21.507, selected
  Internet Service(1): Microsoft-Office365(327782,0,0,0)
  Src address(1):
        192.168.1.0-192.168.1.255
```

4. 查看策略路由中对应的service 1的条目，记录其中的oif参数。

```
SDWAN # diag firewall proute list
list route policy info(vf=root):

id=2097676289(0×7d080001) vwl_service=1(OFFICE_365) vwl_mbr_seq=1 4 2 3 dscp_tag=0×ff 0×ff flags=0×0 tos=0×00 tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(4) oif=4(port2) gwy=202.100.1.192
oif=19(PPPOE1_DR_PENG) gwy=114.100.1.196 ot
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Office365(327782,0,0,0)
hit_count=0 last_used=2023-01-03 00:00:13
```

5. 查看接口索引与具体接口的对应关系。

```
SDWAN # diag ip address list
 …
IP=202.100.1.10→202.100.1.10/255.255.255.0 index=4 devname=port2
IP=101.100.1.10→101.100.1.10/255.255.255.0 index=5 devname=port3
IP=111.100.1.10→111.100.1.10/255.255.255.0 index=6 devname=port4
 …
IP=114.100.1.204→114.100.1.196/255.255.255.255 index=19 devname=PPPOE1_DR_PENG
```

6. 综上所述可以得出SD-WAN接口组成员序号与各个功能模块里面的接口调用关系。

```
接口索引 4      --- 对应 port2 ---对应SD-WAN接口成员组序号1
接口索引 5     --- 对应 port3 ---对应SD-WAN接口成员组序号2
接口索引 6   --- 对应 port4 ---对应SD-WAN接口成员组序号3
接口索引 19   --- 对应 PPPOE1_DR_PENG ---对应SD-WAN接口成员组序号4
```

其他

1. 统计SD-WAN成员接口最近10分钟流量的命令。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # diagnose sys sdwan intf-sla-log port2
Timestamp: Tue Jan  3 01:04:04 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 422346bytes, rx bytes: 422106bytes.
Timestamp: Tue Jan  3 01:04:14 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 423468bytes, rx bytes: 423228bytes.
Timestamp: Tue Jan  3 01:04:24 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 424590bytes, rx bytes: 424350bytes.
Timestamp: Tue Jan  3 01:04:34 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 425712bytes, rx bytes: 425472bytes.
Timestamp: Tue Jan  3 01:04:44 2023, used inbandwidth: 875bps, used outbandwidth: 884bps, used bibandwidth:
1759bps, tx bytes: 426792bytes, rx bytes: 426498bytes.
Timestamp: Tue Jan  3 01:04:54 2023, used inbandwidth: 882bps, used outbandwidth: 882bps, used bibandwidth:
1764bps, tx bytes: 427860bytes, rx bytes: 427620bytes.
Timestamp: Tue Jan  3 01:05:04 2023, used inbandwidth: 875bps, used outbandwidth: 875bps, used bibandwidth:
1750bps, tx bytes: 428940bytes, rx bytes: 428700bytes.
Timestamp: Tue Jan  3 01:05:14 2023, used inbandwidth: 882bps, used outbandwidth: 882bps, used bibandwidth:
1764bps, tx bytes: 430104bytes, rx bytes: 429864bytes.
Timestamp: Tue Jan  3 01:05:24 2023, used inbandwidth: 875bps, used outbandwidth: 875bps, used bibandwidth:
1750bps, tx bytes: 431184bytes, rx bytes: 430944bytes.
Timestamp: Tue Jan  3 01:05:34 2023, used inbandwidth: 890bps, used outbandwidth: 882bps, used bibandwidth:
1772bps, tx bytes: 432306bytes, rx bytes: 432066bytes.
Timestamp: Tue Jan  3 01:05:44 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 433386bytes, rx bytes: 433146bytes.
Timestamp: Tue Jan  3 01:05:54 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 434508bytes, rx bytes: 434268bytes.
Timestamp: Tue Jan  3 01:06:04 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 435630bytes, rx bytes: 435390bytes.
Timestamp: Tue Jan  3 01:06:14 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 436752bytes, rx bytes: 436512bytes.
Timestamp: Tue Jan  3 01:06:24 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 437832bytes, rx bytes: 437592bytes.
Timestamp: Tue Jan  3 01:06:34 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 438954bytes, rx bytes: 438714bytes.
Timestamp: Tue Jan  3 01:06:44 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 440034bytes, rx bytes: 439794bytes.
Timestamp: Tue Jan  3 01:06:54 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 441198bytes, rx bytes: 440958bytes.
Timestamp: Tue Jan  3 01:07:04 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 442278bytes, rx bytes: 442038bytes.
Timestamp: Tue Jan  3 01:07:14 2023, used inbandwidth: 890bps, used outbandwidth: 892bps, used bibandwidth:
1782bps, tx bytes: 443412bytes, rx bytes: 443160bytes.
Timestamp: Tue Jan  3 01:07:24 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 444480bytes, rx bytes: 444240bytes.
Timestamp: Tue Jan  3 01:07:34 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 445560bytes, rx bytes: 445320bytes.
Timestamp: Tue Jan  3 01:07:44 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 446724bytes, rx bytes: 446484bytes.
Timestamp: Tue Jan  3 01:07:54 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 447804bytes, rx bytes: 447564bytes.
Timestamp: Tue Jan  3 01:08:04 2023, used inbandwidth: 890bps, used outbandwidth: 888bps, used bibandwidth:
1778bps, tx bytes: 448968bytes, rx bytes: 448728bytes.
Timestamp: Tue Jan  3 01:08:14 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 450048bytes, rx bytes: 449808bytes.
Timestamp: Tue Jan  3 01:08:24 2023, used inbandwidth: 904bps, used outbandwidth: 904bps, used bibandwidth:
1808bps, tx bytes: 451212bytes, rx bytes: 450972bytes.
Timestamp: Tue Jan  3 01:08:34 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 452292bytes, rx bytes: 452052bytes.
Timestamp: Tue Jan  3 01:08:44 2023, used inbandwidth: 897bps, used outbandwidth: 897bps, used bibandwidth:
1794bps, tx bytes: 453414bytes, rx bytes: 453174bytes.
Timestamp: Tue Jan  3 01:08:54 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 454536bytes, rx bytes: 454296bytes.
Timestamp: Tue Jan  3 01:09:04 2023, used inbandwidth: 897bps, used outbandwidth: 897bps, used bibandwidth:
1794bps, tx bytes: 455658bytes, rx bytes: 455418bytes.
Timestamp: Tue Jan  3 01:09:14 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 456738bytes, rx bytes: 456498bytes.
Timestamp: Tue Jan  3 01:09:24 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 457860bytes, rx bytes: 457620bytes.
Timestamp: Tue Jan  3 01:09:34 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 458982bytes, rx bytes: 458742bytes.
Timestamp: Tue Jan  3 01:09:44 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 460062bytes, rx bytes: 459822bytes.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

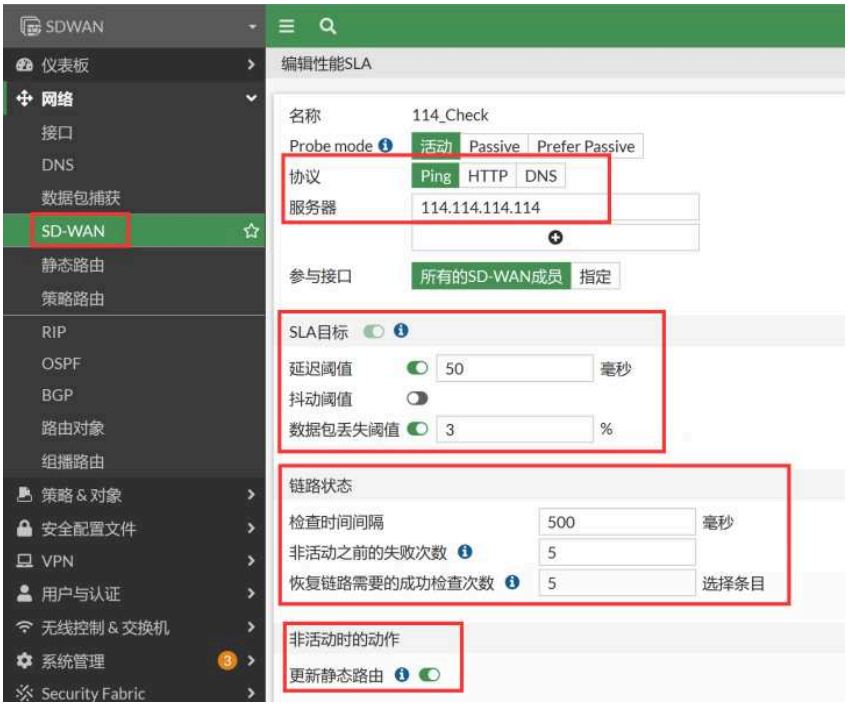
```
Timestamp: Tue Jan  3 01:09:54 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 461226bytes, rx bytes: 460986bytes.
Timestamp: Tue Jan  3 01:10:04 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 462306bytes, rx bytes: 462066bytes.
Timestamp: Tue Jan  3 01:10:14 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 463428bytes, rx bytes: 463188bytes.
Timestamp: Tue Jan  3 01:10:24 2023, used inbandwidth: 882bps, used outbandwidth: 882bps, used bibandwidth:
1764bps, tx bytes: 464496bytes, rx bytes: 464256bytes.
Timestamp: Tue Jan  3 01:10:34 2023, used inbandwidth: 880bps, used outbandwidth: 888bps, used bibandwidth:
1768bps, tx bytes: 465618bytes, rx bytes: 465324bytes.
Timestamp: Tue Jan  3 01:10:44 2023, used inbandwidth: 866bps, used outbandwidth: 875bps, used bibandwidth:
1741bps, tx bytes: 466698bytes, rx bytes: 466404bytes.
Timestamp: Tue Jan  3 01:10:54 2023, used inbandwidth: 873bps, used outbandwidth: 882bps, used bibandwidth:
1755bps, tx bytes: 467820bytes, rx bytes: 467526bytes.
Timestamp: Tue Jan  3 01:11:04 2023, used inbandwidth: 873bps, used outbandwidth: 882bps, used bibandwidth:
1755bps, tx bytes: 468942bytes, rx bytes: 468648bytes.
Timestamp: Tue Jan  3 01:11:14 2023, used inbandwidth: 873bps, used outbandwidth: 890bps, used bibandwidth:
1763bps, tx bytes: 470064bytes, rx bytes: 469716bytes.
Timestamp: Tue Jan  3 01:11:24 2023, used inbandwidth: 875bps, used outbandwidth: 884bps, used bibandwidth:
1759bps, tx bytes: 471144bytes, rx bytes: 470796bytes.
Timestamp: Tue Jan  3 01:11:34 2023, used inbandwidth: 888bps, used outbandwidth: 897bps, used bibandwidth:
1785bps, tx bytes: 472308bytes, rx bytes: 471960bytes.
Timestamp: Tue Jan  3 01:11:44 2023, used inbandwidth: 882bps, used outbandwidth: 890bps, used bibandwidth:
1772bps, tx bytes: 473388bytes, rx bytes: 473040bytes.
Timestamp: Tue Jan  3 01:11:54 2023, used inbandwidth: 882bps, used outbandwidth: 890bps, used bibandwidth:
1772bps, tx bytes: 474510bytes, rx bytes: 474162bytes.
Timestamp: Tue Jan  3 01:12:04 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 475632bytes, rx bytes: 475284bytes.
Timestamp: Tue Jan  3 01:12:14 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 476712bytes, rx bytes: 476364bytes.
Timestamp: Tue Jan  3 01:12:24 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 477834bytes, rx bytes: 477486bytes.
Timestamp: Tue Jan  3 01:12:34 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 478956bytes, rx bytes: 478608bytes.
Timestamp: Tue Jan  3 01:12:44 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 480078bytes, rx bytes: 479730bytes.
Timestamp: Tue Jan  3 01:12:54 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 481158bytes, rx bytes: 480810bytes.
Timestamp: Tue Jan  3 01:13:04 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 482280bytes, rx bytes: 481932bytes.
Timestamp: Tue Jan  3 01:13:14 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 483402bytes, rx bytes: 483054bytes.
Timestamp: Tue Jan  3 01:13:24 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 484482bytes, rx bytes: 484134bytes.
Timestamp: Tue Jan  3 01:13:34 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 485604bytes, rx bytes: 485256bytes.
Timestamp: Tue Jan  3 01:13:44 2023, used inbandwidth: 890bps, used outbandwidth: 892bps, used bibandwidth:
1782bps, tx bytes: 486738bytes, rx bytes: 486378bytes.
Timestamp: Tue Jan  3 01:13:54 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 487806bytes, rx bytes: 487458bytes.
Timestamp: Tue Jan  3 01:14:04 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 488928bytes, rx bytes: 488580bytes.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SD-WAN健康检查

基础配置

1. 进入网络→SD-WAN→性能SLA，新建SLA检测。



2. 对应CLI。

```bash
SDWAN # config system sdwan
SDWAN (sdwan) # config health-check
SDWAN (health-check) # edit "114_Check"
SDWAN (114_Check) # show
config health-check
    edit "114_Check"
        set server "114.114.114.114"    //可以指定两个被检测的server，server可以是IP或者FQDN//
        set protocol ping    //SLA探测使用的协议，可以选择ping、tcp-echo、udp-echo、http、twamp、dns、tcp-connect、ftp//
        set interval 500    //每隔500 milliseconds发送一下健康检测的探测//
        set probe-timeout 500    //探测数据包被视为丢失前的等待时间（毫秒），默认 = 500）//
        set failtime 5    //两个被探测的sla server在连续发起的5次探测都没有回应之后，没有回应的sd-wan接口成员将会被置位为dead状态，会将其在SD-WAN的选路接口组中剔除//
        set recoverytime 5    //sla状态在两个sla server中其中的一个连续响应5次后切换回alive状态，会恢复到SD-WAN的选路接口中//
        set members 0    //指定健康检查发送的出接口，0表示所有//
        config sla    //SLA Targets是可选项,SD-WAN规则中的 “Lowest Cost”规则（mode sla）和 “Maximize Bandwidth“规则(mode load-balance)需要用到SLA Targets中的检测值，基于SLA检测值进行流量路径的判断和选择//
            edit 1
                set link-cost-factor latency packet-loss
                set latency-threshold 50
                set packetloss-threshold 3
            next
        end
    next
end
```

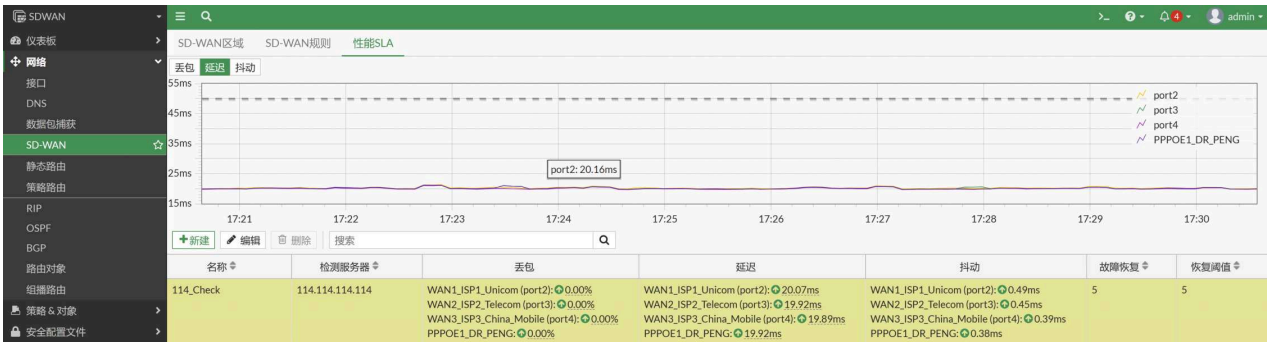
效果验证

1. Server IP后台的处理：填写的SLA server IP会在FGT的内核中添加一个Fib路由条目项，以便每个SD-WAN接口拥有独立指向sla server ip的路由。这些特定的内核路由（被标记为“proto=17”）将使得SD-WAN接口成员到sla服务器的可访问性完全独立于通常的路由表转发表（静态路由、动态路由），从而不管静态/动态路由状态如何都可以对sla服务器的发起探测请求。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # get router info kernel | grep 114.114.114.114     //内核下发的独立于路由转发表的路由//
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 114.100.1.204/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=114.100.1.196 dev=19(PPPOE1_DR_PENG)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 111.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=111.100.1.192 dev=6(port4)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 101.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=101.100.1.192 dev=5(port3)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 202.100.1.10/255.255.255.255/0→114.114.114.114/32 pref=0.0.0.0
gwy=202.100.1.192 dev=4(port2)
```
bash

2. 健康检测SLA历史记录。



3. 实时SLA健康检查参数记录。

```
SDWAN # diagnose sys sdwan health-check status 114_Check
Health Check(114_Check):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(19.972), jitter(0.253), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(19.809), jitter(0.266), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(19.721), jitter(0.256), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(4 PPPOE1_DR_PENG): state(alive), packet-loss(0.000%) latency(19.856), jitter(0.299), bandwidth-up(9999999),
bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x1
```
bash

SLA日志

1. 某一个接口的十分钟的使用统计。

```
SDWAN # diagnose sys sdwan intf-sla-log port3
Timestamp: Tue Jan  3 01:22:04 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 542424bytes, rx bytes: 542130bytes.
Timestamp: Tue Jan  3 01:22:14 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 543504bytes, rx bytes: 543210bytes.
Timestamp: Tue Jan  3 01:22:24 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 544626bytes, rx bytes: 544332bytes.
Timestamp: Tue Jan  3 01:22:34 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 545706bytes, rx bytes: 545412bytes.
Timestamp: Tue Jan  3 01:22:44 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 546828bytes, rx bytes: 546534bytes.
Timestamp: Tue Jan  3 01:22:54 2023, used inbandwidth: 877bps, used outbandwidth: 877bps, used bibandwidth:
1754bps, tx bytes: 547908bytes, rx bytes: 547614bytes.
Timestamp: Tue Jan  3 01:23:04 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 549030bytes, rx bytes: 548736bytes.
Timestamp: Tue Jan  3 01:23:14 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 550152bytes, rx bytes: 549858bytes.
Timestamp: Tue Jan  3 01:23:24 2023, used inbandwidth: 890bps, used outbandwidth: 890bps, used bibandwidth:
1780bps, tx bytes: 551274bytes, rx bytes: 550980bytes.
Timestamp: Tue Jan  3 01:23:34 2023, used inbandwidth: 884bps, used outbandwidth: 884bps, used bibandwidth:
1768bps, tx bytes: 552354bytes, rx bytes: 552060bytes.
......
```
bash

2. SLA的日志记录开启（间隔单位为s）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
SDWAN # config system sdwan
SDWAN (sdwan) # config health-check
SDWAN (health-check) # edit 114_Check
SDWAN (114_Check) # set sla-fail-log-period 10    //当成员处于失败状态时，将按指定的间隔生成sla日志//
SDWAN (114_Check) # set sla-pass-log-period 10    //当成员处于活动状态时，按指定的间隔生成sla日志//
SDWAN (114_Check) # end
SDWAN (sdwan) # end
```

3. SLA PASS日志。

```bash
date=2023-01-03 time=01:36:49 eventtime=1672738609392716352 tz="-0800" logid="0113022925" type="event"
subtype="sdwan" level="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA"
healthcheck="114_Check" slatargetid=1 interface="port4" status="up" latency="20.333" jitter="1.324"
packetloss="0.000" inbandwidthavailable="10.00Gbps" outbandwidthavailable="10.00Gbps"
bibandwidthavailable="20.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps" bibandwidthused="0kbps"
slamap="0x1" msg="Health Check SLA status."
```

4. SLA FAIL日志。

```bash
date=2023-01-03 time=01:38:29 eventtime=1672738709588764152 tz="-0800" logid="0113022933" type="event"
subtype="sdwan" level="notice" vd="root" logdesc="SDWAN SLA notification" eventtype="SLA" healthcheck="114_Check"
slatargetid=1 interface="port4" status="down" latency="0.000" jitter="0.000" packetloss="4.000"
inbandwidthavailable="10.00Gbps" outbandwidthavailable="10.00Gbps" bibandwidthavailable="20.00Gbps"
inbandwidthused="0kbps" outbandwidthused="0kbps" bibandwidthused="0kbps" slamap="0x0" metric="packetloss"
msg="Health Check SLA status. SLA failed due to being over the performance metric threshold."
```

5. 健康检查全部成功的情况。

```bash

SDWAN # diagnose sys sdwan health-check status 114_Check
Health Check(114_Check):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(20.186), jitter(0.659), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(19.979), jitter(0.519), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(3 port4): state(alive), packet-loss(70.000%) latency(20.073), jitter(0.695), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x0
Seq(4 PPPOE1_DR_PENG): state(alive), packet-loss(0.000%) latency(20.122), jitter(0.552), bandwidth-up(9999999),
bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x1
```

6. 制造接口的Member3（Port4）丢包，查看失败的健康检查结果为dead。

```bash
SDWAN # diagnose sys sdwan member
Member(1): interface: port2, flags=0x0 , gateway: 202.100.1.192, priority: 1 1024, weight: 0
Member(2): interface: port3, flags=0x0 , gateway: 101.100.1.192, priority: 100 1024, weight: 0
Member(3): interface: port4, flags=0x0 , gateway: 111.100.1.192, priority: 1 1024, weight: 0
Member(4): interface: PPPOE1_DR_PENG, flags=0x8 , gateway: 114.100.1.196, priority: 1 1024, weight: 0

SDWAN # diagnose sys sdwan health-check status 114_Check
Health Check(114_Check):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(20.068), jitter(0.454), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(19.887), jitter(0.483), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(3 port4): state(dead), packet-loss(18.000%) sla_map=0x0
Seq(4 PPPOE1_DR_PENG): state(alive), packet-loss(0.000%) latency(19.876), jitter(0.497), bandwidth-up(9999999),
bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x1
```

7. 对应的SD-WAN规则下port4接口也会显示dead。

```bash
SDWAN # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x260 use-shortcut-sla
  Gen(4), TOS(0x0/0x0), Protocol(0: 1→65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10),
heath-check(114_Check)
  Members(4):
    1: Seq_num(1 port2), alive, latency: 20.087, selected
    2: Seq_num(4 PPPOE1_DR_PENG), alive, latency: 19.904, selected
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    3: Seq_num(2 port3), alive, latency: 19.950, selected
    4: Seq_num(3 port4), dead    //不再被SD-WAN规则选路使用//
  Internet Service(1): Microsoft-Office365(327782,0,0,0)
  Src address(1):
        192.168.1.0-192.168.1.255
```

8. 查看策略路由列表，SD-WAN转发表中移除了oif index 6：port4接口。

```bash
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2097807361(0x7d0a0001) vwl_service=1(OFFICE_365) vwl_mbr_seq=1 4 2 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=4(port2) gwy=202.100.1.192
oif=19(PPPOE1_DR_PENG) gwy=114.100.1.196 oif=5(port3) gwy=101.100.1.192 default    // SD-WAN转发表中移除了oif index
6: port4接口
source(1): 192.168.1.0-192.168.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Office365(327782,0,0,0)
hit_count=0 last_used=2023-01-03 00:00:13
```

9. 由于健康检查里面的更新静态路由打开了（默认开启），因此相应的SD-WAN静态路由也会将port4对应的SD-WAN路由状态置位为inactive（可以在路由database中看到，但会出现在路由表中）。

非活动时的动作 禁用关联非活动接口的静态路由. 恢复时重置路由.

更新静态路由

```bash
config system sdwan
    config health-check
        edit "114_Check"
            set update-static-route enable
        next
    end
end
```

```bash
SDWAN # get router info routing-table database
...
S     > 0.0.0.0/0 [1/0] via 111.100.1.192, port4 inactive, [1/0]
      *>          [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
      *>          [1/0] via 202.100.1.192, port2, [1/0]
      *>          [1/0] via 101.100.1.192, port3, [100/0]
...
```

10. 只要健康检查失败，则port4就不会被策略路由/SD-WAN规则/路由转发数据了，和link-moniter的效果是类似的，其实进程也是使用的同样一个进程“link-monitor process (lnkmtd)”，debug lnkmtd进程。

link-monitor process (*lnkmtd*)

```
FGT-1 # diag test application lnkmtd
1: Show memory info.
2: Show vdom monitor info.
3: Show fail detection info.
```

lnkmtd is the process responsible for processing *Performance SLA* probes

```
FGT-1 # diag debug enable
FGT-1 # diag debug application link-monitor <level>
Debug messages will be on for 30 minutes.
```

debugging of *lnkmtd*

Level	Description criteria
1	Server up or down events
2	Config changes
4	Engine events
8	ICMP probes
16	UDP probes
32	TCP probes

Level	Description criteria
64	HTTP probes
128	TWAMP probes
256	GRE probes
512	Link detection
1024	DNS messages
2048	Application messages
4096	Policy route messages

FORTINET

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

补充

讨论另外一个事情：SD-WAN健康检查检测到出口异常，就会引起路由出接口变化，那么策略路由/SD-WAN规则/路由在出接口发生了变化的时候，FGT在转发数据的时候是什么样的一个处理逻辑。

1. 首先回答这个问题：SD-WAN规则的下一跳/出接口切换了，流量就会立即切换吗？

2. 有两条命令需要知道：

```bash
config system global
      set snat-route-change disable（默认状态disable）
end
```

路由变化，Snat的会话表是否跟随着一起变化更新？

- disable：会话表项不变化，继续保持该会话，保持原有出口 （默认值为disable）
- enable：会话表项变化，会话状态会置位为dirty，并且新来的数据将会重新上送CPU查询策略/路由等参数，重新进行会话的匹配，一旦路由变化将会匹配新的出口进行数据的转发

> **重要**
>
> 默认配置下的SNAT场景，即使转发流量的SD-WAN成员的健康检查变为dead，只要该线路仍然存在路由（可能关闭了 `update-static-route` ），已有的旧会话仍然不会切换到其他线路。

路由变化，非SNAT会话表是否跟随着一起变化更新？

```bash
config system interface
    edit "port2"
        set preserve-session-route disable（默认状态disable）
    next
```

end

```
- disable：不保持会话。
- enable：强制保持会话，不会主动的更新会话中路由的下一跳地址。
- 这个命令的优先级更高，只要开启了接口的会话保持，无论snat-route-change是否是enable，会话还是为会优先保持，会话/流量不会更变出接口信息。

3. 总结来看：默认情况已存在的SNAT会话将会进行会话保持，不会跟随着SD-WAN规则/路由的出接口变化，而改变数据的转发出口，还是会保持原有出接口进行转发数据。这样的会话数据是不会切换的。新建的SNAT的会话，则会按照新建会话处理流程上送CPU，查询当前最新的SD-WAN规则/路由等信息进行数据转发，会切换到新的出口上去。

4. 而如果没有SNAT的环境下，仅仅是三层路由转发的会话，会话是会随着路由的变化而dirty，强制上送CPU进行SD-WAN规则/路由/策略的重新查询和转发处理，一旦路由出接口有变化，转发数据会立即跟换改会话数据流的出接口。

5. 一旦在接口下配置了会话保持preserve-session-route enable，则会有最高的优先级保障会话保持的机制。

6. 还有另外一个参数（异步路由）会影响到路由变化时候的数据转发逻辑。

```bash
config system settings
    set asymroute disable（默认状态disable）
end
```
```

- disable：默认配置，不允许非对称路由。此时路由变化，Session（NAT/非NAT）是否保持基于“snat-route-change”和“preserve-session-route”的配置结果而定。
- enable：此时无论“snat-route-change”和“preserve-session-route”如何配置，只要路由发生了变化，流量会重新查询路由强制将流量转发到新的下一跳出口。此时任何会话保持都会失效。这个拥有很高的优先级，打破一切的会话保持机制，当然考虑到安全性，不建议开启异步路由。

7. SD-WAN规则的下一跳/出接口切换后，业务流量切换注意：因为SD-WAN的切换会相对频繁一些，以下参数如果调整不合适就会出现SD-WAN一切换就出现业务中断的情况。因此非特殊情况下，尽量保持以下三个参数为默认的状态，这样有利于SD-WAN路由切换时候业务的平滑切换。务必先理解清楚三个参数的含义，然后才可按照自己的需求选择性的开启。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system global
      set snat-route-change disable（默认状态disable）
end
```

```
config system interface
    edit "wan1"
        set preserve-session-route disable（默认状态disable）
    next
end
```

```
config system settings
     set asymroute disable（默认状态disable）
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

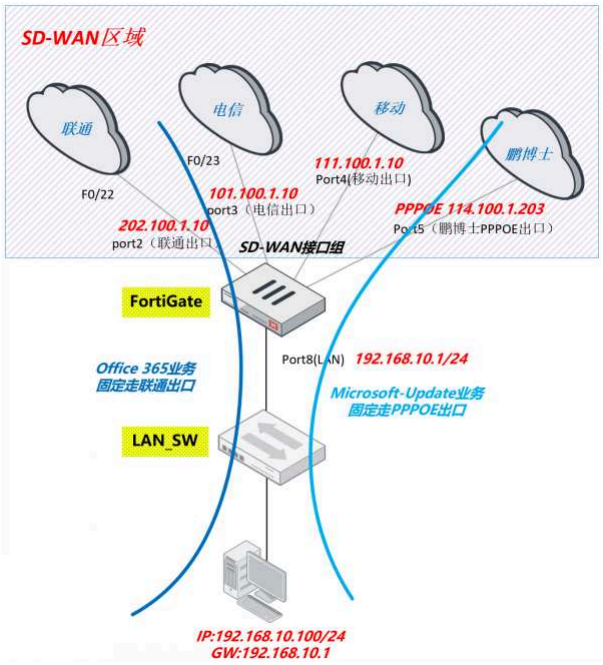
Manual（手动选路）

基本概念

1. 顾名思义让指定的SD-WAN流量从人工选择的固定线路出去。这时候SD-WAN规则的出口是固定的，不存在切换的问题，除非线路DOWN/SD-WAN健康检查失败/Link-Moniter等因素影响让其出口的相关路由消失，SD-WAN规则才会失效，流量才会切换到其他的线路上去，否则将强制让SD-WAN的流量出口固定到这条线路上。
2. 一般有两种常见的使用场景：将优先保障的重要业务固定指向到一条质量好的线路上去；或者反过来使用，将一些优先级不高（比如一些自动更新等占用较大带宽的应用）的业务固定指向到一条质量差的线路上去。具体的使用可按照自己的需求去定义。
3. 手工选路更像传统的策略路由，只能选择一个出接口，但相比策略路由会多跟多的匹配项，比如应用、Internet Service Database等等，更加灵活一些。
4. 总结：
   - 相当于在SD-WAN接口上配置常规的策略路由
   - 不需要调用Performance SLA（SD-WAN状态检查）
   - 源IP地址建议配置为明细，不要配置为any，避免匹配到本机发起流量
   - 目的地址可以调用 IP地址+协议+端口或Internet Service + Application Control
   - 只能选择一个出接口（单接口成员选择）

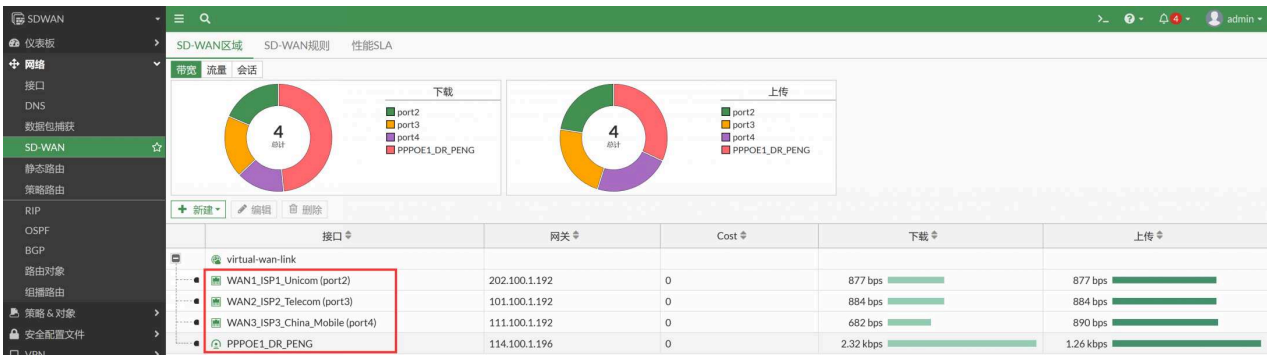
配置举例

网络拓扑



配置步骤

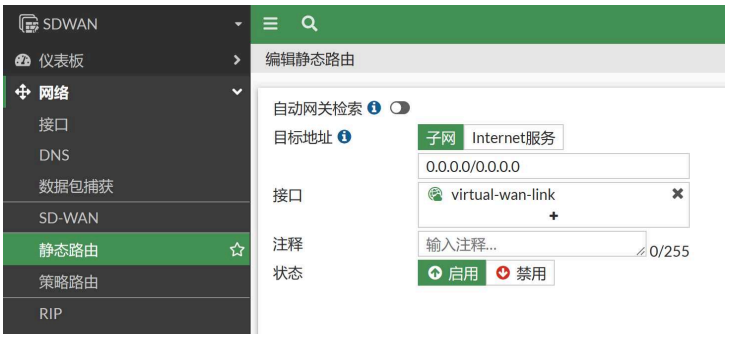
1. SD-WAN接口成员定义。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "port2"
            set gateway 202.100.1.192
        next
        edit 2
            set interface "port3"
            set gateway 101.100.1.192
        next
        edit 3
            set interface "port4"
            set gateway 111.100.1.192
        next
        edit 4
            set interface "PPPOE1_DR_PENG"
        next
    end
 end
```

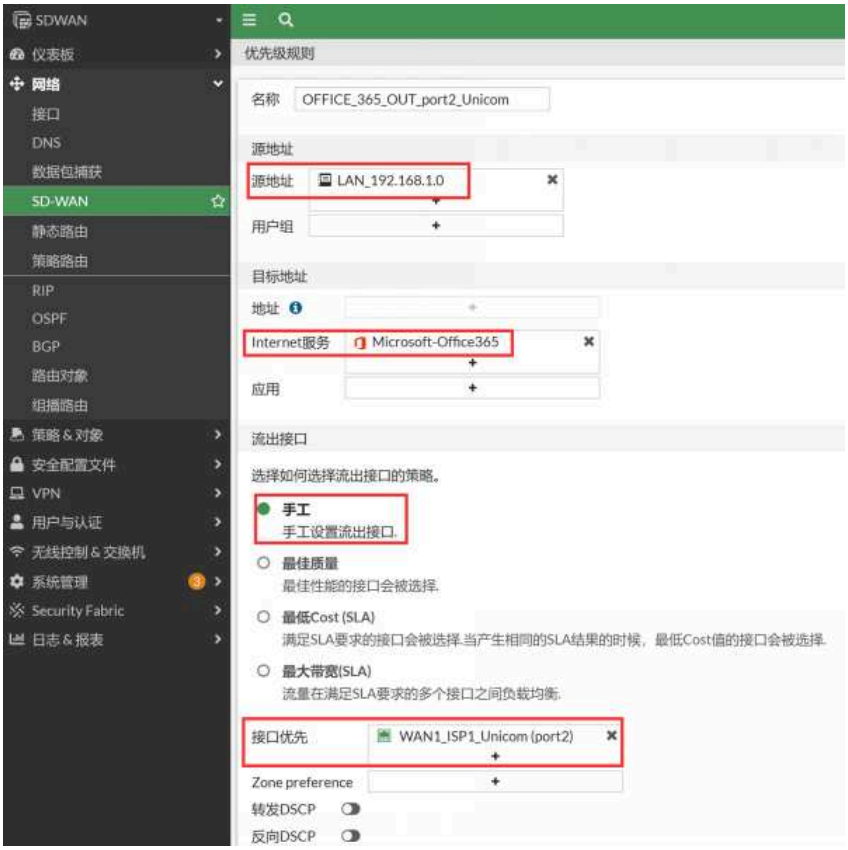
2. 配置SD-WAN关联的默认路由。




```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

3. SD-WAN规则1：Office 365业务固定走联通出口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system sdwan
        config service
        edit 1
            set name "OFFICE_365_OUT_port2_Unicom"
            set src "LAN_192.168.1.0"
            set internet-service enable
            set internet-service-name "Microsoft-Office365"
            set priority-members 1
            set gateway enable
            set default enable
        next
    end
end
```

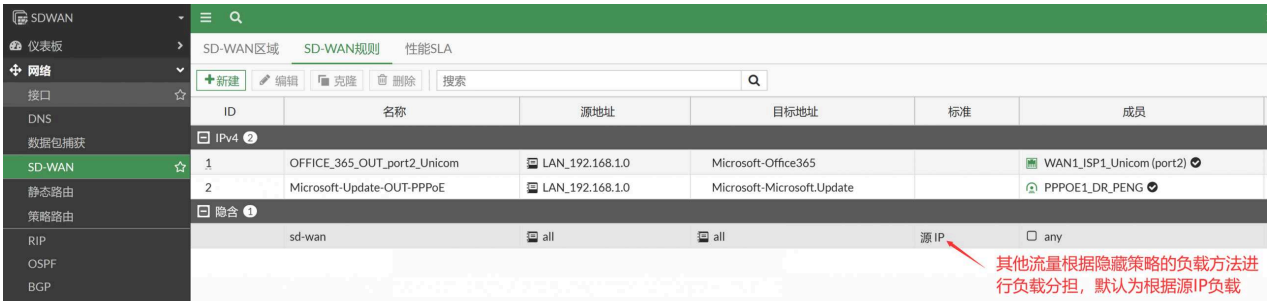
4. SD-WAN规则2：Microsoft-Update业务固定走PPPOE出口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system sdwan
        config service
        edit 2
            set name "Microsoft-Update-OUT-PPPoE"
            set src "LAN_192.168.1.0"
            set internet-service enable
            set internet-service-name "Microsoft-Microsoft.Update"
            set priority-members 4
        next
    end
end
```

5. 剩余流量匹配隐藏规则，根据源IP进行负载。



6. 配置上网策略，放通SDWAN流量。

重要

如果使用ippool的方式做SNAT，在SD-WAN环境下，一定要在ippool下配置绑定接口，防止ippool在SD-WAN成员中转换错误。

```
config firewall ippool
    edit xxxx
        set associated-interface port2
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 1
        set name "To_Internet"
        set srcintf "port8"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

结果验证

1. 查看SD-WAN成员状态。

```
SDWAN # diagnose sys sdwan member
Member(1): interface: port2, flags=0×0 , gateway: 202.100.1.192, priority: 1 1024, weight: 0
Member(2): interface: port3, flags=0×0 , gateway: 101.100.1.192, priority: 1 1024, weight: 0
Member(3): interface: port4, flags=0×0 , gateway: 111.100.1.192, priority: 1 1024, weight: 0
Member(4): interface: PPPOE1_DR_PENG, flags=0×8 , gateway: 114.100.1.196, priority: 1 1024, weight: 0
```

2. 查看SDWAN规则状态，两条规则中的线路均为alive状态。

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×260 use-shortcut-sla
  Gen(2), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(1):
    1: Seq_num(1 port2), alive, selected
  Internet Service(1): Microsoft-Office365(327782,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255

Service(2): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(2), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(1):
    1: Seq_num(4 PPPOE1_DR_PENG), alive, selected
  Internet Service(1): Microsoft-Microsoft.Update(327793,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

3. 查看策略路由条目，可以看到每条策略对应的出接口SD-WAN成员编号与接口index。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2097545217(0×7d060001) vwl_service=1(OFFICE_365_OUT_port2_Unicom) vwl_mbr_seq=1 dscp_tag=0×ff 0×ff flags=0×0
tos=0×00 tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(1) oif=4(port2) gwy=202.100.1.192
default
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Office365(327782,0,0,0)
hit_count=11 last_used=2023-01-03 03:13:30

id=2131099650(0×7f060002) vwl_service=2(Microsoft-Update-OUT-PPPoE) vwl_mbr_seq=4 dscp_tag=0×ff 0×ff flags=0×0
tos=0×00 tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(1) oif=16(PPPOE1_DR_PENG)
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Microsoft.Update(327793,0,0,0)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

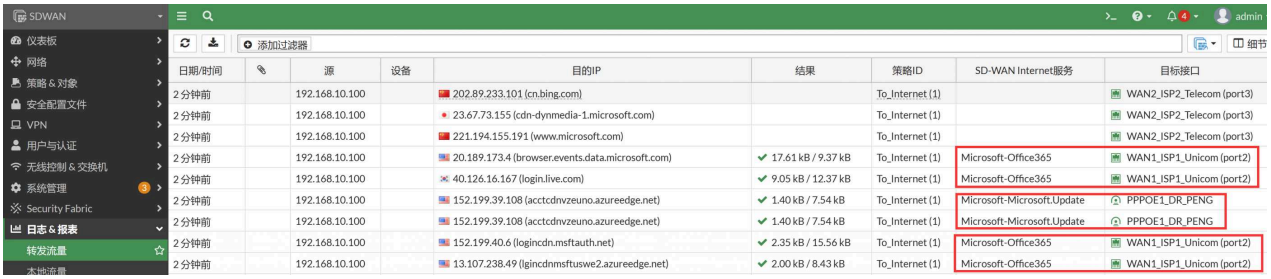
```
hit_count=0 last_used=2023-01-03 02:59:29

SDWAN # diagnose ip address list
...
IP=202.100.1.10→202.100.1.10/255.255.255.0 index=4 devname=port2
IP=101.100.1.10→101.100.1.10/255.255.255.0 index=5 devname=port3
IP=111.100.1.10→111.100.1.10/255.255.255.0 index=6 devname=port4
...
IP=114.100.1.204→114.100.1.196/255.255.255.255 index=16 devname=PPPOE1_DR_PENG
...
```

4. 查看SD-WAN设备路由表。

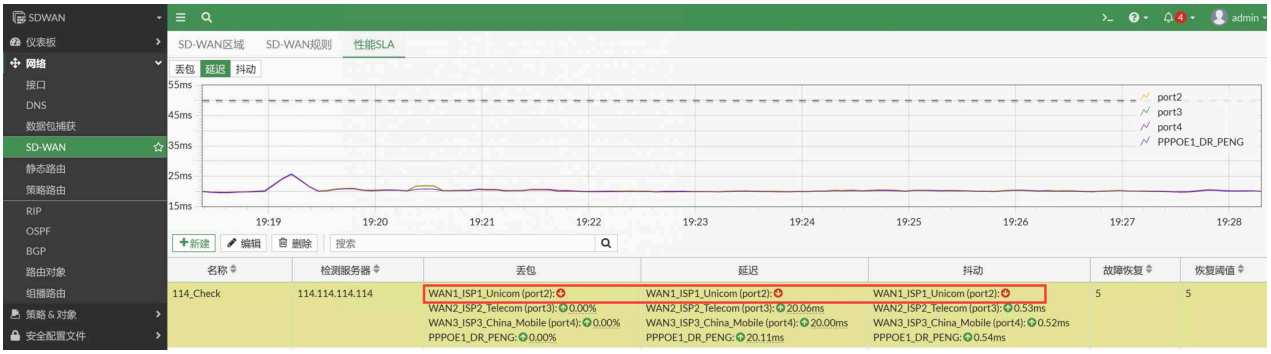
```
SDWAN # get router info routing-table all
...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
...
```

5. 在客户端PC上访问Office365的Internet资源，在SD-WAN设备上查看转发流量日志，Office 365只走port2，MS.Windows.Update只走PPPOE接口出。



故障切换测试

1. 模拟port2故障（SD-WAN健康检查，虽然不需要调用，但是依旧对链路状态和切换起关键作用，也包括DOWN接口/Link-Moniter等其他切换方式）。




```
SDWAN # diagnose sys sdwan health-check
Health Check(114_Check):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0×0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(20.345), jitter(1.146), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(20.197), jitter(1.158), bandwidth-up(9999998), bandwidth-dw(9999997), bandwidth-bi(19999995) sla_map=0×1
Seq(4 PPPOE1_DR_PENG): state(alive), packet-loss(0.000%) latency(20.336), jitter(1.103), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0×1
```

2. 查看SD-WAN成员状态，port2已经变为dead。

```
SDWAN # diagnose sys sdwan member
Member(1): interface: port2, flags=0×0 , gateway: 202.100.1.192, priority: 1 1024, weight: 0
Member(2): interface: port3, flags=0×0 , gateway: 101.100.1.192, priority: 1 1024, weight: 0
Member(3): interface: port4, flags=0×0 , gateway: 111.100.1.192, priority: 1 1024, weight: 0
Member(4): interface: PPPOE1_DR_PENG, flags=0×8 , gateway: 114.100.1.196, priority: 1 1024, weight: 0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0×260 use-shortcut-sla
  Gen(3), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Service disabled caused by no outgoing path.
  Members(1):
    1: Seq_num(1 port2), dead    //检测到port2 dead
  Internet Service(1): Microsoft-Office365(327782,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
Service(2): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(2), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(1):
    1: Seq_num(4 PPPOE1_DR_PENG), alive, selected    //PPPOE接口不受影响
  Internet Service(1): Microsoft-Microsoft.Update(327793,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

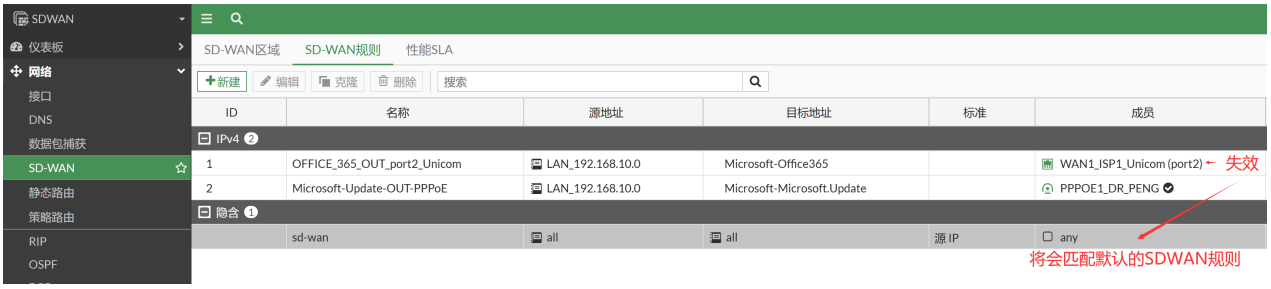
3. 查看SD-WAN设备的路由表，健康检查失败，会触发port2的SD-WAN路由失效。

```
SDWAN # get router info routing-table all
 ...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
 ...
```

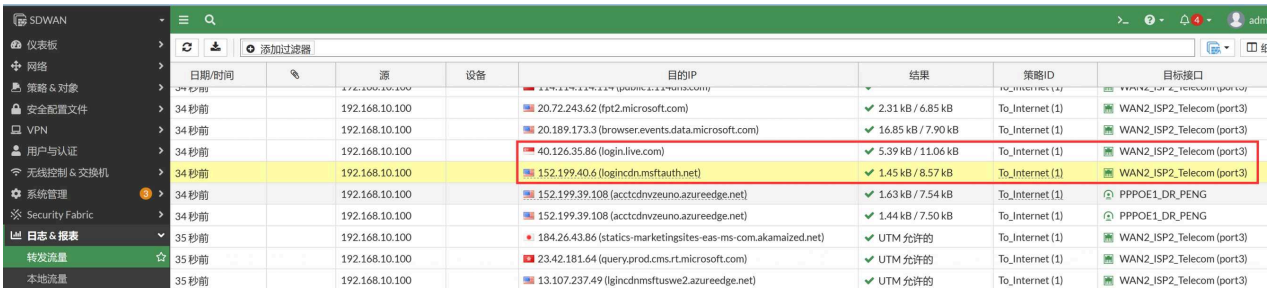
4. 查看策略路由列表。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):
id=2097545217(0×7d060001) vwl_service=1(OFFICE_365_OUT_port2_Unicom) dscp_tag=0×ff 0×ff flags=0×8 disable tos=0×00
tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(0) default
source(1): 192.168.10.0-192.168.10.255    //由于FIB路由表中的port2路由消失，相应的对应SD-WAN规则1也会失效。流量将会匹配到最后一条默认的SD-WAN负载均衡规则，走普通路由表进行转发处理
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Office365(327782,0,0,0)
hit_count=39 last_used=2023-01-03 03:20:36

id=2131099650(0×7f060002) vwl_service=2(Microsoft-Update-OUT-PPPoE) vwl_mbr_seq=4 dscp_tag=0×ff 0×ff flags=0×0
tos=0×00 tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(1) oif=16(PPPOE1_DR_PENG)
source(1): 192.168.10.0-192.168.10.255    //SD-WAN规则2不受影响
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(1): Microsoft-Microsoft.Update(327793,0,0,0)
hit_count=20 last_used=2023-01-03 03:21:06
```



5. 切换后，将不再匹配SD-WAN规则1了，而会匹配SD-WAN的默认规则，实际为查询默认路由（按照源IP负载的方式）选择出接口，此处选择的时候port3接口为出接口。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

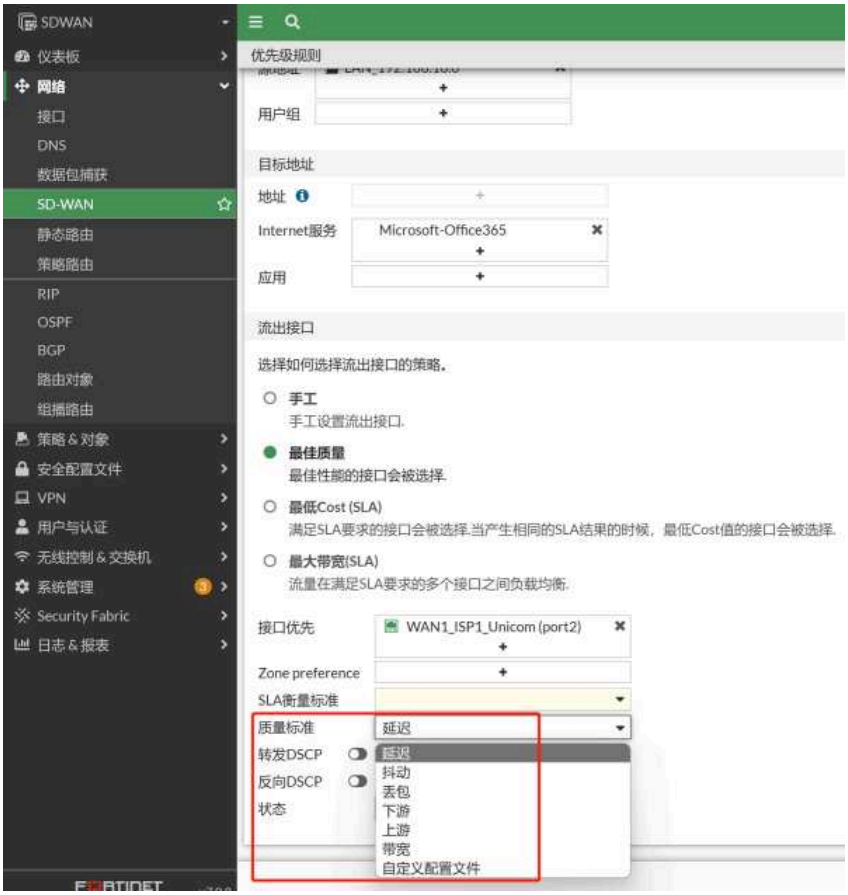
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Best Quality（最佳质量）

基本概念

1. SD-WAN规则选路原则是：选择具有“最佳质量”的链路。

2. 最佳质量的标准有：

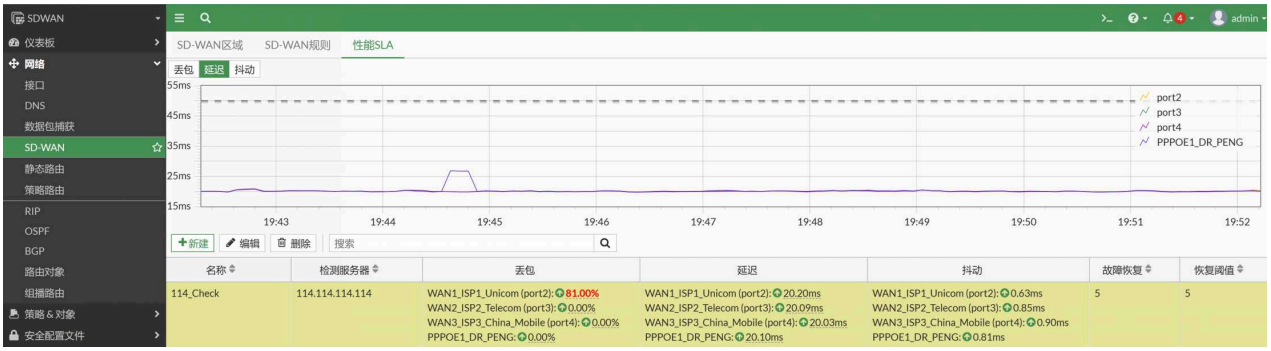


- 延迟
  - 一个数据包从一个节点到另一个节点所需的时间
  - 更少的延迟=更好的吞吐量
  - 延迟大引起的问题：访问速度慢，连接失败
  - 推荐应用：建议用于需要最佳响应时间的应用程序。例如：视频/VoIP
- 抖动
  - 在网络中传输数据包，相邻的数据包被转发之间的时间延迟差异（毫秒级别）。这是设备在按序转发数据包，包和包之间的一个短暂的中断时间。抖动通常是由IP网络中的拥塞引起的
  - 抖动大引起的问题：实时应用程序延迟
  - 推荐应用：建议用于需要实时转发传递数据包的应用程序。例如：VoIP
- 丢包
  - 发生在当通过网络传输的一个或多个数据包无法到达其目标地时候
  - 丢包而引起的问题：信息超时、加载时间慢、加载中断、连接关闭和信息丢失
  - 推荐应用：Oracle DB和SSH这样的CS应用程序
- 下游带宽
  - 内部用户通过网络传输下载数据
  - 带宽不足而引起的问题：传输速度慢
  - 推荐应用：需要网络资源下载数据的应用程序。例如：文件服务器、云存储（Dropbox、OneDrive、百度网盘）
- 上游带宽
  - 内部用户通过网络传输上传数据
  - 带宽不足而引起的问题：传输速度慢，无法完成上传
  - 推荐应用：需要网络资源上传数据的应用程序。例如：备份系统
- 总体带宽
  - 内部用户通过网络传输上传下载数据的总和
- 自定义配置文件

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

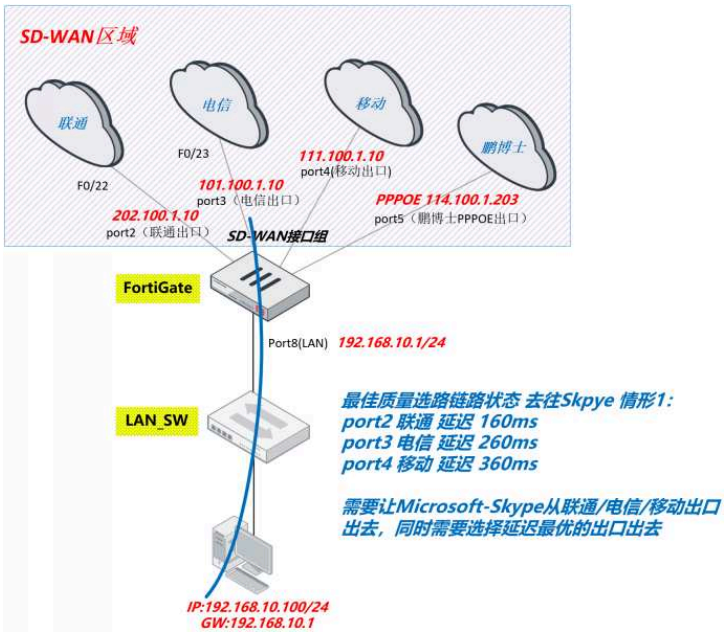
- 基于延迟、抖动、丢包、带宽权重的自定义。计算公式：【Link Quality Index = (packet-loss-weight * packet loss) + (latency-weight * latency) + (jitter-weight * jitter) + (bandwidth-weight / bandwidth)】
- 带宽不足而引起的问题：传输速度慢
- 推荐应用：需要网络资源上传和下载数据的应用程序。示例：文件服务器、云存储（Dropbox、OneDrive）

3. 最佳质量顾名思义就是在SD-WAN规则里配置的多个出接口里面：选择最好的！



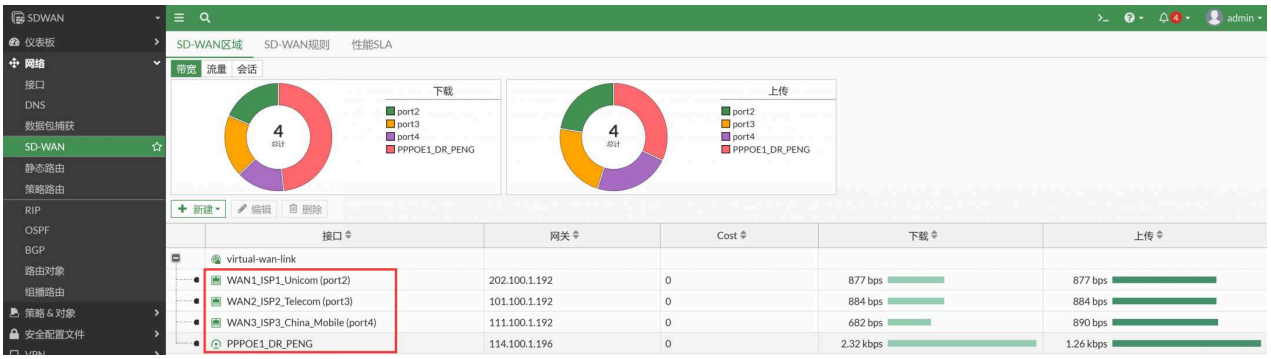
配置举例

网络拓扑



配置步骤

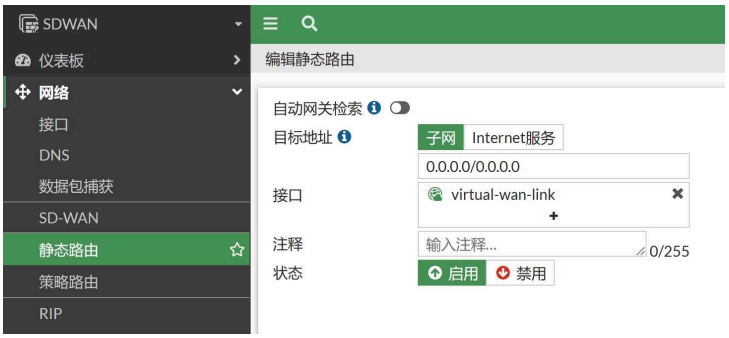
1. SD-WAN接口成员定义。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "port2"
            set gateway 202.100.1.192
        next
        edit 2
            set interface "port3"
            set gateway 101.100.1.192
        next
        edit 3
            set interface "port4"
            set gateway 111.100.1.192
        next
        edit 4
            set interface "PPPOE1_DR_PENG"
        next
    end
 end
```

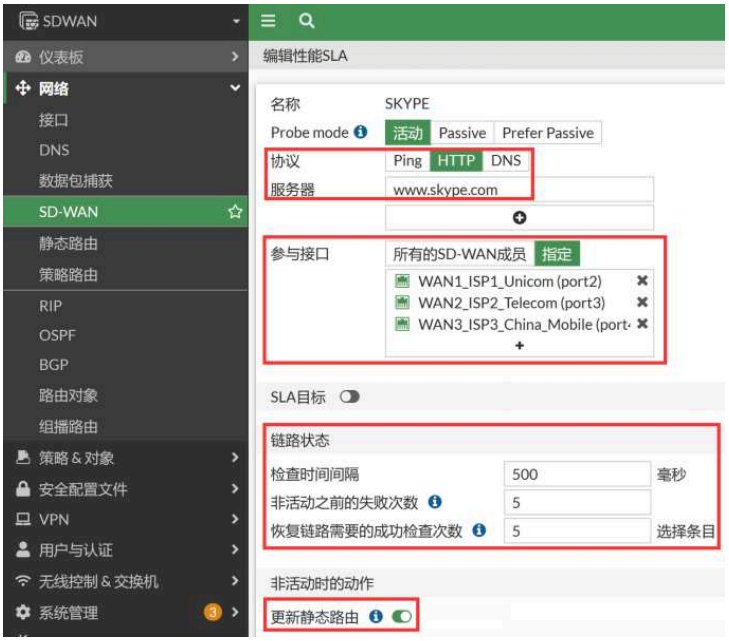
2. 配置SD-WAN关联的默认路由。




```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

3. 配置性能SLA，使用HTTP方法监控www.skype.com网站。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

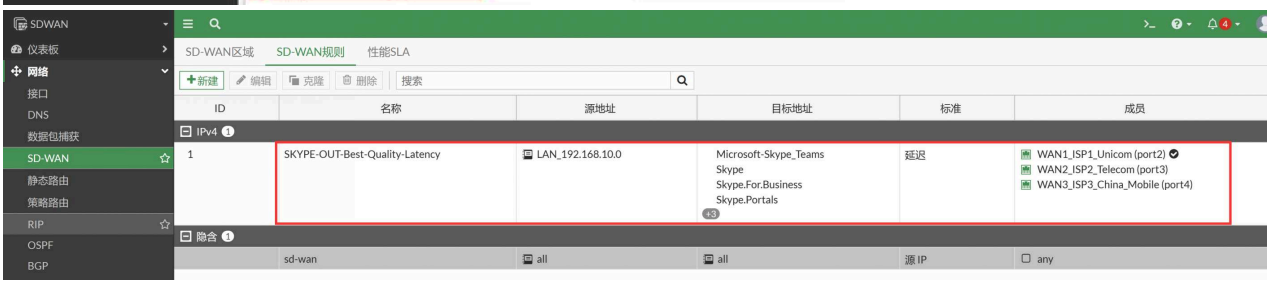



```
config system sdwan
    config health-check
        edit "SKYPE"
            set server "www.skype.com"
            set protocol http
            set members 1 2 3
        next
    end
end
```

4. 配置SD-WAN规则，目标地址为Skype相关应用和Internet服务，流出接口策略选择最佳质量，SLA衡量标准选择上步创建的性能SLA，质量标准选择延迟。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
config system sdwan
    config service
        edit 1
            set name "SKYPE-OUT-Best-Quality-Latency"
            set mode priority
            set link-cost-factor latency    //标准为延迟
            set link-cost-threshold 10    //误差范围10%，避免频繁切换 （默认值）
            set src "LAN_192.168.10.0"
            set internet-service enable
            set internet-service-name "Microsoft-Skype_Teams"
            set internet-service-app-ctrl 10 28554 43540 28587 29350 28597
            set health-check "SKYPE"
            set priority-members 1 2 3
        next
    end
end
```

5. 配置SD-WAN的上网策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

如果使用ippool的方式做SNAT，在SD-WAN环境下，一定要在ippool下配置绑定接口，防止ippool在SD-WAN成员中转换错误。

```
config firewall ippool
       edit xxxx
           set associated-interface port2
       next
end
```




```
config firewall policy
    edit 1
        set name "To_Internet"
        set srcintf "port8"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set webfilter-profile "default"
        set application-list "default"
        set logtraffic all
        set nat enable
    next
end
```

结果验证

1. 查看SD-WAN成员状态，以及健康检查监控状态，可以看到port2、port3、port4的监控延迟分别为160ms左右、260ms左右、360ms左右。

```
SDWAN # diagnose sys sdwan member
Member(1): interface: port2, flags=0×0 , gateway: 202.100.1.192, priority: 1 1024, weight: 0
Member(2): interface: port3, flags=0×0 , gateway: 101.100.1.192, priority: 1 1024, weight: 0
Member(3): interface: port4, flags=0×0 , gateway: 111.100.1.192, priority: 1 1024, weight: 0
Member(4): interface: PPPOE1_DR_PENG, flags=0×8 , gateway: 114.100.1.196, priority: 1 1024, weight: 0

SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10),
heath-check(SKYPE)
  Members(3):
    1: Seq_num(1 port2), alive, latency: 171.847, selected
    2: Seq_num(2 port3), alive, latency: 267.559, selected
    3: Seq_num(3 port4), alive, latency: 366.488, selected
  Internet Service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0 10)
Microsoft.Lync(4294837471,0,0,0 28554) Skype.Portals(4294838961,0,0,0 43540) Lync_Audio(4294837364,0,0,0 28587)
Lync_Apps.Sharing(4294837363,0,0,0 29350) Lync_Video(4294837366,0,0,0 28597)
  Src address(1):
        192.168.10.0-192.168.10.255

SDWAN # diagnose sys sdwan health-check
Health Check(SKYPE):
Seq(1 port2): state(alive), packet-loss(15.000%) latency(178.808), jitter(53.983), bandwidth-up(9999995),
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
bandwidth-dw(9999954), bandwidth-bi(19999949) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(14.000%) latency(261.427), jitter(62.005), bandwidth-up(9999995),
bandwidth-dw(9999952), bandwidth-bi(19999947) sla_map=0x0
Seq(3 port4): state(alive), packet-loss(9.000%) latency(367.605), jitter(58.608), bandwidth-up(9999995),
bandwidth-dw(9999951), bandwidth-bi(19999946) sla_map=0x0
```



2. 查看策略路由列表，将会按照延迟的顺序port2、port3、port4这样排序，优先使用延迟小的出口port2。

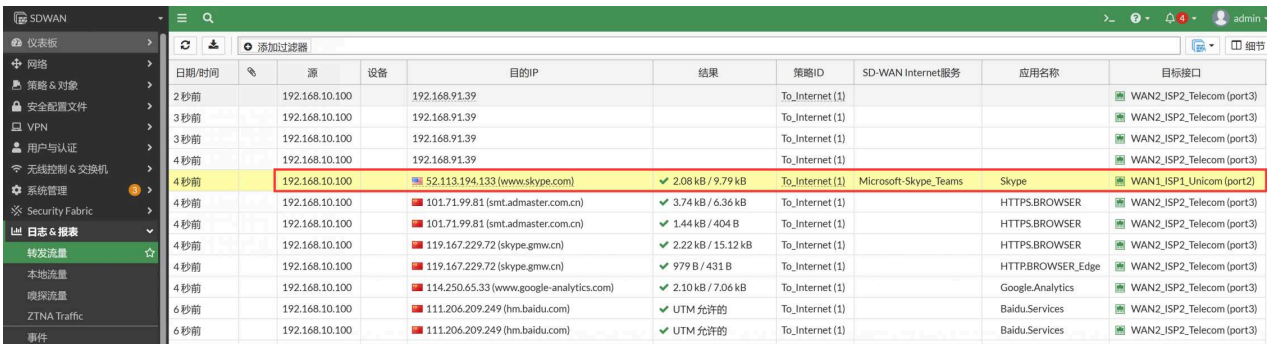
```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2131492865(0x7f0c0001) vwl_service=1(SKYPE-OUT-Best-Quality-Latency) vwl_mbr_seq=1 2 3 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=4(port2)
oif=5(port3) oif=6(port4)
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0, 10)
Microsoft.Lync(4294837471,0,0,0, 28554) Skype.Portals(4294838961,0,0,0, 43540) Lync_Audio(4294837364,0,0,0, 28587)
Lync_Apps.Sharing(4294837363,0,0,0, 29350) Lync_Video(4294837366,0,0,0, 28597)
hit_count=13 last_used=2023-01-03 17:40:51
```

3. 查看SD-WAN设备路由表。

```
SDWAN # get router info routing-table all
 ...
S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
 ...
```

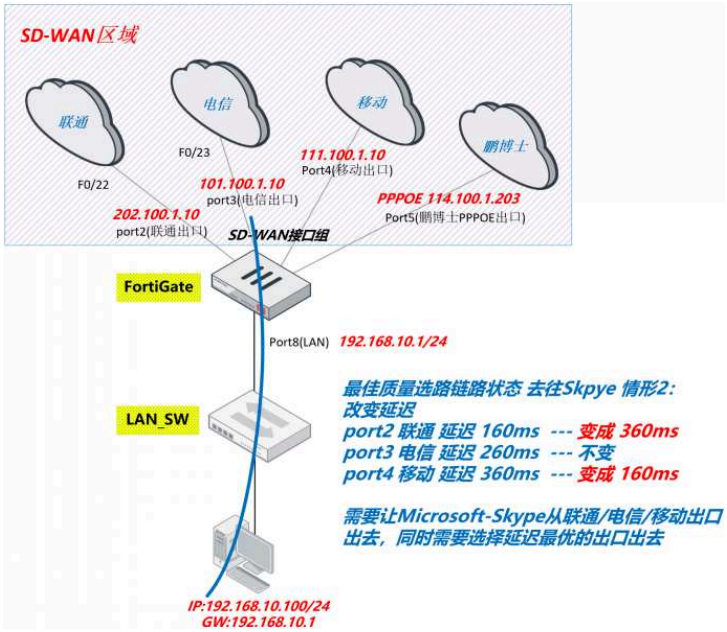
4. 使用客户端PC访问Skype相关资源，在SD-WAN设备上查看流量日志，可以看到相关流量被分配到port2，符合上述SD-WAN检测结果。



故障切换测试

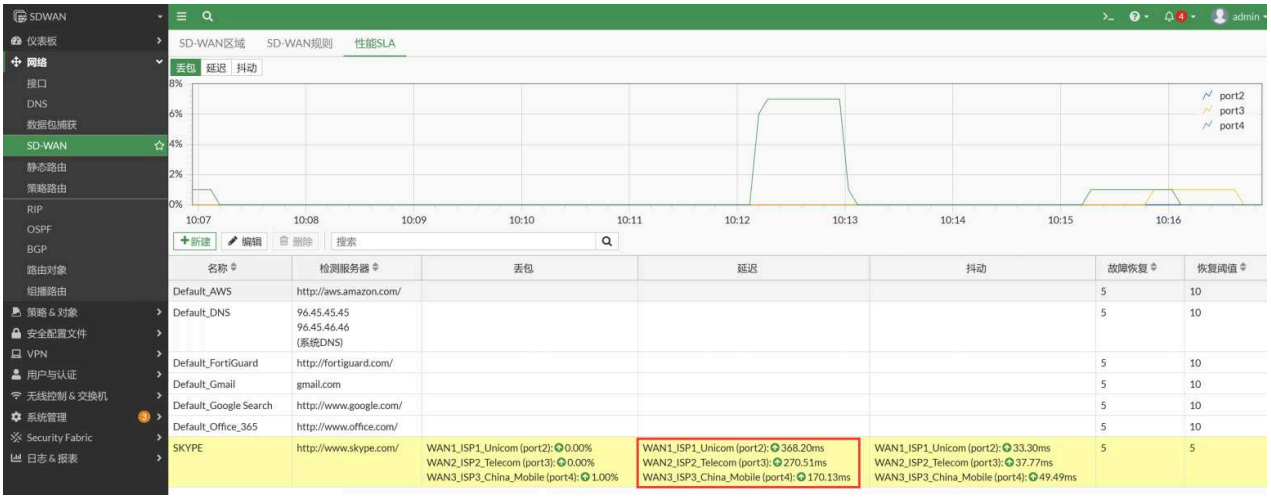
1. 调整port2和port4的延迟，模拟延迟变化，将port2的延迟模拟为360ms，port4的延迟模拟为160ms。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 切换延迟后，查看SLA的检查状态，port2和port4的延迟进行了对调。

```
Seq(1 port2): state(alive), packet-loss(0.000%) latency(367.850), jitter(36.092), bandwidth-up(9999995),
bandwidth-dw(9999953), bandwidth-bi(19999948) sla_map=0×0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(270.216), jitter(37.558), bandwidth-up(9999995),
bandwidth-dw(9999953), bandwidth-bi(19999948) sla_map=0×0
SDWAN # diagnose sys sdwan health-check
Health Check(SKYPE):
Seq(3 port4): state(alive), packet-loss(0.000%) latency(169.290), jitter(28.239), bandwidth-up(9999995),
bandwidth-dw(9999952), bandwidth-bi(19999947) sla_map=0×0
```



3. 查看SD-WAN规则出接口的变化，出接口顺序也相应的对调，变为port4，port3，port2。

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(25), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(priority), link-cost-factor(latency), link-cost-
threshold(10), heath-check(SKYPE)
  Members(3):
    1: Seq_num(3 port4), alive, latency: 168.681, selected    //port4，优先从port13转发
    2: Seq_num(2 port3), alive, latency: 269.862, selected    //port3
    3: Seq_num(1 port2), alive, latency: 367.583, selected    //port2
  Internet Service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0 10)
Microsoft.Lync(4294837471,0,0,0 28554) Skype.Portals(4294838961,0,0,0 43540) Lync_Audio(4294837364,0,0,0 28587)
Lync_Apps.Sharing(4294837363,0,0,0 29350) Lync_Video(4294837366,0,0,0 28597)
  Src address(1):
        192.168.10.0-192.168.10.255
```

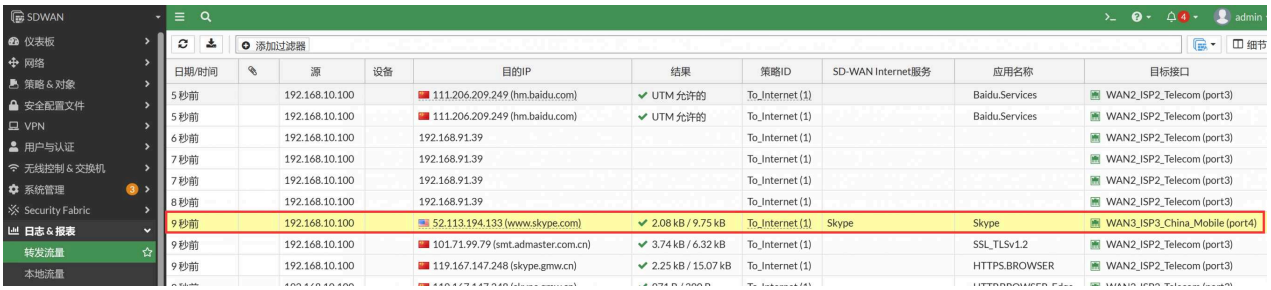

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 查看策略路由中的SD-WAN规则列表，接口顺序已经变化为port4、port3、port2了，依据延迟的大小排序，优先选择延迟小的port4出口。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

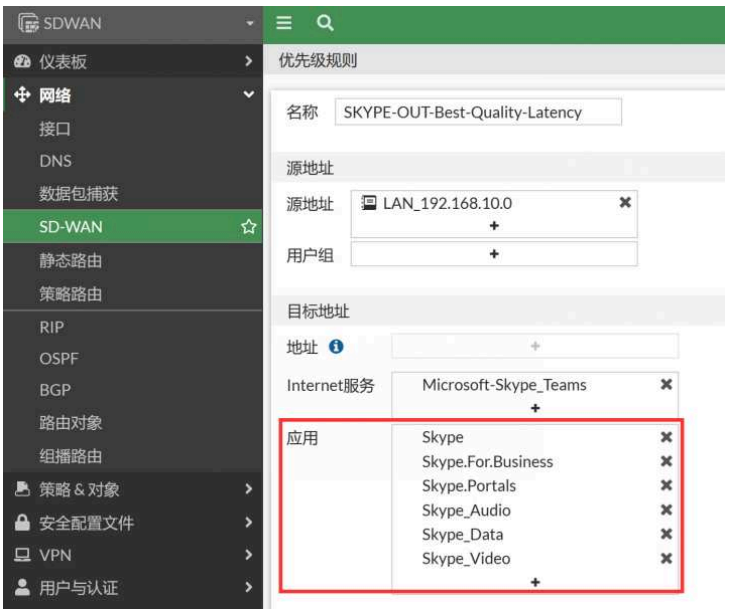
id=2131492865(0x7f0c0001) vwl_service=1(SKYPE-OUT-Best-Quality-Latency) vwl_mbr_seq=3 2 1 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=6(port4)
oif=5(port3) oif=4(port2)
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0, 10)
Microsoft.Lync(4294837471,0,0,0, 28554) Skype.Portals(4294838961,0,0,0, 43540) Lync_Audio(4294837364,0,0,0, 28587)
Lync_Apps.Sharing(4294837363,0,0,0, 29350) Lync_Video(4294837366,0,0,0, 28597)
hit_count=19 last_used=2023-01-03 18:05:39
```

5. 查看客户端访问SKYPE相关资源的流量日志，可以看到流量被分配到了port4。



注意事项

1. 由于我的SD-WAN规则里面选择了应用程序Skype，这样基于应用的SD-WAN规则（策略路由）要生效的话需要满足一些条件：



- 第一步：应用程序是需要先通过内网用户通过使用SKPYE，然后FGT进行应用识别的，因此策略里面一定要开启APP Control才可以（需要识别加密流量需要开启SSL深度检测）。



- 第二步：识别之后将会学习到相应的应用程序（SKYPE）的IP地址，将会形成一个动态的应用程序（SKYPE）IP地址数据库，最终才会将这个学习到的IP数据库加入到SD-WAN规则（策略路由）里面，因此这需要有一个学习的过程，SD-WAN中的应用程序的调用不会立即生效，因此在没有成功学习之前，SKPYE的流量会走到其他线路上去，FGT会去学习这些识别出来的应用程序的IP地址，这并非问题，而是SD-WAN调用应用的工作逻

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

辑就是这样，学习完毕之后，新发起的流量才会匹配到SD-WAN规则（策略路由），我们可以通过命令行查看到学习的应用程序IP数据库信息。

```
SDWAN # diagnose sys sdwan internet-service-app-ctrl-list

Skype(10 4294838051): 52.113.194.133 6 443 Tue Jan  3 18:05:37 2023
Skype.Portals(43540 4294838961): 13.107.42.16 6 443 Tue Jan  3 15:40:51 2023
```

- 如果需要学习将到的Skype数据库立马完全生效，旧的会话是会保持原有出口的，想要这些旧的会话立即生效需要清除旧的会话和路由缓存信息，而新建的会话则不需要此操作，具体命令行如下。

```
SD-WAN # diagnose sys session filter src 192.168.10.100
SD-WAN # diagnose sys session clear    //清除测试机器的会话，让其重新匹配新的SD-WAN规则（有skype的IP数据库更新）
SD-WAN # diagnose ip rtcache flush    //清除路由缓存
```

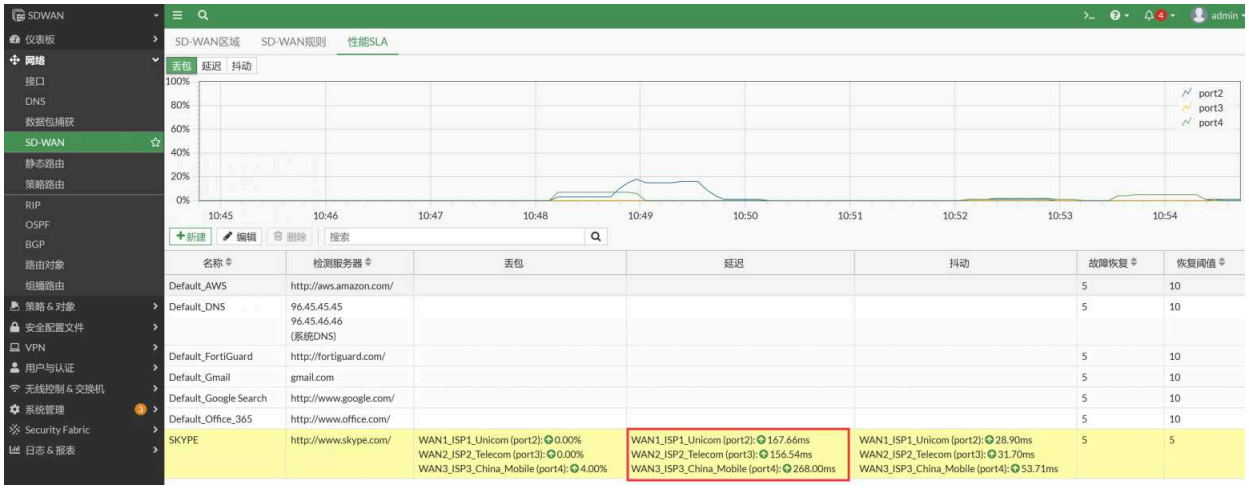
2. SD-WAN规则中参数：link-cost-threshold的作用。

```
SDWAN #  config system sdwan
SDWAN (sdwan) # config service
SDWAN (service) # show full-configuration
config service
    edit 1
        set name "SKYPE-OUT-Best-Quality-Latency"
…
        set link-cost-threshold 10
…
    next
end
```

- 根据上述的实验测试可以看出SD-WAN规则的工作逻辑：
  - 切换前延迟：
    - port2联通延迟160ms //选择延迟小的
    - port3电信延迟260ms
    - port4移动延迟360ms
    - 优先选择port2
  - 切换后的延迟：
    - port2联通延迟360ms
    - port3电信延迟260ms
    - port4移动延迟160ms //选择延迟小的
    - 优先选择port4
- 我们再来做一个测试，让延迟变成下面这个样子：
  - port2联通延迟166ms
  - port3电信延迟156ms //设置port3的延迟比port2低，但是低的不多
  - Port4移动延迟266ms
- 此时如何优先出接口呢？我们来看具体情况。

```
SDWAN # diagnose sys sdwan health-check
Health Check(SKYPE):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(166.441), jitter(42.834), bandwidth-up(9999995),
bandwidth-dw(9999953), bandwidth-bi(19999948) sla_map=0×0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(156.610), jitter(29.137), bandwidth-up(9999995),
bandwidth-dw(9999952), bandwidth-bi(19999947) sla_map=0×0
Seq(3 port4): state(alive), packet-loss(0.000%) latency(268.445), jitter(21.758), bandwidth-up(9999995),
bandwidth-dw(9999953), bandwidth-bi(19999948) sla_map=0×0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 此时看SD-WAN规则的选择，此时port2会被优选，port3延迟虽然比port2低，但是没有被优选，这是为什么呢?

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(priority), link-cost-factor(latency), link-cost-
threshold(10), heath-check(SKYPE)
  Members(3):
    1: Seq_num(1 port2), alive, latency: 166.993, selected    //此时port2会被优选
    2: Seq_num(2 port3), alive, latency: 156.219, selected    //port3延迟虽然比port2低，但是没有被优选，这是为什么呢?
    3: Seq_num(3 port4), alive, latency: 268.677, selected
  Internet Service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0 10)
Microsoft.Lync(4294837471,0,0,0 28554) Skype.Portals(4294838961,0,0,0 43540) Lync_Audio(4294837364,0,0,0 28587)
Lync_Apps.Sharing(4294837363,0,0,0 29350) Lync_Video(4294837366,0,0,0 28597)
  Src address(1):
        192.168.10.0-192.168.10.255
```

- 查看策略路由列表，策略路由的接口顺序port2、port3、port4。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2131623937(0×7f0e0001) vwl_service=1(SKYPE-OUT-Best-Quality-Latency) vwl_mbr_seq=1 2 3 dscp_tag=0×ff 0×ff
flags=0×0 tos=0×00 tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=4(port2)
oif=5(port3) oif=6(port4)    //策略路由的接口顺序port2、port3、port4
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0, 10)
Microsoft.Lync(4294837471,0,0,0, 28554) Skype.Portals(4294838961,0,0,0, 43540) Lync_Audio(4294837364,0,0,0,
28587) Lync_Apps.Sharing(4294837363,0,0,0, 29350) Lync_Video(4294837366,0,0,0, 28597)
hit_count=24 last_used=2023-01-03 18:34:50
```

- 此时SD-WAN规则选择了port2作为出接口，port3延迟虽然比port2低，但是没有被优选，这是为什么呢?
- 答案正是因为set link-cost-threshold 10此参数在起作用：当两个SD-WAN接口成员链路之间的SLA测量值存在显著差异时，结果是可以预期的，越小则越优先被选择。然而，当标准的SLA测量值足够接近时，SD-WAN会优先考虑配置中的靠前位置位置的出口链路。比如port2/port3/port4的延迟差不多的时候，会优先选择port2，这种逻辑是为了避免当SLA相对接近时链接之间的频繁切换而设计的。它由一个名为“set link-cost-threshold”的设置进行控制，该设置默认为10%，如果差距在10%以内的值，会优先选择SD-WAN规则中配置靠前的接口进行数据转发。
  - port2联通延迟166ms，10%的最低值：166 /（1+0.1）= 150.9，150.9 ~ 166 之间的值对于port2来说都是会被忽略的，即便延迟比port2要低，但是没有超过10%，因此就忽略了比较计算值，依旧保持port2出口的选择。
  - port3电信延迟156ms，延迟比port2虽然要低，但是没有超过< 150.9 ~166 （port2百分之10的忽略范围），因此port3不会被优选。
  - port4移动延迟266ms，超过了150.9 ~166的范围，肯定不会被优选。
- 此时将port3的延迟设置为149ms，查看SD-WAN策略中的顺序，发现port3的延迟149.5 < 150.9马上就会被优选。

```
Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(priority), link-cost-factor(latency), link-cost-
threshold(10), heath-check(SKYPE)
  Members(3):
    1: Seq_num(2 port3), alive, latency: 149.569, selected
    2: Seq_num(1 port2), alive, latency: 164.794, selected
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    3: Seq_num(3 port4), alive, latency: 259.659, selected
  Internet Service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0 10)
Microsoft.Lync(4294837471,0,0,0 28554) Skype.Portals(4294838961,0,0,0 43540) Lync_Audio(4294837364,0,0,0 28587)
Lync_Apps.Sharing(4294837363,0,0,0 29350) Lync_Video(4294837366,0,0,0 28597)
  Src address(1):
        192.168.10.0-192.168.10.255
```

- 查看策略路由列表，出接口顺序变为port3，port2，port4。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2131623937(0x7f0e0001) vwl_service=1(SKYPE-OUT-Best-Quality-Latency) vwl_mbr_seq=2 1 3 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=5(port3)
oif=4(port2) oif=6(port4)
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(7): Microsoft-Skype_Teams(327781,0,0,0) Skype(4294838051,0,0,0, 10)
Microsoft.Lync(4294837471,0,0,0, 28554) Skype.Portals(4294838961,0,0,0, 43540) Lync_Audio(4294837364,0,0,0,
28587) Lync_Apps.Sharing(4294837363,0,0,0, 29350) Lync_Video(4294837366,0,0,0, 28597)
hit_count=24 last_used=2023-01-03 18:34:50
```

- 总结来看：Best Quality（最佳质量）在SD-WAN规则中会选择最好质量的线路（延迟、丢包、抖动）最低值的出接口优先用于SD-WAN流量的转发，为了避免频繁的切换，当所有的出接口质量都差不多的时候（差距在10%以内），则会选择SD-WAN规则配置接口顺序靠前的接口用于SD-WAN流量的转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Lowest Cost (SLA)

概念介绍

SLA

Service-Level Agreement，服务品质协议，是服务提供者和客户之间的一个协议，用来保证可计量的网络性能达到所定义的服务品质。SD-WAN的选路基于这个SLA品质标准来判断，SD-WAN规则保障让流量一直走符合SLA品质的链路出去。从而达到业务/客户的SLA品质要求。

SLA-Target

1. SD-WAN可定义SLA-Target设置保障的目标延迟、抖动和丢包率，一旦超出SLA-Target配置的目标值，则切换另外一条线路，以确保持续提供SLA-Target品质级别的服务。
2. SLA Target 有三种类型的判断阈值：
   - Latency (ms)
   - Jitter (ms)
   - Packet Loss (%)




```
config system sdwan
    config health-check
    edit "114_Check"
        set server "114.114.114.114"
        set members 0
        config sla
            edit 1
                set latency-threshold 200
                set packetloss-threshold 2
            next
            edit 2
                set latency-threshold 250
                set jitter-threshold 10
                set packetloss-threshold 5
            next
            edit 3
                set latency-threshold 300
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set jitter-threshold 15
                set packetloss-threshold 8
            next
        end
    next
end

```

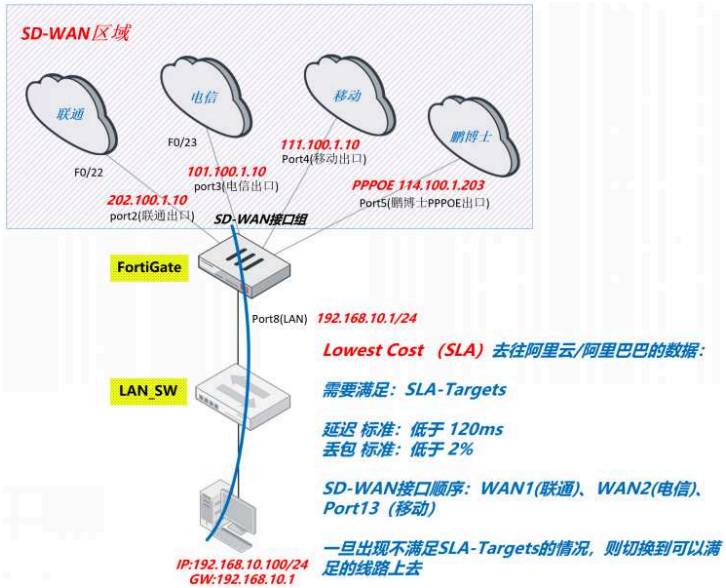
3. **Lowest Cost (SLA) 和Maximize Bandwidth (SLA)都需要调用SLA Target，基于SLA Target进行相关的判断和选路。**

选路原则

1. 只有满足SLA-Targets的出接口才有机会被选中，如果低于SLA-Targets的接口将会被移除选中列表中。
2. 如果有多个接口满足SLA-Targets，那么就选择SD-WAN规则配置接口顺序靠前的接口用于转发SD-WAN流量。
3. 同时只能一个出接口被优选，用于SD-WAN流量的转发。
4. Lowest Cost（SLA）完全基于SLA-Targets进行工作，因此首先需要在SD-WAN状态检查里面配置具体的SLA-Targets标准，然后在SD-WAN规则中选择相应的SLA-Targets，只有符合选择的SLA-Targets标准的出口，才会被SD-WAN规则所计算并用于出口数据的转发，将选择符合SLA-Targets且接口顺序靠前的出口用于数据转发，同时只有一个接口用于数据的转发。

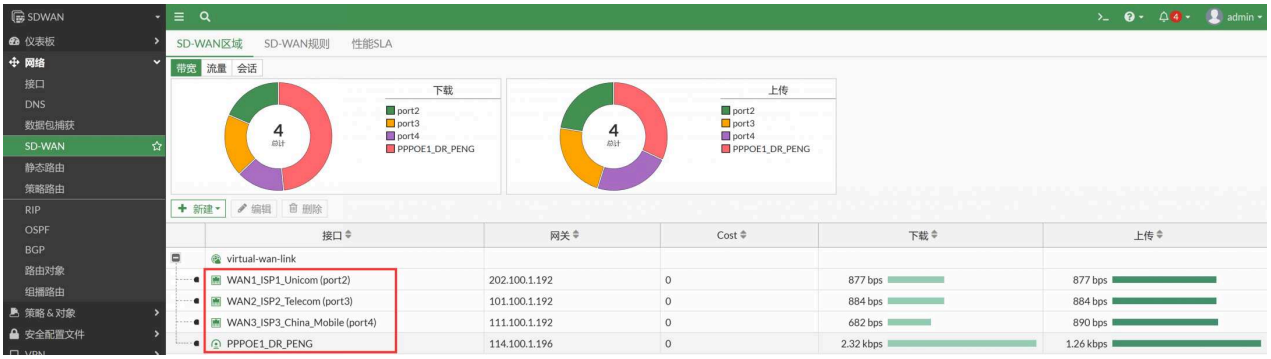
配置举例

网络拓扑



配置步骤

1. SD-WAN接口成员定义。

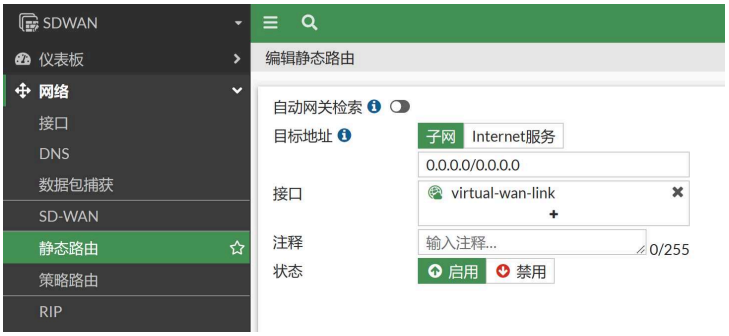



```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

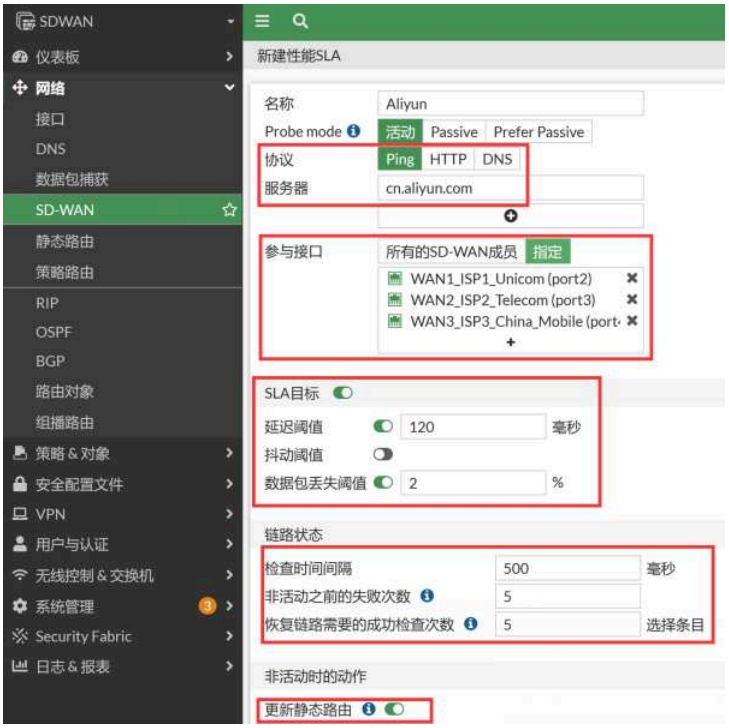
```
    config members
        edit 1
            set interface "port2"
            set gateway 202.100.1.192
        next
        edit 2
            set interface "port3"
            set gateway 101.100.1.192
        next
        edit 3
            set interface "port4"
            set gateway 111.100.1.192
        next
        edit 4
            set interface "PPPOE1_DR_PENG"
        next
    end
end
```

2. 配置SD-WAN关联的默认路由。



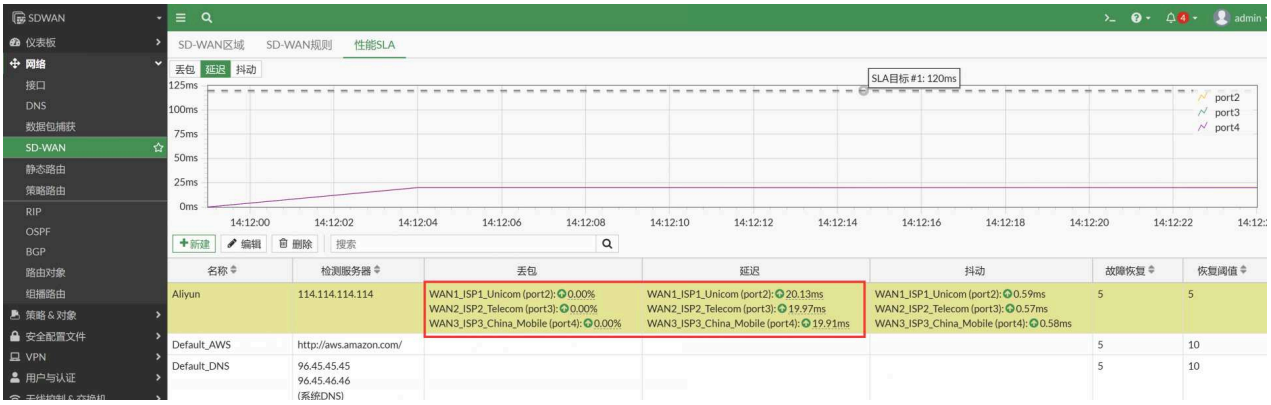

```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

3. 配置健康检查，SLA目标监控阿里云的延迟及丢包率。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system sdwan
config health-check
    edit "Aliyun"
        set server "cn.aliyun.com"
        set members 1 2 3
        config sla
            edit 1
                set link-cost-factor latency packet-loss
                set latency-threshold 120
                set packetloss-threshold 2
            next
        end
    next
end
```



4. 配置SD-WAN规则，目标为阿里云相关Internet服务，引用上步配置的SLA Target。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system sdwan
config service
    edit 1
        set name "To_Aliyun"
        set mode sla
        set src "LAN_192.168.10.0"
        set internet-service enable
        set internet-service-name "Alibaba-Alibaba.Cloud" "Alibaba-DNS" "Alibaba-ICMP" "Alibaba-NTP" "Alibaba-SSH"
"Alibaba-Web"
        config sla
            edit "Aliyun"
                set id 1
            next
        end
        set priority-members 1 2 3
    next
end
```

5. 配置安全策略允许SD-WAN流量。

重要

如果使用ippool的方式做SNAT，在SD-WAN环境下，一定要在ippool下配置绑定接口，防止ippool在SD-WAN成员中转换错误。

```
config firewall ippool
       edit xxxx
           set associated-interface port2
       next
end
```




```
config firewall policy
    edit 1
        set name "To_Internet"
        set srcintf "port8"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set webfilter-profile "default"
        set application-list "default"
        set logtraffic all
        set nat enable
    next
end
```

结果验证

1. 查看健康检查状态，三条链路均为alive状态。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(19.893), jitter(0.531), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(19.704), jitter(0.408), bandwidth-up(9999999), bandwidth-
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(19.719), jitter(0.556), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
```

2. 查看SD-WAN规则状态，出接口顺序为port2，port3，port4。

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(11), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(1 port2), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected
    2: Seq_num(2 port3), alive, sla(0x0), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 port4), alive, sla(0x0), gid(0), cfg_order(2), cost(0), selected
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

3. 查看策略路由中SD-WAN规则的列表，出接口顺序为port2，port3，port4。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2132213761(0x7f170001) vwl_service=1(To_Aliyun) vwl_mbr_seq=1 2 3 dscp_tag=0xff 0xff flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=4(port2) oif=5(port3) oif=6(port4)
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=0 last_used=2023-01-03 22:16:17
```

4. 查看路由表。

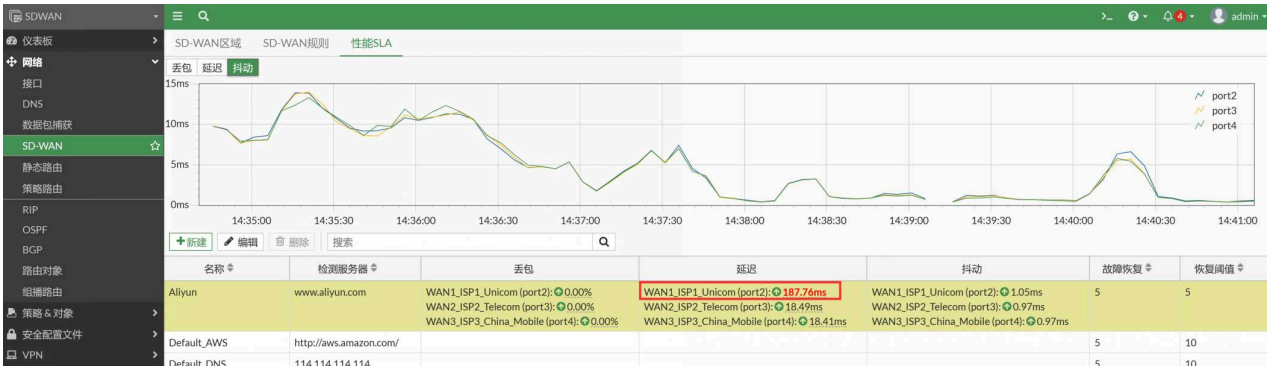
```
SDWAN # get router info routing-table all
 ...

S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
 ...
```

线路切换测试

1. 让port2的延迟超过SLA-Target。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(1.000%) latency(187.502), jitter(8.489), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(1.000%) latency(48.102), jitter(9.499), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(3 port4): state(alive), packet-loss(1.000%) latency(48.508), jitter(8.618), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
```



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 查看SD-WAN策略状态，由于port2的延迟不满足SLA Target，出接口顺序变为port3，port4，port2。

```
SDWAN # diagnose sys sdwan service

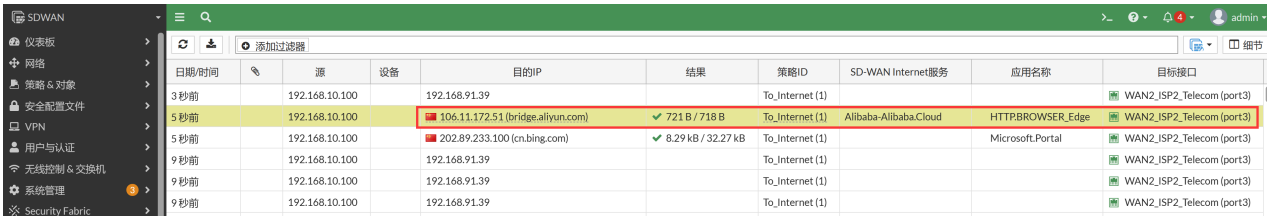
Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(6), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(2 port3), alive, sla(0×1), gid(0), cfg_order(1), cost(0), selected    //port3将会优先选择wan2进行转发
    2: Seq_num(3 port4), alive, sla(0×1), gid(0), cfg_order(2), cost(0), selected
    3: Seq_num(1 port2), alive, sla(0×0), gid(0), cfg_order(0), cost(0), selected    //port2不满足的SLA，顺序置于最后
面了
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

3. 查看策略路由列表中的SD-WAN规则，由于port2的延迟不满足SLA Target，出接口顺序变为port3，port4，port2。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2132344833(0×7f190001) vwl_service=1(To_Aliyun) vwl_mbr_seq=2 3 1 dscp_tag=0×ff 0×ff flags=0×0 tos=0×00
tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=5(port3) oif=6(port4) oif=4(port2)
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=0 last_used=2023-01-03 22:16:17
```

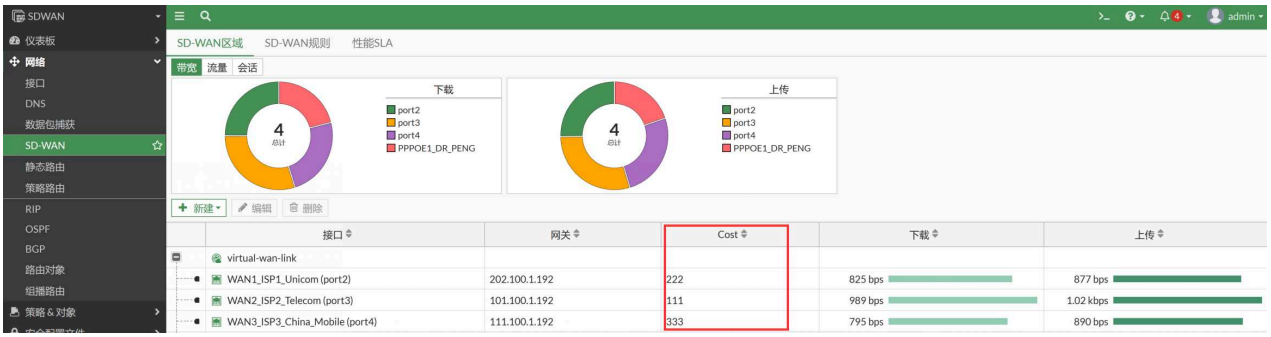
4. 使用内网PC客户端访问阿里云相关资源，查看流量日志，可以看到流量切换到了port3。



接口成员Cost值对选路的影响

1. SD-WAN接口成员的接口Cost值将影响Lowest Cost (SLA)的接口选择顺序，如果SD-WAN成员接口均达到了SLA Target，那么Cost值越小越优先，这将打破配置顺序而进行用户自定义的SD-WAN接口优先级。

2. 比如自定义：port2 Cost 222，port3 Cost 111，port4 Cost 333。此时Lowest Cost (SLA)将会优选Cost较小的WAN2，而忽略配置接口的顺序，Cost值优先进行比较。



3. 查看健康检查状态，三个接口成员均达到了SLA Target。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(20.301), jitter(0.578), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(20.225), jitter(0.610), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0×1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(20.143), jitter(0.571), bandwidth-up(9999999), bandwidth-
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
dw(9999999), bandwidth-bi(19999998) sla_map=0×1
```

4. 查看SD-WAN策略状态，Cost小的port3优先。

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(2 port3), alive, sla(0×1), gid(0), cfg_order(0), cost(111), selected    //Cost小的port3优先
    2: Seq_num(1 port2), alive, sla(0×1), gid(0), cfg_order(2), cost(222), selected
    3: Seq_num(3 port4), alive, sla(0×1), gid(0), cfg_order(1), cost(333), selected
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

5. 查看策略路由列表中的SD-WAN规则，Cost小的port3优先。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2132869121(0×7f210001) vwl_service=1(To_Aliyun) vwl_mbr_seq=2 1 3 dscp_tag=0×ff 0×ff flags=0×0 tos=0×00
tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=5(port3) oif=4(port2) oif=6(port4)
//Cost小的port3优先
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=25 last_used=2023-01-03 22:49:28
```

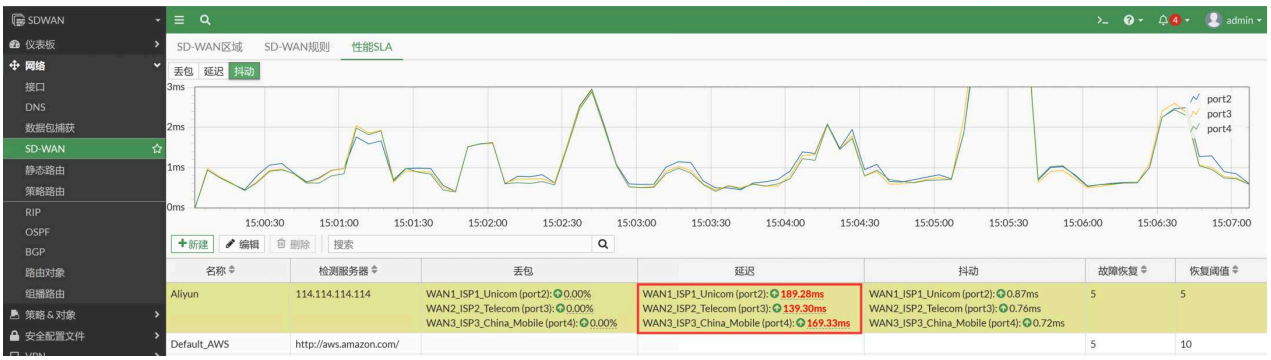
接口成员顺序对选路的影响

1. 将SD-WAN成员接口的cost全部改回0，如果port2、port3、port4 三者都无法满足SLA目标了，那么SD-WAN规则如何选择出接口呢?

2. 答案是：如果三者都无法满足SLA 目标值了，那么将会按照SD-WAN规则配置的接口顺序选择出接口，也就是以port2、port3、port4这样的顺序选择，port2将会优先转发数据。此时顺序优先。

3. 将port2、port3、port4的延迟调整超过SLA Target。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(156.008), jitter(2.069), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0×0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(186.951), jitter(2.078), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0×0
Seq(3 port4): state(alive), packet-loss(0.000%) latency(176.968), jitter(2.055), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0×0
```



4. 查看SD-WAN规则状态，全部不符合SLA Target的时候，按照配置的接口顺序进行选择出接口。

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(sla), sla-compare-order
  Members(3):
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    1: Seq_num(1 port2), alive, sla(0x0), gid(0), cfg_order(0), cost(0), selected    //全部不符合的时候，按照配置的接口顺序进行选择出接口
    2: Seq_num(2 port3), alive, sla(0x0), gid(0), cfg_order(1), cost(0), selected
    3: Seq_num(3 port4), alive, sla(0x0), gid(0), cfg_order(2), cost(0), selected
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0) Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

5. 查看策略路由列表，全部不符合SLA Target的时候，按照配置的接口顺序进行选择出接口。

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2133131265(0x7f250001) vwl_service=1(To_Aliyun) vwl_mbr_seq=1 2 3 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=4(port2) oif=5(port3) oif=6(port4)
//全部不符合的时候，按照配置的接口顺序进行选择出接口
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0) Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=25 last_used=2023-01-03 22:49:28
```

sla-compare-method number对选路的影响

1. 上述情况的一个补充命令：如果全部不符合则相对于没有SLA Target了，这显然不够合理，还有优化的空间，这时候就引出了另外一个参数：set sla-compare-method number。

2. SD-WAN规则可以调用多个SLA Target，然后优化计算的方法。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system sdwan
config service
    edit 1
…
        config sla
            edit "Aliyun"
                set id 1
            next
            edit "114_Check"
                set id 1
            next
            edit "Default_DNS"
                set id 1
            next
            edit "Default_Office_365"
                set id 1
            next
        end
…
        set sla-compare-method order    //默认值，如果按此设置，多个SLA目标之间的逻辑关系是and，只要有其中一个SLA目标不符合，则将该接口剔除SD-WAN规则的选择，如果SLA全部失效，则按照配置的接口顺序进行选择出接口
…
    next
end
```

3. 默认情况下，CLI下SLA的设置为set sla-compare-method order，如果按此设置，多个SLA目标之间的逻辑关系是and，只要有其中一个SLA目标不符合，则将该接口剔除SD-WAN规则的选择，如果SLA全部失效，则按照配置的接口顺序进行选择出接口。

```
SDWAN (1) # set sla-compare-method
order     Compare SLA value based on the order of health-check.
number    Compare SLA value based on the number of satisfied health-check.  Limits health-checks to only
configured member interfaces.
```

4. set sla-compare-method numbe，此参数是SLA目标全部失效的一个补充，如果全部失效，则选择失败数较小的接口进行SD-WAN流量的转发，比如port2失败2个，port3失败3个，port4失败1个，则会选择port4进行数据的转发。

5. 我们配置多个服务器的SLA Target，在SD-WAN规则里面也调用多个SLA Target，然后虽然全部都失败了，但是可以选择符合SLA Target条件更多的接口作为SD-WAN规则的出接口，在全部失败的矮子中选择一个最优的出接口。当然我们需要设置不同的目的IP进行健康检查，同时配置不同的SLA条目，在SD-WAN规则调用的时候也只能调用不同服务器的SLA目标，才可以进行这样的进一步比较。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于轮询的Maximize Bandwidth (SLA)

> **重要**
>
> ADVPN目前不支持Maximize Bandwidth (SLA)模式。

概念介绍

SLA

Service-Level Agreement，服务品质协议，是服务提供者和客户之间的一个协议，用来保证可计量的网络性能达到所定义的服务品质。SD-WAN的选路基于这个SLA品质标准来判断，SD-WAN规则保障让流量一直走符合SLA品质的链路出去。从而达到业务/客户的SLA品质要求。

SLA-Target

1. SD-WAN可定义SLA-Targets设置最低保障的延迟、抖动和丢包率，一旦超过SLA-Targets提供的保障最低值，则立即切换另外一条线路，以确保持续提供SLA-Targets品质级别的服务。
2. SLA Target 有三种类型的判断阈值：
   - Latency (ms)
   - Jitter (ms)
   - Packet Loss (%)




```bash
config system sdwan
    config health-check
    edit "114_Check"
        set server "114.114.114.114"
        set members 0
        config sla
            edit 1
                set latency-threshold 200
                set packetloss-threshold 2
            next
            edit 2
                set latency-threshold 250
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set jitter-threshold 10
                set packetloss-threshold 5
            next
            edit 3
                set latency-threshold 300
                set jitter-threshold 15
                set packetloss-threshold 8
            next
        end
    next
end
```

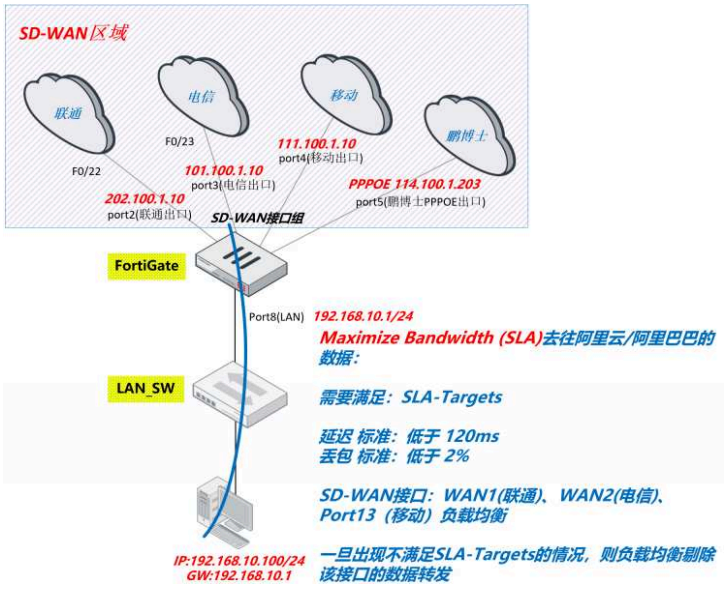
3. **Lowest Cost (SLA) 和Maximize Bandwidth (SLA)都需要调用SLA Target，基于SLA Target进行相关的判断和选路。**

选路原则

1. 只有满足SLA-Targets的出接口才有机会被选中，如果低于SLA-Targets的接口将会被移除选中列表中。
2. 如果有多个接口满足SLA-Targets，这些接口将按照配置的负载方式进行负载均衡来转发SD-WAN的流量，以便达到带宽最大利用率的效果。
3. 负载方法支持round-robin（默认）、source-ip-based、source-dest-ip-based、inbandwidth、outbandwidth、bibandwidth。
4. 本文使用round-robin模式为例，所有流量将按循环顺序等量分配到SD-WAN规则中的成员接口（前提是该接口满足SLA target）。
5. Maximize Bandwidth (SLA)基于SLA-Targets进行工作，因此首先需要在SD-WAN状态检查里面配置具体的SLA-Targets标准，然后再SD-WAN规则中选择相应的SLA-Targets，只有符合选择的SLA-Targets标准的出口，才会被SD-WAN规则所计算并用于出口数据的转发，符合SLA-Targets的接口都会被用于数据的转发，多个接口按照配置的负载方式进行负载均衡处理。

配置举例

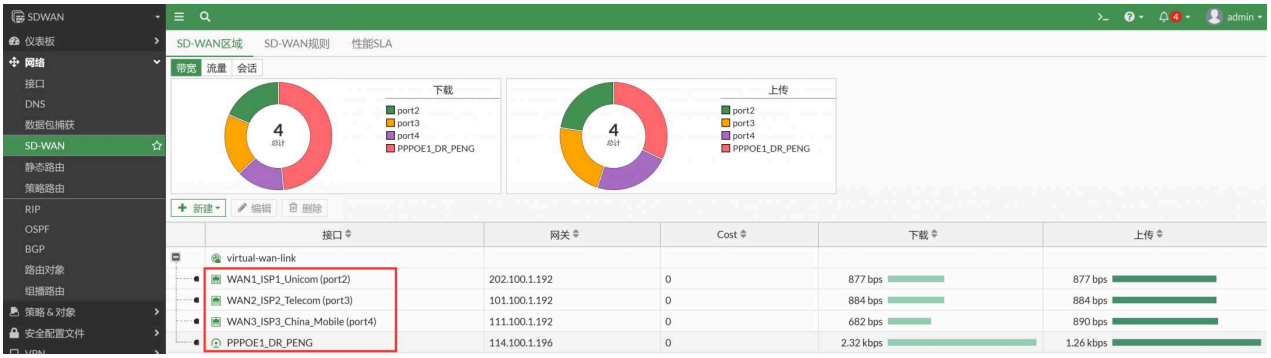
网络拓扑



配置步骤

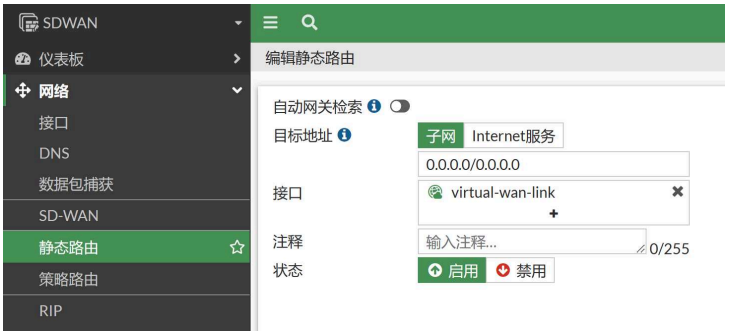
1. 不需要配置SD-WAN成员接口的预估带宽，当Maximize Bandwidth (SLA)类型的SD-WAN规则使用`round-robin`作为hash-mode时（默认配置），SD-WAN不会考虑接口的带宽使用率，SD-WAN会以轮询的方式将流量送至满足SLA target的成员接口。
2. SD-WAN接口成员定义。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "port2"
            set gateway 202.100.1.192
        next
        edit 2
            set interface "port3"
            set gateway 101.100.1.192
        next
        edit 3
            set interface "port4"
            set gateway 111.100.1.192
        next
        edit 4
            set interface "PPPOE1_DR_PENG"
        next
    end
 end
```

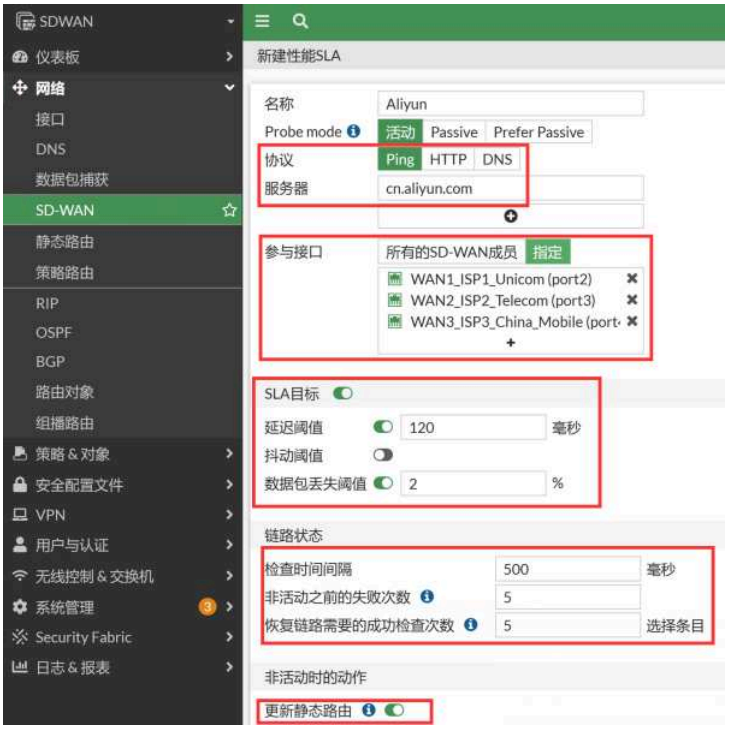
3. 配置SD-WAN关联的默认路由。



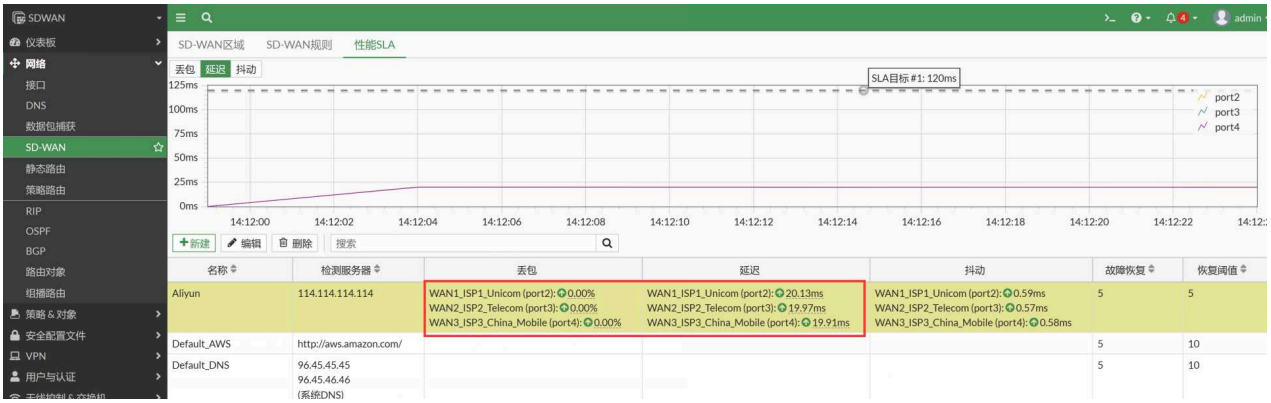

```
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

4. 配置健康检查，SLA目标监控阿里云的延迟及丢包率。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system sdwan
config health-check
    edit "Aliyun"
        set server "cn.aliyun.com"
        set members 1 2 3
        config sla
            edit 1
                set link-cost-factor latency packet-loss
                set latency-threshold 120
                set packetloss-threshold 2
            next
        end
    next
end
```



5. 配置SD-WAN规则，目标为阿里云相关Internet服务，引用上步配置的SLA Target，默认的负载方式为轮询，负载方式只能在CLI下修改。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system sdwan
config service
    edit 1
        set name "To_Aliyun"
        set mode load-balance
        set hash-mode round-robin    //默认负载方式为轮询，即基于会话的负载
        set src "LAN_192.168.10.0"
        set internet-service enable
        set internet-service-name "Alibaba-Alibaba.Cloud" "Alibaba-DNS" "Alibaba-ICMP" "Alibaba-NTP" "Alibaba-SSH"
"Alibaba-Web"
        config sla
            edit "Aliyun"
                set id 1
            next
        end
        set priority-members 1 2 3
    next
end
```

6. 配置安全策略允许SD-WAN流量。

重要

如果使用ippool的方式做SNAT，在SD-WAN环境下，一定要在ippool下配置绑定接口，防止ippool在SD-WAN成员中转换错误。

```
config firewall ippool
       edit xxxx
           set associated-interface port2
       next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 1
        set name "To_Internet"
        set srcintf "port8"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set webfilter-profile "default"
        set application-list "default"
        set logtraffic all
        set nat enable
    next
end
```

结果验证

1. 查看健康检查状态，三条链路均为alive状态。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(29.467), jitter(1.361), bandwidth-up(9999998), bandwidth-dw(9999998), bandwidth-bi(19999996) sla_map=0x1
Seq(2 port3): state(alive), packet-loss(0.000%) latency(29.235), jitter(1.343), bandwidth-up(9999997), bandwidth-dw(9999995), bandwidth-bi(19999992) sla_map=0x1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(29.169), jitter(1.304), bandwidth-up(9999998), bandwidth-dw(9999998), bandwidth-bi(19999996) sla_map=0x1
```

2. 查看SD-WAN规则状态。

```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Members(3):
    1: Seq_num(1 port2), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(2 port3), alive, sla(0x1), gid(2), num of pass(1), selected
    3: Seq_num(3 port4), alive, sla(0x1), gid(2), num of pass(1), selected
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0) Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

3. 查看策略路由中SD-WAN规则的列表，符合SLA目标的接口就会用于基于会话的负载均衡。

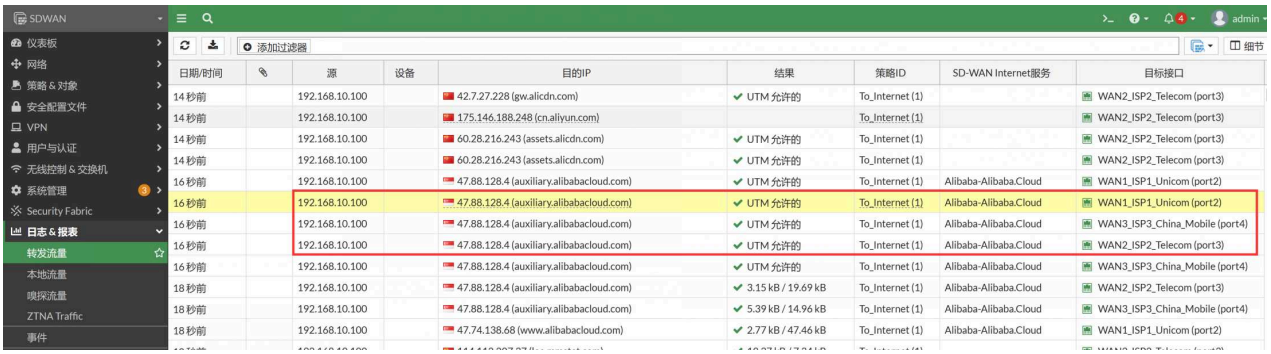
```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2133458945(0x7f2a0001) vwl_service=1(To_Aliyun) vwl_mbr_seq=1 2 3 dscp_tag=0xff 0xff flags=0x10 load-balance hash-mode=round-robin  tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3)
oif=4(port2) num_pass=1 oif=5(port3) num_pass=1 oif=6(port4) num_pass=1
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0) Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=25 last_used=2023-01-03 22:49:28
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 查看路由表。

```
SDWAN # get router info routing-table all
 ...

S*      0.0.0.0/0 [1/0] via 101.100.1.192, port3, [1/0]
                  [1/0] via 111.100.1.192, port4, [1/0]
                  [1/0] via 114.100.1.196, PPPOE1_DR_PENG, [1/0]
                  [1/0] via 202.100.1.192, port2, [1/0]
 ...
```

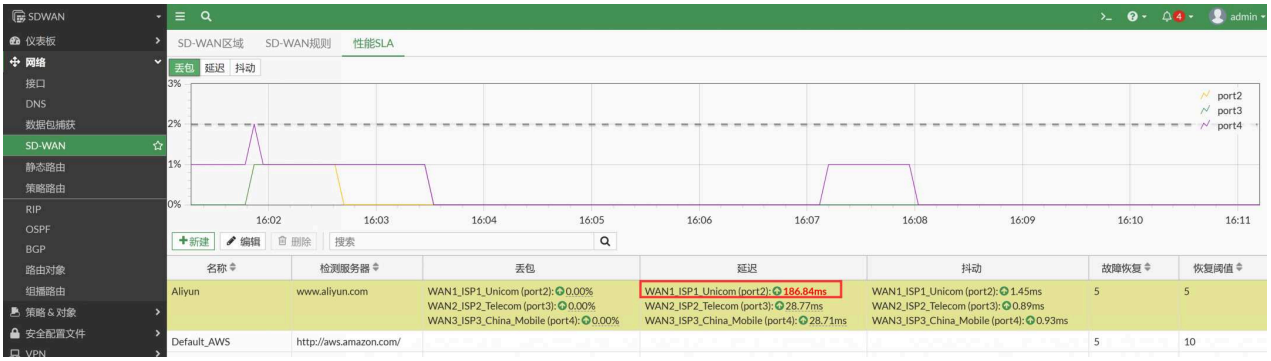
5. 查看SD-WAN设备的流量日志，可以看到客户端访问阿里云相关的业务时，会根据轮询算法负载到三条线路上。



线路切换测试

1. 让port2的延迟超过SLA-Target。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(187.104), jitter(0.777), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x0    //超过SLA的目标值
Seq(2 port3): state(alive), packet-loss(0.000%) latency(28.857), jitter(0.705), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
Seq(3 port4): state(alive), packet-loss(0.000%) latency(28.824), jitter(0.750), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x1
```



2. 查看SD-WAN规则状态，port2不符合SLA目标，从接口列表中剔除，SLA置位为0x0。

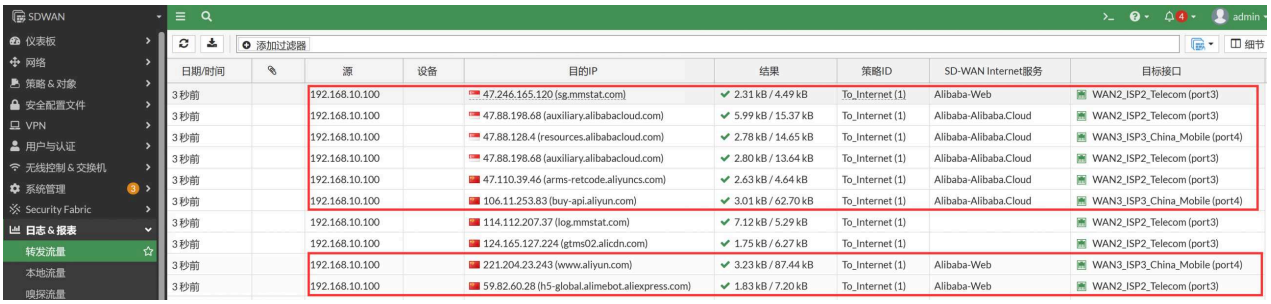
```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Members(3):
    1: Seq_num(2 port3), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(3 port4), alive, sla(0x1), gid(2), num of pass(1), selected
    3: Seq_num(1 port2), alive, sla(0x0), gid(2), num of pass(0), selected  //不符合SLA目标，从接口列表中剔除，SLA置位为
0x0
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 查看策略路由列表，port2的num_pass为0，不用于数据转发。

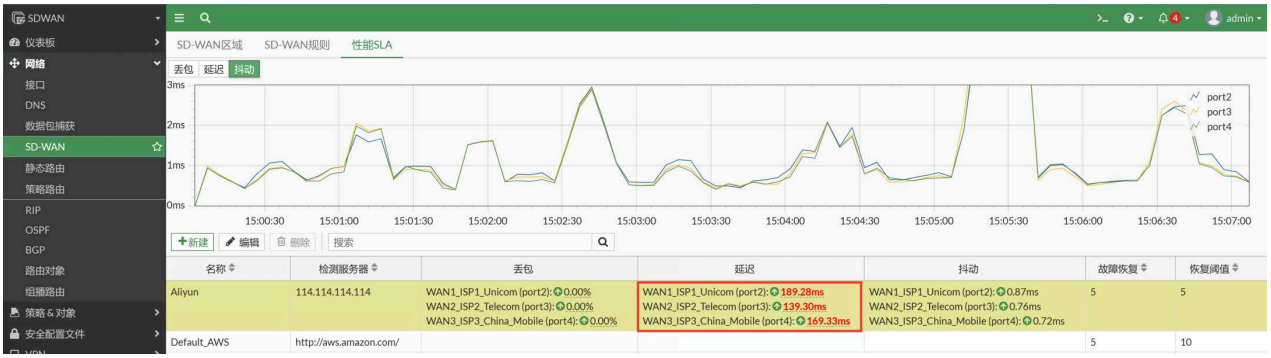
```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2133458945(0x7f2a0001) vwl_service=1(To_Aliyun) vwl_mbr_seq=2 3 1 dscp_tag=0xff 0xff flags=0x10 load-balance
hash-mode=round-robin  tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3)
oif=5(port3) num_pass=1 oif=6(port4) num_pass=1 oif=4(port2) num_pass=0    //port2不用于数据转发
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=86 last_used=2023-01-04 00:02:56
```

4. 查看SD-WAN设备的流量日志，客户端访问阿里云的流量被负载均衡到port3和port4上，不会负载到port2上。



5. 如果port2、port3、port4 三者都无法满足SLA目标了，那么SD-WAN规则如何选择出接口呢？将三条链路的延迟均调整为无法满足SLA Target。

```
SDWAN # diagnose sys sdwan health-check
Health Check(Aliyun):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(182.008), jitter(2.069), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(139.951), jitter(2.078), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x0
Seq(3 port4): state(alive), packet-loss(0.000%) latency(168.968), jitter(2.055), bandwidth-up(9999999), bandwidth-
dw(9999999), bandwidth-bi(19999998) sla_map=0x0
```



6. 答案是：如果三者都无法满足SLA 目标值了，那么还是将会以port2、port3、port4进行基于会话的负载均衡转发。

7. 查看SD-WAN规则状态，三条链路均被选中。

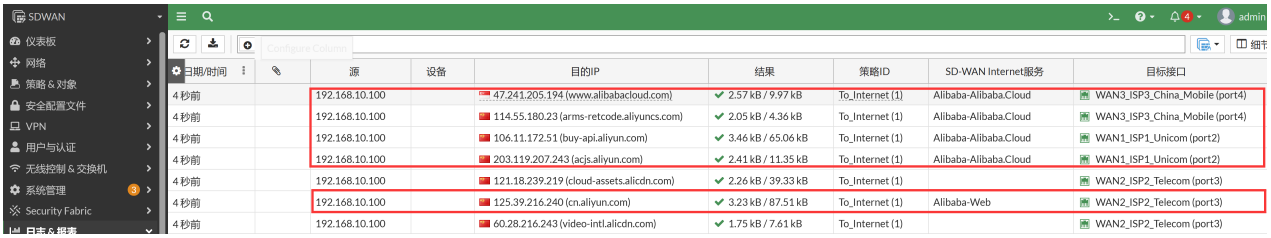
```
SDWAN # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
  Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance  hash-mode=round-robin)
  Members(3):
    1: Seq_num(1 port2), dead, sla(0x0), gid(1), num of pass(0), selected
    2: Seq_num(2 port3), alive, sla(0x0), gid(2), num of pass(0), selected
    3: Seq_num(3 port4), alive, sla(0x0), gid(2), num of pass(0), selected
  Internet Service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

8. 查看策略路由列表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SDWAN # diagnose firewall proute list
list route policy info(vf=root):

id=2133458945(0x7f2a0001) vwl_service=1(To_Aliyun) vwl_mbr_seq=1 2 3 dscp_tag=0xff 0xff flags=0x10 load-balance
hash-mode=round-robin  tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3)
oif=4(port2) num_pass=0 oif=5(port3) num_pass=0 oif=6(port4) num_pass=0
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(6): Alibaba-Alibaba.Cloud(6881402,0,0,0) Alibaba-DNS(6881283,0,0,0) Alibaba-ICMP(6881282,0,0,0)
Alibaba-NTP(6881288,0,0,0) Alibaba-SSH(6881286,0,0,0) Alibaba-Web(6881281,0,0,0)
hit_count=25 last_used=2023-01-03 22:49:28
```

9. 查看SD-WAN设备的流量日志，依旧会在三条链路进行负载均衡。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于带宽的Maximize Bandwidth (SLA)

> **重要**
>
> ADVPN目前不支持Maximize Bandwidth (SLA)模式。

原理介绍

1. FGT监控每个接口的带宽，每秒中更新一次，SDWAN成员的优先级根据可用带宽从高到低排序。当流量匹配到该规则时，FGT将选择第一个成员进行转发。

2. Maximize Bandwidth有三种基于带宽的算法：

```bash
FortiGate # config system sdwan
FortiGate # config service
FortiGate # edit 1
FortiGate # set hash-mode ?

round-robin             All traffic are distributed to selected interfaces in equal portions and circular order.
source-ip-based         All traffic from a source IP is sent to the same interface.
source-dest-ip-based    All traffic from a source IP to a destination IP is sent to the same interface.
inbandwidth             All traffic are distributed to a selected interface with most available bandwidth for
incoming traffic.
outbandwidth            All traffic are distributed to a selected interface with most available bandwidth for
outgoing traffic.
bibandwidth             All traffic are distributed to a selected interface with most available bandwidth for both
incoming and outgoing traffic.
```

网络拓扑



配置步骤

1. 配置预估带宽。

```bash
config system interface
    edit "port1"
        set ip 202.101.1.1 255.255.255.0
        set estimated-upstream-bandwidth 200000
        set estimated-downstream-bandwidth 200000
    next
    edit "port2"
        set ip 202.101.2.1 255.255.255.0
        set estimated-upstream-bandwidth 100000
        set estimated-downstream-bandwidth 100000
    next
end
```

2. 配置SD-WAN。

```bash
config system sdwan
    set status enable
    config zone
        edit "Internet"
        next
    end
    config members
        edit 1
            set interface "port1"
            set zone "Internet"
            set gateway 202.101.1.2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        next
        edit 2
            set interface "port2"
            set zone "Internet"
            set gateway 202.101.2.2
        next
    end
    config health-check
        edit "100.100.100.1"
            set server "100.100.100.1"
            set members 0
            config sla
                edit 1
                    set latency-threshold 100
                    set jitter-threshold 100
                next
            end
        next
    end
config service
    edit 1
        set name "test1"
        set mode load-balance
        set hash-mode inbandwidth
        set dst "all"
        set src "10.0.0.0/8"
        config sla
            edit "100.100.100.1"
                set id 1
            next
        end
        set priority-members 1 2
        next
    end
end

```

3. 配置上网策略。

```bash
config firewall policy
    edit 3
        set srcintf "port3"
        set dstintf "Internet"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

负载方法说明

1. 当 hash-mode 是inbandwidth时，sdwan只监控inbandwith的带宽，可以在接口下只配置：estimated-downstream-bandwidth。如下所示，初始port1剩余带宽200M，port2剩余带宽100M，port1优先。

```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
Members(2):
1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 199991Kbps, selected  //port1优先//
2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 99993Kbps, selected
Src address(1):
10.0.0.0-10.255.255.255

Dst address(1):
0.0.0.0-255.255.255.255
```

2. 当 hash-mode是outbandwidth时，sdwan只监控outbandwith的带宽，可以在接口下只配置：estimated-upstream-bandwidth。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200
Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
Members(2):
1: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 199997Kbps, selected //port1优先//
2: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
Src address(1):
10.0.0.0-10.255.255.255

Dst address(1):
0.0.0.0-255.255.255.255
```

3. 当 hash-mode 是bibandwidth时，sdwan监控的是inbandwidth和outbandwith的带宽之和，需要配置：estimated-upstream-bandwidth和estimated-downstream-bandwidth。

```bash
diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200
Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=bibandwidth)
Members(2):
1: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), bibandwidth: 399988Kbps, selected //port1优先//
2: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), bibandwidth: 199992Kbps, selected
Src address(1):
10.0.0.0-10.255.255.255

Dst address(1):
0.0.0.0-255.255.255.255
```

效果验证

iPerf测试

1. 使用iperf测试，hash-mode设置为outbandwidth，因为iperf打流是upload。

```bash
server命令：iperf3 -s   //默认监听端口5201//
client命令：iperf3 -c 100.100.100.2 -t 6000 -b 150M
```

2. iperf第1条流150M。

```
# iperf3 -c 100.100.100.2 -b 150M -t 6000  //client记录
Connecting to host 100.100.100.2, port 5201
[  4] local 10.1.1.2 port 50470 connected to 100.100.100.2 port 5201
[ ID] Interval           Transfer     Bandwidth       Retr  Cwnd
[  4]   0.00-1.00   sec  16.2 MBytes   136 Mbits/sec    0    389 KBytes
[  4]   1.00-2.00   sec  17.9 MBytes   150 Mbits/sec    0    389 KBytes
[  4]   2.00-3.00   sec  17.9 MBytes   150 Mbits/sec    0    389 KBytes
[  4]   3.00-4.00   sec  17.9 MBytes   150 Mbits/sec    0    389 KBytes
[  4]   4.00-5.00   sec  17.9 MBytes   150 Mbits/sec    0    400 KBytes
[  4]   5.00-6.00   sec  17.9 MBytes   150 Mbits/sec    0    400 KBytes
[  4]   6.00-7.00   sec  17.9 MBytes   150 Mbits/sec    0    400 KBytes
[  4]   7.00-8.00   sec  17.9 MBytes   150 Mbits/sec    0    400 KBytes
```

3. SDWAN监控，每隔10s，敲一次diagnose sys sdwan service查看接口的带宽及SDWAN的排序，SDWAN逐渐监测到接口使用了150M的带宽，约为60s。

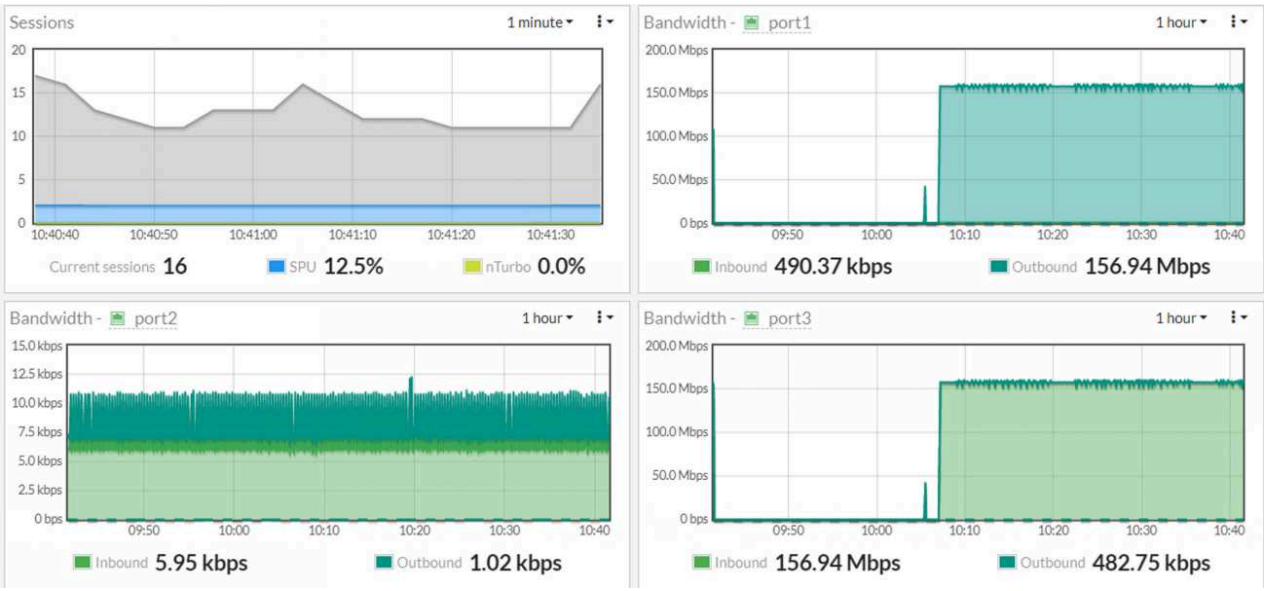
```
# diagnose sys sdwan service  //初始
Service(1): Address Mode(IPV4) flags=0×200
  Gen(5), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 199997Kbps, selected //port1剩余的可用带宽多，port1优先
    2: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# diagnose sys sdwan service //10s
Service(1): Address Mode(IPV4) flags=0×200
  Gen(5), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 171669Kbps, selected
    2: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service //20s
Service(1): Address Mode(IPV4) flags=0×200
  Gen(5), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 140229Kbps, selected
    2: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service //30s

Service(1): Address Mode(IPV4) flags=0×200
  Gen(5), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 108768Kbps, selected
    2: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service //40s
Service(1): Address Mode(IPV4) flags=0×200
  Gen(6), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected  //port2剩余的可
用带宽超过port1，port优先
    2: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 77328Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service  //50s
Service(1): Address Mode(IPV4) flags=0×200
  Gen(6), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
    2: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 45866Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service //60s
Service(1): Address Mode(IPV4) flags=0×200
  Gen(6), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected
    2: Seq_num(1 port1), alive, sla(0×1), gid(2), num of pass(1), outbandwidth: 42754Kbps, selected //1分钟的时间，
port1的带宽监测到使用了150M，剩余40多M
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```

4. 查看接口流量图和会话，第1条iperf的流从port1转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 查看会话列表。

```bash
# diagnose sys session list
session info: proto=6 proto_state=01 duration=1534 expire=3590 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->9/9->11 gwy=202.101.1.2/10.1.1.2
hook=pre dir=org act=noop 10.1.1.2:50482->100.100.100.2:5201(0.0.0.0:0)
hook=post dir=reply act=noop 100.100.100.2:5201->10.1.1.2:50482(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=0
serial=00731dbb tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=132/136, ipid=136/132, vlan=0x0000/0x0000
vlifid=136/132, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=1/1
session info: proto=6 proto_state=01 duration=1534 expire=2065 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=112/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->9/9->11 gwy=202.101.1.2/10.1.1.2
hook=pre dir=org act=noop 10.1.1.2:50480->100.100.100.2:5201(0.0.0.0:0)
hook=post dir=reply act=noop 100.100.100.2:5201->10.1.1.2:50480(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=0
serial=00731dba tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=132/136, ipid=136/132, vlan=0x0000/0x0000
vlifid=136/132, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=5/5
total session 2

# diagnose netlink interface list  | grep port1
if=port1 family=00 type=1 index=9 mtu=1500 link=0 master=0
```

6. 使用diagnose sys sdwan intf-sla-log port1查看 port1监控的带宽也是一样的效果，逐渐查看到port1的带宽消耗了150M。

```bash
#diagnose sys sdwan intf-sla-log port1
Timestamp: Wed Dec 15 17:38:11 2021, used inbandwidth: 78029bps, used outbandwidth: 5949335bps, used bibandwidth:
6027364bps, tx bytes: 4837359868bytes, rx bytes: 20421280bytes.
Timestamp: Wed Dec 15 17:38:21 2021, used inbandwidth: 206010bps, used outbandwidth: 37408566bps, used
bibandwidth: 37614576bps, tx bytes: 5034405643bytes, rx bytes: 21255211bytes.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Timestamp: Wed Dec 15 17:38:31 2021, used inbandwidth: 315768bps, used outbandwidth: 68591735bps, used
bibandwidth: 68907503bps, tx bytes: 5229856283bytes, rx bytes: 21990459bytes.
Timestamp: Wed Dec 15 17:38:41 2021, used inbandwidth: 455947bps, used outbandwidth: 100163534bps, used
bibandwidth: 100619481bps, tx bytes: 5427312580bytes, rx bytes: 22883469bytes.
Timestamp: Wed Dec 15 17:38:51 2021, used inbandwidth: 564881bps, used outbandwidth: 131613259bps, used
bibandwidth: 132178140bps, tx bytes: 5624002692bytes, rx bytes: 23577318bytes.
Timestamp: Wed Dec 15 17:39:01 2021, used inbandwidth: 628638bps, used outbandwidth: 157006755bps, used
bibandwidth: 157635393bps, tx bytes: 5818652090bytes, rx bytes: 24350270bytes.
```

7. iperf打第2条流80M。

```bash
server命令：iperf3 -s -p 5202
client命令：iperf3 -c 100.100.100.2 -t 6000 -b 80M -p 5202
```

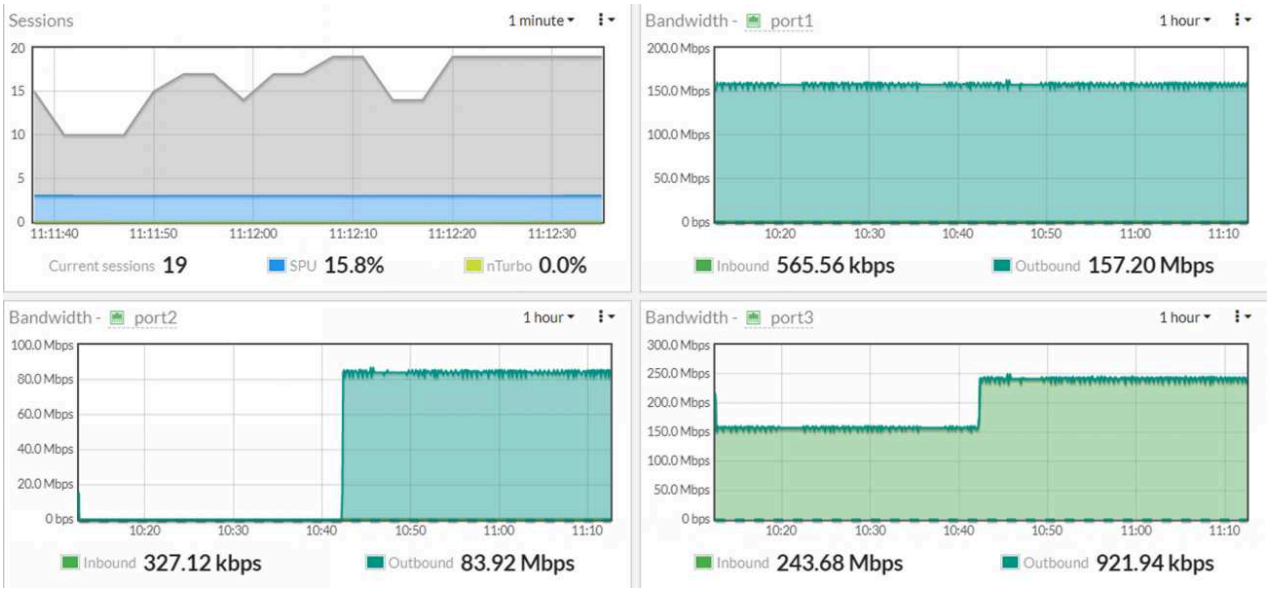
8. SDWAN监控，查看接口的带宽及SDWAN的排序。

```bash
# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 99999Kbps, selected //开始打第2条流
前，port2优先
    2: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 42732Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

 # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 76158Kbps, selected
    2: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 42754Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

 # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 59404Kbps, selected
    2: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 43062Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

 # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 42453Kbps, selected
    2: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 42424Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

 # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 42832Kbps, selected  //port1剩余的可
用带宽多，port1变优先
    2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 25853Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        0.0.0.0-255.255.255.255

 # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=outbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 42832Kbps, selected
    2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), outbandwidth: 25853Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```

9. 查看接口流量图和会话，第2条iperf流从port2转发。第1条iperf流无变化。



.0. 查看会话列表。

```bash
# diagnose sys session list
session info: proto=6 proto_state=01 duration=478 expire=3121 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->10/10->11 gwy=202.101.2.2/10.1.1.3
hook=pre dir=org act=noop 10.1.1.3:59558->100.100.100.2:5202(0.0.0.0:0)
hook=post dir=reply act=noop 100.100.100.2:5202->10.1.1.3:59558(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=0
serial=0073229b tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=134/136, ipid=136/134, vlan=0x0000/0x0000
vlifid=136/134, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/2

session info: proto=6 proto_state=01 duration=478 expire=3590 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->10/10->11 gwy=202.101.2.2/10.1.1.3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

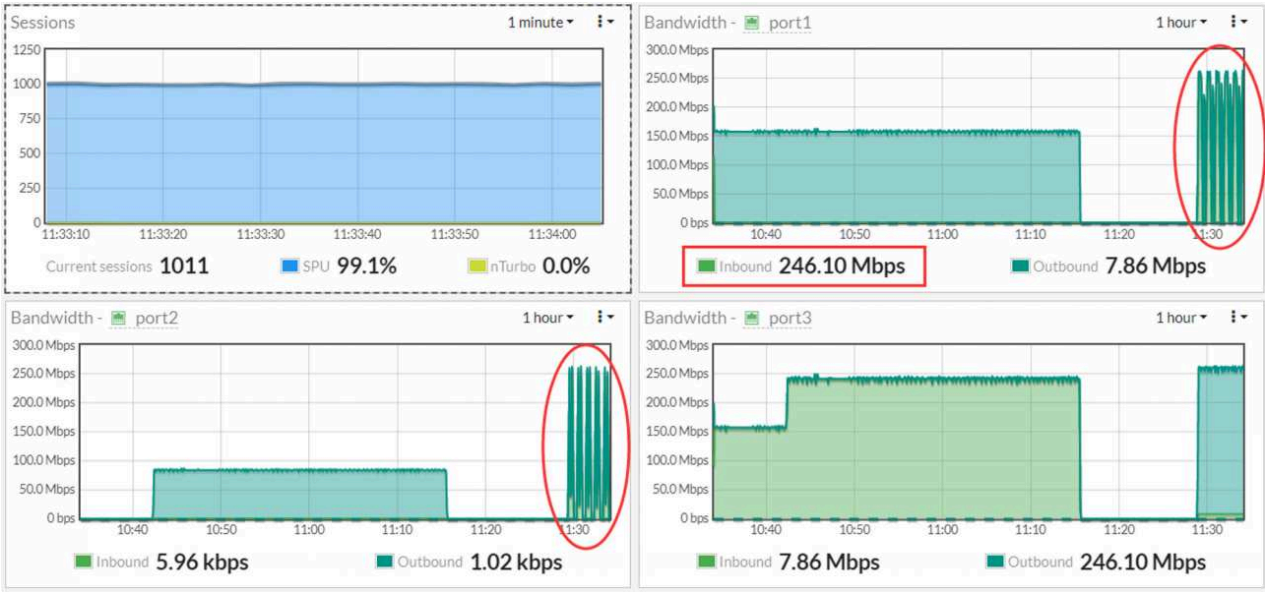
```
hook=pre dir=org act=noop 10.1.1.3:59560->100.100.100.2:5202(0.0.0.0:0)
hook=post dir=reply act=noop 100.100.100.2:5202->10.1.1.3:59560(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=4 auth_info=0 chk_client_info=0 vd=0
serial=0073229c tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=2 sdwan_service_id=1
rpdb_link_id=ff000001 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x000c00
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=134/136, ipid=136/134, vlan=0x0000/0x0000
vlifid=136/134, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=6/6
total session 2

# diagnose netlink interface list | grep port2
if=port2 family=00 type=1 index=10 mtu=1500 link=0 master=0
```

FortiTester测试

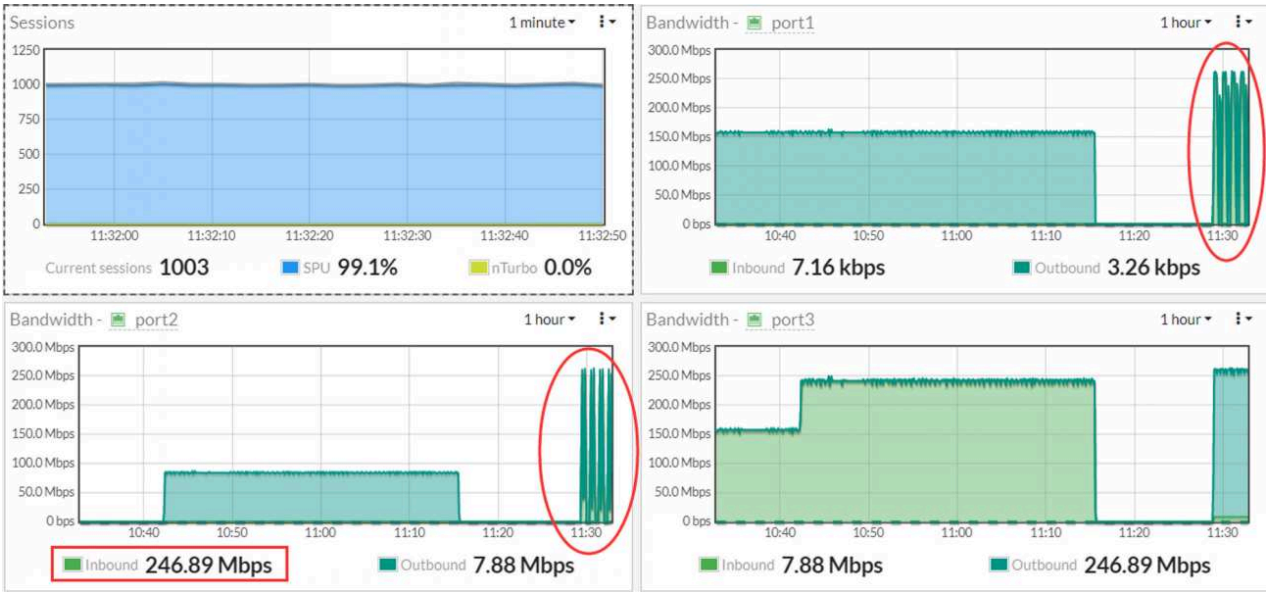
1. hash-mode设置为inbandwidth，因为iperf打流是download，cps=1000，get 30kb。

```bash
# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 199991Kbps, selected //port1优先//
    2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 99993Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```

2. 从接口流量图看，流量一会从port1走，一会从port2，没有负载到两条链路，是由于FortiTester 打流新建会话和拆除会话太快，SDWAN带宽监控反应不过来。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 对应的SD-WAN服务状态。

```bash
# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(13), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 48600Kbps, selected
    2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 0Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(13), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 48600Kbps, selected
    2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 0Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(14), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 48225Kbps, selected
    2: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 554Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255

# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(14), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 48225Kbps, selected
    2: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 554Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

真实流量测试

1. 使用迅雷下载一部电影，速度平均5.2MB/s左右，查看接口带宽分配的实际效果。

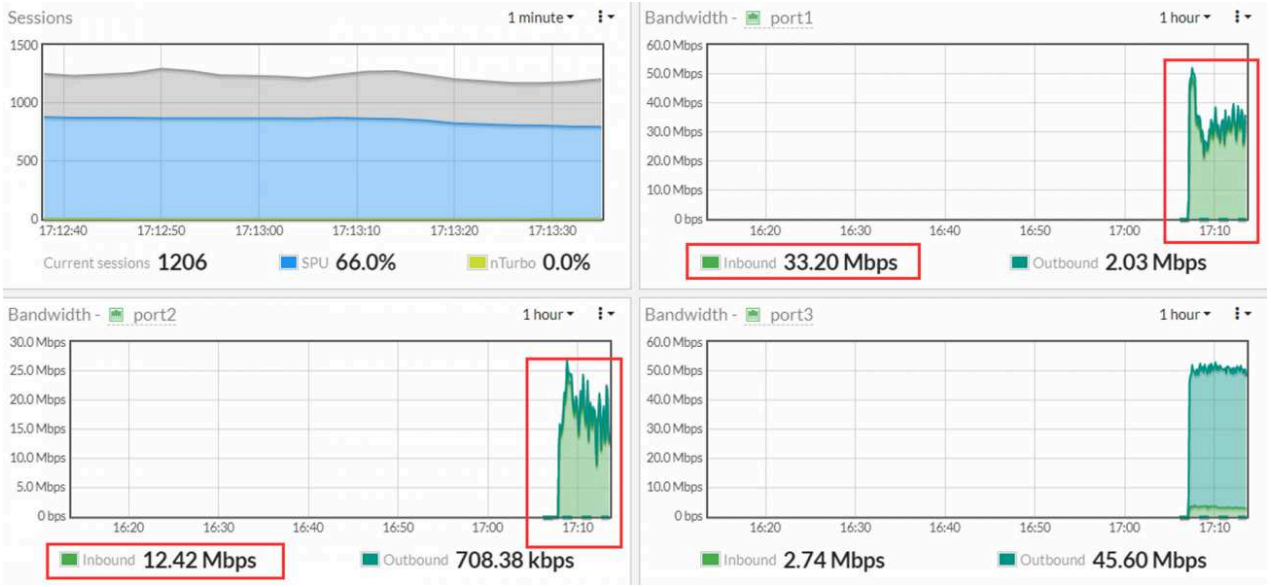
2. 公网实际带宽不大，因此将预估带宽调小，hash-mode使用inbandwidth。

```bash
config system interface
    edit "port1"
        set ip 202.101.1.1 255.255.255.0
        set estimated-upstream-bandwidth 40000
        set estimated-downstream-bandwidth 40000
    next
    edit "port2"
        set vdom "root"
        set estimated-upstream-bandwidth 20000
        set estimated-downstream-bandwidth 20000
    next
end
```

3. 对应的SD-WAN服务状态。

```bash
# diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=inbandwidth)
  Members(2):
    1: Seq_num(1 port1), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 39936Kbps, selected
    2: Seq_num(2 port2), alive, sla(0x1), gid(2), num of pass(1), inbandwidth: 19993Kbps, selected
  Src address(1):
        10.0.0.0-10.255.255.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```

4. 对应带宽图。



总结

1. 基于带宽的Maximize Bandwidth适用于流量缓慢增长，多会话的场景。
2. 下面两种情况不适用：
   - 只有一条会话，且带宽很大，是不会切换的。
   - 突发流量，短时间流量很大，SD-WAN无法及时感知。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

将已关联接口移至SD-WAN区域

网络需求

某台FortiGate已经部署上线，上线时没有使用SD-WAN功能，公网接口已被其他配置引用。现在客户想在这台FortiGate上开启SD-WAN功能，但删除接口关联的配置太过麻烦，容易出现意外，同时影响业务的时间也较长。

解决方法

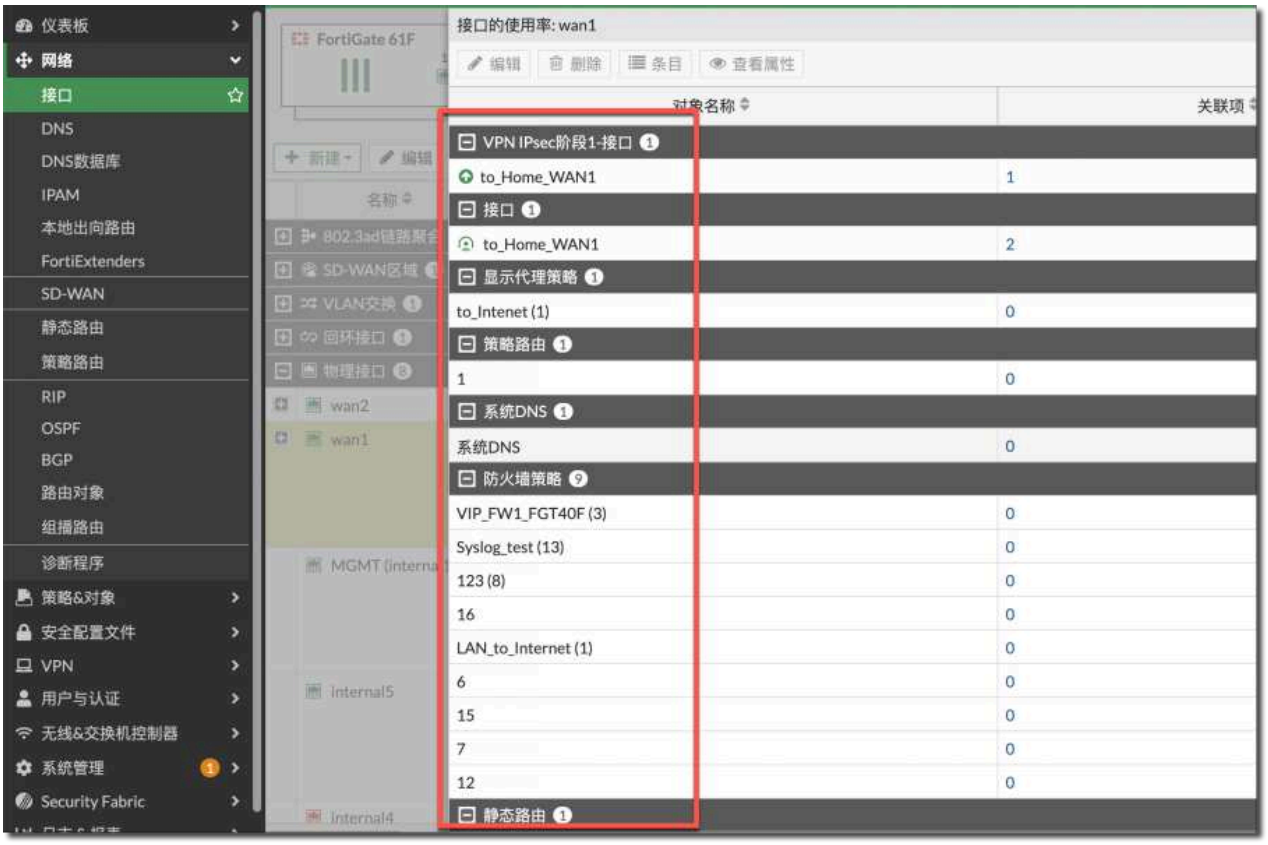
从FortiOS 7.0版本开始，FortiGate支持将已被其他配置关联的接口直接加入SD-WAN区域（不需要删除接口关联的配置）。并自动修改关联配置中引用的接口为SD-WAN区域。

配置步骤

重要

如果FortiGate为HA模式，且需要加入SD-WAN区域的接口被HA监控接口引用，请先手动将该接口从HA监控接口移除。将接口加入SD-WAN区域后，再手动将接口加回HA监控接口。

1. 在一台wan1、wan2接口已经被其他配置引用的FortiGate上，想要将wan1和wan2加入SD-WAN区域。查看wan1和wan2的接口引用，此时直接在SD-WAN区域中加入wan1和wan2是无法执行的。

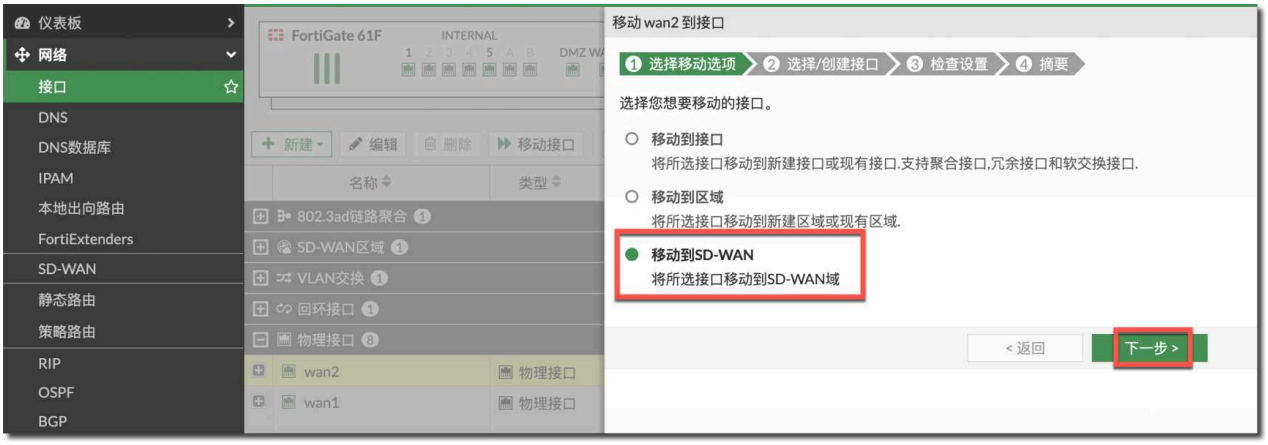


2. 右键点击要加入SD-WAN区域的接口（这里以wan2为例），然后在“设置状态”中选择“移动接口”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在右侧弹出的窗口中，选择“移动到SD-WAN”选项，点击下一步。

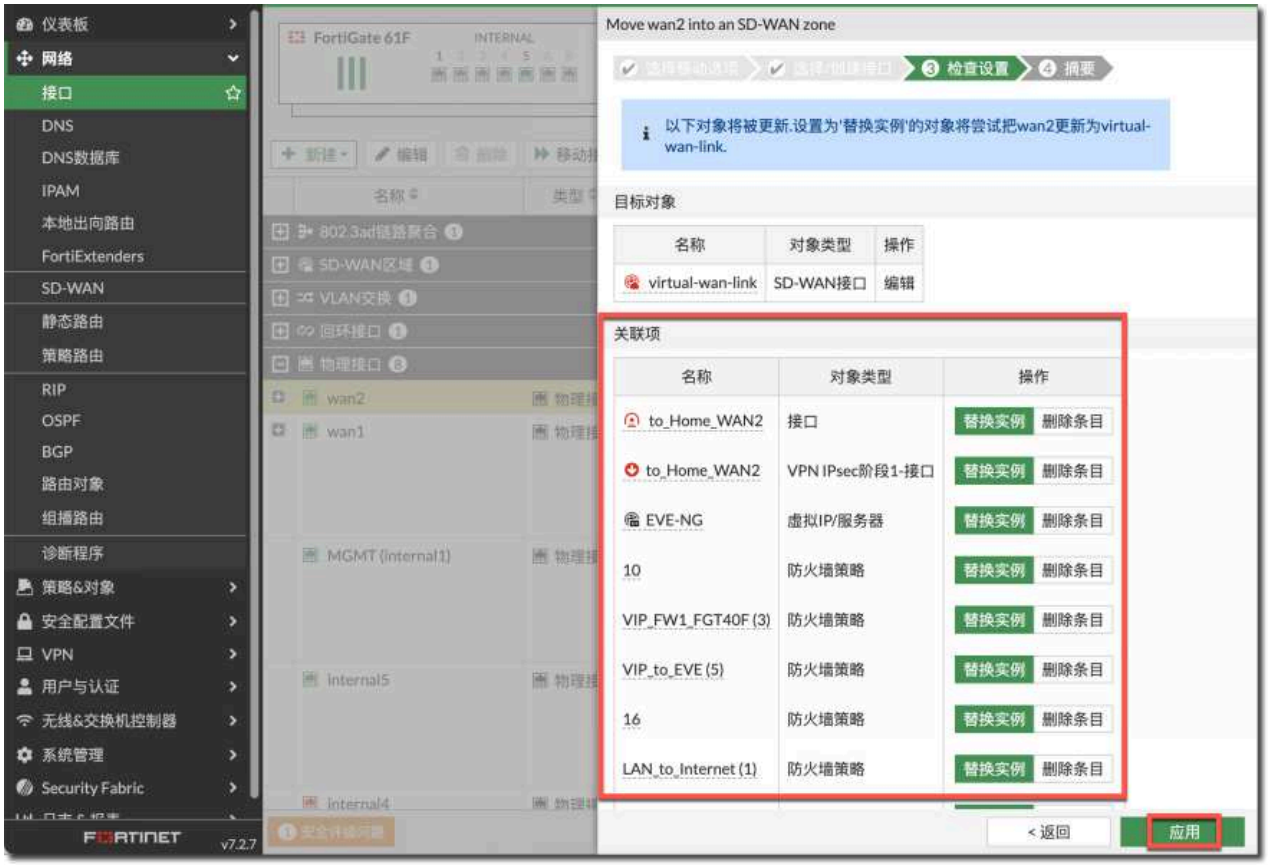


4. 选择要加入的SD-WAN区域，这里以“virtual-wan-link为例”，点击下一步。

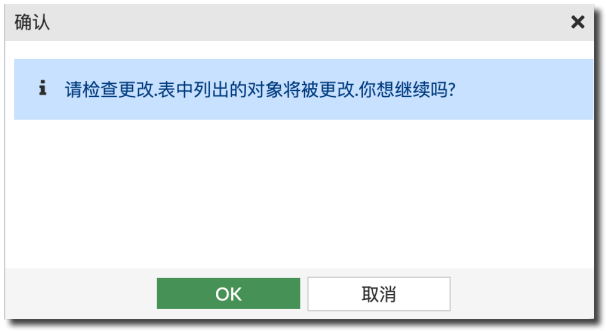


5. “检查设置”步骤中显示关联的配置中的接口将从wan2替换为SD-WAN区域virtual-wan-link（也可以修改为“删除”操作）。检查无误后，点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

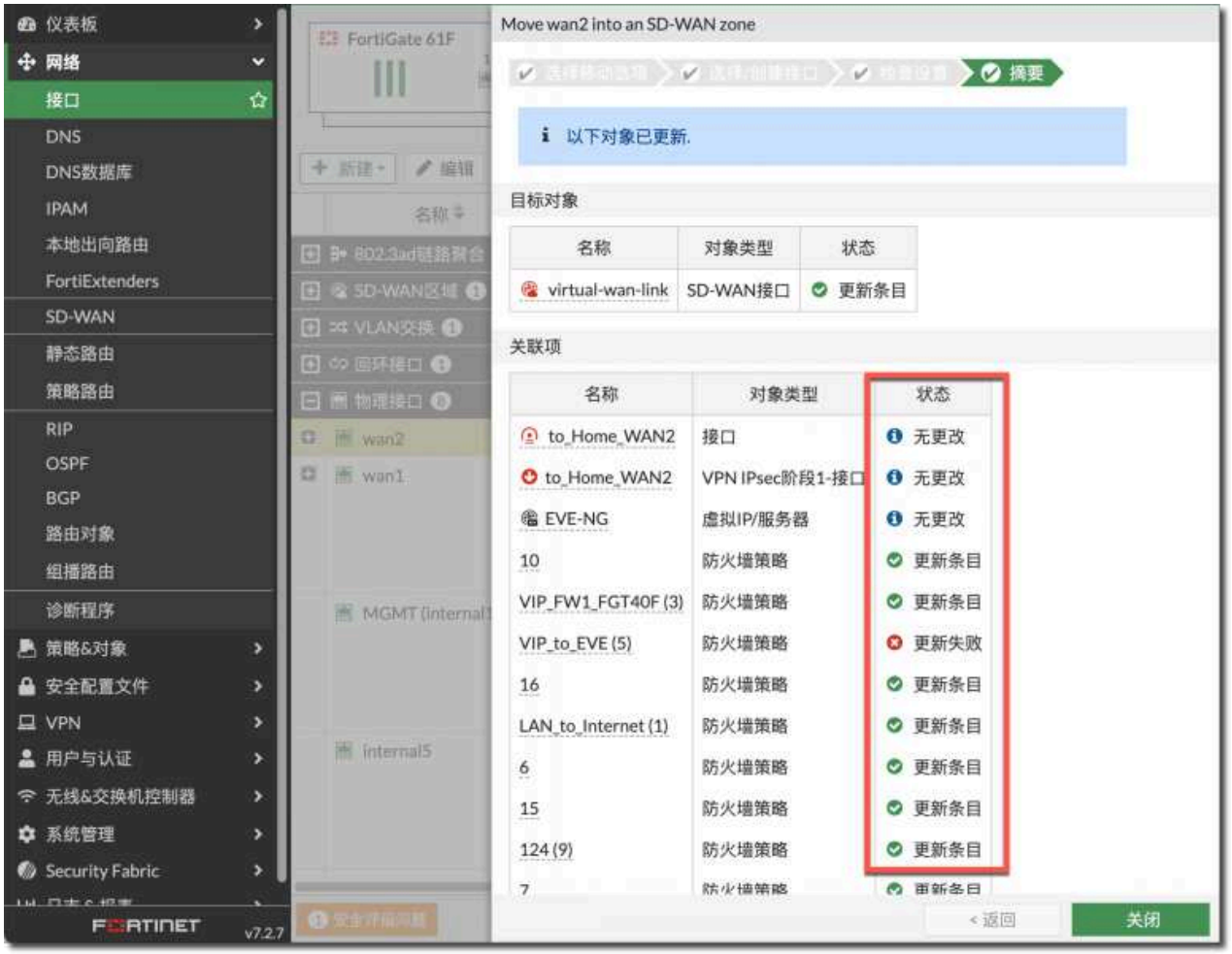


6. 随后会弹出确认窗口，点击OK。



7. 执行完成后会显示执行结果，不需要取消关联的配置会显示“无更改”，已经替换为SD-WAN区域的配置会显示“更新条目”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



结果验证

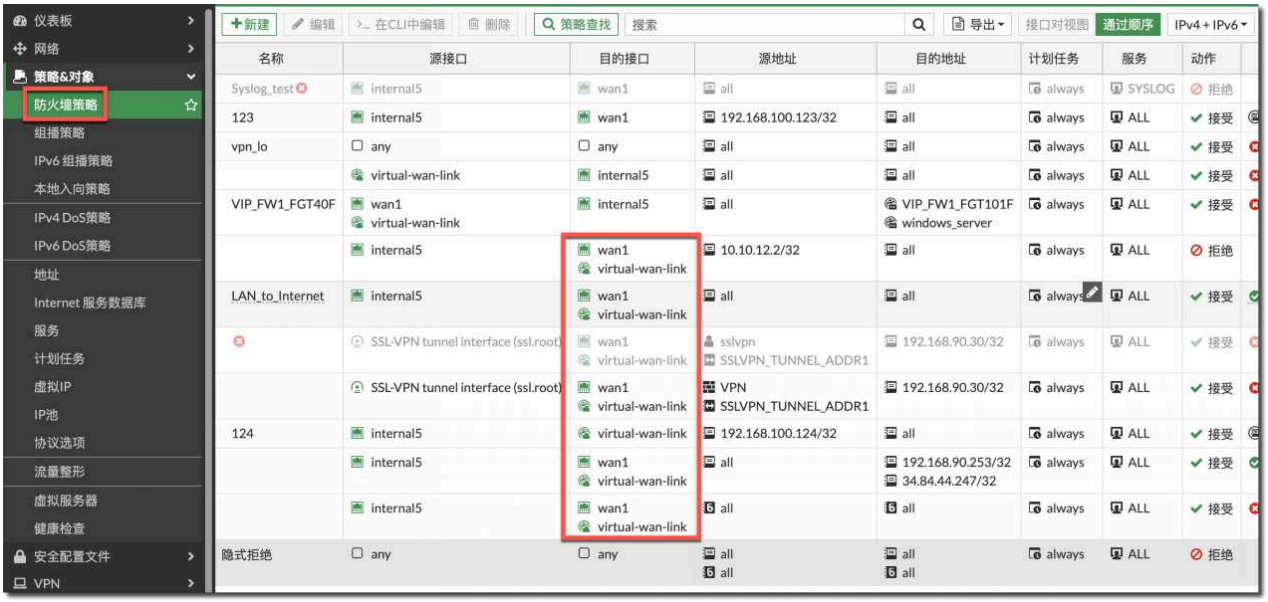
1. 查看SD-WAN区域的成员，wan2已经成功加入（需要手动配置成员的网关）。




```bash
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 2
            set interface "wan2"
        next
    end
end
```

2. 查看防火墙策略，所有原来wan2关联的策略中，wan2都被替换为SD-WAN区域“virtual-wan-link”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

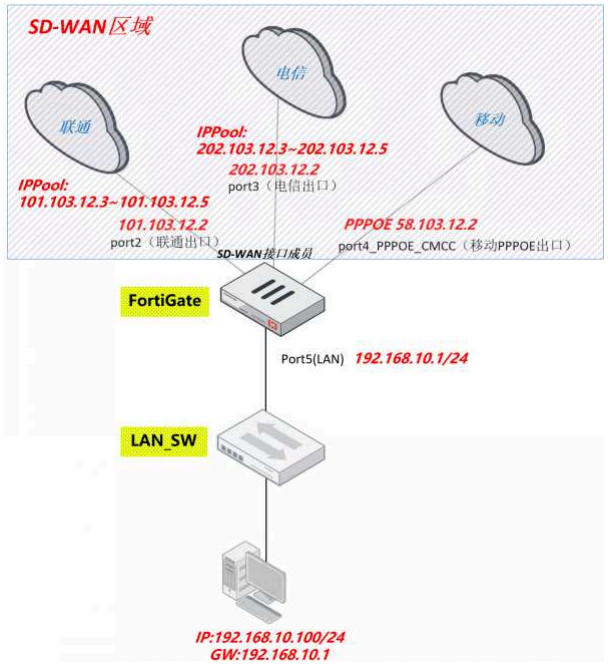


3. 其他不需要替换的关联配置或没有引用wan2的配置不会有变化。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

互联网出口场景

网络拓扑与需求

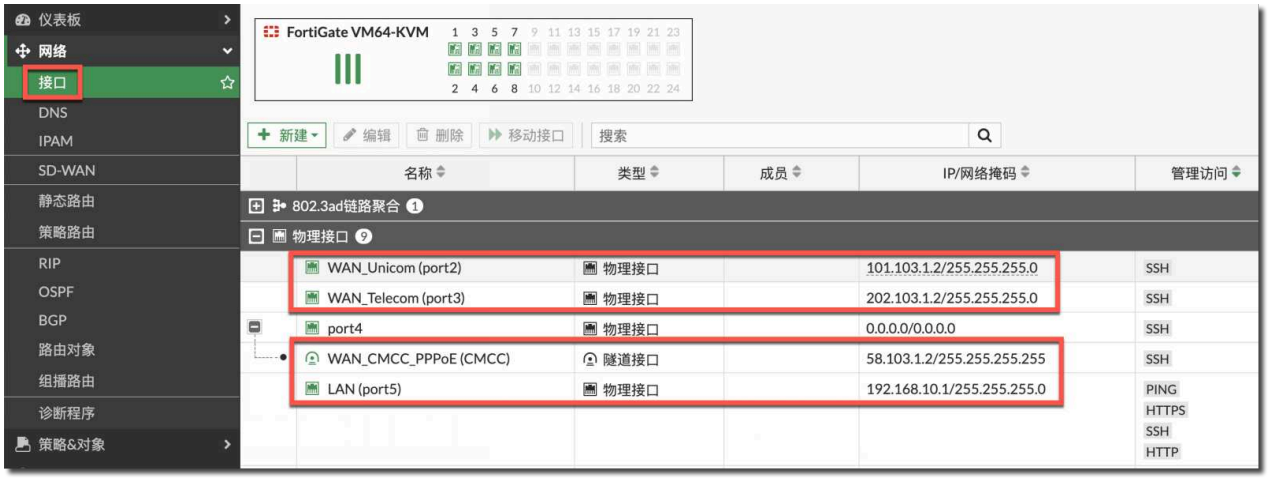


1. FortiGate通过三个运营商（联通、电信、移动）接入Internet，其中联通和电信线路为固定IP，移动线路为PPPoE线路。
2. 联通和电信线路使用运营商分配的IPPool转换SNAT访问Internet，移动线路借用PPPoE接口IP作为SNAT的源地址访问Internet。
3. 配置SD-WAN，基于应用、用户、ISDB等做选路的调用，可以实现更加智能的互联网出口选择和备份，这也是SD-WAN的价值所在。
4. 部署SD-WAN通常在一个全新的设备进行配置，如果需要加入SD-WAN区域的接口已经被其他配置（如防火墙策略）引用，是无法直接加入SD-WAN区域的。要加入SD-WAN区域，又不想删除关联的配置，请参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域 ↗章节。

配置步骤

SD-WAN基础配置

1. 配置三条运营商线路的IP或PPPoE用户（PPPoE请通过CLI配置，参考部署前注意事项→PPPoE接口配置 ↗章节）与内网口IP。



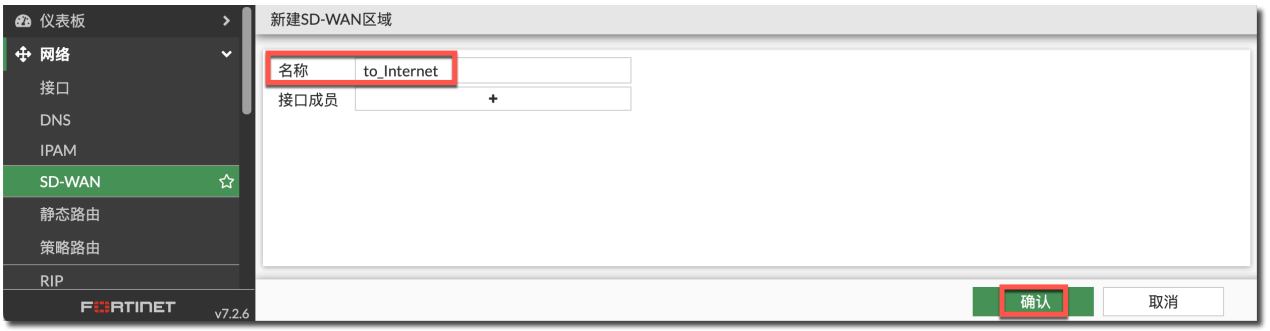

```bash
PPPoE接口配置:
config system pppoe-interface
    edit "CMCC"
        set device "port4"
        set username "user1"
        set password xxxxxxxx
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end

固定IP接口配置:
config system interface
    edit "port2"
        set vdom "root"
        set ip 101.103.1.2 255.255.255.0
        set allowaccess ssh
        set alias "WAN_Unicom"
    next
    edit "port3"
        set vdom "root"
        set ip 202.103.1.2 255.255.255.0
        set allowaccess ssh
        set alias "WAN_Telecom"
    next
    edit "port5"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh http
        set alias "LAN"
    next
end

```

2. 进入FortiGate的网络→SD-WAN→SD-WAN区域页面，新建用于访问Internet的区域“to_Internet”（也可以直接使用预置的SD-WAN区域）。








```bash
config system sdwan
    set status enable
    config zone
        edit "to_Internet"
        next
```

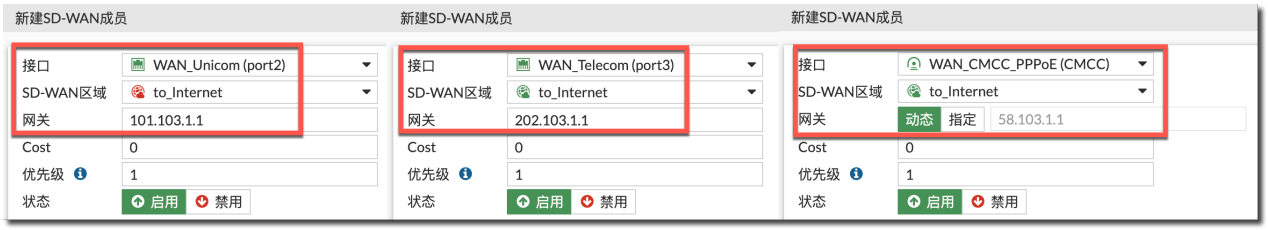

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    end
end
```

3. 在此页面新建用于访问Internet的SD-WAN成员（联通、电信、移动线路3个接口）加入上步创建的SD-WAN区域，注意PPPoE加入SD-WAN区域时不需要填写网关。

> **重要**
>
> 如果WAN接口存在相关配置引用的情况下，是无法直接加入到SD-WAN接口成员的，可参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域↗章节快速将接口加入SD-WAN区域，并自动修改关联配置（也可选择手动将WAN接口的相关配置删除引用，包括策略、Link-monitor、所属区域等）。








```bash
config system sdwan
    config members
        edit 1
            set interface "port2"
            set zone "to_Internet"
            set gateway 101.103.1.1
        next
        edit 2
            set interface "port3"
            set zone "to_Internet"
            set gateway 202.103.1.1
        next
        edit 3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set interface "CMCC"
            set zone "to_Internet"
        next
    end
end
```

4. 配置默认路由指向SD-WAN区域“to_Internet”。




```bash
config router static
    edit 1
        set distance 1
        set sdwan-zone "to_Internet"
    next
end
```

5. 查看FortiGate路由表，默认路由在三个运营商线路上负载。

```bash
FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.1.1, port3, [1/0]
                  [1/0] via 58.103.1.1, CMCC, [1/0]
                  [1/0] via 101.103.1.1, port2, [1/0]
C       58.103.1.1/32 is directly connected, CMCC
C       58.103.1.2/32 is directly connected, CMCC
C       101.103.1.0/24 is directly connected, port2
C       192.168.10.0/24 is directly connected, port5
C       202.103.1.0/24 is directly connected, port3
```

6. 配置联通和电信线路的IPPool，并绑定对应的WAN接口。

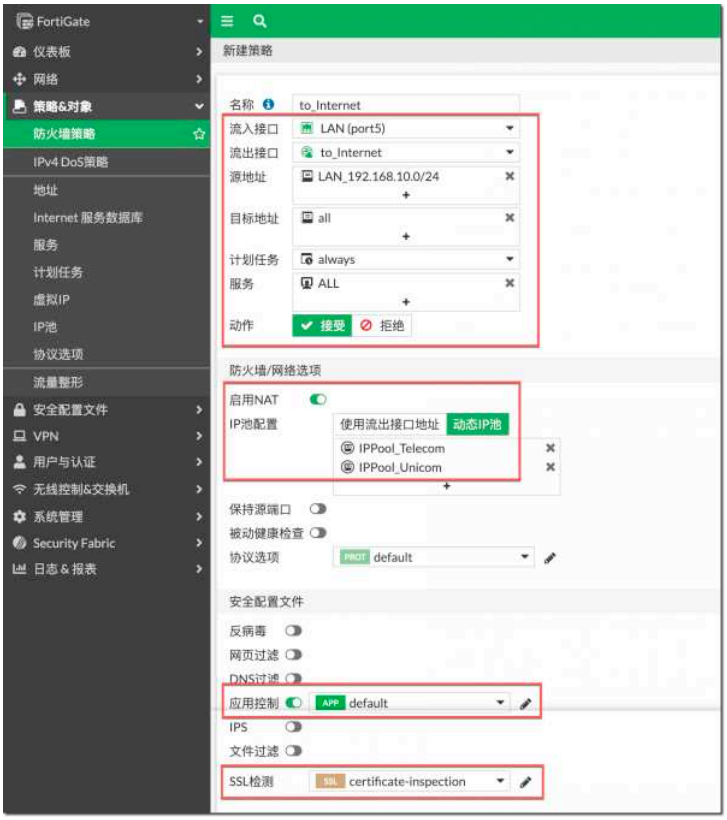
> **重要**
>
> 重要：在SD-WAN场景下，防火墙上网策略选用出接口时只能选择SD-WAN区域接口“to_Internet”（Central-NAT模式例外），不能选择具体的WAN接口，所以配置IPPool时必须将IPPool与具体的WAN接口绑定，否则FortiGate只会使用防火墙策略中配置的第一个IPPool做SNAT。

```bash
config firewall ippool
    edit "IPPool_Unicom"
        set startip 101.203.1.3
        set endip 101.203.1.5
        set associated-interface "port2"
    next
    edit "IPPool_Telecom"
        set startip 202.103.1.3
        set endip 202.103.1.5
        set associated-interface "port3"
    next
end
```

7. 配置防火墙策略，放通内网port5（LAN）到三个运营商线路的Internet访问，并开启SNAT，引用联通和电信线路上的IPPool，开启应用控制功能，用于SD-WAN策略基于应用的识别。

> **重要**
>
> 有了第6步中IPPool关联接口的配置，防火墙策略的SNAT引用IPPool时，会使用具体WAN接口上关联的IPPool中的地址来执行SNAT，而移动线路（PPPoE）则仍会使用出接口地址来作为SNAT的源地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



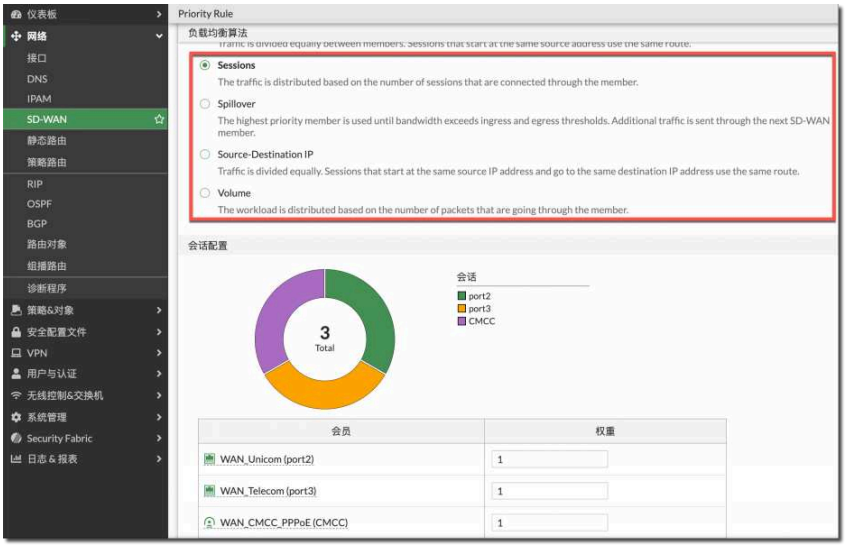

```bash
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port5"
        set dstintf "to_Internet"
        set action accept
        set srcaddr "LAN_192.168.10.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "default"
        set nat enable
        set ippool enable
        set poolname "IPPool_Telecom" "IPPool_Unicom"
    next
end
```

8. 此时SD-WAN的基本配置已经完成，如果不配置SD-WAN规则，所有的访问Internet的流量将会按照源IP负载均衡的方式，也就是我们手工配置的SD-WAN默认路由，按照三条默认路由进行负载均衡处理，如下默认隐式SD-WAN策略所示，编辑此策略，可以修改为其他负载模式。




```bash
config system sdwan
    set load-balance-mode source-ip-based
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



SD-WAN策略配置

需求举例1

<u>去往AWS的重要业务从联通或电信线路（固定IP），选择延迟较低的出口出去。</u>

1. 配置去往AWS的HTTP健康检查。

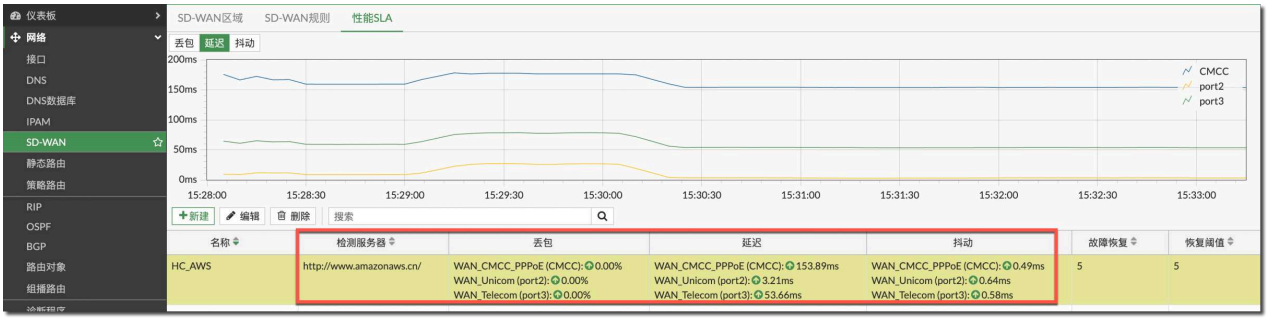





```bash
config system sdwan
    config health-check
        edit "HC_AWS"
            set server "www.amazonaws.cn"
            set protocol http
            set members 0
        next
    end
end
```

2. 查看健康检查的状态，可以看到目前联通线路延迟最低，其次是电信线路，移动线路延迟最高。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



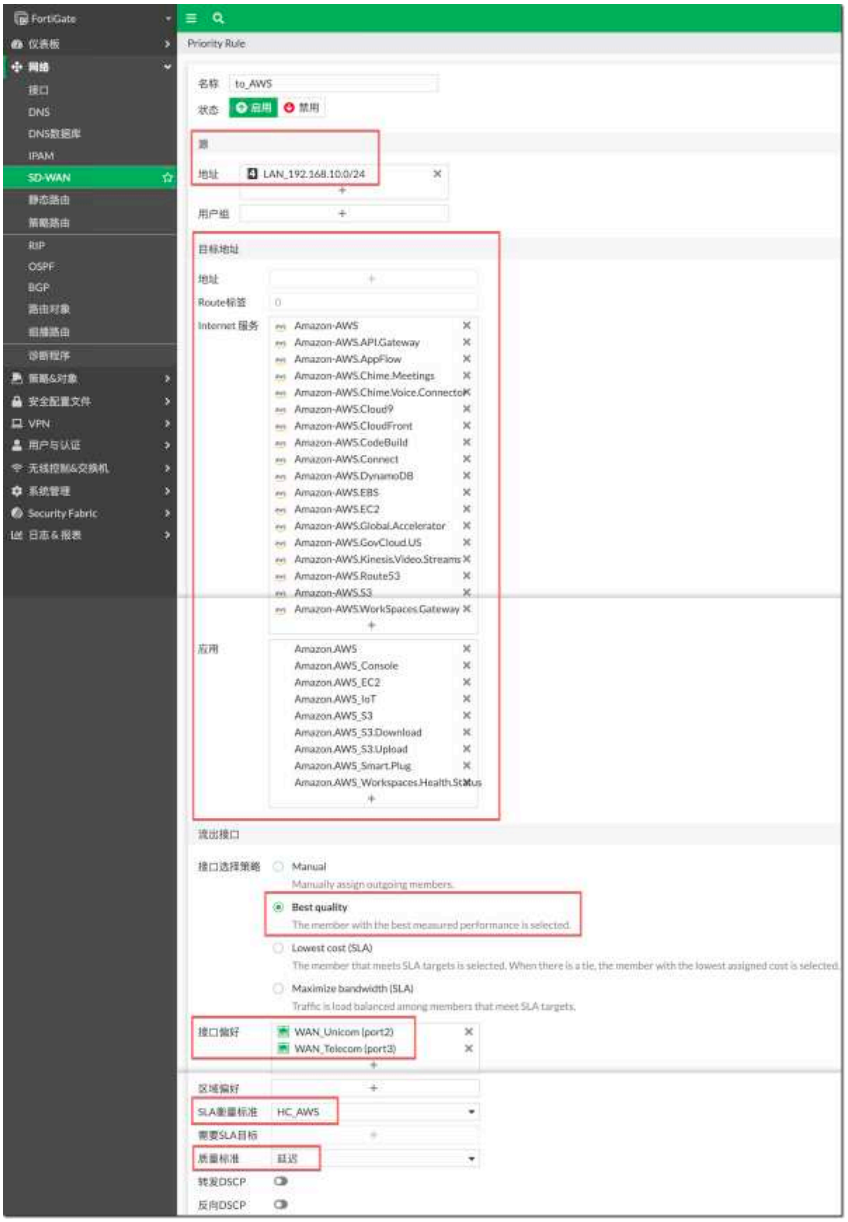

```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(HC_AWS):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(3.216), jitter(0.347), mos(4.402), bandwidth-up(65534995), bandwidth-dw(65534993), bandwidth-bi(131069988) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(53.634), jitter(0.451), mos(4.376), bandwidth-up(65534995), bandwidth-dw(65534993), bandwidth-bi(131069988) sla_map=0x0
Seq(3 CMCC): state(alive), packet-loss(0.000%) latency(153.830), jitter(0.392), mos(4.307), bandwidth-up(65534995), bandwidth-dw(65534993), bandwidth-bi(131069988) sla_map=0x0
```

3. 新建SD-WAN规则1：

- 源地址选择内网网段；目标地址使用ISDB，选择AWS相关的ISDB条目，以及AWS相关的应用控制特征库条目。
- 接口选择策略与质量标准：选择Best Quality和延迟，选用SD-WAN规则接口成员中延迟最低的接口，如果成员接口的延迟差小于10%（默认值），则使用接口偏好中配置较前的接口。
- SLA衡量标准：选择上步创建的健康检查。
- 接口偏好：选择联通线路接口与电信线路接口，联通线路接口排序在前。



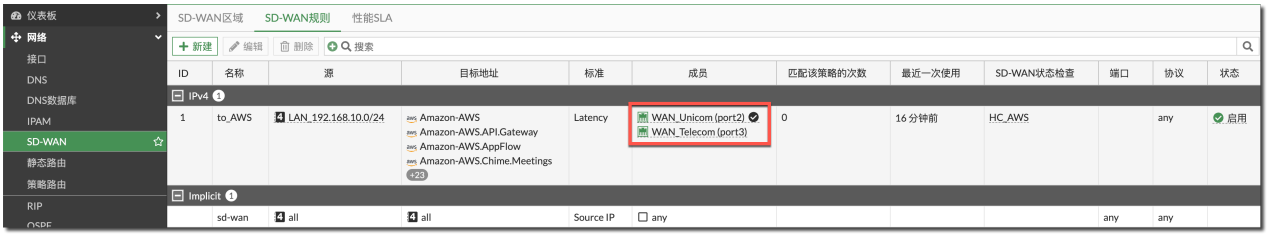
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config service
        edit 1
            set name "to_AWS"
            set mode priority
            set src "LAN_192.168.10.0/24"
            set internet-service enable
            set internet-service-name "Amazon-AWS" "Amazon-AWS.API.Gateway" "Amazon-AWS.AppFlow" "Amazon-AWS.Chime.Meetings" "Amazon-AWS.Chime.Voice.Connector" "Amazon-AWS.Cloud9" "Amazon-AWS.CloudFront" "Amazon-AWS.CodeBuild" "Amazon-AWS.Connect" "Amazon-AWS.DynamoDB" "Amazon-AWS.EBS" "Amazon-AWS.EC2" "Amazon-AWS.Global.Accelerator" "Amazon-AWS.GovCloud.US" "Amazon-AWS.Kinesis.Video.Streams" "Amazon-AWS.Route53" "Amazon-AWS.S3" "Amazon-AWS.WorkSpaces.Gateway"
            set internet-service-app-ctrl 27210 37172 36740 10000051 35944 47432 47433 10000199 51269
            set health-check "HC_AWS"
            set priority-members 1 2
        next
    end
end
```

4. 查看上步创建的SD-WAN规则目前的选路状态，由于联通线路（port2）的延迟较低，电信线路（port3）的延迟较高，访问AWS的业务优先选择联通线路（port2）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
FortiGate # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10),
heath-check(HC_AWS)
  Members(2):
    1: Seq_num(1 port2), alive, latency: 3.135, selected    //联通线路优先
    2: Seq_num(2 port3), alive, latency: 53.637, selected   //电信线路其次
  Internet Service(27): Amazon-AWS(393320,0,0,0,0) Amazon-AWS.API.Gateway(393478,0,0,0,0) Amazon-
AWS.AppFlow(393484,0,0,0,0) Amazon-AWS.Chime.Meetings(393483,0,0,0,0) Amazon-
AWS.Chime.Voice.Connector(393479,0,0,0,0) Amazon-AWS.Cloud9(393471,0,0,0,0) Amazon-AWS.CloudFront(393481,0,0,0,0)
Amazon-AWS.CodeBuild(393482,0,0,0,0) Amazon-AWS.Connect(393480,0,0,0,0) Amazon-AWS.DynamoDB(393472,0,0,0,0)
Amazon-AWS.EBS(393470,0,0,0,0) Amazon-AWS.EC2(393477,0,0,0,0) Amazon-AWS.Global.Accelerator(393476,0,0,0,0)
Amazon-AWS.GovCloud.US(393452,0,0,0,0) Amazon-AWS.Kinesis.Video.Streams(393475,0,0,0,0) Amazon-
AWS.Route53(393473,0,0,0,0) Amazon-AWS.S3(393474,0,0,0,0) Amazon-AWS.WorkSpaces.Gateway(393403,0,0,0,0)
Amazon.AWS(4294836343,0,0,0,0 27210) Amazon.AWS.Console(4294836344,0,0,0,0 37172)
Amazon.AWS_EC2(4294836345,0,0,0,0 36740) Amazon.AWS_IoT(4294838823,0,0,0,0 10000051)
Amazon.AWS_S3(4294836346,0,0,0,0 35944) Amazon.AWS_S3.Download(4294838824,0,0,0,0 47432)
Amazon.AWS_S3.Upload(4294838825,0,0,0,0 47433) Amazon.AWS_Smart.Plug(4294838826,0,0,0,0 10000199)
Amazon.AWS_Workspaces.Health.Status(4294838827,0,0,0,0 51269)
  Src address(1):
        192.168.10.0-192.168.10.255
```

5. 查看SD-WAN规则对应的策略路由状态，出接口优先选择延迟较低的联通线路（port2）。

```bash

FortiGate # diagnose firewall proute list
list route policy info(vf=root):

id=2132869121(0x7f210001) vwl_service=1(to_AWS) vwl_mbr_seq=1 2 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(2) oif=4(port2) oif=5(port3)     //选择延迟较低
的联通线路
source(1): 192.168.10.0-192.168.10.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(27): Amazon-AWS(393320,0,0,0,0) Amazon-AWS.API.Gateway(393478,0,0,0,0) Amazon-
AWS.AppFlow(393484,0,0,0,0) Amazon-AWS.Chime.Meetings(393483,0,0,0,0) Amazon-
AWS.Chime.Voice.Connector(393479,0,0,0,0) Amazon-AWS.Cloud9(393471,0,0,0,0) Amazon-AWS.CloudFront(393481,0,0,0,0)
Amazon-AWS.CodeBuild(393482,0,0,0,0) Amazon-AWS.Connect(393480,0,0,0,0) Amazon-AWS.DynamoDB(393472,0,0,0,0)
Amazon-AWS.EBS(393470,0,0,0,0) Amazon-AWS.EC2(393477,0,0,0,0) Amazon-AWS.Global.Accelerator(393476,0,0,0,0)
Amazon-AWS.GovCloud.US(393452,0,0,0,0) Amazon-AWS.Kinesis.Video.Streams(393475,0,0,0,0) Amazon-
AWS.Route53(393473,0,0,0,0) Amazon-AWS.S3(393474,0,0,0,0) Amazon-AWS.WorkSpaces.Gateway(393403,0,0,0,0)
Amazon.AWS(4294836343,0,0,0,0, 27210) Amazon.AWS.Console(4294836344,0,0,0,0, 37172)
Amazon.AWS_EC2(4294836345,0,0,0,0, 36740) Amazon.AWS_IoT(4294838823,0,0,0,0, 10000051)
Amazon.AWS_S3(4294836346,0,0,0,0, 35944) Amazon.AWS_S3.Download(4294838824,0,0,0,0, 47432)
Amazon.AWS_S3.Upload(4294838825,0,0,0,0, 47433) Amazon.AWS_Smart.Plug(4294838826,0,0,0,0, 10000199)
Amazon.AWS_Workspaces.Health.Status(4294838827,0,0,0,0, 51269)
hit_count=0 last_used=2023-12-15 15:59:10
```

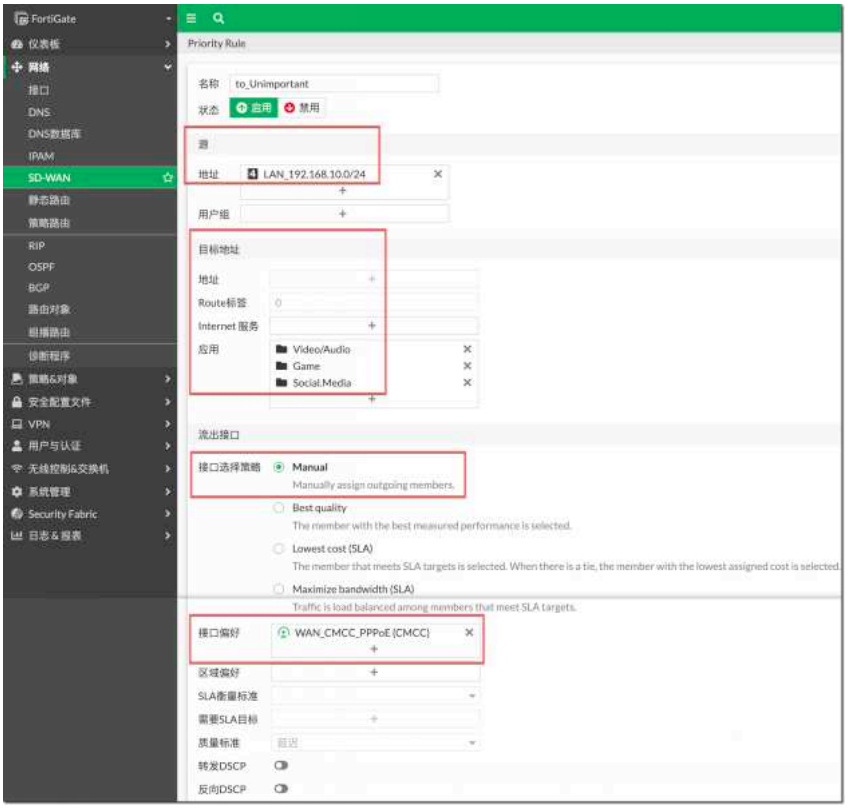
需求举例2

其他不重要的业务从移动线路（PPPoE）接口转发。

1. 新建SD-WAN规则2：

- 源地址选择内网网段；目标地址使用应用分类，选择视频/语音、游戏、社交媒体等对于客户不重要的业务应用分类（SD-WAN规则中的目标地址可以选择应用分类在7.2.0开始支持，之前的版本只支持选择具体的应用特征条目）。
- 接口选择策略：选择Manual模式。
- 接口偏好：选用SD-WAN规则接口成员中的移动PPPoE线路。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config service
        edit 2
            set name "to_Unimportant"
            set src "LAN_192.168.10.0/24"
            set internet-service enable
            set internet-service-app-ctrl-category 5 8 23
            set priority-members 3
        next
    end
end
```

2. 查看此SD-WAN规则状态。

```bash
FortiGate # diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(1):
    1: Seq_num(3 CMCC), alive, selected
  Internet Service(3): Video/Audio(0,5,0,0,0) Game(0,8,0,0,0) Social.Media(0,23,0,0,0)
  Src address(1):
        192.168.10.0-192.168.10.255
```

需求举例3

其他类型的流量从电信线路（port3）或移动线路（PPPoE）中延迟较低的线路转发。

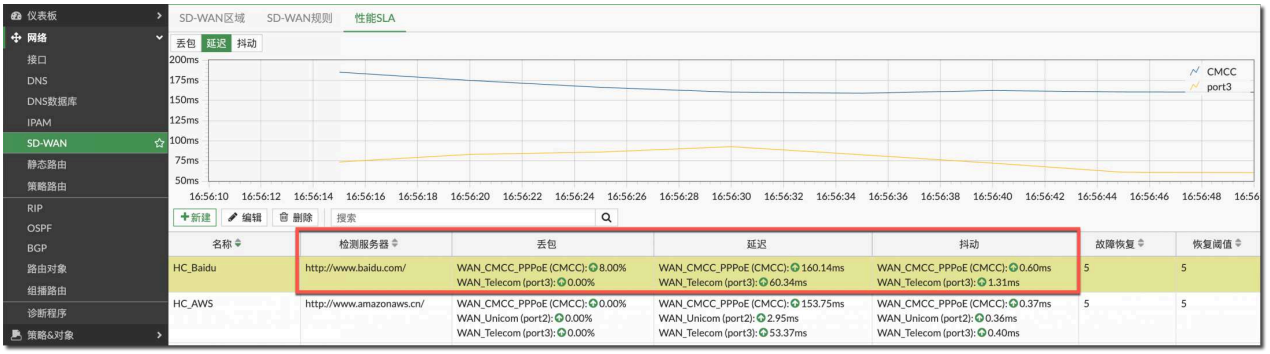
1. 新建SD-WAN健康检查，协议为HTTP，检查目标为网站www.baidu.com ↗ ，参与接口选择电信线路（port3）和移动线路（PPPoE）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system sdwan
    config health-check
        edit "HC_Baidu"
            set server "www.baidu.com"
            set protocol http
            set members 3 2
        next
    end
end
```

2. 创建完成后，可以看到电信线路（port3）比移动线路（PPPoE）的延迟要低（超过了10%的阈值）。

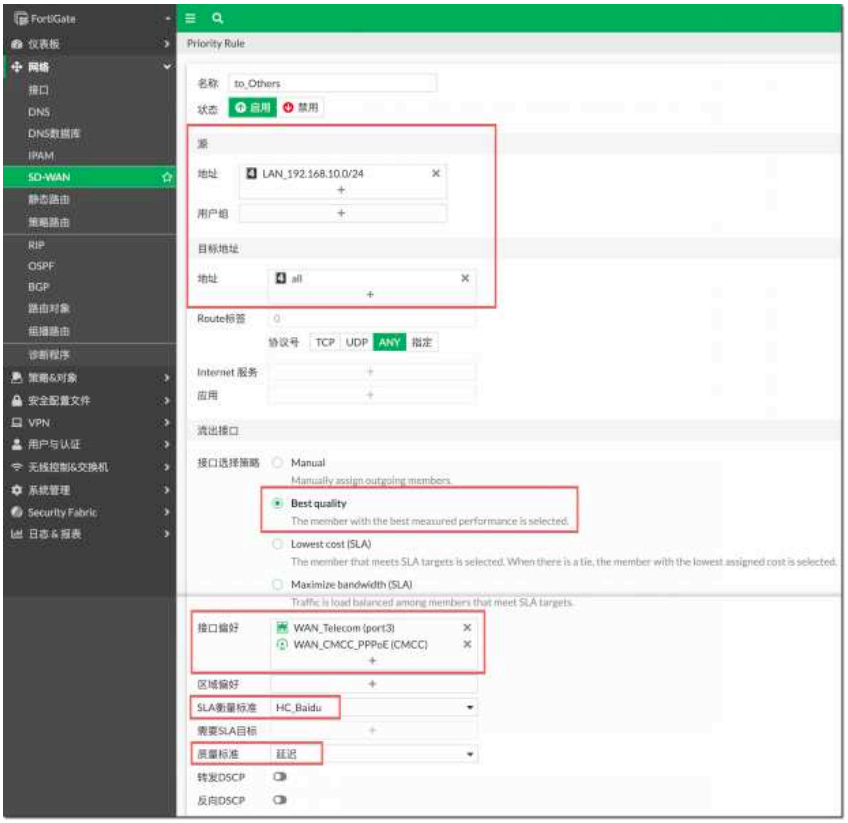



```bash
FortiGate # diagnose sys sdwan health-check status HC_Baidu
Health Check(HC_Baidu):
Seq(3 CMCC): state(alive), packet-loss(1.000%) latency(165.551), jitter(1.748), mos(4.267), bandwidth-
up(65534991), bandwidth-dw(65534974), bandwidth-bi(131069965) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(64.622), jitter(1.523), mos(4.369), bandwidth-
up(65534989), bandwidth-dw(65534969), bandwidth-bi(131069958) sla_map=0x0
```

3. 新建SD-WAN规则3：

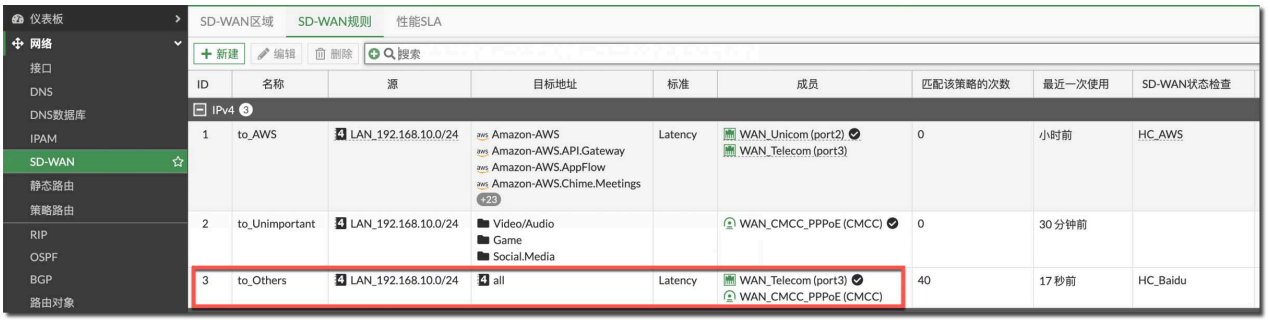
- 源地址选择内网网段；目标地址选择all。
- 接口选择策略和质量标准：选择Best Quality和延迟，选用SD-WAN规则接口成员中延迟最低的接口，如果成员接口的延迟差小于10%（默认值），则使用接口偏好中配置较前的接口。
- SLA衡量标准：选择上步创建的健康检查。
- 接口偏好：选择电信线路接口（port3）与移动线路接口（PPPoE），电信线路接口（port3）排序在前。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config service
        edit 3
            set name "to_Others"
            set mode priority
            set dst "all"
            set src "LAN_192.168.10.0/24"
            set health-check "HC_Baidu"
            set priority-members 2 3
        next
    end
end
```

4. 查看上步创建的SD-WAN规则目前的选路状态，由于电信线路（port2）的延迟较低，移动线路（PPPoE）的延迟较高，访问其他的业务优先选择电信线路（port3）。



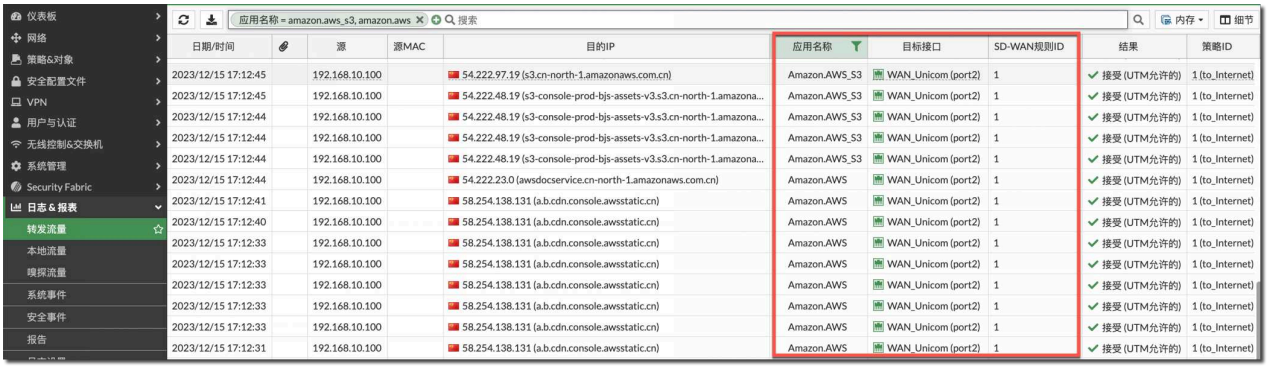

```bash
FortiGate # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10),
heath-check(HC_Baidu)
  Members(2):
    1: Seq_num(2 port3), alive, latency: 66.413, selected    //优先选择电信线路
    2: Seq_num(3 CMCC), alive, latency: 167.769, selected
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Src address(1):
      192.168.10.0-192.168.10.255

Dst address(1):
      0.0.0.0-255.255.255.255
```

结果验证

1. 使用内网PC客户端访问AWS业务，在转发流量日志中查看相关流量，可以看到出接口从联通线路（port2）转发。



2. 查看SD-WAN规则学习应用控制特征的列表。

```bash
FortiGate # diagnose sys sdwan internet-service-app-ctrl-list

Amazon.AWS(27210 4294836343): 54.222.23.0 6 443 Fri Dec 15 17:12:37 2023
Amazon.AWS(27210 4294836343): 58.254.138.131 6 443 Fri Dec 15 17:12:28 2023
Amazon.AWS_S3(35944 4294836346): 52.82.189.181 6 443 Fri Dec 15 17:14:35 2023
Amazon.AWS_S3(35944 4294836346): 54.222.48.19 6 443 Fri Dec 15 17:12:33 2023
Amazon.AWS_S3(35944 4294836346): 54.222.52.141 6 443 Fri Dec 15 17:10:13 2023
Amazon.AWS_S3(35944 4294836346): 54.222.97.19 6 443 Fri Dec 15 17:11:45 2023

通过如下命令可以清除此列表：
diagnose sys sdwan internet-service-app-ctrl-flush
```

重要

关于SD-WAN调用应用特征，需要以下学习过程：

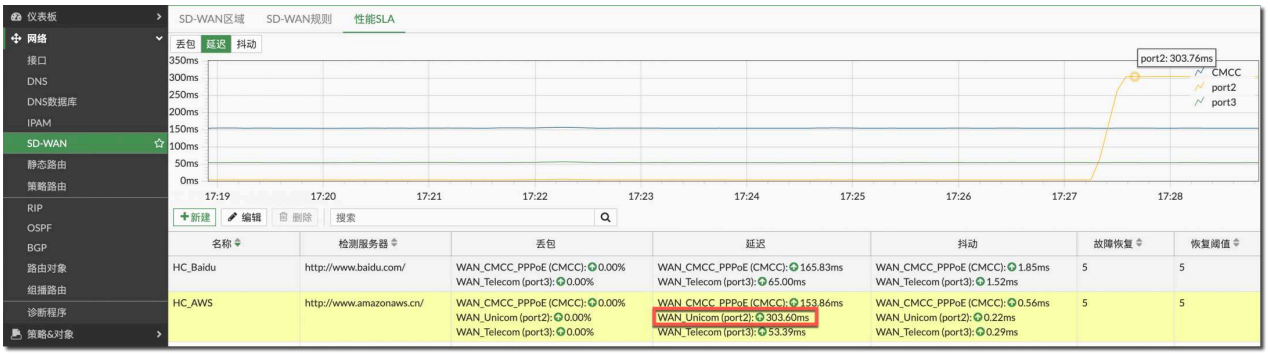
第1步：应用特征是需要先通过内网用户使用AWS，然后FortiGate进行应用识别的，因此策略里面一定要开启APP Control才可以。

第2步：识别之后将会学习到相应的应用特征的IP地址，然后形成一个动态的应用程序IP地址数据库（如上所示），最终才会将这个学习到的IP数据库加入到SD-WAN规则（策略路由）里面。

因此这需要有一个学习的过程，因此在没有成功学习之前，AWS的流量会走到其他线路上去（匹配SD-WAN规则3），这并非问题，而是SD-WAN调用应用的工作逻辑就是这样，学习完毕之后，新发起的AWS流量才会匹配到SD-WAN规则1。

如果直接匹配上了ISDB条目，则会直接匹配SD-WAN规则，不会有以上需要学习的过程。

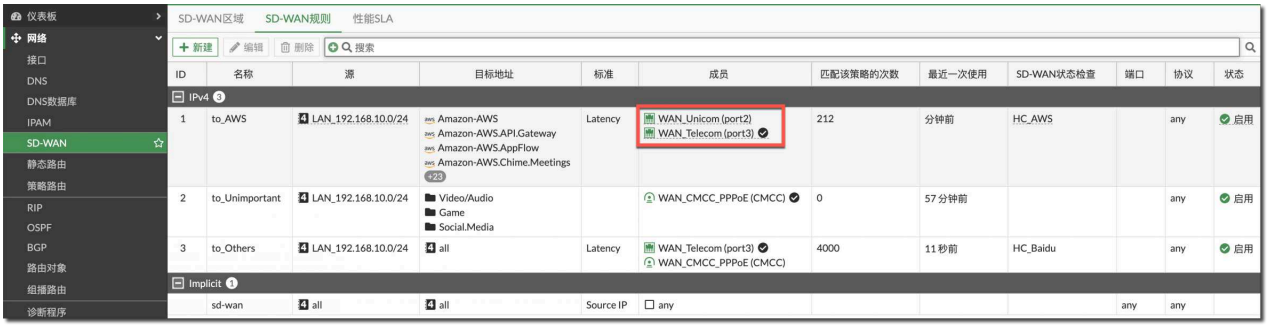
3. 模拟联通线路（port2）到AWS的延迟增加到300ms。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

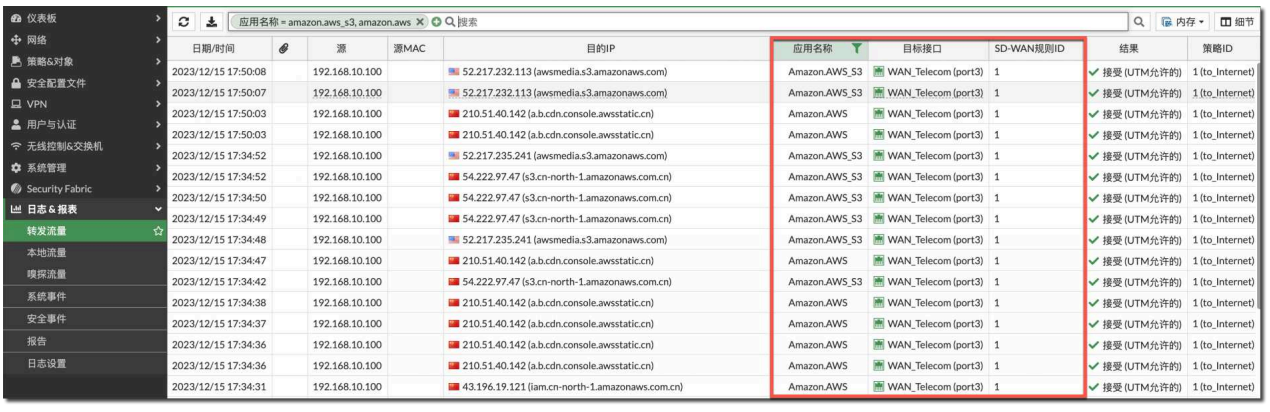
```bash
FortiGate # diagnose sys sdwan health-check status HC_AWS
Health Check(HC_AWS):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(303.826), jitter(0.410), mos(3.767), bandwidth-up(65534995), bandwidth-dw(65534993), bandwidth-bi(131069988) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(53.633), jitter(0.326), mos(4.376), bandwidth-up(65534991), bandwidth-dw(65534973), bandwidth-bi(131069964) sla_map=0x0
Seq(3 CMCC): state(alive), packet-loss(0.000%) latency(153.905), jitter(0.378), mos(4.307), bandwidth-up(65534992), bandwidth-dw(65534975), bandwidth-bi(131069967) sla_map=0x0
```

4. 查看SD-WAN规则1的选路优先选择电信线路（port3）去往AWS业务。



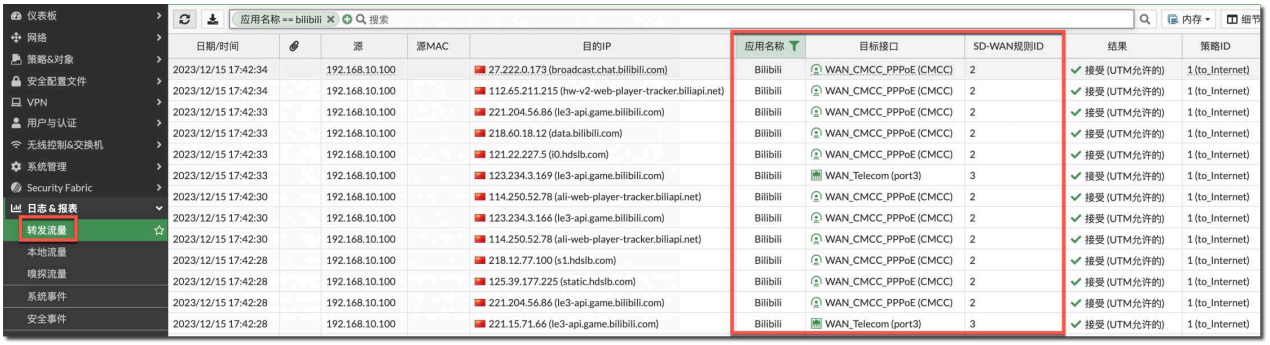

```bash
FortiGate # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10), heath-check(HC_AWS)
  Members(2):
    1: Seq_num(2 port3), alive, latency: 53.560, selected
    //优先选择延迟较低的电信线路//
    2: Seq_num(1 port2), alive, latency: 304.084, selected
  Internet Service(27): Amazon-AWS(393320,0,0,0,0) Amazon-AWS.API.Gateway(393478,0,0,0,0) Amazon-AWS.AppFlow(393484,0,0,0,0) Amazon-AWS.Chime.Meetings(393483,0,0,0,0) Amazon-AWS.Chime.Voice.Connector(393479,0,0,0,0) Amazon-AWS.Cloud9(393471,0,0,0,0) Amazon-AWS.CloudFront(393481,0,0,0,0)
Amazon-AWS.CodeBuild(393482,0,0,0,0) Amazon-AWS.Connect(393480,0,0,0,0) Amazon-AWS.DynamoDB(393472,0,0,0,0)
Amazon-AWS.EBS(393470,0,0,0,0) Amazon-AWS.EC2(393477,0,0,0,0) Amazon-AWS.Global.Accelerator(393476,0,0,0,0)
Amazon-AWS.GovCloud.US(393452,0,0,0,0) Amazon-AWS.Kinesis.Video.Streams(393475,0,0,0,0) Amazon-AWS.Route53(393473,0,0,0,0) Amazon-AWS.S3(393474,0,0,0,0) Amazon-AWS.WorkSpaces.Gateway(393403,0,0,0,0)
Amazon.AWS(4294836343,0,0,0,0 27210) Amazon.AWS.Console(4294836344,0,0,0,0 37172)
Amazon.AWS_EC2(4294836345,0,0,0,0 36740) Amazon.AWS_IoT(4294838823,0,0,0,0 10000051)
Amazon.AWS_S3(4294836346,0,0,0,0 35944) Amazon.AWS_S3.Download(4294838824,0,0,0,0 47432)
Amazon.AWS_S3.Upload(4294838825,0,0,0,0 47433) Amazon.AWS_Smart.Plug(4294838826,0,0,0,0 10000199)
Amazon.AWS_Workspaces.Health.Status(4294838827,0,0,0,0 51269)
  Src address(1):
        192.168.10.0-192.168.10.255
```

5. 再次使用内网PC客户端访问AWS业务，在转发流量日志中查看相关流量，可以看到出接口从电信线路（port3）转发。



6. 使用内网PC客户端访问视频网站业务，在转发流量日志中查看相关流量，可以看到出接口从移动线路（PPPoE）转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 查看SD-WAN规则学习应用控制特征分类的列表（注意和规则1是不一样的命令，这里看的是应用分类，而不是应用）。

```bash
FortiGate # diagnose sys sdwan internet-service-app-ctrl-category-list

Bilibili(53243 4294839067): 27.222.0.173 6 7826 Fri Dec 15 17:41:47 2023
Bilibili(53243 4294839067): 112.65.211.215 6 443 Fri Dec 15 17:41:48 2023
Bilibili(53243 4294839067): 112.83.140.17 6 443 Fri Dec 15 17:39:16 2023
Bilibili(53243 4294839067): 114.250.52.78 6 443 Fri Dec 15 17:41:48 2023
Bilibili(53243 4294839067): 116.130.196.134 6 443 Fri Dec 15 17:41:43 2023
Bilibili(53243 4294839067): 121.22.227.2 6 443 Fri Dec 15 17:39:14 2023
Bilibili(53243 4294839067): 121.22.227.5 6 443 Fri Dec 15 17:41:47 2023
Bilibili(53243 4294839067): 123.234.3.166 6 443 Fri Dec 15 17:41:43 2023
Bilibili(53243 4294839067): 123.234.3.169 6 443 Fri Dec 15 17:42:28 2023
Bilibili(53243 4294839067): 125.39.177.219 6 443 Fri Dec 15 17:39:13 2023
......

通过如下命令可以清除此列表：
diagnose sys sdwan internet-service-app-ctrl-flush
```

重要

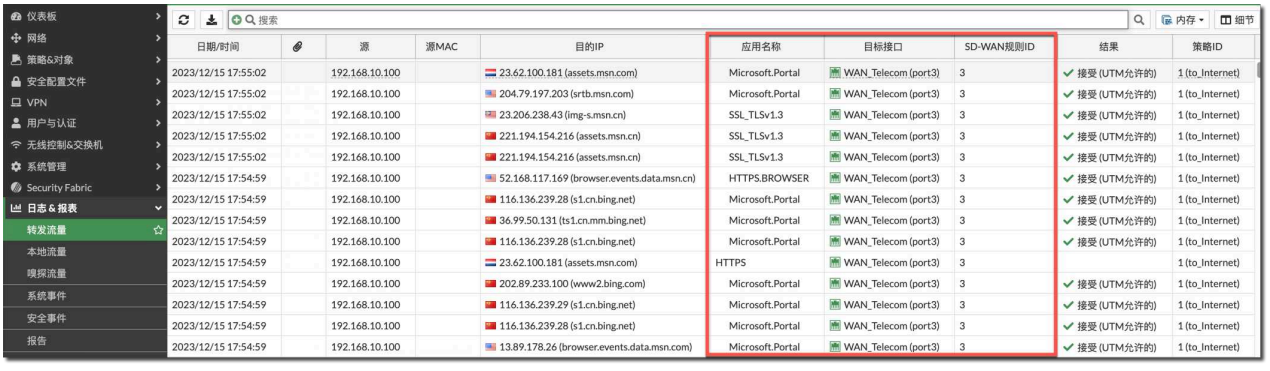
关于SD-WAN调用应用特征，大致需要满足以下要求：

第1步：应用特征是需要内网用户先访问视频网站，然后FortiGate进行应用识别的，因此策略里面一定要开启APP Control才可以。

第2步：识别之后将会学习到相应的应用特征的IP地址，然后形成一个动态的应用程序IP地址数据库（如上所示），最终才会将这个学习到的IP数据库加入到SD-WAN规则（策略路由）里面。

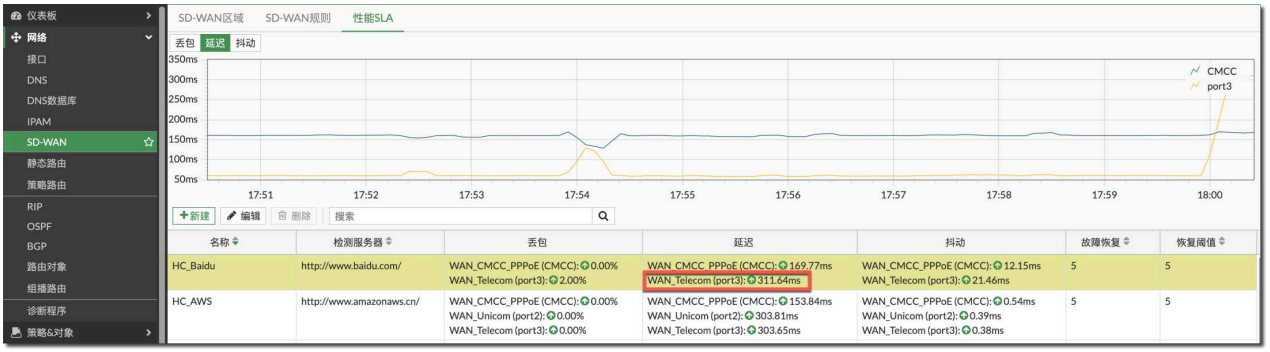
因此这需要有一个学习的过程，因此在没有成功学习之前，AWS的流量会走到其他线路上去（匹配SD-WAN规则3），这并非问题，而是SD-WAN调用应用的工作逻辑就是这样，学习完毕之后，新发起的AWS流量才会匹配到SD-WAN规则2。

8. 使用内网PC客户端访问其他业务网站，如搜索引擎，在转发流量日志中查看相关流量，可以看到出接口从电信线路（port3）转发。



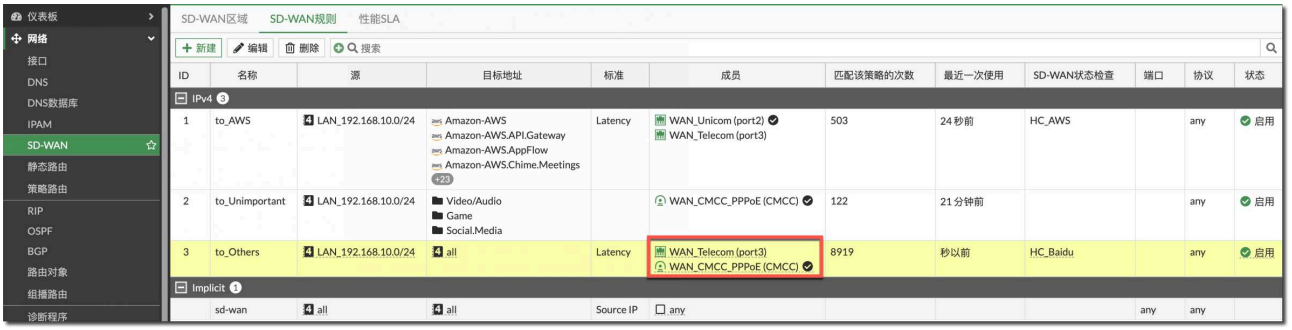
9. 模拟电信线路（port3）到Baidu的延迟增加到300ms。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



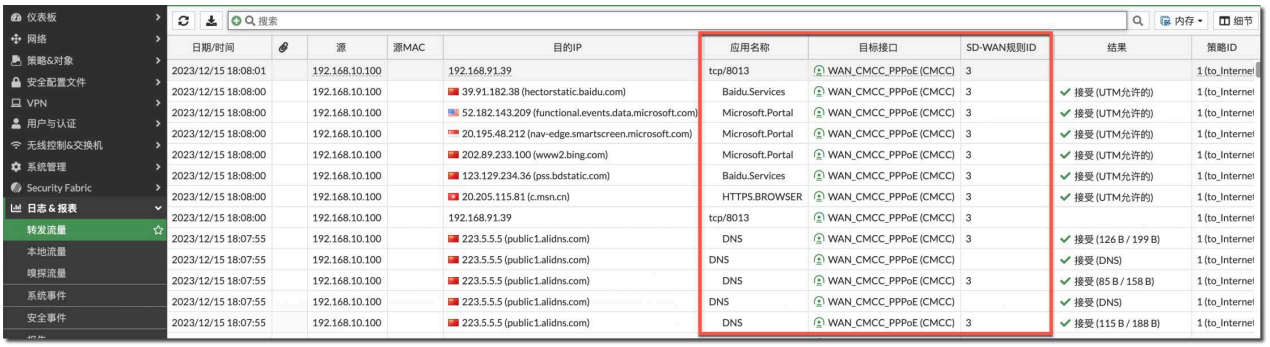

```bash
FortiGate # diagnose sys sdwan health-check status HC_Baidu
Health Check(HC_Baidu):
Seq(3 CMCC): state(alive), packet-loss(0.000%) latency(165.041), jitter(0.734), mos(4.274), bandwidth-up(65534990), bandwidth-dw(65534969), bandwidth-bi(131069959) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(2.000%) latency(304.182), jitter(21.180), mos(3.573), bandwidth-up(65534991), bandwidth-dw(65534973), bandwidth-bi(131069964) sla_map=0x0
```

.0. 查看SD-WAN规则3的选路优先选择移动线路（PPPoE）去往其他业务。




```bash
FortiGate # diagnose sys sdwan service 3

Service(3): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10), heath-check(HC_Baidu)
  Members(2):
    1: Seq_num(3 CMCC), alive, latency: 160.563, selected
    //优先从移动线路转发//
    2: Seq_num(2 port3), alive, latency: 310.831, selected
  Src address(1):
        192.168.10.0-192.168.10.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

.1. 使用内网PC客户端访问其他业务网站，在转发流量日志中查看相关流量，可以看到出接口从移动线路（PPPoE）转发。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

1. 如果需要学习将到的应用数据库立马完全生效，旧的会话是会保持原有出口的，想要这些旧的会话立即生效需要清除旧的会话和路由缓存信息，而新建的会话则不需要此操作，具体命令如下。

```bash
diagnose sys session filter src 192.168.10.100
diagnose sys session clear    //清除测试机器的会话，让其重新匹配新的SD-WAN规则（有skype的IP数据库更新）
```

2. 在SNAT环境的默认配置下，当SD-WAN选路出现变化后，已有的会话不会立即切换到新链路上，只有线路切换后新创建的会话会建立在新的线路上，如果想在SD-WAN线路切换后让已有会话立刻失效，需要使用如下命令（可能会增加CPU消耗，谨慎开启）。

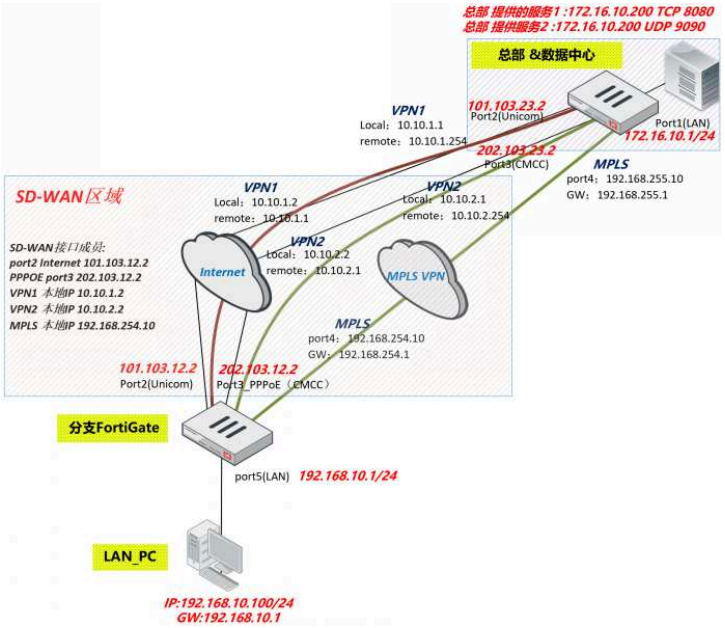
> **重要**
>
> 默认配置下的SNAT场景，即使转发流量的SD-WAN成员的健康检查变为dead，只要该线路仍然存在路由（可能关闭了`update-static-route`），已有的旧会话仍然不会切换到其他线路。

```bash
config system global
    set snat-route-change enable    //默认为disable//
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

互联网出口和VPN混合场景

网络拓扑与需求



1. Internet访问：
   - 分支FortiGate通过2个运营商（联通port2、移动PPPoE）接入Internet，其中联通为固定IP，移动线路为PPPoE线路。联通和移动线路借用出接口IP作为SNAT的源地址访问Internet。
   - 总部FortiGate通过2个运营商（联通port2、移动port3，均为固定IP）接入Internet。
2. 分支FortiGate与总部FortiGate间的流量：
   - 通过MPLS专线互联（port4）。
   - 通过两条Internet线路上的IPSec隧道互联（作为MPLS专线的备份链路）。
3. 分支FortiGate配置SD-WAN，划分2个SD-WAN区域：
   - 一个区域用于访问Internet，成员为联通port2、移动PPPoE接口。
   - 另一个区域用于分支FortiGate与总部FortiGate间的流量，成员为两条Internet线路上的IPSec接口和MPLS专线接口port4。
4. 分支FortiGate的流量控制：
   - 访问Internet的流量优先从联通线路（port2）转发，联通线路的质量不符合标准时，通过移动线路（PPPoE）转发。
   - 访问总部FortiGate内网的流量优先通过MPLS线路（port4）转发，MPLS线路质量不佳或中断时，优先通过联通线路上的IPSec隧道转发，其次通过移动线路上的IPSec隧道转发。
5. 部署SD-WAN通常在一个全新的设备进行配置，如果需要加入SD-WAN区域的接口已经被其他配置（如防火墙策略）引用，是无法直接加入SD-WAN区域的。要加入SD-WAN区域，又不想删除关联的配置，请参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域 ↗章节。

配置步骤

基础配置

Spoke

配置分支FortiGate 2条运营商线路的IP、PPPoE用户（PPPoE请通过CLI配置，参考部署前注意事项→PPPoE接口配置 ↗章节）、MPLS线路IP与内网口IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
PPPoE接口配置:
config system pppoe-interface
    edit "WAN_CMCC_PPPoE"
        set device "port3"
        set username "user1"
        set password xxxxxx
    next
end

固定IP接口配置:
config system interface
    edit "port2"
        set vdom "root"
        set ip 101.103.12.2 255.255.255.0
        set allowaccess ssh
        set alias "WAN_Unicom"
    next
    edit "port4"
        set vdom "root"
        set ip 192.168.254.10 255.255.255.0
        set allowaccess ssh
        set alias "MPLS"
    next
    edit "port5"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh http
        set alias "LAN"
    next
end
```

Hub

配置总部FortiGate 2条运营商线路的IP、MPLS线路IP与内网口IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system interface
    edit "port2"
        set vdom "root"
        set ip 101.103.23.2 255.255.255.0
        set allowaccess ssh
        set alias "WAN_Unicom"
    next
    edit "port3"
        set vdom "root"
        set ip 202.103.23.2 255.255.255.0
        set allowaccess ssh
        set alias "WAN_CMCC"
    next
    edit "port4"
        set vdom "root"
        set ip 192.168.255.10 255.255.255.0
        set allowaccess ssh
        set alias "MPLS"
    next
    edit "port5"
        set vdom "root"
        set ip 172.16.10.1 255.255.255.0
        set allowaccess ping https ssh http
        set alias "LAN"
    next
end
```

IPSec配置

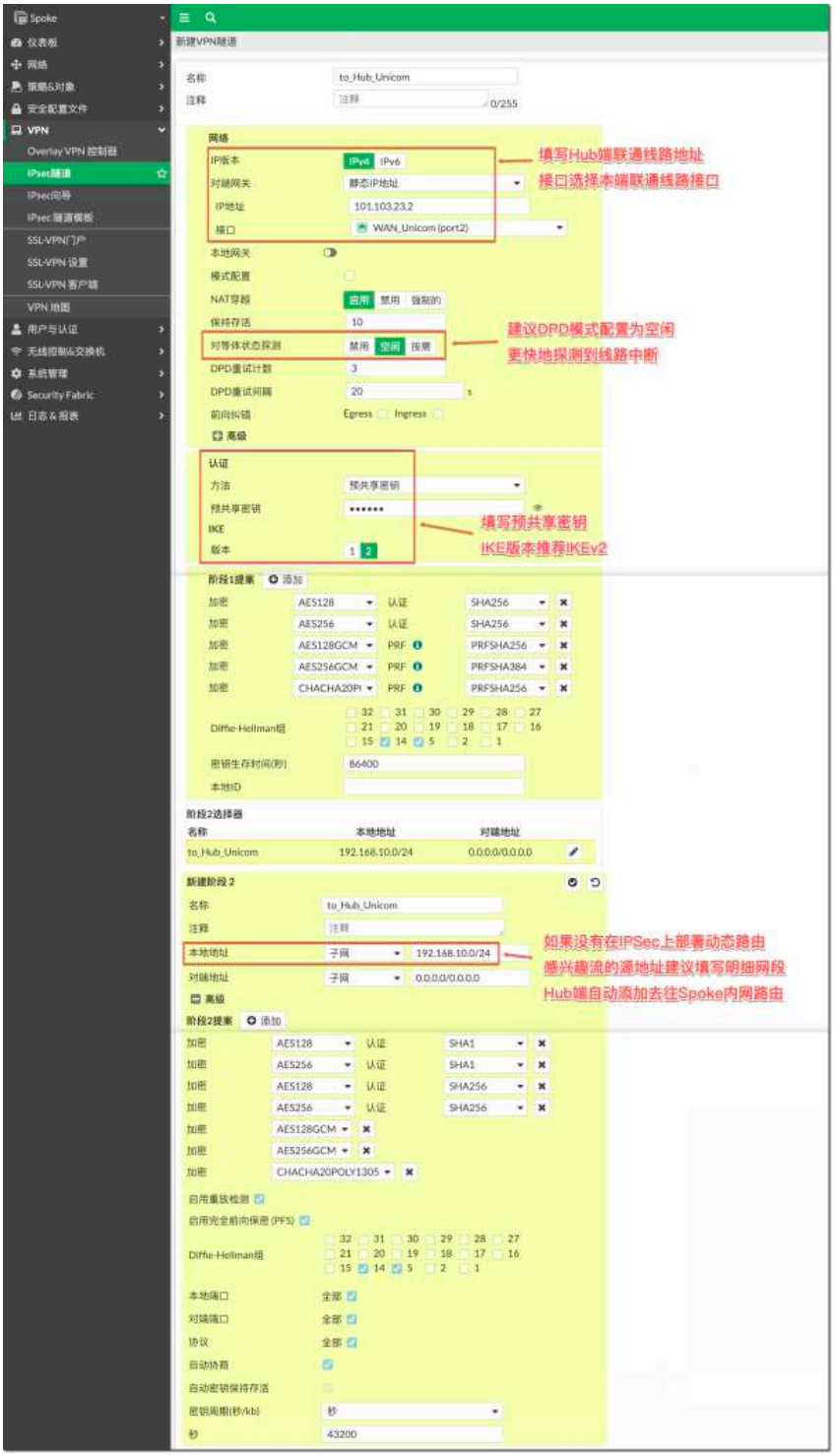
Spoke

1. 在分支（Spoke）FortiGate上进入VPN→IPSec隧道页面，新建联通线路（port2）上的IPSec隧道，选择自定义模式，按照下图所示配置，算法默认即可。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config vpn ipsec phase1-interface
    edit "to_Hub_Unicom"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set dpd on-idle
        set remote-gw 101.103.23.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_Hub_Unicom"
        set phase1name "to_Hub_Unicom"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 192.168.10.0 255.255.255.0
    next
end
```

2. 新建联通线路（port2）上的IPSec隧道，选择自定义模式，按照下图所示配置，算法默认即可。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config vpn ipsec phase1-interface
    edit "to_Hub_CMCC"
        set interface "WAN_CMCC_PPPoE"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set dpd on-idle
        set remote-gw 202.103.23.2
        set psksecret xxxxxx
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase2-interface
    edit "to_Hub_CMCC"
        set phase1name "to_Hub_CMCC"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 192.168.10.0 255.255.255.0
    next
end
```

Hub

1. 在总部（Hub）FortiGate上进入VPN→IPSec隧道页面，新建联通线路（port2）上的IPSec隧道（拨号模式），选择自定义模式，按照下图所示配置，算法默认即可。确保add-route功能开启（默认开启）。

> **重要**
>
> 如果Hub端不使用SD-WAN功能，请配置联通线路IPSec add-route添加路由的优先级为100。优先于移动线路IPSec的优先级200，当Hub端的MPLS专线中断时，优先使用联通线路主动访问Spoke。

> **重要**
>
> 由于Spoke两条线路的IPSec配置的源保护网段一致，Hub端的两个拨号连接在add-route时会产生冲突，导致Spoke两条线路的两条隧道发生震荡，所以在GUI配置下发完成后，需要编辑二阶段接口配置，添加“set route-overlap allow”配置，如下CLI所示。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config vpn ipsec phase1-interface
    edit "Hub_Unicom"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set add-route enable    //确认add-route为enable，如果是disable，手动enable它//
        set dpd on-idle
        set psksecret xxxxxx
        set priority 100    //如果Hub端不配置SD-WAN，配置此项赋值add-route添加路由的优先级//
        set dpd-retryinterval 60
    next
end

config vpn ipsec phase2-interface
    edit "Hub_Unicom"
        set phase1name "Hub_Unicom"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set keepalive enable
        set route-overlap allow    //重要：注意在CLI下添加此配置//
    next
end
```

2. 在总部（Hub）FortiGate上新建移动线路（port3）上的IPSec隧道（拨号模式），选择自定义模式，按照下图所示配置，算法默认即可。确保add-route功能开启（默认开启）。

重要

如果Hub端不使用SD-WAN功能，请配置移动线路IPSec add-route添加路由的优先级为200。次于移动线路IPSec的优先级100，当Hub端的MPLS专线中断时，优先使用联通线路的IPSec主动访问Spoke内网，其次使用移动线路的IPSec主动访问Spoke内网。

重要

由于Spoke两条线路的IPSec配置的源保护网段一致，Hub端的两个拨号连接在add-route时会产生冲突，导致Spoke两条线路的两条隧道发生震荡，所以在GUI配置下发完成后，需要编辑二阶段接口配置，添加“set route-overlap allow”配置，如下CLI所示。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config vpn ipsec phase1-interface
    edit "Hub_CMCC"
        set type dynamic
        set interface "port3"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set add-route enable    //确认add-route为enable，如果是disable，手动enable它//
        set dpd on-idle
        set psksecret xxxxxx
        set priority 200    //如果Hub端不配置SD-WAN，配置此项赋值add-route添加路由的优先级//
        set dpd-retryinterval 60
    next
end

config vpn ipsec phase2-interface
    edit "Hub_CMCC"
        set phase1name "Hub_CMCC"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set keepalive enable
        set route-overlap allow    //重要：注意在CLI下添加此配置//
    next
end
```

SD-WAN基础配置

Spoke

1. 进入分支FortiGate的网络→SD-WAN→SD-WAN区域页面，新建用于访问Internet的区域“to_Internet”（也可以直接使用预置的SD-WAN区域）和用于访问总部FortiGate内网的区域“to_Hub”。







Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system sdwan
    set status enable
    config zone
        edit "to_Internet"
        next
        edit "to_Hub"
        next
    end
end
```

2. 在此页面新建用于访问Internet的SD-WAN成员（联通、移动线路2个接口）加入上步创建的SD-WAN区域"to_Internet"，注意PPPoE加入SD-WAN区域时不需要填写网关。

> **重要**
>
> 如果WAN接口存在相关配置引用的情况下，是无法直接加入到SD-WAN接口成员的，可参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域↗章节快速将接口加入SD-WAN区域，并自动修改关联配置（也可选择手动将WAN接口的相关配置删除引用，包括策略、Link-monitor、所属区域等）。

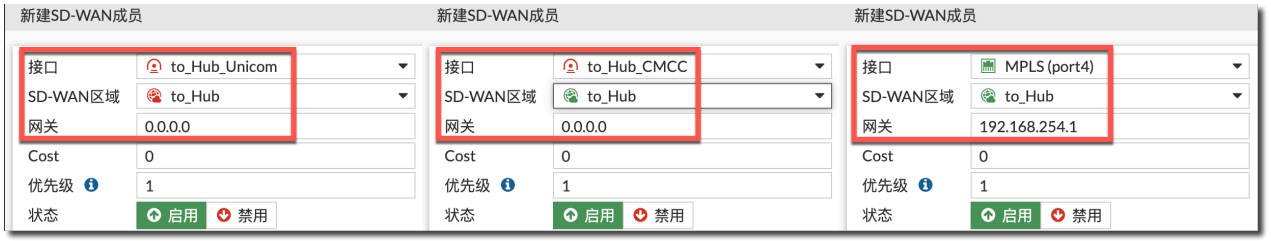




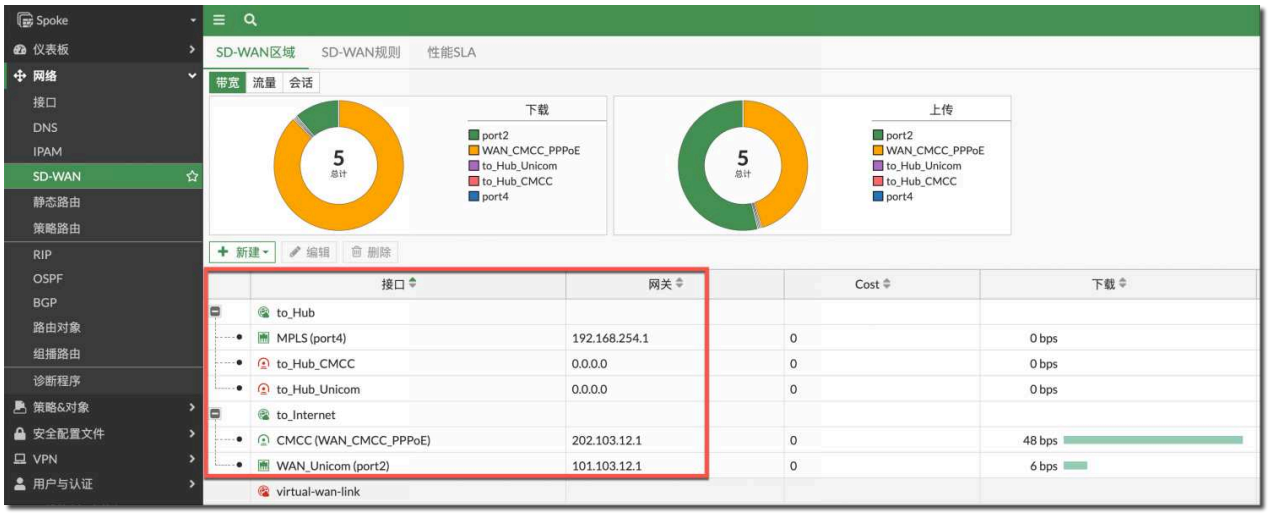

```bash
config system sdwan
    config members
        edit 1
            set interface "port2"
            set zone "to_Internet"
            set gateway 101.103.12.1
        next
        edit 2
            set interface "WAN_CMCC_PPPoE"
            set zone "to_Internet"
        next
    end
end
```

3. 新建用于访问Hub内网的SD-WAN成员（两个IPSec Tunnel接口和MPLS线路接口）加入步骤1创建的SD-WAN区域"to_Hub"。注意IPSec Tunnel接口加入SD-WAN区域时不需要填写网关。

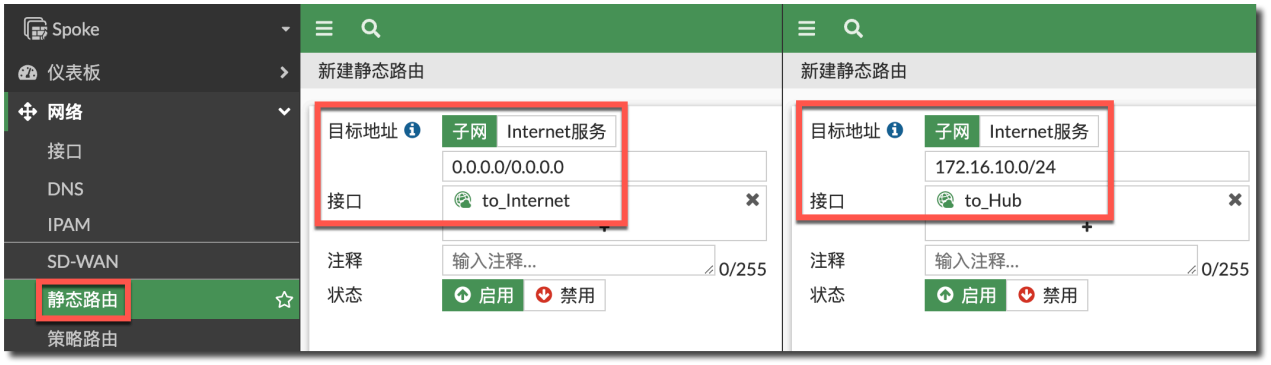
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config members
        edit 3
            set interface "to_Hub_Unicom"
            set zone "to_Hub"
        next
        edit 4
            set interface "to_Hub_CMCC"
            set zone "to_Hub"
        next
        edit 5
            set interface "port4"
            set zone "to_Hub"
            set gateway 192.168.254.1
        next
    end
end
```



4. 配置默认路由指向SD-WAN区域“to_Internet”，配置去往Hub端内网网段的路由指向SD-WAN区域“to_Hub”。

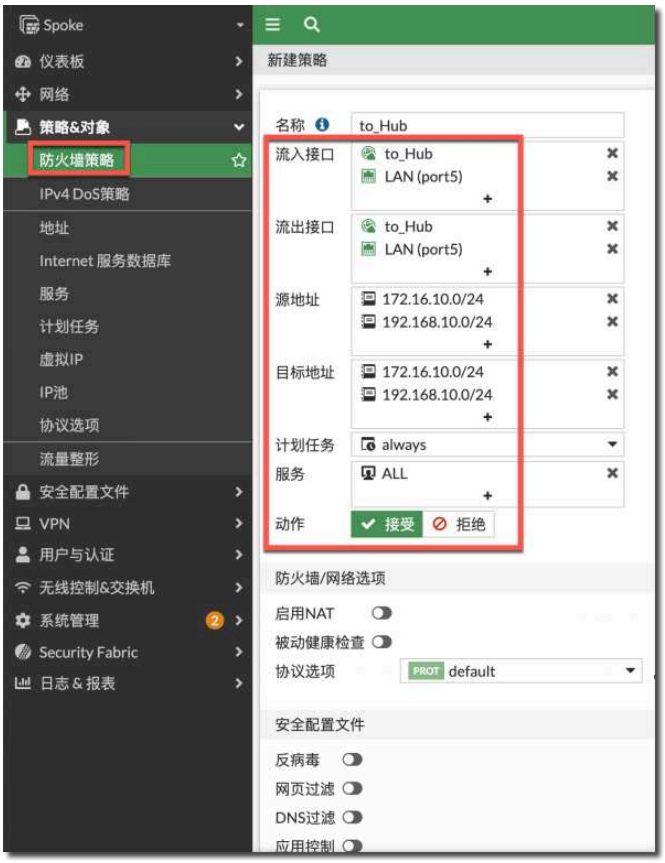



```bash
config router static
    edit 4
        set distance 1
        set sdwan-zone "to_Internet"
    next
    edit 5

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dst 172.16.10.0 255.255.255.0
        set distance 1
        set sdwan-zone "to_Hub"
    next
end
```

5. 配置防火墙策略1，放通内网port5（LAN）与Hub内网之间互相访问的流量（配置前在“系统管理→可见功能”中开启“多接口策略”），通常情况下内网之间的访问不需要开启SNAT。根据需求开启UTM功能。




```bash
config firewall policy
    edit
        set name "to_Hub"
        set srcintf "to_Hub" "port5"
        set dstintf "to_Hub" "port5"
        set action accept
        set srcaddr "172.16.10.0/24" "192.168.10.0/24"
        set dstaddr "172.16.10.0/24" "192.168.10.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置防火墙策略2，放通内网port5（LAN）到2个运营商线路（SD-WAN区域“to_Internet”）的Internet访问，并开启SNAT（借用出接口地址）。根据需求开启UTM功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 2
        set name "to_Internet"
        set srcintf "port5"
        set dstintf "to_Internet"
        set action accept
        set srcaddr "192.168.10.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
    next
end
```



Hub

1. Hub端如果需要配置SD-WAN，可以参考Spoke对应的配置。

2. Hub也可以不配置SD-WAN。如果不配置SD-WAN选路，可以通过静态路由不同的优先级进行选路。这里我们以Hub端不配置SD-WAN为例。

3. 配置路由：

   - 指向联通线路（port2，优先级为100）和移动线路（port3，优先级为200）。优先从联通线路访问Internet，联通线路DOWN时，从移动线路访问Internet。
   - 通过MPLS专线（port4）去往Spoke内网的路由，管理距离配置为15（由于IPSec add-route添加的路由distance默认为15，这里需要配置distance为15，与IPSec add-route添加的两条路由负载，否则无法进入路由表），优先级配置为默认的1（优先于IPSec add-route添加的两条路由）。

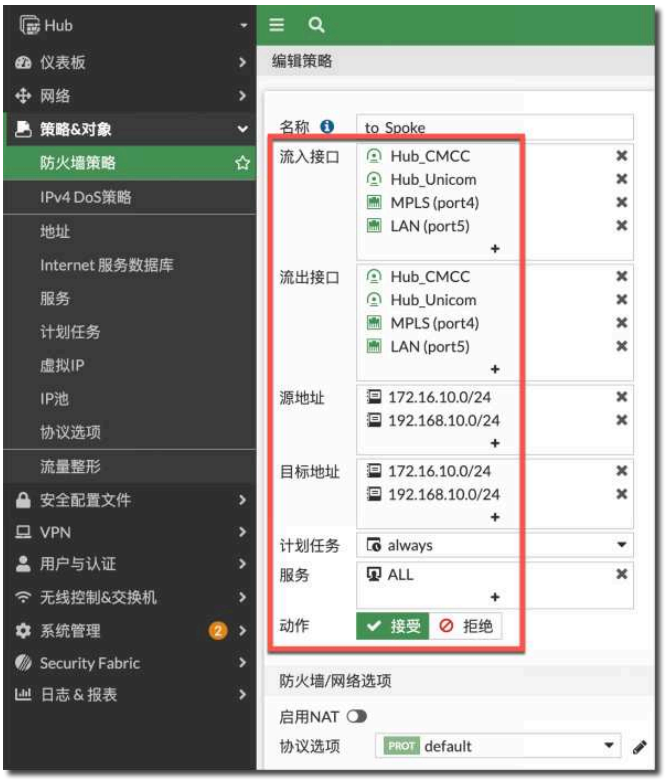
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 去往Spoke内网的路由通过IPSec一阶段配置中的add-route实现，联通线路IPSec自动添加的路由优先级为100，移动线路IPSec自动添加的路由优先级为200。

   - Hub内网主动访问Spoke内网的流量，优先从联通线路的IPSec访问Spoke内网，联通线路IPSec DOWN时，从移动线路的IPSec访问Spoke内网。
   - Spoke内网主动访问Hub内网的流量，在Hub的两条IPSec隧道中源进源出。

5. 配置防火墙策略1，放通内网port5（LAN）与Spoke内网之间互相访问的流量，通常情况下内网之间的访问不需要开启SNAT。根据需求开启UTM功能。




```bash
config firewall policy
    edit 1
        set name "to_Spoke"
        set srcintf "Hub_CMCC" "Hub_Unicom" "port5" "port4"
        set dstintf "Hub_CMCC" "Hub_Unicom" "port5" "port4"
        set action accept
        set srcaddr "172.16.10.0/24" "192.168.10.0/24"
        set dstaddr "172.16.10.0/24" "192.168.10.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置防火墙策略2，放通内网port5（LAN）到2个运营商线路的Internet访问（配置前在“系统管理→可见功能”中开启“多接口策略”），并开启SNAT（借用出接口地址）。根据需求开启UTM功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 2
        set name "to_Internet"
        set srcintf "port5"
        set dstintf "port2" "port3"
        set action accept
        set srcaddr "172.16.10.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

状态检查

1. 查看Hub端IPSec隧道的建立状态，两条线路上的IPSec均有一个拨号连接建立成功。




```bash
Hub # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
......
------------------------------------------------------
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
name=Hub_CMCC_0 ver=2 serial=4 202.103.23.2:0→202.103.12.2:0 tun_id=202.103.12.2 tun_id6=::10.0.0.1 dst_mtu=1500
dpd-link=on weight=1
bound_if=5 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accep0

parent=Hub_CMCC index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=6
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=Hub_CMCC proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:192.168.10.0-192.168.10.255:0
  SA:  ref=3 options=20683 type=00 soft=0 mtu=1438 expire=42881/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43191/43200
  dec: spi=f6555239 esp=aes key=16 9a00355173ec08c39a49eae81d06f85c
       ah=sha1 key=20 217275e45ec62629aee93a6e786f411e9b3469c9
  enc: spi=1b2b0940 esp=aes key=16 2b84a446403798f83ff9ccc559590fac
       ah=sha1 key=20 a811652f1656b85115327fe3504fbfa29566d587
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=202.103.12.2 npu_lgwy=202.103.23.2 npu_selid=0 dec_npuid=0 enc_npuid=0
--------------------------------------------------------

......
--------------------------------------------------------
name=Hub_Unicom_0 ver=2 serial=5 101.103.23.2:0→101.103.12.2:0 tun_id=101.103.12.2 tun_id6=::10.0.0.4
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74408 options[122a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accep0

parent=Hub_Unicom index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=6
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=Hub_Unicom proto=0 sa=1 ref=2 serial=4 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:192.168.10.0-192.168.10.255:0
  SA:  ref=3 options=20683 type=00 soft=0 mtu=1438 expire=42972/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43189/43200
  dec: spi=f655523d esp=aes key=16 2a81dd8faebba5ead18f799af04aebdf
       ah=sha1 key=20 2769c11ebb1bb5fd25f6cafcfa830b738001857a
  enc: spi=1b2b0944 esp=aes key=16 ee9877c4c329c9d95a194859439bcbbc
       ah=sha1 key=20 11338a4d28ff61cbc71052f326d2a3719c07f323
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=101.103.12.2 npu_lgwy=101.103.23.2 npu_selid=4 dec_npuid=0 enc_npuid=0
```

2. 查看分支（Spoke）FortiGate路由表，默认路由在2个运营商线路上负载，去往Hub端内网的路由在两条线路的IPSec和MPLS线路上负载。

```bash
Spoke # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 101.103.12.1, port2, [1/0]
                  [1/0] via 202.103.12.1, WAN_CMCC_PPPoE, [1/0]
C       101.103.12.0/24 is directly connected, port2
S       172.16.10.0/24 [1/0] via to_Hub_Unicom tunnel 101.103.23.2, [1/0]
                       [1/0] via 192.168.254.1, port4, [1/0]
                       [1/0] via to_Hub_CMCC tunnel 202.103.23.2, [1/0]
C       192.168.10.0/24 is directly connected, port5
C       192.168.254.0/24 is directly connected, port4
C       202.103.12.1/32 is directly connected, WAN_CMCC_PPPoE
C       202.103.12.2/32 is directly connected, WAN_CMCC_PPPoE
```

3. 查看总部（Hub）FortiGate路由表，默认路由在2个运营商线路上负载，联通线路的优先级为100，移动线路的优先级为200；去往Spoke端内网的路由在两条线路的IPSec和MPLS线路上负载，MPLS线路IPSec的优先级为1，联通线路IPSec的优先级为100，移动线路IPSec的优先级为200。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Hub # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.103.23.1, port2, [100/0]
                  [10/0] via 202.103.23.1, port3, [200/0]
C       101.103.23.0/24 is directly connected, port2
C       172.16.10.0/24 is directly connected, port5
S       192.168.10.0/24 [15/0] via 192.168.255.1, port4, [1/0]
                        [15/0] via Hub_Unicom tunnel 101.103.12.2, [100/0]
                        [15/0] via Hub_CMCC tunnel 202.103.12.2, [200/0]
C       192.168.255.0/24 is directly connected, port4
C       202.103.23.0/24 is directly connected, port3
```

bash

SD-WAN策略配置

需求举例1

Spoke去往Hub内网的流量优先从MPLS专线（port4）转发，MPLS专线中断或不满足SLA标准后，优先从联通线路的IPSec隧道转发，其次是移动线路的IPSec隧道。

1. 在Spoke的SD-WAN中配置探测Hub端内网服务器的健康检查：

- 成员选择MPLS专线接口（port4）、联通线路的IPSec接口和移动线路的IPSec接口。
- 探测模式为tcp-connect（TCP三次握手），探测端口为8080，指定探测的源IP为Spoke内网口IP（需要通过CLI配置）。
- 开启SLA目标：延迟<250ms/抖动<50ms/丢包率<5%。

```
config system sdwan
    config health-check
        edit "to_Hub"
            set server "172.16.10.200"
            set protocol tcp-connect    //探测模式为TCP三次握手//
            set port 8080    //探测端口为8080//
            set source 192.168.10.1    //指定源IP为Spoke内网口地址（在IPSec感兴趣流中）//
            set members 5 4 3
            config sla
                edit 1
                    set latency-threshold 250
                    set jitter-threshold 50
                    set packetloss-threshold 5
                next
            end
        next
    end
end
```

bash

2. 查看健康检查的状态，可以看到目前3条去往Hub内网的线路都满足SLA标准。




```
Spoke # diagnose sys sdwan health-check status to_Hub
Health Check(to_Hub):
Seq(5 port4): state(alive), packet-loss(0.000%) latency(2.661), jitter(0.672), mos(4.402), bandwidth-up(65534998),
bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x1
Seq(4 to_Hub_CMCC): state(alive), packet-loss(0.000%) latency(108.022), jitter(17.742), mos(4.323), bandwidth-
up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x1
Seq(3 to_Hub_Unicom): state(alive), packet-loss(0.000%) latency(51.611), jitter(13.453), mos(4.362), bandwidth-
up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x1
```

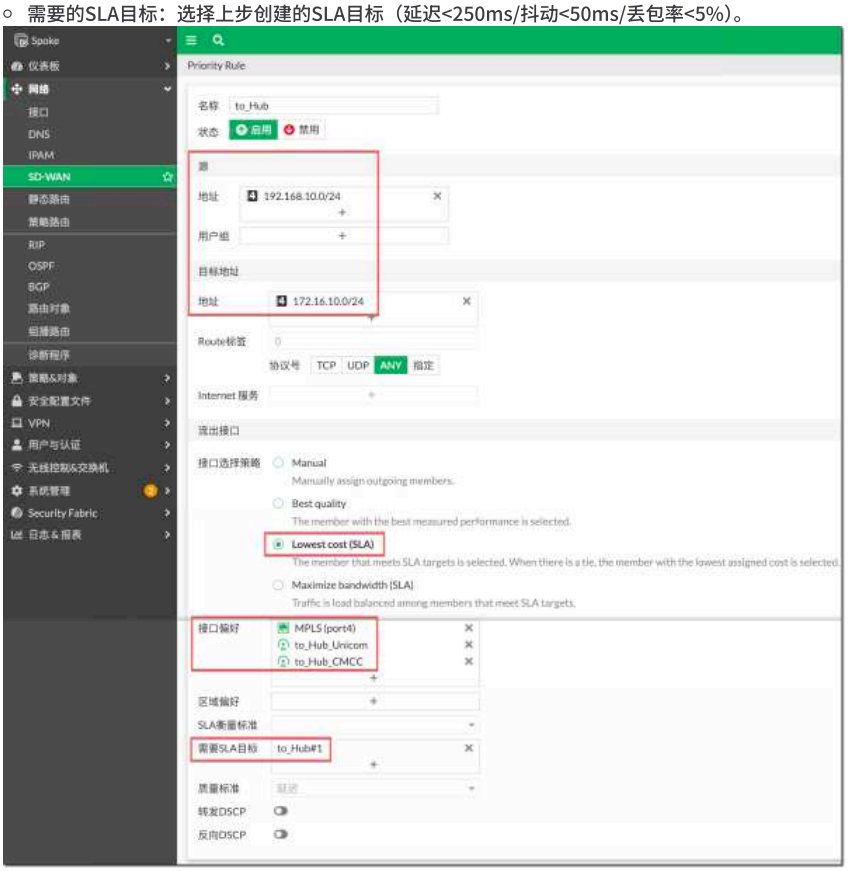
bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 新建SD-WAN规则1：



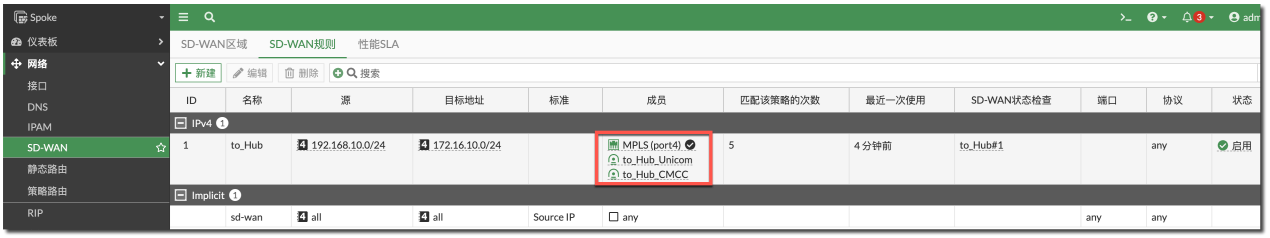
- 源地址选择Spoke内网网段；目标地址为Hub内网网段。
- 接口选择策略：选择Lowest Cost (SLA)，Spoke内部访问Hub内网的流量优先从满足SLA标准（延迟<250ms/抖动<50ms/丢包率<5%）的线路转发。如果3条线路都满足SLA标准，则优先从接口偏好中靠前的接口转发。
- 接口偏好：选择MPLS专线接口（port4）、联通线路IPSec接口与移动线路IPSec接口。MPLS专线接口（port4）排序在前，其次是联通线路IPSec接口，最后是移动线路IPSec接口。
- 需要的SLA目标：选择上步创建的SLA目标（延迟<250ms/抖动<50ms/丢包率<5%）。




```bash
config system sdwan
    config service
        edit 1
            set name "to_Hub"
            set mode sla
            set dst "172.16.10.0/24"
            set src "192.168.10.0/24"
            config sla
                edit "to_Hub"
                    set id 1
                next
            end
            set priority-members 5 3 4
        next
    end
end
```

4. 查看上步创建的SD-WAN规则目前的选路状态，由于目前3条去往Hub内网的线路均满足SLA目标，所以选择接口偏好配置中靠前的MPLS线路接口（port4）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
Spoke # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(5 port4), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected    //优先走MPLS专线接口//
    2: Seq_num(3 to_Hub_Unicom), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(4 to_Hub_CMCC), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
  Src address(1):
        192.168.10.0-192.168.10.255

  Dst address(1):
        172.16.10.0-172.16.10.255
```

5. 查看SD-WAN规则对应的策略路由状态，出接口优先选择MPLS线路接口（port4）。

```bash
Spoke # diagnose firewall proute list
list route policy info(vf=root):

id=2134835201(0x7f3f0001) vwl_service=1(to_Hub) vwl_mbr_seq=5 3 4 dscp_tag=0xfc 0xfc flags=0x0 tos=0x00
tos_mask=0x00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(3) oif=6(port4) oif=22(to_Hub_Unicom)
oif=23(to_Hub_CMCC)    //优先从MPLS线路接口转发//
source(1): 192.168.10.0-192.168.10.255
destination(1): 172.16.10.0-172.16.10.255
hit_count=5 last_used=2023-12-21 16:02:01
```

需求举例2

Spoke内部访问Internet的流量优先从满足SLA标准（延迟<250ms/抖动<50ms/丢包率<5%）的线路转发。如果两条Internet线路都满足SLA标准，则优先从联通线路转发。

1. 在Spoke的SD-WAN中配置探测Internet某个网站的HTTP健康检查，成员选择联通（port2）和移动（PPPoE）线路，开启SLA目标：延迟<250ms/抖动<50ms/丢包率<5%。

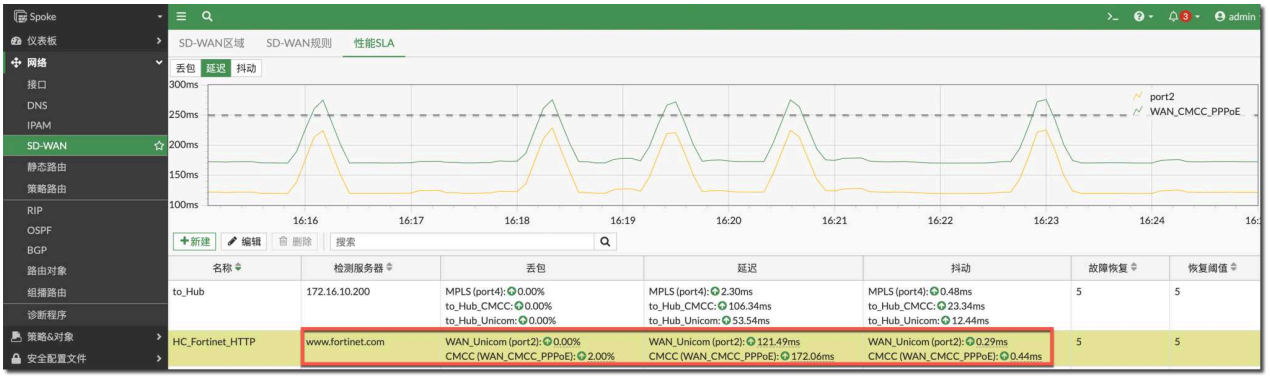


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config health-check
        edit "HC_Fortinet_HTTP"
            set server "www.fortinet.com"
            set members 1 2
            config sla
                edit 1
                    set latency-threshold 250
                    set jitter-threshold 50
                    set packetloss-threshold 5
                next
            end
        next
    end
end
```

2. 查看健康检查的状态，可以看到目前两条Internet线路都满足SLA标准。

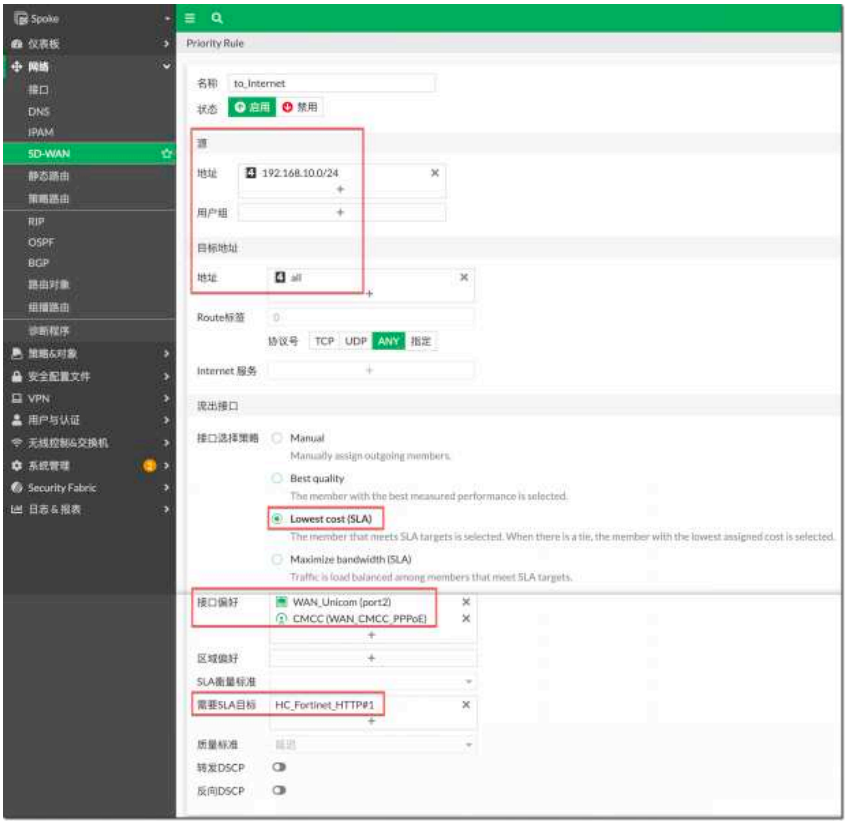



```bash
Spoke # diagnose sys sdwan health-check status HC_Fortinet_HTTP
Health Check(HC_Fortinet_HTTP):
Seq(1 port2): state(alive), packet-loss(1.000%) latency(115.769), jitter(0.618), mos(4.339), bandwidth-up(65534995), bandwidth-dw(65534996), bandwidth-bi(131069991) sla_map=0x1
Seq(2 WAN_CMCC_PPPoE): state(alive), packet-loss(2.000%) latency(166.407), jitter(0.782), mos(4.269), bandwidth-up(65534996), bandwidth-dw(65534997), bandwidth-bi(131069993) sla_map=0x1
```

3. 新建SD-WAN规则2：

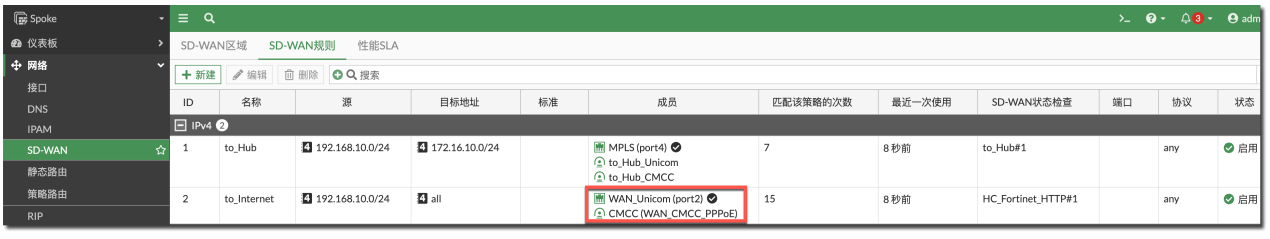
- 源地址选择内网网段；目标地址为all。
- 接口选择策略：选择Lowest Cost (SLA)，Spoke内部访问Internet的流量优先从满足SLA标准（延迟<250ms/抖动<50ms/丢包率<5%）的线路转发。如果两条Internet线路都满足SLA标准，则优先从接口偏好中靠前的接口转发。
- 接口偏好：选择联通线路接口（port2）与移动线路接口（PPPoE），联通线路接口排序在前。
- 需要SLA目标：选择上步创建的SLA目标（延迟<250ms/抖动<50ms/丢包率<5%）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config service
        edit 2
            set name "to_Internet"
            set mode sla
            set dst "all"
            set src "192.168.10.0/24"
            config sla
                edit "HC_Fortinet_HTTP"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

4. 查看上步创建的SD-WAN规则目前的选路状态，由于目前两条Internet线路均满足SLA目标，所以选择接口偏好配置中靠前的联通线路（port2）。




```bash
Spoke # diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 port2), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected    //联通线路（port2）优先//
    2: Seq_num(2 WAN_CMCC_PPPoE), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
```

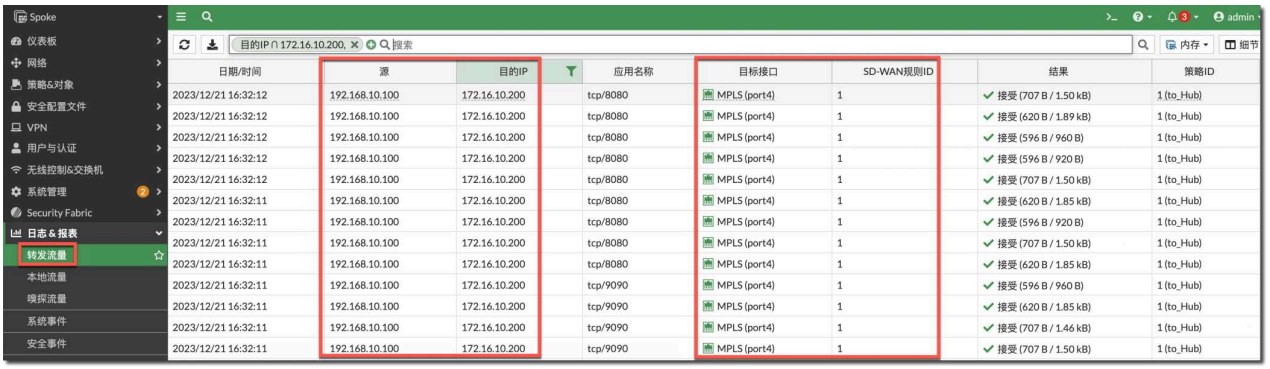

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    Src address(1):
          192.168.10.0-192.168.10.255

    Dst address(1):
          0.0.0.0-255.255.255.255
```

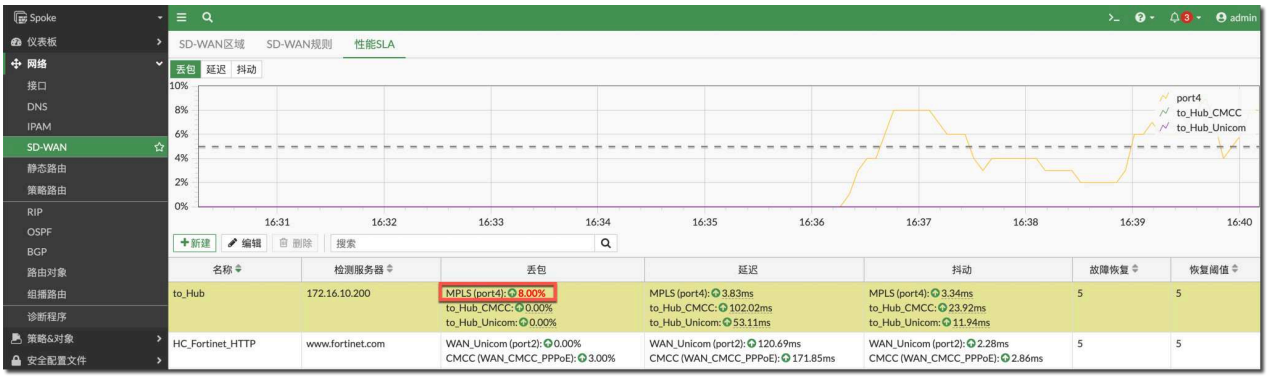
结果验证

Spoke访问Hub

1. 使用Spoke内网PC客户端访问Hub端的业务，流量可以正确的从MPLS线路接口（port4）转发。



2. 模拟MPLS线路（port4）的健康检查的丢包率增加到8%。




```bash
Spoke # diagnose sys sdwan health-check status to_Hub
Health Check(to_Hub):
Seq(5 port4): state(alive), packet-loss(8.000%) latency(2.444), jitter(0.530), mos(4.399), bandwidth-up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x0
Seq(4 to_Hub_CMCC): state(alive), packet-loss(0.000%) latency(106.955), jitter(26.069), mos(4.295), bandwidth-up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x1
Seq(3 to_Hub_Unicom): state(alive), packet-loss(0.000%) latency(57.014), jitter(16.204), mos(4.356), bandwidth-up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x1
```

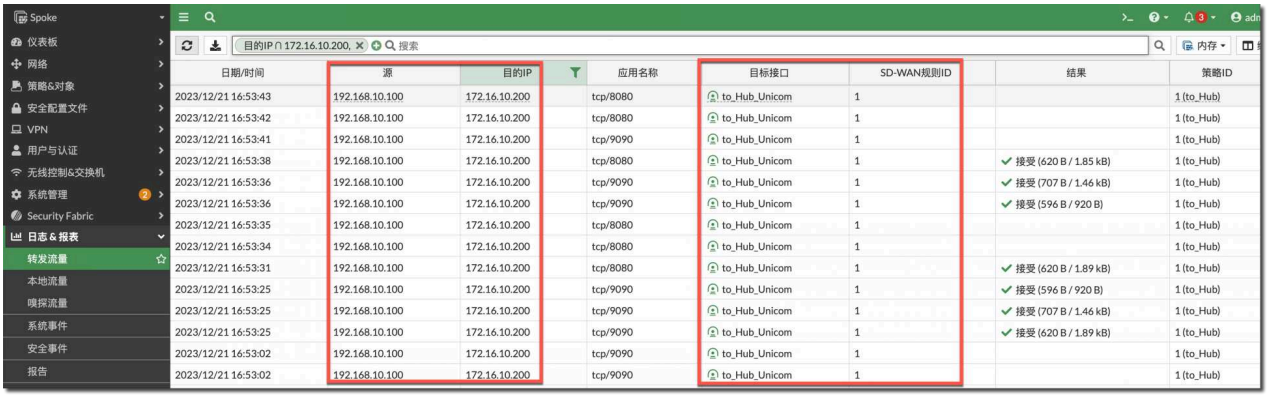
3. 查看SD-WAN规则1的选路优先选择联通线路IPSec接口去往Hub内网。



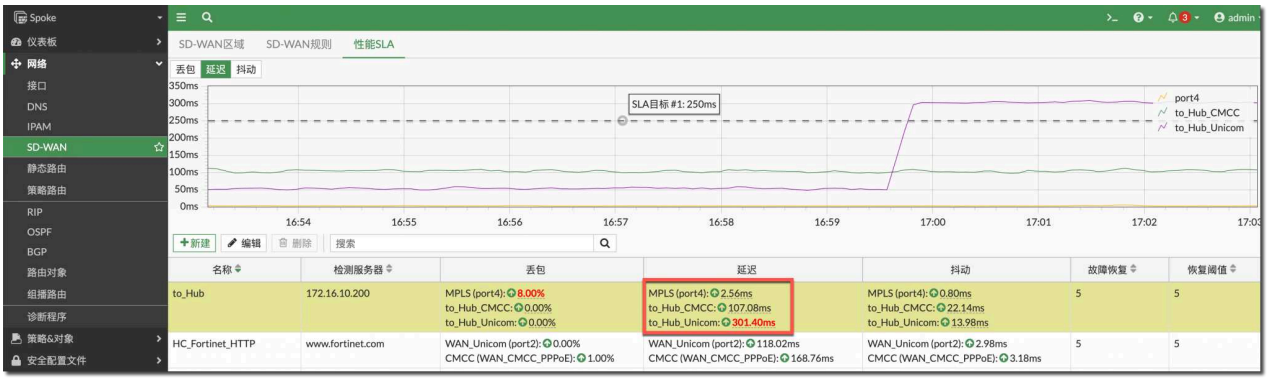
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
Spoke # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(22), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(3 to_Hub_Unicom), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected  //优先选择满足SLA线路中配置靠前的线路//
    2: Seq_num(4 to_Hub_CMCC), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
    3: Seq_num(5 port4), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected    //MPLS线路不满足SLA目标，被移至转发顺序最后//
  Src address(1):
        192.168.10.0-192.168.10.255

  Dst address(1):
        172.16.10.0-172.16.10.255
```

4. 再次使用Spoke内网PC客户端访问Hub端的业务，流量开始从联通线路IPSec接口转发。



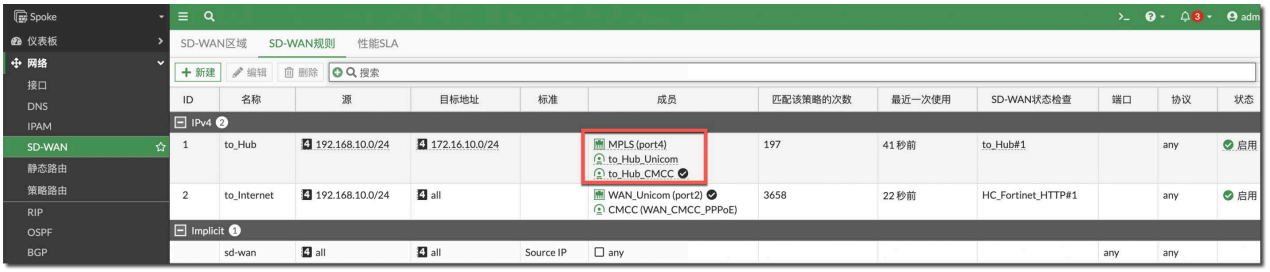
5. 模拟联通线路IPSec隧道健康检查的延迟增加到300ms。




```bash
Spoke # diagnose sys sdwan health-check status to_Hub
Health Check(to_Hub):
Seq(5 port4): state(alive), packet-loss(8.000%) latency(2.540), jitter(0.578), mos(4.399), bandwidth-up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x0
Seq(4 to_Hub_CMCC): state(alive), packet-loss(0.000%) latency(106.433), jitter(17.167), mos(4.325), bandwidth-up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x1
Seq(3 to_Hub_Unicom): state(alive), packet-loss(0.000%) latency(303.372), jitter(15.259), mos(3.635), bandwidth-up(65534998), bandwidth-dw(65534999), bandwidth-bi(131069997) sla_map=0x0
```

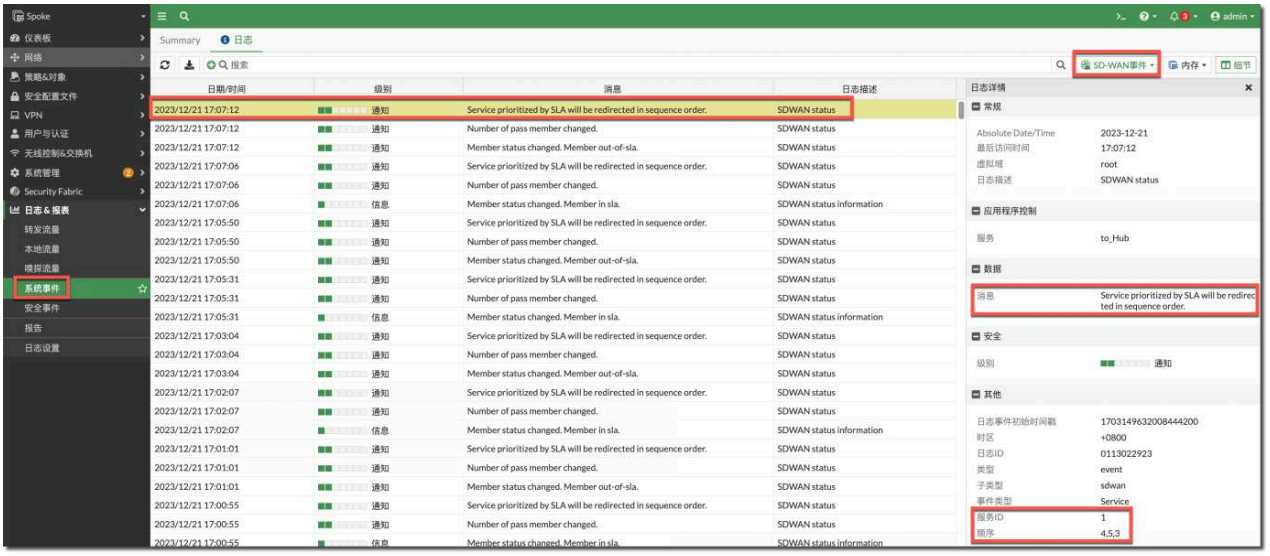
6. 查看SD-WAN规则1的选路优先选择移动线路IPSec接口去往Hub内网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
Spoke # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(33), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(sla), sla-compare-order
  Members(3):
    1: Seq_num(4 to_Hub_CMCC), alive, sla(0×1), gid(0), cfg_order(2), local cost(0), selected    //优先从移动线路IPSec隧道转发//
    2: Seq_num(5 port4), alive, sla(0×0), gid(0), cfg_order(0), local cost(0), selected    //MPLS线路不满足SLA目标//
    3: Seq_num(3 to_Hub_Unicom), alive, sla(0×0), gid(0), cfg_order(1), local cost(0), selected    //联通线路IPSec隧道不满足SLA目标//
  Src address(1):
        192.168.10.0-192.168.10.255

  Dst address(1):
        172.16.10.0-172.16.10.255
```

7. 对应的SD-WAN线路切换系统日志。




```bash
date=2023-12-21 time=17:07:12 eventtime=1703149632008444112 tz="+0800" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="to_Hub" seq="4,5,3" msg="Service prioritized by SLA will be redirected in sequence order."
```

8. 再次使用Spoke内网PC客户端访问Hub端的业务，流量开始从移动线路IPSec接口转发。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Spoke访问Internet

测试结果请参考Spoke访问Hub内网，线路可以根据健康检查结果是否满SLA目标正常切换，这里不再赘述。

注意事项

1. 默认配置下，当Internet线路（有SNAT）SD-WAN选路出现变化后，已有的会话不会立即切换到新链路上，只有线路切换后新创建的会话会建立在新的线路上，如果想在SD-WAN线路切换后让已有会话立刻失效，需要使用如下命令（可能会增加CPU消耗，谨慎开启）。

> **重要**
>
> 默认配置下的SNAT场景，即使转发流量的SD-WAN成员的健康检查变为dead，只要该线路仍然存在路由（可能关闭了`update-static-route`），已有的旧会话仍然不会切换到其他线路。

```bash
config system global
    set snat-route-change enable    //默认为disable//
end
```

2. 默认配置下，当VPN或专线线路（无SNAT）SD-WAN选路出现变化后，已有的会话会立即切换到新链路上，如果想在SD-WAN线路切换后让已有会话保持在原来的线路上，只有新会话创建在新线路上，需要在对应VPN接口或专线接口上使用如下命令。

```bash
config system interface
    edit "to_Hub_Unicom"
        set preserve-session-route enable    //默认为disable//
    next
end
```

3. 如何设置`add-route`功能添加的路由优先级（priority）和管理距离（distance）？开启`add-route`后，默认添加的路由优先级为1，管理距离为15，如果要自定义路由优先级或管理距离，请参考如下配置（注意只有拨号模式的IPSec可以使用`add-route`功能。

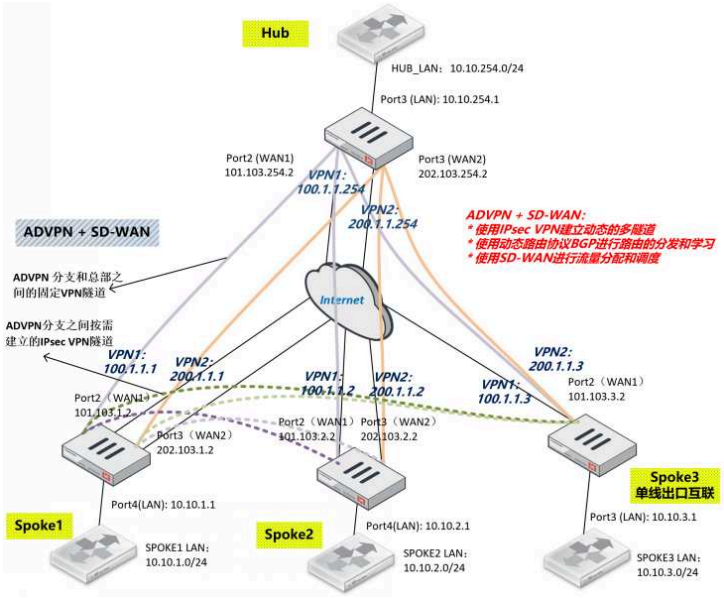
```bash
config vpn ipsec phase1-interface
    edit "Hub_Unicom"
        set type dynamic
        set add-route enable
        set priority 100
        set distance 20
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ADVPN场景

> **重要**
>
> ADVPN目前不支持Maximize Bandwidth (SLA)模式。

网络拓扑与需求



1. 使用IPsec VPN建立动态的多隧道，Hub和Spoke之间是固定的IPSec隧道，而Spoke和Spoke之间则是流量触发的按需动态创建的VPN隧道。
2. 使用动态路由协议BGP进行路由的分发和学习，HUB充当BGP路由反射器进行路由的传递，同时分支需要开启“additional-path”，形成VPN业务路由的负载分担BGP路由，这是SD-WAN可以调度的前提（路由表中有路由）。
3. 使用SD-WAN规则对流量进行分配和调度，可以配置特定的SD-WAN算法进行流量的调度。
4. 部署SD-WAN通常在一个全新的设备进行配置，如果需要加入SD-WAN区域的接口已经被其他配置（如防火墙策略）引用，是无法直接加入SD-WAN区域的。要加入SD-WAN区域，又不想删除关联的配置，请参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域 ↗章节。

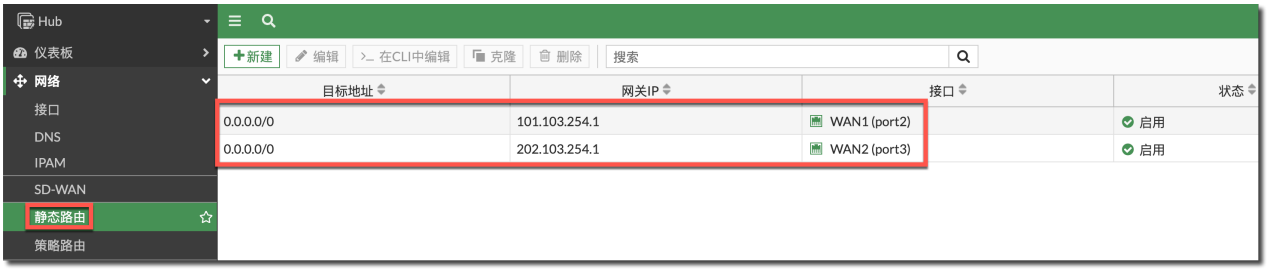
配置步骤

基础配置

Hub

1. 在Hub设备上配置WAN1（port2）、WAN2（port3）以及LAN（port4）的接口IP（略）。

2. 配置两个WAN接口上访问Internet的默认路由。




```bash
config router static
    edit 1
        set gateway 101.103.254.1
        set device "port2"
    next
    edit 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set gateway 202.103.254.1
        set device "port3"
    next
end

Hub # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.103.254.1, port2, [1/0]
                  [10/0] via 202.103.254.1, port3, [1/0]
C       10.10.254.0/24 is directly connected, port4
C       101.103.254.0/24 is directly connected, port2
C       202.103.254.0/24 is directly connected, port3
```

Spoke

1. 配置每个Spoke FortiGate运营商线路的IP（如果是PPPoE线路，PPPoE请通过CLI配置，参考部署前注意事项→PPPoE接口配置↗章节）与内网口IP（略）。
2. 在每个Spoke配置WAN接口上访问Internet的默认路由（略，参考Hub上的配置）。

IPSec相关配置

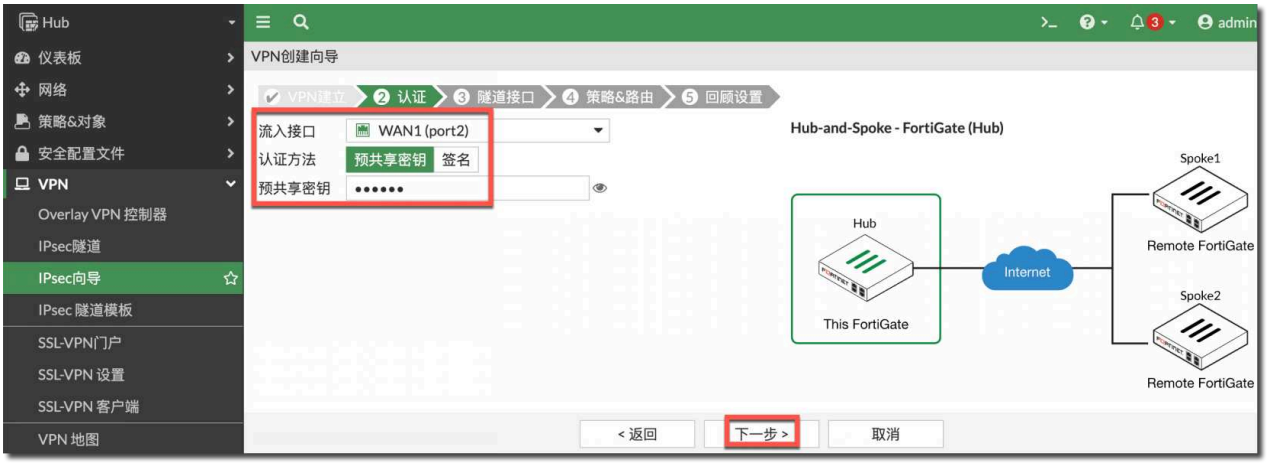
Hub

1. 通过ADVPN向导来配置ADVPN，进入“VPN→IPSec向导”页面，模板类型选择“Hub-and-Spoke”类型，角色选择Hub，点击下一步。

> **重要**
>
> 通过ADVPN向导来配置ADVPN可以快速地部署ADVPN + BGP环境，而不用在每个Spoke上进行相关的具体功能配置，大大增加了部署效率与难度，部署完成后，可以再根据实际需求对配置进行调整。



2. 配置WAN1（port2）接口上的IPSec拨号连接，流入接口选择WAN1（port2），配置认证方法，这里以预共享密钥为例，填入预共享密钥，点击下一步。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 配置Hub端WAN1（port2）上的IPSec Tunnel IP，用于BGP邻居建立，配置“远程IP地址/掩码”为一个24位网络地址（根据Spoke的数量判断掩码位数），点击下一步。

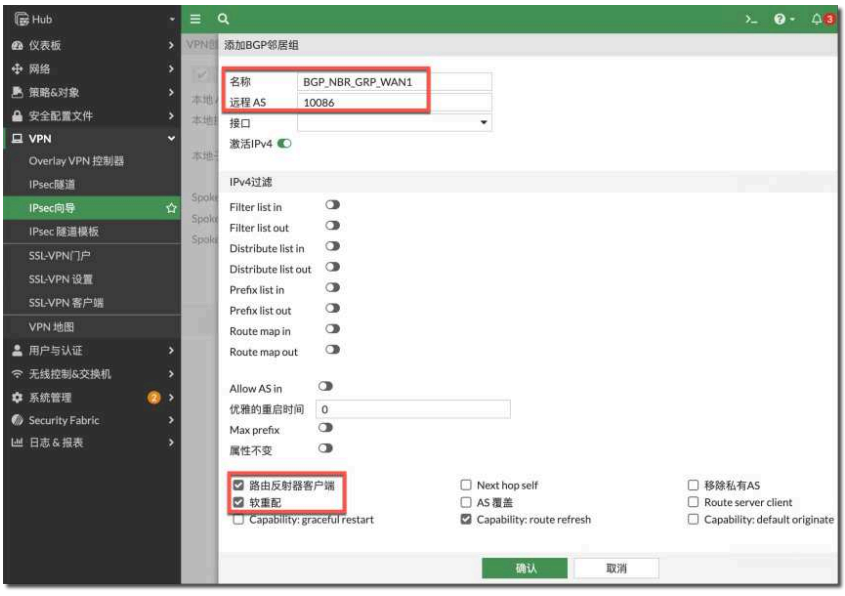


4. 配置BGP路由的本地AS号（此例中Hub和所有的Spoke之间为IBGP邻居），Hub端内网接口与网段（用于自动创建安全策略和BGP路由发布），Spoke type选择“范围”，填写Spoke prefix范围为WAN1线路IPSec对应的Spoke Tunnel接口IP的范围子网，点击Spoke邻居组中的新建按钮。

> **重要**
>
> Spoke type推荐使用“范围”模式，并结合BGP邻居范围和BGP邻居组使用，否则如果Spoke较多，每个Spoke配置一个BGP邻居将是一个巨大的工作量。



5. 在弹出的BGP邻居组窗口中，配置远程AS（此例中Hub和所有的Spoke之间为IBGP邻居），开启路由反射器和软重配。点击确认按钮下发BGP邻居组配置。

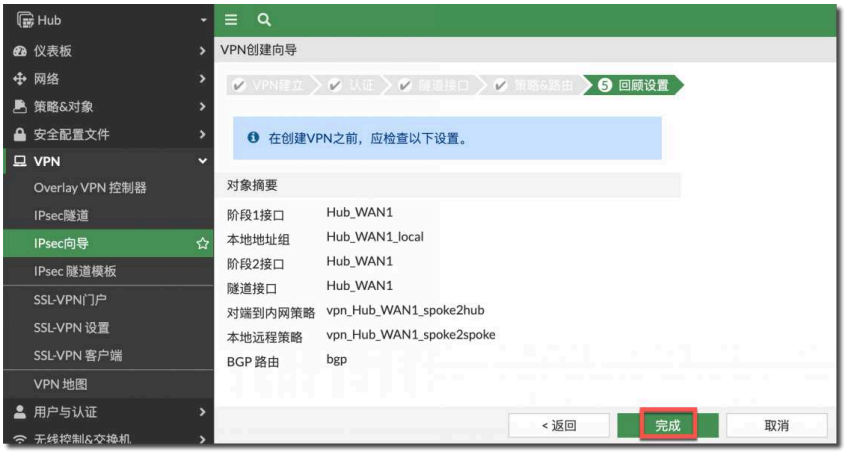


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

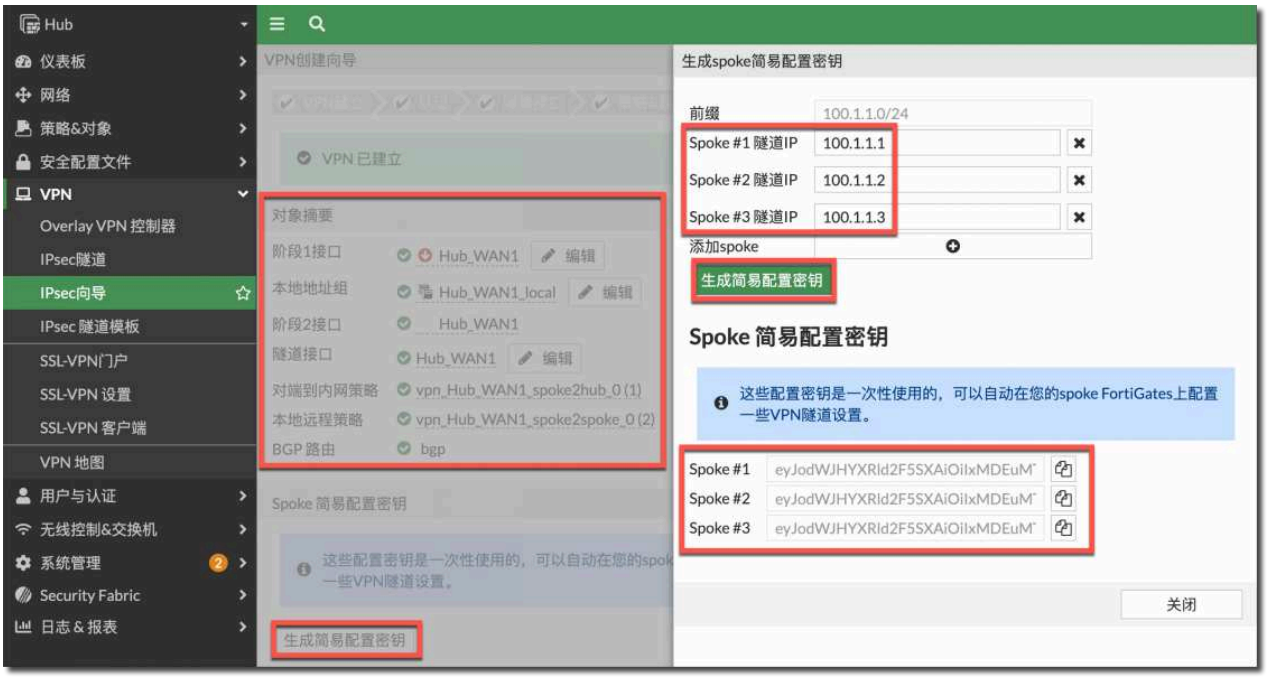
6. Spoke邻居组选择上步创建的BGP邻居组，点击下一步。



7. 查看即将创建的配置内容，点击完成按钮。

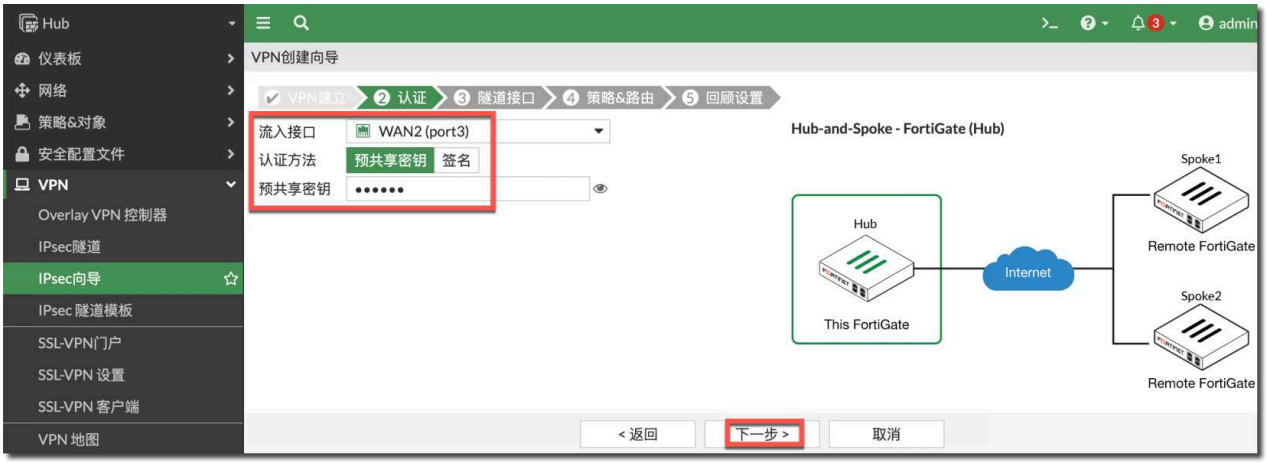


8. 检查对象摘要中的配置是否全部下发成功。然后点击下方的“生成简易配置密钥”按钮，在右侧弹出的窗口中，添加WAN1（port2）线路IPSec隧道对应的三个Spoke的Tunnel接口IP。然后点击“生成简易配置密钥”按钮，将生成的3个Spoke简易配置密钥复制出来并保存。

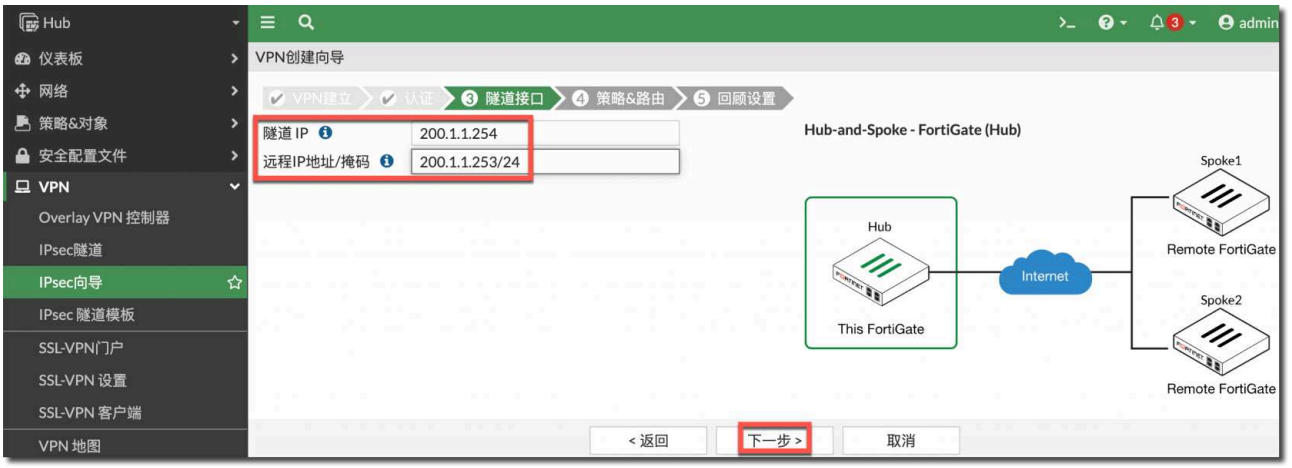


9. 配置WAN2（port3）接口上的IPSec拨号连接，流入接口选择WAN2（port3），配置认证方法，这里以预共享密钥为例，填入预共享密钥，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



10. 配置Hub端WAN2（port3）上的IPSec Tunnel IP，用于BGP邻居建立，配置“远程IP地址/掩码”为一个24位网络地址（根据Spoke的数量判断掩码位数），点击下一步。



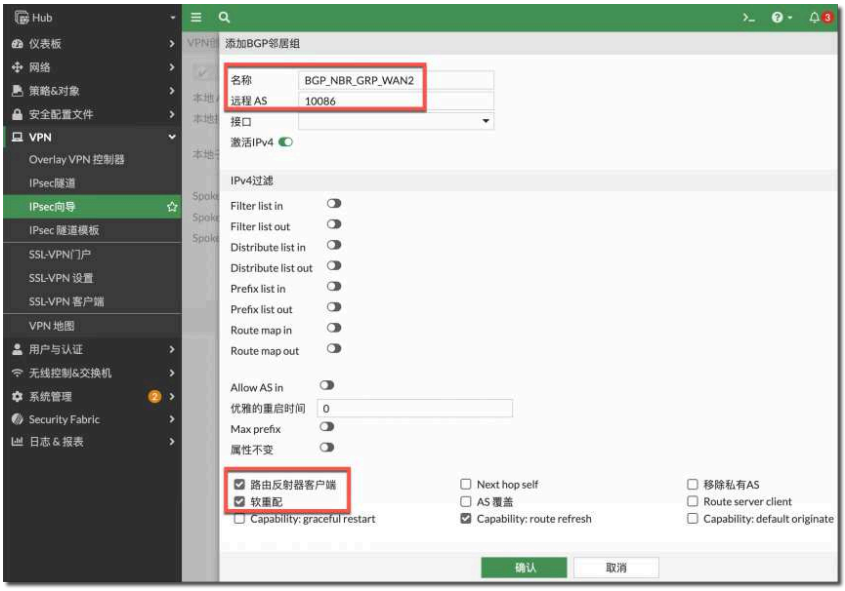
11. 配置BGP路由的本地AS号（此例中Hub和所有的Spoke之间为IBGP邻居），Hub端内网接口与网段（用于自动创建安全策略和BGP路由发布），Spoke type选择“范围”，填写Spoke prefix范围为WAN1线路IPSec对应的Spoke Tunnel接口IP的范围子网，点击Spoke邻居组中的新建按钮。

> **重要**
>
> Spoke type推荐使用“范围”模式，并结合BGP邻居范围和BGP邻居组使用，否则如果Spoke较多，每个Spoke配置一个BGP邻居将是一个巨大的工作量。



12. 在弹出的BGP邻居组窗口中，配置远程AS（此例中Hub和所有的Spoke之间为IBGP邻居），开启路由反射器和软重配。点击确认按钮下发BGP邻居组配置。

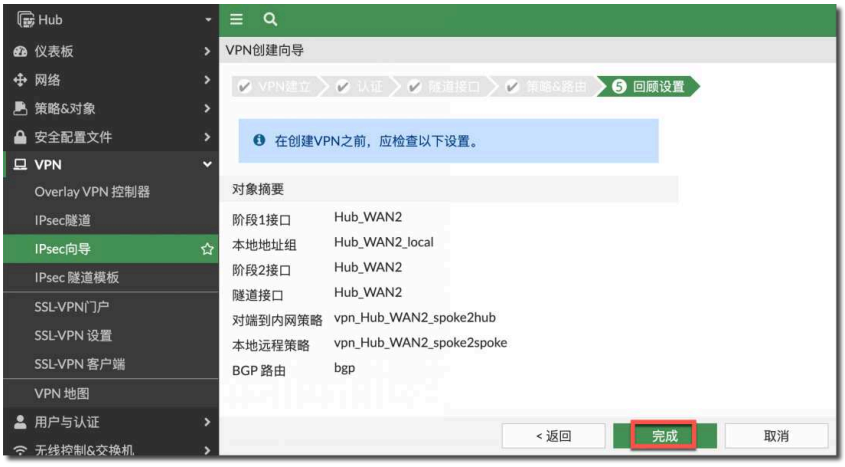
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. Spoke邻居组选择上步创建的BGP邻居组，点击下一步。

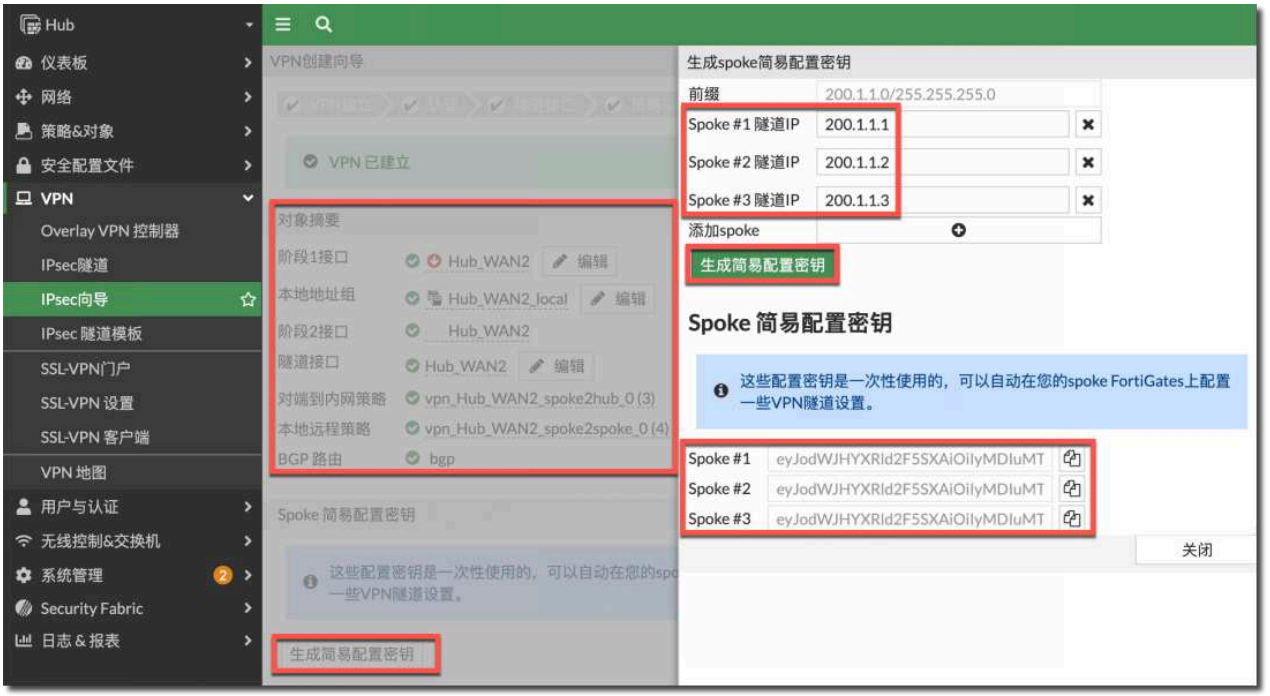


4. 查看即将创建的配置内容，点击完成按钮。



5. 检查对象摘要中的配置是否全部下发成功。然后点击下方的“生成简易配置密钥”按钮，在右侧弹出的窗口中，添加WAN1（port2）线路IPSec隧道对应的三个Spoke的Tunnel接口IP。然后点击“生成简易配置密钥”按钮，将生成的3个Spoke简易配置密钥复制出来并保存。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 查看IPSec向导下发的IPSec配置，以及IPSec Tunnel接口配置。注意要在IPSec一阶段中增加下步中的配置。

```bash
config vpn ipsec phase1-interface
    edit "Hub_WAN1"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: Hub_WAN1 (Created by VPN wizard)"
        set wizard-type hub-fortigate-auto-discovery
        set auto-discovery-sender enable    //确认开启了ADVPN sender//
        set psksecret ENC
LRPVkrjrtBp5qTlA1Bo5E3M0Cr/79r/kqV7vZmqrNqckeTk2kJf2/W5Xi2lni2CPCfSukYx0CY9cyWwu6C2IuwxiK4chuJXZbuhYejUguiHmZE=
    next
    edit "Hub_WAN2"
        set type dynamic
        set interface "port3"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: Hub_WAN2 (Created by VPN wizard)"
        set wizard-type hub-fortigate-auto-discovery
        set auto-discovery-sender enable    //确认开启了ADVPN sender//
        set psksecret ENC
g3UIj62MLpQkr791Zf+pujPQ2QqbzDnvcwLDmF5xr5apZLk8FDRs+YtDJGtJ5vnMEG6K2lEhluoO/M5gjGu5qjJatbTRvblp0FPBUQGW2X2eFY=
    next
end

config vpn ipsec phase2-interface
    edit "Hub_WAN1"
        set phase1name "Hub_WAN1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: Hub_WAN1 (Created by VPN wizard)"
    next
    edit "Hub_WAN2"
        set phase1name "Hub_WAN2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: Hub_WAN2 (Created by VPN wizard)"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system interface
    edit "Hub_WAN1"
        set vdom "root"
        set ip 100.1.1.254 255.255.255.255
        set type tunnel
        set remote-ip 100.1.1.253 255.255.255.0
        set interface "port2"
    next
    edit "Hub_WAN2"
        set vdom "root"
        set ip 200.1.1.254 255.255.255.255
        set type tunnel
        set remote-ip 200.1.1.253 255.255.255.0
        set interface "port3"
    next
end
```

7. 需要在向导配置的基础上，将IKEv1主模式修改为IKEv2，并在每个线路的IPSec上开启network-overlay，配置不同的network-id，WAN1上的IPSec的network-id为1，WAN2上的IPSec的network-id为2。

> **重要**
>
> 使用ADVPN向导创建的IPSec为IKEv1主模式，Hub双线路的情况下，Spoke与Spoke在建立Shortcut时会出现问题（参考VPN技术→IPSec VPN→拨号VPN→野蛮模式/network-id适用场景→ ADVPN下的network-id或野蛮模式ID ↗的说明）。

bash
```
config vpn ipsec phase1-interface
    edit "Hub_WAN1"
        set ike-version 2              //增加配置：将IKE版本修改为2//
        set network-overlay enable     //增加配置：开启network-overlay//
        set network-id 1               //增加配置：第一条线路上的network-id为1//
    next
    edit "Hub_WAN2"
        set ike-version 2              //增加配置：将IKE版本修改为2//
        set network-overlay enable     //增加配置：开启network-overlay//
        set network-id 2               //增加配置：配置第二条线路上的network-id为2//
    next
end
```

8. 查看IPSec向导下发的地址、地址组和安全策略配置，包含放通Hub端IPSec隧道的入向流量、放通IPSec隧道的中转流量，可根据实际需求进行调整或新增（如Hub向Spoke主动发起的方向策略）。

> **重要**
>
> 后续如果需要在Hub上配置SD-WAN，安全策略配置需要删除，否则IPSec Tunnel接口无法加入SD-WAN区域。

bash
```
config firewall address
    edit "Hub_WAN1_local_subnet_1"
        set allow-routing enable
        set subnet 10.10.254.0 255.255.255.0
    next
    edit "Hub_WAN2_local_subnet_1"
        set allow-routing enable
        set subnet 10.10.254.0 255.255.255.0
    next
end
config firewall addrgrp
    edit "Hub_WAN1_local"
        set member "Hub_WAN1_local_subnet_1"
        set comment "VPN: Hub_WAN1 (Created by VPN wizard)"
        set allow-routing enable
    next
    edit "Hub_WAN2_local"
        set member "Hub_WAN2_local_subnet_1"
        set comment "VPN: Hub_WAN2 (Created by VPN wizard)"
        set allow-routing enable
    next
end

config firewall policy
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    edit 1    //放通了WAN1上IPSec隧道的入向流量//
        set name "vpn_Hub_WAN1_spoke2hub_0"
        set srcintf "Hub_WAN1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "Hub_WAN1_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Hub_WAN1 (Created by VPN wizard)"
    next
    edit 2    //放通了WAN1上IPSec隧道的中转流量//
        set name "vpn_Hub_WAN1_spoke2spoke_0"
        set srcintf "Hub_WAN1"
        set dstintf "Hub_WAN1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Hub_WAN1 (Created by VPN wizard)"
    next
    edit 3    //放通了WAN2上IPSec隧道的入向流量//
        set name "vpn_Hub_WAN2_spoke2hub_0"
        set srcintf "Hub_WAN2"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "Hub_WAN2_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Hub_WAN2 (Created by VPN wizard)"
    next
    edit 4    //放通了WAN2上IPSec隧道的中转流量//
        set name "vpn_Hub_WAN2_spoke2spoke_0"
        set srcintf "Hub_WAN2"
        set dstintf "Hub_WAN2"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Hub_WAN2 (Created by VPN wizard)"
    next
end

```

9. 查看IPSec向导下发的BGP配置。

```bash
config router bgp
    set as 10086
    config neighbor-group
        edit "BGP_NBR_GRP_WAN1"
            set soft-reconfiguration enable
            set remote-as 10086
            set route-reflector-client enable
        next
        edit "BGP_NBR_GRP_WAN2"
            set soft-reconfiguration enable
            set remote-as 10086
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 100.1.1.0 255.255.255.0
            set neighbor-group "BGP_NBR_GRP_WAN1"
        next
        edit 2
            set prefix 200.1.1.0 255.255.255.0
            set neighbor-group "BGP_NBR_GRP_WAN2"
        next
    end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    config network
        edit 1
            set prefix 10.10.254.0 255.255.255.0
        next
    end
end
```

0. 在ADVPN环境下，以上BGP配置还需要手动增加如下参数。

```bash
config router bgp
    set ibgp-multipath enable    //必须配置，否则去往Spoke的路由无法负载//
    set additional-path enable    //多线路ADVPN，Hub端必须配置，否则Spoke学到的路由可能不全//
    set additional-path-select 4
    config neighbor-group
        edit "BGP_NBR_GRP_WAN1"
            set link-down-failover enable
            set additional-path send    //多线路ADVPN，Hub端必须配置，否则Spoke学到的路由可能不全//
            set adv-additional-path 4    //配置从几条额外路径上去发送路由//
            set soft-reconfiguration enable
        next
        edit "BGP_NBR_GRP_WAN2"
            set link-down-failover enable
            set additional-path send    //多线路ADVPN，Hub端必须配置，否则Spoke学到的路由可能不全//
            set adv-additional-path 4    //配置从几条额外路径上去发送路由//
            set soft-reconfiguration enable
        next
    end
end
```

Spoke

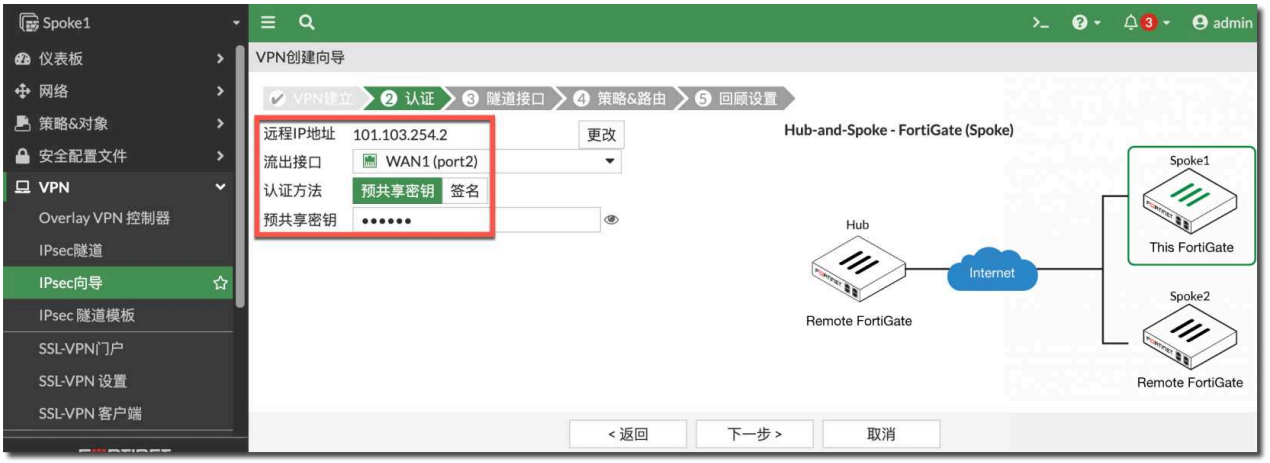
1. Hub端通过向导配置ADVPN后，在Spoke端的配置就轻松很多。准备好在Hub端复制出的Spoke简易配置密钥。

2. 在Spoke1 FortiGate上进入VPN→IPSec隧道页面，新建WAN1（port2）上的IPSec隧道，选择“Hub-and-Spoke”模式，角色选择Spoke，将Spoke1 WAN1的IPSec隧道对应的简易配置密钥粘贴进去，然后点击右侧的应用按钮，会弹出提示“配置已应用”，然后点击下一步。



3. Spoke1自动将Hub端WAN1（port2）的IP地址填入，配置流出接口为WAN1（port2），配置预共享密钥，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. Spoke1自动配置了WAN1（port2）线路IPSec Tunnel口的地址（在Hub端向导中的配置），远程IP地址/掩码为Hub端WAN1线路IPSec Tunnel接口地址。点击下一步。

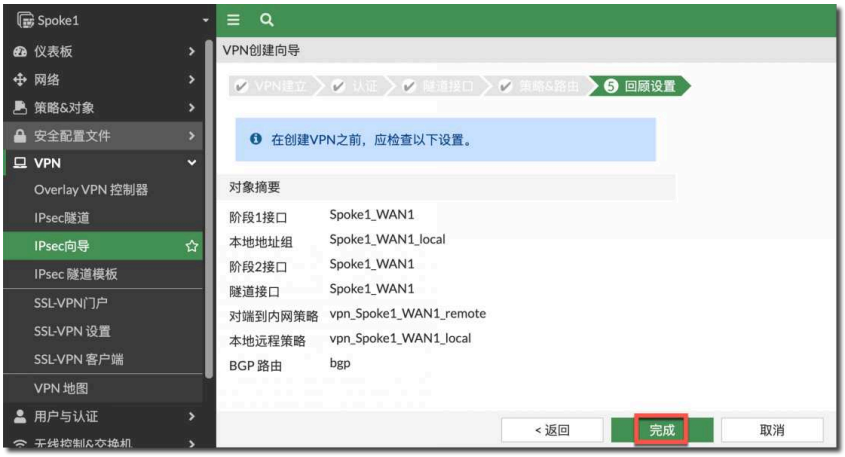


5. 配置BGP本地AS（此例中Hub和所有的Spoke之间为IBGP邻居），配置本地接口和本地子网（用于自动创建安全策略和BGP路由发布）。点击下一步。

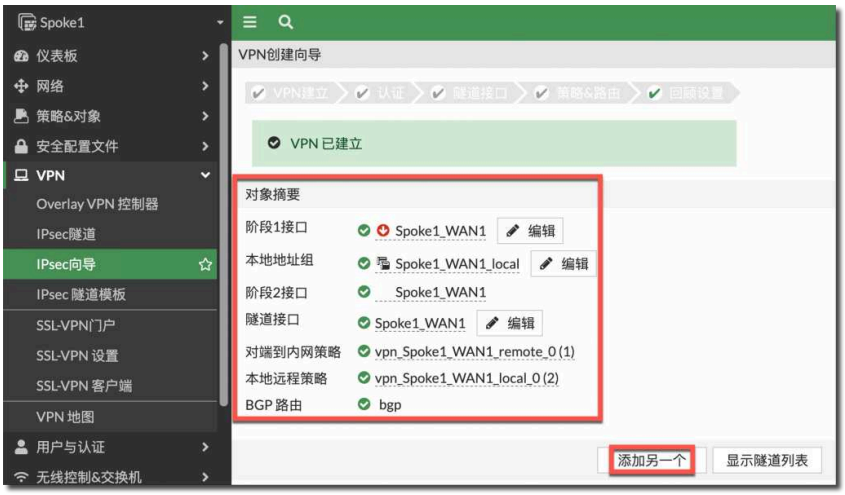


6. 查看即将下发的相关配置，点击完成按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 检查相关配置均下发成功后，点击“添加另一个”按钮。

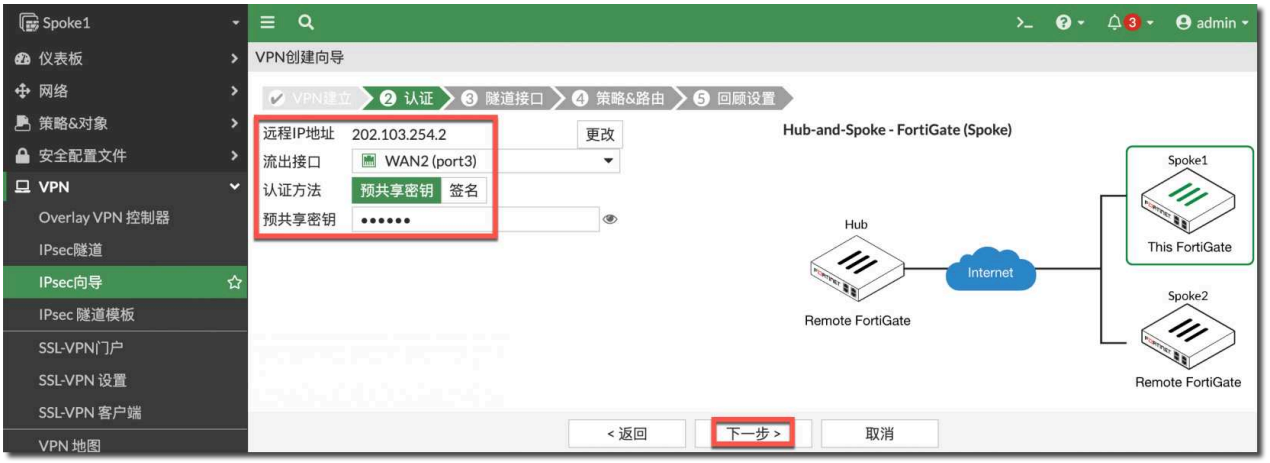


8. 新建WAN2（port3）上的IPSec隧道，选择“Hub-and-Spoke”模式，角色选择Spoke，将Spoke1 WAN2的IPSec隧道对应的简易配置密钥粘贴进去，然后点击右侧的应用按钮，会弹出提示“配置已应用”，然后点击下一步。



9. Spoke1自动将Hub端WAN2（port3）的IP地址填入，配置流出接口为WAN2（port3），配置预共享密钥，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



10. Spoke1自动配置了WAN2（port3）线路IPSec Tunnel口的地址（在Hub端向导中的配置），远程IP地址/掩码为Hub端WAN2线路IPSec Tunnel接口地址。点击下一步。

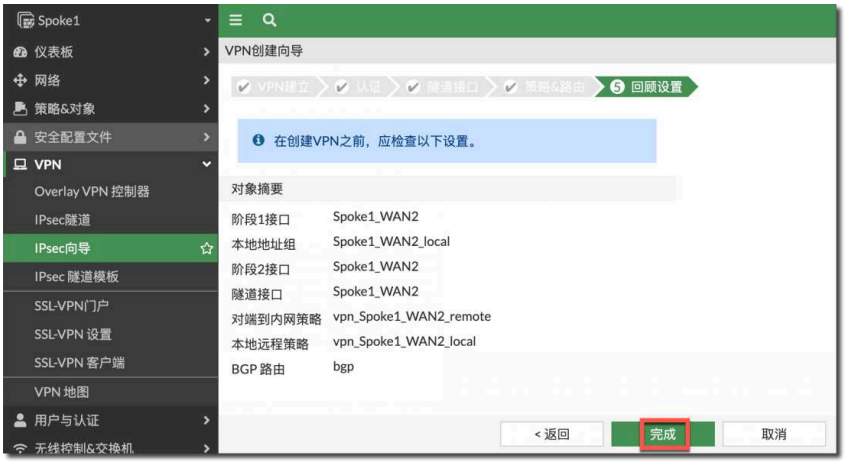


11. 配置BGP本地AS（此例中Hub和所有的Spoke之间为IBGP邻居），配置本地接口和本地子网（用于自动创建安全策略和BGP路由发布）。点击下一步。



12. 查看即将下发的相关配置，点击完成按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 检查相关配置均下发成功。



4. 在Spoke1上查看向导下发的IPSec配置以及IPSec Tunnel接口配置。注意要在IPSec一阶段中增加下步中的配置。

```bash
config vpn ipsec phase1-interface
    edit "Spoke1_WAN1"
        set interface "port2"
        set peertype any
        set net-device enable    //确保Spoke的net-device开启，否则使用SD-WAN时，Shortcut的健康检查无法正常工作//
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: Spoke1_WAN1 (Created by VPN wizard)"
        set wizard-type spoke-fortigate-auto-discovery
        set auto-discovery-receiver enable    //确认开启了ADVPN receiver//
        set remote-gw 101.103.254.2
        set psksecret ENC
jZJjdqGe4N3alz21hgoMkyE1t5HDNMSanAQpDEtCwitgjX2hvApP24ZC3axQP4f9qdqT/oeVmj/5bWBXt1drV/rrwPOHteGqFhMmDuRGpHK7qA=
    next
    edit "Spoke1_WAN2"
        set interface "port3"
        set peertype any
        set net-device enable    //确保Spoke的net-device开启，否则使用SD-WAN时，Shortcut的健康检查无法正常工作//
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: Spoke1_WAN2 (Created by VPN wizard)"
        set wizard-type spoke-fortigate-auto-discovery
        set auto-discovery-receiver enable    //确认开启了ADVPN receiver//
        set remote-gw 202.103.254.2
        set psksecret ENC
uH/eLzEpwUxUfKKcFdZYZ9q/bNsDSKCal2iF7LuF978SppZrpdHQi2BpWdTcSlQaDWZ6QaeyeXn+8crQLCavpKv7fa9XhyI+U/OLf7J0LSHc/n=
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase2-interface
    edit "Spoke1_WAN1"
        set phase1name "Spoke1_WAN1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: Spoke1_WAN1 (Created by VPN wizard)"
    next
    edit "Spoke1_WAN2"
        set phase1name "Spoke1_WAN2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: Spoke1_WAN2 (Created by VPN wizard)"
    next
end

config system interface
    edit "Spoke1_WAN1"
        set vdom "root"
        set ip 100.1.1.1 255.255.255.255
        set type tunnel
        set remote-ip 100.1.1.254 255.255.255.0
        set interface "port2"
    next
    edit "Spoke1_WAN2"
        set vdom "root"
        set ip 200.1.1.1 255.255.255.255
        set type tunnel
        set remote-ip 200.1.1.254 255.255.255.0
        set interface "port3"
    next
end
```

5. 需要在向导配置的基础上，将IKEv1主模式修改为IKEv2，并在每个线路的IPSec上开启network-overlay，配置不同的network-id，WAN1上的IPSec的network-id为1，WAN2上的IPSec的network-id为2。

> **重要**
>
> 使用ADVPN向导创建的IPSec为IKEv1主模式，Hub双线路的情况下，Spoke与Spoke在建立Shortcut时会出现问题（参考VPN技术→IPSec VPN→拨号VPN→野蛮模式/network-id适用场景→ ADVPN下的network-id或野蛮模式ID ↗的说明）。

bash
```
config vpn ipsec phase1-interface
    edit "Spoke1_WAN1"
        set ike-version 2             //增加配置：将IKE版本修改为2//
        set network-overlay enable    //增加配置：开启network-overlay//
        set network-id 1              //增加配置：第一条线路上的network-id为1//
    next
    edit "Spoke1_WAN2"
        set ike-version 2             //增加配置：将IKE版本修改为2//
        set network-overlay enable    //增加配置：开启network-overlay//
        set network-id 2              //增加配置：第二条线路上的network-id为2//
    next
end
```

6. 在SD-WAN（配置了健康检查）+ADVPN环境下，以上IPSec Tunnel接口还需要手动增加允许Ping的配置，用于SD-WAN在Spoke之间的Shortcut隧道自动创建的健康检查。

> **重要**
>
> SD-WAN在Shortcut间自动创建的健康检查为Ping模式，即使配置的健去往Hub的健康检查为其他模式。

bash
```
config system interface
    edit "Spoke1_WAN1"
        append allowaccess ping
    next
    edit "Spoke1_WAN2"
        append allowaccess ping
    next
end
```

7. 查看Spoke1上IPSec向导下发的地址、地址组和安全策略配置，包含放通Spoke IPSec隧道的双向流量的策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

后续要在Spoke配置SD-WAN，这些安全策略配置需要删除，否则IPSec接口无法加入SD-WAN区域。

bash

```
config firewall address
    edit "Spoke1_WAN1_local_subnet_1"
        set allow-routing enable
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Spoke1_WAN2_local_subnet_1"
        set allow-routing enable
        set subnet 10.10.1.0 255.255.255.0
    next
end

config firewall addrgrp
    edit "Spoke1_WAN1_local"
        set member "Spoke1_WAN1_local_subnet_1"
        set comment "VPN: Spoke1_WAN1 (Created by VPN wizard)"
        set allow-routing enable
    next
    edit "Spoke1_WAN2_local"
        set member "Spoke1_WAN2_local_subnet_1"
        set comment "VPN: Spoke1_WAN2 (Created by VPN wizard)"
        set allow-routing enable
    next
end

config firewall policy
    edit 1
        set name "vpn_Spoke1_WAN1_remote_0"
        set srcintf "Spoke1_WAN1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "Spoke1_WAN1_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Spoke1_WAN1 (Created by VPN wizard)"
    next
    edit 2
        set name "vpn_Spoke1_WAN1_local_0"
        set srcintf "port4"
        set dstintf "Spoke1_WAN1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Spoke1_WAN1 (Created by VPN wizard)"
    next
    edit 3
        set name "vpn_Spoke1_WAN2_remote_0"
        set srcintf "Spoke1_WAN2"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "Spoke1_WAN2_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: Spoke1_WAN2 (Created by VPN wizard)"
    next
    edit 4
        set name "vpn_Spoke1_WAN2_local_0"
        set srcintf "port4"
        set dstintf "Spoke1_WAN2"
        set action accept
        set srcaddr "all"
        set dstaddr "all"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set schedule "always"
        set service "ALL"
        set comments "VPN: Spoke1_WAN2 (Created by VPN wizard)"
    next
end
```

8. 查看Spoke1上IPSec向导下发的BGP配置。

```bash
config router bgp
    set as 10086
    config neighbor
        edit "100.1.1.254"
            set remote-as 10086
        next
        edit "200.1.1.254"
            set remote-as 10086
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```

9. 在ADVPN环境下，以上BGP配置还需要手动增加如下参数。

```bash
config router bgp
    set ibgp-multipath enable    //必须配置，否则去往Hub或其他Spoke的路由无法负载//
    config neighbor
        edit "100.1.1.254"
            set additional-path receive    //多线路ADVPN，Spoke端必须配置，否则Spoke学到的路由可能不全//
            set soft-reconfiguration enable
        next
        edit "200.1.1.254"
            set additional-path receive    //多线路ADVPN，Spoke端必须配置，否则Spoke学到的路由可能不全//
            set soft-reconfiguration enable
        next
    end
end
```

10. Spoke2与Spoke3的配置参考Spoke1，这里就不再赘述（注意Spoke3只有一条Internet线路，与Hub的两条线路建立IPSec）。

SD-WAN基础配置

Spoke

1. 在Spoke1上删除IPSec向导自动创建的安全策略（否则IPSec接口无法加入SD-WAN区域）。

2. 进入分支FortiGate的网络→SD-WAN→SD-WAN区域页面，新建用于ADVPN访问的区域“Spoke1_ADVPN”。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



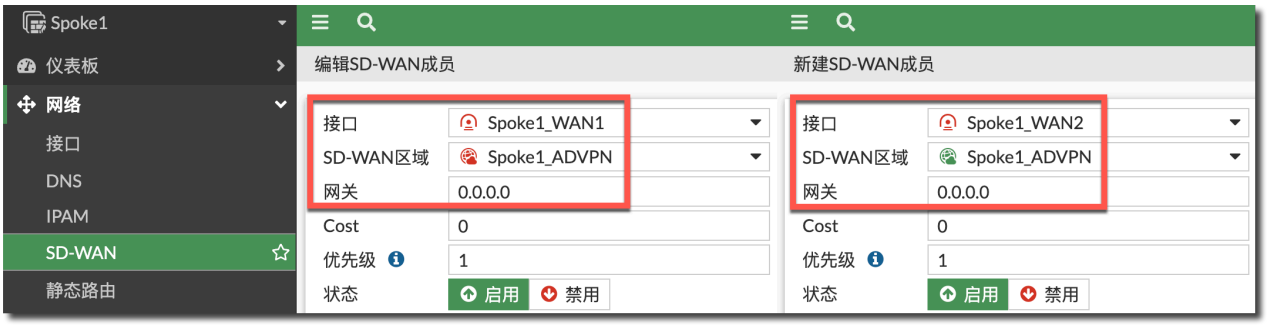

```bash
config system sdwan
    set status enable
    config zone
        edit "Spoke1_ADVPN"
        next
    end
end
```

3. 新建用于访问Hub内网和其他Spoke的SD-WAN成员（两个IPSec Tunnel接口）加入步骤2创建的SD-WAN区域“Spoke1_ADVPN”。注意IPSec Tunnel接口加入SD-WAN区域时不需要填写网关。

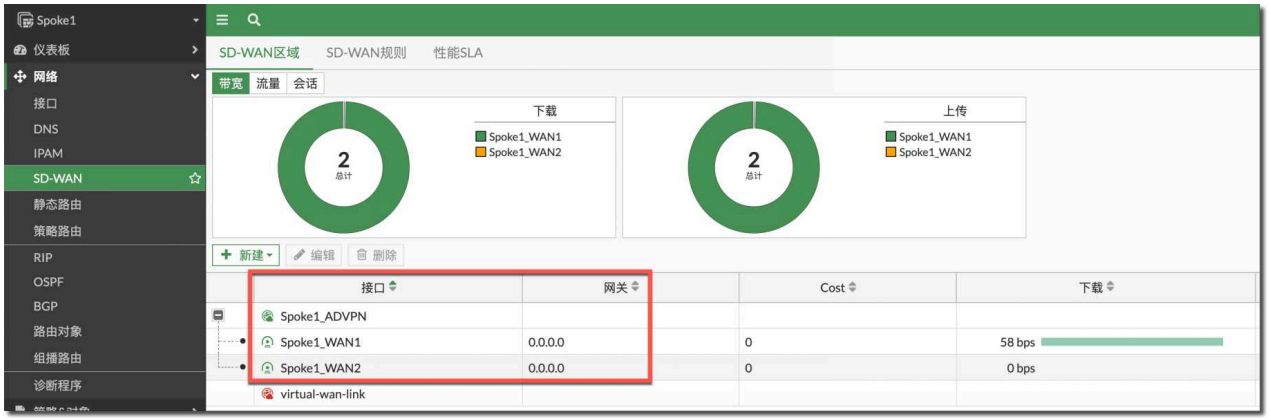
重要

如果IPSec口存在相关配置引用的情况下，是无法直接加入到SD-WAN接口成员的，可参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域章节快速将接口加入SD-WAN区域，并自动修改关联配置（也可选择手动将WAN接口的相关配置删除引用，包括策略、Link-monitor、所属区域等）。



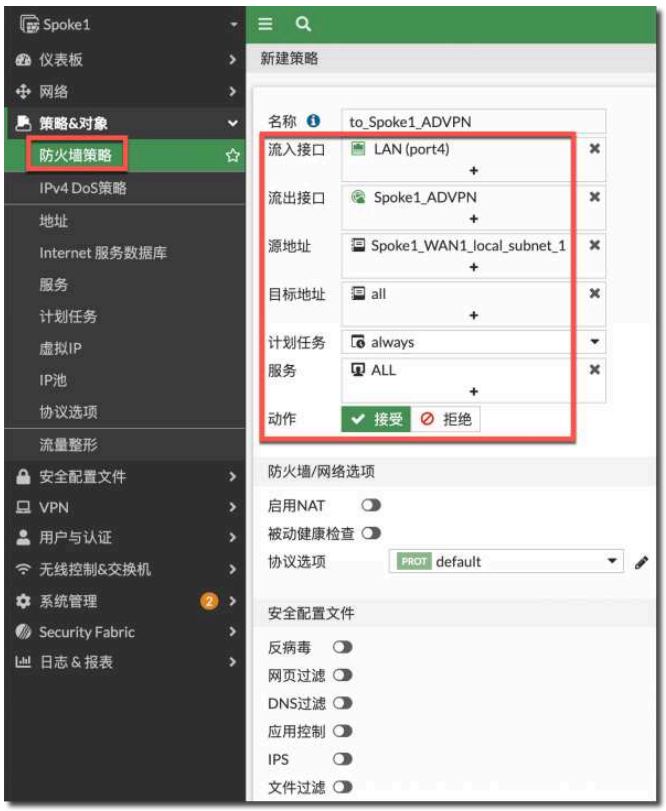


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config members
        edit 1
            set interface "Spoke1_WAN1"
            set zone "Spoke1_ADVPN"
        next
        edit 2
            set interface "Spoke1_WAN2"
            set zone "Spoke1_ADVPN"
        next
    end
end
```

4. 配置防火墙策略1，放通内网port4（LAN）到SD-WAN ADVPN区域的流量，通常情况下内网之间的VPN访问不需要开启SNAT。根据需求开启UTM功能。

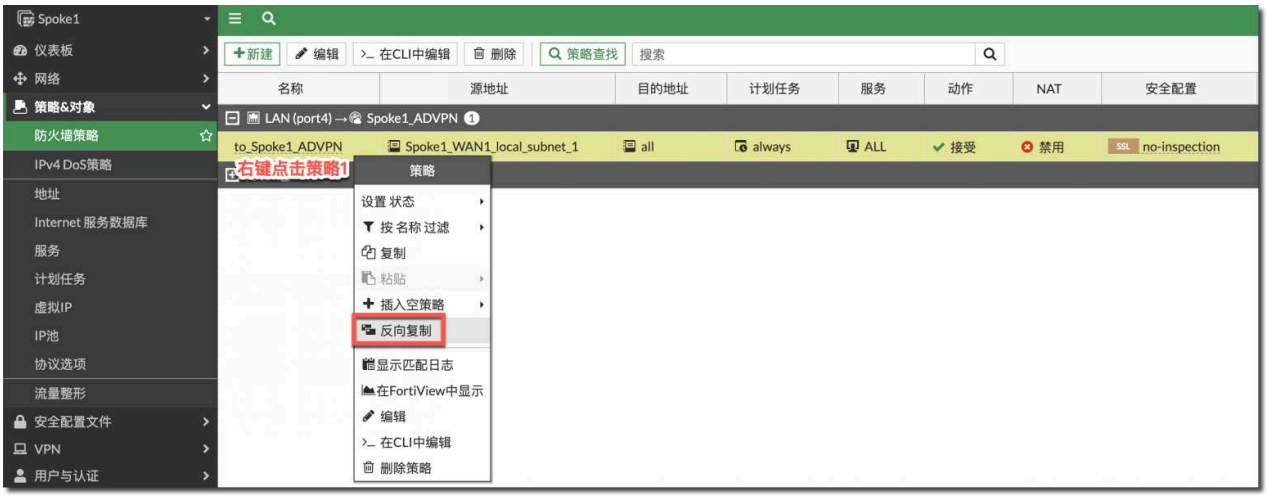


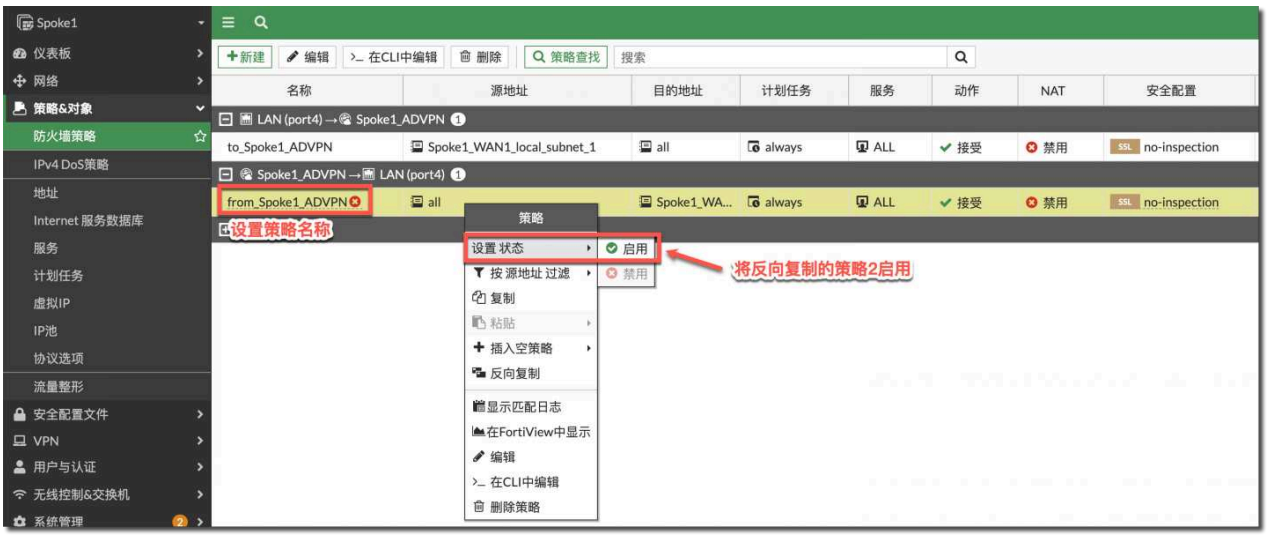

```bash
config firewall policy
    edit 1
        set name "to_Spoke1_ADVPN"
        set srcintf "port4"
        set dstintf "Spoke1_ADVPN"
        set action accept
        set srcaddr "Spoke1_WAN1_local_subnet_1"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

5. 右键点击防火墙策略1，选择反向复制，生成策略2。放通SD-WAN ADVPN区域到内网port4（LAN）的流量，通常情况下内网之间的VPN访问不需要开启SNAT。根据需求开启UTM功能。反向复制的策略名称为空，且为禁用状态，需要手动设置策略名称，然后手动启用该策略。






```bash
config firewall policy
    edit 2
        set name "from_Spoke1_ADVPN"
        set srcintf "Spoke1_ADVPN"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "Spoke1_WAN1_local_subnet_1"
        set schedule "always"
        set service "ALL"
        set comments " (Copy of to_Spoke1_ADVPN) (Reverse of to_Spoke1_ADVPN)"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. Spoke2和Spoke3的配置参考Spoke1，这里就不再赘述。

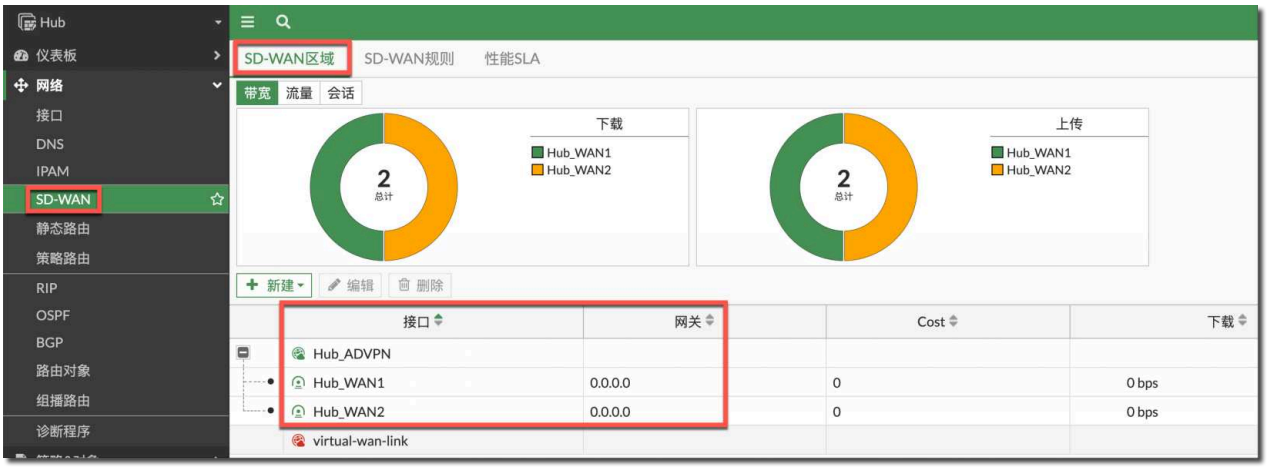
Hub

> **重要**
>
> Hub可以不配置SD-WAN。如果不配置SD-WAN选路，可以通过静态路由不同的优先级进行选路。这里我们以Hub端配置SD-WAN为例。

1. 删除IPSec向导生成的所有安全策略（否则IPSec接口无法加入SD-WAN区域）。

2. 在Hub上新建SD-WAN区域“Hub_ADVPN”与SD-WAN成员（包含WAN1和WAN2上的IPSec拨号连接），将两个IPSec接口加入SD-WAN区域。

> **重要**
>
> 如果IPSec口存在相关配置引用的情况下，是无法直接加入到SD-WAN接口成员的，可参考网络管理→SD-WAN→SD-WAN配置举例→将已关联接口移至SD-WAN区域↗章节快速将接口加入SD-WAN区域，并自动修改关联配置（也可选择手动将WAN接口的相关配置删除引用，包括策略、Link-monitor、所属区域等）。




```bash
config system sdwan
    set status enable
    config zone
        edit "Hub_ADVPN"
        next
    end
    config members
        edit 1
            set interface "Hub_WAN1"
            set zone "Hub_ADVPN"
        next
        edit 2
            set interface "Hub_WAN2"
            set zone "Hub_ADVPN"
        next
    end
end
```

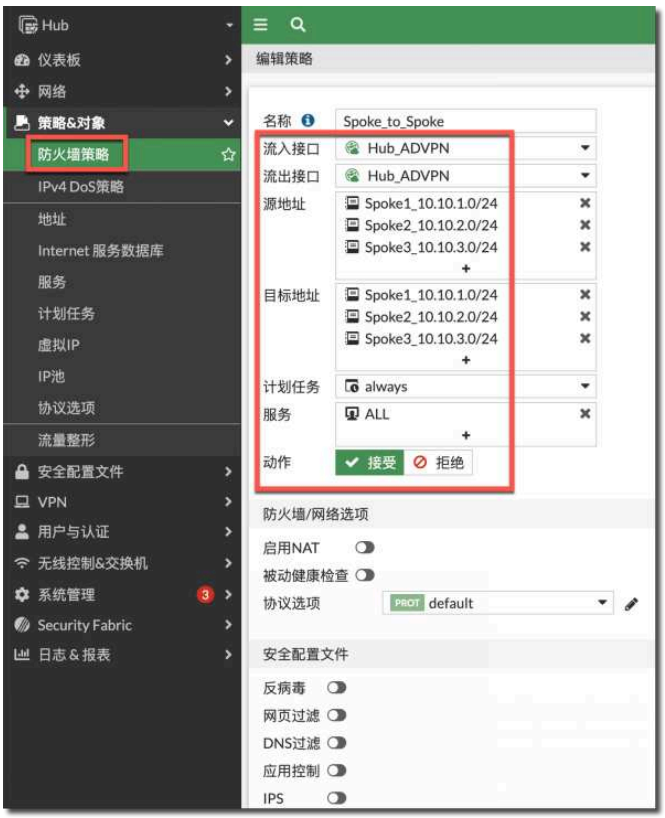
3. 配置防火墙策略1和防火墙策略2，放通内网port4（LAN）与所有Spoke内网之间互相访问的流量，通常情况下内网之间的VPN访问不需要开启SNAT。根据需求开启UTM功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



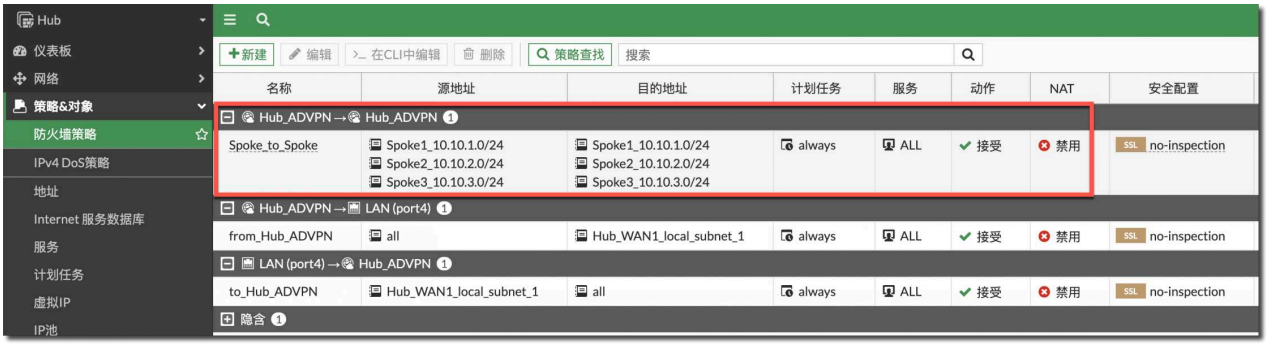

```bash
config firewall policy
    edit 1
        set name "to_Hub_ADVPN"
        set srcintf "port4"
        set dstintf "Hub_ADVPN"
        set action accept
        set srcaddr "Hub_WAN1_local_subnet_1"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "from_Hub_ADVPN"
        set srcintf "Hub_ADVPN"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "Hub_WAN1_local_subnet_1"
        set schedule "always"
        set service "ALL"
        set comments " (Copy of to_Hub_ADVPN) (Reverse of to_Hub_ADVPN)"
    next
end
```

4. 配置防火墙策略3，放通通过Hub中转的Spoke之间的流量。通常情况下VPN之间的VPN访问不需要开启SNAT。根据需求开启UTM功能。



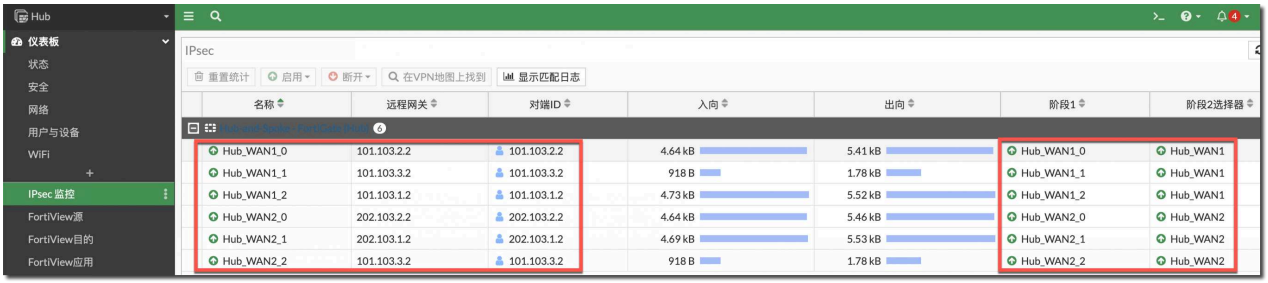
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall policy
    edit 3
        set name "Spoke_to_Spoke"
        set srcintf "Hub_ADVPN"
        set dstintf "Hub_ADVPN"
        set action accept
        set srcaddr "Spoke1_10.10.1.0/24" "Spoke2_10.10.2.0/24" "Spoke3_10.10.3.0/24"
        set dstaddr "Spoke1_10.10.1.0/24" "Spoke2_10.10.2.0/24" "Spoke3_10.10.3.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```



状态检查

1. 查看Hub端IPSec隧道的建立状态，所有Spoke的线路与Hub的两条线路的IPSec建立成功（3个Spoke共6条隧道）。




```bash
Hub # get vpn ipsec tunnel summary
'Hub_WAN1_0' 101.103.2.2:0  selectors(total,up): 1/1  rx(pkt,err): 84/0  tx(pkt,err): 83/0
'Hub_WAN1_1' 101.103.3.2:0  selectors(total,up): 1/1  rx(pkt,err): 20/0  tx(pkt,err): 27/0
'Hub_WAN1_2' 101.103.1.2:0  selectors(total,up): 1/1  rx(pkt,err): 84/0  tx(pkt,err): 83/0
'Hub_WAN2_0' 202.103.2.2:0  selectors(total,up): 1/1  rx(pkt,err): 84/0  tx(pkt,err): 83/1
'Hub_WAN2_1' 202.103.1.2:0  selectors(total,up): 1/1  rx(pkt,err): 84/0  tx(pkt,err): 83/1
'Hub_WAN2_2' 101.103.3.2:0  selectors(total,up): 1/1  rx(pkt,err): 20/0  tx(pkt,err): 27/0
```

2. 查看Hub端FortiGate路由表中的BGP路由，Hub去往每个Spoke的路由在两条线路的IPSec隧道上负载。

```bash
Hub # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 100.1.1.1 (recursive is directly connected, Hub_WAN1), 00:28:29, [1/0]
                     [200/0] via 200.1.1.1 (recursive is directly connected, Hub_WAN2), 00:28:29, [1/0]
B       10.10.2.0/24 [200/0] via 100.1.1.2 (recursive is directly connected, Hub_WAN1), 00:28:32, [1/0]
                     [200/0] via 200.1.1.2 (recursive is directly connected, Hub_WAN2), 00:28:32, [1/0]
B       10.10.3.0/24 [200/0] via 100.1.1.3 (recursive is directly connected, Hub_WAN1), 00:05:24, [1/0]
                     [200/0] via 200.1.1.3 (recursive is directly connected, Hub_WAN2), 00:05:24, [1/0]
```

3. 查看Spoke1 FortiGate路由表中的BGP路由：

- 去往Hub内网的路由在两个线路的IPSec隧道上负载；
- 去往其他Spoke内网的路由通过Hub端的BGP路由反射器反射后学习，通过两个IPSec隧道负载，出接口为去往Hub的IPSec隧道接口（由于Hub和Spoke开启了BGP additional-path send/receive，且Hub端BGP在两个IPSec隧道上都开启了路由反射，Spoke1每条隧道学习另一个Spoke内网的路由会有2条相同的路由）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Spoke1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 100.1.1.2 [2] (recursive via Spoke1_WAN1 tunnel 101.103.254.2), 00:29:51, [1/0]
                     [200/0] via 200.1.1.2 [2] (recursive via Spoke1_WAN2 tunnel 202.103.254.2), 00:29:51, [1/0]
B       10.10.3.0/24 [200/0] via 100.1.1.3 [2] (recursive via Spoke1_WAN1 tunnel 101.103.254.2), 00:06:55, [1/0]
                     [200/0] via 200.1.1.3 [2] (recursive via Spoke1_WAN2 tunnel 202.103.254.2), 00:06:55, [1/0]
B       10.10.254.0/24 [200/0] via 100.1.1.254 (recursive via Spoke1_WAN1 tunnel 101.103.254.2), 00:30:21, [1/0]
                       [200/0] via 200.1.1.254 (recursive via Spoke1_WAN2 tunnel 202.103.254.2), 00:30:21, [1/0]
```

bash

4. Spoke2、Spoke3的路由表与Spoke1类似，这里不再赘述。

SD-WAN策略配置

Spoke

需求1：Spoke去往Hub内网的流量优先从WAN1（port2）的IPSec隧道转发，WAN1的IPSec隧道中断或不满足SLA标准后，从WAN2（port3）的IPSec隧道转发。

1. 在Spoke1的SD-WAN中配置探测Hub端内网服务器的健康检查：

- 成员选择WAN1的IPSec Tunnel接口和WAN2的IPSec Tunnel接口。
- 探测模式为Ping。
- 开启SLA目标：延迟<250ms/抖动<50ms/丢包率<5%。

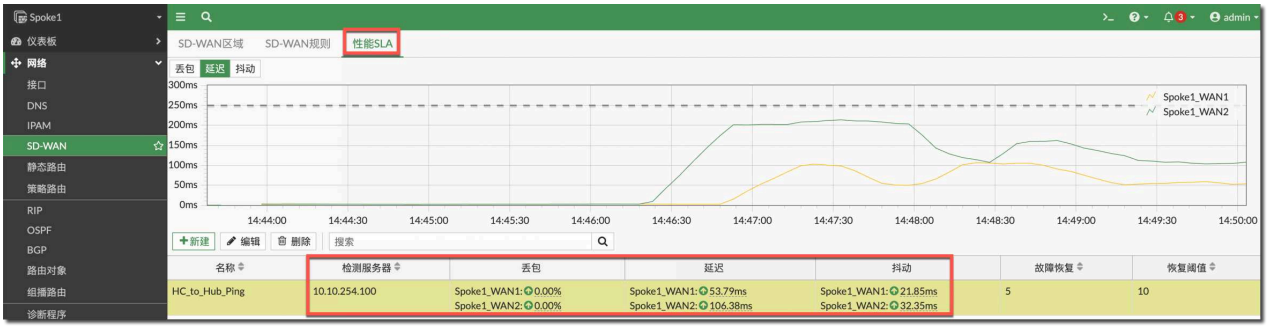



```
config system sdwan
    config health-check
        edit "HC_to_Hub_Ping"
            set server "10.10.254.100"
            set interval 1000
            set recoverytime 10
            set members 0
            config sla
                edit 1
                    set latency-threshold 250
                    set jitter-threshold 50
                    set packetloss-threshold 5
                next
            end
        next
    end
end
```

bash

2. 查看健康检查的状态，可以看到目前2条去往Hub内网的线路都满足SLA标准。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

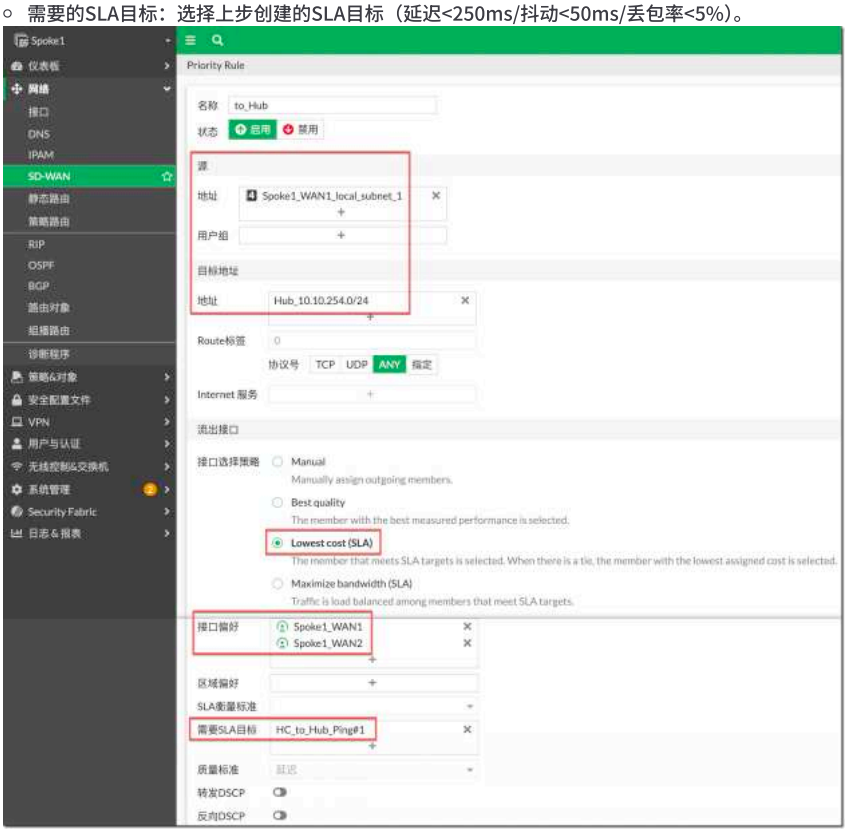



```bash
Spoke1 # diagnose sys sdwan health-check status HC_to_Hub_Ping
Health Check(HC_to_Hub_Ping):
Seq(1 Spoke1_WAN1): state(alive), packet-loss(0.000%) latency(48.060), jitter(20.974), mos(4.356), bandwidth-up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x1
Seq(2 Spoke1_WAN2): state(alive), packet-loss(0.000%) latency(106.973), jitter(30.848), mos(4.268), bandwidth-up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x1
```

3. 新建SD-WAN规则1，用于Spoke内网去往Hub内网的流量：



- 源地址选择Spoke1内网网段；目标地址为Hub内网网段。
- 接口选择策略：选择Lowest Cost (SLA)，Spoke内部访问Hub内网的流量优先从满足SLA标准（延迟<250ms/抖动<50ms/丢包率<5%）的线路转发。如果2条线路都满足SLA标准，则优先从接口偏好中靠前的接口转发。
- 接口偏好：选择WAN1线路IPSec接口与WAN2线路IPSec接口。WAN1线路IPSec接口排序在前，其次是WAN2线路IPSec接口。
- 需要的SLA目标：选择上步创建的SLA目标（延迟<250ms/抖动<50ms/丢包率<5%）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system sdwan
    config service
        edit 1
            set name "to_Hub"
            set mode sla
            set dst "Hub_10.10.254.0/24"
            set src "Spoke1_WAN1_local_subnet_1"
            config sla
                edit "HC_to_Hub_Ping"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

4. 查看上步创建的SD-WAN规则目前的选路状态，由于目前2条去往Hub内网的线路均满足SLA目标，所以选择接口偏好配置中靠前的WAN1上的IPSec线路。




```bash
Spoke1 #  diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 Spoke1_WAN1), alive, sla(0×1), gid(0), cfg_order(0), local cost(0), selected    //优先从WAN1上的
IPSec隧道转发//
    2: Seq_num(2 Spoke1_WAN2), alive, sla(0×1), gid(0), cfg_order(1), local cost(0), selected
  Src address(1):
        10.10.1.0-10.10.1.255

  Dst address(1):
        10.10.254.0-10.10.254.255
```

5. 查看SD-WAN规则对应的策略路由状态，出接口优先选择MPLS线路接口（port4）。

```bash
Spoke1 # diagnose firewall proute list
list route policy info(vf=root):

id=2130837505(0×7f020001) vwl_service=1(to_Hub) vwl_mbr_seq=1 2 dscp_tag=0×fc 0×fc flags=0×0 tos=0×00
tos_mask=0×00 protocol=0 sport=0-65535 iif=0(any) dport=1-65535 path(2) oif=17(Spoke1_WAN1) oif=18(Spoke1_WAN2)
//优先从WAN1上的IPSec隧道转发//
source(1): 10.10.1.0-10.10.1.255
destination(1): 10.10.254.0-10.10.254.255
hit_count=0 last_used=2023-12-26 15:03:45
```

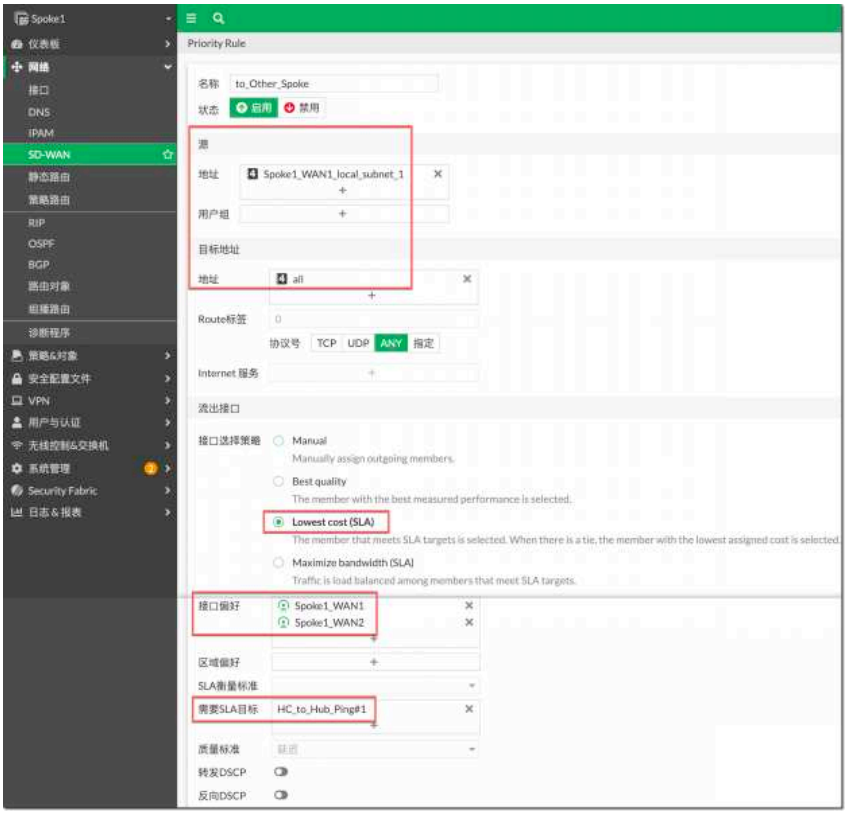
6. Spoke2与Spoke3的配置请参考Spoke1，这里不再赘述。

需求2：Spoke内网访问其他Spoke内网的流量优先从Shortcut隧道转发。Shortcut隧道无法建立时，通过Hub中转。

1. 新建SD-WAN规则2：

- 源地址选择Spoke1内网网段；目标地址为all（或其他Spoke内网的网段集合）。
- 接口选择策略：选择Lowest Cost (SLA)，Spoke内部访问Internet的流量优先从满足SLA标准（延迟<250ms/抖动<50ms/丢包率<5%）的IPSec线路创建的Shortcut隧道转发（如果Shortcut无法建立，则通过去往Hub的IPSec隧道转发）。如果两条IPSec线路都满足SLA标准，则优先从接口偏好中靠前的IPSec隧道创建的Shortcut转发（如果Shortcut无法建立，则通过去往Hub的IPSec隧道转发）。
- 接口偏好：选择WAN1线路IPSec接口与WAN2线路IPSec接口。WAN1线路IPSec接口排序在前，其次是WAN2线路IPSec接口。
- 需要SLA目标：选择上步创建的SLA目标（延迟<250ms/抖动<50ms/丢包率<5%）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system sdwan
    config service
        edit 2
            set name "to_Other_Spoke"
            set mode sla
            set dst "all"
            set src "Spoke1_WAN1_local_subnet_1"
            config sla
                edit "HC_to_Hub_Ping"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
```

2. 查看上步创建的SD-WAN规则目前的选路状态，由于目前两条IPSec线路均满足SLA目标，所以选择接口偏好配置中靠前的Spoke1_WAN1隧道。




```bash
Spoke1 # diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 Spoke1_WAN1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected    //优先从WAN1上的
IPSec隧道转发//
    2: Seq_num(2 Spoke1_WAN2), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    Src address(1):
          10.10.1.0-10.10.1.255

    Dst address(1):
          0.0.0.0-255.255.255.255
```

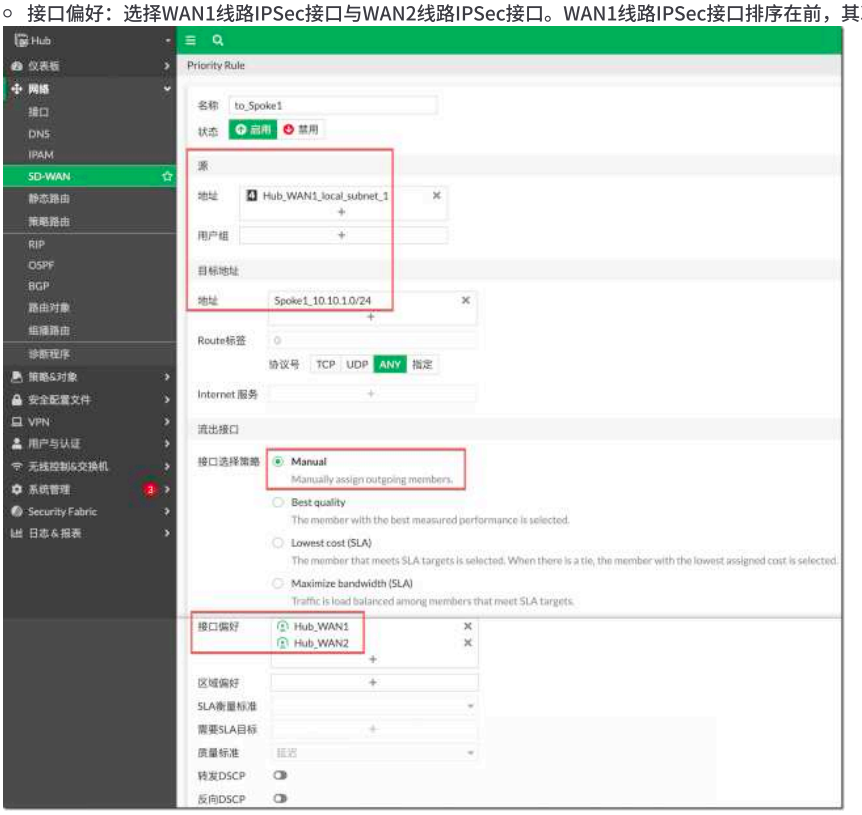
3. Spoke2与Spoke3的配置请参考Spoke1，这里不再赘述。

Hub

需求3：Hub内网主动访问Spoke内网的流量强制从WAN1的IPSec线路转发，当WAN1的IPSec线路中断时，从WAN2的IPSec线路转发。

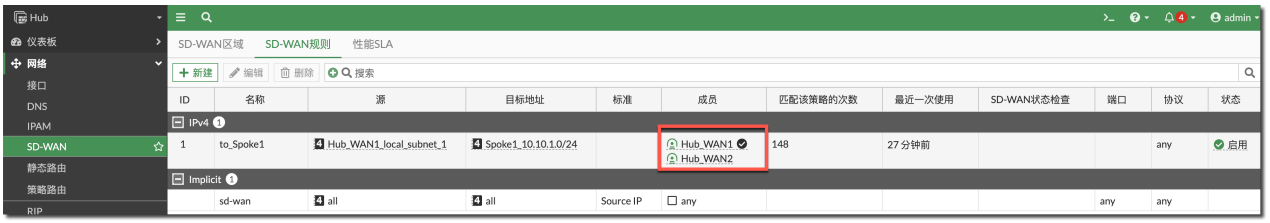
1. 新建SD-WAN规则1（可根据需求使用其他模式）：

- 源地址选择Hub内网网段；目标地址为Spoke1内网网段。
- 接口选择策略：选择Manual，Hub内网访问Spoke1的流量优先从WAN1的IPSec线路转发，当WAN1的IPSec线路中断时，从WAN2的IPSec线路转发。
- 接口偏好：选择WAN1线路IPSec接口与WAN2线路IPSec接口。WAN1线路IPSec接口排序在前，其次是WAN2线路IPSec接口。




```bash
config system sdwan
    config service
        edit 1
            set name "to_Spoke1"
            set dst "Spoke1_10.10.1.0/24"
            set src "Hub_WAN1_local_subnet_1"
            set priority-members 1 2
        next
    end
end
```

2. 查看上步创建的SD-WAN规则目前的选路状态，选择接口偏好配置中靠前的Spoke1_WAN1隧道。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Hub # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 Hub_WAN1), alive, selected    //Hub访问Spoke1的流量优先从WAN1的IPSec隧道转发//
    2: Seq_num(2 Hub_WAN2), alive, selected
  Src address(1):
        10.10.254.0-10.10.254.255

  Dst address(1):
        10.10.1.0-10.10.1.255
```

bash

3. 去往Spoke2和Spoke3的SD-WAN规则可参考步骤1，这里不再赘述。

需求4：当Spoke内网之间的Shortcut隧道无法建立，或Shortcut还未建立Spoke内网之间第一次进行访问时，流量要通过Hub进行中转。Hub中转这类流量时，需要保证流入IPSec隧道和流出IPSec隧道为同一个隧道。

1. 通过CLI新建SD-WAN规则2：

- 源地址（src）选择和目标地址（dst）都选择所有Spoke的内网网段地址。
- 接口选择策略（mode）：使用Manual。
- 接口偏好（priority-members）：选择WAN1的IPSec隧道和WAN2的IPSec隧道。
- tie-break：选择input-device方式，根据入接口来决定SD-WAN策略转发时使用相同的接口作为出接口，接口偏好中配置的接口顺序不会生效（该选项需要7.2.1及以上版本支持，如低于7.2.1版本，请使用策略路由实现此需求）。

```
config system sdwan
    config service
        edit 2
            set name "Spoke_to_Spoke"
            set mode manual
            set dst "Spoke1_10.10.1.0/24" "Spoke2_10.10.2.0/24" "Spoke3_10.10.3.0/24"
            set src "Spoke1_10.10.1.0/24" "Spoke2_10.10.2.0/24" "Spoke3_10.10.3.0/24"
            set priority-members 1 2
            set tie-break input-device    //重要配置//
        next
    end
end
```

bash

2. 查看上步创建的SD-WAN规则目前的状态，Tie break模式为input-device，下方的Member顺序不会生效。

```
Hub # diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: input-device    //tie-break模式为input-device时，下方的Member顺序不会生效//
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 Hub_WAN1), alive, selected
    2: Seq_num(2 Hub_WAN2), alive, selected
  Src address(3):
        10.10.3.0-10.10.3.255
        10.10.2.0-10.10.2.255
        10.10.1.0-10.10.1.255

  Dst address(3):
        10.10.3.0-10.10.3.255
        10.10.2.0-10.10.2.255
        10.10.1.0-10.10.1.255
```

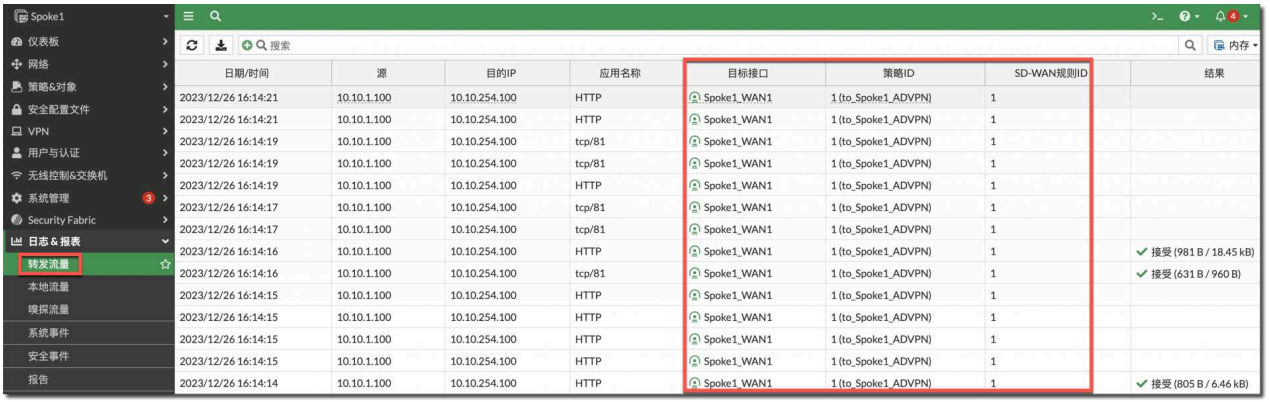
bash

结果验证

Spoke访问Hub

1. 使用Spoke1内网PC客户端访问Hub端的内网业务，流量可以正确从WAN1上的IPSec隧道转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 模拟Spoke1 WAN1上IPSec隧道的健康检查的延迟增加到300ms。




```bash
Spoke1 # diagnose sys sdwan health-check status HC_to_Hub_Ping
Health Check(HC_to_Hub_Ping):
Seq(1 Spoke1_WAN1): state(alive), packet-loss(0.000%) latency(303.576), jitter(19.449), mos(3.595), bandwidth-up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x0
Seq(2 Spoke1_WAN2): state(alive), packet-loss(0.000%) latency(103.569), jitter(34.299), mos(4.258), bandwidth-up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x1
```

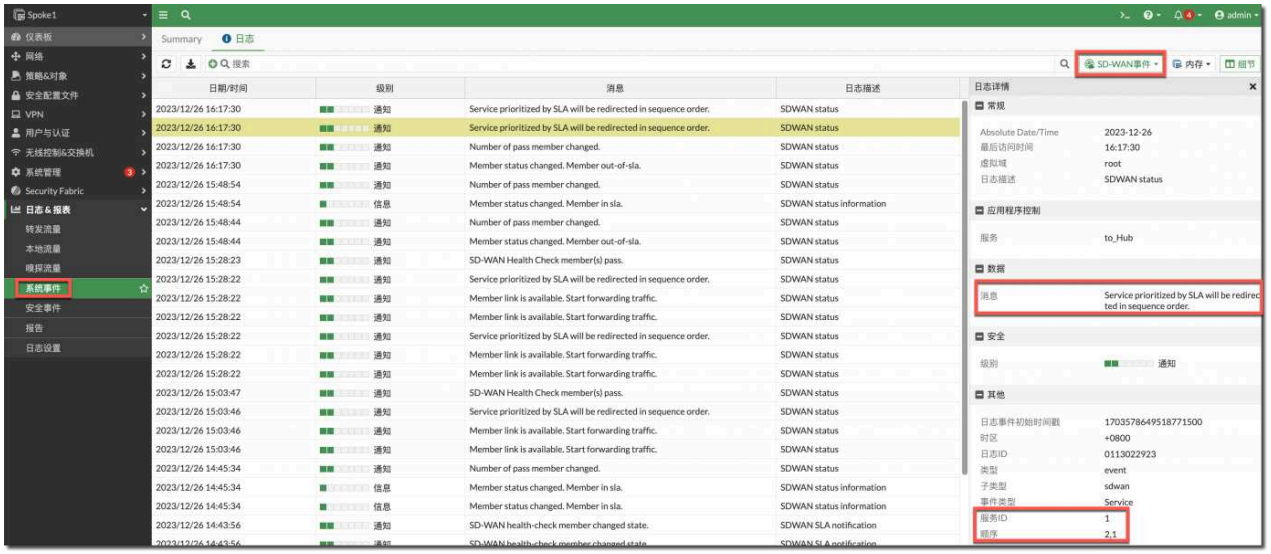
3. 在Spoke1上查看SD-WAN规则1的选路优先选择联通线路IPSec接口去往Hub内网。




```bash
Spoke1 # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(2 Spoke1_WAN2), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected    //去往Hub内网的流量优先从WAN2的IPSec隧道转发//
    2: Seq_num(1 Spoke1_WAN1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.10.1.0-10.10.1.255

  Dst address(1):
        10.10.254.0-10.10.254.255
```

4. 对应的SD-WAN线路切换系统日志。

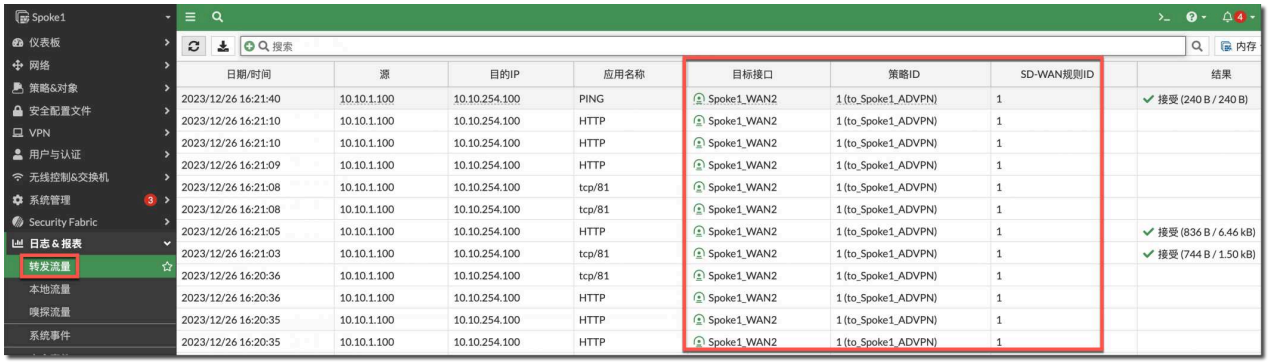
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



```
date=2023-12-26 time=16:17:30 eventtime=1703578649518771555 tz="+0800" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="to_Hub" seq="2,1" msg="Service prioritized by SLA will be redirected in sequence order."
```

bash

5. 再次使用Spoke1内网PC客户端访问Hub端内网的业务，流量开始从WAN2的IPSec接口转发。



6. Spoke2、Spoke3内网访问Hub内网的测试参考Spoke1，这里不再赘述。

Spoke访问Spoke

1. Spoke与Spoke之间互访流量会触发Shortcut隧道的建立（前提是需要Hub开启BGP RR，在Spoke之间反射路由，且Hub开启ADVPN sender，Spoke开启ADVPN receiver），在创建Shortcut隧道之前，第一次Spoke访问其他Spoke的流量会经过Hub进行中转，同时通过Hub进行相关Shortcut信息专递。Shortcut隧道建立后，Spoke与Spoke之间直接通过Shortcut隧道通信。

2. 保留之前线路的延迟状态（Spoke访问Hub时应优先从WAN2的IPSec转发），查看Spoke1的隧道建立状态，只有去往Hub的IPSec隧道，没有去往其他Spoke的Shortcut隧道。

```
Spoke1 # get vpn ipsec tunnel summary
'Spoke1_WAN2' 202.103.254.2:0  selectors(total,up): 1/1  rx(pkt,err): 8423/0  tx(pkt,err): 8408/11
'Spoke1_WAN1' 101.103.254.2:0  selectors(total,up): 1/1  rx(pkt,err): 9284/0  tx(pkt,err): 9193/11
```

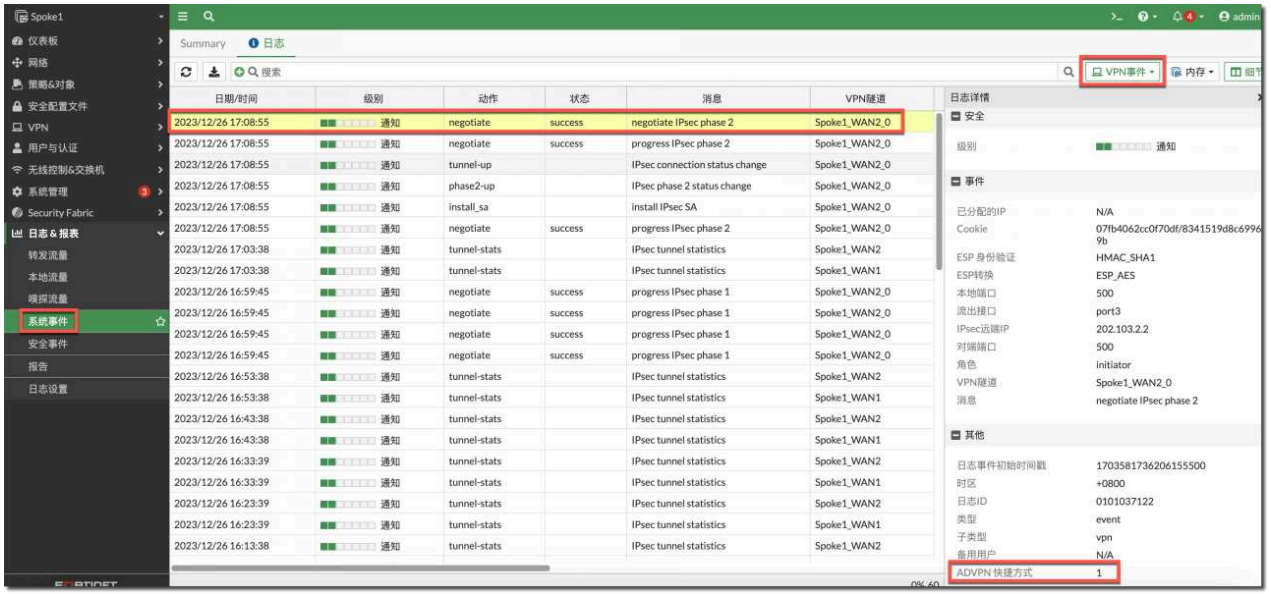
bash

3. 使用Spoke1内网PC访问Spoke2内网PC，触发Shortcut隧道建立，可以看到Shortcut隧道已经建立，名称为“Spoke1_WAN2_0”，通过WAN2上的IPSec隧道建立。

```
Spoke1 # get vpn ipsec tunnel summary
'Spoke1_WAN2' 202.103.254.2:0  selectors(total,up): 1/1  rx(pkt,err): 8825/0  tx(pkt,err): 8810/13
'Spoke1_WAN2_0' 202.103.2.2:0  selectors(total,up): 1/0  rx(pkt,err): 0/0  tx(pkt,err): 0/2
'Spoke1_WAN1' 101.103.254.2:0  selectors(total,up): 1/1  rx(pkt,err): 9686/0  tx(pkt,err): 9595/11
```

bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

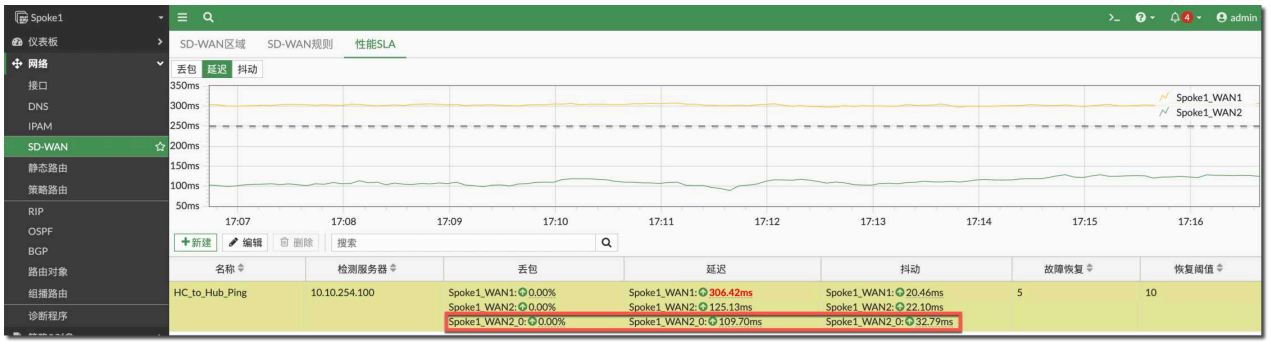



```bash
date=2023-12-26 time=17:08:55 eventtime=1703581736206155498 tz="+0800" logid="0101037122" type="event"
subtype="vpn" level="notice" vd="root" logdesc="Negotiate IPsec phase 2" msg="negotiate IPsec phase 2"
action="negotiate" remip=202.103.2.2 locip=202.103.1.2 remport=500 locport=500 outintf="port3"
cookies="07fb4062cc0f70df/8341519d8c69969b" user="202.103.2.2" group="N/A" useralt="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=N/A vpntunnel="Spoke1_WAN2_0" status="success" role="initiator" esptransform="ESP_AES"
espauth="HMAC_SHA1" advpnsc=1
```

4. 在Hub上抓包查看Spoke1内网访问Spoke2内网第一次访问时的流量转发，可以看到在Spoke1和Spoke2之间的Shortcut建立前，流量是通过Hub中转的，Hub中转时匹配SD-WAN规则2，tie-break的方式input-device生效，流量从Hub_WAN2进入，也从Hub_WAN2发出（不会按照Manual模式的SD-WAN Member顺序从Hub_WAN1发出）。

```bash
Hub # diagnose sniffer packet any 'host 10.10.1.100 and host 10.10.2.100' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.1.100 and host 10.10.2.100]
23.920132 Hub_WAN2 in 10.10.1.100 → 10.10.2.100: icmp: echo request
23.920239 Hub_WAN2 out 10.10.1.100 → 10.10.2.100: icmp: echo request
23.922899 Hub_WAN2 in 10.10.2.100 → 10.10.1.100: icmp: echo reply
23.922913 Hub_WAN2 out 10.10.2.100 → 10.10.1.100: icmp: echo reply
```

5. Shortcut隧道建立后，SD-WAN会基于父隧道（Spoke1_WAN2）关联的SLA配置，自动创建健康检查检测Spoke2的Tunnel接口IP，检测方式固定为Ping（这也就是为什么要在所有Spoke的IPSec Tunnel接口上开启允许Ping访问）。




```bash
Spoke1 # diagnose sys sdwan health-check
Health Check(HC_to_Hub_Ping):
Seq(1 Spoke1_WAN1): state(alive), packet-loss(0.000%) latency(301.470), jitter(20.919), mos(3.591), bandwidth-
up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x0
Seq(2 Spoke1_WAN2): state(alive), packet-loss(0.000%) latency(127.110), jitter(22.480), mos(4.259), bandwidth-
up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x1
Seq(2 Spoke1_WAN2_0): state(alive), packet-loss(0.000%) latency(112.727), jitter(29.479), mos(4.260), bandwidth-
up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x1
```

6. 查看Spoke1上的BGP路由表，去往Spoke2内网路由的出接口已变为在Shortcut隧道接口（Spoke1_WAN2_0）和WAN1上的IPSec隧道接口（Spoke1_WAN1）之间负载。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Spoke1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 100.1.1.2 [2] (recursive via Spoke1_WAN1 tunnel 101.103.254.2), 00:19:40, [1/0]
                     [200/0] via 200.1.1.2 [2] (recursive is directly connected, Spoke1_WAN2_0), 00:19:40, [1/0]
B       10.10.3.0/24 [200/0] via 100.1.1.3 [2] (recursive via Spoke1_WAN1 tunnel 101.103.254.2), 02:33:25, [1/0]
                     [200/0] via 200.1.1.3 [2] (recursive via Spoke1_WAN2 tunnel 202.103.254.2), 02:33:25, [1/0]
B       10.10.254.0/24 [200/0] via 100.1.1.254 (recursive via Spoke1_WAN1 tunnel 101.103.254.2), 02:35:09, [1/0]
                       [200/0] via 200.1.1.254 (recursive via Spoke1_WAN2 tunnel 202.103.254.2), 02:35:09, [1/0]
```

bash

7. 查看Spoke1上SD-WAN规则2的选路状态，现在优先从WAN2上IPSec隧道的Shortcut（Spoke1_WAN2_0）进行转发，而不是从父隧道（Spoke1_WAN2）转发，这说明在SLA类型的SD-WAN规则中，Shortcut隧道优先于其父隧道，除非Shortcut隧道的SLA不满足目标。

```
Spoke1 # diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Member sub interface(3):
    2: seq_num(2), interface(Spoke1_WAN2):
       1: Spoke1_WAN2_0(22)
  Members(3):
    1: Seq_num(2 Spoke1_WAN2_0), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(2 Spoke1_WAN2), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    3: Seq_num(1 Spoke1_WAN1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.10.1.0-10.10.1.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

bash

8. 再次使用Spoke1内网PC访问Spoke2内网PC，在Spoke1上抓包可以看到流量通过WAN2上的Shortcut隧道（Spoke1_WAN2_0）隧道转发。

```
Spoke1 # diagnose sniffer packet any 'host 10.10.2.100' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.100]
7.778827 port4 in 10.10.1.100 -> 10.10.2.100: icmp: echo request
7.778945 Spoke1_WAN2_0 out 10.10.1.100 -> 10.10.2.100: icmp: echo request
7.870455 Spoke1_WAN2_0 in 10.10.2.100 -> 10.10.1.100: icmp: echo reply
7.870486 port4 out 10.10.2.100 -> 10.10.1.100: icmp: echo reply
8.798494 port4 in 10.10.1.100 -> 10.10.2.100: icmp: echo request
8.798518 Spoke1_WAN2_0 out 10.10.1.100 -> 10.10.2.100: icmp: echo request
8.870069 Spoke1_WAN2_0 in 10.10.2.100 -> 10.10.1.100: icmp: echo reply
8.870081 port4 out 10.10.2.100 -> 10.10.1.100: icmp: echo reply
```

bash

9. 调整Spoke1与Spoke2之间Shortcut隧道（Spoke1_WAN2_0）的延迟到400ms，但父隧道（Spoke1_WAN2）延迟不变。




```
Spoke1 # diagnose sys sdwan health-check
Health Check(HC_to_Hub_Ping):
Seq(1 Spoke1_WAN1): state(alive), packet-loss(1.000%) latency(314.047), jitter(16.431), mos(3.573), bandwidth-
up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x0
Seq(2 Spoke1_WAN2): state(alive), packet-loss(0.000%) latency(112.318), jitter(24.059), mos(4.291), bandwidth-
up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x1
Seq(2 Spoke1_WAN2_0): state(alive), packet-loss(2.410%) latency(393.256), jitter(26.858), mos(3.071), bandwidth-
up(65535000), bandwidth-dw(65535000), bandwidth-bi(131070000) sla_map=0x0
```

bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

10. 查看Spoke1上SD-WAN规则2的选路状态，现在优先从WAN2上IPSec父隧道（Spoke1_WAN2）进行转发，而不是从Shortcut隧道（Spoke1_WAN2_0）转发，事实的确如此吗？

```bash
Spoke1 # diagnose sys sdwan service 2

Service(2): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(15), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Member sub interface(3):
    1: seq_num(2), interface(Spoke1_WAN2):
       1: Spoke1_WAN2_0(25)
  Members(3):
    1: Seq_num(2 Spoke1_WAN2), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(1 Spoke1_WAN1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
    3: Seq_num(2 Spoke1_WAN2_0), alive, sla(0x0), gid(0), cfg_order(1), local cost(0), selected
  Src address(1):
        10.10.1.0-10.10.1.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

11. 再次使用Spoke1内网PC访问Spoke2内网PC，在Spoke1上抓包可以看到流量通过WAN1上IPSec隧道（Spoke1_WAN1）隧道转发，而不是Spoke1_WAN2隧道，并没有按照SD-WAN规则状态中的选路从Spoke1_WAN2隧道转发。

```bash
Spoke1 # diagnose sniffer packet any 'host 10.10.2.100' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.100]
4.313351 port4 in 10.10.1.100 -> 10.10.2.100: icmp: echo request
4.313453 Spoke1_WAN1 out 10.10.1.100 -> 10.10.2.100: icmp: echo request
4.639634 Spoke1_WAN1 in 10.10.2.100 -> 10.10.1.100: icmp: echo reply
4.639664 port4 out 10.10.2.100 -> 10.10.1.100: icmp: echo reply
```

12. 这是由于SD-WAN规则选路时也会根据流量的目的地址查询路由表，如果最佳路由下一跳接口是SD-WAN成员，则通过该SD-WAN规则的SLA找到最佳的接口转发，该接口必须要有路由。在Spoke1的路由表中，通过Spoke1_WAN2隧道去往Spoke2内网的路由出接口已变为Shortcut隧道Spoke1_WAN2_0，而不是Spoke1_WAN2，所以跳过成员Spoke1_WAN2，从下一个成员Spoke1_WAN1转发（参考网络管理→SD-WAN→SD-WAN介绍→SD-WAN数据转发逻辑↗章节中的SD-WAN工作流程注意事项）。

13. 随后Spoke1触发了Spoke1_WAN1隧道上的去往Spoke2的Shortcut隧道连接Spoke1_WAN1_0，后续流量通过Shortcut隧道连接Spoke1_WAN1_0转发。

```bash
Spoke1 # diagnose sniffer packet any 'host 10.10.2.100' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.100]
36.862757 port4 in 10.10.1.100 -> 10.10.2.100: icmp: echo request
36.862888 Spoke1_WAN1_0 out 10.10.1.100 -> 10.10.2.100: icmp: echo request
37.167399 Spoke1_WAN1_0 in 10.10.2.100 -> 10.10.1.100: icmp: echo reply
37.167437 port4 out 10.10.2.100 -> 10.10.1.100: icmp: echo reply
```

14. Spoke2、Spoke3之间的Shortcut隧道测试与Spoke1一致，这里不再赘述。

Hub访问Spoke

1. 保留之前线路的延迟状态（Spoke1主动访问Hub时应优先从WAN2的IPSec转发）。

2. 使用Hub内网PC访问Spoke1的内网PC，由于Hub的SD-WAN规则配置为Manual模式，流量强制从Hub_WAN1转发（除非Hub_WAN1隧道中断）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在Spoke1上查看返回的流量走向，只要路由表中存在返回的路由，就会遵循源进源出原则，而不是匹配SD-WAN规则。

```bash
Spoke1 # diagnose sys sdwan service 1

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(12), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(4):
    1: Seq_num(2 Spoke1_WAN2), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
    2: Seq_num(1 Spoke1_WAN1), alive, sla(0x0), gid(0), cfg_order(0), local cost(0), selected
  Src address(1):
        10.10.1.0-10.10.1.255

  Dst address(1):
        10.10.254.0-10.10.254.255

Spoke1 # diagnose sniffer packet any 'host 10.10.254.100 and host 10.10.1.100' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.254.100 and host 10.10.1.100]
1.105333 Spoke1_WAN1 in 10.10.254.100 -> 10.10.1.100: icmp: echo request
1.105377 port4 out 10.10.254.100 -> 10.10.1.100: icmp: echo request
1.105956 port4 in 10.10.1.100 -> 10.10.254.100: icmp: echo reply
1.105979 Spoke1_WAN1 out 10.10.1.100 -> 10.10.254.100: icmp: echo reply
```

注意事项

默认配置下，当VPN或专线线路（无SNAT）SD-WAN选路出现变化后，已有的会话会立即切换到新链路上，如果想在SD-WAN线路切换后让已有会话保持在原来的线路上，只有新会话创建在新线路上，需要在对应VPN接口或专线接口上使用如下命令。

```bash
config system interface
    edit "Spoke1_WAN1"
        set preserve-session-route enable    //默认为disable//
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

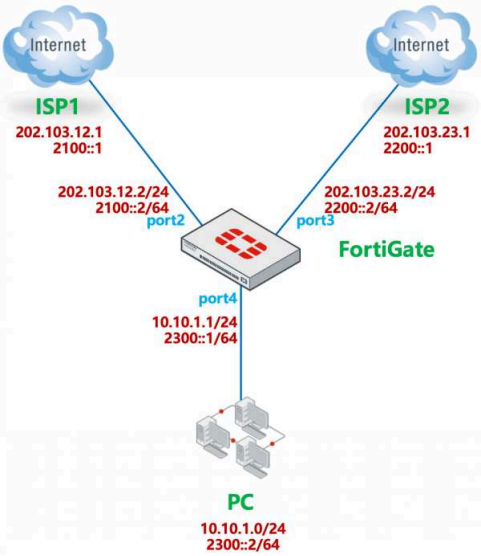
健康检查配置实践

概述

在SD-WAN的健康检查中，探测目标可以配置1个Server或2个Server，本文主要探讨：

- 健康检查探测目标个数/检测状态（up/down）对健康检查状态（alive/dead）的影响。
- 目标服务器数量对Manual模式的SD-WAN规则选路产生的影响。
- 健康检查选项中的“更新静态路由”（`update-static-route`）对SD-WAN选路的作用，以及与探测目标服务器数量相关的差异化表现。
- 针对不同应用场景，提供相应的配置建议。

网络拓扑



- FortiGate有两条ISP线路（IPv4/IPv6双栈）连接Internet，两条ISP线路做双栈SD-WAN。
- FortiGate配置健康检查，检查Internet上目标服务器（IPv4/IPv6）的状态，以健康检查的结果决定SD-WAN选路。
- PC通过FortiGate的SD-WAN选路来访问Internet。
- 基础网络配置略，SD-WAN基础配置与初始路由表，路由表中默认路由在两个ISP接口上负载：

```bash
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "port2"
            set gateway 202.103.12.1
            set gateway6 2100::1
        next
        edit 2
            set interface "port3"
            set gateway 202.103.23.1
            set gateway6 2200::1
        next
    end
end
config router static
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config router static6
    edit 1
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end

FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.12.1, port2, [1/0]
                  [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
FortiGate # get router info6 routing-table
Routing table for VRF=0
S*      ::/0 [1/0] via 2100::1, port2, 17:24:49, [1024/0]
             [1/0] via 2200::1, port3, 17:24:49, [1024/0]
C       ::1/128 via ::, root, 3d18h28m
C       2100::/64 via ::, port2, 17:25:23
C       2200::/64 via ::, port3, 17:25:13
C       2300::/64 via ::, port4, 00:00:04
```

1个健康检查配置2个Server

基础配置

1. 在FortiGate上创建健康检查，配置2个IPv4探测Server，检测223.5.5.5（在前）和223.6.6.6（在后），参与接口选择所有SD-WAN成员（port2和port3），默认开启 `update-static-route` 。

```bash
config health-check
    edit "Server"
        set server "223.5.5.5" "223.6.6.6"
        set members 0
    next
end
```

2. 查看健康检查的状态，两条线路均为alive状态。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(15.662), jitter(11.245), mos(4.385), bandwidth-
up(9999997), bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(15.519), jitter(11.240), mos(4.385), bandwidth-
up(9999998), bandwidth-dw(9999998), bandwidth-bi(19999996) sla_map=0x0
```

3. 配置Manual模式的SD-WAN规则，将PC网段的流量优先通过ISP1（port2）线路进行转发，其次通过ISP2（port3）线路进行转发。

```bash
config system sdwan
    config service
        edit 1
            set name "to_Internet"
            set dst "all"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set src "all"
            set priority-members 1 2
        next
    end
end
```

4. 查看SD-WAN规则选路状态，优先选择ISP1（port2）线路转发。




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(1), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port2), alive, selected
    2: Seq_num(2 port3), alive, selected
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

5. 抓取探测报文可以看到，ISP1（port2）和ISP2（port3）接口会同时探测223.5.5.5和223.6.6.6两个Server。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.386576 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.386658 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
0.386675 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.386698 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.392926 port3 in 223.5.5.5 → 202.103.23.2: icmp: echo reply
0.393021 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
0.393048 port2 in 223.5.5.5 → 202.103.12.2: icmp: echo reply
0.393075 port2 in 223.6.6.6 → 202.103.12.2: icmp: echo reply
```

重要

后续本文使用如下简写来表示每个线路上对两个Server的探测结果：

- `ISP1#1`：ISP1上对223.5.5.5的探测结果。
- `ISP1#2`：ISP1上对223.6.6.6的探测结果。
- `ISP2#1`：ISP2上对223.5.5.5的探测结果。
- `ISP2#2`：ISP2上对223.6.6.6的探测结果。

`ISP1#1` down，其他up

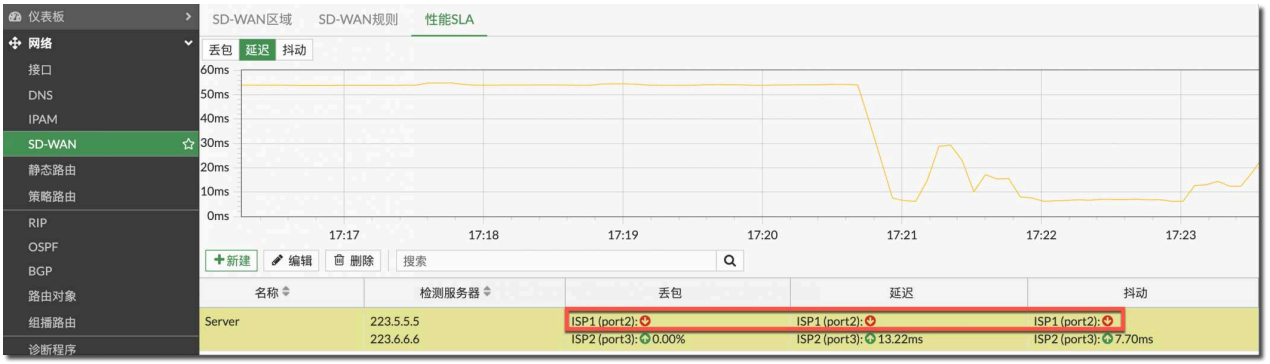
1. 在ISP1上模拟探测的目标服务器223.5.5.5（位于健康检查的Server序列1）失效，其他正常访问。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.316221 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.316311 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
0.316327 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.316354 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.322336 port3 in 223.5.5.5 → 202.103.23.2: icmp: echo reply
0.322364 port2 in 223.6.6.6 → 202.103.12.2: icmp: echo reply
0.322412 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
```

2. 此时查看健康检查状态，显示ISP1的状态变为dead。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(7.209), jitter(2.282), mos(4.399), bandwidth-up(9999998), bandwidth-dw(9999998), bandwidth-bi(19999996) sla_map=0x0
```

3. 查看FortiGate的SD-WAN规则选路状态，选择ISP2线路（port3）进行转发。




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(2 port3), alive, selected
    2: Seq_num(1 port2), dead
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

4. 查看路由表更新状态，port2的默认路由仍然存在于路由表中，没有被删除。

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.12.1, port2, [1/0]
                  [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```

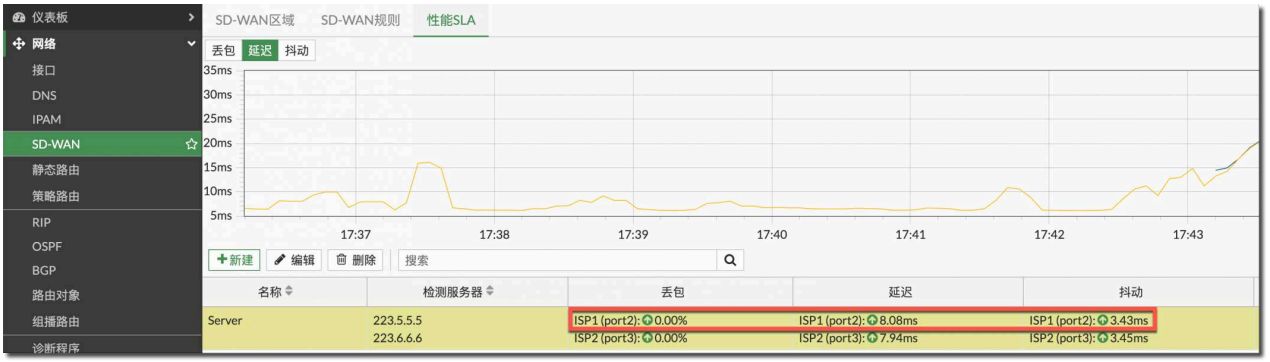
`ISP1#2` down，其他up

1. 将所有ISP故障恢复。在ISP1上模拟223.6.6.6（位于健康检查的Server序列2）故障，其他正常访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.228094 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.228174 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
0.228194 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.228218 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.234403 port3 in 223.5.5.5 → 202.103.23.2: icmp: echo reply
0.234449 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
0.234472 port2 in 223.5.5.5 → 202.103.12.2: icmp: echo reply
```

2. 此时查看健康检查状态，显示ISP1的状态变为仍为alive。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(6.296), jitter(0.547), mos(4.401), bandwidth-up(9999998),
bandwidth-dw(9999999), bandwidth-bi(19999997) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(6.159), jitter(0.528), mos(4.401), bandwidth-up(9999998),
bandwidth-dw(9999998), bandwidth-bi(19999996) sla_map=0x0
```

3. 查看FortiGate的SD-WAN规则选路状态，仍然选择ISP1线路（port2）进行转发。




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port2), alive, selected
    2: Seq_num(2 port3), alive, selected
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

4. 查看路由表更新状态，port2的默认路由仍然存在于路由表中，没有被删除。

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.12.1, port2, [1/0]
                  [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

健康检查状态对Manual模式SD-WAN规则的影响（1个健康检查引用接口）：

- 只要健康检查在这个接口上为alive状态，该线路就会被认为alive，SD-WAN规则不会切换下一个成员接口转发。
- 只要健康检查在这个接口上变为dead状态，该线路就会被认为dead，SD-WAN规则切换下一个alive成员接口转发。

`ISP1#1` & `ISP2#1` down，其他up

1. 将所有ISP故障恢复。在ISP1和ISP2上同时模拟223.5.5.5（位于健康检查的Server序列1）故障，其他正常访问。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.386576 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.386658 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
0.386675 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.386698 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.393021 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
0.393075 port2 in 223.6.6.6 → 202.103.12.2: icmp: echo reply
```

2. 此时查看健康检查状态，显示ISP1和ISP2的状态均为alive。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(7.390), jitter(1.991), mos(4.399), bandwidth-up(9999998),
bandwidth-dw(9999999), bandwidth-bi(19999997) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(7.218), jitter(1.961), mos(4.399), bandwidth-up(9999998),
bandwidth-dw(9999999), bandwidth-bi(19999997) sla_map=0x0
```

3. 查看FortiGate的SD-WAN规则选路状态，仍然选择ISP1线路（port2）进行转发。



4. 查看路由表更新状态，port2的默认路由仍然存在于路由表中，没有被删除。

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.12.1, port2, [1/0]
                  [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

2个Server与健康检查状态的关系：健康检查在每条线路上的状态只由1个Server的探测结果决定。

- **优先使用#1的探测结果**：只要#1在任何一条线路上为up，就忽略#2的探测结果（例如，#1在ISP1为down，但在ISP2为up，此时FortiGate会判断这是线路问题，而不是#1服务器宕机，所以仍然采纳#1的探测结果，不会采纳#2的探测结果）。
- **当#1在所有线路上为down时**：健康检查才会采纳#2的探测结果（此时FortiGate认定#1服务器已经宕机，并开始采纳#2的探测结果）。

`ISP1#1` & `ISP1#2` down，其他up

1. 将所有ISP故障恢复。在ISP1上模拟223.5.5.5和223.6.6.6同时故障（ISP2上223.5.5.5和223.6.6.6都可以访问），其他正常访问。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.382564 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.382643 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
0.382669 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.382692 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.388660 port3 in 223.5.5.5 → 202.103.23.2: icmp: echo reply
0.388690 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
```

2. 此时查看健康检查状态，显示ISP1（port2）的状态变为dead。



3. 查看FortiGate的SD-WAN规则选路状态，选择ISP2线路（port3）进行转发。




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(6), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(2):
    1: Seq_num(2 port3), alive, selected
    2: Seq_num(1 port2), dead
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

4. 查看路由表更新状态，port2的默认路由被删除。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```

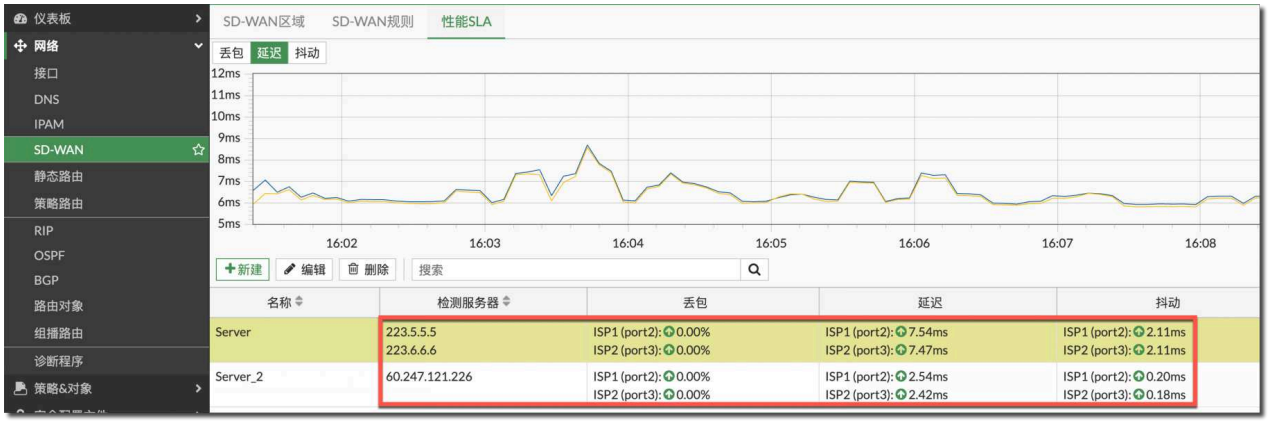
2个健康检查引用相同接口（IPv4）

基础配置

1. 恢复所有的ISP故障模拟。新建1个健康检查“Server_2”，探测Server为60.247.121.226，同时引用ISP1线路接口（port2）和ISP2线路接口（port3）。

```bash
config system sdwan
    config health-check
        edit "Server"
            set server "223.5.5.5" "223.6.6.6"
            set members 0
        next
        edit "Server_2"
            set server "60.247.121.226"
            set members 0
        next
    end
end
```

2. 查看健康检查的状态，两个健康检查在所有ISP上均为alive状态。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(7.180), jitter(3.035), mos(4.398), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(7.134), jitter(3.012), mos(4.398), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
Health Check(Server_2):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(2.530), jitter(0.208), mos(4.403), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(2.419), jitter(0.215), mos(4.403), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
```

重要

后续本文使用如下简写来表示每个线路上对两个Server的探测结果：

- `ISP1#1`：健康检查 “” Server “ISP1上对223.5.5.5的探测结果。
- `ISP1#2`：健康检查 “” Server “ISP1上对223.6.6.6的探测结果。
- `ISP2#1`：健康检查 “” Server “ISP2上对223.5.5.5的探测结果。
- `ISP2#2`：健康检查 “” Server “ISP2上对223.6.6.6的探测结果。
- `ISP1#Server_2`：健康检查 “” Server_2 “ISP1上对60.247.121.226的探测结果。
- `ISP2#Server_2`：健康检查 “” Server_2 “ISP2上对60.247.121.226的探测结果。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

`ISP1#1` down，其他up

1. 在ISP1上模拟探测的目标服务器223.5.5.5（位于健康检查“Server”的序列1）失效，其他正常访问。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.156992 port2 out 202.103.12.2 → 60.247.121.226: icmp: echo request
0.157072 port3 out 202.103.23.2 → 60.247.121.226: icmp: echo request
0.157106 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.157127 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
0.157196 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.157220 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.159406 port2 in 60.247.121.226 → 202.103.12.2: icmp: echo reply
0.159485 port3 in 60.247.121.226 → 202.103.23.2: icmp: echo reply
0.162822 port2 in 223.6.6.6 → 202.103.12.2: icmp: echo reply
0.162899 port3 in 223.5.5.5 → 202.103.23.2: icmp: echo reply
0.162916 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
```

2. 此时查看健康检查状态，健康检查“Server”中的ISP1线路变为dead状态，健康检查“Server_2”中的ISP1线路仍为alive状态。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0×0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(9.357), jitter(4.683), mos(4.395), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0×0
Health Check(Server_2):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(2.509), jitter(0.169), mos(4.403), bandwidth-up(9999996),
bandwidth-dw(9999996), bandwidth-bi(19999992) sla_map=0×0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(2.403), jitter(0.152), mos(4.403), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0×0
```

3. 查看SD-WAN规则选路状态，仍然优先选择ISP1（port2）线路转发。




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(2):
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    1: Seq_num(1 port2), alive, selected
    2: Seq_num(2 port3), alive, selected
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

4. 查看路由表更新状态，port2的默认路由仍然存在于路由表中，没有被删除。

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.12.1, port2, [1/0]
                  [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```

`ISP1#1` & `ISP1#Server_2` down，其他up

1. 将所有ISP故障恢复。在ISP1线路（port2）上模拟探测的目标服务器223.5.5.5（位于健康检查“Server”的序列1）和60.247.121.226（位于健康检查“Server_2”）失效，其他正常访问。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.424523 port2 out 202.103.12.2 → 60.247.121.226: icmp: echo request
0.424724 port3 out 202.103.23.2 → 60.247.121.226: icmp: echo request
0.425029 port2 out 202.103.12.2 → 223.5.5.5: icmp: echo request
0.425091 port2 out 202.103.12.2 → 223.6.6.6: icmp: echo request
0.425162 port3 out 202.103.23.2 → 223.5.5.5: icmp: echo request
0.425210 port3 out 202.103.23.2 → 223.6.6.6: icmp: echo request
0.427347 port3 in 60.247.121.226 → 202.103.23.2: icmp: echo reply
0.430943 port3 in 223.5.5.5 → 202.103.23.2: icmp: echo reply
0.430983 port3 in 223.6.6.6 → 202.103.23.2: icmp: echo reply
0.431002 port2 in 223.6.6.6 → 202.103.12.2: icmp: echo reply
```

2. 此时查看健康检查状态，健康检查“Server_2”中的ISP1线路变为dead状态。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(7.006), jitter(2.388), mos(4.398), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
Health Check(Server_2):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(2.331), jitter(0.189), mos(4.403), bandwidth-up(9999997),
bandwidth-dw(9999997), bandwidth-bi(19999994) sla_map=0x0
```

3. 查看SD-WAN规则选路状态，变为优先选择ISP2（port3）线路转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x200 use-shortcut-sla
 Tie break: cfg
  Gen(5), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(2 port3), alive, selected
    2: Seq_num(1 port2), dead
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

重要

健康检查状态对Manual模式SD-WAN规则的影响（多个健康检查引用接口）：

当配置多个健康检查引用了同一个接口时，需要所有引用此接口的健康检查同时变为dead状态，该线路才会被认为dead，SD-WAN规则选择从下一个alive成员接口转发。

4. 查看路由表更新状态，port2的默认路由仍然存在于路由表中，没有被删除。

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.12.1, port2, [1/0]
                  [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```

`ISP1#1` & `ISP1#2` & `ISP1#Server_2` down，其他up

1. 将所有ISP故障恢复。在ISP1线路（port2）上模拟探测的目标服务器223.5.5.5（位于健康检查“Server”的序列1）、223.6.6.6（位于健康检查“Server”的序列2）和60.247.121.226（位于健康检查“Server_2”）失效，其他正常访问。

```bash
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
0.534318 port2 out 202.103.12.2 -> 223.5.5.5: icmp: echo request
0.534508 port2 out 202.103.12.2 -> 223.6.6.6: icmp: echo request
0.534587 port3 out 202.103.23.2 -> 223.5.5.5: icmp: echo request
0.534648 port3 out 202.103.23.2 -> 223.6.6.6: icmp: echo request
0.534686 port2 out 202.103.12.2 -> 60.247.121.226: icmp: echo request
0.534748 port3 out 202.103.23.2 -> 60.247.121.226: icmp: echo request
0.536783 port3 in 60.247.121.226 -> 202.103.23.2: icmp: echo reply
0.540581 port3 in 223.5.5.5 -> 202.103.23.2: icmp: echo reply
0.540609 port3 in 223.6.6.6 -> 202.103.23.2: icmp: echo reply
```

2. 查看路由表更新状态，port2的默认路由被删除。

```bash
FortiGate # get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 202.103.23.1, port3, [1/0]
C       10.10.1.0/24 is directly connected, port4
C       202.103.12.0/24 is directly connected, port2
C       202.103.23.0/24 is directly connected, port3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

多个健康检查与更新静态路由的关系：

- 只有当接口关联的所有健康检查中的探测服务器都处于down状态时，相关接口上的路由才会被删除。
- 即使接口关联的所有健康检查显示为dead状态，但只要有一个健康检查中的服务器为up（例如：#1为down，#2为up），就不会触发更新静态路由（`update-static-route`）的动作。

2个健康检查引用相同接口（IPv4+IPv6）

1. 在以上配置和故障模拟的基础上，新建健康检查“Server_3”的探测目标为IPv6地址。

```bash
config system sdwan
    config health-check
        edit "Server"
            set server "223.5.5.5" "223.6.6.6"
            set members 0
        next
        edit "Server_2"
            set server "60.247.121.226"
            set members 0
        next
        edit "Server_3"
            set addr-mode ipv6
            set server "::223:5:5:5"
            set members 0
        next
    end
end
```

2. 查看健康检查的状态，IPv4健康检查在ISP1线路（port2）上均为dead状态，IPv6健康检查在ISP2线路（port3）上为alive状态。




```bash
FortiGate # diagnose sys sdwan health-check status
Health Check(Server):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(2.000%) latency(5.965), jitter(0.724), mos(4.400), bandwidth-up(9999996),
bandwidth-dw(9999996), bandwidth-bi(19999992) sla_map=0x0
Health Check(Server_2):
Seq(1 port2): state(dead), packet-loss(100.000%) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(2.000%) latency(2.414), jitter(0.160), mos(4.402), bandwidth-up(9999996),
bandwidth-dw(9999996), bandwidth-bi(19999992) sla_map=0x0
Health Check(Server_3):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(2.351), jitter(0.188), mos(4.403), bandwidth-up(9999996),
bandwidth-dw(9999998), bandwidth-bi(19999994) sla_map=0x0
Seq(2 port3): state(alive), packet-loss(0.000%) latency(2.281), jitter(0.224), mos(4.403), bandwidth-up(9999996),
bandwidth-dw(9999996), bandwidth-bi(19999992) sla_map=0x0
```

3. 查看SD-WAN规则（IPv4）选路状态，变为优先选择ISP1（port2）线路转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
FortiGate # diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0×200 use-shortcut-sla
 Tie break: cfg
  Gen(2), TOS(0×0/0×0), Protocol(0: 1→65535), Mode(manual)
  Members(2):
    1: Seq_num(1 port2), alive, selected
    2: Seq_num(2 port3), alive, selected
  Src address(1):
        0.0.0.0-255.255.255.255

  Dst address(1):
        0.0.0.0-255.255.255.255
```

重要

健康检查状态对Manual模式SD-WAN规则的影响（多个IPv4/IPv6健康检查同时引用接口）：

引用同一接口的健康检查探测目标Server有IPv4、IPv6两种，必须满足所有接口相关的健康检查为dead状态时，该线路才会被认为dead，Manual模式的SD-WAN规则（无论是IPv4规则还是IPv6规则）才会选择从下一个alive成员接口转发。

总结

健康检查目标个数对健康检查状态的影响

- **1个目标服务器：**如果健康检查配置只有1个探测Server，则健康检查状态直接由该目标的状态决定。探测目标down时，健康检查被标记为dead。
- **2个目标服务器：**健康检查在每条线路上的状态只由1个Server的探测结果决定。
  - **优先使用#1的探测结果：**只要#1在任何一条线路上为up，就忽略#2的探测结果（例如，#1在ISP1为down，但在ISP2为up，此时FortiGate会判断这是线路问题，而不是#1服务器宕机，所以仍然采纳#1的探测结果，不会采纳#2的探测结果）。
  - **当#1在所有线路上为down时：**健康检查才会采纳#2的探测结果（此时FortiGate认定#1服务器已经宕机，并开始采纳#2的探测结果）。

健康检查状态对Manual模式SD-WAN规则选路的影响

- **1个健康检查引用接口：**
  - 只要健康检查在这个接口上为alive状态，该线路就会被认为alive，SD-WAN规则不会切换下一个成员接口转发。
  - 只要健康检查在这个接口上变为dead状态，该线路就会被认为dead，SD-WAN规则切换下一个alive成员接口转发（即使健康检查关闭了`update-static-route`），如果SD-WAN规则的所有成员都变为dead状态，则该条SD-WAN规则会被跳过匹配（即使健康检查关闭了`update-static-route`）。
- **多个健康检查引用接口：**

重要

Best quality、Lowest cost (SLA)、Maximize bandwidth (SLA)模式的SD-WAN必须选择一个具体的健康检查，不需要考虑下列情况。

  - 当配置多个健康检查引用了同一个接口时，需要所有引用此接口的健康检查同时变为dead状态，该线路才会被认为dead，SD-WAN规则选择从下一个alive成员接口转发。
  - 引用同一接口的健康检查探测目标Server有IPv4、IPv6两种，必须满足所有接口相关的健康检查为dead状态时，该线路才会被认为dead，SD-WAN规则（无论是IPv4规则还是IPv6规则）才会选择从下一个alive成员接口转发。

多个健康检查与更新静态路由的关系

- 只有当接口关联的所有健康检查中的探测服务器都处于down状态时，相关接口上的路由才会被删除。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 即使接口关联的所有健康检查显示为dead状态，但只要有一个健康检查中的服务器为up（例如：#1为down，#2为up），就不会触发更新静态路由（`update-static-route`）的动作。

配置建议

健康检查的探测目标

- 优选稳定、低延迟、高可靠性的探测目标（如公共DNS服务器）。
- 在高可用需求场景中，可以在健康检查中配置2个目标服务器并合理设置先后顺序。
- 确保接口关联的健康检查数量和目标足够精准，避免冗余，尽量不要使用多个健康检查引用同一个接口。

更新静态路由

在配置健康检查时，是否开启`update-static-route`功能取决于具体的网络环境和需求。以下是关于何时应开启/关闭此功能的建议：

- 建议关闭`update-static-route`的情况：
  - **仅作为测试的健康检查：**即使没有SD-WAN规则引用，`update-static-route`仍会生效，开启该功能可能导致网络中断。因此，对于任何非生产性的测试配置，请关闭`update-static-route`选项。
  - **单一探测目标：**在健康检查仅配置了1个探测服务器，并且FortiGate设备自身需要发起流量（例如IPSec、SSL VPN或BGP通信）的情况下，启用`update-static-route`可能导致相关流量路径变化，进而引起服务中断。
- 可以考虑开启`update-static-route`的情况：
  - **多Server健康检查：** 健康检查配置多个Server时，可以根据实际情况考虑开启更新静态路由（`update-static-route`）。
  - **IPv4/IPv6共存：** 对于同时支持IPv4和IPv6的网络环境，为IPv4/IPv6分别配置了健康检查目标。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SD-WAN常用SNMP监控项

SD-WAN SNMP OID

SNMP节点名称	OID	说明
fgVWLHealthCheckLinkNumber	.1.3.6.1.4.1.12356.101.4.9.1	fgVWLHealthCheckLinkTable中的健康检查的链路数
fgVWLHealthCheckLinkTable	.1.3.6.1.4.1.12356.101.4.9.2	SD-WAN健康检查统计表，包含以下的所有OID结果。该表与fgVdTable存在依赖扩展关系，仅包含已配置成员的健康检查
fgVWLHealthCheckLinkEntry	.1.3.6.1.4.1.12356.101.4.9.2.1	VDOM ID 1上的SD-WAN健康检查统计表（如果是VDOM ID 2，则是.1.3.6.1.4.1.12356.101.4.9.2.2，以此类推）
fgVWLHealthCheckLinkID	.1.3.6.1.4.1.12356.101.4.9.2.1.1	SD-WAN健康检查的Seq ID（对应diagnose sys sdwan health-check中的Seq）。此表中仅包含已配置成员的健康检查（SD-WAN的健康检查链路ID在每个VDOM内是唯一的）
fgVWLHealthCheckLinkName	.1.3.6.1.4.1.12356.101.4.9.2.1.2	健康检查名称
fgVWLHealthCheckLinkSeq	.1.3.6.1.4.1.12356.101.4.9.2.1.3	SD-WAN成员线路的ID
fgVWLHealthCheckLinkState	.1.3.6.1.4.1.12356.101.4.9.2.1.4	某个成员的健康检查状态
fgVWLHealthCheckLinkLatency	.1.3.6.1.4.1.12356.101.4.9.2.1.5	在过去的30次探测周期内，成员健康检查的平均延迟，以float格式表示
fgVWLHealthCheckLinkJitter	.1.3.6.1.4.1.12356.101.4.9.2.1.6	在过去的30次探测周期内，成员健康检查的平均抖动，以float格式表示
fgVWLHealthCheckLinkPacketSend	.1.3.6.1.4.1.12356.101.4.9.2.1.7	在某个成员线路上已发送的健康检查报文总数
fgVWLHealthCheckLinkPacketRecv	.1.3.6.1.4.1.12356.101.4.9.2.1.8	在某个成员线路上已接收的健康检查报文总数
fgVWLHealthCheckLinkPacketLoss	.1.3.6.1.4.1.12356.101.4.9.2.1.9	在过去的30次探测周期内，成员健康检查的平均丢包率，以float格式表示
fgVWLHealthCheckLinkVdom	.1.3.6.1.4.1.12356.101.4.9.2.1.10	健康检查所在的VDOM名称，该名称对应fgVdTable中使用的fgVdEntName
fgVWLHealthCheckLinkBandwidthIn	.1.3.6.1.4.1.12356.101.4.9.2.1.11	健康检查在某个成员链接上检测到的入向可用带宽，以Mbps为单位
fgVWLHealthCheckLinkBandwidthOut	.1.3.6.1.4.1.12356.101.4.9.2.1.12	健康检查在某个成员链接上检测到的出向可用带宽，以Mbps为单位
fgVWLHealthCheckLinkBandwidthBi	.1.3.6.1.4.1.12356.101.4.9.2.1.13	健康检查在某个成员链接上检测到的双向可用带宽，以Mbps为单位
fgVWLHealthCheckLinkIfName	.1.3.6.1.4.1.12356.101.4.9.2.1.14	SD-WAN成员接口名称

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

读取结果参考

读取SNMP项	OID			
fgVWLHealthCheckLinkNumber	.1.3.6.1.4.1.12356.101.4.9.1	3		
fgVWLHealthCheckLinkID	.1.3.6.1.4.1.12356.101.4.9.2.1.1	1	2	3
fgVWLHealthCheckLinkName	.1.3.6.1.4.1.12356.101.4.9.2.1.2	pingserver	pingserver	pingserver
fgVWLHealthCheckLinkSeq	.1.3.6.1.4.1.12356.101.4.9.2.1.3	2	1	3
fgVWLHealthCheckLinkState	.1.3.6.1.4.1.12356.101.4.9.2.1.4	0	0	0
fgVWLHealthCheckLinkLatency	.1.3.6.1.4.1.12356.101.4.9.2.1.5	39.302	43.124	44.348
fgVWLHealthCheckLinkJitter	.1.3.6.1.4.1.12356.101.4.9.2.1.6	4.346	3.951	5.05
fgVWLHealthCheckLinkPacketSend	.1.3.6.1.4.1.12356.101.4.9.2.1.7	3657689	3657689	3657689
fgVWLHealthCheckLinkPacketRecv	.1.3.6.1.4.1.12356.101.4.9.2.1.8	3196258	3220258	3219466
fgVWLHealthCheckLinkPacketLoss	.1.3.6.1.4.1.12356.101.4.9.2.1.9	0	0	0
fgVWLHealthCheckLinkVdom	.1.3.6.1.4.1.12356.101.4.9.2.1.10	root	root	root
fgVWLHealthCheckLinkBandwidthIn	.1.3.6.1.4.1.12356.101.4.9.2.1.11	9999963	9999937	9999999
fgVWLHealthCheckLinkBandwidthOut	.1.3.6.1.4.1.12356.101.4.9.2.1.12	9999981	9999953	9999998
fgVWLHealthCheckLinkBandwidthBi	.1.3.6.1.4.1.12356.101.4.9.2.1.13	19999944	19999890	19999997
fgVWLHealthCheckLinkIfName	.1.3.6.1.4.1.12356.101.4.9.2.1.14	MPLS	port1	port2

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SD-WAN排错

SD-WAN日志

健康检查

1. 健康检查对路由的影响：

- 检测到中断，删除对应接口的静态路由。

```bash
date=2024-01-20 time=17:06:31 eventtime=1618963591590008160 tz="-0700" logid="0100022921" type="event" subtype="system" level="critical" vd="root" logdesc="Routing information changed" name="test" interface="R150" status="down" msg="Static route on interface R150 may be removed by health-check test. Route:  (10.100.1.2->10.100.2.22 ping-down)"
```

- 健康检查检测到恢复，恢复对应接口的静态路由。

```bash
date=2024-01-20 time=17:11:46 eventtime=1618963906950174240 tz="-0700" logid="0100022921" type="event" subtype="system" level="critical" vd="root" logdesc="Routing information changed" name="test" interface="R150" status="up" msg="Static route on interface R150 may be added by health-check test. Route:  (10.100.1.2->10.100.2.22 ping-up)"
```

2. SD-WAN健康检查某个成员的状态变化：

- 健康检查失败（Dead），停止转发流量。

```bash
date=2024-01-20 time=23:04:32 eventtime=1618985072898756700 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" interface="R150" member="1" serviceid=1 service="test" gateway=10.100.1.1 msg="Member link is unreachable or miss threshold. Stop forwarding traffic. "
```

- 健康检查从失败（Dead）恢复为alive，继续转发流量。

```bash
date=2024-01-20 time=23:06:08 eventtime=1618985168018789600 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" interface="R150" member="1" serviceid=1 service="test" gateway=10.100.1.1 msg="Member link is available. Start forwarding traffic. "
```

3. 健康检查中的SLA目标：

- 不满足SLA目标。

```bash
date=2024-01-20 time=21:32:33 eventtime=1618979553388763760 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Health Check" healthcheck="test" slatargetid=1 oldvalue="2" newvalue="1" msg="Number of pass member changed."
date=2024-01-20 time=21:32:33 eventtime=1618979553388751880 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Health Check" healthcheck="test" slatargetid=1 member="1" msg="Member status changed. Member out-of-sla."
```

- SLA目标从不满足目标恢复为满足目标。

```bash
date=2024-01-20 time=21:38:49 eventtime=1618979929908765200 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Health Check" healthcheck="test" slatargetid=1 oldvalue="1" newvalue="2" msg="Number of pass member changed."
date=2024-01-20 time=21:38:49 eventtime=1618979929908754060 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="information" vd="root" logdesc="SDWAN status" eventtype="Health Check" healthcheck="test" slatargetid=1 member="1" msg="Member status changed. Member in sla."
```

成员转发状态

1. 某链路带宽占用：

- 已经达到了配置的该成员的带宽值，停止转发流量。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
date=2024-01-20 time=21:55:14 eventtime=1618980914728863220 tz="-0700" logid="0113022924" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN volume status" eventtype="Volume" interface="R160" member="2" msg="Member enters into conservative status with limited ablity to receive new sessions for too much traffic."
```
bash

- 占用已经恢复小于配置的带宽值，并继续开始转发流量。

```
date=2024-01-20 time=22:12:52 eventtime=1618981972698753360 tz="-0700" logid="0113022924" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN volume status" eventtype="Volume" interface="R160" member="2" msg="Member resume normal status to receive new sessions for internal adjustment"
```
bash

2. 配置SLA类型（Lowest Cost/Maximize bandwidth）的SD-WAN规则，由于SLA检查失败，转发成员顺序发生变化。

```
date=2024-01-20 time=22:40:46 eventtime=1618983646428803040 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="test" seq="2,1" msg="Service prioritized by SLA will be redirected in sequence order."
```
bash

3. 配置Lowest Cost类型的SD-WAN规则，由于SLA检查从失败恢复为通过，转发成员顺序发生变化。

```
date=2024-01-20 time=22:41:51 eventtime=1618983711678827920 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="test" seq="1,2" msg="Service prioritized by SLA will be redirected in sequence order."
```
bash

4. 配置Best Quality类型的SD-WAN规则，转发成员的顺序发生变化。

```
date=2024-01-20 time=22:56:55 eventtime=1618984615708804760 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="test" metric="packet-loss" seq="2,1" msg="Service prioritized by performance metric will be redirected in sequence order."

date=2024-01-20 time=22:56:58 eventtime=1618984618278852140 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="test" metric="packet-loss" seq="1,2" msg="Service prioritized by performance metric will be redirected in sequence order."
```
bash

5. 配置Maximize bandwidth类型的SD-WAN规则：

- 转发成员不满足SLA标准，此成员停止转发流量。

```
date=2024-01-20 time=23:10:24 eventtime=1618985425048820800 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="test" member="2(R160)" msg="Service will be load balanced among members with available routing."
```
bash

- 配置Maximize bandwidth类型的SD-WAN规则，转发成员从不满足SLA标准恢复到满足SLA标准，此成员可以继续转发流量。

```
date=2024-01-20 time=23:11:34 eventtime=1618985494478807100 tz="-0700" logid="0113022923" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN status" eventtype="Service" serviceid=1 service="test" member="2(R160),1(R150)" msg="Service will be load balanced among members with available routing."
```
bash

6. 在健康检查的配置中开启了SLA周期日志：

- 在健康检查的配置中开启了`sla-fail-log-period`，健康检查周期性产生的SLA失败日志。

```
date=2024-01-20 time=23:18:10 eventtime=1618985890469018260 tz="-0700" logid="0113022925" type="event" subtype="sdwan" level="notice" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="test" slatargetid=1 interface="R150" status="up" latency="0.061" jitter="0.004" packetloss="2.000%" inbandwidthavailable="0kbps" outbandwidthavailable="200.00Mbps" bibandwidthavailable="200.00Mbps" inbandwidthused="1kbps" outbandwidthused="1kbps" bibandwidthused="2kbps" slamap="0x0" metric="packetloss" msg="Health Check SLA status. SLA failed due to being over the performance metric threshold."
```
bash

- 在健康检查的配置中开启了`sla-pass-log-period`，健康检查周期性产生的SLA成功日志。

```
date=2024-01-20 time=23:18:12 eventtime=1618985892509027220 tz="-0700" logid="0113022925" type="event" subtype="sdwan" level="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="test" slatargetid=1 interface="R150" status="up" latency="0.060" jitter="0.003" packetloss="0.000%" inbandwidthavailable="0kbps" outbandwidthavailable="200.00Mbps" bibandwidthavailable="200.00Mbps" inbandwidthused="1kbps" outbandwidthused="1kbps" bibandwidthused="2kbps" slamap="0x1" msg="Health Check SLA status."
```
bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SD-WAN调试命令

SD-WAN健康检查

查看SD-WAN健康检查的状态。

```bash
FGT # diagnose sys sdwan health-check
Health Check(server):
Seq(1 R150): state(alive), packet-loss(0.000%) latency(0.110), jitter(0.024) sla_map=0x0
Seq(2 R160): state(alive), packet-loss(0.000%) latency(0.068), jitter(0.009) sla_map=0x0

Health Check(ping):
Seq(1 R150): state(alive), packet-loss(0.000%) latency(0.100), jitter(0.017) sla_map=0x0
Seq(2 R160): state(dead), packet-loss(100.000%) sla_map=0x0

FGT # diagnose sys sdwan health-check ping
Health Check(ping):
Seq(1 R150): state(alive), packet-loss(0.000%) latency(0.100), jitter(0.017) sla_map=0x0
Seq(2 R160): state(dead), packet-loss(100.000%) sla_map=0x0
```

SD-WAN成员状态

1. 使用`source-ip-based`或`source-dest-ip-based`作为`load-balance`的模式时，查看SD-WAN成员的状态。

```bash
FGT # diagnose sys sdwan member
Member(1): interface: R150, gateway: 10.100.1.1 2000:10:100:1::1, priority: 0 1024, weight: 0
Member(2): interface: R160, gateway: 10.100.1.5 2000:10:100:1::5, priority: 0 1024, weight: 0
```

2. 使用`weight-based`作为`load-balance`的模式时，查看SD-WAN成员的状态。

```bash
FGT # diagnose sys sdwan member
Member(1): interface: R150, gateway: 10.100.1.1 2000:10:100:1::1, priority: 0 1024, weight: 33
  Session count: 15
Member(2): interface: R160, gateway: 10.100.1.5 2000:10:100:1::5, priority: 0 1024, weight: 66
  Session count: 1
```

3. 使用`measured-volume-based`作为`load-balance`的模式时：

   - 所有的成员均还有使用余量，查看SD-WAN成员的状态。

```bash
FGT # diagnose sys sdwan member
Member(1): interface: R150, gateway: 10.100.1.1 2000:10:100:1::1, priority: 0 1024, weight: 33
  Config volume ratio: 33, last reading: 218067B, volume room 33MB
Member(2): interface: R160, gateway: 10.100.1.5 2000:10:100:1::5, priority: 0 1024, weight: 66
  Config volume ratio: 66, last reading: 202317B, volume room 66MB
```

   - 某个成员的用量已经用尽。

```bash
FGT # diagnose sys sdwan member
Member(1): interface: R150, gateway: 10.100.1.1 2000:10:100:1::1, priority: 0 1024, weight: 0
  Config volume ratio: 33, last reading: 1287767633B, overload volume 517MB
Member(2): interface: R160, gateway: 10.100.1.5 2000:10:100:1::5, priority: 0 1024, weight: 63
  Config volume ratio: 66, last reading: 1686997898B, volume room 63MB
```

4. 使用`usage-based`或``spillover`作为load-balance`的模式时：

   - 当溢出未发生时，查看SD-WAN成员的状态。

```bash
FGT # diagnose sys sdwan member
Member(1): interface: R150, gateway: 10.100.1.1 2000:10:100:1::1, priority: 0 1024, weight: 255
  Egress-spillover-threshold: 400kbit/s, ingress-spillover-threshold: 300kbit/s
  Egress-overbps=0, ingress-overbps=0
Member(2): interface: R160, gateway: 10.100.1.5 2000:10:100:1::5, priority: 0 1024, weight: 254
  Egress-spillover-threshold: 0kbit/s, ingress-spillover-threshold: 0kbit/s
  Egress-overbps=0, ingress-overbps=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 当某个成员发生溢出时。

```bash
FGT # diagnose sys sdwan member
Member(1): interface: R150, gateway: 10.100.1.1 2000:10:100:1::1, priority: 0 1024, weight: 255
  Egress-spillover-threshold: 400kbit/s, ingress-spillover-threshold: 300kbit/s
  Egress-overbps=1, ingress-overbps=0
Member(2): interface: R160, gateway: 10.100.1.5 2000:10:100:1::5, priority: 0 1024, weight: 254
  Egress-spillover-threshold: 0kbit/s, ingress-spillover-threshold: 0kbit/s
  Egress-overbps=0, ingress-overbps=0
```

- `diagnose netlink dstmac list`命令也可以查看是否发生了溢出情况。

```bash
FGT # diagnose netlink dstmac list R150
dev=R150 mac=00:00:00:00:00:00 vwl rx_tcp_mss=0 tx_tcp_mss=0 egress_overspill_threshold=50000
egress_bytes=100982 egress_over_bps=1 ingress_overspill_threshold=37500 ingress_bytes=40 ingress_over_bps=0
sampler_rate=0 vwl_zone_id=1 intf_qua=0
```

SD-WAN规则状态

1. 使用`manual`模式的SD-WAN规则。

```bash
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 R150), alive, selected
    2: Seq_num(2 R160), alive, selected
  Dst address(1):
        10.100.21.0-10.100.21.255
```

2. 使用`auto`模式的SD-WAN规则。

```bash
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(auto), link-cost-factor(latency), link-cost-threshold(10),
heath-check(ping)
  Members(2):
    1: Seq_num(2 R160), alive, latency: 0.066, selected
    2: Seq_num(1 R150), alive, latency: 0.093
  Dst address(1):
        10.100.21.0-10.100.21.255
```

3. 使用`Priority`模式（Best Quality）的SD-WAN规则。

```bash
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-cost-threshold(10),
heath-check(ping)
  Members(2):
    1: Seq_num(2 R160), alive, latency: 0.059, selected
    2: Seq_num(1 R150), alive, latency: 0.077, selected
  Dst address(1):
        10.100.21.0-10.100.21.255
```

4. 使用`sla`模式（Lowest Cost）的SD-WAN规则。

```bash
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Members(2):
    1: Seq_num(1 R150), alive, sla(0x1), gid(0), cfg_order(0), cost(0), selected
    2: Seq_num(2 R160), alive, sla(0x1), gid(0), cfg_order(1), cost(0), selected
  Dst address(1):
        10.100.21.0-10.100.21.255
```

5. 使用`load-balance`模式（Best Quality）的SD-WAN规则。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FGT # diagnose sys sdwan service
Service(1): Address Mode(IPV4) flags=0x200
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance hash-mode=round-robin)
  Members(2):
    1: Seq_num(1 R150), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(2 R160), alive, sla(0x1), gid(2), num of pass(1), selected
  Dst address(1):
        10.100.21.0-10.100.21.255
```

SD-WAN统计信息

1. 过去15分钟的SD-WAN接口状态统计日志。

```bash
FGT (root) # diagnose sys sdwan intf-sla-log R150
Timestamp: Wed Apr 21 16:58:27 2021, used inbandwidth: 655bps, used outbandwidth: 81655306bps, used bibandwidth:
81655961bps, tx bys: 3413479982bytes, rx bytes: 207769bytes.
Timestamp: Wed Apr 21 16:58:37 2021, used inbandwidth: 649bps, used outbandwidth: 81655540bps, used bibandwidth:
81656189bps, tx bys: 3515590414bytes, rx bytes: 208529bytes.
Timestamp: Wed Apr 21 16:58:47 2021, used inbandwidth: 655bps, used outbandwidth: 81655546bps, used bibandwidth:
81656201bps, tx bys: 3617700886bytes, rx bytes: 209329bytes.
Timestamp: Wed Apr 21 16:58:57 2021, used inbandwidth: 620bps, used outbandwidth: 81671580bps, used bibandwidth:
81672200bps, tx bys: 3719811318bytes, rx bytes: 210089bytes.
Timestamp: Wed Apr 21 16:59:07 2021, used inbandwidth: 620bps, used outbandwidth: 81671580bps, used bibandwidth:
81672200bps, tx bys: 3821921790bytes, rx bytes: 210889bytes.
Timestamp: Wed Apr 21 16:59:17 2021, used inbandwidth: 665bps, used outbandwidth: 81688152bps, used bibandwidth:
81688817bps, tx bys: 3924030936bytes, rx bytes: 211926bytes.
Timestamp: Wed Apr 21 16:59:27 2021, used inbandwidth: 671bps, used outbandwidth: 81688159bps, used bibandwidth:
81688830bps, tx bys: 4026141408bytes, rx bytes: 212726bytes.
......
```

2. 过去10分钟的SLA统计日志（`diagnose sys sdwan sla-log <health-check-name> <seq-num> or <health-check-name> <seq-num> <childname>`，如下所示，`1`为SD-WAN成员接口在SD-WAN区域中的成员ID（seq-num）。

```bash
FGT (root) # diagnose sys sdwan sla-log ping 1
Timestamp: Wed Apr 21 17:10:11 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.079,
jitter: 0.023, packet loss: 0.000%.
Timestamp: Wed Apr 21 17:10:12 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.079,
jitter: 0.023, packet loss: 0.000%.
Timestamp: Wed Apr 21 17:10:12 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.081,
jitter: 0.024, packet loss: 0.000%.
Timestamp: Wed Apr 21 17:10:13 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.081,
jitter: 0.025, packet loss: 0.000%.
Timestamp: Wed Apr 21 17:10:13 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.082,
jitter: 0.026, packet loss: 0.000%.
Timestamp: Wed Apr 21 17:10:14 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.083,
jitter: 0.026, packet loss: 0.000%.
Timestamp: Wed Apr 21 17:10:14 2021, vdom root, health-check ping, interface: R150, status: up, latency: 0.084,
jitter: 0.026, packet loss: 0.000%.
......
```

SD-WAN状态信息

1. SD-WAN规则引用应用控制特征后，应用控制学习的条目状态。

```bash
FGT # diagnose sys sdwan internet-service-app-ctrl-list
Gmail(15817 4294836957): 64.233.191.19 6 443 Thu Apr 22 10:10:34 2021
Gmail(15817 4294836957): 142.250.128.83 6 443 Thu Apr 22 10:06:47 2021
Facebook(15832 4294836806): 69.171.250.35 6 443 Thu Apr 22 10:12:00 2021
Amazon(16492 4294836342): 3.226.60.231 6 443 Thu Apr 22 10:10:57 2021
Amazon(16492 4294836342): 52.46.135.211 6 443 Thu Apr 22 10:10:58 2021
Amazon(16492 4294836342): 52.46.141.85 6 443 Thu Apr 22 10:10:58 2021
Amazon(16492 4294836342): 52.46.155.13 6 443 Thu Apr 22 10:10:58 2021
Amazon(16492 4294836342): 54.82.242.32 6 443 Thu Apr 22 10:10:59 2021
YouTube(31077 4294838537): 74.125.202.138 6 443 Thu Apr 22 10:06:51 2021
YouTube(31077 4294838537): 108.177.121.119 6 443 Thu Apr 22 10:08:24 2021
YouTube(31077 4294838537): 142.250.136.119 6 443 Thu Apr 22 10:02:02 2021
YouTube(31077 4294838537): 142.250.136.132 6 443 Thu Apr 22 10:08:16 2021
YouTube(31077 4294838537): 142.250.148.100 6 443 Thu Apr 22 10:07:28 2021
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
YouTube(31077 4294838537): 142.250.148.132 6 443 Thu Apr 22 10:10:32 2021
YouTube(31077 4294838537): 172.253.119.91 6 443 Thu Apr 22 10:02:01 2021
YouTube(31077 4294838537): 184.150.64.211 6 443 Thu Apr 22 10:04:36 2021
YouTube(31077 4294838537): 184.150.168.175 6 443 Thu Apr 22 10:02:26 2021
YouTube(31077 4294838537): 184.150.168.211 6 443 Thu Apr 22 10:02:26 2021
YouTube(31077 4294838537): 184.150.186.141 6 443 Thu Apr 22 10:02:26 2021
YouTube(31077 4294838537): 209.85.145.190 6 443 Thu Apr 22 10:10:36 2021
YouTube(31077 4294838537): 209.85.200.132 6 443 Thu Apr 22 10:02:03 2021
```

2. 查看IPSec创建的Shortcut隧道的健康检查状态（`diagnose sys link-monitor interface <name> <name>_0`）。

```bash
Spoke1 # diagnose sys link-monitor interface Spoke1_WAN2
Interface(Spoke1_WAN2): state(down, since Fri Jan 19 16:58:13 2024), bandwidth(up:288bps, down:0bps), session
count(IPv4:7, IPv6:0), tx(26595 bytes), rx(21568 bytes).

Spoke1 # diagnose sys link-monitor interface Spoke1_WAN2 Spoke1_WAN2_0
Interface(Spoke1_WAN2_0): state(up, since Fri Jan 19 16:58:08 2024), bandwidth(up:320bps, down:320bps), session
count(IPv4:0, IPv6:0), tx(12360 bytes), rx(12240 bytes), latency(2.15), jitter(0.53), packet-loss(0.00).
```

3. 查看SD-WAN中使用的BGP route-tag。

```bash
FGT # get router info bgp network 10.100.11.0/24
VRF 0 BGP routing table entry for 10.100.11.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   10.100.1.1
  Original VRF 0
  20 10
    10.100.1.1 from 10.100.1.1 (5.5.5.5)
      Origin incomplete metric 0, route tag 15, localpref 100, valid, external, best
      Community: 30:5
      Advertised Path ID: 2
       Last update: Thu Apr 22 10:27:27 2021

  Original VRF 0
  20 10
    10.100.1.5 from 10.100.1.5 (6.6.6.6)
      Origin incomplete metric 0, route tag 15, localpref 100, valid, external, best
      Community: 30:5
      Advertised Path ID: 1
       Last update: Thu Apr 22 10:25:50 2021

FGT # diagnose sys sdwan route-tag-list
Route-tag: 15, address: v4(1), v6(0)Last write/now: 6543391 6566007
        service(1), last read route-tag 15 at 6543420
Prefix(24): Address list(1):
        10.100.11.0-10.100.11.255 oif: 50 48

FGT # diagnose firewall proute list
list route policy info(vf=root):
id=2133196801(0x7f260001) vwl_service=1(DataCenter) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff flags=0x40 order-addr
tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 oif=48(R150) oif=50(R160)
destination(1): 10.100.11.0-10.100.11.255
source wildcard(1): 0.0.0.0/0.0.0.0
hit_count=0 last_used=2021-04-22 10:25:10
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NetFlow的配置

NetFlow介绍

NetFlow允许基于设备接口收集网络流量的统计信息，它提供了在数据进入或离开接口时收集IP网络流量的能力。通过分析NetFlow提供的数据，网络管理员可以确定流量的源和目的地、服务类别以及拥塞的原因。

NetFlow通常使用UDP协议进行导出，并使用NetFlow Collector进行收集。NetFlow Collector的IP地址和目标UDP端口必须在发送设备（FortiGate）上进行配置。标准的NetFlow UDP端口为2055。

在FortiGate中，根据netflow-sampler监控的接口，发送所有此接口相关的会话信息，无法设置NetFlow的接口采样率。

> **重要**
>
> 在任何接口上配置NetFlow都不会影响NP芯片的加速功能。
>
> 但如果使用的是sFlow，是无法被任何NP芯片加速的。

NetFlow配置

NetFlow发送配置

未开启VDOM的配置

```bash
7.0.X、7.2.0~7.2.7、7.4.0~7.4.3版本（只能配置1个Collector）：
config system netflow
    set collector-ip <ip>
    set collector-port <port>
    set source-ip <ip>
    set active-flow-timeout <integer>
    set inactive-flow-timeout <integer>
    set template-tx-timeout <integer>
    set template-tx-counter <integer>
end

其他7.X.X版本（可以配置最多6个Collector）：
config system netflow
    set active-flow-timeout {integer}
    config collectors
        edit <id>
            set collector-ip {string}
            set collector-port {integer}
            set source-ip {string}
            set interface-select-method [auto|sdwan| ... ]
            set interface {string}
        next
    end
    set inactive-flow-timeout {integer}
    set template-tx-counter {integer}
    set template-tx-timeout {integer}
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

参数名称	参数说明
collector-ip [ip]	NetFlow collector的IPv4或IPv6地址（IPv6在7.2.0 GA后支持）
collector-port [port]	NetFlow collector用于接收NetFlow流量的端口，默认为2055
source-ip [ip]	指定FortiGate发送NetFlow流量的源IP，默认根据路由出接口指定源IP
active-flow-timeout [integer]	报告活动中的会话NetFlow信息的间隔，默认为30分钟，范围1~60
inactive-flow-timeout [integer]	报告已结束的会话NetFlow信息的间隔，默认为15秒，范围10~600
template-tx-timeout [integer]	模板数据流的发送间隔，默认30分钟，范围1~1440
template-tx-counter [integer]	数据流记录的产生计数，达到这个计数后也会发送模板数据流到collector，默认为20，范围10~6000

开启多VDOM的配置

重要

在多VDOM环境中，无法在root VDOM或管理VDOM上配置Netflow，root VDOM或管理VDOM的NetFlow配置将从`config system global`下的NetFlow配置继承。

在多VDOM + HA环境中，当HA禁用“ha-direct”功能时，Netflow还是会在独立管理口上发送流量。如果需要通过业务VDOM中的路由接口发送NetFlow流量，必须在`config system global`下禁用NetFlow IP或配置NetFlow IP为0.0.0.0。

bash

```
7.0.X、7.2.0~7.2.7、7.4.0~7.4.3版本:
config vdom
    edit <vdom>
        config system vdom-netflow
            set vdom-netflow enable
            set collector-ip <ip>
            set collector-port <port>
            set source-ip <ip>
        end
    next
end

其他7.X.X版本:
config vdom
    edit <vdom>
        config system vdom-netflow
            set active-flow-timeout {integer}
            config collectors
                edit <id>
                    set collector-ip {string}
                    set collector-port {integer}
                    set source-ip {string}
                    set interface-select-method [auto|sdwan| ... ]
                    set interface {string}
                next
            end
            set inactive-flow-timeout {integer}
            set template-tx-counter {integer}
            set template-tx-timeout {integer}
        end
    next
end
```

NetFlow采样器配置

bash

```
config system interface
    edit <interface>
        set netflow-sampler {disable | tx | rx | both}
    next
end
```

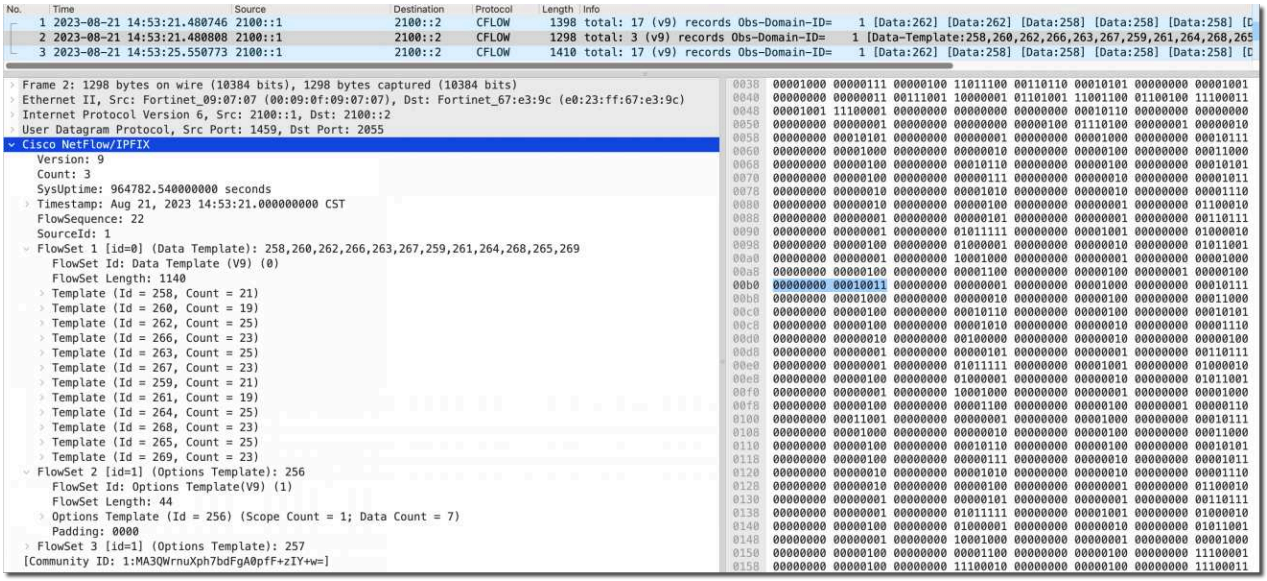

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

参数名称	参数说明
disable	接口下关闭NetFlow采样，默认配置
tx	采样此接口发送的流量
rx	采样此接口接收的流量
both	同时采样此接口发送和接收的流量

配置验证

1. 如果在NetFlow上无法查询到FortiGate的NetFlow数据，可以在FortiGate上抓包查看NetFlow数据是否已发送，如下图所示。

```
diagnose sniffer packet 'host <collector-ip> and port <collector-port>' 6 0 l
```



2. NetFlow功能通过FortiGate的sflow进程工作，通过以下命令，可以看到Netflow的工作状态。

```bash
FortiGate # diagnose test application sflowd 3

==== Netflow Vdom Configuration ====
Global collector:172.22.5.41:[2055] source ip:  active-timeout(seconds):1800 inactive-timeout(seconds):15
___ vdom: root, index=0, is master, collector: disabled (use global config) (mgmt vdom)
   |_ coll_ip:172.22.5.41:2055,src_ip:172.22.5.19
   |_ seq_num:301 pkts/time to next template: 7/1259
   |_ exported: Bytes:114028124, Packets:322978, Sessions:13457 Flows:13494
   |_ active_intf: 1
   |___ interface:wan2 sample_direction:both device_index:6 snmp_index:2
```

3. 查看流量会话是否匹配NetFlow，如下所示，会话被打上了NetFlow-reply方向的标记。

```bash
# diagnose sys session list
session info: proto=1 proto_state=00 duration=1732 expire=59 timeout=0 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty netflow-origin netflow-reply
statistic(bytes/packets/allow_err): org=145572/1733/1 reply=145572/1733/1 tuples=2
tx speed(Bps/kbps): 83/0 rx speed(Bps/kbps): 83/0
orgin->sink: org pre->post, reply pre->post dev=5->26/26->5 gwy=10.39.252.244/172.16.200.55
hook=post dir=org act=snat 172.16.200.55:61290->8.8.8.8:8(10.39.252.243:61290)
hook=pre dir=reply act=dnat 8.8.8.8:61290->10.39.252.243:0(172.16.200.55:61290)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
serial=00001298 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
no_ofld_reason:  non-npu-intf
total session 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NetFlow模板

模板介绍

NetFlow使用模板来捕获和分类收集到的数据流，FortiOS支持以下NetFlow模板ID（7.2.5 GA）：

模板名称	模板ID	模板描述
STAT_OPTIONS	256	发送方的统计信息
APP_ID_OPTIONS	257	应用信息
IPV4	258	非NAT IPv4流量
IPV6	259	非NAT IPv6流量
ICMP4	260	非NAT ICMPv4流量
ICMP6	261	非NAT ICMPv6流量
IPV4_NAT	262	源/目NAT IPv4流量
IPV4_AF_NAT	263	NAT46的IPv4流量
IPV6_NAT	264	源/目NAT IPv6流量
IPV6_AF_NAT	265	NAT64的IPv6流量
ICMP4_NAT	266	源/目NAT ICMPv4流量
ICMP4_AF_NAT	267	NAT46的ICMPv4流量
ICMP6_NAT	268	源/目NAT ICMPv6流量
ICMPv6_AF_NAT	269	NAT64的ICMPv6流量

模板支持参数

STAT_OPTIONS模板

Description	Statistics information about exporter
Scope Field Count	1
Data Field Count	7
Option Scope Length	4
Option Length	28
Padding	0000

Scope字段

Field #	Field	Type	Length
1	System	System (1)	2

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Data字段

Field #	Field	Type	Length
1	TOTAL_BYTES_EXP	TOTAL_BYTES_EXP (40)	8
2	TOTAL_PKTS_EXP	TOTAL_PKTS_EXP (41)	8
3	TOTAL_FLOWS_EXP	TOTAL_FLOWS_EXP (42)	8
4	FLOW_ACTIVE_TIMEOUT	FLOW_ACTIVE_TIMEOUT (36)	2
5	FLOW_INACTIVE_TIMEOUT	FLOW_INACTIVE_TIMEOUT (37)	2
6	SAMPLING_INTERVAL	SAMPLING_INTERVAL (34)	4
7	SAMPLING_ALGORITHM	SAMPLING_ALGORITHM (35)	1

APP_ID_OPTIONS模板

Description	Application information
Scope Field Count	1
Data Field Count	4
Option Scope Length	4
Option Length	16
Padding	0000

Scope字段

Field #	Field	Type	Length
1	System	System (1)	2

Data字段

Field #	Field	Type	Length
1	APPLICATION_ID	APPLICATION_ID (95)	9
2	APPLICATION_NAME	APPLICATION_NAME (96)	64
3	APPLICATION_DESC	APPLICATION_DESC (94)	64
4	applicationCategoryName	applicationCategoryName (372)	32

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPV4模板

Description	Application information
Data Field Count	17

Data字段

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
17	IP_DST_ADDR	IP_DST_ADDR (12)	4

IPV6模板

Description	No NAT IPv6 traffic
Data Field Count	17

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
17	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16

ICMP4模板

Description	No NAT IPv4 traffic
Data Field Count	16

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
16	IP_DST_ADDR	IP_DST_ADDR(12)	4

ICMP6模板

Description	No NAT ICMPv6 traffic
Data Field Count	16

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
16	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16

IPv4_NAT模板

Description	Source/Destination NAT IPv4 traffic
Data Field Count	25

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	postIpDiffServCodePoint	postIpDiffServCodePoint (98)	1
13	IP_TOS	ipClassofService (5)	1
14	DST_DOS	postIpClassOfService (55)	1
15	APPLICATION_ID	APPLICATION_ID (95)	9
16	INTERNET_APPLICATION_ID	INTERNET_APPLICATION_ID(66)	4
17	FLOW_FLAGS	FLOW_FLAGS (65)	2
18	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
19	flowEndReason	flowEndReason (136)	1
20	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
21	IP_DST_ADDR	IP_DST_ADDR (12)	4
22	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
23	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
24	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
25	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

IPV4_AF_NAT模板

Description	AF NAT IPv4 traffic (4->6)
Data Field Count	21

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
17	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
18	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
19	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

IPV6_NAT模板

Description	Source/Destination NAT IPv6 traffic
Data Field Count	21

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
17	IP_DST_ADDR	IP_DST_ADDR (12)	4
18	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
19	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

IPV6_AF_NAT模板

Description	AF NAT IPv6 traffic (6->4)
Data Field Count	21

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
17	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
18	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
19	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

ICMPV4_NAT模板

Description	Source/Destination NAT ICMPv4 traffic
Data Field Count	20

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
16	IP_DST_ADDR	IP_DST_ADDR (12)	4
17	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
18	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

ICMPV4_AF_NAT模板

Description	AF NAT ICMPv4 traffic (4->6)
Data Field Count	20

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
16	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
17	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
18	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

ICMPV6_NAT模板

Description	Source/Destination NAT ICMPv6 traffic
Data Field Count	20

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
16	IP_DST_ADDR	IP_DST_ADDR (12)	4
17	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
18	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

ICMPV6_AF_NAT模板

Description	AF NAT ICMPv6 traffic (6->4)
Data Field Count	20

Data字段

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
16	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
17	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
18	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

在VPN接口上配置NetFlow

NetFlow支持在VPN接口（如IPSec Tunnel、SSL VPN Tunnel、IP in IP Tunnel、GRE Tunnel等）以及FortiExtender接口上配置。

NetFlow配置在VPN接口上时，不会影响到NP的加速功能。

配置举例

1. 配置NetFlow collector信息后，在IPSec tunnel接口下开启NetFlow采样。

```
config system interface
    edit "A-to-B_vpn"
        set vdom "vdom1"
        set type tunnel
        set netflow-sampler both
        set snmp-index 42
        set interface "port3"
    next
end
```

2. 查看NetFlow采样的状态信息。

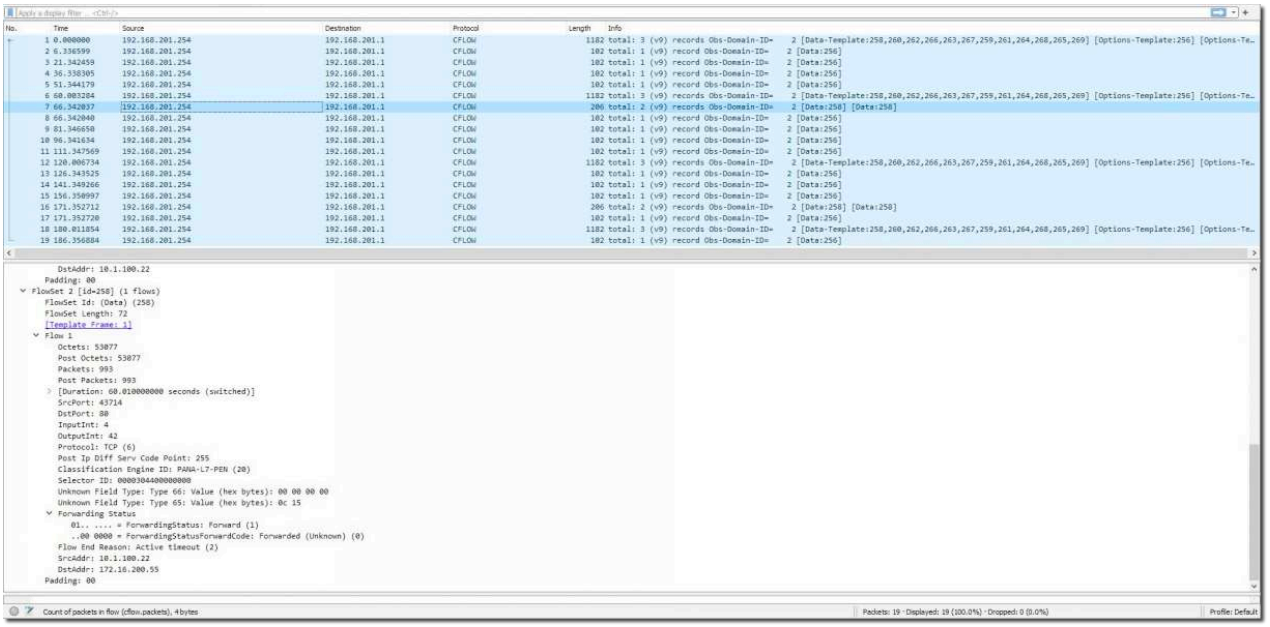
```
# diagnose test application sflowd 3
═══ Netflow Vdom Configuration ═══
Global collector:172.18.60.80:[2055] source ip: 0.0.0.0 active-timeout(seconds):60 inactive-timeout(seconds):15
___ vdom: vdom1, index=1, is master, collector: disabled (use global config) (mgmt vdom)
   |_ coll_ip:172.18.60.80[2055],src_ip:10.1.100.1,seq_num:60,pkts/time to next template: 15/6
   |_ exported: Bytes:11795591, Packets:48160, Sessions:10 Flows:34
   |___ interface:A-to-B_vpn sample_direction:both device_index:52 snmp_index:42
```

3. 查看IPSec隧道内流量相关会话的NetFlow标记。

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=6 expire=3599 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu netflow-origin netflow-reply
statistic(bytes/packets/allow_err): org=6433/120/1 reply=884384/713/1 tuples=2
tx speed(Bps/kbps): 992/7 rx speed(Bps/kbps): 136479/1091
orgin→sink: org pre→post, reply pre→post dev=10→52/52→10 gwy=10.2.2.2/10.1.100.22
hook=pre dir=org act=noop 10.1.100.22:43714→172.16.200.55:80(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.200.55:80→10.1.100.22:43714(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:0c:29:ac:ae:4f
misc=0 policy_id=5 auth_info=0 chk_client_info=0 vd=1
serial=00003b6c tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpdb_link_id=00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0×000001 no_offload
npu info: flag=0×82/0×00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0×0000/0×0000
vlifid=0/0, vtag_in=0×0000/0×0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  disabled-by-policy
total session 1
```

4. 抓包查看FortiGate向Collector发送的NetFlow流量。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

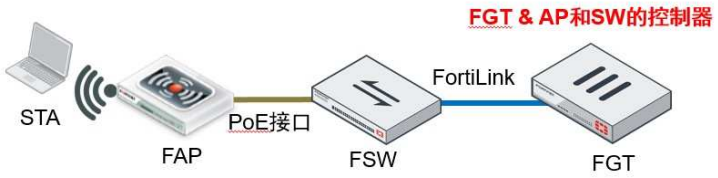


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

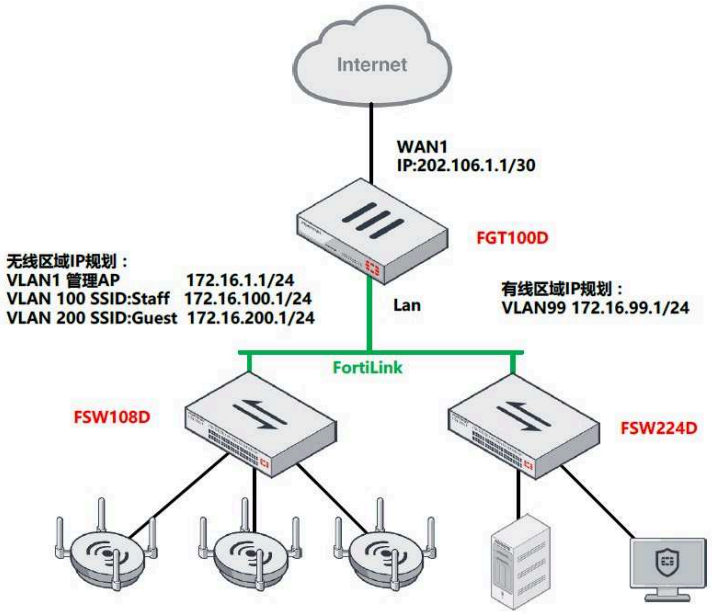
FortiLink简介

简介

1. FortiLink是防火墙和被管理的交换机之间的通讯协议。
2. Fortinet的私有协议，FortiGate基于FortiLink来管理FortiSwitch。
3. FortiLink链路承载了FortiSwitch/FortiAP和FortiGate之间的通讯报文以及用户业务数据报文（FortiLink报文 + CAPWAP控制报文 + 真实业务流量）

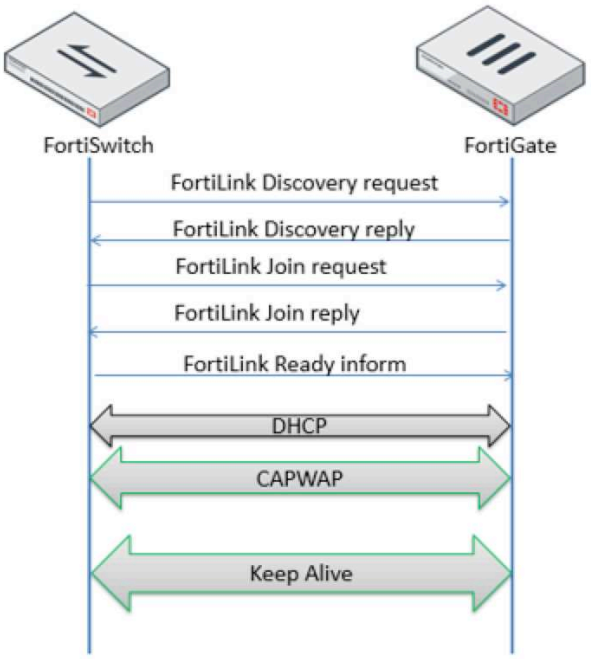


典型组网环境



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink报文交互



CAPWAP 交互过程记录（三层报文, UDP Port 5246）

Discovery:

```
FG100D3G14800154 # diagnose debug application cu_acd 255
79749.723 ==========================cuAcProcRawMsg            14  1==========================
79749.723 cuAcProcDiscoverReqMsg: received DISCOVERY_REQ from S224DF3X15000446 169.254.1.2/5246
79749.724 cuAcProcDiscoverReqMsg: sent CW_CTL_MSG_TYPE_DISCOVERY_RESP to ws (0-169.254.1.2:5246)
79749.724 ==========================cuAcProcRawMsg            14  2==========================
79749.729 ==========================cuAcProcRawMsg            14  1==========================
```

Join:

```
79749.822 cuAcProcPlainCtlMsg: received JOIN_REQ from ws (0-169.254.1.2:5246)
79749.822 AC_EV_GEN - CWAE_JOIN_REQ_RECV me 0x1501d2b0 ws ws (0-169.254.1.2:5246)
79749.825 CUAS_JOIN_enter: sending JOIN RESP msg.
```

Run:

```
79752.513 FSM: old CWAS_DATA_CHECK(10) ev CWAE_DATA_CHECK_TIMER_EXPIRE(33) new CWAS_RUN(11)
79752.513 cu_set_managed_switch_state
79752.513 cu_set_managed_switch_state managed-switch S224DF3X15000446
```

Keep Alive（FGT侧）

FGT对于FortiLink状态的健康，FGT和FSW各自使用不同的Keep alive机制, FGT使用基于CAPWAP机制的Keep Alive，FGT 每30秒发送一次REQ_MSG给FSW, 如果没有收到RSP, 则重传6次,如果重传6次都没有成功, 则认为FSW掉线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FG100D3G14800154 # diagnose debug application cu_acd 255
82790.513 cuAcSendPoeGeneralStatsReq wtp general poe stats request
82790.513 cuAcSend_REQ_MSG: sending  (31) msg.
82790.513 cuAcSendRawMsgQueue: SENDING OUT type 31 seqNum 3

82793.513 cuAcSendPendingMsg: for ws (0-169.254.1.2:5246)... 31 3 0 82790 82793
82793.513 cuAcSendPendingMsg: RESENDING Msg type 31 seqNum 3 retransmitCnt 0.
.................
82859.514 cuAcSendPendingMsg: for ws (0-169.254.1.2:5246)... 31 3 6 82859 82859
82859.514 cuAcSendPendingMsg: Msg type 31 seqNum 3 send failure. MaxRetry is reached.

82859.515 FSM: old CWAS_RUN(11) ev CWAE_MAX_RRTRANSMIT_REACHED(21) new CWAS_DTLS_TD(6)
82859.515 cu_set_managed_switch_state
82859.515 cu_set_managed_switch_state managed-switch S224DF3X15000446
```

Keep Alive（FSW侧）

FSW对于 FortiLink状态的健康检查：

1. FSW会实时监控Fortilink的物理端口状态, 如果端口down, 则FSW认为FortiLink down。

```
S224DF3X15000446 # diagnose debug application fortilinkd 255

448s:942ms:1us fl_node_rec_scan[2356]:connected to controller
449s:152ms:756us flp_event_handler[1120]:node: port24 received event FL_EV_ECHO_TIMEOUT state FL_STATE_READY
449s:213ms:580us flp_event_handler[1120]:node: port24 received event FL_EV_RECV_ECHO_REPLY state FL_STATE_READY
449s:214ms:176us flp_event_handler[1120]:node: port24 received event FL_EV_ECHO_REPLY_VALID state FL_STATE_READY
452s:161ms:286us flp_event_handler[1120]:node: port24 received event FL_EV_ECHO_TIMEOUT state FL_STATE_READY
452s:201ms:355us flp_event_handler[1120]:node: port24 received event FL_EV_RECV_ECHO_REPLY state FL_STATE_READY
452s:201ms:940us flp_event_handler[1120]:node: port24 received event FL_EV_ECHO_REPLY_VALID state FL_STATE_READY

505s:766ms:155us fl_node_rec_scan[2363]:not connected to controller
506s:76ms:152us flp_event_handler[1120]:node: port24 received event FL_EV_DISC_TIMEOUT state FL_STATE_DISC
507s:426ms:644us flp_event_handler[1120]:node: internal received event FL_EV_DISC_TIMEOUT state FL_STATE_DISC
509s:77ms:514us flp_event_handler[1120]:node: port24 received event FL_EV_DISC_TIMEOUT state FL_STATE_DISC
510s:453ms:208us flp_event_handler[1120]:node: internal received event FL_EV_DISC_TIMEOUT state FL_STATE_DISC
512s:86ms:133us flp_event_handler[1120]:node: port24 received event FL_EV_DISC_TIMEOUT state FL_STATE_DISC
513s:436ms:182us flp_event_handler[1120]:node: internal received event FL_EV_DISC_TIMEOUT state FL_STATE_DISC
```

2. FortiLink down后，FSW会继续尝试与FGT建立FortiLink，每3秒发送一次FortiLink Discovery报文，如果由于链路原因没有收到FGT返回的应答，FSW默认有一个30秒的超时时间，超过此时间，则FSW认为FortiLink down。FSW会继续尝试与FGT建立FortiLink，重复FSW上线过程，包括重新CAPWAP协商。

3. FSW对于CAPWAP的监控：

   - switch 每30秒发送一次echo request 并等待echo response
   - 如果连续10个echo 没有response, 则重置CAPWAP状态,交换机认为自己掉线,即capwap超时时间300秒
   - 每次FortiLink重新建立后, 如果当前CAPWAP状态为RUN,会重新开始CAPWAP进程

```
fl_node_set_controller_info[2303]:fl_node_set_controller_info:restaring capwap
```

FortiLink中断检测过程

1. FSW继续使用当前的配置工作，本地转发的数据继续转发。
2. 如果此时重启FSW，FSW重启后会继续使用重启之前的配置工作，本地转发的数据继续转发。
3. 如果FSW在与FGT断了后，被别的FGT发现并授权，此时FSW不会再重启,但会丢弃之前在旧FGT上获得的配置，重新从新的FGT上获取配置。这种情况下，FSW从一个FGT手动切换到另外一个FGT上，最好先清一下配置。
4. 如果FSW掉线后，在FSW上如果又修改了配置后，在FSW重新上线后，FGT会重新下发配置，之前在FSW上修改的配置会被丢弃。

其他

官方参考配置文档：

https://docs.fortinet.com/document/fortiswitch/7.0.8/devices-managed-by-fortios/ ↗

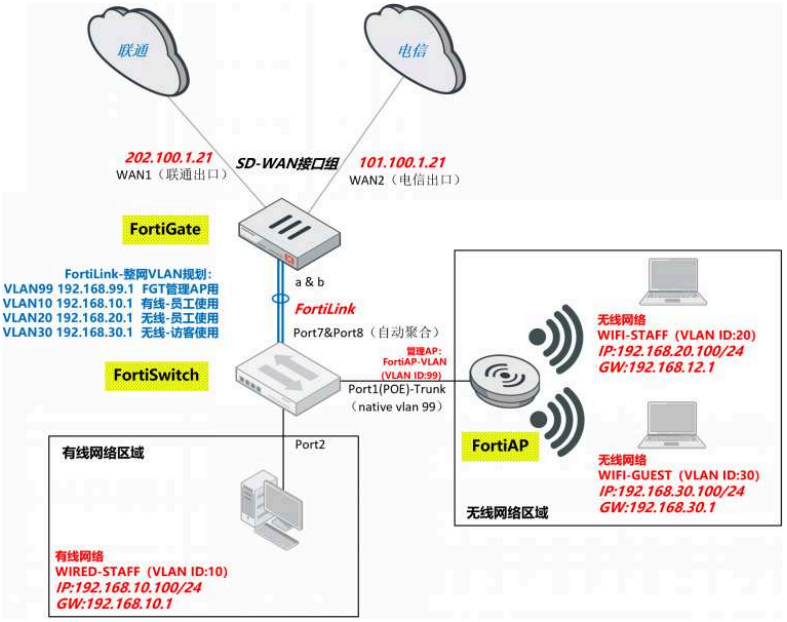
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink简要上线指南

网络需求

1. SAA（Secure Access Architecture）是Fortinet针对中小企业推出的有线无线一体的安全解决方案，包括有线无线设备的接入和认证，通过防火墙来统一管理网络中的有线和无线设备，并且有线交换机和无线AP都是即插即用，非常方便易用。
2. 如果再加入SD-WAN的部分可以组成叫SD-WAN Branch的方案。

网络拓扑



1. 一个最简单的FortiLink部署环境：一台防火墙+一台FortiSwtich+一台FortiAP，通过FortiLink非常便捷的实现一个通过FGT统一管理的可视化的有线+无线的安全网络。
2. 整体规划：
   - 外网IP网段规划：
     - WAN1联通出口：IP 202.100.1.21，GW 202.100.1.192
     - WAN2电信出口：IP 101.100.1.21，GW 101.100.1.192
   - WAN1和WAN2合并成SD-WAN接口。
   - 内网IP网段规划，FGT通过FortiLink+Capwap协议统一的接管FortiSW和FortiAP，为有线和无线统一进行管理和业务处理：
     - 有线网络规划：VLAN 10，192.168.10.1
     - 无线网络规划：员工WIFI VLAN 20，192.168.20.1
     - 无线网络规划：访客WIFI VLAN 30，192.168.30.1
     - 管理FortiAP：VLAN 99，192.168.99.1
   - FortiLink互联部分规划：
     - FortiGate的a和b做聚合接口与Fortiswitch的后两个接口互联即可实现聚合接口的FortiLink管理。
     - 加入FortiLink的接口自动变为聚合口成员。

配置步骤

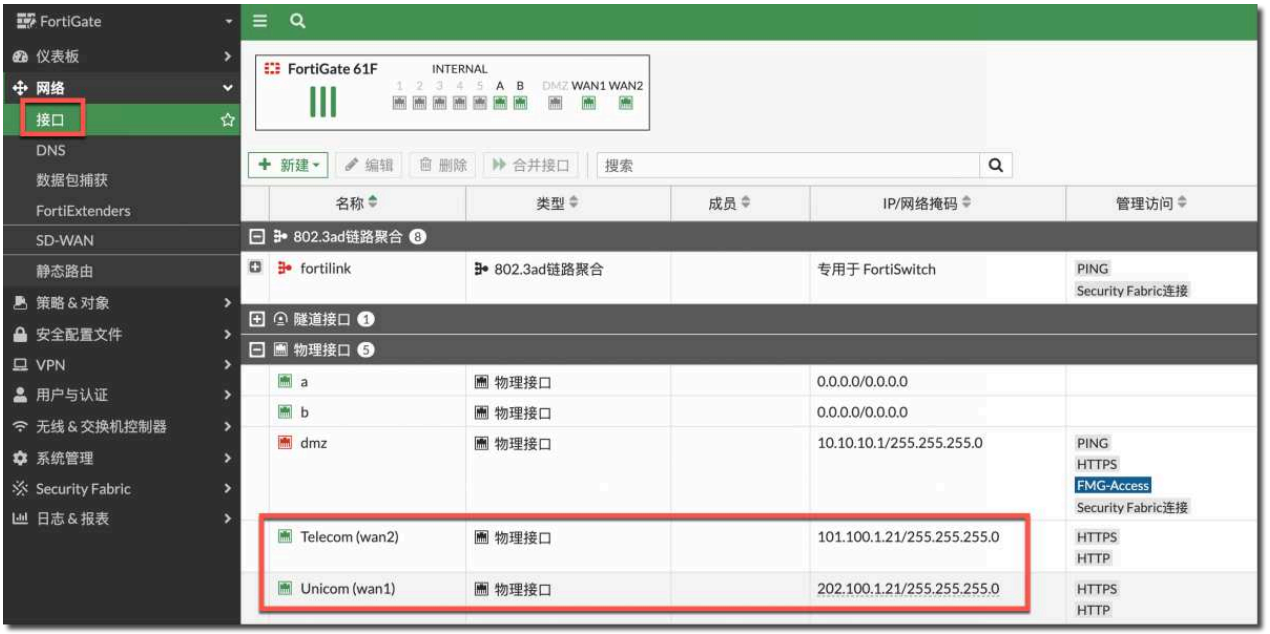
准备事项

1. 首先确认FortiGate如下全局配置已开启（一般默认为开启状态）。

```
config system settings
    set gui-switch-controller enable
end
```

2. 配置wan1和wan2的IP地址。

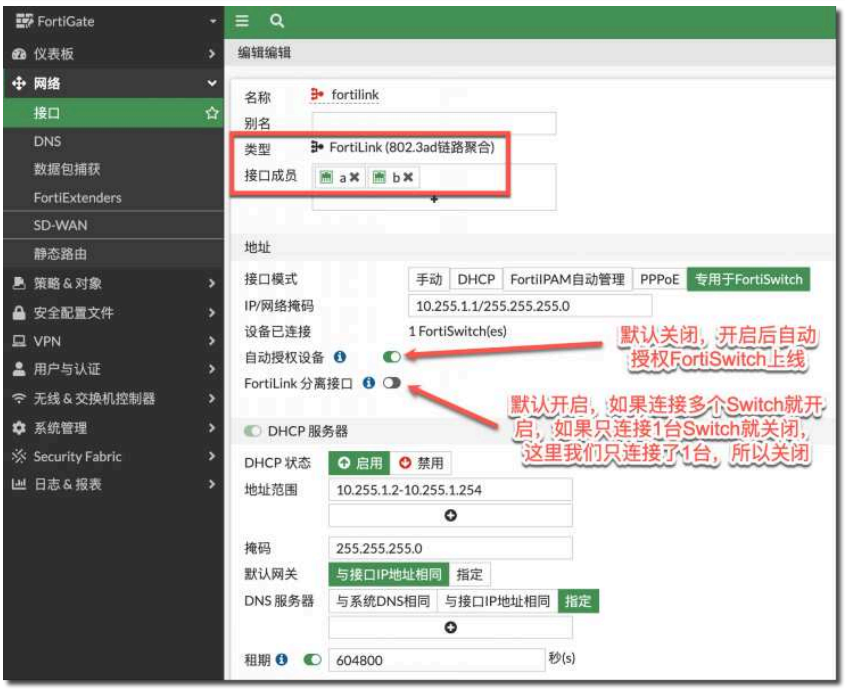
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置FortiLink实现FortiSwith上线，我们只需要将用于FortiLink的成员接口加入FortiLink接口即可。此拓扑中，FortiGate用于连接FortiSwitch的接口为a和b，编辑FortiLink接口，将a和b加入FortiLink（某些产品型号会默认将两个接口加入FortiLink），开启自动授权设备，关闭FortiLink分离接口，其他配置保持默认，可以看到FortiLink为一个聚合接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

FortiLink分离接口什么时候应该开启?

分离接口的意是，如果聚合接口的port1和port2分别连接了一台SW，在没有使用MCLAG的情况下（没开启堆叠功能），则聚合接口的port1和port2没办法同时UP（同时开启聚合接口无法正常工作），因此必须开启FortiLink分离接口功能，让聚合接口只有一个物理接口（port1）是处于UP状态的，另外一个物理接口（port2）处于DOWN的备份状态，当port1接口状态DOWN，则Port2立即接管Port1的工作，让聚合接口的FortiLink继续运行，这是一个聚合接口在FortiLink管理时候的备份机制。



重要

FortiLink split interface 什么时候应该disable?

如果FGT的聚合接口只接到了一台交换机上，并没有跨交换机聚合（没有MCLAG，也不需要FortiLink split interface），因此这种情况应该让聚合接口的两个物理接口port1和port2同时UP，两个接口同时工作起来，以便提供更高带宽和备份的作用。



相关CLI:

```
NTP:
config system ntp
    set ntpsync enable
    set server-mode enable
    set interface "fortilink"
end
------------------------------------------------------------------
DHCP:
config system dhcp server
    edit 2
        set dns-service local
        set ntp-service local
        set default-gateway 10.255.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.255.1.2
                set end-ip 10.255.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end
────────────────────────────────────────────────────────────────────────
FortiLink:
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "a" "b"
        set lldp-reception enable
        set lldp-transmission enable
        set auto-auth-extension-device enable
        set fortilink-split-interface disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
    next
end
```

连接FortiLink

1. 配置完FortiGate之后，这个时候再去接FortiGate的FortiLink到FortiSwitch的线，以及FortiSwitch之间的线，严格按照拓扑图，从核心交换机往接入交换机这样的顺序接线。FortiSwitch如果以前有使用过，建议都恢复一下出厂设置，然后再加入到FortiLink。

2. FortiSwitch的靠后接口一般都默认开启了FortiLink接口属性，如果接前面的接口可能会无法加入到FortiLink，因此FortiSwitch的FortiLink最好都使用靠后的接口进行接线。FortiSwitch各型号默认开启FortiLink功能的接口如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiSwitch型号	默认开启FortiLink的接口
FS-108D-POE	port9–port10
FS-108E, FS-108E-POE, FS-108E-FPOE	port7–port10
FSR-112D-POE	port5–port12
FS-124D, FS-124D-POE	port23–port26
FSR-124D	port1-port4, port21–port28
FS-124E, FS-124E-POE, FS-124E-FPOE	port21–port28
FS-148E, FS-148E-POE	port21–port52
FS-224D-POE	port21–port24
FS-224D-FPOE	port21–port28
FS-224E, FS-224E-POE	port21–port28
FS-248D, FS-248D-FPOE	port45–port52
FS-248D-POE	port47–port50
FS-248E-POE, FS-248E-FPOE	port45–port52
FS-424D, FS-424D-POE, FS-424D-FPOE	port23–port26
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30
FS-548D	port39–port54
FS-548D-FPOE, FS-548DN	port45–port54
FS-1024D	port1–port24
FS-1048D, FS-1048E	port1–port52
FS-3032D, FS-3032E	port1–port32

3. 如果FortiSwitch无法被FortiGate管理，登陆到FortiSwitch上进行确认接口是否开启了FortiLink。

```
FortiSwitch # show switch interface port9
config switch interface
    edit "port9
        set auto-discovery-fortilink enable    //接口下又此命令的接口才可以自动加入到FortiLink中
    next
end
```

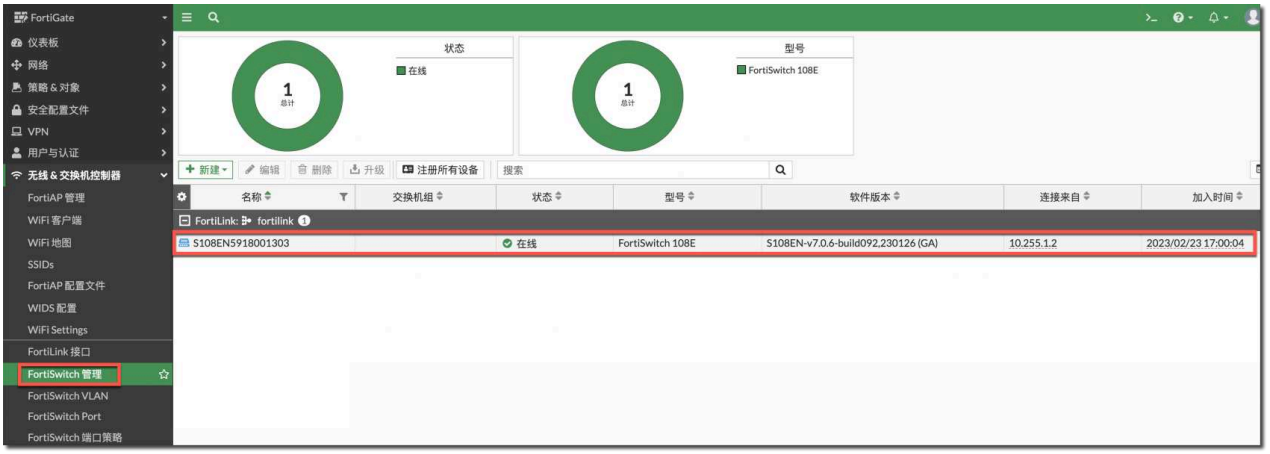
4. 交换机之间如果接多根线，会自动进行聚合，但是FortiLink自动聚合会花比较长的时间，建议可以先接单线，等FortiLink的拓扑较快的形成结束之后，再增加彼此之间的另外一根线，再进行自动聚合，这样效率会比较高一些。

5. 接线是很重要的步骤，仔细看拓扑图，做好接口标签，不要接错。

6. 接好线之后，FortiSwitch和FortiGate之间会自动在后台进行FortiLink、CAPWAP、MSTP、聚合接口的协商加入等操作，等FortiLink的管理结束之后，在FortiGate上会看到一个网站的FortiSwitch拓扑图，和我们规划的拓扑图应该是一致的，可以仔细核对接线是否正确。

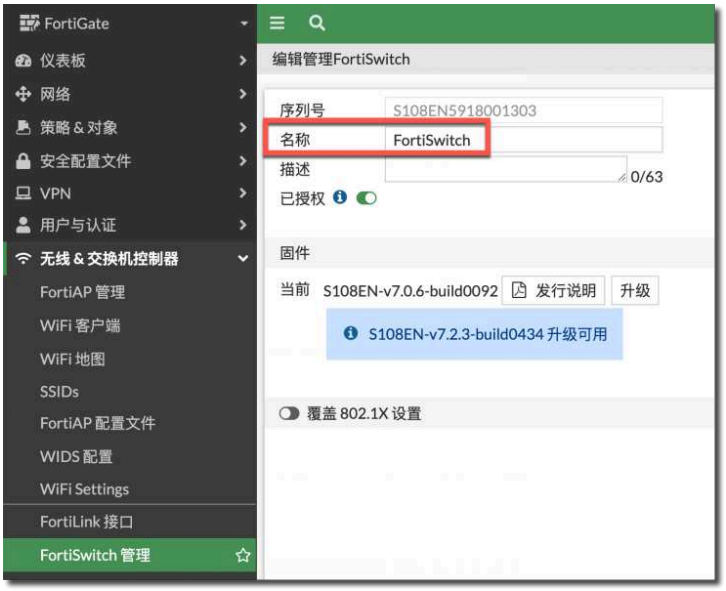
7. 在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，查看交换机被管理状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 交换机加入到FortiGate的FortiLink，会先清除配置再重启，然后从standalone的状态进入到“Fortilink remote control”的状态，后续所有的配置都通过FortiGate下发即可。

9. 编辑该交换机，可以修改交换机名字以及升级版本，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

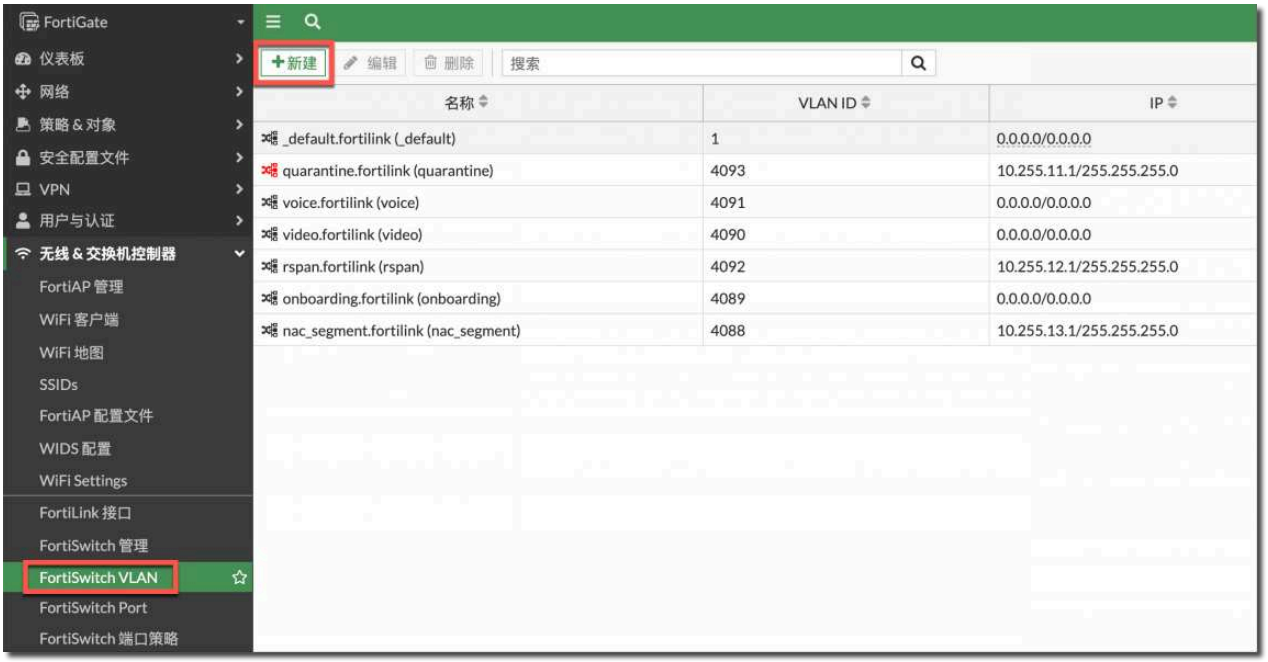


创建VLAN

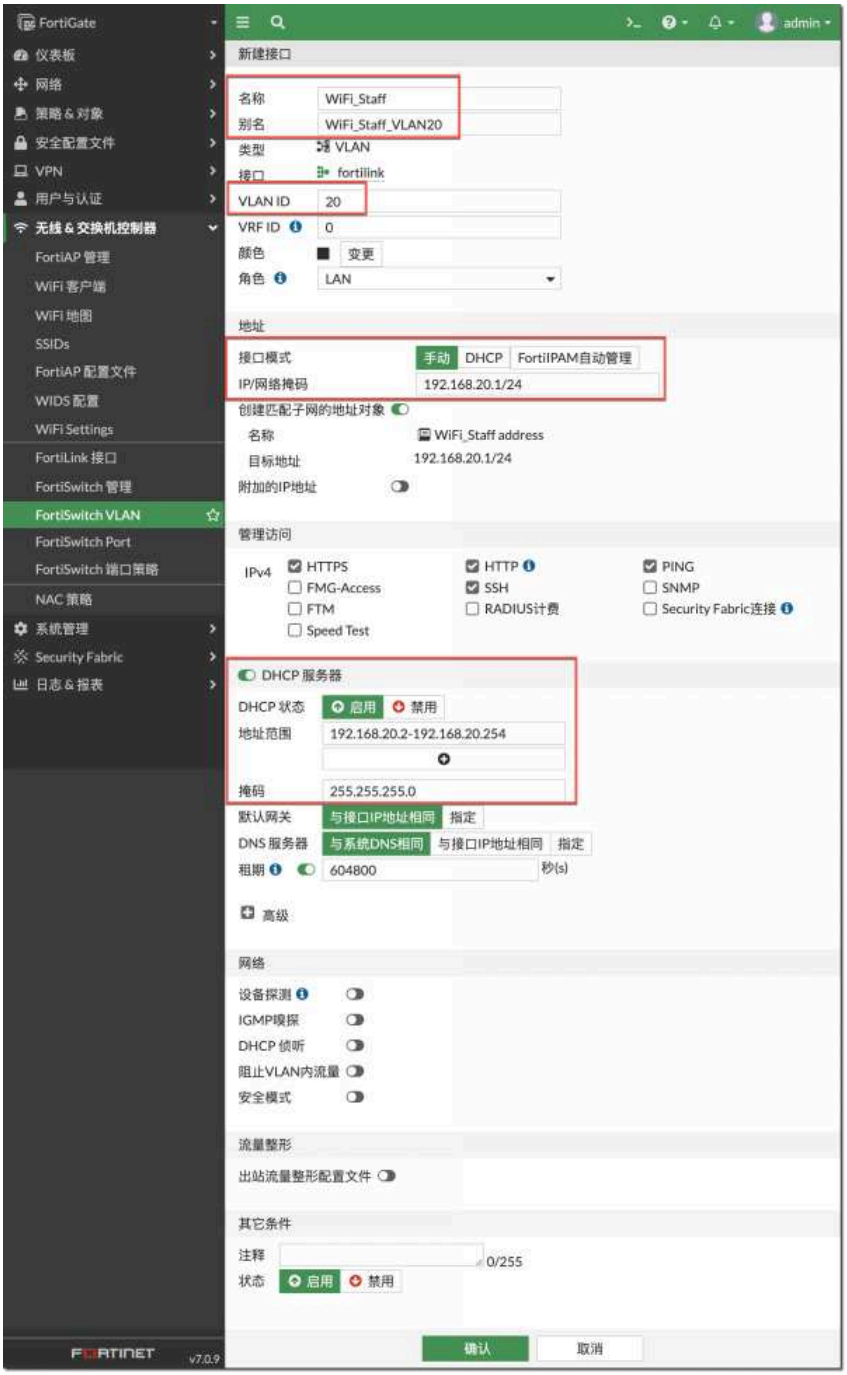
1. FortiGate通过FortiLink + Capwap协议统一的接管FortiSwitch和FortiAP，为有线和无线统一进行管理和业务处理。

2. 进入FortiGate的无线&交换机控制器→FortiSwitch VLAN页面，新建有线网络VLAN 10、员工无线网络VLAN 20、访客无线网络VLAN 30、管理FortiAP VLAN 99。注意管理FortiAP的VLAN接口要开启Security Fabric，包含CAPWAP。

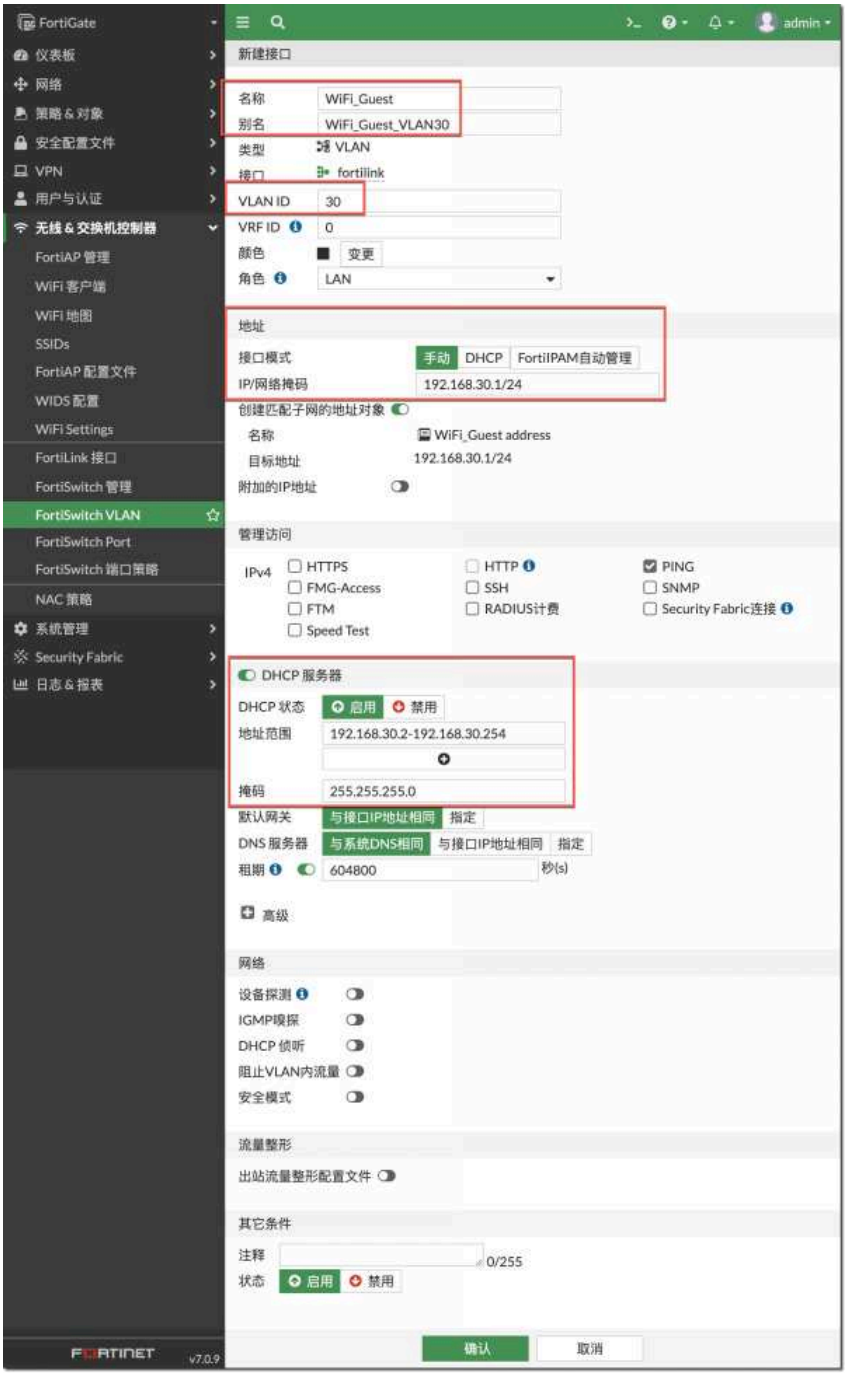
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



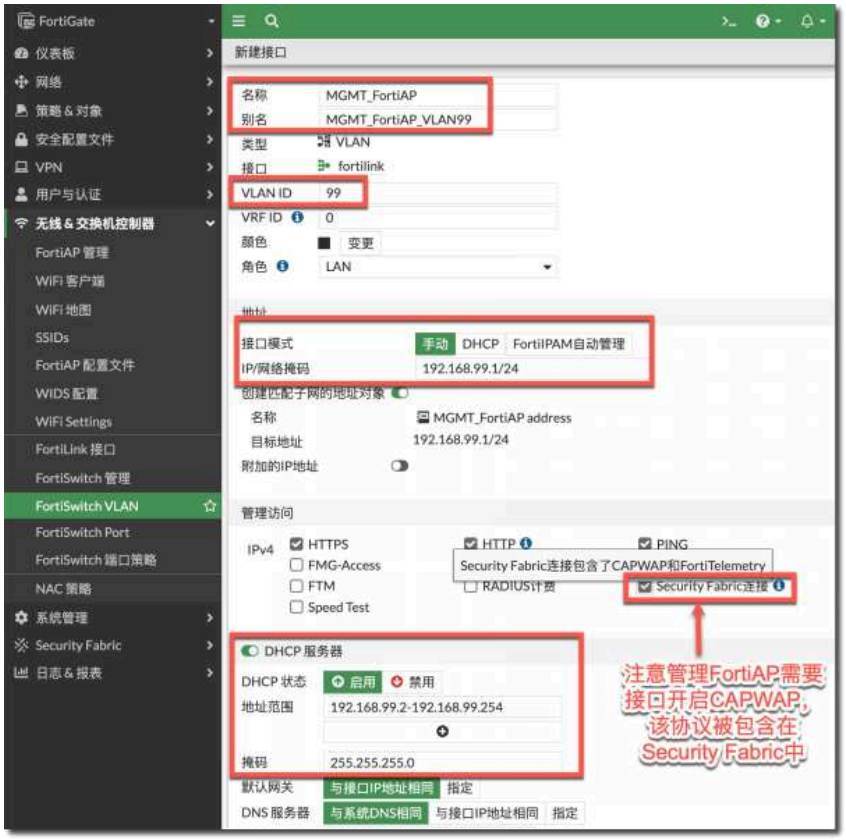
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. VLAN创建完成。

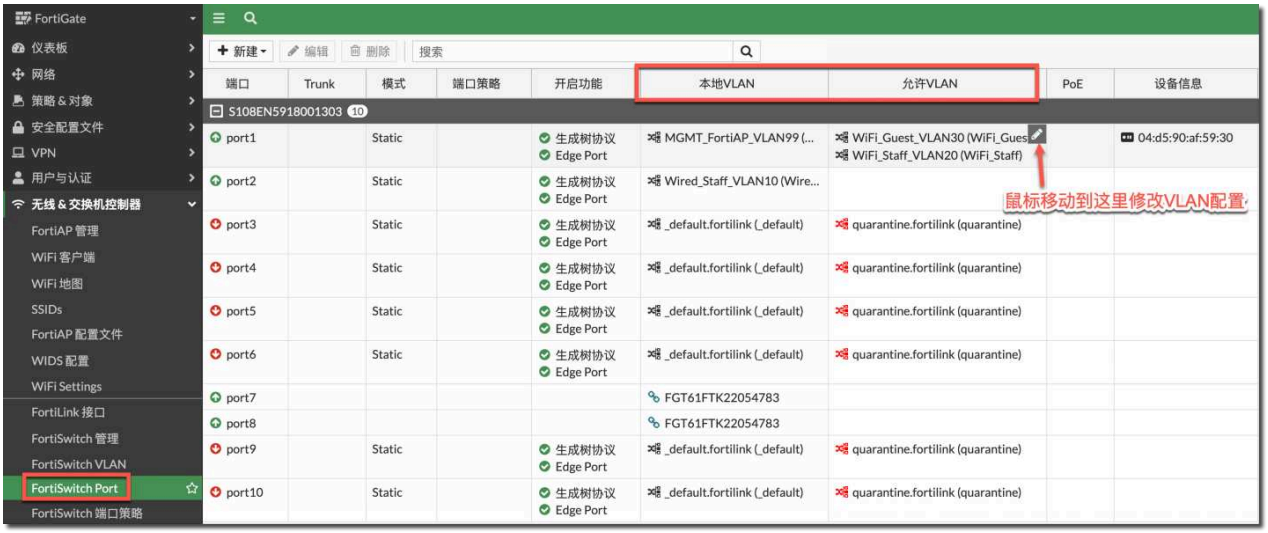


分配VLAN

1. 交换机的port1接FortiAP，配置为Trunk模式，允许 VLAN20和VLAN30，VLAN20用于WIFI-STAFF的SSID用户，VLAN30用于WIFI-GUEST的SSID用户。另外本地VLAN设置为VLAN 99，用于FortiAP的管理（FortiAP的管理相当于使用不打vlan-tag的VLAN 99，本地VLAN默认是VLAN 1，因此只需要将本地VLAN设置为VLAN 99即可）。

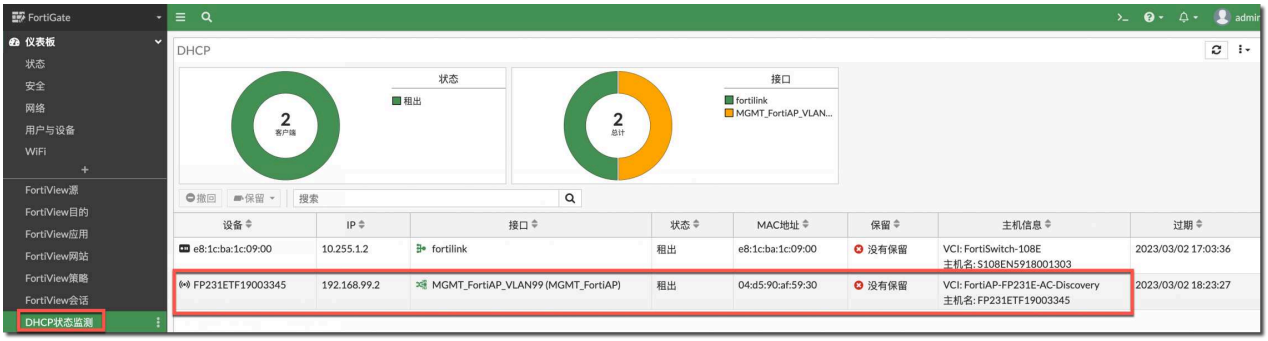
2. Port2接具体的物理PC，因此只需要将Port2设置为access口，分配VLAN 10即可，用FortiSwitch的概念来说就是将本地VLAN设置为VLAN 10，本地VLAN不打vlan-tag，相当于就是设置接口为access vlan 10。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

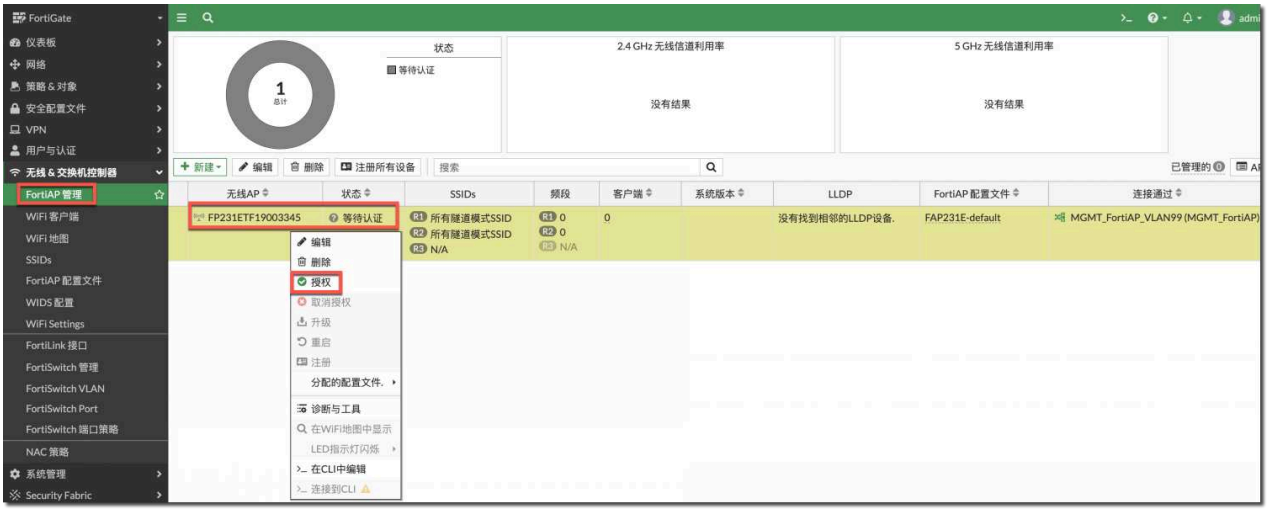


无线配置

1. FortiAP连接后，会通过VLAN 99的DHCP获取到192.168.99.0/24网段的IP地址。



2. 在之前的配置中，VLAN 99的接口开启了CAPWAP协议（包含在Security Fabric中），激活了FortiGate的无线管理功能，这时候FortiAP会自动找到FGT进行注册。因此在FortiAP管理的地方可以看到这个FortiAP的信息（如果没有看到检查配置，并将FortiAP恢复出厂，让FortiAP重新获取IP地址并发起注册）。



3. 右键点击上图中等待认证的FortiAP，点击授权按钮，等待几分钟，FortiAP成功上线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 编辑FortiAP设置，配置FortiAP的名称，或进行升级操作。

5. 进入无线&交换机控制器→SSIDs页面，点击新建按钮。

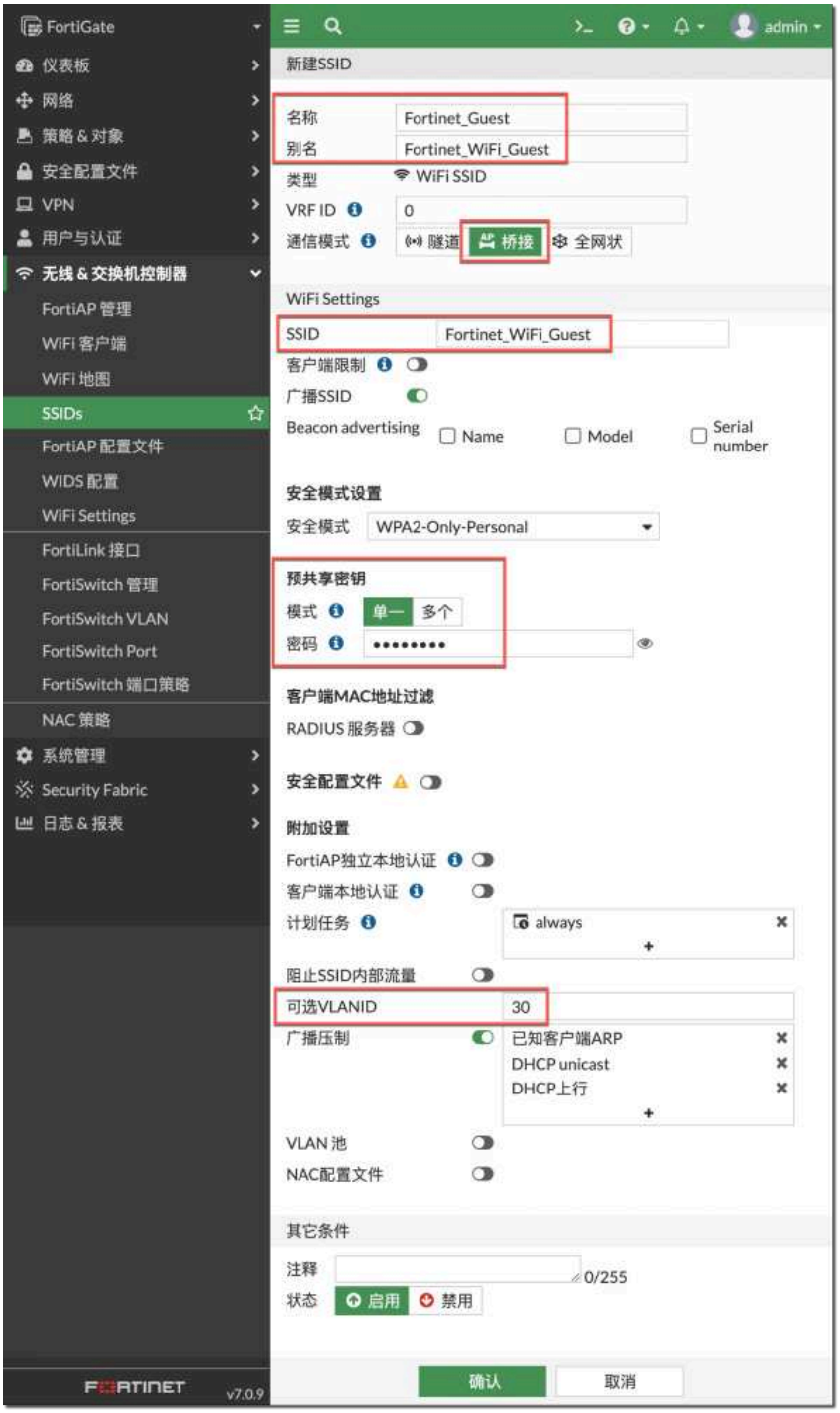


6. 新建SSID：Fortinet_WiFi_Staff VLAN 20用于员工WIFI使用，Fortinet_WiFi_Guest VLAN 30用于访客WiFi使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





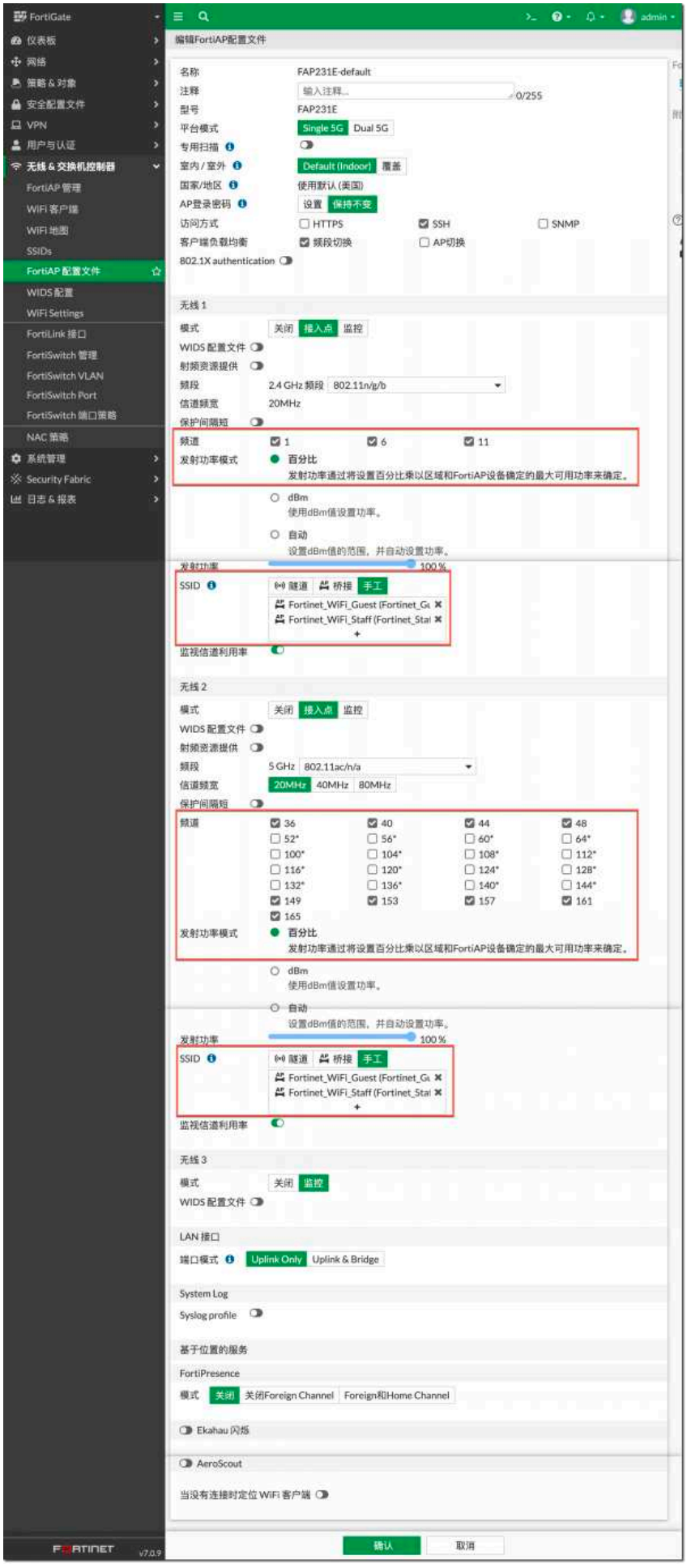
7. 将SSID关联到FortiAP上，然后让FortiAP发布无线SSID信号，这样用户就可以通过SSID连接到无线了。进入FortiAP配置文件页面，编辑FortiAP关联的配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 桥模式的SSID需要在FortiAP配置文件里面手工指定一下，另外下图标示出的配置为推荐配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

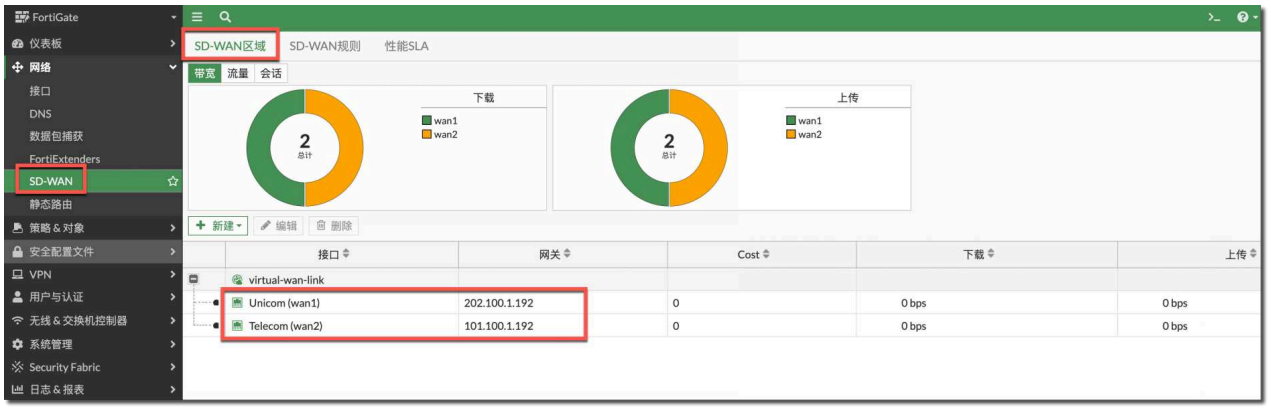


9. FortiAP会自动关联到这个FortiAP配置文件里面的内容，发起SSID的信号。



SD-WAN配置

1. 将wan1和wan2加入SD-WAN接口，并配置各自的网关。

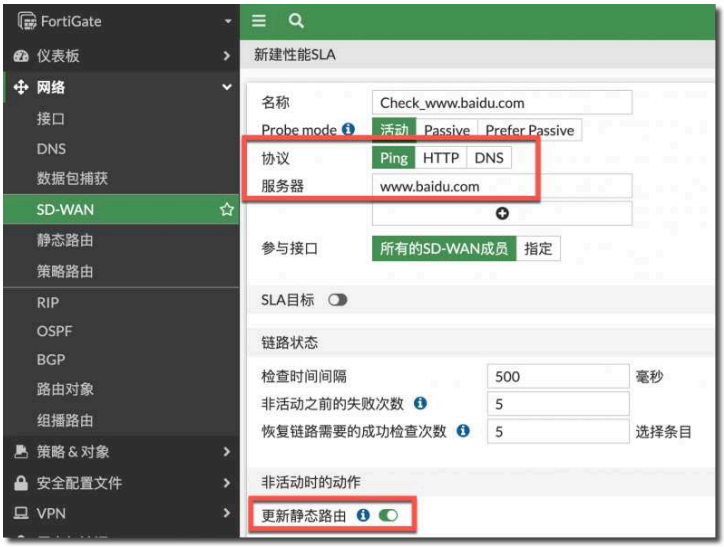


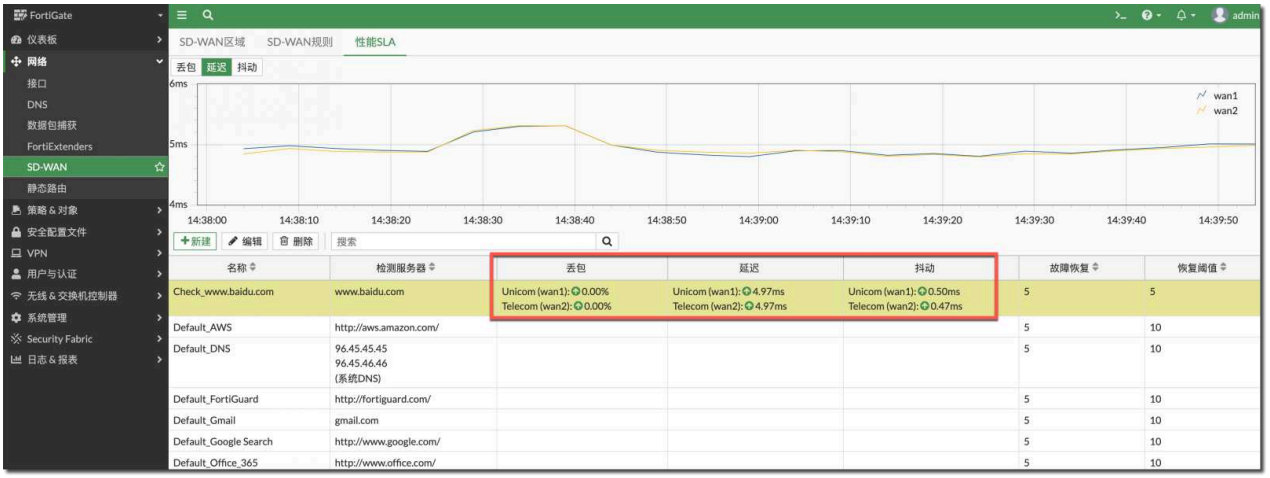
2. 添加SD-WAN的默认路由。



3. 配置SD-WAN的SLA，以便wan1和wan2相互备份和切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. SD-WAN规则可根据需求配置，这里保持默认的按照源IP负载均衡。



安全策略配置

1. 需求与规划：

   - 员工的有线与无线都需要访问互联网
   - 访客的无线仅仅可以访问互联网
   - 员工的有线和无线需要互访

2. 建议将防火墙的接口划分区域，以区域的方式配置策略，有时候可以做到简化配置的目的，甚至未来替换设备的时候，策略的备份和还原也会更加简单一些。规划区域两个区域：

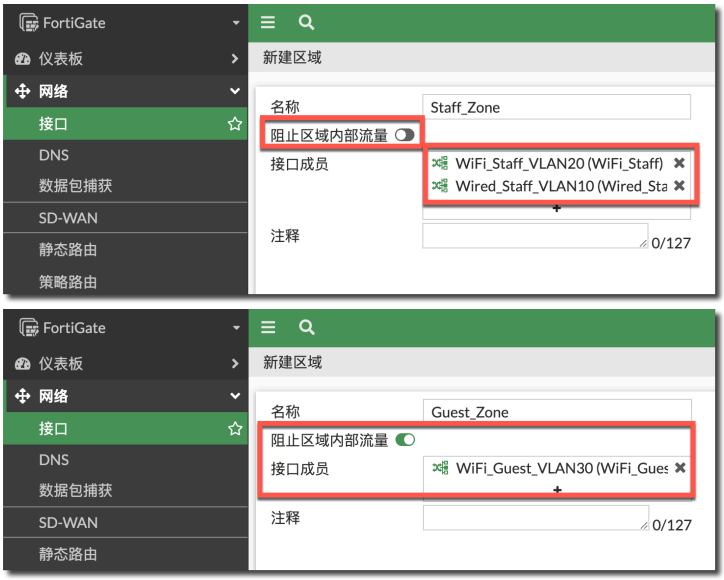
   - 员工网络区域：包括员工的有线VLAN 10和员工的无线VLAN 20 （区域之间的隔离关闭，这样VLAN 10和VLAN 20之间的数据可通）
   - 访问网络区域：包括访问的无线VLAN 30

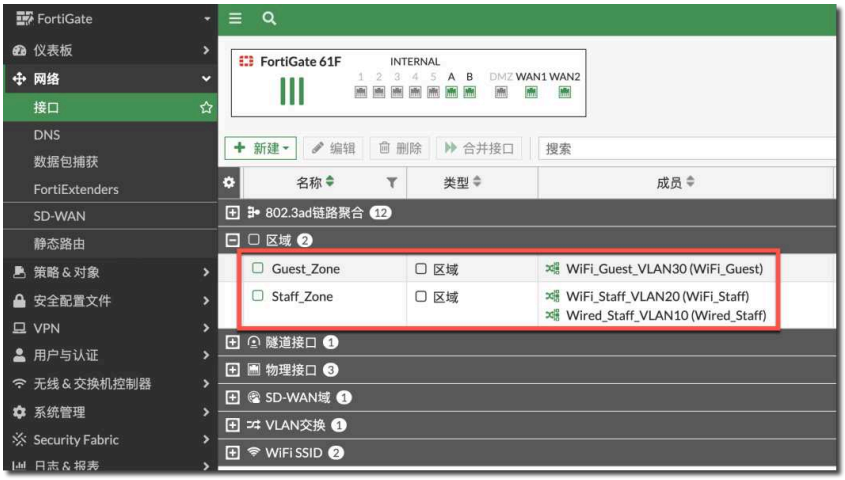
3. 进入网络→接口页面，新建所属区域。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 分别创建Staff_Zone（包含VLAN 10和VLAN20）和Guest_Zone（包含VLAN30）。





5. 如此只需要配置两条策略，就可以实现我们规划的需求，新建Staff-Zone到SD-WAN与Guest-Zone到SD-WAN的安全策略。

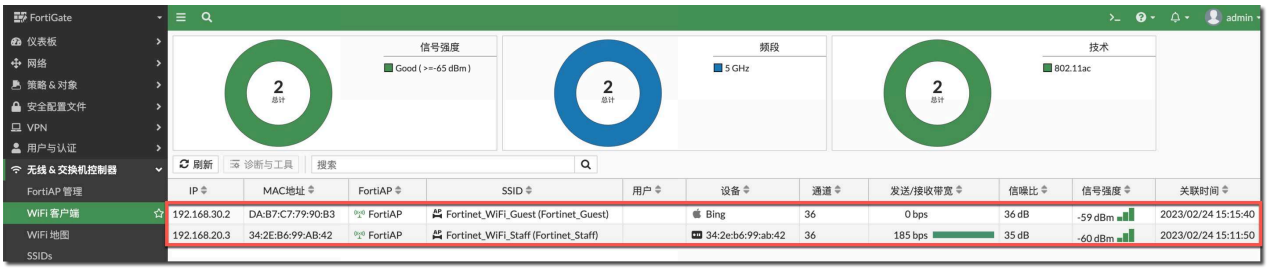
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



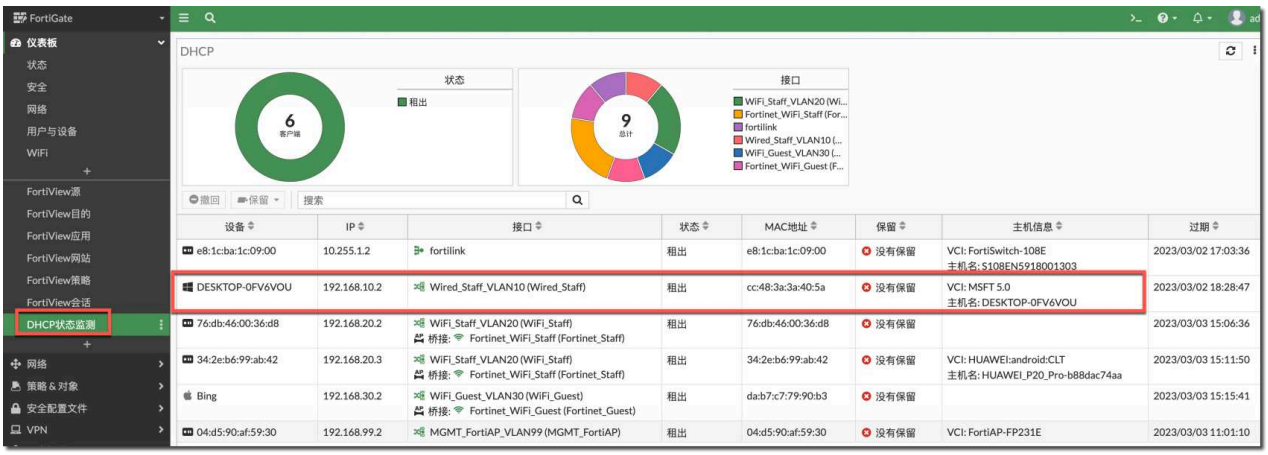
结果验证

客户端访问

1. 进入无线&交换机控制器→WiFi客户端，查看在线的无线客户端。可以看到WiFi_Staff和WiFi_Guest各有一个终端在线。



2. 在DHCP状态检测中查看所有的客户端信息，可以看到有线网络的PC也正常上线。

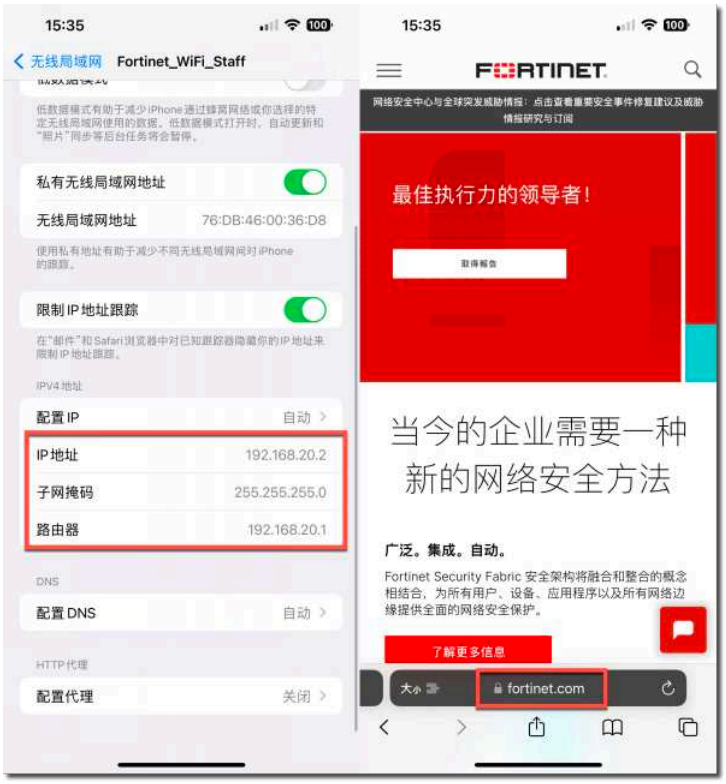


3. 有线网络（VLAN 10）用户访问互联网。

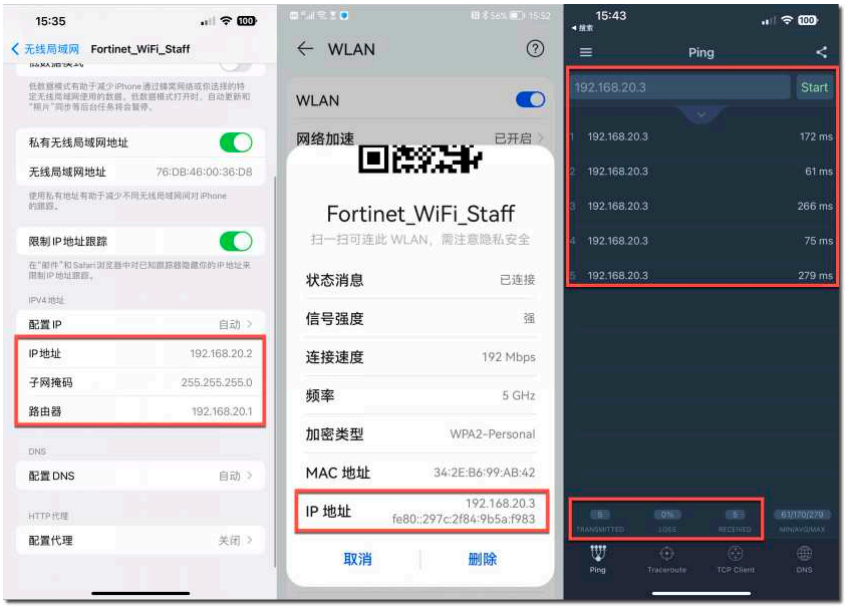


4. 无线网络用户访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

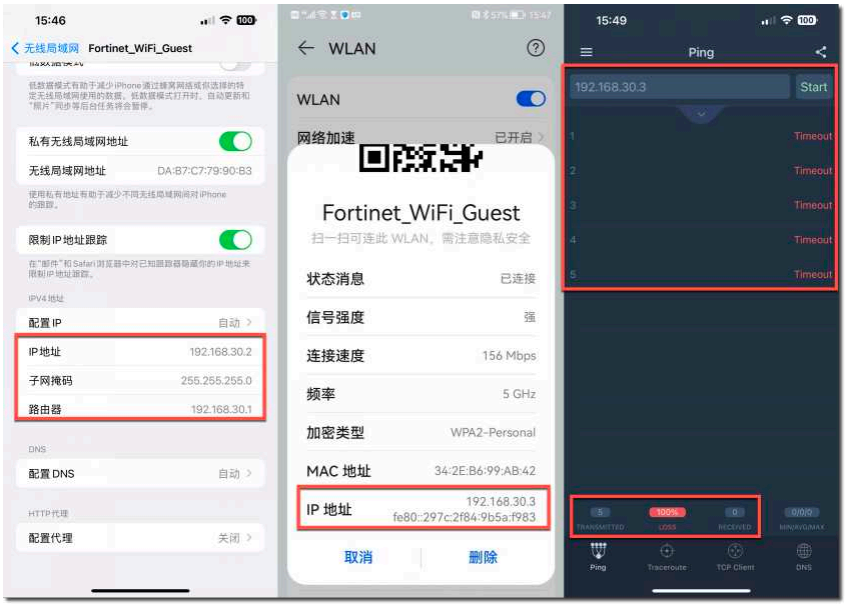


5. 使用VLAN 20下的客户端访问VLAN 20下的另一个客户端（Staff区域）。



6. 使用VLAN 30下的客户端访问VLAN 30下的另一个客户端（Guest区域），可以看到由于该区域配置了禁止相互访问，所以VLAN 30下的客户端是无法互相访问的。

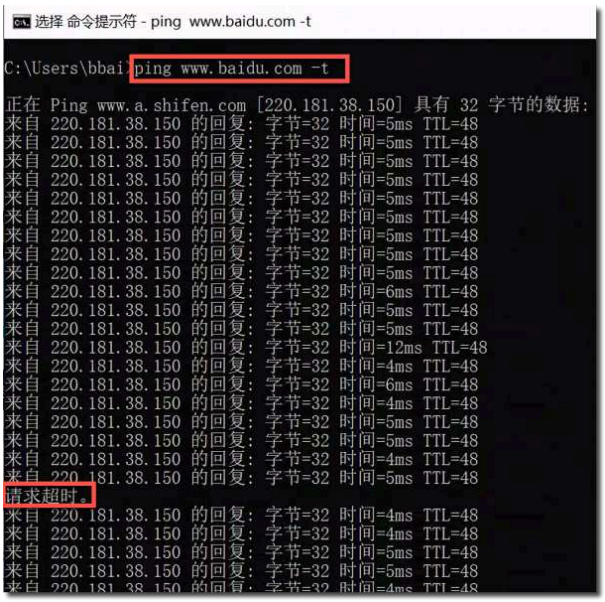
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



切换测试

1. 在我们的测试场景下FortiLink聚合接口的a和b是同时UP起来的，如果a或b DOWN（不能同时DOWN），是否有影响业务呢?

2. 经过测试，DOWN a或b接口，客户端丢包1个或者不丢包。

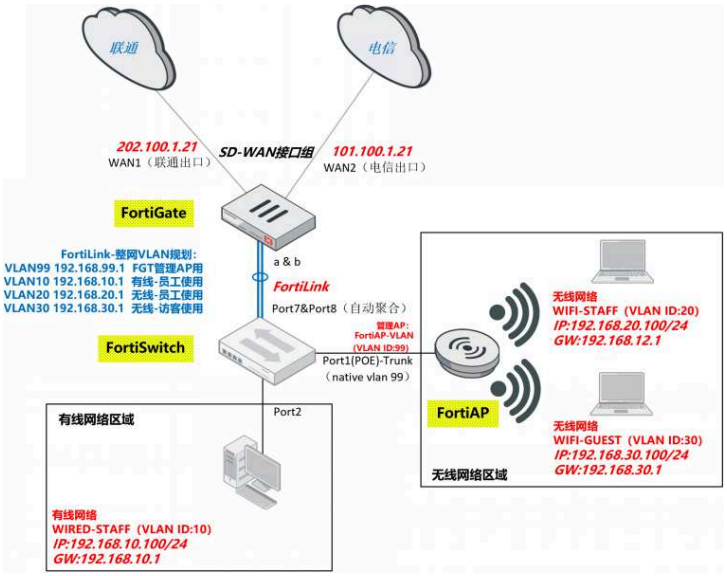


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink星型组网

通过简要上线指南中的拓扑，来说明星型组网部署方案。

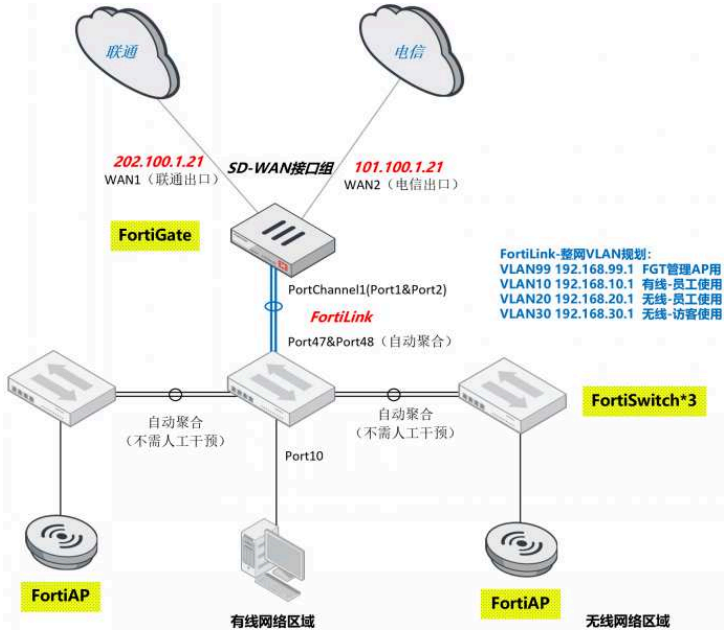
简要上线指南拓扑



星型拓扑

改造方案一

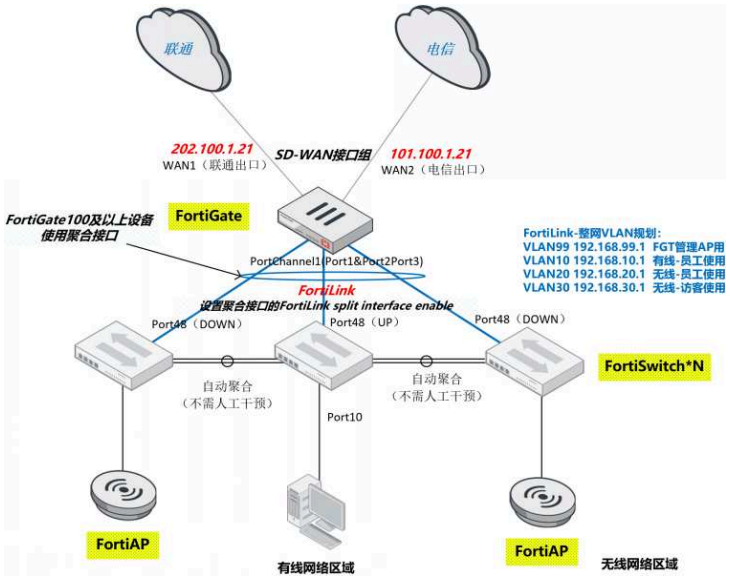
1. 接入交换机直接串联到核心交换机上的FortiLink部署。
2. 这种方案比较简洁，容易理解，存在的问题：核心交换机存在单点故障风险，一旦核心交换机出现故障（比如断电），整网将全部中断。



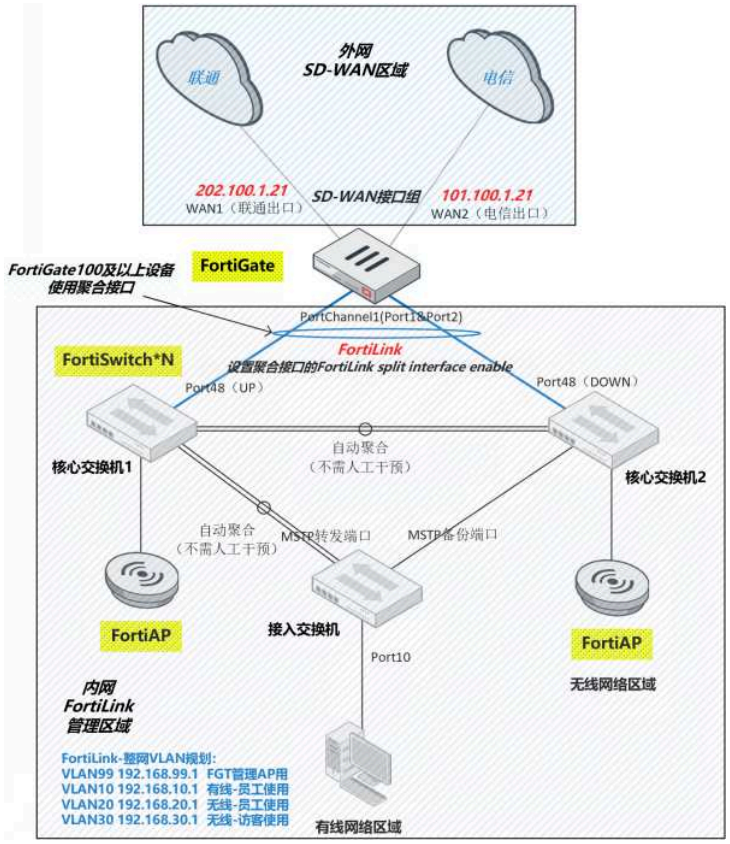
改造方案二

1. 交换机串联，FortiGate使用“FortiLink split interface”特性互联到每一台FortiSwitch核心交换机上。
2. 使用聚合接口并利用“FortiLink split interface”，将防火墙的聚合接口分别接到三台交换机上，但是正常情况下只有接核心交换机的接口是UP的，其他的接口处于备份状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

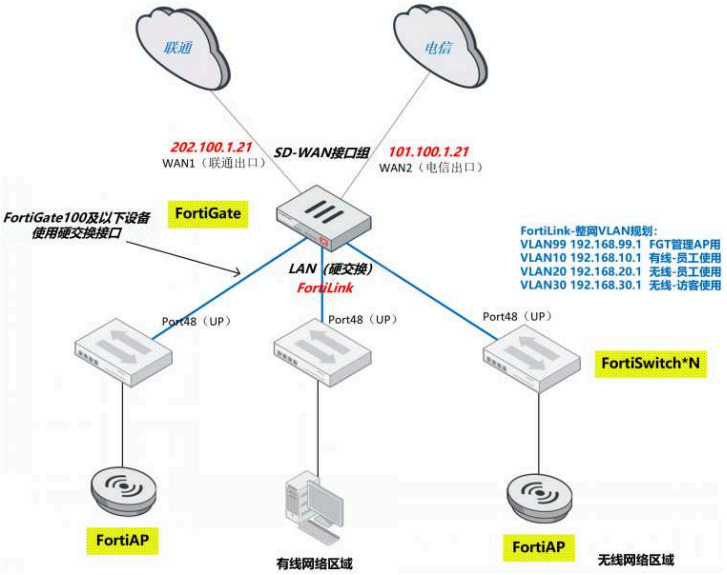


3. 如果交换机很多，可以使用以下方案拓扑。使用聚合接口并利用“FortiLink split interface”，将防火墙的聚合接口分别接到两台核心交换机上，但是正常情况下只有接其中一台核心交换机的接口是UP的，另外一台核心交换机的接口是DOWN的，处于备份状态。



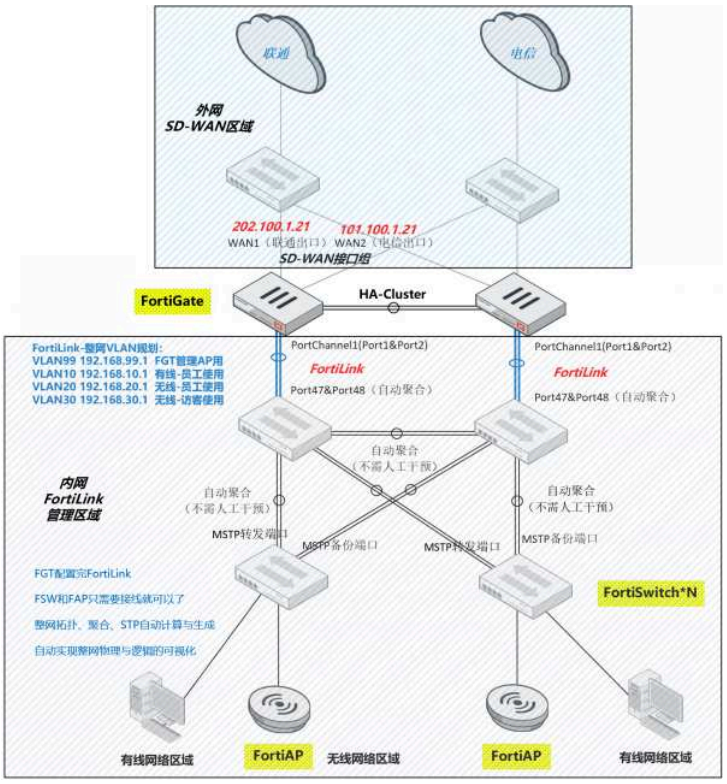
4. FortiGate100及以下型号的设备改进方案。使用硬交换机接口（LAN/Internal）对接三台FortiSwitch，使用硬交换部署FortiLink的时候尽量不要有STP（环路）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



最终方案三

1. 以上两种改善方案也存在自身的问题，实际的情况是，大部分的交换机都不在同一个机架上，可能每个楼层一台交换机，这样的话，如果需要防火墙和每一个交换机进行直接互联，这个部分有时候由于环境问题会存在一定的困难。
2. 另外还有一个问题是防火墙本身也存在单点故障风险。因此一个更加好一点的改进方案是，引进FortiGate的HA机制，然后启用双核心交换机组网完成FortiLink的架构。
3. 继续改善的FortiGate HA加双核心FortiSwitch的星型组网方案。



4. 由于FortiGate使用聚合接口+HA部署FortiLink，这个时候可以不需要使用“FortiLink split interface”进行跨交换机的对接，因为将聚合都接到一台交换机可以增加带宽的使用效率，同时HA可以monitor聚合接口，一旦核心交换机或聚合接口故障，可以HA切换到备防火墙上，相应的流量也会切换到另外一台核心交换机上，从而实现整体的业务备份效果。
5. 对于上述所有的拓扑图，从配置的角度来说只需要选择好适合的方案，然后只需配置FortiGate的FortiLink接口即可，FortiSwitch和FortiAP只需要接物理的线即可，不需要有任何的手工配置FortiSwitch和FortiAP，按照拓扑图接好物理的线之后，等待FortiLink整网收敛完毕之后，就可以通过FortiGate统一的管理和配置FortiSwitch和FortiAP，整网的所有的有线和无线的配置统统都在FortiGate上完成，通过FortiGate的FortiLink做到整网可控、可配、可视化。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

6. 总结来看，越完美的东西就意味着越复杂，有时候简单也是一种优势，因此选择用什么样的FortiLink组网，需要考虑自身的需求和对业务的重视情况而定，并非越简单越好，也并非越复杂越好，适合自己的才是最好的。

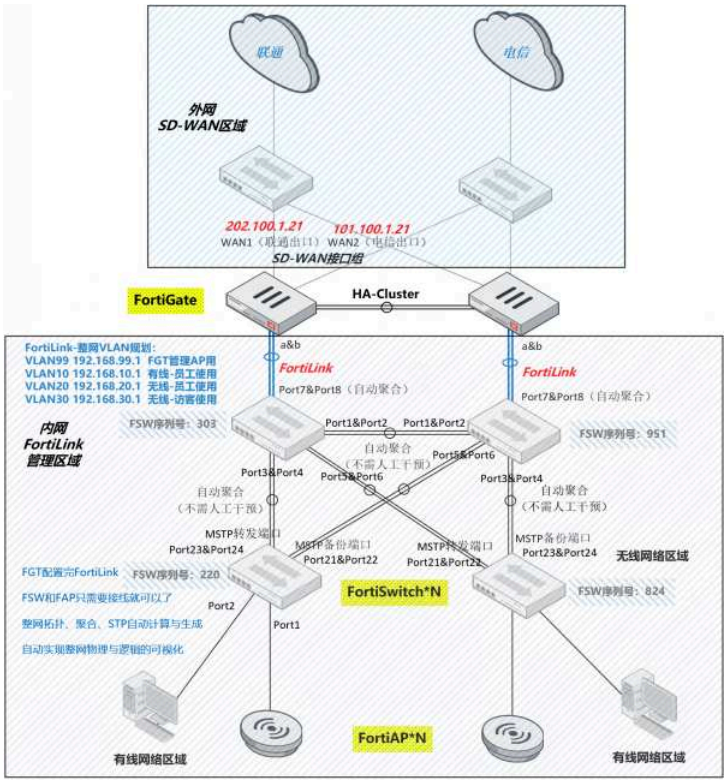
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink星型组网配置举例

网络需求

FortiGate运行HA-Cluster，核心交换和接入交换机采用全聚合接口（FortiSwitch全自动聚合，接线即可，无需手工配置聚合接口）对接的星型组网结构。

网络拓扑



1. 两台FortiGate配置为HA主备模式。
2. 整体规划：
   - 外网IP网段规划：
     - WAN1联通出口：IP 202.100.1.21，GW 202.100.1.192
     - WAN2电信出口：IP 101.100.1.21，GW 101.100.1.192
   - WAN1和WAN2合并成SD-WAN接口。
   - 内网IP网段规划，FGT通过FortiLink+Capwap协议统一的接管FortiSW和FortiAP，为有线和无线统一进行管理和业务处理：
     - 有线网络规划：VLAN 10，192.168.10.1
     - 无线网络规划：员工WIFI VLAN 20，192.168.20.1
     - 无线网络规划：访客WIFI VLAN 30，192.168.30.1
     - 管理FortiAP：VLAN 99，192.168.99.1
   - FortiLink互联部分规划：
     - FortiGate的a和b做聚合接口与Fortiswitch的后两个接口互联即可实现聚合接口的FortiLink管理。
     - 加入FortiLink的接口自动变为聚合口成员。

配置步骤

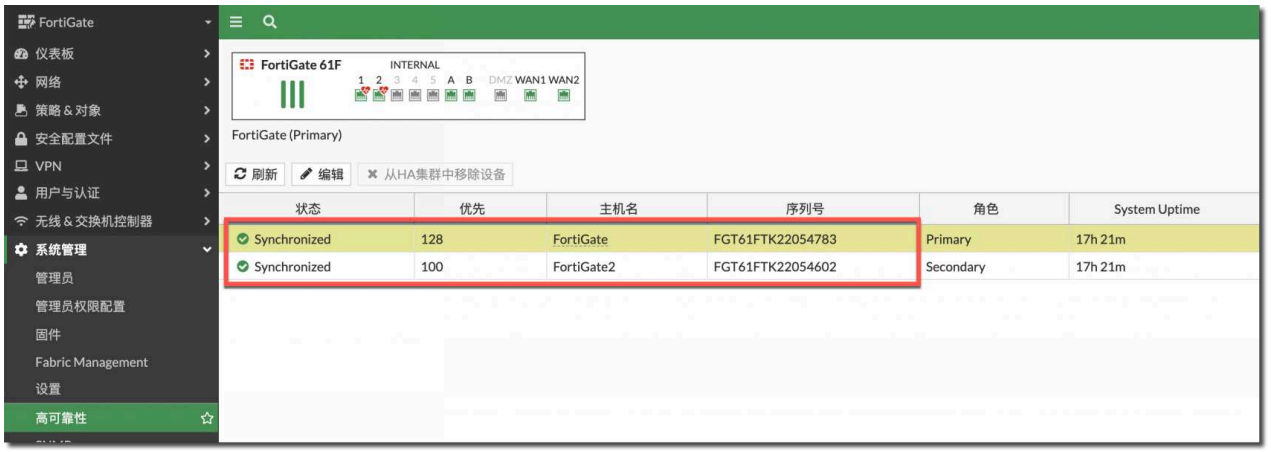
准备事项

1. 首先确认FortiGate如下全局配置已开启（一般默认为开启状态）。

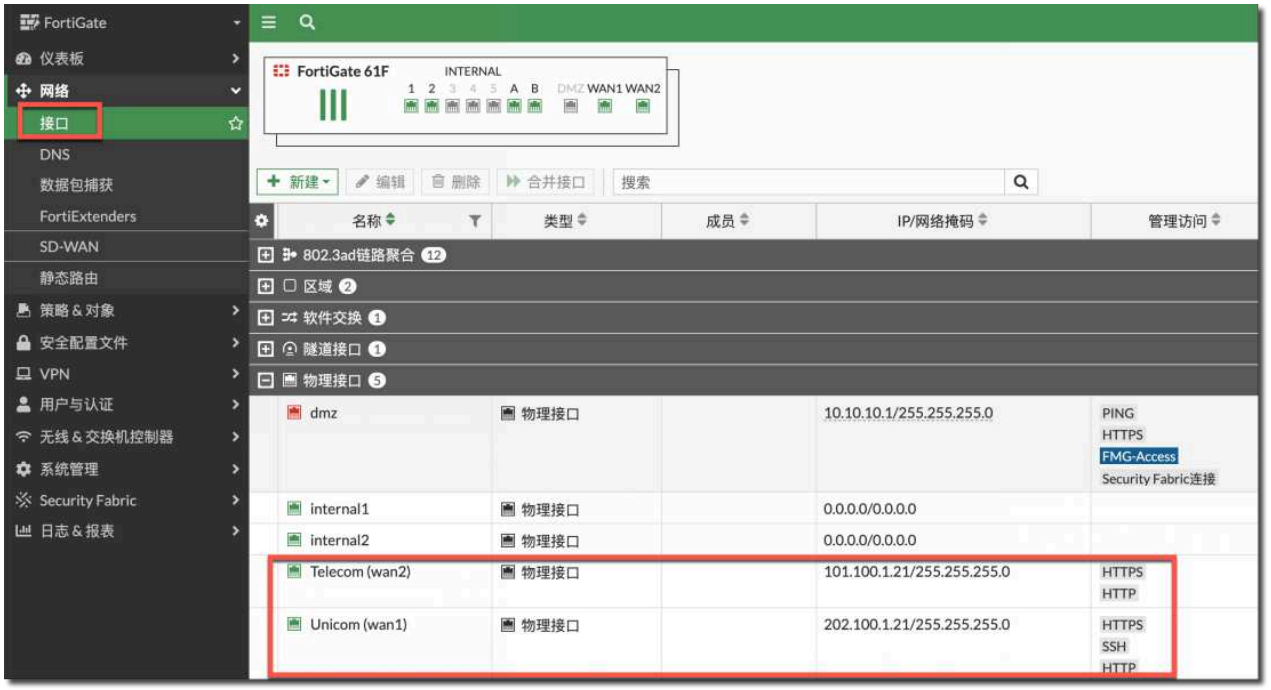
```
config system settings
    set gui-switch-controller enable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置两台FortiGate的HA主备模式（配置方法请参考HA双机热备→HA典型基础配置 ↗）。



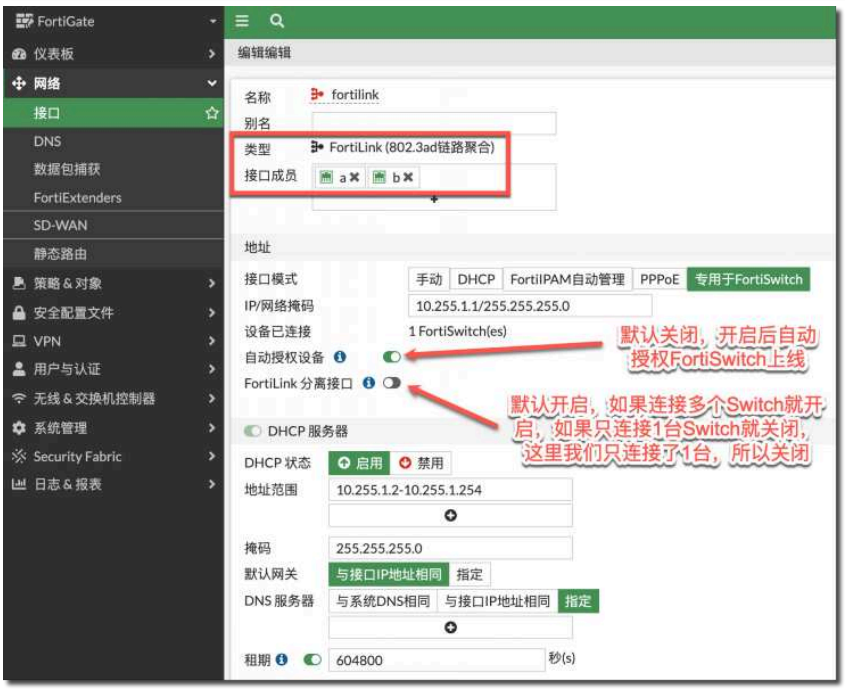
3. 配置wan1和wan2的IP地址。



4. 配置FortiLink实现FortiSwith上线，我们只需要将用于FortiLink的成员接口加入FortiLink接口即可。此拓扑中，FortiGate用于连接FortiSwitch的接口为a和b，编辑FortiLink接口，将a和b加入FortiLink（某些产品型号会默认将两个接口加入FortiLink），开启自动授权设备，关闭FortiLink分离接口，其他配置保持默认，可以看到FortiLink为一个聚合接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

FortiLink分离接口什么时候应该开启?

分离接口的意是，如果聚合接口的port1和port2分别连接了一台SW，在没有使用MCLAG的情况下（没开启堆叠功能），则聚合接口的port1和port2没办法同时UP（同时开启聚合接口无法正常工作），因此必须开启FortiLink分离接口功能，让聚合接口只有一个物理接口（port1）是处于UP状态的，另外一个物理接口（port2）处于DOWN的备份状态，当port1接口状态DOWN，则Port2立即接管Port1的工作，让聚合接口的FortiLink继续运行，这是一个聚合接口在FortiLink管理时候的备份机制。



重要

FortiLink split interface 什么时候应该disable?

如果FGT的聚合接口只接到了一台交换机上，并没有跨交换机聚合（没有MCLAG，也不需要FortiLink split interface），因此这种情况应该让聚合接口的两个物理接口port1和port2同时UP，两个接口同时工作起来，以便提供更高带宽和备份的作用。



相关CLI:

```
NTP:
config system ntp
    set ntpsync enable
    set server-mode enable
    set interface "fortilink"
end
------------------------------------------------------------------
DHCP:
config system dhcp server
    edit 2
        set dns-service local
        set ntp-service local
        set default-gateway 10.255.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.255.1.2
                set end-ip 10.255.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end
────────────────────────────────────────────────────────────────────────
FortiLink:
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "a" "b"
        set lldp-reception enable
        set lldp-transmission enable
        set auto-auth-extension-device enable
        set fortilink-split-interface disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
    next
end
```

连接FortiLink

1. 配置完FortiGate之后，这个时候再去接FortiGate的FortiLink到FortiSwitch的线，以及FortiSwitch之间的线，严格按照拓扑图，从核心交换机往接入交换机这样的顺序接线。FortiSwitch如果以前有使用过，建议都恢复一下出厂设置，然后再加入到FortiLink。

2. FortiSwitch的靠后接口一般都默认开启了FortiLink接口属性，如果接前面的接口可能会无法加入到FortiLink，因此FortiSwitch的FortiLink最好都使用靠后的接口进行接线。FortiSwitch各型号默认开启FortiLink功能的接口如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiSwitch型号	默认开启FortiLink的接口
FS-108D-POE	port9–port10
FS-108E, FS-108E-POE, FS-108E-FPOE	port7–port10
FSR-112D-POE	port5–port12
FS-124D, FS-124D-POE	port23–port26
FSR-124D	port1-port4, port21–port28
FS-124E, FS-124E-POE, FS-124E-FPOE	port21–port28
FS-148E, FS-148E-POE	port21–port52
FS-224D-POE	port21–port24
FS-224D-FPOE	port21–port28
FS-224E, FS-224E-POE	port21–port28
FS-248D, FS-248D-FPOE	port45–port52
FS-248D-POE	port47–port50
FS-248E-POE, FS-248E-FPOE	port45–port52
FS-424D, FS-424D-POE, FS-424D-FPOE	port23–port26
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30
FS-548D	port39–port54
FS-548D-FPOE, FS-548DN	port45–port54
FS-1024D	port1–port24
FS-1048D, FS-1048E	port1–port52
FS-3032D, FS-3032E	port1–port32

3. 如果FortiSwitch无法被FortiGate管理，登陆到FortiSwitch上进行确认接口是否开启了FortiLink。

```
FortiSwitch # show switch interface port9
config switch interface
    edit "port9
        set auto-discovery-fortilink enable    //接口下又此命令的接口才可以自动加入到FortiLink中
    next
end
```

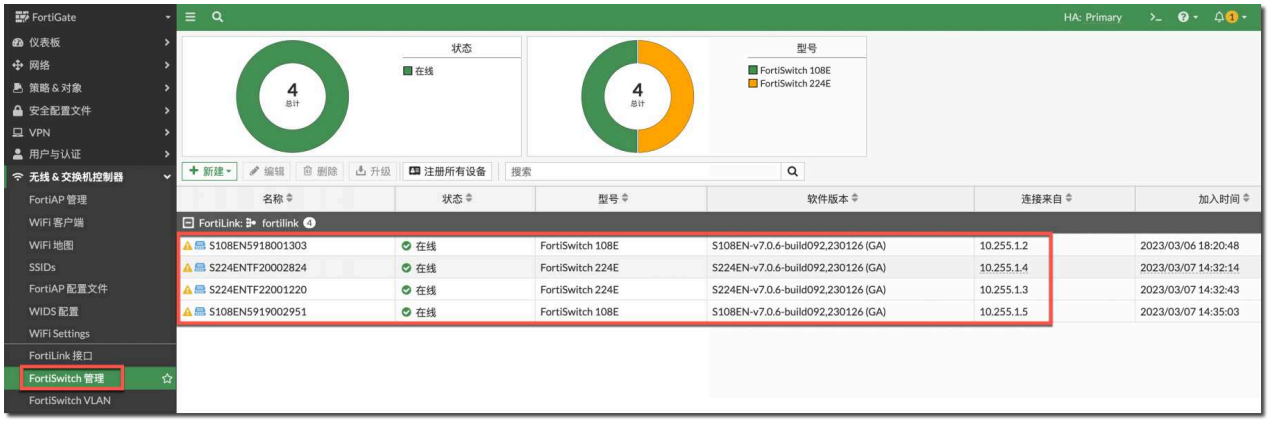
4. 交换机之间如果接多根线，会自动进行聚合，但是FortiLink自动聚合会花比较长的时间，建议可以先接单线，等FortiLink的拓扑较快的形成结束之后，再增加彼此之间的另外一根线，再进行自动聚合，这样效率会比较高一些。

5. 接线是很重要的步骤，仔细看拓扑图，做好接口标签，不要接错。

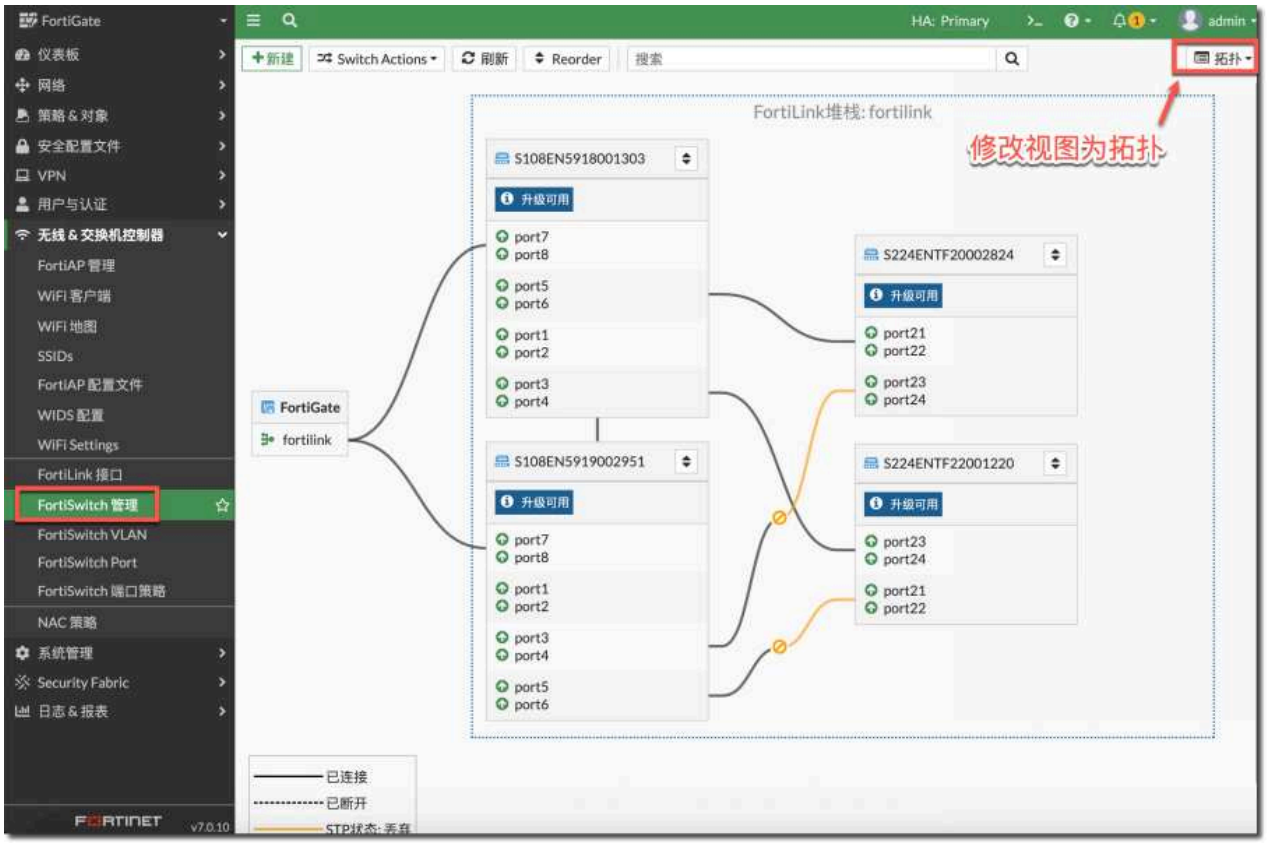
6. 接好线之后，FortiSwitch和FortiGate之间会自动在后台进行FortiLink、CAPWAP、MSTP、聚合接口的协商加入等操作，等FortiLink的管理结束之后，在FortiGate上会看到一个网站的FortiSwitch拓扑图，和我们规划的拓扑图应该是一致的，可以仔细核对接线是否正确。

7. 在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，查看交换机被管理状态，可以看到4台交换机均已上线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



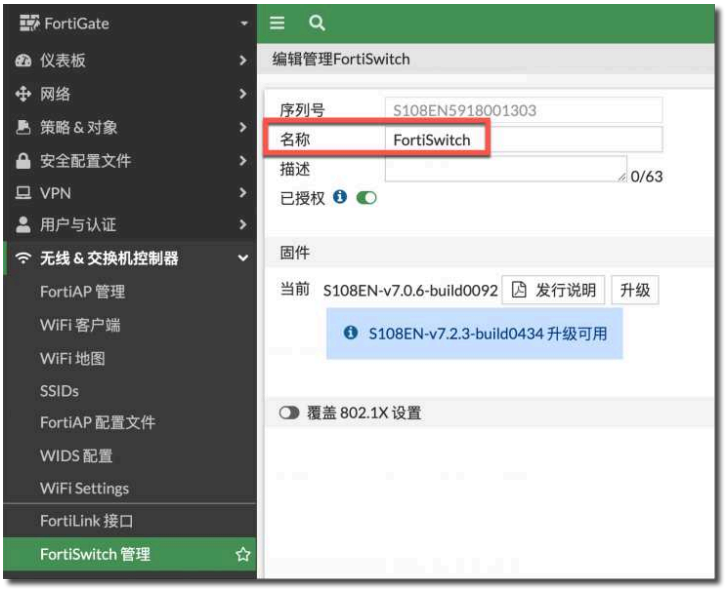
8. 修改视图为拓扑，可以更直观的看到当前防火墙与交换机的接口连接。



9. 交换机加入到FortiGate的FortiLink，会先清除配置再重启，然后从standalone的状态进入到“Fortilink remote control”的状态，后续所有的配置都通过FortiGate下发即可。

0. 编辑交换机，可以修改交换机名字以及升级版本，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. FortiSwitch之间接多根线进行FortiLink互联，会默认自动聚合。其实接一根网线也是聚合的，只是聚合组里面只有一个接口而已，因此多根网线直连，这些直连的线都会自动加入到一个聚合接口里面（注意不能跨交换机，跨交换机的聚合是MCLAG）。

```
FortiGate # exec ssh admin@10.255.1.2
Warning: Permanently added '10.255.1.2' (ED25519) to the list of known hosts.
admin@10.255.1.2's password:

S108EN5918001303 # show switch trunk
path=switch, objname=trunk, tablename=(null), size=752
config switch trunk
    edit "GT61FTK22054783"
        set mode lacp-active
        set auto-isl 1
        set fortilink 1
        set members "port7" "port8"
    next
    edit "4ENTF20002824-0"
        set mode lacp-active
        set auto-isl 1
        set members "port5" "port6"
    next
    edit "4ENTF22001220-0"
        set mode lacp-active
        set auto-isl 1
        set members "port3" "port4"
    next
    edit "8EN5919002951-0"
        set mode lacp-active
        set auto-isl 1
        set members "port1" "port2"
    next
end
```

2. 另外建议给每台交换机命名一个名字，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



STP状态查看

1. FortiLink之间的交换机互联，如果不用MCLAG的话，本质上是MSTP（多实例生成树）在整网统一的进行接口环路计算，从而实现网络的备份，与快速收敛恢复。 可以通过FGT的命令行界面用Telent/SSH到FortiSwitch上并分别查看四台FortiSwitch的STP状态。

   - 主核心交换机（303）上查看：

```
FortiGate # exec ssh admin@10.255.1.2
Warning: Permanently added '10.255.1.2' (ED25519) to the list of known hosts.
admin@10.255.1.2's password:

Primary_Core_Switch #  diagnose stp instance list
MST Instance Information, primary-Channel:
 ...
Instance ID 15
  Config         Priority 24576, VLANs 4094
                 Bridge MAC e81cba1c0900
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 0
                 (This bridge is the regional root)
  //直连主FGT的FSW会自动将网桥优先级降低到：Priority 24576，因此整个FortiLink二层网络中，自己就是根网桥
  TCN Events     Triggered 10 (0d 0h 24m 59s ago), Received 67 (0d 0h 24m 26s ago)
  Port               Speed   Cost       Priority   Role         State        Flags
  _________________  ______  _________  _________  ___________  ___________  _________________
  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
  GT61FTK22054783    2G      10000      128        DESIGNATED   FORWARDING   ED
  //与主FortiGate_FortiLink互联的自动生成的聚合接口，STP为指定接口，转发状态
  4ENTF20002824-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与序列号824结尾的FSW互联的自动生成的聚合接口，STP为指定接口，转发状态
  4ENTF22001220-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与序列号220结尾的FSW互联的自动生成的聚合接口，STP为指定接口，转发状态
  8EN5919002951-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与备核心交换机303互联的自动生成的聚合接口，STP为指定接口，转发状态
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

   - 备核心交换机（951）上查看：

```
FortiGate # exec ssh admin@10.255.1.5
Warning: Permanently added '10.255.1.5' (ED25519) to the list of known hosts.
admin@10.255.1.2's password:

Secondary_Core_Switch # diagnose stp instance list
MST Instance Information, primary-Channel:
 ...
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC 04d59010ff48
                 //自己的MAC
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 1, Root Port 8EN5918001303-0
  //互联根网桥的信息：根网桥MAC e81cba1c0900，根网桥优先级 24576，互联根网桥的接口 8EN5918001303-0
  TCN Events     Triggered 4 (0d 0h 41m 4s ago), Received 2 (0d 0h 41m 32s ago)
  Port               Speed   Cost       Priority   Role         State        Flags
  _________________  ______  _________  _________  ___________  ___________  _________________
  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
  4ENTF22001220-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与序列号220结尾的FSW互联的自动生成的聚合接口，STP为指定接口，转发状态
  8EN5918001303-0    2G      1          128        ROOT         FORWARDING   EN
  //与主核心交换机303互联的自动生成的聚合接口，STP为root接口，转发状态
  4ENTF20002824-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与序列号824结尾的FSW互联的自动生成的聚合接口，STP为指定接口，转发状态
  GT61FTK22054602    2G      10000      128        DESIGNATED   FORWARDING   ED
  //与备FortiGate_FortiLink互联的自动生成的聚合接口，STP为指定接口，转发状态（但由于连的是备防火墙，实际物理口是discarding状
态）
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

- 接入交换机（220）上查看：

```
FortiGate # exec ssh admin@10.255.1.3
admin@10.255.1.3's password:

Access_TAC_Switch # diagnose stp instance list
MST Instance Information, primary-Channel:
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC ac712e465448
                 //自己的MAC地址
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 1, Root Port 8EN5918001303-0
  //互联根网桥的信息：根网桥MAC e81cba1c0900，根网桥优先级 24576，互联根网桥的接口8EN5918001303-0
  TCN Events     Triggered 1 (0d 1h 12m 46s ago), Received 6 (0d 1h 9m 25s ago)
  Port               Speed   Cost       Priority   Role         State        Flags
  _________________  ______  _________  _________  ___________  ___________  _________________
  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
  8EN5918001303-0    2G      1          128        ROOT         FORWARDING   EN
  //接主核心交换机303，STP为根接口，转发状态
  8EN5919002951-0    2G      1          128        ALTERNATIVE  DISCARDING   EN
  //接备核心交换机951，STP为备份接口ALTERNATIVE  DISCARDING，处于阻塞状态
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

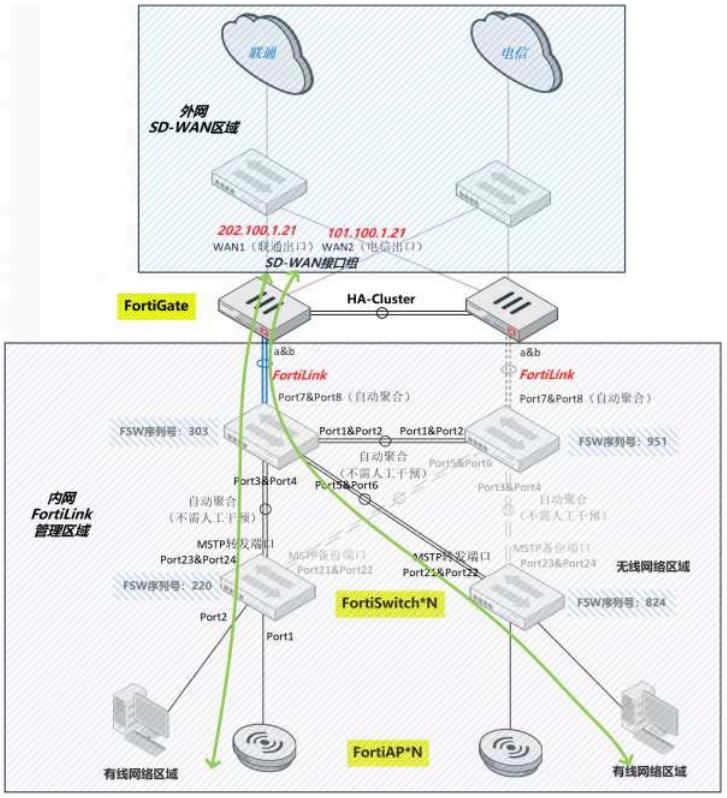
- 接入交换机（824）上查看：

```
FortiGate # exec ssh admin@10.255.1.4
admin@10.255.1.4's password:

Access_Sales_Switch # diagnose stp instance list
MST Instance Information, primary-Channel:
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC e023ff54e7e0
                 //自己的MAC地址
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 1, Root Port 8EN5918001303-0
  //互联根网桥的信息：根网桥MAC e81cba1c0900，根网桥优先级 24576，互联根网桥的接口8EN5918001303-0
  TCN Events     Triggered 1 (0d 1h 22m 45s ago), Received 7 (0d 1h 18m 58s ago)
  Port               Speed   Cost       Priority   Role         State        Flags
  _________________  ______  _________  _________  ___________  ___________  _________________
  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
  8EN5918001303-0    2G      1          128        ROOT         FORWARDING   EN
  //接主核心交换机303，STP为根接口，转发状态
  8EN5919002951-0    2G      1          128        ALTERNATIVE  DISCARDING   EN
  //接备核心交换机951，STP为备份接口ALTERNATIVE  DISCARDING，处于阻塞状态
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

2. FortiLink组网中STP是很重要部分，通常STP是一个稳定的状态，一旦出现FortiLink不稳定，则需要观察STP的状态和选举结果，从中找到相关线索，以便查出为何STP不稳定的原因，对于排错来说是很重要的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. FortiLink+STP稳定状态的实际数据转发拓扑图如下。

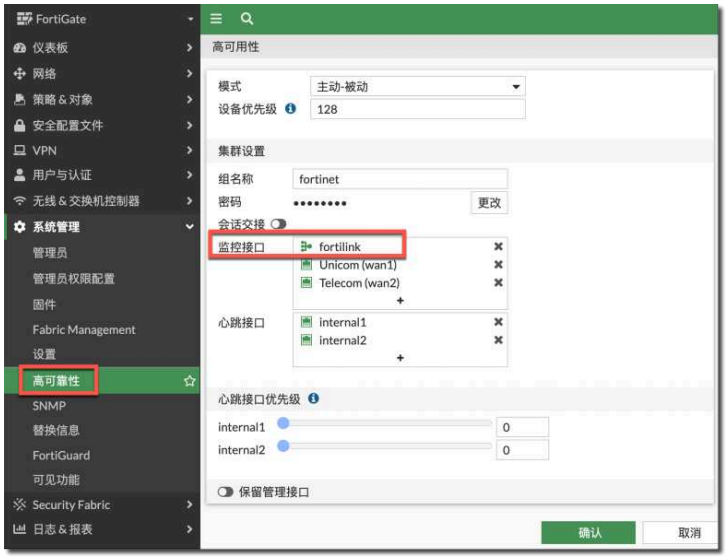


4. 在FortiGate查看交换机管理状态。

```
FortiGate # execute switch-controller get-conn-status
Managed-devices in current vdom root:
FortiLink interface : fortilink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME            NAME
S108EN5918001303  v7.0.6 (092)      Authorized/Up   -   10.255.1.2      Mon Mar  6 18:20:48 2023
Primary_Core_Switch
S224ENTF20002824  v7.0.6 (092)      Authorized/Up   -   10.255.1.4      Tue Mar  7 14:32:14 2023
Access_Sales_Switch
S224ENTF22001220  v7.0.6 (092)      Authorized/Up   -   10.255.1.3      Tue Mar  7 14:32:43 2023
Access_TAC_Switch
S108EN5919002951  v7.0.6 (092)      Authorized/Up   -   10.255.1.5      Tue Mar  7 14:35:03 2023
Secondary_Core_Switch
         Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error, 3=L3
         Managed-Switches: 4 (UP: 4 DOWN: 0)
```

5. 最后不要忘记，在FortiLink的聚合接口和FortiLink管理配置完毕，记得把这个FortiLink聚合接口加入到HA的监控接口列表中，这样当主核心交换机挂了（比如断电）之后，业务才可以平稳切换到备防火墙上。

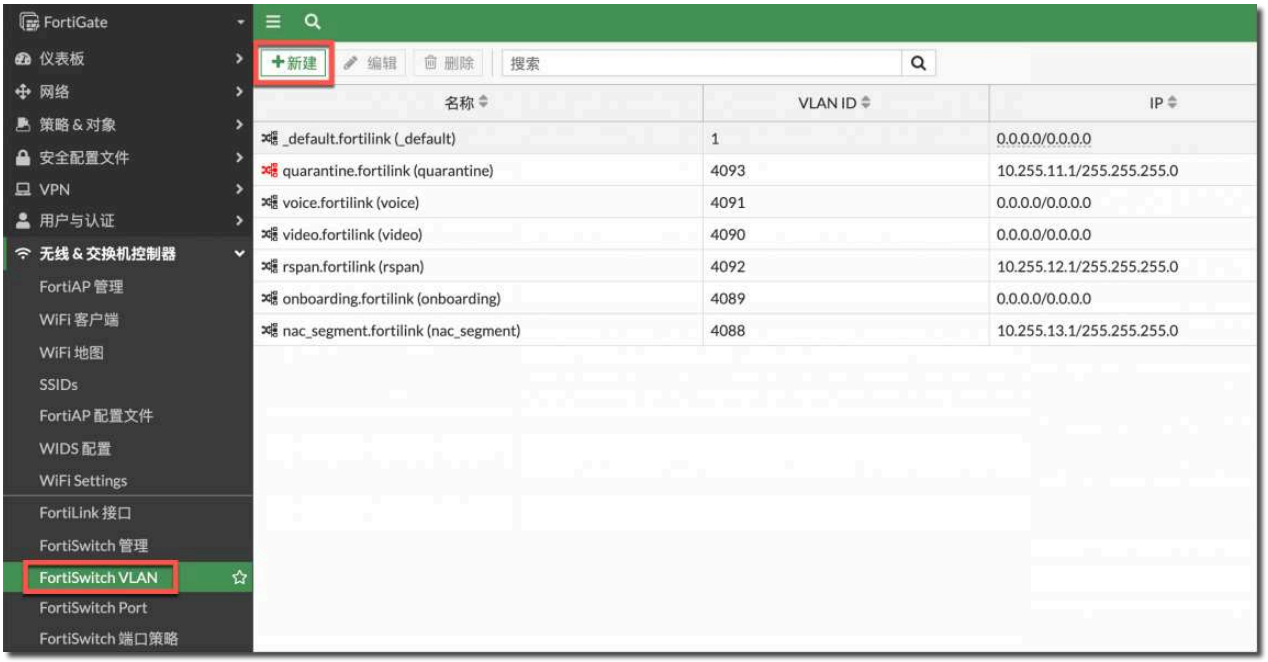
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



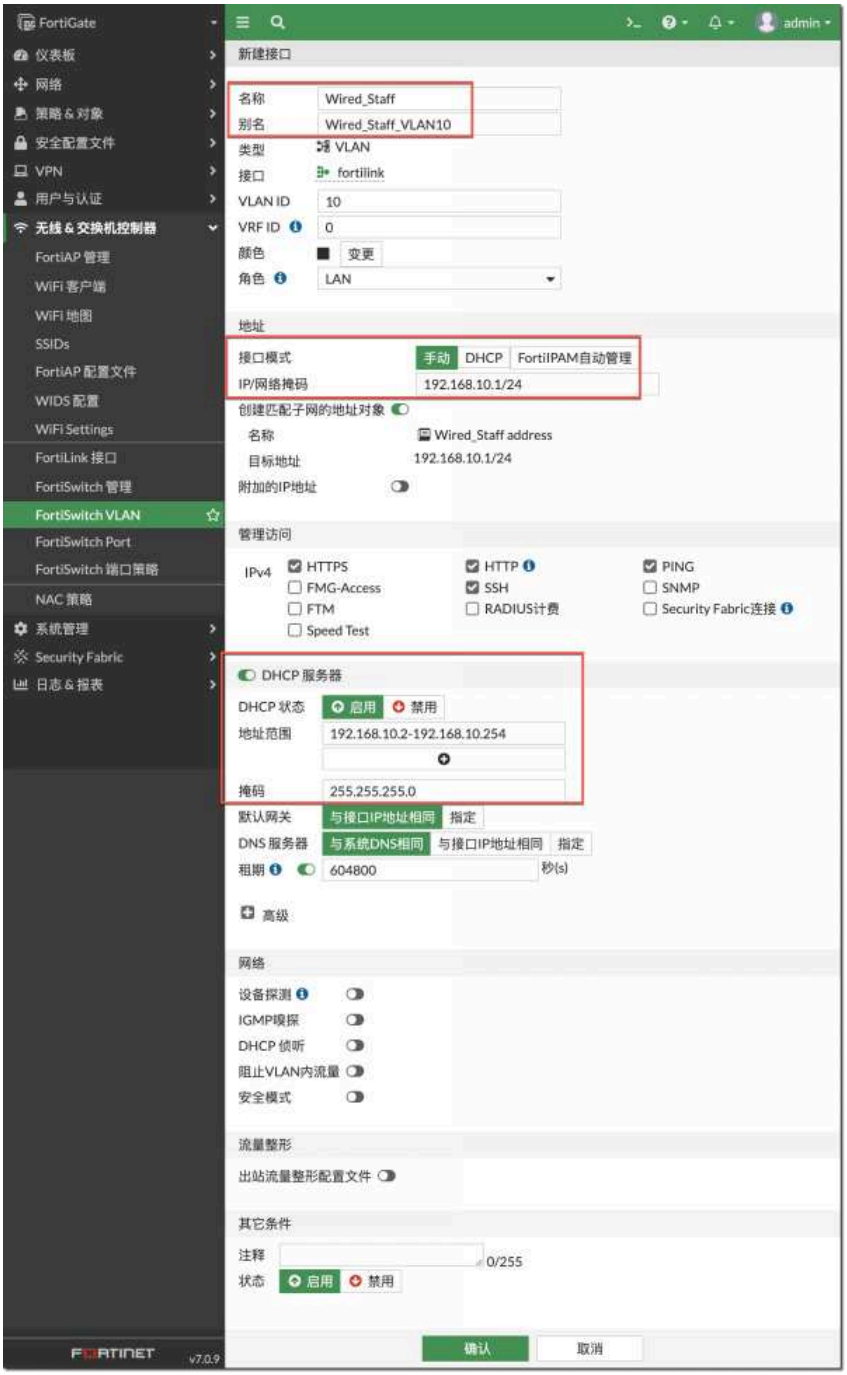
创建VLAN

1. FortiGate通过FortiLink + Capwap协议统一的接管FortiSwitch和FortiAP，为有线和无线统一进行管理和业务处理。
2. 进入FortiGate的无线&交换机控制器→FortiSwitch VLAN页面，新建有线网络VLAN 10、员工无线网络VLAN 20、访客无线网络VLAN 30、管理FortiAP VLAN 99。注意管理FortiAP的VLAN接口要开启Security Fabric，包含CAPWAP。

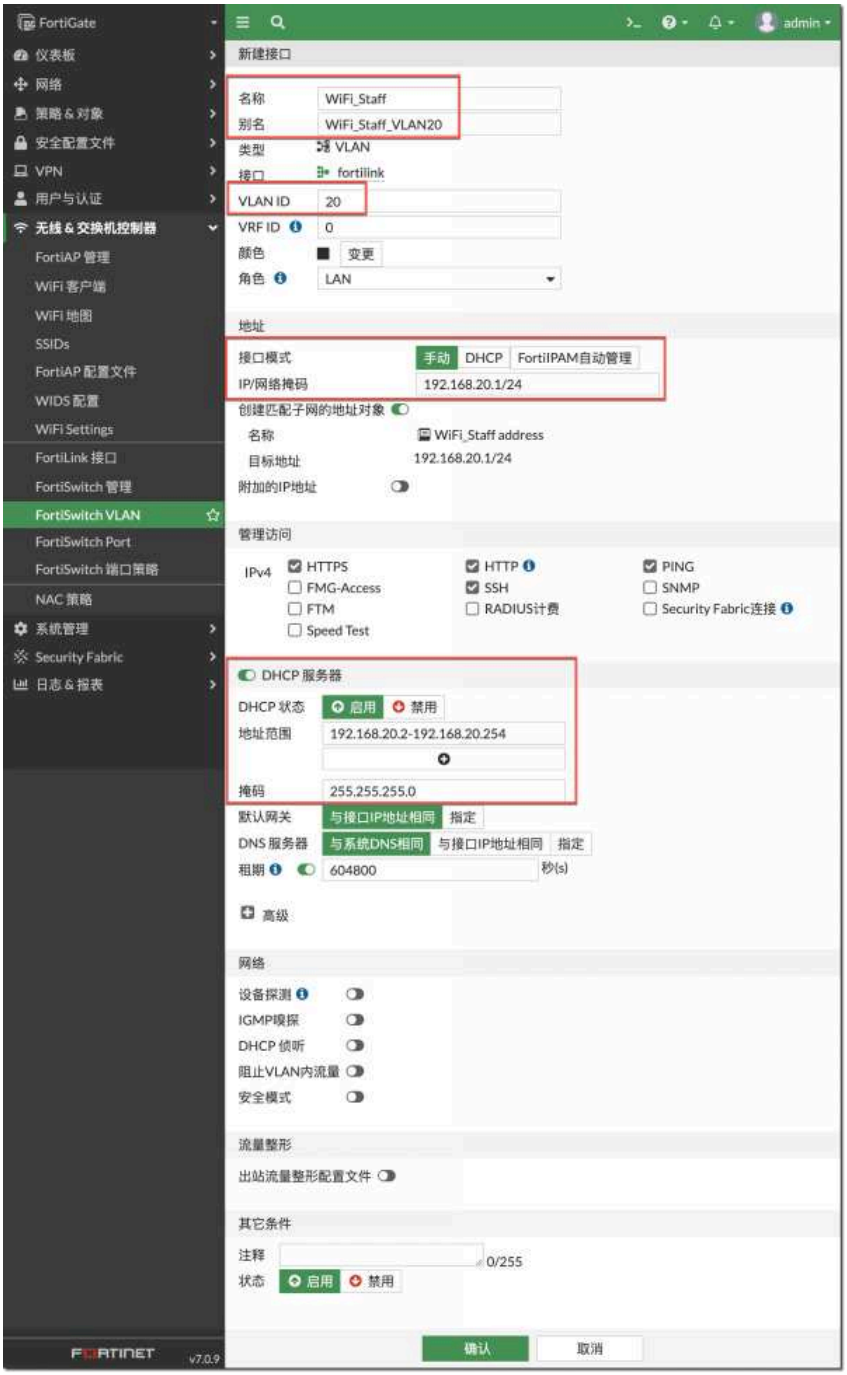
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



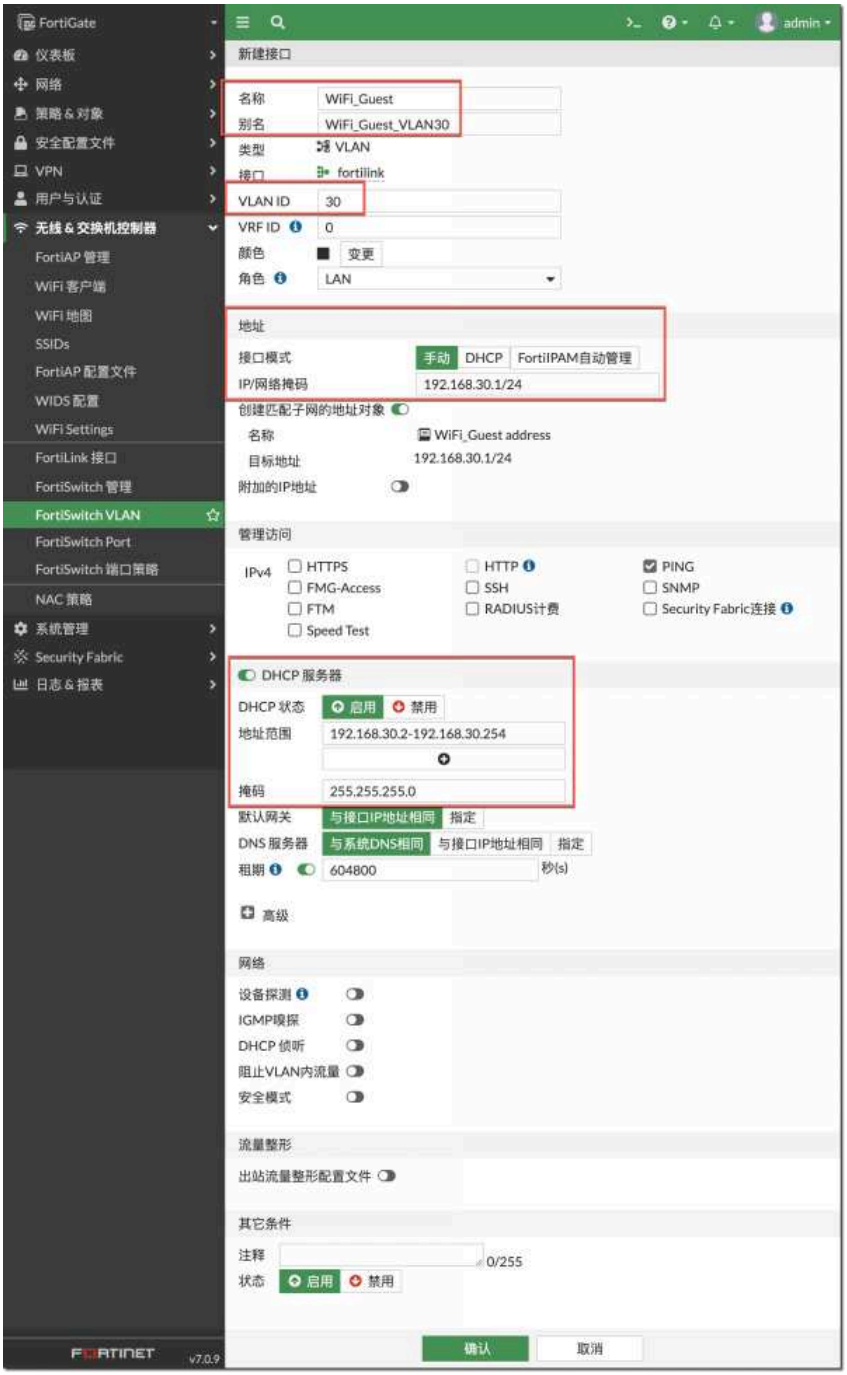
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



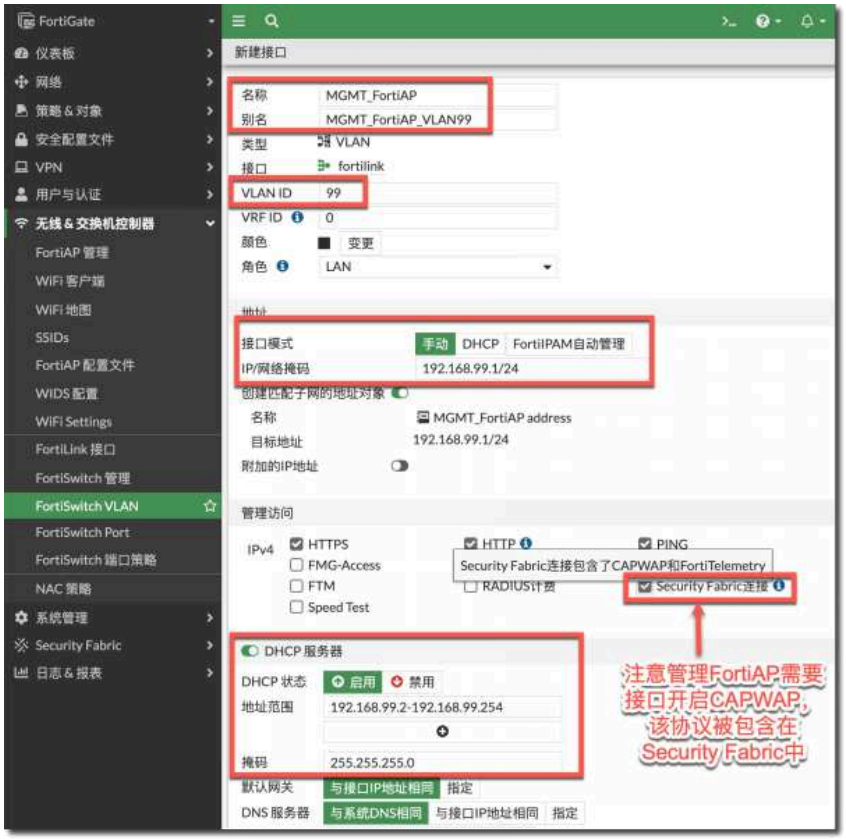
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

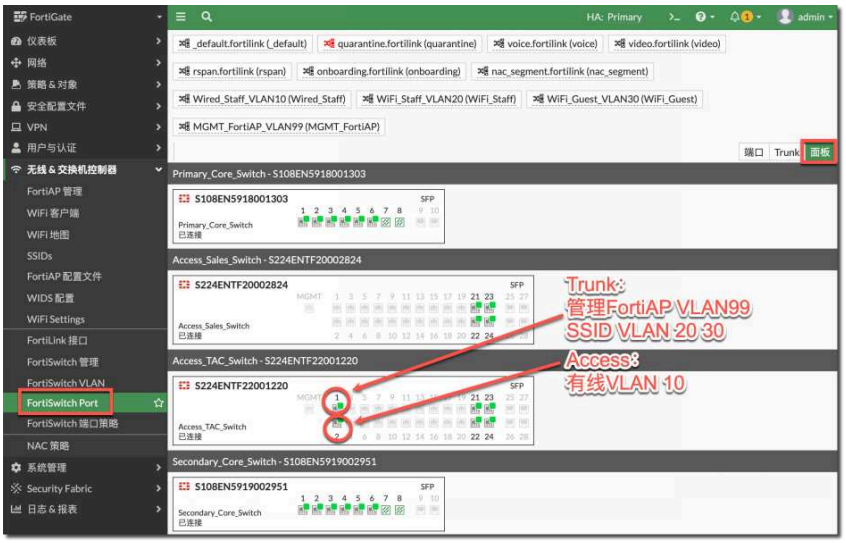


3. VLAN创建完成。



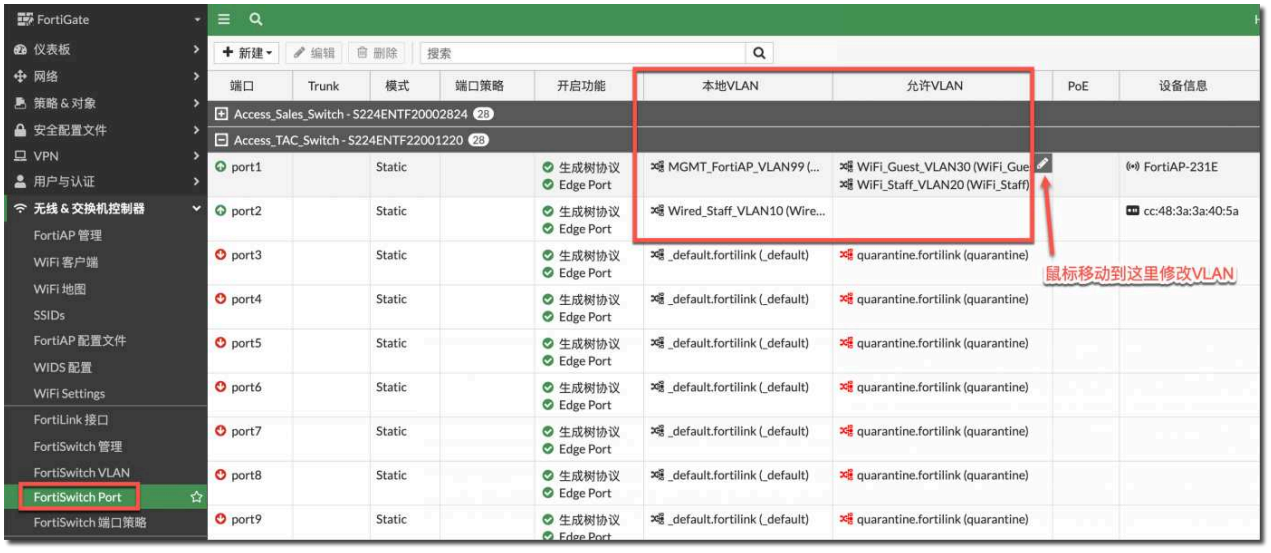
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

分配VLAN



1. 接入交换机的port1接FortiAP，配置为Trunk模式，允许 VLAN20和VLAN30，VLAN20用于WIFI-STAFF的SSID用户，VLAN30用于WIFI-GUEST的SSID用户。另外本地VLAN设置为VLAN 99，用于FortiAP的管理（FortiAP的管理相当于使用不打vlan-tag的VLAN 99，本地VLAN默认是VLAN 1，因此只需要将本地VLAN设置为VLAN 99即可）。

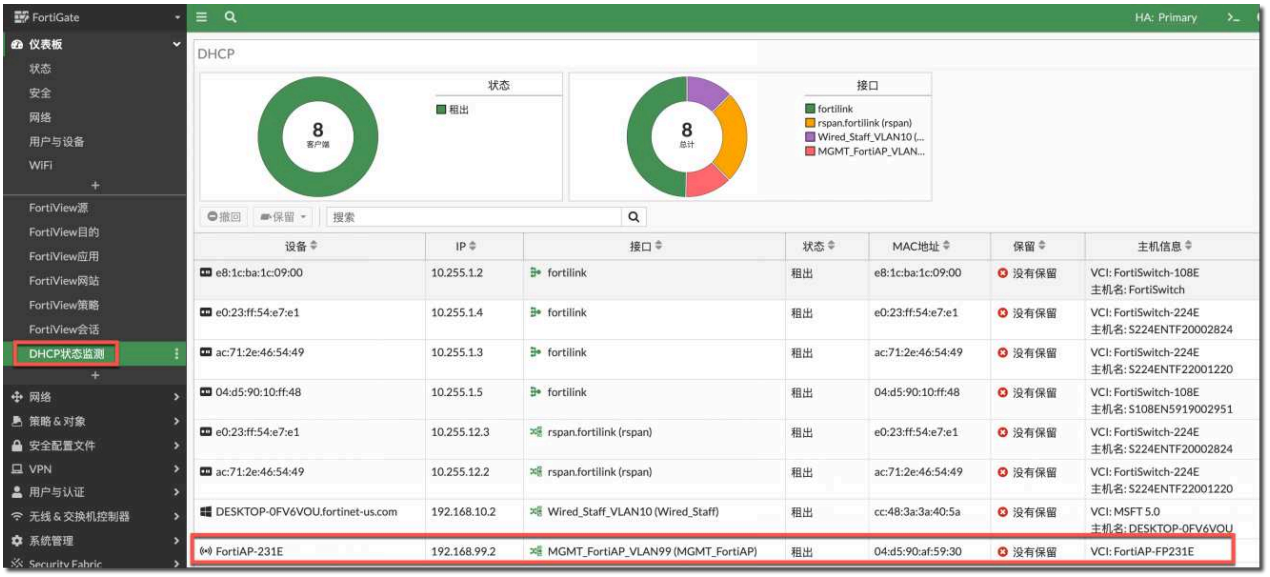
2. Port2接具体的物理PC，因此只需要将Port2设置为access口，分配VLAN 10即可，用FortiSwitch的概念来说就是将本地VLAN设置为VLAN 10，本地VLAN不打vlan-tag，相当于就是设置接口为access vlan 10。



无线配置

1. FortiAP连接后，会通过VLAN 99的DHCP获取到192.168.99.0/24网段的IP地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在之前的配置中，VLAN 99的接口开启了CAPWAP协议（包含在Security Fabric中），激活了FortiGate的无线管理功能，这时候FortiAP会自动找到FGT进行注册。因此在FortiAP管理的地方可以看到这个FortiAP的信息（如果没有看到检查配置，并将FortiAP恢复出厂，让FortiAP重新获取IP地址并发起注册）。



3. 右键点击上图中等待认证的FortiAP，点击授权按钮，等待几分钟，FortiAP成功上线。



4. 编辑FortiAP设置，配置FortiAP的名称，或进行升级操作。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 进入无线&交换机控制器→SSIDs页面，点击新建按钮。

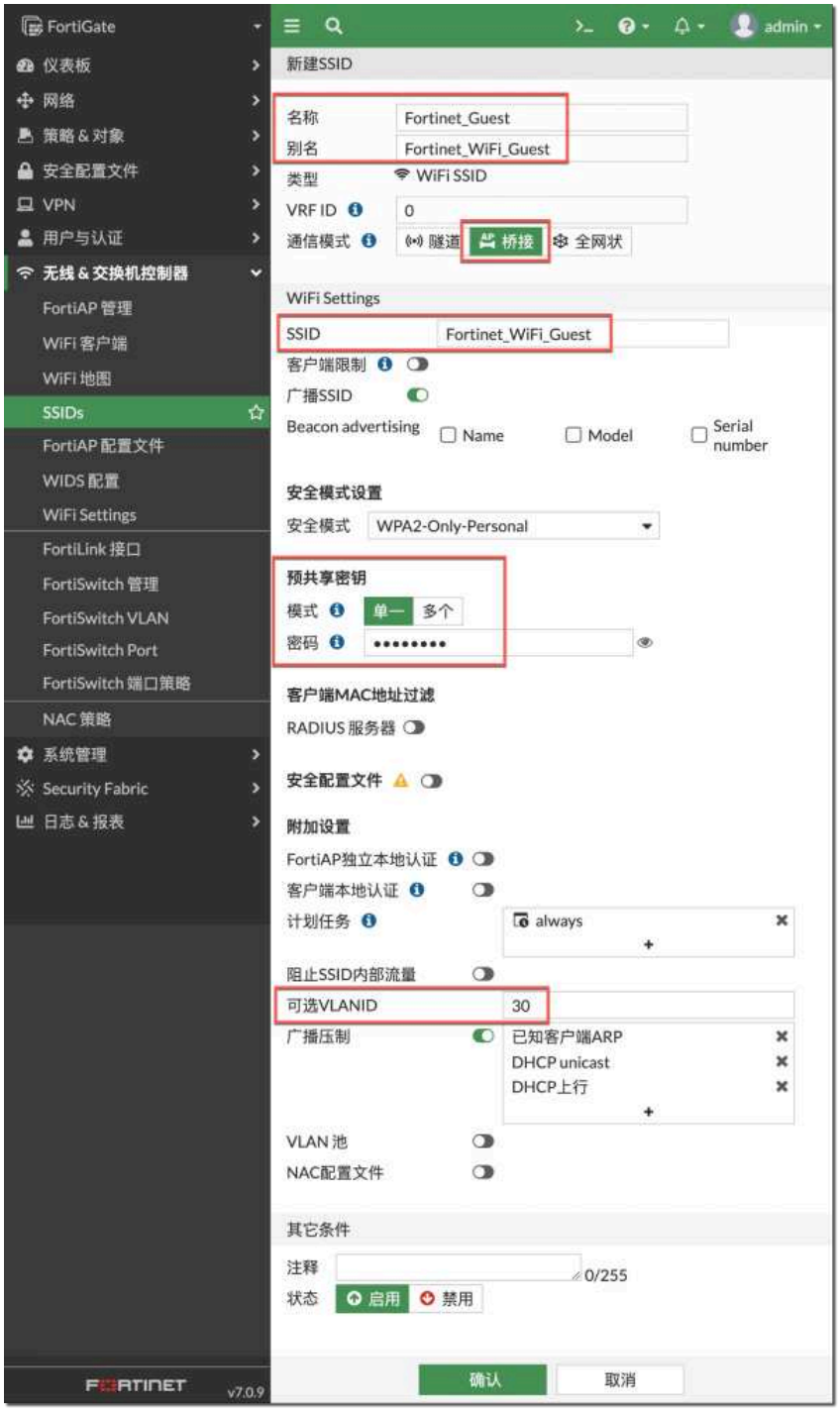


6. 新建SSID：Fortinet_WiFi_Staff VLAN 20用于员工WIFI使用，Fortinet_WiFi_Guest VLAN 30用于访客WiFi使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





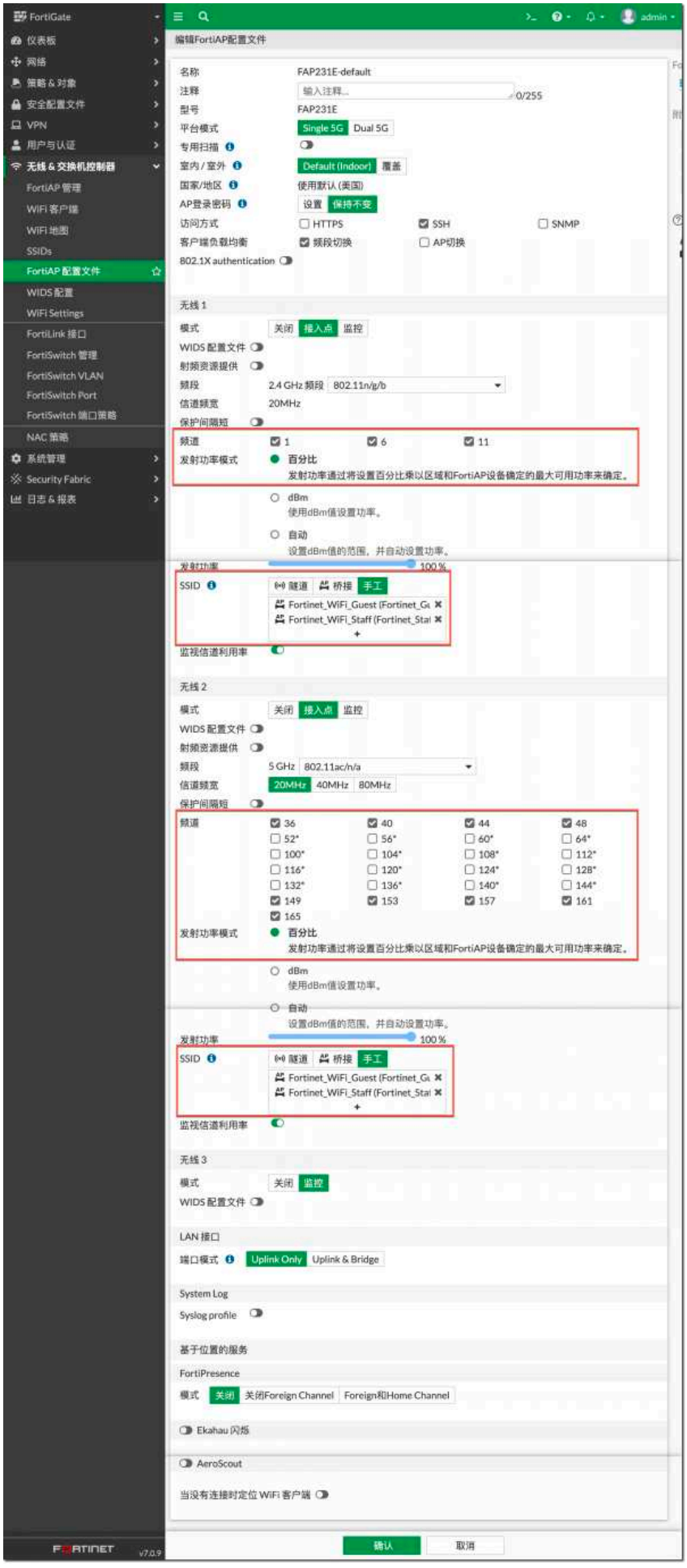
7. 将SSID关联到FortiAP上，然后让FortiAP发布无线SSID信号，这样用户就可以通过SSID连接到无线了。进入FortiAP配置文件页面，编辑FortiAP关联的配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 桥模式的SSID需要在FortiAP配置文件里面手工指定一下，另外下图标示出的配置为推荐配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

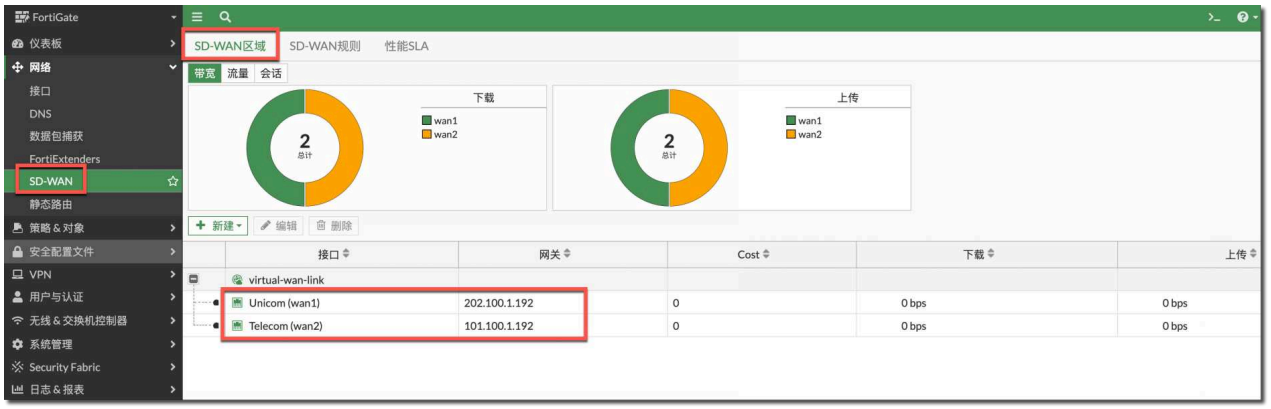


9. FortiAP会自动关联到这个FortiAP配置文件里面的内容，发起SSID的信号。



SD-WAN配置

1. 将wan1和wan2加入SD-WAN接口，并配置各自的网关。

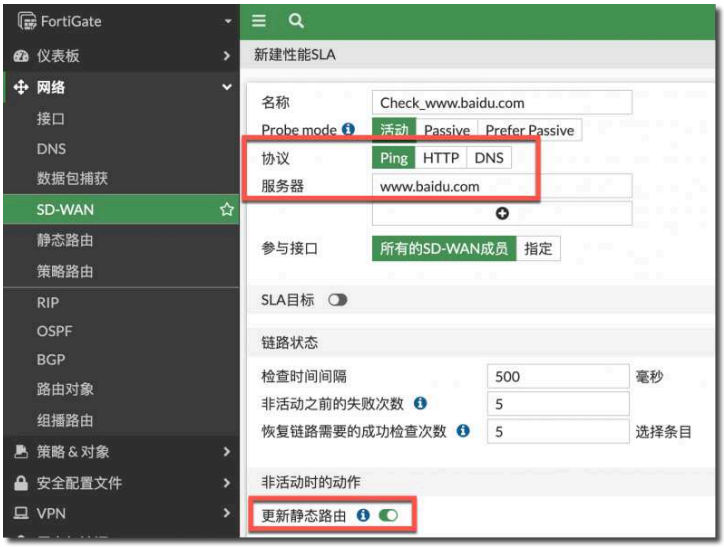


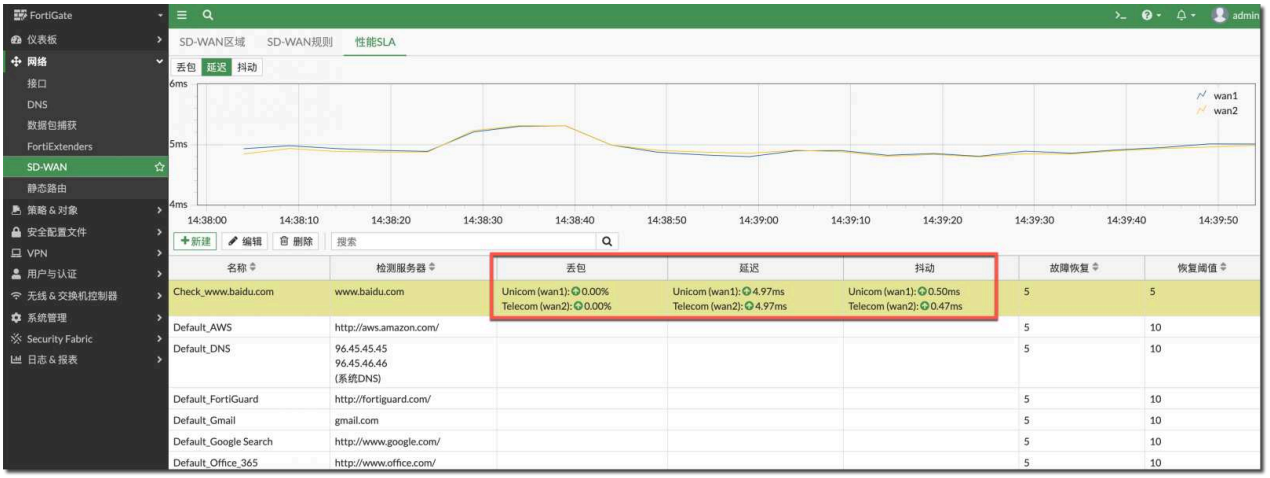
2. 添加SD-WAN的默认路由。



3. 配置SD-WAN的SLA，以便wan1和wan2相互备份和切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. SD-WAN规则可根据需求配置，这里保持默认的按照源IP负载均衡。



安全策略配置

1. 需求与规划：

   - 员工的有线与无线都需要访问互联网
   - 访客的无线仅仅可以访问互联网
   - 员工的有线和无线需要互访

2. 建议将防火墙的接口划分区域，以区域的方式配置策略，有时候可以做到简化配置的目的，甚至未来替换设备的时候，策略的备份和还原也会更加简单一些。规划区域两个区域：

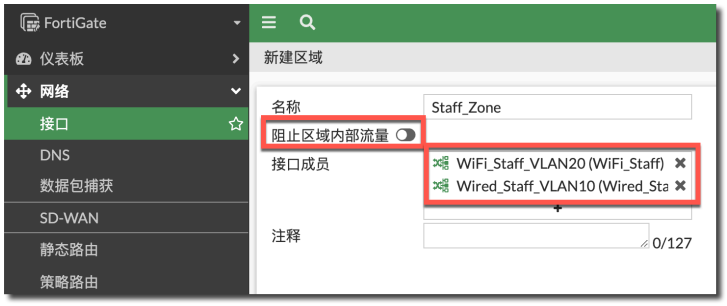
   - 员工网络区域：包括员工的有线VLAN 10和员工的无线VLAN 20 （区域之间的隔离关闭，这样VLAN 10和VLAN 20之间的数据可通）
   - 访问网络区域：包括访问的无线VLAN 30

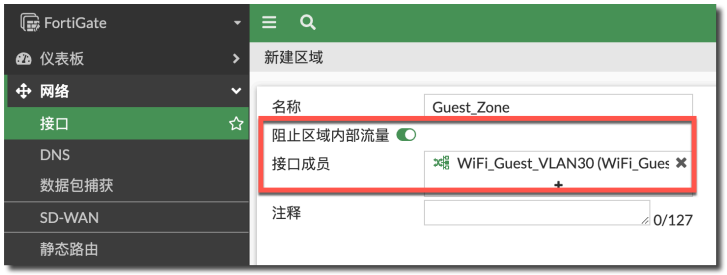
3. 进入网络→接口页面，新建所属区域。

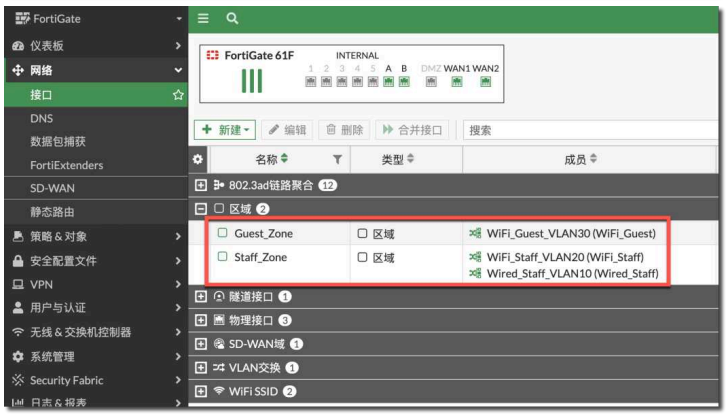
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 分别创建Staff_Zone（包含VLAN 10和VLAN20）和Guest_Zone（包含VLAN30）。







5. 如此只需要配置两条策略，就可以实现我们规划的需求，新建Staff-Zone到SD-WAN与Guest-Zone到SD-WAN的安全策略。

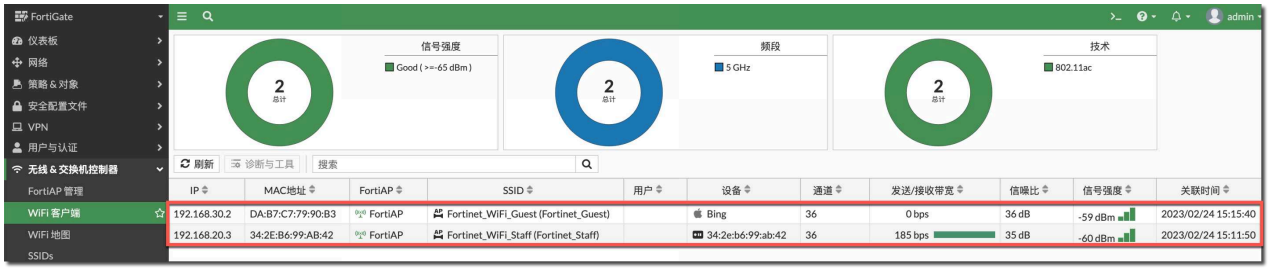


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

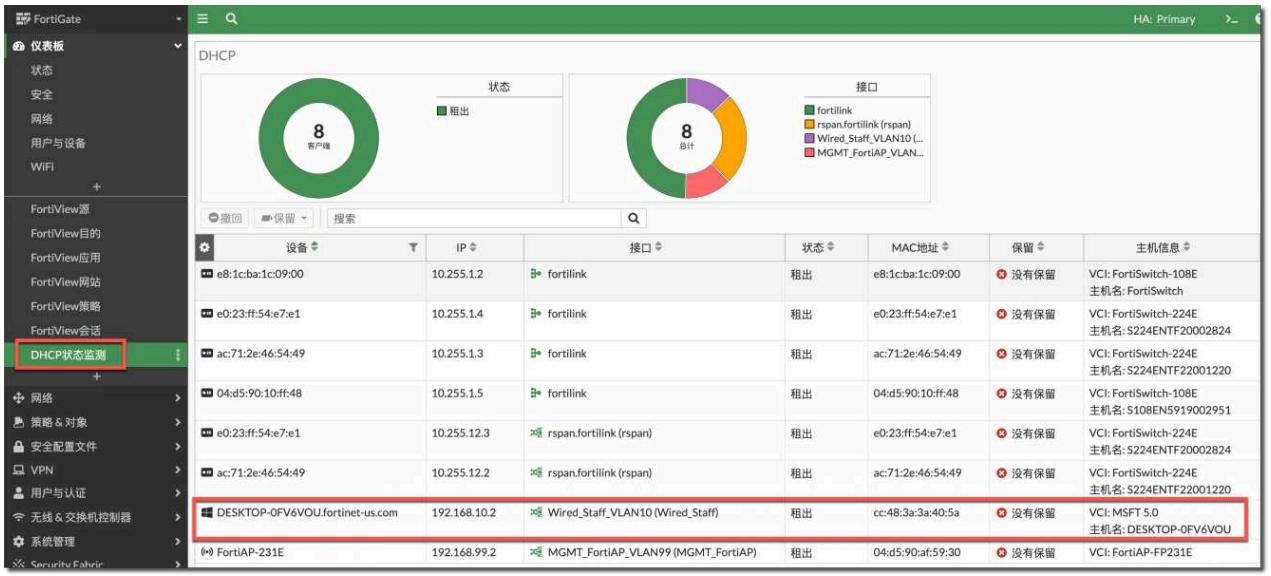
结果验证

客户端访问

1. 进入无线&交换机控制器→WiFi客户端，查看在线的无线客户端。可以看到WiFi_Staff和WiFi_Guest各有一个终端在线。



2. 在DHCP状态检测中查看所有的客户端信息，可以看到有线网络的PC也正常上线。

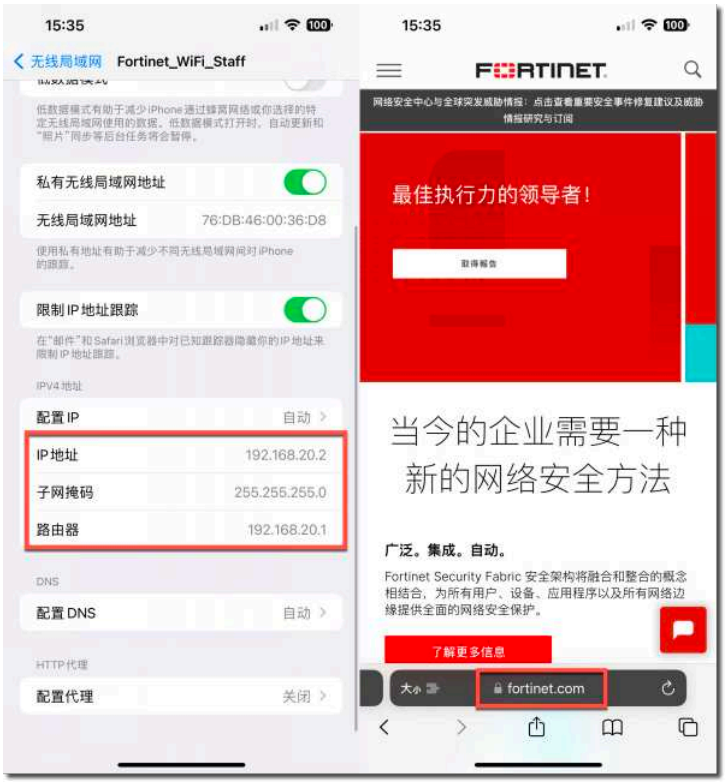


3. 有线网络（VLAN 10）用户访问互联网。

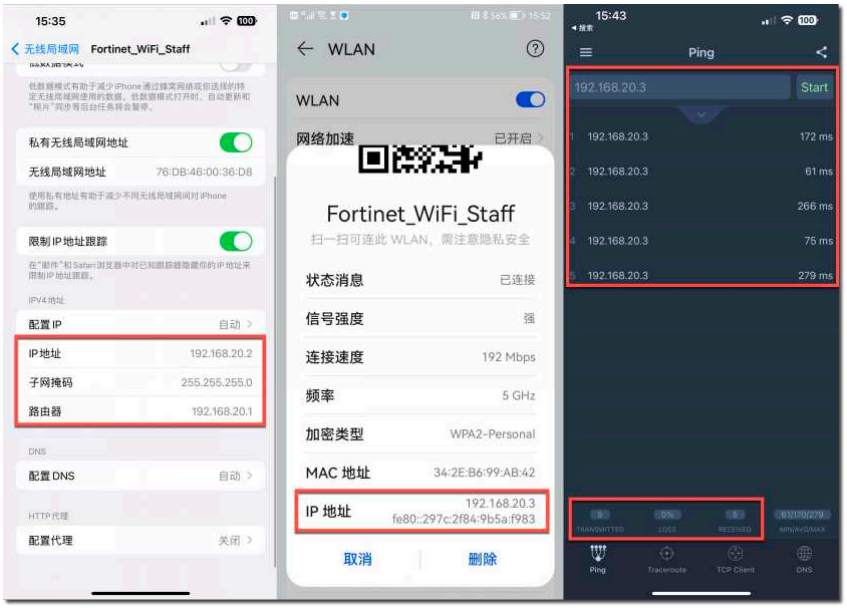


4. 无线网络用户访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

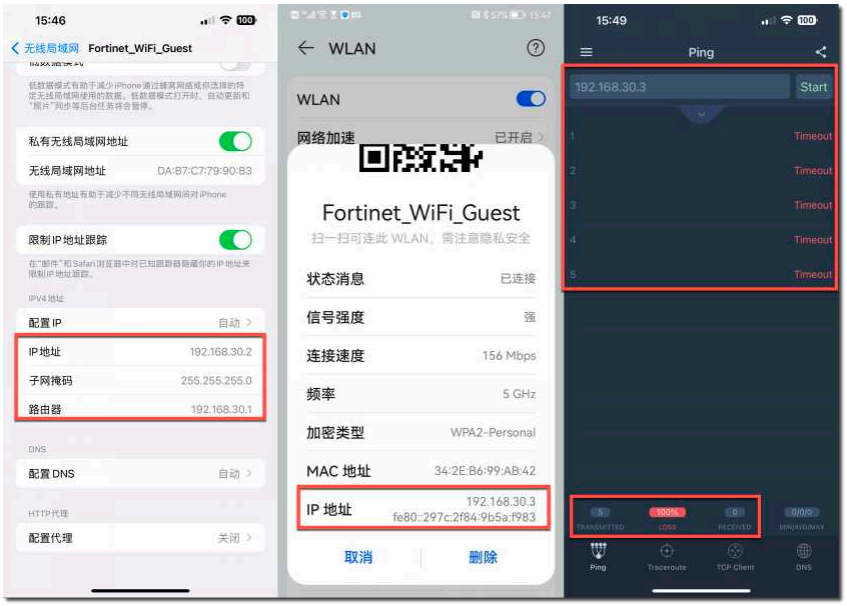


5. 使用VLAN 20下的客户端访问VLAN 20下的另一个客户端（Staff区域）。



6. 使用VLAN 30下的客户端访问VLAN 30下的另一个客户端（Guest区域），可以看到由于该区域配置了禁止相互访问，所以VLAN 30下的客户端是无法互相访问的。

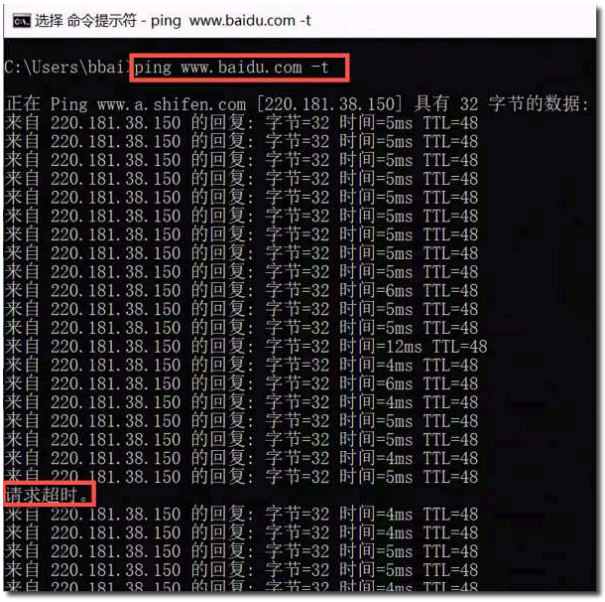
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiLink切换测试

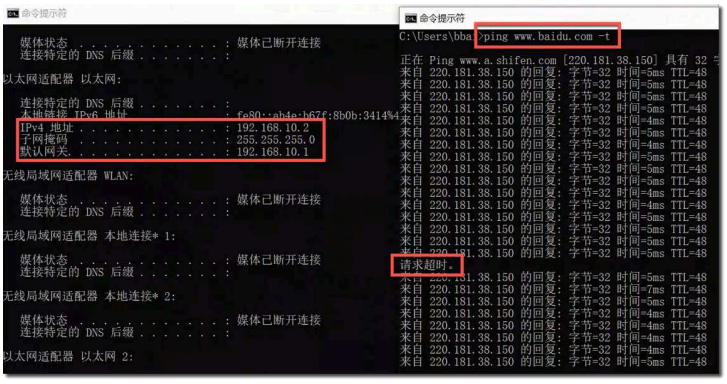
1. 在我们的测试场景下FortiLink聚合接口的a和b是同时UP起来的，如果a或b DOWN（不能同时DOWN），是否有影响业务呢?

2. 经过测试，DOWN a或b接口，客户端丢包1个或者不丢包。



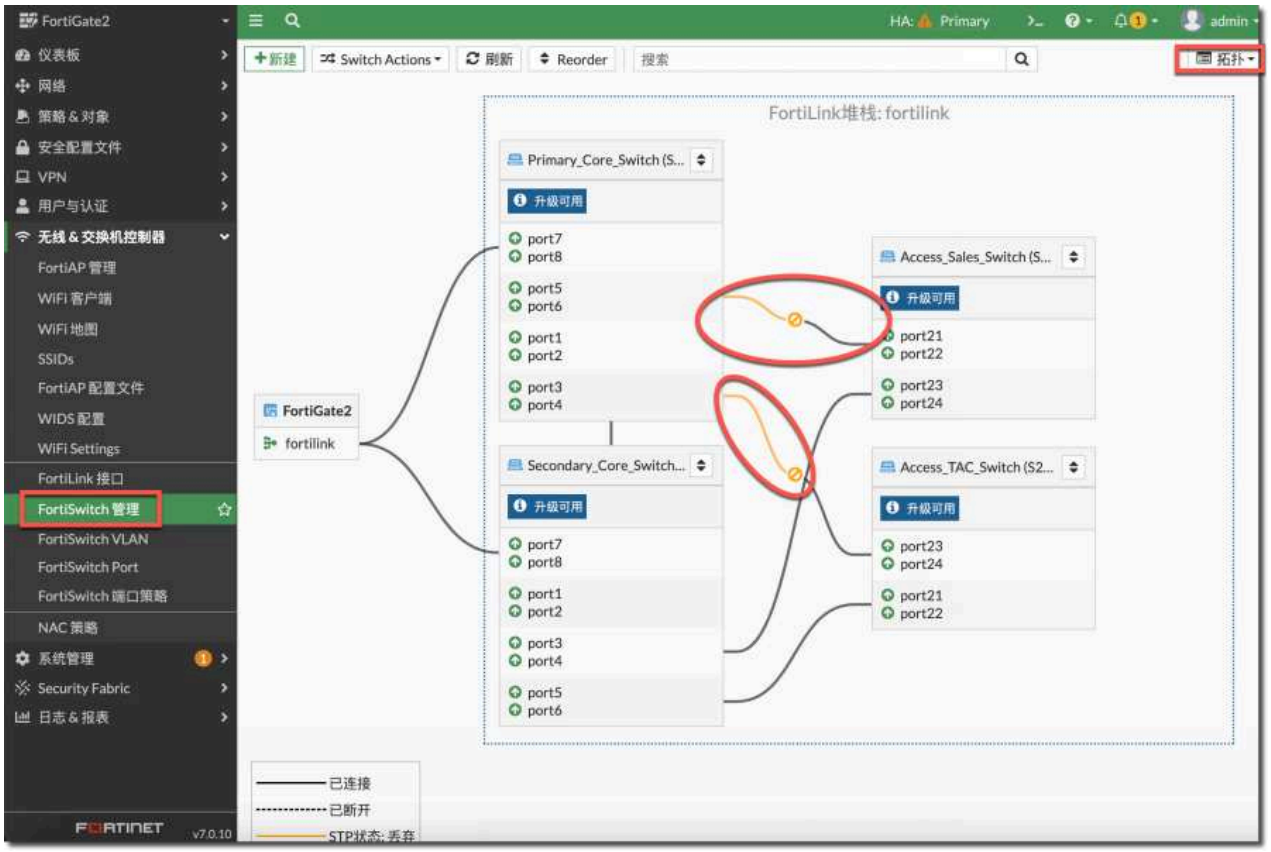
HA切换测试

1. 重启主防火墙查看内网PC丢包情况，HA切换丢包1个。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 此时查看原备（新主）防火墙的FortiLink交换机接管状态，流量全部会切换到备防火墙和备核心交换机上。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink环形组网

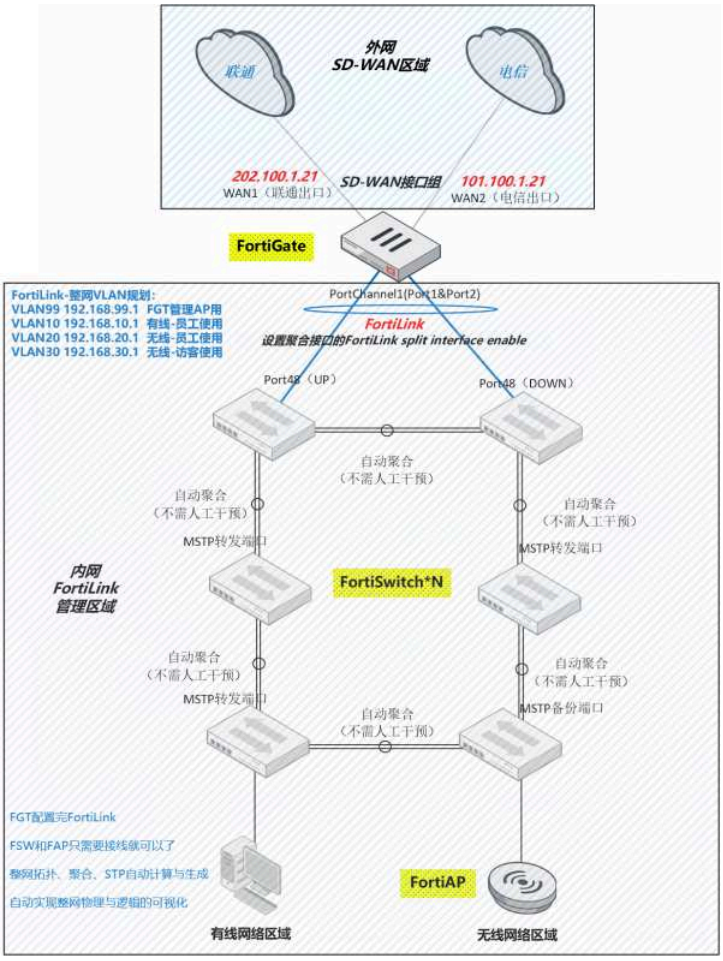
星型组网的另外一个组网方式是环形组网部署。

FortiLink交换机环形组网的特性是设计上无单点故障，任何交换机或交换机的任意接口故障，都不会影响到整体网络的连通性，MSTP自动收敛后业务即可恢复，可靠性比较高。

环形拓扑

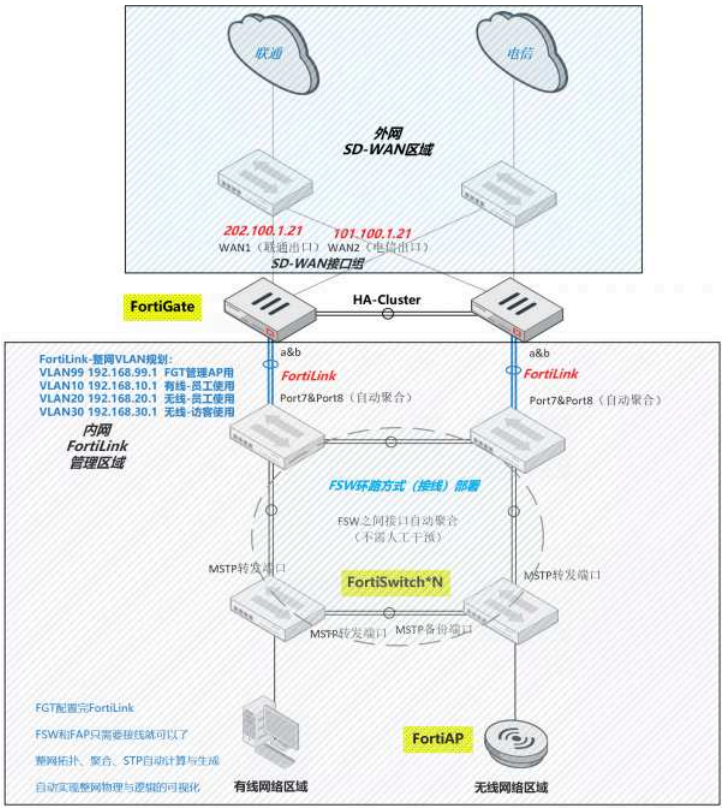
单FortiGate组网

此方案防火墙存在单点故障。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate HA组网



1. 环形组网是比较好的方式，唯一的问题是环路太大了，一旦网络中出现接口震荡等情况，MSTP会出现反复的计算和收敛，一个环内的交换机越多STP速度就越慢，通常不推荐超过16台的FortiLink环（最多20台FortiGate的环路）。
2. 有没有更好的解决办法呢？实际上需要将星型组网和环形组网结合起来就可以比较好的解决环过大的问题。我们可以取名叫做星型环形混合组网，请参考SAA-FortiLink→FortiLink部署方案说明和举例→FortiLink部署之星型环形混合组网 ↗章节。

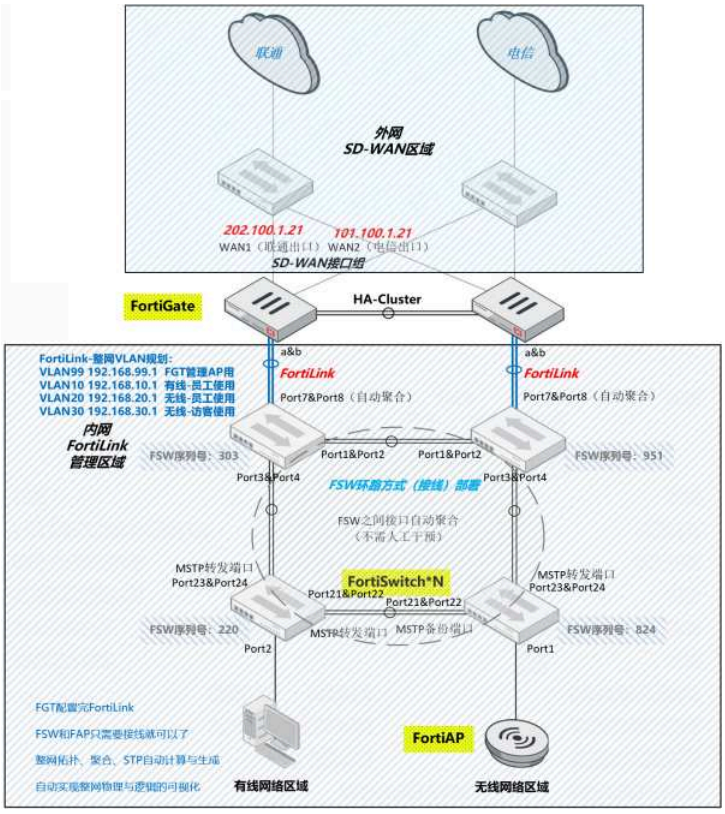
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink环形组网配置举例

网络需求

FortiGate运行HA-Cluster，核心交换和接入交换机采用全聚合接口（FortiSwitch全自动聚合，接线即可，无需手工配置聚合接口）对接的环形组网结构。

网络拓扑



1. 两台FortiGate配置为HA主备模式。
2. 整体规划：
   - 外网IP网段规划：
     - WAN1联通出口：IP 202.100.1.21，GW 202.100.1.192
     - WAN2电信出口：IP 101.100.1.21，GW 101.100.1.192
   - WAN1和WAN2合并成SD-WAN接口。
   - 内网IP网段规划，FGT通过FortiLink+Capwap协议统一的接管FortiSW和FortiAP，为有线和无线统一进行管理和业务处理：
     - 有线网络规划：VLAN 10，192.168.10.1
     - 无线网络规划：员工WIFI VLAN 20，192.168.20.1
     - 无线网络规划：访客WIFI VLAN 30，192.168.30.1
     - 管理FortiAP：VLAN 99，192.168.99.1
   - FortiLink互联部分规划：
     - FortiGate的a和b做聚合接口与Fortiswitch的后两个接口互联即可实现聚合接口的FortiLink管理。
     - 加入FortiLink的接口自动变为聚合口成员。

配置步骤

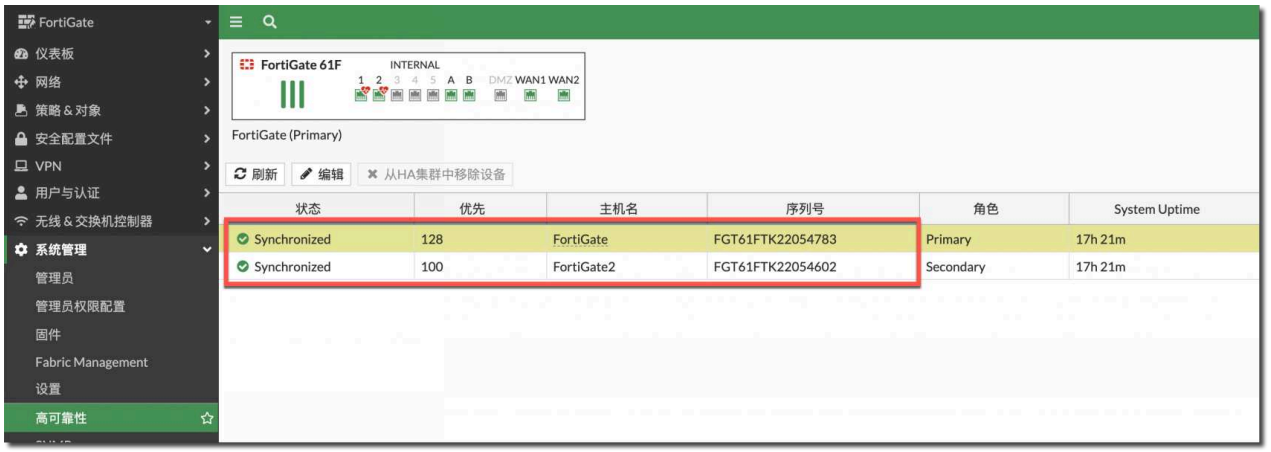
准备事项

1. 首先确认FortiGate如下全局配置已开启（一般默认为开启状态）。

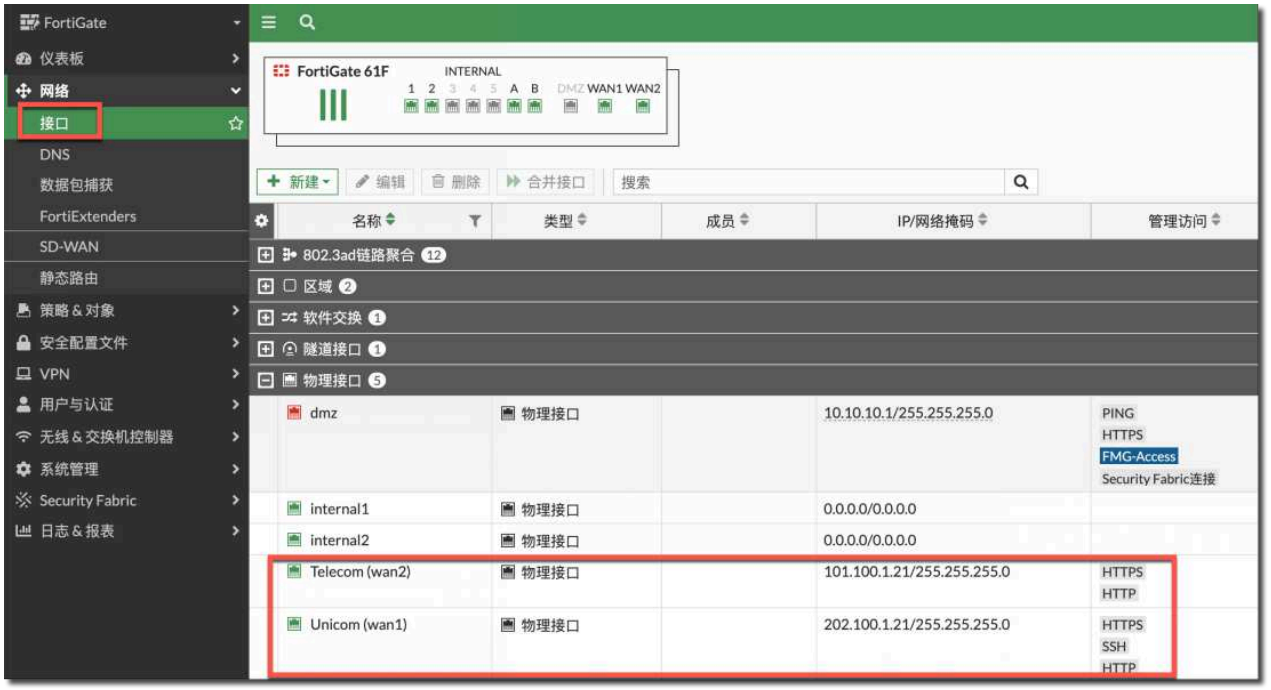
```
config system settings
    set gui-switch-controller enable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置两台FortiGate的HA主备模式（配置方法请参考HA双机热备→HA典型基础配置 ↗）。



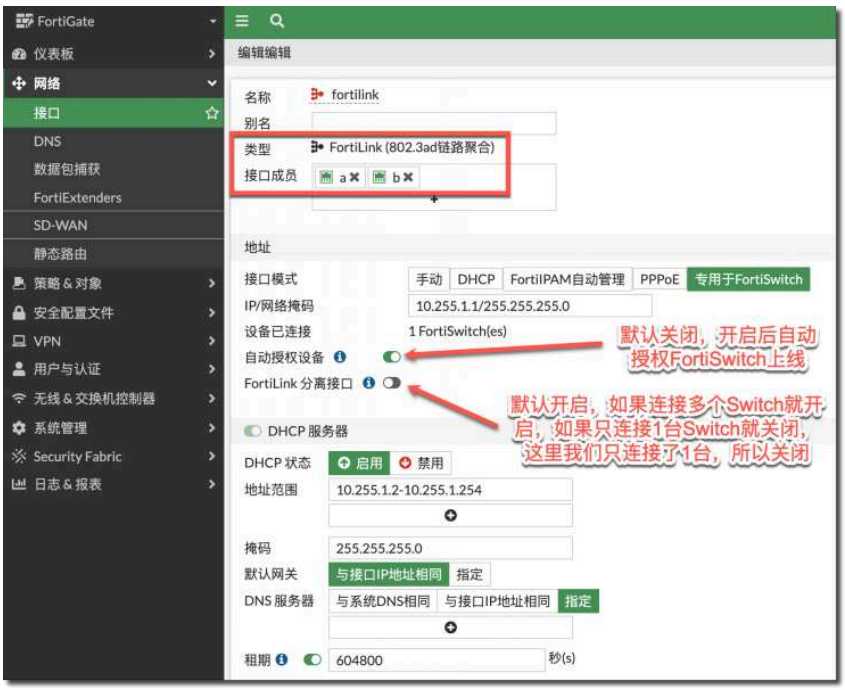
3. 配置wan1和wan2的IP地址。



4. 配置FortiLink实现FortiSwith上线，我们只需要将用于FortiLink的成员接口加入FortiLink接口即可。此拓扑中，FortiGate用于连接FortiSwitch的接口为a和b，编辑FortiLink接口，将a和b加入FortiLink（某些产品型号会默认将两个接口加入FortiLink），开启自动授权设备，关闭FortiLink分离接口，其他配置保持默认，可以看到FortiLink为一个聚合接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

FortiLink分离接口什么时候应该开启?

分离接口的意是，如果聚合接口的port1和port2分别连接了一台SW，在没有使用MCLAG的情况下（没开启堆叠功能），则聚合接口的port1和port2没办法同时UP（同时开启聚合接口无法正常工作），因此必须开启FortiLink分离接口功能，让聚合接口只有一个物理接口（port1）是处于UP状态的，另外一个物理接口（port2）处于DOWN的备份状态，当port1接口状态DOWN，则Port2立即接管Port1的工作，让聚合接口的FortiLink继续运行，这是一个聚合接口在FortiLink管理时候的备份机制。



重要

FortiLink split interface什么时候应该disable?

如果FGT的聚合接口只接到了一台交换机上，并没有跨交换机聚合（没有MCLAG，也不需要FortiLink split interface），因此这种情况应该让聚合接口的两个物理接口port1和port2同时UP，两个接口同时工作起来，以便提供更高带宽和备份的作用。



相关CLI:

```
NTP:
config system ntp
    set ntpsync enable
    set server-mode enable
    set interface "fortilink"
end
--------------------------------------------------------------------
DHCP:
config system dhcp server
    edit 2
        set dns-service local
        set ntp-service local
        set default-gateway 10.255.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.255.1.2
                set end-ip 10.255.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end
────────────────────────────────────────────────────────────────────────
FortiLink:
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "a" "b"
        set lldp-reception enable
        set lldp-transmission enable
        set auto-auth-extension-device enable
        set fortilink-split-interface disable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
    next
end
```

连接FortiLink

1. 配置完FortiGate之后，这个时候再去接FortiGate的FortiLink到FortiSwitch的线，以及FortiSwitch之间的线，严格按照拓扑图，从核心交换机往接入交换机这样的顺序接线。FortiSwitch如果以前有使用过，建议都恢复一下出厂设置，然后再加入到FortiLink。
2. FortiSwitch的靠后接口一般都默认开启了FortiLink接口属性，如果接前面的接口可能会无法加入到FortiLink，因此FortiSwitch的FortiLink最好都使用靠后的接口进行接线。FortiSwitch各型号默认开启FortiLink功能的接口如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiSwitch型号	默认开启FortiLink的接口
FS-108D-POE	port9–port10
FS-108E, FS-108E-POE, FS-108E-FPOE	port7–port10
FSR-112D-POE	port5–port12
FS-124D, FS-124D-POE	port23–port26
FSR-124D	port1-port4, port21–port28
FS-124E, FS-124E-POE, FS-124E-FPOE	port21–port28
FS-148E, FS-148E-POE	port21–port52
FS-224D-POE	port21–port24
FS-224D-FPOE	port21–port28
FS-224E, FS-224E-POE	port21–port28
FS-248D, FS-248D-FPOE	port45–port52
FS-248D-POE	port47–port50
FS-248E-POE, FS-248E-FPOE	port45–port52
FS-424D, FS-424D-POE, FS-424D-FPOE	port23–port26
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30
FS-548D	port39–port54
FS-548D-FPOE, FS-548DN	port45–port54
FS-1024D	port1–port24
FS-1048D, FS-1048E	port1–port52
FS-3032D, FS-3032E	port1–port32

3. 如果FortiSwitch无法被FortiGate管理，登陆到FortiSwitch上进行确认接口是否开启了FortiLink。

```
FortiSwitch # show switch interface port9
config switch interface
    edit "port9
        set auto-discovery-fortilink enable    //接口下又此命令的接口才可以自动加入到FortiLink中//
    next
end
```

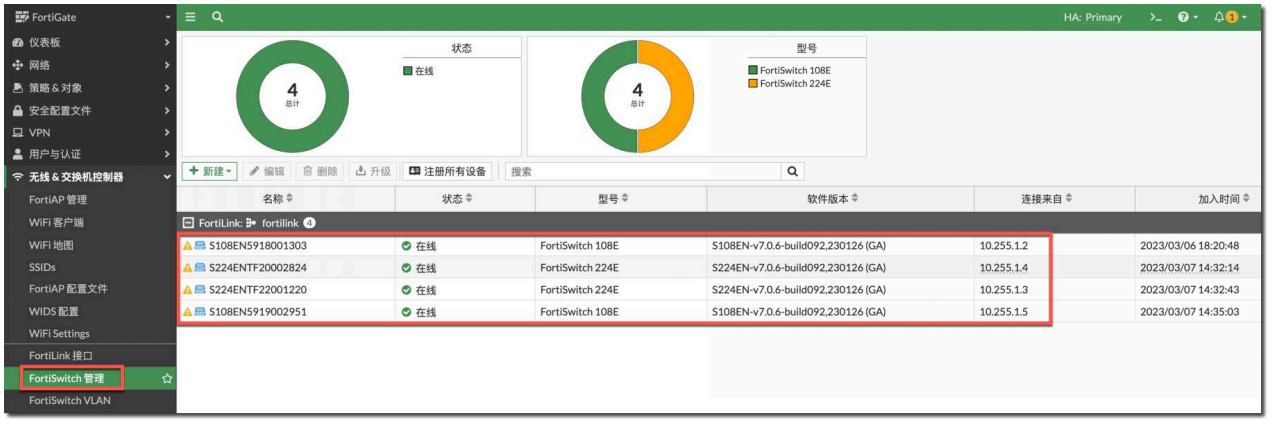
4. 交换机之间如果接多根线，会自动进行聚合，但是FortiLink自动聚合会花比较长的时间，建议可以先接单线，等FortiLink的拓扑较快的形成结束之后，再增加彼此之间的另外一根线，再进行自动聚合，这样效率会比较高一些。

5. 接线是很重要的步骤，仔细看拓扑图，做好接口标签，不要接错。

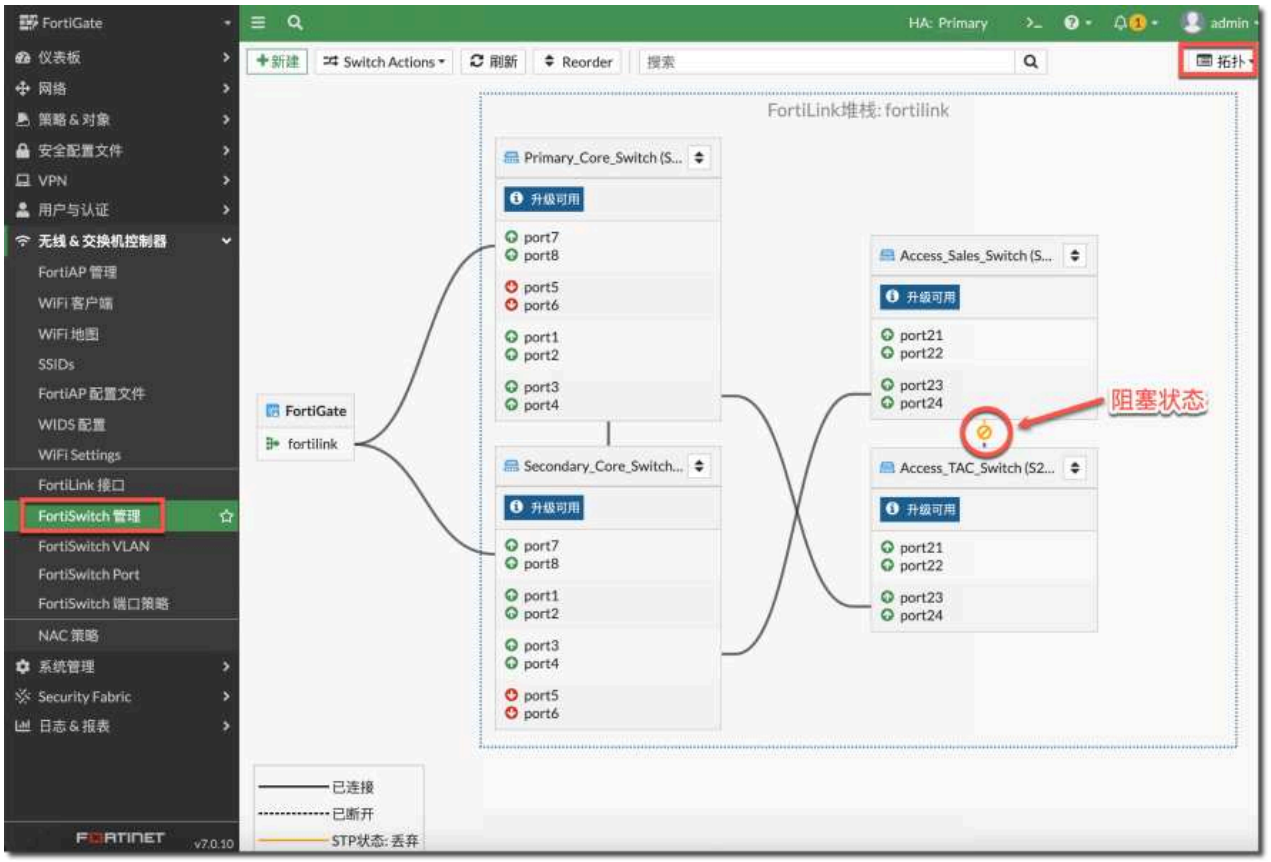
6. 接好线之后，FortiSwitch和FortiGate之间会自动在后台进行FortiLink、CAPWAP、MSTP、聚合接口的协商加入等操作，等FortiLink的管理结束之后，在FortiGate上会看到一个网站的FortiSwitch拓扑图，和我们规划的拓扑图应该是一致的，可以仔细核对接线是否正确。

7. 在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，查看交换机被管理状态，可以看到4台交换机均已上线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



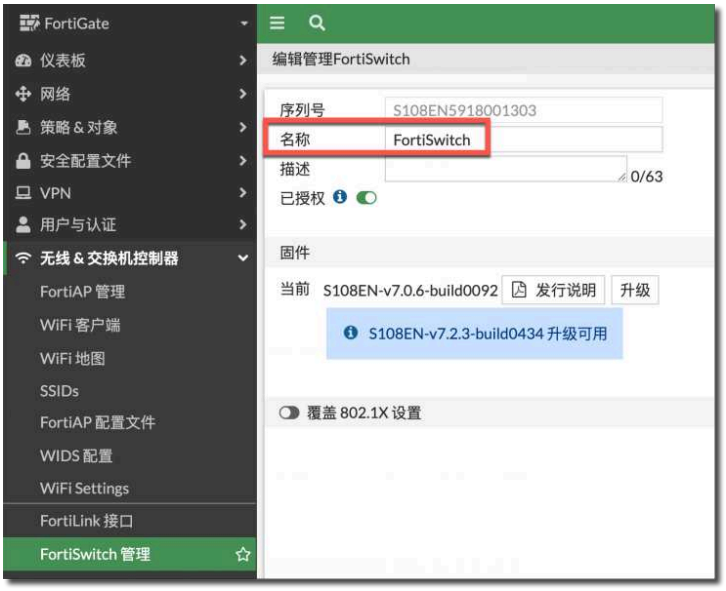
8. 修改视图为拓扑，可以更直观的看到当前防火墙与交换机的接口连接。



9. 交换机加入到FortiGate的FortiLink，会先清除配置再重启，然后从standalone的状态进入到“Fortilink remote control”的状态，后续所有的配置都通过FortiGate下发即可。

0. 编辑交换机，可以修改交换机名字以及升级版本，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. FortiSwitch之间接多根线进行FortiLink互联，会默认自动聚合。其实接一根网线也是聚合的，只是聚合组里面只有一个接口而已，因此多根网线直连，这些直连的线都会自动加入到一个聚合接口里面（注意不能跨交换机，跨交换机的聚合是MCLAG）。

```bash
FortiGate # exec ssh admin@10.255.1.2
Warning: Permanently added '10.255.1.2' (ED25519) to the list of known hosts.
admin@10.255.1.2's password:

S108EN5918001303 # show switch trunk
path=switch, objname=trunk, tablename=(null), size=752
config switch trunk
    edit "GT61FTK22054783"
        set mode lacp-active
        set auto-isl 1
        set fortilink 1
        set members "port7" "port8"
    next
    edit "4ENTF20002824-0"
        set mode lacp-active
        set auto-isl 1
        set members "port5" "port6"
    next
    edit "4ENTF22001220-0"
        set mode lacp-active
        set auto-isl 1
        set members "port3" "port4"
    next
    edit "8EN5919002951-0"
        set mode lacp-active
        set auto-isl 1
        set members "port1" "port2"
    next
end
```

2. 另外建议给每台交换机命名一个名字，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



STP状态查看

1. FortiLink之间的交换机互联，如果不用MCLAG的话，本质上是MSTP（多实例生成树）在整网统一的进行接口环路计算，从而实现网络的备份，与快速收敛恢复。 可以通过FGT的命令行界面用Telent/SSH到FortiSwitch上并分别查看四台FortiSwitch的STP状态。

   - 主核心交换机（303）上查看：

```
FortiGate # exec ssh admin@10.255.1.2
Warning: Permanently added '10.255.1.2' (ED25519) to the list of known hosts.
admin@10.255.1.2's password:

Primary_Core_Switch #  diagnose stp instance list
MST Instance Information, primary-Channel:
 ...
Instance ID 15
  Config         Priority 24576, VLANs 4094
                 Bridge MAC e81cba1c0900
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 0
                 (This bridge is the regional root)
  //直连主FGT的FSW会自动将网桥优先级降低到：Priority 24576，因此整个FortiLink二层网络中，自己就是根网桥//
  TCN Events     Triggered 10 (0d 0h 24m 59s ago), Received 67 (0d 0h 24m 26s ago)
  Port               Speed   Cost       Priority   Role         State        Flags
  _________________  ______  _________  _________  ___________  ___________  _________________
  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
  GT61FTK22054783    2G      10000      128        DESIGNATED   FORWARDING   ED
  //与主FortiGate_FortiLink互联的自动生成的聚合接口，STP为指定接口，转发状态//
  4ENTF22001220-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与序列号220结尾的FSW互联的自动生成的聚合接口，STP为指定接口，转发状态//
  8EN5919002951-0    2G      1          128        DESIGNATED   FORWARDING   EN
  //与备核心交换机303互联的自动生成的聚合接口，STP为指定接口，转发状态//
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

   - 备核心交换机（951）上查看：

```
FortiGate # exec ssh admin@10.255.1.5
Warning: Permanently added '10.255.1.5' (ED25519) to the list of known hosts.
admin@10.255.1.2's password:

Secondary_Core_Switch # diagnose stp instance list
MST Instance Information, primary-Channel:
 ...
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC 04d59010ff48
                 //自己的MAC
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 1, Root Port 8EN5918001303-0
  //互联根网桥的信息：根网桥MAC e81cba1c0900，根网桥优先级 24576，互联根网桥的接口 8EN5918001303-0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  TCN Events     Triggered 4 (0d 0h 41m 4s ago), Received 2 (0d 0h 41m 32s ago)
  Port               Speed   Cost       Priority   Role          State        Flags
  _________________  ______  _________  _________  ____________  ___________  _________________
  internal           1G      20000      128        DESIGNATED    FORWARDING   ED
  8EN5918001303-0    2G      1          128        ROOT          FORWARDING   EN
  //与主核心交换机303互联的自动生成的聚合接口，STP为root接口，转发状态
  4ENTF20002824-0    2G      1          128        DESIGNATED    FORWARDING   EN
  //与序列号824结尾的FSW互联的自动生成的聚合接口，STP为指定接口，转发状态
  GT61FTK22054602    2G      10000      128        DESIGNATED    FORWARDING   ED
  //与备FortiGate_FortiLink互联的自动生成的聚合接口，STP为指定接口，转发状态（但由于连的是备防火墙，实际物理口是discarding状
态）
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

- 接入交换机（220）上查看：

```
FortiGate # exec ssh admin@10.255.1.3
admin@10.255.1.3's password:

Access_TAC_Switch # diagnose stp instance list
MST Instance Information, primary-Channel:
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC ac712e465448
                 //自己的MAC地址
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 1, Root Port 8EN5918001303-0
  //互联根网桥的信息：根网桥MAC e81cba1c0900，根网桥优先级 24576，互联根网桥的接口8EN5918001303-0
  TCN Events     Triggered 1 (0d 1h 12m 46s ago), Received 6 (0d 1h 9m 25s ago)
  Port               Speed   Cost       Priority   Role          State        Flags
  _________________  ______  _________  _________  ____________  ___________  _________________
  internal           1G      20000      128        DESIGNATED    FORWARDING   ED
  8EN5918001303-0    2G      1          128        ROOT          FORWARDING   EN
  //接主核心交换机303，STP为根接口，转发状态
  4ENTF20002824-0    2G      1          128        DESIGNATED    FORWARDING   EN
  //接Sales接入交换机824，STP为指定接口，转发状态
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

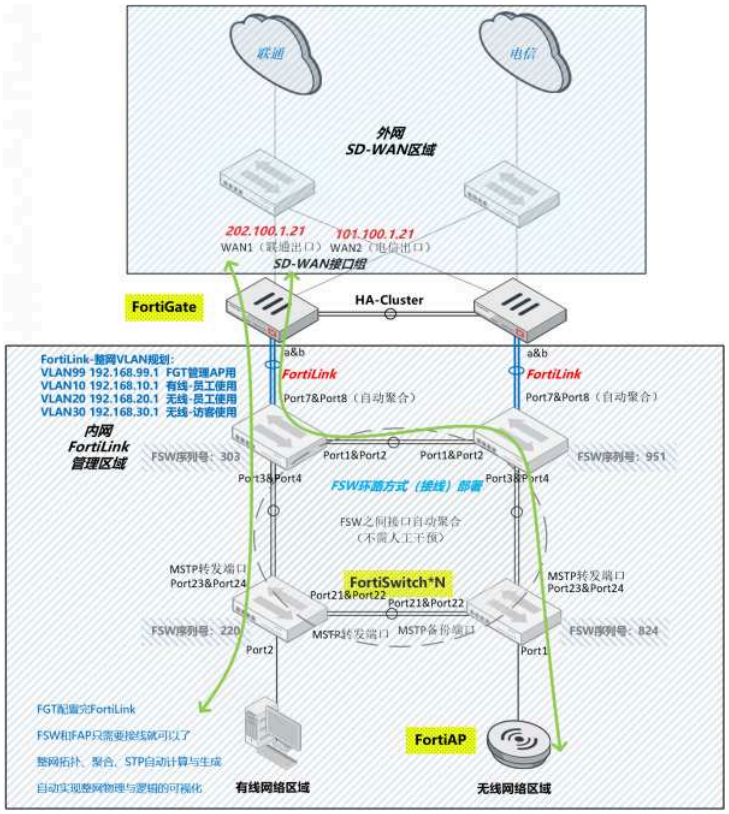
- 接入交换机（824）上查看：

```
FortiGate # exec ssh admin@10.255.1.4
admin@10.255.1.4's password:

Access_Sales_Switch # diagnose stp instance list
MST Instance Information, primary-Channel:
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC e023ff54e7e0
                 //自己的MAC地址
  Regional Root  MAC e81cba1c0900, Priority 24576, Path Cost 1, Root Port 8EN5918001303-0
  //互联根网桥的信息：根网桥MAC e81cba1c0900，根网桥优先级 24576，互联根网桥的接口8EN5918001303-0
  TCN Events     Triggered 1 (0d 1h 22m 45s ago), Received 7 (0d 1h 18m 58s ago)
  Port               Speed   Cost       Priority   Role          State        Flags
  _________________  ______  _________  _________  ____________  ___________  _________________
  internal           1G      20000      128        DESIGNATED    FORWARDING   ED
  4ENTF22001220-0    2G      1          128        ALTERNATIVE   DISCARDING   EN
  //接TAC接入交换机303，STP为备份接口ALTERNATIVE DISCARDING，处于阻塞状态
  8EN5919002951-0    2G      1          128        ROOT          FORWARDING   EN
  //接备核心交换机951，STP为根接口，转发状态
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

2. FortiLink组网中STP是很重要部分，通常STP是一个稳定的状态，一旦出现FortiLink不稳定，则需要观察STP的状态和选举结果，从中找到相关线索，以便查出为何STP不稳定的原因，对于排错来说是很重要的。

3. FortiLink+STP稳定状态的实际数据转发拓扑图如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

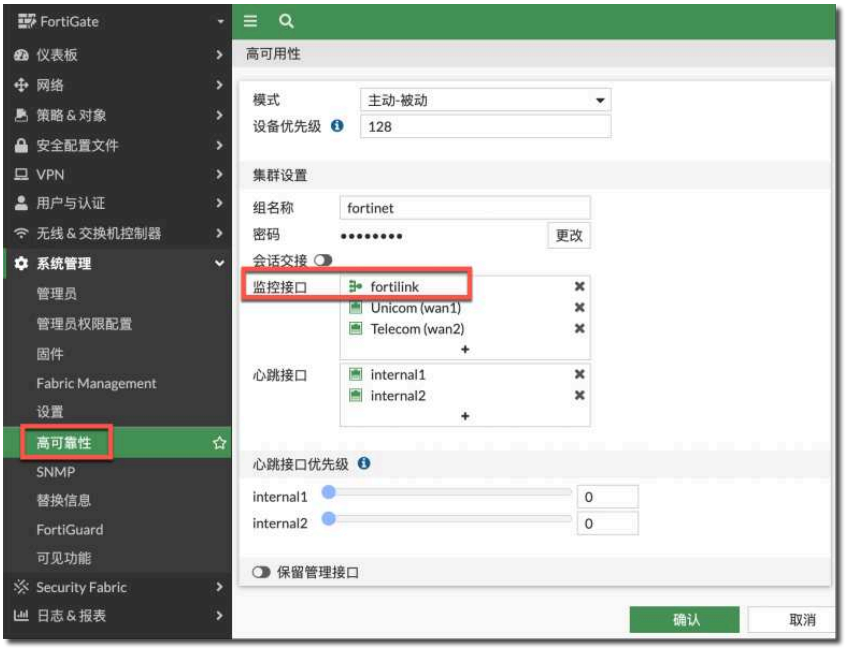


4. 在FortiGate查看交换机管理状态。

```
FortiGate # execute switch-controller get-conn-status
Managed-devices in current vdom root:
FortiLink interface : fortilink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME            NAME
S108EN5918001303  v7.0.6 (092)      Authorized/Up   -   10.255.1.2      Mon Mar  6 18:20:48 2023
Primary_Core_Switch
S224ENTF20002824  v7.0.6 (092)      Authorized/Up   -   10.255.1.4      Tue Mar  7 14:32:14 2023
Access_Sales_Switch
S224ENTF22001220  v7.0.6 (092)      Authorized/Up   -   10.255.1.3      Tue Mar  7 14:32:43 2023
Access_TAC_Switch
S108EN5919002951  v7.0.6 (092)      Authorized/Up   -   10.255.1.5      Tue Mar  7 14:35:03 2023
Secondary_Core_Switch
        Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error, 3=L3
        Managed-Switches: 4 (UP: 4 DOWN: 0)
```

5. 最后不要忘记，在FortiLink的聚合接口和FortiLink管理配置完毕，记得把这个FortiLink聚合接口加入到HA的监控接口列表中，这样当主核心交换机挂了（比如断电）之后，业务才可以平稳切换到备防火墙上。

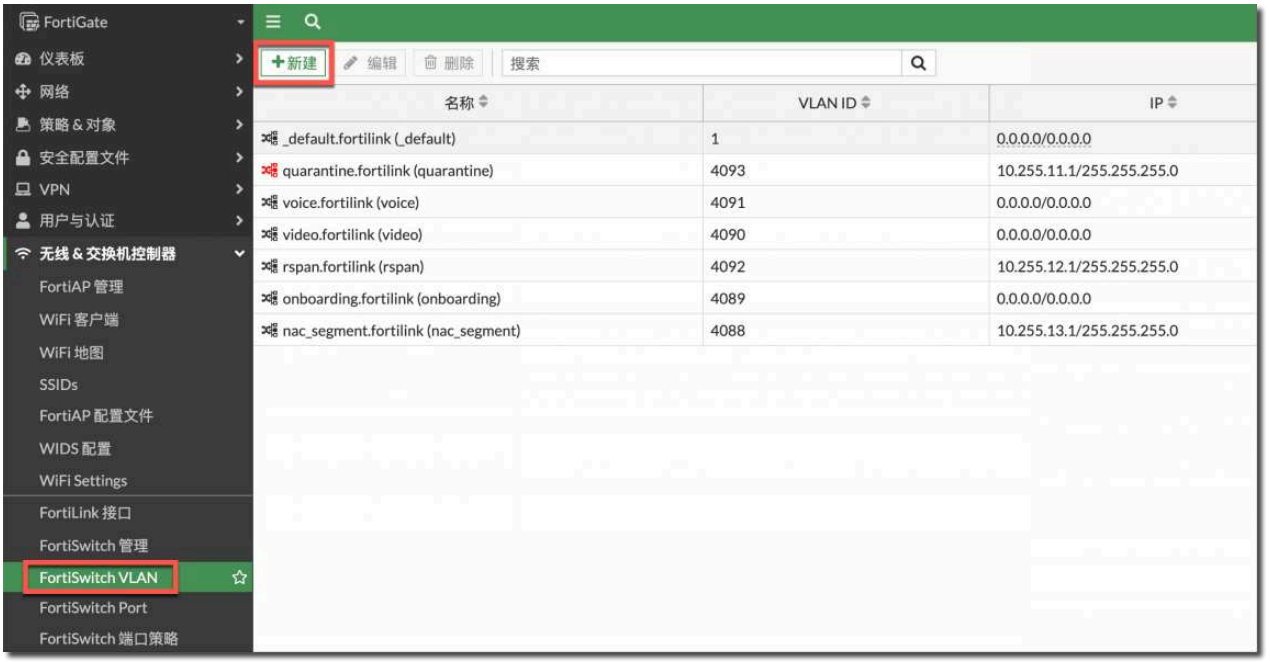
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



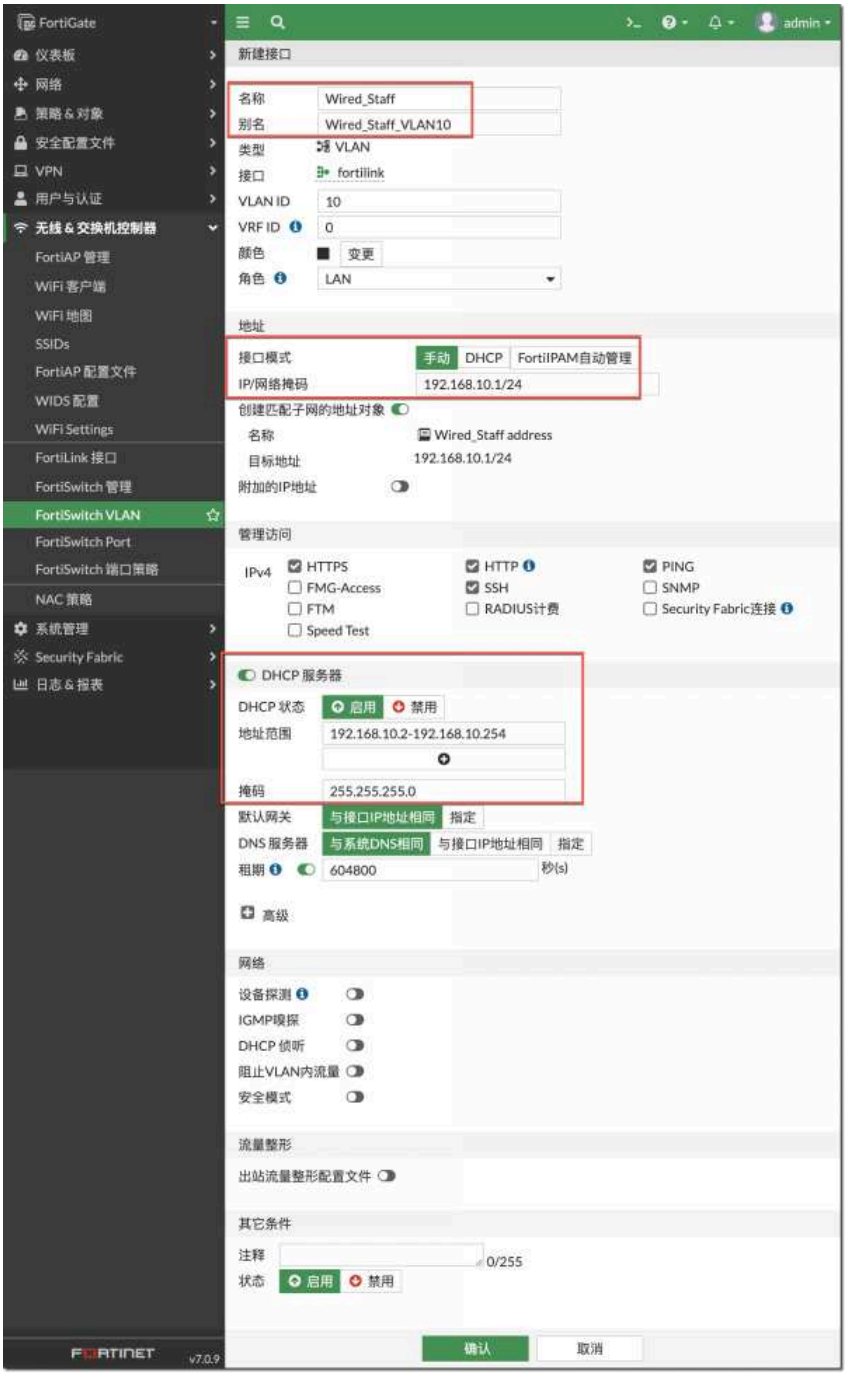
创建VLAN

1. FortiGate通过FortiLink + Capwap协议统一的接管FortiSwitch和FortiAP，为有线和无线统一进行管理和业务处理。
2. 进入FortiGate的无线&交换机控制器→FortiSwitch VLAN页面，新建有线网络VLAN 10、员工无线网络VLAN 20、访客无线网络VLAN 30、管理FortiAP VLAN 99。注意管理FortiAP的VLAN接口要开启Security Fabric，包含CAPWAP。

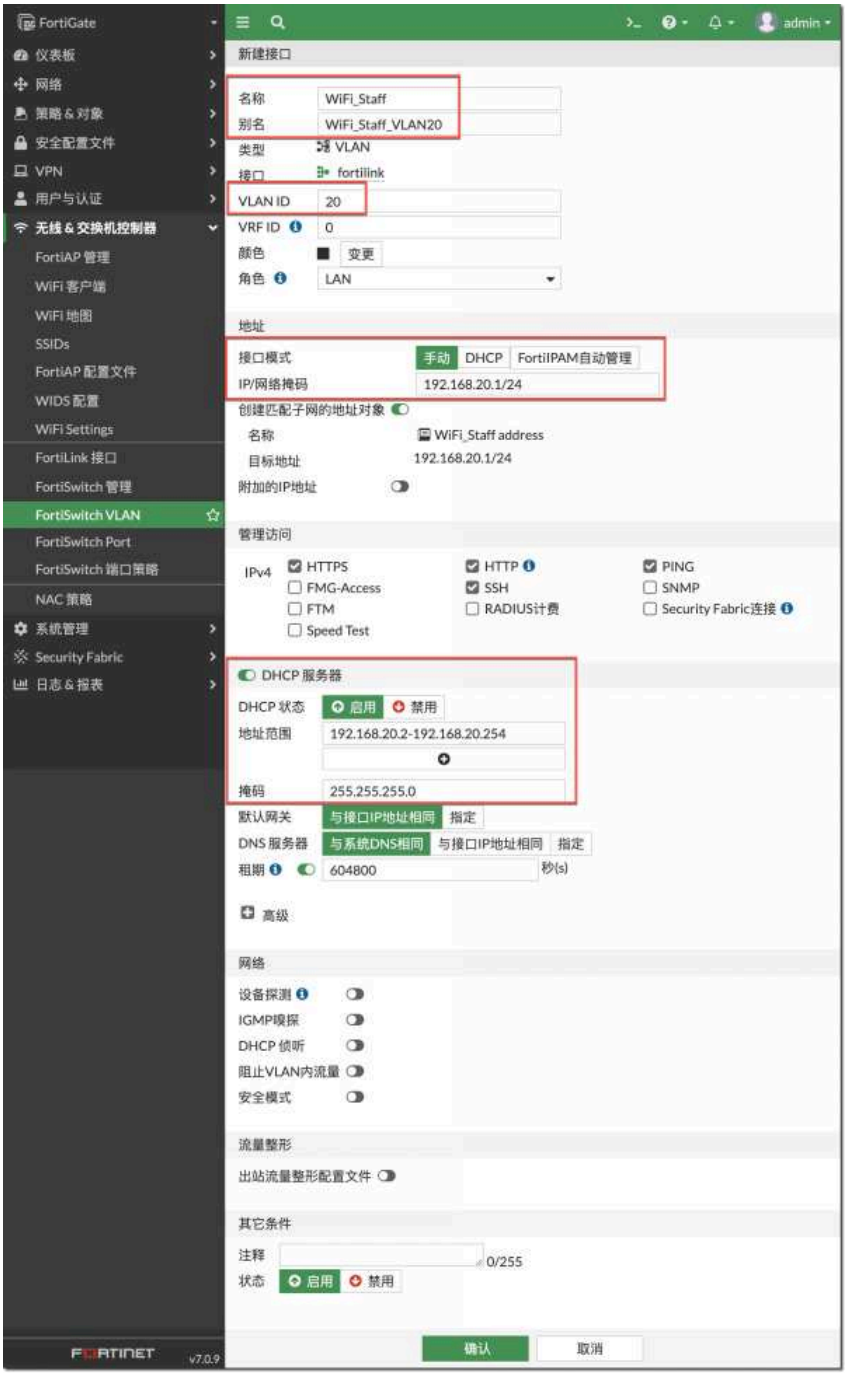
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



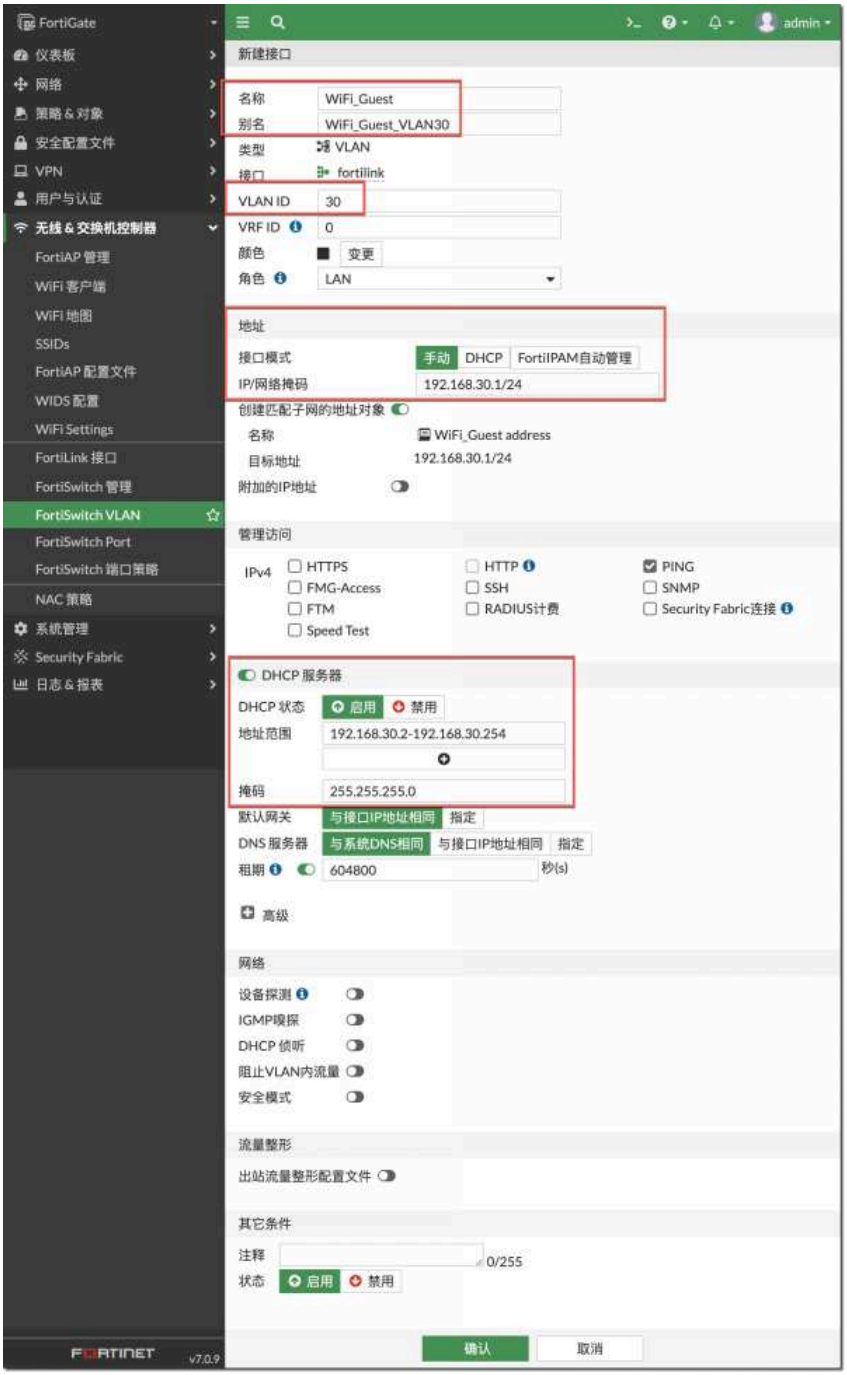
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



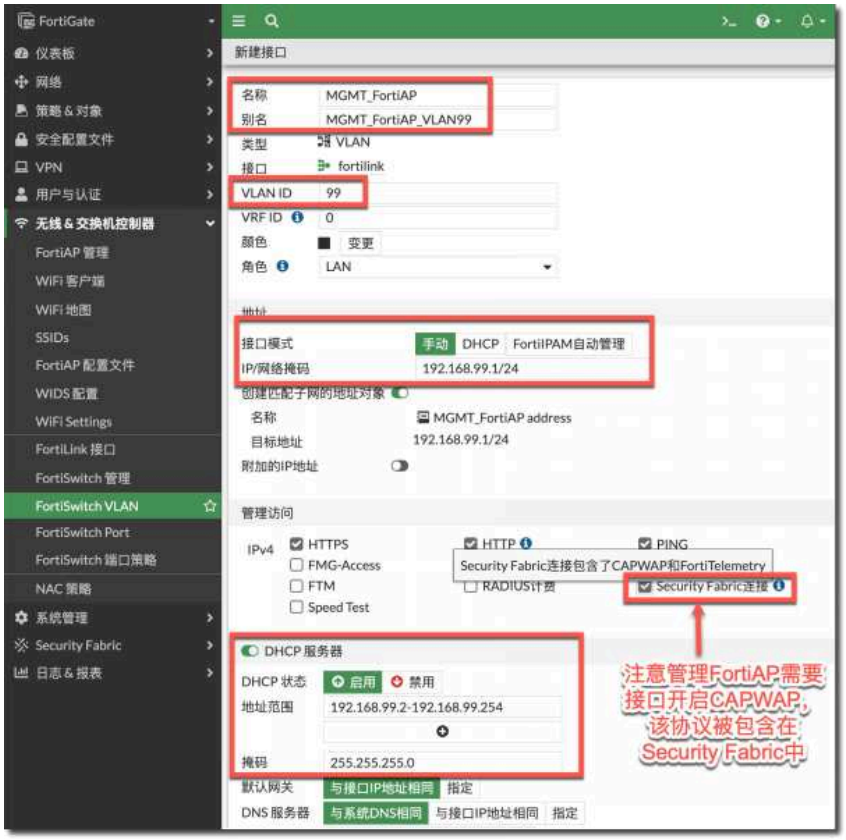
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

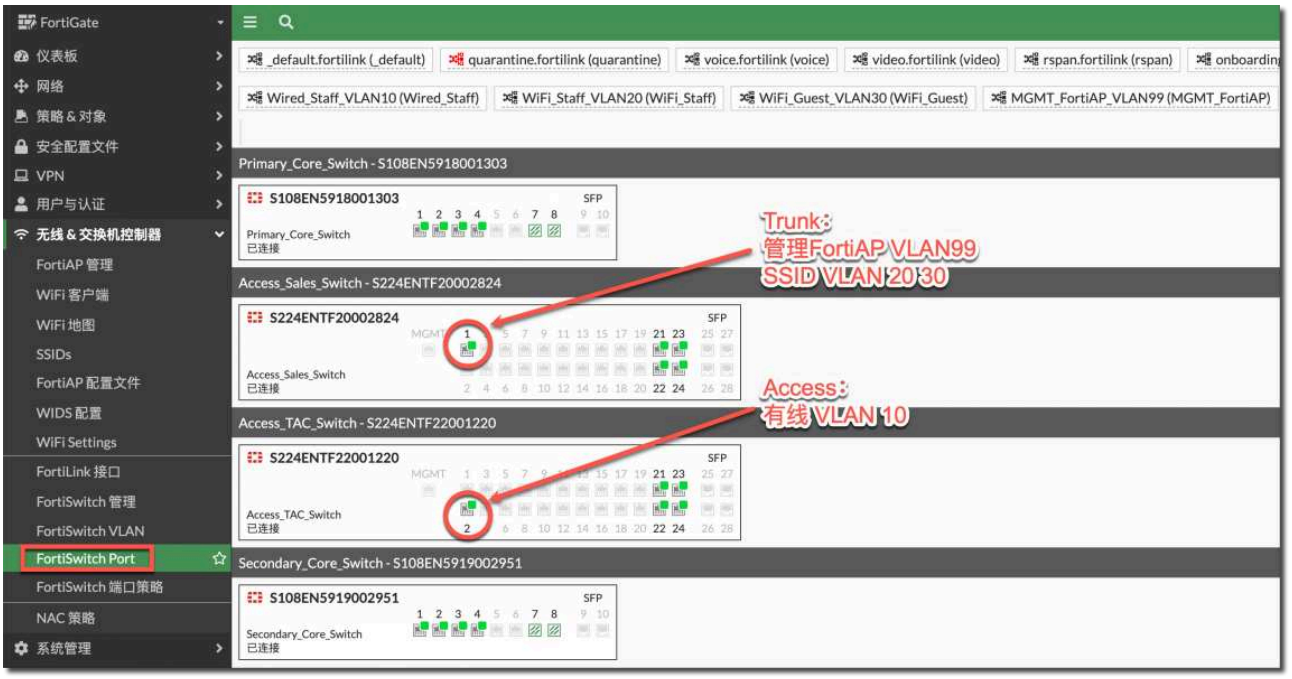


3. VLAN创建完成。

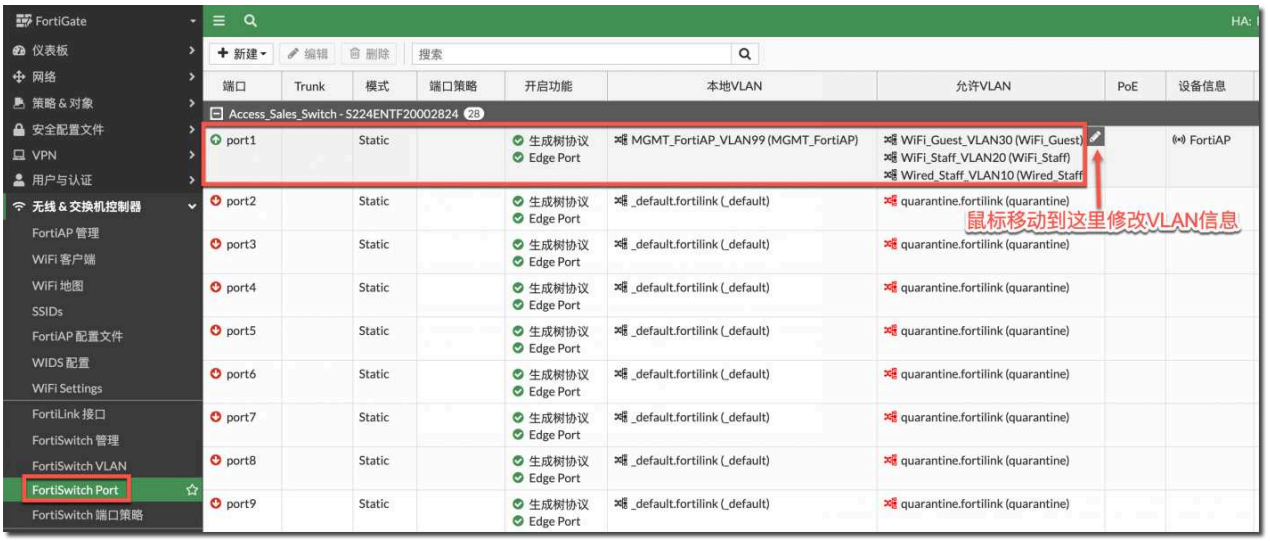


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

分配VLAN

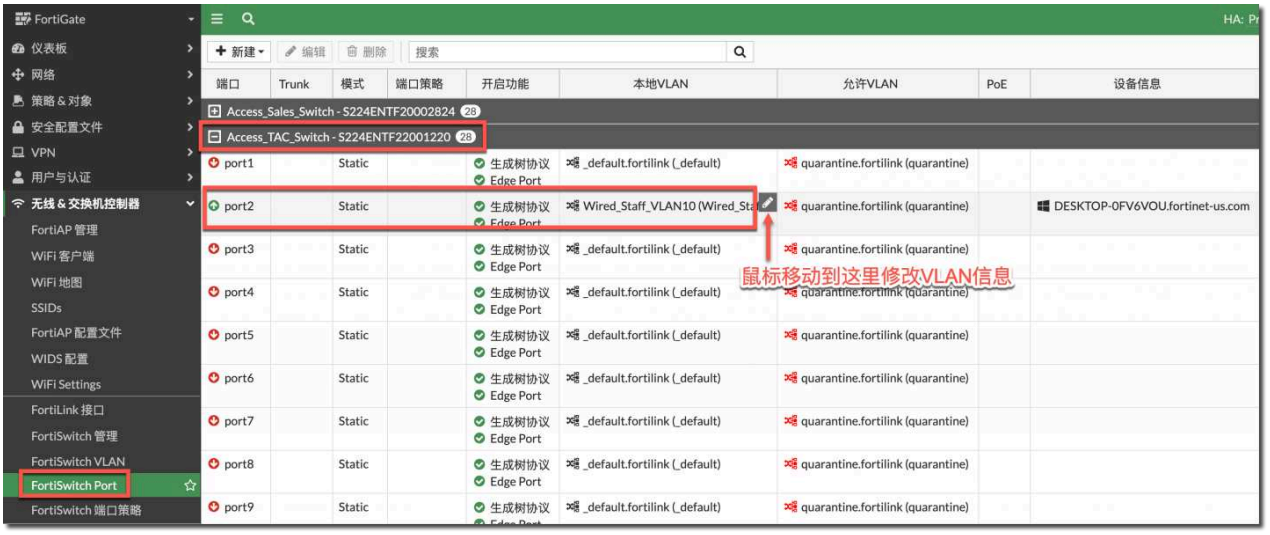


1. Sales接入交换机的port1接FortiAP，配置为Trunk模式，允许 VLAN20和VLAN30，VLAN20用于WIFI-STAFF的SSID用户，VLAN30用于WIFI-GUEST的SSID用户。另外本地VLAN设置为VLAN 99，用于FortiAP的管理（FortiAP的管理相当于使用不打vlan-tag的VLAN 99，本地VLAN默认是VLAN 1，因此只需要将本地VLAN设置为VLAN 99即可）。



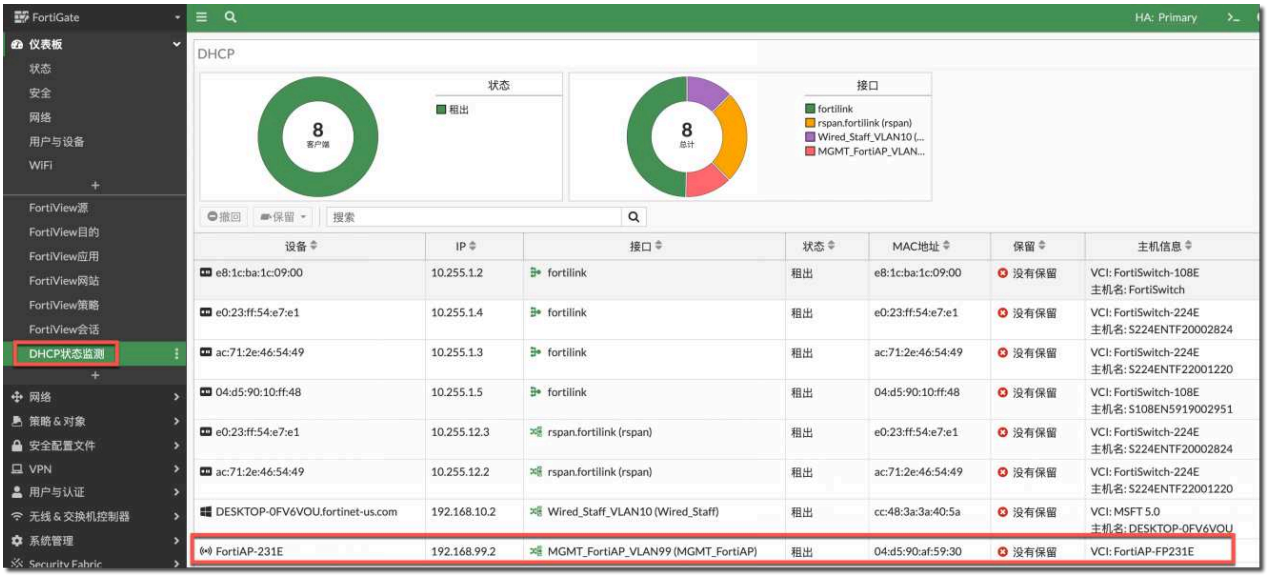
2. TAC接入交换机的Port2接具体的物理PC，因此只需要将Port2设置为access口，分配VLAN 10即可，用FortiSwitch的概念来说就是将本地VLAN设置为VLAN 10，本地VLAN不打vlan-tag，相当于就是设置接口为access vlan 10。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



无线配置

1. FortiAP连接后，会通过VLAN 99的DHCP获取到192.168.99.0/24网段的IP地址。



2. 在之前的配置中，VLAN 99的接口开启了CAPWAP协议（包含在Security Fabric中），激活了FortiGate的无线管理功能，这时候FortiAP会自动找到FGT进行注册。因此在FortiAP管理的地方可以看到这个FortiAP的信息（如果没有看到检查配置，并将FortiAP恢复出厂，让FortiAP重新获取IP地址并发起注册）。



3. 右键点击上图中等待认证的FortiAP，点击授权按钮，等待几分钟，FortiAP成功上线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 编辑FortiAP设置，配置FortiAP的名称，或进行升级操作。



5. 进入无线&交换机控制器→SSIDs页面，点击新建按钮。

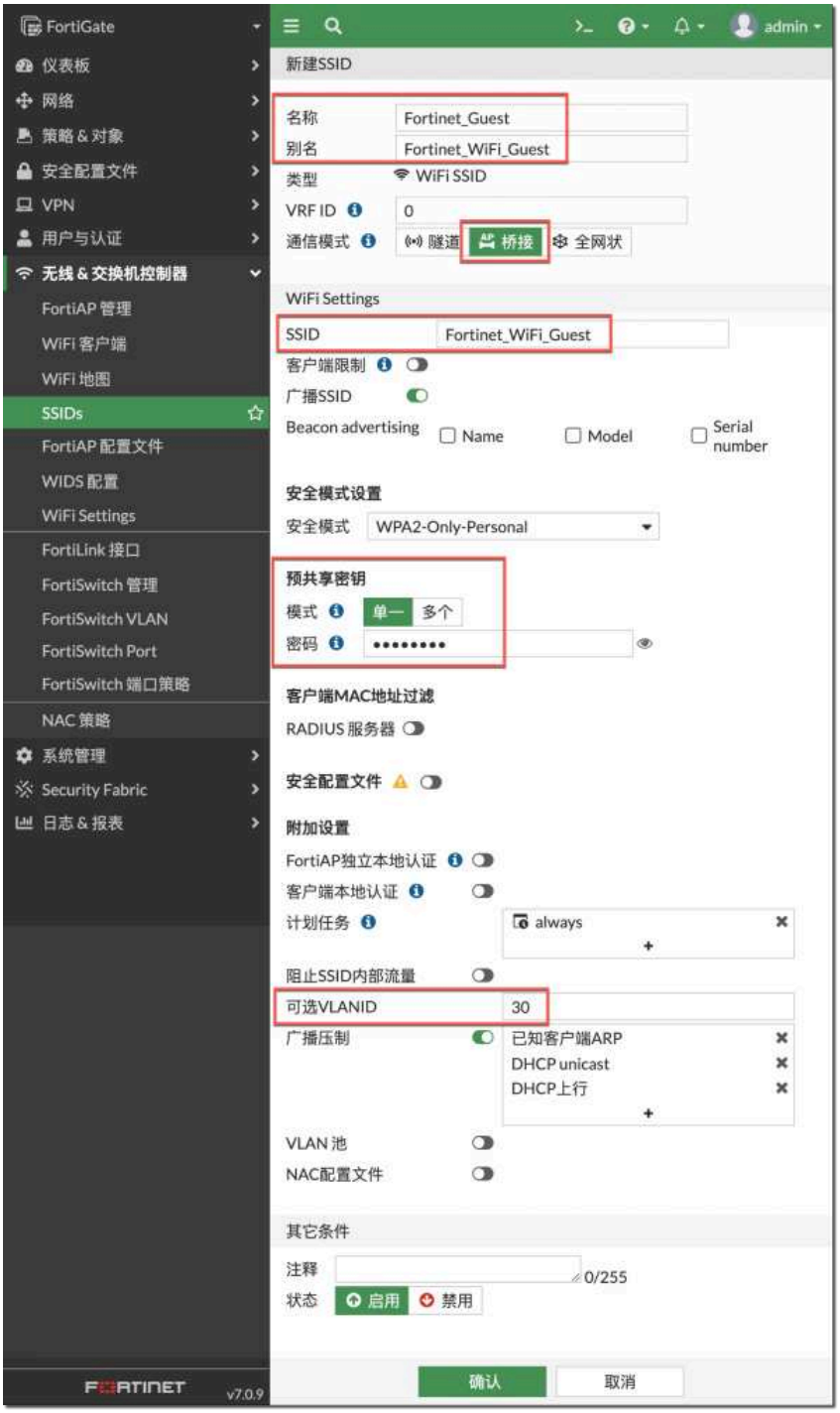


6. 新建SSID：Fortinet_WiFi_Staff VLAN 20用于员工WIFI使用，Fortinet_WiFi_Guest VLAN 30用于访客WiFi使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





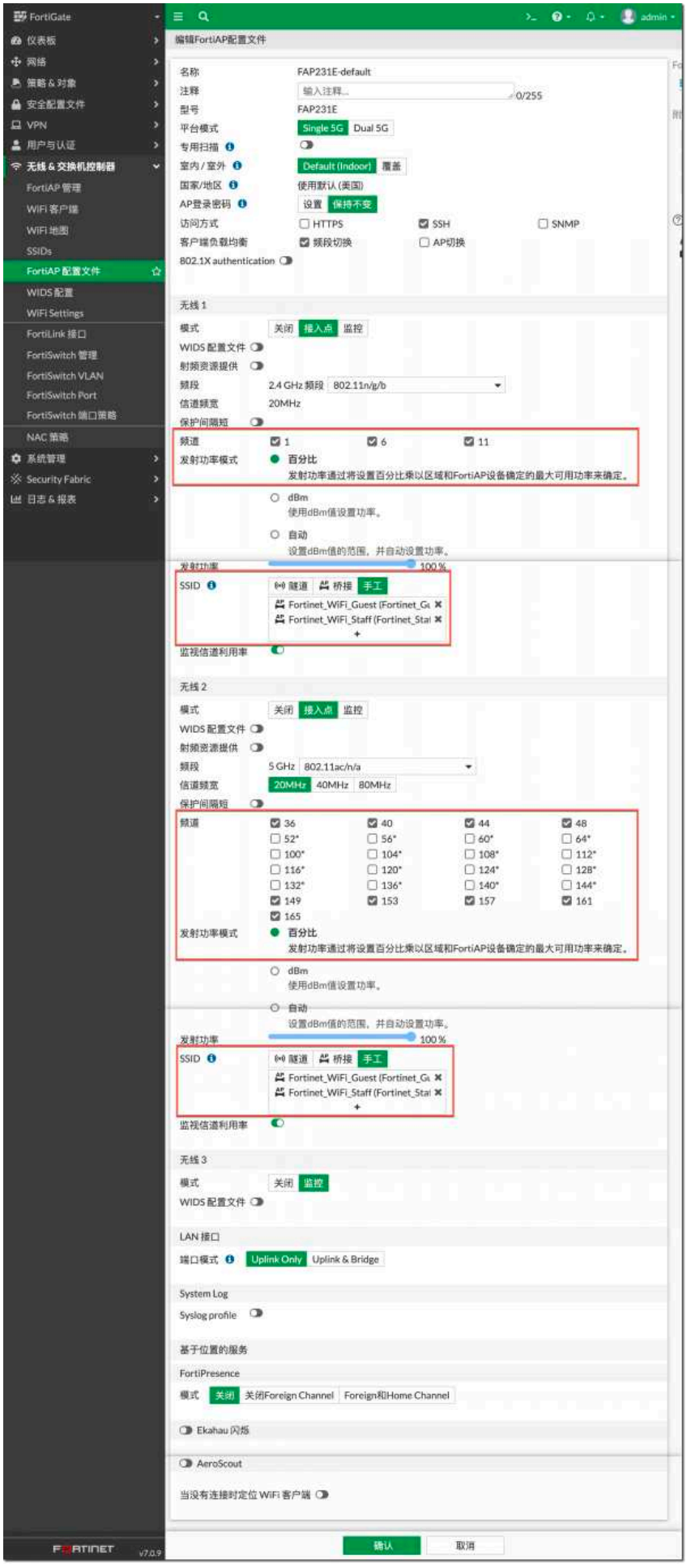
7. 将SSID关联到FortiAP上，然后让FortiAP发布无线SSID信号，这样用户就可以通过SSID连接到无线了。进入FortiAP配置文件页面，编辑FortiAP关联的配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 桥模式的SSID需要在FortiAP配置文件里面手工指定一下，另外下图标示出的配置为推荐配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

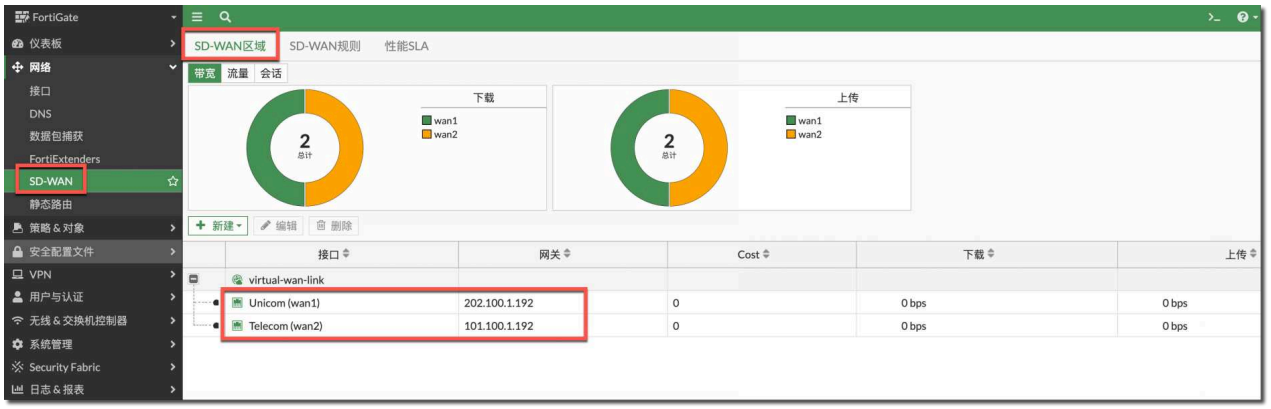


9. FortiAP会自动关联到这个FortiAP配置文件里面的内容，发起SSID的信号。



SD-WAN配置

1. 将wan1和wan2加入SD-WAN接口，并配置各自的网关。

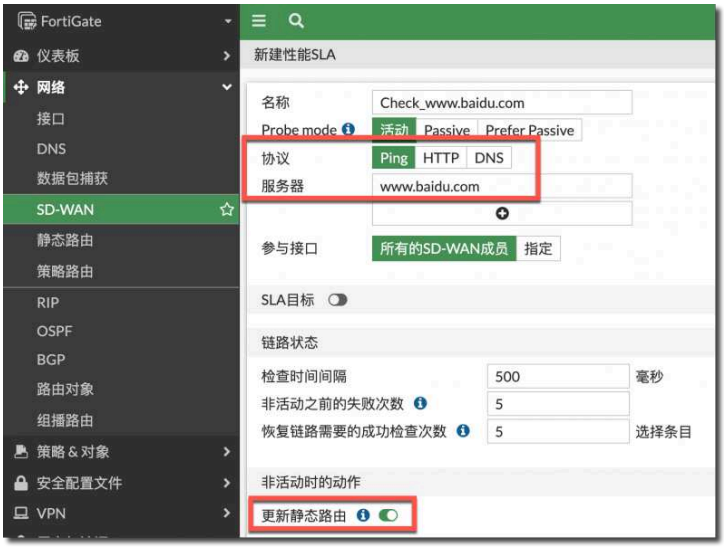


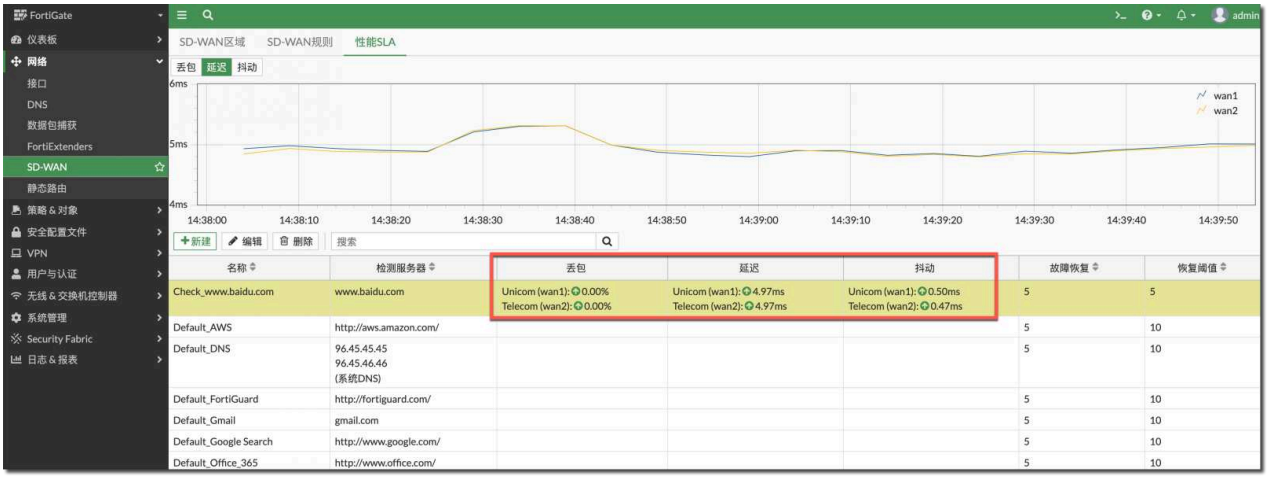
2. 添加SD-WAN的默认路由。



3. 配置SD-WAN的SLA，以便wan1和wan2相互备份和切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. SD-WAN规则可根据需求配置，这里保持默认的按照源IP负载均衡。



安全策略配置

1. 需求与规划：

   - 员工的有线与无线都需要访问互联网
   - 访客的无线仅仅可以访问互联网
   - 员工的有线和无线需要互访

2. 建议将防火墙的接口划分区域，以区域的方式配置策略，有时候可以做到简化配置的目的，甚至未来替换设备的时候，策略的备份和还原也会更加简单一些。规划区域两个区域：

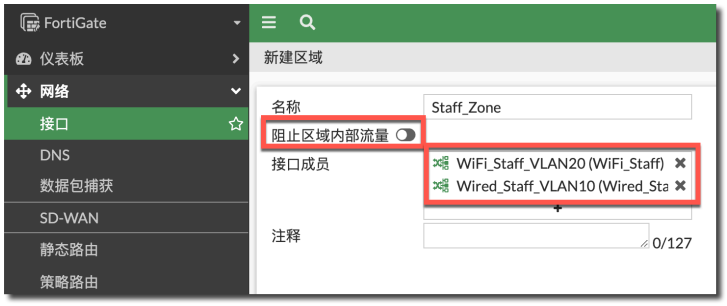
   - 员工网络区域：包括员工的有线VLAN 10和员工的无线VLAN 20 （区域之间的隔离关闭，这样VLAN 10和VLAN 20之间的数据可通）
   - 访问网络区域：包括访问的无线VLAN 30

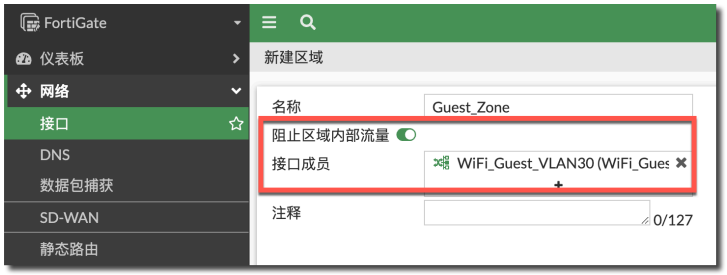
3. 进入网络→接口页面，新建所属区域。

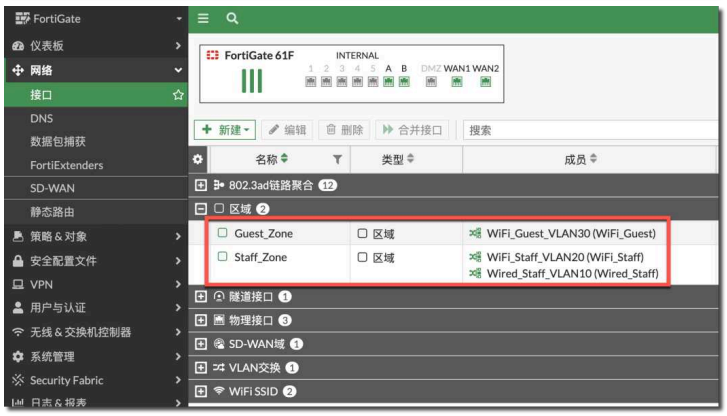
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 分别创建Staff_Zone（包含VLAN 10和VLAN20）和Guest_Zone（包含VLAN30）。







5. 如此只需要配置两条策略，就可以实现我们规划的需求，新建Staff-Zone到SD-WAN与Guest-Zone到SD-WAN的安全策略。

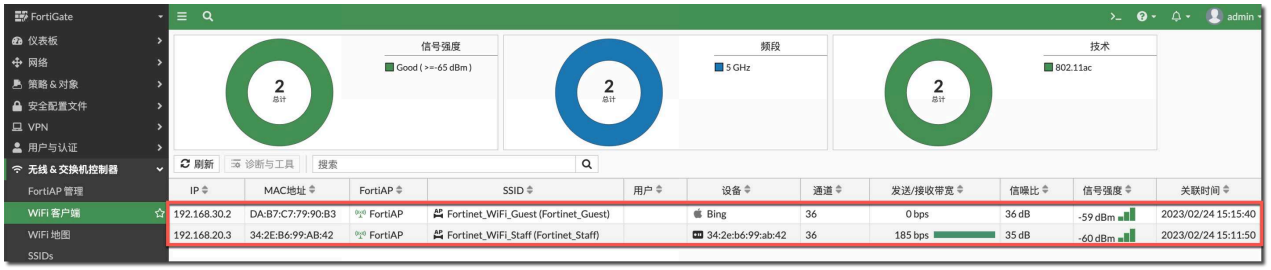


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

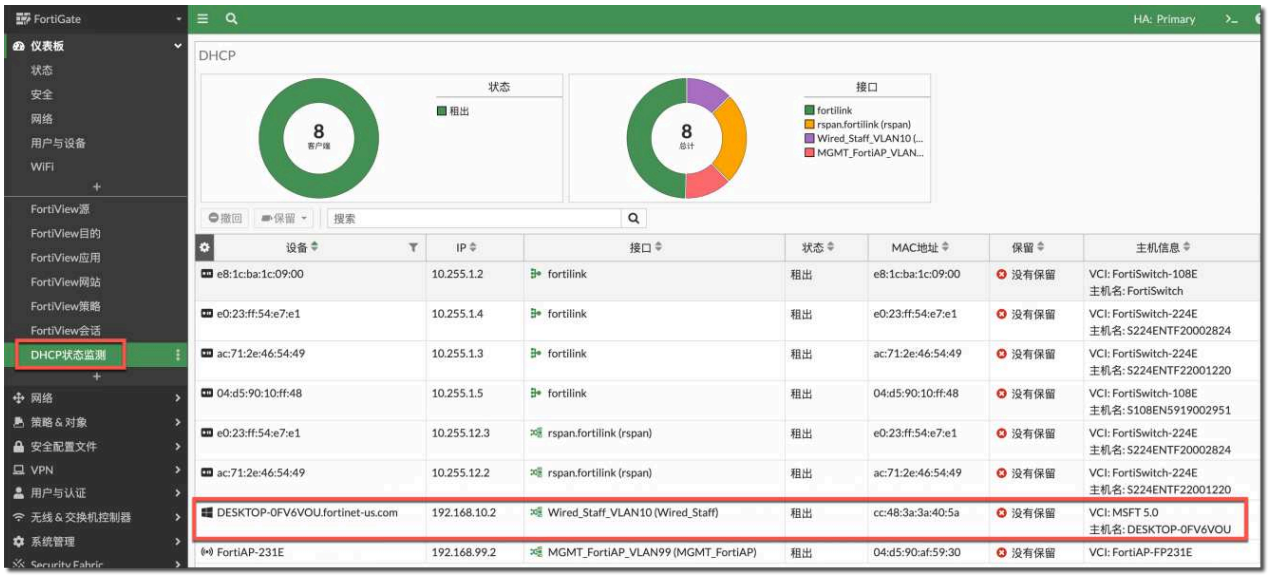
结果验证

客户端访问

1. 进入无线&交换机控制器→WiFi客户端，查看在线的无线客户端。可以看到WiFi_Staff和WiFi_Guest各有一个终端在线。



2. 在DHCP状态检测中查看所有的客户端信息，可以看到有线网络的PC也正常上线。

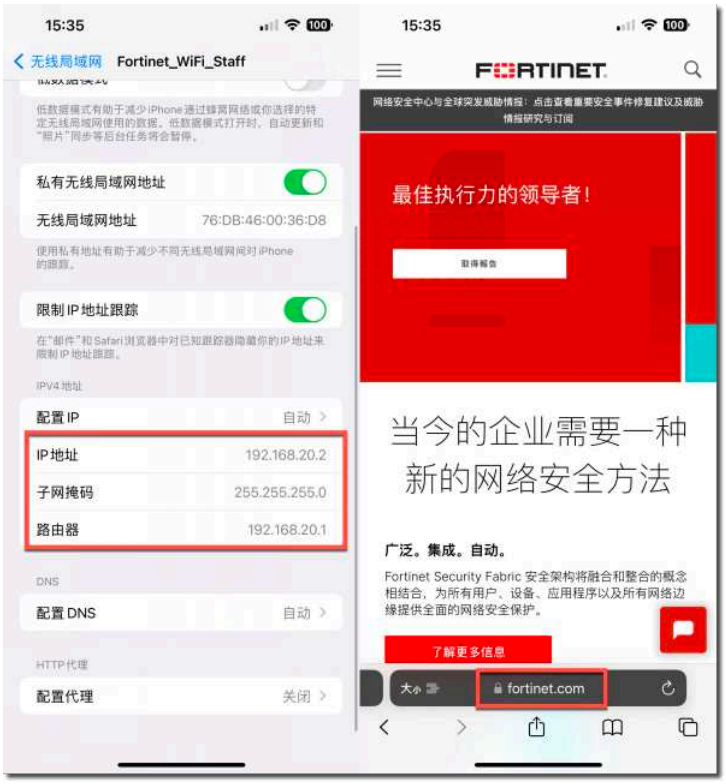


3. 有线网络（VLAN 10）用户访问互联网。

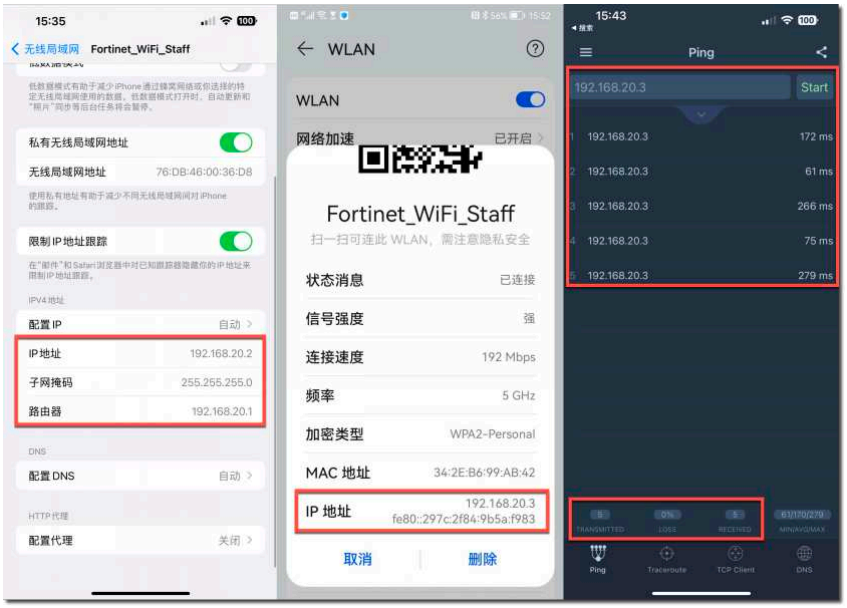


4. 无线网络用户访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

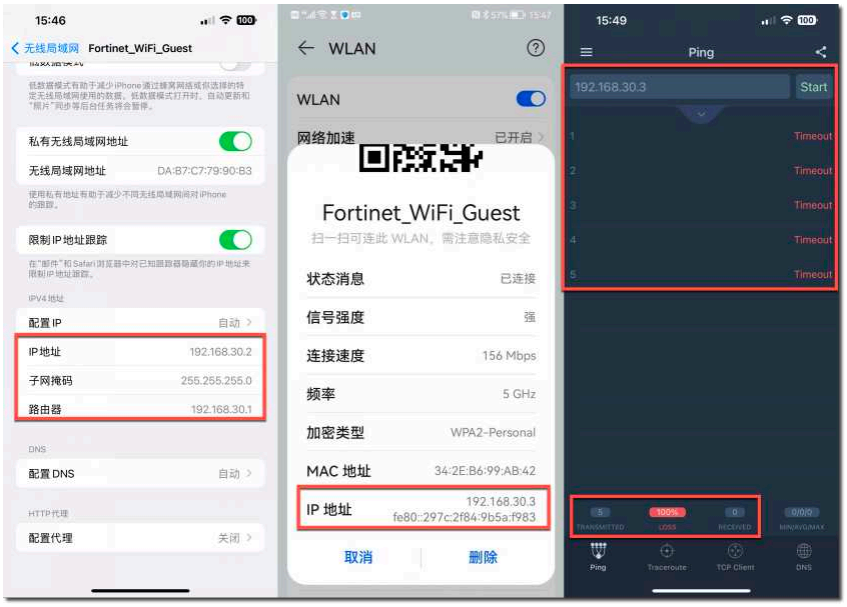


5. 使用VLAN 20下的客户端访问VLAN 20下的另一个客户端（Staff区域）。



6. 使用VLAN 30下的客户端访问VLAN 30下的另一个客户端（Guest区域），可以看到由于该区域配置了禁止相互访问，所以VLAN 30下的客户端是无法互相访问的。

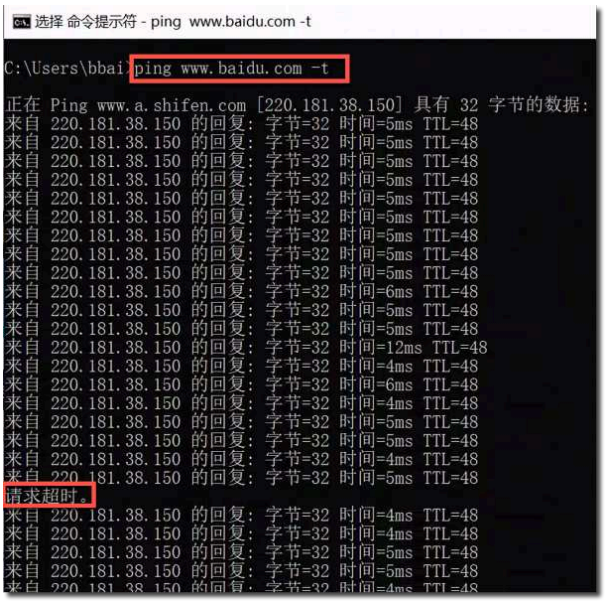
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiLink切换测试

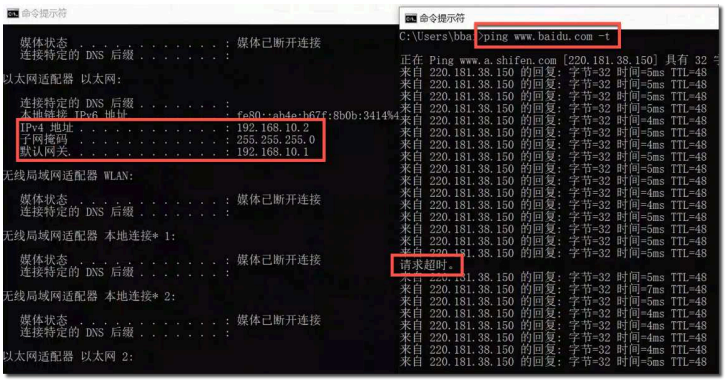
1. 在我们的测试场景下FortiLink聚合接口的a和b是同时UP起来的，如果a或b DOWN（不能同时DOWN），是否有影响业务呢?

2. 经过测试，DOWN a或b接口，客户端丢包1个或者不丢包。



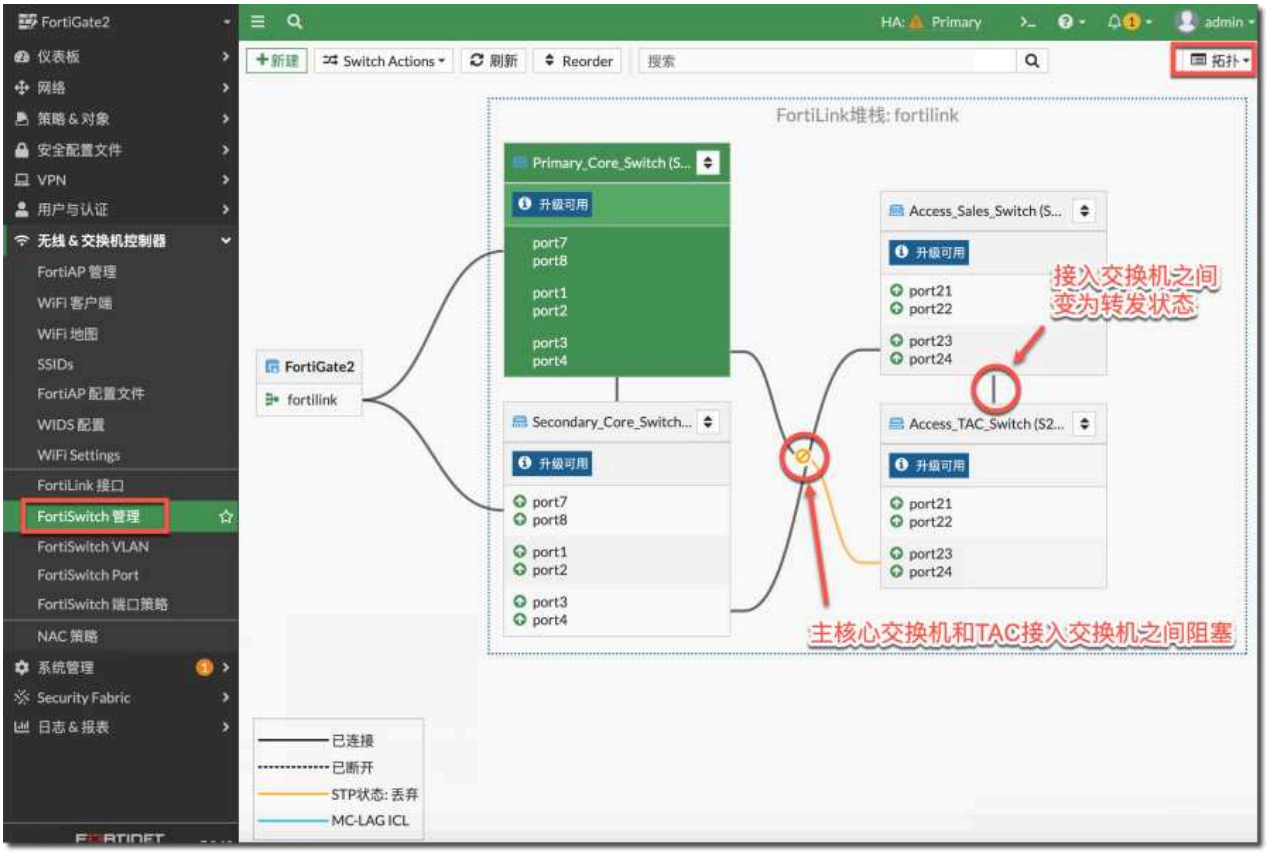
HA切换测试

1. 重启当前主防火墙查看内网PC丢包情况，HA切换丢包1个。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 此时查看原备（新主）防火墙的FortiLink交换机接管状态，流量全部会切换到备防火墙和备核心交换机上（FortiGate HA主备切换后，原主FortiGate下的核心交换机会在新主FortiGate重新上线）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

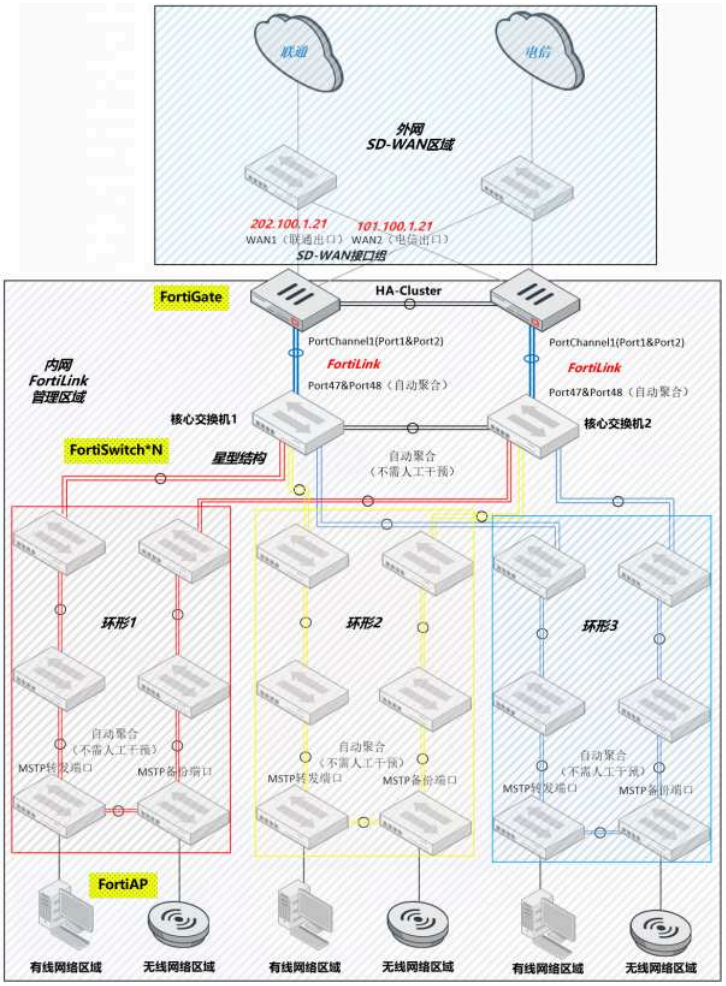
FortiLink星型环形混合组网

网络需求

虽然环形组网是比较好的方式，唯一的问题是环路太大了，一旦网络中出现接口震荡等情况，MSTP会出现反复的计算和收敛，一个环内的交换机越多STP速度就越慢，通常不推荐超过16台的FortiLink环。这样有没有好的解决办法呢?

解决方案

1. 实际上需要将星型组网和环形组网结合起来就可以比较好的解决环过大的问题。我们可以取名叫做星型环形混合组网。
2. FortiGate采用HA-Cluster方式部署，核心到汇聚的部分采用星型架构组网，接入的部分采用环形组网，如下图所示的混合组网方案。



3. FGT配置完FortiLink，FortiSwitch和FortiAP只需要接物理的线即可，不需要有任何的手工配置FSW和FAP，按照拓扑图接好物理的线之后，等待FortiLink整网收敛完毕之后，就可以通过FortiGate统一的管理和配置FSW和FAP，整网的所有的有线和无线的配置统统都在FGT上完成，通过FGT的FortiLink做到整网可控、可配、可视化。
4. 混合型组网的举例略过，其实FortiGate的配置是一样的，混合组网无非就接线的方式不一样而已。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink交换机零配置跨三层部署

从FortiOS 7.2 + FortiSWOS 7.2开始，交换机添加了一个新的功能叫ZTP（Zero-touch Provisioning，也叫Zero-touch Management），主要有以下变化：

- 交换机默认所有的接口都开启了FortiLink管理，之前的版本有的交换机只有后面的端口开启了FortiLink管理。
- 交换机被防火墙授权管理后，不会再自动重启一次，所以建议在交换机上线之前reset一下交换机。
- 交换机取消了命令“switch-mgmt-mode”，增加了命令“config switch auto-network”。

由于上面的变化，在部署交换机的FortiLink跨三层部署时，配置上也会有相应的变化：

- 如果交换机通过DHCP获取IP地址并且通过option 138获得防火墙FortiLink接口IP地址，那么对于交换机的跨三层FortiLink部署也是即插即用，不需要在交换机上添加任何配置，即可上线交换机。
- 如果需要在交换机上手动指定防火墙FortiLink接口IP地址，那么需要在交换机上增加一些配置。

本文档描述了FortiLink跨三层部署时，上面两种情况的配置介绍。请参考：FortiLink交换机零配置跨三层部署 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink部署之MCLAG堆叠组网

方案说明

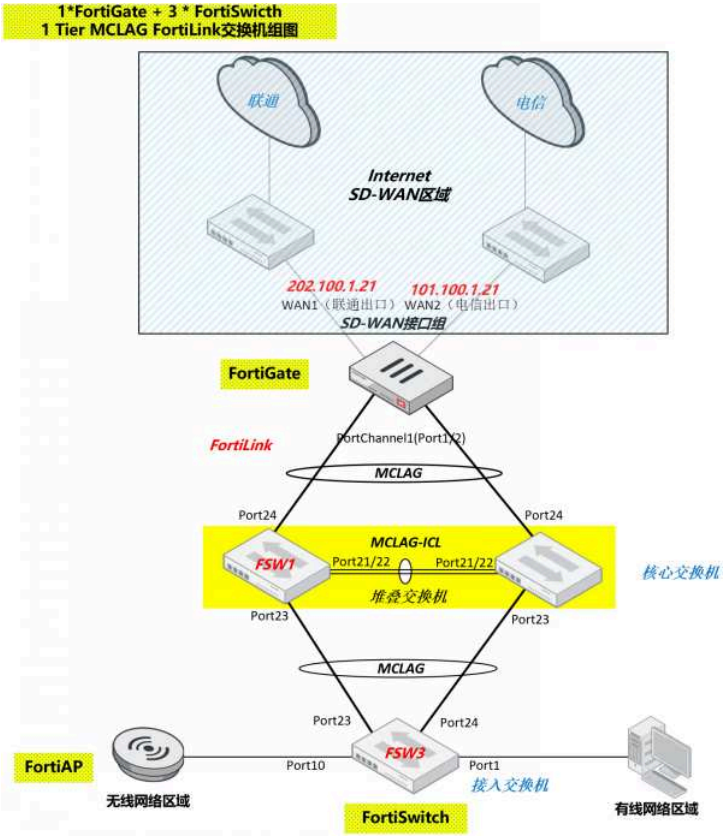
堆叠组网（MCLAG）是最理想的FortiLink部署方法了，目前支持1层堆叠（只堆叠核心交换机）和2层堆叠（堆叠核心交换和接入/汇聚交换机）。

合理的MCLAG（堆叠）组网规划可以规避掉STP阻塞接口（避免环路），整网不需要STP了，并且所有的接口都是更好的利用起来，增加使用带宽的同时且无环路，因此MCLAG的部署在FortiLink部署中是更加优质的选择。

1 Tier MCLAG FortiLink组网方案

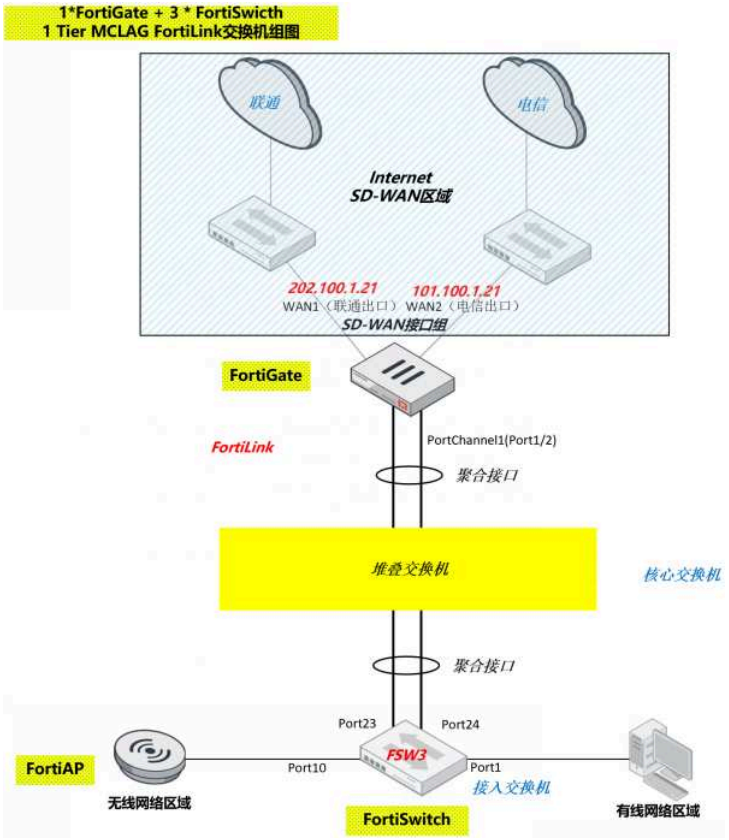
单机FortiGate部署

1. 最简单的一个MCLAG部署拓扑，FortiGate * 1 + FortiSwitch * 3。

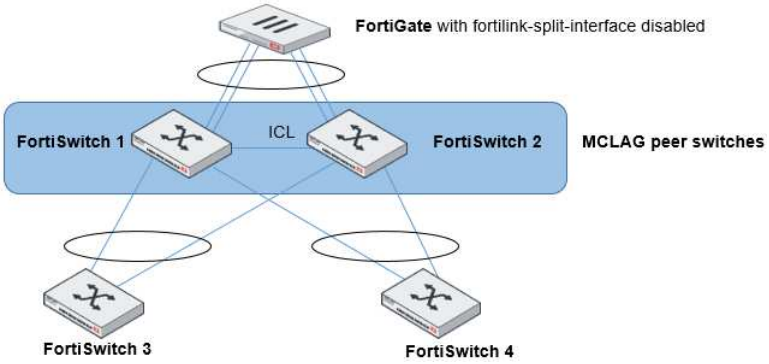


堆叠后的逻辑拓扑：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



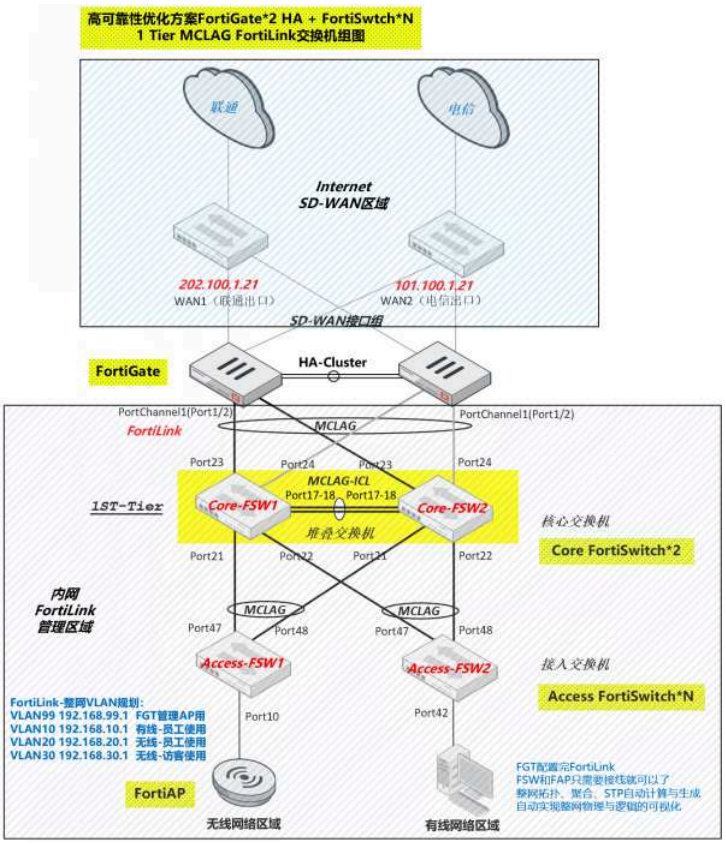
2. 类似的组网。



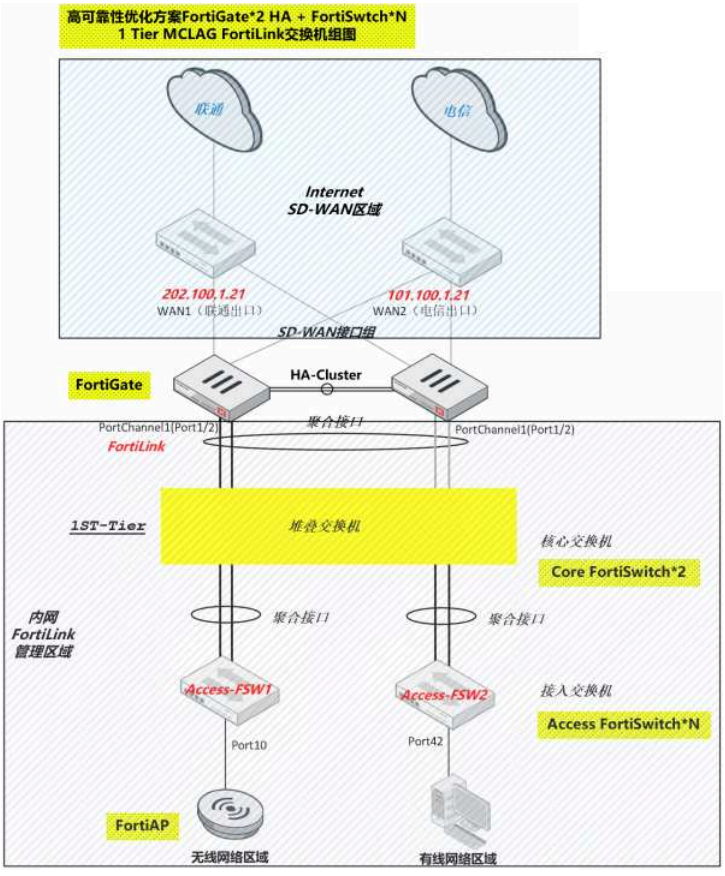
双机FortiGate HA部署

1. FortiGate采用HA-Cluster方式部署，核心到汇聚的部分采用星型架构组网，交换机接入的部分采用MCLAG堆叠组网，如下图所示的1 Tier交换机堆叠组网方案。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

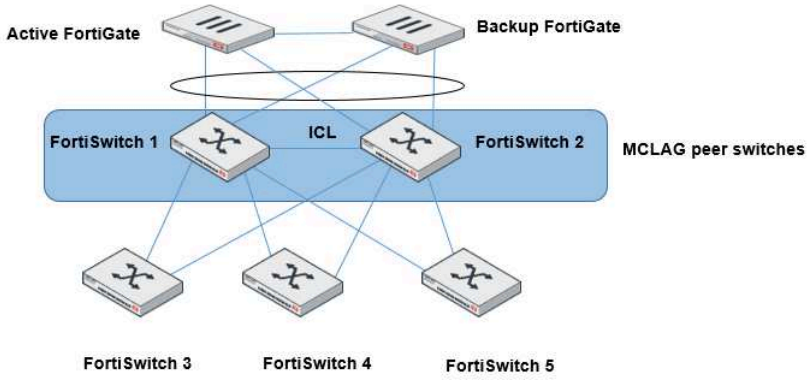


堆叠后的逻辑拓扑：



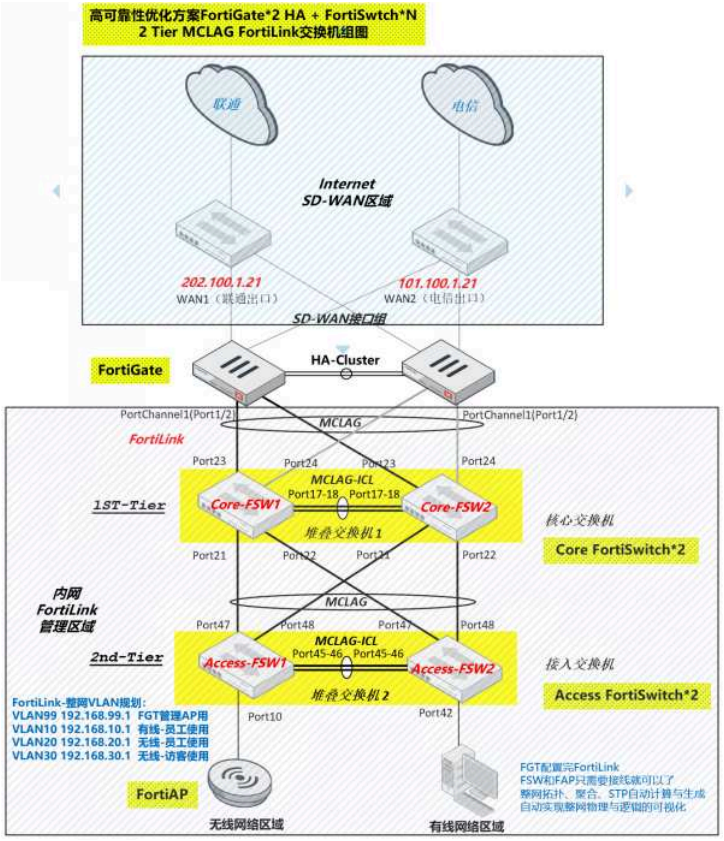
2. 类似的组网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



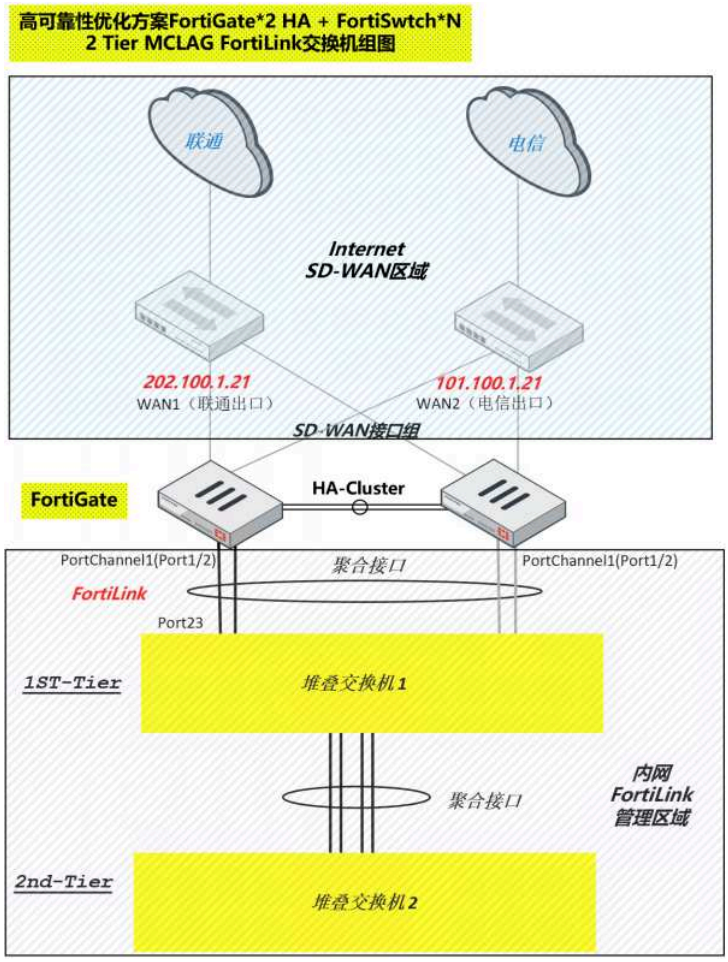
2 Tier MCLAG FortiLink组网方案

1. 双机FortiGate HA部署。

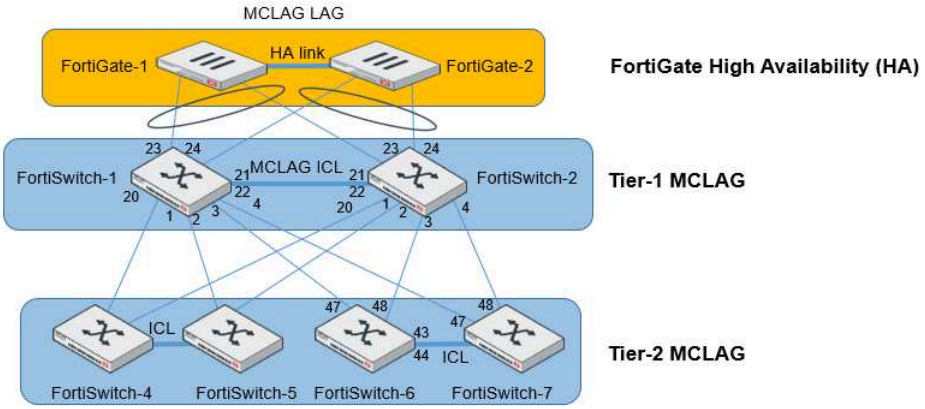


堆叠后的逻辑拓扑：

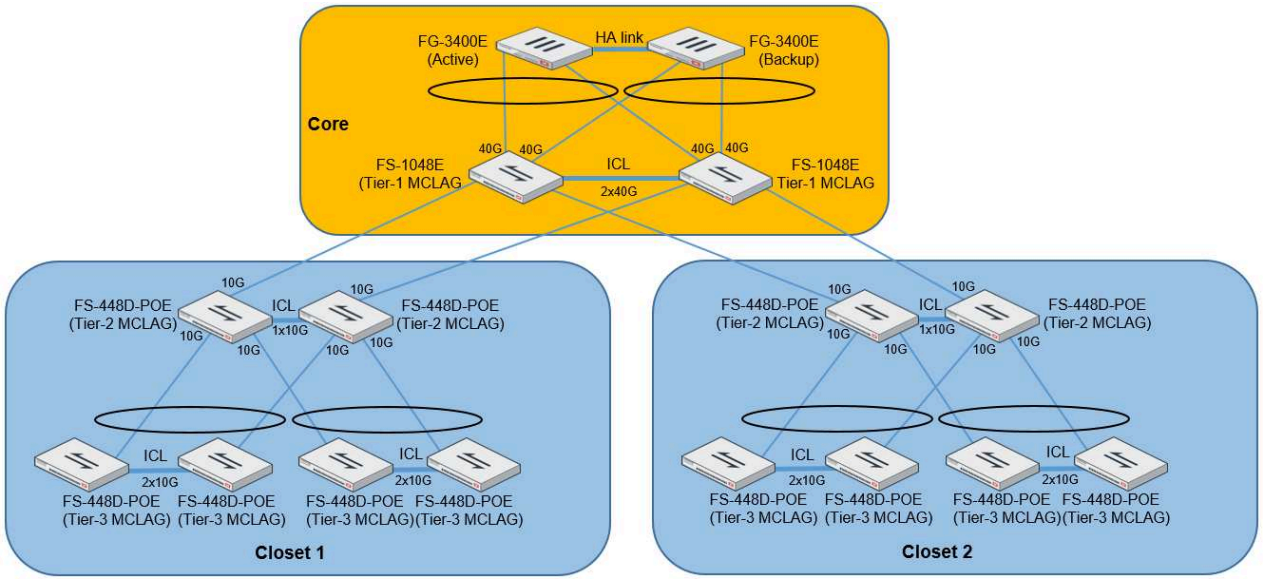
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 类似的拓扑。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



注意事项

- 最多只能是两个交换机组成一对MCLAG。
- 组成MCLAG的两个交换机必须是相同的硬件型号以及相同的软件版本。
- FortiGate的聚合端口在MCLAG Switch上线前为split enable状态，MCLAG Switch上线并配置为MCLAG后，手动修改FortiGate的聚合端口为split disable状态。
- FortiSwitch必须是3.6.4之后的版本才支持MCLAG。
- FortiOS 6.2及以后的版本, 可以配置FortiGate聚合端口为Active模式。
- 某些设备交换机不支持MCLAG, 比如FS-1XX系列,具体请参考Release Notes。
- 1 Tier MCLAG只支持核心的两台防火墙进行堆叠，往下的接入交换机不再支持堆叠，整个FortiLlink网络中只有一组堆叠点，通常用于16~32台以内的FSW组网，更多的交换机可以考虑2 Tier MCLAG FortiLink组网。

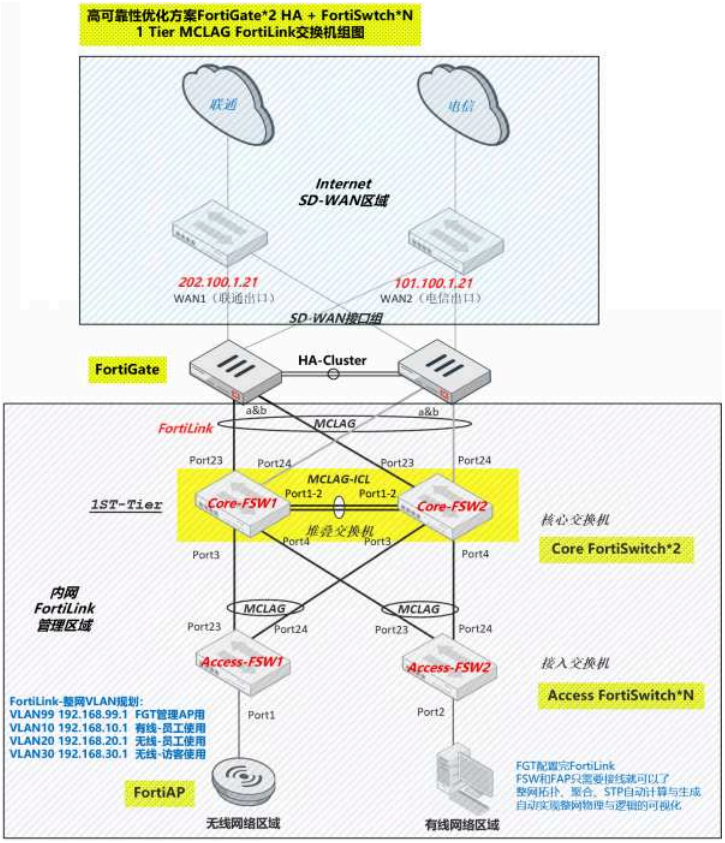
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink MCLAG-堆叠组网1 Tier配置举例

网络需求

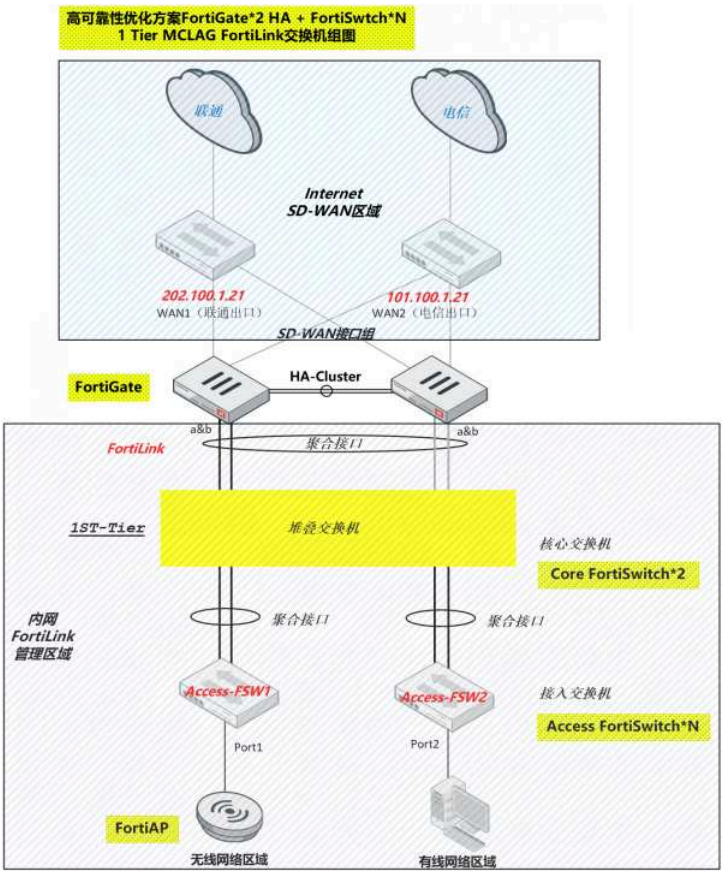
FortiGate运行HA-Cluster，核心交换机采用MCLAG堆叠组网结构。

网络拓扑



形成堆叠之后的逻辑拓扑：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. 两台FortiGate配置为HA主备模式。
2. 整体规划：
   - 外网IP网段规划：
     - WAN1联通出口：IP 202.100.1.21，GW 202.100.1.192
     - WAN2电信出口：IP 101.100.1.21，GW 101.100.1.192
   - WAN1和WAN2合并成SD-WAN接口。
   - 内网IP网段规划，FGT通过FortiLink+Capwap协议统一的接管FortiSW和FortiAP，为有线和无线统一进行管理和业务处理：
     - 有线网络规划：VLAN 10，192.168.10.1
     - 无线网络规划：员工WIFI VLAN 20，192.168.20.1
     - 无线网络规划：访客WIFI VLAN 30，192.168.30.1
     - 管理FortiAP：VLAN 99，192.168.99.1
   - FortiLink互联部分规划：
     - FortiGate的a和b做聚合接口与Fortiswitch的后两个接口互联即可实现聚合接口的FortiLink管理。
     - 加入FortiLink的接口自动变为聚合口成员。

配置要点

1. FortiGate配置聚合端口，并设置split为enable模式。
2. 上线Core-FSW1和Core-FSW2，将FortiGate和Core-FSW1以及Core-FSW2连接起来。
3. 分别登录到Core-FSW2和Core-FSW1上，配置二者直连的ISL 接口为“mclag-icl enable”。配置为ICL堆叠线路（Inter-Chassis-Link），形成两台核心交换机的堆叠。
4. 配置FortiGate聚合端口为split disable模式。
5. 上线Access-FSW1和Access-FSW2。
6. 上线FortiAP和有线PC，并测试无线网络和有线网络的连通性。
7. 注意：如果Switch上线时，有的Switch是旧的版本，最好先升级Switch的版本后，再组建mclag或是让交换机成环。

配置步骤

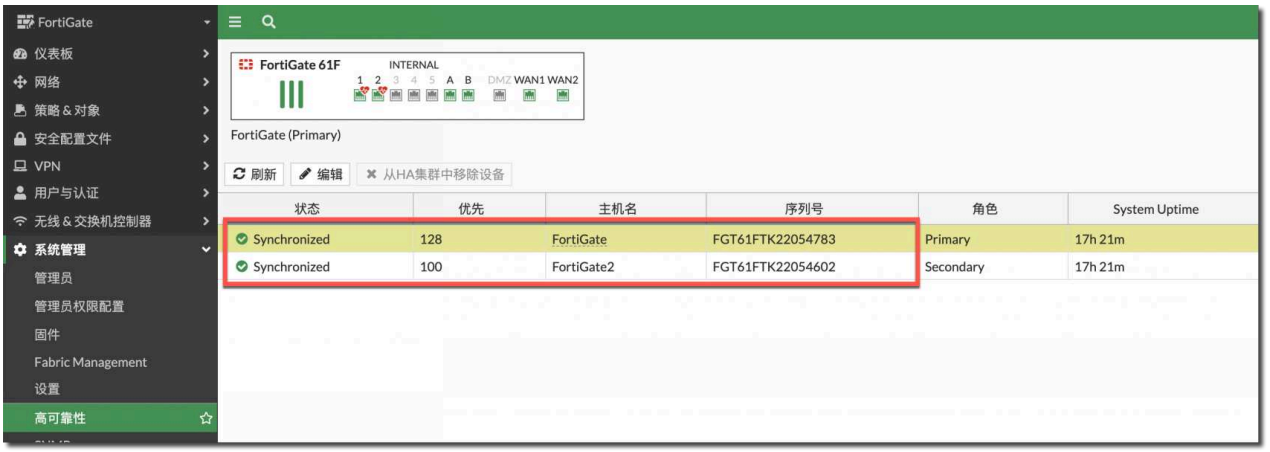
准备事项

1. 首先确认FortiGate如下全局配置已开启（一般默认为开启状态）。

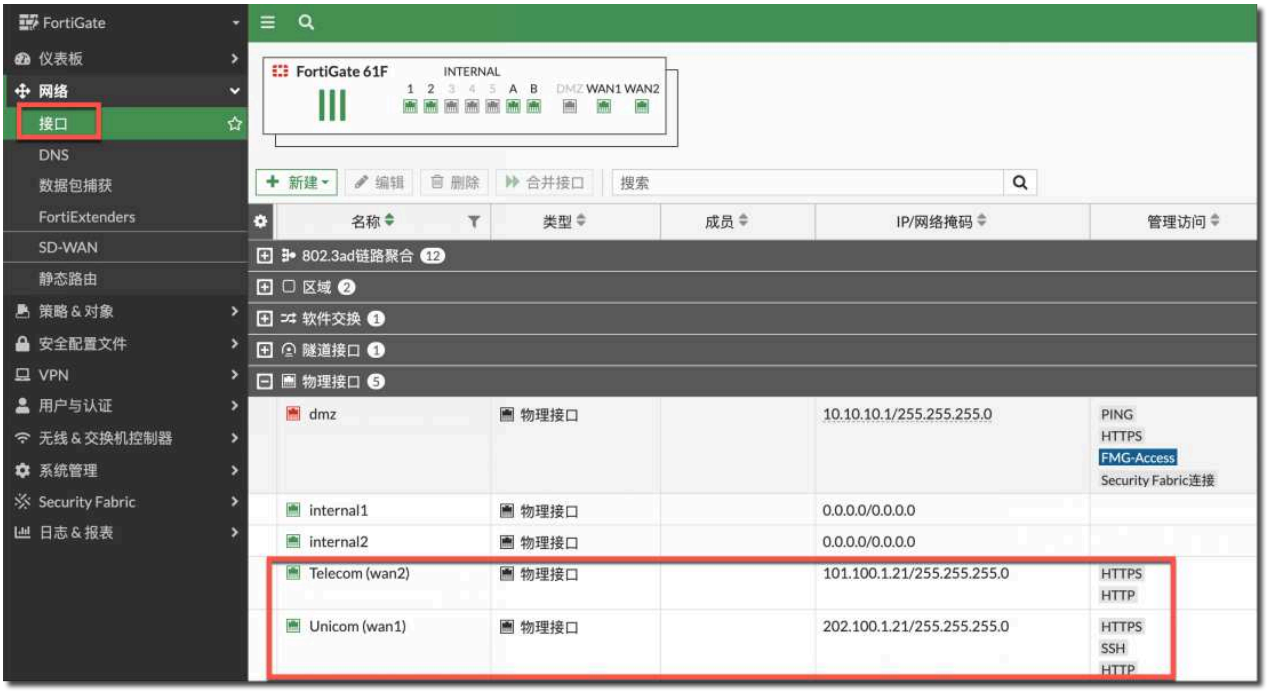
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system settings
    set gui-switch-controller enable
end
```

2. 配置两台FortiGate的HA主备模式（配置方法请参考HA双机热备→HA典型基础配置 ↗）。



3. 配置wan1和wan2的IP地址。



4. 配置FortiLink实现FortiSwith上线，我们只需要将用于FortiLink的成员接口加入FortiLink接口即可。此拓扑中，FortiGate用于连接FortiSwitch的接口为a和b，编辑FortiLink接口，将a和b加入FortiLink（某些产品型号会默认将两个接口加入FortiLink），开启自动授权设备，关闭FortiLink分离接口，其他配置保持默认，可以看到FortiLink为一个聚合接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





重要

FortiLink分离接口什么时候应该开启?

分离接口的意是，如果聚合接口的port1和port2分别连接了一台SW，在没有使用MCLAG的情况下（没开启堆叠功能），则聚合接口的port1和port2没办法同时UP（同时开启聚合接口无法正常工作），因此必须开启FortiLink分离接口功能，让聚合接口只有一个物理接口（port1）是处于UP状态的，另外一个物理接口（port2）处于DOWN的备份状态，当port1接口状态DOWN，则Port2立即接管Port1的工作，让聚合接口的FortiLink继续运行，这是一个聚合接口在FortiLink管理时候的备份机制。



MCLAG配置前是上述组网，因此刚刚开始的时候需要，保持enable状态。聚合接口的Port1和Port2只会UP一个接口，另外一个接口处于DOWN的状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

FortiLink split interface什么时候应该disable?

如果FGT的聚合接口只接到了一台交换机上，并没有跨交换机聚合（没有MCLAG，也不需要FortiLink split interface），因此这种情况应该让聚合接口的两个物理接口port1和port2同时UP，两个接口同时工作起来，以便提供更高带宽和备份的作用。



配置两台交换机MCLAG堆叠之后，就是上述组网，因此交换机堆叠完毕之后，需要修改为disable，让两个聚合接口都可以同时工作起来，最大的利用聚合接口的带宽和资源。这个配置后续会说明。

相关CLI:

```
NTP:
config system ntp
    set ntpsync enable
    set server-mode enable
    set interface "fortilink"
end
--------------------------------------------------------------------------------
DHCP:
config system dhcp server
    edit 2
        set dns-service local
        set ntp-service local
        set default-gateway 10.255.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.255.1.2
                set end-ip 10.255.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
end
--------------------------------------------------------------------------------
FortiLink:
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "a" "b"
        set lldp-reception enable
        set lldp-transmission enable
        set auto-auth-extension-device enable
        set fortilink-split-interface enable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

连接FortiLink

连接核心交换机

1. 配置完FortiGate之后，这个时候再去接FortiGate的FortiLink到FortiSwitch的线，配置Core-FSW1和Core-FSW2设备的互联接口MCLAG注意，先不要把所有的线都接上去，一台一台的来操作，MCLAG配置尽量使用Console去配置，而不是GUI，有时候由于在Fortilink计算和收敛会导致GUI连接不上去，或者先将CORE-FSW1下线，先单独配置CORE-FSW2，然后再将CORE-FSW2下线，再单独配置CORE-FSW1，然后再将二者互联的线接上去，这样是最稳妥的办法，避免GUI的CLI连不上的情况出现。而接入交换机这个时候是不建议接入的，等CORE-FSW1和CORE-FSW2的堆叠形成了之后，再将接入层交换机的线。

   > **重要**
   >
   > FortiSwitch如果以前有使用过，建议都恢复一下出厂设置，然后再加入到FortiLink。

2. FortiSwitch的靠后接口一般都默认开启了FortiLink接口属性，如果接前面的接口可能会无法加入到FortiLink，因此FortiSwitch的FortiLink最好都使用靠后的接口进行接线。FortiSwitch各型号默认开启FortiLink功能的接口如下：

FortiSwitch型号	默认开启FortiLink的接口
FS-108D-POE	port9–port10
FS-108E, FS-108E-POE, FS-108E-FPOE	port7–port10
FSR-112D-POE	port5–port12
FS-124D, FS-124D-POE	port23–port26
FSR-124D	port1-port4, port21–port28
FS-124E, FS-124E-POE, FS-124E-FPOE	port21–port28
FS-148E, FS-148E-POE	port21–port52
FS-224D-POE	port21–port24
FS-224D-FPOE	port21–port28
FS-224E, FS-224E-POE	port21–port28
FS-248D, FS-248D-FPOE	port45–port52
FS-248D-POE	port47–port50
FS-248E-POE, FS-248E-FPOE	port45–port52
FS-424D, FS-424D-POE, FS-424D-FPOE	port23–port26
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30
FS-548D	port39–port54
FS-548D-FPOE, FS-548DN	port45–port54
FS-1024D	port1–port24
FS-1048D, FS-1048E	port1–port52
FS-3032D, FS-3032E	port1–port32

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

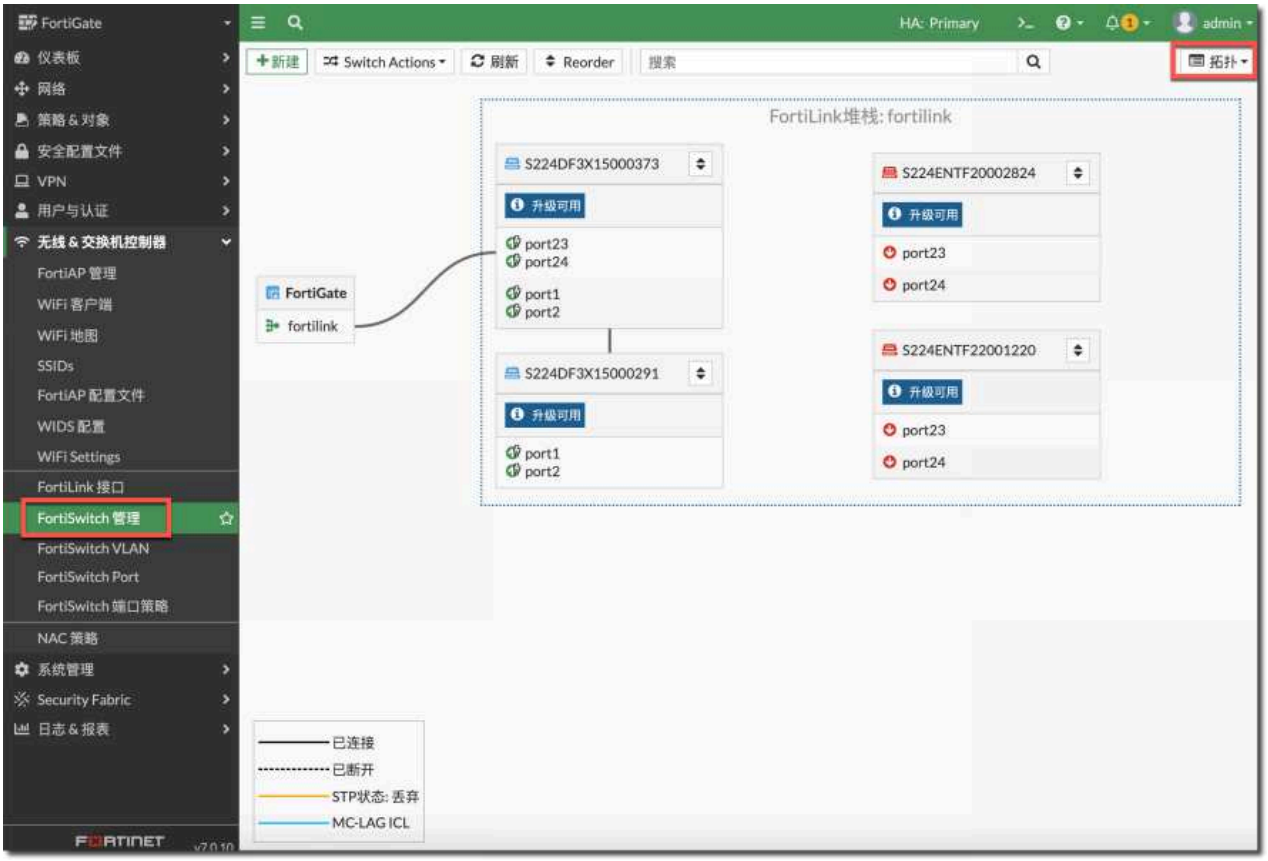
3. 如果FortiSwitch无法被FortiGate管理，登陆到FortiSwitch上进行确认接口是否开启了FortiLink。

```
FortiSwitch # show switch interface port9
config switch interface
    edit "port9
        set auto-discovery-fortilink enable    //接口下又此命令的接口才可以自动加入到FortiLink中
    next
end
```

4. 交换机之间如果接多根线，会自动进行聚合，但是FortiLink自动聚合会花比较长的时间，建议可以先接单线，等FortiLink的拓扑较快的形成结束之后，再增加彼此之间的另外一根线，再进行自动聚合，这样效率会比较高一些。

5. 接线是很重要的步骤，仔细看拓扑图，做好接口标签，不要接错。

6. 先接Core-FSW1的线，再接Core-FSW1和Core-FSW2互联的线，先不要接接入层交换机的线，在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，右上角选择拓扑视图，查看交换机被管理状态。



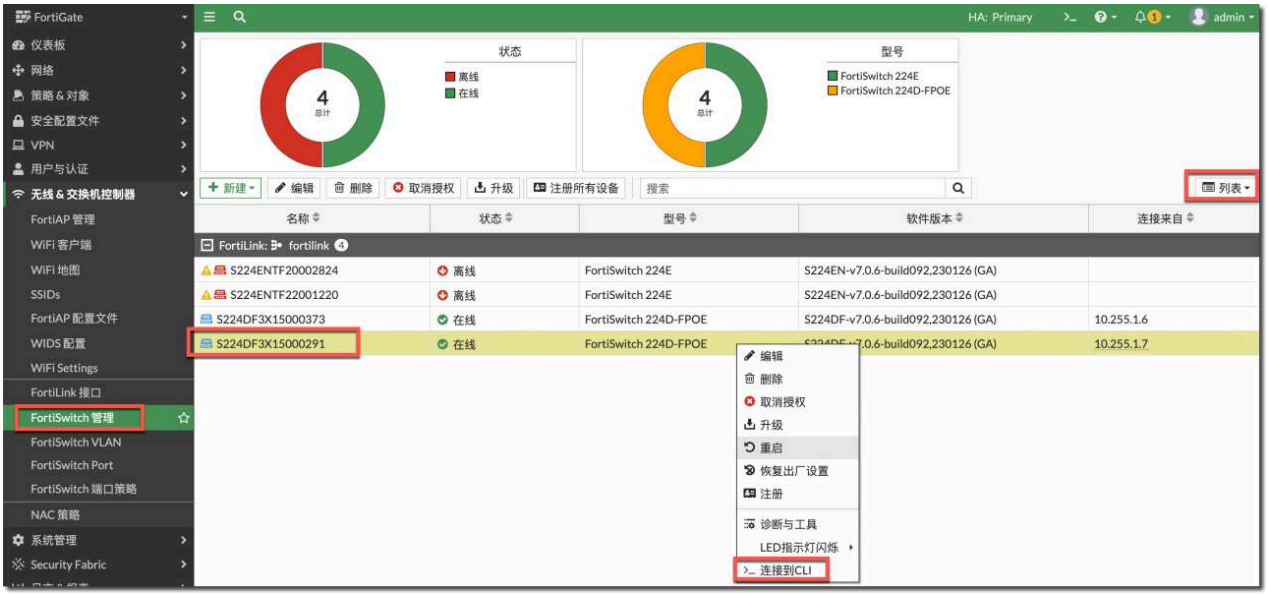
7. 此时我们看防火墙的FortiLink聚合接口，此时应该只有a或b其中一个物理接口是UP的，这是FortiLink split interface enable的结果。



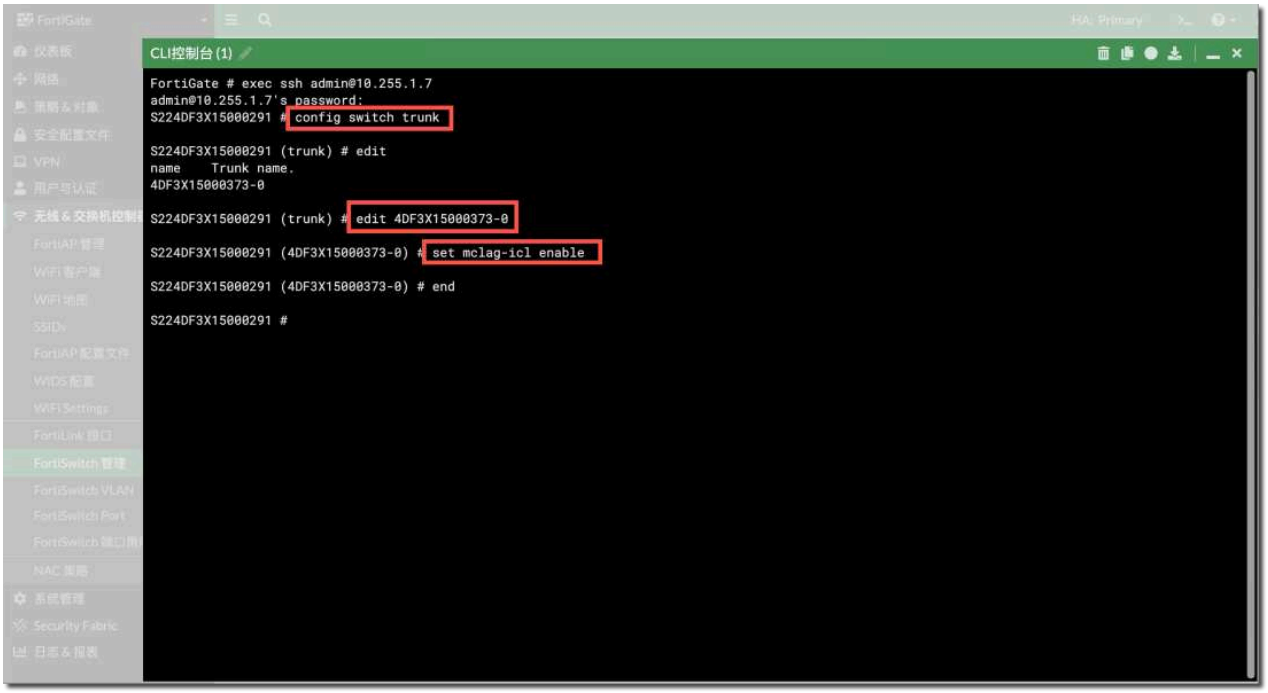
配置MCLAG

1. 通过FortiGate管理交换机页面右键交换机即可SSH到交换机，分别登录到Core-FSW1和Core-FSW2上。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

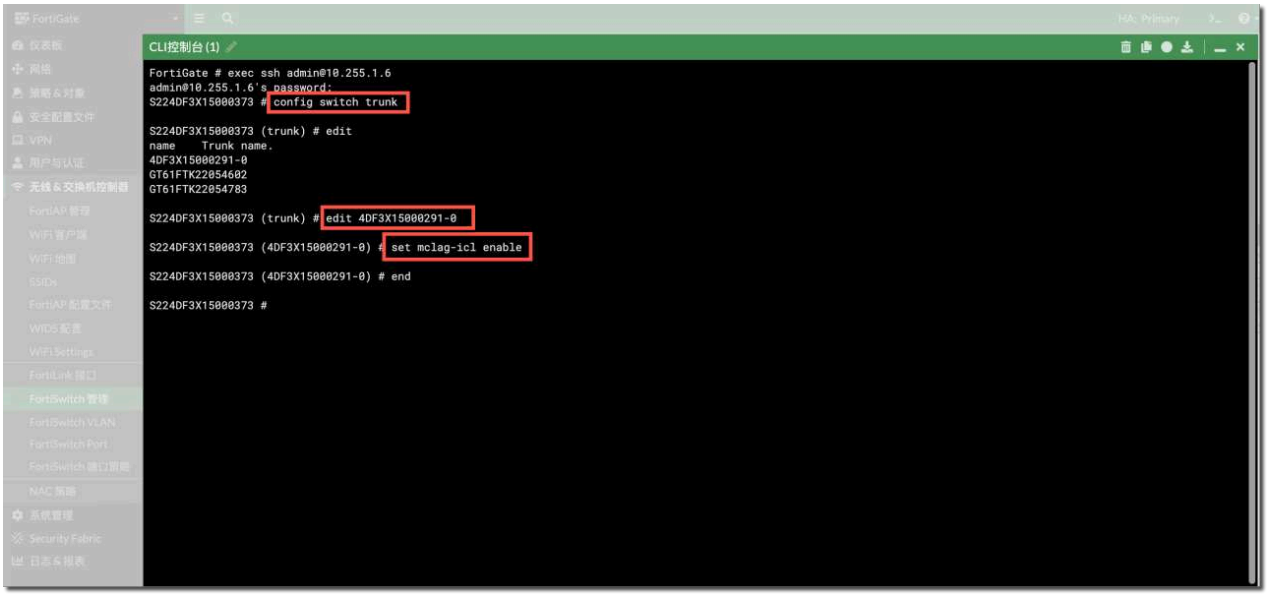


2. 配置二者的互联聚合接口为“set mclag-icl enable”（请注意此例中在GUI配置时一定要先配置CORE-FSW2，因为CORE-FSW2与FortiGate的FortiLink接口处于down的状态，如果先配置了CORE-FSW1，那么CORE-FSW2将无法通过GUI管理）。



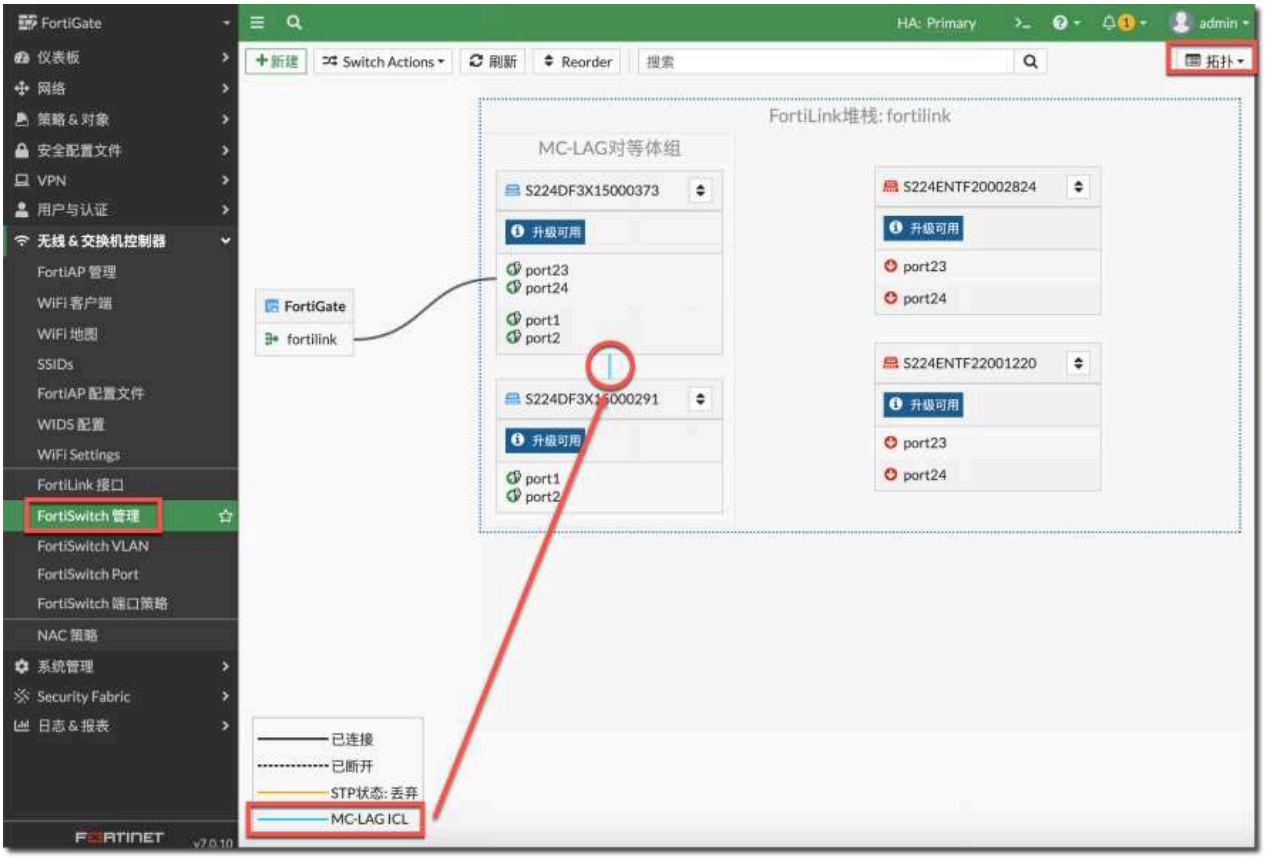

```
config switch trunk
    edit "4DF3X15000373-0"
        set mclag-icl enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



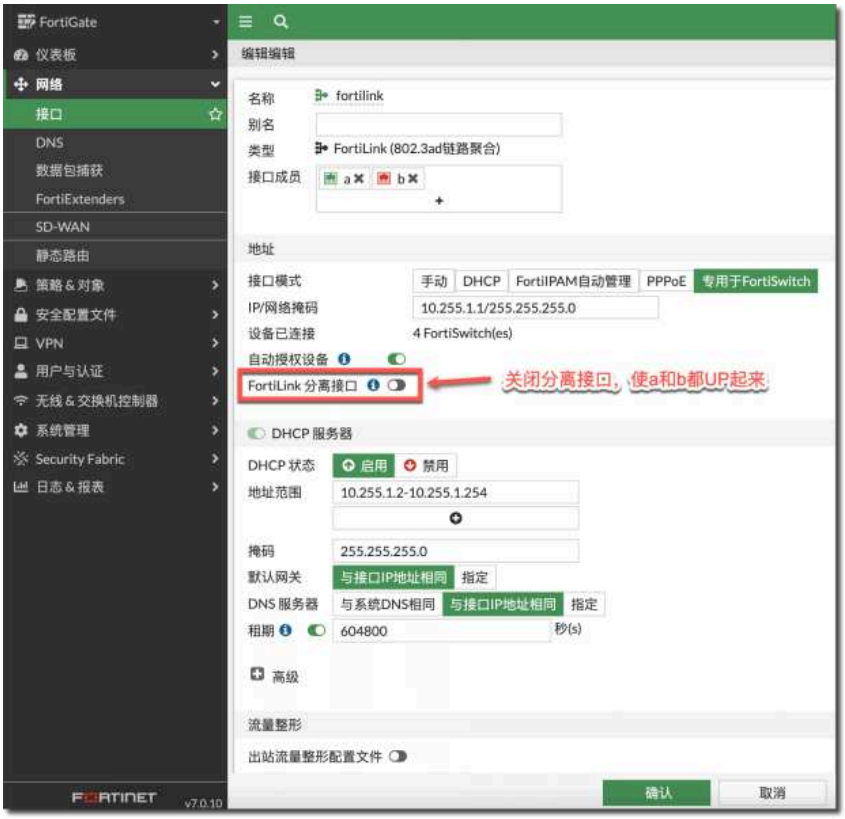

```
config switch trunk
    edit "4DF3X15000291-0"
        set mclag-icl enable
    next
end
```

3. 查看配置MCLAG后的交换机拓扑，可以看到两台交换机已经变为一个MC-LAG组。



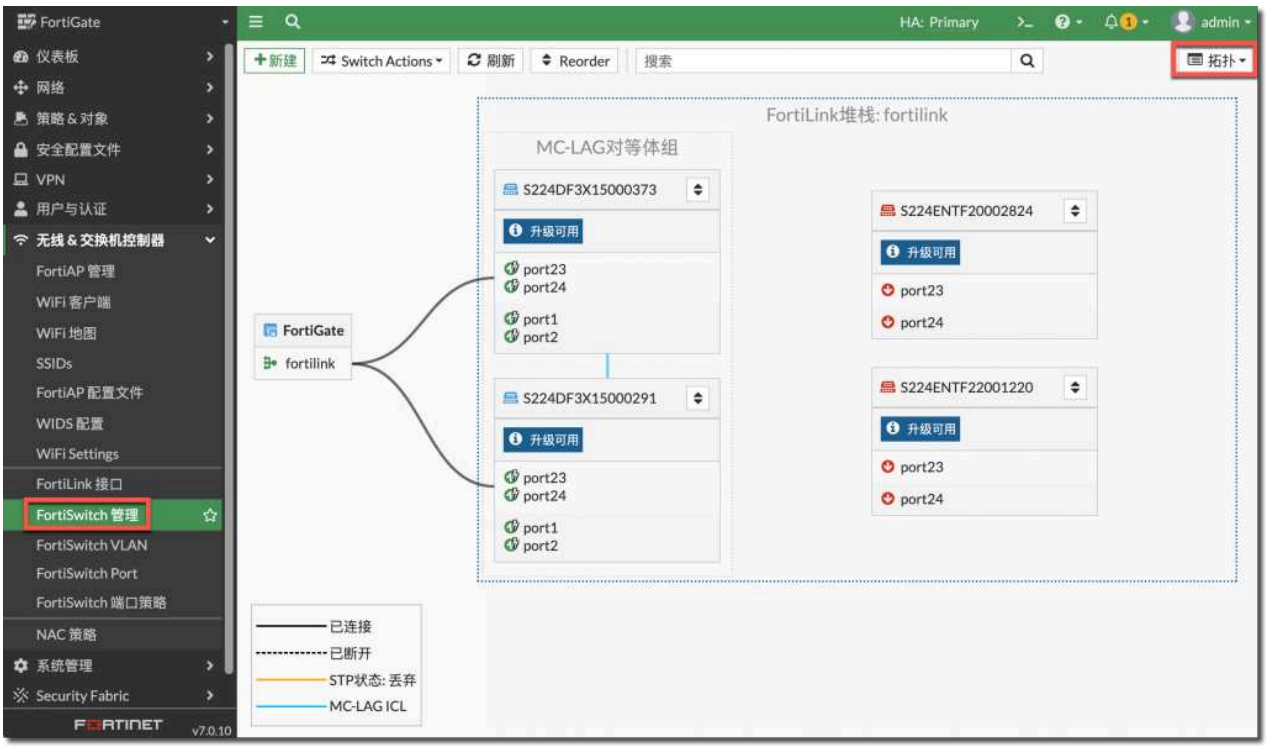
4. MC-LAG配置完成后，将FortiLink接口下的split interface设置为disable，让聚合接口（a和b）全部UP起来，充分利用聚合接口的资源，实现FortiGate与两台交换机（堆叠）的跨交换机聚合。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "fortilink"
        set fortilink-split-interface disable
    next
end
```

5. 等待CORE-FSW2重新在FortiGate上线后，查看Switch管理拓扑，FortiLink的两个成员接口均已UP。



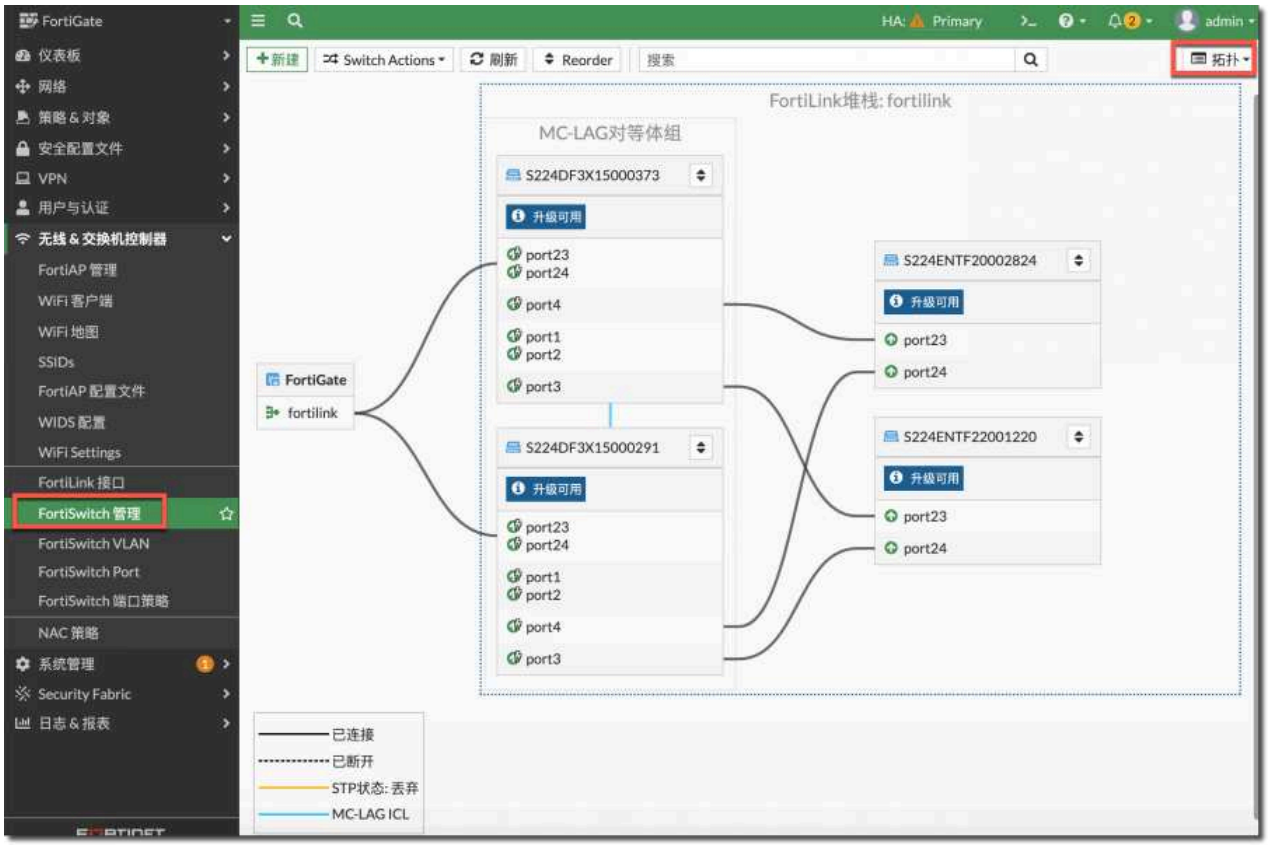
6. 在FortiGate的CLI下查看FortiLink成员状态，可以看到与实际物理连线一致。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # execute switch-controller get-physical-conn standard fortilink

This will display connectivity graph information for FortiLink from FortiGate's perspective
NOTE : If FortiSwitch is not authorized, no connectivity information will be shown
NOTE : If FortiSwitch is in idle state, no connectivity information will be shown
NOTE : If FortiSwitch ISL peer has inconsistent info, no connectivity information will be shown
        FortiLink interface : fortilink
FortiGate(s)
FGT61FTK22054783(a)  «————————————»  S224DF3X15000373(port23)
FGT61FTK22054602(a)  «————————————»  S224DF3X15000373(port24)
FGT61FTK22054783(b)  «————————————»  S224DF3X15000291(port23)
FGT61FTK22054602(b)  «————————————»  S224DF3X15000291(port24)

Tier 1
S224DF3X15000373(port23)  «————————————»  FGT61FTK22054783(a)
S224DF3X15000373(port24)  «————————————»  FGT61FTK22054602(a)
S224DF3X15000291(port23)  «————————————»  FGT61FTK22054783(b)
S224DF3X15000291(port24)  «————————————»  FGT61FTK22054602(b)

Tier 2+
S224DF3X15000373(port1/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port1/4DF3X15000373-0)
S224DF3X15000373(port2/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port2/4DF3X15000373-0)
```

连接接入交换机

1. 将接入层两台交换机的连线接入。在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，查看交换机被管理状态，修改视图为拓扑，可以看到4台交换机均已上线。



2. 接好线之后，FortiSwitch和FortiGate之间会自动在后台进行FortiLink、CAPWAP、MSTP、聚合接口的协商加入等操作，等FortiLink的管理结束之后，在FortiGate上会看到一个网站的FortiSwitch拓扑图，和我们规划的拓扑图应该是一致的，可以仔细核对接线是否正确。

3. 交换机加入到FortiGate的FortiLink，会先清除配置再重启，然后从standalone的状态进入到“Fortilink remote control”的状态，后续所有的配置都通过FortiGate下发即可。

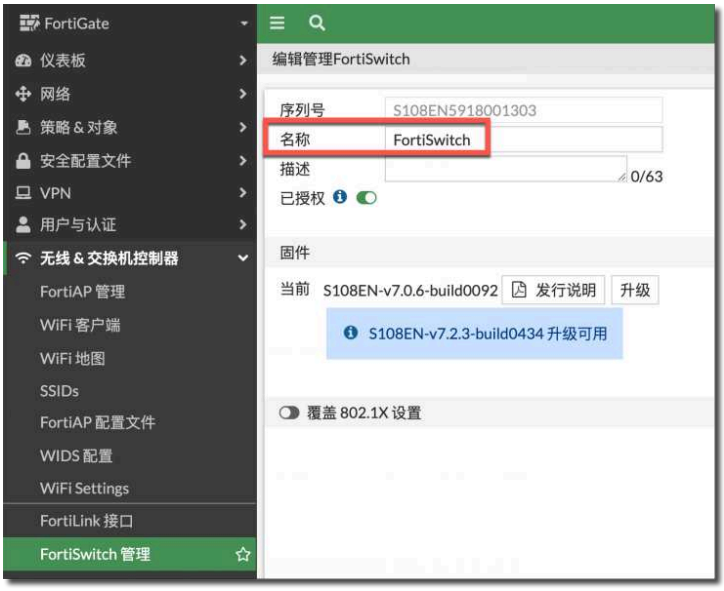
4. 再次查看FortiGate的FortiLink成员，可以看到两台接入交换机已上线，且连线与拓扑一致。

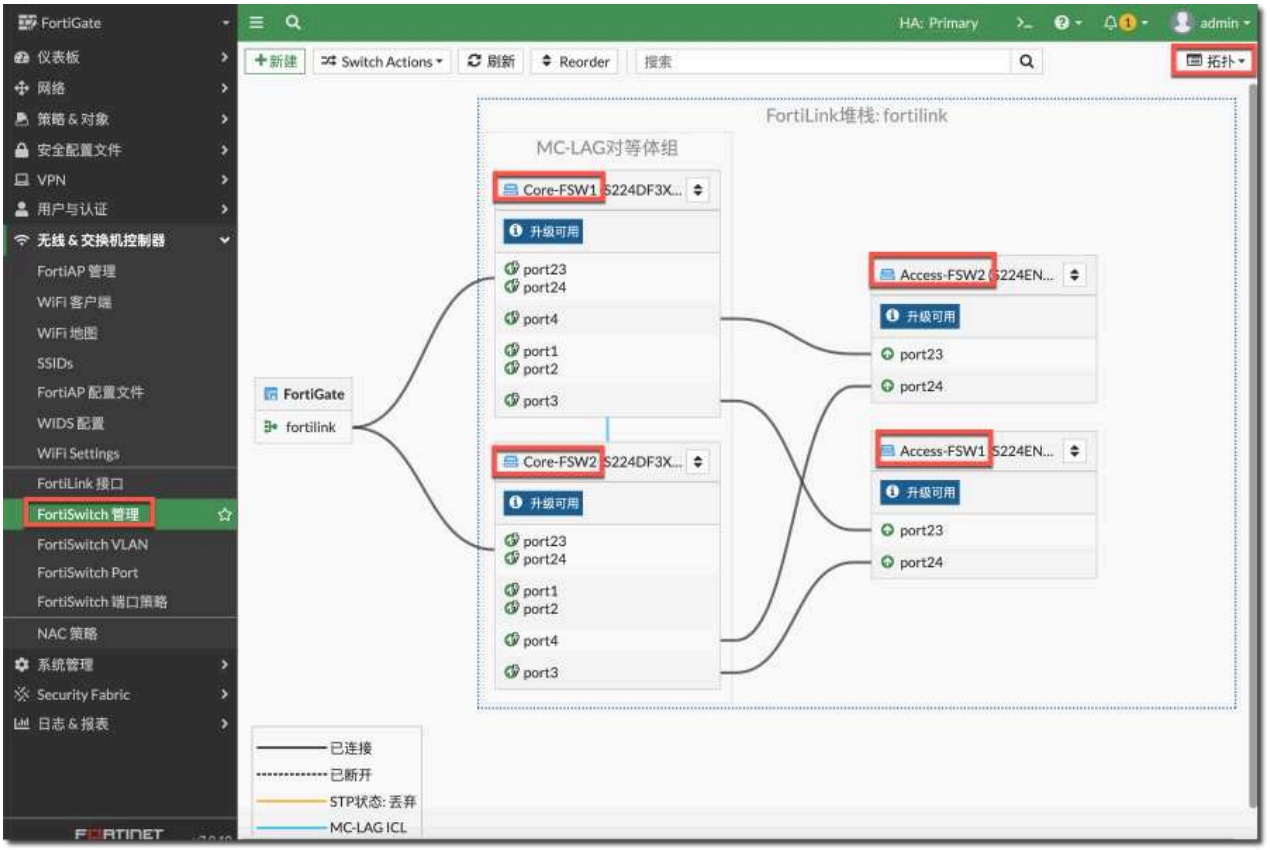
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # execute switch-controller get-physical-conn standard fortilink

This will display connectivity graph information for FortiLink from FortiGate's
        FortiLink interface : fortilink
FortiGate(s)
FGT61FTK22054783(a)  «————————————»  S224DF3X15000373(port23)
FGT61FTK22054602(a)  «————————————»  S224DF3X15000373(port24)
FGT61FTK22054783(b)  «————————————»  S224DF3X15000291(port23)
FGT61FTK22054602(b)  «————————————»  S224DF3X15000291(port24)
Tier 1
S224DF3X15000373(port23)  «————————————»  FGT61FTK22054783(a)
S224DF3X15000373(port24)  «————————————»  FGT61FTK22054602(a)
S224DF3X15000291(port23)  «————————————»  FGT61FTK22054783(b)
S224DF3X15000291(port24)  «————————————»  FGT61FTK22054602(b)
Tier 2+
S224ENTF20002824(port23/_FlInK1_MLAG0_)  «————————————»  S224DF3X15000373(port4/4ENTF20002824-0)
S224ENTF22001220(port23/_FlInK1_MLAG0_)  «————————————»  S224DF3X15000373(port3/4ENTF22001220-0)
S224DF3X15000373(port1/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port1/4DF3X15000373-0)
S224DF3X15000373(port2/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port2/4DF3X15000373-0)
```

5. 编辑交换机，可以修改交换机名字以及升级版本，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





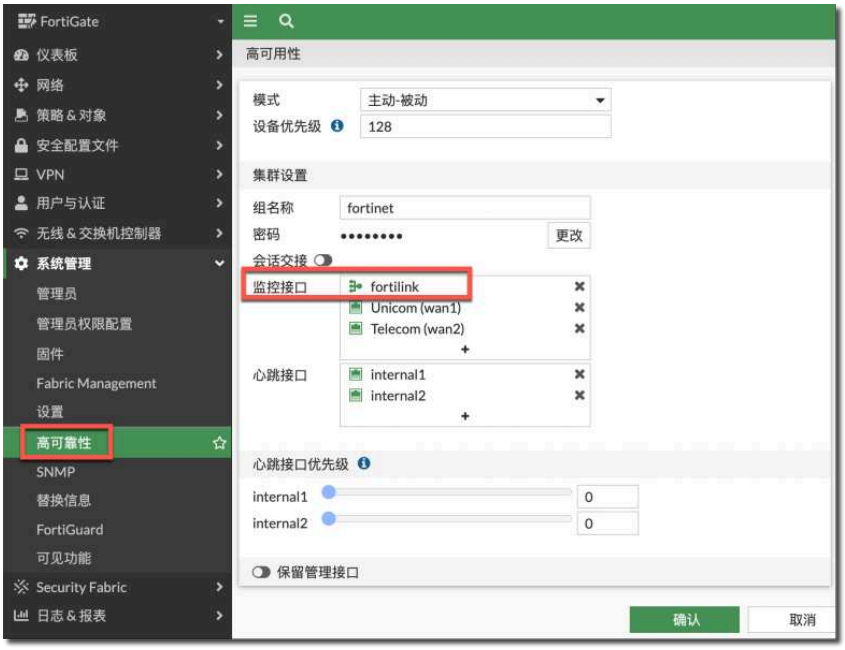
6. FortiSwitch之间接多根线进行FortiLink互联，会默认自动聚合。其实接一根网线也是聚合的，只是聚合组里面只有一个接口而已，因此多根网线直连，这些直连的线都会自动加入到一个聚合接口里面（建议MC-LAG环境尽量使用两条或以上的连线）。

```
FortiGate # exec ssh admin@10.255.1.6
admin@10.255.1.6's password:

Core-FSW1 # show switch trunk

config switch trunk
    edit "GT61FTK22054602"
        set mode lacp-active
        set auto-isl 1
        set fortilink 1
        set mclag enable
        set members "port24"
    next
    edit "GT61FTK22054783"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set mode lacp-active
        set auto-isl 1
        set fortilink 1
        set mclag enable
        set members "port23"
    next
    edit "4DF3X15000291-0"
        set mode lacp-active
        set auto-isl 1
        set mclag-icl enable
        set members "port1" "port2"
    next
    edit "4ENTF20002824-0"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port4"
    next
    edit "4ENTF22001220-0"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port3"
    next
end
```

7. 最后不要忘记，在FortiLink的聚合接口和FortiLink管理配置完毕，记得把这个FortiLink聚合接口加入到HA的监控接口列表中，这样当主核心交换机挂了（比如断电）之后，业务才可以平稳切换到备防火墙上。

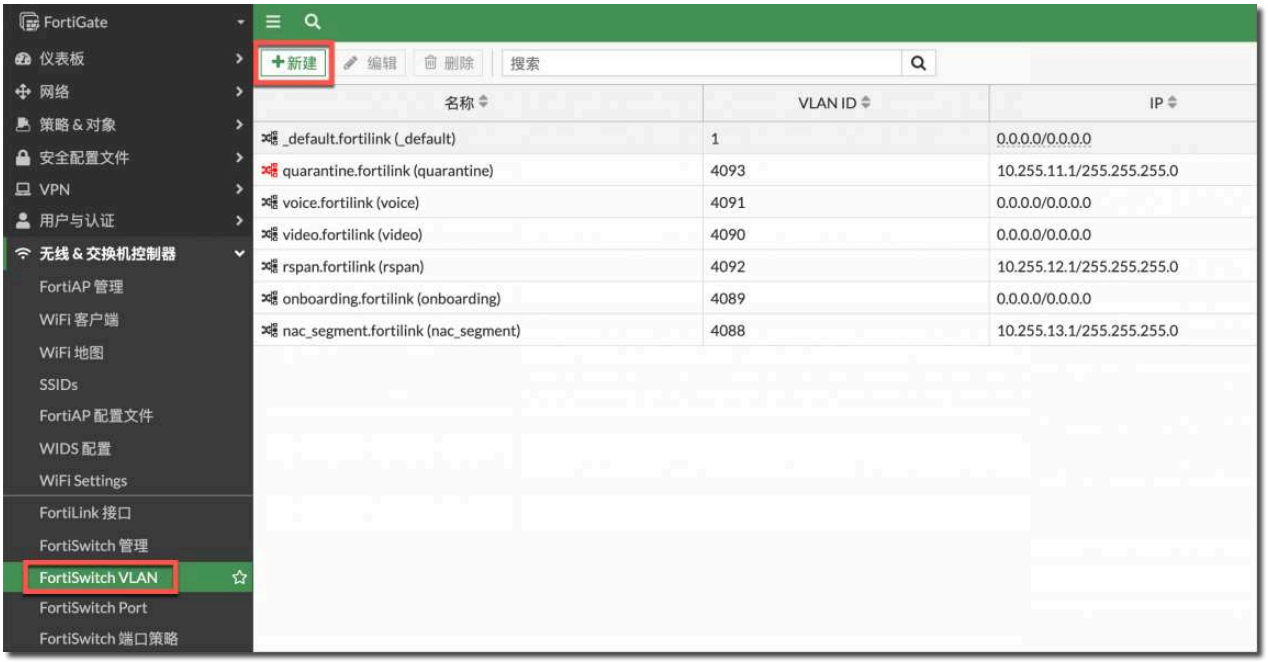


创建VLAN

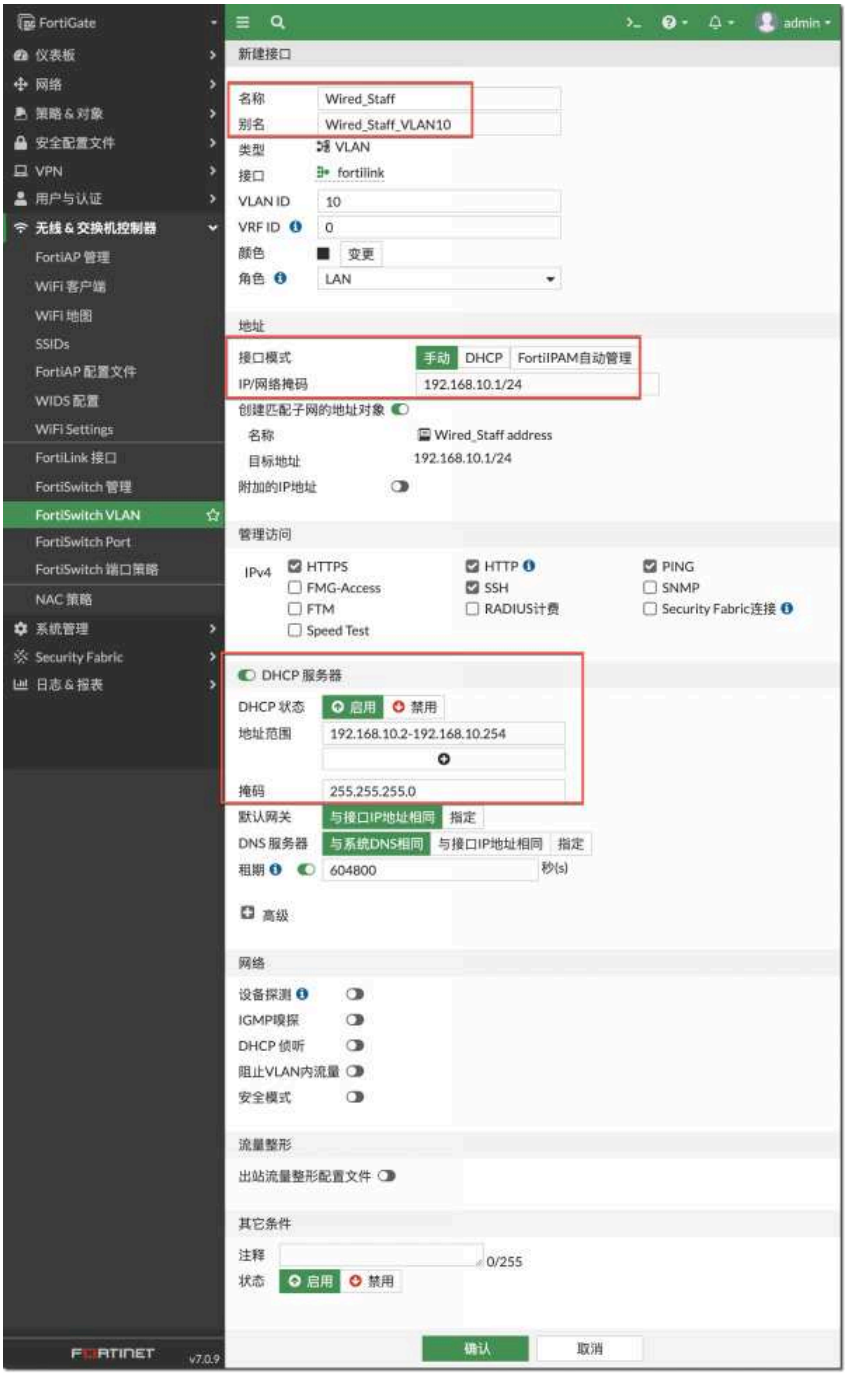
1. FortiGate通过FortiLink + Capwap协议统一的接管FortiSwitch和FortiAP，为有线和无线统一进行管理和业务处理。

2. 进入FortiGate的无线&交换机控制器→FortiSwitch VLAN页面，新建有线网络VLAN 10、员工无线网络VLAN 20、访客无线网络VLAN 30、管理FortiAP VLAN 99。注意管理FortiAP的VLAN接口要开启Security Fabric，包含CAPWAP。

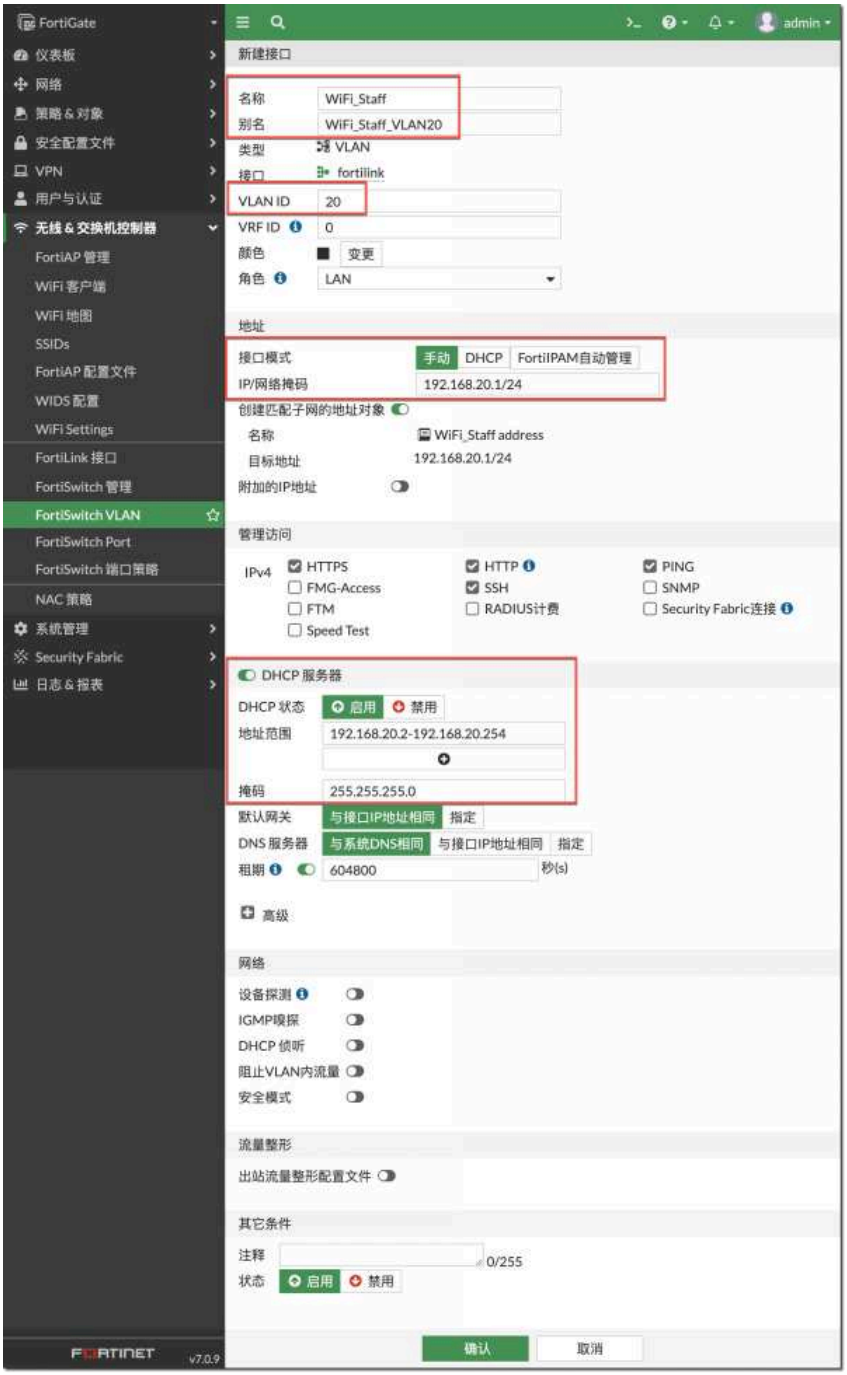
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



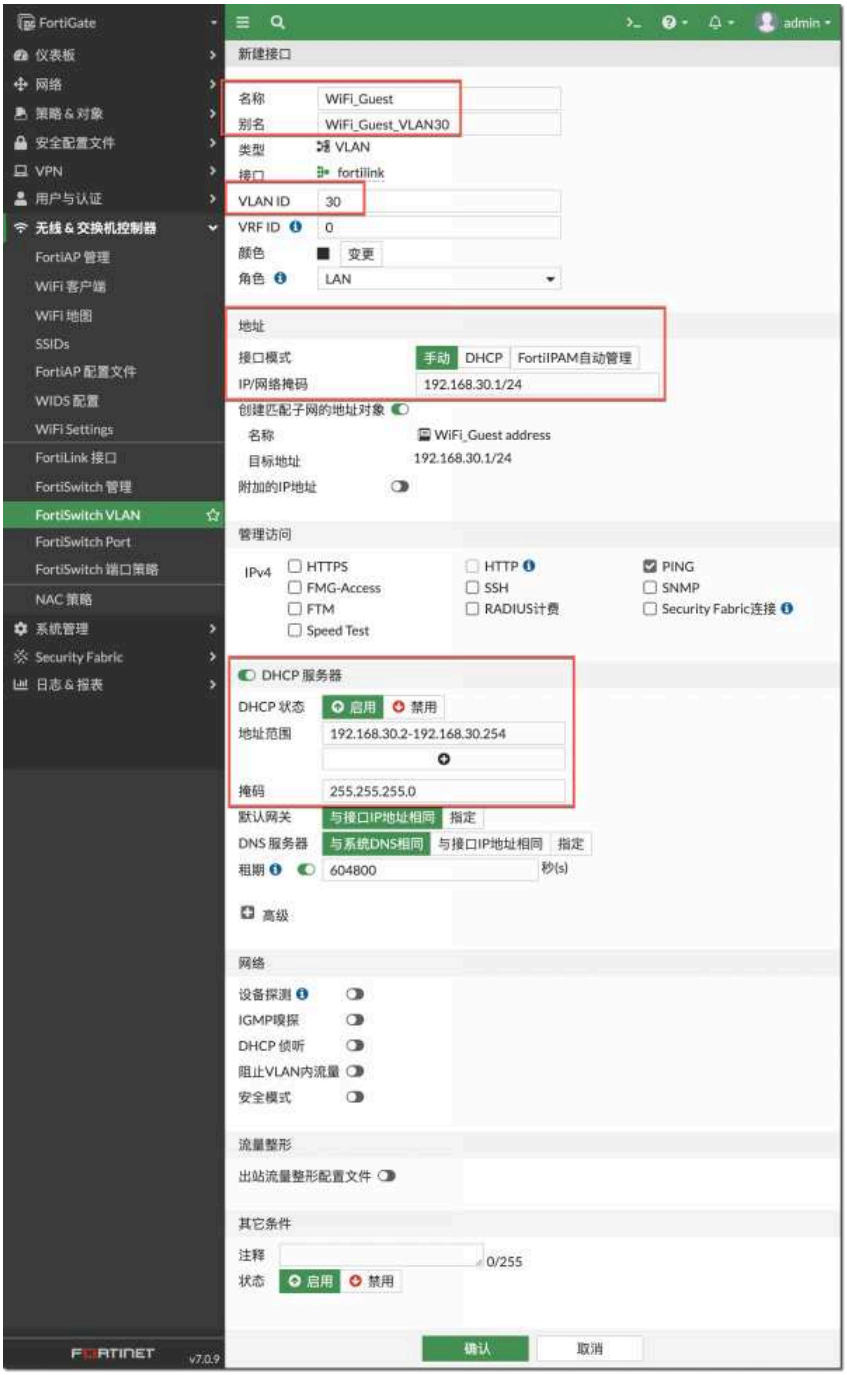
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



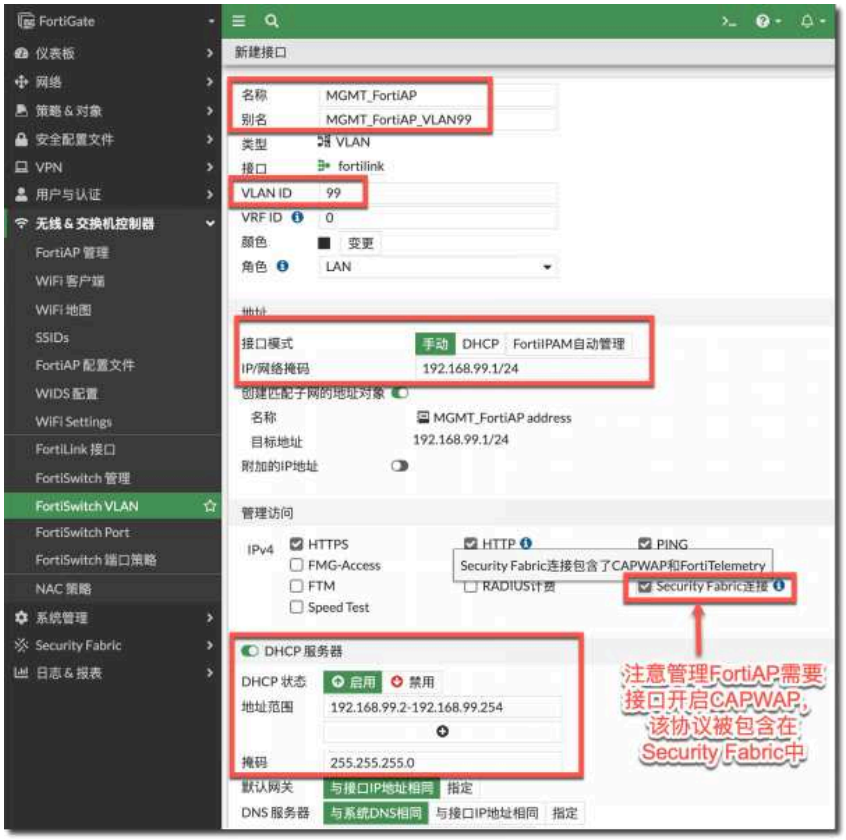
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

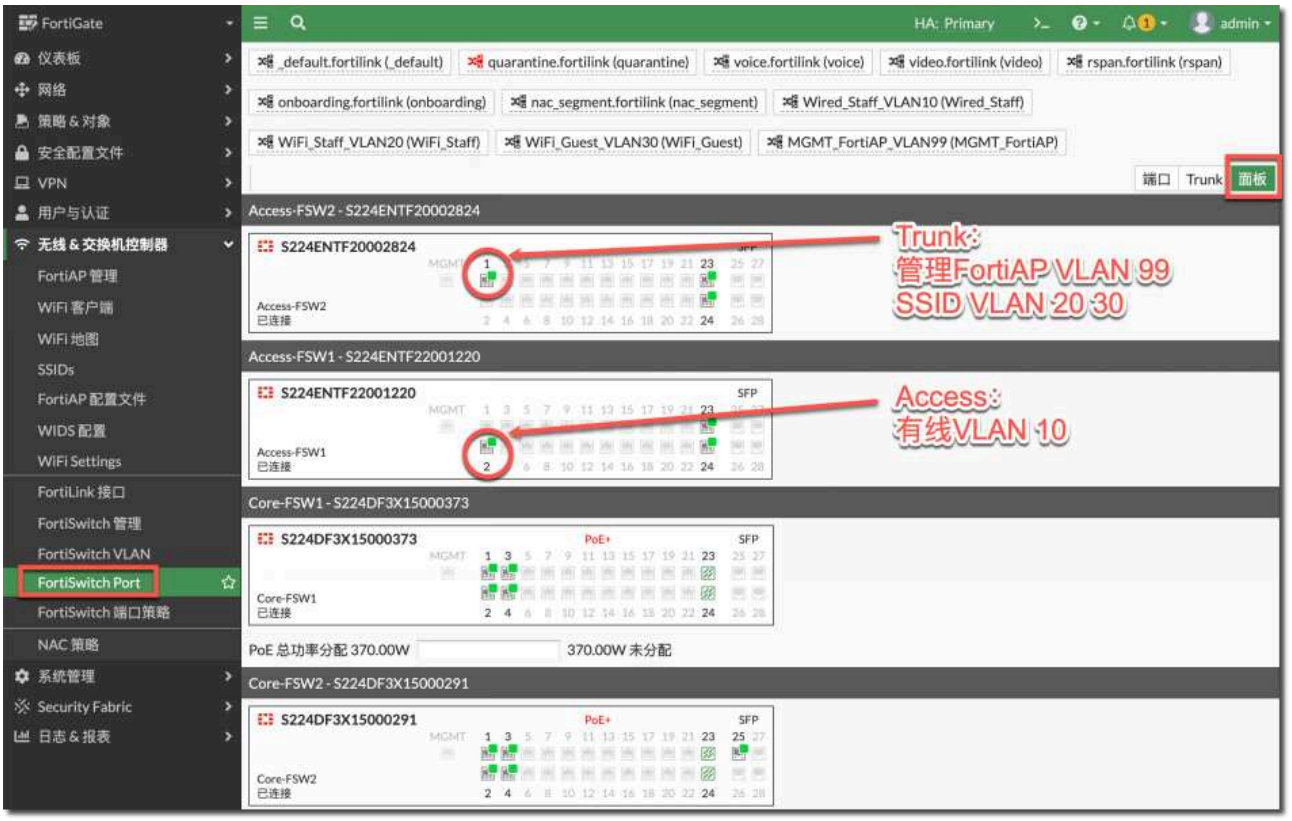


3. VLAN创建完成。

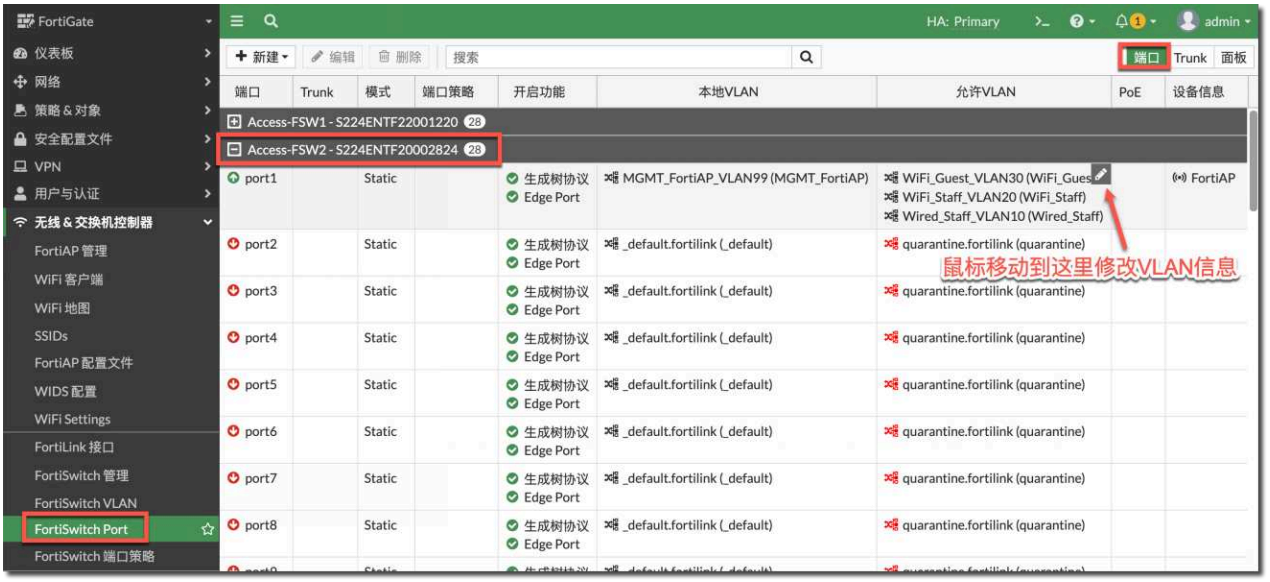


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

分配VLAN

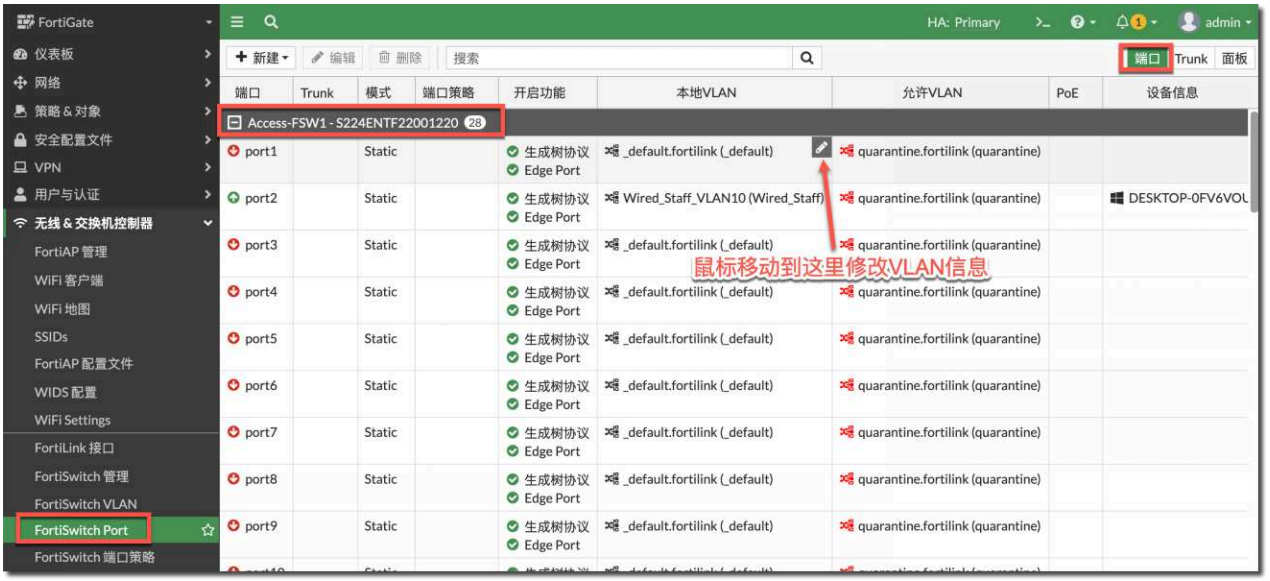


1. Access-FSW2交换机的port1接FortiAP，配置为Trunk模式，允许 VLAN20和VLAN30，VLAN20用于WIFI-STAFF的SSID用户，VLAN30用于WIFI-GUEST的SSID用户。另外本地VLAN设置为VLAN 99，用于FortiAP的管理（FortiAP的管理相当于使用不打vlan-tag的VLAN 99，本地VLAN默认是VLAN 1，因此只需要将本地VLAN设置为VLAN 99即可）。



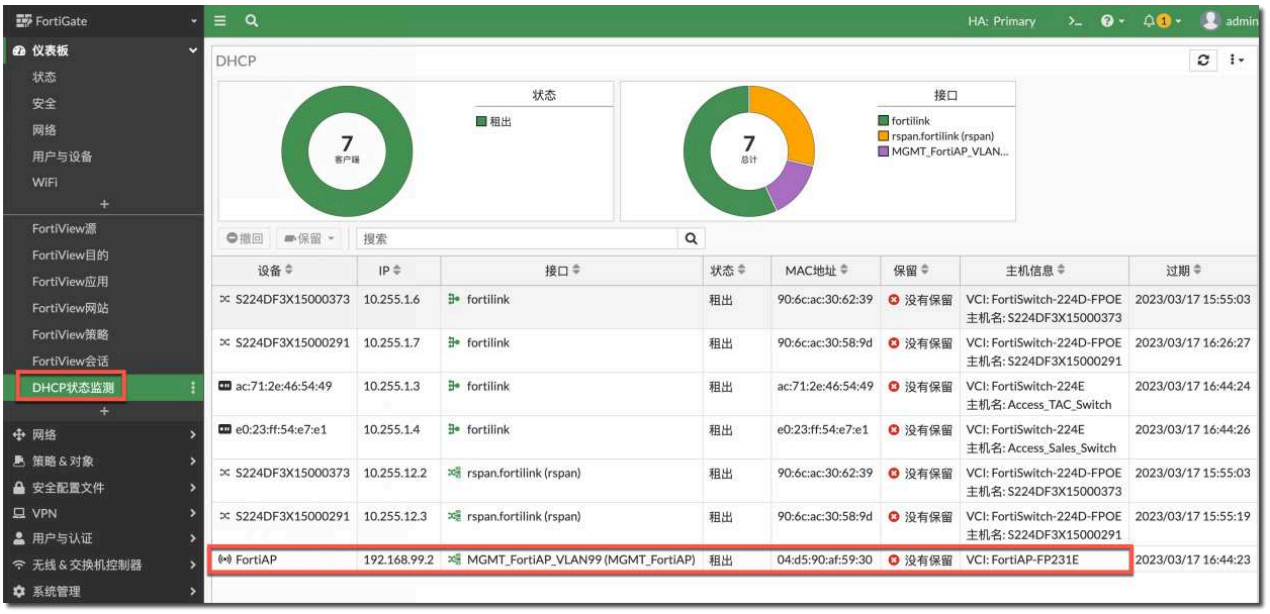
2. Access-FSW1交换机的Port2接具体的物理PC，因此只需要将Port2设置为access口，分配VLAN 10即可，用FortiSwitch的概念来说就是将本地VLAN设置为VLAN 10，本地VLAN不打vlan-tag，相当于就是设置接口为access vlan 10。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



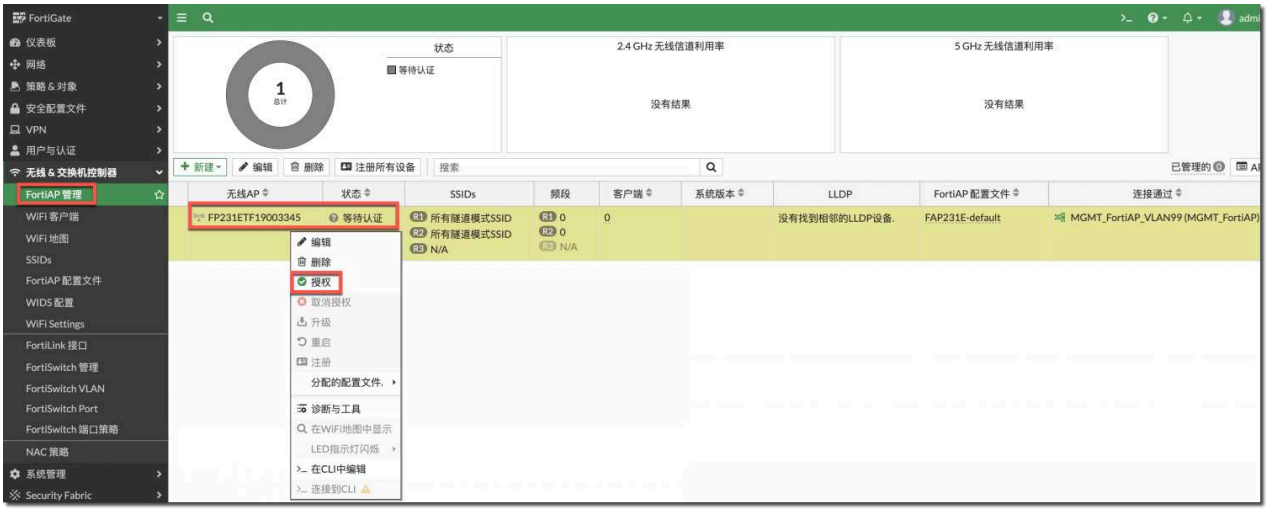
无线配置

1. FortiAP连接后，会通过VLAN 99的DHCP获取到192.168.99.0/24网段的IP地址。

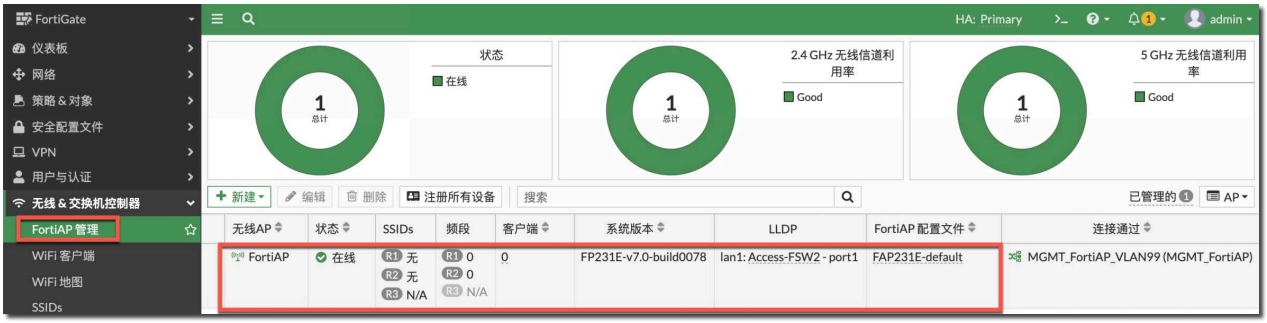


2. 在之前的配置中，VLAN 99的接口开启了CAPWAP协议（包含在Security Fabric中），激活了FortiGate的无线管理功能，这时候FortiAP会自动找到FGT进行注册。因此在FortiAP管理的地方可以看到这个FortiAP的信息（如果没有看到检查配置，并将FortiAP恢复出厂，让FortiAP重新获取IP地址并发起注册）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 右键点击上图中等待认证的FortiAP，点击授权按钮，等待几分钟，FortiAP成功上线。



4. 编辑FortiAP设置，配置FortiAP的名称，或进行升级操作。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 进入无线&交换机控制器→SSIDs页面，点击新建按钮。

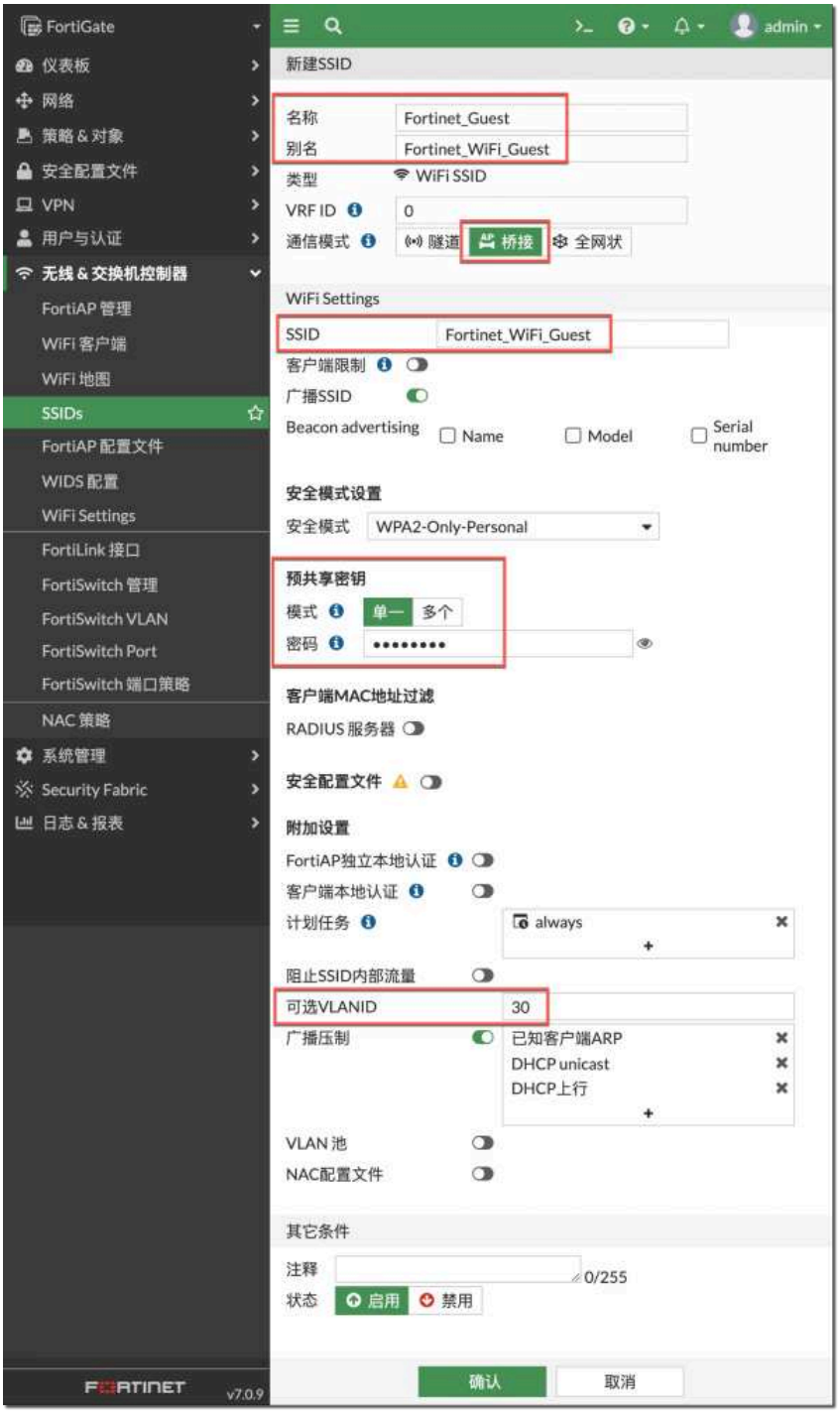


6. 新建SSID：Fortinet_WiFi_Staff VLAN 20用于员工WIFI使用，Fortinet_WiFi_Guest VLAN 30用于访客WiFi使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





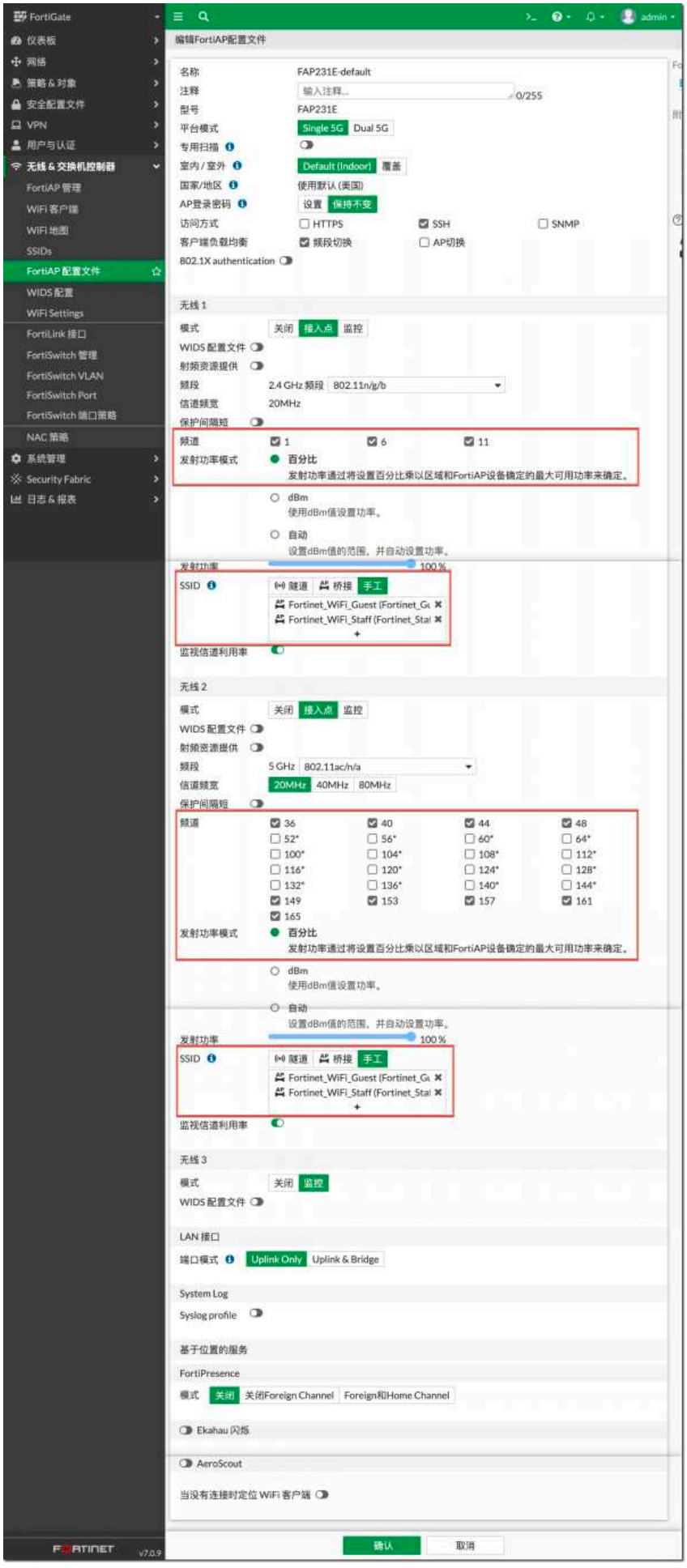
7. 将SSID关联到FortiAP上，然后让FortiAP发布无线SSID信号，这样用户就可以通过SSID连接到无线了。进入FortiAP配置文件页面，编辑FortiAP关联的配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 桥模式的SSID需要在FortiAP配置文件里面手工指定一下，另外下图标示出的配置为推荐配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

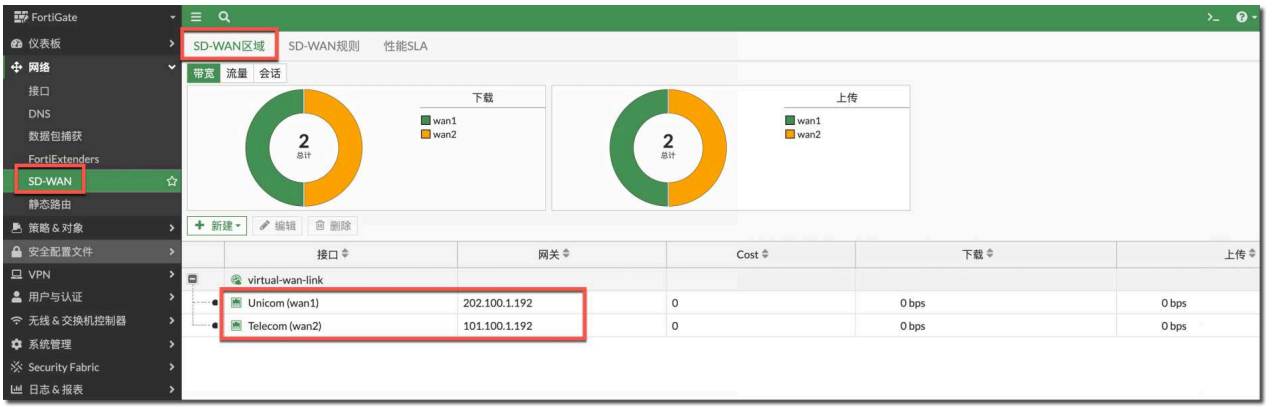


9. FortiAP会自动关联到这个FortiAP配置文件里面的内容，发起SSID的信号。



SD-WAN配置

1. 将wan1和wan2加入SD-WAN接口，并配置各自的网关。

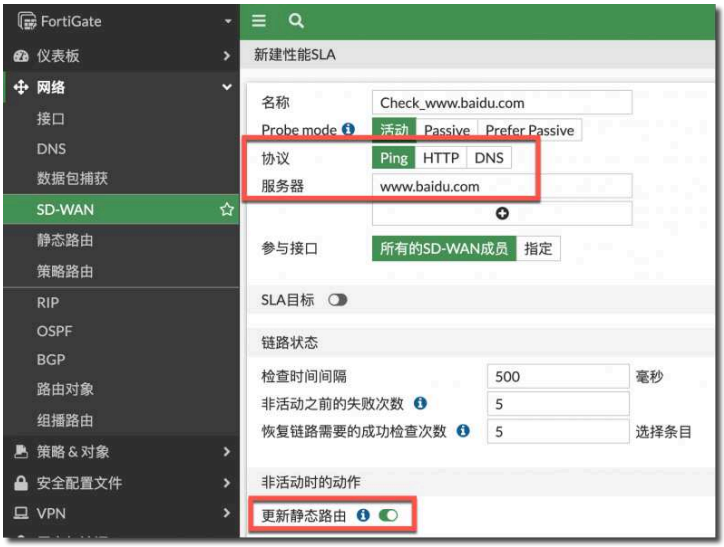


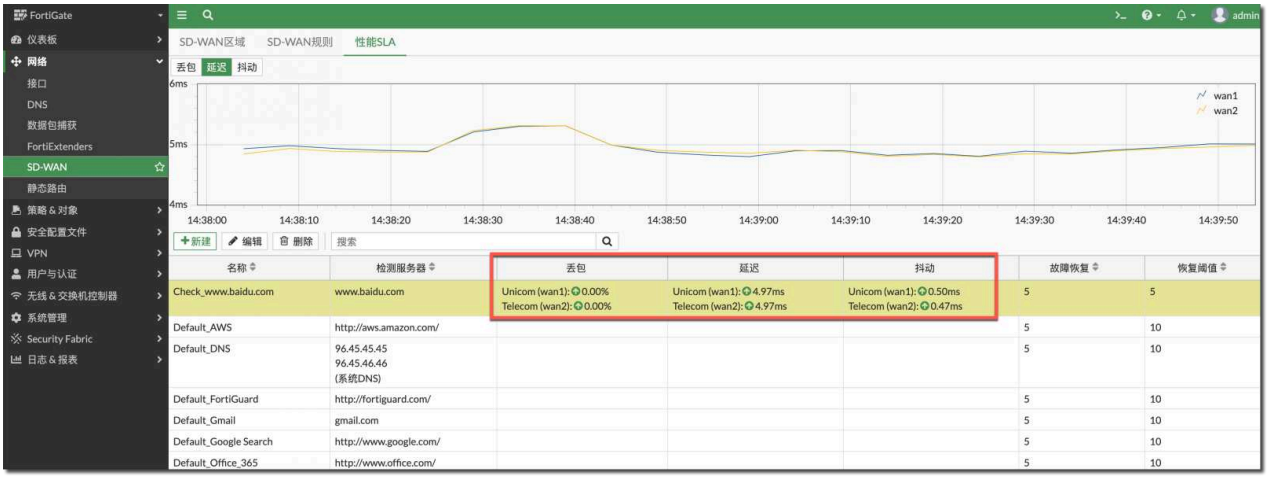
2. 添加SD-WAN的默认路由。



3. 配置SD-WAN的SLA，以便wan1和wan2相互备份和切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. SD-WAN规则可根据需求配置，这里保持默认的按照源IP负载均衡。



安全策略配置

1. 需求与规划：

   - 员工的有线与无线都需要访问互联网
   - 访客的无线仅仅可以访问互联网
   - 员工的有线和无线需要互访

2. 建议将防火墙的接口划分区域，以区域的方式配置策略，有时候可以做到简化配置的目的，甚至未来替换设备的时候，策略的备份和还原也会更加简单一些。规划区域两个区域：

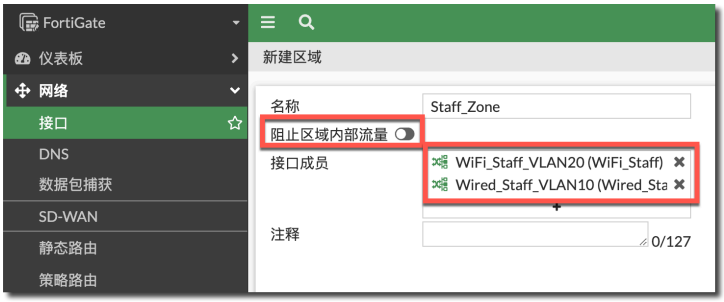
   - 员工网络区域：包括员工的有线VLAN 10和员工的无线VLAN 20 （区域之间的隔离关闭，这样VLAN 10和VLAN 20之间的数据可通）
   - 访问网络区域：包括访问的无线VLAN 30

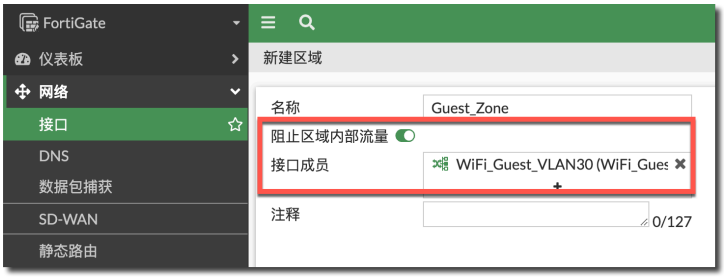
3. 进入网络→接口页面，新建所属区域。

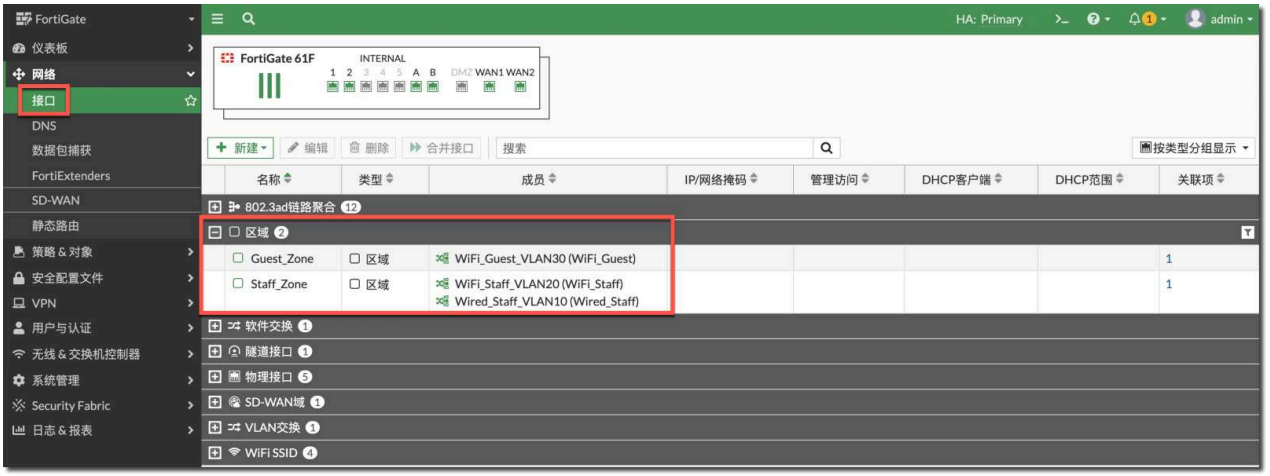
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 分别创建Staff_Zone（包含VLAN 10和VLAN20）和Guest_Zone（包含VLAN30）。







5. 如此只需要配置两条策略，就可以实现我们规划的需求，新建Staff-Zone到SD-WAN与Guest-Zone到SD-WAN的安全策略。

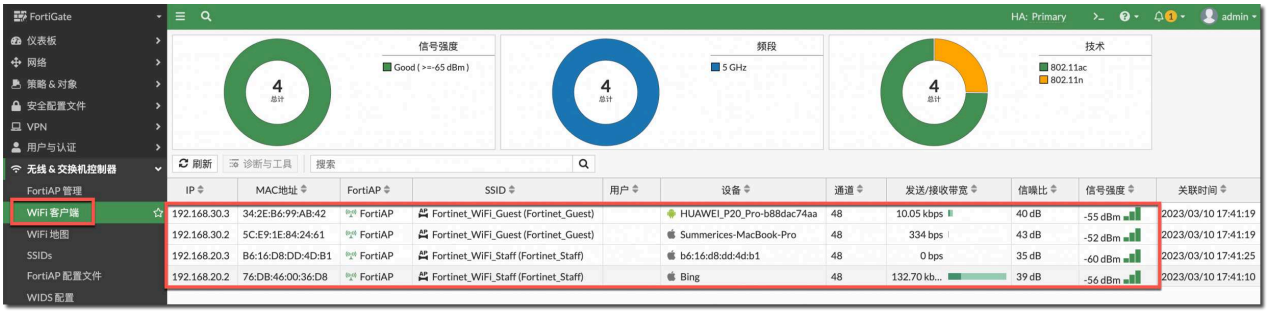


结果验证

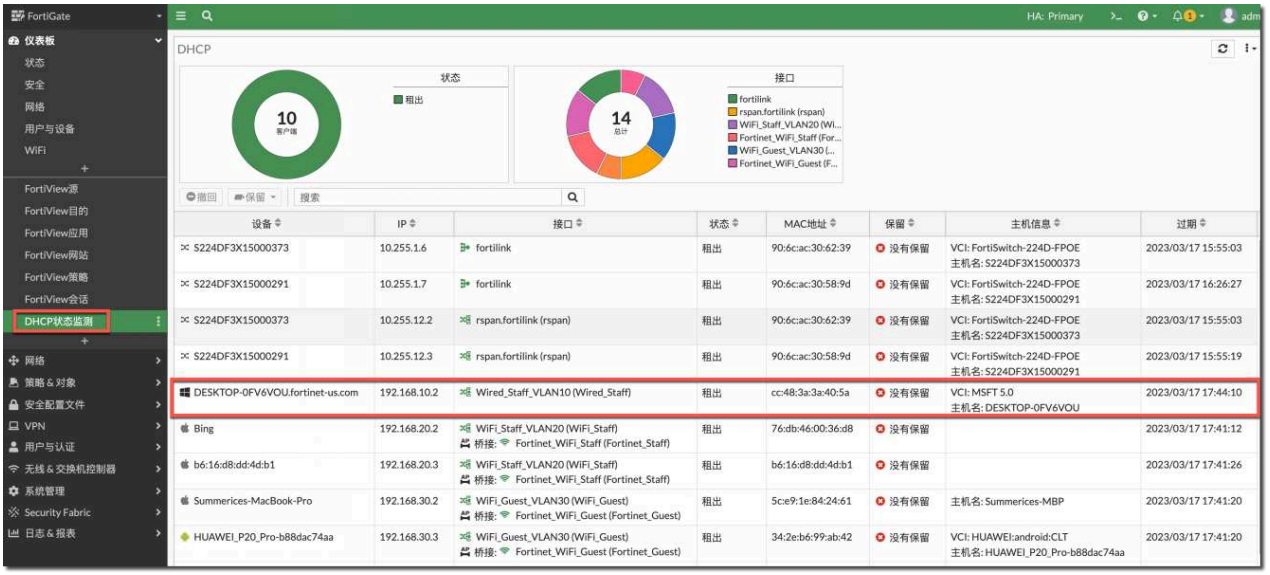
客户端访问

1. 进入无线&交换机控制器→WiFi客户端，查看在线的无线客户端。可以看到WiFi_Staff和WiFi_Guest各有一个终端在线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在DHCP状态检测中查看所有的客户端信息，可以看到有线网络的PC也正常上线。

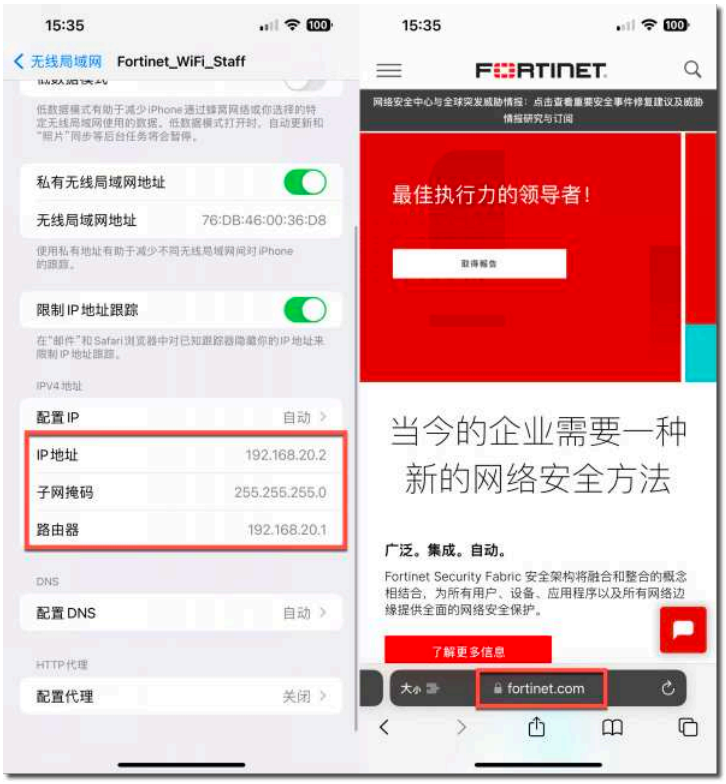


3. 有线网络（VLAN 10）用户访问互联网。

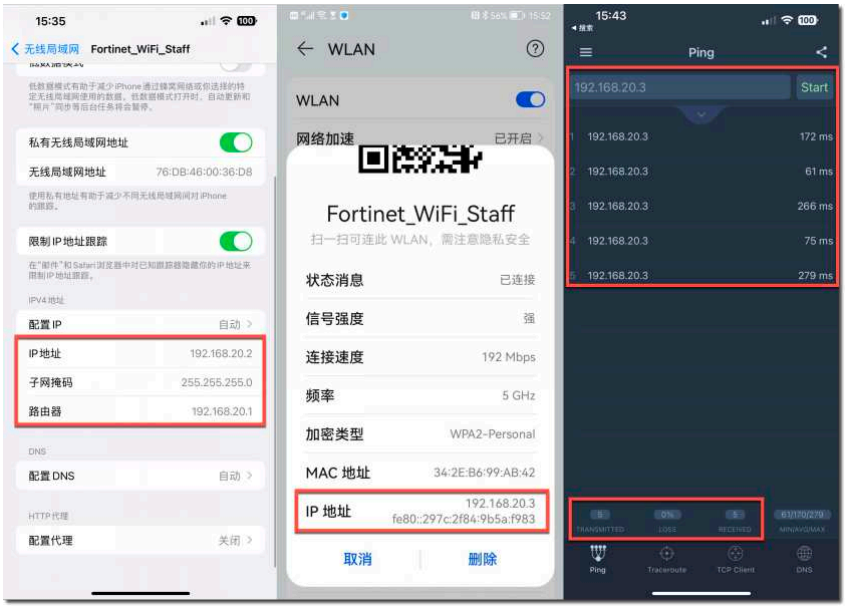


4. 无线网络用户访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

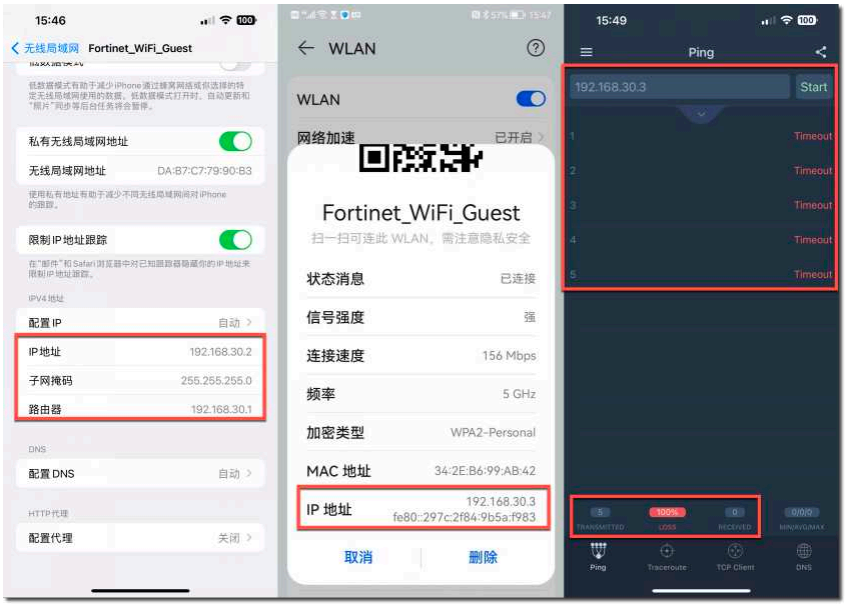


5. 使用VLAN 20下的客户端访问VLAN 20下的另一个客户端（Staff区域）。



6. 使用VLAN 30下的客户端访问VLAN 30下的另一个客户端（Guest区域），可以看到由于该区域配置了禁止相互访问，所以VLAN 30下的客户端是无法互相访问的。

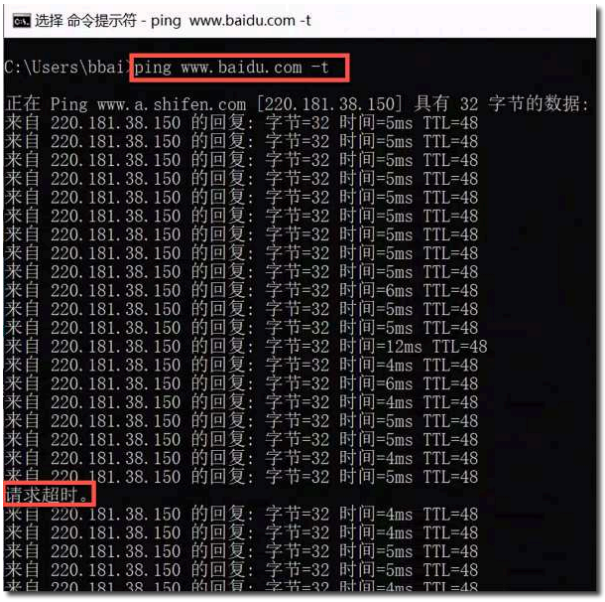
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiLink切换测试

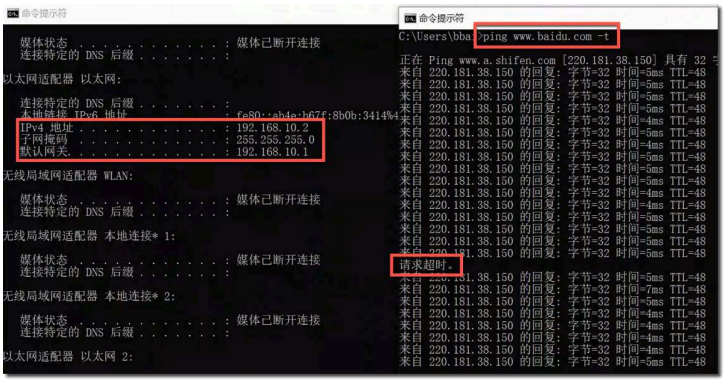
1. 在我们的测试场景下FortiLink聚合接口的a和b是同时UP起来的，如果a或b DOWN（不能同时DOWN），是否有影响业务呢?

2. 经过测试，DOWN a或b接口，客户端丢包1个或者不丢包。



HA切换测试

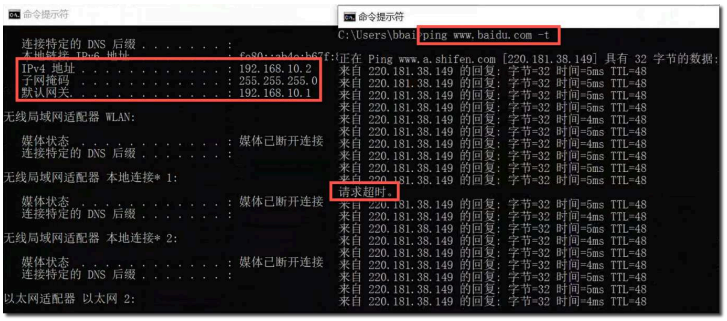
重启当前主防火墙查看内网PC丢包情况，HA切换丢包1个。



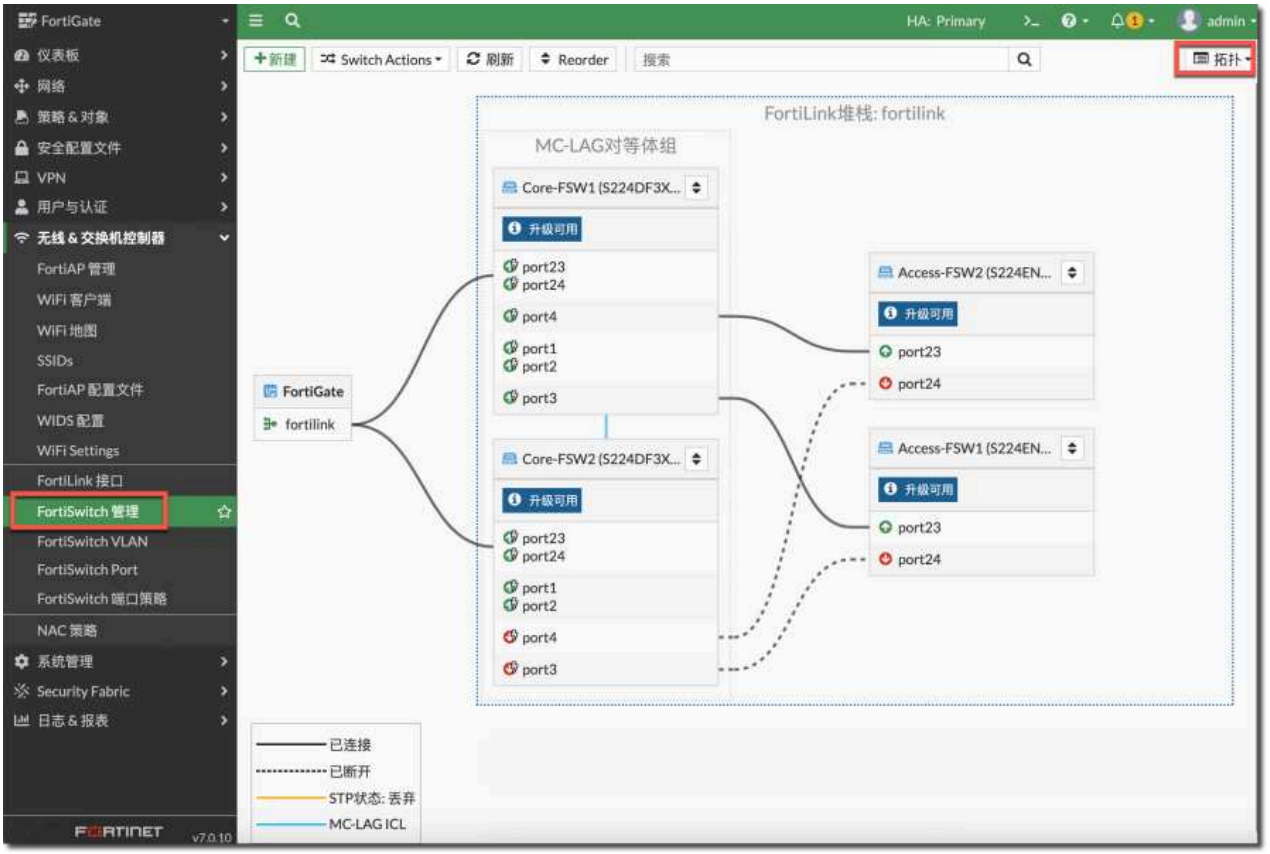
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

核心交换机接口故障模拟

1. Down掉Core-FSW2的Port3和Port4接口，查看内网PC丢包情况，可以看到Core-FSW2连接接入层交换机的接口Down掉时，丢包1个。



2. 查看和Switch管理拓扑，Core-FSW2与接入层交换机的连线已断开。



注意事项

1. 只能是堆叠交换机才可以跨交换机聚合，不同的堆叠交换机组，不支持配置为聚合接口。
2. 如果是与FortiSwith对接，则是自动MCLAG聚合。
3. 如果是和第三方设备对接，比如交换机、路由器、友商防火墙、服务器等等对接的话，推荐使用LACP Active方式动态聚合。

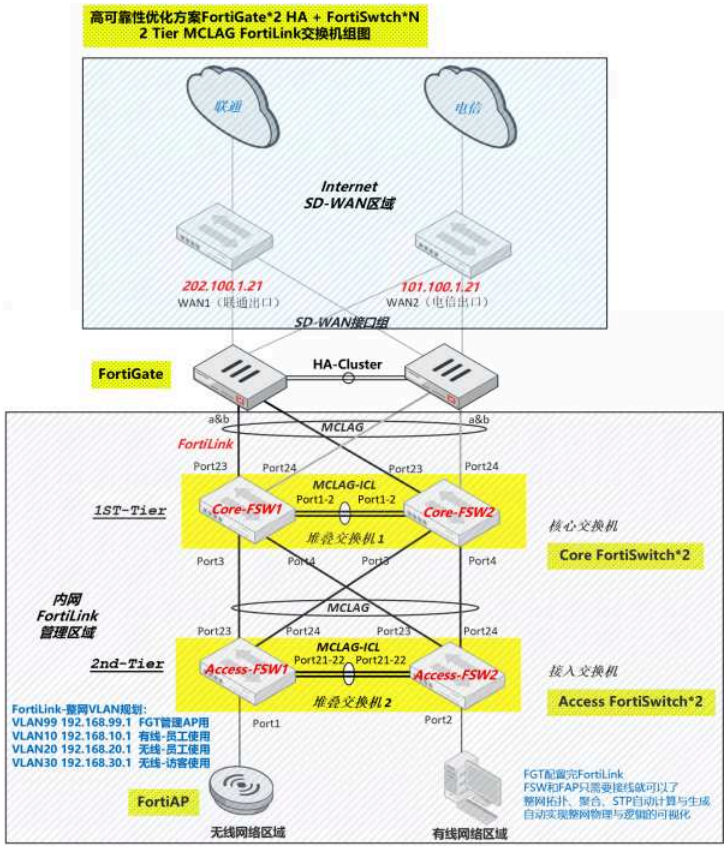
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink MCLAG-堆叠组网2 Tier配置举例

网络需求

FortiGate运行HA-Cluster，核心交换和接入交换机采用MCLAG堆叠组网结构。

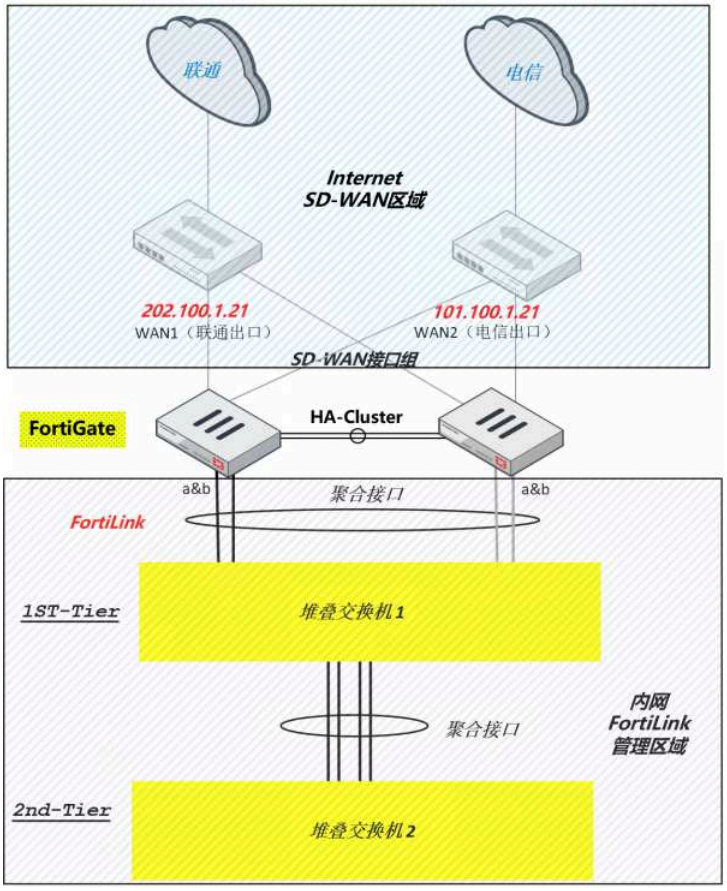
网络拓扑



形成堆叠之后的逻辑拓扑：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

高可靠性优化方案FortiGate*2 HA + FortiSwtch*N
2 Tier MCLAG FortiLink交换机组图



1. 两台FortiGate配置为HA主备模式。
2. 整体规划：
   - 外网IP网段规划：
     - WAN1联通出口：IP 202.100.1.21，GW 202.100.1.192
     - WAN2电信出口：IP 101.100.1.21，GW 101.100.1.192
   - WAN1和WAN2合并成SD-WAN接口。
   - 内网IP网段规划，FGT通过FortiLink+Capwap协议统一的接管FortiSW和FortiAP，为有线和无线统一进行管理和业务处理：
     - 有线网络规划：VLAN 10，192.168.10.1
     - 无线网络规划：员工WIFI VLAN 20，192.168.20.1
     - 无线网络规划：访客WIFI VLAN 30，192.168.30.1
     - 管理FortiAP：VLAN 99，192.168.99.1
   - FortiLink互联部分规划：
     - FortiGate的a和b做聚合接口与Fortiswitch的后两个接口互联即可实现聚合接口的FortiLink管理。
     - 加入FortiLink的接口自动变为聚合口成员。

配置要点

1. FortiGate配置聚合端口，并设置split为enable模式。
2. 上线Core-FSW1和Core-FSW2，将FortiGate和Core-FSW1以及Core-FSW2连接起来。
3. 分别登录到Core-FSW2和Core-FSW1上，配置二者直连的ISL 接口为“mclag-icl enable”。配置为ICL堆叠线路（Inter-Chassis-Link），形成两台核心交换机的堆叠。
4. 配置FortiGate聚合端口为split disable模式。
5. 上线Access-FSW1和Access-FSW2。
6. 分别登录到Access-FSW1和Access-FSW2上，配置二者直连的ISL 接口为“mclag-icl enable”。配置为ICL堆叠线路（Inter-Chassis-Link），形成两台接入交换机的堆叠。
7. 在Core-FSW1和Core-FSW2上分别配置auto-isl-port-group，注意group的名字必须一致，端口可以不一样，这样是为了让核心的堆叠交换机与接入的堆叠交换机相互跨交换机手工形成聚合。
8. 上线FortiAP和有线PC，并测试无线网络和有线网络的连通性。
9. 注意：如果Switch上线时，有的Switch是旧的版本，最好先升级Switch的版本后，再组建mclag或是让交换机成环。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

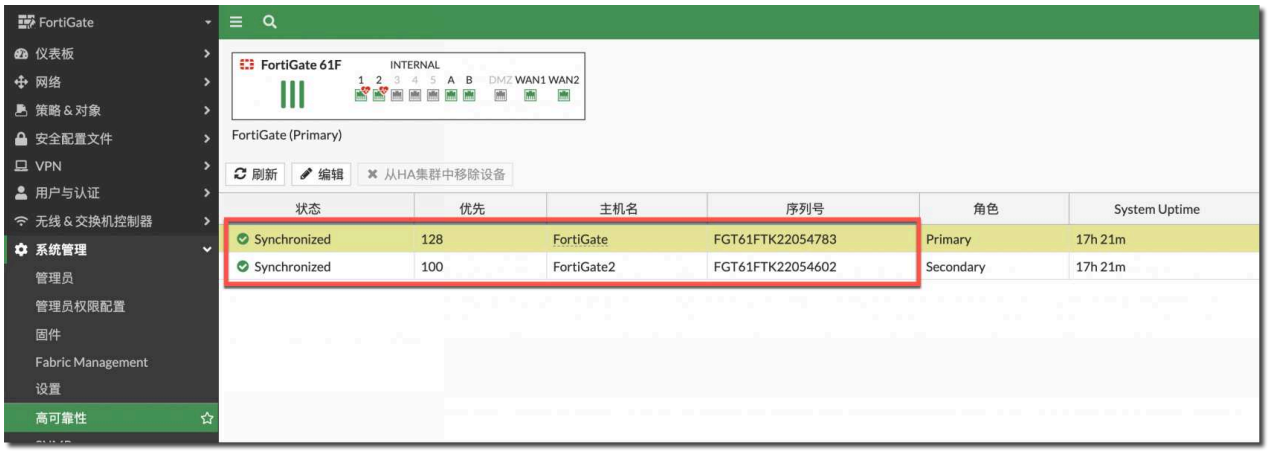
配置步骤

准备事项

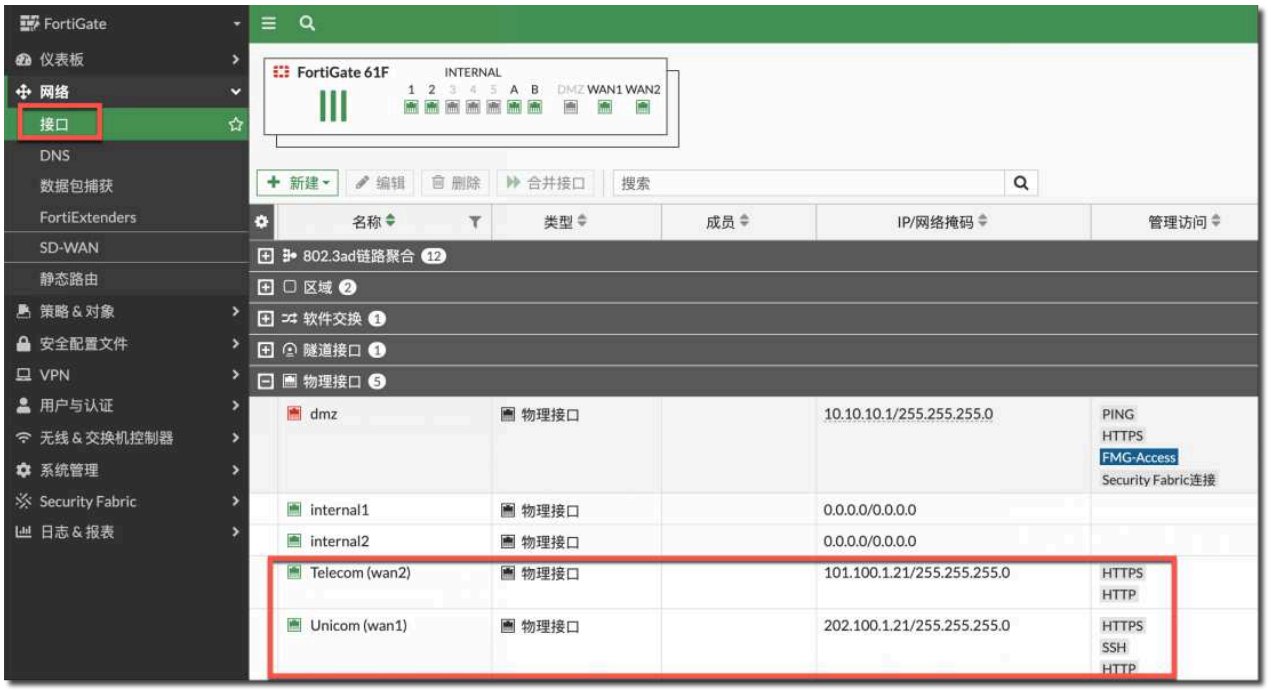
1. 首先确认FortiGate如下全局配置已开启（一般默认为开启状态）。

```
config system settings
    set gui-switch-controller enable
end
```

2. 配置两台FortiGate的HA主备模式（配置方法请参考HA双机热备→HA典型基础配置 ↗）。



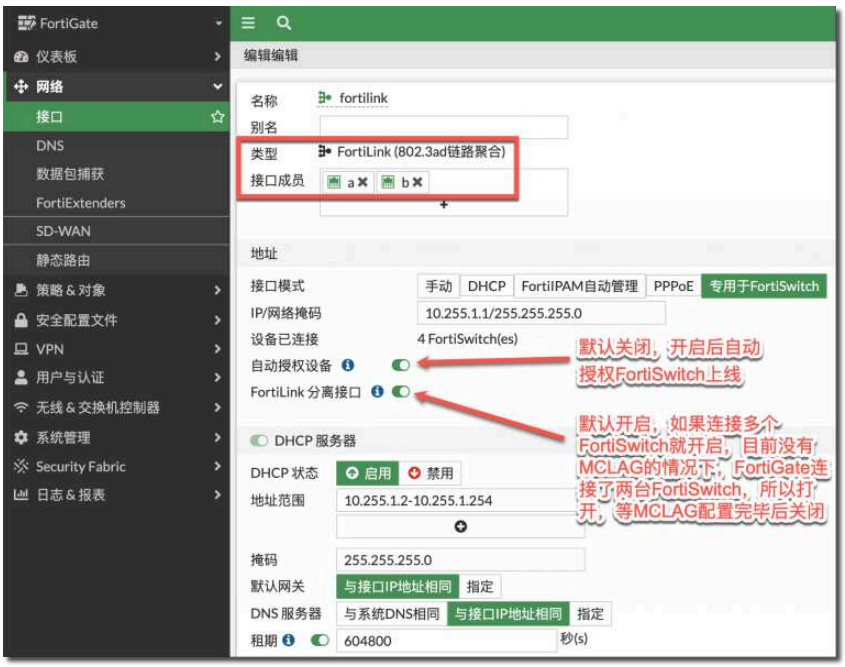
3. 配置wan1和wan2的IP地址。



4. 配置FortiLink实现FortiSwith上线，我们只需要将用于FortiLink的成员接口加入FortiLink接口即可。此拓扑中，FortiGate用于连接FortiSwitch的接口为a和b，编辑FortiLink接口，将a和b加入FortiLink（某些产品型号会默认将两个接口加入FortiLink），开启自动授权设备，关闭FortiLink分离接口，其他配置保持默认，可以看到FortiLink为一个聚合接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

FortiLink分离接口什么时候应该开启?

分离接口的意是，如果聚合接口的port1和port2分别连接了一台SW，在没有使用MCLAG的情况下（没开启堆叠功能），则聚合接口的port1和port2没办法同时UP（同时开启聚合接口无法正常工作），因此必须开启FortiLink分离接口功能，让聚合接口只有一个物理接口（port1）是处于UP状态的，另外一个物理接口（port2）处于DOWN的备份状态，当port1接口状态DOWN，则Port2立即接管Port1的工作，让聚合接口的FortiLink继续运行，这是一个聚合接口在FortiLink管理时候的备份机制。



MCLAG配置前是上述组网，因此刚刚开始的时候需要，保持enable状态。聚合接口的Port1和Port2只会UP一个接口，另外一个接口处于DOWN的状态。

重要

FortiLink split interface什么时候应该disable?

如果FGT的聚合接口只接到了一台交换机上，并没有跨交换机聚合（没有MCLAG，也不需要FortiLink split interface），因此这种情况应该让聚合接口的两个物理接口port1和port2同时UP，两个接口同时工作起来，以便提供更高带宽和备份的作用。



配置两台交换机MCLAG堆叠之后，就是上述组网，因此交换机堆叠完毕之后，需要修改为disable，让两个聚合接口都可以同时工作起来，最大的利用聚合接口的带宽和资源。这个配置后续会说明。

相关CLI:

```
NTP:
config system ntp
    set ntpsync enable
    set server-mode enable
    set interface "fortilink"
end
-------------------------------------------------------------------
DHCP:
config system dhcp server
    edit 2
        set dns-service local
        set ntp-service local
        set default-gateway 10.255.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 10.255.1.2
                set end-ip 10.255.1.254
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtender"
    next
end
--------------------------------------------------------------------------------
FortiLink:
config system interface
    edit "fortilink"
        set vdom "root"
        set fortilink enable
        set ip 10.255.1.1 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set member "a" "b"
        set lldp-reception enable
        set lldp-transmission enable
        set auto-auth-extension-device enable
        set fortilink-split-interface enable
        set switch-controller-nac "fortilink"
        set switch-controller-dynamic "fortilink"
        set swc-first-create 255
    next
end

```

连接FortiLink

连接核心交换机

1. 配置完FortiGate之后，这个时候再去接FortiGate的FortiLink到FortiSwitch的线，配置Core-FSW1和Core-FSW2设备的互联接口MCLAG注意，先不要把所有的线都接上去，一台一台的来操作，MCLAG配置尽量使用Console去配置，而不是GUI，有时候由于在Fortilink计算和收敛会导致GUI连接不上去，或者先将CORE-FSW1下线，先单独配置CORE-FSW2，然后再将CORE-FSW2下线，再单独配置CORE-FSW1，然后再将二者互联的线接上去，这样是最稳妥的办法，避免GUI的CLI连不上的情况出现。而接入交换机这个时候是不建议接入的，等CORE-FSW1和CORE-FSW2的堆叠形成了之后，再将接入层交换机的线。

   > **重要**
   >
   > FortiSwitch如果以前有使用过，建议都恢复一下出厂设置，然后再加入到FortiLink。

2. FortiSwitch的靠后接口一般都默认开启了FortiLink接口属性，如果接前面的接口可能会无法加入到FortiLink，因此FortiSwitch的FortiLink最好都使用靠后的接口进行接线。FortiSwitch各型号默认开启FortiLink功能的接口如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiSwitch型号	默认开启FortiLink的接口
FS-108D-POE	port9–port10
FS-108E, FS-108E-POE, FS-108E-FPOE	port7–port10
FSR-112D-POE	port5–port12
FS-124D, FS-124D-POE	port23–port26
FSR-124D	port1-port4, port21–port28
FS-124E, FS-124E-POE, FS-124E-FPOE	port21–port28
FS-148E, FS-148E-POE	port21–port52
FS-224D-POE	port21–port24
FS-224D-FPOE	port21–port28
FS-224E, FS-224E-POE	port21–port28
FS-248D, FS-248D-FPOE	port45–port52
FS-248D-POE	port47–port50
FS-248E-POE, FS-248E-FPOE	port45–port52
FS-424D, FS-424D-POE, FS-424D-FPOE	port23–port26
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30
FS-548D	port39–port54
FS-548D-FPOE, FS-548DN	port45–port54
FS-1024D	port1–port24
FS-1048D, FS-1048E	port1–port52
FS-3032D, FS-3032E	port1–port32

3. 如果FortiSwitch无法被FortiGate管理，登陆到FortiSwitch上进行确认接口是否开启了FortiLink。

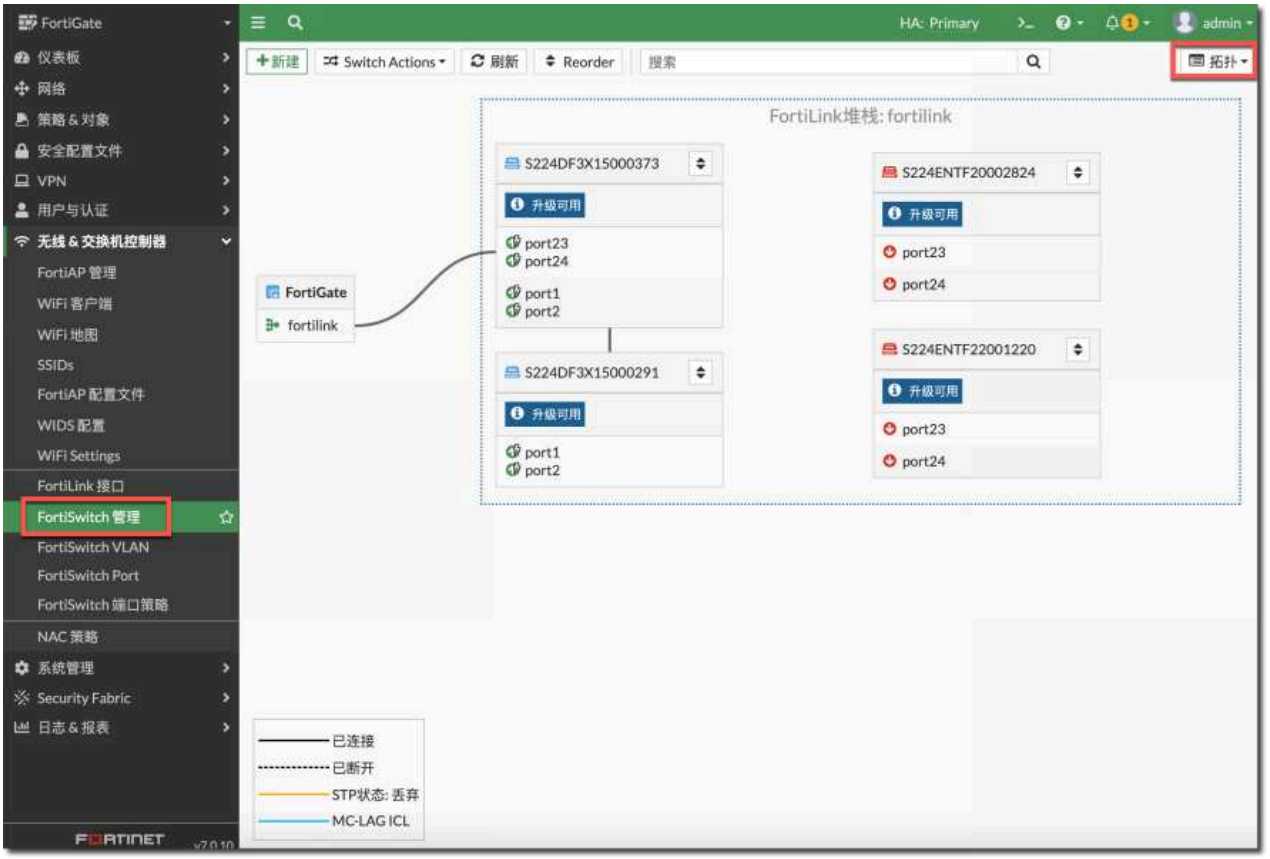
```
FortiSwitch # show switch interface port9
config switch interface
    edit "port9
        set auto-discovery-fortilink enable    //接口下又此命令的接口才可以自动加入到FortiLink中
    next
end
```

4. 交换机之间如果接多根线，会自动进行聚合，但是FortiLink自动聚合会花比较长的时间，建议可以先接单线，等FortiLink的拓扑较快的形成结束之后，再增加彼此之间的另外一根线，再进行自动聚合，这样效率会比较高一些。

5. 接线是很重要的步骤，仔细看拓扑图，做好接口标签，不要接错。

6. 先接Core-FSW1的线，再接Core-FSW1和Core-FSW2互联的线，先不要接接入层交换机的线，在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，右上角选择拓扑视图，查看交换机被管理状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



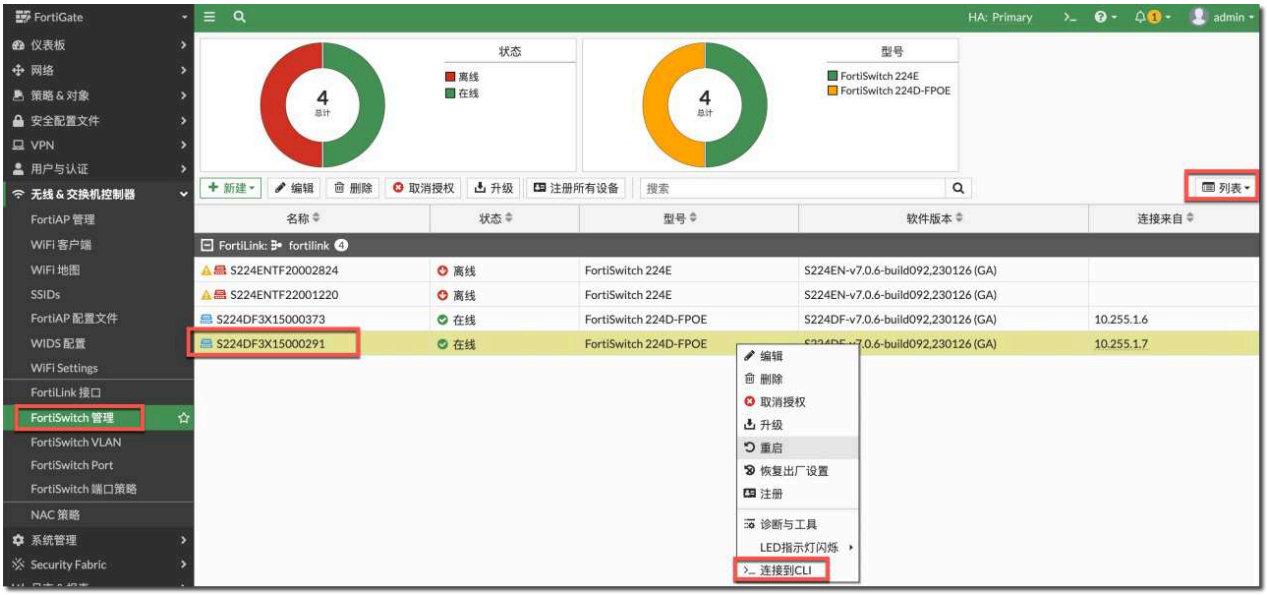
7. 此时我们看防火墙的FortiLink聚合接口，此时应该只有a或b其中一个物理接口是UP的，这是FortiLink split interface enable的结果。



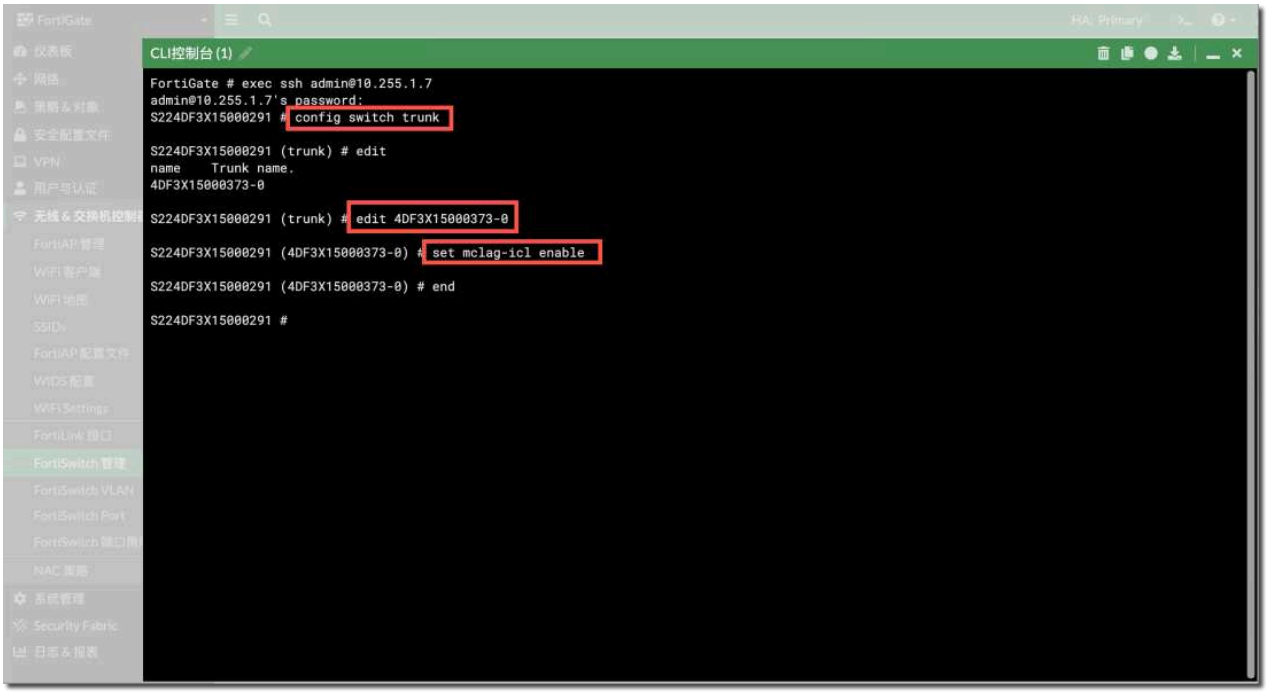
配置核心交换机MC-LAG

1. 通过FortiGate管理交换机页面右键交换机即可SSH到交换机，分别登录到Core-FSW1和Core-FSW2上。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

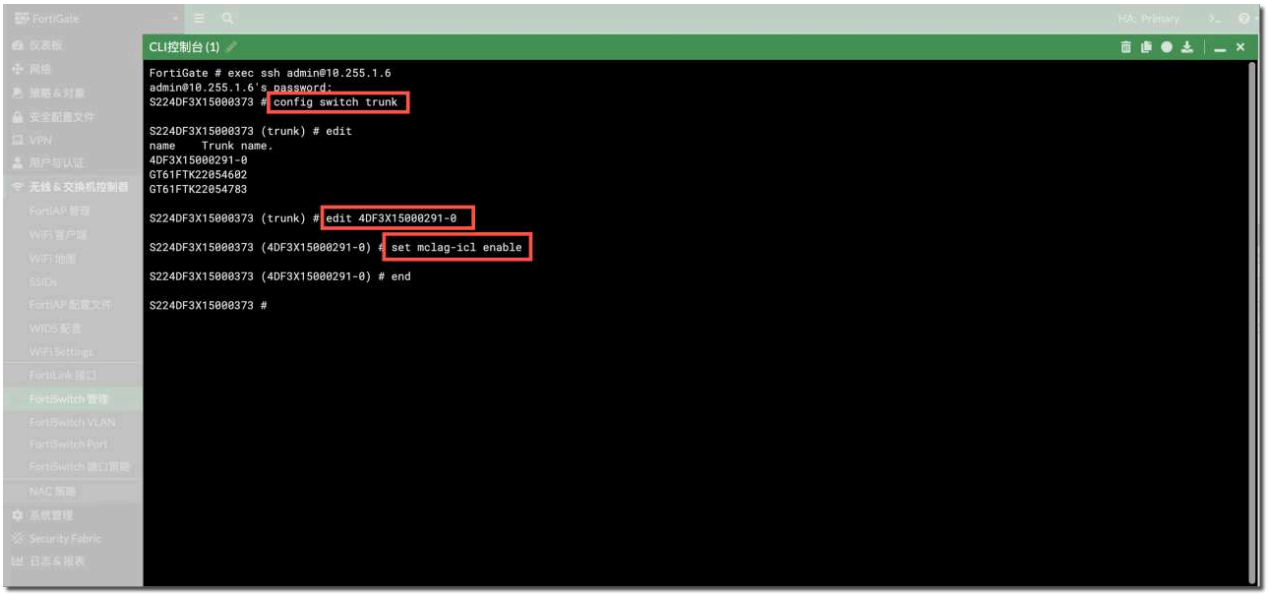


2. 配置二者的互联聚合接口为“set mclag-icl enable”（请注意此例中在GUI配置时一定要先配置CORE-FSW2，因为CORE-FSW2与FortiGate的FortiLink接口处于down的状态，如果先配置了CORE-FSW1，那么CORE-FSW2将无法通过GUI管理）。



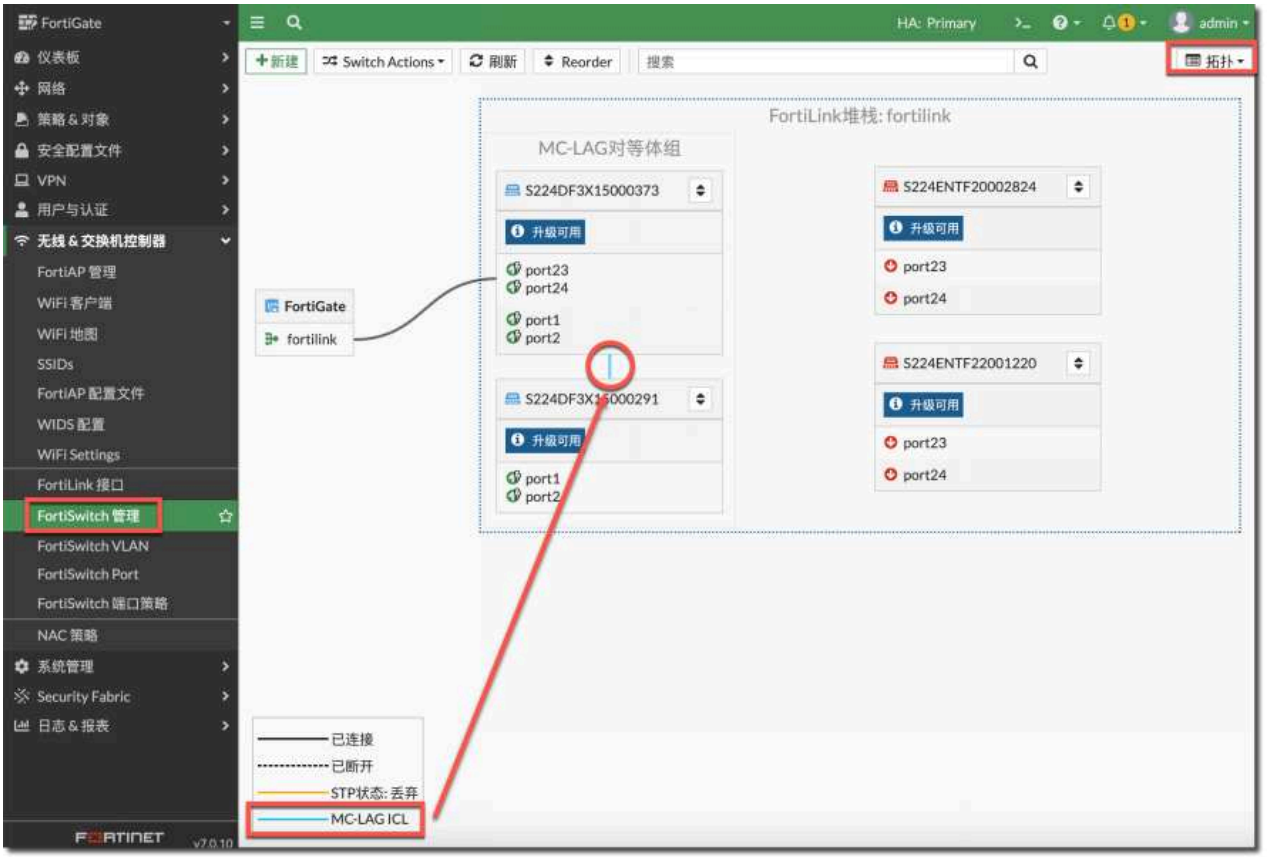

```
config switch trunk
    edit "4DF3X15000373-0"
        set mclag-icl enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



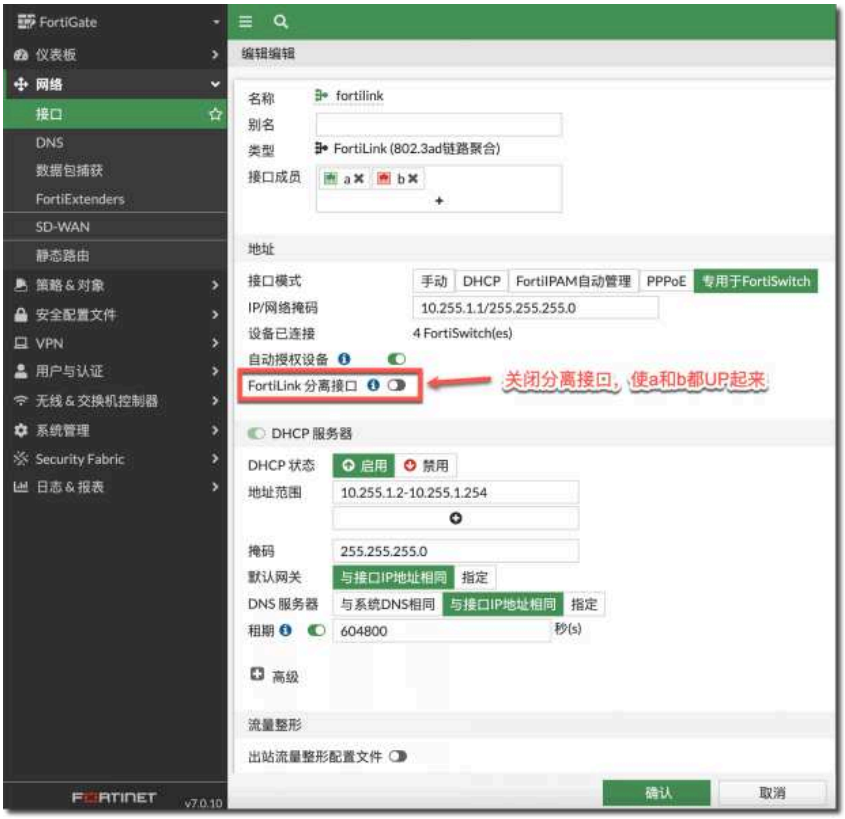

```
config switch trunk
    edit "4DF3X15000291-0"
        set mclag-icl enable
    next
end
```

3. 查看配置MCLAG后的交换机拓扑，可以看到两台交换机已经变为一个MC-LAG组。



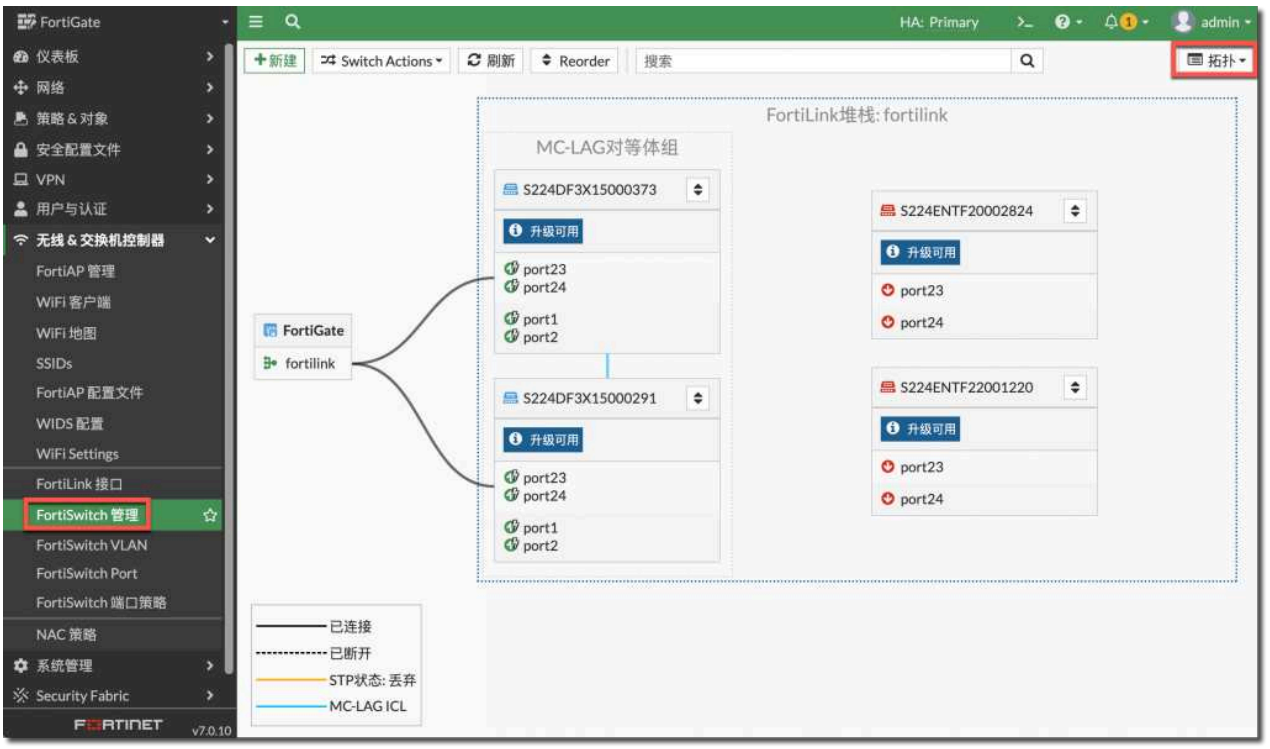
4. MC-LAG配置完成后，将FortiLink接口下的split interface设置为disable，让聚合接口（a和b）全部UP起来，充分利用聚合接口的资源，实现FortiGate与两台交换机（堆叠）的跨交换机聚合。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "fortilink"
        set fortilink-split-interface disable
    next
end
```

5. 等待CORE-FSW2重新在FortiGate上线后，查看Switch管理拓扑，FortiLink的两个成员接口均已UP。



6. 在FortiGate的CLI下查看FortiLink成员状态，可以看到与实际物理连线一致。

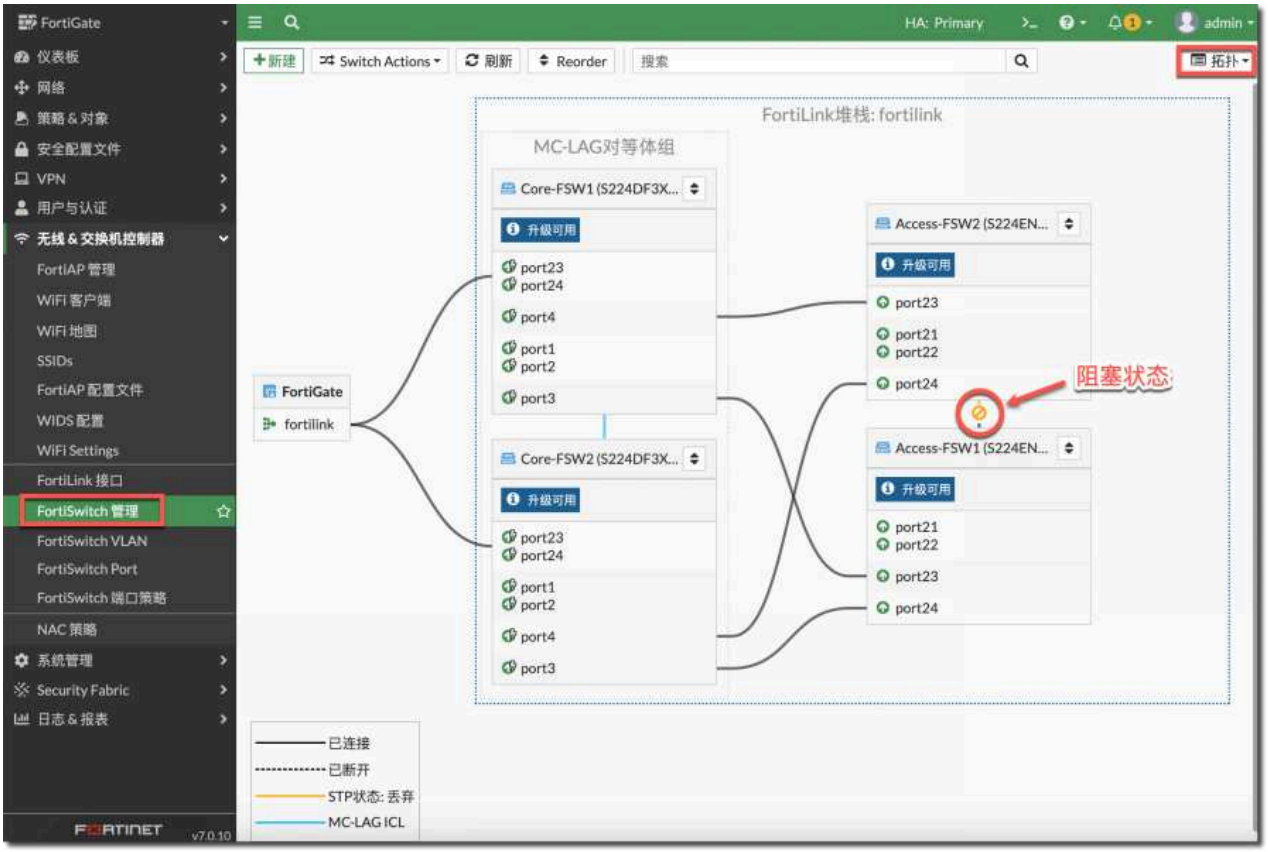
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

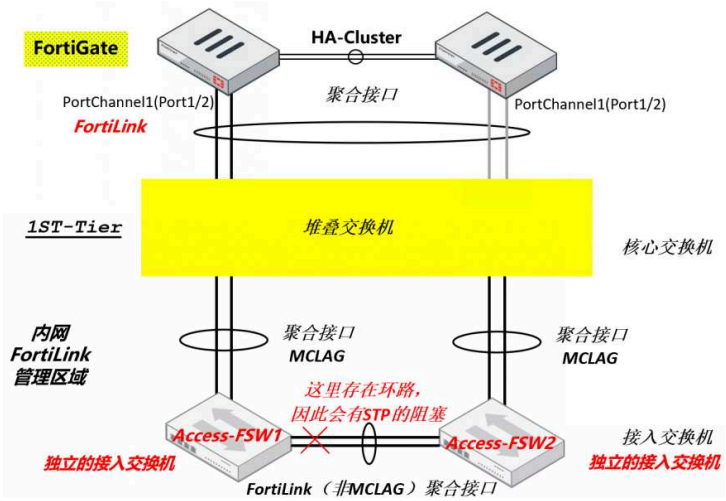
```
FortiGate # execute switch-controller get-physical-conn standard fortilink

This will display connectivity graph information for FortiLink from FortiGate's perspective
NOTE : If FortiSwitch is not authorized, no connectivity information will be shown
NOTE : If FortiSwitch is in idle state, no connectivity information will be shown
NOTE : If FortiSwitch ISL peer has inconsistent info, no connectivity information will be shown
        FortiLink interface : fortilink
FortiGate(s)
FGT61FTK22054783(a)  «————————————»  S224DF3X15000373(port23)
FGT61FTK22054602(a)  «————————————»  S224DF3X15000373(port24)
FGT61FTK22054783(b)  «————————————»  S224DF3X15000291(port23)
FGT61FTK22054602(b)  «————————————»  S224DF3X15000291(port24)

Tier 1
S224DF3X15000373(port23)  «————————————»  FGT61FTK22054783(a)
S224DF3X15000373(port24)  «————————————»  FGT61FTK22054602(a)
S224DF3X15000291(port23)  «————————————»  FGT61FTK22054783(b)
S224DF3X15000291(port24)  «————————————»  FGT61FTK22054602(b)

Tier 2+
S224DF3X15000373(port1/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port1/4DF3X15000373-0)
S224DF3X15000373(port2/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port2/4DF3X15000373-0)
```

连接接入交换机

1. 将接入层两台交换机的连线接入。在FortiGate上进入无线&交换机控制器→FortiSwitch管理页面，查看交换机被管理状态，修改视图为拓扑，可以看到4台交换机均已上线，两台交换机之间的接口为丢弃状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 查看两台接入交换机的STP状态，Access-FSW1的接口均为转发状态，Access-FSW2与Access-FSW1的互联的接口为阻塞状态。

```
FortiGate # exec ssh admin@10.255.1.3
admin@10.255.1.3's password:

Access-FSW1 # diagnose stp instance list 15

MST Instance Information, primary-Channel:
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC ac712e465448
  Regional Root  MAC 906cac30589c, Priority 20480, Path Cost 1, Root Port _FlInK1_MLAG0_
  TCN Events     Triggered 30 (0d 0h 21m 37s ago), Received 76 (0d 0h 21m 31s ago)
  Port               Speed   Cost       Priority   Role         State        Flags
  ________________   _____   ________   ________   ___________  __________   ________________

  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  _FlInK1_MLAG0_     2G      1          128        ROOT         FORWARDING   EN
  4ENTF20002824-0    2G      1          128        DESIGNATED   FORWARDING   EN
  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

```
FortiGate # exec ssh admin@10.255.1.4
admin@10.255.1.4's password:

Access-FSW2 # diagnose stp instance list 15

MST Instance Information, primary-Channel:
Instance ID 15
  Config         Priority 28672, VLANs 4094
                 Bridge MAC e023ff54e7e0
  Regional Root  MAC 906cac30589c, Priority 20480, Path Cost 1, Root Port _FlInK1_MLAG0_
  TCN Events     Triggered 32 (0d 2h 48m 38s ago), Received 99 (0d 2h 48m 33s ago)

  Port               Speed   Cost       Priority   Role         State        Flags
  _________________  ______  _________  _________  ___________  ___________  _________________
  internal           1G      20000      128        DESIGNATED   FORWARDING   ED
  _FlInK1_MLAG0_     2G      1          128        ROOT         FORWARDING   EN
  4ENTF22001220-0    2G      1          128        ALTERNATIVE  DISCARDING   EN

  Flags: EN(STP enable), ED(Edge), LP(Loop Protection Triggered)
  RG(Root Guard Triggered), BG(BPDU Guard Triggered), IC(PVST Port Inconsistent)
  MV(PVST Port Vlan Mismatch)
```

3. 为了防止出现环路导致FortiGate无法管理FortiSwitch，通过Console登录并配置两台接入交换机的互联聚合接口为“set mclag-icl enable”（或先将接入交换机之间互联口Down掉，通过FortiGate SSH到交换机配置）。

```
Access-FSW1:
config switch trunk
    edit "4ENTF20002824-0"
        set mclag-icl enable
    next
end

Access-FSW2:
config switch trunk
    edit "4ENTF22001220-0"
        set mclag-icl enable
    next
end
```

4. 在Core-FSW1和Core-FSW2上分别配置auto-isl-port-group，注意group的名字必须一致，端口成员为与接入交换机互联的接口，这样是为了让核心的堆叠交换机与接入的堆叠交换机相互跨交换机手工形成聚合。

```
Core-FSW1:
config switch auto-isl-port-group
    edit "mclag-tier2"    //手工配置auto-isl-port-group，Core-FSW1和Core-FSW2的名字需要一样，都为mclag-tier2
        set members "port3" "port4"
    next
end

Core-FSW2:
config switch auto-isl-port-group
    edit "mclag-tier2"    //手工配置auto-isl-port-group，Core-FSW1和Core-FSW2的名字需要一样，都为mclag-tier2
        set members "port3" "port4"
    next
end
```

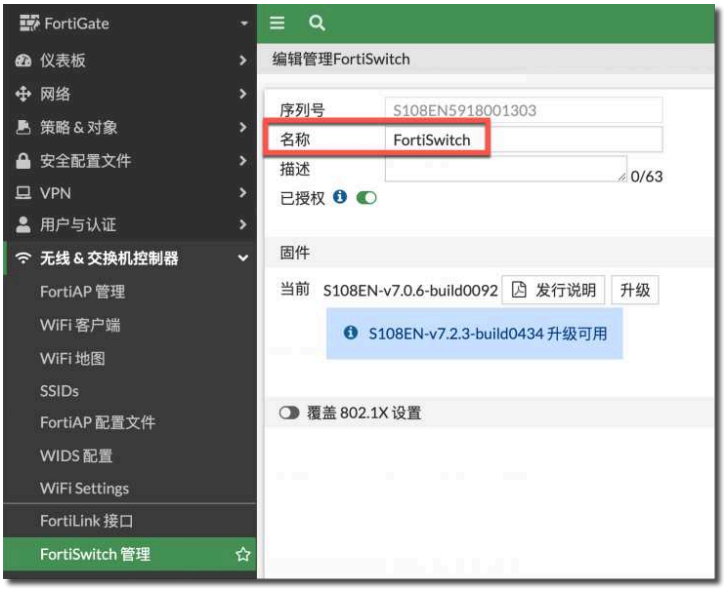
5. 配置完毕之后Core-FSW1和Core-FSW2后会自动生成聚合接口，无需手工配置，此配置可以理解为手工创建了跨堆叠交换机的聚合接口：“mclag-tier2”包括四个物理接口，CORE-FSW1上的两个物理接口Port3和Port4以及 CORE-FSW2上的两个物理接口Port3和Port4，一共四个物理接口，共同属于聚合接口：“mclag-tier2”。

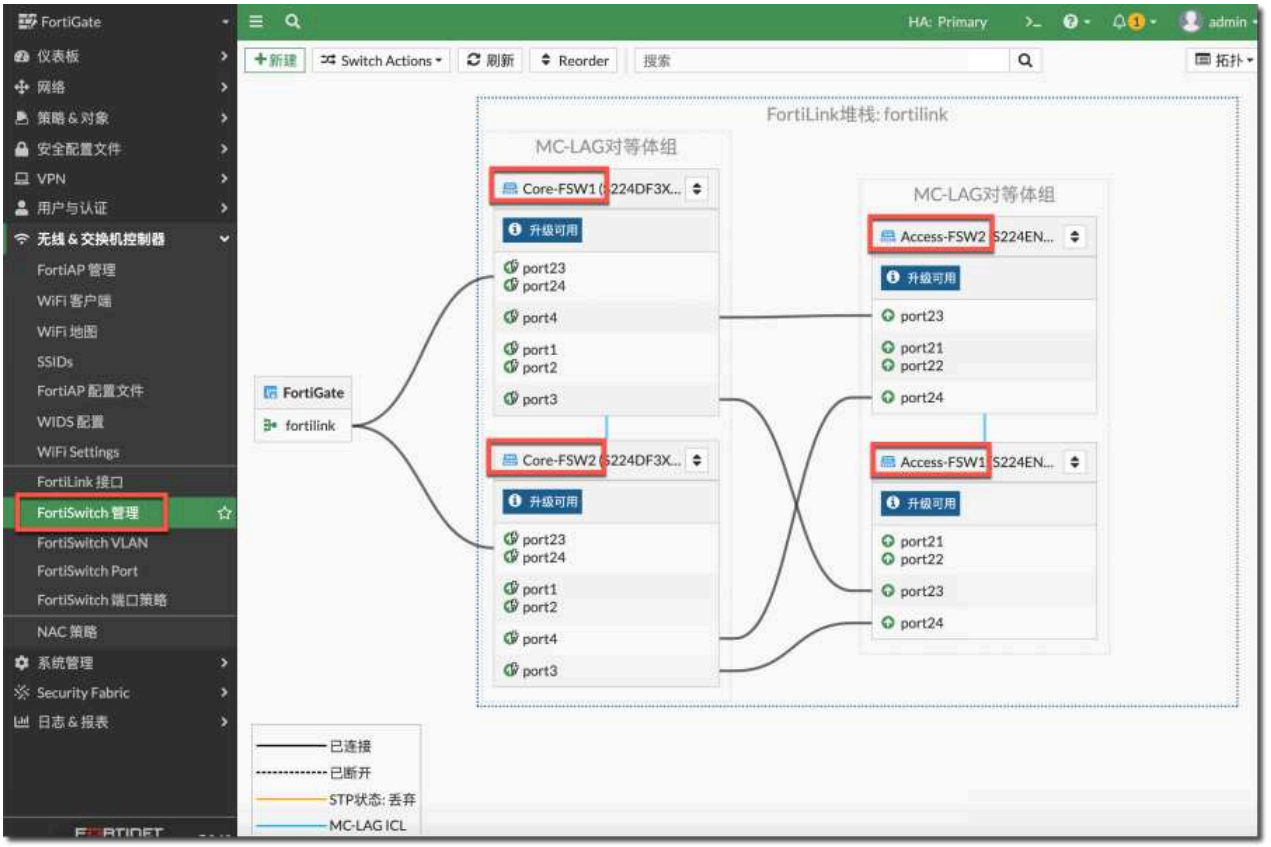
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Core-FSW1 # show switch trunk
config switch trunk
 ...
    edit "mclag-tier2"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port4" "port3"    //对于堆叠交换机而言，名字一样的聚合接口即为跨交换机聚合的聚合接口，这是"mclag-tier2"聚合接口在CORE-FSW1上的两个物理接口Port3和Port4
    next
end

Core-FSW2 # show switch trunk
config switch trunk
 ...
    edit "mclag-tier2"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port4" "port3"    //对于堆叠交换机而言，名字一样的聚合接口即为跨交换机聚合的聚合接口，这是"mclag-tier2"聚合接口在CORE-FSW1上的两个物理接口Port3和Port4
    next
end
```

6. 接好线之后，FortiSwitch和FortiGate之间会自动在后台进行FortiLink、CAPWAP、MSTP、聚合接口的协商加入等操作，等FortiLink的管理结束之后，在FortiGate上会看到一个网站的FortiSwitch拓扑图，和我们规划的拓扑图应该是一致的，可以仔细核对接线是否正确。
7. 交换机加入到FortiGate的FortiLink，会先清除配置再重启，然后从standalone的状态进入到“Fortilink remote control”的状态，后续所有的配置都通过FortiGate下发即可。
8. 编辑交换机，可以修改交换机名字以及升级版本，如果交换机很多的话，规划好的命名可以有效的迅速找到交换机的位置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





9. FortiSwitch之间接多根线进行FortiLink互联，会默认自动聚合。其实接一根网线也是聚合的，只是聚合组里面只有一个接口而已，因此多根网线直连，这些直连的线都会自动加入到一个聚合接口里面（建议MC-LAG环境尽量使用两条或以上的连线）。

```
FortiGate # exec ssh admin@10.255.1.6
admin@10.255.1.6's password:

Core-FSW1 # show switch trunk

config switch trunk
    edit "4DF3X15000291-0"
        set mode lacp-active
        set auto-isl 1
        set mclag-icl enable
        set members "port1" "port2"
    next
    edit "GT61FTK22054602"
        set mode lacp-active
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

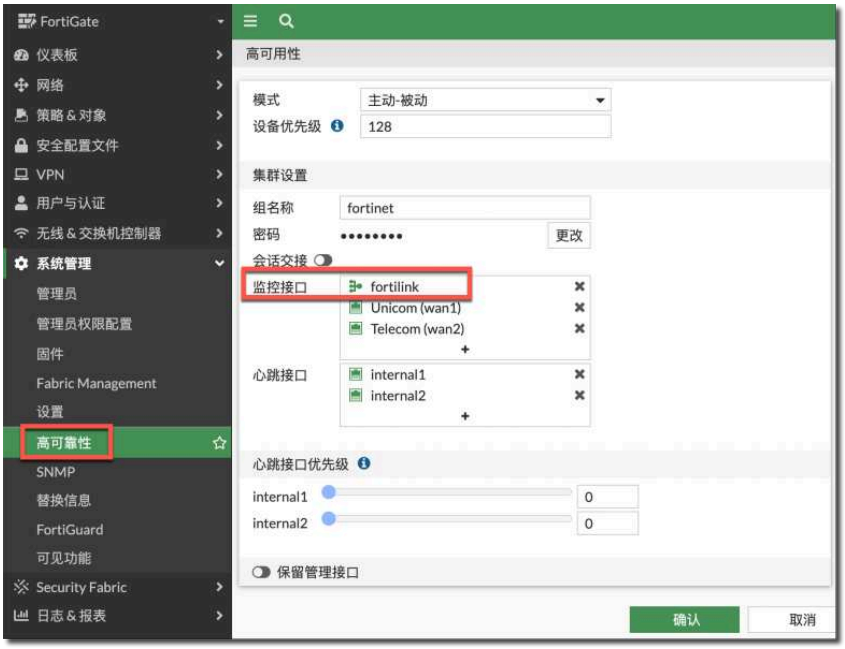
```
        set auto-isl 1
        set fortilink 1
        set mclag enable
        set members "port24"
    next
    edit "GT61FTK22054783"
        set mode lacp-active
        set auto-isl 1
        set fortilink 1
        set mclag enable
        set members "port23"
    next
    edit "mclag-tier2"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port4" "port3"
    next
end
```

10. 再次查看FortiGate的FortiLink成员，可以看到两台接入交换机已上线，且连线与拓扑一致。

```
FortiGate # execute switch-controller get-physical-conn standard fortilink

This will display connectivity graph information for FortiLink from FortiGate's perspective
        FortiLink interface : fortilink
FortiGate(s)
FGT61FTK22054783(a)  «————————————»  S224DF3X15000373(port23)
FGT61FTK22054602(a)  «————————————»  S224DF3X15000373(port24)
FGT61FTK22054783(b)  «————————————»  S224DF3X15000291(port23)
FGT61FTK22054602(b)  «————————————»  S224DF3X15000291(port24)
Tier 1
S224DF3X15000373(port23)  «————————————»  FGT61FTK22054783(a)
S224DF3X15000373(port24)  «————————————»  FGT61FTK22054602(a)
S224DF3X15000291(port23)  «————————————»  FGT61FTK22054783(b)
S224DF3X15000291(port24)  «————————————»  FGT61FTK22054602(b)
Tier 2+
S224ENTF20002824(port23/_FlInK1_MLAG0_)  «————————————»  S224DF3X15000373(port4/mclag-tier2)
S224ENTF20002824(port24/_FlInK1_MLAG0_)  «————————————»  S224DF3X15000291(port4/mclag-tier2)
S224ENTF22001220(port21/4ENTF20002824-0)  «————————————»  S224ENTF20002824(port21/4ENTF22001220-0)
S224ENTF22001220(port22/4ENTF20002824-0)  «————————————»  S224ENTF20002824(port22/4ENTF22001220-0)
S224ENTF22001220(port23/_FlInK1_MLAG0_)  «————————————»  S224DF3X15000373(port3/mclag-tier2)
S224ENTF22001220(port24/_FlInK1_MLAG0_)  «————————————»  S224DF3X15000291(port3/mclag-tier2)
S224DF3X15000373(port1/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port1/4DF3X15000373-0)
S224DF3X15000373(port2/4DF3X15000291-0)  «————————————»  S224DF3X15000291(port2/4DF3X15000373-0)
```

11. 最后不要忘记，在FortiLink的聚合接口和FortiLink管理配置完毕，记得把这个FortiLink聚合接口加入到HA的监控接口列表中，这样当主核心交换机挂了（比如断电）之后，业务才可以平稳切换到备防火墙上。

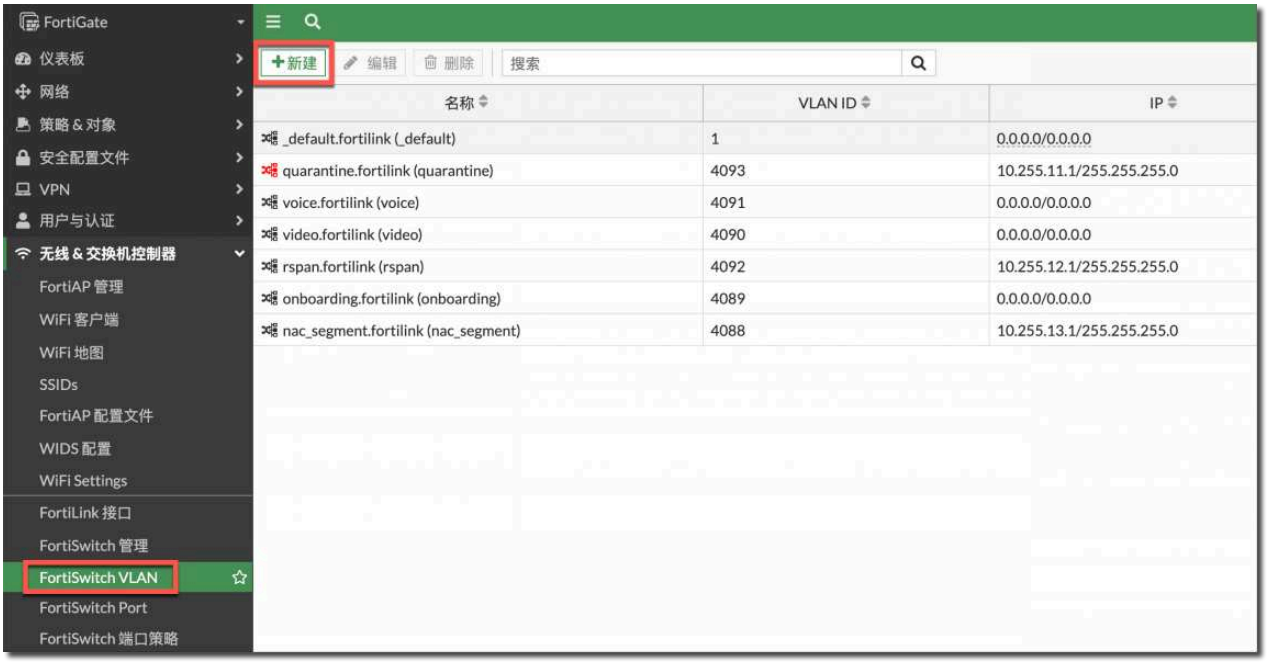
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



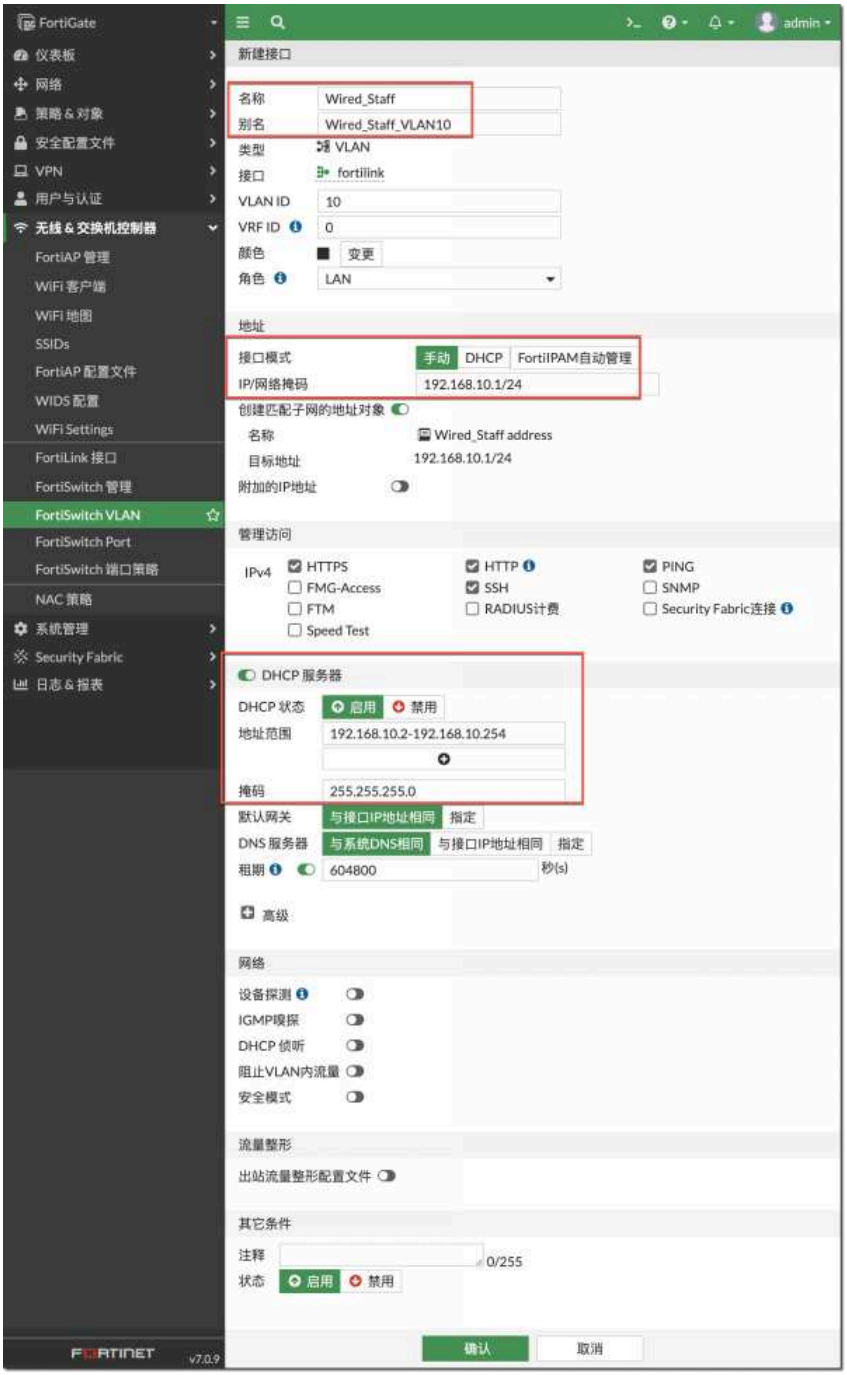
创建VLAN

1. FortiGate通过FortiLink + Capwap协议统一的接管FortiSwitch和FortiAP，为有线和无线统一进行管理和业务处理。
2. 进入FortiGate的无线&交换机控制器→FortiSwitch VLAN页面，新建有线网络VLAN 10、员工无线网络VLAN 20、访客无线网络VLAN 30、管理FortiAP VLAN 99。注意管理FortiAP的VLAN接口要开启Security Fabric，包含CAPWAP。

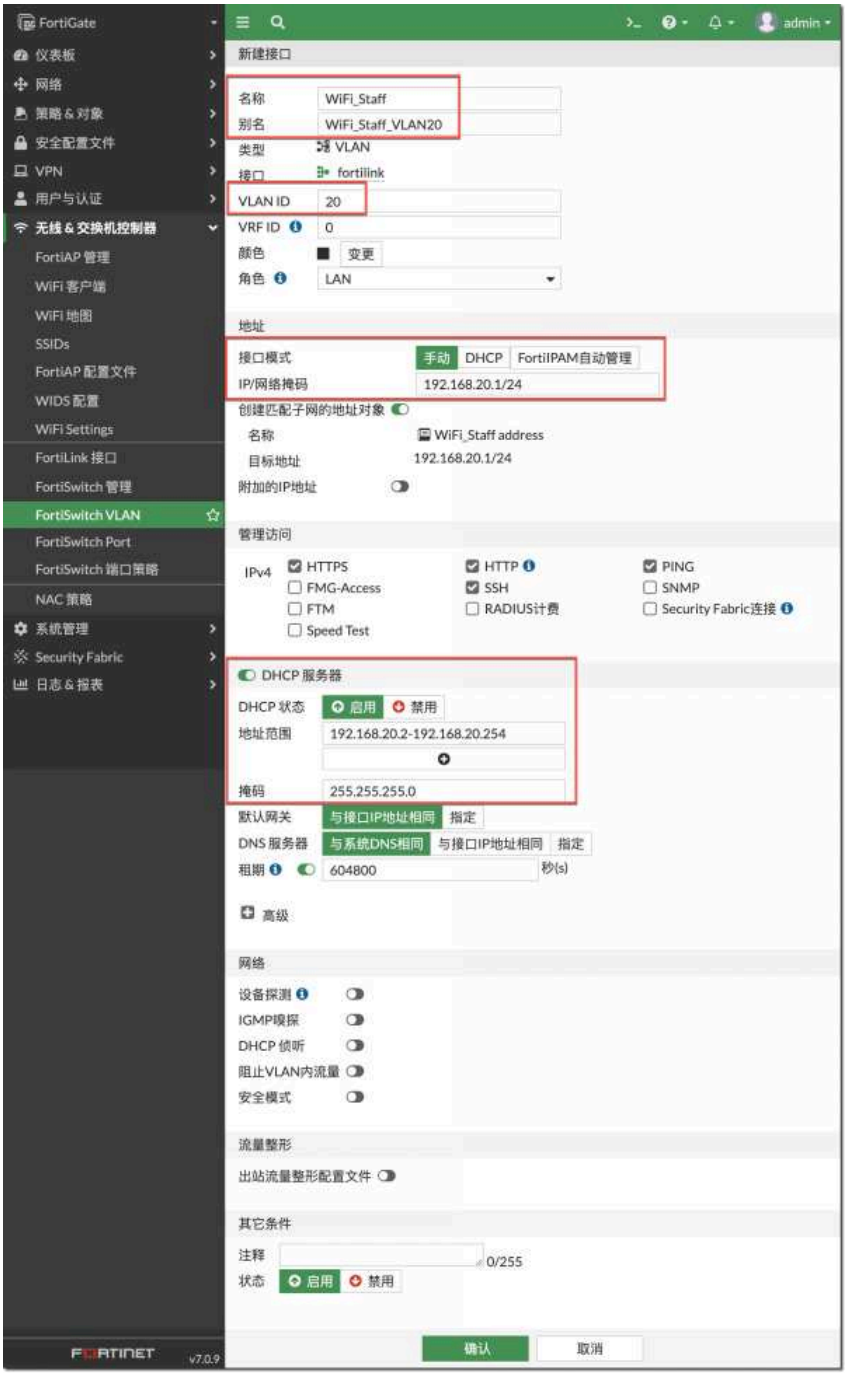
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



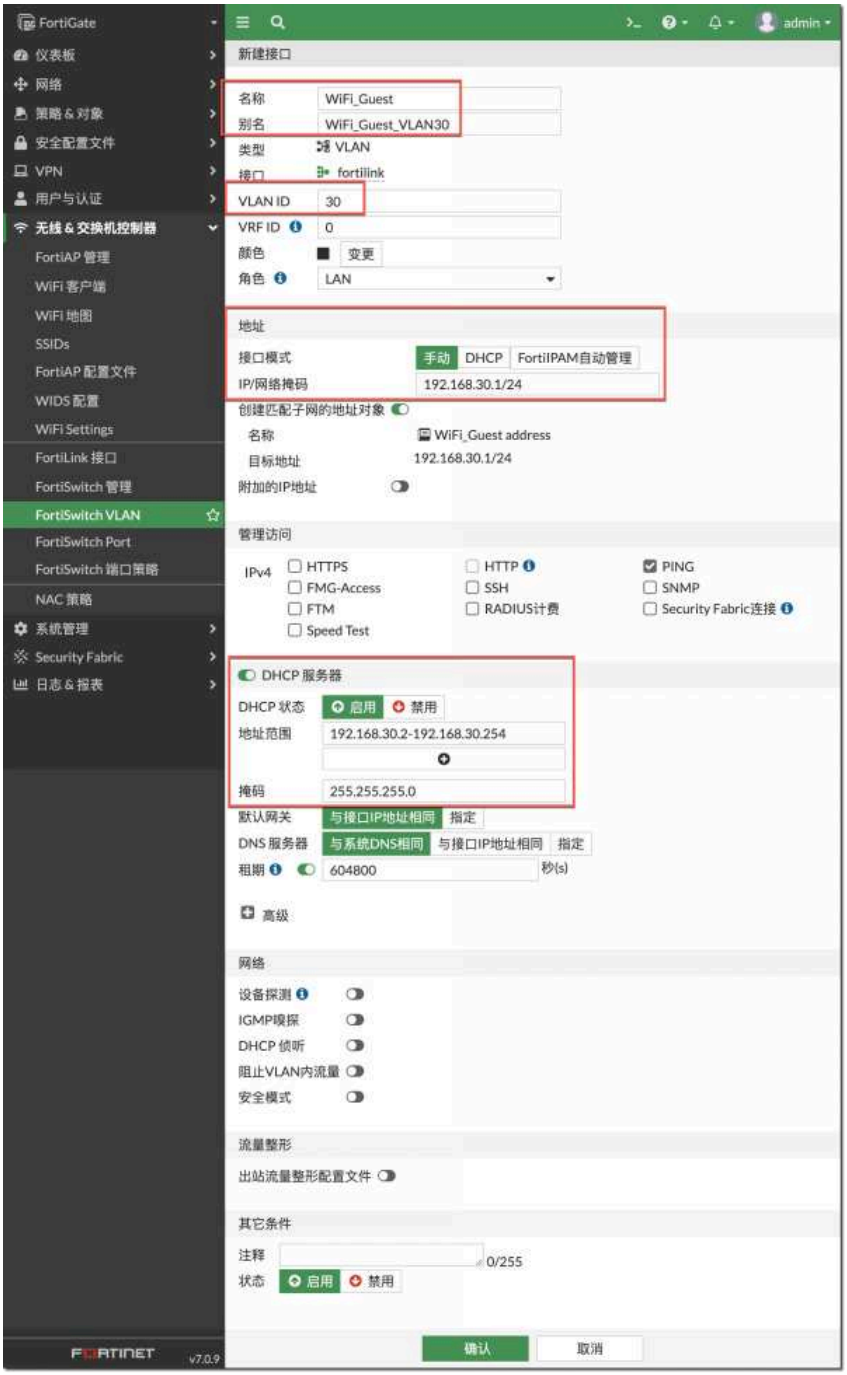
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



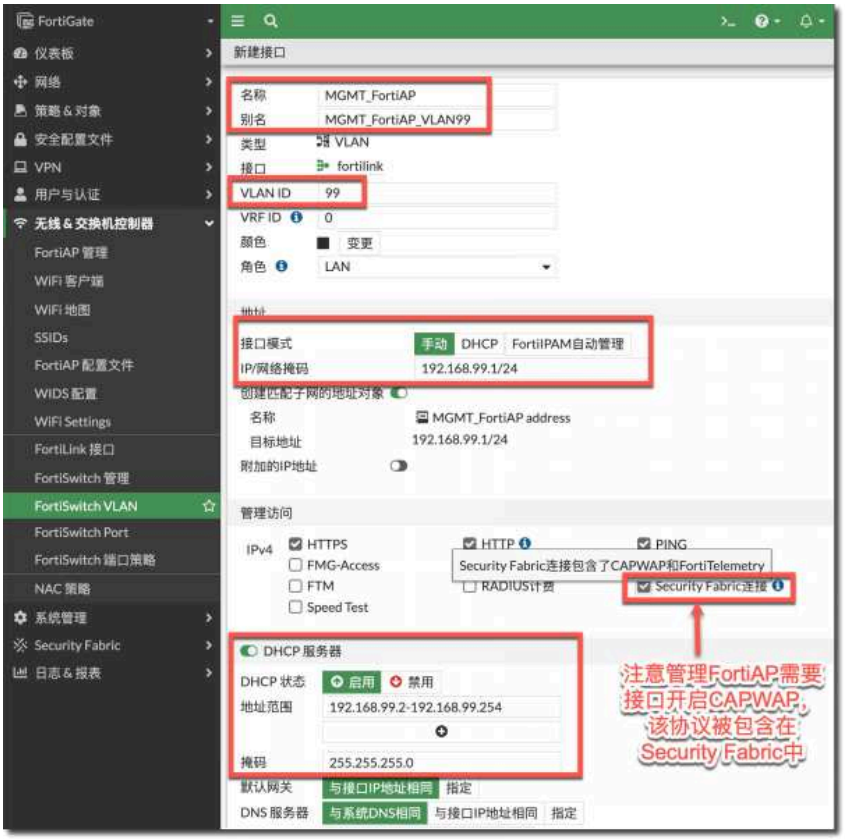
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



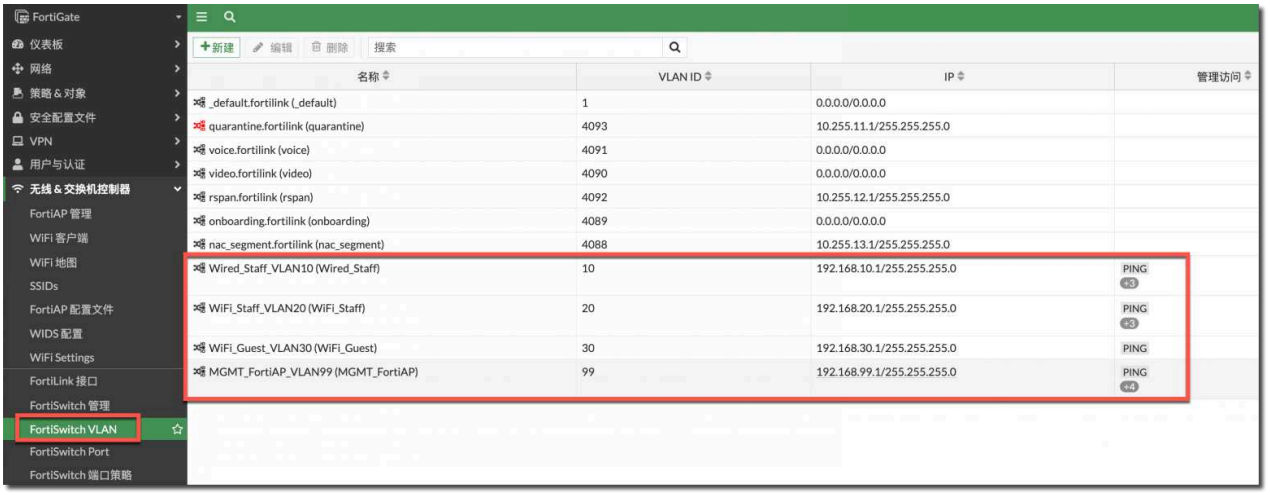
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

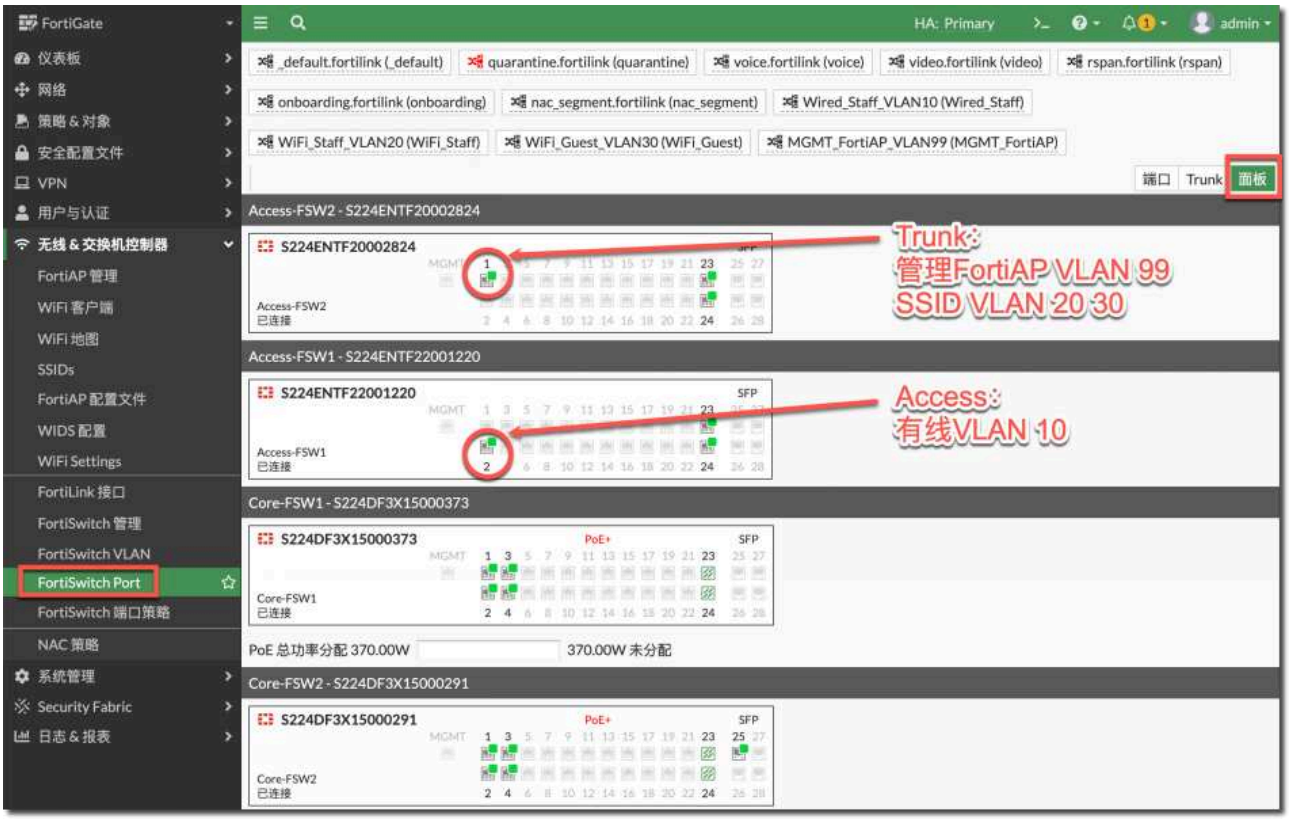


3. VLAN创建完成。

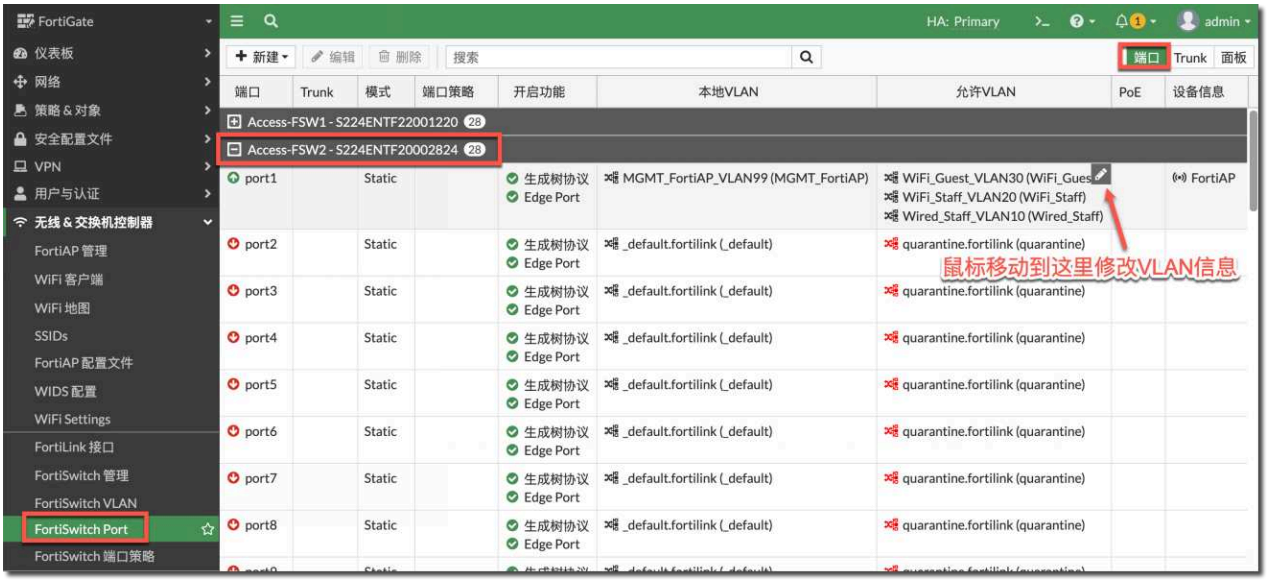


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

分配VLAN

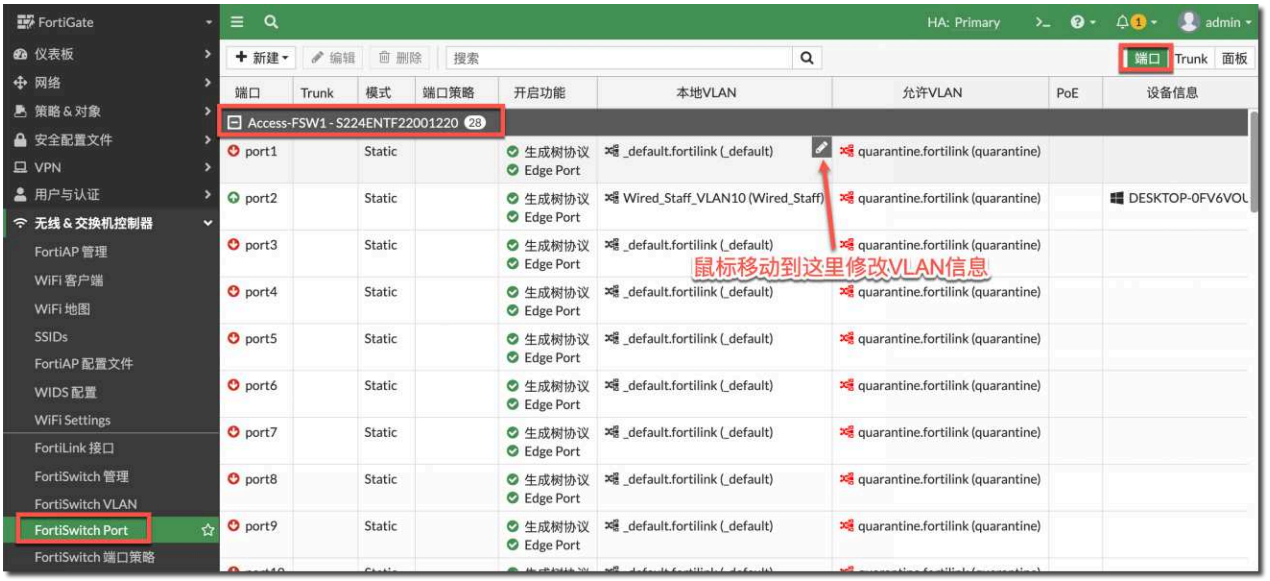


1. Access-FSW2交换机的port1接FortiAP，配置为Trunk模式，允许 VLAN20和VLAN30，VLAN20用于WIFI-STAFF的SSID用户，VLAN30用于WIFI-GUEST的SSID用户。另外本地VLAN设置为VLAN 99，用于FortiAP的管理（FortiAP的管理相当于使用不打vlan-tag的VLAN 99，本地VLAN默认是VLAN 1，因此只需要将本地VLAN设置为VLAN 99即可）。



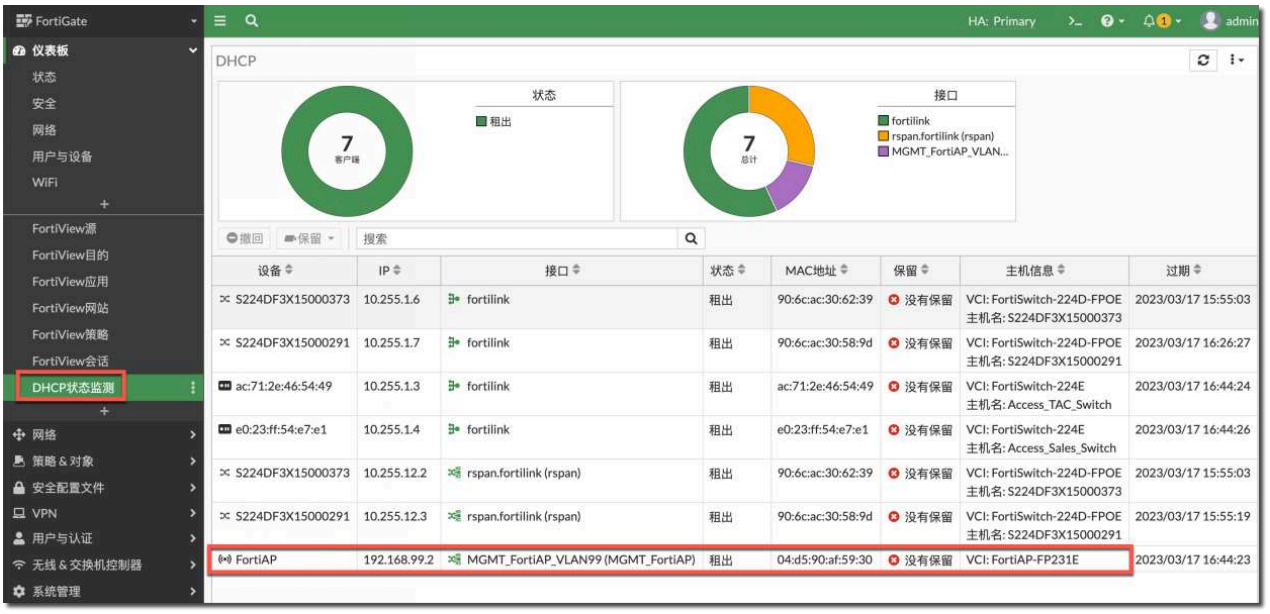
2. Access-FSW1交换机的Port2接具体的物理PC，因此只需要将Port2设置为access口，分配VLAN 10即可，用FortiSwitch的概念来说就是将本地VLAN设置为VLAN 10，本地VLAN不打vlan-tag，相当于就是设置接口为access vlan 10。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



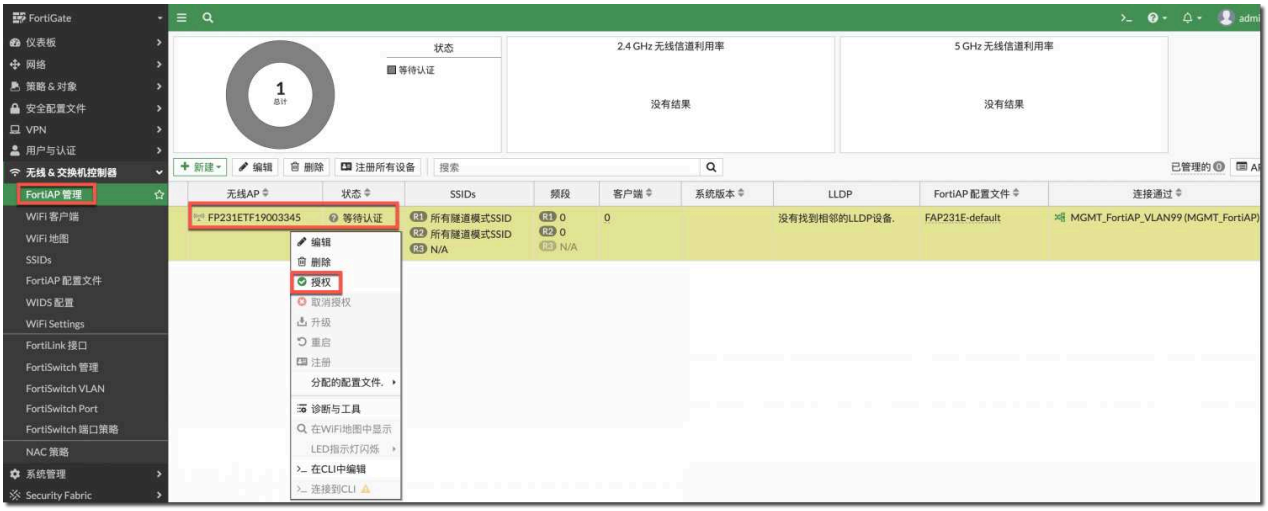
无线配置

1. FortiAP连接后，会通过VLAN 99的DHCP获取到192.168.99.0/24网段的IP地址。

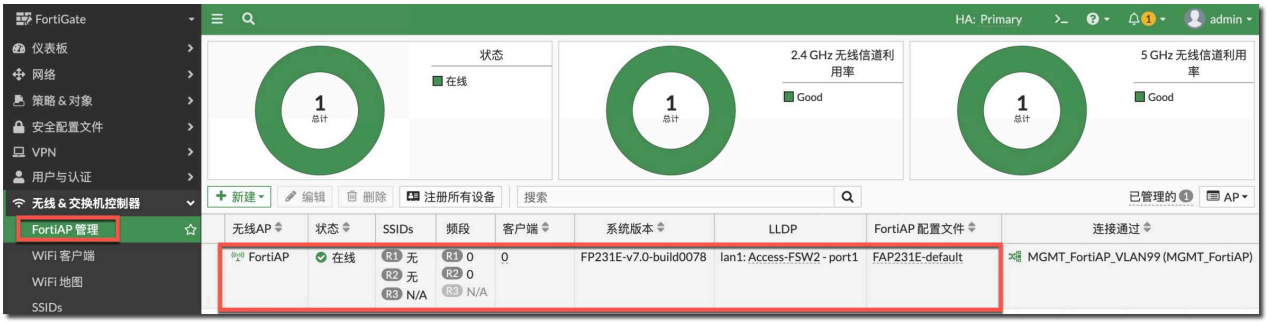


2. 在之前的配置中，VLAN 99的接口开启了CAPWAP协议（包含在Security Fabric中），激活了FortiGate的无线管理功能，这时候FortiAP会自动找到FGT进行注册。因此在FortiAP管理的地方可以看到这个FortiAP的信息（如果没有看到检查配置，并将FortiAP恢复出厂，让FortiAP重新获取IP地址并发起注册）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 右键点击上图中等待认证的FortiAP，点击授权按钮，等待几分钟，FortiAP成功上线。



4. 编辑FortiAP设置，配置FortiAP的名称，或进行升级操作。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 进入无线&交换机控制器→SSIDs页面，点击新建按钮。

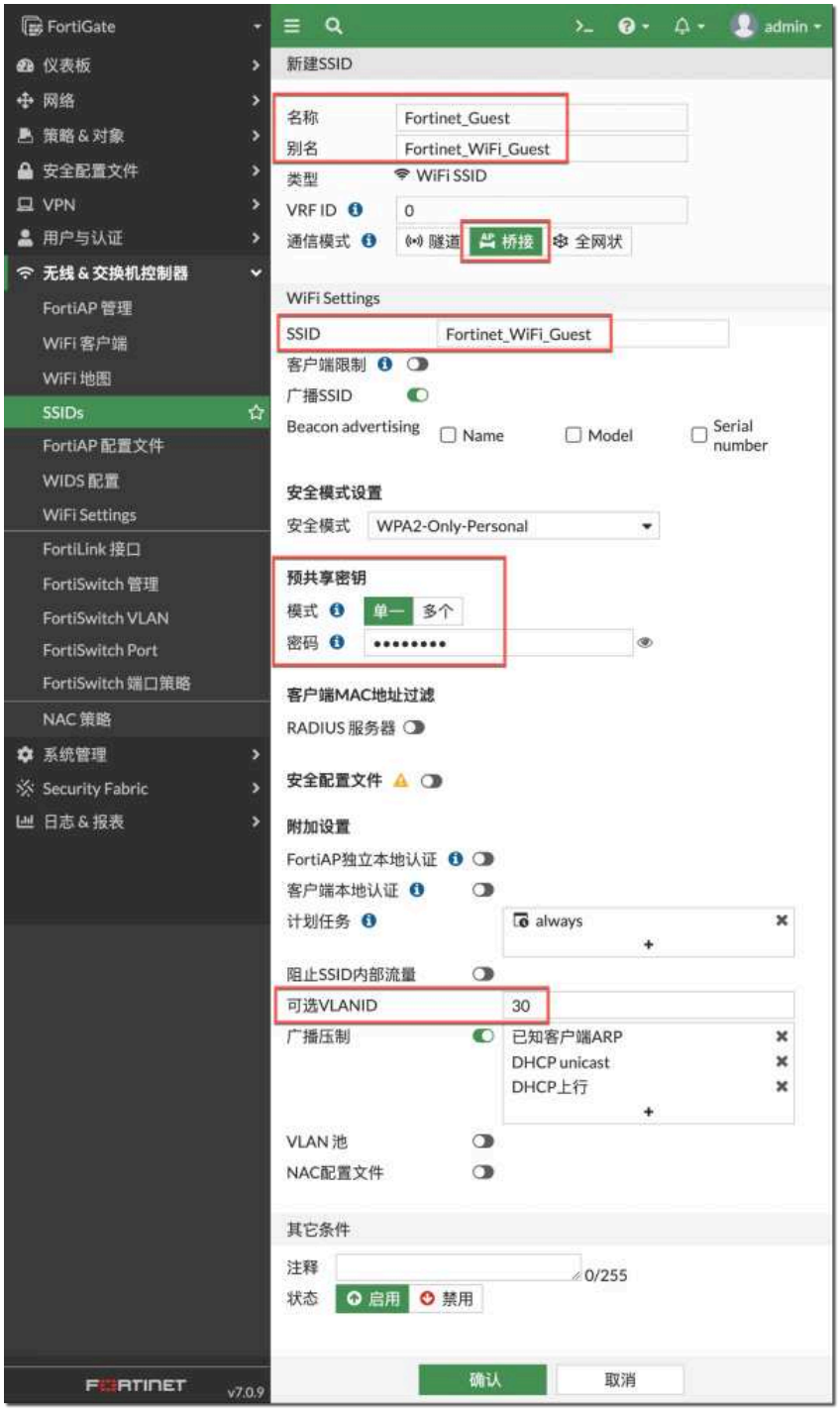


6. 新建SSID：Fortinet_WiFi_Staff VLAN 20用于员工WIFI使用，Fortinet_WiFi_Guest VLAN 30用于访客WiFi使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





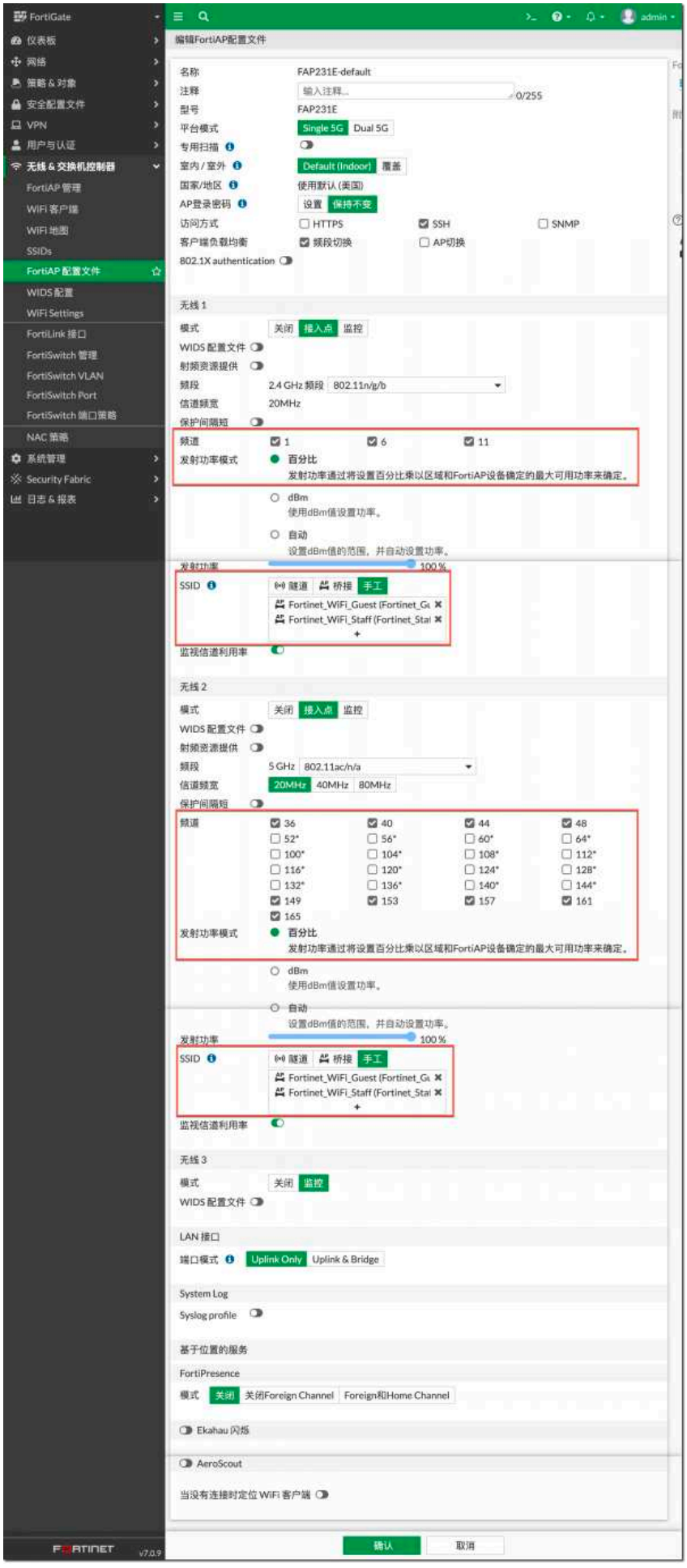
7. 将SSID关联到FortiAP上，然后让FortiAP发布无线SSID信号，这样用户就可以通过SSID连接到无线了。进入FortiAP配置文件页面，编辑FortiAP关联的配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 桥模式的SSID需要在FortiAP配置文件里面手工指定一下，另外下图标示出的配置为推荐配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

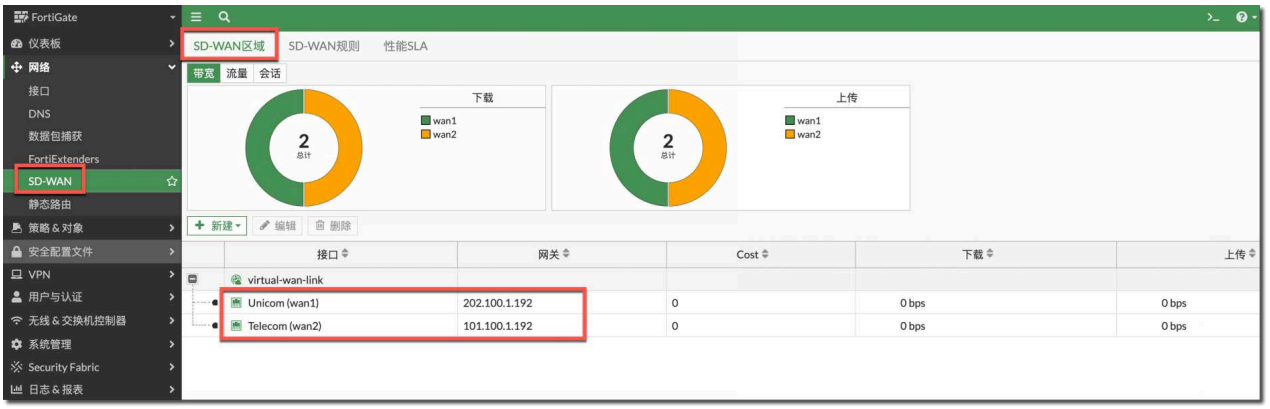


9. FortiAP会自动关联到这个FortiAP配置文件里面的内容，发起SSID的信号。



SD-WAN配置

1. 将wan1和wan2加入SD-WAN接口，并配置各自的网关。

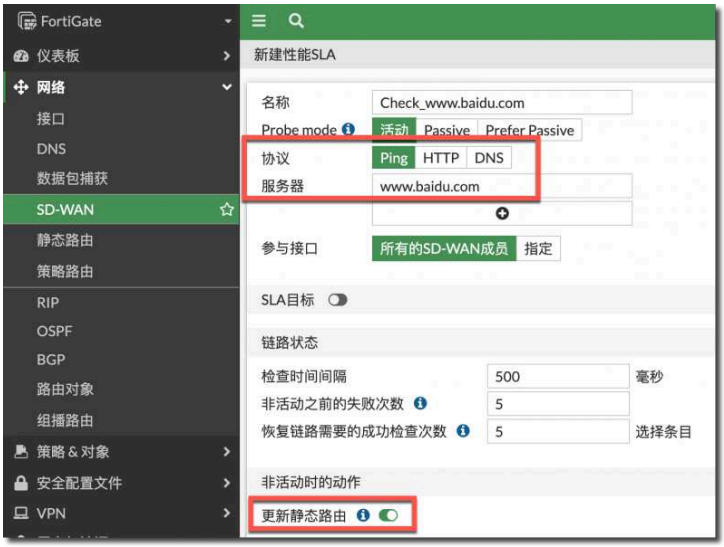


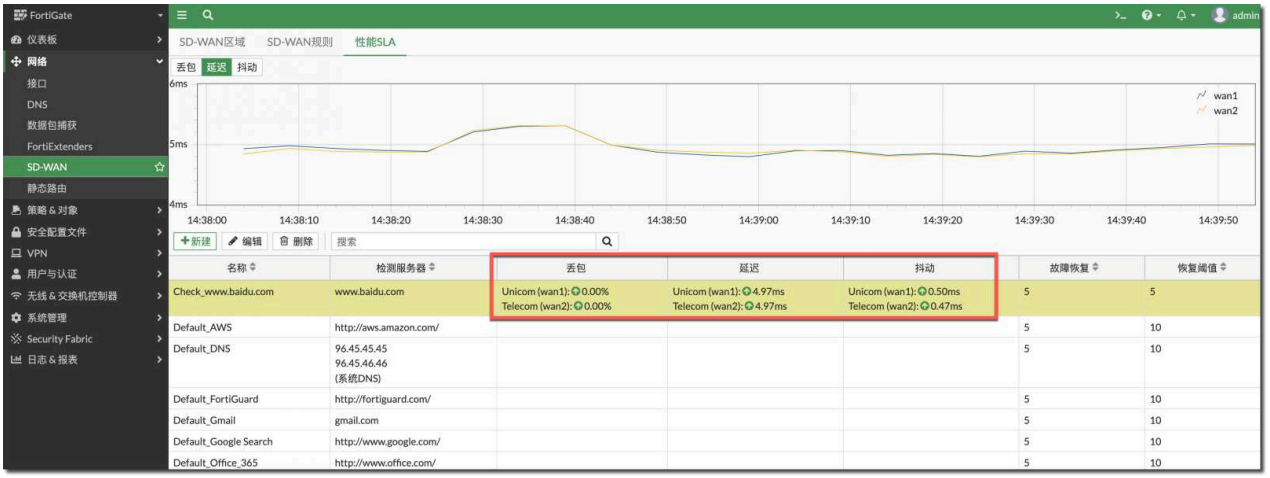
2. 添加SD-WAN的默认路由。



3. 配置SD-WAN的SLA，以便wan1和wan2相互备份和切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. SD-WAN规则可根据需求配置，这里保持默认的按照源IP负载均衡。



安全策略配置

1. 需求与规划：

   - 员工的有线与无线都需要访问互联网
   - 访客的无线仅仅可以访问互联网
   - 员工的有线和无线需要互访

2. 建议将防火墙的接口划分区域，以区域的方式配置策略，有时候可以做到简化配置的目的，甚至未来替换设备的时候，策略的备份和还原也会更加简单一些。规划区域两个区域：

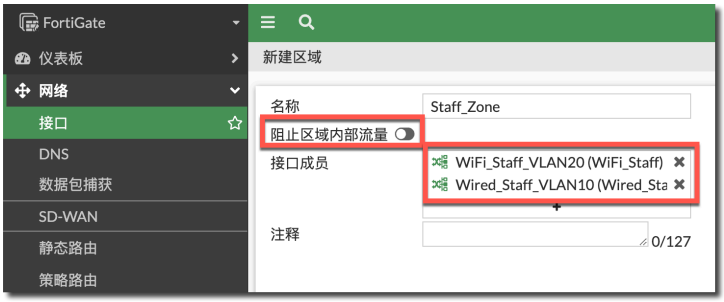
   - 员工网络区域：包括员工的有线VLAN 10和员工的无线VLAN 20 （区域之间的隔离关闭，这样VLAN 10和VLAN 20之间的数据可通）
   - 访问网络区域：包括访问的无线VLAN 30

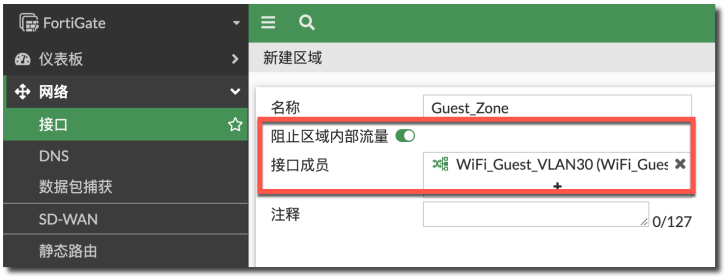
3. 进入网络→接口页面，新建所属区域。

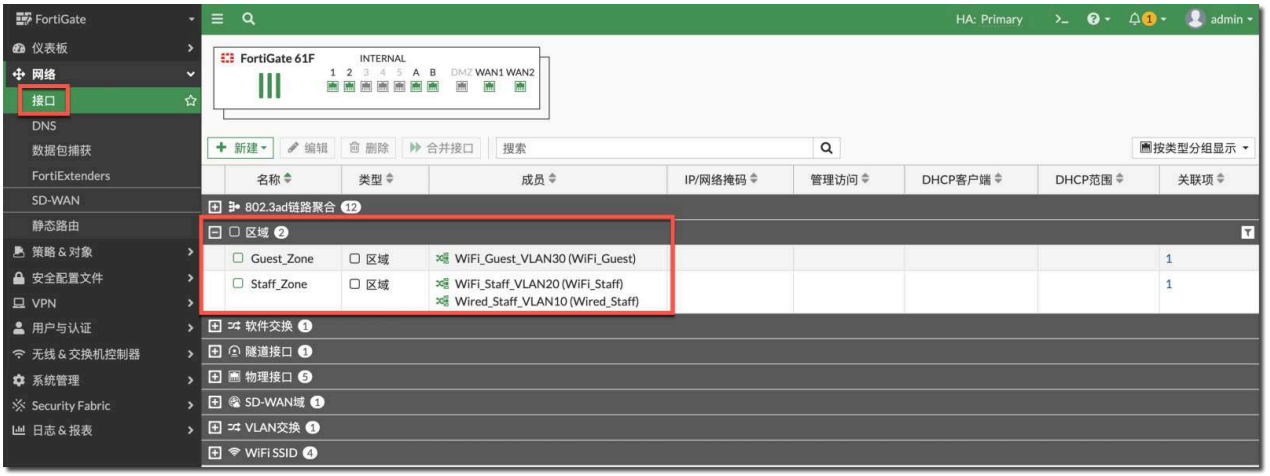
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 分别创建Staff_Zone（包含VLAN 10和VLAN20）和Guest_Zone（包含VLAN30）。







5. 如此只需要配置两条策略，就可以实现我们规划的需求，新建Staff-Zone到SD-WAN与Guest-Zone到SD-WAN的安全策略。

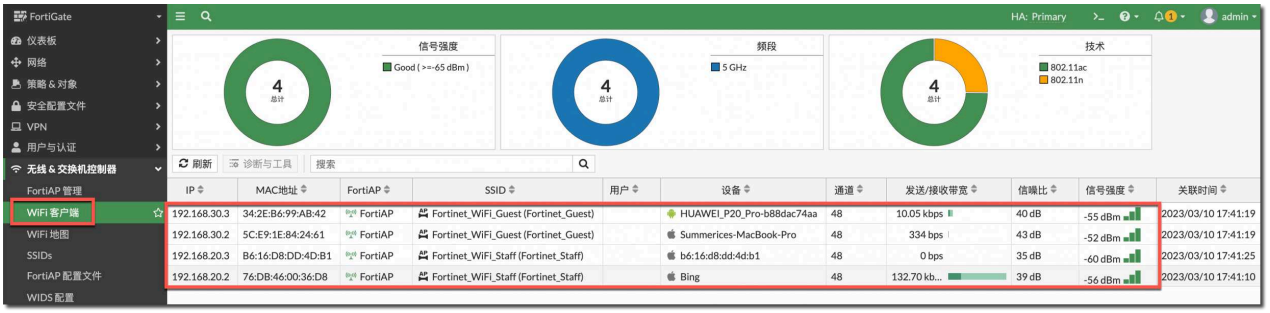


结果验证

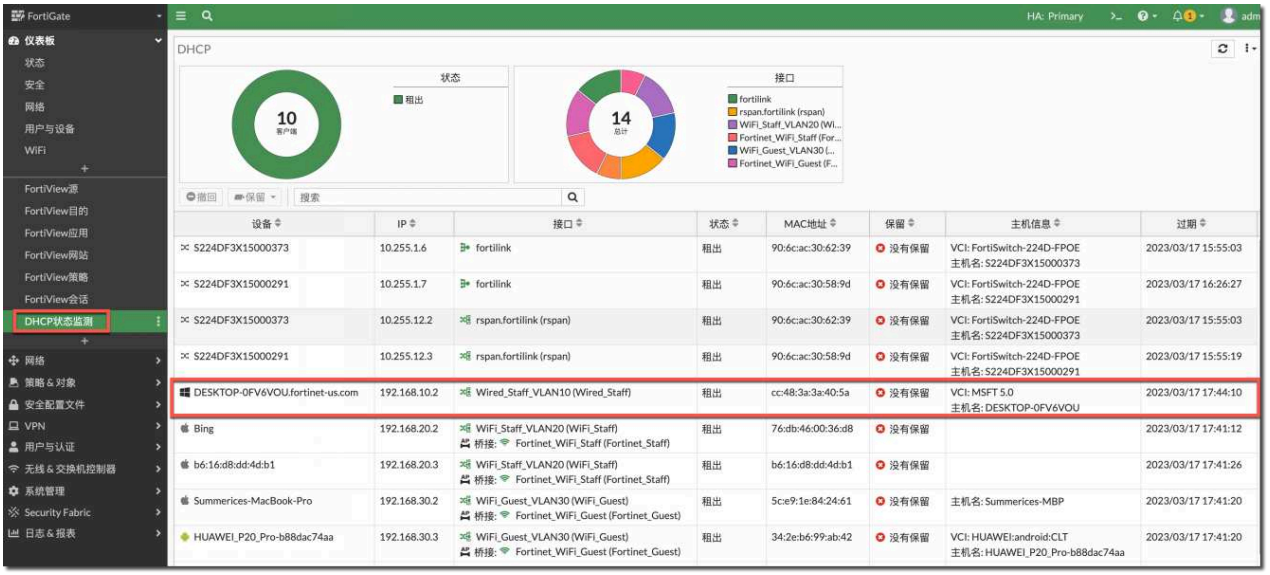
客户端访问

1. 进入无线&交换机控制器→WiFi客户端，查看在线的无线客户端。可以看到WiFi_Staff和WiFi_Guest各有一个终端在线。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在DHCP状态检测中查看所有的客户端信息，可以看到有线网络的PC也正常上线。

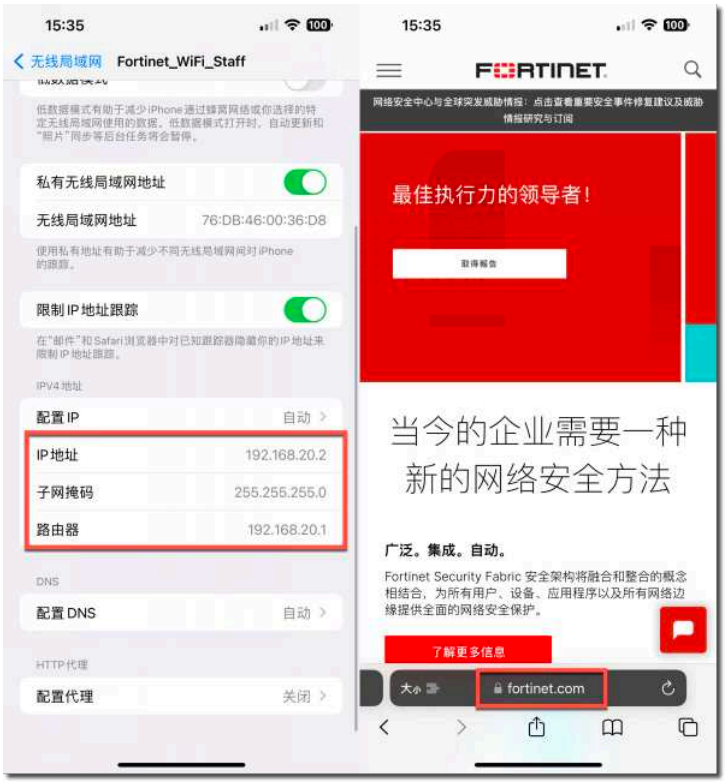


3. 有线网络（VLAN 10）用户访问互联网。

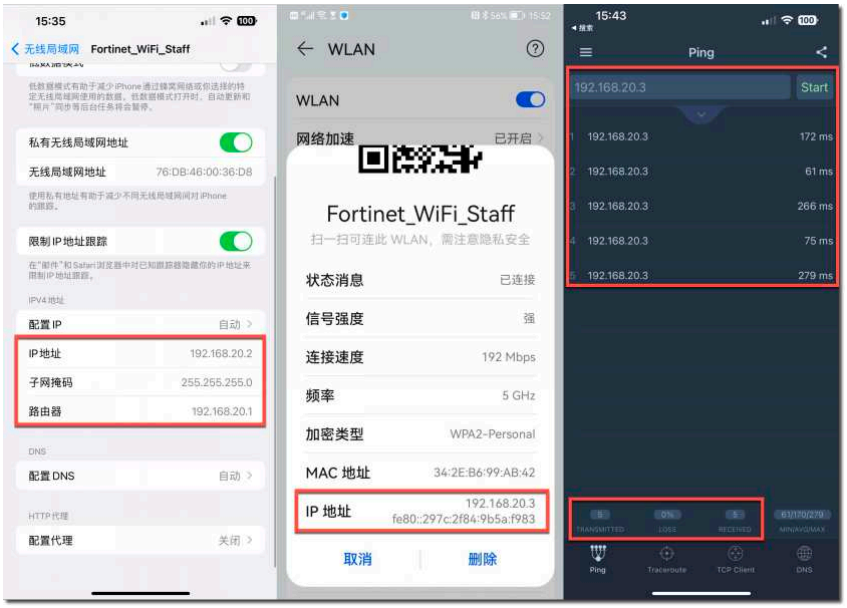


4. 无线网络用户访问互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

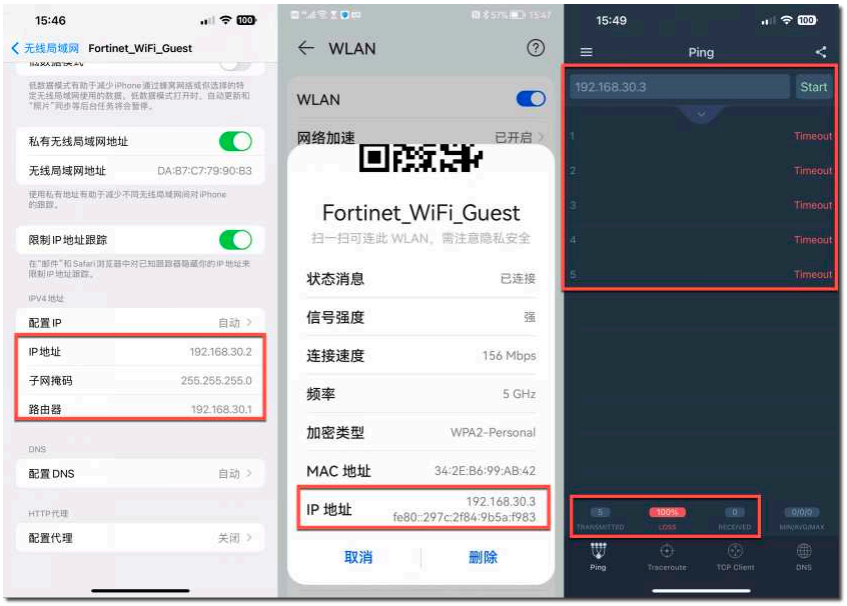


5. 使用VLAN 20下的客户端访问VLAN 20下的另一个客户端（Staff区域）。



6. 使用VLAN 30下的客户端访问VLAN 30下的另一个客户端（Guest区域），可以看到由于该区域配置了禁止相互访问，所以VLAN 30下的客户端是无法互相访问的。

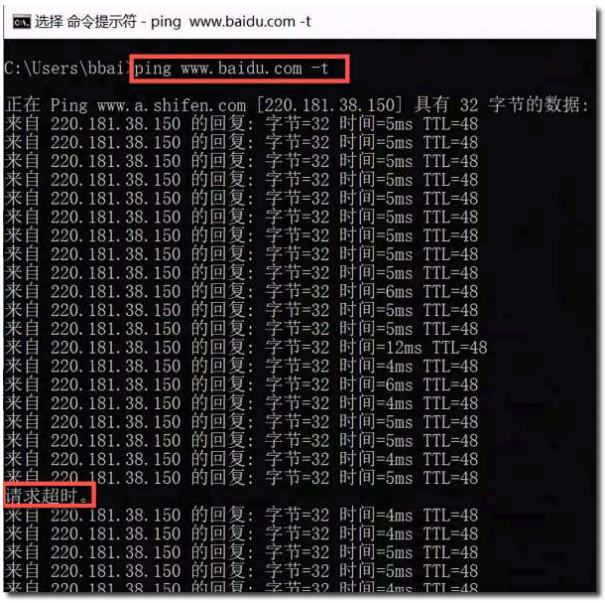
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiLink切换测试

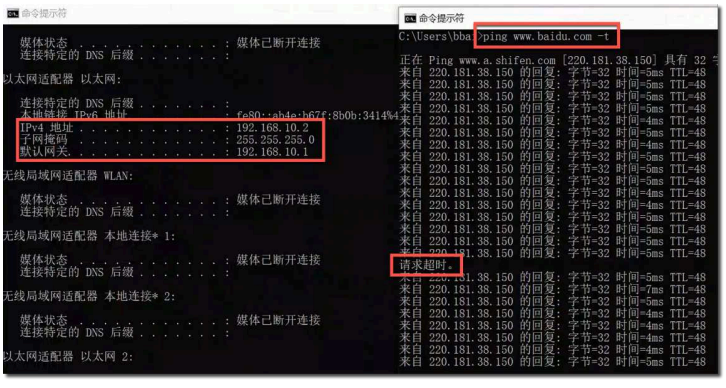
1. 在我们的测试场景下FortiLink聚合接口的a和b是同时UP起来的，如果a或b DOWN（不能同时DOWN），是否有影响业务呢?

2. 经过测试，DOWN a或b接口，客户端丢包1个或者不丢包。



HA切换测试

重启当前主防火墙查看内网PC丢包情况，HA切换丢包1个。



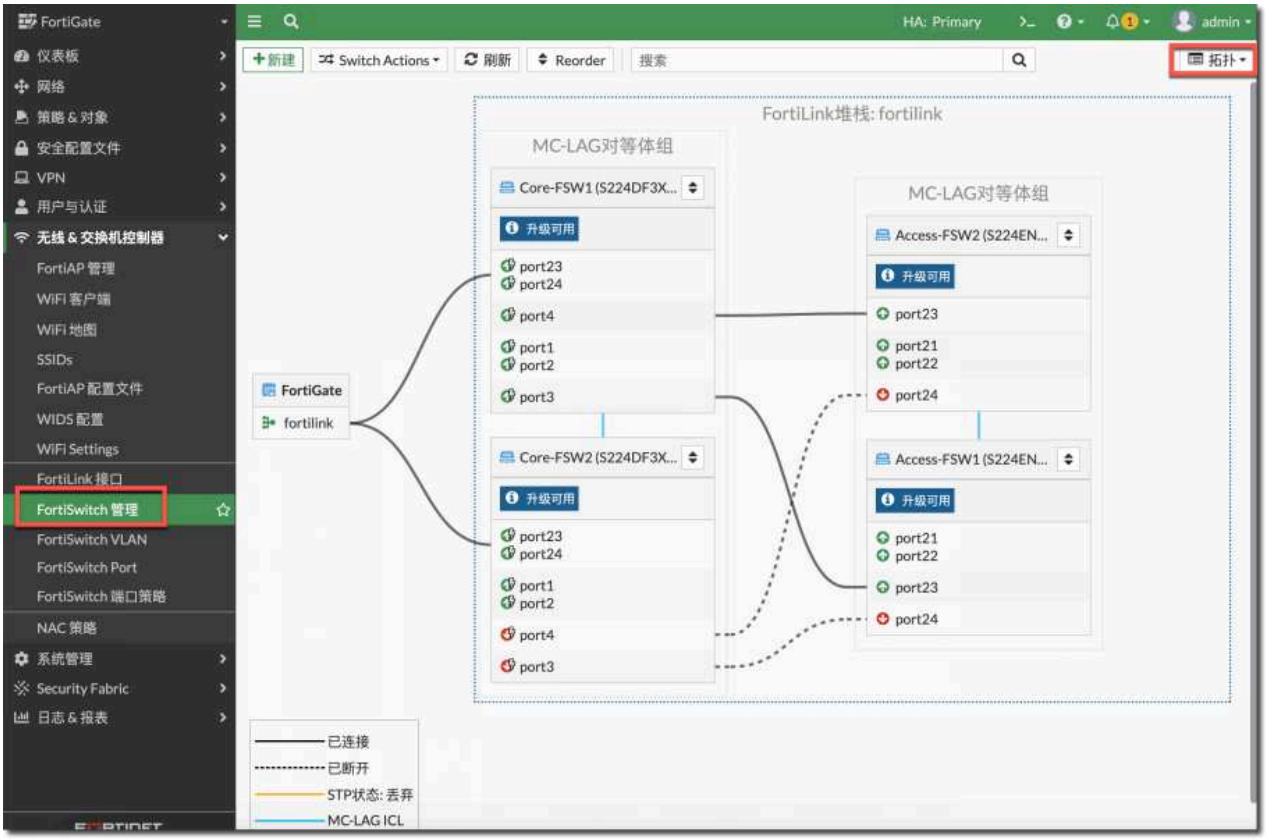
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

核心交换机接口故障模拟

1. Down掉Core-FSW2的Port3和Port4接口，查看内网PC丢包情况，可以看到Core-FSW2连接接入层交换机的接口Down掉时，丢包1个。



2. 查看和Switch管理拓扑，Core-FSW2与接入层交换机的连线已断开。



注意事项

1. 只能是堆叠交换机才可以跨交换机聚合，不同的堆叠交换机组，不支持配置为聚合接口。
2. 如果是与FortiSwith对接，则是自动MCLAG聚合。
3. 如果是和第三方设备对接，比如交换机、路由器、友商防火墙、服务器等等对接的话，推荐使用LACP Active方式动态聚合。

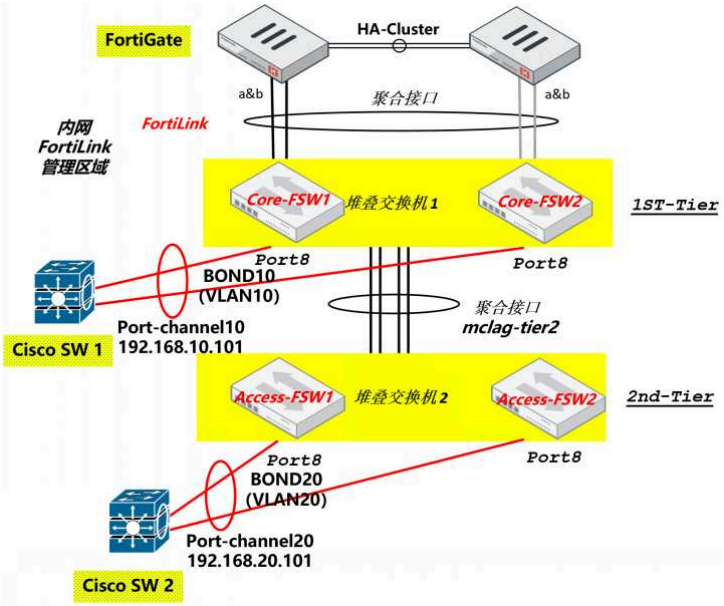
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiLink MCLAG-与第三方设备进行跨堆叠交换机聚合

网络需求

本测试基于上一个章节“FortiLink MCLAG-堆叠组网2 Tier配置举例↗”进行配置。

网络拓扑



1. Cisco SW1 的Port-Channel 10为三层接口，IP地址为192.168.10.101，我们在Core-FSW1和Core-FSW2跨交换机配置一个BOND 10的聚合接口与其对接，将其划分到VLAN10里面。
2. Cisco SW2 的Port-Channel 20为三层接口，IP地址为192.168.20.101，我们在Access-FSW1和Access-FSW2跨交换机配置一个BOND 20的聚合接口与其对接，将其划分到VLAN20里面。

配置步骤

Cisco交换机配置

1. Cisco SW1的聚合配置。

```
!
interface port-channel 10
no switchport
ip address 192.168.10.101 255.255.255.0
!
!
interface FastEthernet2/0/3
no switchport
no ip address
channel-group 10 mode active
!
interface FastEthernet2/0/4
no switchport
no ip address
channel-group 10 mode active
!
```

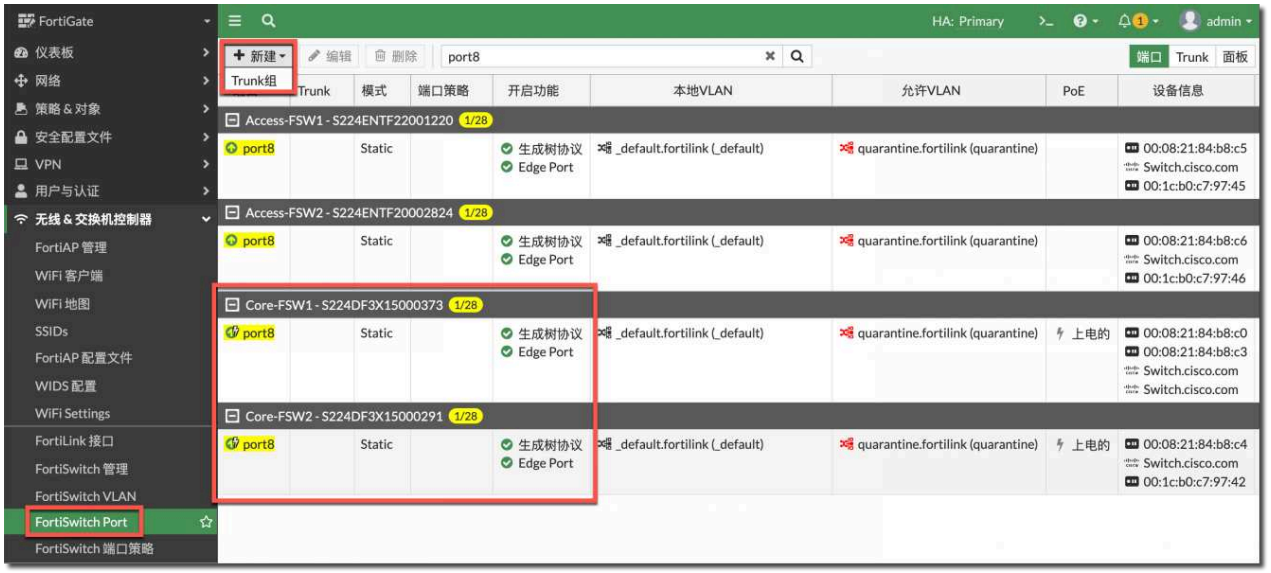
2. Cisco SW2的聚合配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
!
interface Port-channel20
no switchport
ip address 192.168.20.101 255.255.255.0
!
interface FastEthernet2/0/5
no switchport
no ip address
channel-group 10 mode active
!
interface FastEthernet2/0/6
no switchport
no ip address
channel-group 20 mode active
!
```

FortiGate配置

1. 配置基于Core-FSW1和Core-FSW2跨交换机对接的BOND 10。





2. 进入FortiSwitch Port页面的Trunk视图模式，配置Bond10成员接口的本地VLAN为10（相当于Access VLAN 10）。

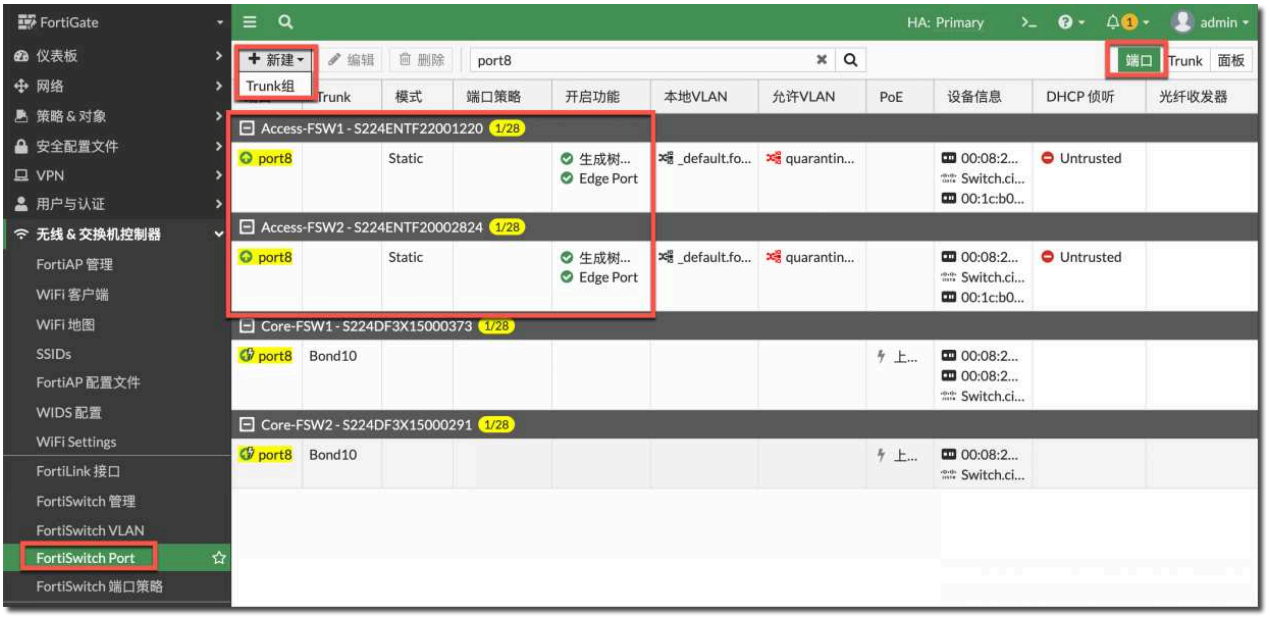
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

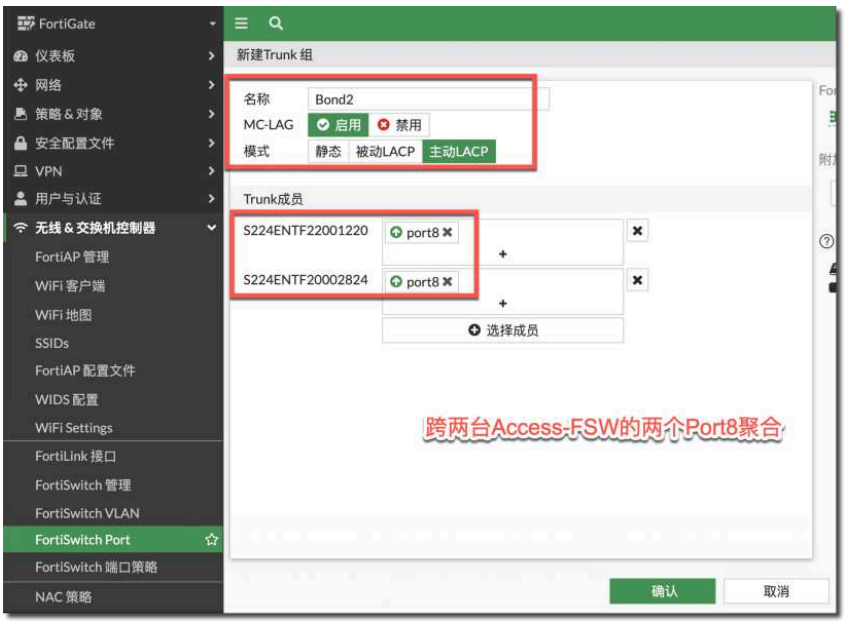



```
Core-FSW1:
config switch trunk
    edit "Bond10"
        set mode lacp-active
        set mclag enable
        set members "port8"
    next
end
config switch interface
    edit "Bond10"
        set native-vlan 10
    next
end

Core-FSW2:
config switch trunk
    edit "Bond10"
        set mode lacp-active
        set mclag enable
        set members "port8"
    next
end
config switch interface
    edit "Bond10"
        set native-vlan 10
    next
end
```

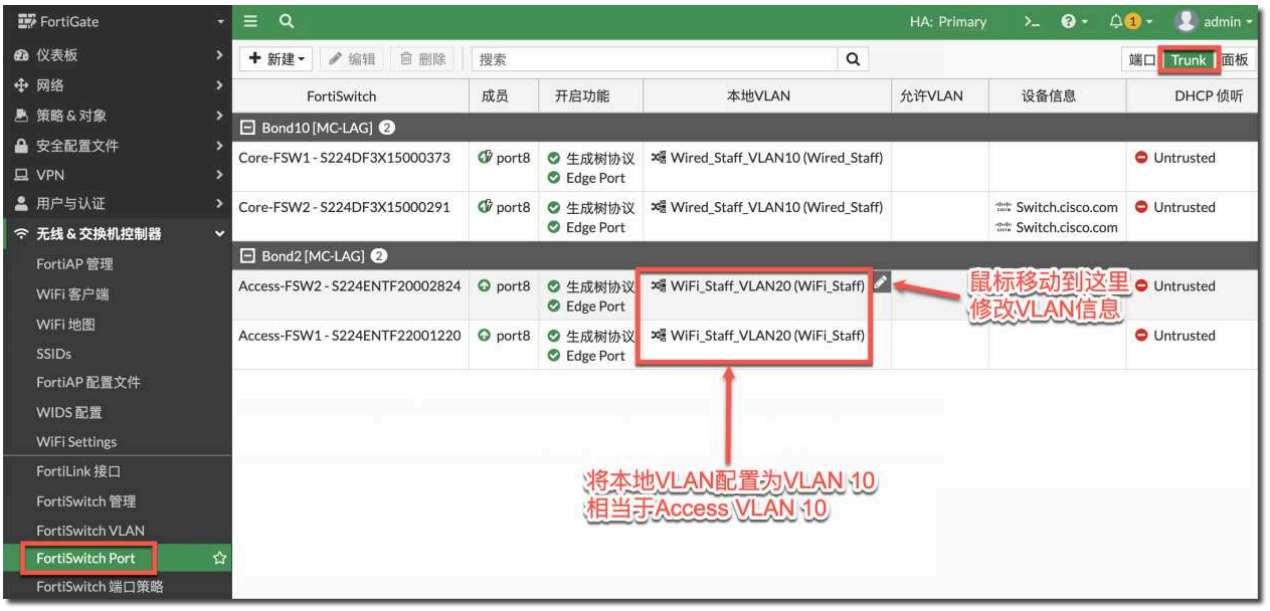
3. 配置基于Access-FSW1和Access-FSW2跨交换机对接的BOND 20。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. 进入FortiSwitch Port页面的Trunk视图模式，配置Bond20成员接口的本地VLAN为20（相当于Access VLAN 20）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Access-FSW1:
config switch trunk
    edit "Bond20"
        set mode lacp-active
        set mclag enable
        set members "port8"
    next
end
config switch interface
    edit "Bond20"
        set native-vlan 20
    next
end

Access-FSW2:
config switch trunk
    edit "Bond20"
        set mode lacp-active
        set mclag enable
        set members "port8"
    next
end
config switch interface
    edit "Bond20"
        set native-vlan 20
    next
end
```

注意事项

重要

FortiSwitch的mclag-icl堆叠组网中，与Cisco交换机聚合口对接时，还必须在FortiSwitch的STP配置中增加如下配置（set mclag-stp-bpdu single）。

bash

```
Core-FSW1:
config switch stp settings
    set mclag-stp-bpdu single
end

Core-FSW2:
config switch stp settings
    set mclag-stp-bpdu single
end

Access-FSW1:
config switch stp settings
    set mclag-stp-bpdu single
end

Access-FSW2:
config switch stp settings
    set mclag-stp-bpdu single
end
```

结果验证

Cisco-SW1

1. 在思科交换机Cisco-SW1上查看聚合状态。

```
Cisco-SW1#show interfaces port-channel 10 etherchannel

Port-channel10   (Primary aggregator)
Age of the Port-channel   = 0d:00h:35m:49s
Logical slot/port   = 10/10          Number of ports = 2
HotStandBy port = null
Passive port list   = Fa2/0/3 Fa2/0/4 Fa2/0/5
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Port state          = Port-channel L3-Ag Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+-----------------+-----------
  0     00     Fa2/0/3  Active             0
  0     00     Fa2/0/4  Active             0
Time since last port bundled:    0d:00h:28m:41s    Fa2/0/4

Cisco-SW1#show interfaces port-channel 10

Port-channel10 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001c.b0c7.9741 (bia 001c.b0c7.9741)
  Internet address is 192.168.10.101/24
  MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa2/0/3 Fa2/0/4
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:30:09, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 6000 bits/sec, 2 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4264 packets input, 1406340 bytes, 0 no buffer
     Received 4264 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 3034 multicast, 0 pause input
     0 input packets with dribble condition detected
     680 packets output, 100803 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

2. 在思科交换机Cisco-SW1上访问FortiGate的VLAN10。

```
Cisco-SW1#ping 192.168.10.1 repeat 100

Sending 100, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/11/1007 ms
```

Cisco-SW2

1. 在思科交换机Cisco-SW2上查看聚合状态。

```
Cisco-SW2#show interfaces port-channel 20 etherchannel

Port-channel20   (Primary aggregator)
Age of the Port-channel   = 0d:00h:38m:50s
Logical slot/port   = 10/20          Number of ports = 1
HotStandBy port = null
Passive port list   = Fa2/0/6
Port state          = Port-channel L3-Ag Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+-----------------+-----------
  0     00     Fa2/0/6  Active             0
Time since last port bundled:    0d:00h:10m:47s    Fa2/0/6

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Cisco-SW2#show interfaces port-channel 20

Port-channel20 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 001c.b0c7.9744 (bia 001c.b0c7.9744)
  Internet address is 192.168.20.101/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Fa2/0/6
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:10:57, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     729 packets input, 249974 bytes, 0 no buffer
     Received 729 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 542 multicast, 0 pause input
     0 input packets with dribble condition detected
     126 packets output, 18528 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

2. 在思科交换机Cisco-SW2上访问FortiGate的VLAN20。

```
Cisco-SW2#ping 192.168.20.1 repeat 100

Sending 100, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/11/1007 ms
```

注意事项

1. 只能是堆叠交换机才可以跨交换机聚合，不同的堆叠交换机组，不支持配置为聚合接口。
2. 如果是与FortiSwith对接，则是自动MCLAG聚合。
3. 如果是和第三方设备对接，比如交换机、路由器、友商防火墙、服务器等等对接的话，推荐使用LACP Active方式动态聚合。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

快速查找异常流量

Fortilink部署场景下， 如果网络中有大流量的异常流量（如大量广播、未知组播影响到网络正常运行），可以通过下面的步骤来查找异常流量的来源。

排查举例

1. 在FortiGate抓包（sniffer 4），发现网络中有大量的ARP广播流量（抓包时指定抓包数量，可以看到在某一段时间内哪些报文出现较多）。

```
FortiGate # diagnose sniffer packet any "" 4 100 l
interfaces=[any]
filters=[]
2023-05-30 09:16:42.833594 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833594 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833595 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833595 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833596 default in arp who-has 183.230.156.254 tell 183.230.156.148
2023-05-30 09:16:42.833596 default in arp who-has 183.230.20.126 tell 183.230.20.89
2023-05-30 09:16:42.833597 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833597 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833598 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833598 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833598 default in arp who-has 183.230.156.254 tell 183.230.156.148
2023-05-30 09:16:42.833598 default in arp who-has 58.254.217.97 tell 58.254.217.99
2023-05-30 09:16:42.833600 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833601 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833601 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833602 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833602 default in arp who-has 192.168.100.118 tell 192.168.100.99
2023-05-30 09:16:42.833602 default in arp who-has 183.230.156.254 tell 183.230.156.148
2023-05-30 09:16:42.833604 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833604 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833605 default in arp who-has 113.204.198.1 tell 113.204.198.2
2023-05-30 09:16:42.833607 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833608 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833608 default in arp who-has 183.230.156.254 tell 183.230.156.148
2023-05-30 09:16:42.833611 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833612 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833612 default in arp who-has 192.168.110.99 tell 192.168.110.7
2023-05-30 09:16:42.833618 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833618 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833619 port6 in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833619 default in arp who-has 183.230.156.254 tell 183.230.156.148
2023-05-30 09:16:42.833619 fortilink in 802.1Q vlan#1 P0
2023-05-30 09:16:42.833620 default in arp who-has 183.230.20.126 tell 183.230.20.89
```

2. 在FortiGate使用sniffer 6抓ARP包，确认异常ARP广播流量的源MAC，源MAC可以在sniffer 6的输出中直接看到，在“0x0000”行的第4~6段，如下所示，“ac71 2ed2 35f2”和“0009 0f09 3c0e”。

```
FortiGate # diagnose sniffer packet any "arp" 6 100 l
interfaces=[any]
filters=[arp]
2023-05-30 09:16:50.423541 default in arp who-has 58.254.217.97 tell 58.254.217.99
0x0000   ffff ffff ffff **→ac71 2ed2 35f2←** 0806 0001        .......q..5.....
0x0010   0800 0604 0001 ac71 2ed2 35f2 3afe d963        .......q..5.:..c
0x0020   0000 0000 0000 3afe d961 0000 0000 0000        ......:..a......
0x0030   0000 0000 0000 0000 0000 0000                  ............

2023-05-30 09:16:50.423554 default in arp who-has 222.178.231.33 tell 222.178.231.34
0x0000   ffff ffff ffff **→0009 0f09 3c0e←** 0806 0001        ..........<.....
0x0010   0800 0604 0001 0009 0f09 3c0e deb2 e722        ..........<...."
0x0020   0000 0000 0000 deb2 e721 0000 0000 0000        .........!......
0x0030   0000 0000 0000 0000 0000 0000                  ............

2023-05-30 09:16:50.423556 default in arp who-has 222.178.231.33 tell 222.178.231.34
0x0000   ffff ffff ffff 0009 0f09 3c0e 0806 0001        ..........<.....
0x0010   0800 0604 0001 0009 0f09 3c0e deb2 e722        ..........<...."
0x0020   0000 0000 0000 deb2 e721 0000 0000 0000        .........!......
0x0030   0000 0000 0000 0000 0000 0000                  ............
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
2023-05-30 09:16:50.423560 default in arp who-has 58.254.217.97 tell 58.254.217.99
0×0000   ffff ffff ffff ac71 2ed2 35f2 0806 0001        .......q..5.....
0×0010   0800 0604 0001 ac71 2ed2 35f2 3afe d963        .......q..5.:..c
0×0020   0000 0000 0000 3afe d961 0000 0000 0000        ......:..a......
0×0030   0000 0000 0000 0000 0000 0000                  ............

2023-05-30 09:16:50.423563 default in arp who-has 58.254.217.97 tell 58.254.217.99
0×0000   ffff ffff ffff ac71 2ed2 35f2 0806 0001        .......q..5.....
0×0010   0800 0604 0001 ac71 2ed2 35f2 3afe d963        .......q..5.:..c
0×0020   0000 0000 0000 3afe d961 0000 0000 0000        ......:..a......
0×0030   0000 0000 0000 0000 0000 0000                  ............

2023-05-30 09:16:50.423574 default in arp who-has 58.254.217.97 tell 58.254.217.99
0×0000   ffff ffff ffff ac71 2ed2 35f2 0806 0001        .......q..5.....
0×0010   0800 0604 0001 ac71 2ed2 35f2 3afe d963        .......q..5.:..c
0×0020   0000 0000 0000 3afe d961 0000 0000 0000        ......:..a......
0×0030   0000 0000 0000 0000 0000 0000                  ............

2023-05-30 09:16:50.423584 default in arp who-has 58.254.217.97 tell 58.254.217.99
0×0000   ffff ffff ffff ac71 2ed2 35f2 0806 0001        .......q..5.....
0×0010   0800 0604 0001 ac71 2ed2 35f2 3afe d963        .......q..5.:..c
0×0020   0000 0000 0000 3afe d961 0000 0000 0000        ......:..a......
0×0030   0000 0000 0000 0000 0000 0000                  ............
```

3. 查看“0009 0f09 3c0e”这个MAC地址是接入在哪个交换机的哪个端口，可以看到这个源MAC地址是从交换机S548DN4K16000312的port34口学习到的。

```
FortiGate # diagnose switch-controller mac-cache show | grep 00:09:0f:09:3c:0e -B 50
.........................................
managed-switch: S548DN4K16000312 vfid:   0
running-clients:
VLANID   PORTID   ACCESS   MAC               LAST-SEEN(secs ago) INTF-NAME
1        34       accept   00:09:0f:09:3c:0a  52                 port34
```

4. 在FortiLink成员交换机S548DN4K16000312上检查流量，发现这个交换机的port34口和port35口的流量异常。

```
S548DN4K16000312 # diagnose switch physical-ports linerate up
```

```
port13 |      94275010153 |   171.1271 Mbps ||              56642 |     0.0000 Mbps |
port14 |      94274885486 |   171.0361 Mbps ||              56642 |     0.0000 Mbps |
port15 |      94274902209 |   170.9338 Mbps ||              56642 |     0.0000 Mbps |
port16 |      94274813829 |   170.8185 Mbps ||              56642 |     0.0000 Mbps |
port17 |      94274911097 |   170.4430 Mbps ||              56642 |     0.0000 Mbps |
port18 |      94274867710 |   170.3595 Mbps ||              56642 |     0.0000 Mbps |
port19 |      94274709770 |   170.3216 Mbps ||              56642 |     0.0000 Mbps |
port20 |      94274769282 |   170.2678 Mbps ||              56642 |     0.0000 Mbps |
port22 |       2565696451 |     0.0410 Mbps ||            2757465 |     0.0000 Mbps |
port23 |       2555226658 |     0.0127 Mbps ||             144944 |     0.0000 Mbps |
port24 |     112619791276 |   170.3063 Mbps ||            1113452 |     0.0012 Mbps |
port25 |     112600069903 |   170.1315 Mbps ||              88603 |     0.0000 Mbps |
port26 |     112600044067 |   170.0476 Mbps ||              88603 |     0.0000 Mbps |
port27 |     112599917226 |   169.9863 Mbps ||              88603 |     0.0000 Mbps |
port28 |     112599916735 |   169.9153 Mbps ||              88603 |     0.0000 Mbps |
port29 |     112599757702 |   169.8759 Mbps ||              88603 |     0.0000 Mbps |
port30 |     112599608054 |   169.8013 Mbps ||              88603 |     0.0000 Mbps |
port31 |     112599588686 |   169.8915 Mbps ||              88618 |     0.0000 Mbps |
port32 |     112599546651 |   169.9003 Mbps ||              88603 |     0.0000 Mbps |
port33 |     112600620342 |   169.9212 Mbps ||              88603 |     0.0000 Mbps |
port34 |     194843122934 |   140.2551 Mbps ||       169016453213 |   722.9183 Mbps |
port35 |     192140484212 |   722.9053 Mbps ||       171691896046 |   140.2281 Mbps |
port36 |         13002345 |     0.0202 Mbps ||              88602 |     0.0000 Mbps |
port39 |         10409162 |     0.0021 Mbps ||              69124 |     0.0000 Mbps |
port40 |     112613197123 |   169.8033 Mbps ||                 13 |     0.0000 Mbps |
port41 |     112610491519 |   169.8336 Mbps ||            1078842 |     0.0000 Mbps |
port42 |     112613831915 |   169.8294 Mbps ||              57731789 |     0.0000 Mbps |
port43 |     112612713061 |   169.8099 Mbps ||             821887254 |     0.0233 Mbps |
port44 |         11529838 |     0.0091 Mbps ||              93459 |     0.0000 Mbps |
port45 |     112609755277 |   169.8417 Mbps ||                 18 |     0.0000 Mbps |
port46 |     112602860412 |   169.7973 Mbps ||            1526419 |     0.0000 Mbps |
port47 |     112604799750 |   169.7663 Mbps ||              44337052 |     0.0039 Mbps |
port48 |     112605154331 |   169.7150 Mbps ||            1180979181 |     0.0323 Mbps |
port51 |      93309196191 |   177.7362 Mbps ||           42263111161 |     0.4944 Mbps |
port52 |     123512702971 |   177.6112 Mbps ||            8140918167 |     0.3305 Mbps |
internal |       149248028 |     0.2892 Mbps ||            13255285 |     0.0425 Mbps |
-------------------------------------------------------------------------------------
                           |  6843.2485 Mbps ||                     |   864.0743 Mbps |
```

5. 查找异常的流量的来源设备，通过LLDP可以查询到接入的设备信息，从而确定异常流量的来源设备。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
S548DN4K16000312 # get switch lldp neighbors-summary
......
  port34      Up       **→FortiGate-601F-down-Test←**  120   BR          -         port13
  port35      Up       **→FortiGate-601F-down-Test←**  120   BR          -         port14
......
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VDOM基本配置

VDOM简介

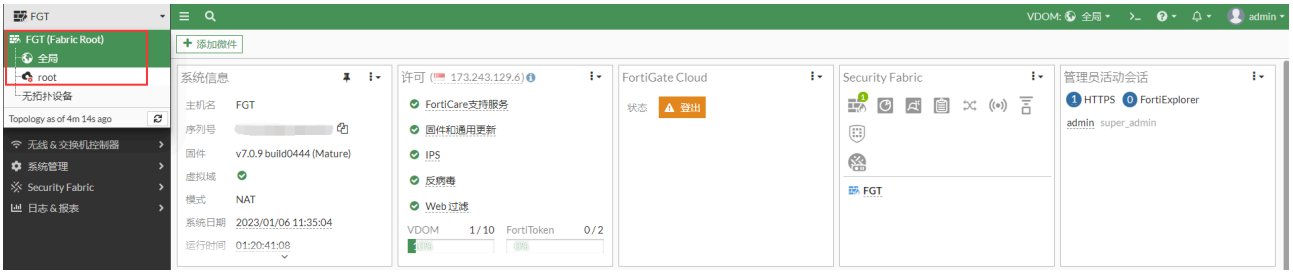
虚拟域(VDOM)，即虚拟防火墙，是将一台物理的 FortiGate 划分为两个或两个以上的可以独 立运行的虚拟防火墙的技术，虚拟域技术可以将FortiGate划分为多个不同的NAT/透明模式多个虚拟FortiGate，为每一个虚拟域提供独立的安全策略，路由及 VPN 配置等。

开启VDOM

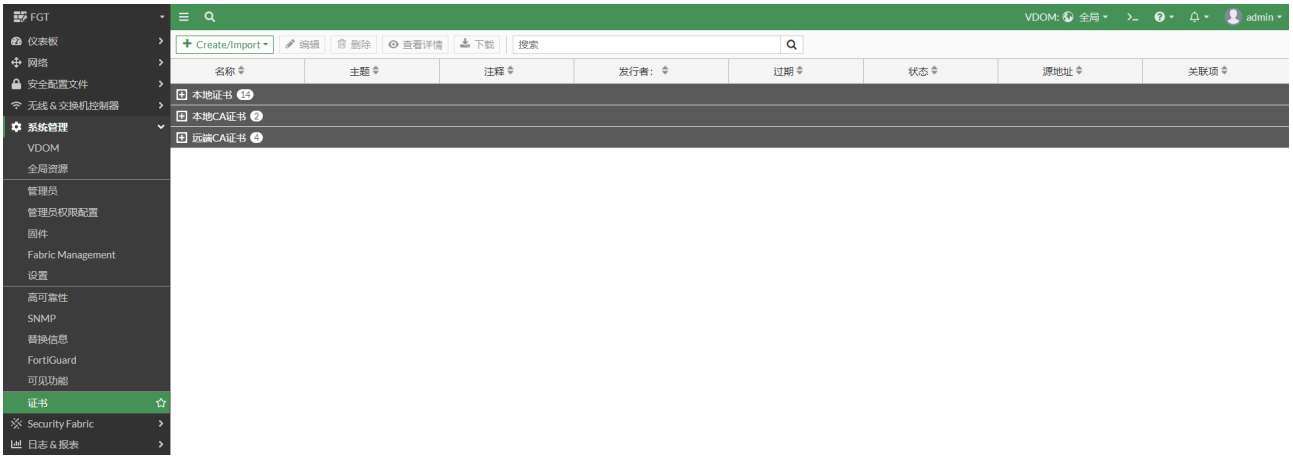
在config system global下开启vdom，vdom模式选择multi-vdom，开启vdom后需要重新登录FortiGate。

```
config system global
    set vdom-mode multi-vdom
end
You will be logged out for the operation to take effect.
Do you want to continue? (y/n)y
```

开启vdom后，FortiGate默认将设备分为全局域和root vdom。可以直接点击“全局”或者“root” 来切换全局域和root vdom。



全局用于所有vdom都共享的配置，如HA，SNMP，证书等。

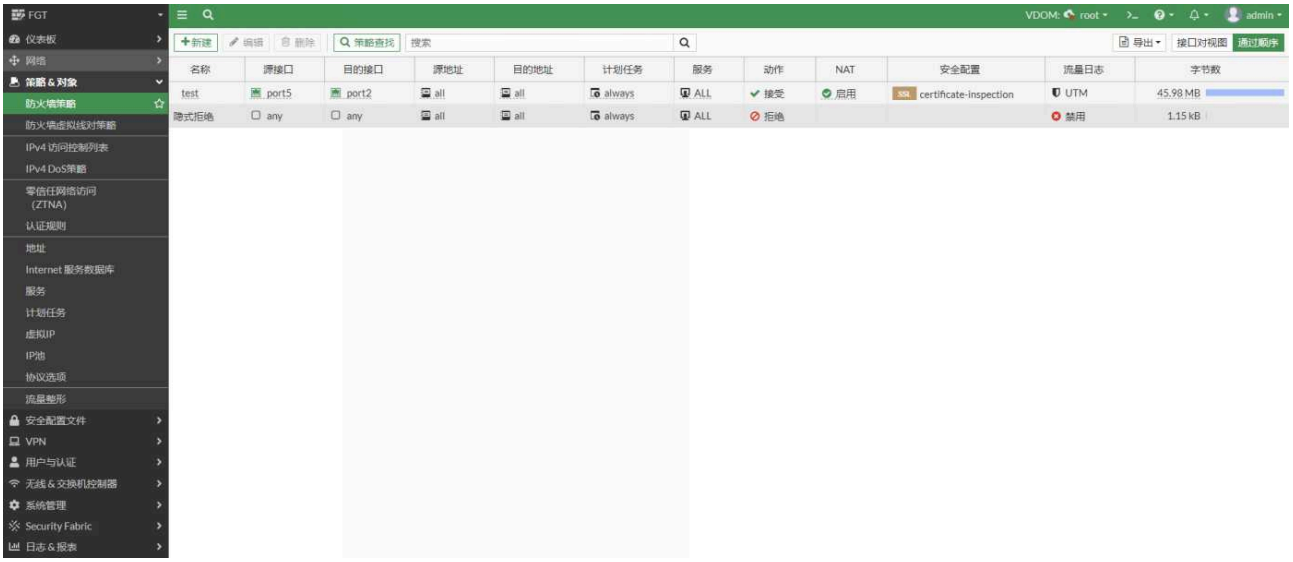


使用CLI配置时，需要使用config global进入全局模式，再配置具体的功能。如配置snmp：

```
config global
    config system snmp sysinfo
        set status enable
    end
end
```

root vdom是一个默认的虚拟防火墙。root vdom默认是管理vdom，用于和FortiGuard通信来更新license，特征库等。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



使用CLI配置时，需要使用config vdom进入对应的vdom，在配置具体的功能，如配置防火墙策略：

```
config vdom
    edit root
    config firewall policy
        edit 3
            set name "test"
            set srcintf "port5"
            set dstintf "port2"
            set action accept
            set srcaddr "all"
            set dstaddr "all"
            set schedule "always"
            set service "ALL"
            set nat enable
        next
    end
end
```

创建vdom

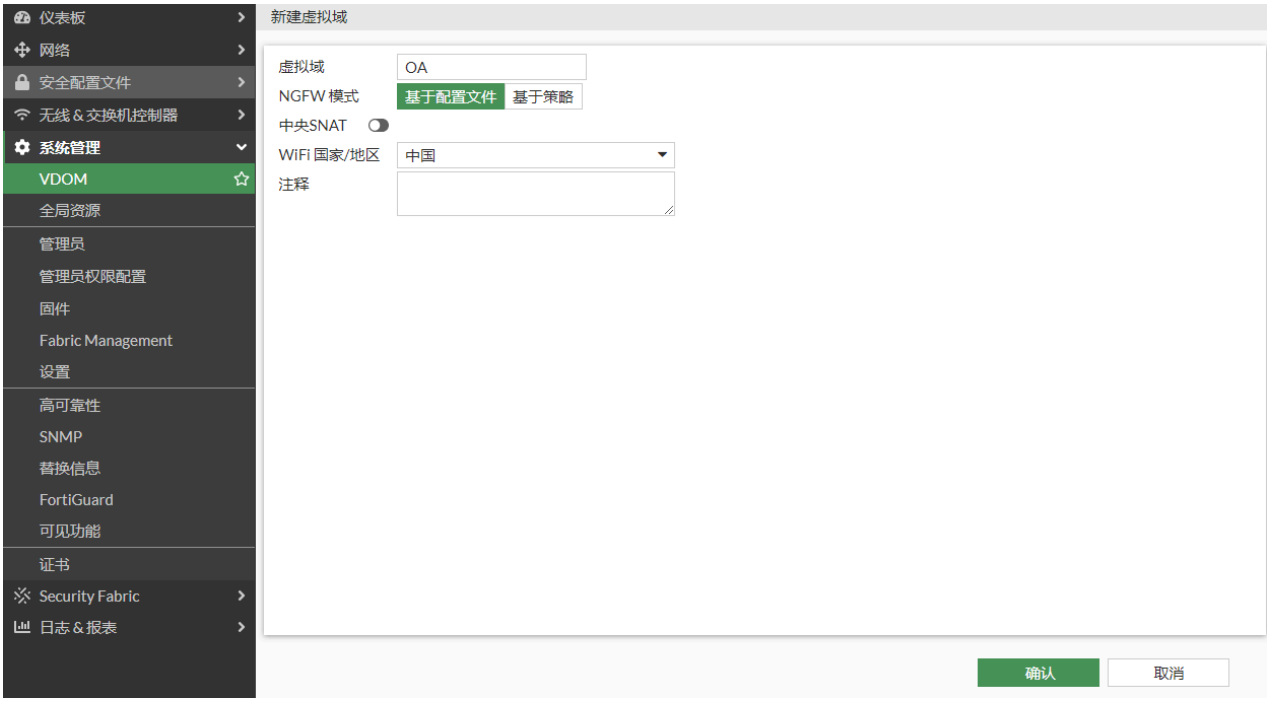
1. **GUI创建vdom**

   在全局中，选择“系统管理”



   创建OA vdom，用于独立的OA业务。创建的vdom默认是NAT模式的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击确认后，创建完成。



2. **CLI创建vdom**

进入vdom，edit vdom名称就会直接创建一个vdom，默认是NAT模式的vdom。

```
config vdom
    edit Database
end
```

创建完成后，可以在GUI界面查看。



可以避免CLI误创建vdom，可以将vdom创建提示打开。

```
config global
    config system global
        set edit-vdom-prompt enable
    end
end
```

再次创建vdom时，CLI会提示。

```
config vdom
edit Web

The input VDOM name doesn't exist.
Do you want to create a new VDOM?
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Please press 'y' to continue, or press 'n' to cancel. (y/n)y

current vf=Web:5

end
```

3. 将vdom改为透明模式

创建vdom时默认是NAT模式，需要通过CLI将vdom修改为透明模式。

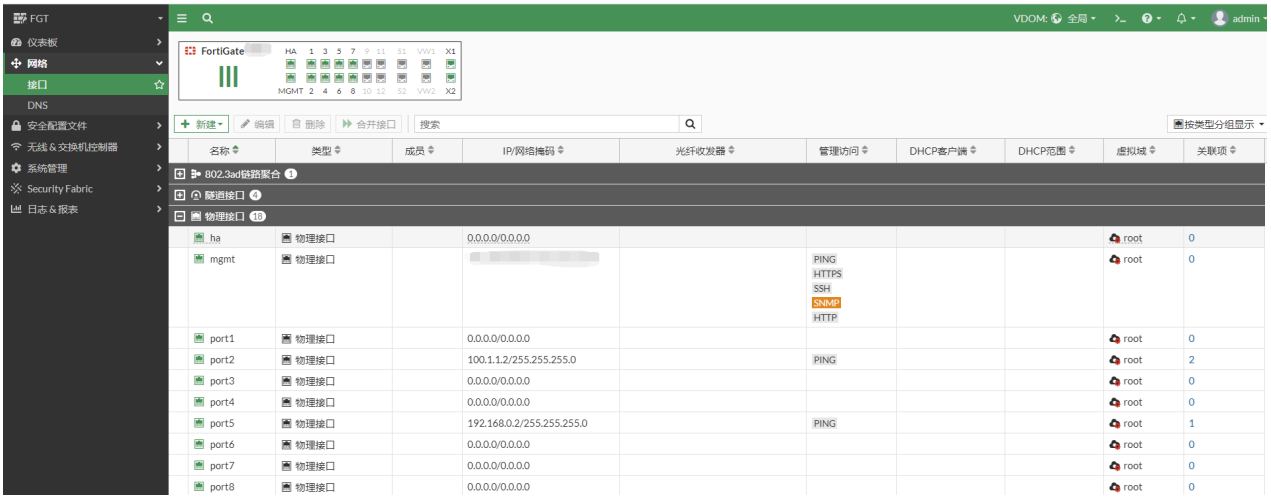
> **重要**
>
> 如果透明模式是一进一出的环境，建议使用虚拟接口对。

```
config vdom
    edit Web
    config system settings
        set opmode transparent
        set manageip 1.1.1.1/255.255.255.0
        set gateway 1.1.1.254
    end
end
```

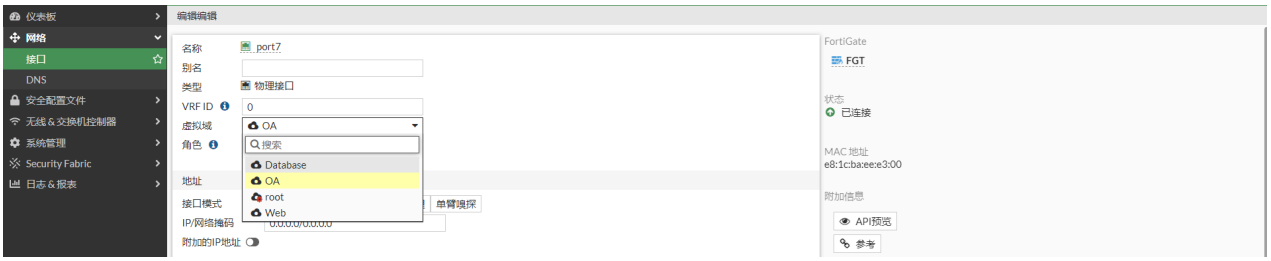
将接口划入vdom

1. GUI方式将接口划入vdom

切换到全局，选择“网络”-->”接口“。

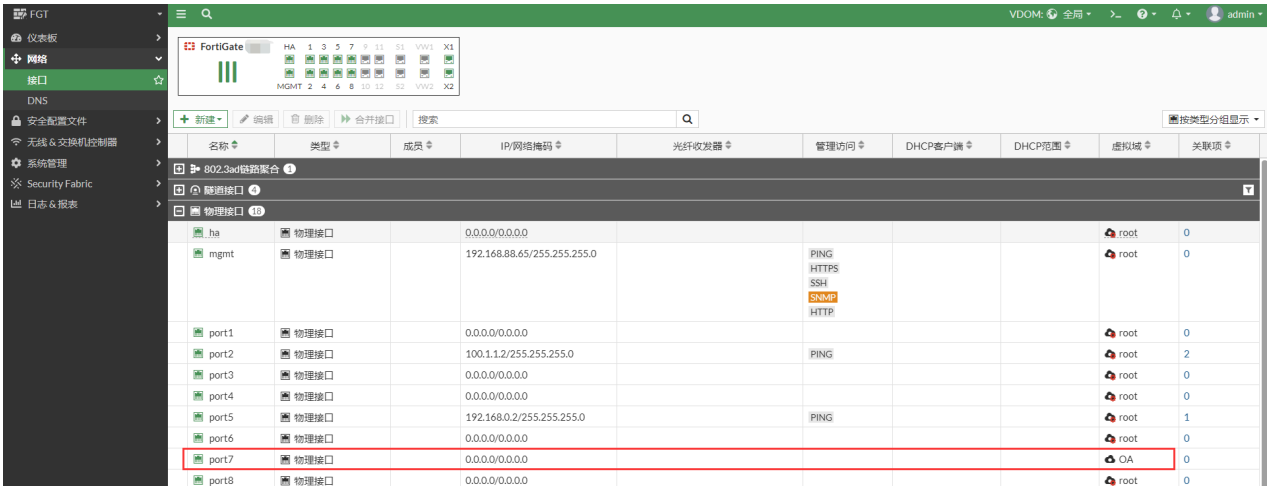


将接口划入OA vdom。



可以看到OA已经划入到OA vdom。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



切换到OA vdom查看接口。



2. **CLI方式将接口划入vdom**

命令行如下：

```
config global
    config system interface
        edit port8
            set vdom OA
        next
    end
end
```

GUI查看OA vdom的接口。（port7是上一个操作划入OA vdom的）



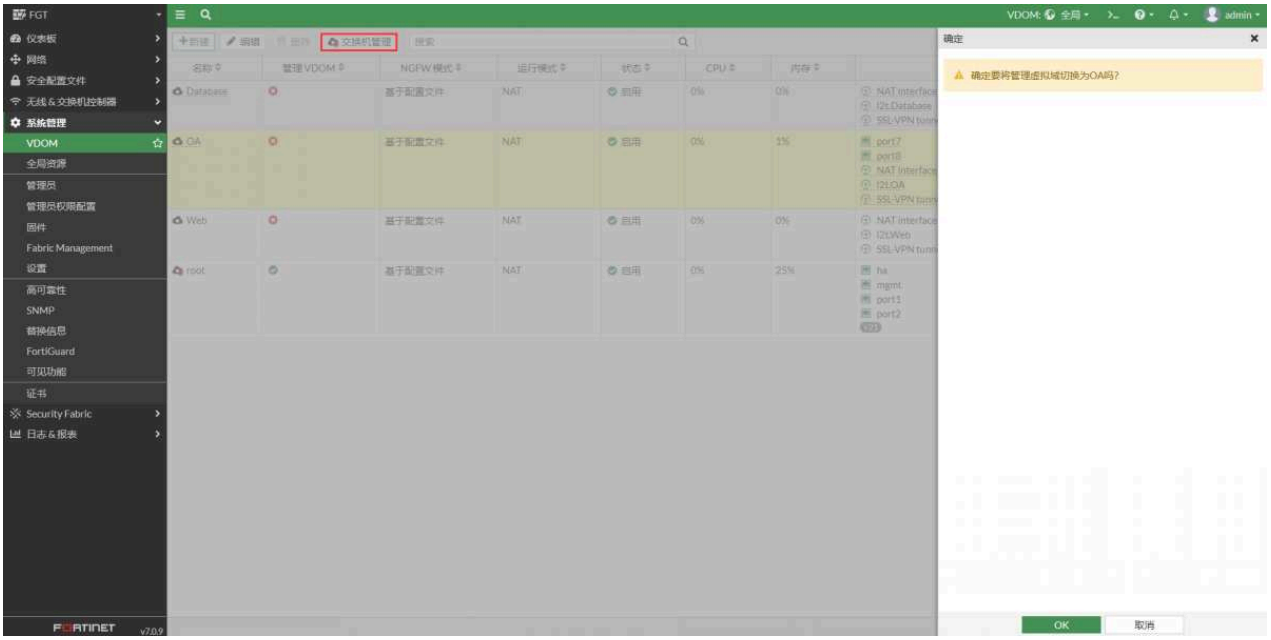
修改管理vdom

管理vdom用于和FortiGuard通信来更新license，特征库等，因此需要连接Internet；也可以连接FortiManager更新，则FortiManager与FortiGuard通信。

1. **GUI修改管理vdom**

切换到全局，选择“系统管理”-->“VDOM”，选择vdom，点击“交换机管理”切换为管理VDOM，点击“OK”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



可以看到OA已设置为管理vdom。



2. CLI修改管理vdom

```
config global
    config system global
        set management-vdom OA
    end
end
```

删除vdom

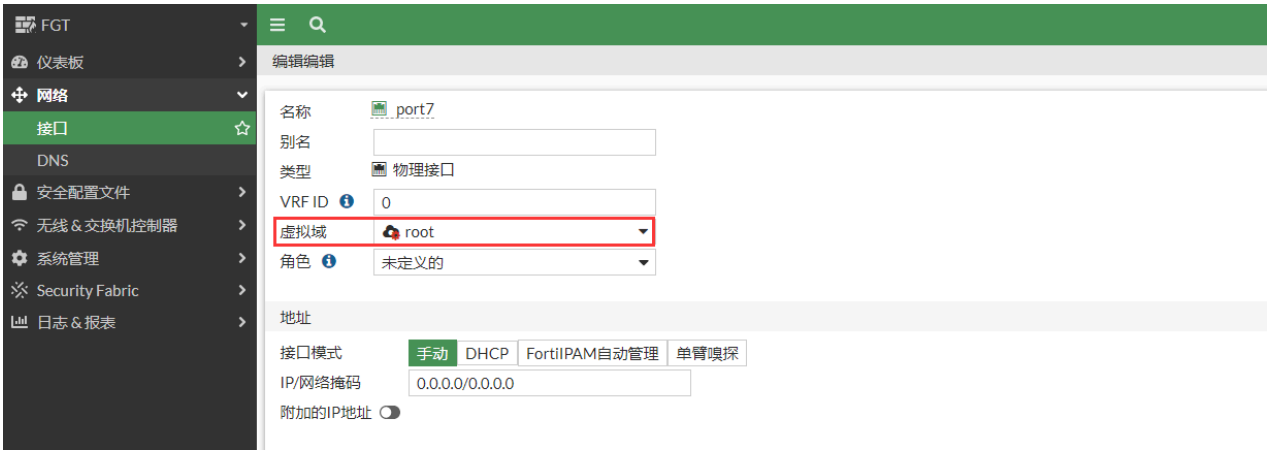
1. GUI删除vdom

在删除vdom前，需要把vdom中的接口以及相关的配置都移除，在没有完全移除之前，是不能删除该vdom的。如OA vdom。



选择“网络”-->“接口”，将接口划入到其他的vdom。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



当OA中的接口及其他相关的配置都移除后，OA vdom可以删除。



点击“删除”。



确认后，OA vdom移除。



2. **CLI删除vdom**

在删除vdom前，需要把vdom中的接口以及相关的配置都移除，在没有完全移除之前，是不能删除该vdom的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vdom
    delete Database
end
```

GUI查看该vdom已经删除。



关闭vdom

将FortiGate的其他vdom都删除后，才可以关闭vdom。



CLI关闭vdom，关闭vdom后，需要重新登录。

```
config global
    config system global
        set vdom-mode no-vdom
    end

You will be logged out for the operation to take effect.
Do you want to continue? (y/n)y
```

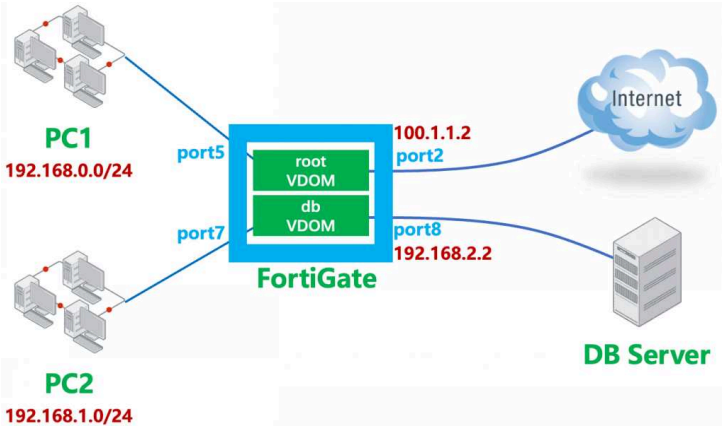

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VDOM使用

网络需求

客户上网的业务和内部数据的业务分离。将FortiGate划分两个不同的vdom，一个root vdom用于上网，一个db vdom用于内网数据库访问。

网络拓扑



配置步骤

1. **创建vdom**

   开启VDOM

```
config system global
    set vdom-mode multi-vdom
end
```

   创建VDOM



2. **将接口划入VDOM**

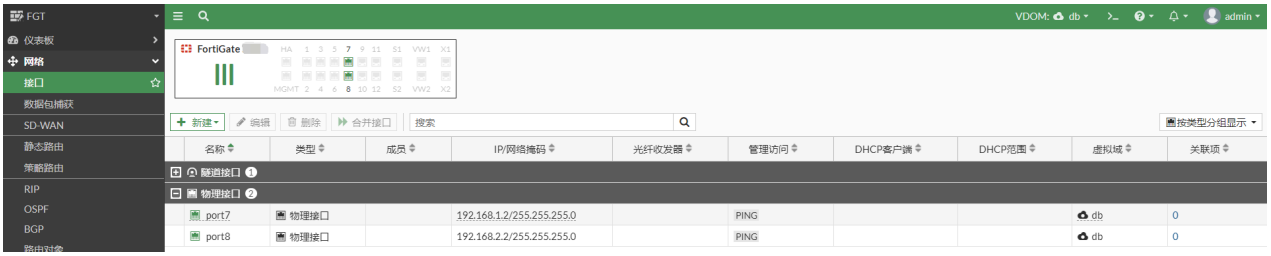
   所有的接口默认都在root VDOM中，因此只需要将port7和port8划入db vdom即可。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



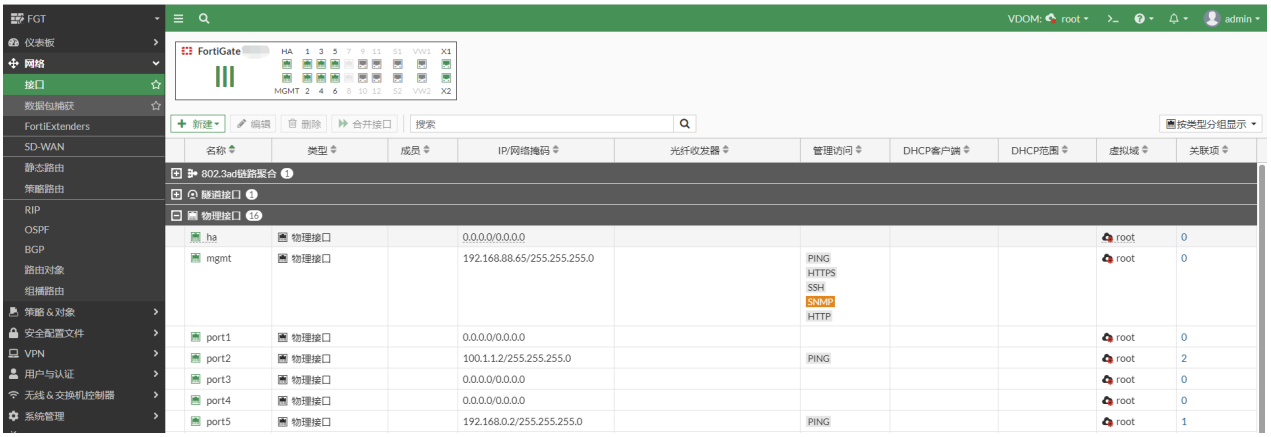


查看db vdom中的接口。



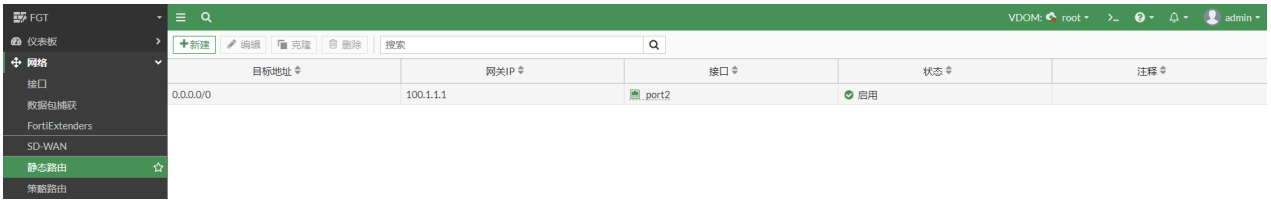
查看root vdom中的接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

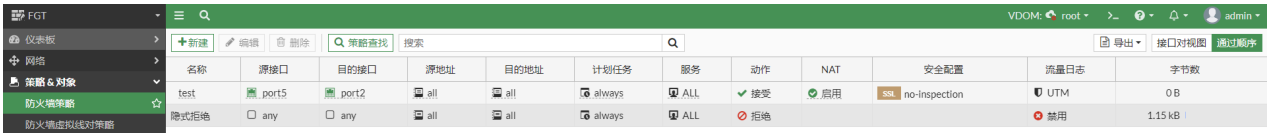


3. root vdom配置路由和策略

配置路由。

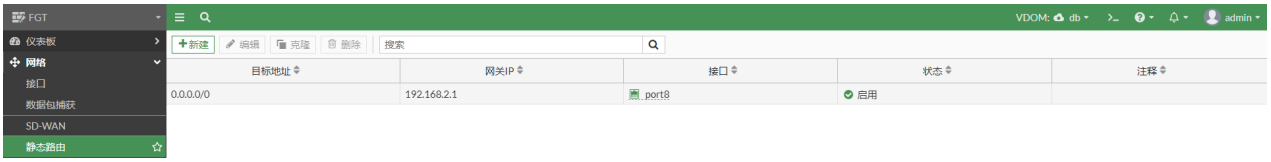


配置策略。



4. db vdom配置路由和策略

配置路由。



配置策略。



业务测试

root vdom测试

1. 查看root vdom路由表

```
进入root vdom
#config vdom
#edit root

# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
```

2. 业务测试

PC1 ping 114.114.114.114

```
PC1# ping 114.114.114.114
PING 114.114.114.114 (114.114.114.114) 56(84) bytes of data.
64 bytes from 114.114.114.114: icmp_seq=1 ttl=64 time=23.2 ms
64 bytes from 114.114.114.114: icmp_seq=2 ttl=82 time=23.3 ms
64 bytes from 114.114.114.114: icmp_seq=3 ttl=79 time=23.3 ms
64 bytes from 114.114.114.114: icmp_seq=4 ttl=78 time=23.4 ms
64 bytes from 114.114.114.114: icmp_seq=5 ttl=77 time=23.1 ms
```

FortiGate抓包

```
进入root vdom
#config vdom
#edit root

抓包
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
1.674117 port5 in 192.168.0.10 → 114.114.114.114: icmp: echo request
1.674142 port2 out 100.1.1.2 → 114.114.114.114: icmp: echo request
1.697234 port2 in 114.114.114.114 → 100.1.1.2: icmp: echo reply
1.697242 port5 out 114.114.114.114 → 192.168.0.10: icmp: echo reply
```

FortiGate查看会话

```
进入vdom
#config vdom
#edit root

查看会话
#diagnose sys session filter proto 1
#diagnose sys session filter vd-name root
#diagnose sys session list

该会话的vdom索引是0，即vd=0，通过diagnose sys vd list查看vdom索引，root vdom的索引是0
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=13→10/10→13 gwy=100.1.1.1/192.168.0.10
hook=post dir=org act=snat 192.168.0.10:3646→114.114.114.114:8(100.1.1.2:64062)
hook=pre dir=reply act=dnat 114.114.114.114:64062→100.1.1.2:0(192.168.0.10:3646)
misc=0 policy_id=3 pol_uuid_idx=515 auth_info=0 chk_client_info=0 vd=0
serial=0003413a tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×4000c00 ofld-O ofld-R
npu info: flag=0×81/0×81, offload=8/8, ips_offload=0/0, epid=150/156, ipid=156/150, vlan=0×0000/0×0000
vlifid=156/150, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/3

进入全局，查看vdom索引
#config global
# diagnose sys vd list | grep name=root
name=root/root index=0 enabled fib_ver=36 rpdb_ver=2 use=168 rt_num=48 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

db vdom测试

1. 查看路由表

```
进入db vdom
#config vdom
#edit db

查看路由表
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 192.168.2.1, port8, [1/0]
C       192.168.1.0/24 is directly connected, port7
C       192.168.2.0/24 is directly connected, port8
```

2. 业务测试

PC2 ping DB Server

```
PC2# ping 192.168.91.201
PING 192.168.91.201 (192.168.91.201) 56(84) bytes of data.
64 bytes from 192.168.91.201: icmp_seq=1 ttl=61 time=0.898 ms
64 bytes from 192.168.91.201: icmp_seq=2 ttl=61 time=1.05 ms
64 bytes from 192.168.91.201: icmp_seq=3 ttl=61 time=0.935 ms
64 bytes from 192.168.91.201: icmp_seq=4 ttl=61 time=0.687 ms

--- 192.168.91.201 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.687/0.892/1.050/0.134 ms
```

FortiGate抓包

```
进入db vdom
#config vdom
#edit db

查看路由表
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
2.484117 port7 in 192.168.1.10 → 192.168.91.201: icmp: echo request
2.484133 port8 out 192.168.1.10 → 192.168.91.201: icmp: echo request
2.484914 port8 in 192.168.91.201 → 192.168.1.10: icmp: echo reply
2.485049 port7 out 192.168.91.201 → 192.168.1.10: icmp: echo reply
```

FortiGate查看会话

```
进入db vdom
#config vdom
#edit db

查看会话
# diagnose sys session filter proto 1
# diagnose sys session filter vd-name db
# diagnose sys session list

该会话的vdom索引是3，即vd=3，通过diagnose sys vd list查看vdom索引，db vdom的索引是3
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=15→16/16→15 gwy=192.168.2.1/192.168.1.10
hook=pre dir=org act=noop 192.168.1.10:2605→192.168.91.201:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.91.201:2605→192.168.1.10:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=617 auth_info=0 chk_client_info=0 vd=3
serial=0003466c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×4000c00 ofld-O ofld-R
npu info: flag=0×81/0×81, offload=8/8, ips_offload=0/0, epid=162/160, ipid=160/162, vlan=0×0000/0×0000
vlifid=160/162, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=3/2

进入全局，查看vdom索引
#config global
# diagnose sys vd list | grep name=db
name=db/db index=3 enabled fib_ver=23 rpdb_ver=0 use=62 rt_num=7 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VDOM间通信

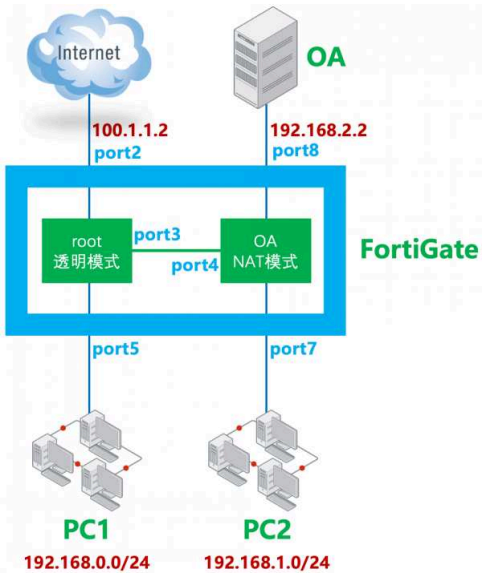
网络需求

OA业务vdom的用户通过Internet vdom上网。

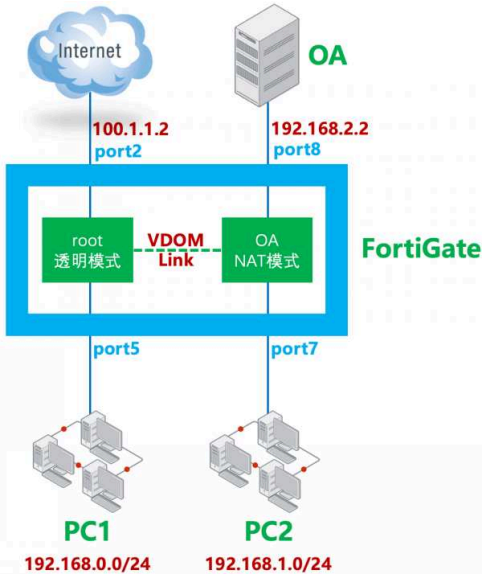
网络拓扑

有两个方式可以让VDOM之间通信：

1. 通过物理线路连接；



2. 通过NPU link内部线路连接，部分硬件设备支持（也可以手动创建虚拟link进行连接，但无法被NP加速）。



配置步骤

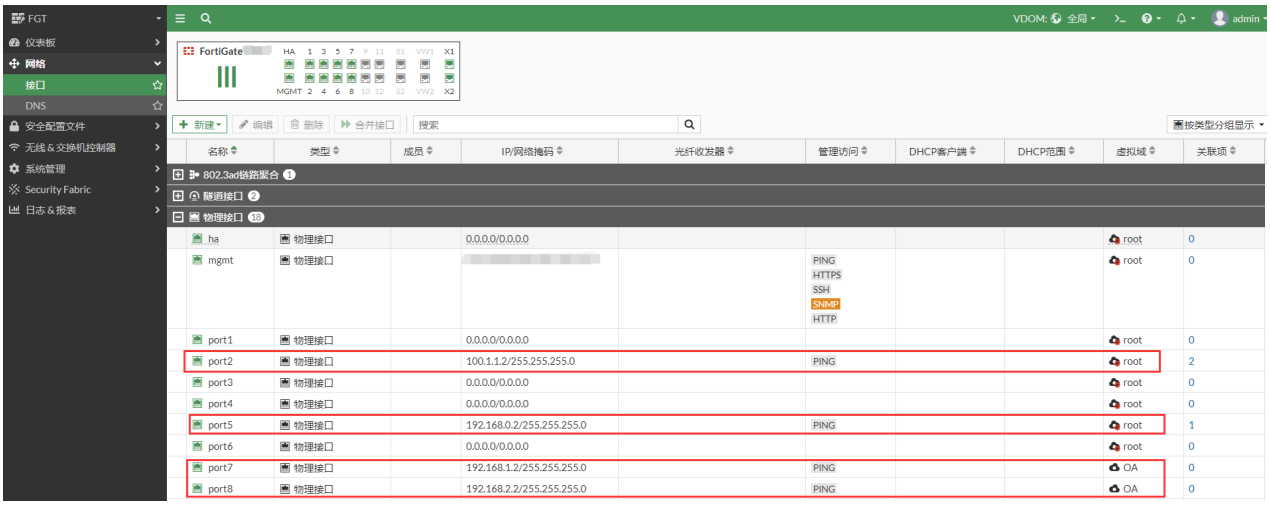
1. 开启vdom并创建vdom。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

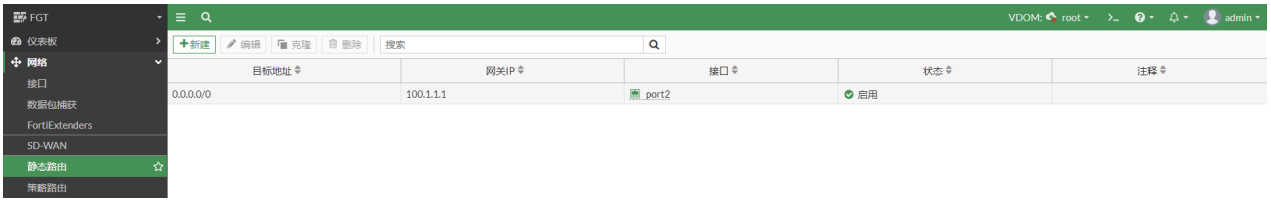



```
config system global
    set vdom-mode multi-vdom
end
```

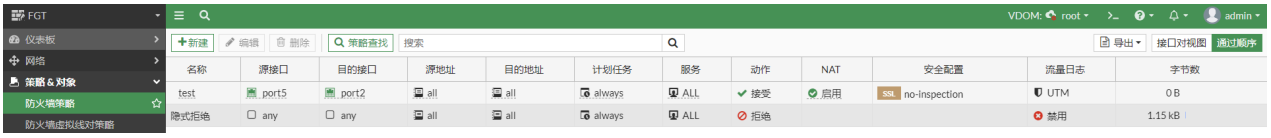
2. 将接口划入vdom，所有的接口默认都在root vdom中，因此只需要将port7和port8划入OA vdom即可。



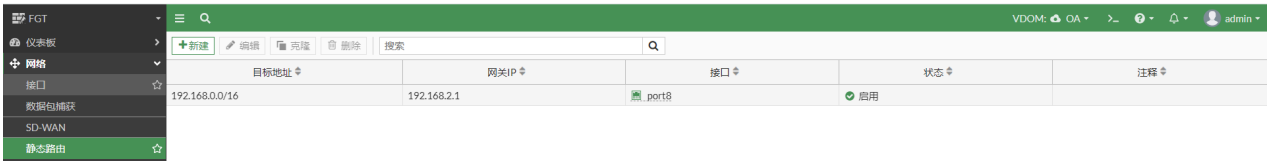
3. root vdom配置路由和策略，这是root vdom自身业务转发的配置。配置路由。



4. 配置策略。



5. OA vdom配置路由和策略，这是OA vdom自身业务转发的配置，配置路由，OA的目的地址范围假设是192.168.0.0/16。



6. 配置策略。

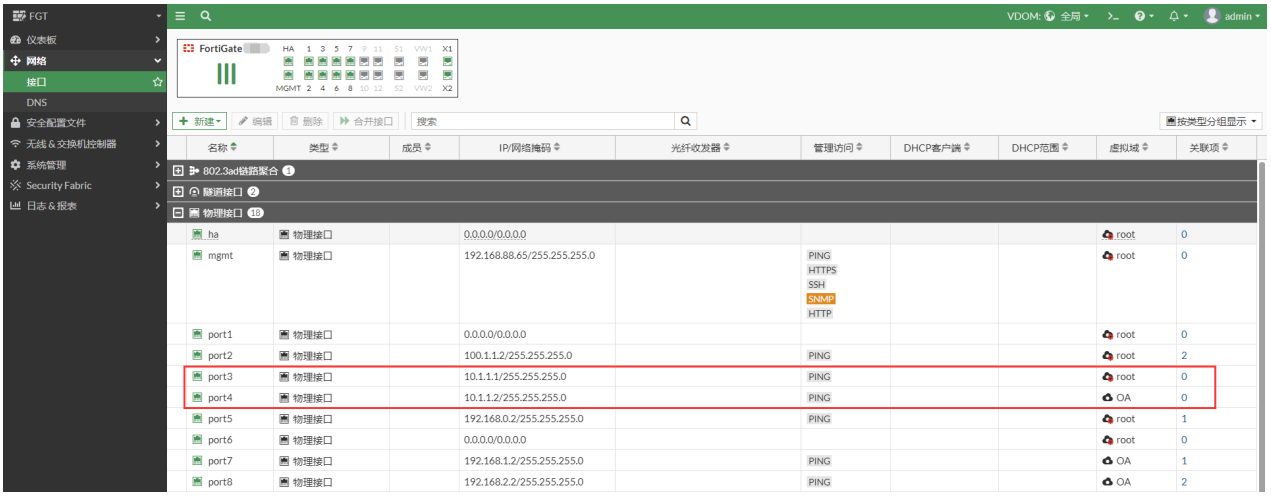


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VDOM间通信配置

物理线路方式

1. 将接口划入vdom，将port3划入root vdom，将port4划入OA vdom，配置ip地址，然后使用网线连接port3和port4。



2. 测试port3和port4之间的连通性。进入root vdom，从root vdom ping OA vdom port4接口地址。

```
进入root vdom，从root vdom ping OA vdom port4接口地址
#config vdom
#edit root
# execute ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2): 56 data bytes
64 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3. 进入OA vdom，从OA vdom Ping root vdom port3接口地址。

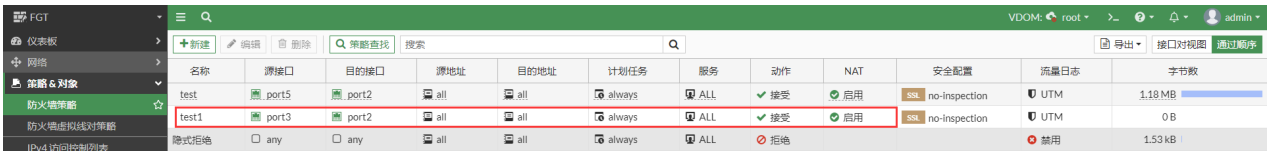
```
#config vdom
#edit OA
#execute ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

4. root vdom配置路由和策略，配置路由，配置root vdom到OA vdom子网的回程路由。

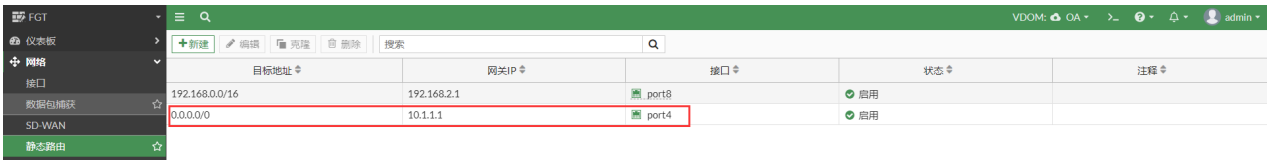


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

5. 配置策略，允许OA vdom到Internet的流量。



6. OA vdom配置路由和策略，配置路由，使OA vdom访问Internet的路由指向root vdom。



7. 配置策略，允许OA vdom到root vdom的流量。



VDOM间通信测试

1. PC2访问Internet。

```
PC2# ping 114.114.114.114
PING 114.114.114.114 (114.114.114.114) 56(84) bytes of data.
64 bytes from 114.114.114.114: icmp_seq=1 ttl=69 time=23.5 ms
64 bytes from 114.114.114.114: icmp_seq=2 ttl=85 time=23.2 ms
64 bytes from 114.114.114.114: icmp_seq=3 ttl=86 time=23.2 ms
64 bytes from 114.114.114.114: icmp_seq=4 ttl=73 time=23.2 ms
```

2. FortiGate抓包可以看出数据流穿过了port3和port4接口（在root vdom或者在OA vdom下抓包都是可以的）。

```
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
2.923717 port7 in 192.168.1.10 → 114.114.114.114: icmp: echo request
2.923771 port4 out 192.168.1.10 → 114.114.114.114: icmp: echo request
2.923782 port3 in 192.168.1.10 → 114.114.114.114: icmp: echo request
2.923794 port2 out 100.1.1.2 → 114.114.114.114: icmp: echo request
2.946967 port2 in 114.114.114.114 → 100.1.1.2: icmp: echo reply
2.946978 port3 out 114.114.114.114 → 192.168.1.10: icmp: echo reply
2.946989 port4 in 114.114.114.114 → 192.168.1.10: icmp: echo reply
2.947163 port7 out 114.114.114.114 → 192.168.1.10: icmp: echo reply
```

3. FortiGate查看会话，ping流量在root vdom和OA vdom都产生了会话。在root vdom或者在OA vdom下查看都可以看到会话，vd=0是root vdom，vd=3是OA vdom。

```
# diagnose sys session list
session info: proto=1 proto_state=00 duration=29 expire=31 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=11->10/10->11 gwy=100.1.1.1/10.1.1.2
hook=post dir=org act=snat 192.168.1.10:2691->114.114.114.114:8(100.1.1.2:63107)
hook=pre dir=reply act=dnat 114.114.114.114:63107->100.1.1.2:0(192.168.1.10:2691)
misc=0 policy_id=4 pol_uuid_idx=636 auth_info=0 chk_client_info=0 vd=0
serial=00036a12 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
npu info: flag=0×81/0×81, offload=8/8, ips_offload=0/0, epid=150/152, ipid=152/150, vlan=0×0000/0×0000
vlifid=152/150, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/7

session info: proto=1 proto_state=00 duration=29 expire=31 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=15→12/12→15 gwy=10.1.1.1/192.168.1.10
hook=pre dir=org act=noop 192.168.1.10:2691→114.114.114.114:8(0.0.0.0:0)
hook=post dir=reply act=noop 114.114.114.114:2691→192.168.1.10:0(0.0.0.0:0)
misc=0 policy_id=2 pol_uuid_idx=637 auth_info=0 chk_client_info=0 vd=3
serial=00036a11 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×4000c00 ofld-O ofld-R
npu info: flag=0×81/0×81, offload=8/8, ips_offload=0/0, epid=154/160, ipid=160/154, vlan=0×0000/0×0000
vlifid=160/154, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/3
```

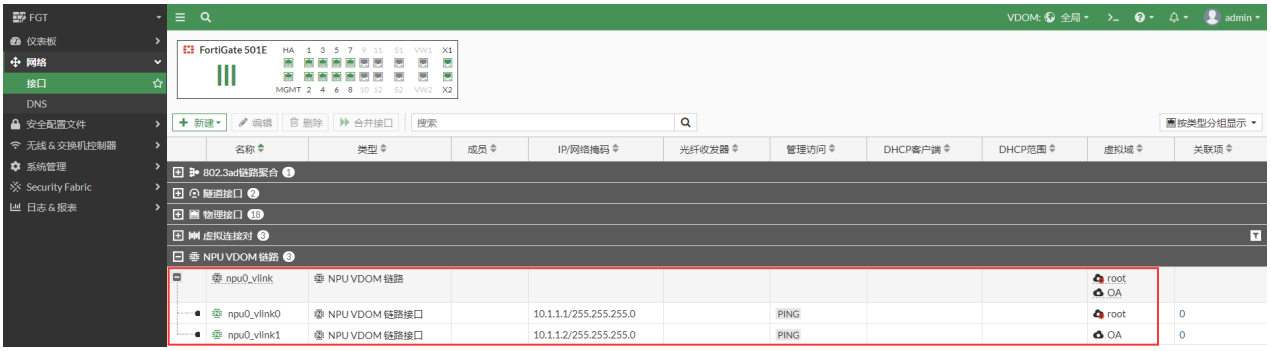
4. 进入全局，查看vdom索引。

```
#config global
# diagnose sys vd list  | grep name=root
name=root/root index=0 enabled fib_ver=49 rpdb_ver=2 use=162 rt_num=46 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0

# diagnose sys vd list  | grep name=OA
name=OA/OA index=3 enabled fib_ver=18 rpdb_ver=0 use=65 rt_num=7 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```

NPU link方式

NPU link方式和物理线路方式思路是一样的，只是接口不一样。

1. 将NPU link接口划入vdom，中高端设备支持NPU link接口，NPU link接口支持NP加速。可以使用NPU link接口进行vdom之间的通信。将npu0_vlink0划入 root vdom，将npu0_vlink1划入OA vdom，并配置IP地址。



2. 测试NPU link之间的连通性，进入root vdom，从root vdom ping OA vdom npu_vlink1接口地址。

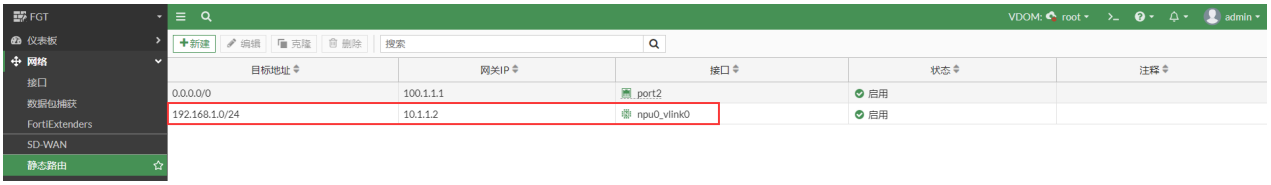
```
#config vdom
#edit root
# execute ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2): 56 data bytes
64 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3. 进入OA vdom，从OA vdom ping root vdom npu_vlink0接口地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
#config vdom
#edit OA
#execute ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1): 56 data bytes
64 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

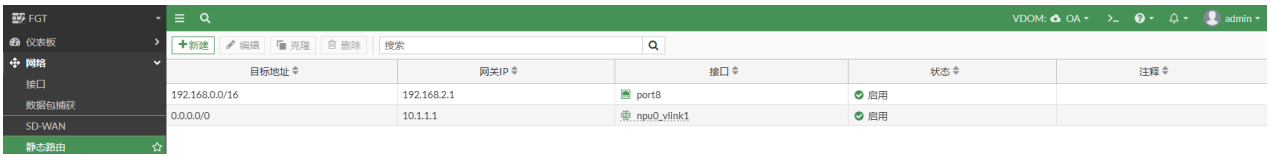
4. root vdom配置路由和策略：配置路由，配置root vdom到OA vdom子网的回程路由。



5. 配置策略，允许OA vdom到Internet的流量。



6. OA vdom配置路由和策略：配置路由，使OA vdom访问Internet的路由指向root vdom。



7. 配置策略，允许OA vdom到root vdom的流量。



VDOM间通信测试

1. PC2 ping 114.114.114.114。

```
PC2# ping 114.114.114.114
PING 114.114.114.114 (114.114.114.114) 56(84) bytes of data.
64 bytes from 114.114.114.114: icmp_seq=1 ttl=69 time=23.5 ms
64 bytes from 114.114.114.114: icmp_seq=2 ttl=85 time=23.2 ms
64 bytes from 114.114.114.114: icmp_seq=3 ttl=86 time=23.2 ms
64 bytes from 114.114.114.114: icmp_seq=4 ttl=73 time=23.2 ms
```

2. FortiGate抓包可以看出数据流穿过了npu_vlink0和npu_vlink1接口（在root vdom或者在OA vdom下抓包都是可以的）。

```
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
3.064987 port7 in 192.168.1.10 → 114.114.114.114: icmp: echo request
3.065007 npu0_vlink1 out 192.168.1.10 → 114.114.114.114: icmp: echo request
3.065012 npu0_vlink0 in 192.168.1.10 → 114.114.114.114: icmp: echo request
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
3.065024 port2 out 100.1.1.2 → 114.114.114.114: icmp: echo request
3.088172 port2 in 114.114.114.114 → 100.1.1.2: icmp: echo reply
3.088199 npu0_vlink0 out 114.114.114.114 → 192.168.1.10: icmp: echo reply
3.088205 npu0_vlink1 in 114.114.114.114 → 192.168.1.10: icmp: echo reply
3.088431 port7 out 114.114.114.114 → 192.168.1.10: icmp: echo reply
```

3. FortiGate查看会话，ping 流量在root vdom和OA vdom都产生了会话，在root vdom或者在OA vdom下查看会话都是可以的,vd=0是root vdom，vd=3是OA vdom。

```
# diagnose sys session list

session info: proto=1 proto_state=00 duration=3 expire=57 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=7→10/10→7 gwy=100.1.1.1/10.1.1.2
hook=post dir=org act=snat 192.168.1.10:2733→114.114.114.114:8(100.1.1.2:63149)
hook=pre dir=reply act=dnat 114.114.114.114:63149→100.1.1.2:0(192.168.1.10:2733)
misc=0 policy_id=4 pol_uuid_idx=638 auth_info=0 chk_client_info=0 vd=0
serial=00037b32 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×4000c00 ofld-O ofld-R
npu info: flag=0×81/0×91, offload=8/8, ips_offload=0/0, epid=150/142, ipid=132/150, vlan=0×0000/0×0000
vlifid=132/150, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/5

session info: proto=1 proto_state=00 duration=3 expire=57 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=15→8/8→15 gwy=10.1.1.1/192.168.1.10
hook=pre dir=org act=noop 192.168.1.10:2733→114.114.114.114:8(0.0.0.0:0)
hook=post dir=reply act=noop 114.114.114.114:2733→192.168.1.10:0(0.0.0.0:0)
misc=0 policy_id=2 pol_uuid_idx=637 auth_info=0 chk_client_info=0 vd=3
serial=00037b31 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×4000c00 ofld-O ofld-R
npu info: flag=0×91/0×81, offload=8/8, ips_offload=0/0, epid=132/160, ipid=160/142, vlan=0×0000/0×0000
vlifid=160/142, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/1
```

4. 进入全局，查看vdom索引。

```
# config global
# diagnose sys vd list  | grep name=root
name=root/root index=0 enabled fib_ver=49 rpdb_ver=2 use=162 rt_num=46 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0

# diagnose sys vd list  | grep name=OA
name=OA/OA index=3 enabled fib_ver=18 rpdb_ver=0 use=65 rt_num=7 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VDOM无法删除的处理方法

问题现象

删除VDOM时，有时会遇到删除了VDOM的所有关联对象后，仍无法删除空VDOM，如下VDOM1无法删除。

```
FortiGate # config vdom
FortiGate (vdom) # delete VDOM1
Domain VDOM1: used by interface, can not delete
Command fail. Return code -23
```

解决方法

1. 通过查VDOM相关对象，只有系统自建的对象的引用，但还是无法删除VDOM。

```
FortiGate (global) # diagnose sys cmdb refcnt show system.vdom.name VDOM1
entry used by table system.interface:name 'l2t.VDOM1'
entry used by table system.interface:name 'naf.VDOM1'
entry used by table system.interface:name 'ssl.VDOM1'
entry used by child table gui-dashboard:id '46' of entry used by child table gui-dashboard:id '47' of
entry used by child table gui-dashboard:id '48' of entry used by child table gui-dashboard:id '49' of
entry used by child table gui-dashboard:id '50' of entry used by child table gui-dashboard:id '51' of
entry used by child table gui-dashboard:id '52' of entry used by child table gui-dashboard:id '53' of
entry used by child table gui-dashboard:id '54' of entry used by child table gui-dashboard:id '55' of
entry used by child table gui-dashboard:id '56' of table system.admin:name 'admin'
entry used by child table gui-dashboard:id '22' of entry used by child table gui-dashboard:id '23' of
entry used by child table gui-dashboard:id '24' of entry used by child table gui-dashboard:id '25' of
entry used by child table gui-dashboard:id '26' of entry used by child table gui-dashboard:id '27' of
entry used by child table gui-dashboard:id '28' of entry used by child table gui-dashboard:id '29' of
entry used by child table gui-dashboard:id '30' of entry used by child table gui-dashboard:id '31' of
table system.admin:name 'nap_fw_admin'
entry used by table system.vdom-property:name 'VDOM1'
```

2. 通过如下命令可以重置VDOM的引用关系：

```
diagnose sys cmdb refcnt reset system.vdom.name VDOM1（VDOM名称）
```

3. 重置引用关系后，可以删除空VDOM VDOM1。

```
FortiGate # config vdom
FortiGate (vdom) # delete VDOM1
FortiGate (vdom) #
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA工作模式和配置要求

工作模式

Active-Passive (A-P) 模式

1. 集群中的所有防火墙必须工作在同一个模式下。可以对运行中的HA集群进行模式的修改，但会造成一定的延时，因为集群需要重新协商并选取新的主设备。A-P模式提供了备机保护。HA集群中由一台主设备，和一台以上的从设备组成。
2. 从设备与主设备一样连接到网络，但不处理任何的数据包，从设备处于备用状态。从设备会自动同步主设备的配置，并时刻监视主设备的运行状态。整个失效保护的过程是透明的，一旦主设备失效，从设备会自动接替其工作。如果设备的接口或链路出现故障，集群内会更新链路状态数据库，重新选举新的主设备。
3. 通常建议部署A-P模式。

Active-Active (A-A) 模式

1. A-A模式下会对占用资源较多的进程进行在各个设备中进行分担。需要处理协议识别、病毒扫描、ips、网页过滤、邮件过滤、数据防泄露、应用程序控制、VoIP内容扫描、协议保护（HTTP/HTTPS/FTP/IMAP/IMAPS/POP3/SMTP/SMTPS/IM/NNTP/SIP/SIMPLE/SCCP）、协议控制等。通过对如上内容的负载均担，A-A模式可以提供更高的UTM性能。安全策略中的终端控制，流控，用户认证功能，在A-A模式下没有什么提高效果。其他非UTM功能不会进行负载分担，还是由主设备进行处理。
2. A-A模式下，集群中的主设备负责对所有通信会话的处理，然后将部分负载分发到所有备机上。备机可以说是活动的，因为要处理UTM的相关会话。但备机只处理由主设备分配的数据，不会响应ARP等。其他方面A-A模式和A-P模式是相同的。
3. 除非单台设备的UTM性能不满足要求，通常建议部署A-P模式。

单机配置同步、单机会话同步模式（FGSP）

从5.0版本开始，全新NGFW下一代防火墙支持单机配置同步、会话同步功能，在一些应用场景中它可以代替双机HA功能，实现控制异步流量的目的。

注意在FGSP + 虚拟接口对（VWP）/透明模式 + UTM检测开启的部署环境下，只支持TCP流量，不支持UDP/ICMP协议流量。

HA配置要求

1. 进行HA配置， 硬件和软件版本需满足如下要求：
   - 防火墙硬件型号相同。
   - 同型号硬件要求硬件版本、内存容量、CPU 型号、硬盘容量等相同。
   - 相同的固件版本。
   - **HA的所有成员必须注册在同一FortiCloud账号下，否则HA虽然可以建立，但无法通过FortiGuard更新。**
2. 假如HA的两台FGT存在上述不一致的情况，那么会出现两端无法同步或无法更新等问题。

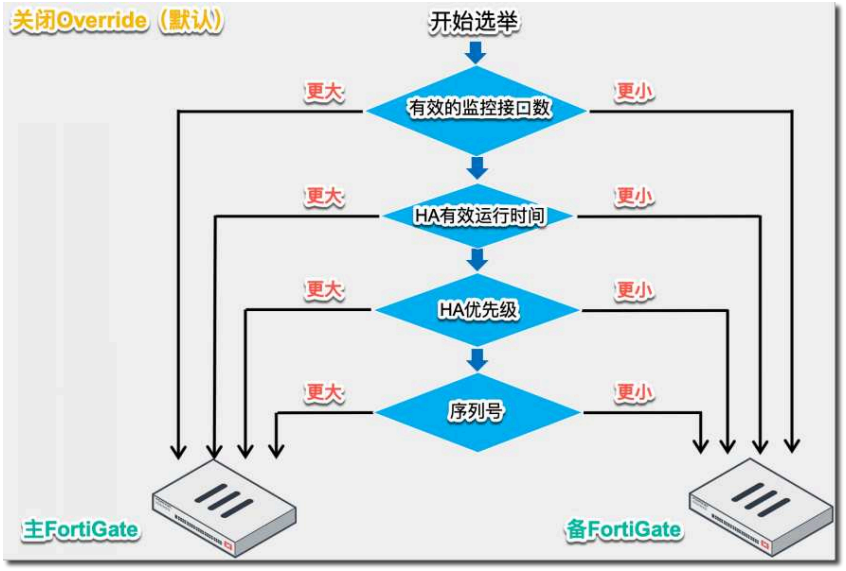
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA选取主设备的方法

主设备选举顺序

> **重要**
>
> FortiGate 6000/7000系列的选举规则与此不同，请参考如下文档：https://community.fortinet.com/t5/FortiGate/Technical-Tip-HA-Master-Election-Process-on-FortiGate-6000-7000/ta-p/193109 ↗

防火墙在组成集群到时候，需要选举一台主设备。主设备的选举根据下图所示进行，主设备之外的设备则成为从设备。主设备硬件故障或者被监控的端口链路故障都会重新进行主设备的选举。防火墙按照如下顺序进行比较，进行主设备的选举。这些因素分别是：监控端口中的有效接口数量，设备HA有效运行时间，HA优先级，设备的序列号。当Override关闭（默认配置）时，选举流程如下。



有效地被监控端口数量

1. 配置了需要被监控的业务端口之后，具有最多数量的有效监控端口的设备会成为主设备。通常情况下当一个HA集群建立起来的时候，所有到被监控的端口都是连接好并工作正常的，所以这个时候监控端口的数量不会成为影响到主设备选举的决定性因素。
2. 当一个被监控的端口出现故障或者链路失效，就会出发协商进行主设备选举，同样这些故障端口恢复到时候也会触发协商。当主设备的某个端口或链路出现故障，而其他设备相关端口和链路都是正常的就会从新选举出一个新的主设备。如port3、port4为被监控端口，当主设备的port3状态down，则其监控端口有效数量减少，从设备此时有效接口数量不变会成为主设备，继续工作。
3. 如果从设备上的监控端口出现故障，也会进行协商选举，选举结果是主设备不变，因为从设备上监控端口数量较少，自然不会成为主设备。如果不同设备的不同接口现了不同的端口故障，则每次都会进行一次选举。
4. **链路故障切换功能的目的就是要保证具有最多有效端口，最少故障点的那台设备成为主设备。**

```
FGT# config system ha
FGT(ha)# set monitor "port3" "port4"
FGT(ha)# end
```

HA有效运行时间

1. HA有效运行时间较长的设备会成为主设备。**请注意该有效运行时间并不是设备已上电的运行时间**，该时间参数是以从上一次设备出现故障以来所正常运行的时间，当然设备重新启动后该时间值也会复位为0。当集群内设备同时启动时，每台设备的HA有效运行时间是相同的。当设备上的监控端口发生设备故障时，HA有效运行时间复位，会低于集群内其他设备，与此同时因为拥有有效监控端口数少于其他设备。当出现故障的监控端口恢复时，虽然与未发生故障的设备具有相同的监控端口数，由于HA有效运行时间被复位后小于其他设备，也无法成为主设备。
2. 在大多数情况下，集群通过age参数减少了选举新的主设备所需要的时间，使集群更加稳定，因为选举过程有可能会中断数据传输。

> **重要**
>
> 设备重新启动后age复位为0，接口失效后设备age复位为0。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

集群启动时间差

有时集群内的某些主机需要更多的启动时间，HA有效启动时间的不同会导致一系列的问题出现，但不会影响集群的操作。为了确保后启动的主机可以成为主设备，FGCP协议默认为忽略5分钟的HA有效运行时间的差异，在大多数情况下该时间差的忽略可以帮助用户更容易实现自己预期的配置。在下列情况下HA有效运行时间差会造成不可以预料的结果：

1. 在升级固件版本的时候，默认情况下uninterruptable-upgrade enabled参数是开启的，集群会在所有的主机都升级完成后选举新的主设备。但由于主机之间升级后造成的HA有效运行时间的差异会小于5分钟，该差异会被忽略，其他的设备会成为新的主机。
2. 在测试失效切换的时候，由于反复切换，造成集群内主机HA有效运行时间的差小于5分钟。在通常情况下，失效切换后，失效的主机重新加入集群，他的HA有效运行时间要短于其他机，因而不会被选举为主设备。但如果失效的机器加入集群后他与其他主机之间的HA有效运行时间差小于5分钟，就有可能被选举为新的主机。

修改时间差

1. 用户可以通过如下命令来修改该参数。

```
FGT# config system ha
FGT(ha)# set ha-uptime-diff-margin 60
FGT(ha)# end
```

2. 这个命令设置时间差为60秒，运行范围为1-65535秒，默认为300秒。如果你不想等待5分钟的时间以便进行测试，你可以减少差值；在非中断升级防火墙OS的过程中减少差值，或者当集群内机器启动时间差加大的时候增加该差值。

HA优先级

1. 当具有相同监控端口数，且同时启动运行的防火墙，具有较高优先级的设备优先成为主设备。防火墙默认的优先级为128，可以通过配置优先级参数使某台设备优先成为主设备。该参数同主机名一样，不会在HA成员之间同步。

2. 当安装一组新的设备的时候，有效接口相同和HA有效运行时间相同，则优先级高会成为选主设备选举的因素。当一个台具有高优先级新设备加入一个现有的HA集群的时候，并不会触发从新协商，直到机群再次协商的时候该设备会由从设备被选举成为主设备。可以通过图形界面，或者如下的命令对优先级参数进行修改。

```
FGT# config system ha
FGT(ha)# set priority 200
FGT(ha)# end
```

3. 可以通过execute ha manage命令对机群中的从设备进行优先级的修改。修改该参数后进行重新选举。

SN序列号

当集群中的设备具相同的有效接口数，HA有效运行时间和优先级的时候，设备的序号会成为最后比较的参数，因为不同的设备具有不同的序列号，具有较大数值的SN number的会成为主设备。

Override参数

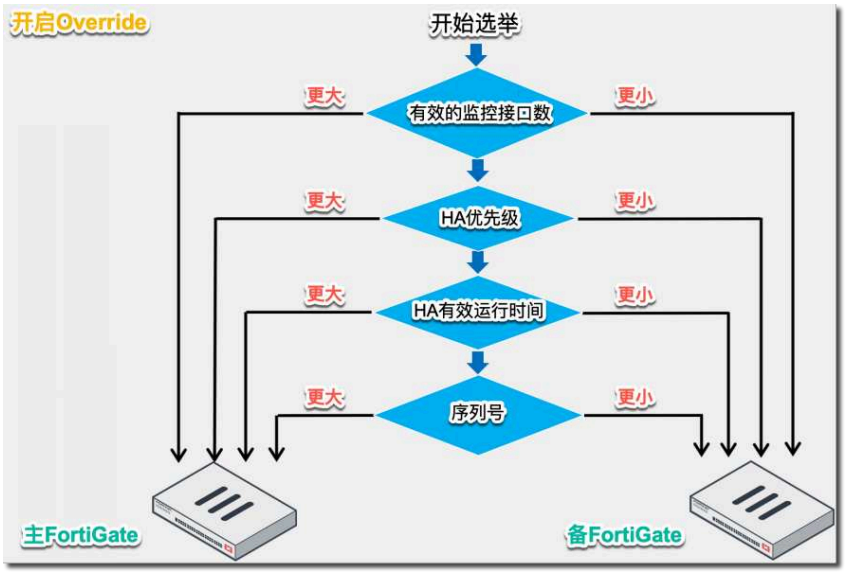
1. 在HA的配置中，override参数会影响到主设备的选举过程。

```
FGT# config system ha
FGT(ha)# set override disable/enable
FGT(ha)# end
```

2. 该参数默认需要通过CLI命令行进行配置，默认值为disable。

3. 当Override参数开启后，主设备的选举方法发生改变，优先级参数成为比HA有效运行时间更优先比较的参数。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



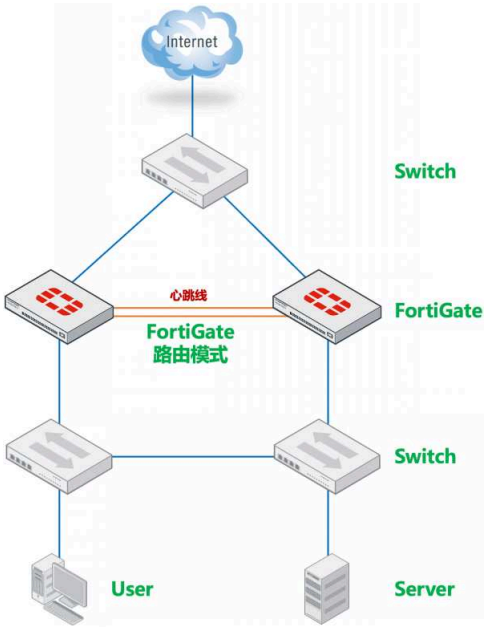
4. 如果一个设备的优先级较高，同时开启了overide选项，则在有效接口相同的情况下，该设备将始终作为主设备工作。由于该参数的这个特性，在实际操作中可能因为误操作造成设备配置的丢失，如下面的例子：

   - A设备优先级200，override enable，B设备优先级100，override disable。
   - A设备故障，B设备成为主设备。
   - 更换新的A设备，新设配仅设置HA参数，优先级200，override enable，但未做任何的业务配置。
   - 新设备所有线路连接好后开启设备，由于新的设备和B设备具有相同的有效接口数量，同时具有较高优先级，选举成主设备。
   - 原来主设备B设备的配置文件被同步成为新设备的空配置，数据丢失。
   - 规避方法：检查override是否开启，检查优先级参数，或者新的设备接入的时候，不连接任何监控端口的线缆，使其具有少的有效端口数。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA典型基础配置（FGCP）

网络拓扑



配置建议

1. 进行HA环境下更换设备前，进行配置备份，防止操作失误而造成的配置丢失。
2. 建议配置两条以上的心跳线缆，防止单心跳故障造成HA机群崩溃，使用独立的心跳接口，尽量避免与业务口混用。
3. 优先使用光纤接口。
4. 开启会话同步：set session-pickup enable（默认关闭）或者在WEB上启用“会话交接”。
5. 谨慎使用override功能。开启override后设备选举过程中HA优先级参数高于设备运行时间参数，可能造成期望成为备机的设备被选举为主设备，造成反向同步配置信息。
6. 在同一个二层环境里面有多个HA Cluster时，注意Group ID不能相同，否则会产生MAC地址冲突。
7. 选择正确的监控端口和心跳端口，在开启vdom虚拟cluster时候，每个cluster需要单独配置。
8. 如果开启ping server功能，则需要再HA配置中添加相应的配置命令。
9. 建议将与防火墙相连的交换机接口配置为stp portfast模式，发生接口Up/Down切换时，交换机的接口可立刻进入转发状态，而不需要stp状态进行侦听、学习、转发等延迟步骤后接口才转发数据。

配置要点

- 进行HA 的配置，硬件和软件版本需满足如下要求：
  - 防火墙硬件型号相同、同型号硬件需要为相同的硬件版本。
  - 内存容量、CPU 型号、硬盘容量等相同。
  - 相同的软件版本版本。
- 配置设备1的HA。
- 配置设备2的HA。
- 组建HA。
- 查看HA集群。

配置步骤

1. 配置主设备，进入菜单系统管理→高可用性，模式选择“主动-被动”模式，优先级配置200（主机高于从机）；组名/密码自定义；勾选“启用会话交接”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 模式：单机模式、主动-被动、主动-主动。在大多数网络中会选择主动-被动，即主设备进行业务处理，备机处于备份状态，当主设备发生设备故障或者接口链路故障后，则由备机继续处理业务。
- 设备优先级：优先级高的设备，优先被选为主设备。
- 组ID：在同一个二层环境里面有多个HA Cluster时，注意Group ID不能相同，否则会产生MAC地址冲突。
- 组名和密码：自行定义即可，做HA的两台机器需要配置相同的参数。
- 启用会话交接：建议启用。主墙和备墙之间实时进行会话信息的同步，当发生HA切换到时候，备墙上有同样的会话信息会对原来的会话进行处理，不会产生会话中断。
- HA的接口配置：
  - 端口监控：HA监控的接口，作为HA切换依据之一；本案例中监控port2（外网口）和port4（内网口）。业务端口需要被防火墙监控，当端口出现故障时会进行切换，具有数量多的有效监控端口的设备会作为主墙处理数据。
  - 心跳接口：启用两个心跳接口：port7、port8。用于配置同步，会话同步，对方存活心跳检测等，为了集群的稳定建议配置 2 条或以上的线条线。在有多条心跳线路的情况下，心跳端口的 心跳优先级 决定了优先使用那条线路同步心跳（优先级高的端口连接的线路优先使用）

2. 配置从设备，除了优先级不同外（优先级低于主机），其他参数均与设备1相同。

3. 组建HA，连接心跳线，FGT主的port7、port8，连接到 FGT从的port7、port8。

4. 防火墙开始协商建立HA集群，此时会暂时失去和防火墙到连接，这是因为在HA协商过程中会改变防火墙接口到MAC地址。可以通过更新电脑的arp表来恢复连接，Windows下的命令为arp -d。

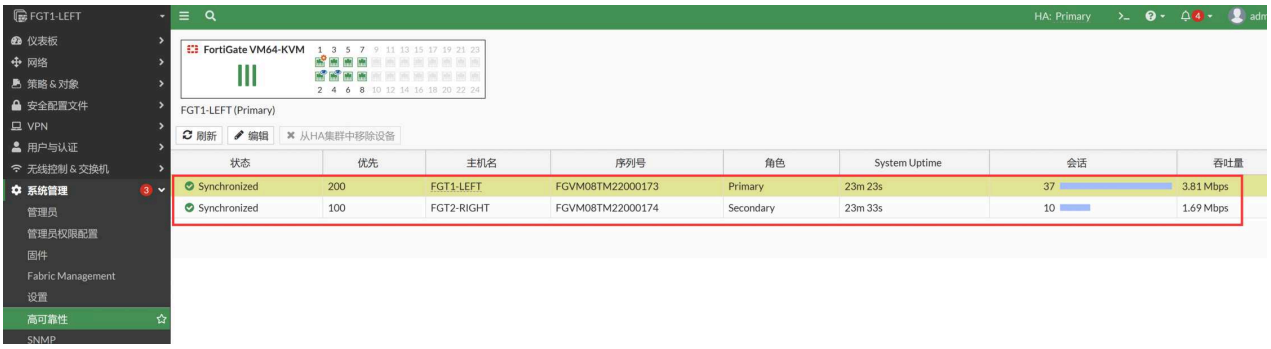
5. 连接业务口链路。

6. 组建好HA后，两台防火墙配置同步，具有相同的配置，通过访问主防火墙来进行业务配置，如IP地址，策略等，更新的配置会自动同步。

> **重要**
>
> HA建立完成后，只能通过主机进行访问、管理主机。如果需要登陆备机管理，请参考HA的网管介绍 ↗章节。

结果验证

1. 进入菜单系统管理→高可用性，就可以看到HA的建立情况。



2. 在主设备的CLI下查看HA状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FGT1-LEFT # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-KVM
Mode: HA A-P
Group: 77
Debug: 0
Cluster Uptime: 0 days 0:23:56
Cluster state change time: 2023-01-04 17:01:52
Primary selected using:
    <2023/01/04 17:01:52> FGVM08TM22000173 is selected as the primary because its override priority is larger than
peer member FGVM08TM22000174.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
Configuration Status:
    FGVM08TM22000173(updated 3 seconds ago): in-sync
    FGVM08TM22000174(updated 4 seconds ago): in-sync
System Usage stats:
    FGVM08TM22000173(updated 3 seconds ago):
        sessions=9, average-cpu-user/nice/system/idle=0%/0%/0%/99%, memory=33%
    FGVM08TM22000174(updated 4 seconds ago):
        sessions=9, average-cpu-user/nice/system/idle=0%/0%/0%/99%, memory=33%
HBDEV stats:
    FGVM08TM22000173(updated 3 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=4230515/13569/0/0, tx=5053711/11897/0/0
        port8: physical/10000full, up, rx-bytes/packets/dropped/errors=3215271/7193/0/0, tx=3246636/7167/0/0
    FGVM08TM22000174(updated 4 seconds ago):
        port7: physical/10000full, up, rx-bytes/packets/dropped/errors=5035221/11873/0/0, tx=4224168/13553/0/0
        port8: physical/10000full, up, rx-bytes/packets/dropped/errors=3244371/7162/0/0, tx=3212142/7186/0/0
MONDEV stats:
    FGVM08TM22000173(updated 3 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=263241/3765/0/0, tx=46197/492/0/0
        port4: physical/10000full, up, rx-bytes/packets/dropped/errors=70859/610/0/0, tx=15210/114/0/0
    FGVM08TM22000174(updated 4 seconds ago):
        port2: physical/10000full, up, rx-bytes/packets/dropped/errors=291104/4091/0/0, tx=14698/104/0/0
        port4: physical/10000full, up, rx-bytes/packets/dropped/errors=69842/597/0/0, tx=14886/106/0/0
Primary     : FGT1-LEFT       , FGVM08TM22000173, HA cluster index = 1
Secondary   : FGT2-RIGHT      , FGVM08TM22000174, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM08TM22000173, HA operating index = 0
Secondary: FGVM08TM22000174, HA operating index = 1
```

```bash
FGT1-LEFT # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:51672 b:21448340
        traffic.total = s:0 p:51674 b:21448444
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=77 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM22000173:      Primary, serialno_prio=1, usr_priority=200, hostname=FGT1-LEFT
FGVM08TM22000174:    Secondary, serialno_prio=0, usr_priority=100, hostname=FGT2-RIGHT

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0:
FGVM08TM22000173:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM22000174:    Secondary, ha_prio/o_ha_prio=1/1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

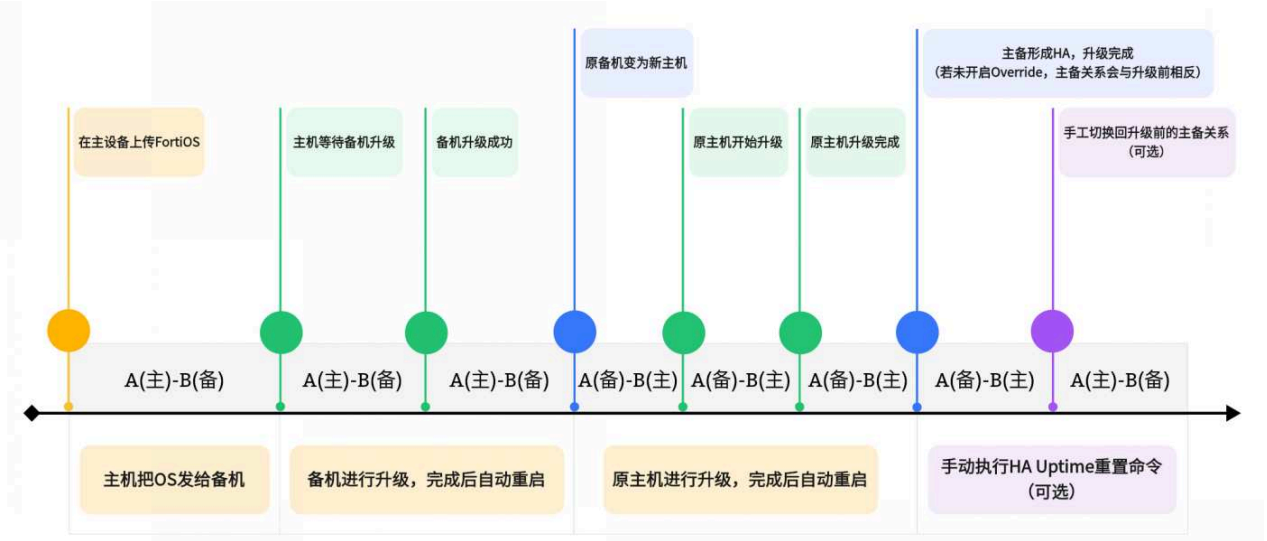
HA-Cluster不间断升级

重要

在HA环境下降级，没有不间断的机制，降级时HA所有成员会同时重启，请务必注意。 降级建议使用系统管理→固件与配置管理→固件切换 ↗中介绍的方法。

不间断升级介绍

1. “HA不间断升级”故名思义就是说在HA升级过程中，HA-cluster中的成员会依次进行升级，从而保证了业务在升级过程中不中断。
2. 上传FortiOS的方法分为Web界面上传和CLI上传，本文介绍以Web界面上传的方式，两台设备升级完成需要15分钟左右，过程如下（未开启Override）：



升级过程

1. 在主机Web界面上点击升级按钮。
2. 主机把FortiOS发给备机，备机准备并开始升级，然后自动重启，此过程需要5分钟（或更长时间），请耐心等待。
3. 备机升级完成，并切换成主机。
4. 主机观察到备机升级成功并切换为新的主机后，开始准备升级，此过程需要5分钟（或更长时间），请耐心等待。
5. 一旦准备完成，主机（此时为备）自动重启加载升级后OS，重启约2分钟。
6. 主机（此时为备）重启后，形成HA 。主机从原来的备同步配置（外部配置和内部配置），约1~3分钟。
7. 此时，HA重新建立，如果HA没有开启Override，主备关系与升级前相反，如果想要主备关系与升级前一致，在新的主机（原备机）手工执行diagnose sys ha reset-uptime命令切换回升级前的主备关系（此命令需要原主机升级完成启动5分钟后，在新主机上执行才会进行主备切换）。

操作建议

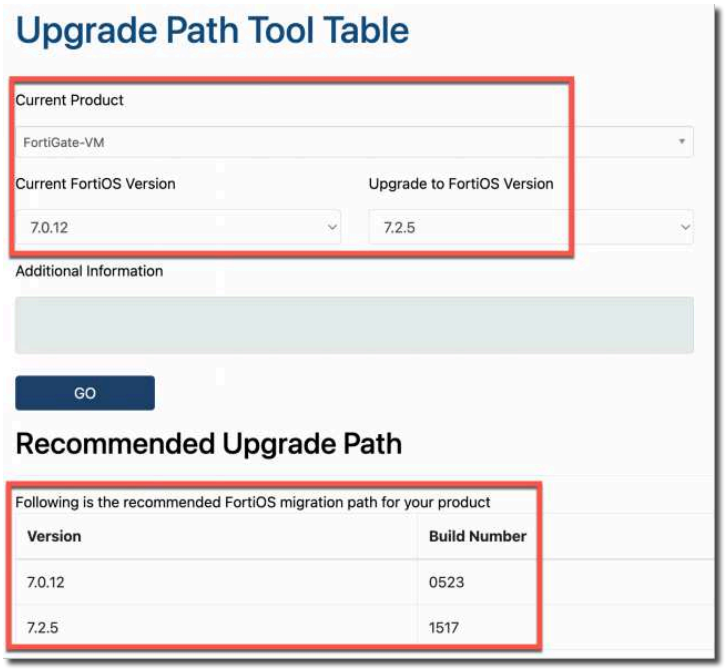
1. 操作前下载并阅读 Release 文档和升级说明文档，做到注意事项心中有数。可以参考官方文档：https://docs.fortinet.com/document/fortigate/7.2.99/fortios-release-notes/ ↗ （进入后找到对应版本的Release Note，此链接为目前7.2.X最新版本的Release Note）
2. 升级前后备份设备配置。
3. 升级固件必须遵循升级路径，参考系统管理→固件与配置管理→固件版本管理→升级路径 ↗章节。
4. 接入Console在主设备上，记录log观察升级过程，做到心中有数。 有问题也可以反馈厂商。
5. 耐心等待，主备机升级的时间都会比较长。

操作步骤

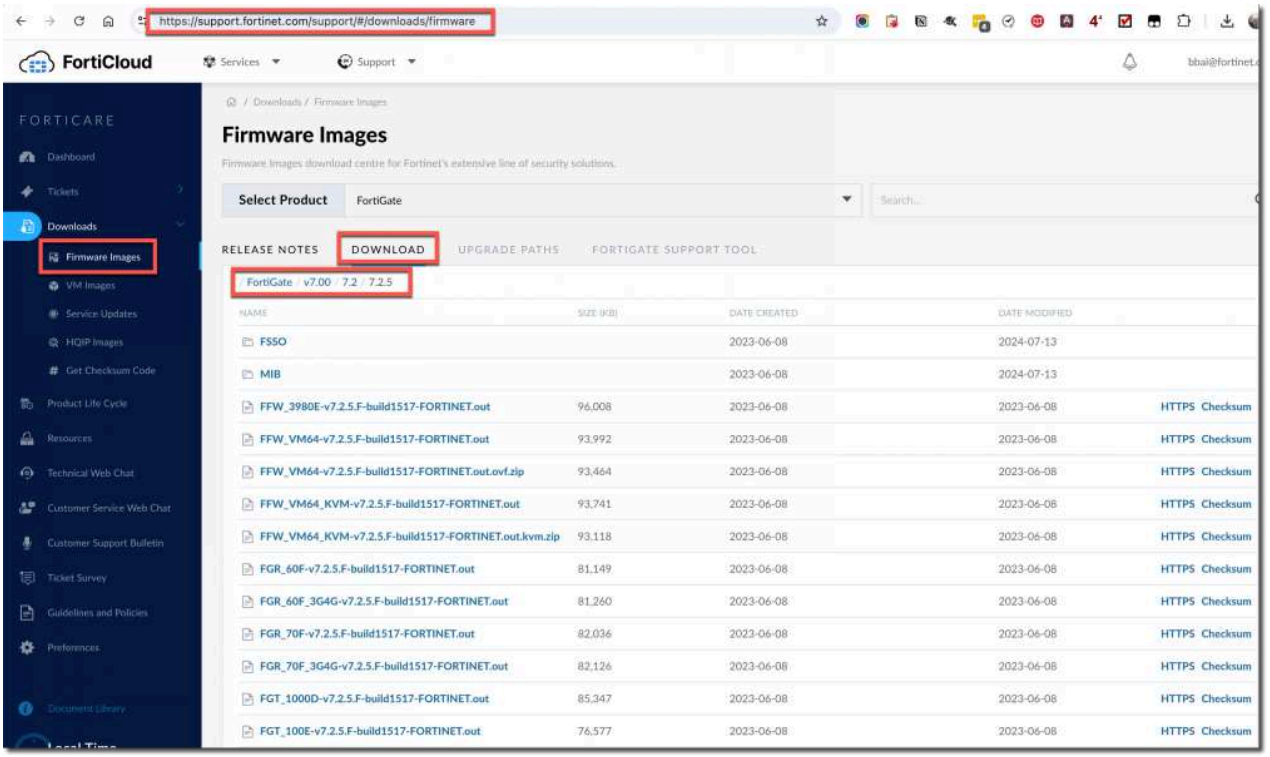
1. 分别备份主备设备的配置文件，参考系统管理→固件与配置管理→配置管理→配置备份及恢复 ↗章节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 举例：FortiGate-VM从FortiOS 7.0.12升级到FortiOS 7.2.5，从https://docs.fortinet.com/upgrade-tool ↗ 得知直接升级即可，无需升级多次版本。

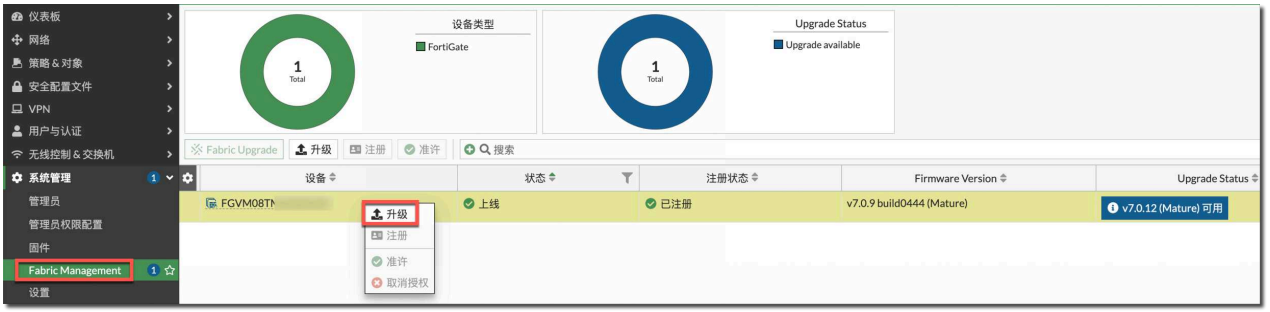


3. 从https://support.fortinet.com/support/#/downloads/firmware ↗ 下载7.2.5版本对应产品的文件到本地，以便通过GUI导入软件版本进行升级。

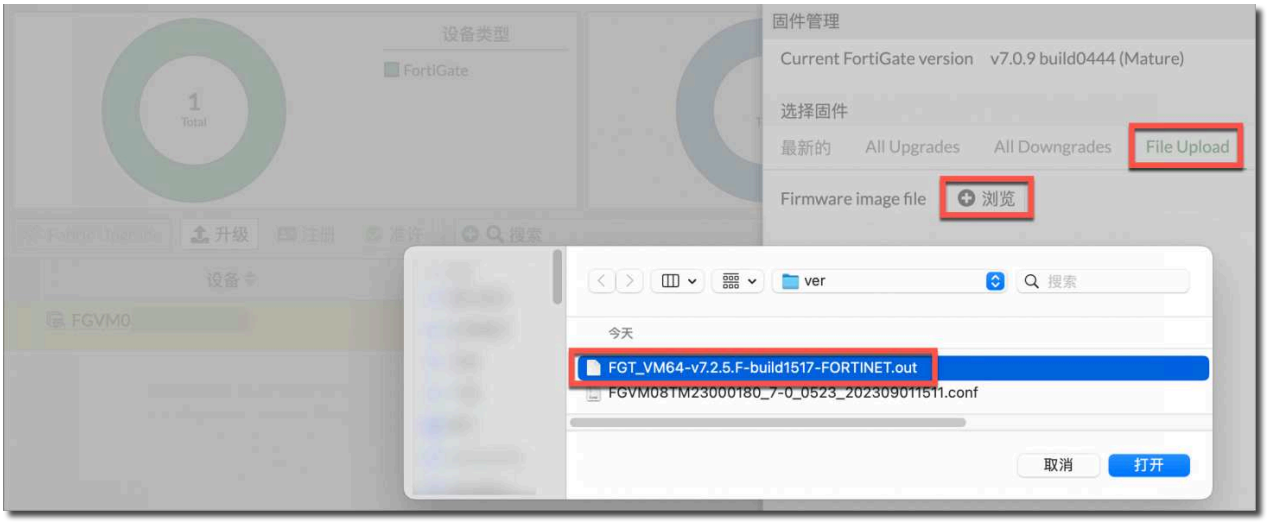


4. 准备工作做完，正式开始升级，在主设备进入系统管理→Fabric管理页面（7.4为Firmware & Registration页面），右键点击要升级的设备，选择升级按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 在弹出的页面中，选择文件上传，并浏览选择需要升级的版本。



6. 点击确认并备份配置，会在升级前下载设备当前的配置文件到本地（只有当前主机的）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





7. 此时FortiOS将先传给备机，业务还是运行在主机上，等备机重启后将接管主机的业务，然后主机再重启升级，此过程业务是不中断的。



Console记录

1. 耐心等待与观察Console输出信息，做到心中有数。以下为升级过程Left设备Consloe打印信息，其实管理员并不需要做什么，只需要请注意阅读并理解，做到心中有数，万一出现故障可以知道大概是哪一步的问题。

```
FGT1-LEFT # Wait for HA to be primary of all clusters ...     //主设备发送FortiOS到备设备
Send image to HA secondary.
..Wait for secondary to restart ...    //备机先升级，升级重启约5分钟，请耐心等待
Wait for first secondary to become new primary ..     //备机升级并重启完毕后，主机会先等待备机变成新的主机，以便业务被备机先接管
Firmware upgrade in progress ...     //当备机成为新主机之后，主机将准备升级
Done.    //主机准备升级结束，开始正式升级主设备，升级过程约5分钟，请耐心等待
The system is going down NOW !!
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Please stand by while rebooting the system.
Restarting system.
SeaBIOS (version rel-1.12.1-0-ga5cab58e9a3f-prebuilt.qemu.org)
Machine UUID 934483a5-b727-447c-b98c-9cb5dd2209fb
Loading flatkc ... ok
Loading /rootfs.gz ... ok
System is starting ...
The config file may contain errors.
Please see details by the command 'diagnose debug config-error-log read'.
Serial number is FGVM08TM22000173
FGT1-LEFT login: admin
Password:
Welcome!
FGT1-LEFT # get system status
Version: FortiGate-VM64-KVM v7.2.5,build1517,230606 (GA.F)    //原主机后升级完毕
Security Level: 1
Firmware Signature: certified
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
IoT-Detect: 0.00000(2022-08-17 17:31)
Serial-Number: FGVM08TM23000180
License Status: Valid
License Expiration Date: 2024-01-19
VM Resources: 2 CPU/8 allowed, 3946 MB RAM
Log hard disk: Available
Hostname: FGVM08TM23000180
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, secondary    //升级完毕之后状态是主还是备将视具体情况而定：主防火墙和备防火墙重启完成时间相差五分钟以内，则后面重启的主机（优先级高的FGT）将会主动抢占为主设备，如果二者升级重启时间相差超过5分钟，则后重启的主设备将会处于备的状态，不会抢占回主的状态
Cluster uptime: 2 hours, 15 minutes, 17 seconds
Cluster state change time: 2023-09-01 05:16:51
Branch point: 1517
Release Version Information: GA
FortiOS x86-64: Yes
System time: Fri Sep  1 15:41:51 2023
Last reboot reason: warm reboot
```

2. RIGHT防火墙的Console记录。

```
FGT2-RIGHT # geGet image from ha primary OK.    //主机发送FortiOS到备机上
Verifying the integrity of the firmware image ...
Check image OK.
Please wait for system to restart.    //备机先开始升级并重启，因此业务在主机上运行
Firmware upgrade in progress ...
Done.
The system is going down NOW !!
Please stand by while rebooting the system.
Restarting system.
SeaBIOS (version rel-1.12.1-0-ga5cab58e9a3f-prebuilt.qemu.org)
Machine UUID fe581bd9-2eb0-4115-896a-dd50f521d0ee
Booting from Hard Disk ...
SYSLINUX 6.04 EDD 6.04-pre1 Copyright (C) 1994-2015 H. Peter Anvin et al
Loading flatkc ... ok
Loading /rootfs.gz ... ok
System is starting ...
The config file may contain errors.
Please see details by the command 'diagnose debug config-error-log read'.
Serial number is FGVM08TM22000174
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FGT2-RIGHT login: admin
Password:
Welcome!
FGT2-RIGHT # get system status
Version: FortiGate-VM64-KVM v7.2.5,build1513,230606 (GA.F)    //原备机升级成功
Security Level: 1
Firmware Signature: certified
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
IoT-Detect: 0.00000(2022-08-17 17:31)
Serial-Number: FGVM08TM23000180
License Status: Valid
License Expiration Date: 2024-01-19
VM Resources: 2 CPU/8 allowed, 3946 MB RAM
Log hard disk: Available
Hostname: FGVM08TM23000180
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, primary    //升级完毕之后状态是主还是备将视具体情况而定：主防火墙和备防火墙重启完成时间相差五分钟以内，则后面重启的主机（优先级高的FGT）将会主动抢占为主设备，如果二者升级重启时间相差超过5分钟，则后重启的主设备将会处于备的状态，不会抢占回主的状态
Cluster uptime: 2 hours, 16 minutes, 28 seconds
Cluster state change time: 2023-09-01 05:16:51
Branch point: 1517
Release Version Information: GA
FortiOS x86-64: Yes
System time: Fri Sep  1 15:41:51 2023
Last reboot reason: warm reboot
```

3. 手工切换HA状态，此步骤不是必要，升级完毕之后状态是主还是备将视具体情况而定：
   - 情况1：主防火墙和备防火墙重启完成时间相差五分钟以内，则后面重启的主机（优先级高的FGT）将会主动抢占为主设备。如果是这种情况，则不需要任何的额外切换动作。
   - 情况2：如果二者升级重启时间相差超过5分钟，则后重启的主设备将会处于备的状态，不会抢占回主的状态。这个时候才需要命令行进行强制的HA切换一下，让HA状态恢复到升级之前的主备状态。
4. 如果有以上第2种情况，HA-Cluster升级完毕之后，备机成了新的主，而旧的主机成为了备，并且想要将HA的状态切换到升级之前的状态，则只需要重启完成5分钟后在备机（新的主机）上敲一条命令即可完成主备切换。

```
FGT2-RIGHT # diagnose sys ha reset-uptime    //此命令会Reset当前设备的HA时间，以便重新进行HA的选举。reset-uptime相当于把备机的HA运行时间清0，这样运行时间长且优先级高的主设备，一定会重新选举为主的
```

5. 再观察HA的状态是否是我们所需要的状态，以下这三个命令都可以看到HA的选举结果和HA状态。

```
# diagnose sys ha status
# get system status
# get system ha status
```

6. 升级后检查是否有重要配置丢失。

```
diagnose debug  config-error-log read
//不丢路由、接口地址、服务对象、防火墙策略、VPN这些，一般问题不大。丢一些默认的配置可能是因为新版本做了功能变
```

7. 检查配置是否同步，查看主备防火墙的配置HA checksum，正常来说二者的配置checksum是一致的，如果状态不同步，可以参考HA双机热备→HA常见问题→HA同步机制和故障诊断↗章节排查（如果升级路径有多个版本，建议在每个版本升级完成，等待HA同步后，再升级下个版本）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FGT1-LEFT # diagnose sys ha checksum show
is_manage_primary()=0, is_root_primary()=0
debugzone
global: a5 20 2d 71 a0 22 13 92 59 82 45 6d 43 b8 fb d9
root: d0 f3 bd a2 b5 f8 df 39 7c 6c 25 c9 91 e1 b9 99
all: b9 3b b3 36 86 d7 ff 08 1d e8 ce 48 e4 85 85 48
checksum
global: a5 20 2d 71 a0 22 13 92 59 82 45 6d 43 b8 fb d9
root: d0 f3 bd a2 b5 f8 df 39 7c 6c 25 c9 91 e1 b9 99
all: b9 3b b3 36 86 d7 ff 08 1d e8 ce 48 e4 85 85 48

FGT2-RIGHT # diagnose sys ha checksum show
is_manage_primary()=0, is_root_primary()=0
debugzone
global: a5 20 2d 71 a0 22 13 92 59 82 45 6d 43 b8 fb d9
root: d0 f3 bd a2 b5 f8 df 39 7c 6c 25 c9 91 e1 b9 99
all: b9 3b b3 36 86 d7 ff 08 1d e8 ce 48 e4 85 85 48
checksum
global: a5 20 2d 71 a0 22 13 92 59 82 45 6d 43 b8 fb d9
root: d0 f3 bd a2 b5 f8 df 39 7c 6c 25 c9 91 e1 b9 99
all: b9 3b b3 36 86 d7 ff 08 1d e8 ce 48 e4 85 85 48
```

8. HA升级完毕，升级完毕之后查看HA的状态、测试业务、最好再次备份一份软件版本升级之后的配置文件。

关闭不间断升级（谨慎使用）

某些特殊情况下，用户需要关闭不间断升级功能，通过如下命令可以关闭不间断升级功能。

> **重要**
>
> 关闭HA的不间断升级功能，执行升级操作（上传版本文件）后，HA的所有成员设备会同时重启升级，业务会发生中断！请务必谨慎使用此命令！！！

```
config system ha
    set uninterruptible-upgrade disable
end

7.4.1版本后，命令变为：
config system ha
    set upgrade-mode simultaneous
end
```

具体解释可参考官方文档：https://docs.fortinet.com/document/fortigate/7.0.99/administration-guide/247944/upgrading-fortigates-in-an-ha-cluster ↗ 中的“Interrupted upgrade”部分。

HA切换测试注意事项

1. 部分用户在做完HA升级或上线后，会做HA的切换测试，上边的步骤中已经介绍，通常建议通过命令“diagnose sys ha reset-uptime”进行HA主备的切换（默认情况下需要主备的HA uptime间隔超过5分钟）。
2. 当需要通过HA主设备监控接口Down的方式测试触发HA切换时，尽量使用手工拔线的方式，切记不要直接在页面将主设备监控接口Shutdown，因为HA备机会同步该配置，随后也将监控接口Shutdown，这会导致HA发生主备切换后再发生一次主备切换。
3. 如果不方便到机房手工拔线，可以使用如下CLI将主机的监控接口物理性Down掉，该操作仅本机生效，不会同步到备机。这样就可以模拟手工拔线相同的效果。

```
fnsysctl ifconfig port1 down
```

4. HA切换测试完成后，记得将原主机HA监控接口UP。

```
fnsysctl ifconfig port1 up
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA共享单一License

重要

- 此功能在FortiOS 7.2.9、7.4.6、7.6.1及更高版本支持。
- 在FortiOS 7.2.12和7.4.9及之后版本上，支持把FortiToken绑定到vSN。之前的版本无法将FortiToken绑定在vSN上。

功能介绍

FortiGate A-P模式的HA现在支持为以下型号的HA成员共享单个FortiGuard服务License：

- 40F-HA及衍生型号
- 60F-HA及衍生型号
- 70F-HA及衍生型号
- 80F-HA及衍生型号
- 100F-HA及衍生型号（**100F-HA在7.2.12、7.4.8、7.6.3及更高版本支持**）

在这之前，客户需要为HA成员的每台设备单独购买License，如果两台设备的服务到期时间不一致，会以较短的那台为准。

现在，当客户购买两台FortiGate设备组成A-P HA集群时（如2 x FortiGate-40F-HA），以上型号可以共享一个FortiGuard服务License（如1x FC-10-0040F-809-02-DD），无需为每台设备单独购买，可共享的服务只支持如下三种：

- Enterprise Protection
- Unified Threat Protection (UTP)
- Advanced Threat Protection (ATP)

两个FortiGate序列号将在FortiCare中关联，FortiCare系统会将两台设备的序列号绑定，生成一个虚拟序列号（vSN），上述服务将注册至这个vSN，而非单个设备的序列号。

实施步骤

重要

HA vSN集群的建立方式有所限制：

- 仅支持HA A-P模式，其他部署模式（如Active-Active）不适用。
- FortiGate-HA（如FortiGate-40F-HA）是单独的SKU，您必须购买带有“HA”后缀的特定型号设备（如2 * FortiGate-40F-HA，这种设备是成对出售的），才能组成HA vSN集群。
- 不带“HA”后缀的普通型号设备（如FortiGate-40F）无法组成HA vSN集群。即使您之前已经购买了两台不带“HA”后缀的设备，它们也无法组成HA vSN，这种设备必须单独购买服务。

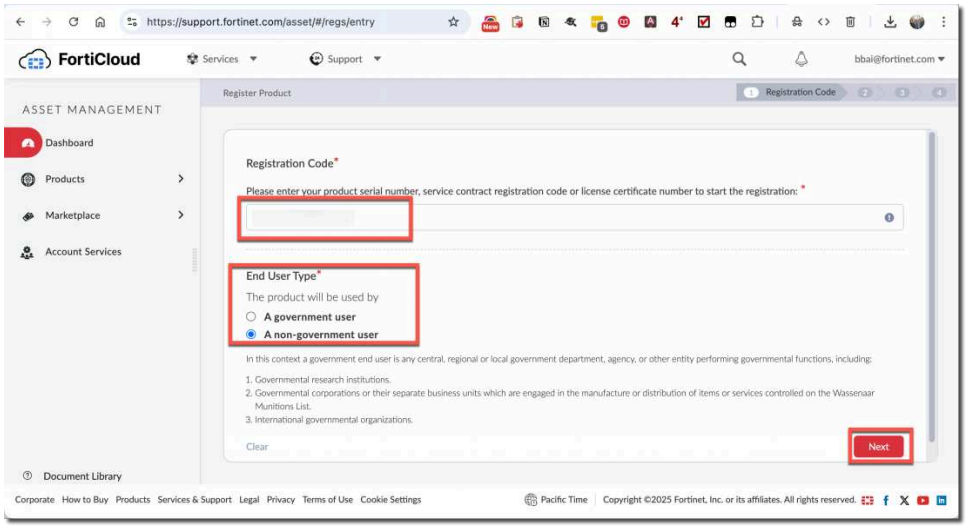
注册HA设备

1. 访问 https://support.fortinet.com/asset/#/dashboard ↗ 并使用要注册设备的FortiCloud账号登录。

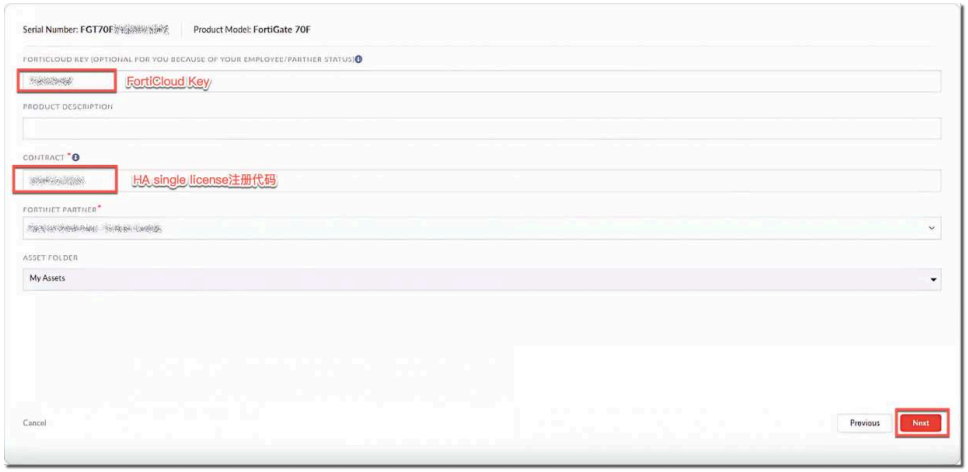
2. 点击页面上的“Register Now”按钮。

3. 在“Registration Code”中，输入一对FortiGate-HA其中任意一台（Device 1）的序列号，选择“End User Type”，然后点击“Next”。

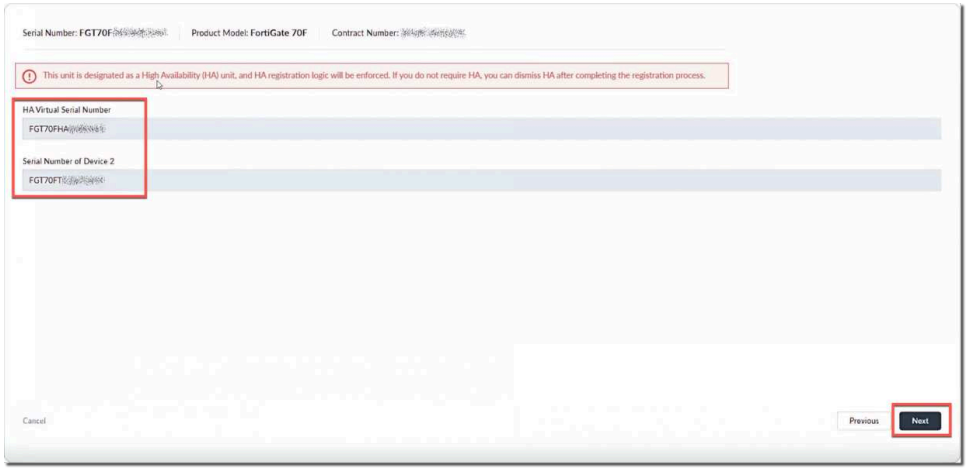
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 填入“FortiCloud Key”（从机身粘贴的标签上获取），HA single license的注册代码（从购买的HA license PDF文件中获取），然后点击“Next”。

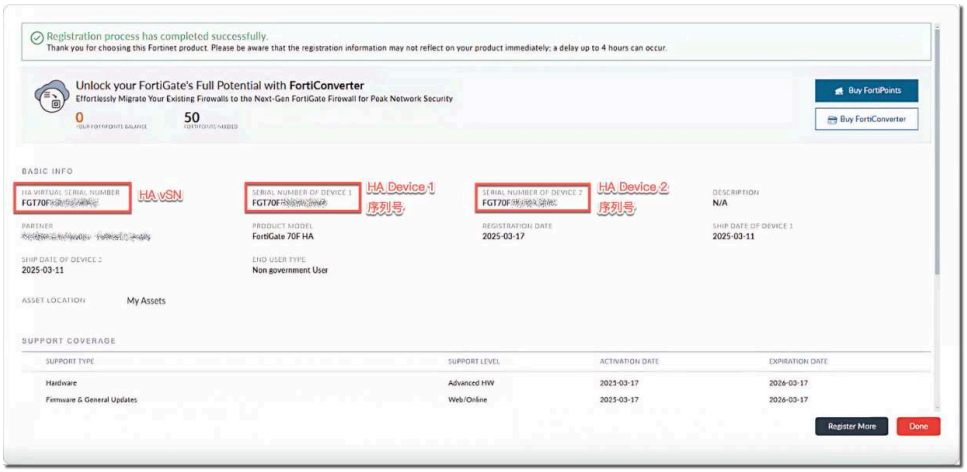


5. 随后会生成HA的vSN，并显示HA另一台设备（Device 2）的序列号。

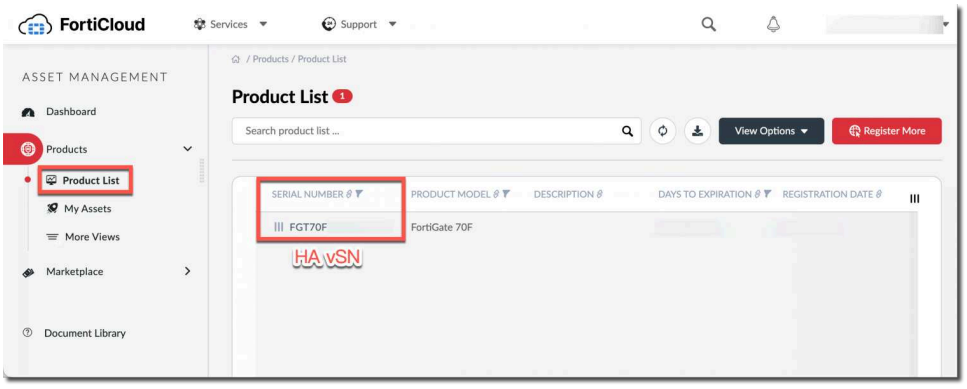


6. 注册完成，显示HA的vSN和两台成员设备的真实序列号。

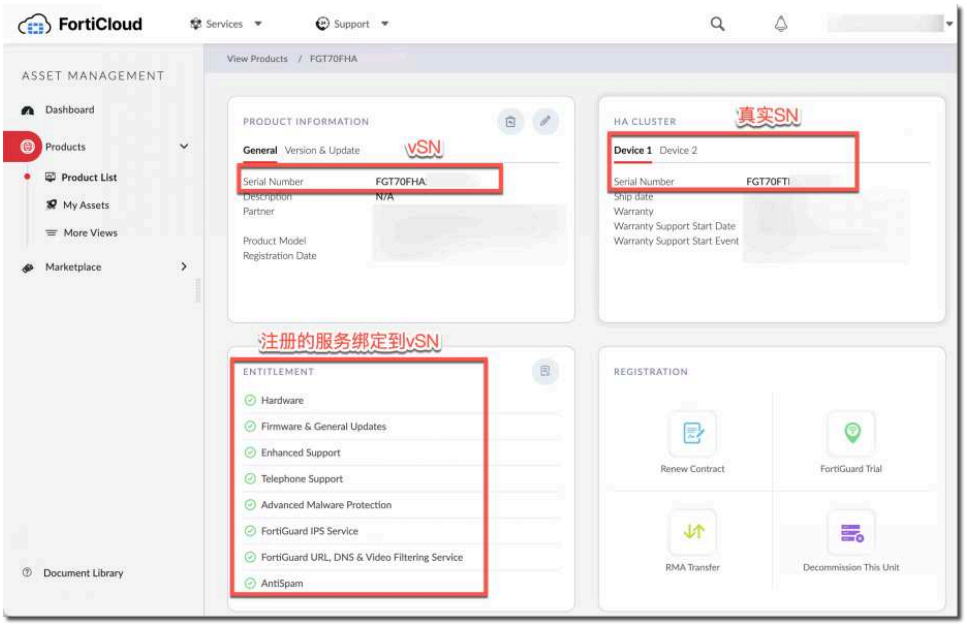
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 注册完成后，vSN会出现在设备列表中。



8. 订阅的服务授权（如UTP/ATP）绑定到了vSN，而非成员设备。



HA设备配置

1. 将两台设备组成A-P模式的HA，参考“HA双机热备→HA典型基础配置（FGCP）↗”。

2. 在HA任意一台设备的CLI下敲入如下命令（主备机会同步该配置）：

```bash
config system ha
    set mode a-p    //仅适用于A-P HA集群，其他部署模式（Active-Active集群）不适用//
    set logical-sn enable    //必须启用以支持共享许可证//
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. HA与FortiGuard同步完成后，通过如下CLI可以看到HA的`logical serial number`，这就是HA的vSN。

```bash
FortiGate-70F # get system ha status
HA Health Status: OK
Model: FortiGate-80F
Mode: HA A-P
Group Name: Branch1-HA
Group ID: 100
Debug: 0
Cluster Uptime: 0 days 2h:33m:2s
......
vcluster 1: work 169.254.0.1
Primary: FGT70FTK22023xxx, HA operating index = 0
Secondary: FGT70FTK20000xxx, HA operating index = 1
Logical Serial Number: FGT70FHA24090xxx

FortiGate-70F # diagnose system ha dump-by debug-zone
            HA information.
is_manage_primary=1,manage_vd=root,ip=169.254.0.1,num=2,nvcluster=1,jiffies=938038.
logical serial number is FGT70FHA24090xxx,
local serial number is FGT70FTK22023xxx,
member's serial number is FGT70FTK20000xxx
```

4. 如果HA未启用`logical-sn`，License将会无法更新成功，`diagnose debug application update -1`会有以下报错。

```bash
upd_status_extract_contract_info[1309]-pending registration(1) support acct() company() industry()
upd_status_extract_contract_info[1317]-valid contract percent=11%

installUpdObjRest[846]-Step 9:Delete backup /tmp/update.backup
upd_install_pkg[1404]-FSCI000(contract) installed successfully
upd_pkg_get_obj_resp_code[1669]-No response code for obj FSSI000
upd_install_pkg[1372]-Failed to find resp code for FSSI000
upd_status_save_status[135]-try to save on status file
upd_status_save_status[201]-Wrote status file
__upd_act_update[312]-Failed installing pkg
upd_comm_disconnect_fds[498]-Disconnecting FDS 149.5.232.66:443
[206] __ssl_data_ctx_free: Done
[1094] ssl_free: Done
[198] __ssl_cert_ctx_free: Done
[1104] ssl_ctx_free: Done
[1085] ssl_disconnect: Shutdown
upd_act_HA_contract_info[747]-Error updating FSCI -1
__update_upd_comp_by_settings[495]-Disabling NIDSDB/ISDB/MUDB components.
do_update[720]-UPDATE failed
calculate_next_update_time_auto[192]-interval=60, cur_time=Fri Jun 13 18:21:00 2025
, next_update=Fri Jun 13 18:21:00 2025
```

5. 此外，“系统管理→FortiGuard”和“系统管理→高可靠性”页面也可以查看HA的vSN。

注意事项

1. 如果HA型号的设备加入了FortiGate Cloud，如下所示。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system central-management
    set type fortiguard
end
```

2. FortiGate Cloud可能会自动向HA设备推送HA配置（不需要手动配置，使用的HA心跳接口为设备接口数字最大的接口），如下所示，其中也包含`logical-sn`配置。

```bash
config system ha
    set group-id 994
    set group-name "ZTP-VSN-HA-194"
    set mode a-p
    setpassword ENC xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    set hbdev "lan3" 50
    set override disable
    set logical-sn enable
end
```

3. 默认配置下，推送的HA配置无法修改（即使手动修改也会被FortiGate Cloud推送的模板配置覆盖）。如果需要HA两台设备单独使用，或自定义HA配置，则需要关闭FortiGate Cloud的配置推送功能（默认开启），之后就可以手动配置HA功能。

```bash
config system central-management
    set allow-push-configuration disable
end
```

4. 也可以关闭FortiGate Cloud管理功能。

```bash
config system central-management
    set type none
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA的ping server配置

功能介绍

1. Ping Server功能是为了防止所谓端口“假死”的问题，链路状态正常，但链路无法工作，防火墙可以通过利用发送ping包，根据对方的响应来判断该端口链路是否可用。

2. 配置命令如下：

```
config system link-monitor
    edit "wan1"
        set srcintf "wan1"
        set server "100.1.1.254"
        set failtime 3
        set ha-priority 5
    next
end
```

3. 如果只配置上述的配置，ping检测失败时HA不会切换，只是去往该接口的路由不再有效。需要在HA配置中告诉防火墙wan1口的 pingserver会作为HA切换的触发条件。

```bash
config system ha
    set pingserver-monitor-interface wan1     //监视wan1口上的pingserver//
    set pingserver-failover-threshold 0         //ha切换的阈值,默认为0//
    set pingserver-flip-timeout 60               //连续2次ping server触发的HA切换的间隔，单位为分钟，在这个时间内，ping server不会连续触发HA切换//
end
```

HA相关配置

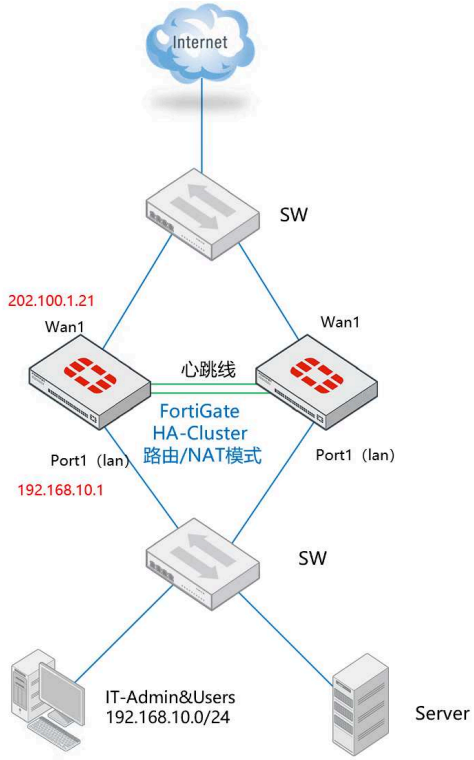
1. set ha-priority 1与pingserver-failover-threshold 0相关联。两者相比较，当wan1接口pingserver检查失效后赋值增加1，已经达到了阈值0，所以触发HA会切换。
2. 如果 pingserver-failover-threshold 2，即使该接口wan1的link-moniter检测失败，set ha-priority 1小于pingserver-failover-threshold 2，达不到触发的阈值，HA不会切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA的网管介绍

使用业务接口进行网管

1. 对网管要求不是太高的情况下推荐使用。



网管方式1：直接使用lan业务接口进行网管：
https://192.168.10.1
ssh admin@192.168.10.1

2. 优点：

- 够直接、够简单、无需考虑太多网管的因素
- 可以直接使用mgmt、lan或wan接口进行网管，直接网管即可，只需要开放接口的网管协议即可。（另外需注意管理员的可信任主机配置）

```
config system interface
    edit "port1"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh http fgfm
        set alias "LAN_Inside"
    next
end
```

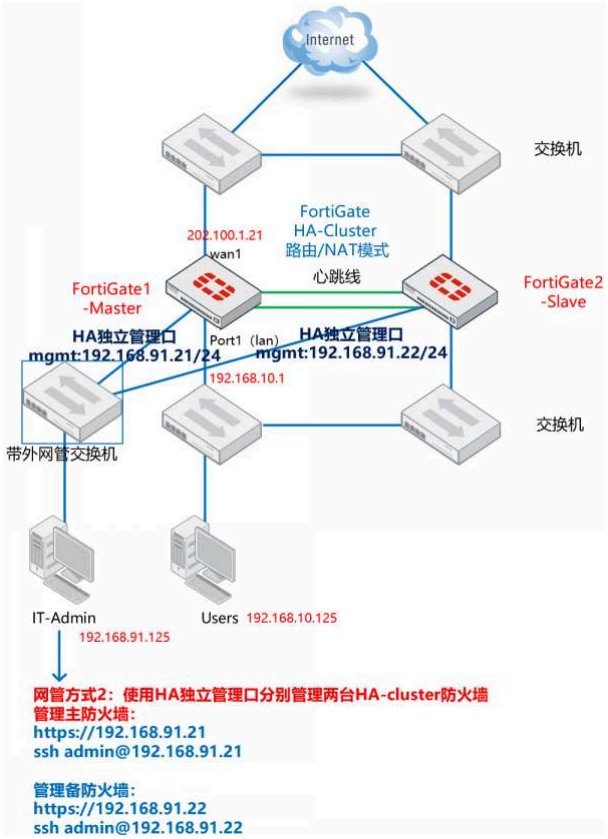
3. 缺点：

- 管理员无法登陆到备机上进行管理和查看，备机处于一种未知的状态（只能通过主机查看到备机的状态，管理员无法直接网管HA备机）
- 对于HA-Cluster来说HA是一个大的整体，此时的两台防火墙配置完全一样，换一句话说备机是完全不可控/不可登陆，完全处于热备的状态，只有主防火墙出现故障的时候备防火墙才会被激活，而在没有激活之前，管理员是无法登陆到备机上进行管理和查看的。这样就有一种小概率，备机坏了的时候（比如硬件故障），相对来说比较难被发现（可以通过主设备查看HA状态可以查看到备机掉线的异常情况）。如果对于设备管理要求较高的话，显然备机的这种未知状态会让人无法完全放心。
- 这就是简单带来的烦恼，既然要解决这样的烦恼，就有了下面的另外两种解决办法，当然这两种办法就不能用简单来形容了，相对要复杂一些。

使用HA独立管理接口进行网管

1. 备机管理员可以直接登陆，对HA的主机和备机进行单独的管理。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 优点：

- HA Cluster的主备两台机器都可以独立的进行网管和配置。
- HA独立管理口拥有一个完全独立的IP转发和路由空间，将网络管理区域和业务数据区域的IP/路由完全独立，二者相互不影响。相当于在后台创建了一个vsys_hamgmt的vdom，是一个轻量级的vdom。GUI是隐藏不可见的状态，让用户尽量较少的感受到此vdom的存在，意在简化用户对于独立管理口的使用和理解。命令行下实际可以进入到vsys_hamgmt进去ping等测试，而GUI是几乎是感受不到vsys_hamgmt的存在的。

```
FGT-LEFT # execute enter ?
<name>    vdom name
vsys_hamgmt    //HA独立管理口轻量级vdom
root    //业务数据的vdom
```

  我们知道业务接口的配置HA-Cluster之间是完全同步的，但HA独立管理口的配置HA-Cluster之间是不同步的，这样才可以确保HA-Cluster各自的独立管理口IP地址可以不一致，以便管理员可以通过不同的管理IP分别管理HA的主和备。

- 基于以上特性，我们可以知道，root和vsys_hamgmt拥有独立的IP/路由空间，因此独立管理口的IP和业务接口的IP地址是可以重叠使用的（允许IP/网段冲突），这个部分可以按照个人需求进行操作，不一定非要如此IP网段冲突的设置。比如业务接口lan的IP为192.168.1.99，这个时候其实可以将独立管理口mgmt的IP设置为192.168.1.198（主）、192.168.1.199（备），二者可以在同一个网段，管理员可以通过192.168.1.198管理到主防火墙，192.168.1.199管理到备防火墙。而192.168.1.99这个业务接口地址则永远只属于当前HA-Cluster的主防火墙。通常来说我们都是不建议管理和业务网段IP地址重叠/冲突的，这样不便于设计、理解、排错，非不得已不要这样使用。

3. 缺点：

- 独立管理口网管是独立的，但是fortiguard的更新无法使用独立管理mgmt进行更新，还是需要通过业务接口进行fortiguard服务的更新。
- 另外关于syslog、Radius等防火墙主动往外发起的业务，默认也是使用业务接口进行处理的，如果有使用独立管理口进行上述业务的需求，需要在HA下面开启“set ha-direct enable”，这样由FGT-LEFT本地发起的数据才会通过独立管理口mgmt去发送。

```
FGT-LEFT # config system ha
...
    set ha-direct ?

    enable    Enable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer,
FortiSandbox, sFlow, and Netflow.
    disable    Disable using ha-mgmt interface for syslog, remote authentication (RADIUS), FortiAnalyzer,
FortiSandbox, sFlow, and Netflow.    //默认为disable，使用业务接口处理以上业务。有需要独立管理的mgmt发送数据的时候才将其
enable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

以上无疑增加了业务和管理的复杂性，需要考虑的东西更多，容易犯错的机会也就更大。

4. HA独立管理口的使用建议：

- 如果仅仅是单纯的管理HA-Cluster的主和备防火墙，这个方法还是挺合适的
- 如果有更多更复杂的需求，则需要搞清楚HA独立管理口的工作逻辑，比如Radius请求/syslog日志是由谁发送的问题。注意命令适当的时候需要开启“set ha-direct enable”命令。可以通过sniffer抓包协助判断HA场景下的FGT-LEFT主动往外发包情况，以便确认是否是你需要的发包效果：# diagnose sniffer packet any "port 1812" 4 0 l（抓取防火墙发起的Radius认证数据）

> **重要**
>
> 开启HA配置下的“HA-direct”后，主机和备机的syslog、FortiAnalyzer、LDAP、Radius、TACACS+、sFlow、NetFlow等报文均会通过各自的独立管理口发出，而不是通过主机的业务口发出。

- 另外如果需要使用独立管理口mgmt进行fortiguard更新的话，则必须使用更加彻底的独立管理VDOM（方法3），将管理与业务的完全隔离，那个也是最彻底的方法，当然相对也更加复杂一些。（DNS解析和Fortiguard更新还是走的业务接口）

5. HA独立管理口命令行配置。

```
主防火墙：
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "mgmt"
            set gateway 192.168.91.254
        next
    end
end
config system interface
    edit "mgmt"
        set ip 192.168.91.21 255.255.255.0
        set allowaccess ping https ssh http
        set alias "HA_Dedicated_MGMT"
    next
end

备防火墙：
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "mgmt"
            set gateway 192.168.91.254
        next
    end
end
config system interface
    edit "port1"
        set ip 192.168.91.22 255.255.255.0
        set allowaccess ping https ssh http
        set alias "mgmt"
    next
end
```

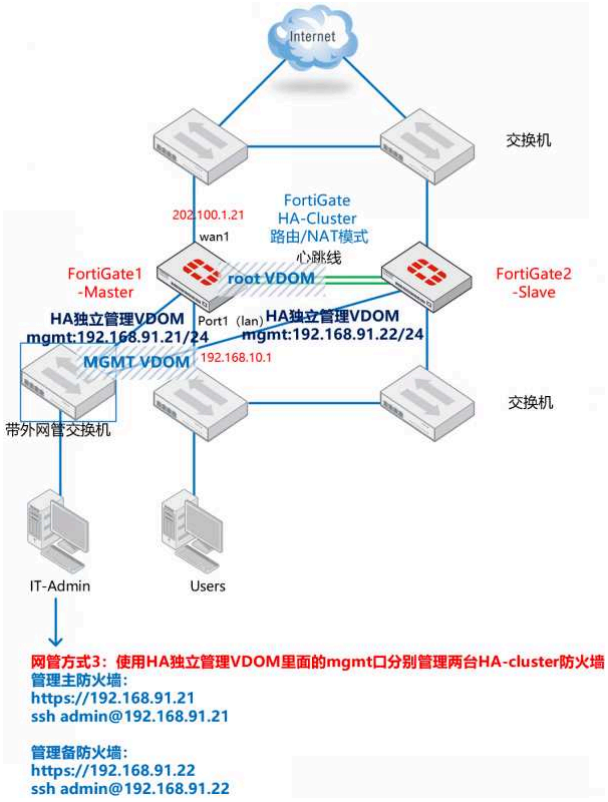
6. HA独立管理口GUI配置。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

使用独立VDOM进行网管

1. HA独立管理口可以简单的理解是一个轻量级的VDOM隔离，而HA独立管理VDOM则是一个完完全全的真实VDOM隔离。如果需要将HA-Cluster的管理和业务彻底隔离开，则建议使用HA独立管理VDOM。
2. HA独立管理口+配置了set ha-direct enable其实实现了一部分的独立管理VDOM的功能，但是还是不够彻底，比如fortigaurd更新等需求，因此这就是独立管理VDOM存在的原因。



3. 优点：
   - 完全的管理和业务独立，管理是管理VDOM，业务是业务VDOM，完全隔离，最符合隔离管理的需求。
4. 缺点：
   - 需要开启VDOM特性，配置相对会复杂一些。
5. 独立管理VDOM的配置，首先需要开启VDOM特性。

```
FGT-LEFT # config system global
FGT-LEFT (global) # set vdom multi-vdom
FGT-LEFT (global) # end
You will be logged out for the operation to take effect
Do you want to continue? (y/n)y
Auto backup config ...
exit
FGT-LEFT login:
FGT-LEFT login: admin
Password: ********
Welcome !
```

6. 创建新的MGMT独立管理VDOM。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
FGT-LEFT # config vdom
FGT-LEFT (vdom) # edit MGMT
FGT-LEFT (MGMt) # end
```

7. 将MGMT独立管理VDOM修改为管理VDOM（只能命令行修改）。

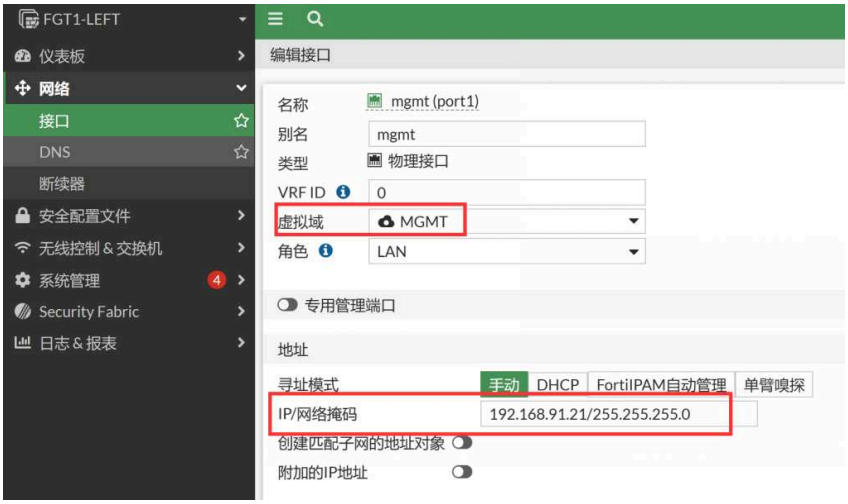
```
FGT-LEFT # config global
FGT-LEFT (global) # config system global
FGT-LEFT (global) # set management-vdom
<string>    please input string value
MGMT    vdom
root    vdom
FGT-LEFT (global) # set management-vdom MGMT
FGT-LEFT (global) # end
FGT-LEFT (global) # end
```

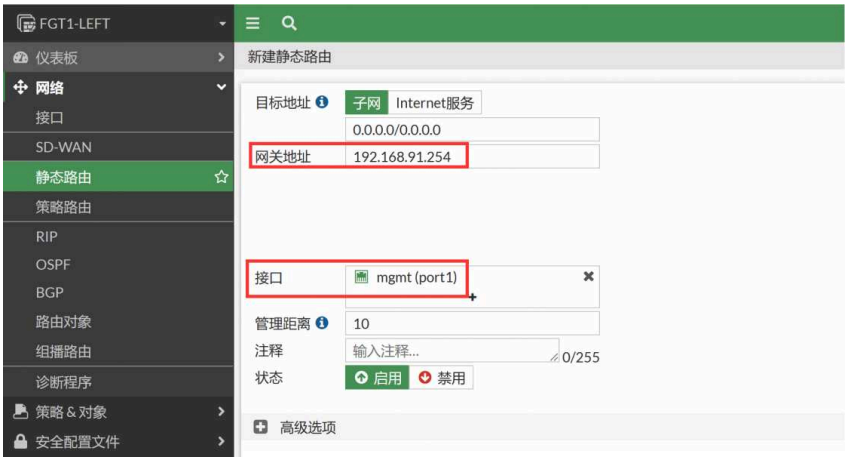
8. HA里面指定MGMT VDOM为独立管理VDOM。

```
FGT-LEFT # config  global
FGT-LEFT (global) # config system ha
FGT-LEFT (ha) # set standalone-mgmt-vdom enable    //此配置HA的主备同步，在主设备配置会自动同步到备设备上
FGT-LEFT (ha) # end
```

9. 将mgmt接口加入到MGMT VDOM中，并配置上管理IP和默认路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
配置mgmt加入到VDOM-MGMT以及配置管理IP地址:
FGT-LEFT # config global
FGT-LEFT (global) # config system interface
FGT-LEFT (interface) # edit port1
FGT-LEFT (mgmt) # set vdom MGMT
FGT-LEFT (mgmt) # set ip 192.168.91.21/24
FGT-LEFT (mgmt) # set alias "MGMT"
FGT-LEFT (mgmt) # end
FGT-LEFT (global) # end

配置默认路由:
FGT-LEFT # config vdom
FGT-LEFT (vdom) # edit MGMT
current vf=MGMT:1
FGT-LEFT (MGMT) # config router static
FGT-LEFT (static) #
FGT-LEFT (static) # edit 0
new entry '0' added
FGT-LEFT (0) # set gateway 192.168.91.254
FGT-LEFT (0) # set device port1
FGT-LEFT (0) # end

FGT-LEFT (MGMT) # execute ping 192.168.91.254
PING 192.168.91.254 (192.168.91.254): 56 data bytes
64 bytes from 192.168.91.254: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.91.254: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.91.254: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.91.254: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.91.254: icmp_seq=4 ttl=255 time=0.1 ms
--- 192.168.91.254 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
```

.0. 此时备机是无法WEB/SSH登陆的需要通过主机的命令（或者Console线）连到备机的命令行界面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FGT-LEFT # config global
FGT-LEFT (global) # execute ha  manage
<id>    please input peer box index.
<1>     Subsidary unit FG101E4Q17000045

FGT-LEFT (global) # execute ha  manage  1    //从主机登陆到备机的命令行

FFGT-LEFT-RIGHT login: admin
Password: ********
Welcome !

FFGT-LEFT-RIGHT $
```

1. 备防火墙那边会自动同步VDOM和mgmt加入到MGMT的配置（如果配置同步不正常，可以将备机重启，并等待配置同步完成，再操作），而独立管理MGMT-VDOM内部的配置是不会同步的，因此只需要修改备防火墙管理VODM、mgmt的接口IP和路由即可。

```
FGT-LEFT # config global
FGT-LEFT (global) # config system global
FGT-LEFT (global) # set management-vdom MGMT
FGT-LEFT (global) # end
FGT-LEFT (global) # end
FGT-LEFT-RIGHT $ config vdom
FGT-LEFT-RIGHT (vdom) $ edit MGMT
current vf=MGMT:1
FGT-LEFT-RIGHT (MGMT) $ config system interface
FGT-LEFT-RIGHT (interface) $ edit mgmt
FGT-LEFT-RIGHT (mgmt) $ set ip 192.168.91.22/24
FGT-LEFT-RIGHT (mgmt) $ set allowaccess https http  ping ssh
FGT-LEFT-RIGHT (mgmt) $ set alias "HA_Dedicated_MGMT"
FGT-LEFT-RIGHT (mgmt) $ show
FGT-LEFT-RIGHT (mgmt) $ end

FGT-LEFT-RIGHT (MGMT) $ config router static
FGT-LEFT-RIGHT (static) $ edit 0
new entry '0' added
FGT-LEFT-RIGHT (0) $ set device mgmt
FGT-LEFT-RIGHT (0) $ set  gateway  192.168.91.254
FGT-LEFT-RIGHT (0) $ end

FGT-LEFT-RIGHT (MGMT) $ execute  ping 192.168.91.254
PING 192.168.91.254 (192.168.91.254): 56 data bytes
64 bytes from 192.168.91.254: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.91.254: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.91.254: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.91.254: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.91.254: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.91.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.2 ms
```

2. 这个时候可以通过GUI登录到备机了（使用备机的独立管理IP）。
3. 这时候可以通过192.168.91.21和192.168.91.22分别管理到主防火墙和备防火墙了。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 此时所有的Radius/SYSLOG/DNS/FORTGUARD都是通过MGMT这个VDOM进行更新的，完全独立于root业务VDOM，彻底的管理是管理，业务是业务。这是HA独立管理的终极解决方案。

5. 越完美的方案，有时候也就是意味着越复杂，实际部署中需按照个人需求进行选择如何管理HA-Cluster。

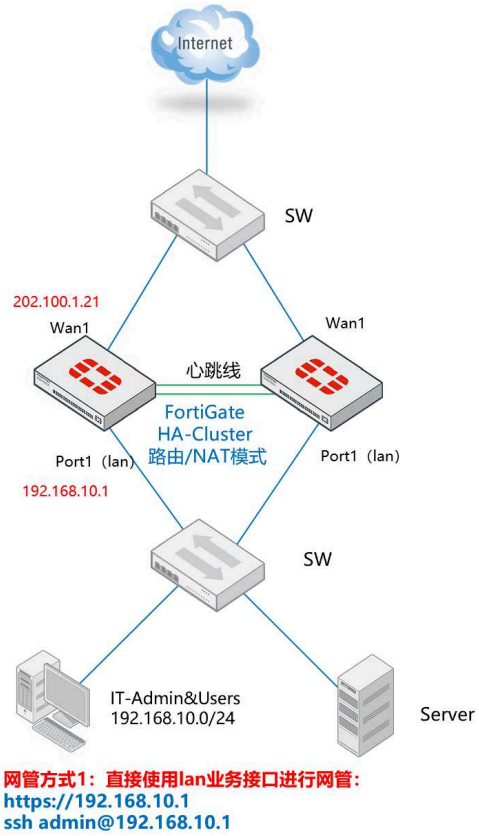
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA集群普通管理

网络需求

通过业务接口管理和配置HA集群。

网络拓扑



配置要点

- 配置HA基础配置
- 配置基础LAN/WAN上网服务
- 配置网络管理的相关参数
- 配置防火墙的SYSLOG、SNMP、FMG

配置步骤和结果验证

HA基础配置

1. 配置HA基础配置，初始化配置防火墙的时候可以通过mgmt口登陆到防火墙上，一般mgmt口的管理IP是192.168.1.99，第一步可以通过此IP登陆防火墙（参考系统管理→管理方式→Web管理↗章节），或者通过console口管理防火墙（参考系统管理→管理方式→Console管理↗章节）。具体型号初始化如果网管和接口的网管IP信息等可参考https://docs.fortinet.com/product/fortigate/hardware↗ 或 https://docs.fortinet.com/document/fortigate/hardware/fortigate-quickstart-guide-high-end?model=all↗ 。
2. 按照以上方式登陆第一次开箱的防火墙。先登陆主防火墙，并配置进行HA的基础配置，然后登陆到备防火墙，配置备防火墙的HA基础配置。
3. 分别配置主防火墙和备防火墙的HA，主防火墙优先级调整为150，备防火墙的优先级保持默认的120，配置HA-cluster组名字和密码，监控业务接口wan1和port1，使用HA1和HA2接口将二者互联。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
XU4Yv532eMH20TXkbxDMQWRNs+ChZrIVXcotCFVP2C86QBl2zhznTNU+0PDKw5Vlvtm6B+NCZ+f+1EiT3MsUteDHW82Aten6q+Yu6zAT5NuXYYIKnV
pG=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set override disable
    set priority 150
    set monitor "port1" "port2"
end
```




```
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
HzpTLoO69D1nrZ9QZbKFDbuUmCefmDRbZqTvgSseAgh2zU8JOHq1bthC750a+p5S/rkfRSROmhVMqOKRbBZkir3C8VWW9l+h7jl7Xp4N5sdA1CmDSU
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
zX=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set override disable
    set priority 120
    set monitor "port1" "port2"
end
```

4. 双方的HA配置完毕之后将ha1和ha2线相互直连，将会进行HA的选举，此时优先级150高的FGT将成为主防火墙，优先级低的120的FGT将成为备防火墙。然后备防火墙的配置将会和主防火墙进行同步，备防火墙所有配置和主防火墙一致，此时备防火墙也将不再可以WEB/SSH登录，仅仅可以Console登录。后续所有的操作和配置都在主防火墙上的GUI、SSH或Console完成。

5. 选举结果如下，FGT1-LEFT成为主设备。

```
FGT1-LEFT # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:22783 b:12890083
        traffic.total = s:0 p:22793 b:12890691
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=0 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM22000173:      Primary, serialno_prio=1, usr_priority=150, hostname=FGT1-LEFT
FGVM08TM22000174:    Secondary, serialno_prio=0, usr_priority=120, hostname=FGT2-RIGHT

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0:
FGVM08TM22000173:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM22000174:    Secondary, ha_prio/o_ha_prio=1/1
```

6. 这三个命令都可以看到HA的选举结果和HA状态。

```
# diagnose sys ha status
# get system status
# get system ha status
```

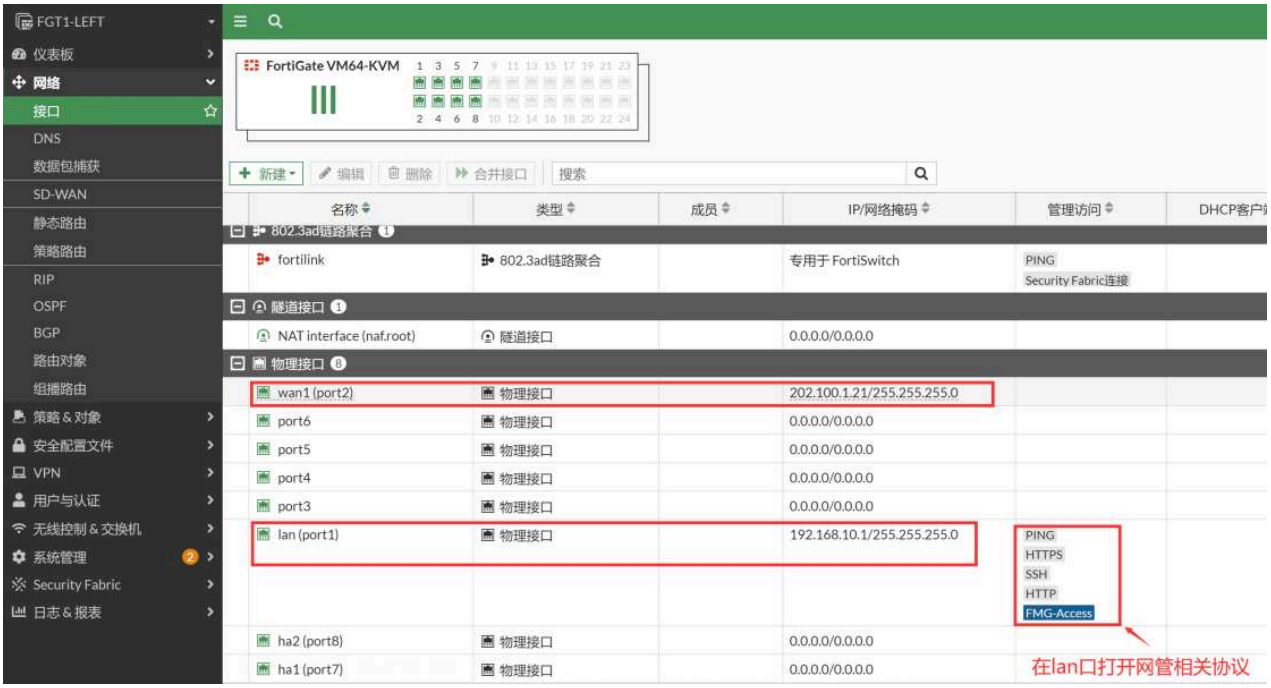
7. GUI查看HA的选举结果和状态。



8. 配置基础LAN/WAN上网服务。此步骤为正常上网的基础配置，大概的步骤是配置接口IP、配置默认路由、配置策略即可实现防火墙的简单上网配置。（所有配置都在主防火墙上完成，备防火墙此时不可以登陆）

9. 配置接口IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 202.100.1.21 255.255.255.0
        set type physical
        set alias "wan1"
        set snmp-index 2
    next
end
```

.0. 配置默认路由。




```
config router static
    edit 1
        set gateway 202.100.1.192
        set device "port2"
    next
end
```

.1. 配置上网策略。

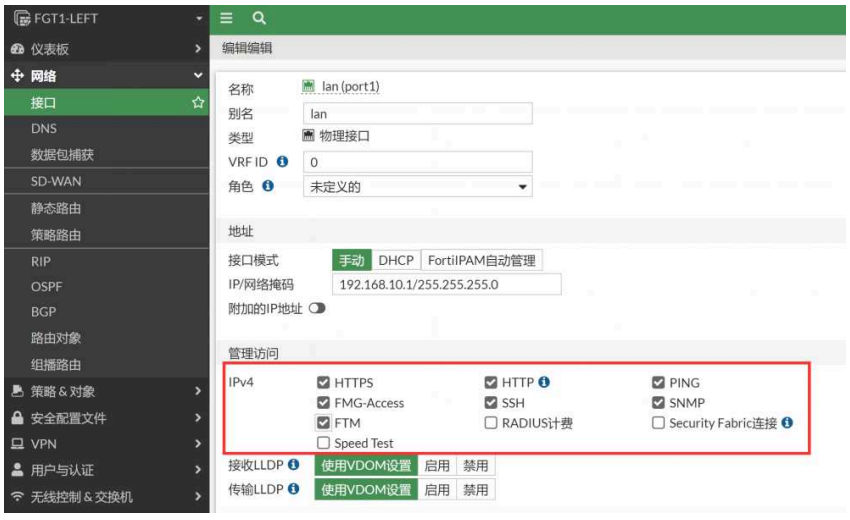
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

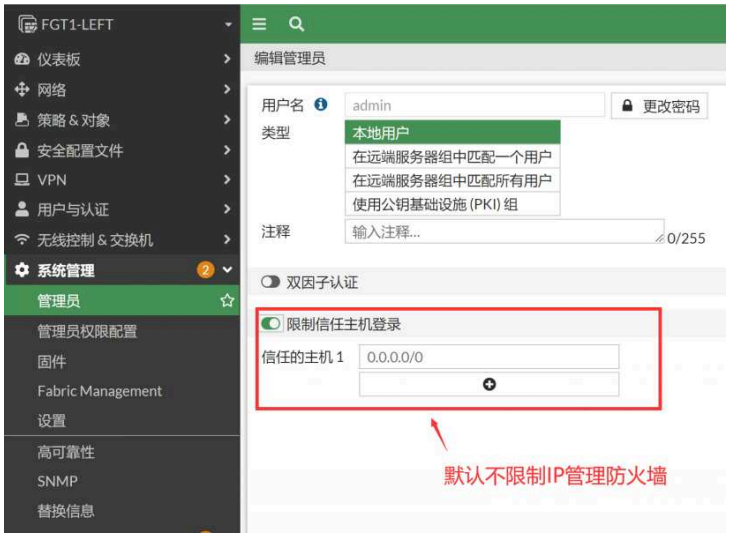
2. 配置LAN口网管相关参数，关于网管目前可以通过port1（lan）的192.168.10.1进行管理，比较关键的网管因素是：

   - port1接口下开启了网管的协议，比如https、http、ssh、snmp等。



   - 管理员可信任主机如果配置了的话，需要包含发起管理请求的主机IP或网段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 客户端PC到FGT的来回路由可达，可以通过ping和tracert测试。
- 上面1、2点确认没有问题之后，还是遇到不通的情况，可以通过sniffer抓包和debug flow确认问题所在。

```
FGT # diagnose sniffer packet any "host 192.168.10.1" 4 0 l
```

- 如果跨接口管理防火墙，比如处于port1的PC要通过防火墙port2接口的IP管理防火墙，则需要主要有port1到port2的放通策略，否则数据也是不通的。
- 出现网管不了的情况，99%就是以上的原因了。

网管配置

SYSLOG

1. 确认通过192.168.10.1网管没问题的话，配置SYSLOG等本机发出的网管配置。

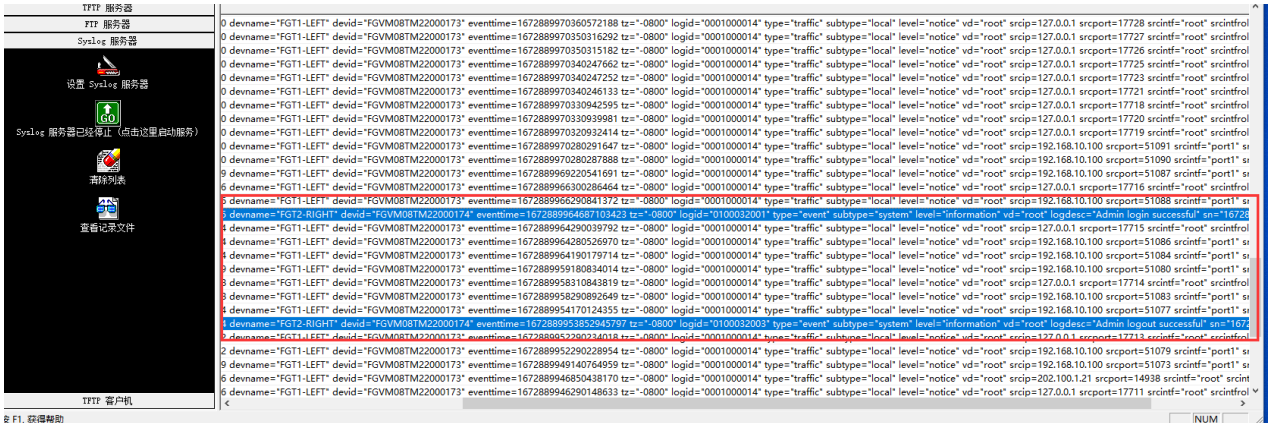


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config log syslogd setting
    set status enable
    set server "192.168.10.100"
end
```

2. 主/备防火墙的日志都会通过业务接口port1 192.168.10.1将syslog日志发送出去，备防火墙的syslog日志会通过心跳线到主机，然后由主机代为转发。

```
FGT1-LEFT # diagnose sniffer packet any "port 514" 4
interfaces=[any]
filters=[port 514]
0.918154 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 635    //主防火墙的syslog日志
0.918225 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 649
5.492057 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 649
5.961902 port_ha in 169.254.0.2.514 → 169.254.0.1.514: udp 454    //备防火墙的console登陆日志
5.962018 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 418
5.968684 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 554
8.314617 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 730
8.507346 port_ha in 169.254.0.2.514 → 169.254.0.1.514: udp 473    //备防火墙的console退出日志
8.507479 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 437
8.964545 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 724
9.074989 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 597
```



SNMP

1. lan接口下开启SNMP协议。

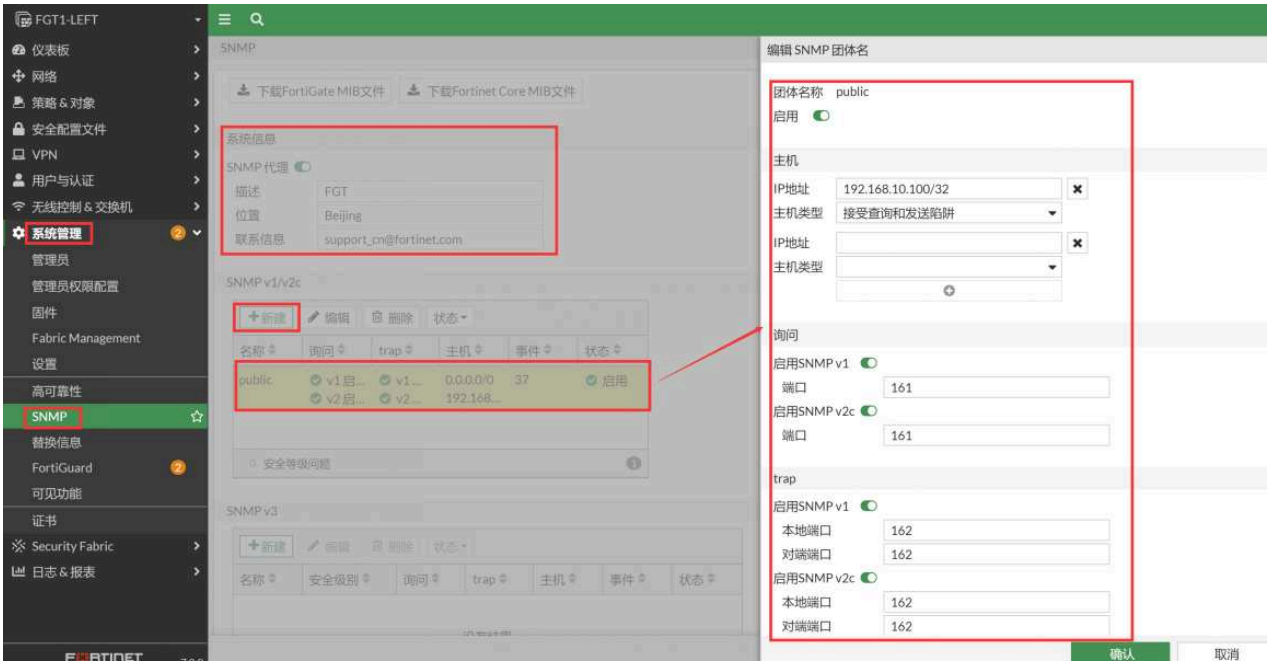



```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set type physical
        set alias "lan"
        set snmp-index 1
    next
end
```

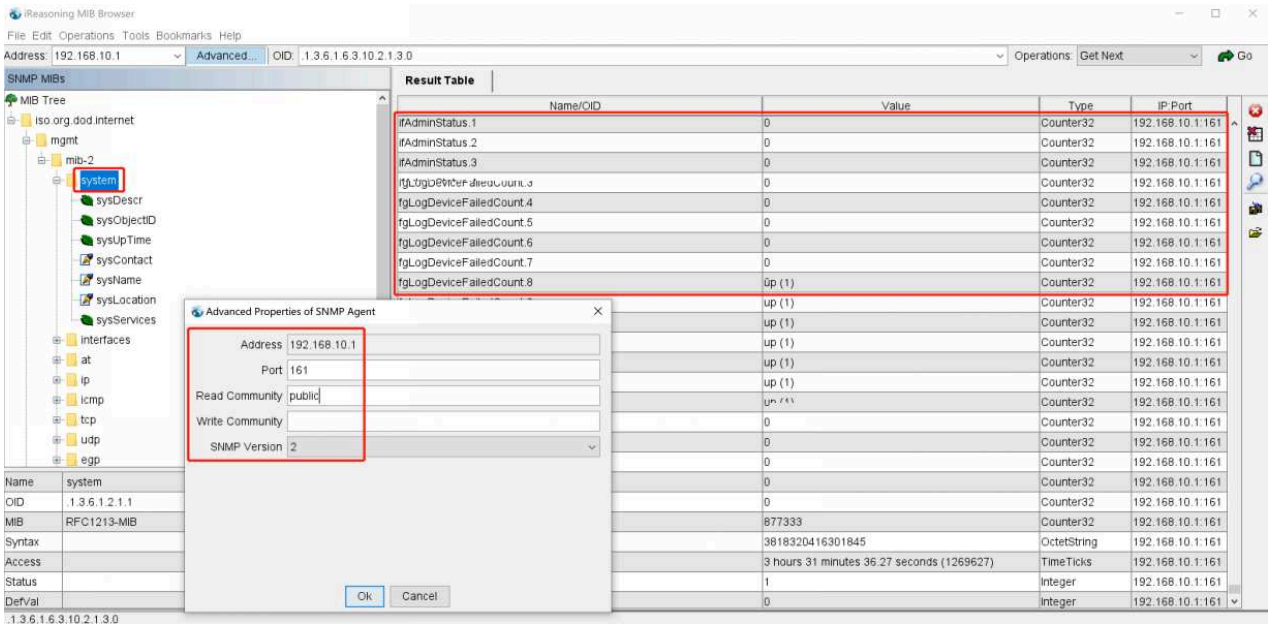
2. 开启SNMP功能。




```
config system snmp sysinfo
    set status enable
    set description "FGT"
    set contact-info "support_cn@fortinet.com"
    set location "Beijing"
end

config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ip 192.168.10.100 255.255.255.255
            next
        end
    next
end
```

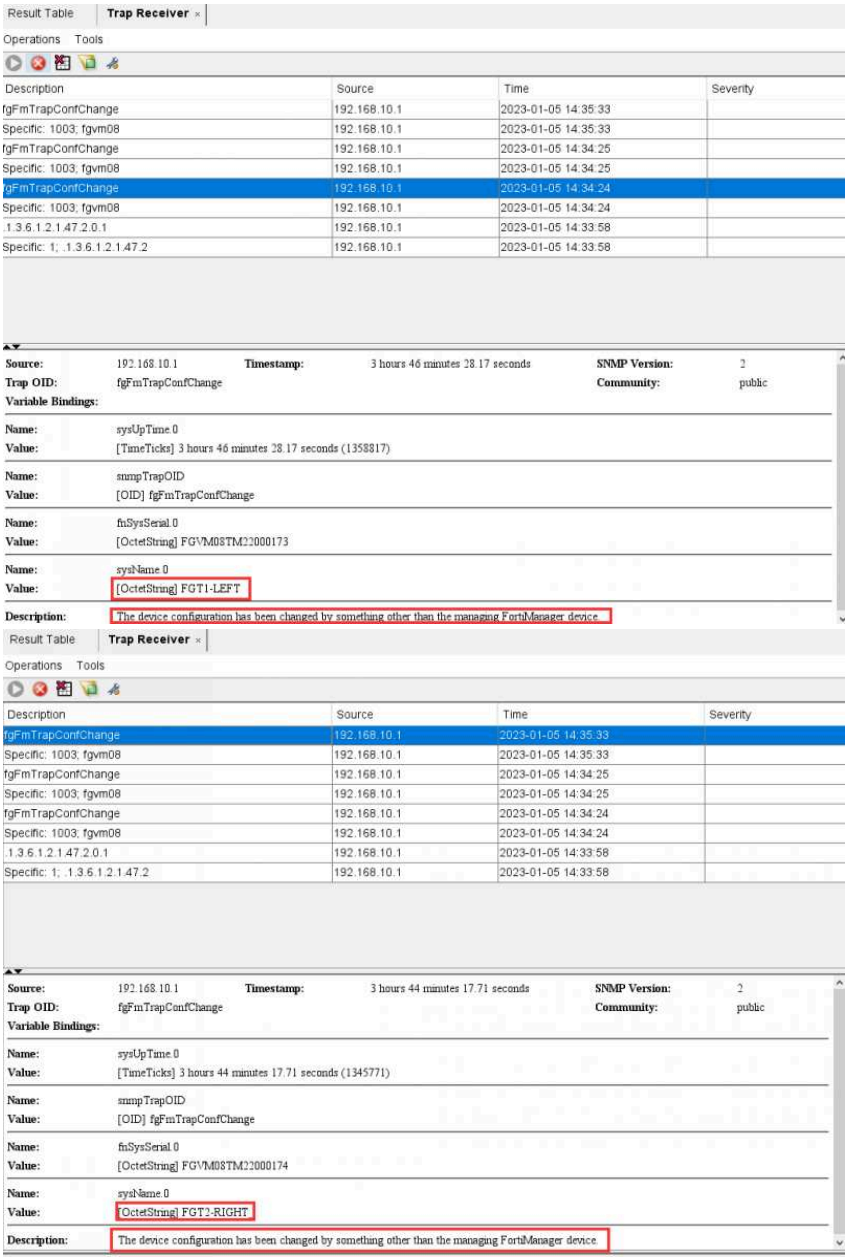
3. 在SNMP客户端对FortiGate的lan口进行get/walk操作，这里以IReasoning MIB Browser为例。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



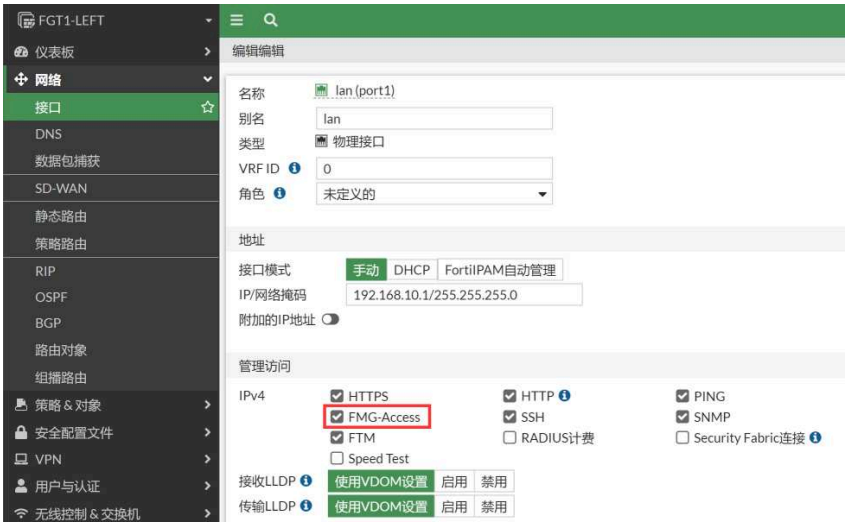
4. SNMP客户端接收到的FGT发送的trap信息，可以看到主备设备均通过主设备进行发送。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiManger管理

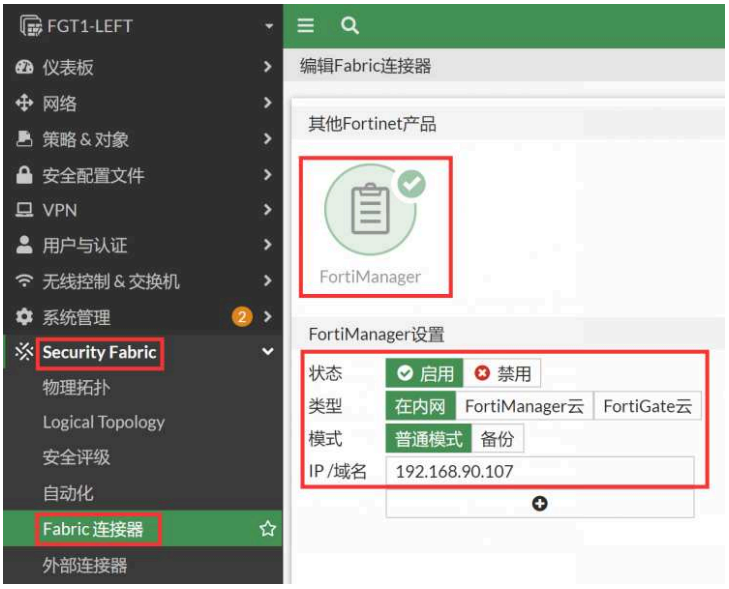
1. FortiManager通过FGT的lan口添加设备，在FGT的lan口下开启FMG管理协议。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

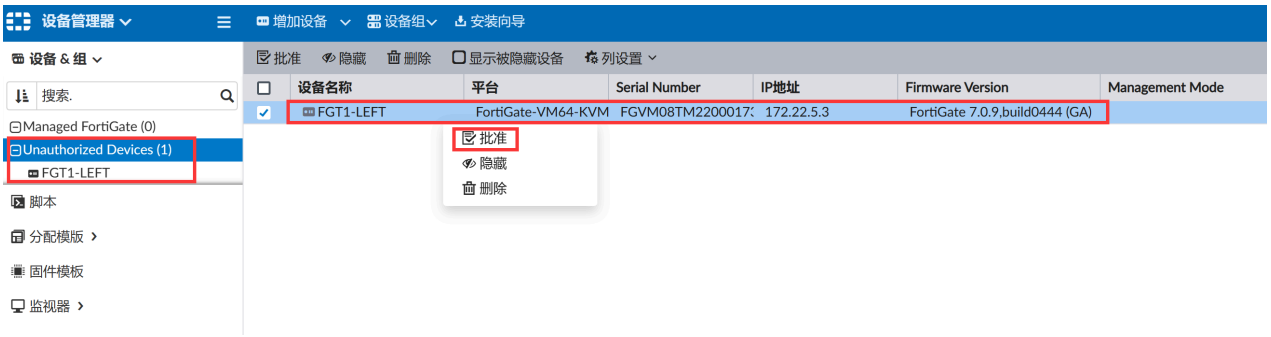
```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
end
```

2. 配置防火墙主动连接FMG（如果FMG可以主动访问到FGT，也可以通过FMG主动添加FGT）。



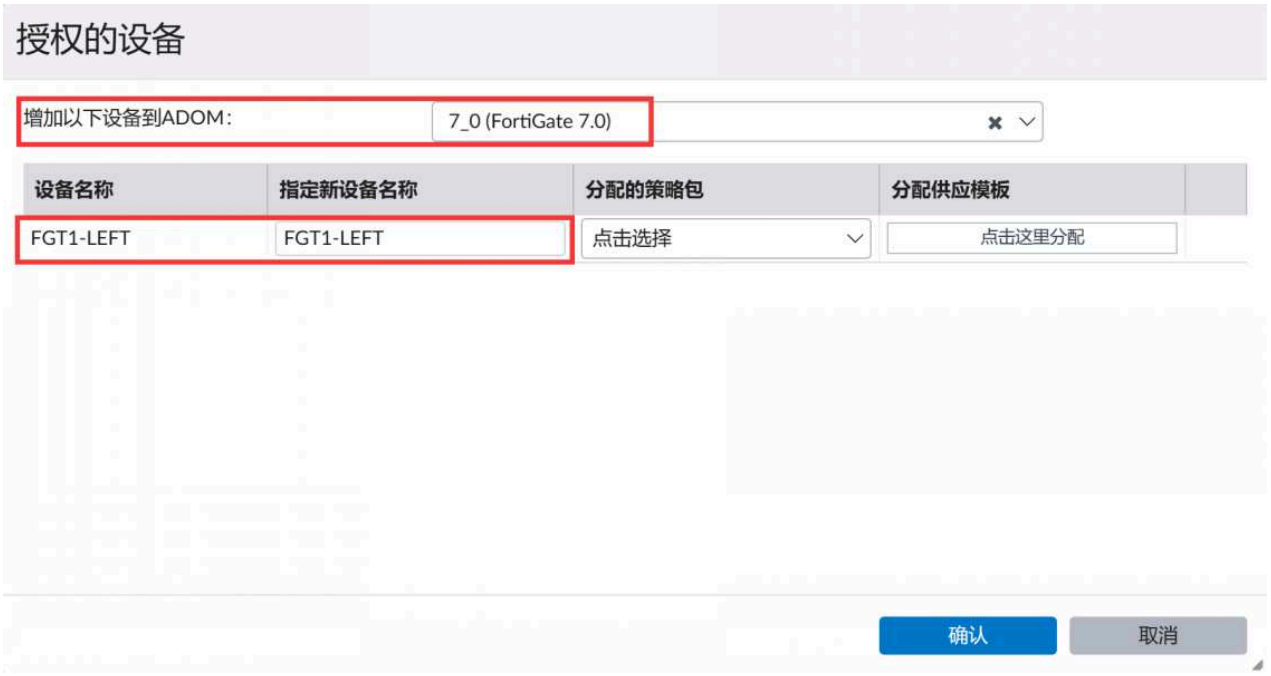

```
config system central-management
    set type fortimanager
    set fmg "192.168.90.107"
end
```

3. 如果是FGT主动去注册FMG，则FMG会有未注册的设备提示。



4. 只需要将设备添加到FMG的对应ADOM的设备管理中即可。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

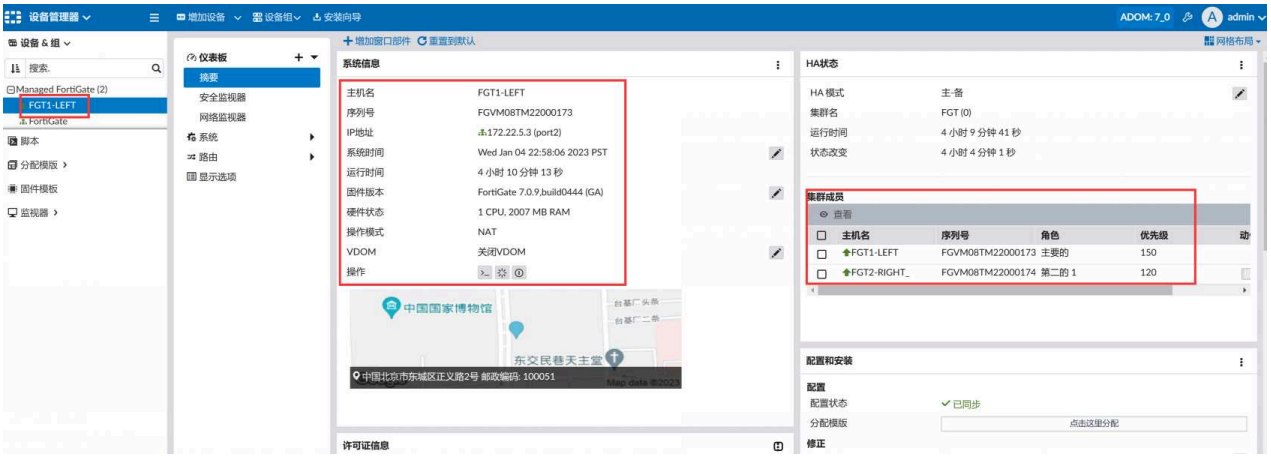


5. 授权完成。



6. 在FMG中可以对FGT进行管理。

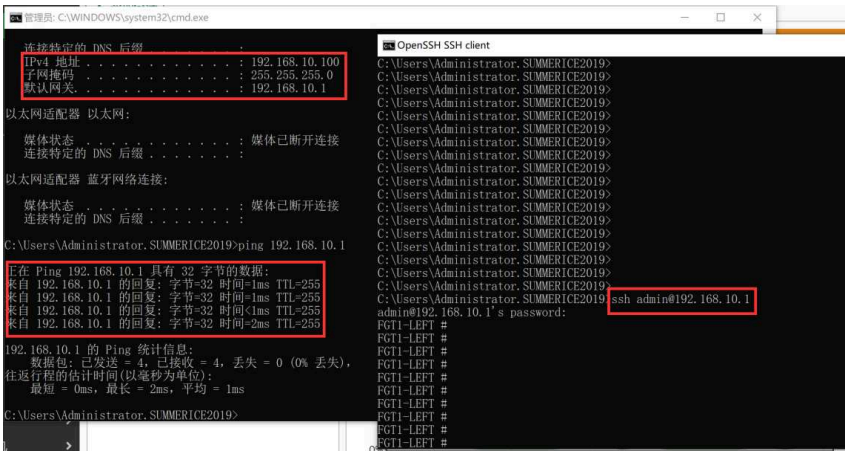
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



SSH、Ping

1. 在lan接口下开启SSH和Ping。

2. 使用PC客户端访问FGT主设备的Ping和SSH。



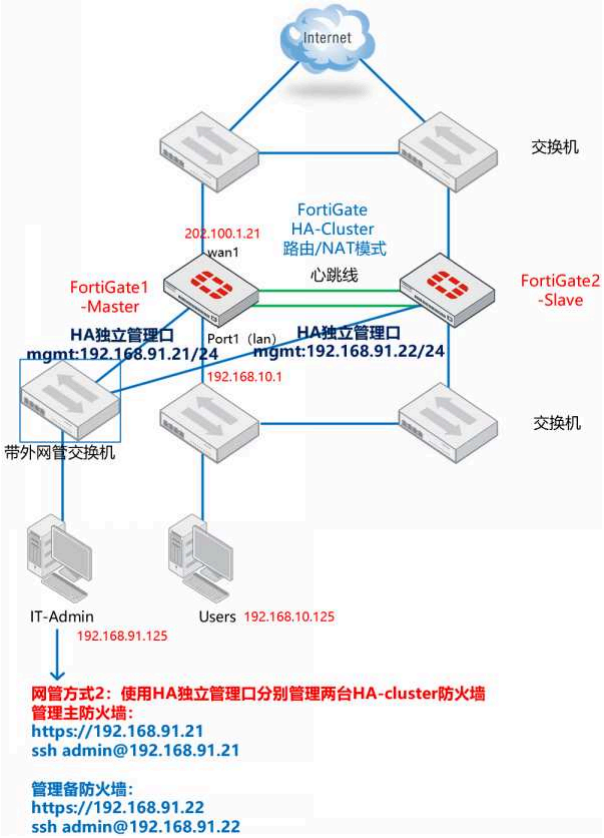
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

独立管理接口

网络需求

1. 在HA集群中，所有集群成员的配置全部相同，通过IP只能管理到主设备，无法通过IP对每个slave设备进行单独的管理。同时为了业务的安全，需要将管理网络与业务网络独立开。
2. 为实现如上需求，可以使用HA使用独立的管理接口来实现带外管理功能。独立管理口的相关配置不会被HA所同步。

网络拓扑



配置要点

- 配置HA基础配置
- 配置基础LAN/WAN上网服务
- 配置“HA独立管理口”
- 配置防火墙的SYSLOG、SNMP和FMG

配置步骤和结果验证

1. 配置HA基础配置，初始化配置防火墙的时候可以通过mgmt口登陆到防火墙上，一般mgmt口的管理IP是192.168.1.99，第一步可以通过此IP登陆防火墙（参考系统管理→管理方式→Web管理 ↗章节），或者通过console口管理防火墙（参考系统管理→管理方式→Console管理 ↗章节）。具体型号初始化如果网管和接口的网管IP信息等可参考https://docs.fortinet.com/product/fortigate/hardware ↗ 或 https://docs.fortinet.com/document/fortigate/hardware/fortigate-quickstart-guide-high-end?model=all ↗ 。
2. 按照以上方式登陆第一次开箱的防火墙。先登陆主防火墙，并配置进行HA的基础配置，然后登陆到备防火墙，配置备防火墙的HA基础配置。
3. 分别配置主防火墙和备防火墙的HA，主防火墙优先级调整为150，备防火墙的优先级保持默认的120，配置HA-cluster组名字和密码，监控业务接口wan1和port1，使用HA1和HA2接口将二者互联。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
XU4Yv532eMH20TXkbxDMQWRNs+ChZrIVXcotCFVP2C86QBl2zhznTNU+0PDKw5Vlvtm6B+NCZ+f+1EiT3MsUteDHW82Aten6q+Yu6zAT5NuXYYIKnV
pG=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set override disable
    set priority 150
    set monitor "port1" "port2"
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
HzpTLoO69D1nrZ9QZbKFDbuUmCefmDRbZqTvgSseAgh2zU8JOHq1bthC750a+p5S/rkfRSROmhVMqOKRbBZkir3C8VWW9l+h7jl7Xp4N5sdA1CmDSU
zX=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set override disable
    set priority 120
    set monitor "port1" "port2"
end
```

4. 双方的HA配置完毕之后将ha1和ha2线相互直连，将会进行HA的选举，此时优先级150高的FGT将成为主防火墙，优先级低的120的FGT将成为备防火墙。然后备防火墙的配置将会和主防火墙进行同步，备防火墙所有配置和主防火墙一致，此时备防火墙也将不再可以WEB/SSH登录，仅仅可以Console登录。后续所有的操作和配置都在主防火墙上的GUI、SSH或Console完成。

5. 选举结果如下，FGT1-LEFT成为主设备。

```
FGT1-LEFT # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:22783 b:12890083
        traffic.total = s:0 p:22793 b:12890691
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=0 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM22000173:      Primary, serialno_prio=1, usr_priority=150, hostname=FGT1-LEFT
FGVM08TM22000174:    Secondary, serialno_prio=0, usr_priority=120, hostname=FGT2-RIGHT

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0:
FGVM08TM22000173:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM22000174:    Secondary, ha_prio/o_ha_prio=1/1
```

6. 这三个命令都可以看到HA的选举结果和HA状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

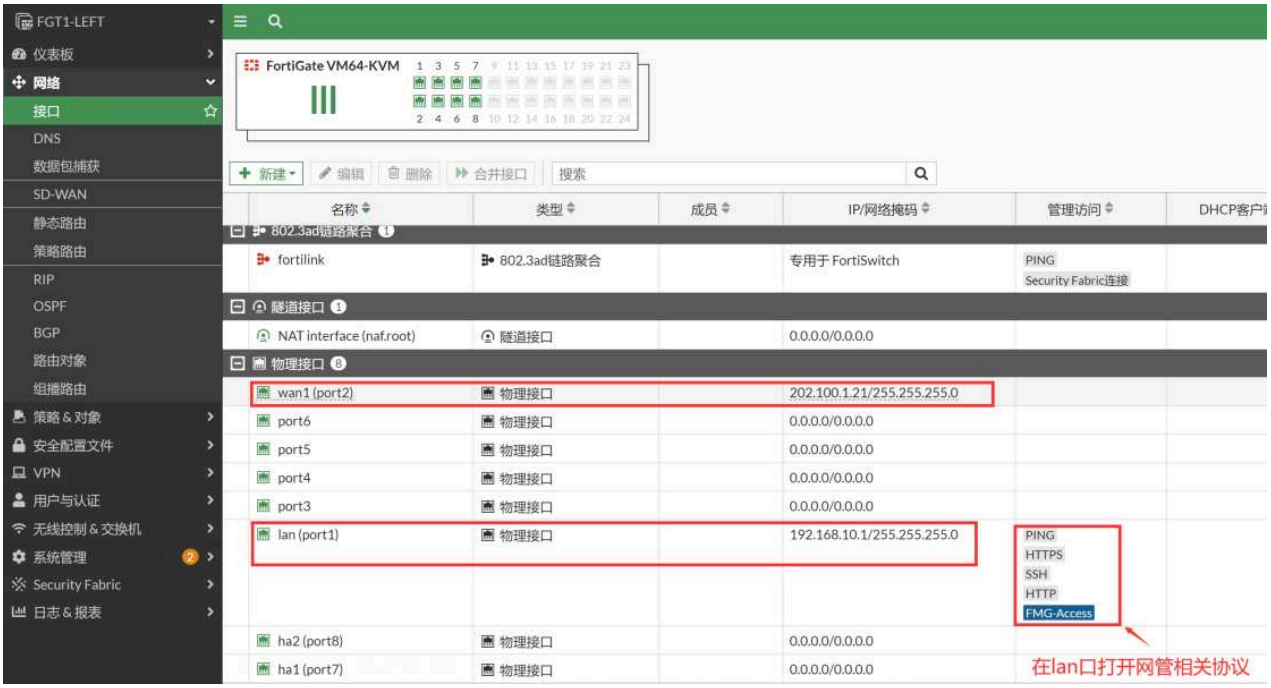
```
# diagnose sys ha status
# get system status
# get system ha status
```

7. GUI查看HA的选举结果和状态。



8. 配置基础LAN/WAN上网服务。此步骤为正常上网的基础配置，大概的步骤是配置接口IP、配置默认路由、配置策略即可实现防火墙的简单上网配置。（所有配置都在主防火墙上完成，备防火墙此时不可以登陆）

9. 配置接口IP。




```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 202.100.1.21 255.255.255.0
        set type physical
        set alias "wan1"
        set snmp-index 2
    next
end
```

.0. 配置默认路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config router static
    edit 1
        set gateway 202.100.1.192
        set device "port2"
    next
end
```

1. 配置上网策略。

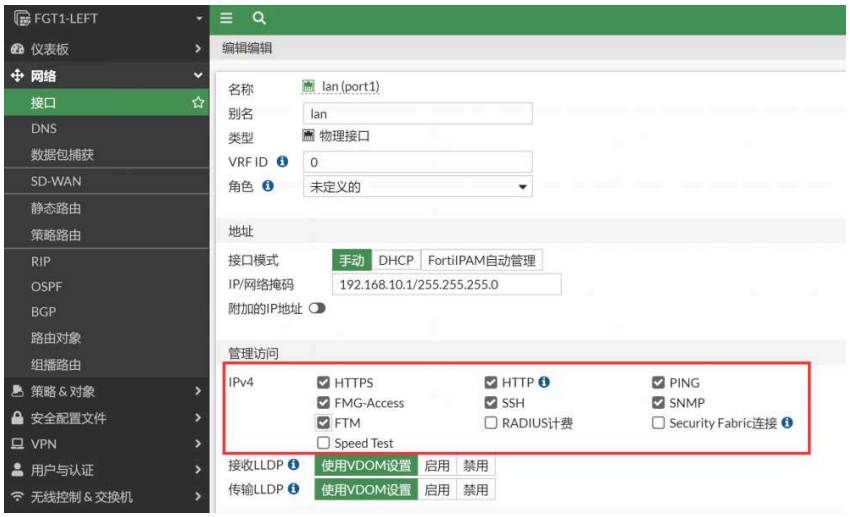



```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

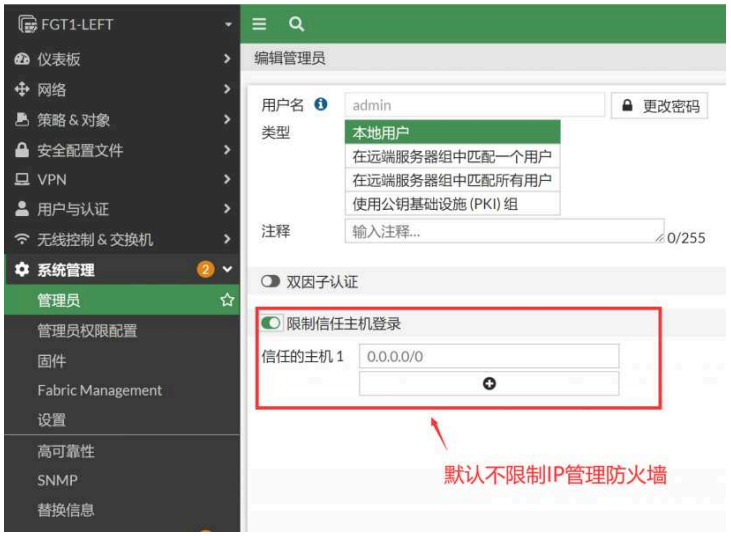
2. 配置LAN口网管相关参数，关于网管目前可以通过port1（lan）的192.168.10.1进行管理，比较关键的网管因素是：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- port1接口下开启了网管的协议，比如https、http、ssh、snmp等。



- 管理员可信任主机如果配置了的话，需要包含发起管理请求的主机IP或网段。



- 客户端PC到FGT的来回路由可达，可以通过ping和tracert测试。
- 上面1、2点确认没有问题之后，还是遇到不通的情况，可以通过sniffer抓包和debug flow确认问题所在。

```
FGT # diagnose sniffer packet any "host 192.168.10.1" 4 0 l
```

- 如果跨接口管理防火墙，比如处于port1的PC要通过防火墙port2接口的IP管理防火墙，则需要主要有port1到port2的放通策略，否则数据也是不通的。
- 出现网管不了的情况，99%就是以上的原因了。

3. 配置HA独立管理口，**要注意如果作为独立管理的接口有关联的配置，则独立管理口不能选择该接口，比如某接口配置了DHCP服务器，则需要把DHCP相关的功能先去掉，然后才可以将该接口指定为独立管理口**。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 在主设备和备设备上将port6（mgmt）接口加入独立管理口，并配置独立管理口的网关。

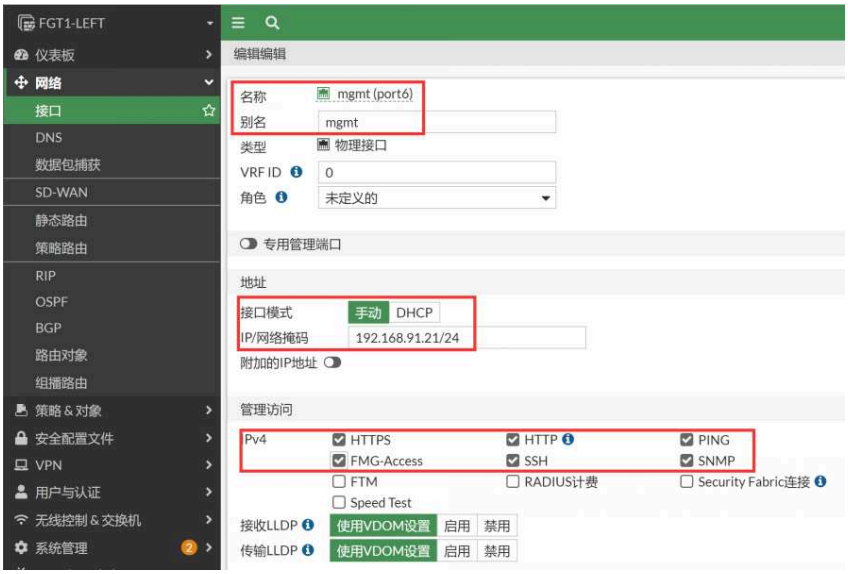



```
config system ha
 ...
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port6"    //此命令会同步到备机
            set gateway 192.168.91.254    //独立管理口的网关IP地址配置不会同步到备防火墙，因为二者可以拥有不同的IP网段和网关地址，不同步可以满足更多的需求，也更加灵活
        next
    end
 ...
end
```

5. 此时如果本身就是通过mgmt接口管理的防火墙，则可能管理会中断，必须使用console口进行mgmt接口IP的配置。如果使用的业务接口lan（port1）管理的防火墙，则直接修改mgmt接口IP地址即可。

6. 配置mgmt接口（port6）的IP，并开启相关的网管服务。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "port6"
        set ip 192.168.91.21 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type physical
        set alias "mgmt"
        set snmp-index 6
    next
end
```

7. 主机的HA独立管理口配置完毕，开始配置备机的独立管理口，此时备机是无法WEB/SSH登陆的需要通过主机的execute ha manage命令（或者Console线）连到备机的命令行界面。

```
FGT1-LEFT # exe ha manage ?
<id>    please input peer box index.
<0>     Subsidiary unit FGVM08TM22000174

FGT1-LEFT # exe ha manage 0 admin
admin@169.254.0.1's password:
FGT2-RIGHT #
```

8. 配置备防火墙的mgmt管理口IP地址（开启HA独立管理口功能之后，mgmt的配置不会再同步，需要手工配置mgmt的IP地址）。

```
FGT2-RIGHT # config system interface
FGT2-RIGHT (interface) # edit port6
FGT2-RIGHT (port6) # set ip 192.168.91.22/24
FGT2-RIGHT (port6) # set allowaccess ping https ssh snmp http fgfm
FGT2-RIGHT (port6) # end
```

9. 配置HA独立管理口的网关（此配置不会从主设备同步，需要单独配置）。

```
FGT2-RIGHT # config system ha
FGT2-RIGHT (ha) # config ha-mgmt-interfaces
FGT2-RIGHT (ha-mgmt-interfaces) # edit 1
FGT2-RIGHT (1) # set gateway 192.168.91.254
FGT2-RIGHT (1) # end
FGT2-RIGHT (ha) # show
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
L2tPmaCKq4nyH9Y6/+wKJQTXF2ROKYww0zCKqylOTEiACqph0eB+Ji5FDv5OimBxc4XvxZD8cU6bsWbRP8l/TcHRgpOvoPB/9m/Qu23voGOSxhLxlg
iz=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port6"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set gateway 192.168.91.254
        next
    end
    set override disable
    set priority 120
    set monitor "port1" "port2"
end
FGT2-RIGHT (ha) # end
```

10. HA独立管理口的配置完毕，此时管理员可以通过192.168.91.21管理主防火墙，192.168.91.22管理备防火墙。两台防火墙拥有独立的管理IP。

11. 如何测试独立管理口和独立管理口的网关是否可以通信？独立管理口实际可以理解为一个轻量级的vdom，如果要测试此vdom里面的数据转发，需要先进入到此轻量级vdom里面然后再发起相应的ping测试，测试才是我们想要的结果。否则直接发起ping的话，就相当于在root vdom（业务处理的VDOM）发包，实际和独立管理口是隔离的是无关的，会引起误会/误解。

12. 测试独立管理口和独立管理口网关的测试，可以看到vsys_hamgmt有独立的路由表和管理路由。

```
FGT1-LEFT # exe enter ?
<name>    vdom name
root
vsys_hamgmt

FGT1-LEFT # exe enter vsys_hamgmt    //进入轻量级独立管理vdom
current vdom=vsys_hamgmt:1

FGT1-LEFT # get router info routing-table all    //拥有独立的路由表
...
Routing table for VRF=0
C       192.168.91.0/24 is directly connected, port6

FGT1-LEFT # diagnose ip route list
...
tab=254 vf=1 scope=0 type=1 proto=17 prio=0 0.0.0.0/0.0.0.0/0→0.0.0.0/0 pref=0.0.0.0 gwy=192.168.91.254
dev=8(port6)    //独立管理的默认路由
...

FGT1-LEFT # exe ping 192.168.91.254
PING 192.168.91.254 (192.168.91.254): 56 data bytes
64 bytes from 192.168.91.254: icmp_seq=0 ttl=128 time=0.9 ms
64 bytes from 192.168.91.254: icmp_seq=1 ttl=128 time=1.3 ms
64 bytes from 192.168.91.254: icmp_seq=2 ttl=128 time=0.8 ms
64 bytes from 192.168.91.254: icmp_seq=3 ttl=128 time=0.5 ms
64 bytes from 192.168.91.254: icmp_seq=4 ttl=128 time=0.7 ms

--- 192.168.91.254 ping statistics ---
5 packets transmitted, 5 packets received, 4 duplicates, 0% packet loss
round-trip min/avg/max = 0.5/1.9/4.3 ms

FGT-LEFT # diagnose sniffer packet any "host 192.168.91.254" 4
interfaces=[any]
filters=[host 192.168.91.254]
3.235814 port6 out 192.168.91.21 → 192.168.91.254: icmp: echo request    //匹配明细直连路由，ping数据从port6 out，可以成功ping通网关
3.235900 port6 in 192.168.91.254 → 192.168.91.21: icmp: echo reply
4.245672 port6 out 192.168.91.21 → 192.168.91.254: icmp: echo request
4.245747 port6 in 192.168.91.254 → 192.168.91.21: icmp: echo reply
```

13. 退出独立管理口轻量级vdom，进入root vdom，查看路由表，并尝试访问独立管理口的网关。

```
FGT1-LEFT # exe enter root
current vdom=root:0

FGT1-LEFT # get router info routing-table all    //业务的独立路由表，和独立管理的路由表完全独立，相当于路由的轻量级隔离
...
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.100.1.192, port2, [1/0]
C       192.168.10.0/24 is directly connected, port1
C       202.100.1.0/24 is directly connected, port2

FGT101E_Master_379 # execute ping 192.168.91.254  // 通过root ping 192.168.91.254
PING 192.168.91.254 (192.168.91.254): 56 data bytes
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

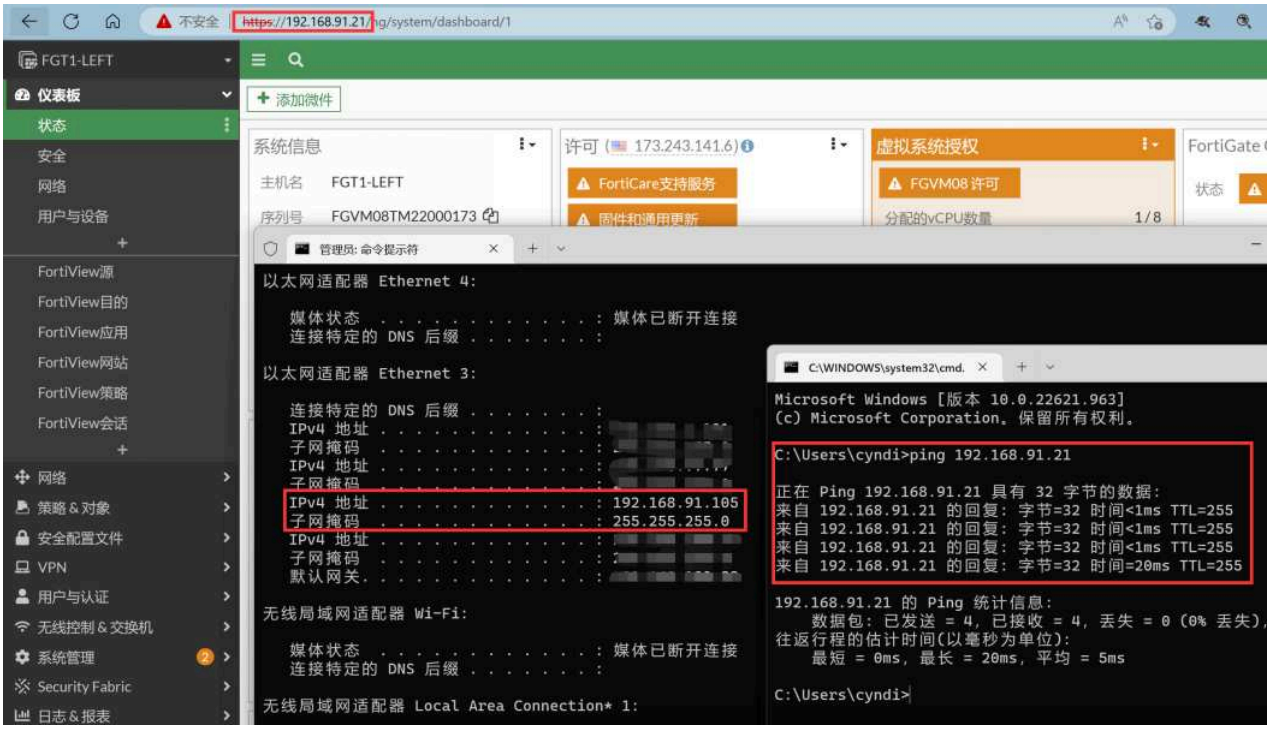
```
13
14  --- 192.168.91.254 ping statistics ---
15  5 packets transmitted, 0 packets received, 100% packet loss
16
17  FGT-LEFT # diagnose sniffer packet any "host 192.168.91.254 and icmp" 4
18  interfaces=[any]
19  filters=[host 192.168.91.254 and icmp]
20  12.785835 port2 out 202.100.1.21 → 192.168.91.254: icmp: echo request  // 匹配到默认路由，ping数据从port2 out，无法
21  ping通独立管理的网关，结果是正确的，但这不是我们想要的结果。处于一个错误的状态，实际并不是不通，只是没有进入vsys_hamgmt而已
22  13.795618 port2 out 202.100.1.21 → 192.168.91.254: icmp: echo request
23  14.805621 port2 out 202.100.1.21 → 192.168.91.254: icmp: echo request
24  15.815615 port2 out 202.100.1.21 → 192.168.91.254: icmp: echo request
    16.825621 port2 out 202.100.1.21 → 192.168.91.254: icmp: echo request
```

4. 测试备机的独立管理口网关ping测试。

```
1   FGT2-RIGHT # exe enter vsys_hamgmt
2   current vdom=vsys_hamgmt:1
3
4   FGT2-RIGHT # execute ping 192.168.91.254    //发起ping测试
5   PING 192.168.91.254 (192.168.91.254): 56 data bytes
6   64 bytes from 192.168.91.254: icmp_seq=0 ttl=255 time=0.3 ms
7   64 bytes from 192.168.91.254: icmp_seq=1 ttl=255 time=0.1 ms
8   64 bytes from 192.168.91.254: icmp_seq=2 ttl=255 time=0.1 ms
9   64 bytes from 192.168.91.254: icmp_seq=3 ttl=255 time=0.1 ms
10  64 bytes from 192.168.91.254: icmp_seq=4 ttl=255 time=0.1 ms
11  --- 192.168.91.254 ping statistics ---
12  5 packets transmitted, 5 packets received, 0% packet loss
13  round-trip min/avg/max = 0.1/0.1/0.3 ms
14
15  FGT2-RIGHT # execute enter root    //测试完毕，退出轻量级独立管理vdom
16  current vdom=root:0
```

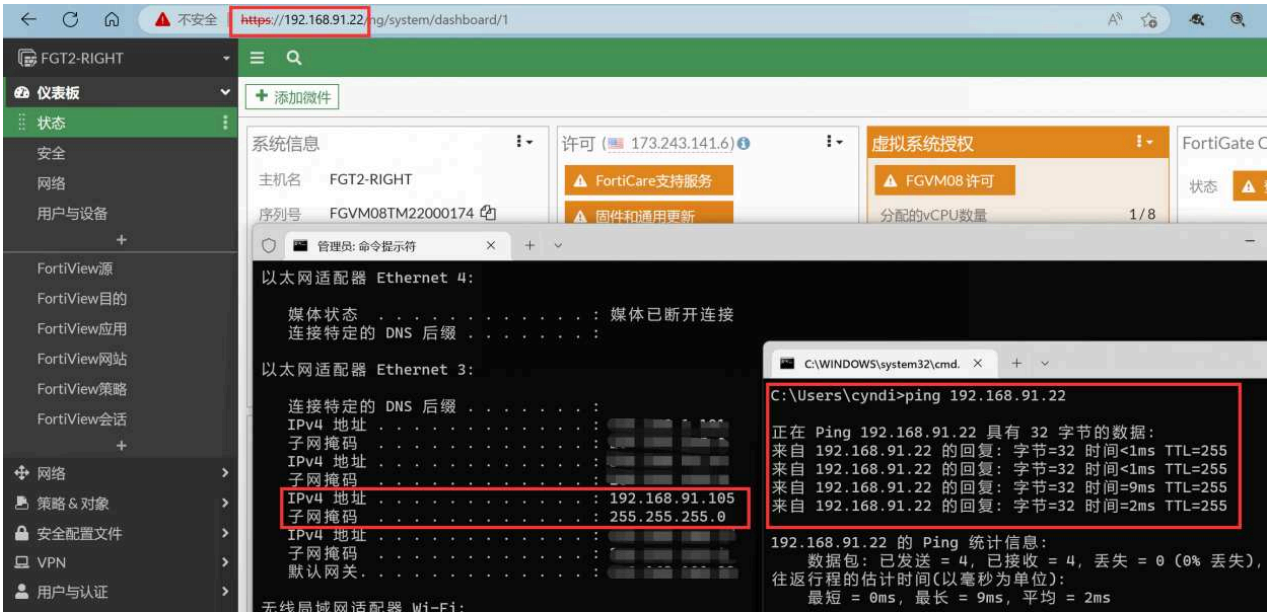
HTTPS、Ping管理

1. 通过独立管理IP：192.168.91.21管理主防火墙。



2. 通过独立管理IP：192.168.91.22管理备防火墙。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



SYSLOG

1. 确认通过192.168.10.1网管没问题的话，配置SYSLOG等本机发出的网管配置。

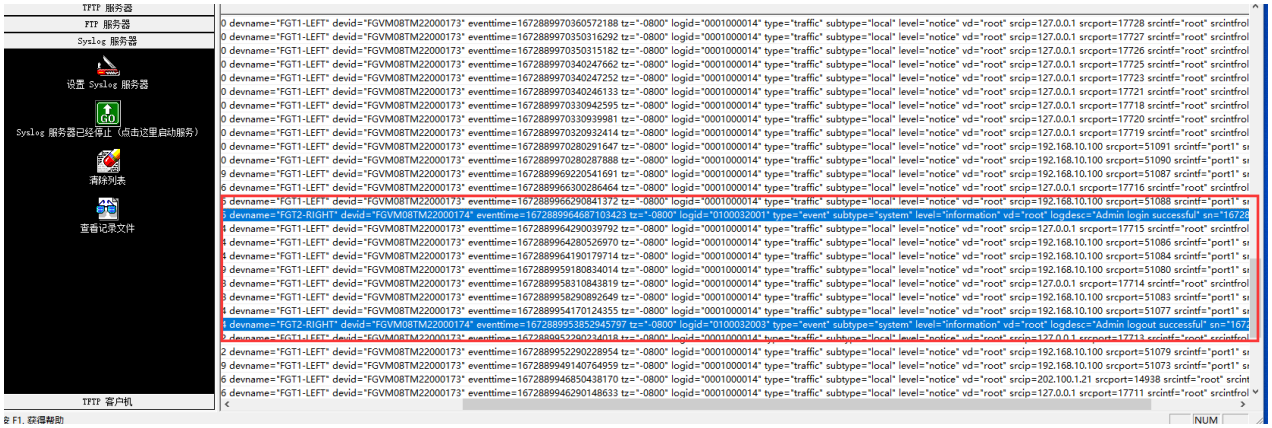



```
config log syslogd setting
    set status enable
    set server "192.168.10.100"
end
```

2. 主/备防火墙的日志都会通过业务接口port1 192.168.10.1将syslog日志发送出去，备防火墙的syslog日志会通过心跳线到主机，然后由主机代为转发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FGT1-LEFT # diagnose sniffer packet any "port 514" 4
interfaces=[any]
filters=[port 514]
0.918154 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 635    //主防火墙的syslog日志
0.918225 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 649
5.492057 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 649
5.961902 port_ha in 169.254.0.2.514 → 169.254.0.1.514: udp 454    //备防火墙的console登陆日志
5.962018 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 418
5.968684 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 554
8.314617 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 730
8.507346 port_ha in 169.254.0.2.514 → 169.254.0.1.514: udp 473    //备防火墙的console退出日志
8.507479 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 437
8.964545 port1 out 192.168.10.1.22418 → 192.168.10.125.514: udp 724
9.074989 port1 out 192.168.10.1.15840 → 192.168.10.125.514: udp 597
```



SNMP

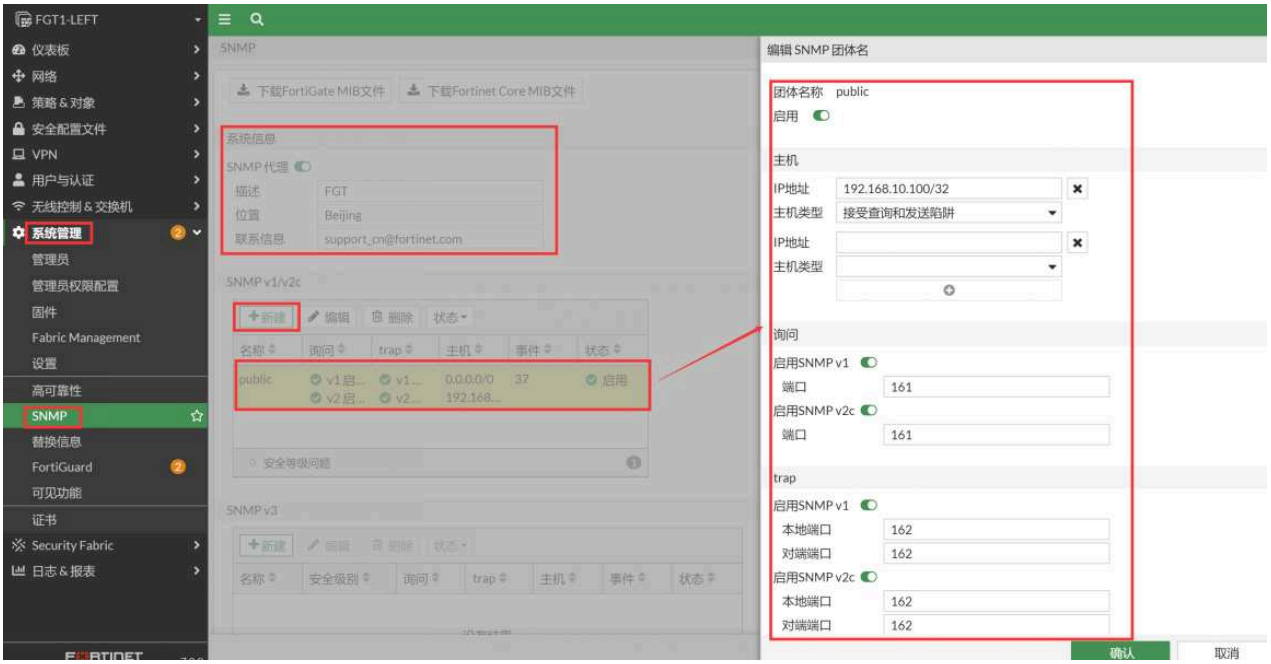
1. lan接口下开启SNMP协议。




```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
end
```

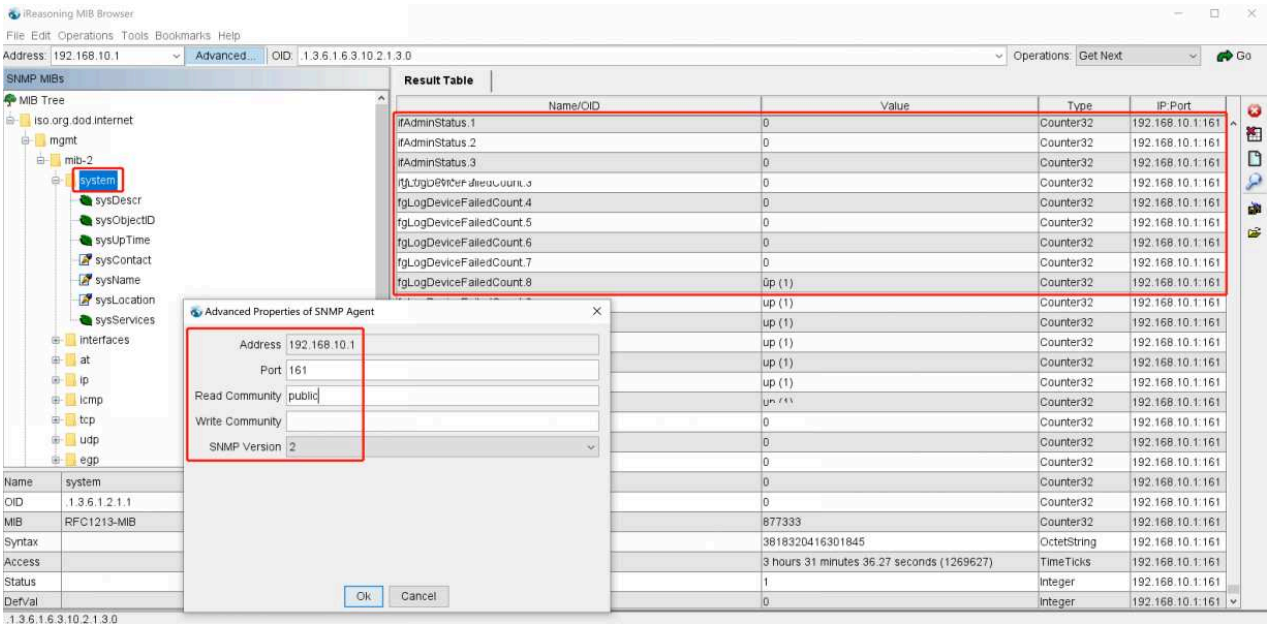
2. 开启SNMP功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



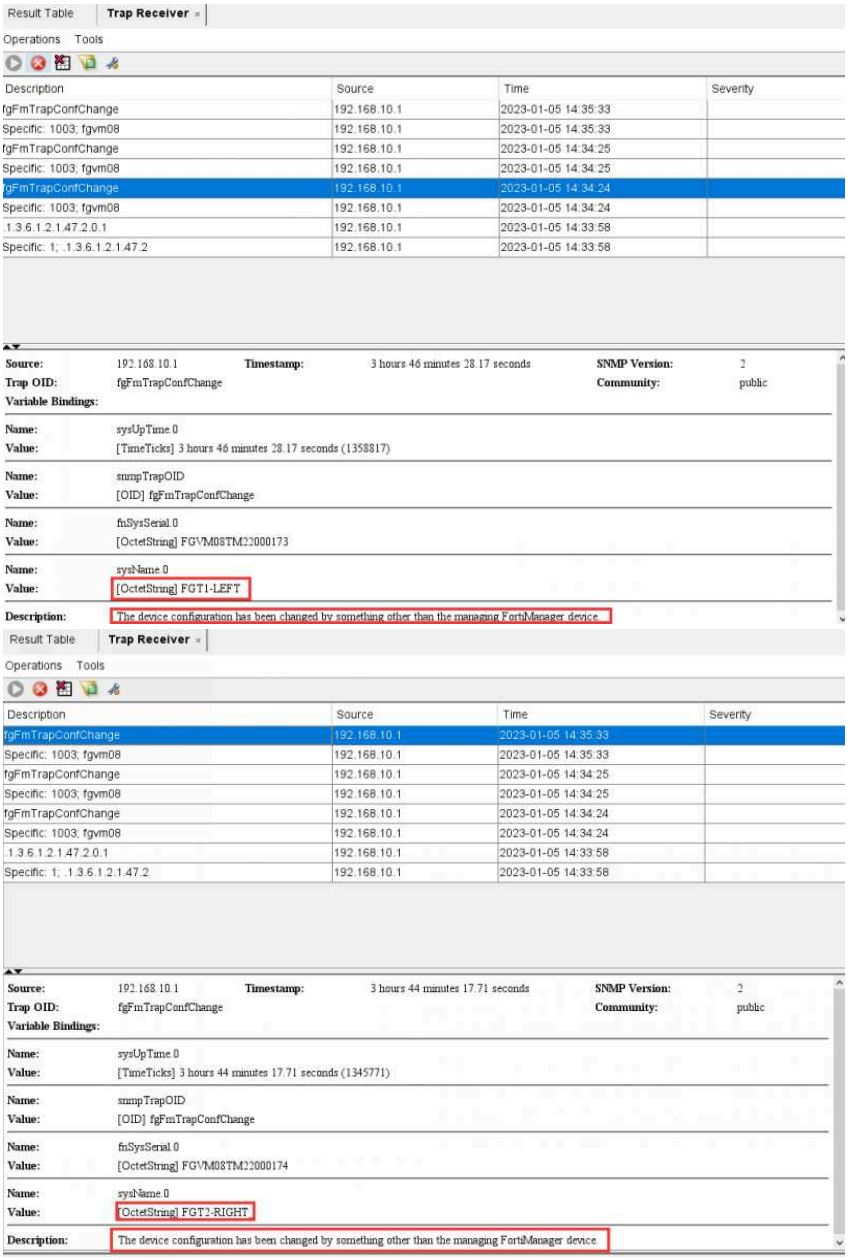

```
config system snmp sysinfo
    set status enable
    set description "FGT"
    set contact-info "support_cn@fortinet.com"
    set location "Beijing"
end

config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ip 192.168.10.100 255.255.255.255
            next
        end
    next
end
```

3. 在SNMP客户端对FortiGate的lan口进行get/walk操作，这里以IReasoning MIB Browser为例。



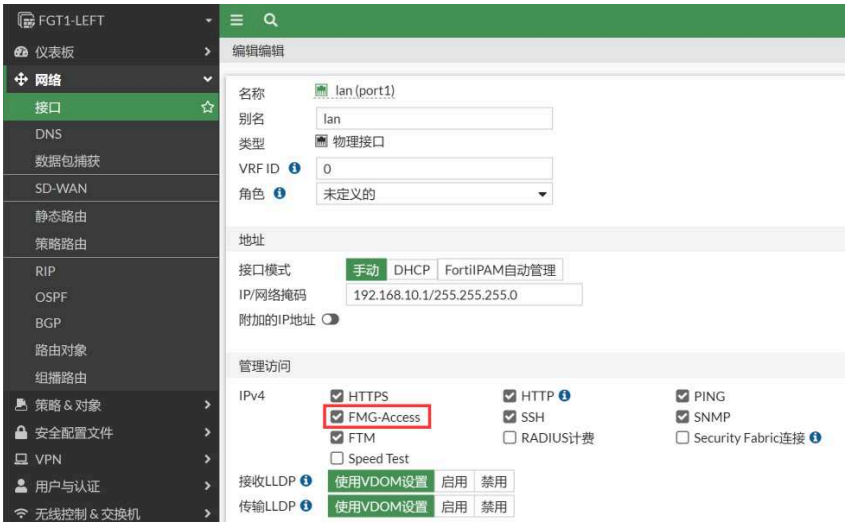
4. SNMP客户端接收到的FGT发送的trap信息，可以看到主备设备均通过主设备进行发送。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiManger管理

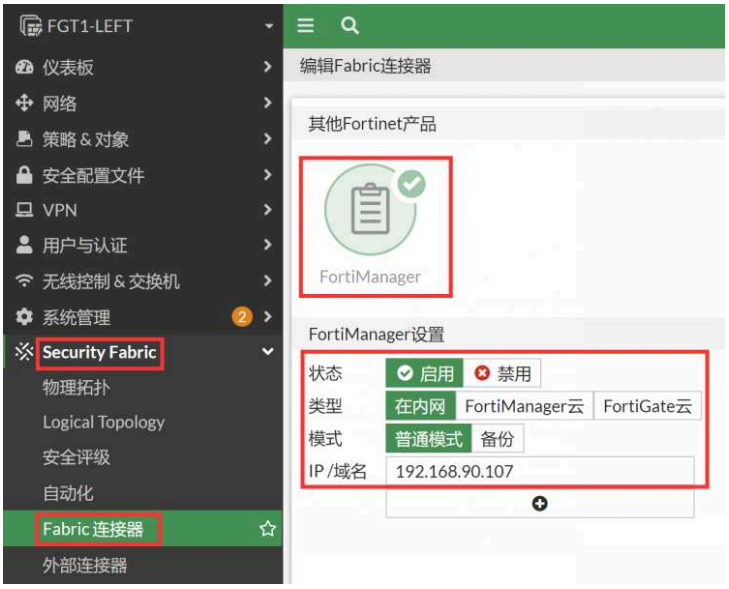
1. FortiManager通过FGT的lan口添加设备，在FGT的lan口下开启FMG管理协议。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
end
```

2. 配置防火墙主动连接FMG（如果FMG可以主动访问到FGT，也可以通过FMG主动添加FGT）。

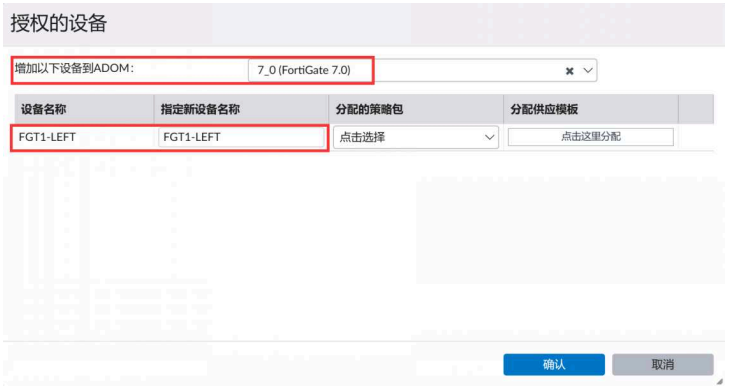



```
config system central-management
    set type fortimanager
    set fmg "192.168.90.107"
end
```

3. 如果是FGT主动去注册FMG，则FMG会有未注册的设备提示。



4. 只需要将设备添加到FMG的对应ADOM的设备管理中即可。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

5. 授权完成。



6. 在FMG中可以对FGT进行管理。



HA-direct

1. 以上的发送syslog都是通过业务接口port1 192.168.10.1发送的，如果想要如syslog、FortiAnalyzer、LDAP、Radius、TACACS+、sFlow、NetFlow等报文通过mgmt（port6）发送出去，则需要在HA里面开启一个ha-direct功能才可以实现。该命令在主机开启后，也会同步到备机。

> **重要**
>
> 开启HA配置下的“HA-direct”后，主机和备机的syslog、FortiAnalyzer、LDAP、Radius、TACACS+、sFlow、NetFlow等报文均会通过各自的独立管理口发出，而不是通过主机的业务口发出。

```
FGT1-LEFT # config sys ha

FGT1-LEFT (ha) # set ha-direct ?
enable     Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer,
FortiSandbox, sFlow, and Netfl.
disable    Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer,
FortiSandbox, sFlow, and Netf.

FGT1-LEFT (ha) # set ha-direct enable
FGT1-LEFT (ha) # end
When ha-direct is enabled, source ip may not work.
We recommend to unset all log-related, netflow and sflow source ip.
By selecting to continue, all source ip will be unset.
Do you want to continue? (y/n)y
```

2. 再次查看syslog的发送情况，syslog这次就从mgmt（port6）发送出去了。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FGT1-LEFT # diagnose sniffer packet any "port 514" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 514]
1.189223 port6 out 192.168.91.21.3320 → 192.168.10.100.514: udp 553
1.189276 port6 out 192.168.91.21.3320 → 192.168.10.100.514: udp 553
1.189278 port6 out 192.168.91.21.3320 → 192.168.10.100.514: udp 553
2.189291 port6 out 192.168.91.21.3320 → 192.168.10.100.514: udp 556
3.188617 port6 out 192.168.91.21.3320 → 192.168.10.100.514: udp 613
4.194761 port6 out 192.168.91.21.3320 → 192.168.10.100.514: udp 488

FGT2-RIGHT # diagnose sniffer packet any "port 514" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 514]
7.137889 port6 out 192.168.91.22.5532 → 192.168.10.100.514: udp 489
8.136846 port6 out 192.168.91.22.5532 → 192.168.10.100.514: udp 554
8.136907 port6 out 192.168.91.22.5532 → 192.168.10.100.514: udp 554
8.136909 port6 out 192.168.91.22.5532 → 192.168.10.100.514: udp 554
8.136911 port6 out 192.168.91.22.5532 → 192.168.10.100.514: udp 554
10.135873 port6 out 192.168.91.22.5532 → 192.168.10.100.514: udp 554
```

3. 如果是snmp的trap想从独立管理口发送（或通过独立管理口读取OID），则需要在SNMP的community配置中，对host开启ha-direct功能，主备同步。

```
config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ip 192.168.10.100 255.255.255.255
                set ha-direct enable
            next
        end
    next
end
```

4. 再次查看snmp trap的发送情况，trap这次就从mgmt（port6）发送出去了。

```
FGT1-LEFT # diagnose sniffer packet any "port 162" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 162]
10.358519 port6 out 192.168.91.21.162 → 192.168.10.100.162: udp 106
10.358662 port6 out 192.168.91.21.162 → 192.168.10.100.162: udp 128

FGT2-RIGHT # diagnose sniffer packet any "port 162" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 162]
6.257505 port6 out 192.168.91.22.162 → 192.168.10.100.162: udp 43
6.257678 port6 out 192.168.91.22.162 → 192.168.10.100.162: udp 68
77.293372 port6 out 192.168.91.22.162 → 192.168.10.100.162: udp 43
77.293562 port6 out 192.168.91.22.162 → 192.168.10.100.162: udp 68
122.341966 port6 out 192.168.91.22.162 → 192.168.10.100.162: udp 107
122.342170 port6 out 192.168.91.22.162 → 192.168.10.100.162: udp 129
```

5. 关于FMG还是建议使用业务接口进行管理，不能使用独立管理口进行管理。对于FMG来说HA-Cluster就是一台设备，因此需要一个固定的IP地址来网管FGT会比较合适，可以有效的避免HA发生切换的时候，FGT和FMG的tunnel中断的情况。

6. 关于DNS和FortiGuard还是通过root VDOM（管理VDOM）进行解析和更新的。

7. 要彻底的完完全全的实现HA-Cluster的独立管理同时又与业务完全隔离，则需要使用独立管理VDOM，请参考HA双机热备→HA-Cluster的网管→HA集群带外管理→独立管理VDOM ↗章节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

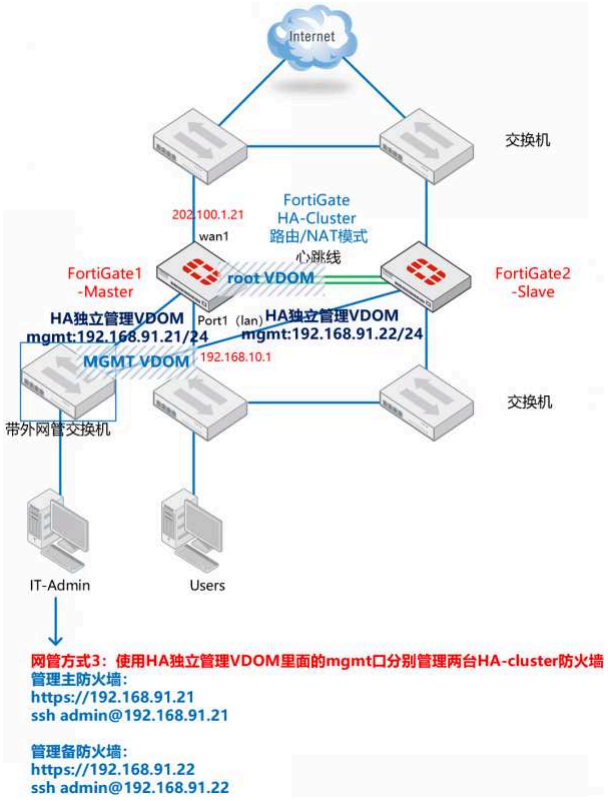
独立管理VDOM

网络需求

1. 在HA集群中，所有集群成员的配置全部相同，通过IP只能管理到主设备，无法通过IP对每个slave设备进行单独的管理。同时为了业务的安全，需要将管理网络与业务网络独立开。包括独立管理，包括syslog日志、SNMP、Radius、TACACS+等。
2. 另外包括DNS、Fortiguard更新也需要通过管理口进行处理。为实现如上需求，HA使用独立的管理接口是无法完全满足了，这是就需要使用最终极的解决方案独立管理VDOM了。

> **重要**
>
> 该功能主要用于单独的VDOM进行FortiGuard更新、DNS查询以及日志/认证/管理业务，HA成员间独立管理VDOM内的配置是不同步的，如果FortiGate被FortiManager管理，请勿开启此功能，否则HA切换后可能导致FortiManager配置与FortiGate不一致。

网络拓扑



配置要点

- 配置HA基础配置
- 配置基础LAN/WAN上网服务
- 配置HA独立VDOM
- 配置防火墙的SYSLOG、SNMP和FMG

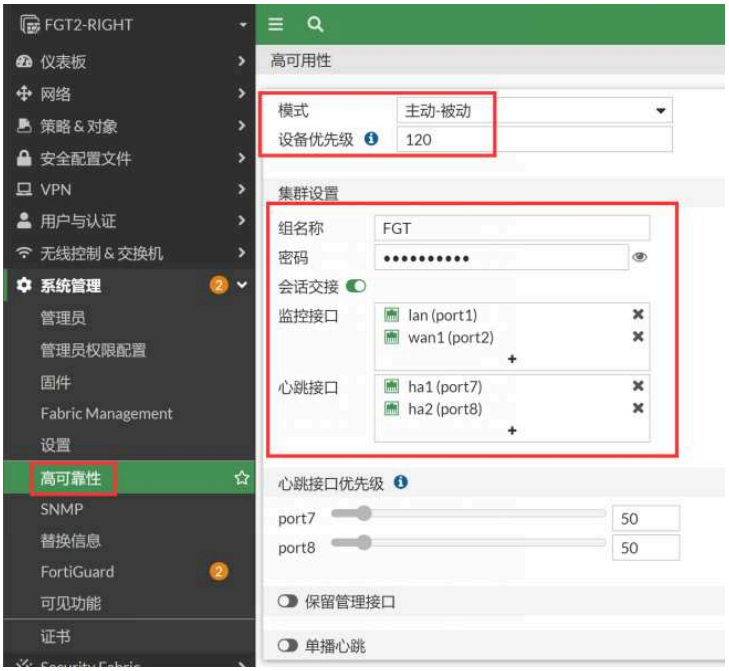
配置步骤和结果验证

1. 配置HA基础配置，初始化配置防火墙的时候可以通过mgmt口登陆到防火墙上，一般mgmt口的管理IP是192.168.1.99，第一步可以通过此IP登陆防火墙（参考系统管理→管理方式→Web管理 ↗章节），或者通过console口管理防火墙（参考系统管理→管理方式→Console管理 ↗章节）。具体型号初始化如果网管和接口的网管IP信息等可参考https://docs.fortinet.com/product/fortigate/hardware ↗ 或 https://docs.fortinet.com/document/fortigate/hardware/fortigate-quickstart-guide-high-end?model=all ↗ 。
2. 按照以上方式登陆第一次开箱的防火墙。先登陆主防火墙，并配置进行HA的基础配置，然后登陆到备防火墙，配置备防火墙的HA基础配置。
3. 分别配置主防火墙和备防火墙的HA，主防火墙优先级调整为150，备防火墙的优先级保持默认的120，配置HA-cluster组名字和密码，监控业务接口wan1和port1，使用HA1和HA2接口将二者互联。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
XU4Yv532eMH20TXkbxDMQWRNs+ChZrIVXcotCFVP2C86QBl2zhznTNU+0PDKw5Vlvtm6B+NCZ+f+1EiT3MsUteDHW82Aten6q+Yu6zAT5NuXYYIKnV
pG=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set override disable
    set priority 150
    set monitor "port1" "port2"
end
```




```
config system ha
    set group-name "FGT"
    set mode a-p
    set password ENC
HzpTLoO69D1nrZ9QZbKFDbuUmCefmDRbZqTvgSseAgh2zU8JOHq1bthC750a+p5S/rkfRSROmhVMqOKRbBZkir3C8VWW9l+h7jl7Xp4N5sdA1CmDSU
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
zX=
    set hbdev "port7" 50 "port8" 50
    set session-pickup enable
    set override disable
    set priority 120
    set monitor "port1" "port2"
end
```

4. 双方的HA配置完毕之后将ha1和ha2线相互直连，将会进行HA的选举，此时优先级150高的FGT将成为主防火墙，优先级低的120的FGT将成为备防火墙。然后备防火墙的配置将会和主防火墙进行同步，备防火墙所有配置和主防火墙一致，此时备防火墙也将不再可以WEB/SSH登录，仅仅可以Console登录。后续所有的操作和配置都在主防火墙上的GUI、SSH或Console完成。

5. 选举结果如下，FGT1-LEFT成为主设备。

```
FGT1-LEFT # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:22783 b:12890083
        traffic.total = s:0 p:22793 b:12890691
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=0 Debug=0
nvcluster=1, ses_pickup=1, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM22000173:      Primary, serialno_prio=1, usr_priority=150, hostname=FGT1-LEFT
FGVM08TM22000174:    Secondary, serialno_prio=0, usr_priority=120, hostname=FGT2-RIGHT

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0:
FGVM08TM22000173:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM22000174:    Secondary, ha_prio/o_ha_prio=1/1
```

6. 这三个命令都可以看到HA的选举结果和HA状态。

```
# diagnose sys ha status
# get system status
# get system ha status
```

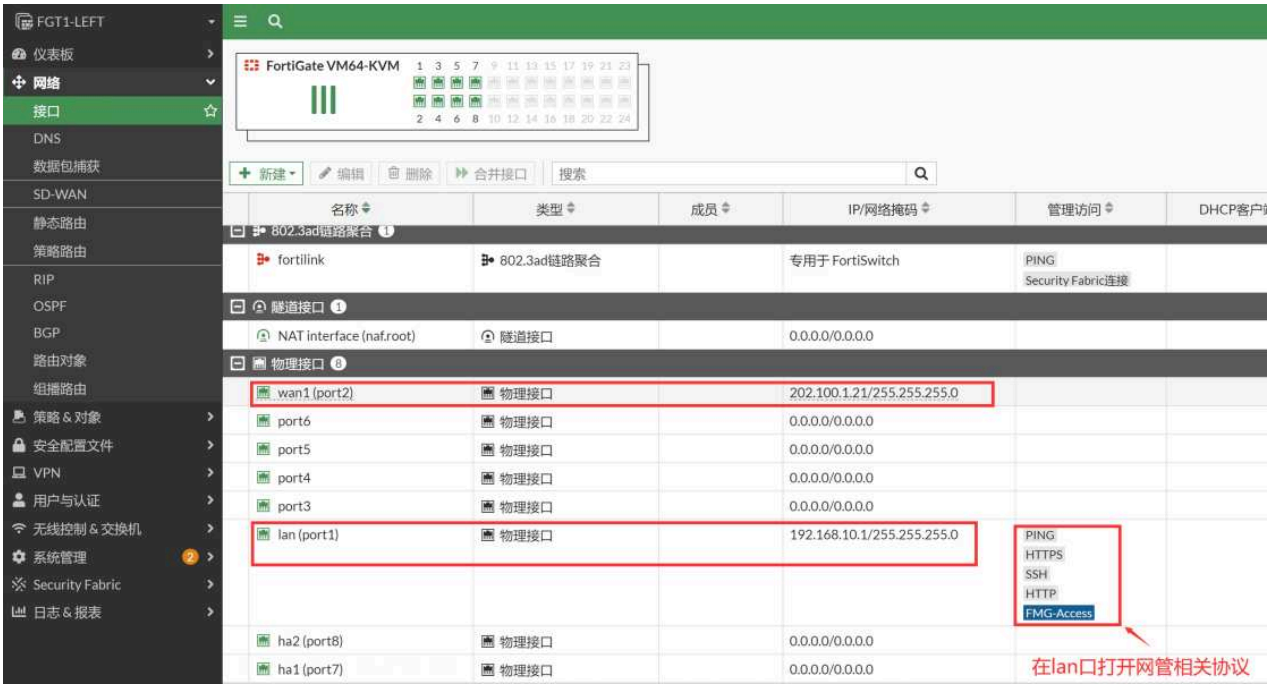
7. GUI查看HA的选举结果和状态。



8. 配置基础LAN/WAN上网服务。此步骤为正常上网的基础配置，大概的步骤是配置接口IP、配置默认路由、配置策略即可实现防火墙的简单上网配置。（所有配置都在主防火墙上完成，备防火墙此时不可以登陆）

9. 配置接口IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 202.100.1.21 255.255.255.0
        set type physical
        set alias "wan1"
        set snmp-index 2
    next
end
```

.0. 配置默认路由。




```
config router static
    edit 1
        set gateway 202.100.1.192
        set device "port2"
    next
end
```

.1. 配置上网策略。

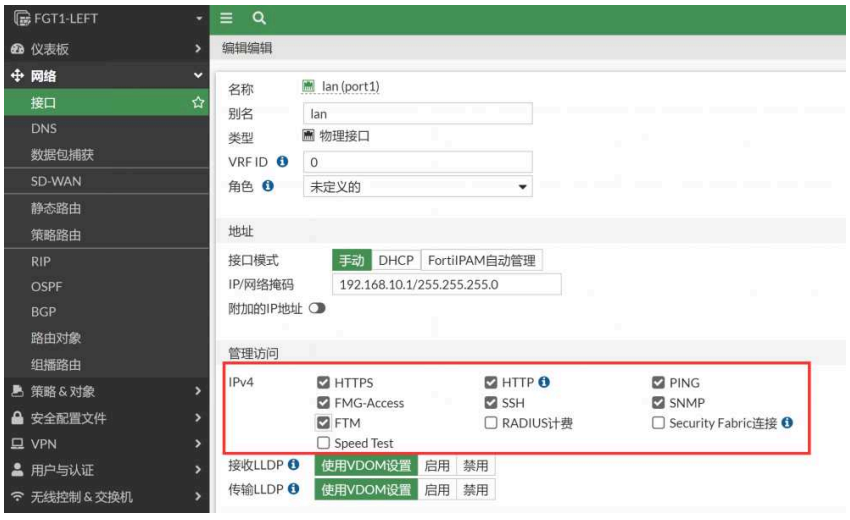
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "LAN_192.168.10.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

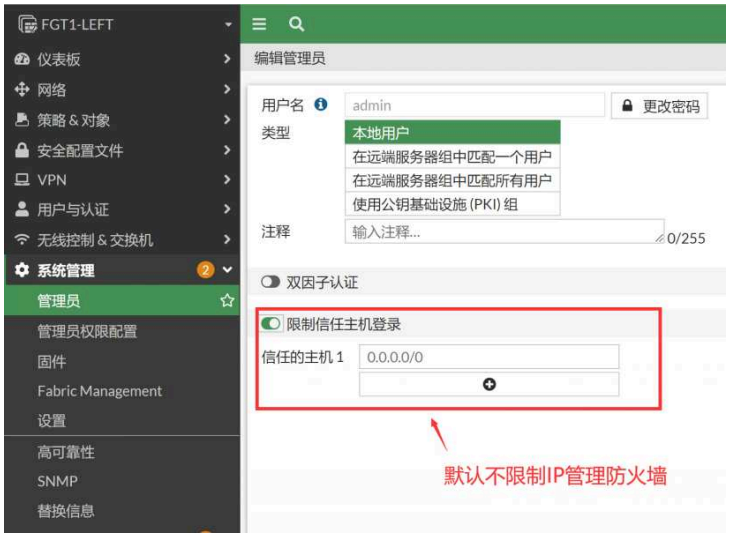
2. 配置LAN口网管相关参数，关于网管目前可以通过port1（lan）的192.168.10.1进行管理，比较关键的网管因素是：

   - port1接口下开启了网管的协议，比如https、http、ssh、snmp等。



   - 管理员可信任主机如果配置了的话，需要包含发起管理请求的主机IP或网段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 客户端PC到FGT的来回路由可达，可以通过ping和tracert测试。
- 上面1、2点确认没有问题之后，还是遇到不通的情况，可以通过sniffer抓包和debug flow确认问题所在。

```
FGT # diagnose sniffer packet any "host 192.168.10.1" 4 0 l
```

- 如果跨接口管理防火墙，比如处于port1的PC要通过防火墙port2接口的IP管理防火墙，则需要主要有port1到port2的放通策略，否则数据也是不通的。
- 出现网管不了的情况，99%就是以上的原因了。

3. 配置HA独立VDOM，首先需要开启VDOM特性（主设备上配置，会自动同步到备机）。

```
FGT1-LEFT # config sys global
FGT1-LEFT (global) # set vdom-mode
FGT1-LEFT (global) # set vdom-mode multi-vdom
FGT1-LEFT (global) # end

You will be logged out for the operation to take effect.
Do you want to continue? (y/n)y
exit

FGT1-LEFT login: admin
Password:
Welcome!
```

4. 创建新的MGMT独立管理VDOM（主设备上配置，会自动同步到备机）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
FGT1-LEFT # config vdom
FGT1-LEFT (vdom) # edit MGMT
FGT1-LEFT (MGMt) # end
```

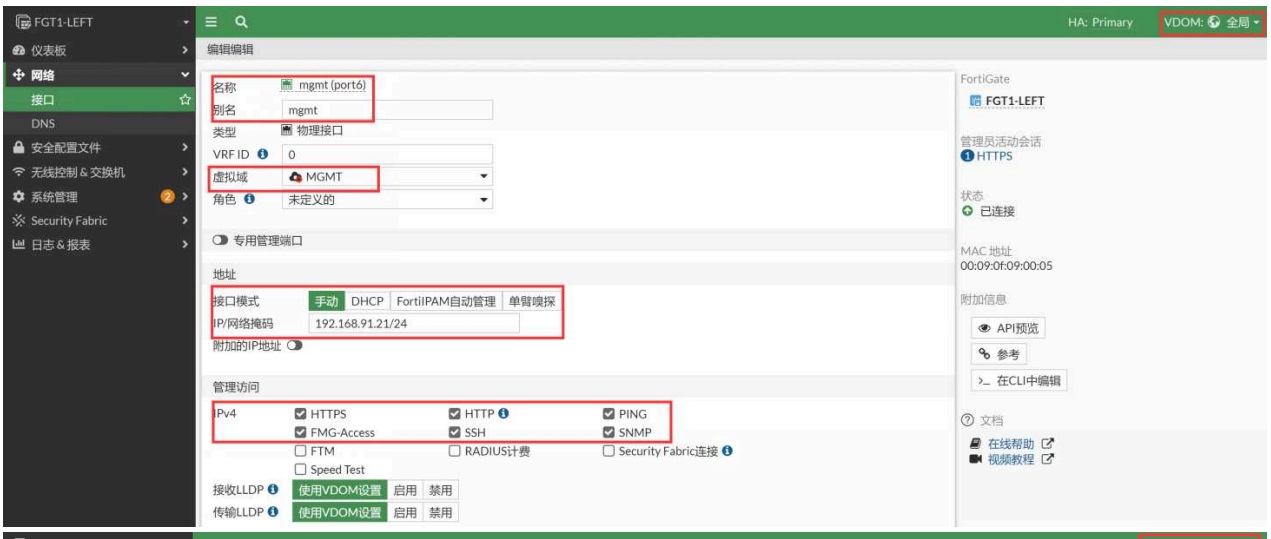
5. 将MGMT独立管理VDOM修改为管理VDOM（只能命令行修改），该配置主备会同步。

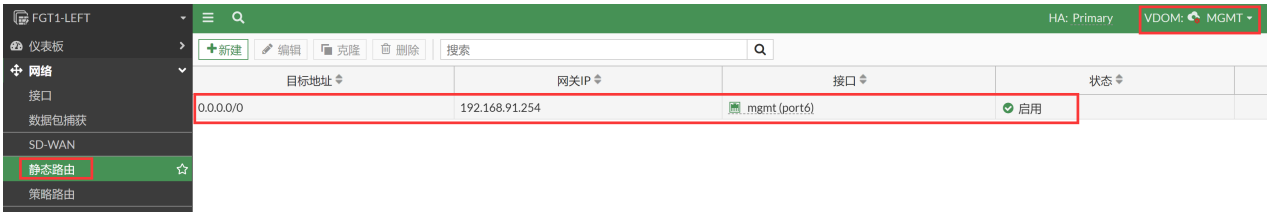
```
FGT1-LEFT # config global
FGT1-LEFT (global) # config system global
FGT1-LEFT (global) # set management-vdom MGMT     //设置MGMT为管理VDOM，也就是说fortiguard、dns、ntp ... 等等主动更新，都是从MGMT这个VDOM发起，是一个管理的VDOM
FGT1-LEFT (global) # end
FGT1-LEFT (global) # end
```

6. HA里面开启独立管理VDOM，该配置主备会同步。

```
FGT1-LEFT # config global
FGT1-LEFT (global) # config system ha
FGT1-LEFT (ha) # set standalone-mgmt-vdom enable
FGT1-LEFT (ha) # end
FGT1-LEFT (global) # end
```

7. 将mgmt（port6）接口加入到MGMT VDOM中，并配置上管理IP和默认路由。






```
config global
config system interface
    edit "port6"
        set vdom "MGMT"
        set ip 192.168.91.21 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type physical
        set alias "mgmt"
        set snmp-index 6
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FGT1-LEFT # config vdom
FGT1-LEFT (vdom) # edit MGMT
current vf=MGMT:4
config router static
    edit 1
        set gateway 192.168.91.254
        set device "port6"
    next
end
```

8. 在主机的MGMT VDOM中ping网关192.168.91.254。

```
FGT1-LEFT # config vdom
FGT1-LEFT (vdom) # edit MGMT
current vf=MGMT:4

FGT1-LEFT (MGMT) # exe ping 192.168.91.254
PING 192.168.91.254 (192.168.91.254): 56 data bytes
64 bytes from 192.168.91.254: icmp_seq=0 ttl=128 time=1.3 ms
64 bytes from 192.168.91.254: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 192.168.91.254: icmp_seq=2 ttl=128 time=0.6 ms
64 bytes from 192.168.91.254: icmp_seq=3 ttl=128 time=0.5 ms
64 bytes from 192.168.91.254: icmp_seq=4 ttl=128 time=0.8 ms
--- 192.168.91.254 ping statistics ---
5 packets transmitted, 5 packets received, 4 duplicates, 0% packet loss
round-trip min/avg/max = 0.5/0.7/1.4 ms
```

9. 此时备机是无法WEB/SSH登陆的需要通过主机的命令（或者Console线）连到备机的命令行界面。

```
FGT1-LEFT # config global
FGT1-LEFT (global) # exe ha manage ?
<id>    please input peer box index.
<0>     Subsidiary unit FGVM08TM22000174

FGT1-LEFT (global) # exe ha manage 0 admin
Warning: Permanently added '169.254.0.1' (ED25519) to the list of known hosts.
admin@169.254.0.1's password:
FGT2-RIGHT #
```

10. 备防火墙那边会自动同步VDOM和mgmt加入到MGMT的配置（如果配置同步不正常，可以将备机重启，并等待配置同步完成，再操作），而独立管理MGMT-VDOM内部的配置是不会同步的，因此只需要修改备防火墙的mgmt的接口IP和路由即可。

```
FGT2-RIGHT # config vdom
FGT2-RIGHT (vdom) # edit MGMT
current vf=MGMT:4

FGT2-RIGHT (MGMT) # config system interface
FGT2-RIGHT (interface) # edit port6
FGT2-RIGHT (port6) # set ip 192.168.91.22/24
FGT2-RIGHT (port6) # set allowaccess ping https ssh snmp http fgfm
FGT2-RIGHT (port6) # set alias "mgmt"
FGT2-RIGHT (port6) # end
FGT2-RIGHT (MGMT) # end
```

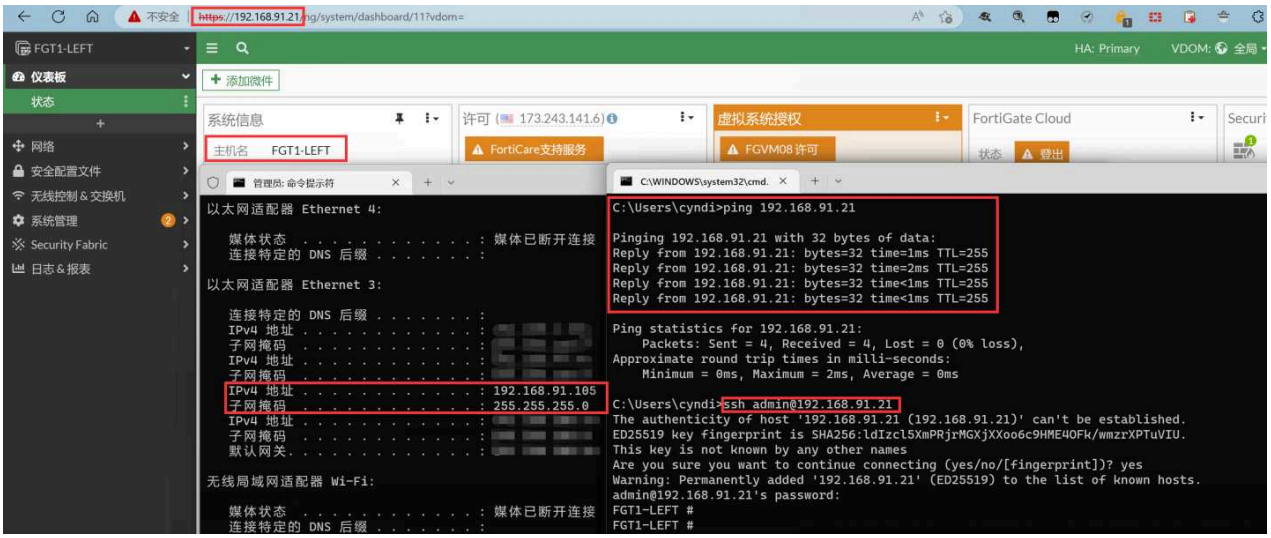
11. 备机使用MGMT VDOM ping网关192.168.91.254。

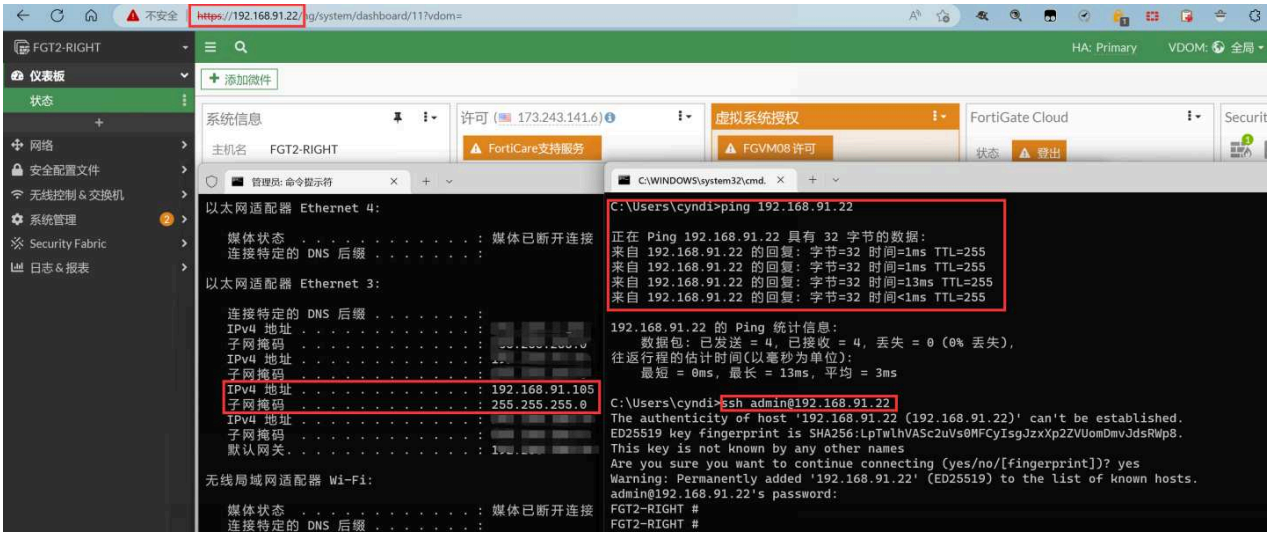
```
FGT2-RIGHT # config vdom
FGT2-RIGHT (vdom) # edit MGMT
current vf=MGMT:4

FGT2-RIGHT (MGMT) # exe ping 192.168.91.254
PING 192.168.91.254 (192.168.91.254): 56 data bytes
64 bytes from 192.168.91.254: icmp_seq=0 ttl=128 time=2.2 ms
64 bytes from 192.168.91.254: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 192.168.91.254: icmp_seq=2 ttl=128 time=0.7 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
64 bytes from 192.168.91.254: icmp_seq=3 ttl=128 time=0.7 ms
64 bytes from 192.168.91.254: icmp_seq=4 ttl=128 time=0.5 ms
--- 192.168.91.254 ping statistics ---
5 packets transmitted, 5 packets received, 4 duplicates, 0% packet loss
round-trip min/avg/max = 0.5/1.0/2.3 ms
```

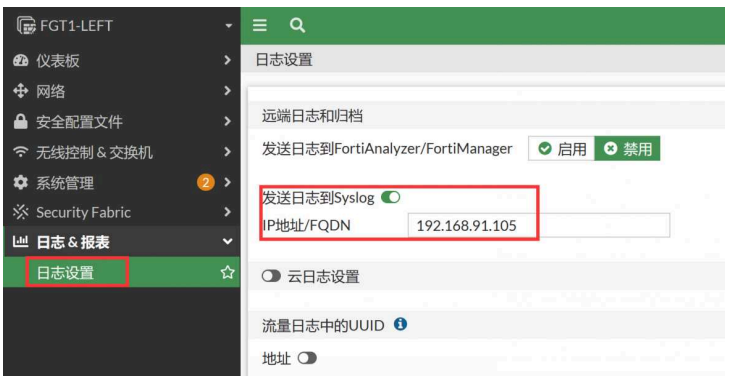
2. 备机也配置完毕，这个时候可以通过GUI登录到备机，查看备机的GUI配置。可以通过192.168.91.21和192.168.91.22分别管理到主防火墙和备防火墙了。





SYSLOG

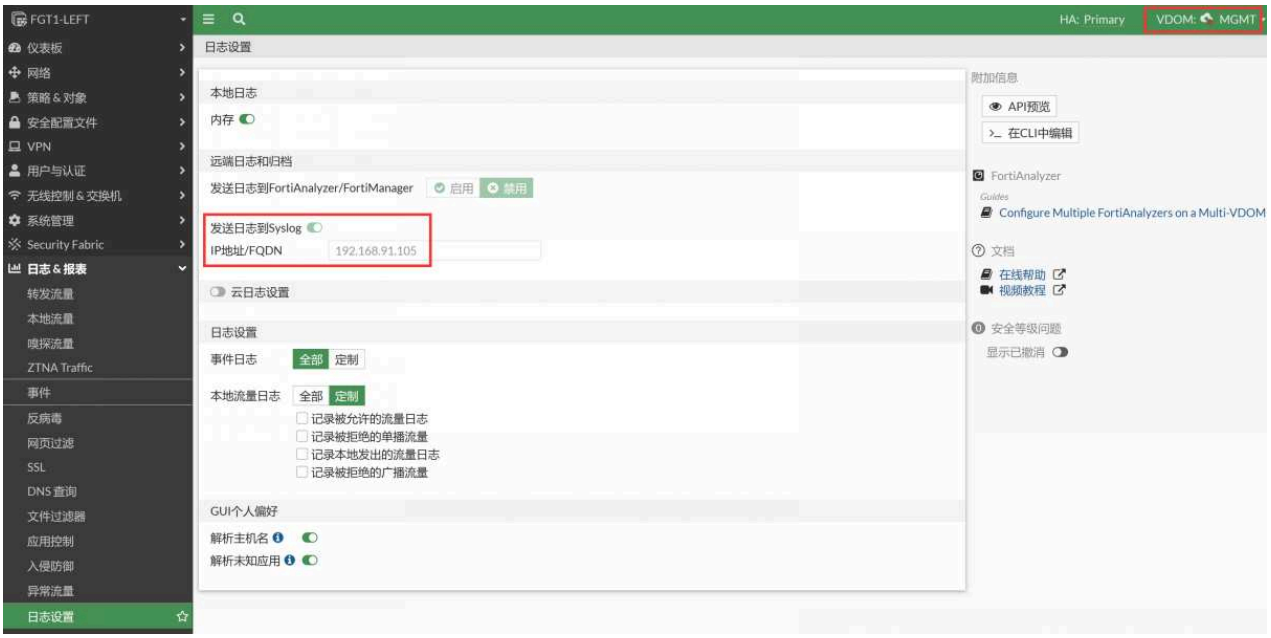
1. 配置SYSLOG等本机发出的网管配置。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config global
config log syslogd setting
    set status enable
    set server "192.168.91.105"
end
```

2. 默认情况下MGMT和root会继承global的syslog日志配置。



3. 主/备防火墙的日志都会通过独立管理VDOM的mgmt（port6）192.168.91.21和192.168.91.22将syslog日志发送出去。

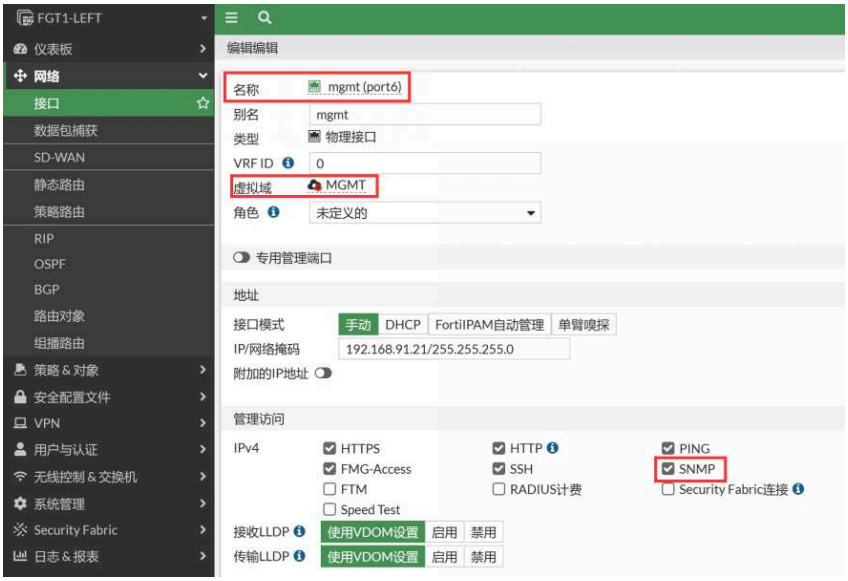
```
FGT1-LEFT (MGMT) # diagnose sniffer packet any "port 514" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 514]
1.159125 port6 out 192.168.91.21.19604 → 192.168.91.105.514: udp 600
1.159404 port6 out 192.168.91.21.19604 → 192.168.91.105.514: udp 553
1.159522 port6 out 192.168.91.21.19604 → 192.168.91.105.514: udp 553
3.158564 port6 out 192.168.91.21.19604 → 192.168.91.105.514: udp 553
5.159318 port6 out 192.168.91.21.19604 → 192.168.91.105.514: udp 608
6.158835 port6 out 192.168.91.21.19604 → 192.168.91.105.514: udp 600

FGT2-RIGHT (MGMT) # diagnose sniffer packet any "port 514" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 514]
4.513098 port6 out 192.168.91.22.12931 → 192.168.91.105.514: udp 554
10.513817 port6 out 192.168.91.22.12931 → 192.168.91.105.514: udp 554
11.512382 port6 out 192.168.91.22.12931 → 192.168.91.105.514: udp 554
11.512444 port6 out 192.168.91.22.12931 → 192.168.91.105.514: udp 554
11.512445 port6 out 192.168.91.22.12931 → 192.168.91.105.514: udp 554
11.512447 port6 out 192.168.91.22.12931 → 192.168.91.105.514: udp 554
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



SNMP

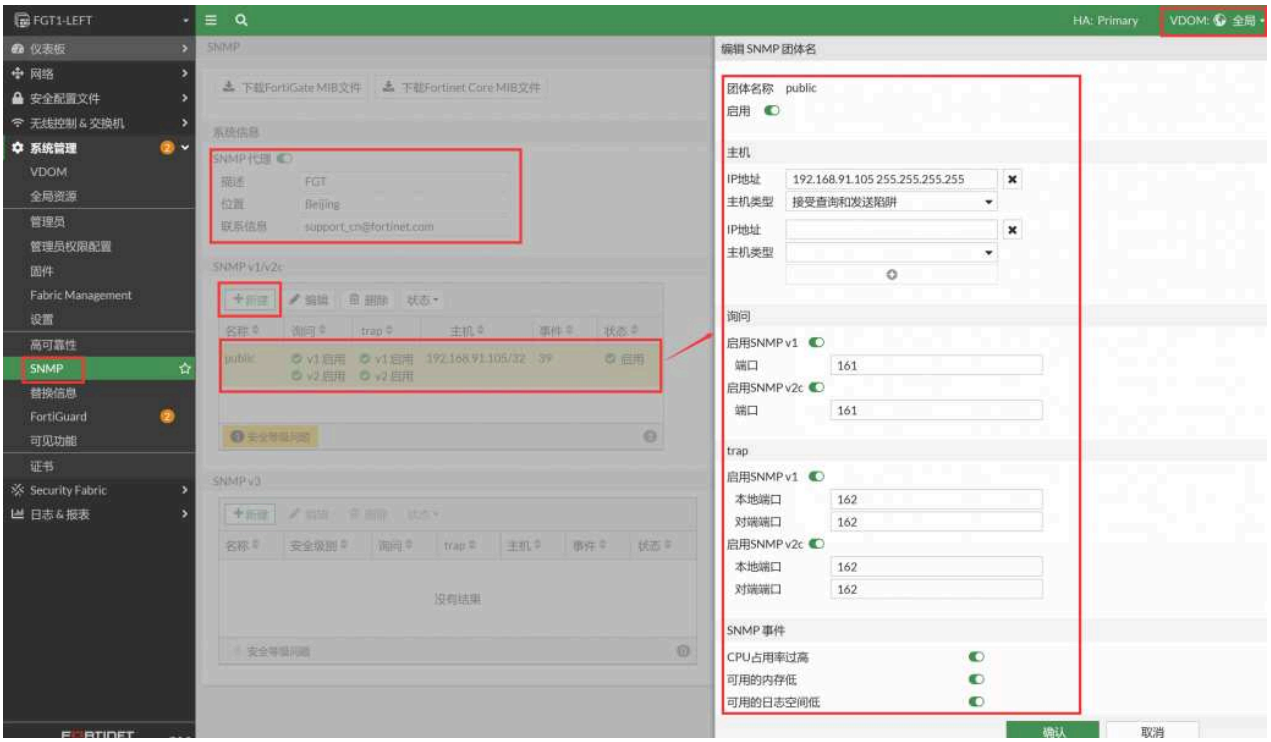
1. VDOM-MGMT的mgmt（port6）接口下开启SNMP协议，主设备和备设备都要开，VDOM-MGMT里面的配置不同步。




```
FGT1-LEFT:
config vdom
edit MGMT
config system interface
    edit "port6"
        set vdom "root"
        set ip 192.168.91.21 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm
        set type physical
        set alias "mgmt"
    next
end

FGT2-RIGHT:
config vdom
edit MGMT
config system interface
    edit "port6"
        set vdom "root"
        set ip 192.168.91.22 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm
        set type physical
        set alias "mgmt"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 进入全局VDOM，开启SNMP功能，此配置主备同步。

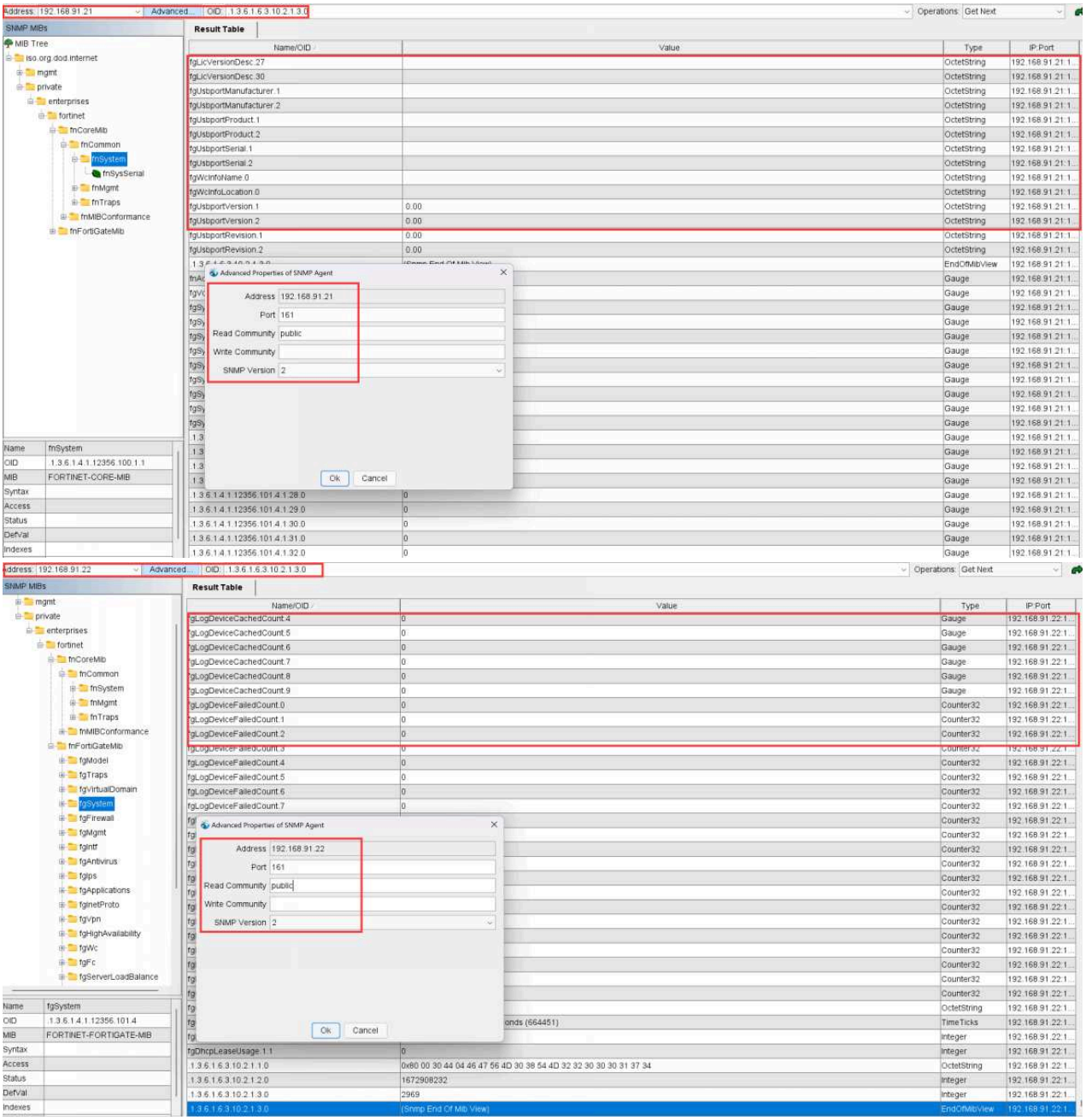



```
config global
config system snmp sysinfo
    set status enable
    set description "FGT"
    set contact-info "support_cn@fortinet.com"
    set location "Beijing"
end

config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
                set ip 192.168.91.105 255.255.255.255
            next
        end
    next
end
```

3. 在SNMP客户端对主设备和备设备的port6口进行get/walk操作，这里以iReasoning MIB Browser为例，可以正常读取SNMP节点信息。

```
FGT1-LEFT (MGMT) # dia sniff pa any "port 161" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 161]
44.345632 port6 in 192.168.91.105.50268 → 192.168.91.21.161: udp 45
44.346025 port6 in 192.168.91.105.50268 → 192.168.91.21.161: udp 45
44.346912 port6 out 192.168.91.21.161 → 192.168.91.105.50268: udp 45
44.347040 port6 out 192.168.91.21.161 → 192.168.91.105.50268: udp 45

FGT2-RIGHT (MGMT) # dia sniff pa any "port 161" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 161]
8.956697 port6 in 192.168.91.105.50265 → 192.168.91.22.161: udp 45
8.957084 port6 in 192.168.91.105.50265 → 192.168.91.22.161: udp 45
8.958027 port6 out 192.168.91.22.161 → 192.168.91.105.50265: udp 45
8.958123 port6 out 192.168.91.22.161 → 192.168.91.105.50265: udp 45
```

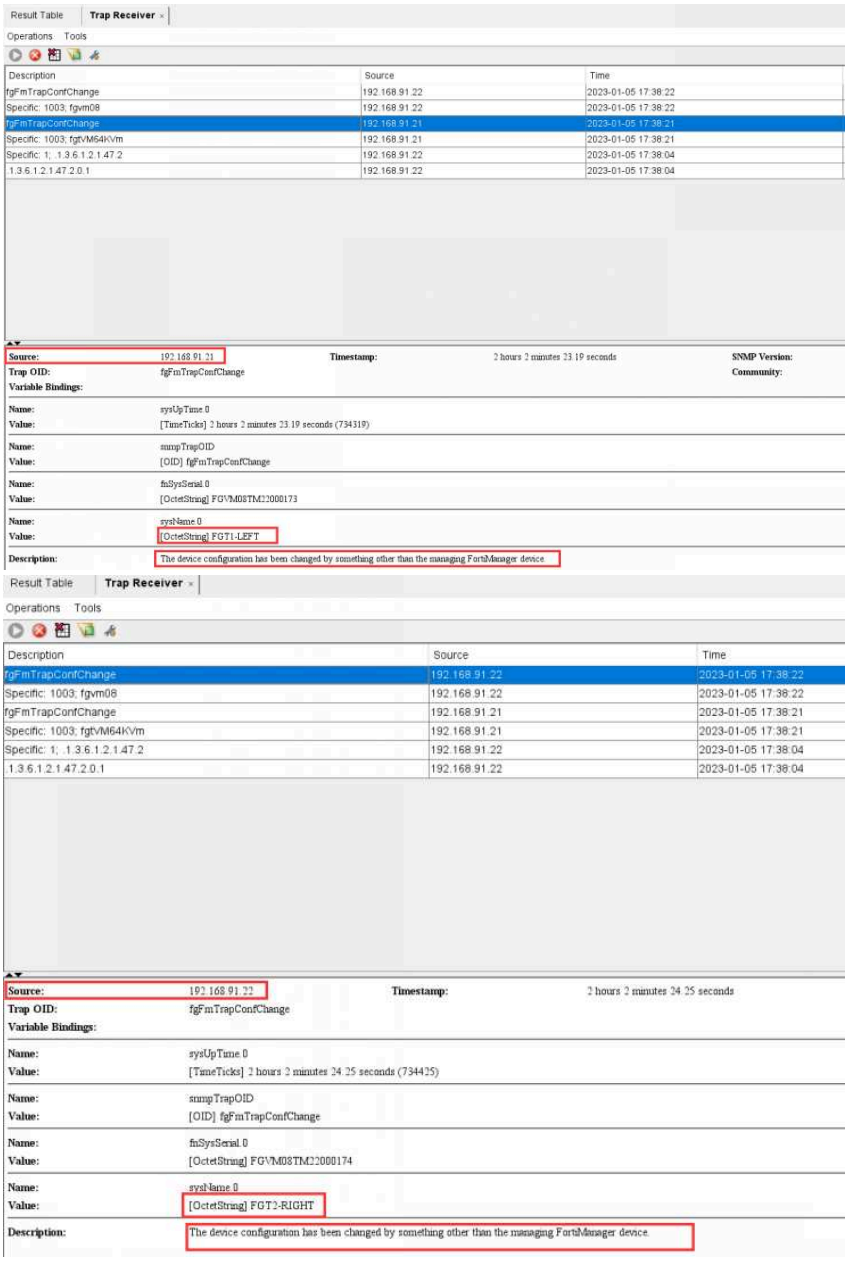

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. SNMP客户端接收到的FGT发送的trap信息，可以看到主备设备均通过自身进行发送。

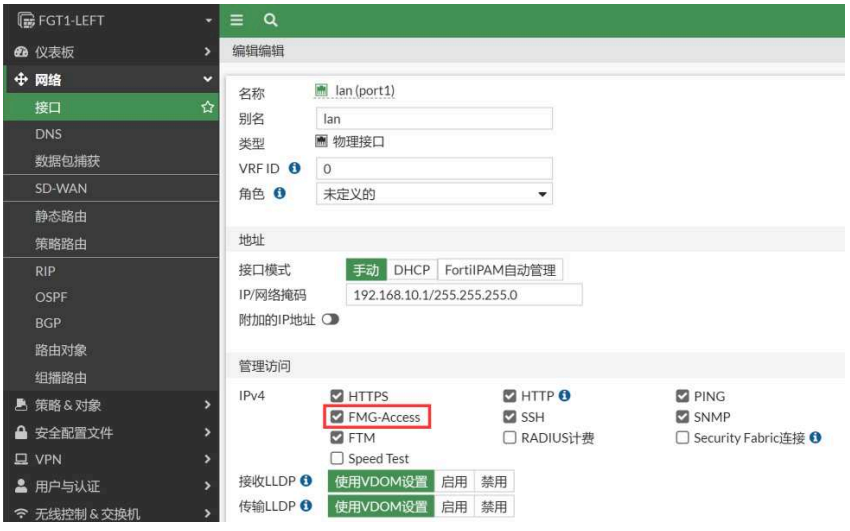
```
FGT1-LEFT (MGMT) # dia sniff pa any "port 162" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 162]
38.445858 port6 out 192.168.91.21.162 → 192.168.91.105.162: udp 104
38.446035 port6 out 192.168.91.21.162 → 192.168.91.105.162: udp 128

FGT2-RIGHT (MGMT) # dia sniff pa any "port 162" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 162]
150.833321 port6 out 192.168.91.22.162 → 192.168.91.105.162: udp 43
150.833537 port6 out 192.168.91.22.162 → 192.168.91.105.162: udp 68
168.867406 port6 out 192.168.91.22.162 → 192.168.91.105.162: udp 107
168.867504 port6 out 192.168.91.22.162 → 192.168.91.105.162: udp 129
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiManger管理

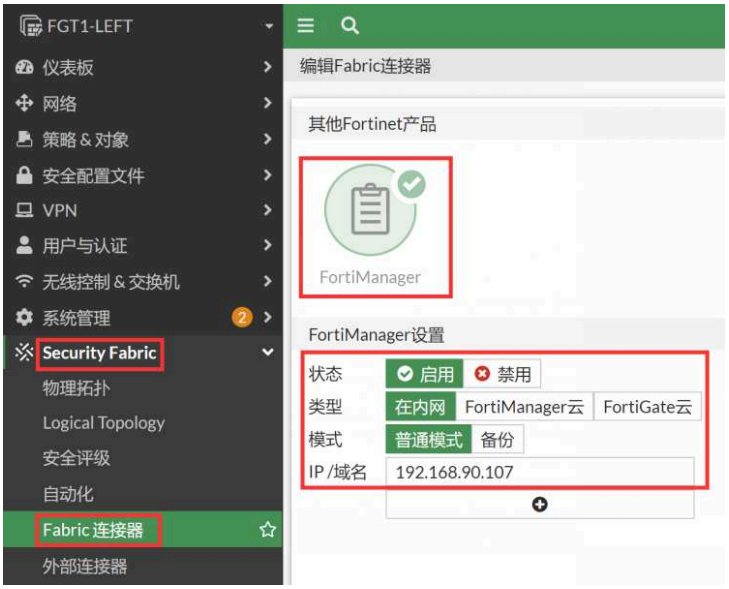
1. FortiManager只能通过业务接口添加，通过FGT的port2（wan）口添加设备，在FGT的wan口下开启FMG管理协议。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

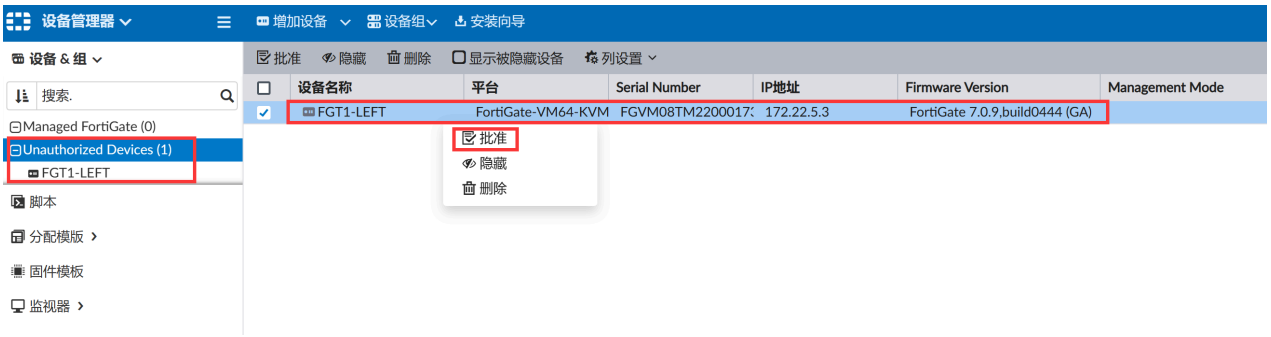
```
config global
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm ftm
        set type physical
        set alias "lan"
        set snmp-index 1
    next
end
```

2. 配置防火墙主动连接FMG（如果FMG可以主动访问到FGT，也可以通过FMG主动添加FGT）。



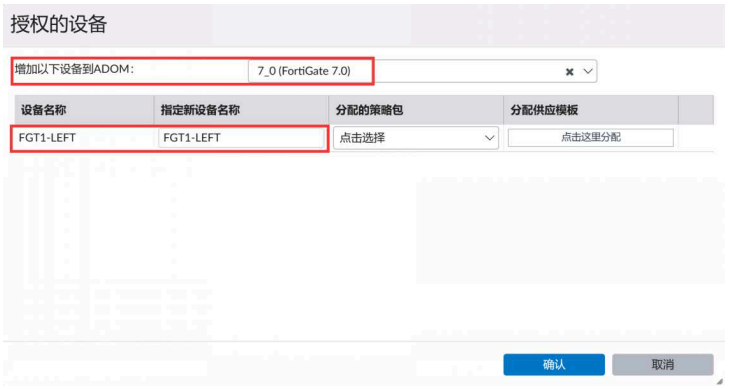

```
config global
config system central-management
    set type fortimanager
    set fmg "192.168.90.107"
end
```

3. 如果是FGT主动去注册FMG，则FMG会有未注册的设备提示。



4. 只需要将设备添加到FMG的对应ADOM的设备管理中即可。

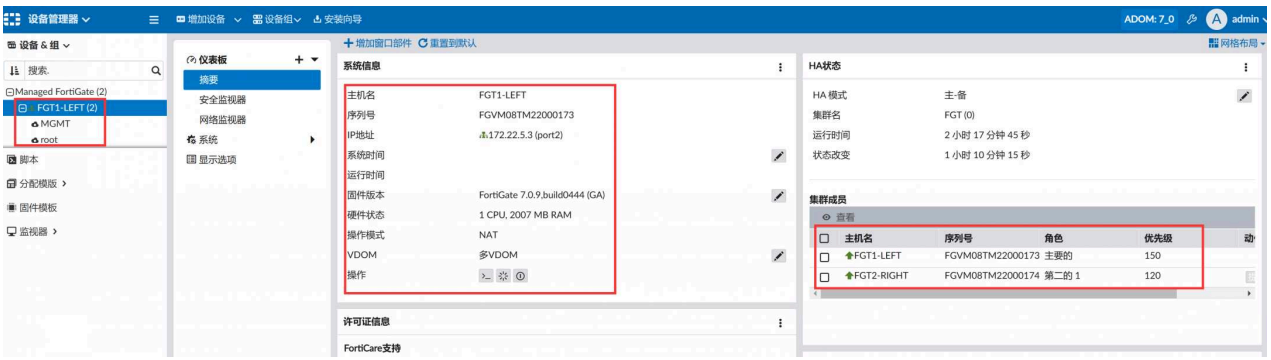
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 授权完成。



6. 在FMG中可以对FGT进行管理。



7. 关于FMG还是建议使用业务接口进行管理，不能使用独立管理口/独立管理VDOM进行管理。对于FMG来说HA-Cluster就是一台设备，因此需要一个固定的IP地址来网管FGT会比较合适，可以有效的避免HA发生切换的时候，FGT和FMG的tunnel中断的情况。

总结

此时所有的SNMP/Radius/SYSLOG/DNS/FORTGUARD都是通过MGMT这个VDOM进行更新的，完全独立于root业务VDOM，彻底的管理是管理，业务是业务。这是HA独立管理的终极解决方案。

重要

FortiManger管理HA-Cluster的时候只能通过业务接口进行管理，不能通过独立管理口或者独立管理VDOM进行管理。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

单独指定用于更新的VDOM

重要

此功能在FortiOS 7.2.3及以后版本上支持。

网络需求

FortiGate工作于多VDOM场景，管理VDOM无法访问Internet（如下管理VDOM配置），业务VDOM是可以访问Internet的，客户想使用业务VDOM来实现Fortiguard更新。

```
config system global
    set management-vdom "mgmt_vdom"
end
```

解决方案

1. 通过非管理VDOM实现Fortiguard更新。

```
config system fortiguard
    set vdom "UPDATE"
end
```

2. 连接FortiGuard需要该VDOM通过DNS服务器解析FortiGuard服务器域名，需要配置对应的VDOM DNS，如下所示。

```
config system vdom-dns
    set vdom-dns enable
    set primary 223.5.5.5
end
```

具体请参考：https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-use-non-management-VDOM-for-Fortiguard/ta-p/231010 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA配置命令集

HA配置命令config system ha，如下是常用的配置命令。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置参数	参数说明
set group-id 0	配置HA机群的组ID，一个机群内的成员必须有相同的组ID。该ID会成为生成防火墙接口的的虚拟MAC的一个组成因素，因此当同一个广播域有２组以上的HA机群的时候需要配置不同的组ID,防止MAC地址冲突
set group-name "FGT-HA"	一个集群内的成员必须有相同的组名字
set mode standalone/a-a/a-p	HA工作模式，常用为a-p模式。AA模式下在HA状态中查看到HA的角色，有主设备及从设备,通常会被认为工作在主被模式下,实际上主主下设备虽然都在工作,仍会有一台作为集群的主设备用来控制和分配流量和会话给集群中的其他设备。AA模式默认情况下仅负载均衡UTM的流量,所以在下不使用UTM功能时建议使用AP模式
set password	一个集群内的成员必须有相同的密码
set hbdev "port1" 50 "port2" 50	配置心跳接口。其中50为优先级，优先级高的被优先使用
unset session-sync-dev	可以配置专门的心跳接口用于会话信息同步，默认和控制信息为同一心跳接口
set route-ttl 10	当一个备机被选举成主机后，其从原主机同步来的转发表的存活时间，单位秒。 HA设备之间只同步转发表，不同步路由表。随后新主机通过静态或动态路由协议生成新的转发表，继续工作。 建议在HA+动态路由环境下，配置为较长时间（可以覆盖新主机动态路由邻居建立与学习的时间，如120s）。
set route-wait 0	主设备收到新的路由条目后，会等待x秒后，再同步给从设备
set route-hold 10	主设备进行２次路由同步之间的间隔，防止路由震荡而造成反复更新路由
set sync-config enable	配置文件自动同步，需要开启
set encryption disable	是否允许使用AES-128和SHA1对心跳信息进行加密和完整性验证
set authentication disable	是否使用SHA1算法验证心跳信息的完整性
set hb-interval 2	发送心跳数据包的间隔，单位为每100ms.如配置2,则每200ms发送一个心跳信息
set hb-lost-threshold 6	心跳信息连续丢失６个后则认为对方不再存活
set helo-holddown 20	Hello状态时间。设备加入HA机群前等待的时间，防止由于未能发现所有的机群成员而造成Ha的反复协商
set arps 5	设备成为主设备后，要发送免费arp来宣布自己的MAC地址，以便相连的交换机能够及时更新MAC地址表，该参数用于配置其发送的数量
set arps-interval 8	发送免费arp的间隔，单位秒
set session-pickup enable/disable	关闭或者开启会话同步，默认为disable。一般需要开启
set session-pickup-delay {enable/disable}	仅对存活30秒以上的会话进行同步。开启后会对性能有所优化，但小于30秒的会话在HA切换的时候会丢失。默认为关闭，谨慎使用
set link-failed-signal disable	防火墙上发生被监控端口失效触发HA切换的时候，是否将除心跳口外的所有端口shutdown一秒钟的时间，便于与之相连的交换机及时更新MAC表。
set uninterruptable-upgrade enable	是否允许无中断升级OS。系统自动分别对机群内的设备升级，并自动切换，不会造成业务的中断
set ha-uptime-diff-margin 300	当进行HA选举时，启动时间为一个选举的一个参数，当２台设备启动时间差小于300时则将该部分差异忽略，视为相同
set override disable	默认为disable,H A 选举按如下顺序进行比较：有效接口数量>运行时间>HA优先级>设备序列号。Enable情况下，讯据顺序改变。有效接口数量> HA优先级>运行时间>设备序列号。每次设备加入或者离开机群，都会强制整个机群重新进行主设备的选举
set priority 128	HA优先级，为便于管理，建议主设备200,从设备100
set monitor port3 port4	配置需要被监控的端口，其有效数量多的设备成为主设备
unset pingserver-monitor-	是否设置pingserver监控端口

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

interface	是否设置pingserver监控端口
set pingserver-failover-threshold 0	pingserver触发的阀值，0则意味着任何的pingserver失效都会触发HA的切换
set pingserver-flip-timeout 60	两次pingserver失效切换之间的间隔。如A发生失效，切换到B. 切过去之后发现B也是失效的，则需要等待60分钟的时间允许切换回A
set ha-mgmt-status enable HA的带外管理配置命令	set ha-mgmt-status enable set ha-mgmt-interface port1 set ha-mgmt-interface-gateway x.x.x.x

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA同步机制和故障诊断

同步配置说明

1. FGCP协议用联合的增量同步和周期性同步去确保所有HA Cluster中的成员与主设备的配置一致，下面的配置不会在cluster成员中同步：
   - 主机名
   - GUI 仪表盘中的微件
   - HA中的override抢占
   - HA设备priority优先级
   - 虚拟cluster priority优先级
   - HA下的Ping server 优先级
   - HA专用管理接口的配置
   - HA专用管理接口的下的默认路由配置
2. 多数订阅服务和授权是不同步的，每一个FortiGate授权是独立的（在系统→FortiGuard中，License的到期时间只会显示较近到期的那台的时间，如果HA成员的某个License过期，那么所有HA成员的该License都会过期）。

   > **重要**
   >
   > FortiToken Mobile是一个例外，它们注册到主设备然后同步给备设备。

3. 主设备同步所有其它的配置给集群成员，包括HA下的一些配置。
4. 所有同步活动在HA hearbert心跳接口用TCP /703 和UDP/703。

禁用自动同步配置

1. 在一些情况下你可能想用下面的命令关掉自动同步主设备的配置到所有集群中的设备。

```
config system ha
    set sync-config disable
end
```

2. 当这个选项disable禁用后，集群不再同步配置变更。如果一个设备发生故障，新的主设备可能没有相同的配置和失败的主设备。结果，新的主设备可能处理会话不同或者不能以相同的方式工作。
3. 在绝大多数情况下不应该disable禁用自动同步配置。然而，如果你disable 自动同步，你可以用execute ha synchronize 命令手工的同步配置。
4. 你必须在备设备上执行execute ha synchronize。用execute ha manage能切换到备设备上。
5. 例子：访问备设备然后执行HA同步，即便自动同步是禁用的。

```
execute ha manage 0    //切到备设备上
execute ha synchronize start    //执行HA同步
```

6. 你能用下面的命令停止在同步中的过程。

```
execute ha synchronize stop
```

增量同步

1. 当你登录进集群用GUI或者CLI做配置变更时，你实际上登录在主设备上。
2. 所有的配置首先被做应用到主设备，增量同步然后立即同步这些变更给其它成员设备。
3. 当你登录备设备的CLI（例如使用execute ha manage切换登录进备设备），所有的在备设备做的配置变更也立即同步到所有集群成员，包括主设备。
4. 增量同步也同步其它动态的配置信息例如DHCP Server address lease 数据库，路由更新，IPSec SAs，MAC地址表 等等。
5. 只要在一个集群成员做配置变更，增量同步将通过心跳链接发送相同的信息到所有其它成员。
6. 运行在每一个成员HA同步进程接收配置变更并应用它。
7. HA同步进程通过输入CLI命令进行配置更改，该命令看起来像是由第一次进行配置更改的管理员输入的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

8. 同步静默的进行，没有日志记录HA同步活动。然而，当同步进程执行CLI命令，日志消息能被记录在成员设备，你能看到这些消息在成员设备如果你启用了事件日志并且日志级别设置为information 信息。
9. 你也能看到这些日志在主设备当你做了配置变更在成员设备上。

周期性同步

1. 增量同步确保管理员做的配置变更，这边配置变更依然是相同的在集群成员。
2. 然而，一些因素可能导致一个或多个集群成员与主设备不同步。例如，当增加一个新的成员到集群中，这个新的成员的配置没有匹配其它成员，使用增量同步配置变更对于新的成员来说是不现实的。
3. 周期性同步是一种寻找同步问题并修复它们的机制，集群每分钟都会将主设备的配置文件校验和与每个成员设备的配置文件校验和进行比较。
4. 如果所有备设备checksums校验和是与主设备一致，所有的集群成员认为是同步的。
5. 如果一个或多个备设备的checksums校验和与主设备不同，备设备的配置被认为out of sync 不同步与主设备，checksums校验和不同步的备设备每15秒检查一次，如果由于增量配置序列未完成而导致配置不同步，则需要重新检查。
6. 如果校验和在5次检查后不匹配，那么不同步的备设备将从主设备索要配置。
7. 然后，备设备重新加载其配置，并作为备设备以与主设备相同的配置继续运行。
8. 备设备的配置通过这种方式重置因为当备设备配置与主设备配置不同步时，没有有效的方法来确定配置的差异是什么并纠正它们。重置备设备配置成为重新同步备设备的最有效方法。
9. 同步要求所有集群成员运行在相同的FortiOS版本，如果一些成员运行在不同的版本，不稳定和同步错误有可能发生。

同步成功的Console上输出的消息

当集群最初形成时，或者当一个新成员作为从属成员添加到集群中时，CLI控制台上会出现以下消息，表明该成员加入了集群，并使其配置与主设备同步。

```
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
logout all admin users
slave succeeded to sync with master
```

同步失败的Console上输出的消息

1. 如果您连接到与主设备不同步的备设备的console控制台，将显示类似如下的消息。

```
slave is not in sync with master, sequence:0. (type 0×3)
slave is not in sync with master, sequence:1. (type 0×3)
slave is not in sync with master, sequence:2. (type 0×3)
slave is not in sync with master, sequence:3. (type 0×3)
slave is not in sync with master, sequence:4. (type 0×3)
global compared not matched
```

2. 如果出现同步问题，Console控制台消息序列可能会一再重复。
3. 所有消息都包含一个类型值(type 0x3)。type值可以帮助诊断同步问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA对象消息和它们引用的配置对象不同步的参考

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

消息类型	配置对象
HA_SYNC_SETTING_CONFIGURATION = 0x03	/data/config
HA_SYNC_SETTING_AV = 0x10	
HA_SYNC_SETTING_VIR_DB = 0x11	/etc/vir
HA_SYNC_SETTING_SHARED_LIB = 0x12	/data/lib/libav.so
HA_SYNC_SETTING_SCAN_UNIT = 0x13	/bin/scanunitd
HA_SYNC_SETTING_IMAP_PRXY = 0x14	/bin/imapd
HA_SYNC_SETTING_SMTP_PRXY = 0x15	/bin/smtp
HA_SYNC_SETTING_POP3_PRXY = 0x16	/bin/pop3
HA_SYNC_SETTING_HTTP_PRXY = 0x17	/bin/thttp
HA_SYNC_SETTING_FTP_PRXY = 0x18	/bin/ftpd
HA_SYNC_SETTING_FCNI = 0x19	/etc/fcni.dat
HA_SYNC_SETTING_FDNI = 0x1a	/etc/fdnservers.dat
HA_SYNC_SETTING_FSCI = 0x1b	/etc/sci.dat
HA_SYNC_SETTING_FSAE = 0x1c	/etc/fsae_adgrp.cache
HA_SYNC_SETTING_IDS = 0x20	/etc/ids.rules
HA_SYNC_SETTING_IDSUSER_RULES = 0x21	/etc/idsuser.rules
HA_SYNC_SETTING_IDSCUSTOM = 0x22	
HA_SYNC_SETTING_IDS_MONITOR = 0x23	/bin/ipsmonitor
HA_SYNC_SETTING_IDS_SENSOR = 0x24	/bin/ipsengine
HA_SYNC_SETTING_NIDS_LIB = 0x25	/data/lib/libips.so
HA_SYNC_SETTING_WEBLISTS = 0x30	
HA_SYNC_SETTING_CONTENTFILTER = 0x31	/data/cmdb/webfilter.bword
HA_SYNC_SETTING_URLFILTER = 0x32	/data/cmdb/webfilter.urlfilter
HA_SYNC_SETTING_FTGD_OVRD = 0x33	/data/cmdb/webfilter.fgtd-ovrd
HA_SYNC_SETTING_FTGD_LRATING = 0x34	/data/cmdb/webfilter.fgtd-ovrd
HA_SYNC_SETTING_EMAILLISTS = 0x40	
HA_SYNC_SETTING_EMAILCONTENT = 0x41	/data/cmdb/spamfilter.bword
HA_SYNC_SETTING_EMAILBWLIST = 0x42	/data/cmdb/spamfilter.emailbwl
HA_SYNC_SETTING_IPBWL = 0x43	/data/cmdb/spamfilter.ipbwl
HA_SYNC_SETTING_MHEADER = 0x44	/data/cmdb/spamfilter.mheader
HA_SYNC_SETTING_RBL = 0x45	/data/cmdb/spamfilter.rbl
HA_SYNC_SETTING_CERT_CONF = 0x50	/etc/cert/cert.conf
HA_SYNC_SETTING_CERT_CA = 0x51	/etc/cert/ca
HA_SYNC_SETTING_CERT_LOCAL = 0x52	/etc/cert/local

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA_SYNC_SETTING_CERT_CRL = 0x53	/etc/cert/crl
HA_SYNC_SETTING_DB_VER = 0x55	
HA_GET_DETAIL_CSUM = 0x71	
HA_SYNC_CC_SIG = 0x75	/etc/cc_sig.dat
HA_SYNC_CC_OP = 0x76	/etc/cc_op
HA_SYNC_CC_MAIN = 0x77	/etc/cc_main
HA_SYNC_FTGD_CAT_LIST = 0x7a	/migadmin/webfilter/ublock/ftgd/data/

checksums校验和

1. 可以使用diagnose sys ha checksum show命令比较所有集群单元的配置校验和。该命令的输出显示了标记为global和all的校验和，以及每个VDOM(包括root VDOM)的校验和。可以使用get system ha-nonsync-csum命令显示类似信息（这个命令仅供FortiManager使用）。
2. 主设备和备设备用这个命令show出来的checksums校验和应该是相同的。如果他们不同你可以用 execute ha synchronize start命令做一下强制同步。
3. 下面命令的输出是主设备的（没有多个VDOM启用）。

```
diagnose sys ha checksum show
is_manage_master()=1, is_root_master()=1
debugzone
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5

checksum
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5
```

4. 下面命令的输出是在相同集群中的备设备的。

```
diagnose sys ha checksum show
is_manage_master()=0, is_root_master()=0
debugzone
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5

checksum
global: a0 7f a7 ff ac 00 d5 b6 82 37 cc 13 3e 0b 9b 77
root: 43 72 47 68 7b da 81 17 c8 f5 10 dd fd 6b e9 57
all: c5 90 ed 22 24 3e 96 06 44 35 b6 63 7c 84 88 d5
```

5. 下面的输出是启用了VDOM（test 和Eng_vdm.）的主设备输出。

```
config global
diagnose sys ha checksum show
is_manage_master()=1, is_root_master()=1
debugzone
global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53

checksum
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53
```

6. 备设备输出。

```
config global
diagnose sys ha checksum show
is_manage_master()=0, is_root_master()=0
debugzone
global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53

checksum
global: 65 75 88 97 2d 58 1b bf 38 d3 3d 52 5b 0e 30 a9
test: a5 16 34 8c 7a 46 d6 a4 1e 1f c8 64 ec 1b 53 fe
root: 3c 12 45 98 69 f2 d8 08 24 cf 02 ea 71 57 a7 01
Eng_vdm: 64 51 7c 58 97 79 b1 b3 b3 ed 5c ec cd 07 74 09
all: 30 68 77 82 a1 5d 13 99 d1 42 a3 2f 9f b9 15 53
```

诊断HA out of sync 不同步问题

这部分描述怎样使用diagnose sys ha checksum show和diagnose debug命令诊断HA不同步消息。如果同步不成功，用下面的步骤在每一个成员执行发现问题。

确定为什么没有进行HA同步

1. 连接每一个设备的console 口（或者SSH登录）。
2. 使用下面的debug命令启用诊断。

```
diagnose debug enable
diagnose debug console timestamp enable
diagnose debug application hatalk -1
diagnose debug application hasync -1
```

3. 收集debug输出信息，然后对比上个章节中的消息信息表格。
4. 关掉debug。

```
diagnose debug disable
diagnose debug reset
```

确定哪一部分配置导致的问题

1. 如果上面的步骤显示的消息中包含了同步对象0x30（例如，HA_SYNC_SETTING_CONFIGURATION = 0x03），则说明配置存在同步问题。使用以下步骤来确定导致问题的配置部分。
2. 如果您的集群由两个集群成员组成，则使用此过程捕获每个成员的配置校验和。如果您的集群包含两个以上的集群成员，则对所有返回包含0x30同步对象消息的集群成员重复此过程。
3. 连接每个成员的console口（或者SSH命令行）。
4. 启用debug命令。

```
diagnose debug enable
```

5. 停止HA同步。

```
execute ha sync stop
```

6. 显示global下的checksum校验和。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
diagnose sys ha checksum show global
```

7. 把输出存为一个text文件。
8. 在所有集群设备重复这个过程。
9. 比较主设备的text文件和成员设备的，发现不匹配的部分。可以用一个文本对比器来对比。
0. 对比root vdom的校验和。

```
diagnose sys ha checksum show root
```

1. 对比所有VDOM的校验和。

```
diagnose sys ha checksum show <vdom-name>
```

2. 你也可以用grep选项仅仅显示部分的checksums。例如，仅仅显示和system相关的checksums在 root Vdom或者log相关的checksums在global下的，通常情况下第一个不匹配的校验和意味这个是导致不同问题的原因。

```
diagnose sys ha checksum root | grep system
diagnose sys ha chechsum global | grep log
```

3. 尝试删除或者改变这导致问题配置部分，你可以在主设备或者备设备上修改配置。
4. 然后用下面的命令重启开启HA同步，停掉debug。

```
execute ha sync start
diagnose debug disable
diagnose debug reset
```

重新计算checksums校验和解决HA不同步问题

1. 有时，在集群计算校验和时可能会发生错误。由于这种计算错误，即使集群正常运行，CLI控制台也可能显示out of sync错误消息。有时，在diagnostic sys ha checksum命令的输出中也会出现校验和计算错误，原因是debug zone中的校验和与输出的校验和部分不匹配。
2. 解决这个问题的一个方法是重新计算校验和。重新计算的校验和应该匹配，不同步的错误消息应该停止出现。
3. 您可以使用以下命令重新计算HA校验和。

```
diagnose sys ha checksum recalculate [<vdom-name> | global]
```

4. 仅仅输入不带选项的命令就会重新计算所有校验和。您可以指定一个VDOM名称来重新计算该VDOM的校验和。您也可以输入global来重新计算全局校验和。

确定导致配置同步问题的原因

有25个配置同步的FortiOS模块。要分析这么多数据，它是困难的找到导致同步问题的原因。您可以使用以下诊断命令更容易地找到可能导致同步问题的模块。

```
diagnose sys ha hasync-stats {all | most-recent <seconds> | by object <number>}
```

- all显示自hasync进程开始运行(通常是集群启动后)以来发生的所有模块的同步活动。
- `most-recent [<seconds>]` 显示最近发生的同步事件。可以包括以秒为单位的时间，以显示在时间间隔内发生的最近事件。如果不包含秒数，该命令将显示最近5秒内的最新事件。此选项可用于确定当前正在同步或试图同步的一个或多个模块。如果当前没有正在同步的模块，该命令只显示最近的同步事件。
- `by-object [<number>]` 显示指定模块的同步活动，`<number>` 是模块号，取值范围是1 ~ 25。要显示所有25个模块及其编号，请输入：

```
diagnose sys ha hasync-stats by-object ?
```

- 要显示最近的活动，输入：

```
diagnose sys ha hasync-stats most-recent 10
current-time/jiffies=2018-03-28 13:01:42/1148242:
hasync-obj=2(arp):
   epoll_handler=1(ev_arp_handler): start=1522256500.354400(2018-03-28 13:01:40), end=1522256500.354406(2018-03-28
13:01:40), total=0.000006/1699
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
hasync-obj=5(config):
    timer=0(check_sync_status), add=1141764(2018-03-28 13:01:26), expire=1142764(2018-03-28 13:01:36),
end=1142764(25018-03-28 13:01:36), del=0(), total_call=1143
hasync-obj=8(time):
   obj_handler=0(packet): start=1522256497.851550(2018-03-28 13:01:37), end=1522256497.851570(2018-03-28
13:01:37), total=0.000020/381
   timer=0(sync_timer), add=1140106(2018-03-28 13:01:10), expire=1143106(2018-03-28 13:01:40), end=1143106(2018-
03-28 13:01:40), del=0(), total_call=381
hasync-obj=21(hastats):
   obj_handler=0(packet): start=1522256499.760934(2018-03-28 13:01:39), end=1522256499.760936(2018-03-28
13:01:39), total=0.000002/2285
   timer=0(hastats_timer), add=1142556(2018-03-28 13:01:34), expire=1143056(2018-03-28 13:01:39),
end=1143056(2018-03-28 13:01:39), del=0(), total_call=2286
```

- 该输出的最后几行显示了hastats模块的活动，该模块是模块21。您可以使用以下命令查看更多关于此模块的同步活动的信息:

```
diagnose sys ha hasync-stats by-object 21
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

HA无法更新特征库/License

问题现象

自2025年2月下旬起，当FortiGate的HA成员注册到不同FortiCloud账户（或其中一个未注册账户）时，HA集群会出现如下情况：

- 无法执行在线固件升级。
- 不能在线更新IPS、AV、应用控制等特征库。
- 不能更新License合同信息。

诊断方法

1. 在CLI下执行以下Debug命令。

```bash
diagnose debug application update -1
diagnose debug enable
execute update-now
```

2. 完成后，使用以下命令清除调试信息。

```bash
diagnose debug disable
diagnose debug reset
```

3. Debug日志中会出现类似“Missing contracts, got X, expect X”的错误信息，如下所示。

```bash
upd_act_report_fmg_list[846]-ContractItem (1) does not contain all HA (2): FGVM04TMXXXXXX03
<>
upd_status_set_ha_expiry[1532]-Serial Number: FGVM04TMXXXXXX03 - contract processed
upd_status_set_ha_expiry[1498]-Extracting contract ... (SupportLevelDesc=06:Web/Online*10:8*5*20:Premium)
<>
upd_status_set_ha_expiry[1547]-Missing contracts, got 1, expect 2  <——错误信息
upd_status_set_ha_expiry[1565]-Reset expiry
do_update[690]-UPDATE failed
```

解决方法

1. 确保FortiGate HA集群成员注册到相同的FortiCloud账户。
2. 如果HA成员不在同一FortiCloud账户下，请联系support_cn@fortinet.com进行账户转移。

Workaround

1. 可以关闭HA成员的备机，或将其进行网络隔离，然后通过HA主设备执行FortiGuard更新。
2. 使用相同的办法更新HA的其他成员。
3. 更新完成后，将其他成员恢复到HA集群中。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

路由介绍

路由转发表

1. FIB (Forwarding Information Base)，包含所有已知的本地或非本地路由，从路由表载入，由内核访问。

2. 内核转发数据时看diagnose ip route list，而非get router info routing-table all。

```
diagnose ip route list
```

路由表

1. 路由表包括最具体的路由条目、最长掩码匹配原则、路由的管理距离、度量值等决定哪个协议产生的哪条路由被内核采用。

```
get router info routing-table all
```

2. 路由表中的相关元素。

Routing-table（路由表）元素

```
# get router info routing-table database
O E2 *> 10.0.0.1/32     [110/10] via 192.168.90.41, wan1, 18:40:59
O IA *> 192.168.8.0/24 [110/2] via 192.168.90.41, wan1, 18:40:59
O       192.168.90.0/24 [110/1] is directly connected, wan1, 19:15:57
C    *> 192.168.90.0/24 is directly connected, wan1
S    *> 192.168.0.0/16 [5/0] via 192.168.90.253, wan1, [2/4]
S       192.168.0.0/16 [10/0] via 192.168.90.254, wan1, [1/2]
```

目的网络 /子网掩码　　下一跳地址/出接口

Distance（管理距离）　Metric（度量值）　Priority（优先级）　Weight（权重）

```
#get router info routing-table all
O E2    10.0.0.1/32     [110/10] via 192.168.90.41, wan1, 18:44:24
O IA    192.168.8.0/24 [110/2] via 192.168.90.41, wan1, 18:44:24
C       192.168.90.0/24 is directly connected, wan1
O       192.168.90.0/24[110/1] is directly connected, wan1, 19:07:01
S       192.168.0.0/16 [5/0] via 192.168.90.253, wan1, [2/4]
```

- Distance（管理距离）

Distance（管理距离）

一条相同的路由条目通过不同的路由协议（RIP/IS-IS/OSPF）学习到，那么哪一条应该安装进转发路由表呢？

管理距离：路由协议及该路由协议产生的路由的优先级，0-256，越小越优先。一般只在本设备内有效。

FortiGate默认管理距离值：

直连路由	0
DHCP网关	5
静态路由	10
EBGP	20
OSPF	110
IS-IS	115
RIP	120
IBGP	200

- Metric（度量值）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Metric（度量值）

一条相同的路由条目通过相同的路由协议（RIP）学习到，那么哪一条应该安装进转发路由表呢?

度量值：路由协议产生的路由到目标网络的开销，越小越优先，只在同一路由协议内起作用，不同的路由协议产生的路由度量值没有可比性。

RIP	路由的跳数作为度量值
OSPF/IS-IS	路径Cost之和作为度量值
BGP	Metric是起一个可选不可传递的属性

- Priority（优先级）

Priority（优先级）

想要实现浮动路由的效果，同时备份的出口又需要能够作为SSL VPN的登录IP/VIP映射/管理IP使用?

- 静态路由使用它来计算到达目的地址的最佳路由
- 如果多条静态路由拥有相同的distance值，而拥有不同的Priority
  - 他们全都会被加载到路由表中
  - 但是，只有拥有最低优先级priority值的路由条目会被用来指导转发

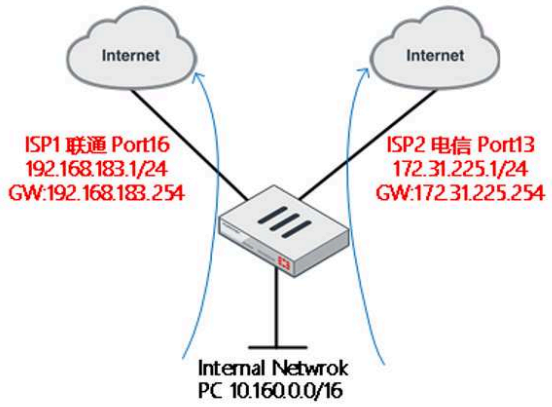
Priority通常用于以下情形中：为了接受入方向的流量（VIP/VPN/SNMP请求），需要在路由转发表中存在一条静态路由，以便通过Reverse Path Forwarding检查（Anti-Spoofing），否则数据将被丢弃。

Priority 越小越优先，低Priority的路由用于出方向的目的路由转发，高Priority的路由只是存在于路由表中，不用于出方向目的路由转发，当有数据从高Priority的接口入时，会启用RPF源路由检查，只有通过RPF检查的数据才会被防火墙所处理，这条高Priority的路由存在的意义正在于此。

路由选路

1. 情景1：相同的distance，相同的priority。

Distance（管理距离） /Priority（优先级）路由选择



Scenario 1 : same distance , same priority.

配置:

```
config router static
    edit 1
        set device "port16"
        set distance 10 （默认）
        set gateway 192.168.183.254
    next
    edit 2
        set device "port14"
        set distance 10 （默认）
        set gateway 172.31.225.254
    next
end
```

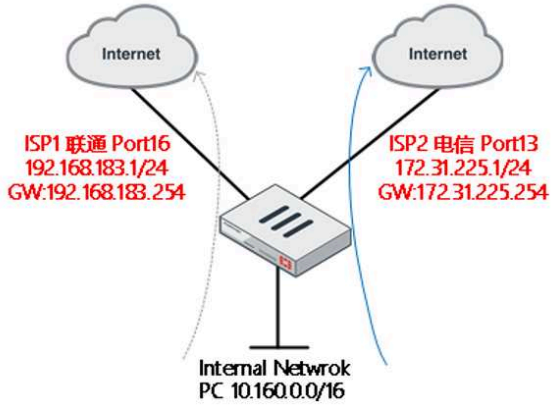
结果：EMCP（等价链路负载）

```
FGT# get router  info routing-table static
S*      0.0.0.0/0 [10/0] via 172.31.225.254, port13
                  [10/0] via 192.168.183.254, port16
```

2. 情景2：不同的distance，相同的priority。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Distance（管理距离） /Priority（优先级）路由选择



Scenario 2 : different distance , same priority.

配置:

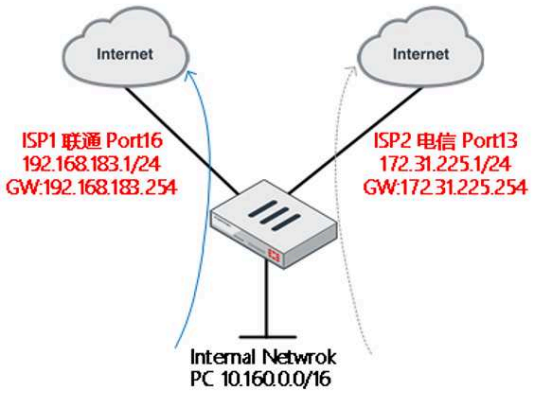
```
config router static
    edit 1
        set device "port16"
        set distance 10 （默认）
        set gateway 192.168.183.254
    next
    edit 2
        set device "port13"
        set distance 5
        set gateway 172.31.225.254
    next
end
```

结果：选择管理距离小的

```
FGT# get router  info routing-table static
S*      0.0.0.0/0 [5/0] via 172.31.225.254, port13
```

3. 情景3：相同的distance，不同的priority。

Distance（管理距离） /Priority（优先级）路由选择



Scenario 3a : same distance , different priority.

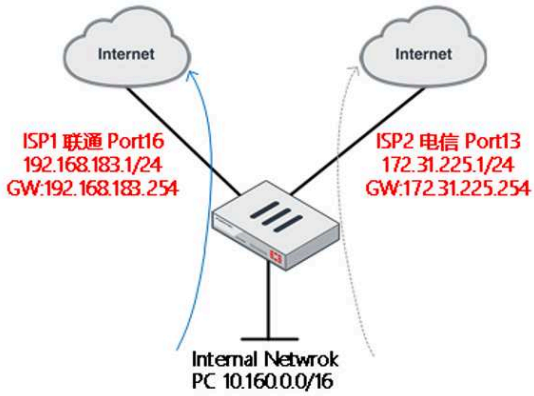
配置:

```
config router static
    edit 1
        set device "port16"
        set gateway 192.168.183.254
        set priority 2
    next
    edit 2
        set device "port13"
        set gateway 172.31.225.254
        set priority 5
    next
end
```

结果：都被加入路由表，但只有优先级小的用于路由转发数据

```
FGT# get router  info routing-table static
S*      0.0.0.0/0 [10/0] via 192.168.183.254, port16, [2/0]
                  [10/0] via 172.31.225.254,  port13, [5/0]
```

Distance（管理距离） /Priority（优先级）路由选择



Scenario 3b : same distance , different priority.

配置:

```
config router static
    edit 1
        set device "port16"
        set gateway 192.168.183.254
        set priority 2
    next
    edit 2
        set device "port13"
        set gateway 172.31.225.254
        set priority 1
    next
end
```

结果：都被加入路由表，但只有优先级小的用于路由转发数据

```
FGT# get router  info routing-table static
S*      0.0.0.0/0 [10/0] via 172.31.225.254,  port13, [1/0]
                  [10/0] via 192.168.183.254, port16, [2/0]
```

4. Weight（权重）对选路的影响。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Weight（权重）

多出口组网中如果配置了多条等价缺省路由，设备使用HASH算法使流量均衡分担到各个链路上。缺省情况下基于源IP负载。当链路带宽不同时，为了充分利用链路带宽还可以按带宽比例进行流量分担。例如WAN1对应链路带宽为10M，WAN2对应链路带宽为20M，可以在出接口上指定权重比为10:20

```
system virtual-wan-link
set v4-ecmp-mode weight-based
end
config system interface（配置接口的权重）
    edit "wan1"
       set weight 10
       next
    edit "wan2"
       set weight 20
end
```

OR

```
system virtual-wan-link
    set v4-ecmp-mode weight-based
end
config router static （配置路由的权重）
    edit 1
        set gateway 101.1.1.2
        set weight 10
        set device "wan1"
    next
    edit 2
        set gateway 202.1.1.2
        set weight 20
        set device "wan2"
    next
end
```

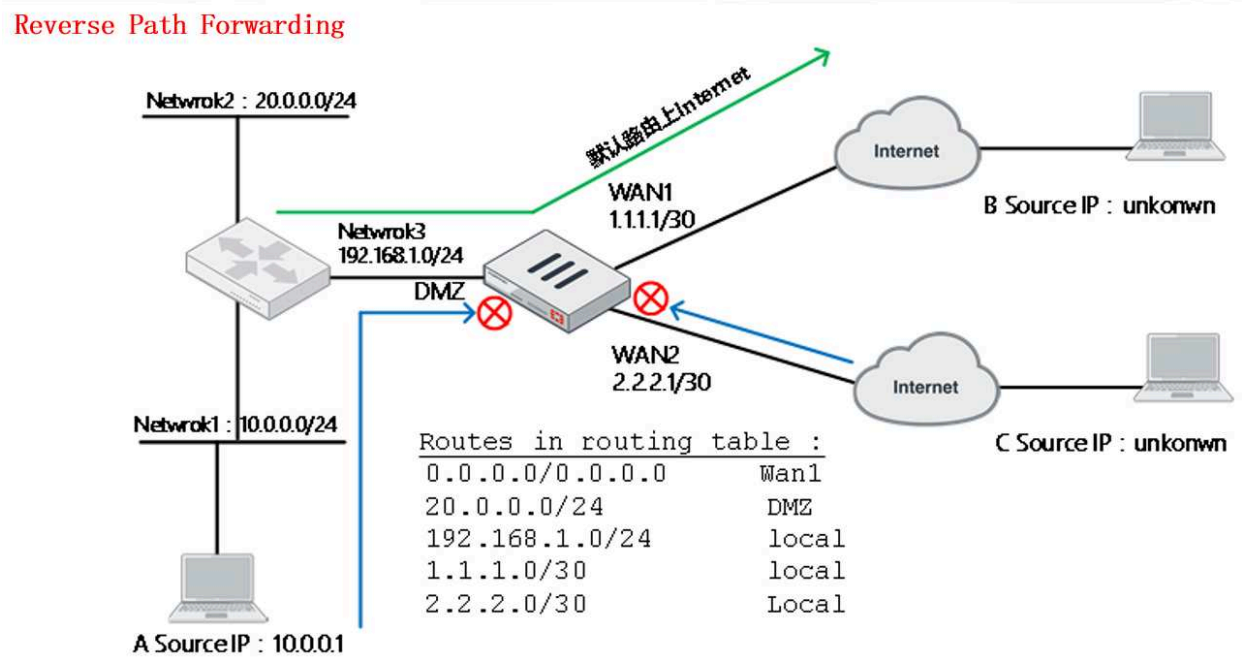
5. 总结：

- 策略路由比路由表优先
- 如果接口down则没有相关的路由（包括没有直连路由）
- 目标网段不同，都优选
- 目标网段相同，子网掩码不同时，都优选:转发时最长掩码匹配目标网段、子网掩码都相同时，最低管理距离优先
- 目标网段、子网掩码、管理距离都相同时，最低度量值优先目标网段、子网掩码、管理距离、度量值都相同时，视具体协议而定，一般可形成等开销负载分担路由

RPF（Reverse Path Forwarding，反向路径转发）

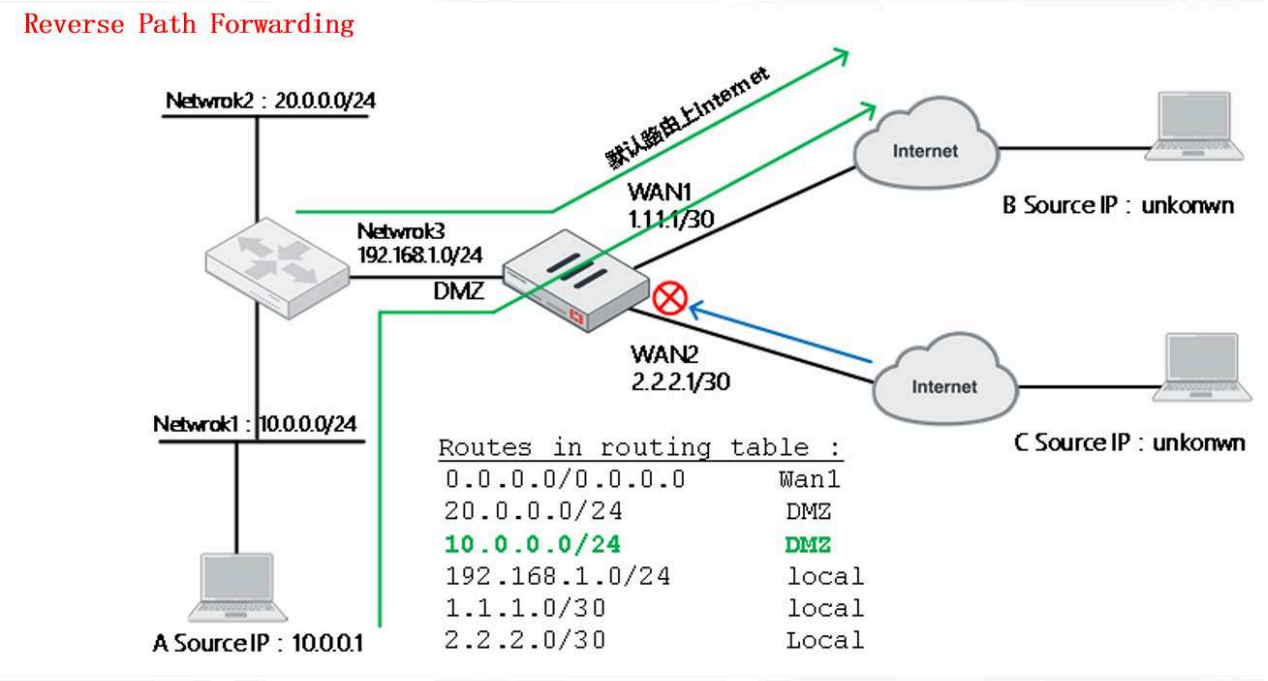
RPF的作用：

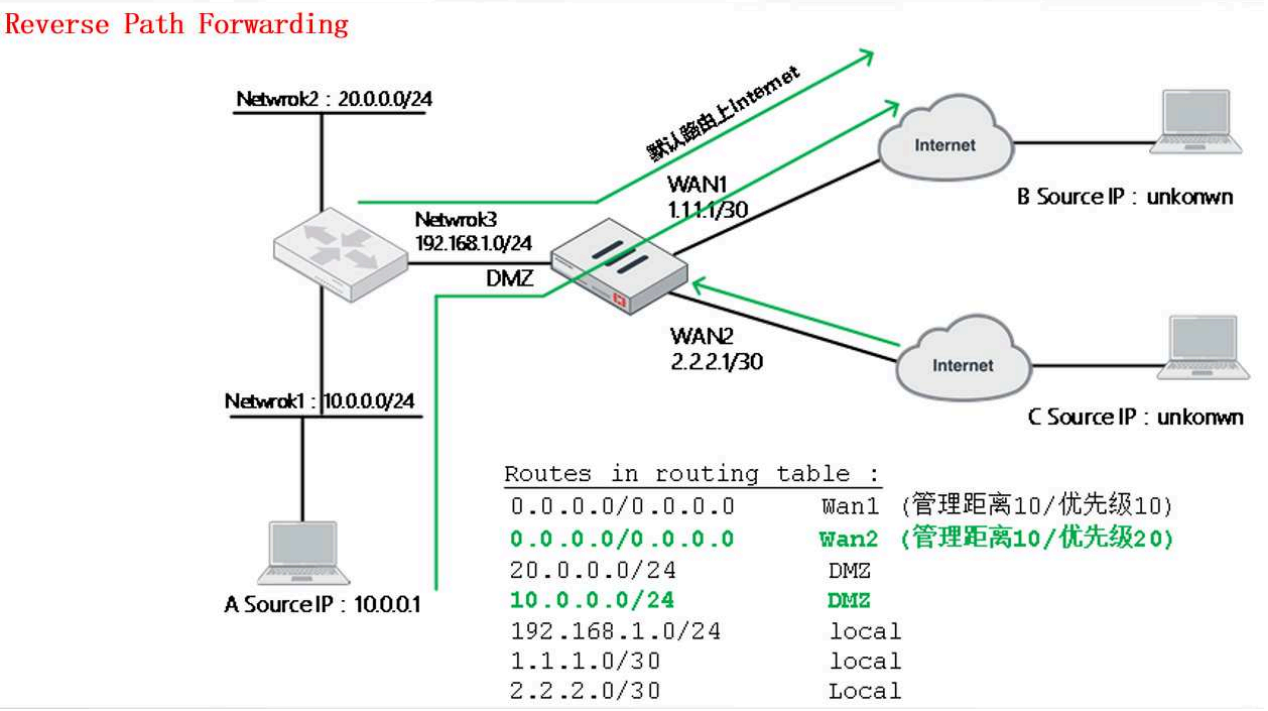
- 阻止IP欺骗攻击
  - 测试DDoS不成功的原因（攻击源IP为随机IP）
- 校验所有包的源地址
  - 和接口相关的路由比较IP地址
  - 丢弃那些源IP没有返回路由的包



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 如果源IP地址的返回路径与包来的路径不匹配，则这个包被丢弃





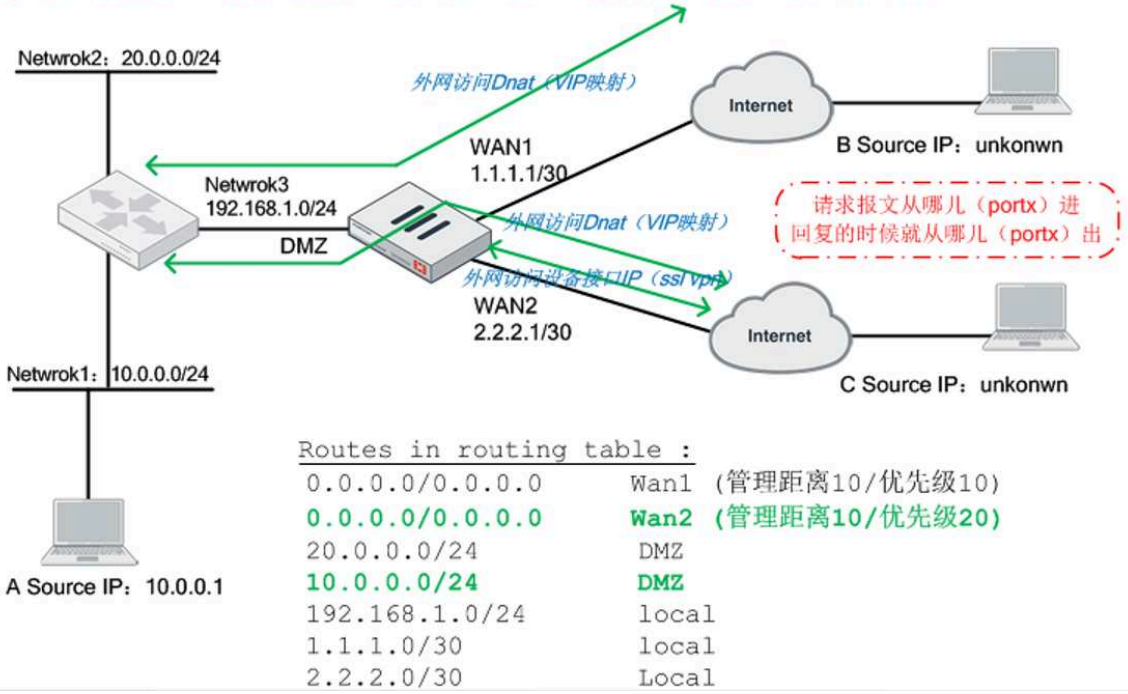
- RPF只检查会话的第一个包
  - 来去路径相同时，不检查回应包（也没有必要）
  - 异步情况下，对回包也执行检查

源进源出

1. 源进源出介绍：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

原接口进原接口出属性（请求报文从哪个接口进，回复报文必然从哪个接口出）



2. 如何关闭RPF（同时源进源出特性跟随关闭）：

   - 开启异步路由（一般情况下不建议，会话安全性检查将降低）：

```
config system settings
    set asymroute enable    //default = disable
end
```

   - 基于接口关闭RPF：

```
config system interface
    edit <interface>
        set src-check disable
end
```

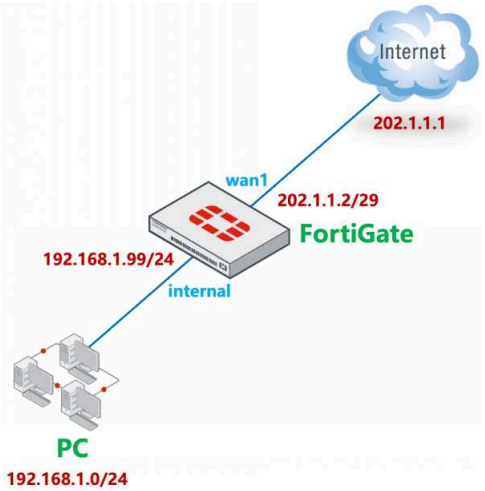

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

静态路由

网络需求

静态路由是由系统管理员，根据网络的结构，在防火墙上手工添加路由条目。对于防火墙设备来说，静态路由是最基本的方式，也是最常用的添加路由的方式。

网络拓扑

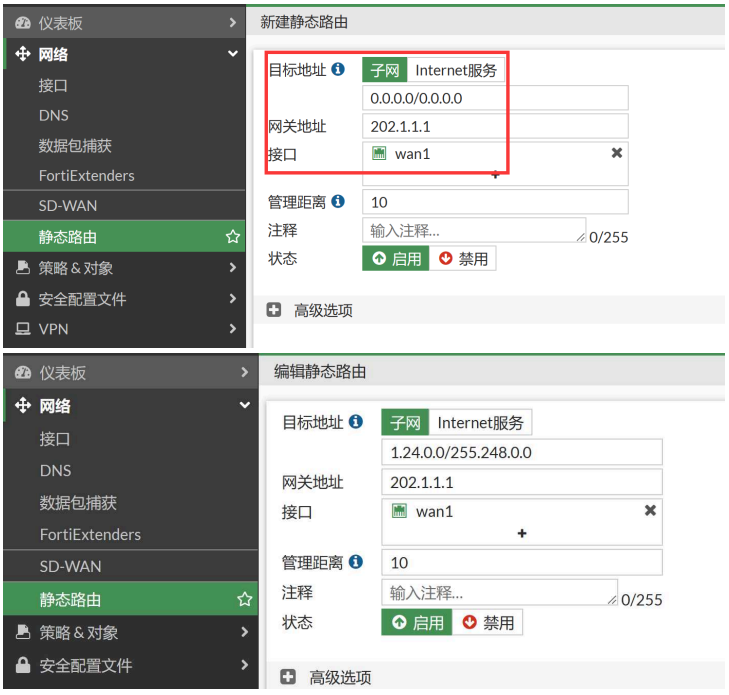


防火墙外网口wan1 ip地址为202.1.1.2， 对端ISP路由器地址为202.1.1.1。

配置步骤

1. 配置相关接口IP（略）。

2. 进入网络→静态路由，点击 新建，按如下方式创建路由表。



- 目的的IP/子网掩码： 由于是默认网关，使用默认的0.0.0.0/0.0.0.0即可
- 设备： 该路由所关联的接口，wan1口，必须正确填写，否则该路由无法工作
- 网关： 下一跳ip地址， 即wan1口对端运营商设备接口的ip地址
- 路径长度：默认10。 对于相同的路由条目，管理距离短的会被放入路由表。如果管理距离相同，则都会被放入路由表
- 优先级：默认0.管理距离相同的两条路由，防火墙优先使用优先级参数较低的路由工作。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 对应CLI。

```
FortiGate # config router static
FortiGate (static) # edit 1
FortiGate (1) # set gateway 202.1.1.1    //本条目没有定义dst目的网络，则默认为为0.0.0.0/0.0.0.0
FortiGate (1) # set device wan1
FortiGate (1) # next

FortiGate (static) # edit 2
FortiGate (2) # set dst 1.24.0.0 255.248.0.0
FortiGate (2) # set gateway 202.1.1.1
FortiGate (2) # set device wan1
FortiGate (2) # end
```

结果验证

1. 通过图形页面查看路由表，进入仪表盘，添加路由监控组件。



2. 或通过命令行查看该路由是否生效：get router info routing-table static。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.1.1.1, wan1, [1/0]
S       1.24.0.0/13 [10/0] via 202.1.1.1, wan1, [1/0]
C       192.168.100.0/24 is directly connected, lan
```

3. 通过ping 202.1.1.1，确认链路正常。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

策略路由

基本概念

1. 静态动态路由等，都属于目的路由，即根据目的地址进行选路。
2. 策略路由则可以根据原地址，协议类型，流控标签，目的地址等多个参数进行选路。
3. 策略路由优于静态路由，被先执行。

应用示例

1. 场景参考策略与对象→多线路上网配置→双线路不同运营商上网配置↗。

2. 强制192.168.1.0/29的地址，从wan2口访问互联网。

3. 进入系统管理→可见功能，开启高级路由功能。



4. 进入网络→策略路由，新建策略路由，强制192.168.1.0/29的地址，从wan2口访问互联网，该策略路由定义所有从internal1进入的，源地址是192.168.1.0 255.255.255.248，目的地址是0.0.0.0 0.0.0.0的数据包，都会被强制由wan2转发，转发时下一条的网关地址为100.1.1.1。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 协议：协议类型，ANY为所有任何协议，可以指定6 tcp,17 udp,132等
- 流入接口：流量进入接口
- 源地址掩码： 数据包的源地址
- 目的地址掩码：数据包的目的地址
- 目的端口：目的端口，默认为所有。从1-65536
- 强制流量到：
  - 流出接口： 数据包的流出接口
  - 网关地址： 流出接口的下一条网关地址

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

黑洞路由不生效

问题现象

通常会在IPSec VPN环境下配置高管理距离（distance）的黑洞路由，避免IPSec连接中断时，VPN流量匹配默认路由被送到Internet。

1. 某用户在配置VPN路由对应的黑洞路由，如下所示，distance配置为255。

```bash
config router static
    edit 15
        set status disable
        set dst 192.168.123.0 255.255.255.0
        set distance 20
        set device "VPN_Tunnel1"
    next
    edit 16
        set dst 192.168.123.0 255.255.255.0
        set distance 255
        set blackhole enable
        set vrf 0
    next
end
```

2. 查看路由表中没有该黑洞路由，VPN隧道中断后，流量仍然匹配默认路由从wan1接口转发。

```bash
FortiGate # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 172.22.6.1, wan1, [1/0]
```

3. 但在路由Database中可以看到该黑洞路由。

```bash
FortiGate # get router info routing-table database | grep 192.168.123.0
S       192.168.123.0/24 [20/0] via VPN_Tunnel1 tunnel 10.0.0.2, [1/0]
S       192.168.123.0/24 [255/0] is a summary, Null, [1/0]
```

问题原因

路由管理距离（distance）255表示该路由无效。路由只能在routing-table database中可见。不会插入到路由转发表中，所以VPN流量不会按预期丢弃（路由），而是匹配默认路由从wan1接口转发。

解决方法

任何静态路由的管理距离都需要 ≤ 254。否则，路由条目将被视为无效路由。

```bash
config router static
    edit 16
        set dst 192.168.123.0 255.255.255.0
        set distance 254
        set blackhole enable
        set vrf 0
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

策略路由不生效

问题现象

1. 配置的策略路由如下。

```bash
config router policy
    edit 1
        set input-device "lan"
        set src "192.168.100.77/255.255.255.255"
        set dst "223.5.5.5/255.255.255.255"
        set gateway 10.10.12.1
        set output-device "wan1"
    next
end
```

2. 实际使用中该策略路由不生效，查看策略路由列表（`diagnose firewall proute list`），该条策略路由有`disable`标记，但该策略路由配置中未disable。



问题原因

1. 可能是由于配置了link-monitor或SD-WAN的健康检查功能，默认配置下`update-policy-route`为开启状态，当link-monitor的检查状态由UP变为DOWN后，会将相应出接口的策略路由禁用。

```bash
config system link-monitor
    edit "test"
        set srcintf "wan1"
        set server "10.10.12.1"
        set update-cascade-interface enable    //默认开启//
        set update-static-route enable    //默认开启//
        set update-policy-route enable    //默认开启//
    next
end
```

2. 查看link-monitor的状态为DOWN，导致对应出接口的策略路由为disable状态。

```bash
FW1_FGT101F # diagnose sys link-monitor status

Link Monitor: test, Status: dead, Server num(1), HA state: local(dead), shared(dead)
Flags=0x9 init log_downgateway, Create time: Wed Apr 24 16:19:13 2024
Source interface: wan1 (7)
VRF: 0
Interval: 500 ms
Service-detect: disable
Diffservcode: 000000
Class-ID: 0
  Peer: 10.10.12.1(10.10.12.1)
        Source IP(10.10.12.2)
        Route: 10.10.12.2→10.10.12.1/32, gwy(10.10.12.2)
        protocol: ping, state: dead
                Packet lost: 100.000%
                MOS: 4.350
                Number of out-of-sequence packets: 0
                Recovery times(0/5) Fail Times(1/5)
                Packet sent: 1231, received: 287, Sequence(sent/rcvd/exp): 1232/475/476
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

解决方法

1. 关闭link-monitor中的`update-policy-route`。

```bash
config system link-monitor
    edit "test"
        set update-policy-route disable
    next
end
```

2. 再次查看对应出接口的策略路由状态，disable标记消失，流量可以正确匹配该策略路由。

```bash
FW1_FGT101F # diagnose firewall proute list
list route policy info(vf=root):

id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=48(lan) dport=0-65535
path(1) oif=7(wan1) gwy=10.10.12.1
source wildcard(1): 192.168.100.77/255.255.255.255
destination wildcard(1): 223.5.5.5/255.255.255.255
hit_count=1 last_used=2024-04-24 16:32:24
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

RIP

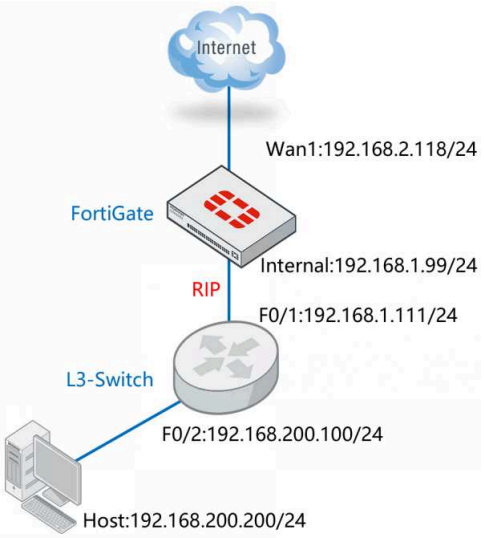
应用场景

1. 当网络路由设备较多，且不超过16个，为避免写大量静态路由，且路由可自动学习，可在FortiGate上配置RIP路由协议，让FortiGate也能动态学习到其他网络的路由，且能自动老化更新。
2. 若网络中路由设备超过16个，建议使用OSPF，它的路由学习更新速度更快，更适合16个路由设备以上的网络。
3. 当网络中路由设备较少，建议使用静态路由即可，维护简单，且对路由器要求不高，因为路由器都支持静态路由，而普通小路由一般不支持RIP协议。

网络需求

1. 内网三层交换机和出口FortiGate间通过动态路由RIP互相通告路由，实现内网用户正常上网。
2. FortiGate手动配置默认路由，并将其重发布引入RIP，三层交换机与FortiGate之间通过RIP互相学习路由，实现内网用户正常上网。

网络拓扑



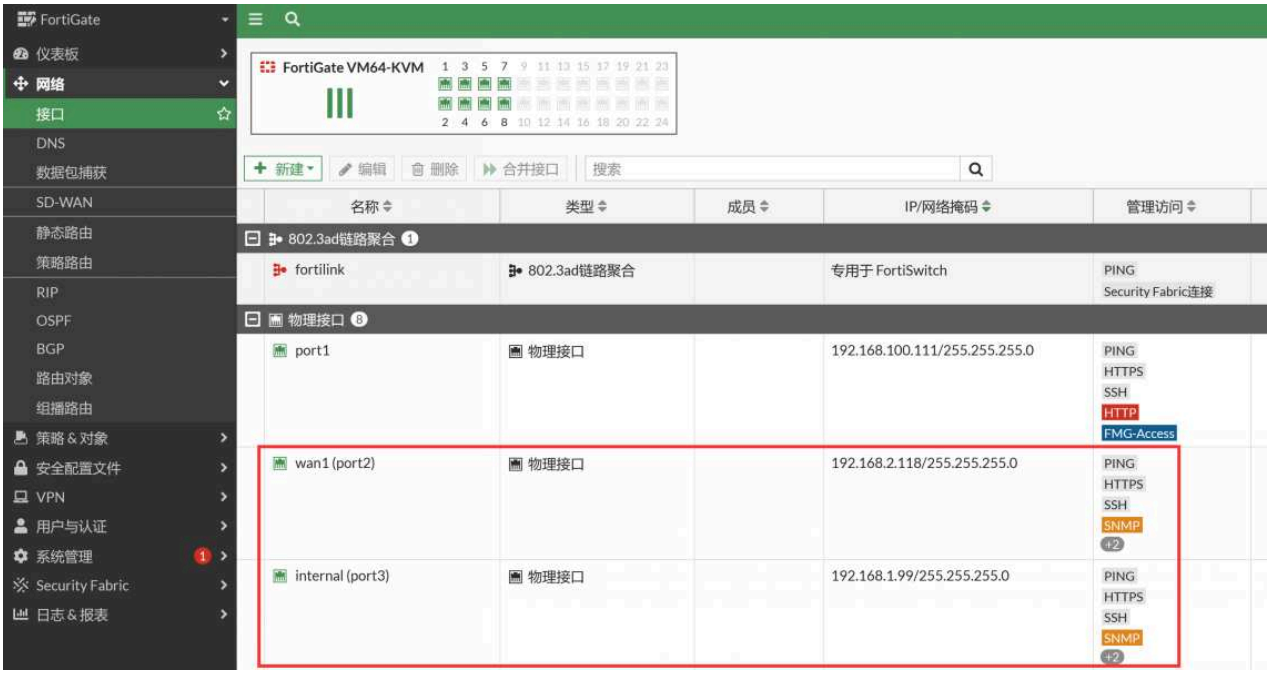
配置要点

- 配置接口地址
- 配置防火墙
- 配置路由器

配置步骤

1. 配置FortiGate接口IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置默认路由。

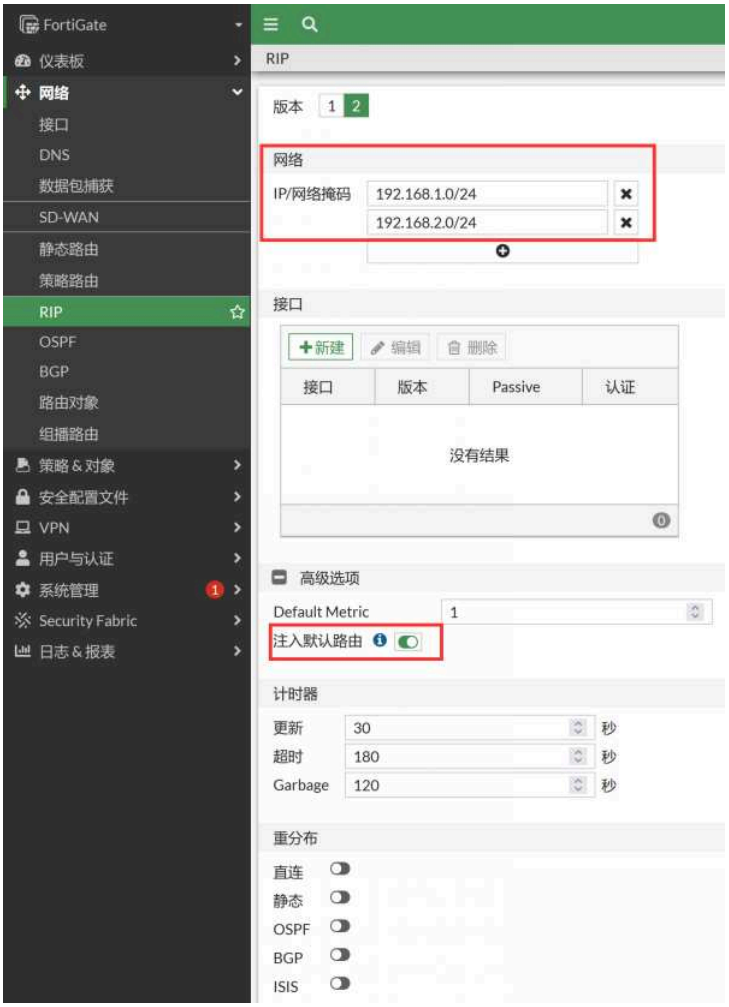


3. 配置RIP，需要进入系统管理→可见功能中打开高级路由。



4. 进入网络→RIP，配置基本信息：选择版本2，添加RIP网络，启用产生缺省路由，向邻居（路由器）发送缺省路由（路由分发：是否对其他协议的路由进行分发）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config router rip
    set default-information-originate enable
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```

5. 配置路由器。

```
interface Ethernet0/1
 ip address 192.168.1.111 255.255.255.0
 duplex auto
!
interface Ethernet0/2
 ip address 192.168.200.100 255.255.255.0
!
router rip
version 2
network 192.168.1.0
network 192.168.10.0
no auto-summary
```

结果验证

1. 查看FortiGate的路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 192.168.100.99, port1, [1/0]
C       192.168.1.0/24 is directly connected, port3
C       192.168.2.0/24 is directly connected, port2
C       192.168.100.0/24 is directly connected, port1
R       192.168.200.0/24 [120/2] via 192.168.1.111, port3, 00:01:18

FortiGate # get router info rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
   Network            Next Hop         Metric From            If     Time
Rs 0.0.0.0/0                               1                   --
Rc 192.168.1.0/24                          1                  port3
Rc 192.168.2.0/24                          1                  port2
R  192.168.200.0/24   192.168.1.111        2 192.168.1.111    port3  02:18
```

2. 查看思科路由器的路由表。

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.1.99 to network 0.0.0.0

R*    0.0.0.0/0 [120/1] via 192.168.1.99, 00:00:07, Ethernet0/1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Ethernet0/1
L        192.168.1.111/32 is directly connected, Ethernet0/1
R     192.168.2.0/24 [120/1] via 192.168.1.99, 00:00:07, Ethernet0/1
      192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.200.0/24 is directly connected, Ethernet0/2
L        192.168.200.100/32 is directly connected, Ethernet0/2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

OSPF基础配置

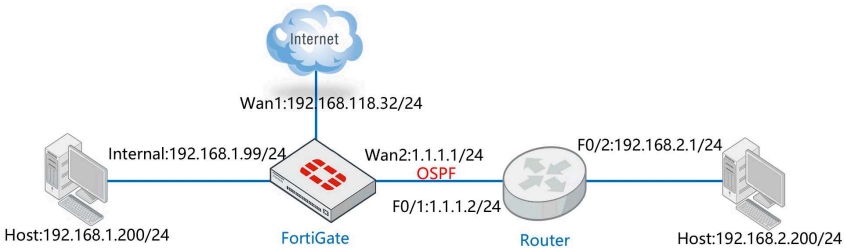
应用场景

1. 若网络中路由设备超过16个，建议使用OSPF，它的路由学习更新速度更快，更适合16个路由设备以上的网络。
2. 当网络路由设备较多，且不超过16个，为避免写大量静态路由，且路由可自动学习，可在FortiGate上配置RIP路由协议功能，让FortiGate也能动态学习到其他网络的路由， 且能自动老化更新。
3. 当网络中路由设备较少，建议使用静态路由即可，维护简单，且对路由器要求不高，因为路由器都支持静态路由，而普通小路由一般不支持RIP协议。

网络需求

1. 内网三层交换机和出口FortiGate间通过动态路由OSPF互相通告路由，实现内网用户正常上网。
2. FortiGate手动配置默认路由，并将其重发布引入OSPF，三层交换机与FortiGate之间通过OSPF互相学习路由，实现内网用户正常上网。

网络拓扑



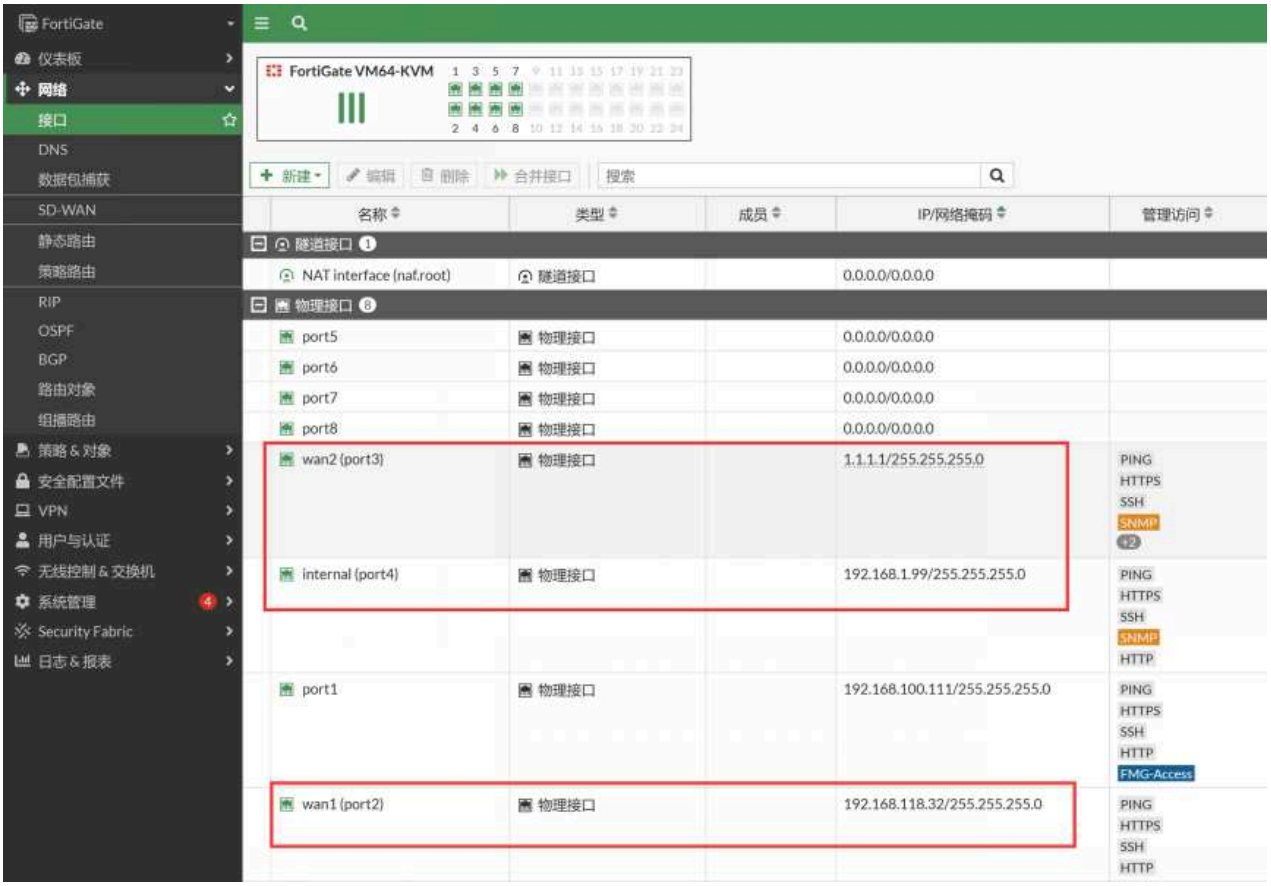
配置要点

- 配置接口地址
- 配置默认路由
- 配置OSPF
- 配置路由器ID
- 发布缺省路由
- 重发布
- 建立OSPF区
- 添加OSPF网络
- 添加接口
- 配置对端路由器

配置步骤

1. 配置接口地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置默认路由。

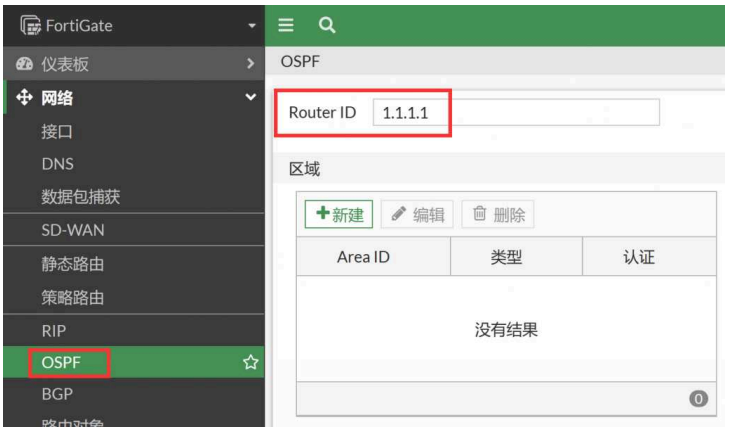


3. 配置OSPF，首先需要在系统配置→可见功能中，开启高级路由功能。

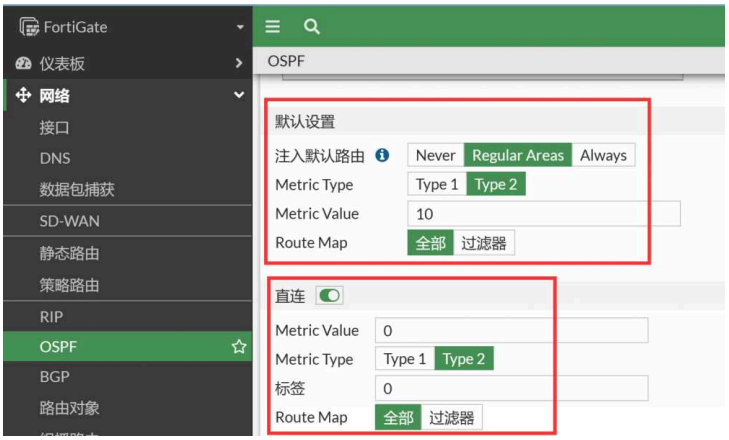
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 进入网络→OSPF页面，配置Router ID。



5. 开启默认路由注入，并开启重发布直连路由。

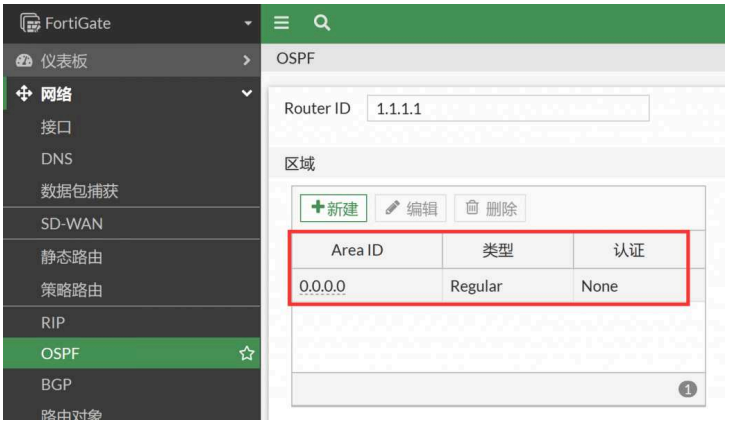


- 配置Router ID，填写ID为1.1.1.1
- 注入缺省路由： 选择 "Regular Areas"，其三个选项意义如下：
  - Never： 从不发送缺省路由表
  - Regular Areas： 如果有则发布，没有则不发布
  - Always： 无论是否有缺省路由表，都发布一条缺省路由出去
- 重发布：勾选 "直连"，将直连的192.168.1.0/24路由信息发送给OSPF邻居

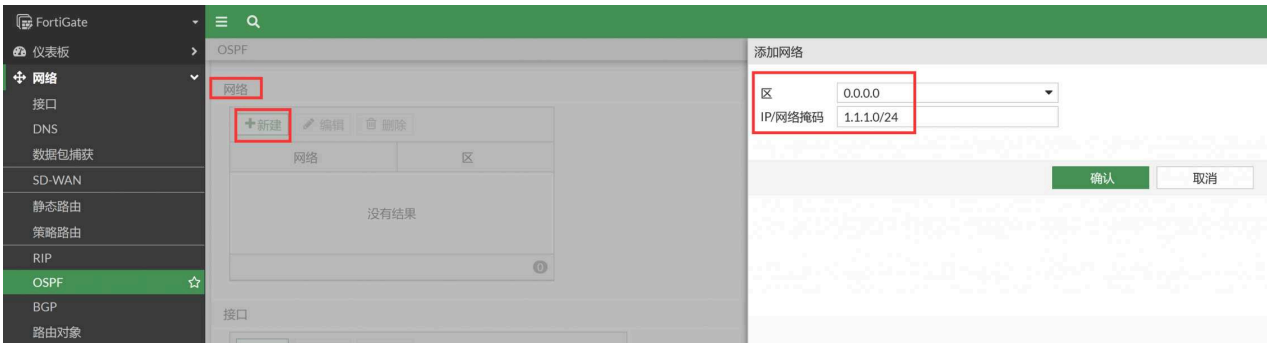
6. 建立OSPF区域，在区域部分点击新建按钮，创建根区域 0.0.0.0（area 0）。

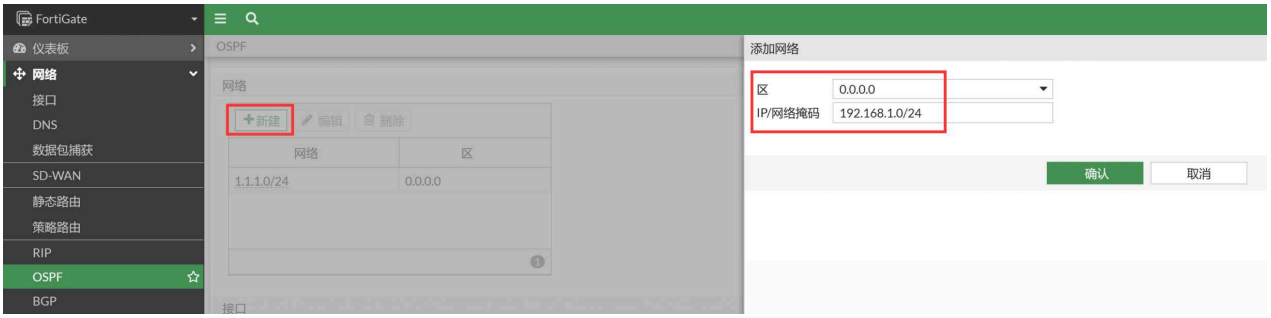
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

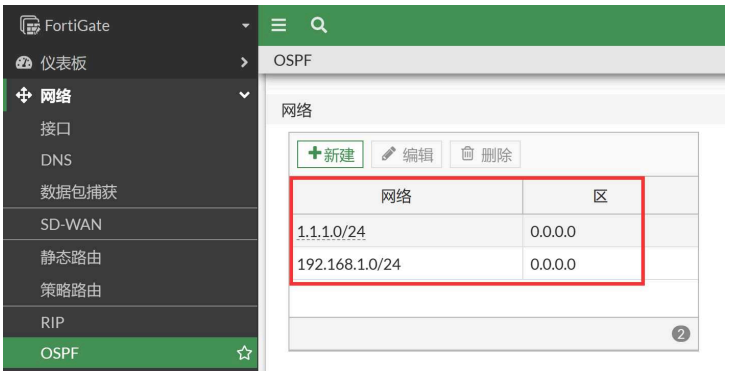




7. 添加OSPF网络，在网络部分点击新建按钮，将1.1.1.0/24和192.168.1.0/24网络加入OSPF区域0.0.0.0，之后点击页面下方的应用按钮应用配置。

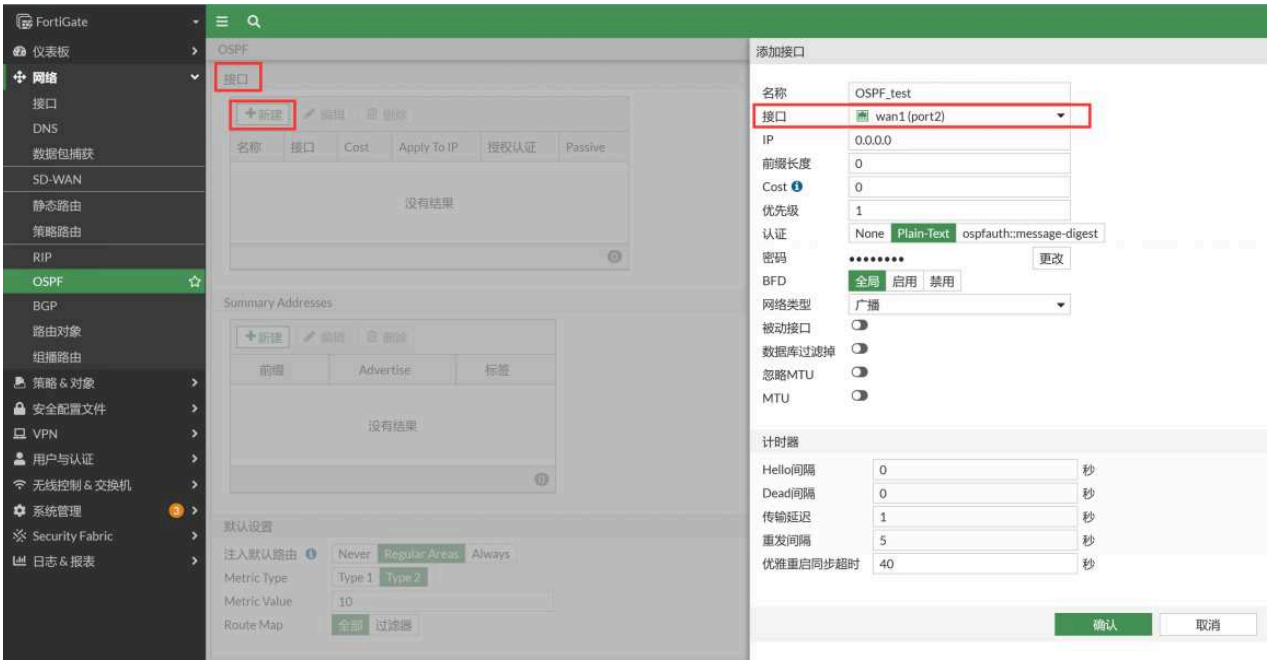






8. 添加OSPF接口（可选，可以自定义OSPF的协商参数），在接口部分点击新建按钮，配置相关的协商参数。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 名称： 标识作用
- 接口：需要编辑的接口
- 认证： 是否需要对该接口进行OSPF的认证，支持Plain-Text（明文），none（无），几种方式
- Cost：接口OSPF cost值，用于SPF的计算，值越小代表越可用于优先转发
- 密码： 输入key的秘钥
- 计时：
  - Hello间隔： hello包的发送间隔默认为10秒，根据需要进行修改，对OSPf邻居协商时，该参数需要相同
  - Dead间隔： 默认为40秒，根据需要进行修改，对OSPf邻居协商时，该参数需要相同

9. 对应的CLI。

```
config router ospf
    set default-information-originate enable
    set router-id 1.1.1.1
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 1.1.1.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.1.0 255.255.255.0
        next
    end
    config redistribute "connected"
        set status enable
    end
    config redistribute "static"
    end
    config redistribute "rip"
    end
    config redistribute "bgp"
    end
    config redistribute "isis"
    end
end
```

.0. 配置路由器。

```
配置接口IP:
interface e 0/1
ip address 1.1.1.2 255.255.255.0
interface e 0/2
ip address 192.168.2.1 255.255.255.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
配置OSPF:
router ospf 10
network 1.1.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0    //该条目也可以采用直连分发的方式发布
```

结果验证

1. 查看FortiGate的路由表，可以看到FortiGate学到了路由器发布的路由192.168.2.0/24。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 192.168.118.1, port2, [1/0]
C       1.1.1.0/24 is directly connected, port3
C       192.168.1.0/24 is directly connected, port4
O       192.168.2.0/24 [110/11] via 1.1.1.2, port3, 00:00:33
C       192.168.100.0/24 is directly connected, port1
C       192.168.118.0/24 is directly connected, port2
```

2. 查看路由器的路由表，可以看到路由器学到了FortiGate重发布的两个直连网段192.168.1.0/24、192.168.118.0/24，以及FortiGate注入的默认路由。

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/10] via 1.1.1.1, 00:00:49, Ethernet0/1
      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.1.1.0/24 is directly connected, Ethernet0/1
L        1.1.1.2/32 is directly connected, Ethernet0/1
O     192.168.1.0/24 [110/11] via 1.1.1.1, 00:00:49, Ethernet0/1
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Ethernet0/2
L        192.168.2.1/32 is directly connected, Ethernet0/2
O E2  192.168.118.0/24 [110/10] via 1.1.1.1, 00:00:49, Ethernet0/1
```

注意事项

route-ttl

1. 在HA主备模式部署环境下，主机会将自己的路由转发表项（FIB）同步给备机。

2. 默认配置下，当一个备机被选举成主机后，其会保留从原主机同步来的FIB表项10s，同时动态路由进程会发起邻居建立过程，重新学习相关的动态路由。HA切换10s后，从原主机同步来的FIB表项会被删除，如果在这10s内动态路由邻居没有建立，无法学习到动态路由表项，会造成HA切换后业务中断的情况。

3. 建议HA主备模式+动态路由的部署模式下，在HA配置中配置route-ttl的时间可以覆盖新主机建立动态路由邻居与学习路由的时间，如下所示。

```
config system ha
    set route-ttl 120
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

graceful-restart

1. 在HA主备模式+动态路由的部署环境下，默认配置下，当HA切换后（或动态路由进程重启），上下游的动态路由邻居设备会删除动态路由邻居，并删除从FortiGate学习到的动态路由，这也会造成HA切换后业务的中断。
2. 解决方法是开启动态路由的graceful-restart功能（并配置restart-period），FortiGate与上下游动态路由邻居设备都需要开启GR功能。

```
config router ospf
    set restart-mode graceful-restart
    set restart-period 120
end
```

3. 开启GR后，FortiGate发生HA主备切换后，上下游的动态路由邻居设备会自动开启GR Helper模式，在此模式下，上下游的动态路由邻居不会删除FortiGate HA切换前与原主机的OSPF邻居关系与其学习到的动态路由，直到FortiGate的新主机与上下游邻居重新建立动态路由邻居或FortiGate配置的restart-period（默认为120s）到期。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

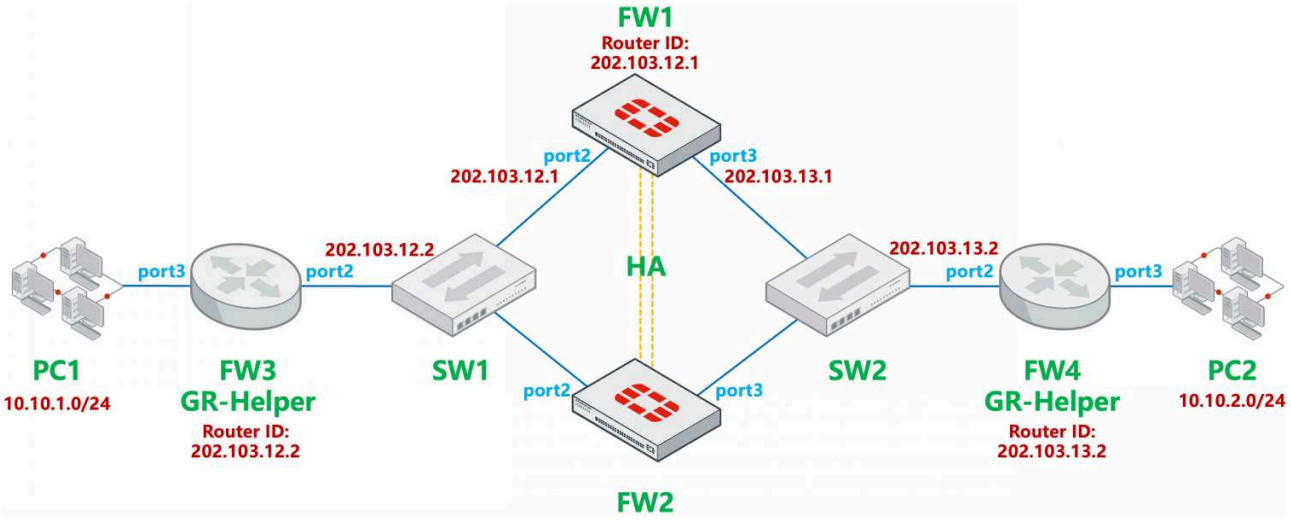
OSPF GR

网络需求

FortiGate HA集群与上下游路由器运行OSPF协议，并开启GR。在FortiGate的HA发生主备切换时，GR需要确保每个路由器（包括FortiGate及其它路由器）在HA切换期间保持其路由表中的OSPF路由（GR Helper），以避免流量中断。

在FortiGate HA集群中，OSPF进程相关工作仅在主设备上运行。当发生HA切换时，将在新选举的主机上启动一个新的OSPF协商过程，在此过程中，新的主机需要在路由Kernel表中维持从原主机学习到的OSPF路由，直至新的OSPF邻居形成。

网络拓扑



1. FW1与FW2建立A-P模式的HA。
2. FW1/FW2与FW3、FW4分别建立OSPF邻居，并宣告各自的网段。
3. FW1/FW2与FW3、FW4开启OSPF Graceful Restart，FW1/FW2发生主备切换后，FW3、FW4可以进入GR Helper模式，协助FW1/FW2的GR过程。

配置步骤

1. 基础网络配置（略）。

2. FW1与FW2的HA配置（略）。

3. 安全策略配置（略）。

4. 配置FW1/FW2的OSPF，宣告网络，开启GR功能，restart-period设置为600s。

```bash
config router ospf
    set router-id 202.103.12.1
    set restart-mode graceful-restart
    set restart-period 600
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 202.103.12.0 255.255.255.0
        next
        edit 2
            set prefix 202.103.13.0 255.255.255.0
        next
    end
end
```

5. 配置FW3的OSPF，宣告网络，路由器作为GR-Helper也需要开启GR功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config router ospf
    set router-id 202.103.12.2
    set restart-mode graceful-restart
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 2
            set prefix 202.103.12.0 255.255.255.0
        next
        edit 3
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```

6. 配置FW4的OSPF，路由器作为GR-Helper也需要开启GR功能。

```bash
config router ospf
    set router-id 202.103.13.2
    set restart-mode graceful-restart
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 202.103.13.0 255.255.255.0
        next
        edit 2
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

7. 配置FW1/FW2 HA配置中的route-ttl为600s（默认10s），在此时间内，新的主机需要在路由Kernel表中维持从原主机学习到的OSPF路由，直至新的OSPF邻居形成。

> **重要**
>
> 重要步骤，防止HA切换后，新主机建立新的OSPF邻居前，路由消失导致业务中断。

```bash
config system ha
    set route-ttl 600
end
```

结果验证

1. 初始状态下，FW1为主设备，FW2为备设备。

```bash
FW1 # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:42869 b:39035389
        traffic.total = s:0 p:42867 b:39033889
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=7 Debug=0
nvcluster=1, ses_pickup=0, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM23000175:      Primary, serialno_prio=1, usr_priority=128, hostname=FW1
FGVM08TM23000176:    Secondary, serialno_prio=0, usr_priority=100, hostname=FW2


```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0
FGVM08TM23000175:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM23000176:    Secondary, ha_prio/o_ha_prio=1/1
```

2. 初始状态下查看FW3的OSPF邻居状态与路由信息，邻居状态为Full，OSPF路由学习正常，未进入GR Helper状态。

```bash
FW3 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
202.103.12.1      1   Full/DR         00:00:34    202.103.12.1    port2

FW3 # get router info routing-table ospf
Routing table for VRF=0
O       10.10.2.0/24 [110/3] via 202.103.12.1, port2, 02:47:00, [1/0]
O       202.103.13.0/24 [110/2] via 202.103.12.1, port2, 02:47:00, [1/0]
```

3. 初始状态下查看FW4的OSPF邻居状态与路由信息，邻居状态为Full，OSPF路由学习正常，未进入GR Helper状态。

```bash
FW4 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
202.103.12.1      1   Full/Backup     00:00:33    202.103.13.1    port2

FW4 # get router info routing-table ospf
Routing table for VRF=0
O       10.10.1.0/24 [110/3] via 202.103.13.1, port2, 02:50:08, [1/0]
O       202.103.12.0/24 [110/2] via 202.103.13.1, port2, 02:50:08, [1/0]
```

4. 初始状态下查看FW1的OSPF邻居状态与路由信息，邻居状态为Full，OSPF路由学习正常。

```bash
FW1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
202.103.12.2      1   Full/Backup     00:00:38    202.103.12.2    port2
202.103.13.2      1   Full/DR         00:00:40    202.103.13.2    port3

FW1 # get router info routing-table ospf
Routing table for VRF=0
O       10.10.1.0/24 [110/2] via 202.103.12.2, port2, 02:49:28, [1/0]
O       10.10.2.0/24 [110/2] via 202.103.13.2, port3, 02:49:28, [1/0]
```

5. 使FW1和FW2发生HA主备倒换，此时FW2成为HA主设备。

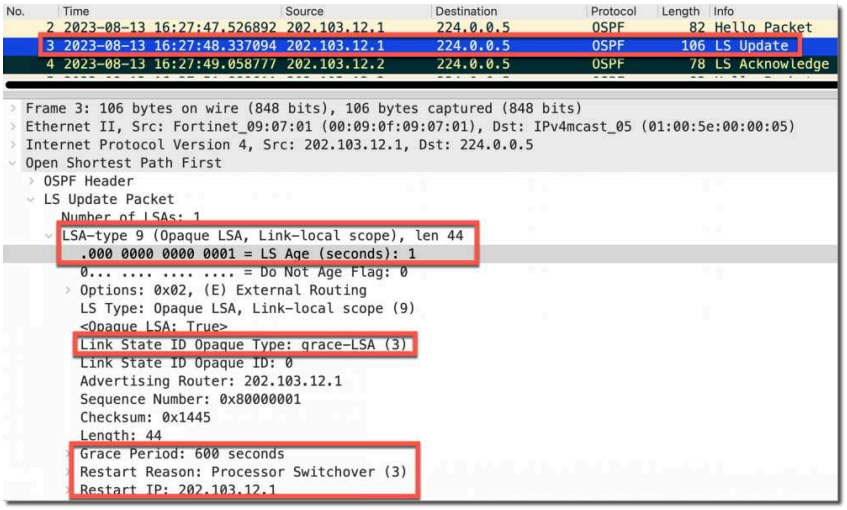
```bash
FW2 # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:6233 b:4732229
        traffic.total = s:0 p:6286 b:4735596
        activity.ha_id_changes = 4
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=7 Debug=0
nvcluster=1, ses_pickup=0, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM23000176:      Primary, serialno_prio=0, usr_priority=100, hostname=FW2
FGVM08TM23000175:    Secondary, serialno_prio=1, usr_priority=128, hostname=FW1

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0
FGVM08TM23000176:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM23000175:    Secondary, ha_prio/o_ha_prio=1/1
```

6. 查看FW2的OSPF Debug信息，FW2成为HA主后，向OSPF邻居发送grace LSA（Type 9），通知邻居自己进入了GR过程，包含GR的原因和GR最大时间，LS Age为1s。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW2 # diagnose ip router ospf level info
FW2 # diagnose ip router ospf all enable
FW2 # diagnose debug console time enable

2023-08-13 16:27:48 OSPF: SEND[LS-Upd]: To 224.0.0.5 via port2:202.103.12.1, length 120
2023-08-13 16:27:48 OSPF:     LS type 9 (Link-Local Opaque-LSA)
2023-08-13 16:27:48 OSPF:     Grace-LSA
2023-08-13 16:27:48 OSPF:     Grace Period: 600
2023-08-13 16:27:48 OSPF:     Graceful Restart Reason: Switch to redundant control processor
2023-08-13 16:27:48 OSPF:     IP interface Address: 202.103.12.1
```

7. 该报文格式如下图所示，LS age为1。



8. 在FW2进入GR状态后，查看FW3的OSPF邻居状态与OSPF路由状态，FW3进入GR Helper状态（*标记），Dead Time变为FW1/FW2配置的GR period 600s。（FW4也是一样的状态，这里就不再赘述）

```bash
FW3 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
202.103.12.1      1   Full/Backup     00:09:51*   202.103.12.1    port2

FW3 # get router info routing-table ospf
Routing table for VRF=0
O       10.10.2.0/24 [110/3] via 202.103.12.1, port2, 00:33:17, [1/0]
O       202.103.13.0/24 [110/2] via 202.103.12.1, port2, 00:34:16, [1/0]
```

9. 在FW3上查看OSPF的Debug信息，FW3收到GR LSA后，进入GR Helper模式。（FW4也是一样的状态，这里就不再赘述）

```bash
FW3 # diagnose ip router ospf level info
FW3 # diagnose ip router ospf all enable
FW3 # diagnose debug console time enable

2023-08-13 16:27:48 OSPF: RECV[LS-Upd]: From 202.103.12.1 via port2:202.103.12.2 (202.103.12.1 -> 224.0.0.5)
2023-08-13 16:27:48 OSPF:     LS type 9 (Link-Local Opaque-LSA)
2023-08-13 16:27:48 OSPF:   Grace-LSA
2023-08-13 16:27:48 OSPF:     Grace Period: 600
2023-08-13 16:27:48 OSPF:     Graceful Restart Reason: Switch to redundant control processor
2023-08-13 16:27:48 OSPF:     IP interface Address: 202.103.12.1
2023-08-13 16:27:48 OSPF: Router: Enter Helper mode by grace LSA
```

0. 查看FW3上的OSPF 9类LSA的状态，此时LS Age未到达3600s。（FW4也是一样的状态，这里就不再赘述）

```bash
FW3 # get router info ospf database opaque-area

            OSPF Router with ID (202.103.12.2) (Process ID 0, VRF 0)
                Link-Local Opaque-LSA (Link port2:202.103.12.2)
  LS age: 5
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: Link-Local Opaque-LSA
  Link State ID: 3.0.0.0 (Link-Local Opaque-Type/ID)
  Opaque Type: 3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  Opaque ID: 0
  Advertising Router: 202.103.12.1
  LS Seq Number: 80000001
  Checksum: 0x1445
  Length: 44
      Grace Period: 600
      Graceful Restart Reason: Switch to redundant control processor
      IP Interface Address: 202.103.12.1
```

1. 等待FW2与FW3的OSPF邻居变为Full状态后，FW2的GR完成，FW3退出GR Helper状态，期间OSPF路由没有丢失，Dead Time从40s开始倒计时。（FW4也是一样的状态，这里就不再赘述）

```bash
FW3 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
202.103.12.1      1   Full/Backup     00:00:36    202.103.12.1    port2

FW3 # get router info routing-table ospf
Routing table for VRF=0
O       10.10.2.0/24 [110/3] via 202.103.12.1, port2, 00:00:03, [1/0]
O       202.103.13.0/24 [110/2] via 202.103.12.1, port2, 00:34:31, [1/0]
```

2. 在FW2上查看OSPF的Debug信息，FW2正常退出了GR，并发送Age为3600的grace-LSA。

```bash
FW2 # diagnose ip router ospf level info
FW2 # diagnose ip router ospf all enable
FW2 # diagnose debug console time enable

2023-08-13 16:27:57 OSPF: ROUTER[Process:0, RouterID:202.103.12.1]: Exit Restarting normally
2023-08-13 16:27:57 OSPF: SEND[LS-Upd]: To 224.0.0.5 via port3:202.103.13.1, length 72
2023-08-13 19:05:59 OSPF:     LS age 3600
2023-08-13 19:05:59 OSPF:     LS type 9 (Link-Local Opaque-LSA)
2023-08-13 19:05:59 OSPF:   Grace-LSA
```

3. 在FW3上查看OSPF的Debug信息，FW3收到FW2发送的maxage的LSA后，等待几秒后退出GR Helper状态。

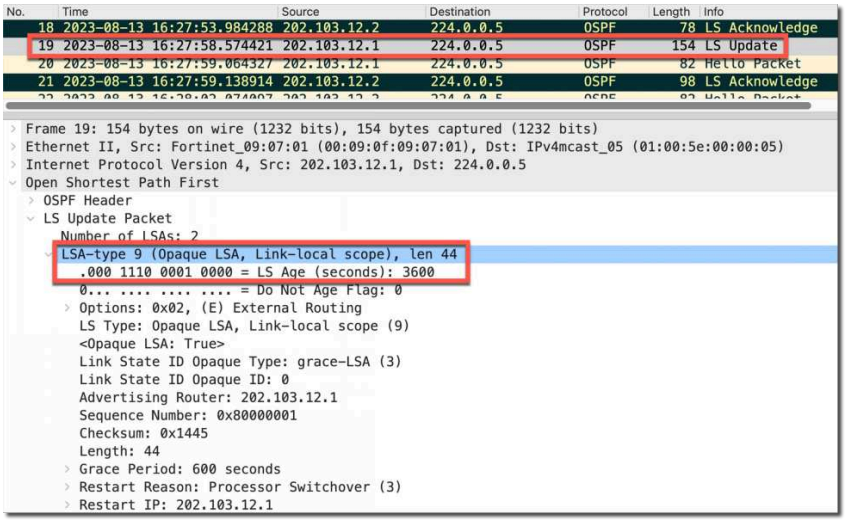
```bash
2023-08-13 16:28:08 OSPF: ROUTER: Exit Restart Helper mode for neighbor(port2:202.103.12.2-202.103.12.1) by receiving maxage grace-LSA
```

4. 再次查看FW3上的OSPF 9类LSA的状态，此时LS Age直接到达3600s。

```bash
FW3 # get router info ospf database opaque-link

            OSPF Router with ID (202.103.12.2) (Process ID 0, VRF 0)
                Link-Local Opaque-LSA (Link port2:202.103.12.2)
  LS age: 3600
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: Link-Local Opaque-LSA
  Link State ID: 3.0.0.0 (Link-Local Opaque-Type/ID)
  Opaque Type: 3
  Opaque ID: 0
  Advertising Router: 202.103.12.1
  LS Seq Number: 80000001
  Checksum: 0x1445
  Length: 44
      Grace Period: 600
      Graceful Restart Reason: Switch to redundant control processor
      IP Interface Address: 202.103.12.1
```

5. 抓包查看FW3收到的这个maxage grace-LSA，可以看到LSA的age为3600s，达到了OSPF定义的maxage（https://www.rfc-editor.org/rfc/rfc2328#appendix-B ↗），可以理解为FW2的OSPF邻居状态为Full后，会通过再次发送此类型的LSA告知GR Helper，可以退出GR Helper模式了。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. GR期间，FW2/FW4从FW1重启前同步的路由一直存在（route-ttl 600，prio=2164260865）。

```
FW2 # get router info kernel | grep 10.10.
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.1.0/24 pref=0.0.0.0 gwy=202.103.12.2
dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.2.0/24 pref=0.0.0.0 gwy=202.103.13.2
dev=5(port3)
```

bash

7. GR结束后，学到了新的OSPF路由（prio=1）。

```
FW2 # get router info kernel | grep 10.10.
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.1.0/24 pref=0.0.0.0 gwy=202.103.12.2
dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.1.0/24 pref=0.0.0.0 gwy=202.103.12.2
dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.2.0/24 pref=0.0.0.0 gwy=202.103.13.2
dev=5(port3)
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.2.0/24 pref=0.0.0.0 gwy=202.103.13.2
dev=5(port3)
```

bash

8. 整个HA切换引起的GR期间，所有设备路由转发表未发生实际变化，流量不会中断。

注意事项

1. 在以上测试步骤过程中，如果FW1/FW2在GR的过程中发现了OSPF拓扑变化，则会直接终端并退出GR的过程，同时通知FW3/FW4退出GR Helper状态，导致OSPF路由提前从GR Helper设备上消失，导致业务临时中断。

```
FW2 # diagnose ip router ospf level info
FW2 # diagnose ip router ospf all enable
FW2 # diagnose debug console time enable

2023-08-13 17:45:46 OSPF: ROUTER[Process:0, RouterID:202.103.12.1]: Exit Restarting by NbrChanged
(port3:202.103.13.1-202.103.13.2)
2023-08-13 17:45:46 OSPF: LSA[-:Type9:3.0.0.0:(self)]: Flooding via interface[port2:202.103.12.1]
2023-08-13 17:45:46 OSPF: LSA[-:Type9:3.0.0.0:(self)]: Flooding to neighbor[202.103.12.2]
......
2023-08-13 17:45:46 OSPF: SEND[LS-Upd]: To 224.0.0.5 via port2:202.103.12.1, length 72
2023-08-13 17:45:46 OSPF:     LS age 3600
2023-08-13 17:45:46 OSPF:     LS type 9 (Link-Local Opaque-LSA)
```

bash

2. 为了避免OSPF拓扑变化导致的GR提前退出，可以在FW1/FW2上开启OSPF的restart-on-topology-change，开启后，OSPF进程在GR的过程中将忽略拓扑变化，继续完成GR的整个过程。

> **重要**
>
> 仅支持7.2.0及以后版本。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config router ospf
    set restart-on-topology-change enable
end
```

3. 如下Debug信息所示，FW1/FW2在GR期间探测到拓扑变化，但没有立即退出GR，而是继续正常完成了GR。

```bash
2023-08-13 19:05:56 OSPF: ROUTER[Process:0, RouterID:202.103.12.1]: Exit Restarting by NbrChanged
(port3:202.103.13.1-202.103.13.2)
2023-08-13 19:05:56 OSPF: ROUTER[Process:0, RouterID:202.103.12.1]: skip exiting restart due to topology change
......
2023-08-13 19:05:59 OSPF: ROUTER[Process:0, RouterID:202.103.12.1]: Exit Restarting normally
......
2023-08-13 19:05:59 OSPF: SEND[LS-Upd]: To 224.0.0.6 via port2:202.103.12.1, length 72
2023-08-13 19:05:59 OSPF:     LS age 3600
2023-08-13 19:05:59 OSPF:     Options 0×2
2023-08-13 19:05:59 OSPF:     LS type 9 (Link-Local Opaque-LSA)
2023-08-13 19:05:59 OSPF:     Advertising Router 202.103.12.1
2023-08-13 19:05:59 OSPF:   Grace-LSA
......
```

GR与BFD的使用关系

> **重要**
>
> BGP GR或OSPF GR不建议与BFD同时使用。

GR用于FortiGate通知邻居自己的路由进程将重启，并且邻居从FortiGate学到的路由应在重启期间保留。但BFD检测到故障时会将动态路由邻居重置。这种操作上的差异使得在GR的同时使用BFD会导致功能上的冲突，可能导致GR期间流量中断。

业界通用的做法是在使用GR时关闭BFD。例如在 FortiGate和GCP（Google 云平台）之间配置动态路由 + GR + BFD时：

- GCP将关闭BFD并发送AdminDown（BFD事件）到FortiGate（参考https://cloud.google.com/network-connectivity/docs/router/concepts/bfd#graceful-restart-and-bfd ）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP基础配置

BGP简介

边界网关协议（BGP）是一种标准化的路由协议，用于在互联网上路由流量。它在互联网上的自治系统（AS）之间交换路由信息，并根据路径、网络策略和规则集做出路由决策。BGP包含两个子集：内部BGP（iBGP）和外部BGP（eBGP）。iBGP用于在自己的网络内部使用。eBGP用于连接不同的网络，并且是互联网骨干的主要路由协议。

FortiGate的BGP基础配置参数如下：

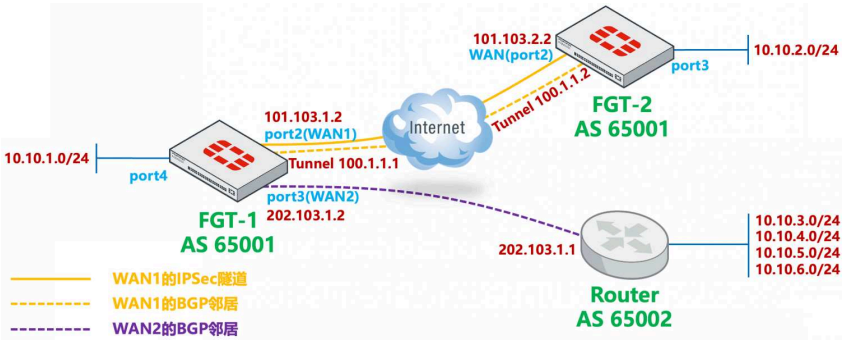
选项	描述
本地AS	本地FortiGate的AS号。
Router ID	一个用于在网络中标识你的路由器的唯一ID，通常以x.x.x.x的格式表示。
邻居	FortiGate将与之进行BGP连接的邻居。配置远程路由器的自治系统（Remote AS）号码，与邻居连接所使用的任何其他属性，以及IPv4和IPv6路由过滤。
邻居组	共享相同出站策略配置的邻居组，一般用于被多个BGP邻居主动连接的情况。
邻居范围	BGP邻居的源地址范围，用于分配给一个邻居组。
IPv4 & IPv6网络	要宣告给其他BGP路由器的网络。
IPv4 & IPv6重分发	启用协议的重分发。指定某个路由协议的路由，可以通过route-map进行过滤。
Dampening	启用路由振荡抑制以减少振荡路由的传播。
优雅重启（graceful-restart）	启用BGP优雅重启（graceful-restart），相邻的路由器在FortiGate重启BGP进程时保持BGP路由条目。在HA中发生主备切换时非常有用（暂不支持GR Helper配置为GR Helper-only模式）。
高级选项	多种BGP高级选项，如Local Preference、Local Preference、Distance internal、Keepalive、Holdtime等。
最佳路径选择	路径选择的相关属性配置。

BGP选路原则

1. 优先选择具有最高的Weight的路由（Weight仅本地生效）。
2. 优先选择具有最高的Local Preference的路由（仅在本AS内生效）。
3. 优先选择本地路由器产生的路由（下一跳为0.0.0.0）。
4. 优先选择具有最短的AS-Path的路由。
5. IGP路由 > EGP路由 > incomplete路由。
6. 优先选择具有最低MED（可在AS之间交换）的路由。
7. eBGP路径优先于iBGP路由。
8. iBGP路由优先选择更近的iBGP邻居学习到的路由。
9. eBGP路由优先选择更早学习到的eBGP路由。
0. 优先选择具有最小邻居Router ID的路由。
1. 优先选择具有最小邻居IP的路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

网络拓扑



1. 网络连接：

- FGT-1与FGT-2通过ISP1的Internet建立IPSec隧道，二阶段保护网段两端均为0.0.0.0/0（配置略）。
- 为两台FortiGate的IPSec Tunnel接口配置IP，并配置IPSec业务互访的放通策略（配置略）：
  - FGT-1 Tunnel IP：100.1.1.1。
  - FGT-2 Tunnel IP：100.1.1.2。
- FGT-1与Router为直连网段设备。

2. BGP邻居：

- FGT-1与FGT-2通过IPSec隧道建立iBGP邻居，BGP均创建在IPSec Tunnel接口上。
- FGT-1与Router之间使用物理口建立eBGP邻居。

3. 路由学习：

- FGT-1和FGT-2互相学习IBGP路由并通过IPSec隧道通信。
- FGT-1从Router学习eBGP路由，并发布到FGT-2，但不允许发布任何iBGP路由到Router。
- FGT-1通过eBGP向Router发布默认路由。

配置步骤

基础配置

1. FGT-1的VPN配置。

```bash
config vpn ipsec phase1-interface
    edit "to_FGT-2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set dpd on-idle
        set remote-gw 101.103.2.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FGT-2"
        set phase1name "to_FGT-2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

2. FGT-2的VPN配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config vpn ipsec phase1-interface
    edit "to_FGT-1"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set dpd on-idle
        set remote-gw 101.103.1.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FGT-1"
        set phase1name "to_FGT-1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

3. FGT-1的接口与静态路由配置。

```bash
config system interface
    edit "port2"
        set vdom "root"
        set ip 101.103.1.2 255.255.255.0
        set alias "WAN1"
    next
    edit "port3"
        set vdom "root"
        set ip 202.103.1.2 255.255.255.0
        set alias "WAN2"
    next
    edit "port4"
        set vdom "root"
        set ip 10.10.1.1 255.255.255.0
        set allowaccess ping https http
        set alias "LAN"
    next
    edit "to_FGT-2"
        set vdom "root"
        set ip 100.1.1.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 100.1.1.254 255.255.255.0
        set interface "port2"
    next
end

config router static
    edit 1
        set gateway 101.103.1.1
        set device "port2"
    next
end
```

4. FGT-2的接口与静态路由配置。

```bash
config system interface
    edit "port2"
        set vdom "root"
        set ip 101.103.2.2 255.255.255.0
        set alias "WAN"
    next
    edit "port3"
        set vdom "root"
        set ip 10.10.2.1 255.255.255.0
        set alias "LAN"
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    edit "to_FGT-1"
        set vdom "root"
        set ip 100.1.1.2 255.255.255.255
        set allowaccess ping https http
        set type tunnel
        set remote-ip 100.1.1.254 255.255.255.0
        set interface "port2"
    next
end

config router static
    edit 1
        set gateway 101.103.2.1
        set device "port2"
    next
end

```

5. 配置安全策略，放通FGT-1和FGT-2间IPSec隧道的流量，按需配置其他安全策略（略）。

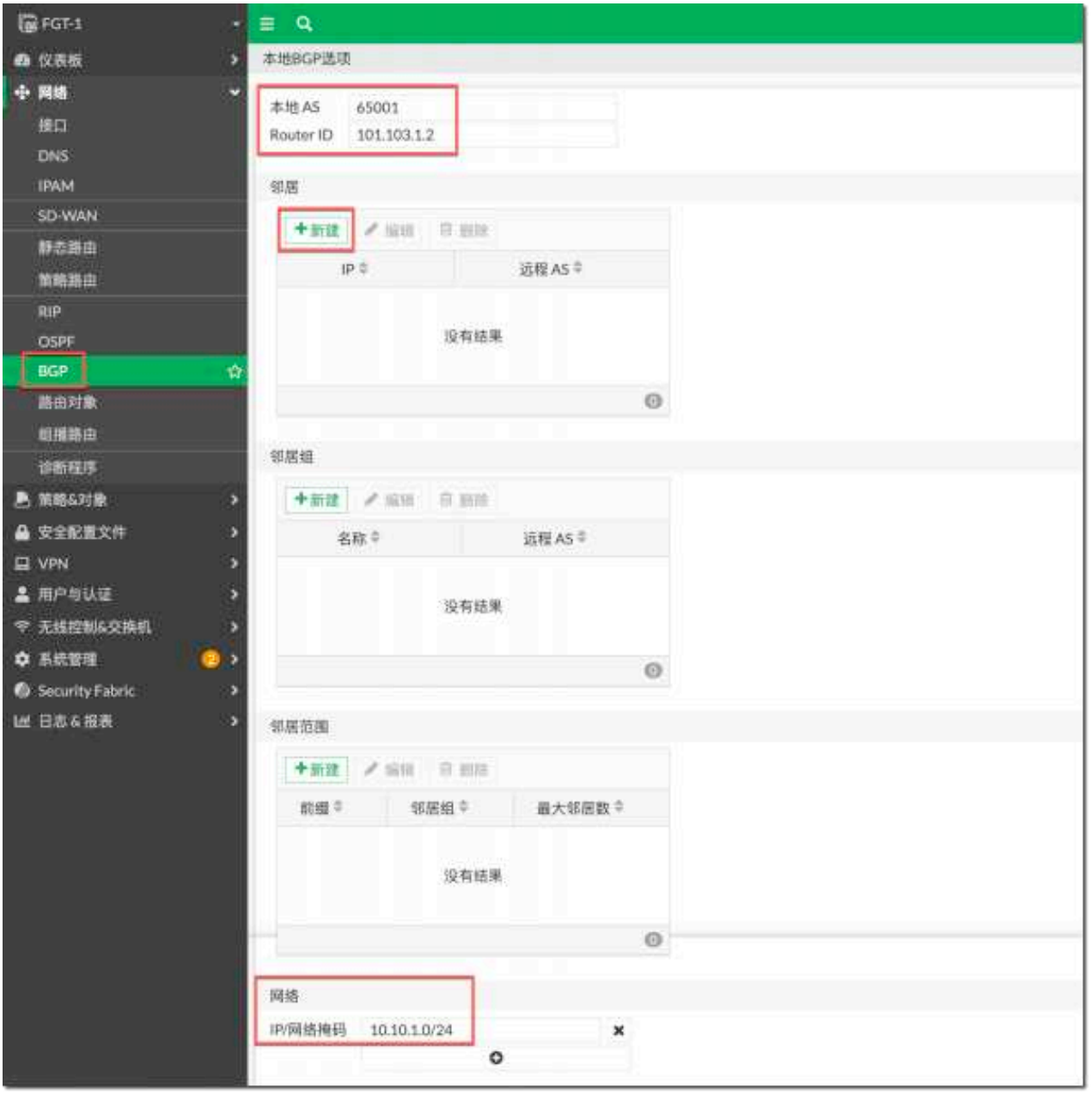
6. 等待FGT-1和FGT-2之间的IPSec隧道建立成功。

```bash
FGT-1 # get vpn ipsec tunnel summary
'to_FGT-2' 101.103.2.2:0  selectors(total,up): 1/1  rx(pkt,err): 395/0  tx(pkt,err): 396/0

FGT-2 # get vpn ipsec tunnel summary
'to_FGT-1' 101.103.1.2:0  selectors(total,up): 1/1  rx(pkt,err): 397/0  tx(pkt,err): 396/0
```

iBGP（FGT-1 to FGT-2）

1. 在FGT-1上进入网络→BGP页面，配置本地AS和Router ID，在网络选项中配置要发布的本地路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



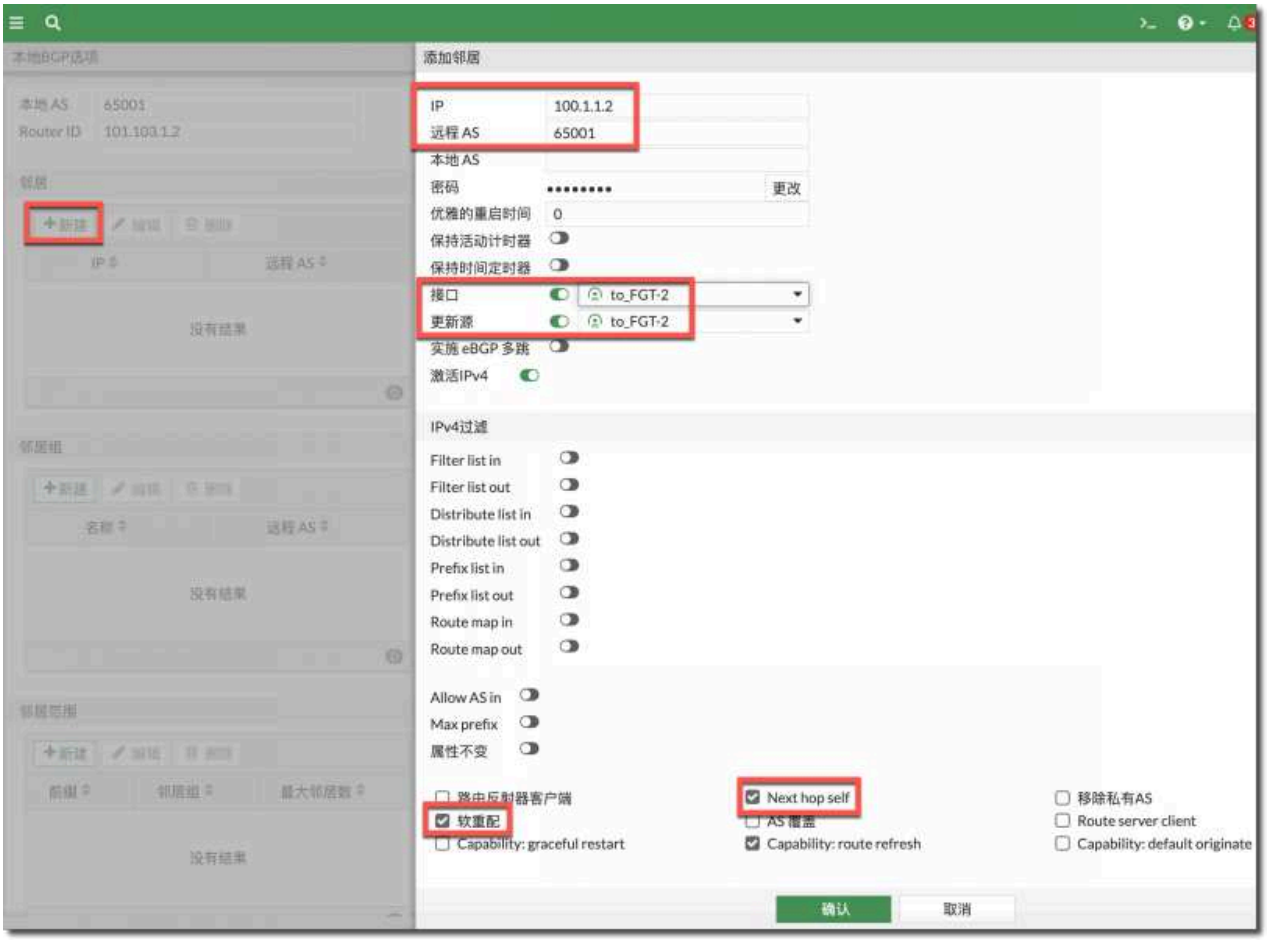
重要

默认配置下，BGP只能发布设备自身路由表中已经存在的路由条目（路由与掩码都要一致），如果需要发布路由表中不存在的路由条目，需要使用如下CLI关闭发布路由的检查。

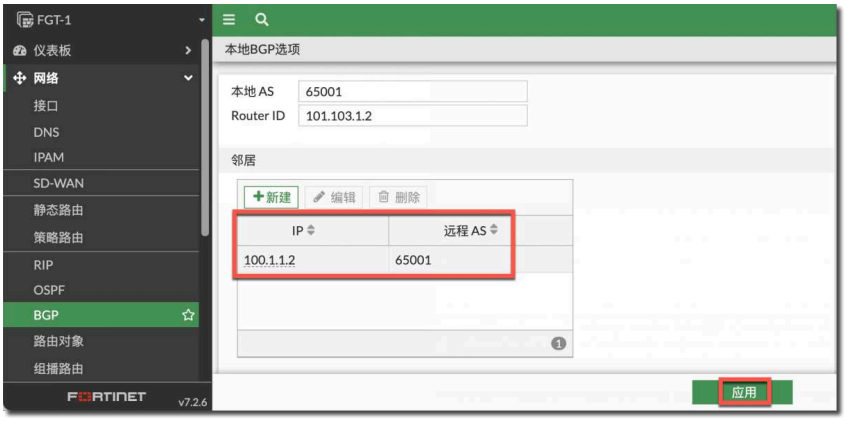
```bash
config router bgp
    set network-import-check disable
end
```

2. 点击邻居选项中的新建按钮，在弹出的新建邻居页面中配置iBGP邻居的IP、远程AS，接口和更新源都选择IPSec Tunnel接口，开启“Next hop self”（FGT-1向FGT-2宣告Router发送的eBGP路由时，将下一跳改为自己的IPSec tunnel口IP），建议开启软重配功能，点击确认下发BGP邻居配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在BGP页面点击应用下发BGP配置。



4. 相关CLI如下。

```bash
config router bgp
    set as 65001
    set router-id 101.103.1.2
    config neighbor
        edit "100.1.1.2"
            set next-hop-self enable
            set soft-reconfiguration enable
            set interface "to_FGT-2"
            set remote-as 65001
            set update-source "to_FGT-2"
        next
    end
    config network
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```

5. 在FGT-2使用与FGT-1同样的步骤配置iBGP，过程略，相关配置CLI如下。

```bash
config router bgp
    set as 65001
    set router-id 101.103.2.2
    config neighbor
        edit "100.1.1.1"
            set soft-reconfiguration enable
            set interface "to_FGT-1"
            set remote-as 65001
            set update-source "to_FGT-1"
        next
    end
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

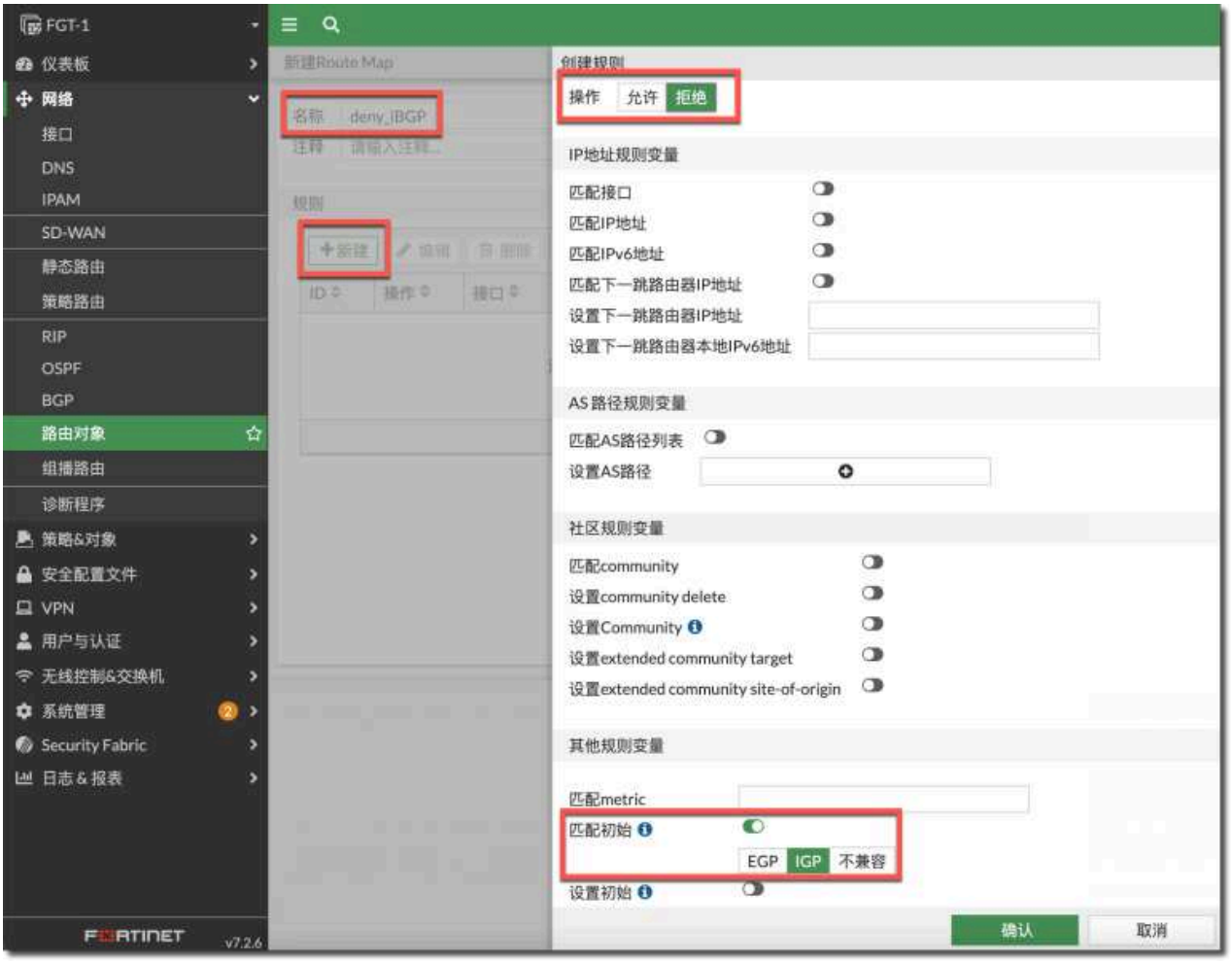
eBGP

1. 在FGT-1上新建Route Map，用于阻止从FGT-2学到的iBGP路由发布到eBGP邻居Router。进入网络→路由对象页面，点击新建→Route Map。



2. 配置Route Map的名称，并点击规则下的新建按钮。在弹出的新建规则页面中配置动作为拒绝，在“其他规则变量”中开启“匹配初始”，并选择IGP，下发规则和Route Map的配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

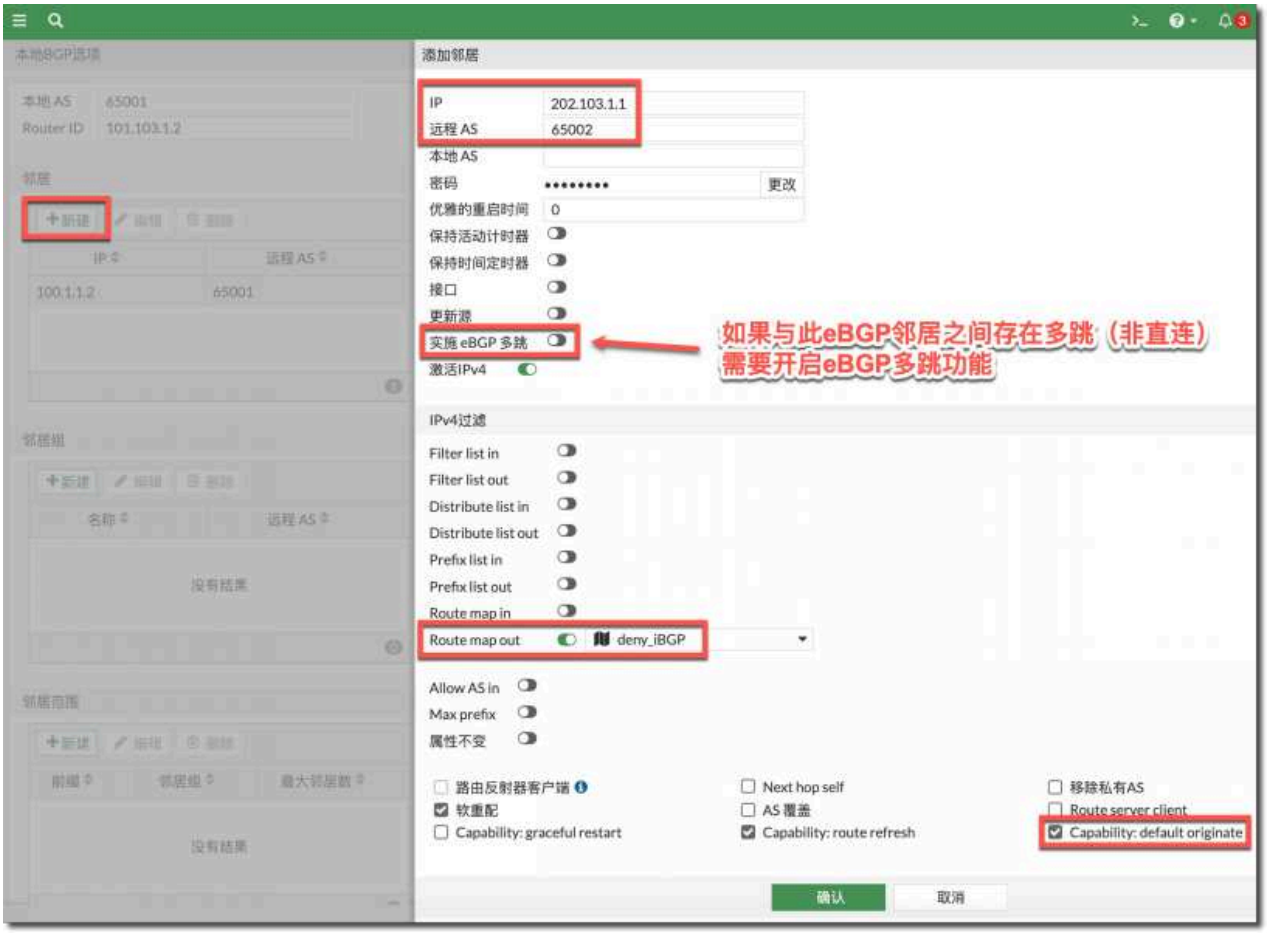



```bash
config router route-map
    edit "deny_iBGP"
        config rule
            edit 1
                set action deny
                set match-origin igp
            next
        end
    next
end
```

3. 在FGT-1上进入网络→BGP页面，点击邻居选项中的新建按钮，在弹出的新建邻居页面中配置eBGP邻居的IP、远程AS，在“IPv4过滤”中的“Route map out”引用上步创建的Route Map，开启“Capability: default originate”功能，向Router宣告默认路由，建议开启软重配功能，随后下发BGP邻居配置和BGP配置。

> **重要**
>
> 如果与此eBGP邻居之间存在多跳（非直连），需要开启eBGP多跳功能（set ebgp-enforce-multihop enable）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config router bgp
    config neighbor
        edit "202.103.1.1"
            set capability-default-originate enable
            set soft-reconfiguration enable
            set remote-as 65002
            set route-map-out "deny_iBGP"
        next
    end
end
```

4. 在Router上参考FGT-1配置eBGP邻居，配置略，相关CLI如下。

```bash
config router bgp
    set as 65002
    set router-id 202.103.1.1
    config neighbor
        edit "202.103.1.2"
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 10.10.3.0 255.255.255.0
        next
        edit 2
            set prefix 10.10.4.0 255.255.255.0
        next
        edit 3
            set prefix 10.10.5.0 255.255.255.0
        next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        edit 4
            set prefix 10.10.6.0 255.255.255.0
        next
    end
end
```

结果验证

FGT-1

1. 在FGT-1上查看BGP邻居状态，可以看到和FGT-2、Router分别建立了BGP邻居，并学习到路由（从FGT-2学到1条，从Router学习到4条）。

> **重要**
>
> 查看BGP邻居的详细信息，请使用`get router info bgp neighbors`。

bash
```
FGT-1 # get router info bgp summary

VRF 0 BGP router identifier 101.103.1.2, local AS number 65001
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.1.1.2   4      65001     142     162        8    0    0 00:29:39        1
202.103.1.1 4      65002      15      16        8    0    0 00:11:01        4

Total number of neighbors 2
```

2. 在FGT-1上查看从不同邻居收到的路由条目。

bash
```
FGT-1 # get router info bgp neighbors 100.1.1.2 received-routes
VRF 0 BGP table version is 3, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.2.0/24     100.1.1.2                   100      0        0 i ←/→

Total number of prefixes 1

FGT-1 # get router info bgp neighbors 202.103.1.1 received-routes
VRF 0 BGP table version is 3, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.3.0/24     202.103.1.1                           0        0 65002 i ←/→
*> 10.10.4.0/24     202.103.1.1                           0        0 65002 i ←/→
*> 10.10.5.0/24     202.103.1.1                           0        0 65002 i ←/→
*> 10.10.6.0/24     202.103.1.1                           0        0 65002 i ←/→

Total number of prefixes 4
```

3. 在FGT-1上查看向不同邻居发布的路由条目。

bash
```
FGT-1 # get router info bgp neighbors 100.1.1.2 advertised-routes
VRF 0 BGP table version is 3, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.1.0/24     100.1.1.1                   100  32768        0 i ←/→
*>i10.10.3.0/24     100.1.1.1                   100      0        0 65002 i ←/→
*>i10.10.4.0/24     100.1.1.1                   100      0        0 65002 i ←/→
*>i10.10.5.0/24     100.1.1.1                   100      0        0 65002 i ←/→
*>i10.10.6.0/24     100.1.1.1                   100      0        0 65002 i ←/→
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Total number of prefixes 5

FGT-1 # get router info bgp neighbors 202.103.1.1 advertised-routes
VRF 0 BGP table version is 3, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        202.103.1.2                    100  32768        0 i ←/→

Total number of prefixes 1
```

4. 在FGT-1上查看BGP路由数据库，可以看到iBGP路由前边会有i标记，包含本地发布的路由（weight为32768）。

```
FGT-1 # get router info bgp network
VRF 0 BGP table version is 8, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                        100  32768        0 i ←/1>
*>i10.10.2.0/24     100.1.1.2       0              100      0        0 i ←/1>
*> 10.10.3.0/24     202.103.1.1     0                       0        0 65002 i ←/1>
*> 10.10.4.0/24     202.103.1.1     0                       0        0 65002 i ←/1>
*> 10.10.5.0/24     202.103.1.1     0                       0        0 65002 i ←/1>
*> 10.10.6.0/24     202.103.1.1     0                       0        0 65002 i ←/1>

Total number of prefixes 6
```

5. 查看指定的某个BGP路由详细信息可以在该命令后加相应网段。

```
FGT-1 # get router info bgp network 10.10.3.0
VRF 0 BGP routing table entry for 10.10.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   100.1.1.2
  Original VRF 0
  65002
    202.103.1.1 from 202.103.1.1 (202.103.1.1)
      Origin IGP metric 0, localpref 100, valid, external, best
      Last update: Fri Jan  5 17:12:47 2024
```

6. 查看FGT-1的路由表中的BGP路由，可以看到FGT-1从FGT-2、Router学习到的路由均已被放入路由表，iBGP路由的distance为200，eBGP路由的distance为20。

```
FGT-1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 100.1.1.2 (recursive via to_FGT-2 tunnel 101.103.2.2), 00:34:19, [1/0]
B       10.10.3.0/24 [20/0] via 202.103.1.1 (recursive is directly connected, port3), 00:17:59, [1/0]
B       10.10.4.0/24 [20/0] via 202.103.1.1 (recursive is directly connected, port3), 00:17:59, [1/0]
B       10.10.5.0/24 [20/0] via 202.103.1.1 (recursive is directly connected, port3), 00:17:59, [1/0]
B       10.10.6.0/24 [20/0] via 202.103.1.1 (recursive is directly connected, port3), 00:17:59, [1/0]
```

7. FGT-1内网PC可以正常访问FGT-2和Router内网PC。

FGT-2

1. 在FGT-2上查看BGP邻居状态，可以看到和FGT-1建立了BGP邻居，并学习到路由（从FGT-1学到5条，其中1条为FGT-1发布，4条为Router发布）。

> **重要**
>
> 查看BGP邻居的详细信息，请使用`get router info bgp neighbors`。

```
FGT-2 # get router info bgp summary

VRF 0 BGP router identifier 101.103.2.2, local AS number 65001
BGP table version is 2
2 BGP AS-PATH entries
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
0 BGP community entries

Neighbor  V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.1.1.1 4      65001     172     154        1    0    0 00:39:35        5

Total number of neighbors 1
```

2. 在FGT-2上查看从BGP邻居收到的路由条目。

```
FGT-2 # get router info bgp neighbors 100.1.1.1 received-routes
VRF 0 BGP table version is 2, local router ID is 101.103.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.1.0/24     100.1.1.1                     100      0        0 i ←/→
*>i10.10.3.0/24     100.1.1.1                     100      0        0 65002 i ←/→
*>i10.10.4.0/24     100.1.1.1                     100      0        0 65002 i ←/→
*>i10.10.5.0/24     100.1.1.1                     100      0        0 65002 i ←/→
*>i10.10.6.0/24     100.1.1.1                     100      0        0 65002 i ←/→

Total number of prefixes 5
```

3. 在FGT-2上查看向邻居发布的路由条目。

```
FGT-2 # get router info bgp neighbors 100.1.1.1 advertised-routes
VRF 0 BGP table version is 2, local router ID is 101.103.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.2.0/24     100.1.1.2                     100  32768        0 i ←/→

Total number of prefixes 1
```

4. 在FGT-2上查看BGP路由数据库，可以看到iBGP路由前边会有i标记，包含本地发布的路由（weight为32768）。Router发布的路由经过FGT-1发送给FGT-2，变为iBGP路由。

```
FGT-2 # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 101.103.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.1.0/24     100.1.1.1       0             100      0        0 i ←/1>
*> 10.10.2.0/24     0.0.0.0                       100  32768        0 i ←/1>
*>i10.10.3.0/24     100.1.1.1       0             100      0        0 65002 i ←/1>
*>i10.10.4.0/24     100.1.1.1       0             100      0        0 65002 i ←/1>
*>i10.10.5.0/24     100.1.1.1       0             100      0        0 65002 i ←/1>
*>i10.10.6.0/24     100.1.1.1       0             100      0        0 65002 i ←/1>

Total number of prefixes 6
```

5. 查看指定的某个BGP路由详细信息可以在该命令后加相应网段。

```
FGT-2 # get router info bgp network 10.10.3.0
VRF 0 BGP routing table entry for 10.10.3.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  65002
    100.1.1.1 from 100.1.1.1 (101.103.1.2)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Last update: Fri Jan  5 17:12:50 2024
```

6. 查看FGT-2的路由表中的BGP路由，可以看到FGT-2从FGT-1学习到的路由均已被放入路由表，iBGP路由的distance为200。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FGT-2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 100.1.1.1 (recursive via to_FGT-1 tunnel 101.103.1.2), 00:43:14, [1/0]
B       10.10.3.0/24 [200/0] via 100.1.1.1 (recursive via to_FGT-1 tunnel 101.103.1.2), 00:24:36, [1/0]
B       10.10.4.0/24 [200/0] via 100.1.1.1 (recursive via to_FGT-1 tunnel 101.103.1.2), 00:24:36, [1/0]
B       10.10.5.0/24 [200/0] via 100.1.1.1 (recursive via to_FGT-1 tunnel 101.103.1.2), 00:24:36, [1/0]
B       10.10.6.0/24 [200/0] via 100.1.1.1 (recursive via to_FGT-1 tunnel 101.103.1.2), 00:24:36, [1/0]
```

7. FGT-2内网PC可以正常访问FGT-1和Router内网PC。

Router

1. 在Router上查看BGP邻居状态，可以看到和FGT-1建立了BGP邻居，并学习到路由（从FGT-1学到1条，为FGT-1发布的默认路由）。

> **重要**
>
> 查看BGP邻居的详细信息，请使用`get router info bgp neighbors`。

```bash
Router # get router info bgp summary

VRF 0 BGP router identifier 202.103.1.1, local AS number 65002
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.1.2 4      65001      86      95        1    0    0 00:27:29        1

Total number of neighbors 1
```

2. 在Router上查看从BGP邻居收到的路由条目。

```bash
Router # get router info bgp neighbors 202.103.1.2 received-routes
VRF 0 BGP table version is 1, local router ID is 202.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        202.103.1.2                             0        0 65001 i ←/→

Total number of prefixes 1
```

3. 在FGT-2上查看向邻居发布的路由条目。

```bash
Router # get router info bgp neighbors 202.103.1.2 advertised-routes
VRF 0 BGP table version is 1, local router ID is 202.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.3.0/24     202.103.1.1                       100  32768        0 i ←/→
*> 10.10.4.0/24     202.103.1.1                       100  32768        0 i ←/→
*> 10.10.5.0/24     202.103.1.1                       100  32768        0 i ←/→
*> 10.10.6.0/24     202.103.1.1                       100  32768        0 i ←/→

Total number of prefixes 4
```

4. 在Router上查看BGP路由数据库，可以看到除了本地发布的路由（weight为32768）和FGT-1发布的默认路由，无法学习到FGT-1和FGT-2发布的iBGP路由，这说明在FGT-1上配置的route-map已生效（过滤IGP路由）。

```bash
Router # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 202.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        202.103.1.2     0                       0        0 65001 i ←/1>
*> 10.10.3.0/24     0.0.0.0                           100  32768        0 i ←/1>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
*> 10.10.4.0/24     0.0.0.0                  100  32768        0 i <-/1>
*> 10.10.5.0/24     0.0.0.0                  100  32768        0 i <-/1>
*> 10.10.6.0/24     0.0.0.0                  100  32768        0 i <-/1>

Total number of prefixes 5
```

5. 查看指定的某个BGP路由详细信息可以在该命令后加相应网段。

```bash
Router # get router info bgp network 0.0.0.0
VRF 0 BGP routing table entry for 0.0.0.0/0
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  65001
    202.103.1.2 from 202.103.1.2 (101.103.1.2)
      Origin IGP metric 0, localpref 100, valid, external, best
      Last update: Fri Jan  5 17:12:51 2024
```

6. 查看Router的路由表中的BGP路由，只有一条默认路由指向FGT-1，distance为20（eBGP路由）。

```bash
Router # get router info routing-table bgp
Routing table for VRF=0
B*      0.0.0.0/0 [20/0] via 202.103.1.2 (recursive is directly connected, port2), 00:31:31, [1/0]
```

7. Router内网PC可以正常访问FGT-1和FGT-2内网PC。

BGP邻居建立排错

1. 检查FGT-1的WAN1接口与FGT-2的WAN接口之间的连通性。
2. 检查FGT-1和FGT-2之间的IPSec隧道是否建立成功，并验证IPSec隧道的连通性。
3. 检查BGP建立的状态：
   - Idle：本地FortiGate尚未与邻居启动BGP进程。这可能是因为eBGP对等方距离较远，但未启用multihop。
   - Connect：本地FortiGate已启动BGP进程，但尚未发起TCP连接，可能是由于不正确的路由导致无法发起协商。
   - Active：本地FortiGate已启动TCP连接，但没有收到对端的响应。
4. 如果BGP邻居间建立TCP连接存在问题，可以使用命令 `diagnose sniffer packet any 'tcp and port 179' 4` 来判断协商问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP计时器

基础计时器

keepalive-timer

- 设置FortiGate向已建立连接的对等体发送BGP保活消息的频率（0~65535s，默认值为60s）。
- `keepalive-timer` 是BGP的全局设置（`config router bgp`）。可以在每个对等体的配置上（`config neighbor` / `config neighbor-group`）使用 `keep-alive-timer` 选项覆盖全局配置。

holdtime-timer

- 设置BGP在将对等体标记为不可用之前等待的最长时间（3~65535s，默认值为180s）。当FortiGate收到来自对等体的keepalive消息时，`holdtime-timer` 会重置为配置的值。如果在此期间没有收到保活消息，FortiGate会认为对等体不再活跃，并将重置BGP邻居关系。
- `holdtime-timer` 是BGP的全局设置（`config router bgp`）。可以在每个对等体的配置上（`config neighbor` / `config neighbor-group`）使用 `holdtime-timer` 选项（名称相同）覆盖全局配置。

重要

- 可以在配置中将 `keepalive-timer` 设置为大于 `holdtime-timer` 的三分之一，但FortiOS实际使用的 `keepalive-timer` 最多会限制为 `holdtime-timer` 的三分之一（执行RFC 4271中的建议）。允许使用短于 `holdtime-timer` 三分之一的 `keepalive-timer` 。例如：
- 若 `keepalive-timer` = 20s且 `holdtime-timer` = 30s，FortiOS将使用10s的实际 `keepalive-timer` 和30s的 `holdtime-timer` 。
- 若 `keepalive-timer` = 5s且 `holdtime-timer` = 30s，FortiOS将使用5s的实际 `keepalive-timer` 和30s的 `holdtime-timer` 。
- BGP `keepalive-timer` / `holdtime-timer` 在对等体之间协商，双方会选择通告的最小保活/保持时间值。
- 更改BGP `keepalive-timer` 和 `holdtime-timer` 不会影响已建立的BGP邻居关系，除非它们被重置并重新建立，软重置（soft-reconfiguration）在此情况下无效。

advertisement-interval

- 设置BGP发送路由更新的最小间隔（0~600s，默认值为30s）。
- 受 `advertisement-interval` 影响的路由更新包括：BGP邻居状态变为ESTABLISHED后的初始路由通告、添加或撤销路由，以及软重置（soft-reconfiguration）后通告路由。
- 对等体之间的 `advertisement-interval` 值不需要协商。每个BGP对等体根据本地配置的 `advertisement-interval` 等待发送自己的路由通告。
- 建议为iBGP连接设置较短的间隔（如RFC 4271的第10节建议）。

connect-timer

- 设置BGP邻居状态在转换到idle状态之前，尝试通过TCP与BGP对等体尝试建立连接的最长时间（1~65535s，默认值为120s）。
- 此设置仅在每个对等体（`config neighbor` / `config neighbor-group`）上配置，没有全局设置。

scan-time

- 设置BGP扫描所有BGP路由下一跳可达性的间隔（5~60s，默认值为60s，设置为0表示禁用）。如果BGP路由条目的下一跳失效，则不使用该BGP路由条目。

路由抑制计时器

重要

- 必须先在 `config router bgp` 下设置 `set dampening enable`，这些路由抑制计时器才会出现在CLI中，且这些设置仅对BGP全局有效（不能在对等体的基础上配置）。
- 具体配置方法请参考：路由→动态路由→BGP→BGP常见问题→路由震荡↗章节。

dampening-max-suppress-time

- 设置路由可以被抑制的最长时间（1~255min，默认值为60min），无论路由的稳定性如何。
- 默认值为 `dampening-reachability-half-life` 的四倍。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

dampening-reachability-half-life

- 设置惩罚的半衰期时间（1~45min，默认值为15min）。如果路由被认为是可达的（无论是否被抑制），路由的惩罚将减少一半。

dampening-unreachability-half-life

- 设置惩罚的半衰期时间（1~45min，默认值为15min）。如果路由被认为是不可达的，路由的惩罚将减少一半。

平滑重启计时器

> **重要**
>
> 具体配置请参考：路由→动态路由→BGP→BGP GR ↗章节。

graceful-restart-time

- 设置BGP在对等体重启时等待的时间长度（1~3600s，默认值为120s）。一旦FortiGate在对等体重启后收到BGP OPEN消息，此计时器就会结束。请确保 `graceful-restart-time` 小于或等于 `holdtime-timer` 。
- `graceful-restart-time` 是BGP的全局设置（ `config router bgp` ）。可以在每个对等体的基础上（ `config neighbor` / `config neighbor-group` ）使用 `restart-time` 选项覆盖此设置。

graceful-stalepath-time

- 设置BGP保留之前从正在重启的BGP对等体接收的陈旧路由（stalepath）的时间（1~3600s，默认值为360s）。
- 一旦BGP检测到对等体重启（例如，收到带有Graceful Restart Capability字段，且“Restart State”置位的BGP Open报文），此计时器就会启动，允许BGP保留现有的陈旧路由（stalepath）足够长的时间，以保证BGP与正在重启的对等体重建过程中路由不会中断。
- `graceful-stalepath-time` 是BGP的全局设置（ `config router bgp` ）。可以在每个对等体的基础上（ `config neighbor` / `config neighbor-group` ）使用 `retain-stale-time` 选项覆盖此设置。

graceful-update-delay

- 设置BGP进程在重启后等待更新BGP路由选择的时间（1~3600s，默认值为120s）。
- 与前两个计时器不同，此计时器适用于FortiGate自身重启BGP的情况（而非对等体重启）。
- FortiGate将保留重启BGP前的陈旧路由（stalepath），并且在以下情况之前不会更新BGP路由选择：
  - 它从所有对等体（除了不支持GR的对等体以及“Restart State”置位的对等体）收到RIB结束的BGP标记。
  - 此计时器到期。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP GR

网络需求

FortiGate HA集群与上下游路由器运行BGP协议，并开启GR。在FortiGate的HA发生主备切换时，GR需要确保每个路由器（包括FortiGate及其它路由器）在HA切换期间保持其路由表中的BGP路由（GR Helper），以避免流量中断。

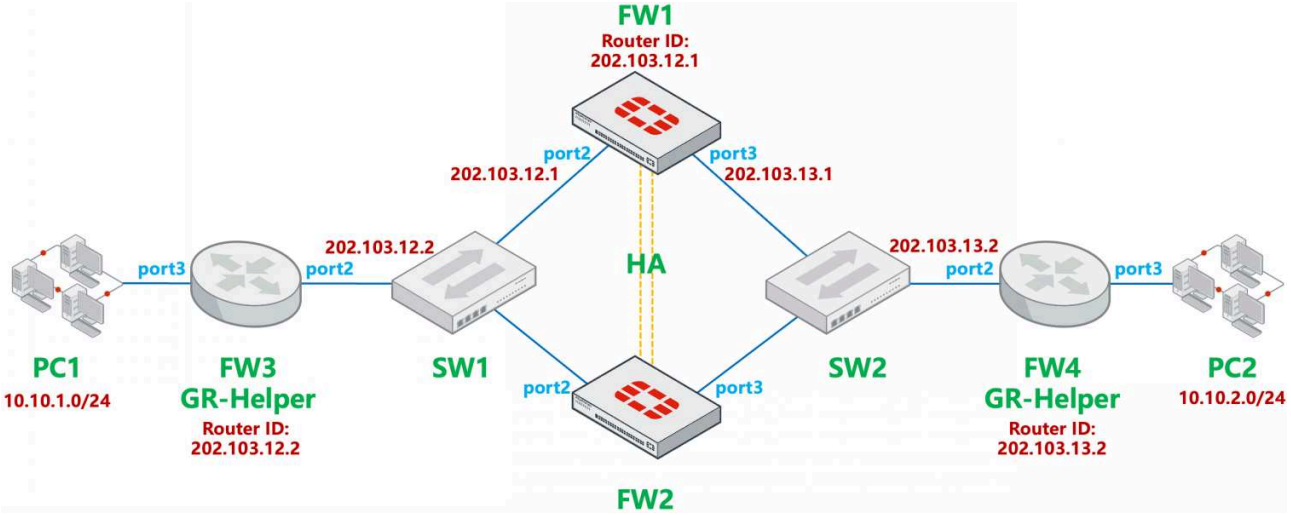
> **重要**
>
> 如果FortiGate的上下游为只支持GR Helper Only（只能作为GR Helper，不具有GR Restarter功能）模式的路由器，需要FortiGate运行FortiOS 7.4.2及以上版本才能正常完成GR过程。

在FortiGate HA集群中，BGP进程相关工作仅在主设备上运行。当发生HA切换时，将在新选举的主机上启动一个新的BGP协商过程，在此过程中，新的主机需要在路由Kernel表中维持从原主机学习到的BGP路由，直至新的BGP邻居形成。

对于BGP的GR，有以下几个计时器需要了解：

- `holdtime-timer`（默认180s）：将BGP邻居标记为死亡的秒数。即在考虑与对等方的连接关闭之前，在Keepalive、Update或Notification消息之间等待的秒数。
- `graceful-restart-time`（默认120s）：邻居重新启动所需的时间，即GR-Helper在删除过时路由之前等待OPEN消息的秒数。请确保`graceful-restart-time`小于或等于`holdtime-timer`。
- `graceful-update-delay`（默认120s）：GR完成后，路由宣告/学习的延迟时间。
- `graceful-stalepath-time`（默认360s）：在GR-Helper上保持GR邻居的过时路由的时间，即在删除之前保持过时路由的最大总时间。

网络拓扑



1. FW1与FW2建立A-P模式的HA。
2. FW1/FW2与FW3、FW4分别建立IBGP邻居，FW3、FW4宣告各自的网段。
3. FW1/FW2与FW3、FW4开启BGP Graceful Restart，FW1/FW2发生主备切换后，FW3、FW4可以进入GR Helper模式，协助FW1/FW2的GR过程。

配置步骤

1. 基础网络配置（略）。
2. FW1与FW2的HA配置（略）。
3. 安全策略配置（略）。
4. 配置FW1/FW2的BGP，开启GR功能，restart-period设置为600s，计时器配置均保持默认，邻居配置中开启路由反射器（RR），将两个IBGP邻居的路由互相反射，反射时将下一跳改为自己。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

- 虽然GR Restarter配置了`graceful-restart-time`，但该参数只是告知邻居（GR Helper）GR过程的最大时间。只要GR Restarter认为自己完成了GR（路由收敛完成），即使时间没有达到配置的`graceful-restart-time`，也会向GR Helper发送EoR（End-of-Rib）报文来告知邻居自身GR已完成，此时GR Helper会直接删除陈旧（Stale）路由。
- 这在某些ADVPN环境下下可能存在问题：例如Hub的BGP使用neighbor-group模式，且Hub与内网路由器还有BGP GR关系，当Hub发生HA切换后，由于Hub无法主动向Spoke发起BGP协商，在Spoke再次与Hub建立BGP并收敛前，Hub会认为GR已经完成并提前结束GR，从而导致内网路由器无法保持Spoke的相关路由。
- 如果想让GR Restarter只在`graceful-restart-time`到期时才向GR Helper发送EoR（End-of-Rib），则需要开启如下命令：

```
config router bgp
    set graceful-end-on-timer enable
end
```

bash

```
config router bgp
    set as 65001
    set router-id 202.103.12.1
    set graceful-restart enable
    set graceful-restart-time 120
    set graceful-stalepath-time 360
    set graceful-update-delay 120
    config neighbor
        edit "202.103.12.2"
            set capability-graceful-restart enable
            set next-hop-self-rr enable
            set soft-reconfiguration enable
            set remote-as 65001
            set route-reflector-client enable
        next
        edit "202.103.13.2"
            set capability-graceful-restart enable
            set next-hop-self-rr enable
            set soft-reconfiguration enable
            set remote-as 65001
            set route-reflector-client enable
        next
    end
end
```

bash

5. 配置FW3的BGP，宣告内网网络，路由器作为GR-Helper也需要开启GR功能，计时器配置均保持默认。

```
config router bgp
    set as 65001
    set router-id 202.103.12.2
    set graceful-restart enable
    config neighbor
        edit "202.103.12.1"
            set capability-graceful-restart enable
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```

bash

6. 配置FW4的BGP，宣告内网网络，路由器作为GR-Helper也需要开启GR功能，计时器配置均保持默认。

```
config router bgp
    set as 65001
    set router-id 202.103.13.2
    set graceful-restart enable
    config neighbor
        edit "202.103.13.1"
            set capability-graceful-restart enable
            set soft-reconfiguration enable
```

bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

7. 配置FW1/FW2 HA配置中的route-ttl为360s（默认10s），在此时间内，新的主机需要在路由Kernel表中维持从原主机学习到的BGP路由，直至新的BGP邻居形成，并完成BGP路由学习。

> **重要**
>
> 重要步骤，防止HA切换后，新主机建立新的BGP邻居前，路由消失导致业务中断。

```bash
config system ha
    set route-ttl 360
end
```

结果验证

1. 初始状态下，FW1为主设备，FW2为备设备。

```bash
FW1 # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:42869 b:39035389
        traffic.total = s:0 p:42867 b:39033889
        activity.ha_id_changes = 2
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=7 Debug=0
nvcluster=1, ses_pickup=0, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM23000175:      Primary, serialno_prio=1, usr_priority=128, hostname=FW1
FGVM08TM23000176:    Secondary, serialno_prio=0, usr_priority=100, hostname=FW2

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.2, primary_id=0
FGVM08TM23000175:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM23000176:    Secondary, ha_prio/o_ha_prio=1/1
```

2. 初始状态下查看FW3的BGP邻居状态与路由信息，邻居状态为已建立状态，BGP路由学习正常。

```bash
FW3 # get router info bgp summary

VRF 0 BGP router identifier 202.103.12.2, local AS number 65001
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.1 4      65001    1229    1229        2    0    0 16:55:54        1

Total number of neighbors 1

FW3 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 202.103.12.1 (recursive is directly connected, port2), 00:02:15, [1/0]
```

3. 初始状态下查看FW4的BGP邻居状态与路由信息，邻居状态为已建立状态，BGP路由学习正常。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW4 # get router info bgp summary

VRF 0 BGP router identifier 202.103.13.2, local AS number 65001
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.13.1 4      65001    1232    1233        2    0    0 17:01:22        1

Total number of neighbors 1

FW4 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 202.103.13.1 (recursive is directly connected, port2), 00:03:00, [1/0]
```

4. 初始状态下查看FW1的BGP邻居状态与路由信息，邻居状态为已建立，BGP路由学习正常。

```bash
FW1 # get router info bgp summary

VRF 0 BGP router identifier 202.103.12.1, local AS number 65001
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.2 4      65001    1232    1241        1    0    0 17:03:12        1
202.103.13.2 4      65001    1233    1238        1    0    0 17:03:11        1

Total number of neighbors 2

FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 202.103.12.2 (recursive is directly connected, port2), 17:02:56, [1/0]
B       10.10.2.0/24 [200/0] via 202.103.13.2 (recursive is directly connected, port3), 17:02:55, [1/0]
```

5. 使FW1和FW2发生HA主备倒换，此时FW2成为HA主设备。

```bash
FW2 # diagnose sys ha status
HA information
Statistics
        traffic.local = s:0 p:6233 b:4732229
        traffic.total = s:0 p:6286 b:4735596
        activity.ha_id_changes = 4
        activity.fdb  = c:0 q:0

Model=80008, Mode=2 Group=7 Debug=0
nvcluster=1, ses_pickup=0, delay=0

[Debug_Zone HA information]
HA group member information: is_manage_primary=1.
FGVM08TM23000176:      Primary, serialno_prio=0, usr_priority=100, hostname=FW2
FGVM08TM23000175:    Secondary, serialno_prio=1, usr_priority=128, hostname=FW1

[Kernel HA information]
vcluster 1, state=work, primary_ip=169.254.0.1, primary_id=0
FGVM08TM23000176:      Primary, ha_prio/o_ha_prio=0/0
FGVM08TM23000175:    Secondary, ha_prio/o_ha_prio=1/1
```

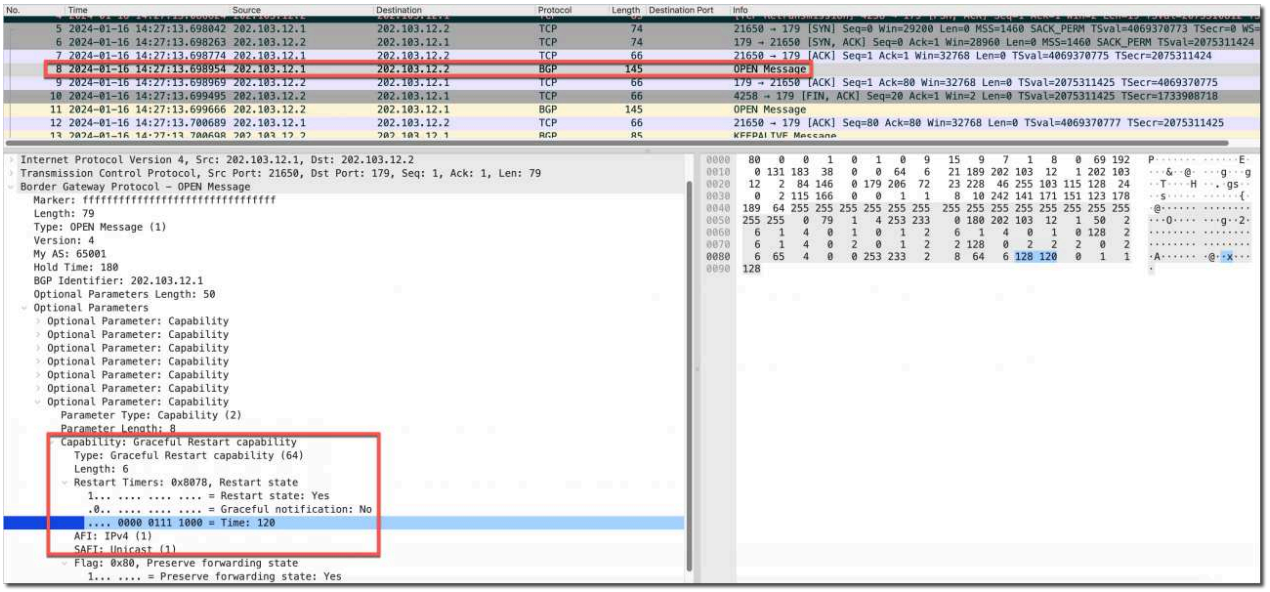
6. 查看FW2的BGP Debug信息，FW2成为HA主后，向BGP邻居发送BGP OPEN消息，其中包含Cap GR，Restarting时间为120s。

```bash
FW2 # diagnose ip router bgp level info
FW2 # diagnose ip router bgp all enable
FW2 # diagnose debug console time enable
......
2024-01-16 14:53:33 BGP: 202.103.12.2-Outgoing [ENCODE] Open: Ver 4 MyAS 65001 Holdtime 180
......
2024-01-16 14:53:33 BGP: 202.103.12.2-Outgoing [DECODE] Open Opt: Option Type 2, Option Len 8
2024-01-16 14:53:33 BGP: 202.103.12.2-Outgoing [DECODE] Open Cap: Cap Code 64, Cap Len 6
2024-01-16 14:53:33 BGP: 202.103.12.2-Outgoing [DECODE] Cap GR: Restart Flag Off, Restart Time 120
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
diagnose ip2024-01-16 14:53:33 BGP: 202.103.12.2-Outgoing [DECODE] Cap GR: AFI/SAFI 1/1 Fwd-state Flag 1, action:
Set
......
2024-01-16 14:53:34 2024-01-16 14:53:34 BGP: 202.103.12.2-Outgoing [GRST] GRST Init Announce:GRST Defer Announce
Timer(120) Started
id=20300 msg="BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 202.103.12.2 Up "
......
2024-01-16 14:53:59 BGP: 202.103.12.2-Outgoing [FSM] Update: IPv4 Unicast End-Of-Rib Marker Received
2024-01-16 14:53:59 BGP: 202.103.12.2-Outgoing [FSM] Process End-of-RIB: Received for afi/safi: 1/1
```

7. 该报文格式如下图所示。



8. 在FW2进入GR状态后，查看FW3的BGP邻居状态与BGP路由状态，FW3进入GR Helper状态，开始与FW2建立新的BGP邻居，之前已学习到的BGP路由未消失，被打上S（Stale）标记。（FW4也是一样的状态，这里就不再赘述）

```bash
FW3 # get router info bgp summary

VRF 0 BGP router identifier 202.103.12.2, local AS number 65001
BGP table version is 10
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.1 4      65001     101     104        0    0    0    never OpenConfirm

Total number of neighbors 1

FW3 # get router info bgp network
VRF 0 BGP table version is 7, local router ID is 202.103.12.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                           100  32768        0 i <-/1>
S>i10.10.2.0/24     202.103.12.1    0                 100      0        0 i <-/1>

Total number of prefixes 2

FW3 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 202.103.12.1 (recursive is directly connected, port2), 00:01:06, [1/0]
```

9. 在FW3上查看BGP的Debug信息，FW3与FW1的BGP连接断开后，进入GR Helper模式，GR倒计时120s。（FW4也是一样的状态，这里就不再赘述）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

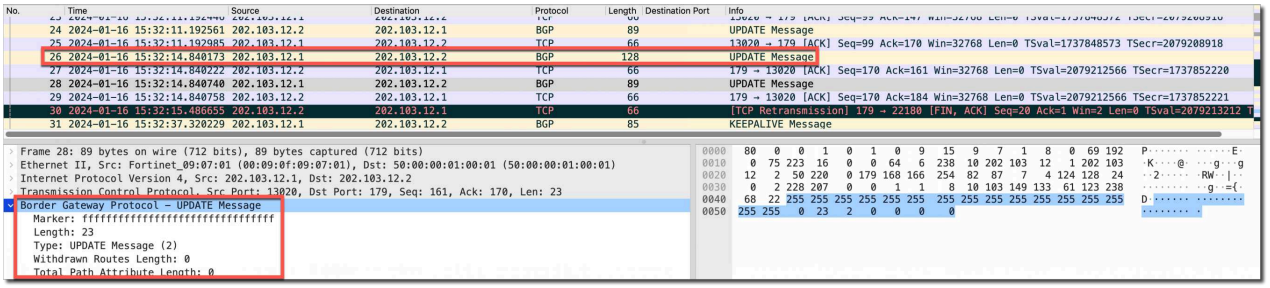
```bash
FW3 # diagnose ip router bgp level info
FW3 # diagnose ip router bgp all enable
FW3 # diagnose debug console time enable

2024-01-16 15:13:53 BGP: [NETWORK] Accept Thread: Incoming conn from host 202.103.12.1 (FD=26 VRF=0)
2024-01-16 15:13:53 BGP: 202.103.12.1-Outgoing [FSM] State: Established Event: 14
......
2024-01-16 15:14:22 BGP: 202.103.12.1-Outgoing [RIB] Update: Received Prefix 10.10.2.0/24 path_id 0
......
```

10. 等待FW2与FW3的BGP邻居建立完成后，FW2的GR完成，FW3退出GR Helper状态，期间被打上S标记的旧BGP路由没有消失，重新和FW2建立BGP邻居并学习BGP路由后，S标记变为*标记。（FW4也是一样的状态，这里就不再赘述）

```bash
FW3 # get router info bgp summary

VRF 0 BGP router identifier 202.103.12.2, local AS number 65001
BGP table version is 7
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.1 4      65001      79      81        0    0    0 00:00:05        1

FW3 # get router info bgp network
VRF 0 BGP table version is 12, local router ID is 202.103.12.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                           100  32768        0 i ←/1>
*>i10.10.2.0/24     202.103.12.1    0                 100      0        0 i ←/1>

Total number of prefixes 2

FW3 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 202.103.12.1 (recursive is directly connected, port2), 00:01:06, [1/0]
```

11. 在FW3上查看BGP的Debug信息，FW3从FW2完成了新的BGP路由学习后，向FW2发送了End-of-RIB报文，报文格式如下（空的BGP Update报文），通知其路由已经学习完成。

```bash
2024-01-16 15:14:22 BGP: VRF 0 NSM announce: 10.10.2.0/24
2024-01-16 15:14:22 BGP: 202.103.12.1-Outgoing [FSM] Update: IPv4 Unicast End-Of-Rib Marker Received
2024-01-16 15:14:22 BGP: 202.103.12.1-Outgoing [FSM] Process End-of-RIB: Received for afi/safi: 1/1
```



12. 在FW3上查看BGP邻居状态，其中包含GR相关信息，如邻居的GR时间为120s。

```bash
FW3 # get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 202.103.12.1, remote AS 65001, local AS 65001, internal link
  BGP version 4, remote router ID 202.103.12.1
  BGP state = Established, up for 00:04:58
  Last read 00:00:02, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
 ......
 For address family: IPv4 Unicast
  BGP table version 13, neighbor version 12
  Index 1, Offset 0, Mask 0x2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  AF-dependant capabilities:
    Graceful restart: advertised, received, negotiated
......
 Connections established 13; dropped 12
 Graceful-restart Status:
  Remote restart-time is 120 sec
......
```

3. GR期间，FW2从FW1重启前同步的路由一直存在（route-ttl 360，prio=2164260865）。

```bash
FW2 # get router info kernel | grep 10.10.
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.1.0/24 pref=0.0.0.0 gwy=202.103.12.2
dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.2.0/24 pref=0.0.0.0 gwy=202.103.13.2
dev=5(port3)
```

4. GR结束后，学到了新的BGP路由（prio=1）。

```bash
FW2 # get router info kernel | grep 10.10.
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.1.0/24 pref=0.0.0.0 gwy=202.103.12.2
dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.1.0/24 pref=0.0.0.0 gwy=202.103.12.2
dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.2.0/24 pref=0.0.0.0 gwy=202.103.13.2
dev=5(port3)
tab=254 vf=0 scope=0 type=1 proto=30 prio=2164260865 0.0.0.0/0.0.0.0/0→10.10.2.0/24 pref=0.0.0.0 gwy=202.103.13.2
dev=5(port3)
```

5. 整个HA切换引起的GR期间，所有设备路由转发表未发生实际变化，流量不会中断。

GR与BFD的使用关系

重要

BGP GR或OSPF GR不建议与BFD同时使用。

GR用于FortiGate通知邻居自己的路由进程将重启，并且邻居从FortiGate学到的路由应在重启期间保留。但BFD检测到故障时会将动态路由邻居重置。这种操作上的差异使得在GR的同时使用BFD会导致功能上的冲突，可能导致GR期间流量中断。

业界通用的做法是在使用GR时关闭BFD。例如在 FortiGate和GCP（Google 云平台）之间配置动态路由 + GR + BFD时：

- GCP将关闭BFD并发送AdminDown（BFD事件）到FortiGate（参考https://cloud.google.com/network-connectivity/docs/router/concepts/bfd#graceful-restart-and-bfd ↗）。
- FortiGate不会因为AdminDown类型的BFD通知重置BGP连接（参考https://handbook.fortinet.com.cn/routing/bfd/bfd_and_bgp.html#注意事项 ↗）。

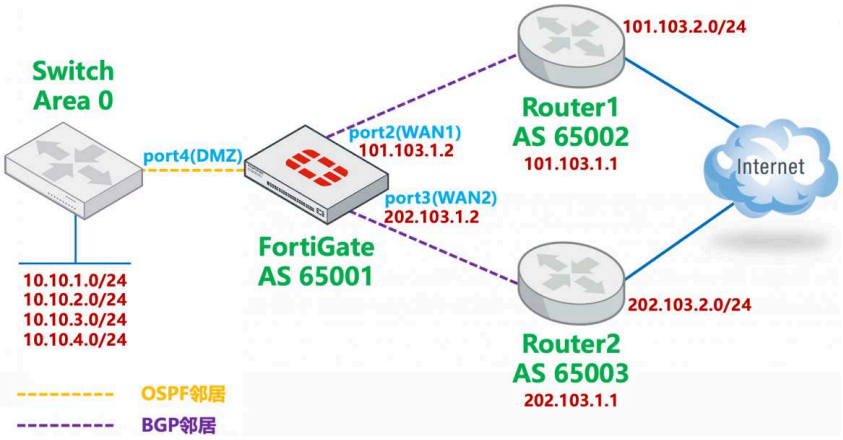
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP路由过滤

网络需求

在BGP路由中通过prefix-list + route-map实现路由过滤功能。

网络拓扑



1. OSPF邻居：

   - FortiGate与内网Switch建立OSPF邻居。
   - Switch发布内网网段路由，宣告给FortiGate。

2. BGP邻居：

   - FortiGate与Router1建立eBGP邻居。
   - FortiGate与Router2建立eBGP邻居。

3. 路由学习：

   - FortiGate将学习到的OSPF路由重发布到两个eBGP邻居。
   - FortiGate将从Router1和Router2学习到的BGP路由重发布到OSPF邻居。
   - Router1和Router2都向FortiGate发布默认路由。
   - FortiGate从Router1学习到的BGP路由不能发布给Router2。
   - FortiGate从Router1和Router2学习到的BGP默认路由不能发布给Router2和Router1。

配置步骤

基础配置

1. FortiGate的接口配置。

```bash
config system interface
    edit "port2"
        set vdom "root"
        set ip 101.103.1.2 255.255.255.0
        set allowaccess ping
        set alias "WAN1"
    next
    edit "port3"
        set vdom "root"
        set ip 202.103.1.2 255.255.255.0
        set allowaccess ping
        set alias "WAN2"
    next
    edit "port4"
        set vdom "root"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set ip 10.10.254.1 255.255.255.0
        set allowaccess ping
        set alias "DMZ"
    next
end
```

2. 配置安全策略，放通FortiGate、Switch、Router间的流量，按需配置其他安全策略（略）。

OSPF（FortiGate to Switch）

配置FortiGate的OSPF，将BGP路由重发布至OSPF。

```bash
config router ospf
    set router-id 10.10.254.1
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 10.10.254.0 255.255.255.0
        next
    end
    config redistribute "bgp"
        set status enable
    end
end
```

BGP（FortiGate to Router）

1. 在FortiGate上配置2个prefix-list：

   - 一个prefix-list匹配Router1宣告的BGP路由101.103.2.0/24，不设置ge和le（表示严格匹配），动作为permit（表示匹配）。
   - 另一个prefix-list匹配Router1和Router2宣告的默认路由，不设置ge和le（表示严格匹配），动作为permit（表示匹配）。

```bash
config router prefix-list
    edit "Block_101.103.2.0/24"
        config rule
            edit 1
                set prefix 101.103.2.0 255.255.255.0
                unset ge
                unset le
            next
        end
    next
    edit "Block_0.0.0.0/0"
        config rule
            edit 1
                set prefix 0.0.0.0 0.0.0.0
                unset ge
                unset le
            next
        end
    next
end
```

2. 在FortiGate上配置Route-map引用prefix-list，FortiGate从Router1学习到的BGP细化路由不能发布给Router2，FortiGate从Router1和Router2学习到的BGP默认路由不能发布给Router2和Router1，其他路由条目可以正常宣告。

   - 序号10：匹配条件为Router1宣告网段的prefix-list：Block_101.103.2.0/24，动作为deny（表示拒绝）。
   - 序号20：匹配条件为prefix-list：Block_0.0.0.0/0，动作为deny（表示拒绝）。
   - 序号100：匹配条件为any，即所有路由，动作为permit（表示允许）。

```bash
config router route-map
    edit "RMP_out"
        config rule
            edit 10
                set action deny
                set match-ip-address "Block_101.103.2.0/24"
            next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            edit 20
                set action deny
                set match-ip-address "Block_0.0.0.0/0"
            next
            edit 100
            next
        end
    next
end
```

3. 在FortiGate上配置BGP，在邻居Router1和Router2上分别使用route-map-out调用上步创建的route-map，重发布OSPF路由，开启ebgp-multipath。

```bash
config router bgp
    set as 65001
    set router-id 101.103.1.2
    set ebgp-multipath enable
    config neighbor
        edit "101.103.1.1"
            set soft-reconfiguration enable
            set route-map-out "RMP_out"
            set remote-as 65002
        next
        edit "202.103.1.1"
            set soft-reconfiguration enable
            set route-map-out "RMP_out"
            set remote-as 65003
        next
    end
    config redistribute "ospf"
        set status enable
    end
end
```

4. 在Router1（使用FortiGate模拟）上配置BGP，向FortiGate发布自身网段和默认路由。

```bash
config router bgp
    set as 65002
    set router-id 101.103.1.1
    config neighbor
        edit "101.103.1.2"
            set capability-default-originate enable
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 101.103.2.0 255.255.255.0
        next
    end
end
```

5. 在Router2（使用FortiGate模拟）上配置BGP，向FortiGate发布自身网段和默认路由。

```bash
config router bgp
    set as 65003
    set router-id 202.103.1.1
    config neighbor
        edit "202.103.1.2"
            set capability-default-originate enable
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        edit 1
            set prefix 202.103.2.0 255.255.255.0
        next
    end
end
```

结果验证

FortiGate

1. 在FortiGate上查看OSPF邻居状态与OSPF路由，可以看到和Switch建立了OSPF邻居，并学习到了Switch发布的4条OSPF路由。

```bash
FortiGate # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.254.2       1   Full/DR         00:00:36    10.10.254.2     port4

FortiGate # get router info routing-table ospf
Routing table for VRF=0
O       10.10.1.0/24 [110/2] via 10.10.254.2, port4, 01:23:49, [1/0]
O       10.10.2.0/24 [110/2] via 10.10.254.2, port4, 01:23:49, [1/0]
O       10.10.3.0/24 [110/2] via 10.10.254.2, port4, 01:23:49, [1/0]
O       10.10.4.0/24 [110/2] via 10.10.254.2, port4, 01:23:49, [1/0]
```

2. 在FortiGate上查看BGP邻居状态，可以看到和Router1、Router2分别建立了BGP邻居，并学习到路由。

> **重要**
>
> 查看BGP邻居的详细信息，请使用`get router info bgp neighbors`。

```bash
FortiGate # get router info bgp summary

VRF 0 BGP router identifier 101.103.1.2, local AS number 65001
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
101.103.1.1 4      65002     101     117        5    0    0 01:25:48        2
202.103.1.1 4      65003     106     115        5    0    0 01:17:25        2

Total number of neighbors 2
```

3. 在FortiGate上查看从邻居Router1和Router2收到的路由条目，可以看到收到了Router1/Router2发布的自身网段路由和默认路由。

```bash
FortiGate # get router info bgp neighbors 101.103.1.1 received-routes
VRF 0 BGP table version is 7, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        101.103.1.1                             0        0 65002 i ←/→
*> 101.103.2.0/24   101.103.1.1                             0        0 65002 i ←/→

Total number of prefixes 2

FortiGate # get router info bgp neighbors 202.103.1.1 received-routes
VRF 0 BGP table version is 7, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        202.103.1.1                             0        0 65003 i ←/→
*> 202.103.2.0      202.103.1.1                             0        0 65003 i ←/→

Total number of prefixes 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 在FortiGate上查看向邻居Router1、Router2发布的路由条目，可以看到route-map-out生效，没有将学习到的Router1的BGP路由发布给Router2（但将学习到的Router2的BGP路由发布给了Router1），没有发布从Router1、Router2学习到的默认路由，重发布了OSPF路由。

```bash
FortiGate # get router info bgp neighbors 101.103.1.1 advertised-routes
VRF 0 BGP table version is 7, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     101.103.1.2     2                  32768        0 ? ←/→
*> 10.10.2.0/24     101.103.1.2     2                  32768        0 ? ←/→
*> 10.10.3.0/24     101.103.1.2     2                  32768        0 ? ←/→
*> 10.10.4.0/24     101.103.1.2     2                  32768        0 ? ←/→
*> 202.103.2.0      101.103.1.2                            0        0 65003 i ←/→

Total number of prefixes 5

FortiGate # get router info bgp neighbors 202.103.1.1 advertised-routes
VRF 0 BGP table version is 7, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     202.103.1.2     2                  32768        0 ? ←/→
*> 10.10.2.0/24     202.103.1.2     2                  32768        0 ? ←/→
*> 10.10.3.0/24     202.103.1.2     2                  32768        0 ? ←/→
*> 10.10.4.0/24     202.103.1.2     2                  32768        0 ? ←/→

Total number of prefixes 4
```

5. 在FortiGate上查看BGP路由数据库，可以看到eBGP路由的路径（AS-Path）信息。

```bash
FortiGate # get router info bgp network
VRF 0 BGP table version is 7, local router ID is 101.103.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*  0.0.0.0/0        202.103.1.1     0                      0        0 65003 i ←/→
*>                  101.103.1.1     0                      0        0 65002 i ←/1>
*> 10.10.1.0/24     10.10.254.2     2                  32768        0 ? ←/1>
*> 10.10.2.0/24     10.10.254.2     2                  32768        0 ? ←/1>
*> 10.10.3.0/24     10.10.254.2     2                  32768        0 ? ←/1>
*> 10.10.4.0/24     10.10.254.2     2                  32768        0 ? ←/1>
*> 101.103.2.0/24   101.103.1.1     0                      0        0 65002 i ←/1>
*> 202.103.2.0      202.103.1.1     0                      0        0 65003 i ←/1>

Total number of prefixes 7
```

6. 查看指定的某个BGP路由详细信息可以在该命令后加相应网段。

```bash
FortiGate # get router info bgp network 0.0.0.0
VRF 0 BGP routing table entry for 0.0.0.0/0
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  65003
    202.103.1.1 from 202.103.1.1 (202.103.1.1)
      Origin IGP metric 0, localpref 100, valid, external
      Last update: Wed Jan 17 11:32:12 2024

  Original VRF 0
  65002
    101.103.1.1 from 101.103.1.1 (101.103.1.1)
      Origin IGP metric 0, localpref 100, valid, external, best
      Last update: Wed Jan 17 11:32:12 2024
```

7. 查看FortiGate的路由表中的BGP路由，由于开启了ebgp-multipath，从Router1和Router2学习到的默认路由在路由表中负载。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # get router info routing-table bgp
Routing table for VRF=0
B*      0.0.0.0/0 [20/0] via 101.103.1.1 (recursive is directly connected, port2), 01:50:31, [1/0]
                 [20/0] via 202.103.1.1 (recursive is directly connected, port3), 01:50:31, [1/0]
B       101.103.2.0/24 [20/0] via 101.103.1.1 (recursive is directly connected, port2), 00:09:04, [1/0]
B       202.103.2.0/24 [20/0] via 202.103.1.1 (recursive is directly connected, port3), 00:09:08, [1/0]
```

Router1

1. 在Router1上查看BGP邻居状态，可以看到和FortiGate建立了BGP邻居，并学习到路由。

> **重要**
>
> 查看BGP邻居的详细信息，请使用`get router info bgp neighbors`。

```bash
Router1 # get router info bgp summary

VRF 0 BGP router identifier 101.103.1.1, local AS number 65002
BGP table version is 3
3 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
101.103.1.2 4      65001     126     112        2    0    0 01:34:48        5

Total number of neighbors 1
```

2. 在Router1上查看从BGP邻居收到的路由条目，可以看到学习到了FortiGate重发布的OSPF路由，以及FortiGate从Router2学习到的BGP路由。

```bash
Router1 # get router info bgp neighbors 101.103.1.2 received-routes
VRF 0 BGP table version is 3, local router ID is 101.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     101.103.1.2     2                      0        0 65001 ? ←/→
*> 10.10.2.0/24     101.103.1.2     2                      0        0 65001 ? ←/→
*> 10.10.3.0/24     101.103.1.2     2                      0        0 65001 ? ←/→
*> 10.10.4.0/24     101.103.1.2     2                      0        0 65001 ? ←/→
*> 202.103.2.0      101.103.1.2                            0        0 65001 65003 i ←/→

Total number of prefixes 5
```

3. 在Router1上查看向邻居发布的路由条目，包含自身网段路由和默认路由。

```bash
Router1 # get router info bgp neighbors 101.103.1.2 advertised-routes
VRF 0 BGP table version is 3, local router ID is 101.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        101.103.1.1                    100  32768        0 i ←/→
*> 101.103.2.0/24   101.103.1.1                    100  32768        0 i ←/→

Total number of prefixes 2
```

4. 在Router1上查看BGP路由数据库，可以看到eBGP路由的路径（AS-Path）信息。

```bash
Router1 # get router info bgp network
VRF 0 BGP table version is 3, local router ID is 101.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     101.103.1.2     2                      0        0 65001 ? ←/1>
*> 10.10.2.0/24     101.103.1.2     2                      0        0 65001 ? ←/1>
*> 10.10.3.0/24     101.103.1.2     2                      0        0 65001 ? ←/1>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
*> 10.10.4.0/24     101.103.1.2     2                      0        0 65001 ? ←/1>
*> 101.103.2.0/24   0.0.0.0                       100  32768        0 i ←/1>
*> 202.103.2.0      101.103.1.2     0                      0        0 65001 65003 i ←/1>

Total number of prefixes 6
```

5. 查看指定的某个BGP路由详细信息可以在该命令后加相应网段。

```bash
Router1 # get router info bgp network 202.103.2.0
VRF 0 BGP routing table entry for 202.103.2.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  65001 65003
    101.103.1.2 from 101.103.1.2 (101.103.1.2)
      Origin IGP metric 0, localpref 100, valid, external, best
      Last update: Wed Jan 17 11:32:27 2024
```

6. 查看Router1的路由表中的BGP路由，可以看到Router1从FortiGate学习到的路由均已被放入路由表（包含FortiGate重发布的OSPF路由，以及FortiGate从Router2学习到的BGP路由），eBGP路由的distance为20。

```bash
Router1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [20/2] via 101.103.1.2 (recursive is directly connected, port2), 01:59:33, [1/0]
B       10.10.2.0/24 [20/2] via 101.103.1.2 (recursive is directly connected, port2), 01:59:33, [1/0]
B       10.10.3.0/24 [20/2] via 101.103.1.2 (recursive is directly connected, port2), 01:59:33, [1/0]
B       10.10.4.0/24 [20/2] via 101.103.1.2 (recursive is directly connected, port2), 01:59:33, [1/0]
B       202.103.2.0/24 [20/0] via 101.103.1.2 (recursive is directly connected, port2), 00:10:12, [1/0]
```

Router2

1. 在Router2上查看BGP邻居状态，可以看到和FortiGate建立了BGP邻居，并学习到路由。

> **重要**
>
> 查看BGP邻居的详细信息，请使用`get router info bgp neighbors`。

```bash
Router2 # get router info bgp summary

VRF 0 BGP router identifier 202.103.1.1, local AS number 65003
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.1.2 4      65001     156     147        3    0    0 01:52:16        4

Total number of neighbors 1
```

2. 在Router2上查看从BGP邻居收到的路由条目，可以看到学习到了FortiGate重发布的OSPF路由，没有FortiGate从Router1学习到的BGP路由。

```bash
Router2 # get router info bgp neighbors 202.103.1.2 received-routes
VRF 0 BGP table version is 4, local router ID is 202.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     202.103.1.2     2                      0        0 65001 ? ←/→
*> 10.10.2.0/24     202.103.1.2     2                      0        0 65001 ? ←/→
*> 10.10.3.0/24     202.103.1.2     2                      0        0 65001 ? ←/→
*> 10.10.4.0/24     202.103.1.2     2                      0        0 65001 ? ←/→

Total number of prefixes 4
```

3. 在Router2上查看向邻居发布的路由条目，包含自身网段路由和默认路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
Router2 # get router info bgp neighbors 202.103.1.2 advertised-routes
VRF 0 BGP table version is 4, local router ID is 202.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 0.0.0.0/0        202.103.1.1                    100  32768        0 i ←/→
*> 202.103.2.0      202.103.1.1                    100  32768        0 i ←/→

Total number of prefixes 2
```

4. 在Router2上查看BGP路由数据库，可以看到eBGP路由的路径（AS-Path）信息。

```bash
Router2 # get router info bgp network
VRF 0 BGP table version is 4, local router ID is 202.103.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     202.103.1.2     2                      0        0 65001 ? ←/1>
*> 10.10.2.0/24     202.103.1.2     2                      0        0 65001 ? ←/1>
*> 10.10.3.0/24     202.103.1.2     2                      0        0 65001 ? ←/1>
*> 10.10.4.0/24     202.103.1.2     2                      0        0 65001 ? ←/1>
*> 202.103.2.0      0.0.0.0                        100  32768        0 i ←/1>

Total number of prefixes 5
```

5. 查看指定的某个BGP路由详细信息可以在该命令后加相应网段。

```bash
Router2 # get router info bgp network 10.10.1.0
VRF 0 BGP routing table entry for 10.10.1.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  65001
    202.103.1.2 from 202.103.1.2 (101.103.1.2)
      Origin incomplete metric 2, localpref 100, valid, external, best
      Last update: Wed Jan 17 11:32:27 2024
```

6. 查看Router2的路由表中的BGP路由，包含FortiGate重发布的OSPF路由，没有FortiGate从Router1学习到的路由，distance为20（eBGP路由）。

```bash
Router2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [20/2] via 202.103.1.2 (recursive is directly connected, port2), 01:43:33, [1/0]
B       10.10.2.0/24 [20/2] via 202.103.1.2 (recursive is directly connected, port2), 01:43:33, [1/0]
B       10.10.3.0/24 [20/2] via 202.103.1.2 (recursive is directly connected, port2), 01:43:33, [1/0]
B       10.10.4.0/24 [20/2] via 202.103.1.2 (recursive is directly connected, port2), 01:43:33, [1/0]
```

Switch

在Switch上查看路由表，可以看到Switch学习到了FortiGate在OSPF中重发布的BGP路由。

```bash
Switch # get router info routing-table ospf
Routing table for VRF=0
O E2    101.103.2.0/24 [110/10] via 10.10.254.1, port2, 00:11:32, [1/0]
O E2    202.103.2.0/24 [110/10] via 10.10.254.1, port2, 00:11:36, [1/0]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP路由刷新

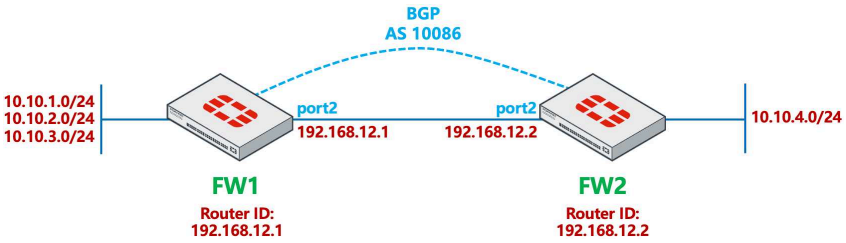
功能介绍

默认的BGP配置下，当BGP邻居配置中引用的路由策略（如route-map、distribute-list等）修改了属性或过滤的路由条目时，BGP路由表并不会立即更新，需要执行路由刷新来重新获取BGP路由，并进行路由过滤/修改。

FortiGate路由刷新的方法有以下3种：

- 方法1-使用BGP route-refresh
- 方法2-使用soft-reconfiguration
- 方法3-重置BGP邻居

网络拓扑



1. FW1与FW2建立iBGP邻居。
2. 初始状态下，FW1发布自己的路由10.10.1.0/24、10.10.2.0/24、10.10.3.0/24给FW2，FW1与FW2都不开启`soft-reconfiguration`功能。
3. 初始状态下，FW2的BGP入方向引用route-map，只允许学习FW1发送的路由10.10.1.0/24、10.10.2.0/24。

配置步骤

1. 基础网络配置（略）。

2. 配置FW1的BGP，与FW2建立iBGP邻居，并发布自己的路由10.10.1.0/24、10.10.2.0/24、10.10.3.0/24给FW2。

```bash
config router bgp
    set as 10086
    set router-id 192.168.12.1
    config neighbor
        edit "192.168.12.2"
            set remote-as 10086
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
        edit 2
            set prefix 10.10.2.0 255.255.255.0
        next
        edit 3
            set prefix 10.10.3.0 255.255.255.0
    end
end
```

3. 在FW2上配置prefix-list，内容为FW1的发布的BGP路由10.10.1.0/24、10.10.2.0/24。

```bash
config router prefix-list
    edit "Prefix_FW1"
        config rule
            edit 1
                set prefix 10.10.1.0 255.255.255.0
                unset ge
                unset le
            next
            edit 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set prefix 10.10.2.0 255.255.255.0
                unset ge
                unset le
            next
        end
    next
end
```

4. 在FW2上配置route-map，允许Prefix `Prefix_FW1` 中的BGP路由，拒绝其他路由。

```bash
config router route-map
    edit "RMP_from_FW1"
        config rule
            edit 1
                set match-ip-address "Prefix_FW1"
            next
            edit 2
                set action deny
            next
        end
    next
end
```

5. 在FW2上配置BGP，与FW2建立iBGP邻居，并发布自己的路由10.10.4.0/24给FW2。在入方向引用步骤4配置的route-map，只允许接收FW1发布的BGP路由10.10.1.0/24、10.10.2.0/24。

```bash
config router bgp
    set as 10086
    set router-id 192.168.12.2
    config neighbor
        edit "192.168.12.1"
            set remote-as 10086
            set route-map-in "RMP_from_FW1"
        next
    end
    config network
        edit 1
            set prefix 10.10.4.0 255.255.255.0
        next
    end
end
```

6. 在FW1上查看BGP路由学习情况，可以正确学习到FW2宣告的路由10.10.4.0/24。

```bash
FW1 # get router info bgp summary

VRF 0 BGP router identifier 192.168.12.1, local AS number 10086
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2 4      10086      22      23        1    0    0 00:17:28        1
Total number of neighbors 1

FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.4.0/24 [200/0] via 192.168.12.2 (recursive is directly connected, port2), 00:17:13, [1/0]
```

7. 在FW1上查看通告给FW2的BGP路由，与配置一致。

```bash
FW1 # get router info bgp neighbors 192.168.12.2 advertised-routes
VRF 0 BGP table version is 6, local router ID is 192.168.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
*>i10.10.1.0/24     192.168.12.1                100  32768        0 i ←/→
*>i10.10.2.0/24     192.168.12.1                100  32768        0 i ←/→
*>i10.10.3.0/24     192.168.12.1                100  32768        0 i ←/→

Total number of prefixes 3
```

8. 在FW2上查看BGP路由学习情况，可以正确学习到FW1发布的BGP路由10.10.1.0/24、10.10.2.0/24，而10.10.3.0/24被route-map过滤掉。

```bash
FW2 # get router info bgp summary

VRF 0 BGP router identifier 192.168.12.2, local AS number 10086
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1 4      10086       3       4        1    0    0 00:00:30        2
Total number of neighbors 1

FW2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:00:07, [1/0]
B       10.10.2.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:00:07, [1/0]
```

9. 在FW2的route-map引用的prefix中增加10.10.3.0/24的路由，这样route-map就开始允许接收10.10.3.0/24的BGP路由。

```bash
config router prefix-list
    edit "Prefix_FW1"
        config rule
            edit 3
                set prefix 10.10.3.0 255.255.255.0
                unset ge
                unset le
            next
        end
    next
end
```

0. 在FW2上查看学习到的BGP路由，仍然只有之前学习到的BGP路由10.10.1.0/24、10.10.2.0/24，没有FW1发布的10.10.3.0/24路由。

```bash
FW2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 02:37:10, [1/0]
B       10.10.2.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 02:37:10, [1/0]
```

1. 如果没有任何操作，路由将一直不会更新。可以使用如下3种方法进行路由刷新。

路由刷新方法

方法1-使用BGP route-refresh

1. 在FW2上查看在内存中保存的从FW1收到的BGP路由，由于没有开启软重配（soft-reconfiguration）功能，内存中不会保存从FW1收到的所有路由。

```bash
FW2 # get router info bgp neighbors 192.168.12.1 received-routes
% Inbound soft reconfiguration not enabled
% No prefix for neighbor 192.168.12.1
```

2. 确保FW1和FW2的BGP邻居配置中都开启了`capability-route-refresh`功能（默认开启）。

> **重要**
>
> `capability-route-refresh`用于手动路由刷新时向邻居发送route-refresh请求。
>
> 该功能符合RFC 2918，如果BGP邻居设备不是FortiGate，需要也支持RFC 2918才行。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config router bgp
        edit "192.168.12.1"
            set capability-route-refresh enable
        next
    end
end
```

3. 在FW2上使用`execute router clear bgp ip 192.168.12.1 in`命令进行BGP邻居路由入方向的刷新，向FW1请求BGP Update，并重新匹配route-map接收路由。等待若干秒后，再次查看FW2的BGP路由表，可以看到10.10.3.0/24已经入表。

> **重要**
>
> 如果BGP邻居配置中没有开启`soft-reconfiguration`，使用`execute router clear bgp ip 192.168.12.1 soft in`，将会与此步命令（`execute router clear bgp ip 192.168.12.1 in`）执行相同的操作。

```
FW2 # execute router clear bgp ip 192.168.12.1 in

FW2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 03:08:47, [1/0]
B       10.10.2.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 03:08:47, [1/0]
B       10.10.3.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:10:43, [1/0]
```

4. FW2上的BGP Debug信息，显示FW2向FW1发送了NLRI（Route-Refresh）的更新请求（RFC 2918），收到FW1的BGP Update后，从中取出10.10.1.0/24、10.10.2.0/24、10.10.3.0/24路由条目，10.10.3.0/24被放入路由表，10.10.1.0/24和10.10.2.0/24由于路由表中已存在而忽略。

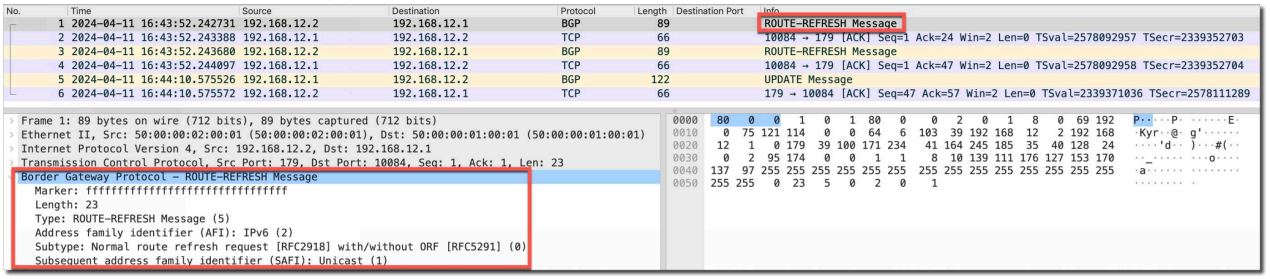
```
FW2 # diagnose ip router bgp level info
FW2 # diagnose ip router bgp all enable
FW2 # diagnose debug console time enable
FW2 # diagnose debug enable

2024-04-11 14:46:27 BGP: 192.168.12.1-Outgoing [ENCODE] Route-Refresh: RR-Type New MsgSize 23
2024-04-11 14:46:27 BGP: 192.168.12.1-Outgoing [ENCODE] Msg-Hdr: Type 5
2024-04-11 14:46:27 BGP: 192.168.12.1-Outgoing [ENCODE] Route-Refresh: RR-Type New MsgSize 23
2024-04-11 14:46:27 BGP: 192.168.12.1-Outgoing [ENCODE] Msg-Hdr: Type 5
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Bytes To Read (37),
msg_size (37)
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [DECODE] Update: NLRI Len(12)
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [FSM] State: Established Event: 27
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [RIB] Update: Received Prefix 10.10.1.0/24 path_id 0
2024-04-11 14:46:33 BGP: [DAMP] bgp_rfd_rt_update(): Route State: NONE, ret=0
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [RIB] Update: ...duplicate route ignored
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [RIB] Update: Received Prefix 10.10.3.0/24 path_id 0
2024-04-11 14:46:33 BGP: VRF 0 NSM announce: 10.10.3.0/24
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [RIB] Update: Received Prefix 10.10.2.0/24 path_id 0
2024-04-11 14:46:33 BGP: [DAMP] bgp_rfd_rt_update(): Route State: NONE, ret=0
2024-04-11 14:46:33 BGP: 192.168.12.1-Outgoing [RIB] Update: ...duplicate route ignored
```

5. FW1上的BGP Debug信息，显示FW1收到了FW2的BGP NLRI更新请求（Route-Refresh），并向FW2发送了BGP Update。

```
FW1 # diagnose ip router bgp level info
FW1 # diagnose ip router bgp all enable
FW1 # diagnose debug console time enable
FW1 # diagnose debug enable

2024-04-11 14:46:27 BGP: 192.168.12.2-Outgoing [FSM] State: Established Event: 29
2024-04-11 14:46:27 BGP: 192.168.12.2-Outgoing [DECODE] Msg-Hdr: type 5, length 23
2024-04-11 14:46:27 BGP: 192.168.12.2-Outgoing [DECODE] R-Refresh: AFI/SAFI (1/1)
2024-04-11 14:46:27 BGP: 192.168.12.2-Outgoing [DECODE] PEER_STATUS_ORF_NOT_WAIT_REFRESH set!

2024-04-11 14:46:33 BGP: 192.168.12.2-Outgoing [ENCODE] Msg-Hdr: Type 2
2024-04-11 14:46:33 BGP: 192.168.12.2-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 21
2024-04-11 14:46:33 BGP: 192.168.12.2-Outgoing [ENCODE] Update: Msg #9 Size 56
```

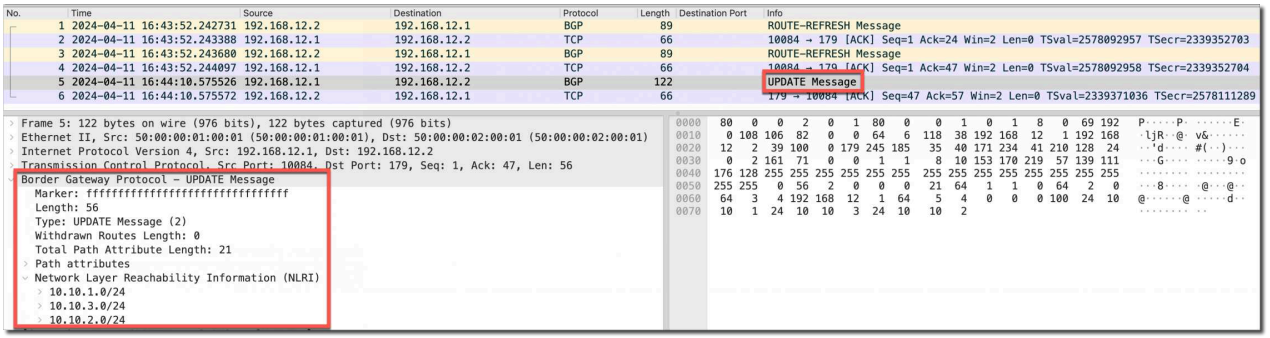
6. FW2发出的BGP Route-Rfresh请求报文的格式如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. FW1返回的BGP Update报文如下，包含自己宣告的3条路由，抓包文件请参考bgp_route_refresh.pcap ↗。

> **重要**
>
> 由于未开启 `soft-reconfiguration` ，邻居发布的全量路由不会保存在内存表中。所以使用 `capability-route-refresh` 功能请求对端更新路由，并不会马上得到对端的更新响应，会由对端配置的 `advertisement-interval` （FortiGate默认30s）决定。



8. FW2上查看BGP capability-route-refresh功能的开启状态，如下所示，在BGP邻居配置中开启capability-route-refresh的状态下，FW2即有Route refresh的通告功能，也有Route refresh的接受功能。

```bash
FW2 # get router info bgp neighbors 192.168.12.1 | grep refresh
    Route refresh: advertised and received (old and new)
  Route refresh request: received 0, sent 0
```

9. 期间相关BGP邻居不会中断，路由表中原有的BGP路由没有消失。

方法2-使用soft-reconfiguration

1. 在FW2上的BGP中开启 `soft-reconfiguration` 功能（对于BGP IPv6路由，该功能为 `soft-reconfiguration6` ）。

```bash
config router bgp
    config neighbor
        edit "192.168.12.1"
            set soft-reconfiguration enable
        next
    end
end
```

2. 在FW2上查看在内存中保存的从FW1收到的BGP路由，由于开启了软重配（soft-reconfiguration）功能，内存中会保存从FW1收到的所有BGP路由（被route-map过滤前的路由）。

```bash
FW2 # get router info bgp neighbors 192.168.12.1 received-routes
VRF 0 BGP table version is 2, local router ID is 192.168.12.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.1.0/24     192.168.12.1                    100      0         0 i ←/→
*>i10.10.2.0/24     192.168.12.1                    100      0         0 i ←/→
*>i10.10.3.0/24     192.168.12.1                    100      0         0 i ←/→

Total number of prefixes 3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在FW2上使用`execute router clear bgp ip 192.168.12.1 soft in`命令进行BGP邻居路由入方向的刷新，不需要向FW1请求BGP Update，直接从内存中保存的BGP路由遍历，并重新匹配route-map接收路由。再次查看FW2的BGP路由表，可以看到10.10.3.0/24直接入表（不需要像“方法1-使用BGP route-refresh”等待若干秒）。

```bash
FW2 # execute router clear bgp ip 192.168.12.1 soft in

FW2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:08:26, [1/0]
B       10.10.2.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:08:26, [1/0]
B       10.10.3.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:03:02, [1/0]
```

4. FW2上的BGP Debug信息，显示BGP从内存中读取从FW1收到的所有BGP路由，从中取出10.10.1.0/24、10.10.2.0/24、10.10.3.0/24路由条目，10.10.3.0/24被放入路由表，10.10.1.0/24和10.10.2.0/24由于路由表中已存在而忽略。

> **重要**
>
> 不需要向FW1发送BGP Route-Refresh请求报文。

```bash
FW2 # diagnose ip router bgp level info
FW2 # diagnose ip router bgp all enable
FW2 # diagnose debug console time enable
FW2 # diagnose debug enable

2024-04-11 17:22:54 BGP: [RIB] Scanning BGP RIB for VRF 0...
2024-04-11 17:22:54 BGP: [NSM] Verified NH 192.168.12.1 with NSM
2024-04-11 17:22:58 BGP: 192.168.12.1-Outgoing [RIB] Update: Received Prefix 10.10.1.0/24 path_id 0
2024-04-11 17:22:58 BGP: [DAMP] bgp_rfd_rt_update(): Route State: NONE, ret=0
2024-04-11 17:22:58 BGP: 192.168.12.1-Outgoing [RIB] Update: ...duplicate route ignored
2024-04-11 17:22:58 BGP: 192.168.12.1-Outgoing [RIB] Update: Received Prefix 10.10.2.0/24 path_id 0
2024-04-11 17:22:58 BGP: [DAMP] bgp_rfd_rt_update(): Route State: NONE, ret=0
2024-04-11 17:22:58 BGP: 192.168.12.1-Outgoing [RIB] Update: ...duplicate route ignored
2024-04-11 17:22:58 BGP: 192.168.12.1-Outgoing [RIB] Update: Received Prefix 10.10.3.0/24 path_id 0
2024-04-11 17:22:58 BGP: VRF 0 NSM announce: 10.10.3.0/24
```

5. 期间相关BGP邻居不会中断，路由表中原有的BGP路由没有消失。

方法3-重置BGP邻居

1. 在FW2上使用`execute router clear bgp ip 192.168.12.1`命令进行BGP邻居重置，重新建立与FW1的BGP邻居并学习BGP路由。

> **重要**
>
> 不推荐使用此方法，BGP邻居需要重新建立，流量中断时间长。
>
> 使用execute router clear bgp all可以重置所有的BGP邻居，请谨慎使用。

```bash
FW2 # execute router clear bgp ip 192.168.12.1
```

2. 随后FW2与FW1的BGP邻居被重置，并重新建立BGP邻居。

```bash
FW2 # get router info bgp summary

VRF 0 BGP router identifier 192.168.12.2, local AS number 10086
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1 4      10086      17      20        0    0    0    never Idle
Total number of neighbors 1
```

3. 等待BGP邻居建立完成并重新学习BGP路由后，10.10.3.0/24被放入路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW2 # get router info bgp summary

VRF 0 BGP router identifier 192.168.12.2, local AS number 10086
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.1 4      10086      30      33        2    0    0 00:09:03        3
Total number of neighbors 1

FW2 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:08:45, [1/0]
B       10.10.2.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:08:45, [1/0]
B       10.10.3.0/24 [200/0] via 192.168.12.1 (recursive is directly connected, port2), 00:08:45, [1/0]
```

4. FW2上的BGP Debug信息，显示FW2主动重置了BGP邻居，并通知了FW1。

> **重要**
>
> 不需要向FW1发送BGP Route-Refresh请求报文。

```bash
FW2 # diagnose ip router bgp level info
FW2 # diagnose ip router bgp all enable
FW2 # diagnose debug console time enable
FW2 # diagnose debug enable

2024-04-11 17:28:23 id=20300 msg="BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 192.168.12.1 Down BGP Notification CEASE"
2024-04-11 17:28:23 id=20300 msg="BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 192.168.12.1 Down User reset"
```

5. 期间相关BGP中断，路由表中原有的BGP路由消失。

总结

1. 三种刷新路由的方法优缺点总结：
   - 方法1-使用BGP route-refresh：
     - 优点：BGP邻居和已有路由不会中断，相比方法2，不需要在本地内存中保存未经路由策略过滤/修改的路由，节省内存。
     - 缺点：需要BGP邻居设备厂商支持RFC 2918（FortiGate支持）；根据对端配置的`advertisement-interval`，收到更新报文存在一定延迟。
     - 配合`exe router clear bgp ip 192.168.12.2 in`使用。
   - 方法2-使用soft-reconfiguration**（推荐）**：
     - 优点：BGP邻居和已有路由不会中断，不需要向BGP邻居发送Refresh-Route请求，仅本地执行。
     - 缺点：针对每个已建立的BGP邻居需要在内存中保存一份未经路由策略过滤/修改的路由列表，内存消耗较方法1稍大。
     - 配合`exe router clear bgp ip 192.168.12.2 soft in`使用。
   - 方法3-重置BGP邻居：
     - 优点：不需要BGP邻居设备的任何RFC支持，所有厂商原生支持。
     - 缺点：BGP邻居会重新建立并通告路由，流量中断时间长。
     - 配合`exe router clear bgp ip 192.168.12.2 all`或`exe router clear bgp all`使用。
2. FortiGate不支持路由过滤/修改条件更改后的BGP路由条目自动更新，必须使用上述三种方法手动刷新路由。
3. 对于out方向的路由策略（路由过滤/修改），使用`exe router clear bgp ip 192.168.12.2 out`和`exe router clear bgp ip 192.168.12.2 soft out`都可以触发out方向的路由更新，从而向邻居发送BGP Update更新报文，本文就不再赘述。

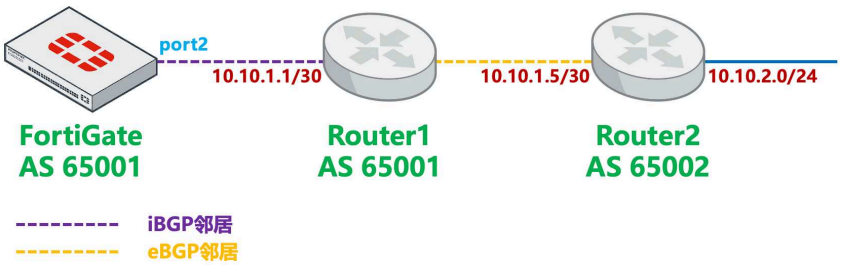
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP下一跳递归

网络需求

默认情况下，当BGP路由的下一跳需要递归解析时，不会被考虑通过其他BGP路由进行递归。启recursive-next-hop后，才通过其他BGP路由进行递归。

网络拓扑



1. FortiGate想要学习Router2的网段10.10.2.0/24。
2. FortiGate从Router1学习到了Router2的网段10.10.2.0/24，下一跳为10.10.1.5。
3. FortiGate从Router1学习到了10.10.1.4/30的路由，下一跳为10.10.1.1。

配置步骤

1. 配置基础网络（略）。

2. 配置FortiGate的BGP，与Router1建立iBGP邻居。

```bash
config router bgp
    set as 65001
    set router-id 10.10.1.2
    config neighbor
        edit "10.10.1.1"
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
end
```

3. 配置Router1的BGP，与FortiGate建立iBGP邻居，与Router2建立eBGP邻居，发布网段10.10.1.4/30。

```bash
config router bgp
    set as 65001
    set router-id 10.10.1.1
    config neighbor
        edit "10.10.1.2"
            set soft-reconfiguration enable
            set remote-as 65001
        next
        edit "10.10.1.5"
            set soft-reconfiguration enable
            set remote-as 65002
        next
    end
    config network
        edit 1
            set prefix 10.10.1.4 255.255.255.252
        next
    end
end
```

4. 配置Router2的BGP，与Router1建立eBGP邻居，发布网段10.10.2.0/24。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config router bgp
    set as 65002
    set router-id 10.10.1.5
    config neighbor
        edit "10.10.1.6"
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

结果验证

1. FortiGate从Router1学习到了两条BGP路由：

- Router2发布的路由，下一跳为Router2的接口IP。
- Router1发布的路由，下一跳为Router1的接口IP。

```bash
FortiGate # get router info bgp network
VRF 0 BGP table version is 1, local router ID is 10.10.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*>i10.10.1.4/30     10.10.1.1       0             100      0        0 i ←/1>
*>i10.10.2.0/24     10.10.1.5       0             100      0        0 65002 i ←/1>

Total number of prefixes 2
```

2. 但是Router2发布的路由未被FortiGate放入路由表，因为默认配置下，其下一跳10.10.1.5是无法通过BGP路由递归的。

```bash
FortiGate # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.4/30 [200/0] via 10.10.1.1 (recursive is directly connected, port2), 00:06:20, [1/0]
```

3. 在FortiGate上开启BGP的recursive-next-hop。

```bash
config router bgp
    set recursive-next-hop enable
end
```

4. 再次查看FortiGate的路由表中的BGP路由，Router2发布的路由被放入路由表，下一跳通过Router1发布的BGP路由递归。

```bash
FortiGate # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.4/30 [200/0] via 10.10.1.1 (recursive is directly connected, port2), 00:08:35, [1/0]
B       10.10.2.0/24 [200/0] via 10.10.1.5 (recursive via 10.10.1.1, port2), 00:00:02, [1/0]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

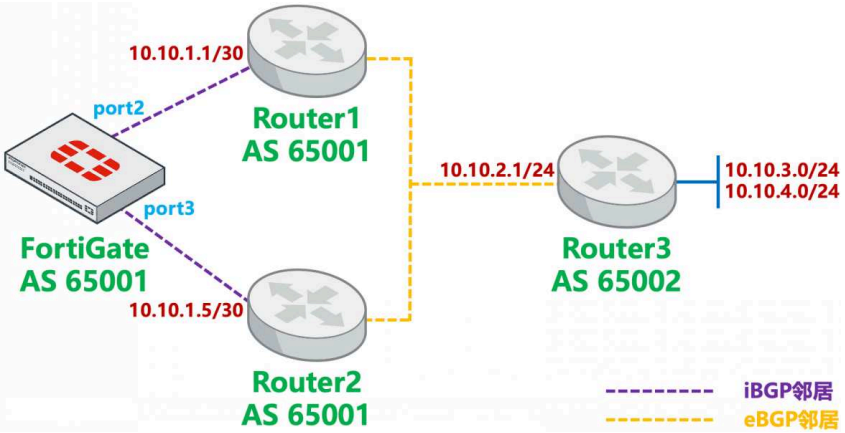
BGP多路径

网络需求

当存在多条ECMP（Equal-Cost Multipath）的BGP路由到达目标网络时，默认情况下只有第1个路由（先学习到的）会被放入路由表。

当开启BGP multipath功能后，所有这些ECMP的BGP路由都会被放入路由表，实现出站流量的负载均衡。允许同时使用多条等效路径，以提高网络性能和容错性。

网络拓扑



1. FortiGate与Router1和Router2分别建立iBGP邻居，FortiGate宣告自己的内网网段。
2. Router1和Router2分别与Router3建立eBGP邻居，Router3宣告自己的内网网段。

配置步骤

1. 基础网络配置（略）。

2. 配置FortiGate的BGP，与Router1和Router2分别建立iBGP邻居。

```bash
config router bgp
    set as 65001
    set router-id 10.10.1.2
    config neighbor
        edit "10.10.1.1"
            set soft-reconfiguration enable
            set remote-as 65001
        next
        edit "10.10.1.5"
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 10.10.3.0 255.255.255.0
        next
    end
end
```

3. 配置Router1的BGP，与FortiGate建立iBGP邻居，将路由下一跳修改为自己。与Router3建立eBGP邻居。

```bash
config router bgp
    set as 65001
    set router-id 10.10.1.1
    config neighbor
        edit "10.10.1.2"
            set next-hop-self enable
            set soft-reconfiguration enable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set remote-as 65001
        next
        edit "10.10.2.1"
            set soft-reconfiguration enable
            set remote-as 65002
        next
    end
end
```

4. 配置Router2的BGP，与FortiGate建立iBGP邻居，将路由下一跳修改为自己。与Router3建立eBGP邻居。

```bash
config router bgp
    set as 65001
    set router-id 10.10.1.5
    config neighbor
        edit "10.10.1.6"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65001
        next
        edit "10.10.2.1"
            set soft-reconfiguration enable
            set remote-as 65002
        next
    end
end
```

5. 配置Router3的BGP，分别与Router1和Router2建立eBGP邻居。

```bash
config router bgp
    set as 65002
    set router-id 10.10.2.1
    config neighbor
        edit "10.10.2.2"
            set soft-reconfiguration enable
            set remote-as 65001
        next
        edit "10.10.2.3"
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 10.10.4.0 255.255.255.0
        next
    end
end
```

结果验证

1. 在FortiGate上查看BGP学习到的路由，可以看到分别从iBGP邻居Router1和Router2学习到了Router3发布的BGP路由，下一跳分别为Router1和Router2。

```bash
FortiGate # get router info bgp network
VRF 0 BGP table version is 4, local router ID is 10.10.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.3.0/24     0.0.0.0                          100  32768        0 i ←/1>
*>i10.10.4.0/24     10.10.1.1       0                100      0        0 65002 i ←/1>
* i                 10.10.1.5       0                100      0        0 65002 i ←/→

Total number of prefixes 2

FortiGate # get router info bgp network 10.10.4.0
VRF 0 BGP routing table entry for 10.10.4.0/24
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  65002
    10.10.1.1 from 10.10.1.1 (10.10.1.1)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Last update: Thu Jan 18 11:46:37 2024

  Original VRF 0
  65002
    10.10.1.5 from 10.10.1.5 (10.10.1.5)
      Origin IGP metric 0, localpref 100, valid, internal
      Last update: Thu Jan 18 11:47:05 2024
```

2. 但在FortiGate上只有下一跳为Router1的BGP路由被放入路由表。

```bash
FortiGate # get router info routing-table bgp
Routing table for VRF=0
B       10.10.4.0/24 [200/0] via 10.10.1.1 (recursive is directly connected, port2), 02:41:00, [1/0]
```

3. 配置FortiGate的BGP开启ibgp-multipath。

```bash
config router bgp
    set ibgp-multipath enable
end
```

4. 再次查看FortiGate的路由表，下一跳为Router2的BGP路由也被放入路由表，路由下一跳在Router1和Router2间负载。

```bash
FortiGate # get router info routing-table bgp
Routing table for VRF=0
B       10.10.4.0/24 [200/0] via 10.10.1.1 (recursive is directly connected, port2), 00:00:55, [1/0]
                     [200/0] via 10.10.1.5 (recursive is directly connected, port3), 00:00:55, [1/0]
```

5. 在Router3上查看BGP学习到的路由，可以看到分别从eBGP邻居Router1和Router2学习到了FortiGate发布的BGP路由，下一跳分别为Router1和Router2（eBGP路由会自动更改下一跳为自身）。

```bash
Router3 # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 10.10.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.3.0/24     10.10.2.2       0                      0        0 65001 i ←/1>
*                   10.10.2.3       0                      0        0 65001 i ←/→
*> 10.10.4.0/24     0.0.0.0                       100  32768        0 i ←/1>

Total number of prefixes 2
```

6. 但在Router3上只有下一跳为Router1的BGP路由被放入路由表。

```bash
Router3 # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 10.10.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.3.0/24     10.10.2.2       0                      0        0 65001 i ←/1>
*                   10.10.2.3       0                      0        0 65001 i ←/→
*> 10.10.4.0/24     0.0.0.0                       100  32768        0 i ←/1>

Total number of prefixes 2

Router3 # get router info bgp network 10.10.3.0
VRF 0 BGP routing table entry for 10.10.3.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   10.10.2.3
  Original VRF 0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  65001
    10.10.2.2 from 10.10.2.2 (10.10.1.1)
      Origin IGP metric 0, localpref 100, valid, external, best
      Last update: Thu Jan 18 14:17:19 2024

  Original VRF 0
  65001
    10.10.2.3 from 10.10.2.3 (10.10.1.5)
      Origin IGP metric 0, localpref 100, valid, external
      Last update: Thu Jan 18 14:17:13 2024
```

7. 配置FortiGate的BGP开启ebgp-multipath。

```bash
config router bgp
    set ebgp-multipath enable
end
```

8. 再次查看Router3的路由表，下一跳为Router2的BGP路由也被放入路由表，路由下一跳在Router1和Router2间负载。

```bash
Router3 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.3.0/24 [20/0] via 10.10.2.2 (recursive is directly connected, port2), 00:00:21, [1/0]
                     [20/0] via 10.10.2.3 (recursive is directly connected, port2), 00:00:21, [1/0]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP Debug

1. BGP Debug过滤器：

```bash
diagnose ip router bgp set-filter [vrf <vrf-id> | neighbor <neighbor-ip> | reset]
diagnose ip router bgp filters enable
```

2. 例如过滤BGP邻居202.103.1.1的Debug信息：

```bash
diagnose ip router bgp set-filter neighbor 202.103.1.1
diagnose ip router bgp filters enable
```

3. 开启BGP Debug：

```bash
diagnose ip router bgp level info
diagnose ip router bgp all enable
diagnose debug console time enable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

清除BGP路由条目

> **重要**
>
> 在route-map等路由对象更新后，路由刷新需要手动执行，请参考路由→动态路由→BGP→路由刷新 ↗章节。

1. 为了查看新路由是否被正确添加到路由表中，可以使用 `execute router clear bgp` 命令来清除所有或一些BGP邻居的BGP连接（会话）。
2. 例如，如果你在BGP路由表中有10个路由，并且想要清除邻居为10.10.10.1的特定路由，使用如下CLI实现。

```bash
execute router clear bgp ip 10.10.10.1
```

3. 要移除AS号为65001的所有路由，使用如下CLI实现。

```bash
execute router clear bgp as 65001
```

4. 注意，如果BGP的邻居配置中开启了soft-reconfiguration，则在执行 `execute router clear bgp` 时可以在后边加入soft命令进行软重配，不需要重新与对端重新建立BGP邻居，仅重新学习路由。

```bash
exe router clear bgp all soft
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

路由震荡

产生原因

1. 当一条线路上的路由器频繁下线并重新上线，导致其他路由成员频繁的学习和删除相关路由，这被称为路由震荡（Flapping）。在BGP中，路由振荡是一个很大的问题，每当BGP邻居下线时，连接到该邻居的所有路由器都会在其路由表中发生对应变化。这会在网络上产生大量的BGP管理流量。当该路由器重新上线时，相同的流量会再次出现。如果是由于网络线路故障，比如每隔10秒就会交替在线和离线，就可能发送大量非必要的路由更新。
2. 另一个可能导致路由振荡的原因是在HA模式下有多个FortiGate设备。当HA的主设备切换到另一个成员时，网络上的其他路由器可能会将HA集群视为离线，导致路由振荡。虽然这不经常发生，但仍可能导致网络用户的服务中断。解决此问题的简单方法是增加HA集群上的route-ttl，以确保从原主设备上同步的BGP路由在故障切换后不会立即过期。另外，配置HA集群上的Graceful Restart有助于实现平滑故障切换。

处理方法

1. 处理路由振荡的首先应该检查硬件。如果线缆松动或损坏，可以更换并消除问题。如果是路由器上的接口有问题，要么避免使用该接口，要么更换一个正常的路由器。如果路由器上的电源有问题，要么更换电源，要么使用备用电源。这些快速简单的修复方法可以避免配置更复杂的BGP选项。
2. 如果路由振荡是由于其他原因，配置BGP以处理中断将确保网络用户获得不间断的服务。一些缓解BGP路由振荡的方法包括：
   - 调整Holdtime计时器
   - Dampening
   - Graceful Restart
   - BFD

调整Holdtime计时器

在排查路由振荡问题时应先考虑调整Holdtime计时器，此计时器可以降低路由器下线导致路由更新的频率。

一旦Holdtime计时器激活，其将在持续时间内禁止FortiGate接受对该邻居的任何更改。例如在Holdtime计时器期间对端路由器振荡5次，FortiGate只会识别到第1次中断。在后续Holdtime计时器持续时间内，不会发生任何变化，FortiGate在Holdtime期间内都将这个路由器视为离线。如果路由器在Holdtime计时器到期后仍在振荡，将重新启动计时器。

如果对端路由器没有振荡（例如下线后重新上线，并保持在线），计时器仍然会倒计时，并在计时器持续时间内忽略该路由器的上线。在这种情况下，路由被视为下线的时间比实际时间长。在实际使用中，这不会引起严重问题，因为更新不是频繁的。而且当一个在线的路由器被视为离线时，可以看作是一种BGP的健壮性功能。通常情况下，我们不希望大部分流量通过一个不稳定的路由，这由Holdtime计时器来实现。

以下3种不同的路由振荡情况，都可以使用 holdtime 计时器来处理：

- 路由频繁上下波动。
- 路由在很长一段时间内下线再上线一次。
- 或者路由在很长一段时间内下线并保持下线。

例如，你的网络有两个路由邻居需要设置计时器：

- 一个是主路由邻居（101.103.1.1），所有的互联网流量都经过这个路由，如果它下线时间过长则会引起较大影响，主要路由的Holdtime计时器应该相对较短，如60s。
- 另一个是很少使用的邻居（202.103.1.1）。主要路由的计时器应该相对较短（例如，60秒）。次要路由邻居的Holdtime计时器可以较长，如默认值180s。

```bash
config router bgp
    config neighbor
        edit 101.103.1.1
            set holdtime-timer 60
            set keepalive-timer 60
        next
        edit 202.103.1.1
            set holdtime-timer 180
            set keepalive-timer 60
        next
    end
end
```

Dampening

Dampening是一种通过限制对端学习的路由而限制路由振荡的方法。使用Dampening时，虽然路由仍然会振荡，但对该对端路由的关注会逐渐减少。第一次振荡不会启动Dampening，但第二次振荡将启动一个计时器，FortiGate在计时器持续时间内将无视该路由器发送的路由。如果在Dampening计时器到期之前对端路由器再次振荡，计时器将继续增加。有一个称为dampening-reachability-half-life的时间，之后路由振荡将被抑制Dampening计

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

时器一半的时间。当一个路由已经稳定一段时间，但尚未完全清除所有Dampening时，这个half-life就会生效。想要再次将振荡的路由加入路由表中，必须等待Dampening计时器到期。

如果路由振荡是暂时的，可以通过使用`execute router clear bgp` CLI从FortiGate设备的缓存中清除Dampening：

```
# execute router clear bgp dampening {<ip_address> | <ip_address/netmask>}
或
# execute router clear bgp flap-statistics {<ip_address> | <ip_address/netmask>}
```

例如，要删除10.10.1.0/24子网的路由Dampening信息，请输入以下CLI命令：

```
# execute router clear bgp dampening 10.10.1.0/24
```

配置Dampening：

```bash
config router bgp
    set dampening {enable | disable}
    set dampening-max-suppress-time <minutes_integer>
    set dampening-reachability-half-life <minutes_integer>
    set dampening-reuse <reuse_integer>
    set dampening-route-map <routemap-name_str>
    set dampening-suppress <limit_integer>
    set dampening-unreachability-half-life <minutes_integer>
end
```

Graceful Restart

在某些情况下，路由振荡是由BGP邻居中断但硬件部分（控制平面）仍然可以正常运行的情况引起的。例如当BGP进程重新启动，但硬件仍然可以正常运行和转发流量。Graceful Restart适用于这种情况，GR期间路由不会中断，但路由器对路由更新是不响应的。需要网络中的其他BGP路由器也支持优雅重启。

FortiGate HA也可以从Graceful Restart中受益。当发生HA切换时，HA集群会广播它即将下线，其他路由器不会视其为路由振荡。例如，FortiGate是四个相互发送更新的BGP路由器之一。其中任何一个路由器都支持GR。当FortiGate（GR Restarter）发生HA切换后，GR Restarter向其邻居发送一条消息，通知它正在重新启动。BGP邻居（GR Helper）将所有正在重新启动的路由器的路由标记为Stale，但它们继续使用这些路由。在重新启动完成后，将检查其路由并在需要时对其进行处理。对等方还知道在路由器重新启动期间可以维护哪些服务。在路由器完成重新启动后，路由器向其对等方发送一条消息，通知它已完成重新启动。

FortiGate设备支持其自己的BGP GR和作为邻居BGP路由器的GR Helper，配置请参考路由→动态路由→BGP→BGP GR ↗章节。

BFD

Bidirectional Forwarding Detection（BFD）是一种用于快速定位网络中硬件故障的协议。运行BFD的路由器相互通信，如果检测计时器超时，那么该路由器将被宣告为下线。然后，BFD将此信息通知给路由协议，路由信息将得到更新。

BFD的原理和相关配置请参考：https://handbook.fortinet.com.cn/routing/bfd/ ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

使用Loopback接口建立BGP

当使用Loopback接口建立BGP邻居时，注意两端FortiGate的Loopback接口必须使用32位掩码的IP地址，否则BGP邻居将无法建立。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BGP与静态路由的优先顺序

优先顺序

在路由表中，如果存在2条相同目的地址、AD（distance）的BGP路由和静态路由，那么2条路由无法同时存在于路由表中，较新一次更新的路由会被放入路由表，而旧路由会被取代。也就是说，谁最后有更新谁进路由表。

1. 如下所示，本来路由表中已存在IBGP路由192.168.123.0/24（distance为200）。

```bash
61F_A # get router info routing-table bgp
Routing table for VRF=0
B       192.168.123.0/24 [200/0] via 10.10.10.3 (recursive via to_SH_WAN1 tunnel 10.0.0.1), 03w3d12h, [1/0]
```

2. 配置distance为200且与BGP路由内容一致的静态路由。

```bash
config router static
    edit 5
        set dst 192.168.123.0 255.255.255.0
        set distance 200
        set device "to_SH_WAN1"
    next
end
```

3. 查看路由表，静态路由取代BGP路由入表，路由优选静态路由。

```bash
FortiGate # get router info routing-table all
......
Routing table for VRF=0
......
S       192.168.123.0/24 [200/0] via to_SH_WAN1 tunnel 10.0.0.1, [1/0]


FortiGate # get router info routing-table details 192.168.123.0
Routing table for VRF=0
Routing entry for 192.168.123.0/24
  Known via "static", distance 200, metric 0, best ←——静态路由被优选
  * via to_SH_WAN1 tunnel 10.0.0.1 vrf 0, tun_id

Routing entry for 192.168.123.0/24
  Known via "bgp", distance 200, metric 0
  Last update 03w3d13h ago
    vrf 0 10.10.10.3 priority 1 (recursive via to_SH_WAN1 tunnel 10.0.0.1)
```

4. 此时重置BGP邻居，让FortiGate重新学习BGP路由，再次查看路由表，BGP路由取代静态路由入表，路由优选BGP路由。

```bash
FortiGate # get router info routing-table all
......
Routing table for VRF=0
......
B       192.168.123.0/24 [200/0] via 10.10.10.3 (recursive via to_SH_WAN1 tunnel 10.0.0.1), 00:00:26, [1/0]

FortiGate # get router info routing-table details 192.168.123.0
Routing table for VRF=0
Routing entry for 192.168.123.0/24
  Known via "bgp", distance 200, metric 0, best ←——BGP路由被优选
  Last update 00:01:50 ago
  * vrf 0 10.10.10.3 priority 1 (recursive via to_SH_WAN1 tunnel 10.0.0.1)

Routing entry for 192.168.123.0/24
  Known via "static", distance 200, metric 0
    via to_SH_WAN1 tunnel 10.0.0.1 vrf 0, tun_id
```

其他

1. 如果想确保BGP路由进路由表，而静态路由不进路由表（作为BGP路由失效时的备份路由），可以通过Router Map改大BGP学习到的路由的Weight（默认是0，与静态路由一致）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config router prefix-list
    edit "acl-weight"
        config rule
            edit 1
                set prefix 192.168.123.0 255.255.255.0
                unset ge
                unset le
            next
        end
    next
end

config router route-map
    edit "weight-in"
        config rule
            edit 1
                set match-ip-address "acl-weight"
                set set-weight 40000
            next
            edit 2
            next
        end
    next
end

config router bgp
    config neighbor
        edit "10.10.10.3"
            set route-map-in "weight-in"
        next
    end
end
```

2. 此时BGP路由入表，而静态路由只存在于路由database中，当BGP路由异常消失时，静态路由可以作为备用路由生效。

```bash
FortiGate # get router info routing-table database    //查看路由数据库//
...
B    *> 192.168.123.0/24 [200/0] via 10.10.10.3 (recursive via to_SH_WAN1 tunnel 10.0.0.1), 00:03:41, [1/0]
S       192.168.123.0/24 [200/0] via to_Home_WAN1 tunnel 10.0.0.1, [1/0]
...

FortiGate # get router info routing-table all    //查看路由表//
...
B       192.168.123.0/24 [200/0] via 10.10.10.3 (recursive via to_SH_WAN1 tunnel 10.0.0.1), 00:03:46, [1/0]
...
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

如何关闭Leftmost AS检查

1. 默认情况下，FortiGate会检查学习到的BGP路由的AS Path属性，要求AS Path最左侧的AS（Leftmost AS，最近的AS）要和本地AS一致，当收到的BGP路由的AS Path属性的Leftmost AS与本地AS不一致时，会拒绝接收BGP Update，并在BGP Debug信息中显示类似`Attr ASPATH: Incorrect leftmost AS number, should be 65001`信息。

```bash
diagnose ip router bgp all enable
diagnose ip router bgp level info
diagnose debug enable

BGP: 10.10.10.2-Outgoing [DECODE] Update: Starting UPDATE decoding... Bytes To Read (4005), msg_size (86)
BGP: 10.10.10.2-Outgoing [DECODE] Attr ASPATH: Incorrect leftmost AS number, should be 65001
BGP: 10.10.10.2-Outgoing [FSM] State: Established Event: 28
BGP: 10.10.10.2-Outgoing [ENCODE] Msg-Hdr: Type 3
BGP: %BGP-3-NOTIFICATION: sending to 10.10.10.2 3/11 (UPDATE Message Error/Malformed AS_PATH.) 13 data-bytes [40
02 0a 02 02 00 00 4f f9 00 00 f4 73]
id=20300 logdesc="BGP neighbor status changed" msg="BGP: %BGP-5-ADJCHANGE: VRF 0 neighbor 10.10.10.2 Down BGP
Notification FSM-ERR"
```

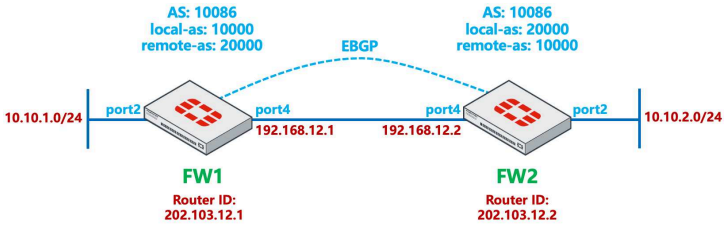
2. 通过如下CLI可以关闭对BGP路由AS Path的Leftmost AS的检查。

```
config router bgp
    set enforce-first-as disable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

多个本地AS的配置和通告

网络拓扑



1. 例如同一数据中心的双Hub场景：

   - 两个Hub（FW1与FW2）与Spoke建立IBGP邻居（使用AS 10086），并做路由反射。
   - 两个Hub之间通过EBGP（AS使用10000和20000）备份IBGP路由。
   - 此例为了简要说明问题，使用简化拓扑。

2. FW1与FW2在`config router bgp`下（以下简称“全局配置”）配置的AS均为10086，用于维护同一个AS下的IBGP邻居路由。

```bash
FW1:
config router bgp
    set as 10086
    set router-id 202.103.12.1
end

FW2:
config router bgp
    set as 10086
    set router-id 202.103.12.2
end
```

3. FW1与FW2建立EBGP邻居，FW1在`config neighbor`下配置FW2的EBGP邻居，`local-as`为10000，`remote-as`为20000，并宣告自身的路由`10.10.1.0/24`。

```bash
config router bgp
    config neighbor
        edit "202.103.12.2"
            set soft-reconfiguration enable
            set interface "port4"
            set remote-as 20000
            set local-as 10000
            set update-source "port4"
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```

4. FW2在`config neighbor`下配置FW1的EBGP邻居，`local-as`为20000，`remote-as`为10000，并宣告自身的路由`10.10.2.0/24`。

```bash
config router bgp
    config neighbor
        edit "202.103.12.1"
            set soft-reconfiguration enable
            set interface "port4"
            set remote-as 10000
            set local-as 20000
            set update-source "port4"
        next
    end
    config network
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

问题现象

1. FW1与FW2的EBGP邻居建立完成。

2. 查看FW1的BGP邻居状态和BGP路由表，邻居已建立，但学不到任何路由。

```bash
FW1 # get router info bgp summary
VRF 0 BGP router identifier 202.103.12.1, local AS number 10086
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.2 4      20000      84      83        2    0    0 00:13:31        0

Total number of neighbors 1

FW1 # get router info bgp network
VRF 0 BGP table version is 2, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                          100  32768        0 i ←/1>

Total number of prefixes 1
```

3. 查看FW2的BGP邻居状态和BGP路由表，邻居已建立，但学不到任何路由。

```bash
FW2 # get router info bgp summary
VRF 0 BGP router identifier 202.103.12.2, local AS number 10086
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.1 4      10000     112     128        3    0    0 00:13:48        0

Total number of neighbors 1

FW2 # get router info bgp network
VRF 0 BGP table version is 3, local router ID is 202.103.12.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.2.0/24     0.0.0.0                          100  32768        0 i ←/1>

Total number of prefixes 1
```

4. 在FW2上查看向FW1发送的BGP路由，可以看到FW2向FW1宣告了自身路由`10.10.2.0/24`。

```bash
FW2 # get router info bgp neighbors 202.103.12.1 advertised-routes
VRF 0 BGP table version is 3, local router ID is 202.103.12.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.2.0/24     202.103.12.2                     100  32768        0 i ←/→

Total number of prefixes 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

5. 在FW1上查看从FW2接收的BGP路由，可以看到FW1从FW2收到了路由 `10.10.2.0/24` ，但并未放入BGP路由表。该路由的AS Path为 `20000 10086` ， `10086` 为FW2在全局（ `config router bgp` ）下配置的 `local-as` 。

```bash
FW1 # get router info bgp neighbors 202.103.12.2 received-routes
VRF 0 BGP table version is 2, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.2.0/24     202.103.12.2                         0        0 20000 10086 i ←/→

Total number of prefixes 1
```

问题原因

1. 如果 `config neighbor` 下没有配置 `local-as` ，EBGP会以AS路径长度为1的方式公布源自其AS内的路由，只列出在BGP全局配置下指定的AS号。
2. 当 `config neighbor` 下的 `local-as` 设置了AS号（此例中为20000），默认配置下，BGP会将其作为全局配置的AS号（此例中为10086）的前缀，从而导致FW2发布给FW1的路由的AS Path变为 `20000 10086` 。
3. 同理，如果路由是从一个EBGP邻居学到，发布给另一个EBGP邻居，则会AS Path长度会变成3。例如FW2从另一个EBGP邻居（AS 30000）学到的路由发送给FW1，在FW1上看到的AS Path为 `20000 10086 30000` 。
4. 在FW1上查看BGP Debug信息，可以看到FW1收到FW2发布的路由 `10.10.2.0/24` ，但AS Path为 `20000 10086` ，其中包含在全局配置中设置的AS 10086，根据BGP防环机制，FW1将该路由丢弃（ `Prefix 10.10.2.0/24 path_id 0 denied due to as-path contains our own AS` ）。

```bash
diagnose ip router bgp set-filter neighbor 202.103.12.2
diagnose ip router bgp filters enable
diagnose ip router bgp level info
diagnose ip router bgp all enable

FW1# BGP: 202.103.12.2-Outgoing [DECODE] Msg-Hdr: type 2, length 51
BGP: 202.103.12.2-Outgoing [DECODE] Update: Starting UPDATE decoding... Bytes To Read (32), msg_size (32)
BGP: 202.103.12.2-Outgoing [DECODE] Update: NLRI Len(4)
BGP: 202.103.12.2-Outgoing [FSM] State: Established Event: 27
BGP: 202.103.12.2-Outgoing [RIB] Update: Prefix 10.10.2.0/24 path_id 0 denied due to as-path contains our own AS
```

5. FW2学不到FW1发布的路由 `10.10.1.0/24` 也是同样的原因。

解决方法

local-as-replace-as（推荐）

> **重要**
>
> `local-as-replace-as` 与 `local-as-no-prepend` 都需要在 `config router bgp` 下配置了 `local-as` ，且与全局（ `config router bgp` ）下配置的AS号不一样时才能配置。

1. 在FW2上的EBGP邻居配置中，开启 `local-as-replace-as` 。开启后，FW2会使用 `config neighbor` 下配置的 `local-as` 替换在全局（ `config router bgp` ）下配置的AS号。

```bash
config router bgp
    config neighbor
        edit "202.103.12.1"
            set local-as-replace-as enable
        next
    end
end
```

2. 在FW1上查看收到的BGP路由，FW1将收到AS Patch长度为1的路由，如下所示，AS Patch为 `20000` ，此为FW2在 `config neighbor` 下配置的 `local-as` ，FW2没有添加在全局（ `config router bgp` ）下配置的AS号 `10086` 。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

`local-as-replace-as` 只会在出方向使用 `config neighbor` 下配置的 `local-as` 替换全局（`config router bgp`）下配置的AS号，已有的AS Path不会更改。

```bash
FW1 # get router info bgp neighbors 202.103.12.2 received-routes
VRF 0 BGP table version is 3, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.2.0/24     202.103.12.2                            0        0 20000 i ←/→

Total number of prefixes 1
```

3. 在FW1上查看BGP路由表，从FW2学习到的路由 `10.10.2.0/24` 已被正确加载，并添加了自己在 `config neighbor` 下配置的 `local-as` 号 `10000`。

```bash
FW1 # get router info bgp network
VRF 0 BGP table version is 3, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                          100  32768        0 i ←/1>
*> 10.10.2.0/24     202.103.12.2    0                       0        0 10000 20000 i ←/1>

Total number of prefixes 2
```

4. 在FW1上查看路由表中的BGP路由，从FW2学习到的EBGP路由被正确加载。

```bash
FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [20/0] via 202.103.12.2 (recursive is directly connected, port4), 00:07:42, [1/0]
```

5. 同理，在FW1上的EBGP邻居中开启 `local-as-replace-as`，FW2也可以正常学习到FW1发布的路由。

6. **附加测试** `local-as-no-prepend`：在FW1的EBGP邻居配置中，开启 `local-as-no-prepend`，FW1将不会在BGP路由表中添加自己在 `config neighbor` 中配置的 `local-as`。

重要

`local-as-no-prepend` 作用于入方向，例如FGT在与EBGP邻居A（配置了 `local-as`），开启 `local-as-no-prepend` 后，向EBGP邻居B（未配置 `local-as`）转发通告A的EBGP路由时，不会在AS Path中加上与EBGP邻居A配置的 `local-as`。

```bash
config router bgp
    config neighbor
        edit "202.103.12.2"
            set local-as-no-prepend enable
        next
    end
end

FW1 # get router info bgp network
VRF 0 BGP table version is 5, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                          100  32768        0 i ←/1>
*> 10.10.2.0/24     202.103.12.2    0                       0        0 20000 i ←/1>

Total number of prefixes 2
```

allowas-in-enable

1. 恢复默认配置（在FW1和FW2上禁用 `local-as-replace-as`）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 在FW1上的EBGP邻居配置中，开启`allowas-in-enable`。开启后，FW1会允许AS Path包含自身AS号的BGP路由加载（EBGP防环失效）。

```bash
config router bgp
    config neighbor
        edit "202.103.12.2"
            set allowas-in-enable enable
            set allowas-in 3    //默认配置，允许自身AS号在AS Path中出现的最大次数//
        next
    end
```

3. 在FW1上查看从FW2接收的BGP路由，可以看到FW1从FW2收到了路由`10.10.2.0/24`。该路由的AS Path为`20000 10086`，`10086`为FW2在全局（`config router bgp`）下配置的`local-as`。

```bash
FW1 # get router info bgp neighbors 202.103.12.2 received-routes
VRF 0 BGP table version is 6, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.2.0/24     202.103.12.2                           0        0 20000 10086 i ←/→

Total number of prefixes 1
```

4. 在FW1上查看BGP路由表，从FW2学习到的路由`10.10.2.0/24`已被正确加载，并添加了自己在`config neighbor`下配置的`local-as`号`10000`。

```bash
FW1 # get router info bgp network
VRF 0 BGP table version is 6, local router ID is 202.103.12.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Weight RouteTag Path
*> 10.10.1.0/24     0.0.0.0                          100  32768        0 i ←/1>
*> 10.10.2.0/24     202.103.12.2    0                     0        0 10000 20000 10086 i ←/1>

Total number of prefixes 2
```

5. 在FW1上查看路由表中的BGP路由，从FW2学习到的EBGP路由被正确加载。

```bash
FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [20/0] via 202.103.12.2 (recursive is directly connected, port4), 00:09:25, [1/0]
```

6. 同理，在FW2上的EBGP邻居中开启`allowas-in-enable`，FW2也可以正常学习到FW1发布的路由。

7. 不推荐使用此方法解决，会破坏EBGP的防环机制。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Route Map

Route Map一种强大的工具，可以根据特定条件对动态路由协议进行操作。主要用于BGP，用于操作由FortiGate宣告的路由（route-map-out）或从其他路由器接收的路由（route-map-in）。

在OSPF中，可以使用Route Map进行条件性的default-information-originate（宣告默认路由）、过滤邻居宣告的路由，或者匹配特定路由进行重分发。Route Map也可以被RIP使用来匹配重分发的路由。

一个Route Map可以包含多个规则，按照自上而下的顺序进行处理。每个规则都有允许或拒绝的动作。这些规则根据各种属性匹配路由，并根据匹配的路由设置路由相关属性，最后的隐含动作为deny any。

例如可以使用Route Map来匹配特定Community的BGP路由，然后设置匹配路由的AS Path。然后在BGP邻居的设置中应用此Route Map。

配置方法

```bash
config router route-map
    edit <name>
        config rule
            edit <id>
                set action {permit | deny}
                set match-as-path <string>
                set match-community <string>
                set match-ip-address <string>
                set match-ip6-address <string>
                set match-ip-nexthop <string>
                set match-ip6-nexthop <string>
            next
        end
    next
end
```

- `match-as-path <string>`：匹配一个BGP AS Path List。
- `match-community <string>`：匹配一个BGP Community。
- `match-ip-address <string>`：匹配一个access-list或prefix-list。
- `match-ip6-address <string>`：匹配一个access-list6或prefix-list6。
- `match-ip-nexthop <string>`：匹配IPv4路由的下一跳，通过access-list或prefix-list表示。
- `match-ip6-nexthop <string>`：匹配IPv6路由的下一跳，通过access-list6或prefix-list6表示。

引用Route Map

被RIP引用

```bash
config router rip
    config redistribute
        edit <name>
            set routemap <string>
        next
    end
end
```

被OSPF引用

```bash
config router ospf
    set default-information-route-map <string>
    set distribute-route-map-in <string>
    config redistribute <string>
        set routemap <string>
    end
end
```

- `default-information-route-map <string>`：根据Route Map中匹配的路由是否存在于路由表，决定是否宣告默认路由。
- `distribute-route-map-in <string>`：入方向根据引用的Route Map操作路由。
- `redistribute <string>`：在重发布中引用Route Map过滤路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

被BGP引用

```bash
config router bgp
    config neighbor
        edit <ip>
            set route-map-in <string>
            set route-map-in6 <string>
            set route-map-in-vpnv4 <string>
            set route-map-out <string>
            set route-map-out-preferable <string>
            set route-map-out6 <string>
            set route-map-out6-preferable <string>
            set route-map-out-vpnv4 <string>
            set route-map-out-vpnv4-preferable <string>
        next
    end
    config network
        edit <id>
            set prefix <IP/netmask>
            set route-map <string>
        next
    end
    config redistribute <string>
        set route-map <string>
    end
end
```

- `route-map-in <string>`：在入方向引用Route Map操作IPv4路由。
- `route-map-in6 <string>`：在入方向引用Route Map操作IPv6路由。
- `route-map-in-vpnv4 <string>`：在入方向引用Route Map操作VPNv4路由。
- `route-map-out <string>`：在出方向引用Route Map操作IPv4路由。
- `route-map-out-preferable <string>`：在SD-WAN Neighbor中满足SLA标准的BGP邻居使用的出方向Route Map，针对IPv4路由（不满足SLA标准的BGP路由使用普通的route-map-out）。
- `route-map-out6 <string>`：在出方向引用Route Map操作IPv6路由。
- `route-map-out6-preferable <string>`：在SD-WAN Neighbor中满足SLA标准的邻居使用的出方向Route Map，针对IPv6路由（不满足SLA标准的BGP路由使用普通的route-map-out6）。
- `route-map-out-vpnv4 <string>`：在出方向引用Route Map操作VPNv4路由。
- `route-map-out-vpnv4-preferable <string>`：在SD-WAN Neighbor中满足SLA标准的BGP邻居使用的出方向Route Map，针对VPNv4路由（不满足SLA标准的BGP路由使用普通的route-map-out-vpnv4）。
- `route-map <string>`：引用Route Map操作本地宣告的BGP路由。
- `redistribute <string>`：在重发布中调用Route Map。

```bash
config router bgp
    set as <AS_number>
    config neighbor
        edit <ip>
            set remote-as <AS_number>
            config conditional-advertise
                edit <advertise-routemap>
                    set condition-routemap <name1>, <name2>, ...
                    set condition-type {exist | non-exist}
                next
            end
        next
    end
end
```

- `<advertise-routemap>`：引用Route Map匹配要宣告的网络。
- `condition-routemap <name1>, <name2>, ...`：Route Map匹配条件的路由是否存在于路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Access List

访问列表（Access List）是用于基于IPv4/IPv6地址 + 掩码的prefix进行路由过滤的简单列表。

配置方法

```bash
IPv4:
config router access-list
    edit <name>
        config rule
            edit <id>
                set action {permit | deny}
                set prefix <IPv4_address>
                set wildcard <wildcard_filter>
                set exact-match {enable | disable}
            next
        end
    next
end

IPv6:
config router access-list6
    edit <name>
        config rule
            edit <id>
                set action {permit | deny}
                set prefix <IPv6_address>
                set exact-match {enable | disable}
            next
        end
    next
end
```

- `action {permit | deny}`：动作是允许还是拒绝路由条目。
- `prefix <IPv4_address>`：IPv4路由的前缀 + 掩码，如 `10.10.1.0/24`。该配置与 `wildcard` 互斥。
- `wildcard <wildcard_filter>`：以通配符掩码（反掩码）方式匹配路由，如 `10.0.104.0 0.255.0.255`（匹配掩码为1的位，为0的位忽略），该配置与 `prefix` 互斥。
- `exact-match {enable | disable}`：是否严格匹配，如果开启严格匹配，只有prefix和wildcard（掩码）完全相同的路由会匹配此Access List；如果关闭严格匹配，大于该掩码的CIDR路由也会匹配，默认关闭（仅在使用 `prefix` 模式时生效）。

引用Access List

被RIP引用

```bash
config router rip
    config distribute-list
        edit <id>
            set direction {in | out}
            set listname <string>
        next
    end
    config offset-list
        edit <id>
            set direction {in | out}
            set access-list <string>
            set offset <integer>
        next
    end
end
```

- `listname <string>`：引用Access List或Prefix List用于出/入方向路由过滤。
- `access-list <string>`：针对Access List匹配的路由修改路由的跳数（这里Access List中的动作permit/deny表示匹配/不匹配）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

被OSPF引用

```bash
config router ospf
    set distribute-list-in <string>
    config distribute-list
        edit <id>
            set access-list <string>
            set protocol {connected | static | rip}
        next
    end
end
```

- `distribute-list-in <string>`：入方向引用Access List过滤路由。
- `access-list <string>`：发布路由时引用Access List过滤路由。

被BGP引用

```bash
config router bgp
    config neighbor
        edit <ip>
            set distribute-list-in <string>
            set distribute-list-in6 <string>
            set distribute-list-in-vpnv4 <string>
            set distribute-list-out <string>
            set distribute-list-out6 <string>
            set distribute-list-out-vpnv4 <string>
        next
    end
end
```

- `distribute-list-in <string>`：入方向引用Access List过滤IPv4路由。
- `distribute-list-in6 <string>`：入方向引用Access List过滤IPv6路由。
- `distribute-list-in-vpnv4 <string>`：入方向引用Access List过滤VPNv4路由。
- `distribute-list-out <string>`：出方向引用Access List过滤IPv4路由。
- `distribute-list-out6 <string>`：出方向引用Access List过滤IPv6路由。
- `distribute-list-out-vpnv4 <string>`：出方向引用Access List过滤VPNv4路由。

被Route Map引用

重要

被Route Map引用时，Access List中的动作permit/deny表示匹配/不匹配，而不是允许/禁用。

```bash
config router route-map
    edit <name>
        config rule
            edit <id>
                set match-ip-address <string>
                set match-ip6-address <string>
                set match-ip-nexthop <string>
                set match-ip6-nexthop <string>
            next
        end
    next
end
```

- `match-ip-address <string>`：引用Access List匹配IPv4路由条目。
- `match-ip6-address <string>`：引用Access List匹配IPv6路由条目。
- `match-ip-nexthop <string>`：引用Access List匹配IPv4路由下一跳。
- `match-ip6-nexthop <string>`：引用Access List匹配IPv6路由下一跳。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Prefix List

与Access List类似，前缀列表（Prefix List）是用于匹配IPv4/IPv6地址 + 掩码的前缀进行路由过滤的简单列表。但前缀列表可以指定要匹配的最小（ge，大于或等于）和最大（le，小于或等于）前缀长度。例如，具有ge为16的10.0.0.0/8前缀将匹配10.0.0.0/8网络中的任何具有/16或更长前缀的内容（10.10.0.0/16匹配，而10.10.0.0/12不匹配）。

配置方法

```bash
IPv4:
config router prefix-list
    edit "prefix-list1"
        config rule
            edit 1
                set action {permit | deny}
                set prefix <IPv4_address>
                set ge <integer>
                set le <integer>
            next
        end
    next
end

IPv6:
config router prefix-list6
    edit "prefix-list-IPv6"
        config rule
            edit 1
                set action {permit | deny}
                set prefix6 <IPv6_address>
                set ge <integer>
                set le <integer>
            next
        end
    next
end
```

引用Prefix List

被RIP引用

```bash
config router rip
    config distribute-list
        edit <id>
            set direction {in | out}
            set listname <string>
        next
    end
end
```

- `listname <string>`：引用Access List或Prefix List用于出/入方向路由过滤。

被OSPF引用

```bash
config router ospf
    set distribute-list-in <string>
end
```

- `distribute-list-in <string>`：引用Prefix List用于入方向路由过滤。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

被BGP引用

```bash
config router bgp
    config neighbor
        edit <ip>
            set prefix-list-in <string>
            set prefix-list-in6 <string>
            set prefix-list-in-vpnv4 <string>
            set prefix-list-out <string>
            set prefix-list-out6 <string>
            set prefix-list-out-vpnv4 <string>
        next
    end
end
```

- `prefix-list-in <string>`：引用Prefix List用于该邻居入方向IPv4路由过滤。
- `prefix-list-in6 <string>`：引用Prefix List用于该邻居入方向IPv6路由过滤。
- `prefix-list-in-vpnv4 <string>`：引用Prefix List用于该邻居入方向VPNv4路由过滤。
- `prefix-list-out <string>`：引用Prefix List用于该邻居出方向IPv4路由过滤。
- `prefix-list-out6 <string>`：引用Prefix List用于该邻居出方向IPv6路由过滤。
- `prefix-list-out-vpnv4 <string>`：引用Prefix List用于该邻居出方向VPNv4路由过滤。

被Route Map引用

重要

被Route Map引用时，Prefix List中的动作permit/deny表示匹配/不匹配，而不是允许/禁用。

```bash
config router route-map
    edit <name>
        config rule
            edit <id>
                set match-ip-address <string>
                set match-ip6-address <string>
                set match-ip-nexthop <string>
                set match-ip6-nexthop <string>
            next
        end
    next
end
```

- `match-ip-address <string>`：引用Prefix List匹配IPv4路由条目。
- `match-ip6-address <string>`：引用Prefix List匹配IPv6路由条目。
- `match-ip-nexthop <string>`：引用Prefix List匹配IPv4路由下一跳。
- `match-ip6-nexthop <string>`：引用Prefix List匹配IPv6路由下一跳。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

AS Path List

AS Path List使用正则表达式来匹配BGP路由的AS_PATH属性。可用于从BGP邻居筛选入站或出站路由，或者作为Route Map中的匹配条件，以匹配BGP路由中的AS_PATH属性。

配置方法

```bash
config router aspath-list
    edit <name>
        config rule
            edit <id>
                set action {deny | permit}
                set regexp <string>
            next
        end
    next
end
```

引用AS Path List

被BGP引用

```bash
config router bgp
    config neighbor
        edit <ip>
            set filter-list-in <string>
            set filter-list-in6 <string>
            set filter-list-out <string>
            set filter-list-out6 <string>
        next
    end
end
```

- `filter-list-in <string>`：针对该邻居引用AS Path List过滤入方向的IPv4路由。
- `filter-list-in6 <string>`：针对该邻居引用AS Path List过滤入方向的IPv6路由。
- `filter-list-out <string>`：针对该邻居引用AS Path List过滤出方向的IPv4路由。
- `filter-list-out6 <string>`：针对该邻居引用AS Path List过滤出方向的IPv6路由。

被Rout Map引用

```bash
config router route-map
    edit <name>
        config rule
            edit <id>
                set match-as-path <string>
            next
        end
    next
end
```

- `match-as-path <string>`：引用AS Path List匹配路由条目。

配置举例

1. 查看设备BGP学习到的路由属性，学习到两条BGP路由，需要过滤掉AS Path起源是100的路由。

```bash
get router info bgp neighbors 169.254.1.2 routes
VRF 0 BGP table version is 1, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete


```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Network Next Hop Metric LocPrf Weight RouteTag Path
*> 100.100.100.0/24 169.254.1.2 0 0 300 100 i ←/→    //过滤AS Path起源是100的路由//
*> 200.200.200.0/24 169.254.1.2 0 0 300 200 i ←/→
```

2. 配置AS Path List，使用正则表达式匹配AS Path末尾是`100`结尾的AS Path。

```bash
config router aspath-list
    edit "AS100"
        config rule
            edit 1
                set action permit
                set regexp "_100$"
            next
        end
    next
end
```

3. 在Route Map中引用该AS Path List，禁止接收匹配该AS Path List的路由，其他路由可以正常接收。

```bash
config router route-ma
    edit "RM_INBOUND"
        config rule
            edit 1
                set action deny
                set match-as-path "AS100"
            next
            edit 2
                set action permit
            next
        end
    next
end
```

4. 在BGP邻居中引用该Route Map。

```
config router bgp
    config neighbor
        edit "169.254.1.2"
            set route-map-in "RM_INBOUND"
        next
    end
end
```

5. 刷新入方向的BGP路由，再次查看学习到的BGP路由，可以看到起源为AS 100的BGP路由已经被过滤掉。

```bash
FortiGate # get router info bgp neighbors 169.254.1.2 routes
VRF 0 BGP table version is 1, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight RouteTag Path
*> 200.200.200.0/24 169.254.1.2 0 0 0 300 200 i ←/1>

Total number of prefixes 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Community List

Community List使用Community字符串过滤/操作BGP路由，可以在Route Map中使用，匹配在Community List中定义的具有特定Community属性的路由。

配置方法

```bash
config router community-list
    edit <name>
        set type {standard | expanded}
        config rule
            edit <id>
                set action {deny | permit}
                set regexp <string>
                set match <string>
            next
        end
    next
end
```

- `type {standard | expanded}`：Community List的类型：
  - standard：匹配精确的Community字符，通常用于直接过滤Community精确字符。
  - expanded：基于正则表达式进行匹配。在处理较多的Community时，非常有用。
- `action {deny | permit}`：action的permit/deny表示匹配/不匹配。
- `regexp <string>`：使用正则表达式匹配Community List，`type`配置为`expanded`时可用。
- `match <string>`：使用完整Community字符方式匹配Community List，`type`配置为`standard`时可用。

引用Community List

被Route Map引用

```bash
config router route-map
    edit <name>
        config rule
            edit <id>
                set match-community <string>
            next
        end
    next
end
```

- `match-community <string>`：匹配BGP路由中的community属性。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

动态路由协议排错

OSPF邻居无法建立

OSPF邻居建立不起来原因？

最常见的是如下几种情况：
1. OSPF网络类型是NBMA的，但忘记在OSPF协议模式下配置Peer邻居了；
2. OSPF邻居的Hello及Dead Interval值不一致；
3. 在Stub或NSSA区域，有些FortiGate没有配置成Stub或NSSA；
4. OSPF验证配置错误；
5. OSPF Router ID有问题，可能和某个其他设备一样了；
6. OSPF链路两端的网络类型不一致；
7. OSPF链路两端的MTU相差比较大，尤其注意和不同厂商实现互通时（需要在其接口下配置OSPF忽略MTU检查或修改MTU）；
8. 该网络根本就没有启动OSPF；
9. 区域号不一致；链路的网络地址不一致，注意检查两边的mask；

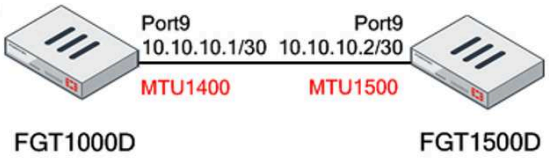
有什么好的办法知道OSPF出了什么问题？

调试开关是需要打开的，它能让你对OSPF的大部分问题看的一目了然

```
#diagnose ip router ospf  level warn
#diagnose ip router ospf  all  enable
#diagnose debug enable
```

OSPF不能建立邻接关系

症状：OSPF邻居关系卡在Exstart/Exchange状态



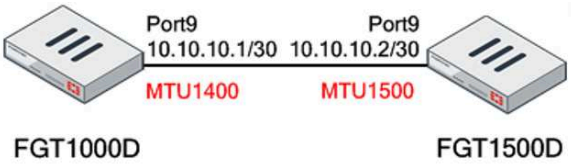

```
FG1000D # get router info ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.2        1   ExStart/Backup  00:00:36    10.10.10.2      port9

FG1000D # get router info ospf interface
port9 is up, line protocol is up
Internet Address 10.10.10.1/30, Area 0.0.0.0, MTU 1400
Process ID 0, Router ID 10.10.10.1, Network Type BROADCAST, Cost: 1

FG1500D # get router info ospf interface
port9 is up, line protocol is up
Internet Address 10.10.10.2/30, Area 0.0.0.0, MTU 1500
Process ID 0, Router ID 10.10.10.2, Network Type BROADCAST, Cost: 1
```

```
FG1000D # diagnose ip router ospf  level warn
FG1000D # diagnose ip router ospf all enable
FG1000D # diagnose  debug enable
FG1000D # id=20301 logdesc="Routing log" msg="OSPF: RECV[DD]: From
10.10.10.2 via port9:10.10.10.1: MTU size is too large (1500)"     //开启调试
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

OSPF不能建立邻接关系

解决办法



解决办法一：修改接口MTU为一致

```
FG1000D # config system interface
FG1000D (interface) # edit port9
FG1000D (port9) # set mtu 1500
FG1000D (port9) # end
//或者//
config router ospf
          config ospf-interface
            edit "port9"
                set interface "port9"
                set mtu 1500
                end
```

解决办法二：在OSPF-interface配置mtu-ignore

```
config router ospf
          config ospf-interface
            edit "port9"
                set interface "port9"
                set mtu-ignore enable
            next
        end
```

```
FG1000D # get router info ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.2        1   Full/DR         00:00:37    10.10.10.2      port9

FG1500D # get router info ospf  neighbor          //邻居关系变为Full
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.1        1   Full/Backup     00:00:38    10.10.10.1      port9
```

BGP邻居无法建立

有哪些原因会导致BGP连接建立不起来？

最常见原因如下：

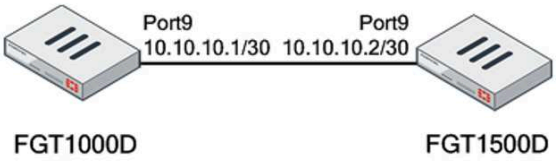
1) 两边BGP peer地址不可达，一般是底层原因或者缺少可达的路由，可以使用扩展的ping命令检查TCP/IP(TCP 179)连接是否正常,由于一台路由器可能有多个接口能够到达对端，应使用execute ping-options source x.x.x.x 命令指定发送ping包的源IP地址
2) 对等体IP地址和AS配置错误，常为配置错误；
3) OPEN报文协商失败，OPEN报文需要协商BGP版本、Holdtime、RouterID以及可选项参数（包括各种能力参数）等；
4) BGP的MD5验证配置错误；
5) BGP的RouterID冲突；

有哪些排错手段针对BGP连接建立不起来的情况？

1) 首先打开调试开关，确认状态机在哪一步出现错误；
   diagnose ip router bgp level warn 或 info
   diagnose ip router bgp all enable
   diagnose debug enable
2) 如果BGP状态始终在active状态徘徊，表示TCP建立不起来，首先排除底层不通和路由不可达的情况；
3) 如果BGP状态始终在active状态徘徊，其次排除BGP的MD5验证问题；
4) 如果BGP状态始终在active状态徘徊，最后特殊配置问题，比如EBGP peer的ebgp-enforce-multihop；
5) 如果是Open报文协商错误，通过调试开关可以很方便的查看到具体的错误类别和信息，然后根据错误提示采取具体措施；

BGP不能建立邻接关系

症状：邻居无法起来




```
FG1000D # get router info bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle

FG1500D # get router info bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
```

```
FG1000D # diagnose ip router bgp level warn
FG1000D # diagnose ip router bgp all  enable
FG1000D # diagnose  debug enable
FG1000D # id=20301 logdesc="Routing log" msg="BGP: 10.10.10.2-Outgoing [DECODE] Open: Invalid Router ID
1.1.1.1"  //通过diagnose发现，Router-id存在异常
id=20301 logdesc="Routing log" msg="BGP: %BGP-3-NOTIFICATION: sending to 10.10.10.2 2/3 (OPEN Message
Error/Bad BGP Identifier.) 4 data-bytes [01 01 01 01]"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

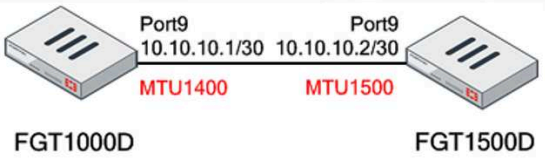
重要

如果BGP邻居较多，可以使用如下CLI命令来过滤特定BGP邻居的Debug信息：

```bash
diagnose ip router bgp set-filter neighbor x.x.x.x
```

BGP不能建立邻接关系

解决办法：通过diagnose_debug得知是Router-ID错误，检查BGP配置，修改Router-ID



检查配置：

```
FG1000D # show router bgp
config router bgp
    set as 100
    set router-id 1.1.1.1
        config neighbor
            edit "10.10.10.2"
                set remote-as 200
```

检查配置：

```
FG1500D # show router bgp
config router bgp
    set as 200
    set router-id 1.1.1.1 //冲突的R-ID
        config neighbor
            edit "10.10.10.1"
                set remote-as 100
```

解决办法：修改Router-ID不冲突即可

```
FG1500D # config router bgp
FG1500D (bgp) # set router-id 1.1.1.2
FG1500D (bgp) # end
```

修改结果：

```
FG1000D # get router info bgp neighbors
BGP neighbor is 10.10.10.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 1.1.1.2
  BGP state = Established, up for 00:00:12

FG1500D # get router  info bgp neighbors
BGP neighbor is 10.10.10.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 1.1.1.1
  BGP state = Established, up for 00:00:29
```

重启路由进程

```bash
execute router clear ospf process
execute router clear bgp all (in/out/soft/prefix-filter)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD原理

BFD简介

Bidirectional Forwarding Detection（BFD）是一种可用于快速检测对端网络硬件/软件故障的协议。运行BFD的两台路由设备以协商的速率相互发送BFD数据包。如果来自启用BFD的对端路由器的BFD包未能到达，则对端路由器将被本端认为故障。 BFD将此信息传递给关联的路由协议（如静态路由/OSPF/BGP等）并更新对应的路由信息。它有助于检测单向设备故障并用于路由协议的快速收敛。

BFD优点

上层协议（如BGP、OSPF）的检测时间都在1s以上，这样的故障检测时间对某些应用来说是不能容忍的。一般动态路由协议检测时间最小只能达到1秒的精度，且无法为其它路由协议提供快速故障检测。

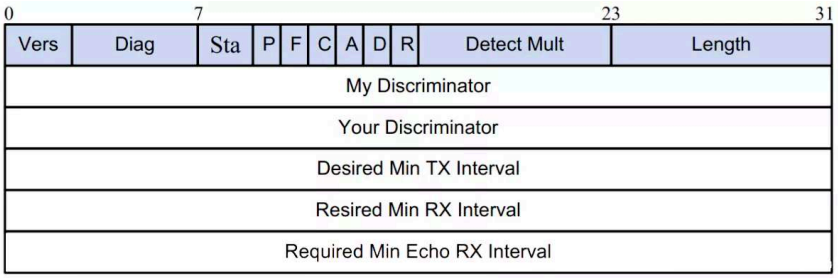
- 可以为不同的上层应用服务（如OSPF、BGP、静态路由等），提供一致的快速故障检测时间。
- 提供小于1秒的检测时间，从而加快网络收敛速度，减少应用中断时间。
- 可以对设备间多种类型的双向转发路径进行故障检测，包括直连物理链路、VPN隧道、多跳路径（FortiOS 7.2.0开始支持）等。

BFD缺点

- BFD进行链路故障的检测依赖于BFD会话能够正常协商完成。
- 当创建BFD会话过程中链路存在问题时，即BFD会话无法通过三次握手状态切换为UP时，BFD无法检测链路状态，此时当上层应用不存在自身保活时，就无法感知链路故障，导致上层应用无法进行相应的处理。
- 由于对网络质量非常敏感，只适用于链路状态较好的环境下，如专线、直连环境。链路质量较差的环境下BFD可能会产生误报行为导致线路波动，所以不建议在诸如Internet上的VPN线路上使用该功能。
- 与动态路由的Graceful Restart（GR）功能冲突，不建议同时使用。GR用于FortiGate通知邻居自己的路由进程将重启，并且邻居从FortiGate学到的路由应在重启期间保留。但BFD检测到故障时会将动态路由邻居重置。这种操作上的差异使得在GR的同时使用BFD会导致功能上的冲突，可能导致GR期间流量中断。业界通用的做法是在使用GR时关闭BFD。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD报文格式

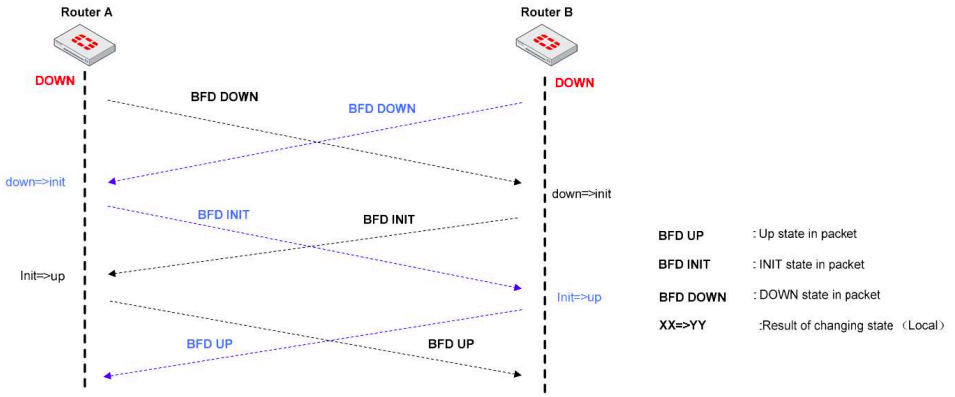


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

字段	含义
Vers	BFD协议版本号，目前版本号为1
Diag	诊断码，表明发送方最近一次会话Down的原因： 0：No Diagnostic 1：Control Detection Time Expired 2：Echo Function Failed 3：Neighbor Signaled Session Down 4：Forwarding Plane Reset 5：Path Down 6：Concatenated Path Down 7：Administratively Down 8：Reverse Concatenated Path Down 9~31：Reserved for future use **For Fortinet:** 0x01: Local inactive timer expired 0x03: Remote peer indicates it's down 0x23: Remote peer indicates restarting
Sta	发送方BFD会话当前状态，取值为： 0：AdminDown 1：Down 2：Init 3：Up
P	会话参数变化时置位，参数发生改变时，发送方在BFD报文中置该标志，接收方必须立即响应该报文： 1：表示发送系统请求进行连接确认，或者发送请求参数改变的确认 0：表示发送系统不请求确认
F	如果收到的BFD控制报文P字段置位，则将下一个发送的BFD控制报文的F字段置位作为应答： 1：表示发送系统响应一个接收到P比特为1的BFD包 0：表示发送系统不响应一个P比特为1的包
C	转发/控制分离标志，一旦置位，控制平面的变化不影响BFD检测，如：控制平面为IS-IS，当IS-IS重启/GR时，BFD可以继续监测链路状态： 1：表示发送系统的BFD实现不依赖于它的控制平面。即，BFD报文在转发平面传输，即使控制平面失效，BFD仍然能够起作用 0：表示BFD报文在控制平面传输
A	该字段置位表明报文包含认证部分，会话需要进行认证
D	该字段置位表明发送方希望以查询模式运行，不置位表明不希望以查询模式运行或不支持查询模式
R	保留位，发送时设为0，接收时忽略该字段
Detect Mult	检测时间倍数，用于检测方计算检测超时时间
Length	BFD控制报文长度，单位为字节
My Discriminator	BFD会话连接本地标识符。发送系统产生的一个唯一的、非0鉴别值，用来区分一个系统的多个BFD会话
Your Discriminator	BFD会话连接远端标识符。从远端系统接收到的鉴别值，这个域直接返回接收到的“My Discriminator”，如果不知道这个值就返回0
Desired Min TX Interval	本地支持的最小BFD报文接收间隔，单位为毫秒
Required Min RX Interval	发送方支持的最小BFD控制报文接收时间间隔，单位为毫秒
Required Min Echo RX Interval	本地支持的最小Echo报文接收间隔，单位为微秒 （如果本地不支持Echo功能，则设置0）
Auth Type	认证类型
Auth Len	可选认证部分长度，包括Auth Type和Auth Len字段，单位为字节

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD会话建立



BFD使用三路握手的机制来建立会话，发送方在发送BFD控制报文时会在Sta字段填入本地当前的会话状态，接收方根据收到的BFD控制报文的Sta字段以及本地当前会话状态来进行状态机的迁移，建立会话。Router A和Router B的BFD收到上层应用的通知后，发送状态为DOWN的BFD控制报文。Router B的BFD状态变化同Router A。

- Router B收到对端状态为DOWN的BFD控制报文后，本地会话状态由DOWN迁移到INIT，随后发送的BFD控制报文中将Sta字段填为2表明会话状态为INIT。Router A的BFD状态变化同Router B。
- Router A收到对端状态为INIT的BFD控制报文后，本地会话状态由INIT迁移到UP，随后发送的BFD控制报文中将Sta字段填为3表明会话状态为UP。Router B的BFD状态变化同Router A。
- BFD双方状态都为UP，会话成功建立并开始检测链路状态。

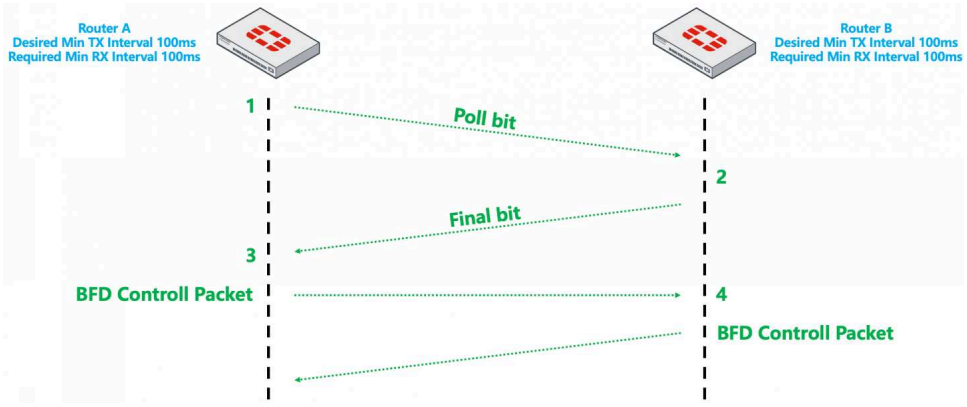
BFD定时器协商

FortiGate BFD会话建立前BFD控制报文以5s的时间间隔周期发送以减小报文流量。在BFD会话建立后则以协商到的时间间隔发送BFD控制报文以实现快速检测的目的。在BFD会话建立的同时，BFD控制报文发送时间间隔以及检测超时时间也会通过报文交互协商确定。在BFD会话有效期间，这些定时器可以随时协商修改而不影响会话状态。

BFD会话不同方向的定时器协商是分别独立进行的，两端定时器时间可以不同。BFD控制报文发送时间间隔为本端Desired Min TX Interval与对端Required Min RX Interval之中的最大值，也就是说比较慢的一方决定了发送频率。

- 检测超时时间为对端BFD控制报文中的Detect Mult乘以经过协商的对端BFD控制报文发送时间间隔。
- 如果加大本端Desired Min TX Interval，那么本端实际发送BFD控制报文的时间间隔必须要等收到对端F字段置位的报文后才能改变，这是为了确保在本端加大BFD控制报文发送时间间隔前对端已经加大了检测时间，否则可能导致对端检测定时器错误超时。
- 如果减小本端Required Min RX Interval，那么本端检测超时时间必须要等收到对端F字段置位的报文后才能改变，这是为了确保在本端减小检测超时时间前对端已经减小了BFD控制报文发送间隔时间，否则可能导致本端检测定时器错误超时。
- 如果减小本端Desired Min TX Interval，本端BFD控制报文发送时间间隔将会立即减小；加大Required Min RX Interval，本端检测超时时间将会立即加大。

BFD协商举例



1. Router A与Router B创建BFD配置，双方的Desired Min TX Interval和Required Min RX Interval都为100ms，Detect Mult都为3。根据上面介绍的BFD定时器协商规则，Router A的发送时间间隔为Router A的TX与Router B的RX中的最大值：100ms，Router B的发送时间间隔也是100ms，双方的检测超时时间都为100ms * Detect Mult (3) = 300ms。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 此时将Router A的TX和RX加大到150ms。
   - Router A比较本端的RX（150ms）和Router B的TX（100ms），从而将本端检测时间改为450ms。同时向对端发送P字段置位的BFD控制报文（TX和RX均为150ms）。
   - Router B收到报文后，给Router A回复F字段置位的BFD控制报文（TX和RX均为100ms）。同时将收到报文中的RX与本端的TX进行比较，由于对端Router A TX较大，故Router B的发送间隔改为150ms。经过比较本端RX和对端的TX，从而将检测超时时间也增大到450ms。
   - Router A收到对端发来F字段置位的控制报文。根据报文中的RX与本端的TX进行比较计算出新的时间间隔为150ms。
   - 定时器协商完成，双方的发送间隔和检测超时时间分别为150ms和450ms。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD基本配置

BFD参数配置

1. BFD支持基于FortiGate的2个层面进行参数的配置。
   - FortiGate全局（基于每VDOM）：

```bash
config system settings
    set bfd {enable | disable}
    set bfd-desired-min-tx <ms>
    set bfd-required-min-rx <ms>
    set bfd-detect-mult <multiplier>
    set bfd-dont-enforce-src-port {enable | disable}
end
```

     - `enable`：开启所有接口下的BFD配置（如果接口下的BFD配置为global）。
     - `disable`：关闭所有接口下的BFD配置（如果接口下的BFD配置为global）。
     - `bfd-desired-min-tx`：发送方支持的最小BFD控制报文发送时间间隔，单位为毫秒，默认为250ms。
     - `bfd-required-min-rx`：发送方支持的最小BFD控制报文接收时间间隔，单位为毫秒，默认为250ms。
     - `bfd-detect-mult`：检测时间倍数。
     - `bfd-dont-enforce-src-port`：开启后不强制验证BFD数据包的源端口（默认关闭）。
   - FortiGate接口，接口下的BFD开关有三种模式：

```bash
config system interface
    edit <interface-name>
        set bfd {global | enable | disable}
        set bfd-desired-min-tx <ms>
        set bfd-required-min-rx <ms>
        set bfd-detect-mult <multiplier>
    next
end
```

     - `global`：继承config system settings下的bfd开关（默认配置）。
     - `enable`：覆盖config system settings下的bfd开关，在此接口下开启BFD。
     - `disable`：覆盖config system settings下的bfd开关，在此接口下关闭BFD。
     - `bfd-desired-min-tx`：发送方支持的最小BFD控制报文发送时间间隔，单位为毫秒，默认为250ms。
     - `set bfd-required-min-rx`：发送方支持的最小BFD控制报文接收时间间隔，单位为毫秒，默认为250ms。
     - bfd-detect-mult：检测时间倍数。
2. 较低层级（接口）的配置可以覆盖较高层级（全局）的配置，例如在特定接口上配置BFD为enable后，配置的BFD参数会优先于全局下配置的BFD参数。

> **重要**
>
> FortiGate的BFD目前不支持BFD Echo模式。

BFD邻居配置

当BFD被静态路由引用时，需要通过配置BFD邻居来让BFD协议获取BFD邻居。

> **重要**
>
> 当BFD被动态路由如OSPF、BGP引用时，可以通过OSPF和BGP的邻居信息获取到BFD的邻居信息，不需要配置BFD邻居。

```bash
config router {bfd | bfd6}
    config neighbor
        edit <IP-address>
            set interface <interface-name>
        next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    end
end
```

BFD多跳配置

重要

该功能在7.2.0 GA及以后版本支持。

1. 默认配置下，不论是被OSPF、BGP还是静态路由引用，FortiGate的BFD邻居只支持直连网段的设备。如果FortiGate的BFD邻居不是直连网络的设备，需要在BFD下配置multihop-template，指定BFD流量的源（自身IP）和目的（邻居IP），这里配置的BFD邻居可以是多跳的不同网段的设备IP。
   - 当BFD被静态路由引用时，src和dst需要配置Host级别的netmask，IPv4为32位，IPv6为128位。
   - 当BFD被动态路由（如OSPF和BGP）引用时，src和dst可以配置为网段（包含BFD本地地址和邻居地址），如192.168.13.0/24，2100::/64，邻居地址通过动态路由协议获取。这样可以方便的配置多个BFD多跳邻居。
2. 同时可以在multihop-template中配置BFD的相关参数与认证功能，这些BFD参数（匹配模板的BFD流量）优先于接口及全局级别。
3. 在只有BFD多跳邻居的情况下，配置multihop-template后，不需要再配置BFD neighbor。

```bash
config router {bfd | bfd6}
    config multihop-template
        edit <ID>
            set src <IP address/netmask>
            set dst <IP address/netmask>
            set bfd-desired-min-tx <integer>
            set bfd-required-min-rx <integer>
            set bfd-detect-mult <integer>
            set auth-mode {none | md5}
            set md5-key <password>
        next
    end
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD与静态路由

当静态路由开启BFD后，BFD检测到BFD邻居故障时，BFD会从路由表中删除静态路由，如果路由的目的地恢复，则BFD将路由在路由表中恢复。

举例：添加两条目的相同但下一跳不同的启用BFD的静态路由。如果其中一条路由具有较高优先级，则所有匹配流量都使用该路由。如果BFD检测到高优先级路由到网关的链路故障，则将高优先级路由从路由表中删除，所有匹配的流量都使用低优先级路由。如果较高优先级路由到网关的链路恢复正常，BFD会将该路由重新添加到路由表中，所有匹配的流量都会切换为使用较高优先级路由。

FortiGate的BFD同时支持IPv4和IPv6的静态路由。

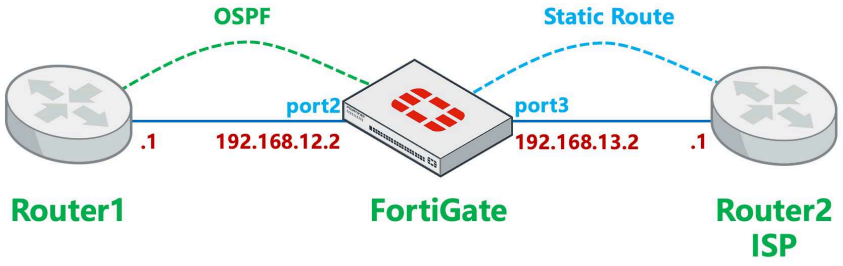
基本配置

当BFD被静态路由引用时，需要通过配置BFD邻居来让BFD协议获取BFD邻居信息。

```bash
config router {bfd | bfd6}
    config neighbor
        edit <IP-address>
            set interface <interface-name>
        next
    end
end
```

```bash
config router {static | static6}
    edit <sequence-number>
        set bfd {enable | disable}
        set device <gateway-out-interface>
    next
end
```

网络拓扑



- FortiGate与Router1建立OSPF邻居，并重发布静态路由。
- FortiGate与Router2（ISP）之间使用静态路由，并开启BFD，当BFD检测UP时，静态路由存在于FortiGate的路由表，会被重发布到OSPF；当BFD检测DOWN时，删除FortiGate上开启BFD的静态路由，不会重分发到OSPF。
- Router1配置与FortiGate的OSPF邻居。（略）

配置步骤

1. 配置网络接口IP（略）。

2. 配置FortiGate与Router1建立OSPF邻居，并重发布静态路由。

```bash
config router ospf
    set router-id 192.168.12.2
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 192.168.12.0 255.255.255.0
        next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    end
    config redistribute "static"
        set status enable
    end
end
```

3. 在FortiGate的port3上开启BFD，配置BFD邻居为Router2（ISP），并配置静态路由，去往ISP的两条静态路由开启BFD，去往内部网络的路由不开启BFD。

```bash
config system interface
    edit "port3"
        set ip 192.168.13.2 255.255.255.0
        set bfd enable
    next
end

config router bfd
    config neighbor
        edit 192.168.13.1
            set interface "port3"
        next
    end
end

config router static
    edit 1
        set dst 223.5.5.5 255.255.255.255
        set gateway 192.168.13.1
        set device "port3"
        set bfd enable
    next
    edit 2
        set dst 114.114.114.114 255.255.255.255
        set gateway 192.168.13.1
        set device "port3"
    next
    edit 3
        set dst 10.10.1.0 255.255.255.0
        set gateway 192.168.12.1
        set device "port2"
    next
end
```

结果验证

1. 在Router2还未配置BFD的状态下，查看FortiGate的BFD邻居和静态路由状态。BFD邻居状态为DOWN，开启BFD的静态路由未放入路由表，未开启BFD的静态路由被放入路由表。

> **重要**
>
> 与动态路由（如OSPF和BGP）不同，静态路由引用BFD时，静态路由是否放入路由表依赖于相关的BFD邻居状态，BFD邻居状态为UP时将开启BFD的相关静态路由放入路由表，BFD邻居状态为DOWN时将开启BFD的相关静态路由从路由表中移除（具体信息可见本章节最后的注意事项）。

```bash
FortiGate # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.13.2    192.168.13.1    DOWN        port3           1/1

FortiGate # get router info routing-table all
Routing table for VRF=0
S       10.10.1.0/24 [10/0] via 192.168.12.1, port2, [1/0]
S       114.114.114.114/32 [10/0] via 192.168.13.1, port3, [1/0]
C       192.168.12.0/24 is directly connected, port2
C       192.168.13.0/24 is directly connected, port3
```

2. 在Router2（ISP）上开启BFD功能后，再次查看FortiGate的BFD邻居和静态路由状态。BFD邻居状态为UP，开启BFD的静态路由被放入路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.13.2    192.168.13.1    UP          port3           1/1

FortiGate # get router info routing-table all
Routing table for VRF=0
S       10.10.1.0/24 [10/0] via 192.168.12.1, port2, [1/0]
S       114.114.114.114/32 [10/0] via 192.168.13.1, port3, [1/0]
C       192.168.12.0/24 is directly connected, port2
C       192.168.13.0/24 is directly connected, port3
S       223.5.5.5/32 [10/0] via 192.168.13.1, port3, [1/0]
```

3. FortiGate上的相关BFD日志与抓包如下所示，BFD邻居状态由Init变为UP。

```bash
date=2023-10-19 time=11:28:21 eventtime=1697686101603684308 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.13.2->192.168.13.1,49152,port3,1]: state INIT → UP local_diag=0×00"
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-10-19 11:28:11.613310	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
2	2023-10-19 11:28:16.618795	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
3	2023-10-19 11:28:21.602440	192.168.13.1	192.168.13.2	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
4	2023-10-19 11:28:21.603008	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Init, Flags: 0x00
5	2023-10-19 11:28:21.603554	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
6	2023-10-19 11:28:21.603708	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
7	2023-10-19 11:28:21.834751	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
8	2023-10-19 11:28:21.835450	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
9	2023-10-19 11:28:22.066236	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
10	2023-10-19 11:28:22.066481	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00

4. 模拟FortiGate与Router2之间的线路异常，查看FortiGate的BFD邻居和静态路由状态。BFD邻居状态为DOWN，开启BFD的静态路由未放入路由表，未开启BFD的静态路由仍然存在于路由表。

```bash
FortiGate # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.13.2    192.168.13.1    DOWN        port3           1/1

FortiGate # get router info routing-table all
Routing table for VRF=0
S       10.10.1.0/24 [10/0] via 192.168.12.1, port2, [1/0]
S       114.114.114.114/32 [10/0] via 192.168.13.1, port3, [1/0]
C       192.168.12.0/24 is directly connected, port2
C       192.168.13.0/24 is directly connected, port3
```

5. FortiGate上的相关BFD日志与抓包如下所示，BFD邻居状态由UP变为DWON，local_diag=0x01（表示Control Detection Time Expired）。

```bash
date=2023-10-19 time=15:06:50 eventtime=1697699210346884501 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.13.2->192.168.13.1,49152,port3,1]: state UP → DOWN local_diag=0×01"
```

29	2023-10-19 15:06:49.594358	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
30	2023-10-19 15:06:49.754854	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
31	2023-10-19 15:06:49.985309	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
32	2023-10-19 15:06:50.225972	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
33	2023-10-19 15:06:50.346924	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
34	2023-10-19 15:06:55.353093	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00

6. 恢复FortiGate与Router2之间的线路，查看FortiGate的BFD邻居和静态路由状态。BFD邻居状态变为UP，开启BFD的静态路由被放入路由表。

```bash
FortiGate # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.13.2    192.168.13.1    UP          port3           1/1

FortiGate # get router info routing-table all
Routing table for VRF=0
S       10.10.1.0/24 [10/0] via 192.168.12.1, port2, [1/0]
S       114.114.114.114/32 [10/0] via 192.168.13.1, port3, [1/0]
C       192.168.12.0/24 is directly connected, port2
C       192.168.13.0/24 is directly connected, port3
S       223.5.5.5/32 [10/0] via 192.168.13.1, port3, [1/0]
```

7. FortiGate上的相关BFD日志与抓包如下所示，BFD邻居状态由INIT变为UP。

```bash
date=2023-10-19 time=15:54:03 eventtime=1697702043275319216 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.13.2-
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
>192.168.13.1,49152,port3,1]: state INIT → UP local_diag=0×00"
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-10-19 15:53:51.267802	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
2	2023-10-19 15:53:53.389096	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
3	2023-10-19 15:53:58.395090	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
4	2023-10-19 15:54:03.274526	192.168.13.1	192.168.13.2	BFD Control	66	Diag: Control Detection Time Expired, State: Down, Flags: 0x00
5	2023-10-19 15:54:03.274666	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Init, Flags: 0x00
6	2023-10-19 15:54:03.275247	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
7	2023-10-19 15:54:03.276714	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
8	2023-10-19 15:54:03.477716	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
9	2023-10-19 15:54:03.498376	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00

8. 关闭Router2（由FortiGate模拟）的BFD功能，Router2会向FortiGate发送Administratively Down类型的BFD通知。

57	2023-10-19 16:45:49.942872	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
58	2023-10-19 16:45:49.983121	192.168.13.2	192.168.13.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
59	2023-10-19 16:45:50.153884	192.168.13.1	192.168.13.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
60	2023-10-19 16:45:50.213521	192.168.13.1	192.168.13.2	BFD Control	66	Diag: Administratively Down, State: AdminDown, Flags: 0x00
61	2023-10-19 16:45:50.213708	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Neighbor Signaled Session Down, State: Down, Flags: 0x00
62	2023-10-19 16:45:55.219047	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Neighbor Signaled Session Down, State: Down, Flags: 0x00
63	2023-10-19 16:46:00.224542	192.168.13.2	192.168.13.1	BFD Control	66	Diag: Neighbor Signaled Session Down, State: Down, Flags: 0x00

9. 查看FortiGate的BFD邻居和静态路由状态。BFD邻居状态变为DOWN，但开启BFD的静态路由没有从路由表中移除。

```bash
FortiGate # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.13.2    192.168.13.1    DOWN        port3           1/1

FortiGate # get router info routing-table all
Routing table for VRF=0
S       10.10.1.0/24 [10/0] via 192.168.12.1, port2, [1/0]
S       114.114.114.114/32 [10/0] via 192.168.13.1, port3, [1/0]
C       192.168.12.0/24 is directly connected, port2
C       192.168.13.0/24 is directly connected, port3
C       192.168.100.0/24 is directly connected, port1
S       223.5.5.5/32 [10/0] via 192.168.13.1, port3, [1/0]
```

10. FortiGate上的相关BFD日志与抓包如下所示，BFD邻居状态由UP变为DOWN，local_diag=0x23（表示Remote peer indicates restarting）。

```bash
date=2023-10-19 time=16:45:50 eventtime=1697705150213670782 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.13.2-
>192.168.13.1,49152,port3,1]: state UP → DOWN local_diag=0×23"
```

注意事项

1. 与动态路由协议（如OSPF和BGP）不同，静态路由没有对等体邻居发现的方法。因此，当配置了BFD时，静态路由网关的可达性完全取决于指定邻居的BFD会话的状态。
   - 当BFD邻居状态为DOWN，就认为静态路由的网关不可达，相关静态路由不会被安装在路由表中（不需要BFD邻居状态有一个从UP→DOWN的过程）。
   - 当BFD邻居状态为UP，就认为静态路由的网关可达，相关静态路由会被安装在路由表中。
   - 这是为了防止在FortiGate在HA环境下，BFD邻居状态为DOWN时，主备切换后，新主机将原主机已经从路由表中移除的静态路由错误地放入路由表。
2. 由于以上BFD与静态路由之间的特性，建议项目实施中配置静态路由与BFD时，在对端设备还未配置BFD的情况下，先不要在FortiGate的静态路由中开启BFD，等待对端设备完成BFD配置后，再将FortiGate的静态路由开启BFD，这样可以防止上述结果验证步骤1中初始状态下静态路由无法放入路由表的情况出现。
3. 对于动态路由（如OSPF和BGP），BFD必须要有一个从UP→DOWN的状态转换，才会执行邻居关系的重置。
4. 当开启BFD的静态路由已经放入路由表后，邻居不是因为链路故障DOWN，例如对端设备配置关闭BFD功能（向FortiGate发送了Administratively Down类型的BFD通知），或是修改FortiGate自身的BFD配置导致BFD邻居DOWN，这种情况下FortiGate不会将静态路由从路由表中移除。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD与OSPF

基本配置

> **重要**
>
> 必须配置并建立OSPF邻居后，BFD才能从OSPF获取BFD邻居信息，从而发送BFD报文。

1. 在OPSF中开启BFD。

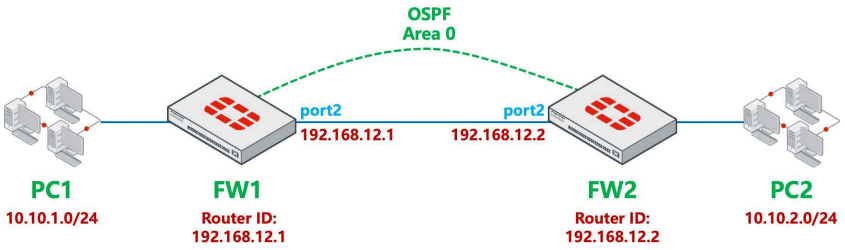
```bash
config router {ospf | ospf6}
    set bfd {enable | disable}
end
```

2. 也可以在特定的OSPF接口下开启BFD。

```bash
config router {ospf | ospf6}
    set bfd enable
    config {ospf-interface | ospf6-interface}
        edit <ID>
            set bfd {global | enable | disable}
            set area-id <IP address>
        next
    end
end
```

- global：继承config router ospf/ospf6下的BFD开关配置（注意不是继承config system setting下的BFD开关配置）。
- enable：仅在此接口下开启BFD，覆盖config router ospf/ospf6下的BFD开关配置。
- disable：在此接口下关闭BFD，覆盖config router ospf/ospf6下的BFD开关配置。

网络拓扑



- FW1与FW2建立IPv4的OSPF邻居。
- BFD检测失败时，重置OSPF邻居。

配置步骤

1. 基本网络配置（略）。

2. 在FW1和FW2的port2上分别开启BFD。

```bash
config system interface
    edit "port2"
        set bfd enable
    next
end
```

3. 在FW1和FW2上分别配置OSPF，配置OSPF邻居，宣告IPv4内网网段，在OSPF接口port2上开启BFD。

```bash
FW1:
config router ospf
    set router-id 192.168.12.1
    config area
        edit 0.0.0.0
        next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    end
    config ospf-interface
        edit "port2"
            set interface "port2"
            set bfd enable
        next
    end
    config network
        edit 1
            set prefix 192.168.12.0 255.255.255.0
        next
        edit 2
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```

bash

```
FW2:
config router ospf
    set router-id 192.168.12.2
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "port2"
            set interface "port2"
            set bfd enable
        next
    end
    config network
        edit 1
            set prefix 192.168.12.0 255.255.255.0
        next
        edit 2
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

结果验证

1. 在FW1上查看BFD邻居状态均为UP（FW2略）。

bash

```
FW1 # get router info bfd requests
BFD Peer Requests:
    client types(ct in 0x): 01=external 02=static
        04=ospf 08=bgp 10=pim-sm
src=192.168.12.1     dst=192.168.12.2     ct=04 ifi=4 type=S
```

bash

```
FW1 # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.12.1    192.168.12.2    UP          port2           1/4
```

2. 在FW1上查看BFD相关日志与抓包（FW2略），BFD状态由INIT变为UP。

bash

```
date=2023-10-20 time=15:45:27 eventtime=1697787926746001101 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.12.1-
>192.168.12.2,49152,port2,1]: state DOWN → UP local_diag=0×00"
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-10-20 15:45:18.856104	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Down, Flags: 0x00
2	2023-10-20 15:45:23.862082	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Down, Flags: 0x00
3	2023-10-20 15:45:26.533192	192.168.12.1	192.168.12.2	BFD Control	66	Diag: No Diagnostic, State: Down, Flags: 0x00
4	2023-10-20 15:45:26.533698	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Init, Flags: 0x00
5	2023-10-20 15:45:26.744988	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Init, Flags: 0x00
6	2023-10-20 15:45:26.746187	192.168.12.1	192.168.12.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
7	2023-10-20 15:45:26.747592	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
8	2023-10-20 15:45:26.967934	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
9	2023-10-20 15:45:26.978397	192.168.12.1	192.168.12.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
10	2023-10-20 15:45:27.160012	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在FW1上查看OSPF邻居与路由状态，邻居状态正常建立，OSPF路由学习正常。

```bash
FW1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.12.2      1   Full/DR         00:00:31    192.168.12.2    port2

FW1 # get router info routing-table ospf
Routing table for VRF=0
O       10.10.2.0/24 [110/2] via 192.168.12.2, port2, 00:02:50, [1/0]
```

4. 模拟线路问题10s（10s后恢复）导致BFD中断，查看FW1上BFD邻居消失（因为BFD DOWN后重置了OSPF连接，BFD邻居信息依赖于OSPF已建立的邻居信息）。

```bash
FW1 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
```

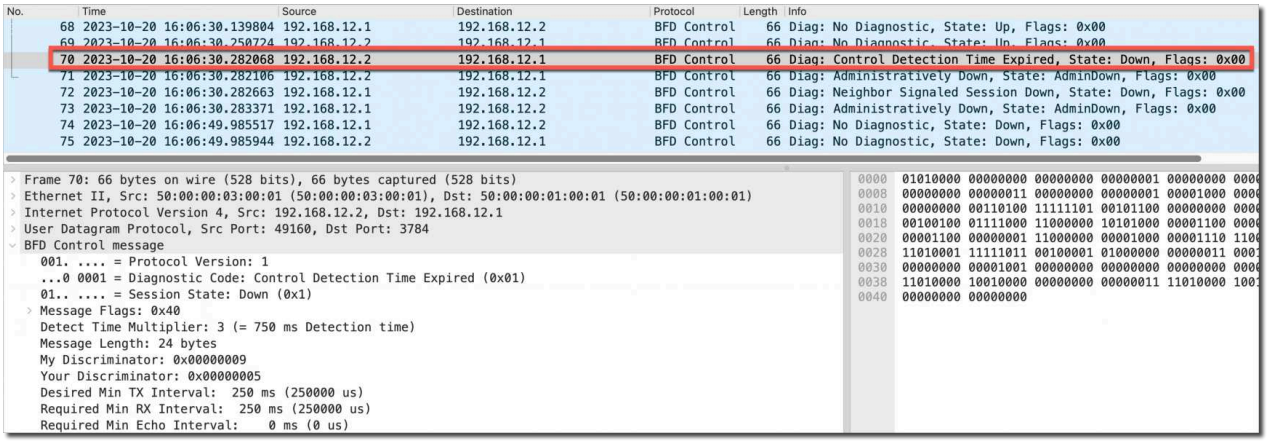
5. 在FW1上查看BFD相关日志，BFD DOWN后，对应的OSPF邻居关系跟随DOWN。local_diag=0x01（表示Control Detection Time Expired）。

```bash
date=2023-10-20 time=16:06:30 eventtime=1697789190283253338 tz="+0800" logid="0103020302" type="event"
subtype="router" level="warning" vd="root" logdesc="OSPF neighbor status changed" msg="OSPF: %OSPF-5-ADJCHANGE:
neighbor port2:192.168.12.1-192.168.12.2 Down "
date=2023-10-20 time=16:06:30 eventtime=1697789190282633679 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.12.1-
>192.168.12.2,49156,port2,5]: state UP → DOWN local_diag=0×01"
```

6. 在FW1上查看OSPF邻居状态，邻居断开，并开始重建OSPF邻居。

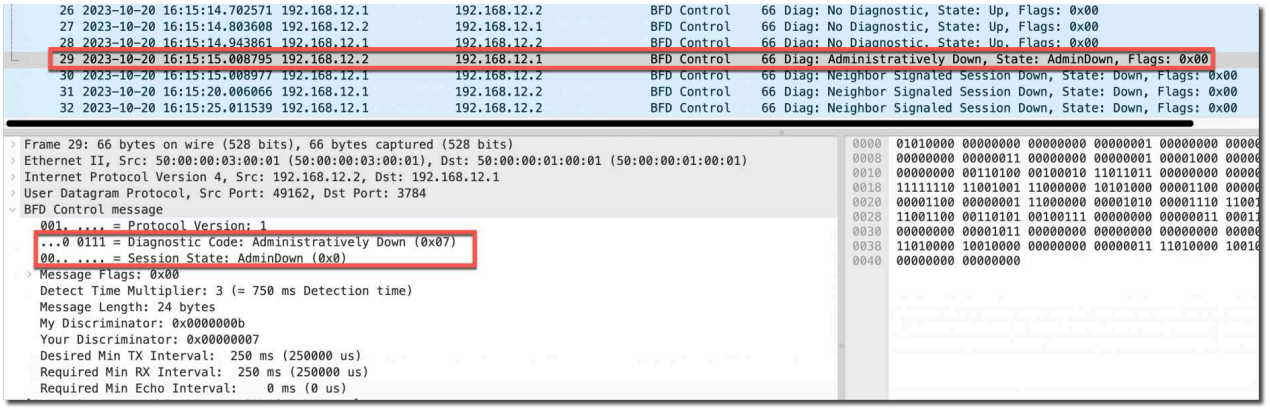
```bash
FW1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.12.2      1   Init/DROther    00:00:39    192.168.12.2    port2

FW1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.12.2      1   Full/Backup     00:00:37    192.168.12.2    port2
```

7. 抓包查看BFD DOWN的报文，FW2发现检测超时，向FW1发送BFD Time Expired报文，随后两端互相发送Admin DOWN的BFD控制报文，随后双向BFD字段中的Diagnostic Code为空，状态为DOWN。



8. 关闭FW2（由FortiGate模拟）的BFD功能，FW2会向FW1发送Administratively Down类型的BFD通知。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



9. 查看FortiGate的BFD邻居和OSPF状态。BFD邻居状态变为DOWN，但开启BFD的OSPF邻居没有重建。

```bash
FW1 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.12.1    192.168.12.2    DOWN        port2           7/11

FW1 # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.12.2      1   Full/DR         00:00:35    192.168.12.2    port2
```

0. FW1上的相关BFD日志如下所示，BFD邻居状态由UP变为DOWN，local_diag=0x23（表示Remote peer indicates restarting），路由事件日志中没有OSPF邻居断开的日志。

```bash
date=2023-10-20 time=16:15:15 eventtime=1697789715008917984 tz="+0800" logid="0103020304" type="event" subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.12.1->192.168.12.2,49158,port2,7]: state UP → DOWN local_diag=0×23"
```

注意事项

1. Admin类型的Down不会导致OSPF邻居重建。
2. BFD Down后触发了OSPF邻居重建，如果BFD一直没有UP，则重建后的OSPF邻居不会受任何影响，除非再次发生了BFD从UP到Down的状态转换（静态路由不是这样）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD与BGP

基本配置

> **重要**
>
> 必须配置并建立BGP邻居后，BFD才能从BGP获取BFD邻居信息，从而发送BFD报文。

在BGP中开启BFD。

```bash
config router bgp
    config neighbor
        edit <neighbor-IP-address>
            set bfd {enable | disable}
        next
    end
end
```

网络拓扑



- FW1与FW2建立IPv4的IBGP邻居。
- BFD检测失败时，重置BGP邻居。

配置步骤

1. 基本网络配置（略）。

2. 在FW1和FW2的port2上分别开启BFD。

```bash
config system interface
    edit "port2"
        set bfd enable
    next
end
```

3. 在FW1和FW2上分别配置BGP，配置BGP邻居，宣告IPv4内网网段，在BGP邻居中开启BFD。

```bash
FW1:
config router bgp
    set as 10086
    set router-id 192.168.12.1
    config neighbor
        edit "192.168.12.2"
            set bfd enable
            set remote-as 10086
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
    end
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW2:
config router bgp
    set as 10086
    set router-id 192.168.12.2
    config neighbor
        edit "192.168.12.1"
            set bfd enable
            set remote-as 10086
        next
    end
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
```

结果验证

1. 在FW1上查看BFD邻居状态均为UP（FW2略）。

```bash
FW1 # get router info bfd requests
BFD Peer Requests:
    client types(ct in 0x): 01=external 02=static
        04=ospf 08=bgp 10=pim-sm
src=192.168.12.1     dst=192.168.12.2     ct=08 ifi=4 type=SM
```

```bash
FW1 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.12.1    192.168.12.2    UP          port2           8/12
```

2. 在FW1上查看BFD相关日志与抓包（FW2略），BFD状态由INIT变为UP。

```bash
date=2023-10-20 time=16:31:11 eventtime=1697790670835673328 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.12.1-
>192.168.12.2,49159,port2,8]: state INIT → UP local_diag=0×00"
```



No.	Time	Source	Destination	Protocol	Length	Info
1	2023-10-20 16:31:01.021260	192.168.12.1	192.168.12.2	BFD Control	66	Diag: Neighbor Signaled Session Down, State: Down, Flags: 0x00
2	2023-10-20 16:31:06.026305	192.168.12.1	192.168.12.2	BFD Control	66	Diag: Neighbor Signaled Session Down, State: Down, Flags: 0x00
3	2023-10-20 16:31:10.644666	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Down, Flags: 0x00
4	2023-10-20 16:31:10.644821	192.168.12.1	192.168.12.2	BFD Control	66	Diag: No Diagnostic, State: Init, Flags: 0x00
5	2023-10-20 16:31:10.835155	192.168.12.1	192.168.12.2	BFD Control	66	Diag: No Diagnostic, State: Init, Flags: 0x00
6	2023-10-20 16:31:10.835587	192.168.12.2	192.168.12.1	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00
7	2023-10-20 16:31:10.835685	192.168.12.1	192.168.12.2	BFD Control	66	Diag: No Diagnostic, State: Up, Flags: 0x00

3. 在FW1上查看BGP邻居与路由状态，邻居状态正常建立，BGP路由学习正常。

```bash
FW1 # get router info bgp summary
VRF 0 BGP router identifier 192.168.12.1, local AS number 10086
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2 4      10086      11      11        1    0    0 00:06:44        1
Total number of neighbors 1

FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [200/0] via 192.168.12.2 (recursive is directly connected, port2), 00:06:27, [1/0]
```

4. 模拟线路问题10s（10s后恢复）导致BFD中断，中断过程中查看FW1上BFD邻居消失（因为BFD DOWN后重置了BGP连接，BFD邻居信息依赖于BGP已建立的邻居信息）。

```bash
FW1 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
```

5. 在FW1上查看BFD相关日志，BFD DOWN后，对应的BGP邻居关系跟随DOWN。local_diag=0x01（表示Control Detection Time Expired）。

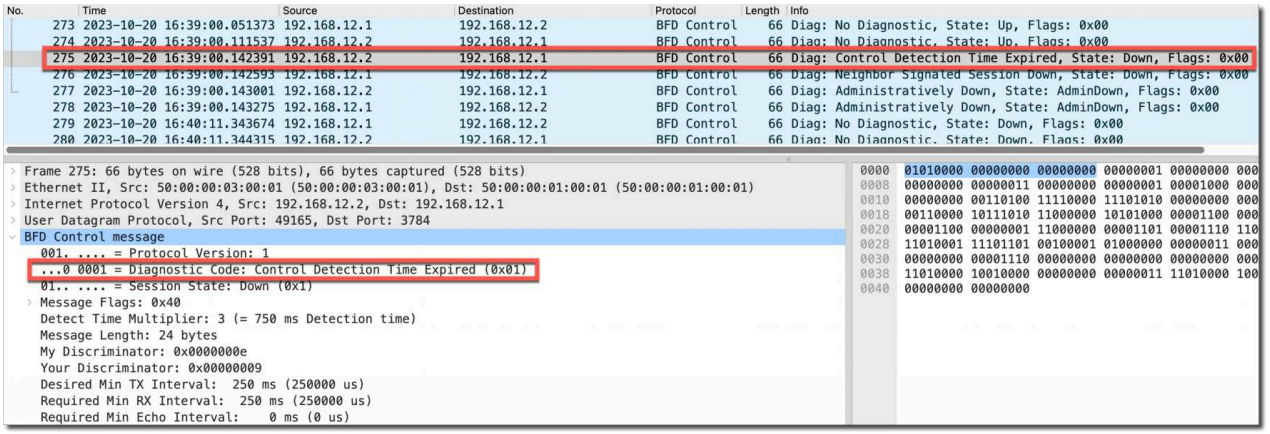
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
date=2023-10-20 time=16:39:00 eventtime=1697791140142880643 tz="+0800" logid="0103020300" type="event"
subtype="router" level="warning" vd="root" logdesc="BGP neighbor status changed" msg="BGP: %BGP-5-ADJCHANGE: VRF 0
neighbor 192.168.12.2 Down BFD Down; User reset added"
date=2023-10-20 time=16:39:00 eventtime=1697791140142553520 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.12.1-
>192.168.12.2,49160,port2,9]: state UP → DOWN local_diag=0×01"
```
bash

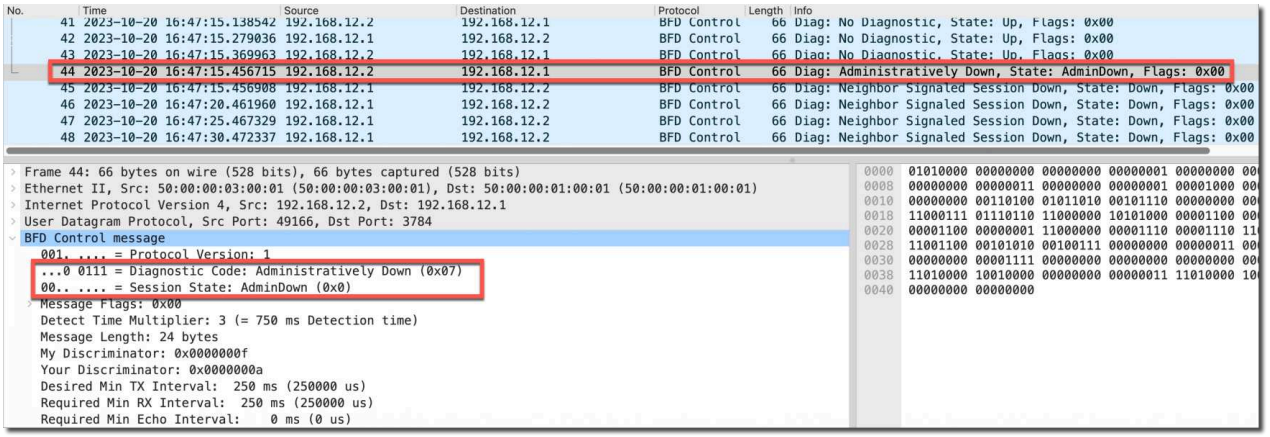
6. 在FW1上查看BGP邻居状态，邻居断开，并开始重建BGP邻居。

```
FW1 # get router info bgp summary
VRF 0 BGP router identifier 192.168.12.1, local AS number 10086
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries
Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2 4      10086      18      19        0    0    0    never Connect
Total number of neighbors 1

FW1 # get router info bgp summary
VRF 0 BGP router identifier 192.168.12.1, local AS number 10086
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries
Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2 4      10086      21      22        3    0    0 00:00:27        1
Total number of neighbors 1
```
bash

7. 抓包查看BFD DOWN的报文，FW2发现检测超时，向FW1发送BFD Time Expired报文，随后两端互相发送Admin DOWN的BFD控制报文，随后双向BFD字段中的Diagnostic Code为空，状态为DOWN。



8. 关闭FW2（由FortiGate模拟）的BFD功能，FW2会向FW1发送Administratively Down类型的BFD通知。



9. 查看FortiGate的BFD邻居和BGP状态。BFD邻居状态变为DOWN，但开启BFD的BGP邻居没有重建。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW1 # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
192.168.12.1    192.168.12.2    DOWN        port2           10/15

FW1 # get router info bgp summary
VRF 0 BGP router identifier 192.168.12.1, local AS number 10086
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries
Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.12.2 4      10086      30      31        3    0    0 00:08:37        1
Total number of neighbors 1
```

0. FW1上的相关BFD日志如下所示，BFD邻居状态由UP变为DOWN，local_diag=0x23（表示Remote peer indicates restarting），路由事件日志中没有BGP邻居断开的日志。

```bash
date=2023-10-20 time=16:47:15 eventtime=1697791635456872179 tz="+0800" logid="0103020304" type="event" subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[192.168.12.1->192.168.12.2,49161,port2,A]: state UP → DOWN local_diag=0×23"
```

注意事项

1. Admin类型的Down不会导致BGP邻居重建。
2. BFD Down后触发了BGP邻居重建，如果BFD一直没有UP，则重建后的BGP邻居不会受任何影响，除非再次发生了BFD从UP到Down的状态转换（静态路由不是这样）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

BFD多跳模式

重要

该功能在7.2.0 GA及以后版本支持。

功能介绍

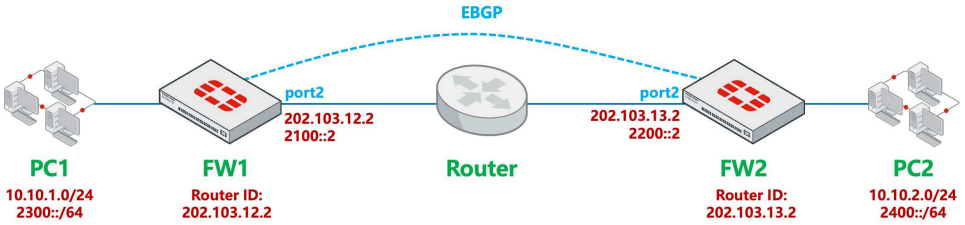
1. 默认配置下，不论是被OSPF、BGP还是静态路由引用，FortiGate的BFD邻居只支持直连网段的设备。如果FortiGate的BGP邻居不是直连网络的设备，需要在BFD下配置multihop-template，指定BFD流量的源（自身IP）和目的（邻居IP），这里配置的BFD邻居可以是多跳的不同网段的设备IP。
   - 当BFD被静态路由引用时，src和dst需要配置Host级别的netmask，IPv4为32位，IPv6为128位。
   - 当BFD被动态路由（如OSPF和BGP）引用时，src和dst可以配置为网段（包含BFD本地地址和邻居地址），如192.168.13.0/24，2100::/64，邻居地址通过动态路由协议获取。这样可以方便的配置多个BFD多跳邻居。
   - 不支持OSPF和静态路由的BFD多跳模式（OSPF邻居本来就必须直连建立）。

2. 同时可以在multihop-template中配置BFD的相关参数与认证功能，这些BFD参数（匹配模板的BFD流量）优先于接口及全局级别。

3. 在只有BFD多跳邻居的情况下，配置multihop-template后，不需要再配置BFD neighbor。

```bash
config router {bfd | bfd6}
    config multihop-template
        edit <ID>
            set src <IP address/netmask>
            set dst <IP address/netmask>
            set bfd-desired-min-tx <integer>
            set bfd-required-min-rx <integer>
            set bfd-detect-mult <integer>
            set auth-mode {none | md5}
            set md5-key <password>
        next
    end
end
```

网络拓扑



- FW1与FW2建立IPv4与IPv6的EBGP邻居，网段非直连。
- FW1与FW2之间的IPv4/IPv6 EBGP邻居启用多跳BFD。

配置步骤

1. 基础网络配置（略）。

2. 在FW1和FW2的port2上分别开启BFD，并分别配置IPv4和IPv6的多跳BFD模版（多跳环境下必须配置）。

```bash
config system interface
    edit "port2"
        set bfd enable
    next
end
```

```bash
FW1:
config router bfd
    config multihop-template
        edit 1
            set src 202.103.12.0 255.255.255.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set dst 202.103.13.0 255.255.255.0
        next
    end
end
config router bfd6
    config multihop-template
        edit 1
            set src 2100::/64
            set dst 2200::/64
        next
    end
end
```

bash

```
FW2:
config router bfd
    config multihop-template
        edit 1
            set src 202.103.13.0 255.255.255.0
            set dst 202.103.12.0 255.255.255.0
        next
    end
end
config router bfd6
    config multihop-template
        edit 1
            set src 2200::/64
            set dst 2100::/64
        next
    end
end
```

3. 在FW1和FW2上分别配置BGP，配置EBGP邻居（包含IPv4和IPv6），宣告IPv4和IPv6内网网段。

bash

```
FW1:
config router bgp
    set as 10086
    set router-id 202.103.12.2
    config neighbor
        edit "202.103.13.2"
            set bfd enable
            set ebgp-enforce-multihop enable
            set remote-as 10010
        next
        edit "2200::2"
            set bfd enable
            set ebgp-enforce-multihop enable
            set remote-as 10010
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
    end
    config network6
        edit 1
            set prefix6 2300::/64
        next
    end
end
```

bash

```
FW2:
config router bgp
    set as 10010
    set router-id 202.103.13.2
    config neighbor
        edit "202.103.12.2"
            set bfd enable
            set ebgp-enforce-multihop enable
            set remote-as 10086
        next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        edit "2100::2"
            set bfd enable
            set ebgp-enforce-multihop enable
            set remote-as 10086
        next
    end
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
    config network6
        edit 1
            set prefix6 2400::/64
        next
    end
end
```

结果验证

1. 在FW1上查看BFD IPv4和IPv6邻居状态均为UP（FW2略）。

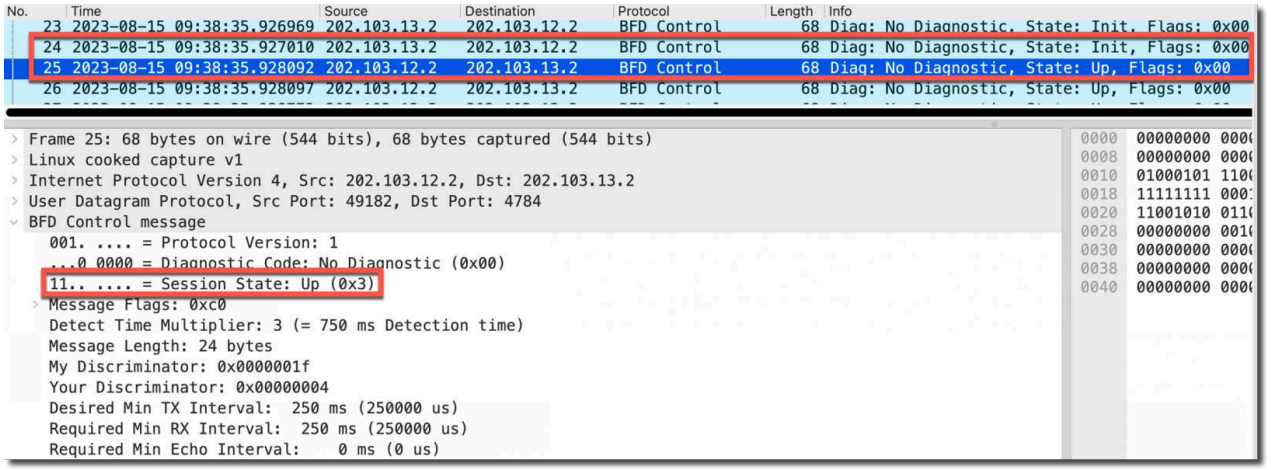
```bash
FW1 # get router info bfd requests
BFD Peer Requests:
    client types(ct in 0x): 01=external 02=static
        04=ospf 08=bgp 10=pim-sm
src=202.103.12.2     dst=202.103.13.2     ct=08 ifi=4 type=SM

FW1 # get router info6 bfd requests
BFD Peer Requests:
    client types(ct in 0x): 01=external 02=static
        04=ospf 08=bgp 10=pim-sm
src=2100::2
dst=2200::2
ct=08 ifi=4 type=SM
```

```bash
FW1 # get router info bfd neighbor
OurAddress      NeighAddress    State       Interface       LDesc/RDesc
202.103.12.2    202.103.13.2    UP          port2           3/4/M

OurAddress: 2100::2FW1 # get router info6 bfd neighbor
NeighAddress: 2200::2
State: UP Interface: port2 Desc: 4/3 Multi-hop
```

2. 在FW1上查看BFD相关日志与抓包（FW2略），IPv4和IPv6的BFD状态由INIT变为UP。

```bash
date=2023-08-14 time=17:07:51 eventtime=1692004071014368092 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[202.103.12.2-
>202.103.13.2,49154,port2,3,multi]: state INIT → UP local_diag=0×00"

date=2023-08-14 time=17:07:51 eventtime=1692004070970891127 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[2100::2-
>2200::2,49155,port2,4,multi]: state INIT → UP local_diag=0×00"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在FW1上查看IPv4和IPv6的BGP邻居与BGP路由状态，邻居状态正常建立，IPv4和IPv6的BGP路由学习正常。

```bash
FW1 # get router info bgp summary
VRF 0 BGP router identifier 202.103.12.2, local AS number 10086
BGP table version is 1
3 BGP AS-PATH entries
0 BGP community entries
Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/DOWN  State/PfxRcd
202.103.13.2 4      10010      35      37        1    0    0 00:27:54        1
2200::2      4      10010      36      36        1    0    0 00:26:57        1

Total number of neighbors 2

FW1 # get router info routing-table bgp
Routing table for VRF=0
B       10.10.2.0/24 [20/0] via 202.103.13.2 (recursive via 202.103.12.1, port2), 00:27:31, [1/0]

FW1 # get router info6 routing-table bgp
Routing table for VRF=0
B       2400::/64 [20/0] via 2200::2 (recursive via 2100::1, port2), 00:27:34, [1024/0]
```

4. 模拟IPv6的BFD中断，查看FW1上BFD IPv6邻居DOWN。

```bash
FW1 # get router info6 bfd neighbor

OurAddress: 2100::2
NeighAddress: 2200::2
State: DOWN Interface: port2 Desc: 10/12 Multi-hop
```

5. 在FW1上查看BFD相关日志，BFD DOWN后，对应的IPv6 BGP邻居关系跟随DOWN。

```bash
date=2023-08-14 time=17:33:33 eventtime=1692005613533793725 tz="+0800" logid="0103020300" type="event"
subtype="router" level="warning" vd="root" logdesc="BGP neighbor status changed" msg="BGP: %BGP-5-ADJCHANGE: VRF 0
neighbor 2200::2 DOWN User reset"
date=2023-08-14 time=17:33:33 eventtime=1692005613533476560 tz="+0800" logid="0103020300" type="event"
subtype="router" level="warning" vd="root" logdesc="BGP neighbor status changed" msg="BGP: %BGP-5-ADJCHANGE: VRF 0
neighbor 2200::2 DOWN BGP Notification CEASE"
......
date=2023-08-14 time=17:33:33 eventtime=1692005613533219142 tz="+0800" logid="0103020300" type="event"
subtype="router" level="warning" vd="root" logdesc="BGP neighbor status changed" msg="BGP: %BGP-5-ADJCHANGE: VRF 0
neighbor 2200::2 DOWN BFD DOWN; User reset added"
date=2023-08-14 time=17:33:33 eventtime=1692005613532847101 tz="+0800" logid="0103020304" type="event"
subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[2100::2-
>2200::2,49155,port2,4,multi]: state UP → DOWN local_diag=0×01"
```

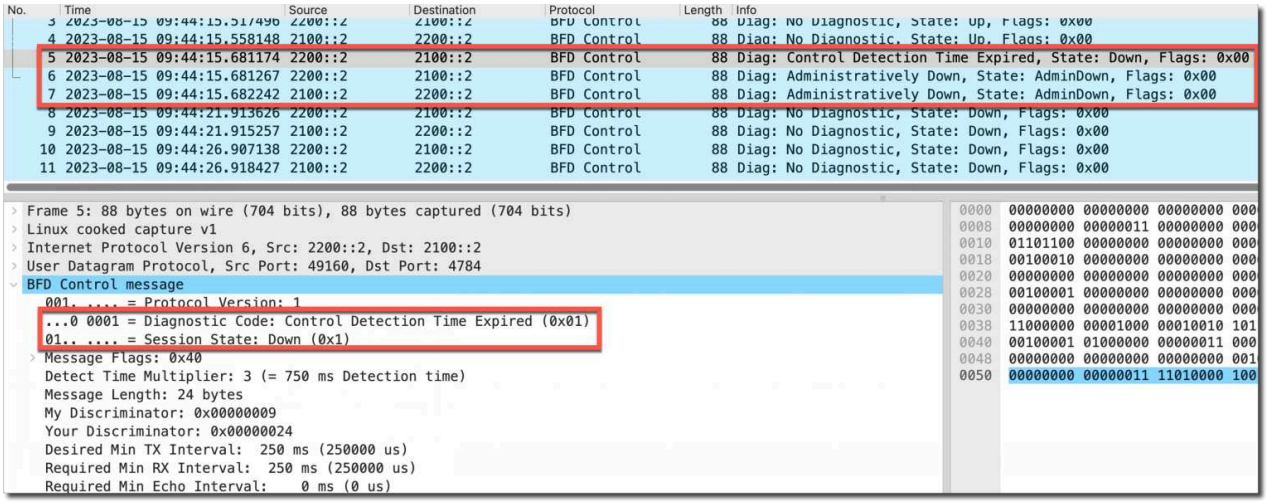
6. 在FW1上查看IPv4和IPv6的BGP邻居状态，IPv6邻居断开，并开始重建EBGP邻居。

```bash
FW1 # get router info bgp summary
VRF 0 BGP router identifier 202.103.12.2, local AS number 10086
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/DOWN  State/PfxRcd
202.103.13.2 4      10010     113     114        1    0    0 01:24:53        1
2200::2      4      10010     111     113        0    0    0    never Active
Total number of neighbors 2

FW1 # get router info bgp summary
VRF 0 BGP router identifier 202.103.12.2, local AS number 10086
BGP table version is 2
3 BGP AS-PATH entries
0 BGP community entries
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/DOWN  State/PfxRcd
202.103.13.2 4      10010     114     115        1    0    0 01:25:49        1
2200::2      4      10010     116     119        2    0    0 00:00:55        1
```

7. 抓包查看IPv6 BFD DOWN的报文，FW2发现检测超时，向FW1发送BFD Time Expired报文，两端互相发送AdminDOWN的BFD控制报文，随后双向BFD字段中的Diagnostic Code为空，状态为DOWN。



8. 在FW1上删除IPv4的BFD多跳模版，模拟未配置多跳模板情况下的BFD多跳状态。

```bash
FW1 # config router bfd
FW1 (bfd) # config multihop-template
FW1 (multihop-template) # delete 1
FW1 (multihop-template) # end
FW1 (bfd) # end
```

9. 查看FW1和FW2上的IPv4 BFD邻居状态，均变为DOWN。

```bash
FW1 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
202.103.12.2    202.103.13.2    DOWN        port2           16/0

FW2 # get router info bfd neighbor

OurAddress      NeighAddress    State       Interface       LDesc/RDesc
202.103.13.2    202.103.12.2    DOWN        port2           8/17/M
```

0. FW1和FW2的IPv4 BGP邻居都没有发生重建。

```bash
FW1 # get router info bgp summary

VRF 0 BGP router identifier 202.103.12.2, local AS number 10086
BGP table version is 2
3 BGP AS-PATH entries
0 BGP community entries
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.13.2 4      10010     123     124        1    0    0 01:32:59        1
2200::2      4      10010     124     127        2    0    0 00:08:05        1

FW2 # get router info bgp summary

VRF 0 BGP router identifier 202.103.13.2, local AS number 10010
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
BGP table version is 6
3 BGP AS-PATH entries
0 BGP community entries
Neighbor     V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
202.103.12.2 4      10086     215     216        5    0    0 01:41:32        1
2100::2      4      10086     193     203        6    0    0 00:16:37        1
```

1. 在FW1上查看路由相关日志，显示IPv4 BFD为Admin Down，后续没有IPv4 BGP断开的日志。

```
date=2023-08-14 time=19:40:54 eventtime=1692013254437017862 tz="+0800" logid="0103020304" type="event" subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[202.103.12.2->202.103.13.2,49168,port2,11,multi]: state UP → ADMIN DOWN local_diag=0×27"
```

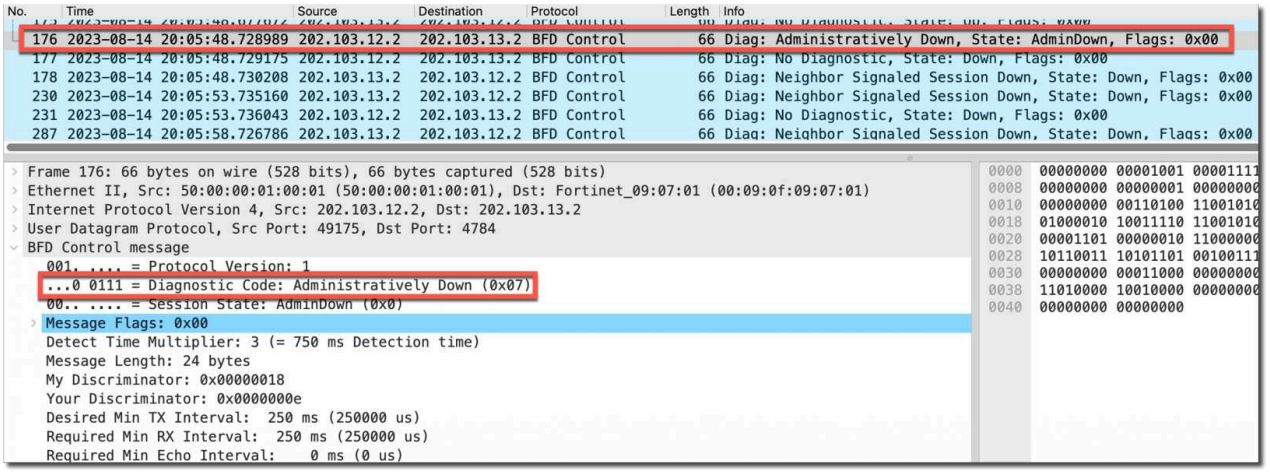
bash

2. 在FW2上查看路由相关日志，显示IPv4 BFD Down，后续没有也IPv4 BGP断开的日志。

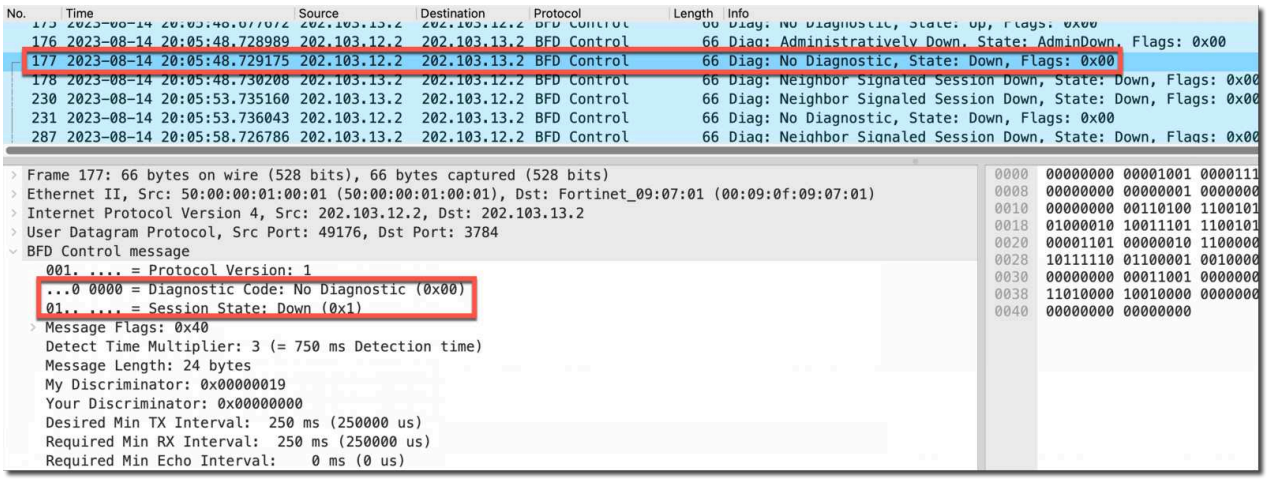
```
date=2023-08-14 time=19:40:54 eventtime=1692013254462567015 tz="+0800" logid="0103020304" type="event" subtype="router" level="warning" vd="root" logdesc="Routing log warning" msg="BFD: BFD session[202.103.13.2->202.103.12.2,49159,port2,8,multi]: state UP → DOWN local_diag=0×23"
```

bash

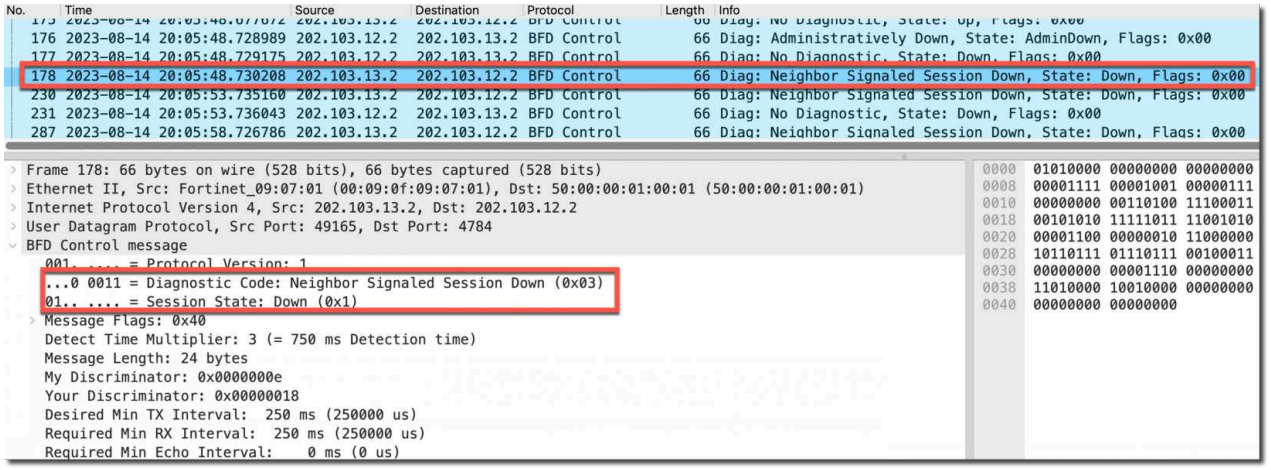
3. 同时抓包查看IPv4的BFD，FW1向FW2发送了Administratively Down类型的BFD。



4. 随后FW1→FW2方向的BFD Down中的Diagnostic Code变为空，FW2→FW1方向的BFD Down中的Diagnostic Code变为Neighbor Signaled Session Down。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



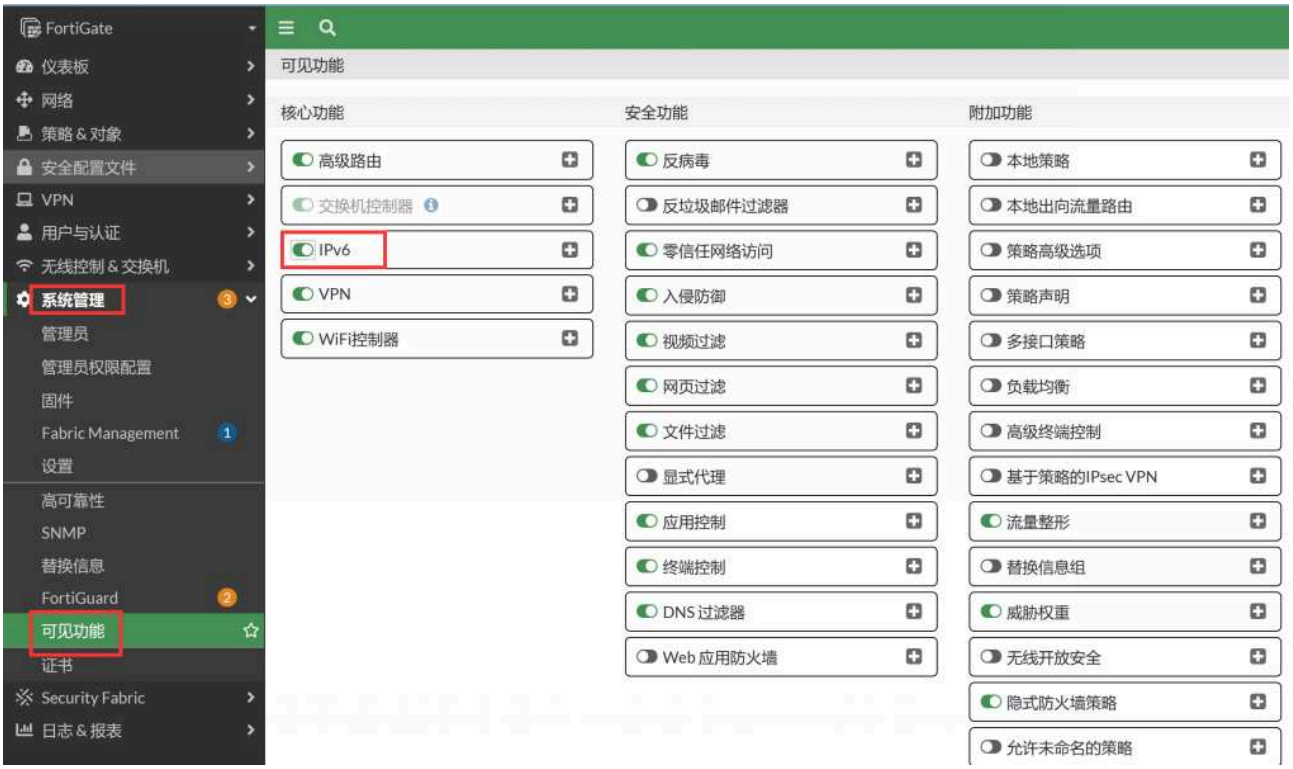
注意事项

1. Admin类型的Down不会导致BGP邻居重建。
2. BFD Down后触发了BGP邻居重建，如果BFD一直没有UP，则重建后的BGP邻居不会受任何影响，除非再次发生了BFD从UP到Down的状态转换（静态路由不是这样）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

页面开启IPv6

需要使用IPv6时，需要在系统管理→可见功能中开启IPv6。




```bash
config system global
    set gui-ipv6 enable
end
```

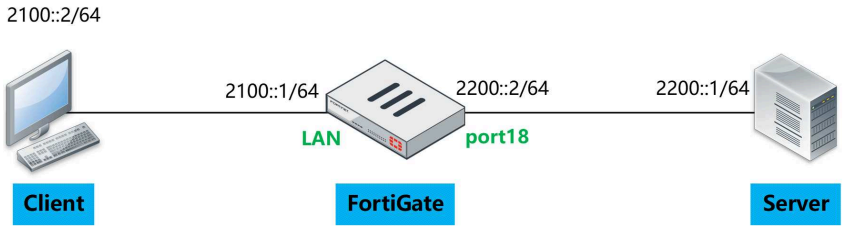

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

上网配置

网络需求

1. 用户内部使用IPv6网络，FortiGate作为客户网络的互联网边界介入防火墙，实现对互联网的访问。
2. 外部互联网接入服务商为IPv6网络。
3. 内部也为IPv6网络。

网络拓扑



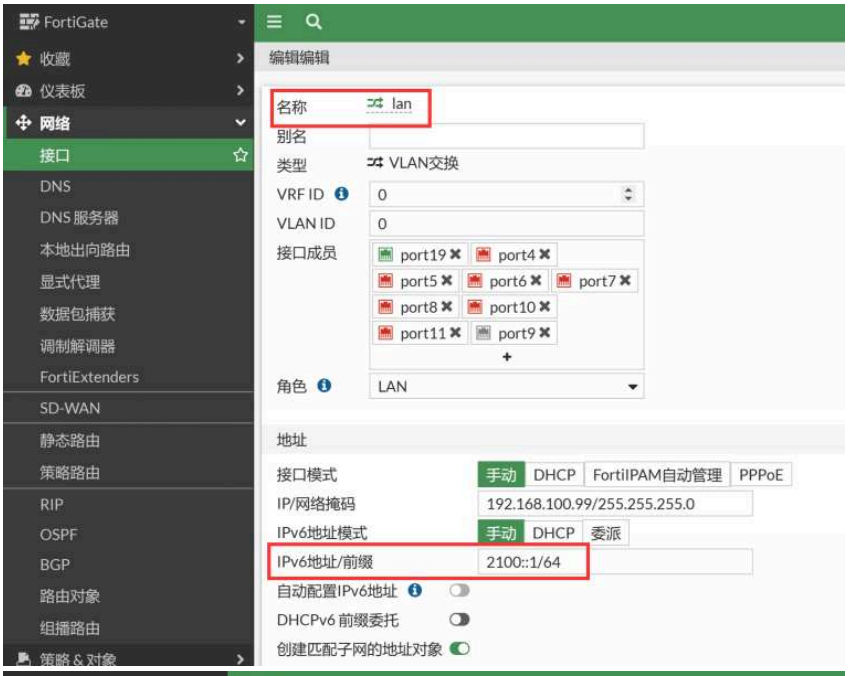
配置要点

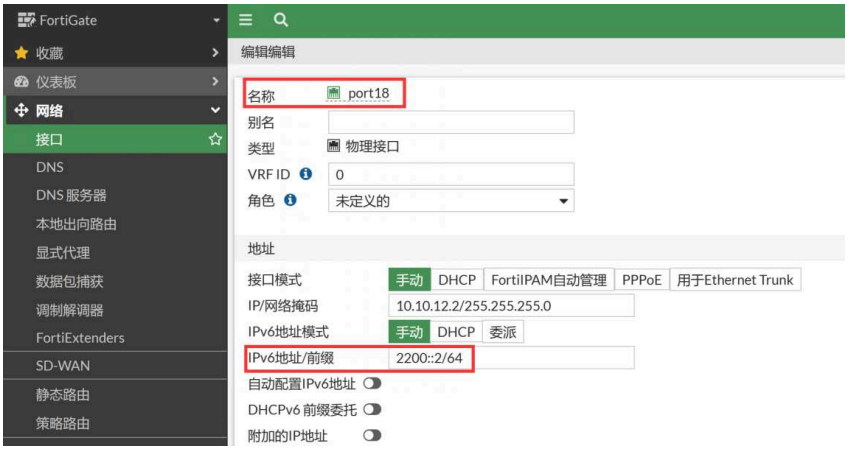
- 配置接口IP
- 配置路由
- 配置策略

配置步骤

1. 配置接口IPv6地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

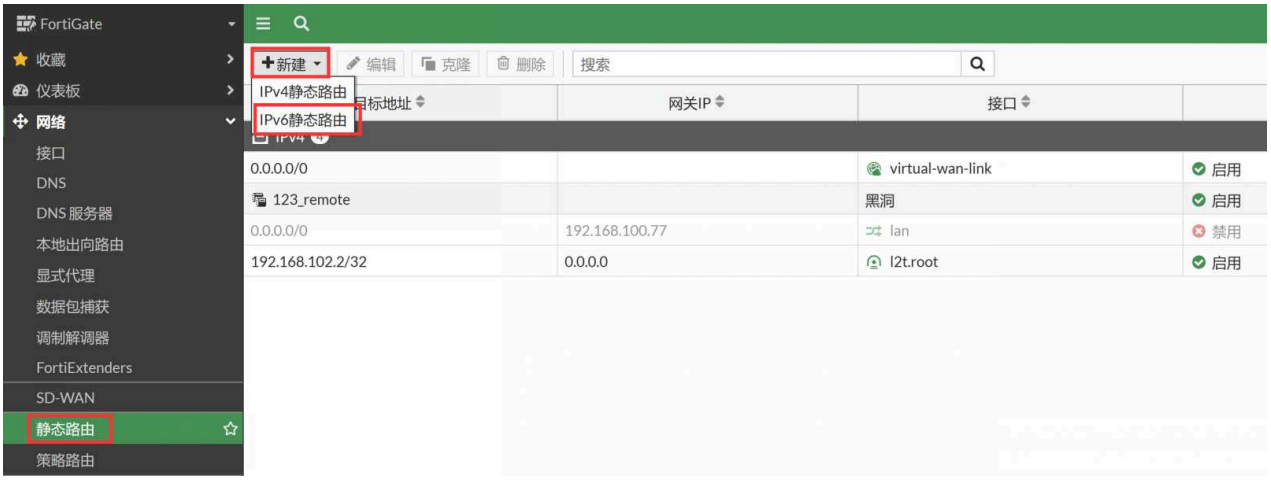


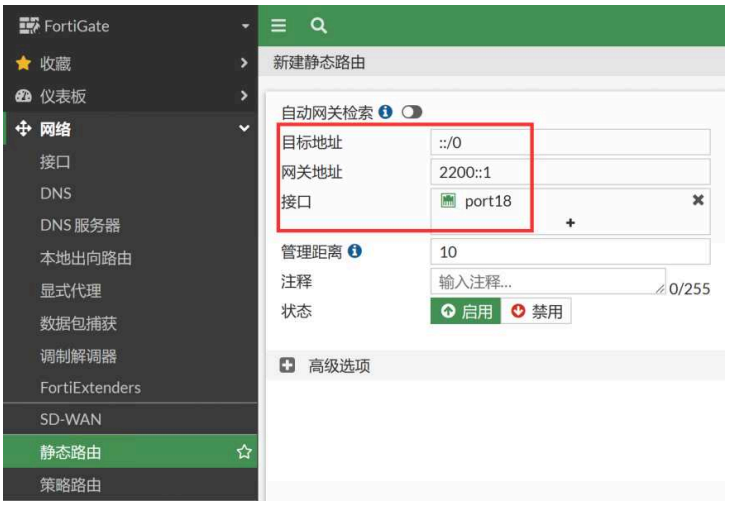



```
config system interface
    edit "lan"
        config ipv6
            set ip6-address 2100::1/64
            set ip6-allowaccess ping https ssh snmp http fgfm fabric
        end
    next
    edit "port18"
        config ipv6
            set ip6-address 2200::2/64
            set ip6-allowaccess ping https ssh snmp http fgfm fabric
        end
    next
end
```

2. 配置IPv6路由。

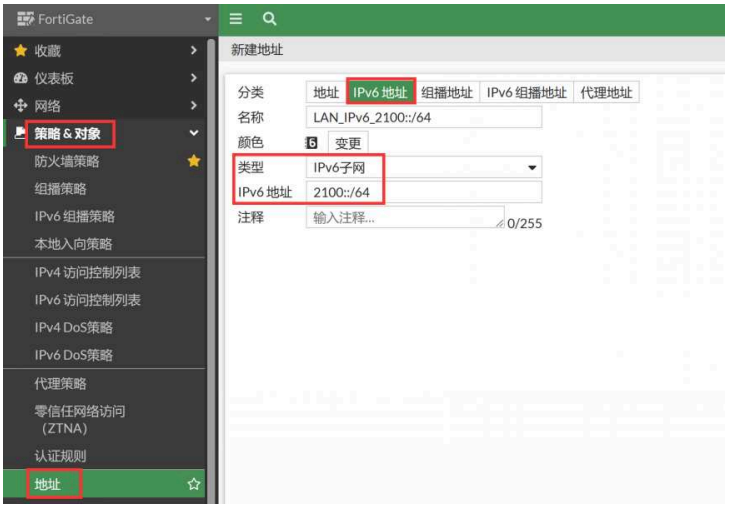
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
config router static6
    edit 1
        set gateway 2200::1
        set device "port18"
    next
end
```

3. 创建内网网段的IPv6地址对象，进入策略&对象→地址，新建内网的IPv6地址对象。

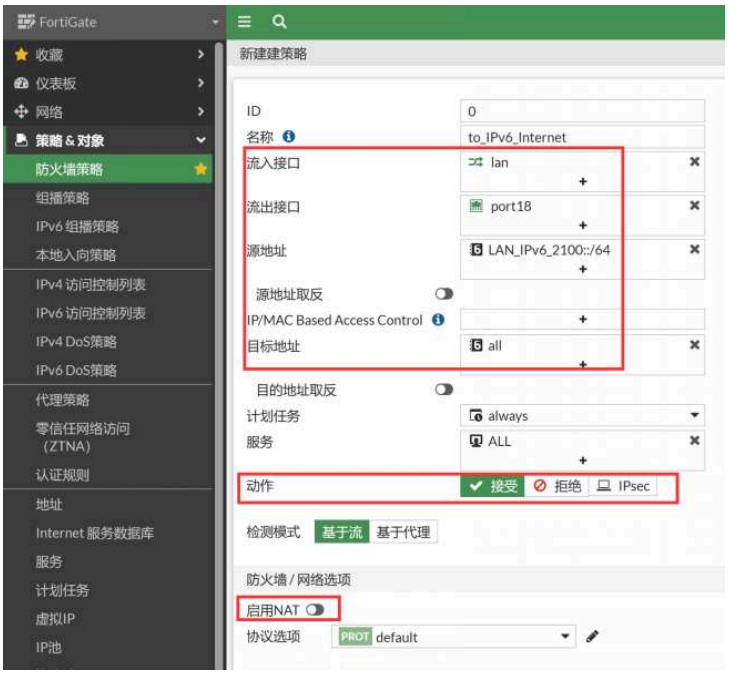



```
config firewall address6
    edit "LAN_IPv6_2100::/64"
        set uuid 042a2792-8d96-51ed-39e3-a512a3f5e16d
        set ip6 2100::/64
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end
```

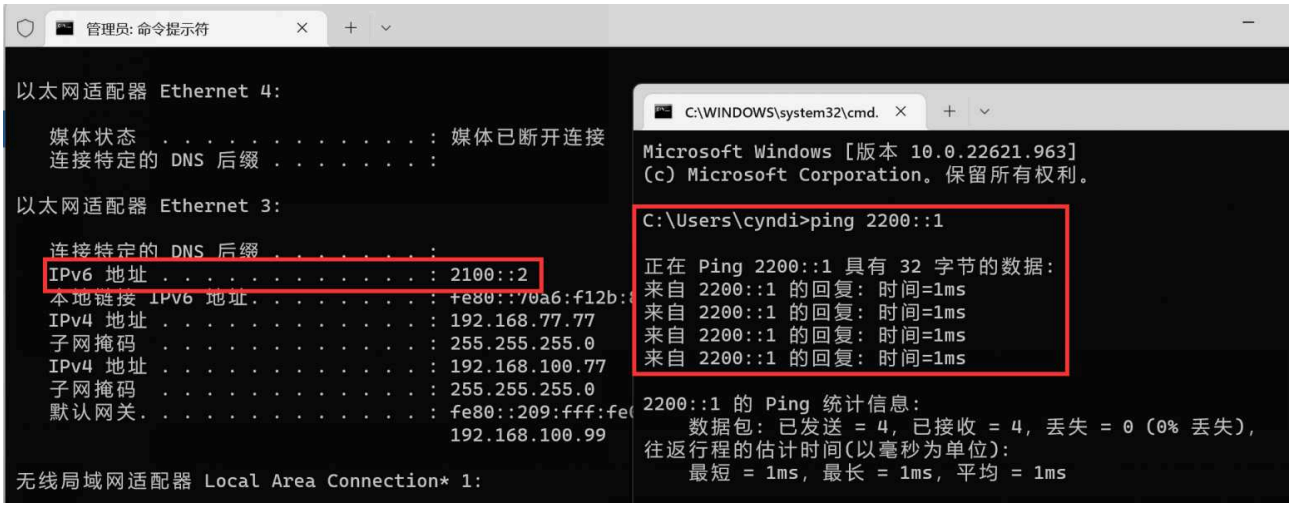
4. 新建防火墙策略，允许内部IPv6访问外部IPv6网络，由于都是IPv6地址，可以直接通信，不需要开启NAT。




```
config firewall policy
    edit 10
        set name "to_IPv6_Internet"
        set srcintf "lan"
        set dstintf "port18"
        set action accept
        set srcaddr6 "LAN_IPv6_2100::/64"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
    next
end
```

结果验证

客户端PC可以通过FortiGate正常访问IPv6 Internet。



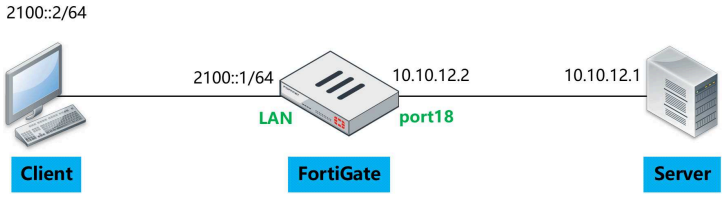
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NAT64映射

网络需求

将IPv4内部服务器，发布到IPv6网络之中，允许用户通过IPv6来对其进行访问。

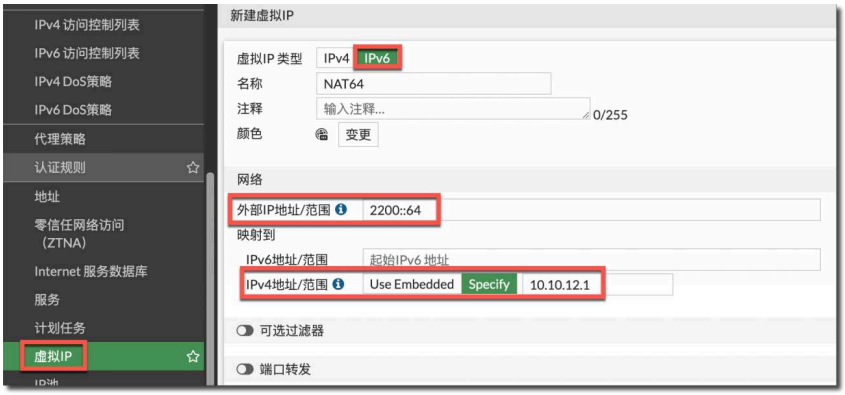
网络拓扑



Client侧为IPv6，Server侧为IPv4，使用Client访问Server，FortiGate做NAT64转换。

配置步骤

1. 创建VIP，选择类型为IPv6，“映射到”填写IPv4 Server真实地址，“外部IP地址/范围”填写IPv6 VIP地址，NAT64 VIP的外部地址如果是一个范围，必须填写为一个完整的subnet，否则GUI报错。




```
config firewall vip6
    edit "NAT64"
        set extip 2200::64
        set nat66 disable
        set nat64 enable
        set ipv4-mappedip 10.10.12.1
        set add-nat64-route enable
    next
end
```

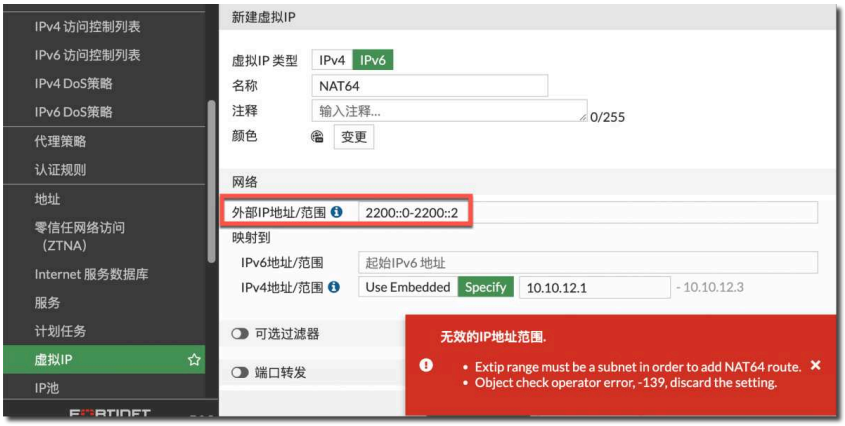
2. 可以看默认存在一个naf.root接口，用于处理NAT64流量，创建VIP完成后，如果开启了add-nat64-route（默认开启），针对naf.root接口生成去往VIP IPv6地址的路由，关闭add-nat64-route后，该路由会消失。

```
FortiGate-101F # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

```
FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=11(zebra) flag=00000000 prio=1024 dst:2200::64/128 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

3. 注意：如果是NAT64 VIP，“外部IP范围”配置的不是一个完整的subnet，或范围中包含subnet的广播地址，则下发时页面或CLI会报错，因为无法为naf接口下发路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 创建IPv4 Pool，配置地址池范围，注意不要和port18地址冲突，配置冲突这里并不会提示，后续会讲到为什么不能配成一样的，开启NAT64后，须填写为一个完整的subnet（最小32位）的IPv4地址范围，否则GUI报错。




```
config firewall ippool
    edit "NAT64"
        set startip 10.10.200.0
        set endip 10.10.200.127
        set nat64 enable
        set add-nat64-route enable
    next
end
```

5. 创建完成后，如果开启了add-nat64-route（默认开启），可以看到生成了IPv4的kernel路由，针对naf.root接口生成去往IPPool IPv4地址的路由，IPPool关闭NAT64或关闭add-nat64-route后，该路由会消失。

```
FortiGate # get router info kernel | grep naf
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0→10.10.200.0/25 pref=0.0.0.0 gwy=0.0.0.0
dev=37(naf.root)
```

6. 开启NAT64后，如果IPPool配置的不是一个完整的subnet，则下发时页面或CLI会报错，因为无法为naf接口下发路由。



7. 创建防火墙策略，先在NAT选项中开启NAT64，在Source中引用IPv6的all，然后在Destination中引用VIP，在IPPool中引用IPPool。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 2
        set name "NAT64"
        set srcintf "lan"
        set dstintf "port18"
        set action accept
        set nat64 enable
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "NAT64"
        set schedule "always"
        set service "ALL"
        set ippool enable
        set poolname "NAT64"
    next
end
```

结果验证与注意事项

1. Client访问FortiGate的NAT64 VIP地址2200::64，抓包查看NAT64过程，可以看到经过naf.root接口，目标地址被转换为Server IPv4，源IPv6地址被转换为IPPool中的IPv4地址，返回的流量从IPv4被还原为IPv6。

```
FortiGate-101F # diagnose sniffer packet any 'icmp or icmp6' 4
interfaces=[any]
filters=[icmp or icmp6]
2.844158 lan in 2100::2 -> 2200::64: icmp6: echo request seq 78
2.844203 naf.root out 2100::2 -> 2200::64: icmp6: echo request seq 78
2.844210 naf.root in 10.10.200.20 -> 10.10.12.1: icmp: echo request
2.844231 port18 out 10.10.200.20 -> 10.10.12.1: icmp: echo request
2.844401 port18 in 10.10.12.1 -> 10.10.200.20: icmp: echo reply
2.844415 naf.root out 10.10.12.1 -> 10.10.200.20: icmp: echo reply
2.844419 naf.root in 2200::64 -> 2100::2: icmp6: echo reply seq 78
2.844432 lan out 2200::64 -> 2100::2: icmp6: echo reply seq 78
```

2. debug flow IPv4/IPv6，可以看到DNAT64整个过程都需要经过naf.root接口处理。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate-101F # id=20085 trace_id=876 func=resolve_ip6_tuple_fast line=4787 msg="vd-root:0 received a packet(proto=58, 2100::2:1->2200::64:128) from lan."
id=20085 trace_id=876 func=resolve_ip6_tuple line=4926 msg="allocate a new session-00001d16"
id=20085 trace_id=876 func=get_vip64_addr line=1174 msg="find DNAT64: IP-10.10.12.1, port-8(fixed port)"
id=20085 trace_id=876 func=vf_ip6_route_input line=1201 msg="find a route: gw-2200::64 via naf.root err 0 flags 01000001"
id=20085 trace_id=876 func=fw6_forward_handler line=435 msg="Check policy between lan -> naf.root"
id=20085 trace_id=876 func=get_new_addr64 line=1110 msg="find SNAT64: IP-10.10.200.20(from IPPOOL), port-16716"
id=20085 trace_id=876 func=fw6_forward_handler line=567 msg="Allowed by Policy-2: SNAT"
id=20085 trace_id=876 func=ip6_nat_af_input line=298 msg="nat64 ipv6 received a packet proto=58"
id=20085 trace_id=876 func=init_ip_session_common line=6003 msg="allocate a new session-0014068b, tun_id=0.0.0.0"
id=20085 trace_id=876 func=vf_ip_route_input_common line=2604 msg="find a route: flag=04000000 gw-10.10.12.1 via port18"
id=20085 trace_id=876 func=fw_forward_handler line=874 msg="Allowed by Policy-2:"
id=20085 trace_id=873 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=1, 10.10.12.1:16716->10.10.200.20:0) tun_id=0.0.0.0 from port18. type=0, code=0
, id=16716, seq=87."
id=20085 trace_id=873 func=resolve_ip_tuple_fast line=5910 msg="Find an existing session, id-0014068b, reply direction"
id=20085 trace_id=873 func=vf_ip_route_input_common line=2604 msg="find a route: flag=04000000 gw-10.10.200.20 via naf.root"
id=20085 trace_id=873 func=fw_forward_dirty_handler line=410 msg="state=00000200, state2=00000000, npu_state=04040000"
id=20085 trace_id=873 func=ip4_nat_af_input line=261 msg="nat64 ipv4 received a packet proto=1"
id=20085 trace_id=873 func=vf_ip6_route_input line=1201 msg="find a route: gw-2100::2 via lan err 0 flags 01000001"
id=20085 trace_id=873 func=fw6_forward_dirty_handler line=371 msg="state=00010200, state2=00000000, npu_state=04040000"
```

3. 在FortiGate查看IPv6会话，可以看到源接口为物理入接口lan，目标接口为index 37，为naf.root，naf被标记为1，IPv6流量未被加速，会话中还包含相关的IPv4的相关信息。

```
session6 info: proto=58 proto_state=00 duration=1 expire=58 timeout=0 flags=00000000 sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty npu
statistic(bytes/packets/allow_err): org=80/1/0 reply=80/1/0 tuples=2
tx speed(Bps/kbps): 48/0 rx speed(Bps/kbps): 48/0
orgin->sink: org pre->post, reply pre->post dev=41->37/37->41
hook=pre dir=org act=noop 2100::2:1->2200::64:128(:::0)
hook=post dir=reply act=noop 2200::64:1->2100::2:129(:::0)
peer=10.10.200.20:33100->10.10.12.1:8 naf=1
hook=pre dir=org act=noop 10.10.200.20:33100->10.10.12.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.12.1:33100->10.10.200.20:0(0.0.0.0:0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00001d1f tos=ff/ff ips_view=25718 app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

```
FortiGate-101F # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

4. 在FortiGate查看IPv4会话，可以看到源接口为index 37，为naf.root，目标接口为物理出接口port18，naf被标记为2，IPv4流量未被加速，会话中还包含相关的IPv6会话信息。

```
session info: proto=1 proto_state=00 duration=1 expire=58 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=60/1/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 56/0 rx speed(Bps/kbps): 56/0
orgin->sink: org pre->post, reply pre->post dev=37->30/30->37 gwy=10.10.12.1/10.10.200.20
hook=pre dir=org act=noop 10.10.200.20:12620->10.10.12.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.12.1:12620->10.10.200.20:0(0.0.0.0:0)
peer=2200::64:1->2100::2:129 naf=2
hook=pre dir=org act=noop 2100::2:1->2200::64:128(:::0)
hook=post dir=reply act=noop 2200::64:1->2100::2:129(:::0)
misc=0 policy_id=2 pol_uuid_idx=563 auth_info=0 chk_client_info=0 vd=0
serial=0014090b tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

```
FortiGate-101F # diagnose netlink interface list | grep port18
if=port18 family=00 type=1 index=30 mtu=1500 link=0 master=0
```

5. 修改IPPool的地址范围和IPv4出接口地址一致，再次测试NAT64转换。

```
config firewall ippool
    edit "NAT64"
        set startip 10.10.12.2
        set endip 10.10.12.2
        set nat64 enable

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    next
end
```

6. 查看kernel路由中关于naf.root的路由，可以看到未产生IPPool的路由，这样返回的流量肯定是被丢掉的，接下来验证一下。

```
FortiGate-101F # get router info kernel | grep naf

FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=11(zebra) flag=00000000 prio=1024 dst:2200::64/128 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

7. debug flow IPv4&IPv6可以看到，Client到Server方向的NAT46的DNAT和SNAT均正常工作，但返回的IPv6流量未匹配到naf.root接口的路由，而gw查找到的是root接口，返回的流量无法到达Client。

```
FortiGate-101F # id=20085 trace_id=925 func=resolve_ip6_tuple_fast line=4787 msg="vd-root:0 received a packet(proto=58, 2100::2:1->2200::64:128) from lan."
id=20085 trace_id=925 func=resolve_ip6_tuple line=4926 msg="allocate a new session-00001d49"
id=20085 trace_id=925 func=get_vip64_addr line=1174 msg="find DNAT64: IP-10.10.12.1, port-8(fixed port)"
id=20085 trace_id=925 func=vf_ip6_route_input line=1201 msg="find a route: gw-2200::64 via naf.root err 0 flags 01000001"
id=20085 trace_id=925 func=fw6_forward_handler line=435 msg="Check policy between lan -> naf.root"
id=20085 trace_id=925 func=get_new_addr64 line=1110 msg="find SNAT64: IP-10.10.12.2(from IPPOOL), port-8524"
id=20085 trace_id=925 func=fw6_forward_handler line=567 msg="Allowed by Policy-2: SNAT"
id=20085 trace_id=925 func=ip6_nat_af_input line=298 msg="nat64 ipv6 received a packet proto=58"
id=20085 trace_id=925 func=init_ip_session_common line=6003 msg="allocate a new session-00140e71, tun_id=0.0.0.0"
id=20085 trace_id=925 func=vf_ip_route_input_common line=2604 msg="find a route: flag=00000000 gw-10.10.12.1 via port18"
id=20085 trace_id=925 func=fw_forward_handler line=874 msg="Allowed by Policy-2:"
id=20085 trace_id=876 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=1, 10.10.12.1:8524->10.10.12.2:0) tun_id=0.0.0.0 from port18. type=0, code=0, id=8524, seq=90."
id=20085 trace_id=876 func=resolve_ip_tuple_fast line=5910 msg="Find an existing session, id-00140e71, reply direction"
id=20085 trace_id=876 func=vf_ip_route_input_common line=2604 msg="find a route: flag=84000000 gw-10.10.12.2 via root"
```

8. **所以配置NAT64时，需要注意，IPPool不要配置成和出接口地址相同的地址，配置不会报错，但实际会不通，如果是IPv4的第二地址，实际测试也是不行的。**

9. 还原IPPool的配置，这次修改VIP6的External IP和物理入接口IP一致。

```
config firewall vip6
    edit "NAT64"
        set extip 2100::1
        set nat66 disable
        set nat64 enable
        set ipv4-mappedip 10.10.12.1
    next
end
```

10. 查看kernel路由中关于naf.root的路由，可以看到未产生naf.root接口的VIP6的路由，这样NAT64的Client发起方流量应该是无法进入NAT64流程的，接下来验证一下。

```
FortiGate-101F # get router info kernel | grep naf
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->10.10.200.0/24 pref=0.0.0.0 gwy=0.0.0.0 dev=37(naf.root)

FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

11. debug flow IPv4&IPv6可以看到，Client到Server方向的NAT64流量被FortiGate路由到root接口，未进入naf.root接口，由FortiGate直接返回了reply报文，没有IPv4的debug flow产生。

```
FortiGate-101F # id=20085 trace_id=973 func=resolve_ip6_tuple_fast line=4787 msg="vd-root:0 received a packet(proto=58, 2100::2:1->2100::1:128) from lan."
id=20085 trace_id=973 func=resolve_ip6_tuple line=4926 msg="allocate a new session-00001d70"
id=20085 trace_id=973 func=get_vip64_addr line=1174 msg="find DNAT64: IP-10.10.12.1, port-8(fixed port)"
id=20085 trace_id=973 func=vf_ip6_route_input line=1201 msg="find a route: gw-:: via root err 0 flags 80200001"
id=20085 trace_id=974 func=resolve_ip6_tuple_fast line=4787 msg="vd-root:0 received a packet(proto=58, 2100::1:1->2100::2:129) from local."
id=20085 trace_id=974 func=resolve_ip6_tuple_fast line=4827 msg="Find an existing session, id-00001d70, reply direction"
```

12. **所以配置NAT64时，需要注意，IPv6 VIP的extip不要配置成和入接口地址相同的地址，配置不会报错，但实际会不通，如果是IPv6的第二地址，实际测试也是不行的。**

CLI相关

VIP CLI

1. IPv4类型的VIP支持三种组合，NAT44、NAT46、NAT44+NAT46。

```
config firewall vip
    edit "vip1"
        set extip 30.0.0.110-30.0.0.120
        set extintf "port3"
        set arp-reply disable
        set portforward enable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set srcintf-filter "port3"
        set nat44 disable    ←──────── new option enabled by default
        set nat46 enable    ←──────── new option disabled by default
        set ipv6-mappedip 2040::20-2040::30    ←──────── new option available when nat46 enabled
        set extport 10
        set ipv6-mappedport 100    ←──────── new option available when nat46 enabled
    next
end

```

2. IPv6类型的VIP支持三种组合，NAT66、NAT64、NAT66+NAT64。

```
config firewall vip6
    edit "vip3"
        set extip 2002::100-2002::200
        set portforward enable
        set nat66 disable    ←──── new option enabled by default
        set nat64 enable    ←──── new option disabled by default
        set ipv4-mappedip 8.8.8.8-8.8.8.108    ←──── new option available when nat64 is enabled
        set ipv4-mappedport 1000    ←── new option available when nat64 is enabled
        set extport 100
    next
end
```

3. NAT64也支持Virtual Server，开启NAT64后，RS必须配置为IPv4地址，实现的NAT过程和普通的NAT64是一样的。

```
config firewall vip6
    edit "vip2"
        set type server-load-balance
        set extip 2002::2
        set server-type udp
        set monitor "ping-mon-l"
        set nat64 enable
        set extport 53
        config realservers
            edit 1
                set ip 8.8.8.8    ←──── server ip must be ipv4 when nat64 is abled
                set port 53
            next
            edit 2
                set ip 8.8.4.4
                set port 53
            next
        end
    next
end
```

IPPool CLI

1. IPv4类型的IPPool，类型为NAT64，地址池范围必须是一个subnet的范围，默认会开启add-nat64-route。

```
config firewall ippool
    edit "pol64"
        set startip 10.0.0.0    ←── ip range must be a subnet if nat64 enabled
        set endip 10.0.255.255
        set nat64 enable    ←── new option
        set add-nat64-route enable    ←──── new option available when nat64 enabled (by default enable)
    next
end
```

2. IPv6类型的IPPool，类型为NAT46，地址池范围必须是一个subnet的范围，默认会开启add-nat46-route。

```
config firewall ippool6
    edit "pol46"
        set startip 2002::    ←──── ip range must be a subnet if nat46 enabled
        set endip 2002::ffff
        set nat46 enable
        set add-nat46-route enable    ←──── new option available when nat46 enabled (by default enable)
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Firewall Policy & Central SNAT CLI

1. NAT64 Firewall Policy。

```
config firewall policy
     edit 3
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"    <——— both ipv4 and ipv6 addresses are required when nat64 enable
        set srcaddr6 "all"
        set dstaddr6 "vip3"    <—— vip6 with nat64 enabled
        set action accept
        set schedule "always"
        set service "ALL"
        set ippool enable
        set poolname "po1"    <——— ipv4 pool with nat64 enabled
        set nat64 enable    <—— new option to enable nat64
    next
end
```

2. NAT64 Central SNAT。

```
config firewall central-snat-map
    edit 3
        set type ipv6
        set srcintf "any"
        set dstintf "any"
        set orig-addr6 "all"
        set dst-addr6 "all"
        set nat64 enable    <——— new option for ipv6 rule
        set nat-ippool "po1"    <——— available when nat64 is enabled, ipv4 pool with nat64 enabled
    next
end
```

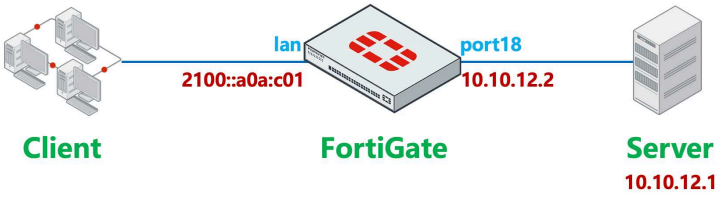

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Embedded模式的NAT64

网络需求

将IPv4内部服务器，发布到IPv6网络之中，同时将IPv4服务器的IPv4地址嵌入IPv6 VIP地址的最后32位中，允许用户通过IPv6来对其进行访问。

网络拓扑



Client侧为IPv6，Server侧为IPv4，FortiGate做NAT64转换，将IPv4服务器的IPv4地址嵌入IPv6 VIP地址的最后32位中，使用Client访问Server的IPv6 VIP地址。

配置步骤

1. 创建VIP，选择类型为IPv6，“外部IP地址/范围”填写IPv6 VIP地址，“映射到”选择Use Embedded，这里会根据IPv6外部地址的最后32位二进制数字，计算出映射的IPv4地址，并显示在提示信息中，这里计算出的是Server IPv4 10.10.12.1。




```
config firewall vip6
    edit "NAT64_embedded"
        set extip 2100::a0a:c01
        set nat66 disable
        set nat64 enable
        set add-nat64-route enable
        set embedded-ipv4-address enable
    next
end
```

2. 可以看默认存在一个naf.root接口，用于处理NAT64流量，创建VIP完成后，如果开启了add-nat64-route（默认开启），针对naf.root接口生成去往VIP IPv6地址的路由，关闭add-nat64-route后，该路由会消失。

```
FortiGate-101F # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

```
FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=11(zebra) flag=00000000 prio=1024 dst:2100::a0a:c02/128 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

3. 创建IPv4 Pool，配置地址池范围，配置地址池范围，注意不要和port18地址冲突，开启NAT64后，须填写为一个完整的subnet（最小32位）的IPv4地址范围。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall ippool
    edit "NAT64_embedded"
        set startip 10.10.200.0
        set endip 10.10.200.127
        set nat64 enable
        set add-nat64-route enable
    next
end
```

4. 创建完成后，如果开启了add-nat64-route（默认开启），可以看到生成了IPv4的kernel路由，针对naf.root接口生成去往IPPool IPv4地址的路由，IPPool关闭NAT64或关闭add-nat64-route后，该路由会消失。

```
FortiGate # get router info kernel | grep naf
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0→10.10.200.0/25 pref=0.0.0.0 gwy=0.0.0.0
dev=37(naf.root)
```

5. 创建防火墙策略，先在NAT选项中开启NAT64，在源地址中引用IPv6的all，然后在目标地址中引用VIP，在IP池配置中引用IPPool。




```
config firewall policy
    edit 2
        set name "NAT64"
        set srcintf "lan"
        set dstintf "port18"
        set action accept
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

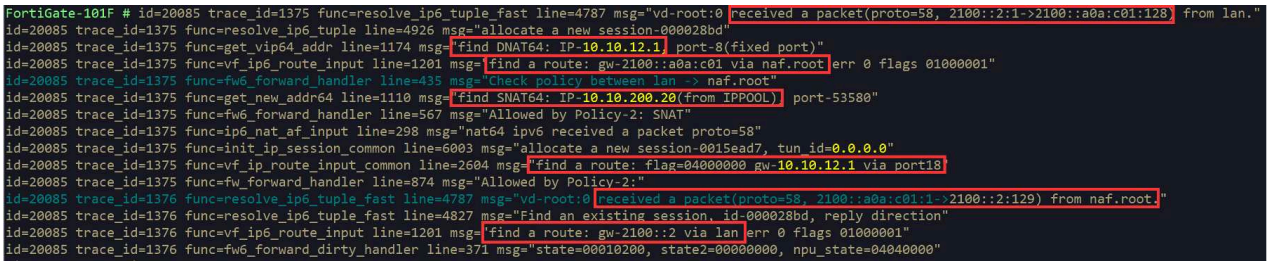
```
        set nat64 enable
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "NAT64"
        set schedule "always"
        set service "ALL"
        set ippool enable
        set poolname "NAT64"
    next
end
```

结果验证

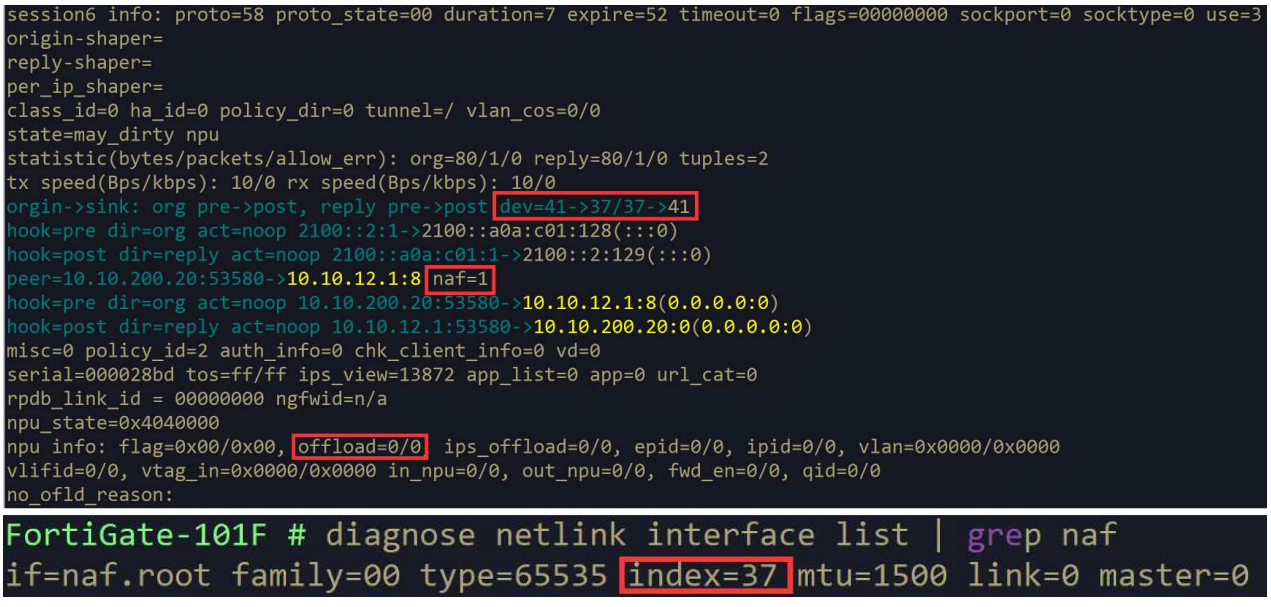
1. Client访问FortiGate的NAT64 VIP地址2100::a0a:c01，抓包查看NAT64过程，可以看到经过naf.root接口，目标地址被转换为IPv6的extip的最后32位二进制数字的embedded IP 10.10.12.1。



2. debug flow IPv4/IPv6，可以看到DNAT64整个过程都需要经过naf.root接口处理。



3. 在FortiGate查看IPv6会话，可以看到源接口为物理入接口lan，目标接口为index 37，为naf.root，naf被标记为1，IPv6流量未被加速，会话中还包含相关的IPv4的相关信息。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 在FortiGate查看IPv4会话，可以看到源接口为index 37，为naf.root，目标接口为物理出接口port18，naf被标记为2，IPv4流量未被加速，会话中还包含相关的IPv6会话信息。

```
session info: proto=1 proto_state=00 duration=10 expire=49 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=60/1/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=37->30/30->37 gwy=10.10.12.1/10.10.200.20
hook=pre dir=org act=noop 10.10.200.20:53580->10.10.12.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.12.1:53580->10.10.200.20:0(0.0.0.0:0)
peer=2100::a0a:c01:1->2100::2:129 naf=2
hook=pre dir=org act=noop 2100::2:1->2100::a0a:c01:128(:::0)
hook=post dir=reply act=noop 2100::a0a:c01:1->2100::2:129(:::0)
misc=0 policy_id=2 pol_uuid_idx=567 auth_info=0 chk_client_info=0 vd=0
serial=0015ead7 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

```
FortiGate-101F # diagnose netlink interface list | grep port18
if=port18 family=00 type=1 index=30 mtu=1500 link=0 master=0
```

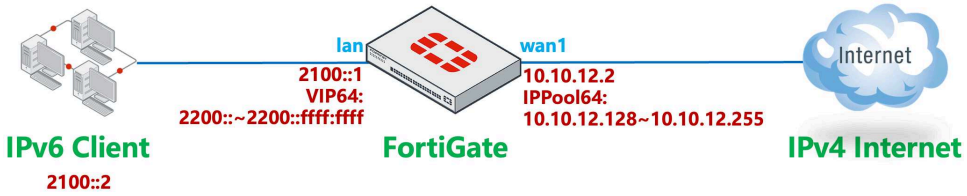

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NAT64+DNS64上网

网络需求

内网用户为IPv6网络，Internet网络为IPv4网络，内部IPv6用户通过NAT64+DNS64访问IPv4的Internet网络。

网络拓扑

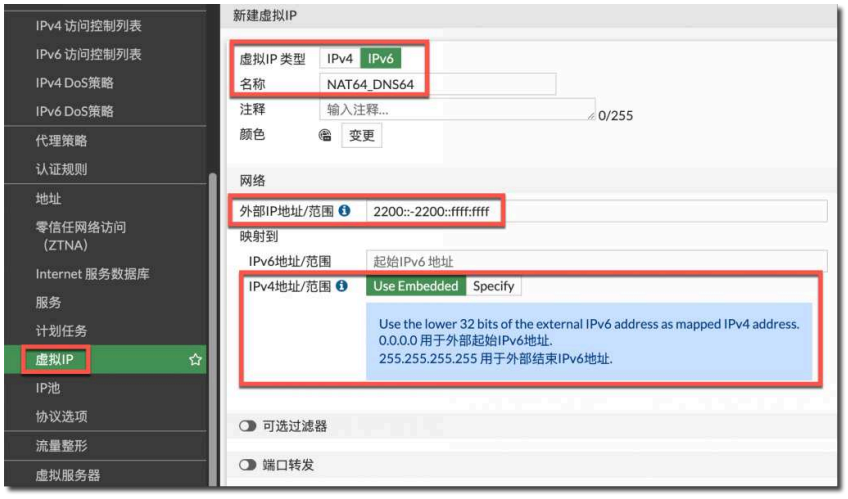


1. Client侧为IPv6，Server侧为IPv4，FortiGate做NAT64+DNS64转换，内部IPv6用户通过NAT64+DNS64访问IPv4的Internet网络。
2. 配置IPv6 Client的IPv6为21001，FortiGate内网口lan的IPv6为2100::1/64。
3. 配置FortiGate外网口wan1的IP为10.10.12.2/24，默认路由指向IPv4 Internet 10.10.12.1。

配置步骤

NAT64配置

1. 创建VIP，选择类型为IPv6，“外部IP地址/范围”填写IPv6 VIP地址，“映射到”选择Use Embedded，这里填写的IPv6地址范围要写96位的IPv6前缀（注意不要配置和接口IPv6地址相同的网段），最后32位范围为0.0.0.0~255.255.255.255的16进制格式，用于映射所有的IPv4地址。




```
config firewall vip6
    edit "NAT64_DNS64"
        set uuid f913176c-48aa-51ee-62dd-5d5b772dede2
        set extip 2200::-2200::ffff:ffff
        set nat66 disable
        set nat64 enable
        set embedded-ipv4-address enable
    next
end
```

2. 可以看默认存在一个naf.root接口，用于处理NAT64流量，创建VIP完成后，如果开启了add-nat64-route（默认开启），针对naf.root接口生成去往VIP IPv6地址的路由，关闭add-nat64-route后，该路由会消失。

```
FortiGate-101F # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

```
FortiGate # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=11(zebra) flag=00000000 prio=1024 dst:2200::/96 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 创建IPv4 Pool，配置地址池范围，配置地址池范围，注意不要和wan1地址冲突，开启NAT64后，须填写为一个完整的subnet（最小32位）的IPv4地址范围。




```
config firewall ippool
    edit "NAT64_DNS64"
        set startip 10.10.12.128
        set endip 10.10.12.255
        set nat64 enable
        set add-nat64-route enable
    next
end
```

4. 创建完成后，如果开启了add-nat64-route（默认开启），可以看到生成了IPv4的kernel路由，针对naf.root接口生成去往IPPool IPv4地址的路由，IPPool关闭NAT64或关闭add-nat64-route后，该路由会消失。

```
FortiGate # get router info kernel | grep naf
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0→10.10.12.128/25 pref=0.0.0.0 gwy=0.0.0.0
dev=37(naf.root)
```

5. 创建防火墙策略，先在NAT选项中开启NAT64，在源地址中引用IPv6的all，然后在目标地址中引用VIP，在IP池配置中引用IPPool。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 9
        set name "NAT64_DNS64"
        set srcintf "lan"
        set dstintf "wan1"
        set action accept
        set nat64 enable
        set srcaddr "all"
        set dstaddr "all"
        set srcaddr6 "all"
        set dstaddr6 "NAT64_DNS64"
        set schedule "always"
        set service "ALL"
        set ippool enable
        set poolname "NAT64_DNS64"
    next
end
```

DNS64配置

1. 在CLI下开启DNS64，配置dns64-prefix为NAT64 VIP的前96位2200::/96，确认always-synthesize-aaaa-record为开启状态（默认开启）。

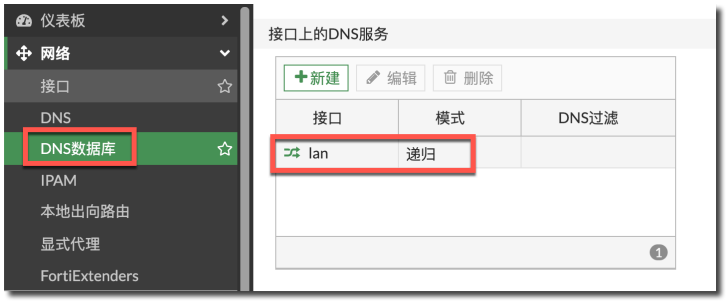
```
config system dns64
    set status enable
    set dns64-prefix 2200::/96
    set always-synthesize-aaaa-record enable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

- enable：默认配置，所有从IPv6客户端发送的DNS AAAA Record请求会被FortiGate无条件转换为A Record请求，通过IPv4 DNS发送至系统配置的DNS服务器（不会发送AAAA请求），IPv4 DNS服务器返回A Record后，将A Record中的IPv4地址嵌入dns64-prefix的后32位中，然后封装为IPv6的AAAA Record回应，返回给IPv6客户端。
- disable：所有从IPv6客户端发送的DNS AAAA Record请求首先会被FortiGate封装在IPv4的DNS报文中发送至系统配置的DNS服务器：
  - 如果DNS服务器返回了AAAA Record，FortiGate将此AAAA Record回应封装为IPv6 DNS返回给IPv6客户端（这里返回的AAAA Record为原服务器响应的IPv6，FortiGate不做任何修改）。
  - 如果DNS服务器返回的DNS报文中没有AAAA Record的IPv6地址或没有响应DNS请求，FortiGate会执行always-synthesize-aaaa-record enable时相同的操作，向DNS服务器发送A Record请求的IPv4 DNS报文，IPv4 DNS服务器返回A Record后，将A Record中的IPv4地址嵌入dns64-prefix的后32位中，然后封装为IPv6的AAAA Record回应，返回给IPv6客户端。
- 当always-synthesize-aaaa-record配置为disable时，DNS服务器返回的AAAA Record会被FortiGate不经修改直接返回给IPv6客户端，客户端访问此IPv6时，可能不在NAT64 VIP的IPv6地址范围中，导致被FortiGate丢弃，所以建议always-synthesize-aaaa-record的配置保持默认开启，不要关闭。
- 关于always-synthesize-aaaa-record的说明请参考官方文档：https://docs.fortinet.com/document/fortigate/7.99.99/administration-guide/443324/nat64-policy-and-dns64-dns-proxy ↗ 。

2. 在lan口上开启DNS服务器，IPv6网络侧用户发起AAAA Record查询，FortiGate的DNS64代理请求IPv4网络中对应FQDN的A Record，得到A Record响应后，DNS64服务器将A Record响应中的IPv4地址嵌入dns64-prefix的后32位中，然后封装为IPv6的AAAA Record回应，返回给IPv6客户端。




```
config system dns-server
    edit "lan"
    next
end
```

3. 为系统配置IPv4 DNS服务器（也可以使用默认服务器）。

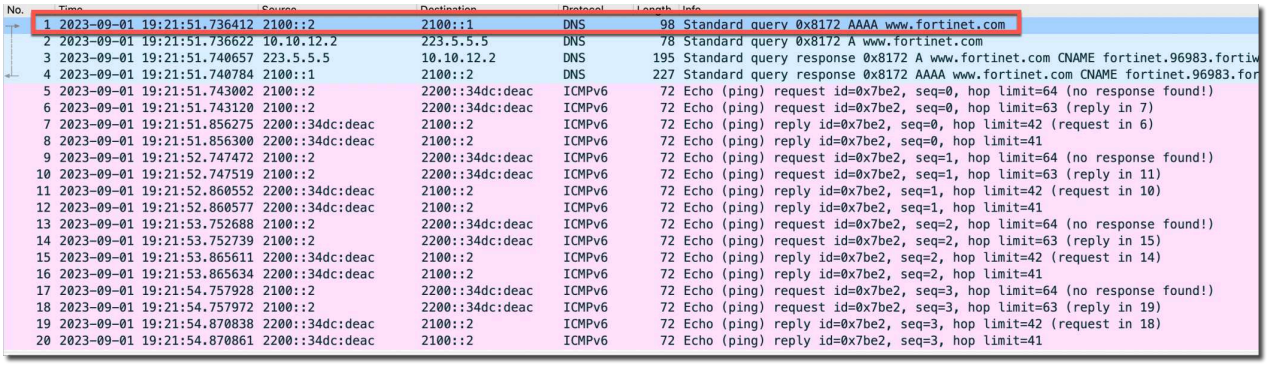



```
config system dns
    set primary 223.5.5.5
end
```

结果验证

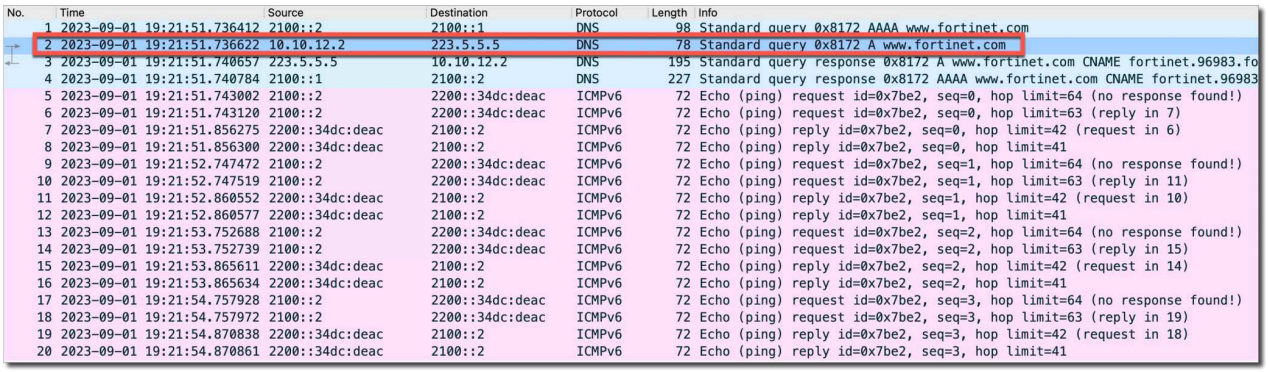
1. IPv6 Client访问IPv4 Internet域名，抓包查看DNS64过程，客户端发出IPv6的AAAA请求，请求域名www.fortinet.com ↗ 的AAAA Record。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



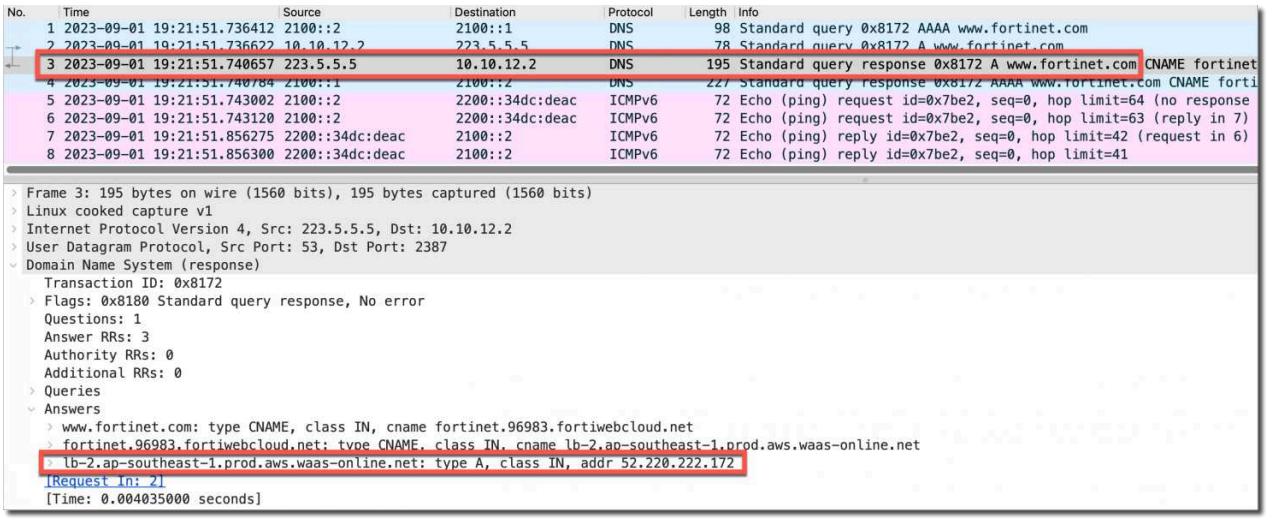
No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-01 19:21:51.736412	2100::2	2100::1	DNS	98	Standard query 0x8172 AAAA www.fortinet.com
2	2023-09-01 19:21:51.736622	10.10.12.2	223.5.5.5	DNS	78	Standard query 0x8172 A www.fortinet.com
3	2023-09-01 19:21:51.740657	223.5.5.5	10.10.12.2	DNS	195	Standard query response 0x8172 A www.fortinet.com CNAME fortinet.96983.fortiw
4	2023-09-01 19:21:51.740784	2100::1	2100::2	DNS	227	Standard query response 0x8172 AAAA www.fortinet.com CNAME fortinet.96983.for
5	2023-09-01 19:21:51.743002	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=0, hop limit=64 (no response found!)
6	2023-09-01 19:21:51.743120	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=0, hop limit=63 (reply in 7)
7	2023-09-01 19:21:51.856275	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=0, hop limit=42 (request in 6)
8	2023-09-01 19:21:51.856300	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=0, hop limit=41
9	2023-09-01 19:21:52.747472	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=1, hop limit=64 (no response found!)
10	2023-09-01 19:21:52.747519	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=1, hop limit=63 (reply in 11)
11	2023-09-01 19:21:52.860552	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=1, hop limit=42 (request in 10)
12	2023-09-01 19:21:52.860577	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=1, hop limit=41
13	2023-09-01 19:21:53.752688	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=2, hop limit=64 (no response found!)
14	2023-09-01 19:21:53.752739	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=2, hop limit=63 (reply in 15)
15	2023-09-01 19:21:53.865611	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=2, hop limit=42 (request in 14)
16	2023-09-01 19:21:53.865634	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=2, hop limit=41
17	2023-09-01 19:21:54.757928	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=3, hop limit=64 (no response found!)
18	2023-09-01 19:21:54.757972	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=3, hop limit=63 (reply in 19)
19	2023-09-01 19:21:54.870838	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=3, hop limit=42 (request in 18)
20	2023-09-01 19:21:54.870861	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=3, hop limit=41

2. FortiGate将此AAAA Record请求转换为A Record请求封装在IPv4 DNS中，发送给DNS服务器223.5.5.5。



No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-01 19:21:51.736412	2100::2	2100::1	DNS	98	Standard query 0x8172 AAAA www.fortinet.com
2	2023-09-01 19:21:51.736622	10.10.12.2	223.5.5.5	DNS	78	Standard query 0x8172 A www.fortinet.com
3	2023-09-01 19:21:51.740657	223.5.5.5	10.10.12.2	DNS	195	Standard query response 0x8172 A www.fortinet.com CNAME fortinet.96983.fo
4	2023-09-01 19:21:51.740784	2100::1	2100::2	DNS	227	Standard query response 0x8172 AAAA www.fortinet.com CNAME fortinet.96983
5	2023-09-01 19:21:51.743002	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=0, hop limit=64 (no response found!)
6	2023-09-01 19:21:51.743120	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=0, hop limit=63 (reply in 7)
7	2023-09-01 19:21:51.856275	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=0, hop limit=42 (request in 6)
8	2023-09-01 19:21:51.856300	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=0, hop limit=41
9	2023-09-01 19:21:52.747472	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=1, hop limit=64 (no response found!)
10	2023-09-01 19:21:52.747519	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=1, hop limit=63 (reply in 11)
11	2023-09-01 19:21:52.860552	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=1, hop limit=42 (request in 10)
12	2023-09-01 19:21:52.860577	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=1, hop limit=41
13	2023-09-01 19:21:53.752688	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=2, hop limit=64 (no response found!)
14	2023-09-01 19:21:53.752739	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=2, hop limit=63 (reply in 15)
15	2023-09-01 19:21:53.865611	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=2, hop limit=42 (request in 14)
16	2023-09-01 19:21:53.865634	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=2, hop limit=41
17	2023-09-01 19:21:54.757928	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=3, hop limit=64 (no response found!)
18	2023-09-01 19:21:54.757972	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=3, hop limit=63 (reply in 19)
19	2023-09-01 19:21:54.870838	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=3, hop limit=42 (request in 18)
20	2023-09-01 19:21:54.870861	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=3, hop limit=41

3. DNS服务器使用IPv4 DNS返回该域名的A Record IPv4地址52.220.222.172。

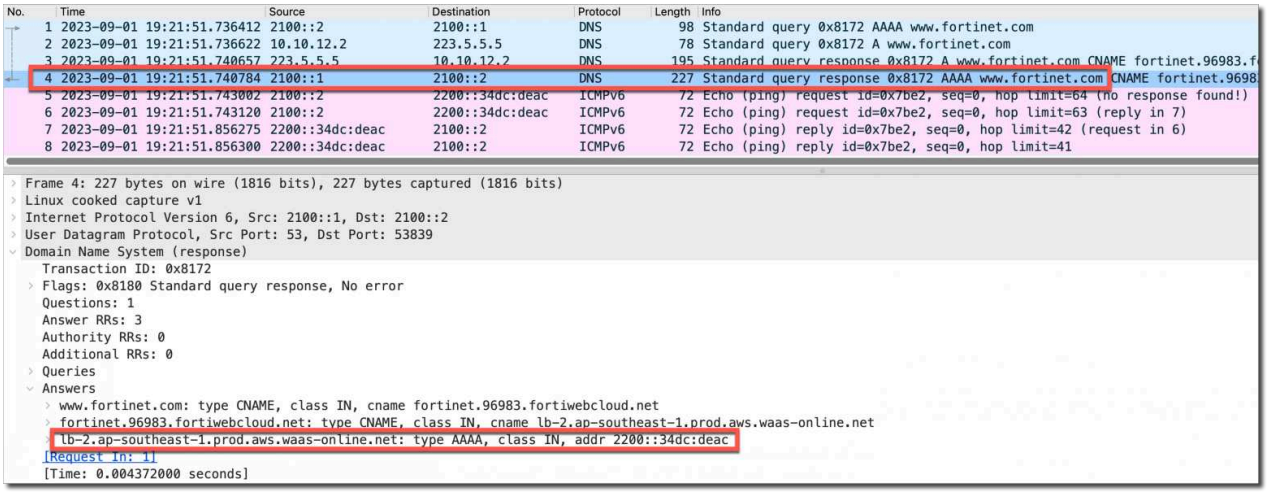


No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-01 19:21:51.736412	2100::2	2100::1	DNS	98	Standard query 0x8172 AAAA www.fortinet.com
2	2023-09-01 19:21:51.736622	10.10.12.2	223.5.5.5	DNS	78	Standard query 0x8172 A www.fortinet.com
3	2023-09-01 19:21:51.740657	223.5.5.5	10.10.12.2	DNS	195	Standard query response 0x8172 A www.fortinet.com CNAME fortinet
4	2023-09-01 19:21:51.740784	2100::1	2100::2	DNS	227	Standard query response 0x8172 AAAA www.fortinet.com CNAME forti
5	2023-09-01 19:21:51.743002	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=0, hop limit=64 (no response
6	2023-09-01 19:21:51.743120	2100::2	2200::34dc:deac	ICMPv6	72	Echo (ping) request id=0x7be2, seq=0, hop limit=63 (reply in 7)
7	2023-09-01 19:21:51.856275	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=0, hop limit=42 (request in 6)
8	2023-09-01 19:21:51.856300	2200::34dc:deac	2100::2	ICMPv6	72	Echo (ping) reply id=0x7be2, seq=0, hop limit=41

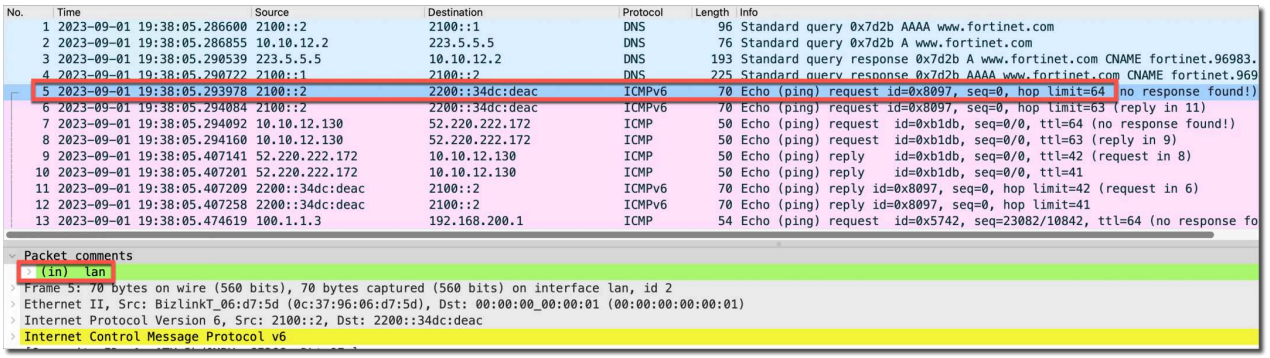
```
> Frame 3: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 223.5.5.5, Dst: 10.10.12.2
> User Datagram Protocol, Src Port: 53, Dst Port: 2387
v Domain Name System (response)
    Transaction ID: 0x8172
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > www.fortinet.com: type CNAME, class IN, cname fortinet.96983.fortiwebcloud.net
    > fortinet.96983.fortiwebcloud.net: type CNAME, class IN, cname lb-2.ap-southeast-1.prod.aws.waas-online.net
    > lb-2.ap-southeast-1.prod.aws.waas-online.net: type A, class IN, addr 52.220.222.172
    [Request In: 2]
    [Time: 0.004035000 seconds]
```

4. FortiGate收到DNS返回的该域名的A Record IPv4地址52.220.222.172转换为16进制后将其嵌入dns64-prefix 210034dc:deac，将其转换为AAAA Record，并封装在IPv6 DNS报文中返回给IPv6 Client。

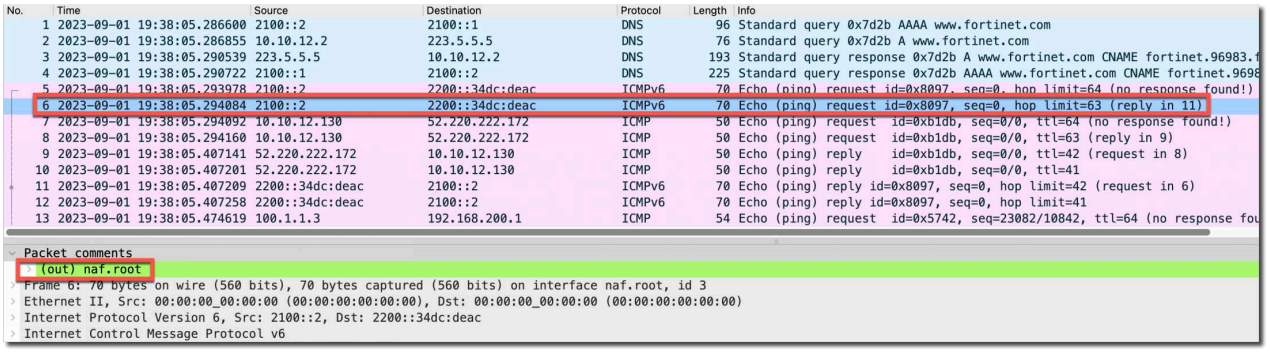
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



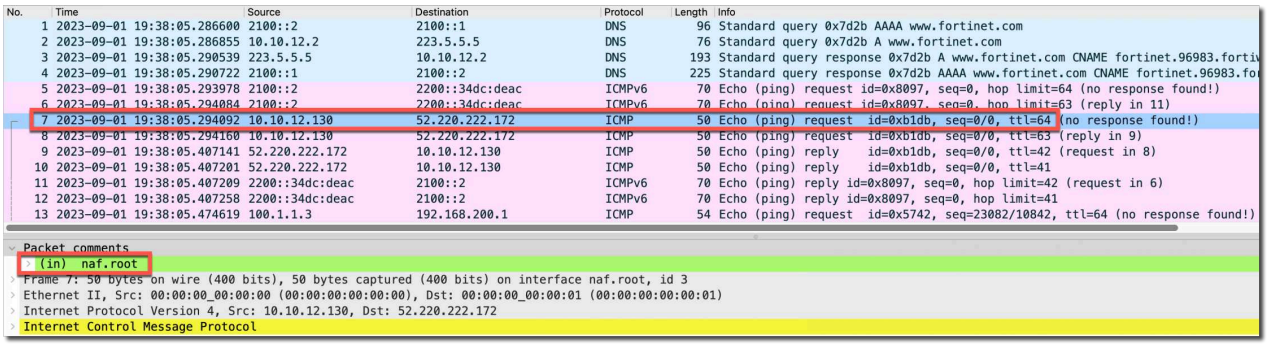
5. 客户端收到FortiGate发送的AAAA Record回应后，解析到www.fortinet.com ↗ 的IPv6 IP为2200::34dc:deac，所以直接访问该IPv6地址，FortiGate从lan口收到该IPv6请求包。



6. 该IPv6请求包经由FortiGate的naf接口，执行NAT64转换。

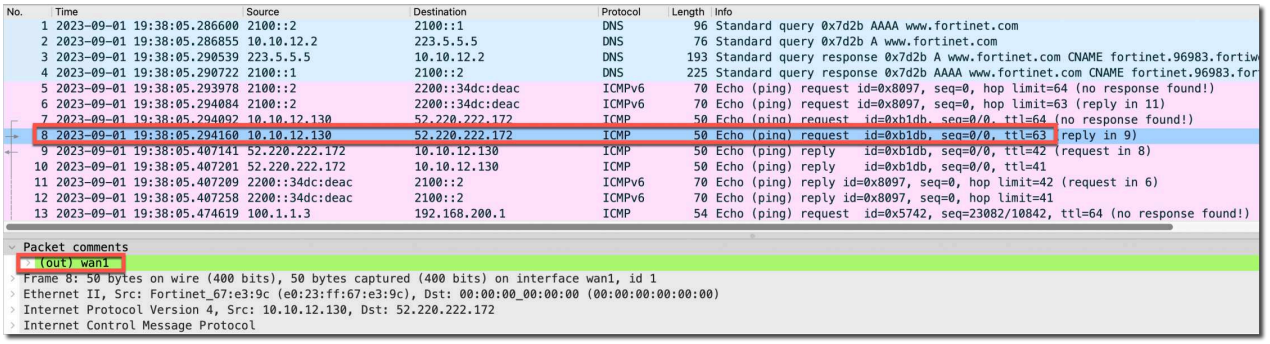


7. 经由FortiGate的naf接口进行NAT64后，转换为IPv4报文，源地址为NAT64的地址池中的IPv4地址，目标地址为原IPv6请求包目标IPv6地址2200::34dc:deac的最后32位转换为10进制后的IPv4地址52.220.222.172。

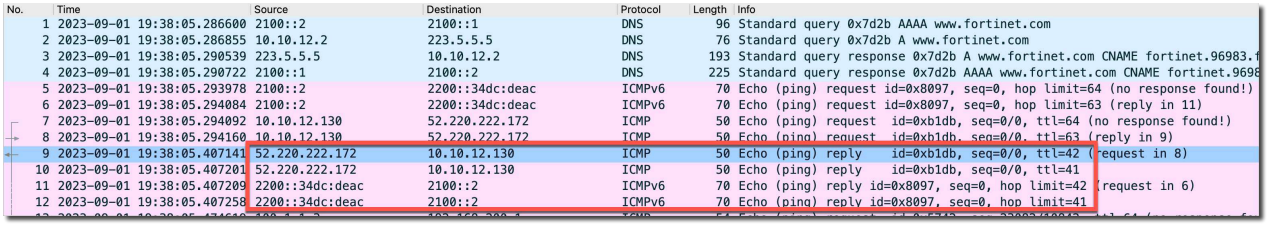


8. 最终由wan1接口发出送往Internet上的目的IPv4地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



9. 服务器Reply的IPv4报文从FortiGate的wan1收到，经由naf接口做NAT64还原后，从lan口返回IPv6 Client。



.0. 查看IPv6会话，如下所示，会话没有被NP加速，流量均经过naf接口处理，naf标记为1。

```
FortiGate # diagnose sys session6 list

session6 info: proto=58 proto_state=00 duration=110 expire=59 timeout=0 flags=00000000 sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=may_dirty npu npd
statistic(bytes/packets/allow_err): org=6160/110/0 reply=6160/110/0 tuples=2
tx speed(Bps/kbps): 54/0 rx speed(Bps/kbps): 56/0
orgin->sink: org pre->post, reply pre->post dev=45->37/37->45
hook=pre dir=org act=noop 2100::2:33956->2200::34dc:deac:128(:::0)
hook=post dir=reply act=noop 2200::34dc:deac:33956->2100::2:129(:::0)
peer=10.10.12.130:30184->52.220.222.172:8 naf=1
hook=pre dir=org act=noop 10.10.12.130:30184->52.220.222.172:8(0.0.0.0:0)
hook=post dir=reply act=noop 52.220.222.172:30184->10.10.12.130:0(0.0.0.0:0)
src_mac=0c:37:96:06:d7:5d
misc=0 policy_id=9 pol_uuid_idx=587 auth_info=0 chk_client_info=0 vd=0
serial=0000a1d7 tos=ff/ff ips_view=0 app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x81/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=95/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  offload-denied

FortiGate # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

.1. 查看IPv4会话，如下所示，会话没有被NP加速，流量均经过naf接口处理，naf标记为2。

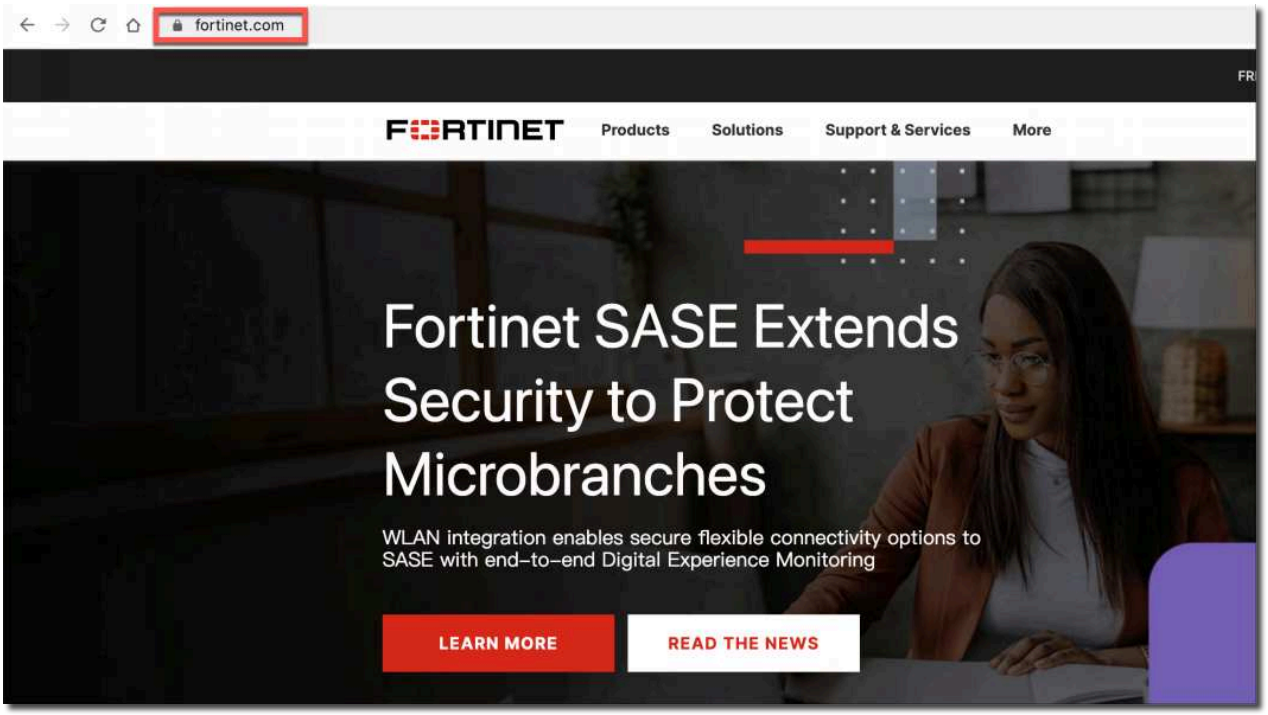
```
FortiGate # diagnose sys session list

session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=72/2/1 reply=72/2/1 tuples=2
tx speed(Bps/kbps): 57/0 rx speed(Bps/kbps): 57/0
orgin->sink: org pre->post, reply pre->post dev=37->7/7->37 gwy=10.10.12.1/10.10.12.130
hook=pre dir=org act=noop 10.10.12.130:30184->52.220.222.172:8(0.0.0.0:0)
hook=post dir=reply act=noop 52.220.222.172:30184->10.10.12.130:0(0.0.0.0:0)
peer=2200::34dc:deac:33956->2100::2:129 naf=2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
hook=pre dir=org act=noop 2100::2:33956->2200::34dc:deac:128(:::0)
hook=post dir=reply act=noop 2200::34dc:deac:33956->2100::2:129(:::0)
misc=0 policy_id=9 pol_uuid_idx=587 auth_info=0 chk_client_info=0 vd=0
serial=000ecb4f tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:

FortiGate # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

2. IPv6客户端可以正常访问IPv6的服务器。

```
~ ping6  www.fortinet.com
PING6(56=40+8+8 bytes) 2100::2 --> 2200::34dc:deac
16 bytes from 2200::34dc:deac, icmp_seq=0 hlim=41 time=114.818 ms
16 bytes from 2200::34dc:deac, icmp_seq=1 hlim=41 time=113.894 ms
16 bytes from 2200::34dc:deac, icmp_seq=2 hlim=41 time=114.014 ms
16 bytes from 2200::34dc:deac, icmp_seq=3 hlim=41 time=113.918 ms
16 bytes from 2200::34dc:deac, icmp_seq=4 hlim=41 time=113.714 ms
^C
--- lb-2.ap-southeast-1.prod.aws.waas-online.net ping6 statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 113.714/114.072/114.818/0.386 ms
```



附件

附NAT64+DNS64过程抓取的报文：dns64.pcapng ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

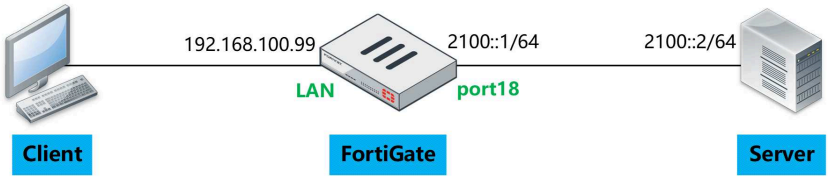
NAT46映射

网络需求

将IPv6内部服务器，发布到IPv4网络之中，允许用户通过IPv4来对其进行访问。

网络拓扑

192.168.100.77



Client侧为IPv4，Server侧为IPv6，使用Client访问Server，FortiGate做NAT46转换。

配置步骤

1. 创建VIP，选择类型为IPv4，“映射到”填写IPv6 Server真实地址，“外部IP地址/范围”填写IPv4 VIP地址，如果是一个范围，必须填写为一个完整的subnet（最小31位）的单播地址范围，不能填写广播和网络号，否则GUI报错。




```
config firewall vip
    edit "NAT46"
        set extip 192.168.200.99
        set nat44 disable
        set nat46 enable
        set extintf "lan"
        set ipv6-mappedip 2100::2
        set add-nat46-route enable
    next
end
```

2. 可以看默认存在一个naf.root接口，用于处理NAT46流量，创建VIP完成后，如果开启了add-nat46-route（默认开启），针对naf.root接口生成去往VIP IPv4地址的路由，关闭add-nat46-route后，该路由会消失。

```
FortiGate-101F # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
FortiGate-101F # get router info kernel | grep naf
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->192.168.200.99/32 pref=0.0.0.0 gwy=0.0.0.0 dev=37(naf.root)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 如果是NAT46，“外部IP范围”配置的不是一个完整的subnet，或范围中包含subnet的广播地址，则下发时页面或CLI会报错，因为无法为naf接口下发路由。



4. 创建IPv6 Pool，配置地址池范围，注意不要和port18地址冲突，配置冲突这里并不会提示，后续会讲到为什么不能配成一样的，开启NAT46后，须填写为一个完整的subnet（最小128位）的IPv6地址范围，否则GUI报错。




```
config firewall ippool6
    edit "NAT46"
        set startip 2200::
        set endip 2200::ffff
        set nat46 enable
        set add-nat46-route enable
    next
end
```

5. 创建完成后，如果开启了add-nat46-route（默认开启），可以看到生成了IPv6的kernel路由，针对naf.root接口生成去往IPPool IPv6地址的路由，IPPool6关闭NAT46或关闭add-nat46-route后，该路由会消失。

```
FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=11(zebra) flag=00000000 prio=1024 dst:2200::/112 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

6. 开启NAT46后，如果IPPool6配置的不是一个完整的subnet，则下发时页面或CLI会报错，因为无法为naf接口下发路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 创建防火墙策略，先在“启用NAT”选项中开启NAT46，然后源地址引用IPv4的all，然后在目标地址中引用NAT46 VIP，在IPPool中引用IPPool6。




```
config firewall policy
    edit 2
        set name "NAT46"
        set srcintf "lan"
        set dstintf "port18"
        set action accept
        set nat46 enable
        set srcaddr "all"
        set dstaddr "NAT46"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
        set ippool enable
        set poolname6 "NAT46"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证与注意事项

1. Client访问FortiGate的NAT46 VIP地址192.168.200.99，抓包查看NAT46过程，可以看到经过naf.root接口，目标地址被转换为Server IPv6，源IPv4地址被转换为IPPool6中的IPv6地址，返回的流量从IPv6被还原为IPv4。

```
FortiGate-101F # diagnose sniffer packet any 'icmp or icmp6' 4
interfaces=[any]
filters=[icmp or icmp6]
3.380842 lan in 192.168.100.77 -> 192.168.200.99: icmp: echo request
3.380968 naf.root out 192.168.100.77 -> 192.168.200.99: icmp: echo request
3.380978 naf.root in 2200::24f6 -> 2100::2: icmp6: echo request seq 2035
3.381071 port18 out 2200::24f6 -> 2100::2: icmp6: echo request seq 2035
3.381213 port18 in 2100::2 -> 2200::24f6: icmp6: echo reply seq 2035 [flowlabel 0x69fcf]
3.381256 naf.root out 2100::2 -> 2200::24f6: icmp6: echo reply seq 2035 [flowlabel 0x69fcf]
3.381264 naf.root in 192.168.200.99 -> 192.168.100.77: icmp: echo reply
3.381304 lan out 192.168.200.99 -> 192.168.100.77: icmp: echo reply
```

2. debug flow IPv4/IPv6，可以看到整个NAT46过程都需要经过naf.root接口处理。

```
FortiGate-101F # id=20085 trace_id=649 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=1, 192.168.100.77:1->192.168.200.99:2048) tun_id=0.0.0.0 from
lan. type=8, code=0, id=1, seq=2035."
id=20085 trace_id=649 func=init_ip_session_common line=6003 msg="allocate a new session-0013ba16, tun_id=0.0.0.0"
id=20085 trace_id=649 func=get_vip46_addr line=1091 msg="find DNAT46: IP-2100::2, port-128(fixed port)"
id=20085 trace_id=649 func=vf_ip_route_input_common line=2604 msg="find a route: flag=04000000 gw-192.168.200.99 via naf.root"
id=20085 trace_id=649 func=get_new_addr46 line=1154 msg="find SNAT46: IP-2200::24f6(from IPPOOL), port-60417"
id=20085 trace_id=649 func=fw_forward_handler line=874 msg="Allowed by Policy-2: SNAT"
id=20085 trace_id=649 func=ip4_nat_af_input line=261 msg="nat64 ipv4 received a packet proto=1"
id=20085 trace_id=649 func=resolve_ip6_tuple line=4926 msg="allocate a new session-00001c8b"
id=20085 trace_id=649 func=vf_ip6_route_input line=1201 msg="find a route: gw-2100::2 via port18 err 0 flags 01000001"
id=20085 trace_id=649 func=fw6_forward_handler line=435 msg="Check policy between naf.root -> port18"
id=20085 trace_id=649 func=fw6_forward_handler line=567 msg="Allowed by Policy-2:"
id=20085 trace_id=586 func=resolve_ip6_tuple_fast line=4787 msg="Vd-root:0 received a packet(proto=58, 2100::2:60417->2200::24f6:129) from port18."
id=20085 trace_id=586 func=resolve_ip6_tuple_fast line=4827 msg="Find an existing session, id-00001c8b, reply direction"
id=20085 trace_id=586 func=vf_ip6_route_input line=1201 msg="find a route: gw-2200::24f6 via naf.root err 0 flags 01000001"
id=20085 trace_id=586 func=fw6_forward_dirty_handler line=371 msg="state=00000204, state2=00000000, npu_state=04040000"
id=20085 trace_id=586 func=ip6_nat_af_input line=298 msg="nat64 ipv6 received a packet proto=58"
id=20085 trace_id=586 func=vf_ip_route_input_common line=2604 msg="find a route: flag=04000000 gw-192.168.100.77 via lan"
id=20085 trace_id=586 func=npu_handle_session64 line=1246 msg="Trying to offloading session from naf.root to lan, skb.npu_flag=00000080 ses.state=00010204 ses.npu_state=0x0
4040000"
id=20085 trace_id=586 func=fw_forward_dirty_handler line=410 msg="state=00010204, state2=00000001, npu_state=04040000"
```

3. 在FortiGate查看IPv4会话，可以看到源接口为物理入接口lan，目标接口为index 37，为naf.root，naf被标记为1，IPv4流量未被加速，会话中还包含相关的IPv6的相关信息。

```
session info: proto=1 proto_state=00 duration=8 expire=51 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=60/1/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 6/0 rx speed(Bps/kbps): 6/0
orgin->sink: org pre->post, reply pre->post dev=41->37/37->41 gwy=192.168.200.99/192.168.100.77
hook=pre dir=org act=noop 192.168.100.77:1->192.168.200.99:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.200.99:1->192.168.100.77:0(0.0.0.0:0)
peer=2200::24f6:60417->2100::2:128 naf=1
hook=pre dir=org act=noop 2200::24f6:60417->2100::2:128(:::0)
hook=post dir=reply act=noop 2100::2:60417->2200::24f6:129(:::0)
misc=0 policy_id=2 pol_uuid_idx=555 auth_info=0 chk_client_info=0 vd=0
serial=0013ba16 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
ofld_fail_reason(kernel, drv): none/not-established, none(0)/none(0)
npu_state_err=00/04
```

dev_index37即为naf.root接口

```
FortiGate-101F # diagnose netlink interface list | grep naf
if=naf.root family=00 type=65535 index=37 mtu=1500 link=0 master=0
```

4. 在FortiGate查看IPv6会话，可以看到源接口为index 37，为naf.root，目标接口为物理出接口port18，naf被标记为2，IPv6流量未被加速，会话中还包含相关的IPv4会话信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
session6 info: proto=58 proto_state=00 duration=15 expire=44 timeout=0 flags=00000000 sockport=0 socktype=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty npu
statistic(bytes/packets/allow_err): org=80/1/0 reply=80/1/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=37->30/30->37
hook=pre dir=org act=noop 2200::24f6:60417->2100::2:128(:::0)
hook=post dir=reply act=noop 2100::2:60417->2200::24f6:129(:::0)
peer=192.168.200.99:1->192.168.100.77:0 naf=2
hook=pre dir=org act=noop 192.168.100.77:1->192.168.200.99:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.200.99:1->192.168.100.77:0(0.0.0.0:0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=00001c8b tos=ff/ff ips_view=0 app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000 ngfwid=n/a
npu_state=0x4040000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
ofld_fail_reason(kernel, drv): none/not-established, none(0)/none(0)
npu_state_err=00/04
```

```
FortiGate-101F # diagnose netlink interface list | grep port18
if=port18 family=00 type=1 index=30 mtu=1500 link=0 master=0
```

5. 修改IPPool6的地址范围和IPv6出接口地址一致，再次测试NAT46转换。

```
config firewall ippool6
    edit "NAT46"
        set startip 2100::1
        set endip 2100::1
        set nat46 enable
    next
end
```

6. 查看kernel路由中关于naf.root的路由，可以看到未产生IPPool6的路由，这样返回的流量肯定是被丢掉的，接下来验证一下。

```
FortiGate-101F # get router info kernel | grep naf
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->192.168.200.99/32 pref=0.0.0.0 gwy=0.0.0.0 dev=37(naf.root)

FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

7. debug flow IPv4&IPv6可以看到，Client到Server方向的NAT46的DNAT和SNAT均正常工作，但返回的IPv6流量未匹配到naf.root接口的路由，而gw查找到的是root接口，返回的流量无法到达Client。

```
FortiGate-101F # id=20085 trace_id=858 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=1, 192.168.100.77:1->192.168.200.99:2048) tun_id=0.0.0.0 from
lan. type=8, code=0, id=1, seq=2051."
id=20085 trace_id=858 func=init_ip_session_common line=6003 msg="allocate a new session-0013c852, tun_id=0.0.0.0"
id=20085 trace_id=858 func=get_vip46_addr line=1091 msg="find DNAT46: IP-2100::2, port-128(fixed port)"
id=20085 trace_id=858 func=vf_ip_route_input_common line=2604 msg="find a route: flag=04000000 gw-192.168.200.99 via naf.root"
id=20085 trace_id=858 func=get_new_addr46 line=1154 msg="find SNAT46: IP-2100::1(from IPPOOL), port-60417"
id=20085 trace_id=858 func=fw_forward_handler line=874 msg="Allowed by Policy-2: SNAT"
id=20085 trace_id=858 func=ip4_nat_af_input line=261 msg="nat64 ipv4 received a packet proto=1"
id=20085 trace_id=858 func=resolve_ip6_tuple line=4926 msg="allocate a new session-00001c92"
id=20085 trace_id=858 func=vf_ip6_route_input line=1201 msg="find a route: gw-2100::2 via port18 err 0 flags 01000001"
id=20085 trace_id=858 func=fw6_forward_handler line=435 msg="Check policy between naf.root -> port18"
id=20085 trace_id=858 func=fw6_forward_handler line=567 msg="Allowed by Policy-2:"
id=20085 trace_id=624 func=resolve_ip6_tuple_fast line=4787 msg="vd-root:0 received a packet(proto=58, 2100::2:60417->2100::1:129) from port18."
id=20085 trace_id=624 func=resolve_ip6_tuple_fast line=4827 msg="Find an existing session, id-00001c92, reply direction"
id=20085 trace_id=624 func=vf_ip6_route_input line=1201 msg="find a route: gw-:: via root err 0 flags 80200001"
```

8. **所以配置NAT46时，需要注意，IPPool6不要配置成和出接口地址相同的地址，配置不会报错，但实际会不通，如果是IPv6的第二地址，实际测试也是不行的。**

```
config system interface
    edit "port18"
        config ipv6
            set ip6-address 2100::1/64
            config ip6-extra-addr
                edit 2100::3/64
            end
        end
end
```

9. 还原IPPool6的配置，这次修改VIP的External IP和物理入接口IP一致。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall vip
    edit "NAT46"
        set extip 192.168.100.99
        set nat44 disable
        set nat46 enable
        set extintf "lan"
        set ipv6-mappedip 2100::2
    next
end
```

10. 查看kernel路由中关于naf.root的路由，可以看到未产生naf.root接口的VIP的路由，这样NAT46的Client发起方流量应该是无法进入NAT46流程的，接下来验证一下。

```
FortiGate-101F # get router info kernel | grep naf

FortiGate-101F # get router info6 kernel | grep naf
vf=0 tbl=254 type=01(unicast) protocol=11(zebra) flag=00000000 prio=1024 dst:2100::100/128 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00000000 prio=256 dst:fe80::/64 dev=37(naf.root) pmtu=1500
vf=0 tbl=254 type=01(unicast) protocol=3(boot) flag=00000000 prio=256 dst:ff00::/8 dev=37(naf.root) pmtu=1500
```

11. debug flow IPv4&IPv6可以看到，Client到Server方向的NAT46流量被FortiGate路由到root接口，未进入naf.root接口，由FortiGate直接返回了reply报文，没有IPv6的debug flow产生。

```
FortiGate-101F # id=20085 trace_id=442 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=1, 192.168.100.77:1->192.168.100.99:2048) tun_id=0.0.0.0 from lan. type=8, code=0, id=1, seq=1940."
id=20085 trace_id=442 func=init_ip_session_common line=6003 msg="allocate a new session-0011c351, tun_id=0.0.0.0"
id=20085 trace_id=442 func=get_vip46_addr line=1091 msg="find DNAT46: IP-2100::2, port-128(fixed port)"
id=20085 trace_id=442 func=vf_ip_route_input_common line=2604 msg="find a route: flag=84000000 gw-192.168.100.99 via root"
id=20085 trace_id=443 func=print_pkt_detail line=5824 msg="vd-root:0 received a packet(proto=1, 192.168.100.99:1->192.168.100.77:0) tun_id=0.0.0.0 from local. type=0, code=0, id=1, seq=1940."
id=20085 trace_id=443 func=resolve_ip_tuple_fast line=5910 msg="Find an existing session, id-0011c351, reply direction"
```

12. **所以配置NAT46时，需要注意，IPv4 VIP的extip不要配置成和入接口地址相同的地址，配置不会报错，但实际会不通，如果是IPv4的第二地址，实际测试也是不行的。**

CLI相关

VIP CLI

1. IPv4类型的VIP支持三种组合，NAT44、NAT46、NAT44+NAT46。

```
config firewall vip
    edit "vip1"
        set extip 30.0.0.110-30.0.0.120
        set extintf "port3"
        set arp-reply disable
        set portforward enable
        set srcintf-filter "port3"
        set nat44 disable    <-------- new option enabled by default
        set nat46 enable    <-------- new option disabled by default
        set ipv6-mappedip 2040::20-2040::30    <-------- new option available when nat46 enabled
        set extport 10
        set ipv6-mappedport 100    <-------- new option available when nat46 enabled
    next
end
```

2. NAT46也支持Virtual Server，开启NAT46后，RS必须配置为IPv6地址，实现的NAT过程和普通的NAT46是一样的。

```
config firewall vip
    edit "vip_svr"
        set type server-load-balance
        set extip 30.0.0.130
        set extintf "port3"
        set arp-reply disable
        set server-type http
        set monitor "ping-mon-l"
        set nat46 enable
        set extport 80
            config realservers
                edit 1
                    set ip 2040::20    <-------- server ip must be ipv6 when nat46 is enabled


```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                    set port 80
                next
            end
        next
    end
```

3. IPv6类型的VIP支持三种组合，NAT66、NAT64、NAT66+NAT64。

```
config firewall vip6
    edit "vip3"
        set extip 2002::100-2002::200
        set portforward enable
        set nat66 disable    <------ new option enabled by default
        set nat64 enable    <------ new option disabled by default
        set ipv4-mappedip 8.8.8.8-8.8.8.108    <------- new option available when nat64 is enabled
        set ipv4-mappedport 1000    <------ new option available when nat64 is enabled
        set extport 100
    next
end
```

IPPool CLI

1. IPv4类型的IPPool，类型为NAT64，地址池范围必须是一个subnet的范围，默认会开启add-nat64-route。

```
config firewall ippool
    edit "pol64"
        set startip 10.0.0.0    <------ ip range must be a subnet if nat64 enabled
        set endip 10.0.255.255
        set nat64 enable    <------ new option
        set add-nat64-route enable    <------- new option available when nat64 enabled (by default enable)
    next
end
```

2. IPv6类型的IPPool，类型为NAT46，地址池范围必须是一个subnet的范围，默认会开启add-nat46-route。

```
config firewall ippool6
    edit "pol46"
        set startip 2002::    <------ ip range must be a subnet if nat46 enabled
        set endip 2002::ffff
        set nat46 enable
        set add-nat46-route enable    <------- new option available when nat46 enabled (by default enable)
    next
end
```

Firewall Policy & Central SNAT CLI

1. NAT46 Firewall Policy。

```
config firewall policy
    edit 1
        set srcintf "port3"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "vip1"    <-- vip with nat46 enabled
        set srcaddr6 "all"
        set dstaddr6 "all"    <------ both ipv4 and ipv6 addresses are required when nat46 enable
        set action accept
        set schedule "always"
        set service "ALL"
        set dnsfilter-profile "default"
        set ippool enable
        set poolname6 "ipv6_po1"    <------ ipv6 pool with nat46 enabled
        set nat46 enable    <------- new option to enable nat46
    next
end
```

2. NAT46 Central SNAT。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall central-snat-map
    edit 2
        set srcintf "any"
        set dstintf "any"
        set orig-addr "all"
        set dst-addr "all"
        set nat46 enable    ←——— new option for ipv4 rule
        set nat-ippool6 "ipv6_po1"    ←——— available when nat46 is enabled, ipv6 pool with nat46 enabled
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DHCPv6原理

DHCPv6获取方式

1. DHCPv6客户端获取Global Address的方式有两种：
   - 无状态（Stateless）：根据路由通告报文RA（Router Advertisement）包含的prefix前缀信息自动配置IPv6地址，组成方式是Prefix + (EUI64 or 随机)，Stateless也可以称为SLAAC（Stateless Address Auto Configuration）。
   - 有状态（Stateful）：通过DHCPv6方式获得IPv6地址。
2. 上边的有状态又分为两种方式：
   - 有状态DHCPv6（Stateful DHCPv6）：IPv6地址、其他参数（如DNS）均通过DHCPv6获取。
   - 无状态DHCPv6（Stateless DHCPv6）：IPv6地址依然通过路由通告RA方式生成，其他参数（如DNS）通过DHCPv6获取。

重要

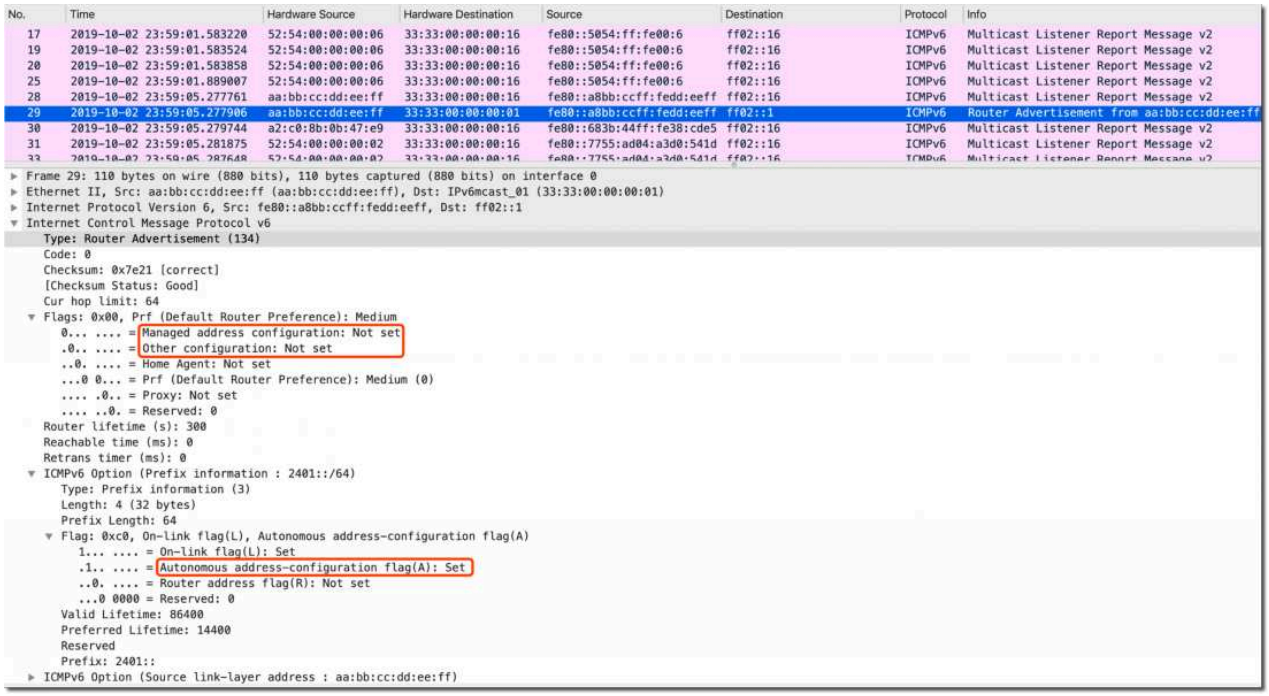
适用场景：

- 有状态、无状态仅针对于IPv6地址分配方式，并不包含其他参数。
- 有状态：可控、可管理。在网络中存在一个IP地址管理者，它能够识别客户端，根据不同的客户端，分配对应的IPv6地址，客户端与服务端之间需要维护IP地址的租期及续约。目前实现这种效果的，就是DHCPv6协议，IP地址管理者就是DHCPv6 Server。
- 无状态：不可控、难管理。在网络中只有网关，没有IP地址管理者。因此无人去识别客户端，每个客户端根据网关发送的相同的RA报文内容，自行配置IPv6地址。

IPv6 RA中的Flag

1. DHCPv6客户端通过网络中路由器/防火墙发送的IPv6 RA（Router Advertisement）报文中的Flag来控制获取IPv6和DNS等信息的方式。
   - Autonomous flag（自治flag，简称A flag）：表示是否配置无状态IP。在一个RA报文中，可存在多个prefix，比如2401/64、2403::/64，每个prefix都可以独立配置A flag。
     - 为on时（对应bit位为1）：表示客户端应当在该prefix范围内自动生成IPv6地址（客户端通过DAD_Duplicate Address Detection自行保证地址可用），并配置子网路由条目、网关。
     - 为off时（对应bit位为0）：表示客户端不应当在该prefix范围内自动生成IPv6地址，但是可以配置子网路由条目、网关。
   - Managed flag（简称M flag）：表示是否配置有状态IP。M flag是RA报文的全局参数，一个RA报文只有一个M flag。
     - 为on时（对应bit位为1）：表示在stateless流程结束后开始stateful流程，也就是告诉客户端可以通过DHCPv6来获得IPv6地址和其他参数（如DNS列表）。
     - 为off时（对应bit位为0）：表示不通过DHCPv6来获得IPv6地址。
   - Other flag（简称O flag）：表示是否通过DHCPv6获得除IP以外的其他参数（如DNS列表）。O flag也是RA报文中的全局参数，一个RA报文只有一个O flag。注意：仅当M flag为off时，该参数才会被读取。
     - 为on时（对应bit位为1）：当M flag为on，或者M flag为off且至少有一个A flag为on时，将通过DHCPv6获得其他参数。
     - 为off时（对应bit位为0）：当M flag为on时，依然将通过DHCPv6获得其他参数；当M flag也为off时，将不通过DHCPv6获得其他参数。
2. 如下图的RA报文， A flag置为1，M flag和O flag均置为0，表示要求客户端仅通过RA中的prefix自动配置IPv6地址，并配置子网路由条目、网关，其他参数不通过DHCPv6获取。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



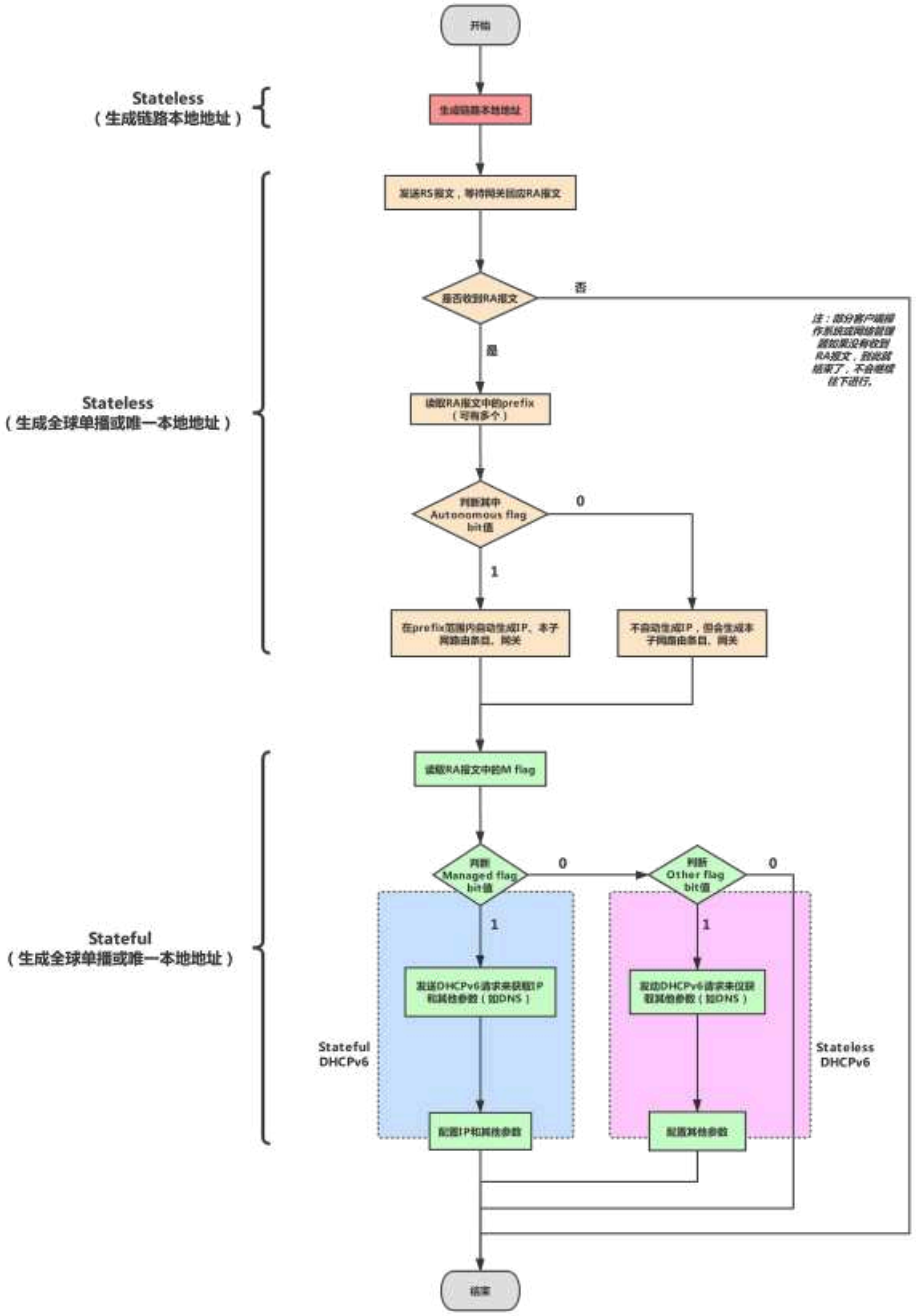
No.	Time	Hardware Source	Hardware Destination	Source	Destination	Protocol	Info
17	2019-10-02 23:59:01.583220	52:54:00:00:00:06	33:33:00:00:00:16	fe80::5054:ff:fe00:6	ff02::16	ICMPv6	Multicast Listener Report Message v2
19	2019-10-02 23:59:01.583524	52:54:00:00:00:06	33:33:00:00:00:16	fe80::5054:ff:fe00:6	ff02::16	ICMPv6	Multicast Listener Report Message v2
20	2019-10-02 23:59:01.583858	52:54:00:00:00:06	33:33:00:00:00:16	fe80::5054:ff:fe00:6	ff02::16	ICMPv6	Multicast Listener Report Message v2
25	2019-10-02 23:59:01.889007	52:54:00:00:00:06	33:33:00:00:00:16	fe80::5054:ff:fe00:6	ff02::16	ICMPv6	Multicast Listener Report Message v2
28	2019-10-02 23:59:05.277761	aa:bb:cc:dd:ee:ff	33:33:00:00:00:16	fe80::a8bb:ccff:fedd:eeff	ff02::16	ICMPv6	Multicast Listener Report Message v2
29	2019-10-02 23:59:05.277906	aa:bb:cc:dd:ee:ff	33:33:00:00:00:01	fe80::a8bb:ccff:fedd:eeff	ff02::1	ICMPv6	Router Advertisement from aa:bb:cc:dd:ee:ff
30	2019-10-02 23:59:05.279744	a2:c0:8b:0b:47:e9	33:33:00:00:00:16	fe80::683b:44ff:fe38:cde5	ff02::16	ICMPv6	Multicast Listener Report Message v2
31	2019-10-02 23:59:05.281875	52:54:00:00:00:02	33:33:00:00:00:16	fe80::7755:ad04:a3d0:541d	ff02::16	ICMPv6	Multicast Listener Report Message v2
33	2019-10-02 23:59:05.287648	52:54:00:00:00:02	33:33:00:00:00:16	fe80::7755:ad04:a3d0:541d	ff02::16	ICMPv6	Multicast Listener Report Message v2

```
▶ Frame 29: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▶ Ethernet II, Src: aa:bb:cc:dd:ee:ff (aa:bb:cc:dd:ee:ff), Dst: IPv6mcast_01 (33:33:00:00:00:01)
▶ Internet Protocol Version 6, Src: fe80::a8bb:ccff:fedd:eeff, Dst: ff02::1
▼ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x7e21 [correct]
    [Checksum Status: Good]
    Cur hop limit: 64
  ▼ Flags: 0x00, Prf (Default Router Preference): Medium
      0... .... = Managed address configuration: Not set
      .0.. .... = Other configuration: Not set
      ..0. .... = Home Agent: Not set
      ...0 0... = Prf (Default Router Preference): Medium (0)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 300
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ▼ ICMPv6 Option (Prefix information : 2401::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    ▼ Flag: 0xc0, On-link flag(L), Autonomous address-configuration flag(A)
        1... .... = On-link flag(L): Set
        .1.. .... = Autonomous address-configuration flag(A): Set
        ..0. .... = Router address flag(R): Not set
        ...0 0000 = Reserved: 0
      Valid Lifetime: 86400
      Preferred Lifetime: 14400
      Reserved
      Prefix: 2401::
  ▶ ICMPv6 Option (Source link-layer address : aa:bb:cc:dd:ee:ff)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

总结

DHCPv6流程



- Stateless自动配置“全球地址”（或“唯一本地地址”）。
- Stateful自动配置“全球地址”（或“唯一本地地址”）和其他参数，其中Stateful阶段中存在Stateful DHCPv6或Stateless DHCPv6。

重要

部分客户端操作系统或网络管理器当Stateless阶段没有收到RA报文后，就到此结束，不会走Stateful阶段，比如CentOS 7、Ubuntu 17的默认逻辑都是这样，而Windows Server就会继续走Stateful阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Flag组合对应客户端动作

Managed Flag	Other Flag	Autonomous Flag	RA IP	RA 子网路由	RA gateway	DHCPv6 IP	DHCPv6 dns
M on	O on	A on	Y	Y	Y	Y	Y
		A off	N	Y	Y	Y	Y
	O off	A on	Y	Y	Y	Y	Y
		A off	N	Y	Y	Y	Y
M off	O on	A on	Y	Y	Y	N	Y
		A off	N	Y	Y	N	Y
	O off	A on	Y	Y	Y	N	N
		A off	N	Y	Y	N	N

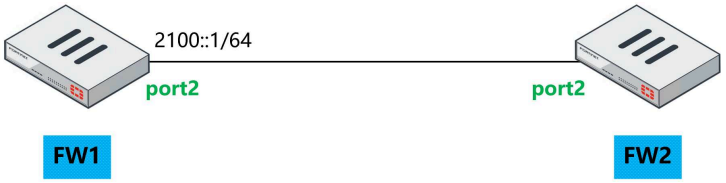
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

有状态模式

网络需求

FortiGate作为DHCPv6服务器，FortiGate或PC为客户端，客户端通过DHCPv6获取IPv6地址以及DNS等信息，不通过RA进行自动配置。

网络拓扑

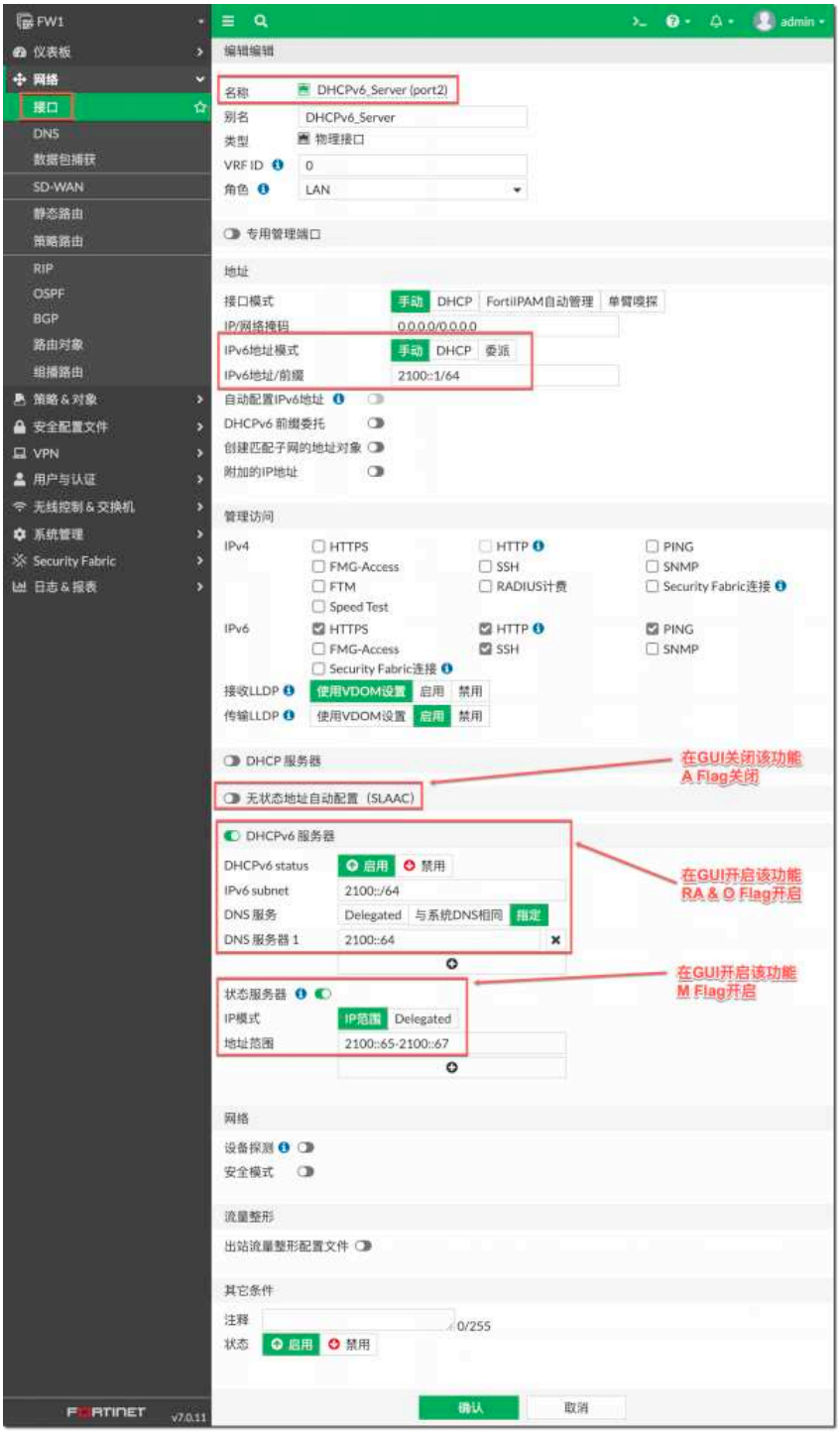


FW1和FW2（或PC）直连，FW1作为DHCPv6服务器，FW2（或PC）为客户端，FW2（或PC）通过DHCPv6获取IPv6地址以及DNS等信息，不通过RA进行自动配置。

配置步骤

1. FW1上配置IPv6地址2100::1/64，并关闭“无状态地址自动配置（SLAAC）”，开启“DHCPv6服务器”，配置DNS服务器，开启“状态服务器”，并配置分配IP范围。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

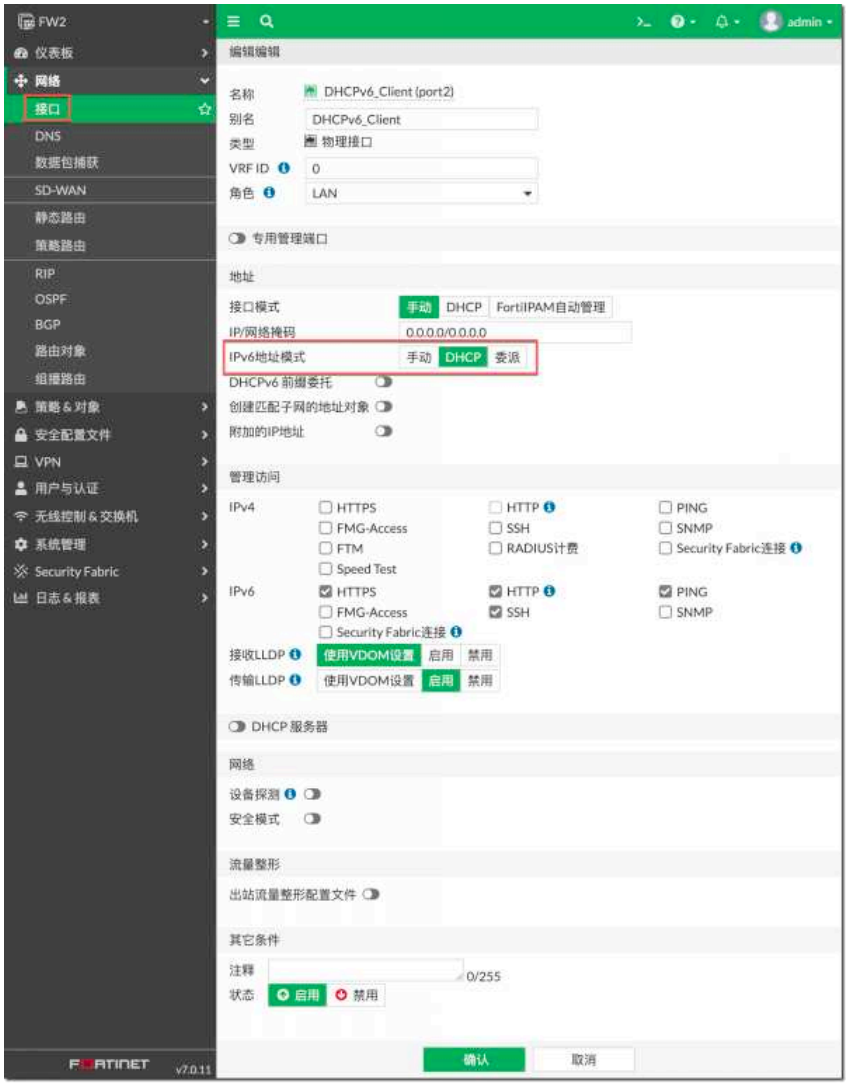



```
config system interface
    edit "port2"
        config ipv6
            set ip6-address 2100::1/64
            set ip6-allowaccess ping https ssh http
            set ip6-send-adv enable    //开启RA
            set ip6-manage-flag enable    //开启M Flag
            set ip6-other-flag enable    //开启O Flag
        end
    next
en

config system dhcp6 server
    edit 1
        set subnet 2100::/64
        set interface "port2"
        config ip-range
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            edit 1
                set start-ip 2100::65
                set end-ip 2100::67
            next
        end
        set dns-server1 2100::64
    next
end
```

2. FW2上配置port2的“IPv6地址模式”为“DHCP”。



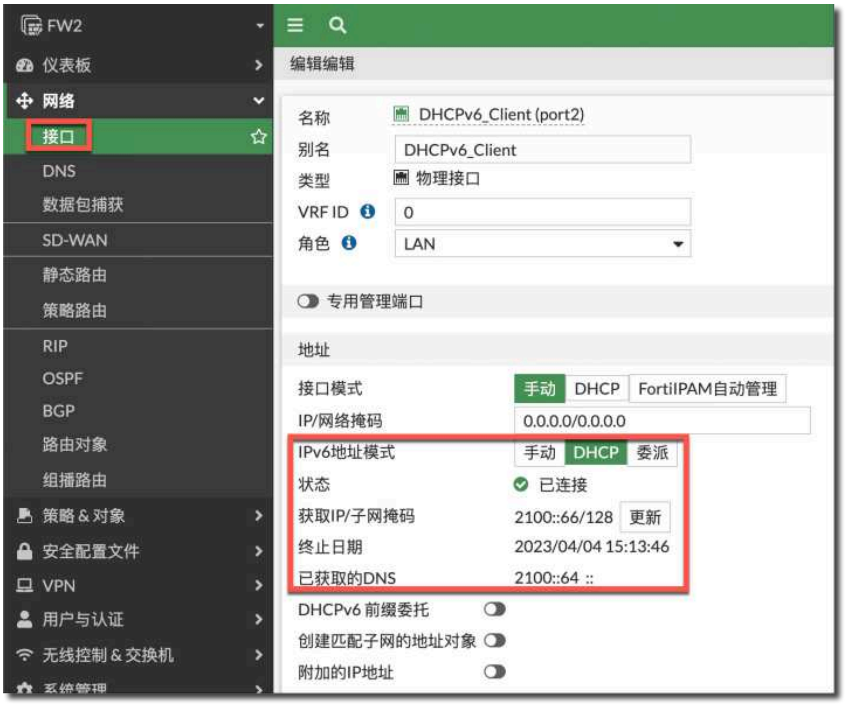

```
config system interface
    edit "port2"
        config ipv6
            set ip6-mode dhcp
        end
    next
end
```

结果验证

1. 在FW2上查看DHCPv6获取的IPv6地址和DNS服务器地址，并自动添加了IPv6网关为FW1的port2的IPv6本地链路地址。

> **重要**
>
> - FortiGate作为IPv6客户端时，获取IPv6地址后，默认路由的添加需要通过IPv6路由kernel表（get router info6 kernel）中看到。
> - 客户端添加的默认路由的下一跳为服务器端接口的IPv6本地地址，而非手工配置的IPv6地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



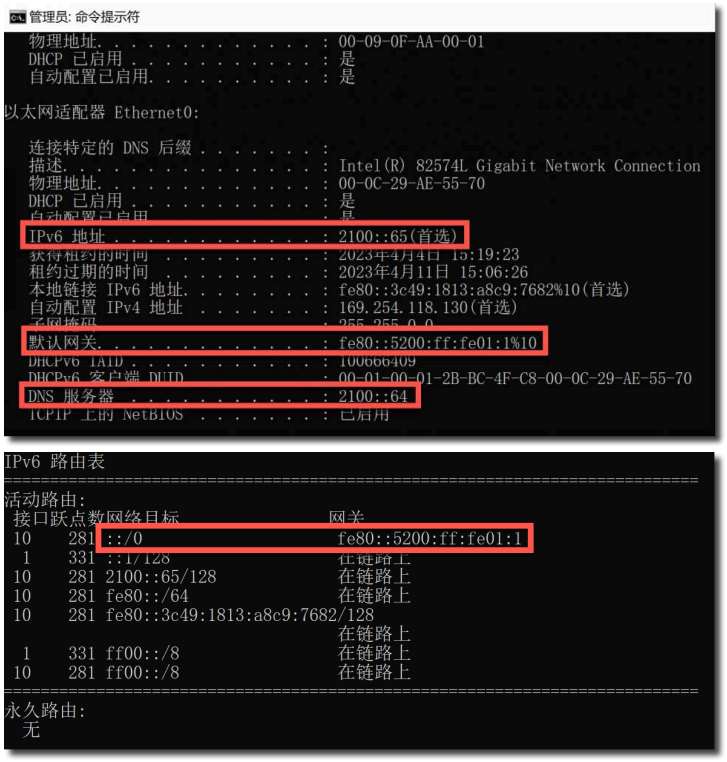

```
FW2 # config system interface
FW2 (interface) # edit port2

FW2 (port2) # get | grep ip6
    ip6-mode            : dhcp
    ip6-address         : 2100::66/128
    ip6-allowaccess     : ping https ssh http
    ip6-reachable-time  : 0
    ip6-retrans-time    : 0
    ip6-hop-limit       : 0
    vrip6_link_local    : ::
    ip6-dns-server-override: enable

FW2 (port2) # get | grep DNS
delegated-DNS1      : ::
delegated-DNS2      : ::
Acquired DNS1       : 2100::64
Acquired DNS2       : ::
Acquired DNS1       : 0.0.0.0
Acquired DNS2       : 0.0.0.0
```

```
FW2 # get router info6 kernel | grep gwy
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00450000 prio=1024 gwy:fe80::5200:ff:fe01:1 dev=4(port2)
pmtu=1500

FW1 # diagnose ipv6 address list | grep port2
dev=4 devname=port2 flag=P scope=0 prefix=64 addr=2100::1 preferred=4294967295 valid=4294967295 cstamp=1790
tstamp=1790
dev=4 devname=port2 flag=P scope=253 prefix=64 addr=fe80::5200:ff:fe01:1 preferred=4294967295 valid=4294967295
cstamp=1790 tstamp=1790
```

2. 使用Windows PC替换FW2，来获取IPv6地址，可以看到Windows客户端获取到了2100::/64前缀的IPv6地址，并将FW1的port2的IPv6本地地址作为IPv6网关。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
FW1 # diagnose ipv6 address list | grep port2
dev=4 devname=port2 flag=P scope=0 prefix=64 addr=2100::1 preferred=4294967295 valid=4294967295 cstamp=1790
tstamp=1790
dev=4 devname=port2 flag=P scope=253 prefix=64 addr=fe80::5200:ff:fe01:1 preferred=4294967295 valid=4294967295
cstamp=1790 tstamp=1790
```

3. FW1上查看DHCPv6地址分配情况。

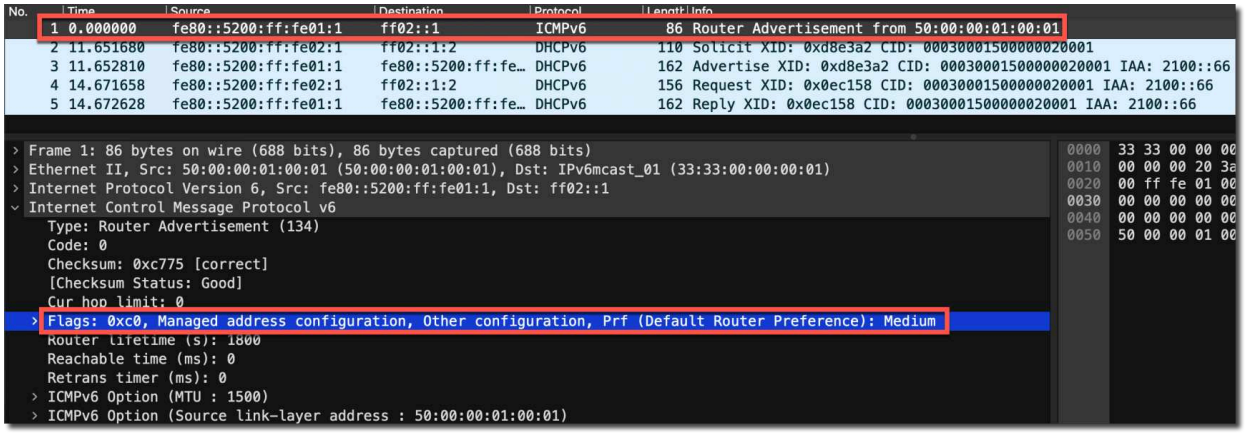


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

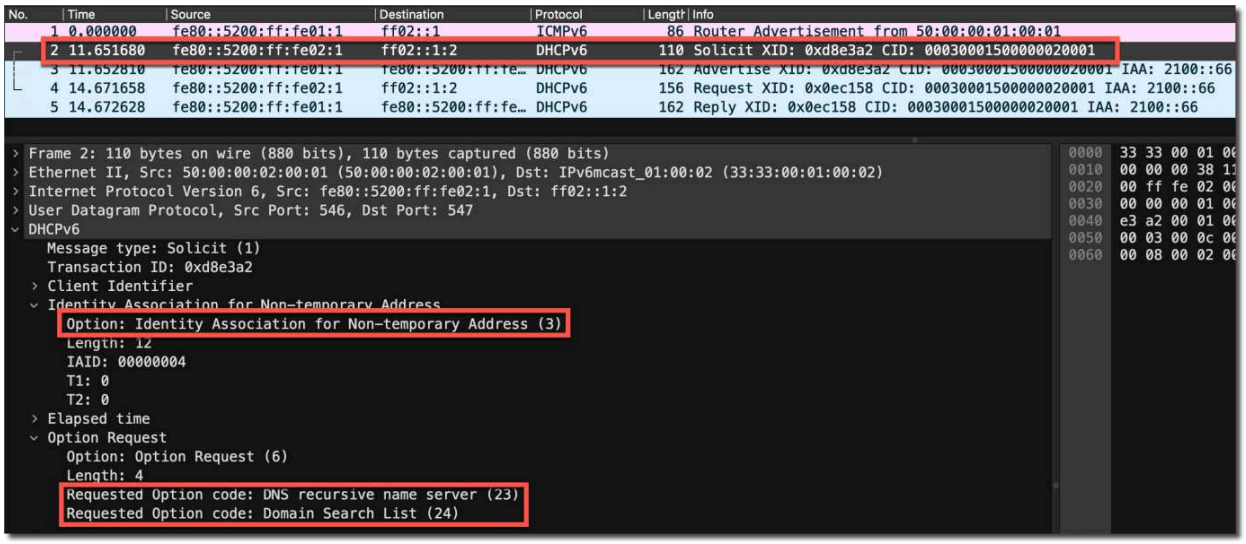
```
FW1 # exe dhcp6 lease-list port2
Interface       DUID                                          IAID       IP/Prefix                    Expiry
port2           00:01:00:01:2b:bc:4f:c8:00:0c:29:ae:55:70     100666409  2100::65                     Tue Apr 11
15:19:19 2023

port2           00:03:00:01:50:00:00:02:00:01                 4          2100::66                     Tue Apr 11
15:25:13 2023
```

4. 抓包查看整个流程。

   - 查看FW1发出的RA报文，可以看到RA中开启了M和O Flag，未开启A Flag（没有SLAAC prefix）。

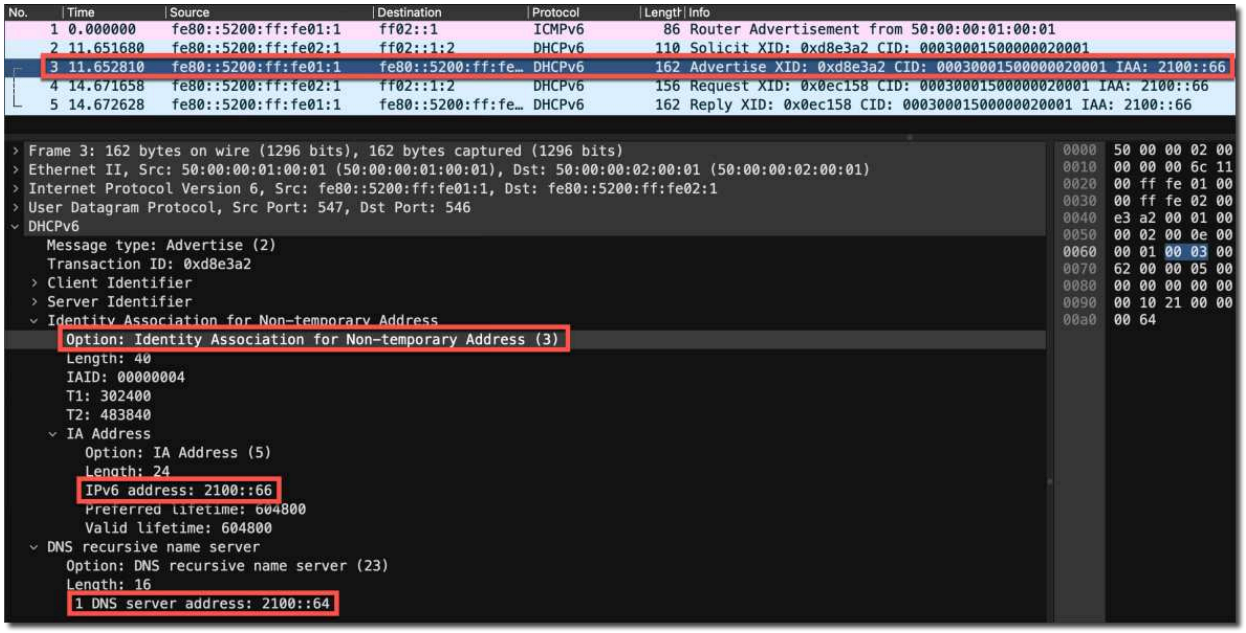


   - FW2配置接口模式为DHCPv6后，发出DHCPv6 Solicit报文，请求非临时IP地址与DNS地址，目标IP地址（ff021:2 ）和MAC均为组播。

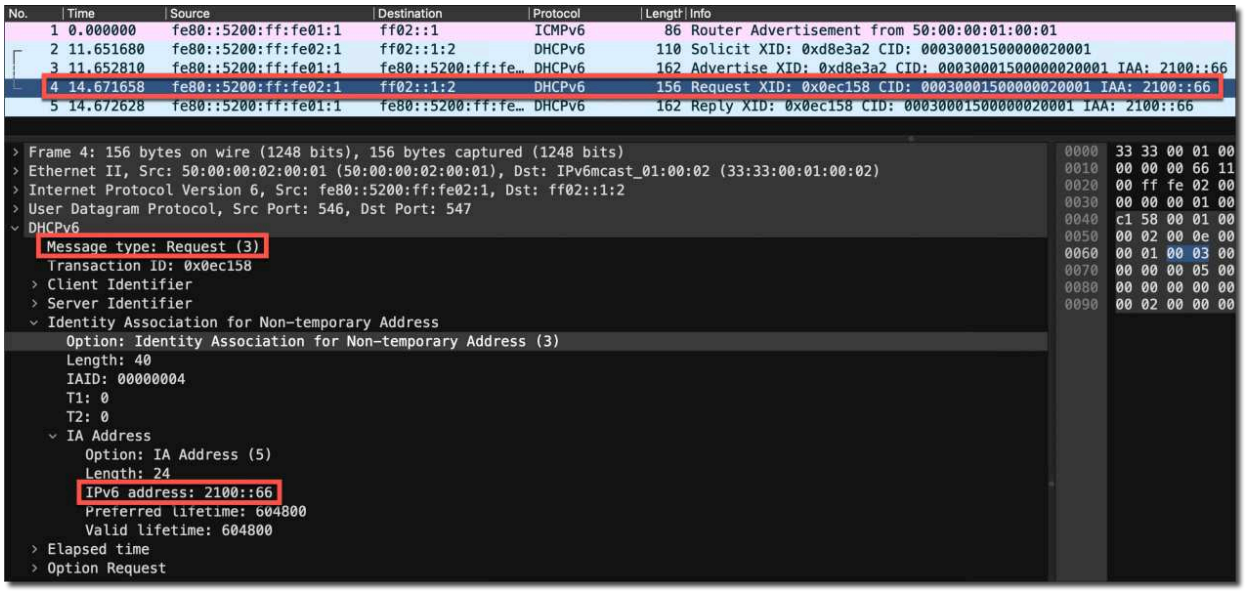


   - FW1返回DHCPv6 Advertise报文，包含可用的IPv6地址以及DNS服务器地址，报文为单播，目标IP地址为FW2的本地IPv6地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

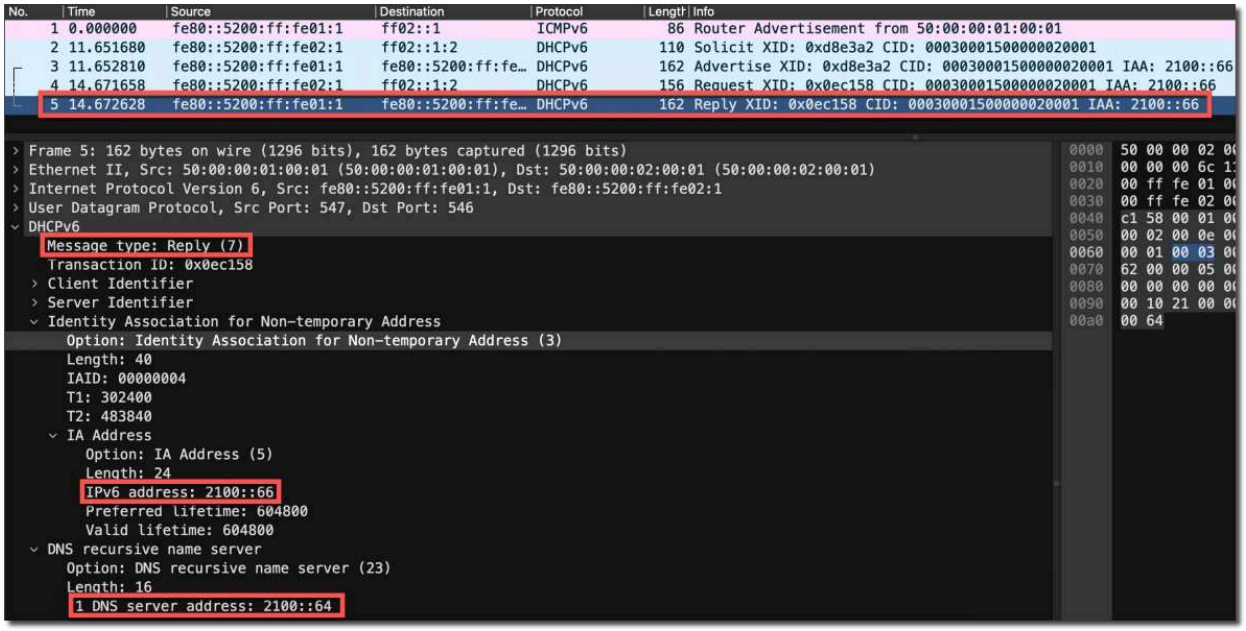


- FW2请求占用FW1提供的IPv6 21001:2， DHCPv6保留的组播地址ff02::1:2 ）和MAC均为组播。



- FW1发送DHCPv6 Reply报文，确认客户端可以使用该IPv6并携带了DNS服务器地址，目标IP为单播FW2的本地IPv6地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



补充说明

1. 服务器端（FW1）A Flag和M Flag同时开启，客户端（FW2）会生成几个地址?

   - 客户端（FW2）的IPv6地址配置为“Manual”+“Auto configure IPv6 addres”时，只会发出RS报文，然后FW1返回RA报文，客户端根据RA中的prefix自动配置地址。
   - 客户端（FW2）的IPv6地址配置为“DHCP”时，不会发出RS报文，只会发出DHCPv6报文，然后通过DHCPv6获取IP和DNS等信息，即使服务器端发出了携带prefix的RA报文，FW2依然会通过DHCPv6获取IP地址和DNS等信息。
   - 也就是对于FortiGate作为Client，Server同时开启M和A Flag，地址生成方式取决于客户端的IPv6地址模式。
   - 对于PC Client来说，当配置为DHCP获取地址时，仍然会发出RS报文，通过Server端发出的RA报文中的Flag来确定地址获取的方式，当RA中的A Flag和M Flag同时开启时，PC Client会同时获取两种地址，一种从RA中的prefix自动生成，一种从DHCPv6 Server获取，如下图所示。



2. 接口下开启DHCPv6状态服务器后，请确保DHCPv6分配的IPv6地址与该接口的IPv6地址在同一网段，否则状态服务器不会响应任何DHCPv6请求。

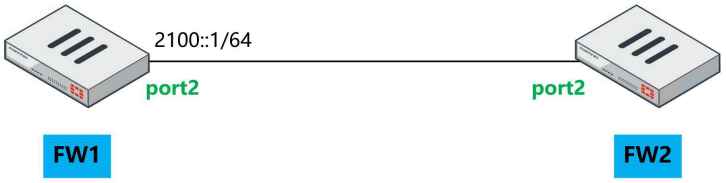
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

无状态 + 有状态模式

网络需求

FortiGate作为DHCPv6服务器，FortiGate或PC为客户端，客户端从FortiGate的RA报文中自动配置IPv6地址，并使用DHCPv6从FortiGate获取DNS服务器地址。

网络拓扑

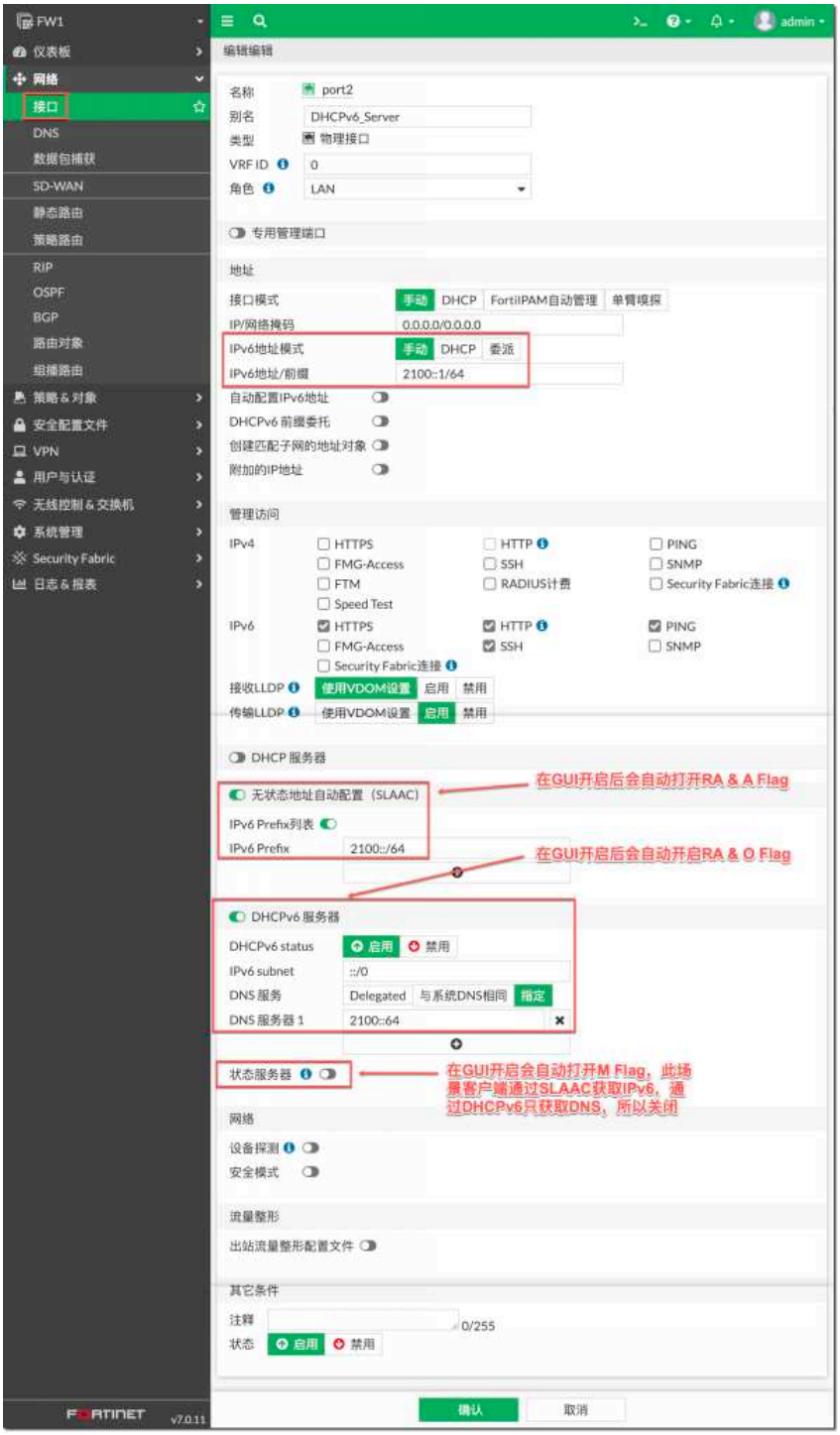


FW1和FW2（或PC）直连，FW1作为DHCPv6服务器，FW2（或PC）为客户端，FW2（或PC）从FW1的RA报文中自动配置IPv6地址，并使用DHCPv6从FW1获取DNS服务器地址。

配置步骤

1. FW1上配置IPv6地址2100/64，开启“DHCPv6服务器”，配置DNS服务器，不开启“状态服务器”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config system interface
    edit "port2"
        config ipv6
            set ip6-address 2100::1/64
            set ip6-allowaccess ping https ssh http
            set ip6-send-adv enable    //开启RA
            set ip6-other-flag enable    //开启O Flag
            set ip6-manage-flag disable    //关闭M Flag
            config ip6-prefix-list
                edit 2100::/64
                    set autonomous-flag enable    //开启A Flag
                next
            end
        end
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config system dhcp6 server
    edit 1
        set subnet 2100::/64
        set interface "port2"
        set dns-server1 2100::64
    next
end
```

2. FW2上配置port2的IPv6配置为“手动”模式，开启“自动配置IPv6地址”。



3. FW2想要从FW1获取静态地址后，再通过DHCPv6获取DNS服务器信息，需要开启dhcp6-Information-request，该功能只能在CLI下开启，用于在IPv6自动配置后再通过DHCPv6获取DNS服务器等信息，最终配置如下。

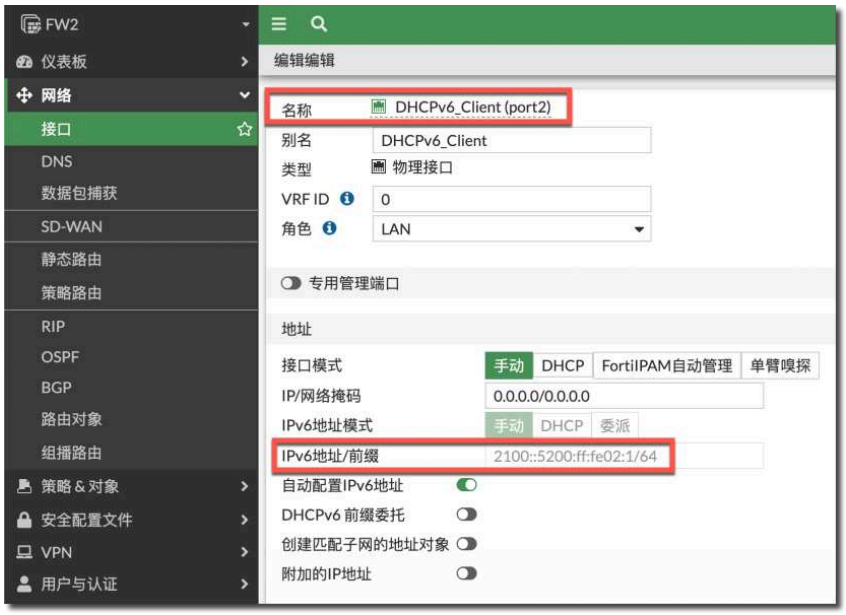
```
config system interface
    edit "port2"
        config ipv6
            set ip6-allowaccess ping https ssh http
            set dhcp6-information-request enable
            set autoconf enable
        end
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

1. 在FW2上查看自动配置的IPv6地址和DNS服务器地址，自动配置的IPv6地址根据前缀 + EUI自动生成，DNS通过DHCPv6获取，并自动添加了IPv6网关为FW1的port2的IPv6本地链路地址。

> **重要**
> - FortiGate作为IPv6客户端时，获取IPv6地址后，默认路由的添加需要通过IPv6路由kernel表（get router info6 kernel）中看到。
> - 客户端添加的默认路由的下一跳为服务器端接口的IPv6本地地址，而非手工配置的IPv6地址。



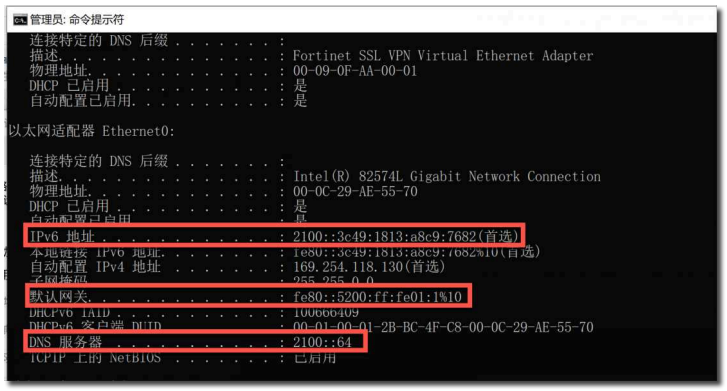

```
FW2 # config system interface
FW2 (interface) # edit port2
FW2 (port2) # get | grep ip6
    ip6-mode            : static
    ip6-address         : 2100::5200:ff:fe02:1/64
    ip6-allowaccess     : ping https ssh http
    ip6-reachable-time  : 0
    ip6-retrans-time    : 0
    ip6-hop-limit       : 0
    vrip6_link_local    : ::
    ip6-dns-server-override: enable
    ip6-send-adv        : disable

FW2 (port2) # get | grep DNS
Acquired DNS1       : 2100::64
Acquired DNS2       : ::
Acquired DNS1       : 0.0.0.0
Acquired DNS2       : 0.0.0.0
```

```
FW2 # get router info6 kernel | grep gwy
vf=0 tbl=254 type=01(unicast) protocol=2(kernel) flag=00450000 prio=1024 gwy:fe80::5200:ff:fe01:1 dev=4(port2)
pmtu=1500

FW1 # diagnose ipv6 address list | grep port2
dev=4 devname=port2 flag=P scope=0 prefix=64 addr=2100::1 preferred=4294967295 valid=4294967295 cstamp=1790
tstamp=1790
dev=4 devname=port2 flag=P scope=253 prefix=64 addr=fe80::5200:ff:fe01:1 preferred=4294967295 valid=4294967295
cstamp=1790 tstamp=1790
```

2. 使用Windows PC替换FW2，来获取IPv6地址，可以看到Windows客户端获取到了2100::/64前缀的IPv6地址，并将FW1的port2的IPv6本地地址作为IPv6网关。

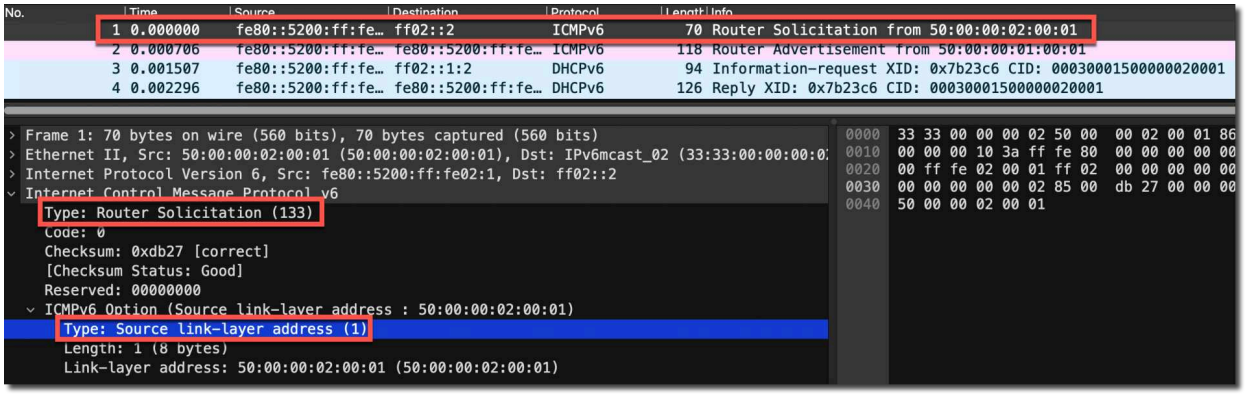
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





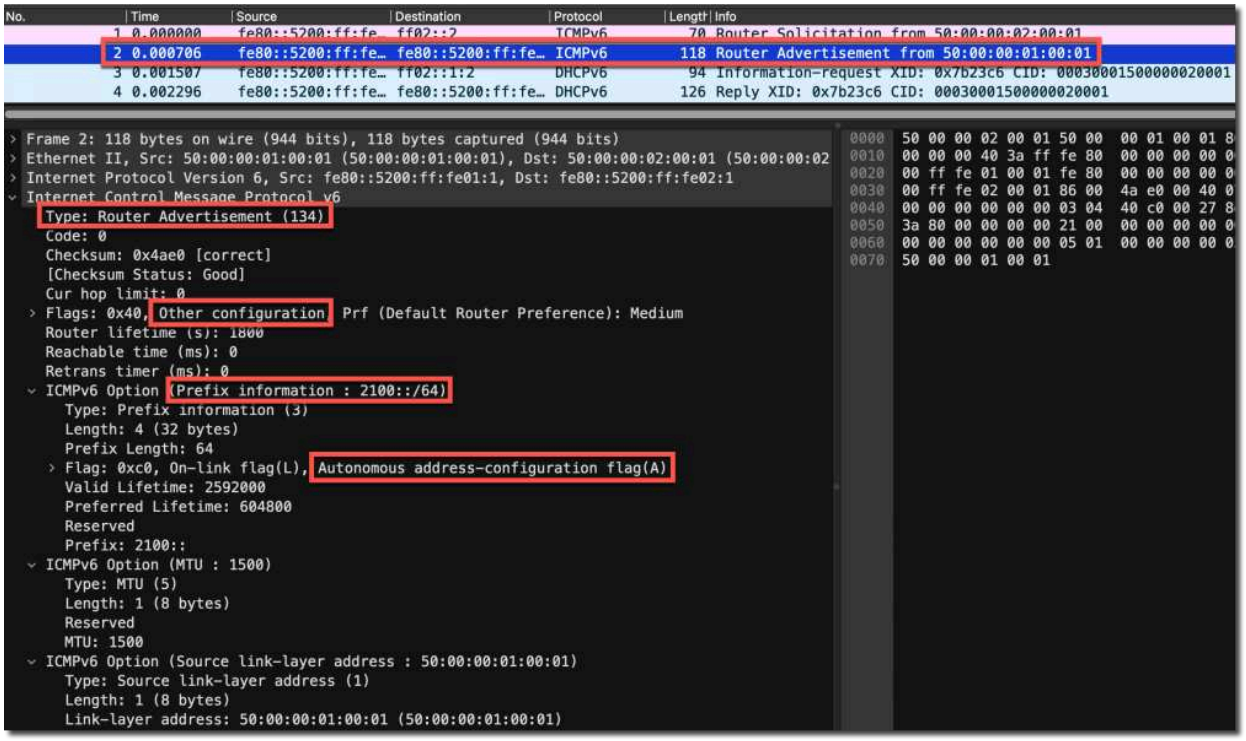

```
FW1 # diagnose ipv6 address list | grep port2
dev=4 devname=port2 flag=P scope=0 prefix=64 addr=2100::1 preferred=4294967295 valid=4294967295 cstamp=1790
tstamp=1790
dev=4 devname=port2 flag=P scope=253 prefix=64 addr=fe80::5200:ff:fe01:1 preferred=4294967295 valid=4294967295
cstamp=1790 tstamp=1790
```

3. 抓包查看整个流程。
   - FW2配置自动配置后，发出RS报文，请求IP地址配置，目标IP（ff02::2，链路本地范围的所有路由器）和MAC均为组播。

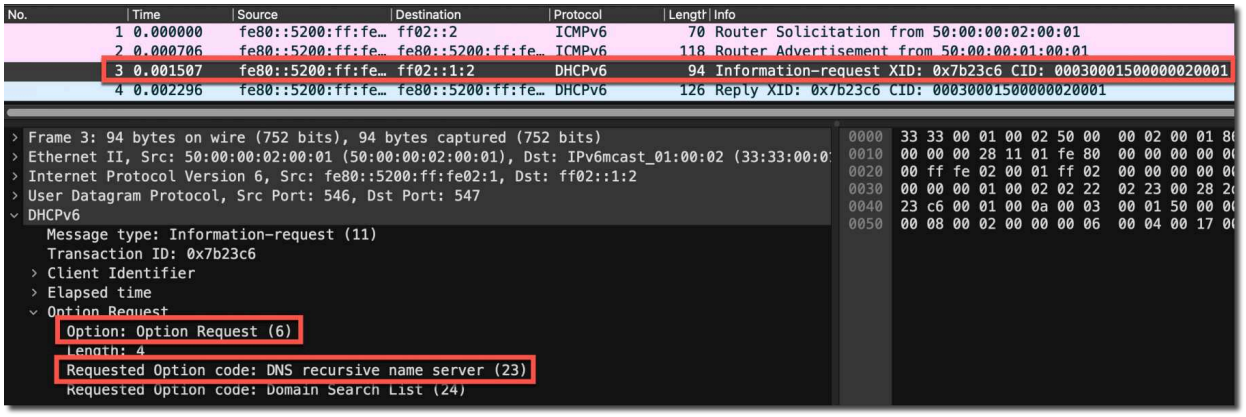


   - FW1发送RA报文，通报自身IPv6 prefix-list，可以看到前缀网段中标记了A Flag，RA中标记了O Flag，该报文为单播。

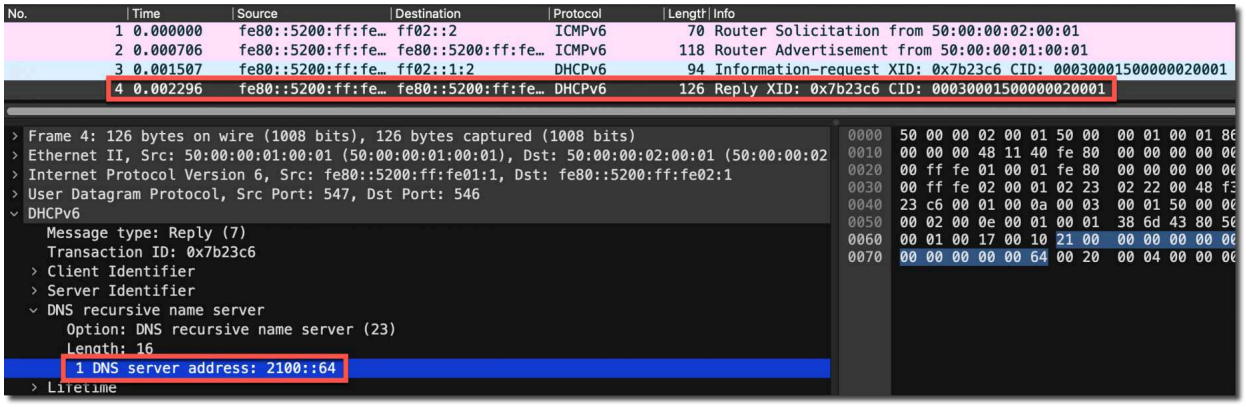
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 由于开启了DHCP6-Information-request，FW2会继续通过DHCPv6请求DNS服务器等信息，该报文为组播，目标IP为DHCPv6保留的组播地址ff02::1:2。



- FW1返回DHCPv6 Reply给FW2，携带DNS服务器地址，该报文为单播。



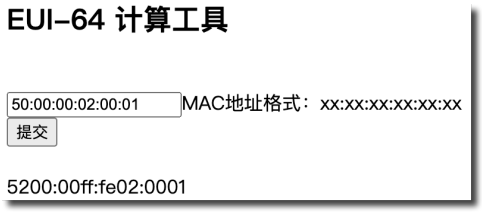
补充说明

1. 客户端获取到Prefix后，有两种方式生成IPv6地址：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- Prefix+EUI-64（FortiGate使用）：自动将48bit的以太网MAC地址扩展成64bit，再组合一个≤64位的IPv6地址前缀，组成一个IPv6地址（Link-Local地址也是通过此方法生成）。经过测试，如果Prefix不足64位，则用0补齐Prefix和EUI-64之间的内容（根据EUI-64计算器，您可自行查看上述步骤中FW2获取的IPv6地址是否符合EUI64标准）。

```
FW2 # diagnose netlink dstmac list port2
dev=port2 mac=50:00:00:02:00:01 policy6 rx_tcp_mss=0 tx_tcp_mss=0
...
```



- 随机生成：RFC4941引入了一种随机地址机制，他包含了用一组随机数字代替由MAC地址转换的接口ID。该地址具有一定的生存周期，随着生存周期的结束，该地址会自动更换，该地址在用户对外发起连接的时候充当连接发起的IPv6地址，这一行为的目的在于保证主机在对外通信时候的匿名性。Windows、macOS和Linux默认均为这种方式生成IPv6，可以使用如下命令关闭随机地址。

```
Windows:
netsh interface IPV6 set global randomizeidentifiers=disabled    //禁用地址随机
netsh interface ipv6 set privacy state=disable    //禁用临时地址

linux下修改sysctl.conf:
net.ipv6.conf.all.use_tempaddr=0
net.ipv6.conf.eth0.use_tempaddr=0
net.ipv6.conf.default.use_tempaddr=0
或sysctl net.ipv6.conf.INTERFACE.use_tempaddr=0

macOS:
sysctl net.inet6.ip6.use_tempaddr=0
```

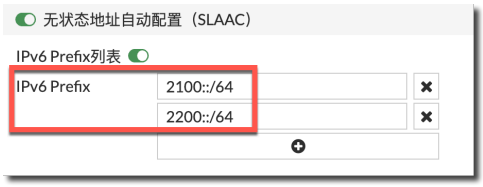
重要

EUI的生成过程详见：https://ccie.lol/knowledge-base/ipv6-use-eui-64-convert-link-local-address/

EUI-64在线生成器：http://www.wlts.cc/eui64/eui64.php ，https://www.vultr.com/zh/resources/mac-converter/

2. RA中包含多个prefix时，客户端是否会自动配置多个IPv6?

- 服务器端（FW1）的SLAAC配置两个prefix（RA报文中包含两个prefix）。

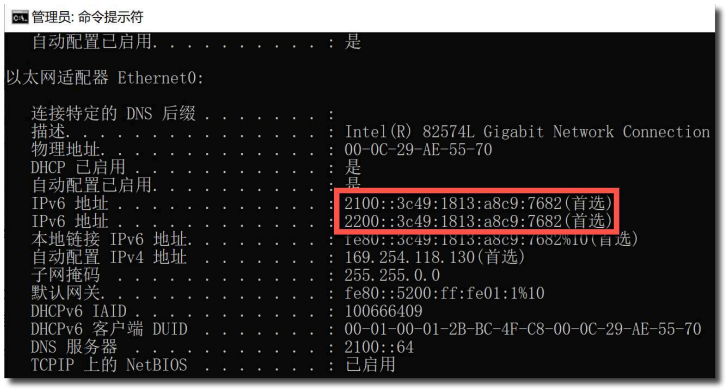


- 客户端（FW2）自动配置IPv6地址，可以看到两个prefix均生成了IPv6地址。

```
FW2 # diagnose ipv6 address list | grep port2
dev=4 devname=port2 flag= scope=0 prefix=64 addr=2200::5200:ff:fe02:1 preferred=604794 valid=2591994
cstamp=255528 tstamp=258728
dev=4 devname=port2 flag= scope=0 prefix=64 addr=2100::5200:ff:fe02:1 preferred=604794 valid=2591994
cstamp=139822 tstamp=258728
dev=4 devname=port2 flag=P scope=253 prefix=64 addr=fe80::5200:ff:fe02:1 preferred=4294967295 valid=4294967295
cstamp=2901 tstamp=2901
```

- PC客户端也会生成2个prefix的IPv6地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DHCPv6-PD

网络需求

DHCPv6-PD（Prefix Delegation，前缀分配）是DHCPv6的扩展，传统的DHCPv6注重的是将地址等网络配置参数从服务器端传递给IPv6客户主机，而DHCPv6-PD注重的是前缀分配，即PD服务器端将一个子网范围的前缀地址段以及DNS等其他网络配置信息下发给PD客户端，这就意味PD服务器下发的是一个**“**子网地址段”，而不是具体的可以直接供主机使用的IPv6地址。

举个例子，PD服务器可以将2022:da8::/60前缀通过某个IPv6接口下发给PD客户端，同时一般会在PD客户端的上联设备上生成相应的路由。PD客户端收到该前缀后，可以在本地IPv6接口上动态使用该前缀的/64子网地址。

那么DHCPv6-PD到底用在什么场景中呢？这样做又有什么好处呢？DHCPv6-PD在运营商场景中最为常见，当然也可以用在其他较大的分层设计的网络中。

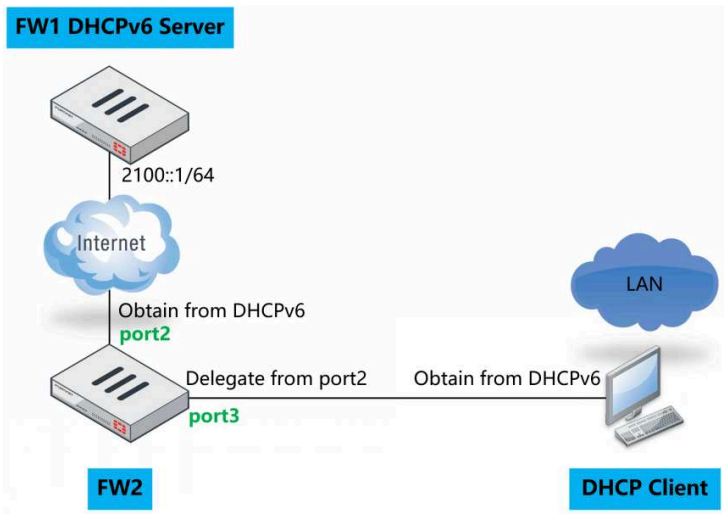
以运营商为例，DHCPv6-PD服务器往往是供应商边界（Provider Edge，PE）路由器，而DHCPv6-PD客户端则是客户前置设备（Customer Premise Equipment，CPE）路由器。首先，PE路由器作为PD服务器，会提前设置好一定范围的前缀分配列表，然后将这些前缀列表通过直连CPE的接口自动分配给各个CPE路由器。然后，CPE路由器从上联接口收到PE路由器自动分配的前缀后，对此前缀做子网划分，这个子网划分一般是提前规划好并应用在各个下联接口的。待获取到前缀后，CPE路由器自动就在各个下联接口下生成了IPv6地址，并可进一步通过自动地址配置技术下发给最终客户主机使用。

DHCPv6-PD请求过程

- PD客户端向PD服务器发送DHCPv6请求报文，此报文携带IA_PD选项，表明自己需要申请IPv6前缀。
- PD服务器收到请求报文后，从自己的前缀列表池中取出可用的前缀，附带在IA_PD选项中，回复给PD客户端。
- 前缀分配到期后，PD客户端重新向PD服务器发送DHCPv6请求报文，请求更新前缀。
- PD服务器重新为PD客户端分配前缀（在原有前缀未被占用的情况下，一般就是续租）。
- PD客户端需要释放前缀时，向PD服务器发送快速请求报文，以释放前缀。
- PD服务器接收快速请求报文后，回收前缀，并对PD客户端的快速请求报文进行回应。

从上述通信过程可以看出，DHCPv6-PD与DHCPv6的主要区别就是前者申请的是前缀，后者申请的是地址。

网络拓扑



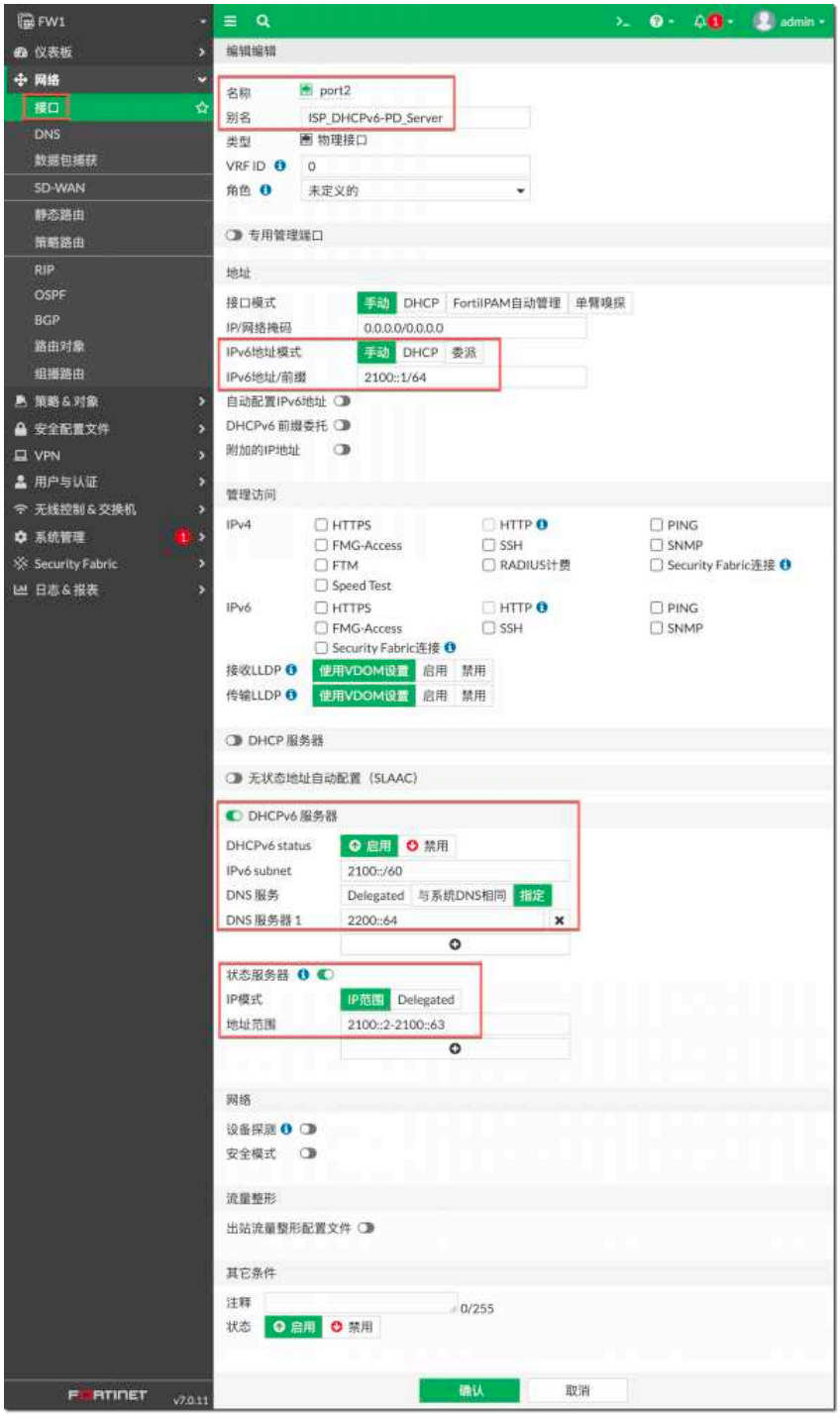
- FW1的port2从DHCPv6-PD服务器获取IPv6地址和Prefix，port3通过Delegate（继承）的方式从port2获取IPv6前缀，配合自身配置的subnet组成port3的IPv6地址。
- FW1的port3开启delegated DHCP Server，为内网PC分配port2获取的前缀中的IPv6地址。

配置步骤

FW1（模拟ISP）

1. FW1配置DHCPv6 Server，模拟Internet运营商。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system interface
    edit "port2"
        config ipv6
            set ip6-address 2100::1/64
            set ip6-send-adv enable
            set ip6-manage-flag enable
            set ip6-other-flag enable
        end
    next
end
```

2. FW1开启DHCPv6-PD服务器，该功能只能在CLI开启。在config system dhcp6 server中，config prefix-range为PD的配置，这里的配置就是可以给FW2分配的Prefix范围。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

这个范围不能超过prefix-length，比如运营商的地址池为60位，分配的prefix为64位，则最多可以分配$2^{(64-60)}$=16个prefix，否则下发配置报错。

```bash
config system dhcp6 server
    edit 1
        set subnet 2100::/60
        set interface "port2"
        config prefix-range
            edit 1
                set start-prefix 2100:0:0:3::
                set end-prefix 2100:0:0:4::
                set prefix-length 64
            next
        end
        config ip-range
            edit 1
                set start-ip 2100::2
                set end-ip 2100::63
            next
        end
        set dns-server1 2200::64
    next
end
```

FW2（模拟用户边界设备）

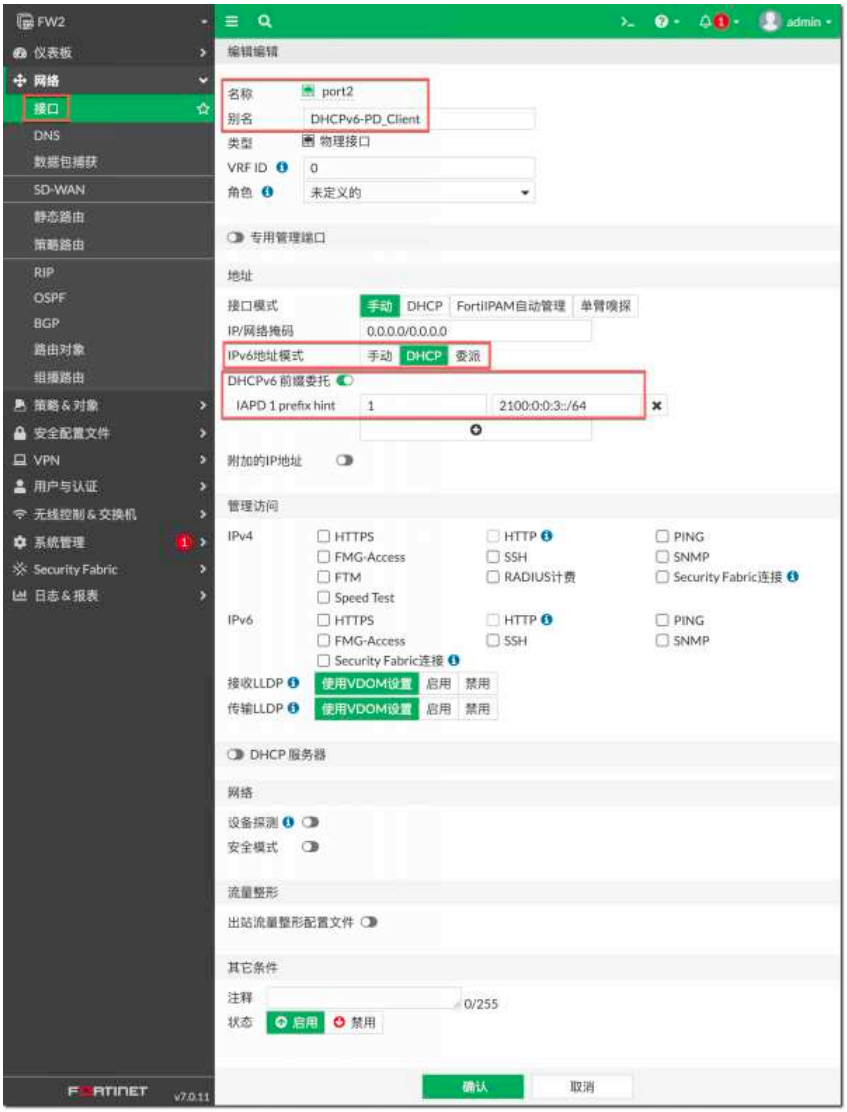
1. FW2上配置port2接口的IPv6为DHCP方式获取，并开启DHCPv6 prefix delegation，填写DHCPv6 prefix hint为想要从DHCPv6-PD服务器获取的prefix。

重要

这里的DHCPv6 prefix hint ID（dhcp6-iapd-list ID）最好配置为1，否则在下步GUI配置继承接口时，无法选择到上游接口（CLI可以配置）。

如果不知道需要向运营商申请哪一个prefix，请填写为::/0，表示不指定请求的prefix，让运营商选择分配的prefix。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

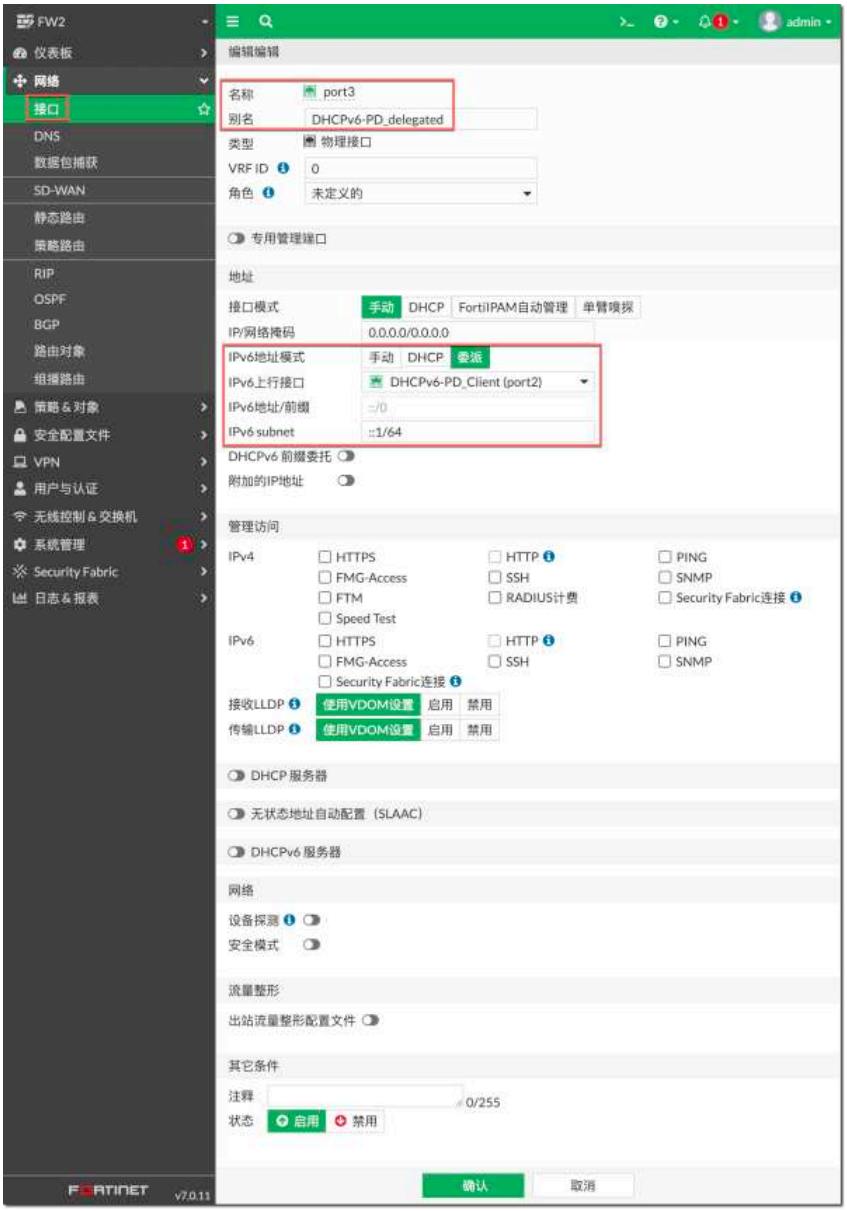



```bash
config system interface
    edit "port2"
        config ipv6
            set ip6-mode dhcp
            set dhcp6-prefix-delegation enable
            config dhcp6-iapd-list
                edit 1
                    set prefix-hint 2100:0:0:3::/64    //可以填写为::/0或不填写，表示不指定请求的prefix，让运营商选择分配的prefix//
                next
            end
        end
    next
end
```

2. 在FW2的port3上，设置IPv6的IP地址获取模式为“委派”，配置“IPv6上行接口”为port2，并配置“IPv6 Subnet”，从port2继承prefix后，加上配置的subnet地址，就组成了port3的IPv6地址。

> **重要**
>
> 如果GUI中无法选择IPv6上行接口，可通过CLI配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system interface
    edit "port3"
        config ipv6
            set ip6-mode delegated
            set ip6-delegated-prefix-iaid 1    //与步骤1中port2下配置的dhcp6-iapd序列号对应//
            set ip6-upstream-interface "port2"
            set ip6-subnet ::1/64    //获取prefix后填充的子网IPv6//
        end
    next
end
```

3. 那么FW2获取到这个prefix之后，除了可以分配给port3使用，还有什么作用呢？还可以通过自建DHCPv6服务器，将该Prefix中的IPv6分配给内网的IPv6客户端。

4. 在FW2上的port3开启DHCPv6服务器，配置subnet为port3接口网段，配置DNS Server，开启Stateful Server，配置分配IP mode为Delegated，配置upstream interface为port2，从port2获取的prefix分配IP地址给port3，需要特别注意配置中引用步骤1中port2下配置的IAPD。

> **重要**
>
> 该配置需要在CLI下配置，在GUI下配置会出现无法下发的情况。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system dhcp6 server
    edit 1
        set subnet 2100:0:0:3::/64
        set interface "port3"
        set ip-mode delegated
        set upstream-interface "port2"
        set delegated-prefix-iaid 1    //重要步骤：配置中引用port2中配置的IAPD//
        set dns-server1 2200::64
    next
end
```

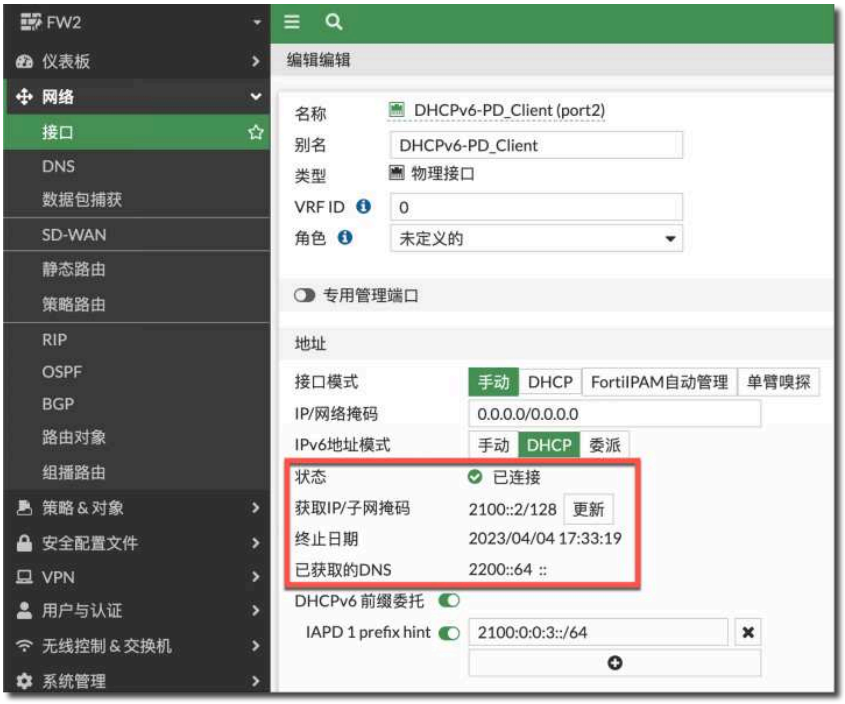
5. 再次在FW2查看port3的配置，可以看到RA、M Flag、O Flag均被开启。

```bash
config system interface
    edit "port3"
        config ipv6
            set ip6-mode delegated
            set ip6-delegated-prefix-iaid 1
            set ip6-send-adv enable
            set ip6-manage-flag enable
            set ip6-other-flag enable
            set ip6-upstream-interface "port2"
            set ip6-subnet ::1/64
        end
    next
end
```

结果验证

DHCPv6-PD

1. 在FW2上查看port2获取到的IPv6地址。




```bash
FW2 # diagnose ipv6 address list | grep port2
dev=4 devname=port2 flag=P scope=0 prefix=128 addr=2100::2 preferred=4294967295 valid=4294967295 cstamp=352820
tstamp=352820
 ...
```

2. 在FW1上查看分配的DHCPv6客户端，可以看到FW1向FW2分别分配了一个IPv6地址和一个IPv6 prefix，prefix IAID为FW2的port2配置的IAID 1，DUID（DHCPv6 Unique Identifier）为FW2的DUID。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



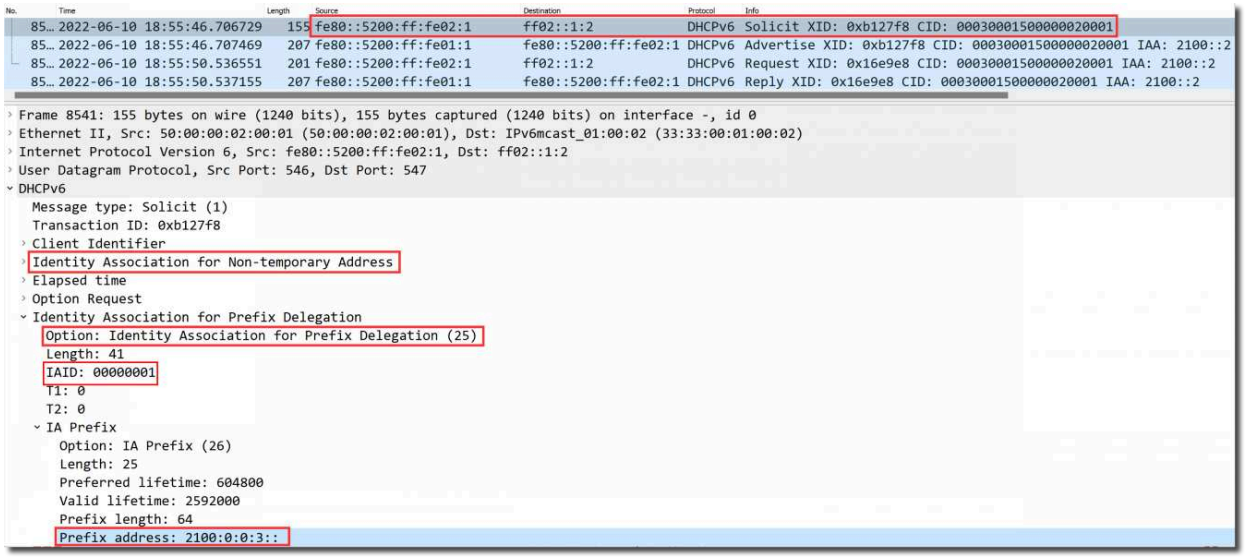

```bash
FW1 # exe dhcp6 lease-list
Interface       DUID                              IAID       IP/Prefix                 Expiry
port2           00:03:00:01:50:00:00:02:00:01     1          2100:0:0:3::/64           Tue Apr 11
17:33:19 2023

port2           00:03:00:01:50:00:00:02:00:01     4          2100::2                   Tue Apr 11
17:33:19 2023
```

3. 查看FW1 IAPD（Identity Association for Prefix Delegation）的debug信息（`diagnose debug application dhcp6s -1`）。

```
[debug]dhcp6_get_options() get DHCP option IA_PD, len 41
[debug]    IA_PD: ID=1, T1=0, T2=0
[debug]copyin_option() get DHCP option IA_PD prefix, len 25
[debug]copyin_option()    IA_PD prefix: 2100:0:0:3::/64 pltime=604800 vltime=604800
[debug]react_request() found a host configuration named 00:03:00:01:50:00:00:02:00:01
```

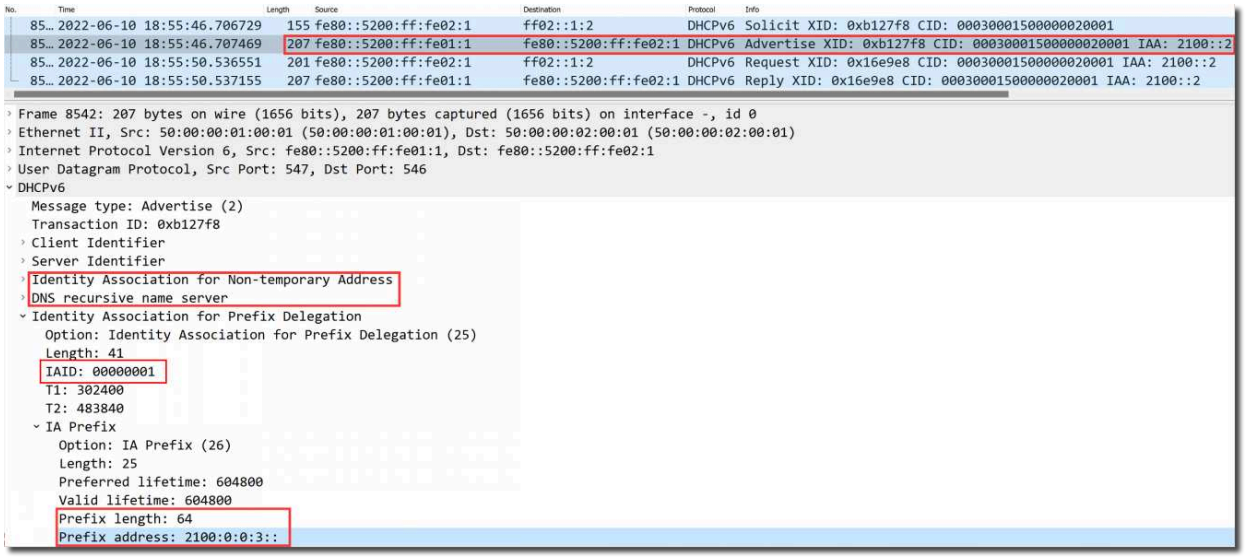
4. 抓包查看以上获取过程。

   - 客户端DHCPv6请求中既包含IPv6地址请求，也包含prefix的请求（IAPD），请求的Prefix与配置的一致，这里看到的IAID的值与dhcp6-iapd-list的ID一致，如果配置了多个dhcp6-iapd-list，则会携带多个IAPD请求。

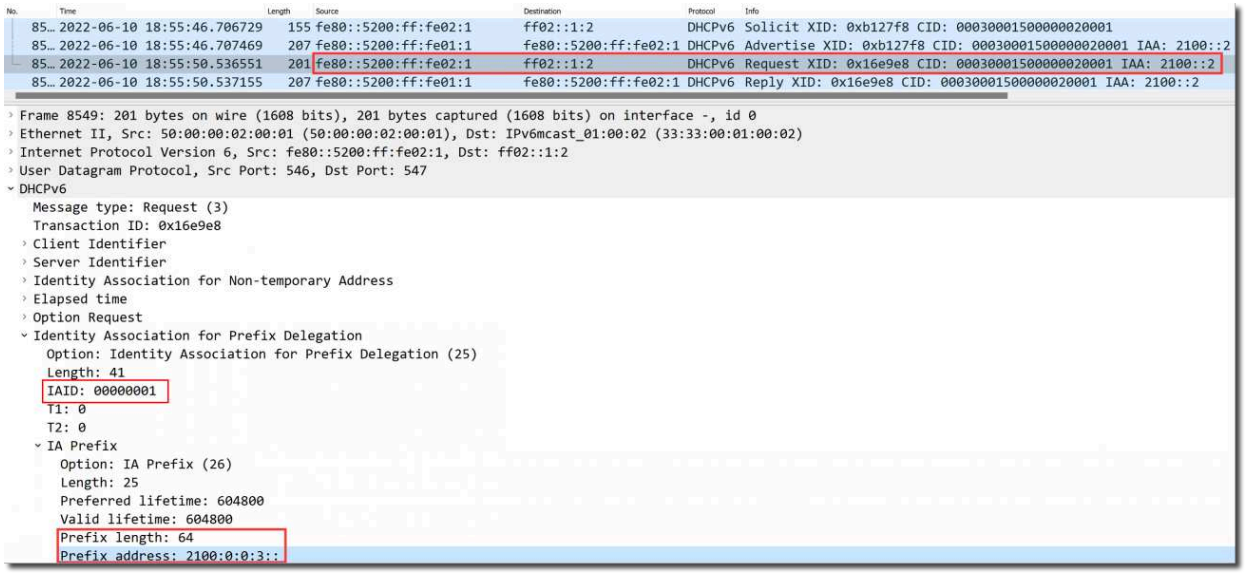


   - 服务器通过DHCPv6 Advertise告知可用的IPv6地址，并确认该prefix可用，返回的prefix IAID也为1。

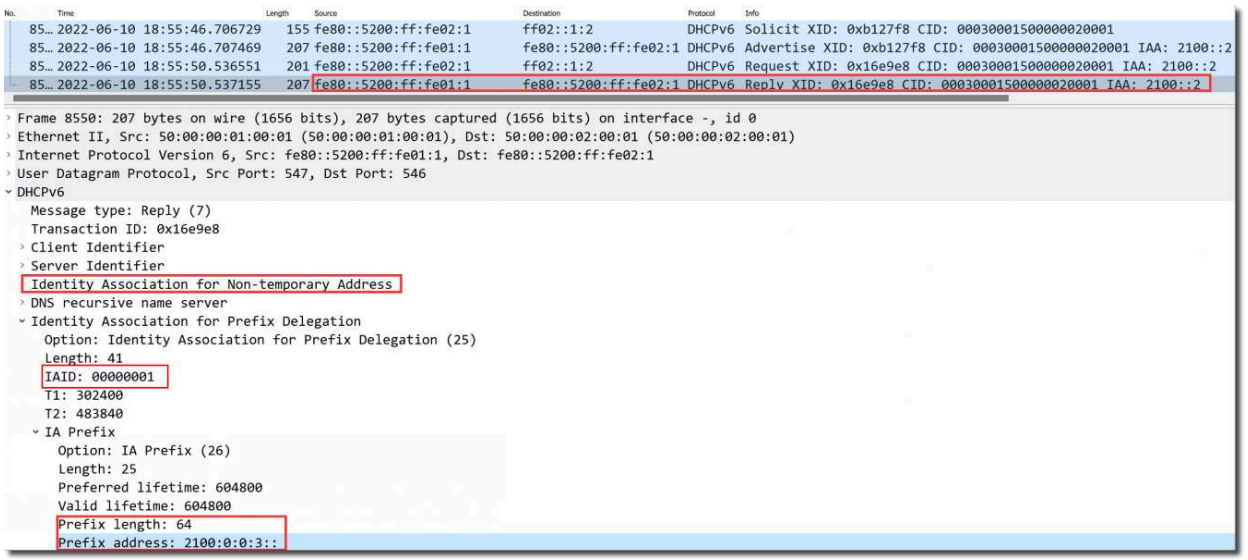
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 客户端请求确认占用该IPv6地址和prefix，IAID与dhcp6-iapd-list的ID一致，如果配置了多个dhcp6-iapd-list，则会携带多个IAPD请求。

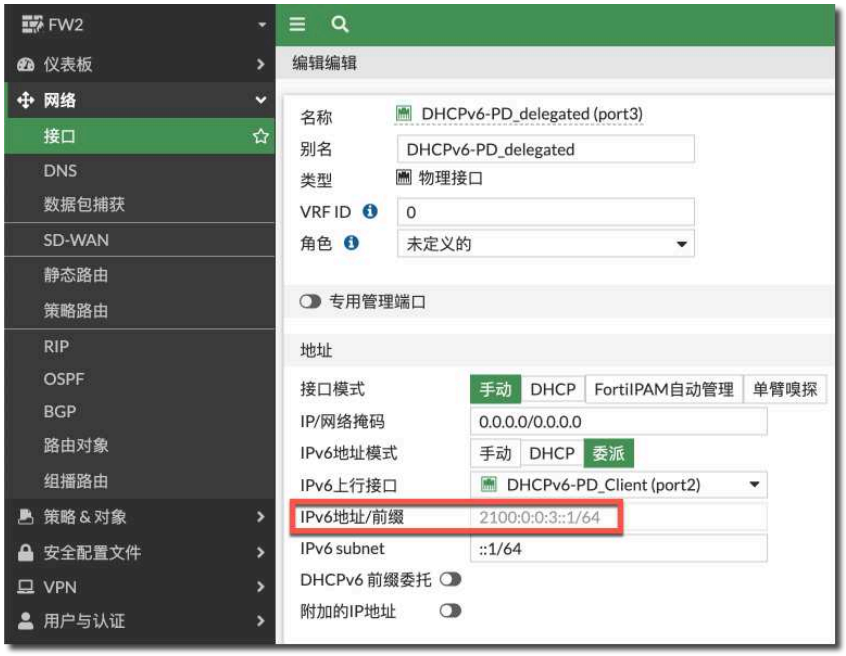


- 服务器返回Reply确认分配IPv6与Prefix，原报文见附件。



5. 查看FW2上的port3继承获取的IPv6地址，可以看到port3已经从port2的DHCP-PD Client获取到了前缀，加上自己的subnet Address，组成了自己的IPv6地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



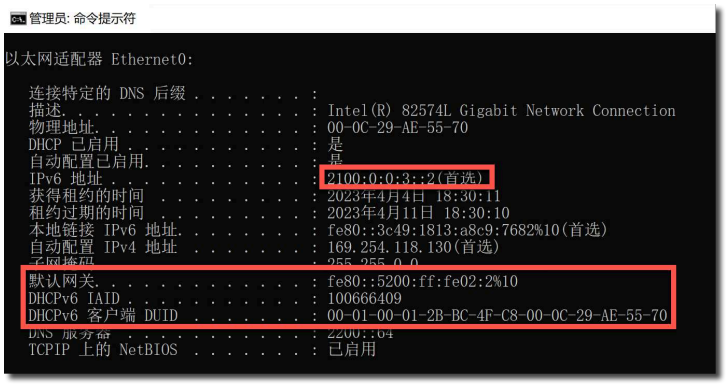

```bash
FW2 # diagnose ipv6 address list | grep port3
dev=5 devname=port3 flag=P scope=0 prefix=64 addr=2100:0:0:3::1 preferred=4294967295 valid=4294967295
cstamp=485929 tstamp=485929
...
```

DHCPv6 Client

1. 配置PC客户端的IPv6获取方式为自动获取。



2. 查看获取的IPv6地址、默认网关与DNS服务器，可以看到PC成功获取到了upstream delegated prefix中的IPv6地址。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在FW2上查看DHCP Client列表，DUID为PC客户端的DUID，IANA的IAID与客户端申请时的IAID一致（100666409）。

```bash
FW2 # exe dhcp6 lease-list
Interface       DUID                                    IAID       IP/Prefix                    Expiry
port3           00:01:00:01:2b:bc:4f:c8:00:0c:29:ae:55:70     100666409  2100:0:0:3::2                Tue Apr 11
18:30:05 2023
```

4. FW2上IAPD（Identity Association for Prefix Delegation）的debug信息（`diagnose debug application dhcp6s -1`）。

```bash
...
[debug]dhcp6_get_options() get DHCP option option request, len 6
[debug]   requested option: vendor specific info
[debug]   requested option: DNS
[debug]   requested option: domain search list
[debug]react_confirm() found a host configuration named 00:01:00:01:2b:bc:4f:c8:00:0c:29:ae:55:70
...
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DS-Lite

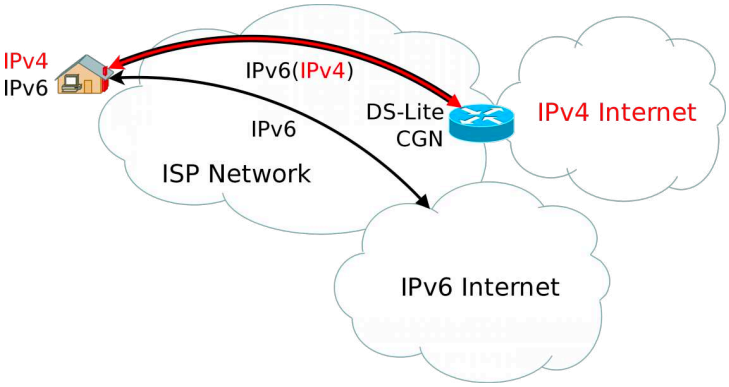
重要

该功能在7.2.0及以后版本支持。

DS-Lite简介

Dual-StackLite，简称DS-Lite，是一种使用IPv4overIPv6隧道将IPv4数据包发送到运营商来实现IPv4私网地址用户穿越IPv6网络访问IPv4公网的解决方案。

支持此技术的客户端设备（CPE）会将IPv4数据包封装到IPv6数据包中，并且将数据包发送至运营商的电信级NAT（CGNAT）。CGNAT收到数据包后，将其还原为IPv4数据包，在进行NAT处理后发送到IPv4互联网。CGNAT通过记录IPv6源地址、私有IPv4地址，以及TCP或UDP端口号来标识流量。



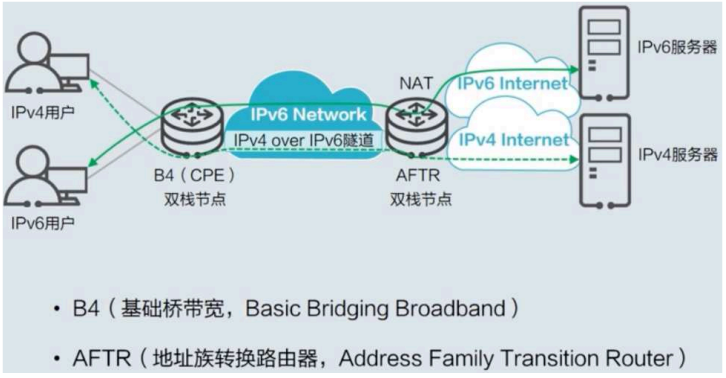
DS-Lite中的几个角色：

B4（Basic Bridging Broadband）和AFTR（Address Family Transition Router）都具有双栈能力：

- B4是IPv4 over IPv6的创建者，一般位于用户侧（CPE）。
- AFTR是IPv4 over IPv6的终结者，负责IPv4 over IPv6报文的解封装与NAT，一般部署于ISP设备上，也被叫作BR（Border Relay）。

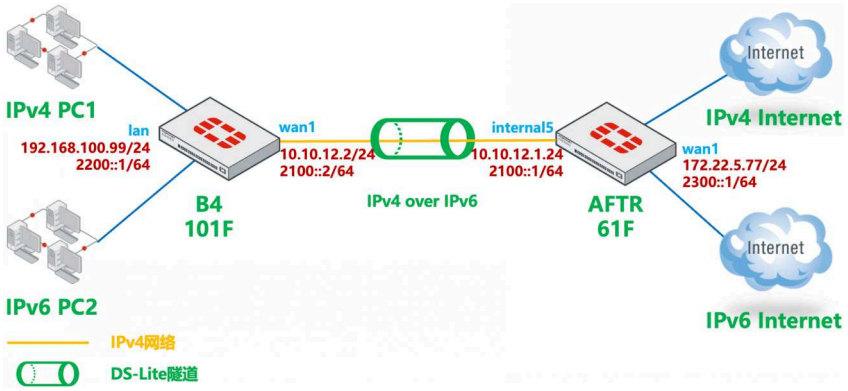
IPv6和IPv4用户都可以正常访问对应IP栈的Internet：

- IPv6用户通过B4和AFTR之间的IPv6线路直接访问IPv6 Internet。
- IPv4用户访问IPv4的Internet，通过B4的IPv4 over IPv6隧道封装IPv6外层IP头，到达AFTR后，解封装为原始的IPv4流量，通过NAT转换后访问IPv4 Internet。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

网络拓扑



1. B4与AFTR（BR）设备均为FortiGate，之间配置IPv4 over IPv6隧道（DS-Lite类型的VNE隧道，Virtual Network Enabler）。
2. IPv4 PC1访问IPv4 Internet的流量被B4的VNE隧道封装为IPv4 over IPv6流量送至AFTR，AFTR解封装后得到IPv4流量，做SNAT后送至IPv4 Internet。
3. IPv6 PC2访问IPv6 Internet的流量直接由B4和AFTR的IPv6协议栈转发至IPv6 Internet。

配置步骤

1. 基础IPv4/IPv6双栈网络配置（根据网络拓扑配置，略）。

2. 在B4设备上配置VNE（Virtual Network Enabler）隧道，隧道类型为DS-Lite，绑定接口为与AFTR的接口wan1，br地址为AFTR的IPv6地址，开启DS-Lite隧道的加速。

```bash
config system vne-tunnel
    set status enable
    set interface "wan1"
    set auto-asic-offload enable
    set br "2100::1"    //也可配置FQDN//
    set mode ds-lite
end
```

3. 在AFTR设备上配置反向的VNE（Virtual Network Enabler）隧道，隧道类型为DS-Lite，绑定接口为与AFTR的接口wan1，br地址为B4的IPv6地址，开启DS-Lite隧道的NP加速。

```bash
config system vne-tunnel
    set status enable
    set interface "internal5"
    set auto-asic-offload enable
    set br "2100::2"    //也可配置FQDN//
    set mode ds-lite
end
```

4. 在B4上配置IPv4和IPv6默认路由，IPv4默认路由指向VNE隧道，IPv6默认路由指向AFTR。

```bash
config router static
    edit 5
        set device "vne.root"
    next
end
config router static6
    edit 1
        set gateway 2100::1
        set device "wan1"
    next
end
```

5. 在AFTR设备上配置反向的IPv4路由和IPv6路由，IPv4路由指向VNE隧道，IPv6路由指向B4。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config router static
    edit 12
        set dst 192.168.100.0 255.255.255.0
        set device "vne.root"
    next
end
config router static6
    edit 1
        set dst 2200::/64
        set gateway 2100::2
        set device "internal5"
    next
end
```

6. 在B4上配置安全策略，放通lan到VNE隧道的IPv4流量，以及lan到wan1的IPv6流量。

```bash
config firewall policy
    edit 6
        set name "dslite"
        set srcintf "lan"
        set dstintf "vne.root"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    edit 7
        set name "IPv6"
        set srcintf "lan"
        set dstintf "wan1"
        set action accept
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
    next
end
```

7. 在AFTR设备上配置安全策略，放通VNE隧道到wan1的IPv4流量，开启SNAT，放通Internal5到wan1的IPv6流量。

```bash
config firewall policy
    edit 11
        set name "dslite"
        set srcintf "vne.root"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 12
        set srcintf "internal5"
        set dstintf "wan1"
        set action accept
        set srcaddr6 "all"
        set dstaddr6 "all"
        set schedule "always"
        set service "ALL"
end
```

结果验证

1. 在B4上查看VNE隧道状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
B4 # diagnose test application vned 1
```

bash

```
vdom: root/0, is master, devname=wan1 link=1 tun=vne.root mode=fixed-ip ssl_cert=Fortinet_Factory
end user ipv6 perfix: ::/0
interface ipv6 addr: 2100::2
config ipv4 perfix: 0.0.0.0/0.0.0.0
config br: 2100::1
tunnel br: 2100::1
tunnel ipv6 addr: 2100::2
tunnel ipv4 addr: 0.0.0.0/0.0.0.0
DS-Lite rule client: state=succeed retries=0 interval=0 expiry=0 reply_code=0
fqdn=2100::1 num=1 cur=0 ttl=4294967295 expiry=0
2100::1
```

2. 在AFTR设备上查看VNE隧道状态。

```
AFTR # diagnose test application vned 1
```

bash

```
vdom: root/0, is master, devname=internal5 link=1 tun=vne.root mode=fixed-ip ssl_cert=Fortinet_Factory
end user ipv6 perfix: ::/0
interface ipv6 addr: 2100::1
config ipv4 perfix: 0.0.0.0/0.0.0.0
config br: 2100::2
tunnel br: 2100::2
tunnel ipv6 addr: 2100::1
tunnel ipv4 addr: 0.0.0.0/0.0.0.0
DS-Lite rule client: state=succeed retries=0 interval=0 expiry=0 reply_code=0
fqdn=2100::2 num=1 cur=0 ttl=4294967295 expiry=0
2100::2
```

3. 使用IPv4 PC1访问IPv4 Internet，在B4和AFTR上同时抓包，原始IPv4从B4的lan口收到后，根据IPv4默认路由被送入VNE接口，VNE接口封装新的IPv6头后，从wan1发送给AFTR，AFTR收到后，解封装为原始IPv4，查IPv4默认路由从wan1发出并做SNAT，返回流量也是相同的流程。

```
B4 # diagnose sniffer packet any '(host 223.5.5.5 and icmp) or host 2100::1)' 4
interfaces=[any]
filters=[(host 223.5.5.5 and icmp) or host 2100::1]
9.415112 lan in 192.168.100.77 → 223.5.5.5: icmp: echo request
9.415202 vne.root out 192.168.100.77 → 223.5.5.5: icmp: echo request
9.415216 wan1 out 2100::2 → 2100::1: 192.168.100.77 → 223.5.5.5: icmp: echo request
9.419797 vne.root in 223.5.5.5 → 192.168.100.77: icmp: echo reply
9.419828 lan out 223.5.5.5 → 192.168.100.77: icmp: echo reply

AFTR # diagnose sniffer packet any '(host 223.5.5.5 and icmp) or host 2100::2' 4
interfaces=[any]
filters=[(host 223.5.5.5 and icmp) or host 2100::2]
3.640262 vne.root in 192.168.100.77 → 223.5.5.5: icmp: echo request
3.640354 wan1 out 172.22.5.77 → 223.5.5.5: icmp: echo request
3.644756 wan1 in 223.5.5.5 → 172.22.5.77: icmp: echo reply
3.644785 vne.root out 223.5.5.5 → 192.168.100.77: icmp: echo reply
3.644801 internal5 out 2100::1 → 2100::2: 223.5.5.5 → 192.168.100.77: icmp: echo reply
```

4. 在B4上查看IPv4流量（VNE隧道内层）的会话，流量被NP加速，无法看到IPv6的流量会话。

```
session info: proto=1 proto_state=00 duration=32 expire=28 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=120/2/1 reply=120/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=42->52/52->42 gwy=223.5.5.5/192.168.100.77
hook=pre dir=org act=noop 192.168.100.77:1->223.5.5.5:8(0.0.0.0:0)
hook=post dir=reply act=noop 223.5.5.5:1->192.168.100.77:0(0.0.0.0:0)
src_mac=00:e0:4c:b9:97:7c
misc=0 policy_id=6 pol_uuid_idx=606 auth_info=0 chk_client_info=0 vd=0
serial=007e0aab tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
```

bash

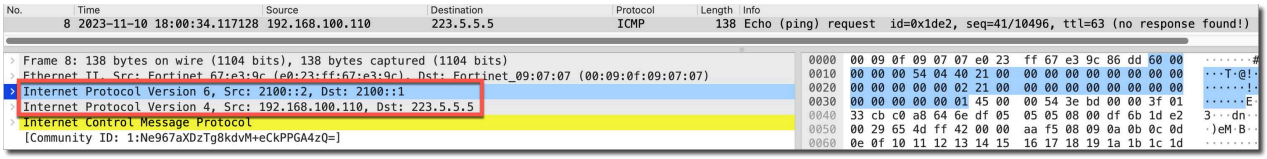
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
npu info: flag=0x84/0x81, offload=8/8, ips_offload=0/0, epid=66/95, ipid=95/66, vlan=0x0000/0x0000
vlifid=95/245, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=1/1

B4 # diagnose sys session6 list
total session6 0:
```

5. 在AFTR上查看IPv4流量（VNE隧道内层）的会话，流量被NP加速，无法看到IPv6的流量会话。

```bash
session info: proto=1 proto_state=00 duration=238 expire=28 timeout=0 flags=00000000 socktype=0 sockport=0
av_idx=0 use=4
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=12300/205/1 reply=12300/205/1 tuples=2
tx speed(Bps/kbps): 51/0 rx speed(Bps/kbps): 51/0
orgin->sink: org pre->post, reply pre->post dev=34->5/5->34 gwy=172.22.5.1/192.168.100.77
hook=post dir=org act=snat 192.168.100.77:1->223.5.5.5:8(172.22.5.77:1)
hook=pre dir=reply act=dnat 223.5.5.5:1->172.22.5.77:0(192.168.100.77:1)
misc=0 policy_id=11 pol_uuid_idx=594 auth_info=0 chk_client_info=0 vd=0
serial=005f4689 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x84, offload=8/8, ips_offload=0/0, epid=64/71, ipid=71/64, vlan=0x0000/0x0000
vlifid=247/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=1/2

AFTR # diagnose sys session6 list
total session6 0:
```

6. 对应的DS-Lite IPv4 over IPv6报文，就是IPv4 over IPv6封装，没有其他协议层。



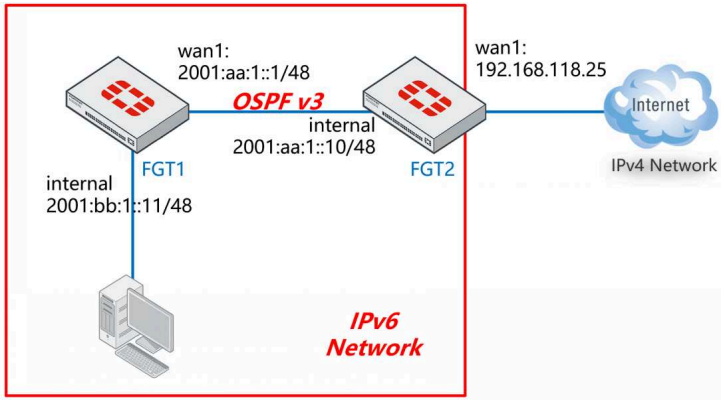
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

OSPFv3

网络需求

在IPv6网络内部使用OSPFv3。

网络拓扑



配置要点

FGT1:

- 配置基本上网功能
- 配置OSPFv3

FGT2:

- 配置NAT64访问IPv4 Internet
- 配置OSPF

配置步骤

FGT1

1. 配置基本上网功能，参考IPv6→上网配置↗章节。

```
config system interface
    edit "internal"
        config ipv6
            set ip6-allowaccess ping https http
            set ip6-address 2001:bb:1::1/48
        next
    edit "wan1"
           config ipv6
            set ip6-allowaccess ping https
            set ip6-address 2001:aa:1::1/48
        next
  end
```

2. 配置OSPFv3。

```
config router ospf6
    set router-id 192.168.1.200    //指定路由ID
    config area
        edit 0.0.0.0    //配置area 0
        next
    end
    config ospf6-interface
        edit "wan1"    // 名字，可自定义
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set interface "wan1"    //配置wan1口运行OSPFv3
        next
        end
    config redistribute "connected"    //重分发直连路由
        set status enable
    end
end
```

FGT2

1. 配置NAT64上网功能（参考NAT64+DNS64上网↗章节）。

2. 配置OSPFv3。

```
config router ospf6
   set default-information-originate always    //向OSPF邻居FGT1发布一条默认路由
   set router-id 192.168.1.99    //配置路由ID
       config area    //配置区域 0.0.0.0
           edit 0.0.0.0
           next
       end
       config ospf6-interface     //指定internal接口运行OSPF协议
           edit "internal"    //名字，可自定义
               set interface "internal"
           next
       end
end
```

结果验证

1. 查看FGT1 OSPF邻居。

```
FortiGate # get router info6   ospf  neighbor
OSPFv3 Process (*null*)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
192.168.1.99      1   Full/Backup     00:00:34    wan1       0
```

2. 查看FGT1路由表。

```
FortiGate # get  router  info6   routing-table
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
      IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      I - IS-IS, B - BGP
      * - candidate default
Timers: Uptime
O*E2    ::/0 [110/1] via fe80::a5b:eff:fe6f:f7a6, wan1, 00:20:29    //学到的默认路由
C       ::1/128 via ::, root, 02:21:41
C       2001:aa:1::/48 via ::, wan1, 02:13:38
C       2001:bb:1::/48 via ::, internal, 01:58:51
```

3. FGT1用户可以通过FGT2访问IPv4互联网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

常用命令

1. IPv6抓包。

```
FGT # diagnose sniffer packet any 'host 2001:aa:1::10' 4    //基于ipv6地址
interfaces=[any]
filters=[host 2001:aa:1::10]
1.389573 internal in 2001:bb:1::10 → 2001:aa:1::10: icmp6: echo request seq 415
1.389692 wan1 out 2001:bb:1::10 → 2001:aa:1::10: icmp6: echo request seq 415
1.389912 wan1 in 2001:aa:1::10 → 2001:bb:1::10: icmp6: echo reply seq 415
1.389983 internal out 2001:aa:1::10 → 2001:bb:1::10: icmp6: echo reply seq 415
2.391299 internal in 2001:bb:1::10 → 2001:aa:1::10: icmp6: echo request seq 416
2.391426 wan1 out 2001:bb:1::10 → 2001:aa:1::10: icmp6: echo request seq 416
2.391671 wan1 in 2001:aa:1::10 → 2001:bb:1::10: icmp6: echo reply seq 416
2.391735 internal out 2001:aa:1::10 → 2001:bb:1::10: icmp6: echo reply seq 416
8 packets received by filter
0 packets dropped by kernel

FGT # diagnose sniffer packet any icmp6 4 2    //基于icmp6
interfaces=[any]
filters=[icmp6]
1.410860 internal in 2001:bb:1::10 → 2001:aa:1::10: icmp6: echo request seq 431
1.410986 wan1 out 2001:bb:1::10 → 2001:aa:1::10: icmp6: echo request seq 431
```

2. IPv6会话。

```
FGT # diagnose sys session6 list
session6 info: proto=17 proto_state=01 duration=0 expire=179 timeout=0 flags=00000000 sockport=0 sockflag=0 use=3
origin-shaper=shared-1M-pipe prio=2  guarantee 0Bps  max 131072Bps  traffic 787Bps)
reply-shaper=shared-1M-pipe prio=2  guarantee 0Bps  max 131072Bps traffic 787Bps)
per_ip_shaper=
ha_id=0
policy_dir=0 tunnel=/
state=may_dirty os rs
statistic(bytes/packets/allow_err): org=83/1/0 reply=276/1/0 tuples=2
orgin→sink: org pre→post, reply pre→post dev=3→5/5→3
hook=pre dir=org act=noop 2001:bb:1::10:57194 →2001:aa:1::10:53(:::0)
hook=post dir=reply act=noop 2001:aa:1::10:53 →2001:bb:1::10:57194(:::0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0 serial=000003f1
npu_state=00000000

FGT # diagnose sys session6 full-stat
session table:           table_size=131072 max_depth=1 used=188
misc info:       session_count=94 setup_rate=20 exp_count=0 clash=0
       memory_tension_drop=0 ephemeral=0/0 removeable=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
        19 in ESTABLISHED state
```

3. debug flow 命令。

```
diagnose debug enable
diagnose debug flow filter6 proto 1
diagnose debug flow show con enable
diagnose debug flow trace start6 10
```

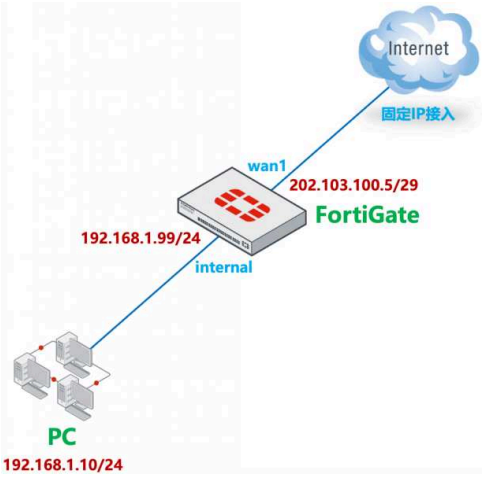

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

静态地址线路上网配置

网络需求

外网接口使用专线，由运营商分配指定的静态地址，内网为192.168.1.0/24网段，实现基本上网功能。

网络拓扑



假设运营商分配的地址如下：

网段	分配IP	网关地址	DNS
202.103.100.0/29	202.103.100.5	202.103.100.1	202.106.196.115

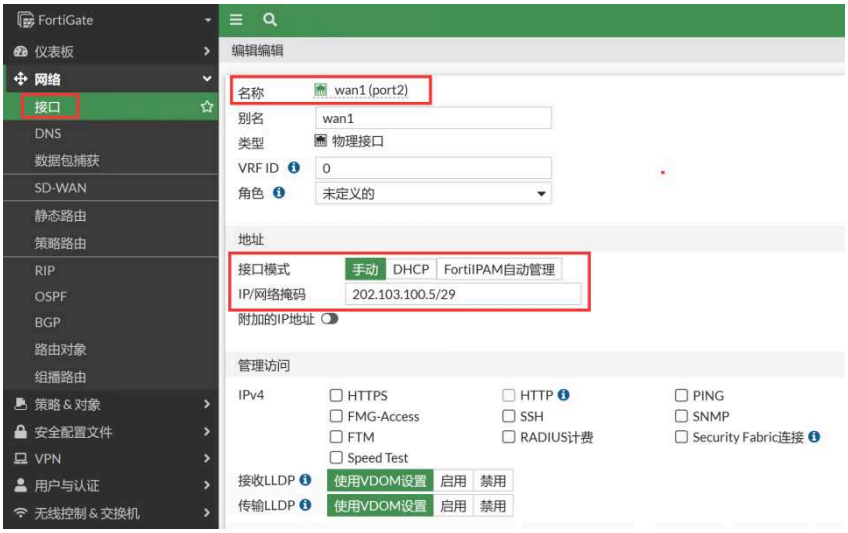
配置要点

- wan1（port2）口：IP地址配置为互联网运营商所提供的地址
- internal（port3）口：IP地址设置格式为：192.168.1.99/24，可选择性地开启接口的管理功能
- 配置静态路由表
- 配置地址对象lan，内容为192.168.1.0/24
- 配置从internal（port3）到wan1（port2）口的策略，并开启NAT

配置步骤

1. 进入网络→接口，配置wan1口的IP地址。对于202.103.100.0/29网段，202.103.100.0网络地址和202.103.100.7广播地址均不可用，202.103.100.1为运营商网关所用，202.103.100.2—202.103.100.6为可用IP地址范围。所以配置给wan接口的地址我们选择为202.103.100.5。

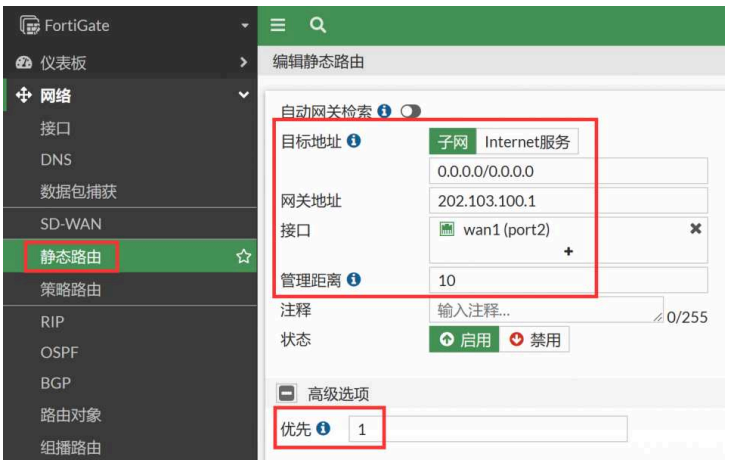
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置internal（port3）接口的IP为192.168.1.99/24。选择性地开启接口的管理功能，建议内部开启https ,ssh, ping服务。



3. 配置静态路由，添加默认路由指向运营商网关。

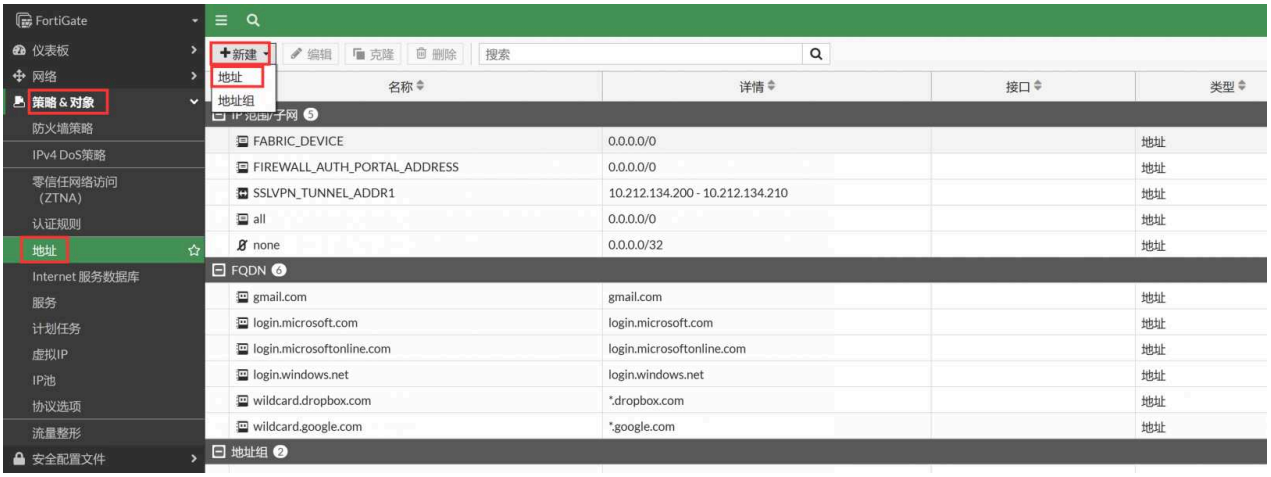


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

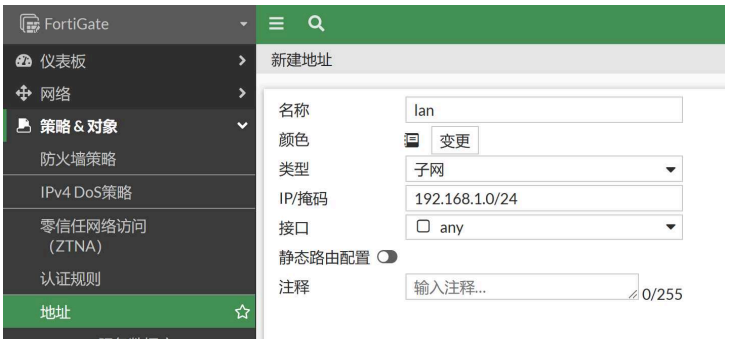
```
config router static
    edit 1
        set gateway 202.103.100.1
        set device "port2"
    next
end
```

- 目的的IP/子网掩码：由于是默认网关，使用默认的0.0.0.0/0.0.0.0即可
- 接口：该路由所关联的接口，wan1口，必须正确填写，否则该路由无法工作
- 网关：下一跳IP地址， 即wan1口对端运营商设备接口的ip地址
- 管理距离：默认10
- 高级选项-优先级：默认1

4. 配置地址资源，进入防火墙&对象→地址，点击新建地址按钮。



5. 名称配置为lan，地址节点选择子网：192.168.1.0/24，点击确认。



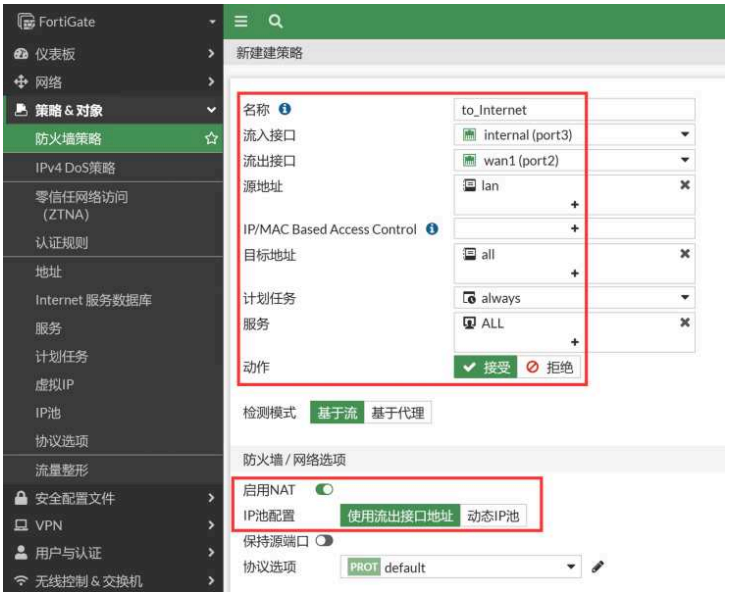

```
config firewall address
    edit "lan"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，放通内网到Internet的流量，并开启NAT，点击确定按钮后，系统自动保存配置，策略生效。

重要

如果选择“动态IP池”作为“IP池配置”，所引用IPPool配置中的外部IP范围不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置IPPool后，IPPool中的地址属于FortiGate自身的IP地址，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port3"
        set dstintf "port2"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

- 流入接口：internal（port3）
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：wan1（port2）
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为wan1接口地址，进行互联网访问
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

结果验证

将电脑IP地址设置为192.168.1.10/24，网关设置地为192.168.1.99，DNS一般设置为当地的DNS即可，电脑可正常上网。

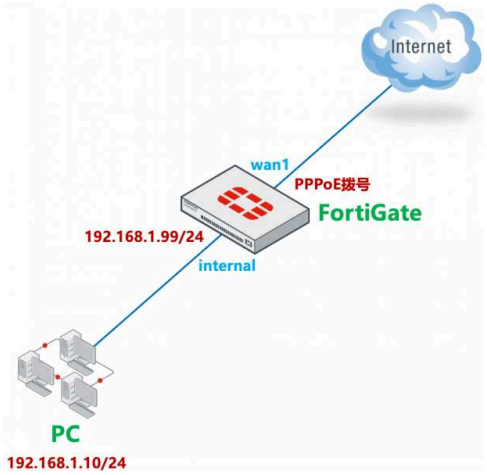
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

单条ADSL线路上网配置

网络需求

外网接口使用ADSL拨号，内网为192.168.1.0/24网段，实现基本上网功能。

网络拓扑



配置要点

- wan1（port2）口: 接ADSL的接口，务必开启自动获取网关，这样ADSL拨号成功后设备会自动生成默认路由，无需手动配置默认路由
- internal（port3）口: IP地址设置格式为：192.168.1.99/24，可选择性地开启接口的管理功能
- 配置地址对象“lan”，内容为192.168.1.0/24
- 配置从internal（port3）到PPPoE口的策略，并开启NAT

配置步骤

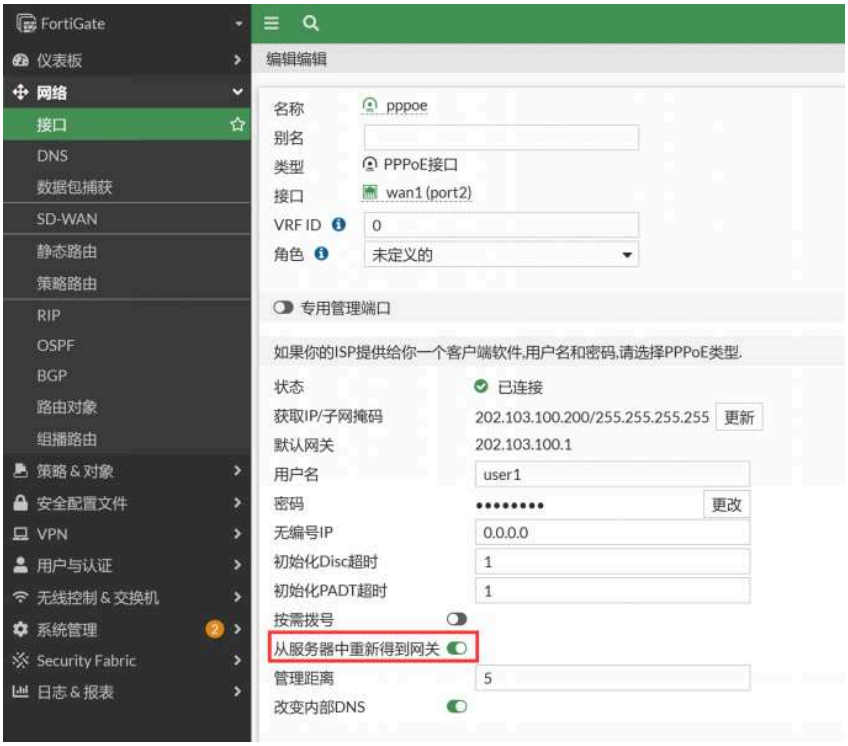
1. 配置wan1口的PPPoE，建议在CLI下配置PPPoE接口，使用此方式配置获取到IP后会自动添加默认路由到运营商。

> **重要**
>
> 建议通过CLI的方式新建PPPoE虚拟接口，参考：部署前注意事项→PPPoE接口 ↗配置章节。

```
config system pppoe-interface
    edit "pppoe"
        set device "port2"
        set username "user1"
        set password xxxxxxxx
    next
end

以上命令执行后，会自动在system interface下创建同名接口，其中包含“从服务器中重新得到网关”的配置
FortiGate # show full sys int pppoe
config system interface
    edit "pppoe"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set defaultgw enable
        set interface "port2"
    next
end
```

2. 以上配置完成后，可以在GUI上看到wan1（port2）下多了一个PPPoE接口，并获取到了运营商的IP。可以看到“从服务器中重新得到网关”已开启。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



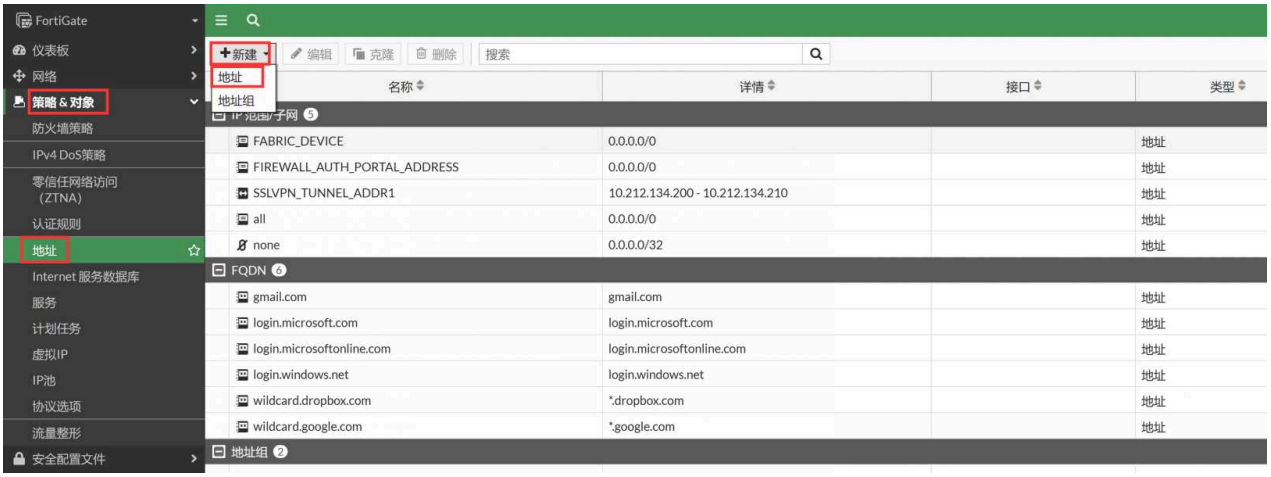

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 202.103.100.1, pppoe, [1/0]
C       192.168.1.0/24 is directly connected, port3
C       202.103.100.1/32 is directly connected, pppoe
C       202.103.100.200/32 is directly connected, pppoe
```

3. 配置internal（port3）接口的IP为192.168.1.99/24。选择性地开启接口的管理功能，建议内部开启https ,ssh, ping服务。

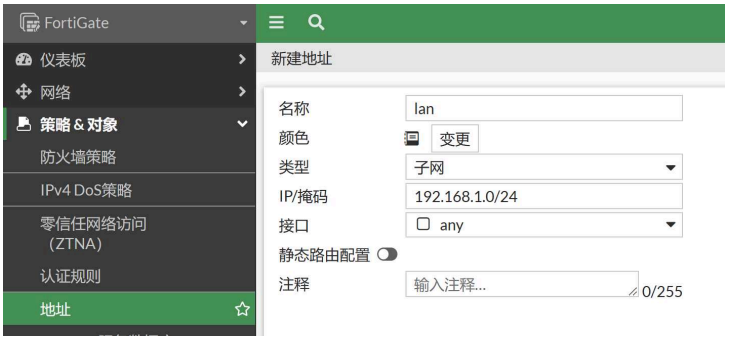


4. 配置地址资源，进入防火墙&对象→地址，点击新建地址按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

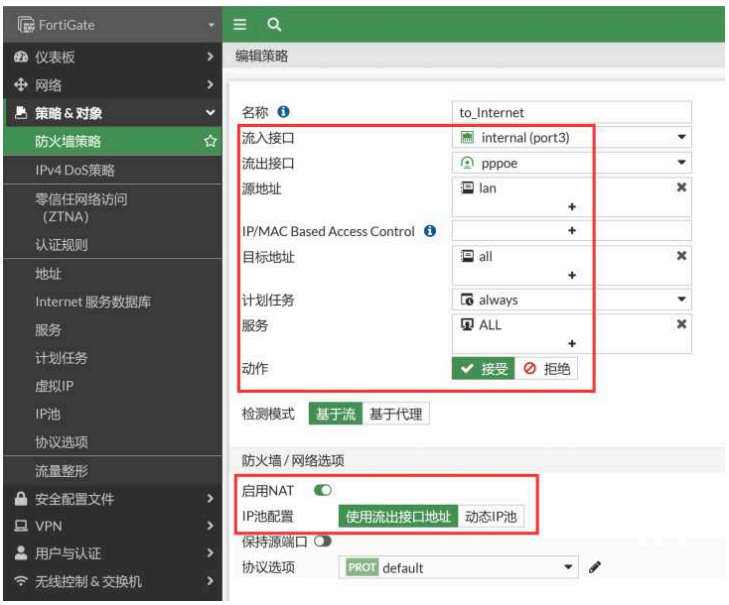


5. 名称配置为lan，地址节点选择子网：192.168.1.0/24，点击确认。




```
config firewall address
    edit "lan"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，放通内网到Internet的流量，并开启NAT，点击确定按钮后，系统自动保存配置，策略生效。




```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port3"
        set dstintf "port2"
        set action accept
        set srcaddr "lan"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

- 流入接口：internal（port3）
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：pppoe接口
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为wan1接口地址，进行互联网访问
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

结果验证

将电脑IP地址设置为192.168.1.10/24，网关设置地为192.168.1.99，DNS一般设置为当地的DNS即可，电脑可正常上网。

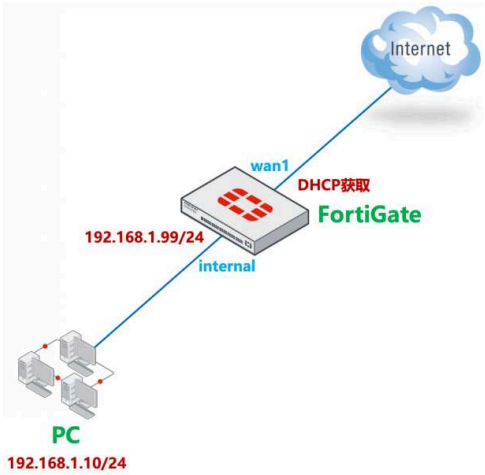
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DHCP线路上网配置

网络需求

外网接口使用DHCP，内网为192.168.1.0/24网段，实现基本上网功能。

网络拓扑

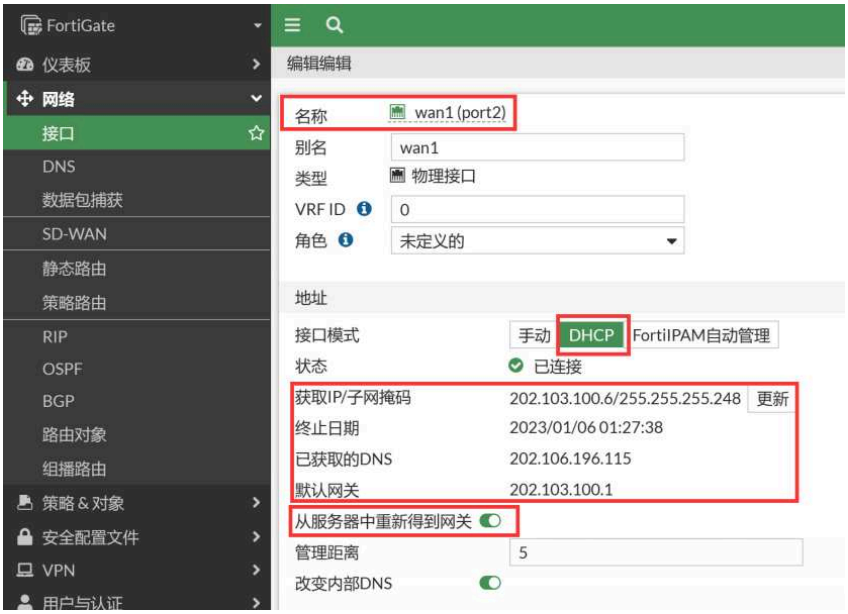


配置要点

- wan1（port2）口：务必勾选“从服务器重新得到网关”，这样DHCP地址获取成功后设备会自动生成默认路由，无需手动配置默认路由
- internal（port3）口: IP地址设置格式为：192.168.1.99/24，可选择性地开启接口的管理功能
- 配置地址对象“lan”，内容为192.168.1.0/24
- 配置从internal（port3）到wan1（port2）口的策略，并开启NAT

配置步骤

1. 进入网络→接口，编辑wan1（port2）接口，将接口的模式配置为DHCP，并勾选“从服务器重新得到网关”。

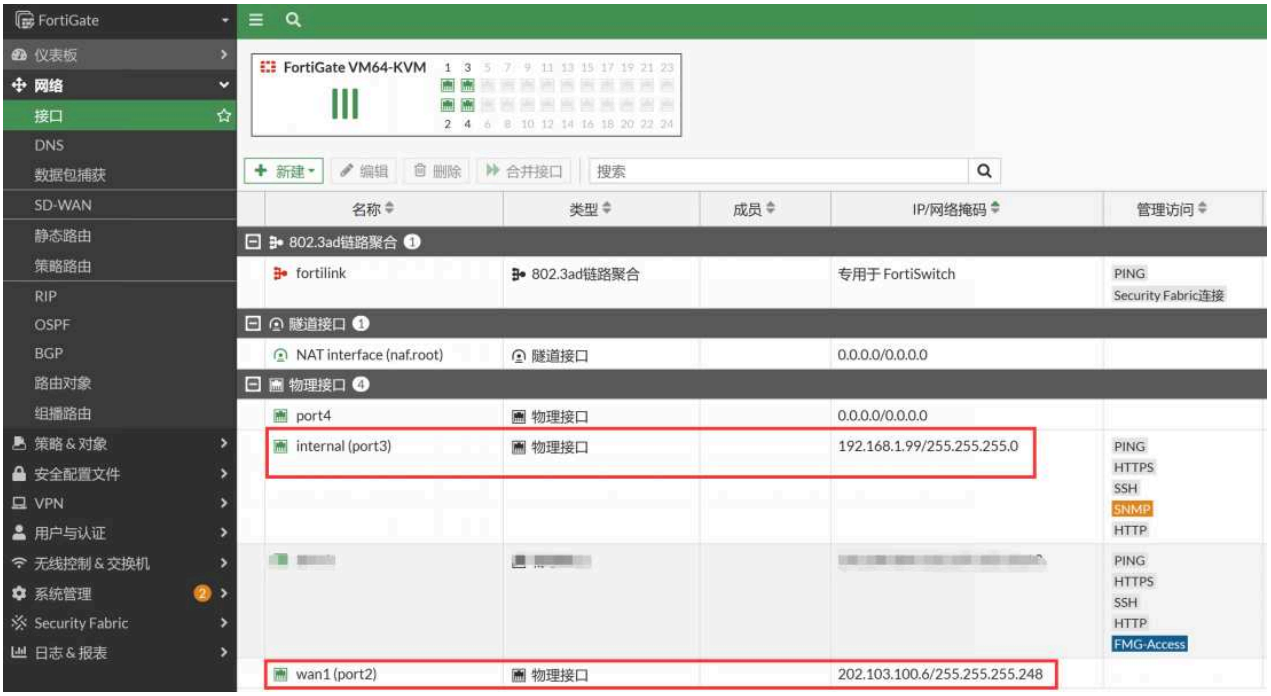


2. 以上配置完成后，等待DHCP获取到IP地址，然后查看路由表，可以看到通过DHCP自动添加了默认路由。

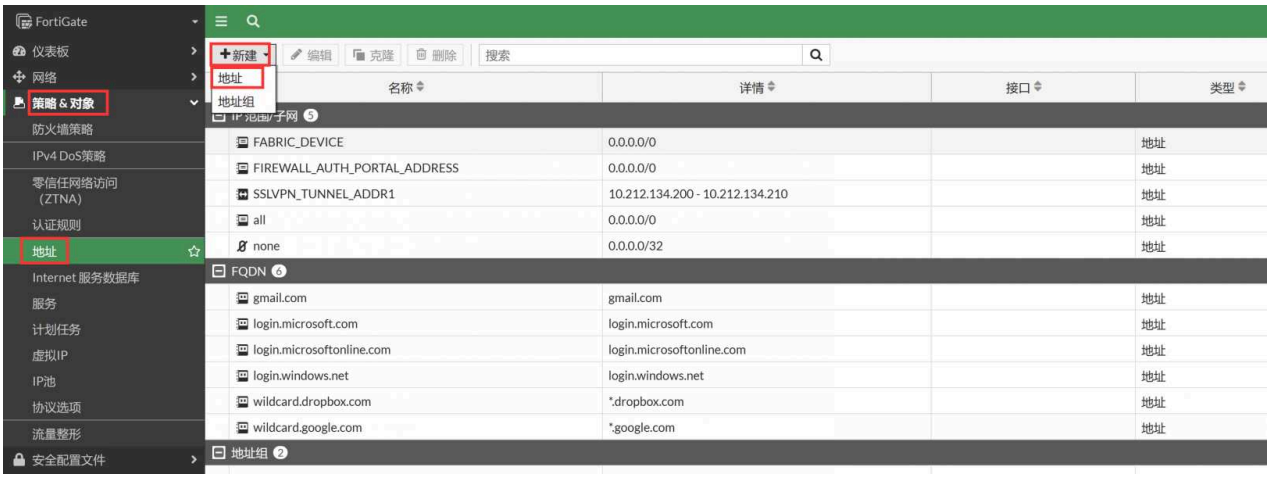
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate #  get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 202.103.100.1, port2, [1/0]
C       192.168.1.0/24 is directly connected, port3
C       202.103.100.0/29 is directly connected, port2
```

3. 配置internal（port3）接口的IP为192.168.1.99/24。选择性地开启接口的管理功能，建议内部开启https ,ssh, ping服务。

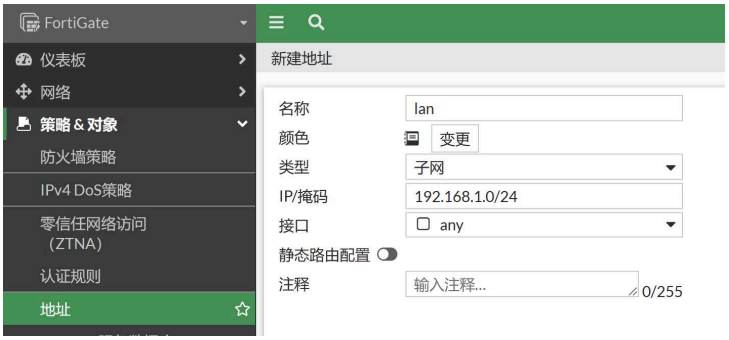


4. 配置地址资源，进入防火墙&对象→地址，点击新建地址按钮。



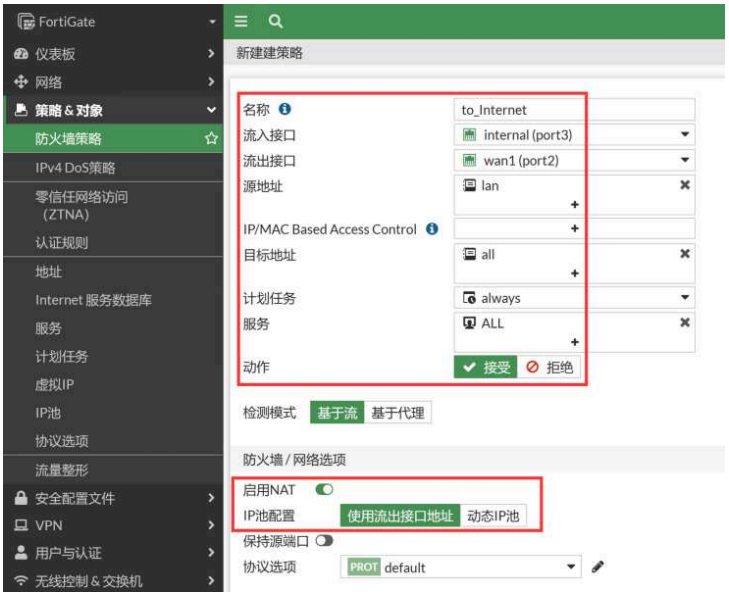
5. 名称配置为lan，地址节点选择子网：192.168.1.0/24，点击确认。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall address
    edit "lan"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，放通内网到Internet的流量，并开启NAT，点击确定按钮后，系统自动保存配置，策略生效。




```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "port3"
        set dstintf "port2"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

- 流入接口：internal（port3）
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：pppoe接口
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为wan1接口地址，进行互联网访问
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

将电脑IP地址设置为192.168.1.10/24，网关设置地为192.168.1.99，DNS一般设置为当地的DNS即可，电脑可正常上网。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

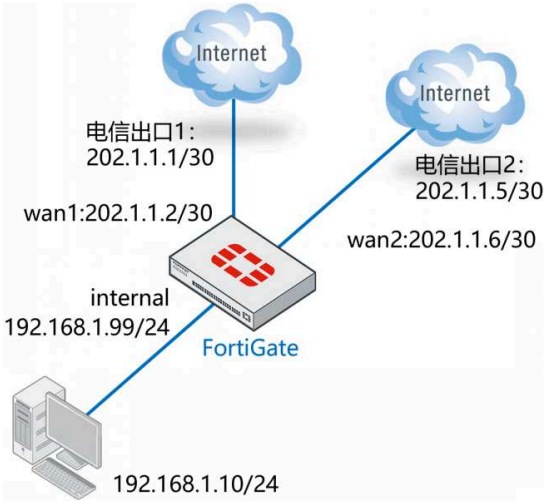
双线路同运营商上网配置

网络需求

现设备上申请了两条电信线路，带宽大小相同 ，通过配置实现负载均衡、冗余备份。

- 电信1：wan1（port2）口：202.1.1.2/30，网关为202.1.1.1
- 电信2：wan2（port3）口：202.1.1.6/30，网关为202.1.1.5

网络拓扑



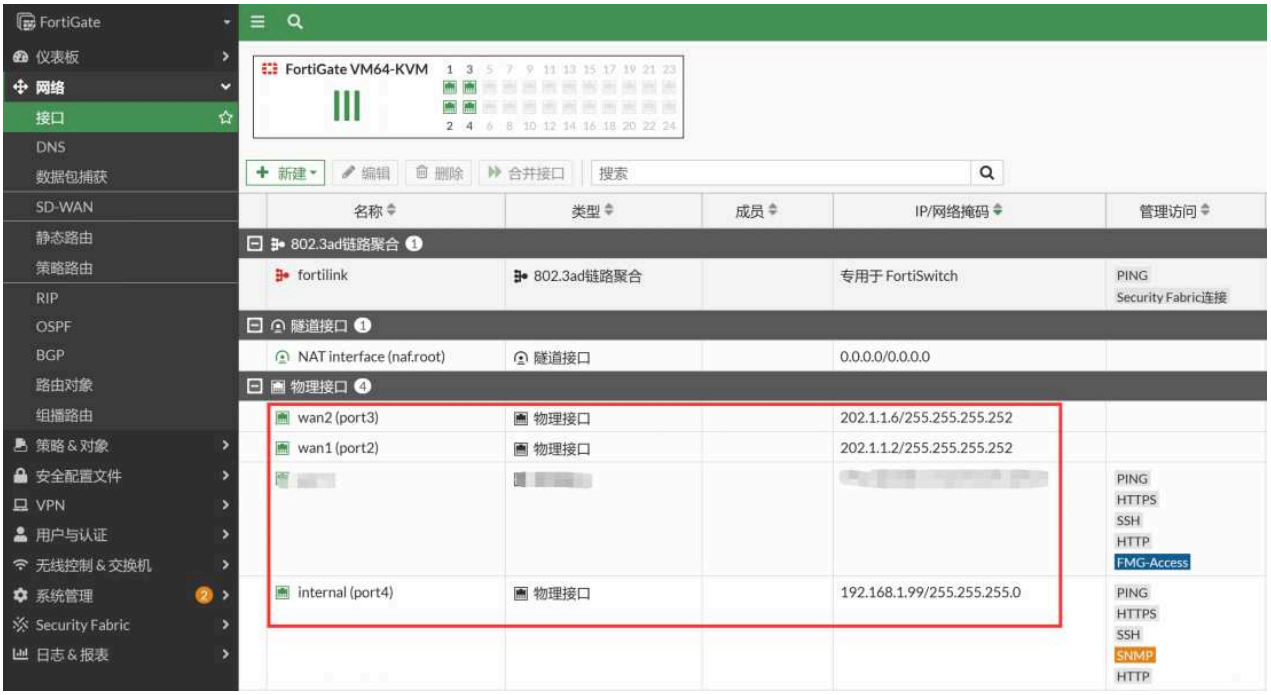
配置要点

- 配置接口IP
- 配置路由
- 配置zone（untrust和 trust）
- 配置策略
- 配置ECMP负载均衡方式

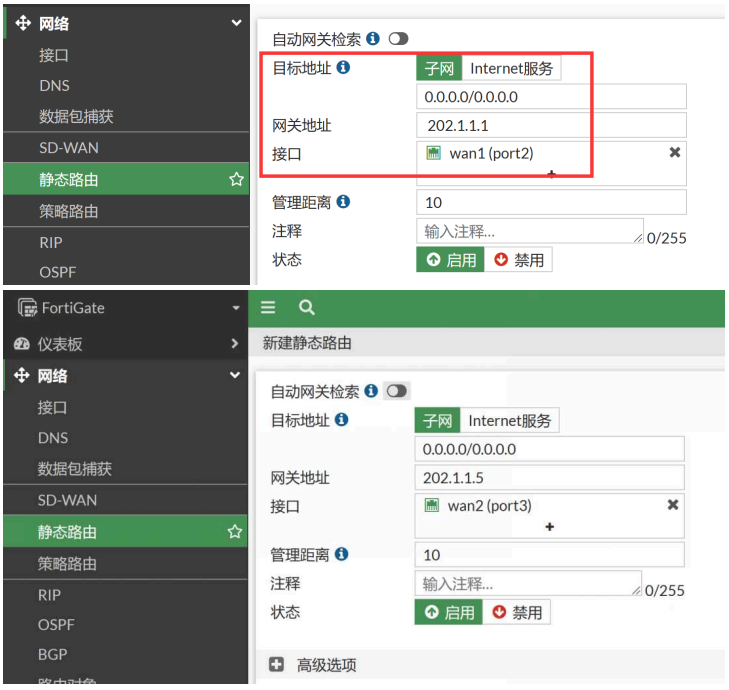
配置步骤

1. 配置接口IP，进入网络→接口页面，编辑wan1（port2）、wan2（port3）internal（port4），分别配置为 202.1.1.2/30、202.1.1.6/30、192.168.1.99/24。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置静态路由，创建两条链路的默认路由。




```
config router static
    edit 1
        set gateway 202.1.1.1
        set device "port2"
    next
    edit 2
        set gateway 202.1.1.5
        set device "port3"
    next
end
```

- 目的的IP/子网掩码：由于是默认网关，使用默认的0.0.0.0/0.0.0.0即可
- 接口：该路由所关联的接口，wan1口，必须正确填写，否则该路由无法工作
- 网关：下一跳IP地址， 即wan1口对端运营商设备接口的ip地址
- 管理距离：默认10
- 高级选项-优先级：默认1，优先级小的优先使用
- 注意：

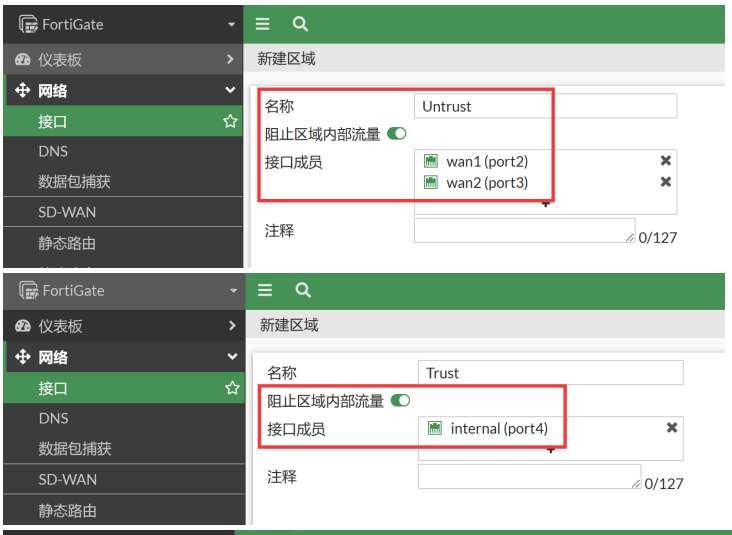
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 要想实现两个出口线路同时工作，两条路由表的管理距离必须相同。否则路径长度长的路由条目，不会装入路由表
- 管理距离相等的同时，优先级必须相同。 如果路径相等优先级不同，则虽然两条路由都会被装入路由表，防火墙会优先采用优先级数值较小的路由工作，无法实现两条链路的流量均担

3. 配置区域，采用区域的方式，为了配置更加快捷、精简。如果采用基于物理接口的方式，则可能需要配置多条防火墙策略。进入网络→接口，点击新建→所属区域按钮。



4. 分别创建Untrust和Trust区域，





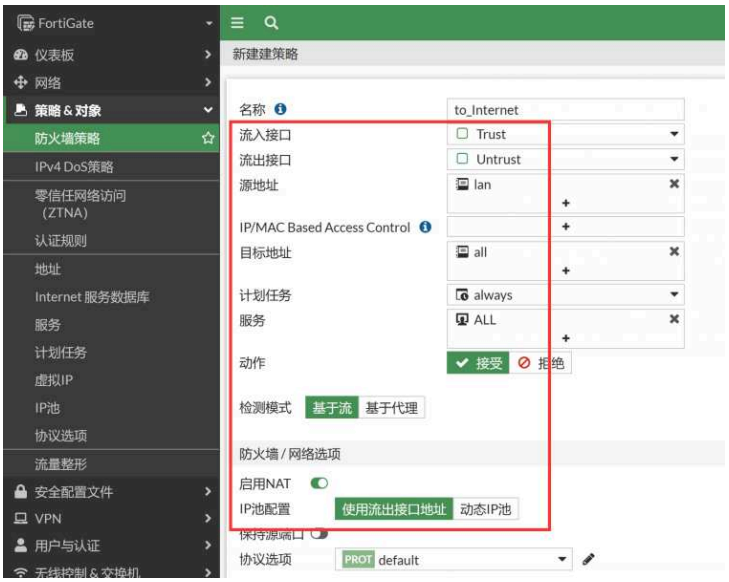

```
config system zone
    edit "Untrust"
        set interface "port2" "port3"
    next
    edit "Trust"
        set interface "port4"
    next
end
```

5. 配置上网放通策略，进入策略&对象→防火墙策略，新建安全策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

如果选择“动态IP池”作为“IP池配置”，所引用IPPool配置中的外部IP范围不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置IPPool后，IPPool中的地址属于FortiGate自身的IP地址，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。




```
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "Trust"
        set dstintf "Untrust"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

- 流入接口：trust
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：untrust
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT： 选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为untrust的接口组里的wan1/wan2接口地址，进行互联网访问
- 点击"确定"按钮后，系统自动保存配置，策略生效
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

6. 配置ECMP负载均衡方式（具体可参考https://community.fortinet.com/t5/FortiGate/Technical-Tip-ECMP-Load-balancing-algorithms-for-IPv4-and-IPv6/ta-p/191149 ↗ ）。

```
FortiGate # config system settings
FortiGate (settings) # set v4-ecmp-mode ?
source-ip-based         Select next hop based on source IP.
weight-based            Select next hop based on weight.
usage-based             Select next hop based on usage.
source-dest-ip-based    Select next hop based on both source and destination IPs.
```

- 基于源IP：默认配置，根据源地址的不同选择不同的下一跳
- 权重负载均衡： 根据权重值来选择路由（在默认路由的CLI下配置）
  - 比如wan1 50， wan2 50，其他为0 则2条链路会1:1的比例分配流量
  - 比如wan1 50， wan2 100，则流量会按照1:2的比例分配
- 用量：根据线路带宽用量，选择用量较少的线路
- 源目IP：根据源地址-目的地址对的不同选择不同的下一跳

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 推荐采用“基于源IP”的负载均衡方式（默认）。因为例如网银、网游会进行源IP的验证，如果存在不同IP的多条流的交互（同时通过wan1/wan2做不同的NAT转换成不同的公网IP，一个网银user使用了多个公网IP访问网银业务），将会导致网银业务交互失败、游戏掉线等问题。

结果验证

不同的源IP的客户端的上网流量被分配到了不通的链路。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

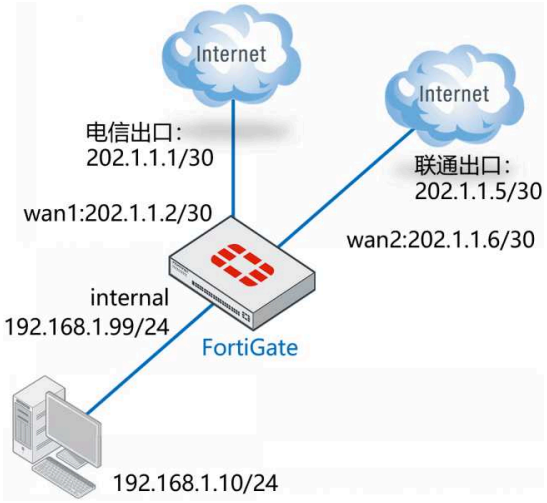
双线路不同运营商上网配置

网络需求

防火墙到电信和联通分别有一条链路，去往电信的IP，通过wan1（port2）口；去往联通的IP，通过wan2（port3）口。

- 电信：wan1（port2）口：202.1.1.2/30，网关为202.1.1.1，NAT地址池：202.1.1.1-10
- 联通：wan2（port3）口：102.1.1.2/30，网关为102.1.1.1，NAT地址池：200.0.0.1-10

网络拓扑



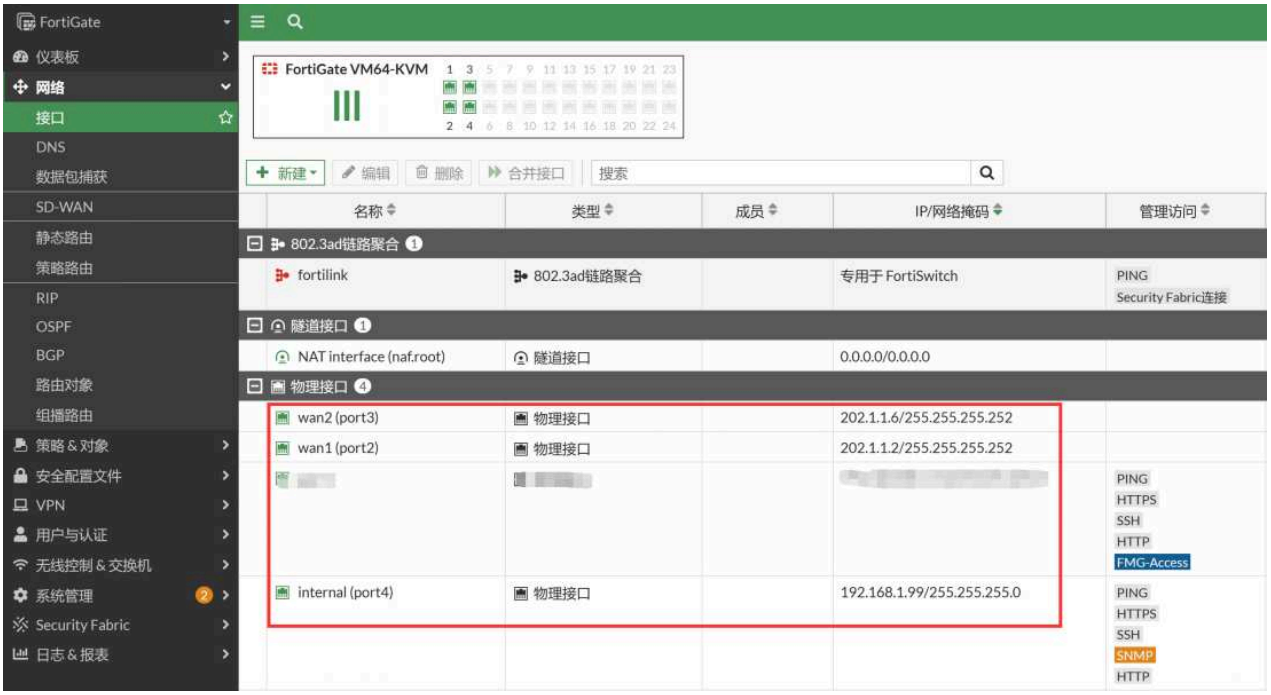
配置要点

- 配置接口IP
- 配置路由
- 配置地址池
- 配置策略
- 注意：部分低端型号路由表规格有限，不适用导入运营商路由表的方法

配置步骤

1. 配置接口IP，进入网络→接口页面，编辑wan1（port2）、wan2（port3）internal（port4），分别配置为 202.1.1.2/30、202.1.1.6/30、192.168.1.99/24。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置静态路由，创建电信链路（wan1）的默认路由。




```
config router static
    edit 1
        set gateway 202.1.1.1
        set device "port2"
    next
end
```

- 目的的IP/子网掩码：由于是默认网关，使用默认的0.0.0.0/0.0.0.0即可
- 接口：该路由所关联的接口，wan1口，必须正确填写，否则该路由无法工作
- 网关：下一跳IP地址， 即wan1口对端运营商设备接口的ip地址
- 管理距离：默认10
- 高级选项-优先级：默认1，优先级小的优先使用
- 注意：
  - 要想实现两个出口线路同时工作，两条路由表的管理距离必须相同。否则路径长度长的路由条目，不会装入路由表
  - 管理距离相等的同时，优先级必须相同。 如果路径相等优先级不同，则虽然两条路由都会被装入路由表，防火墙会优先采用优先级数值较小的路由工作，无法实现两条链路的流量均担

3. 参照附件→命令行脚本批量转换工具说明↗和附件→FortiGate通用多运营商路由导入脚本↗附件章节，将联通明细路由导入FortiGate（注意脚本中要开启允许静态路由引用地址对象）。

4. 配置地址池，进入策略&对象→IP池，新建两个运营商的地址池。

重要

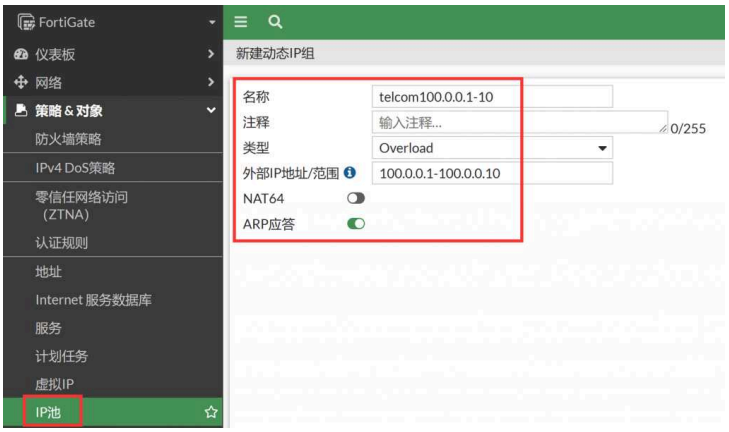
如果在SD-WAN中使用ippool的方式做SNAT，一定要在ippool下配置绑定接口，防止ippool在SD-WAN成员中转换错误。

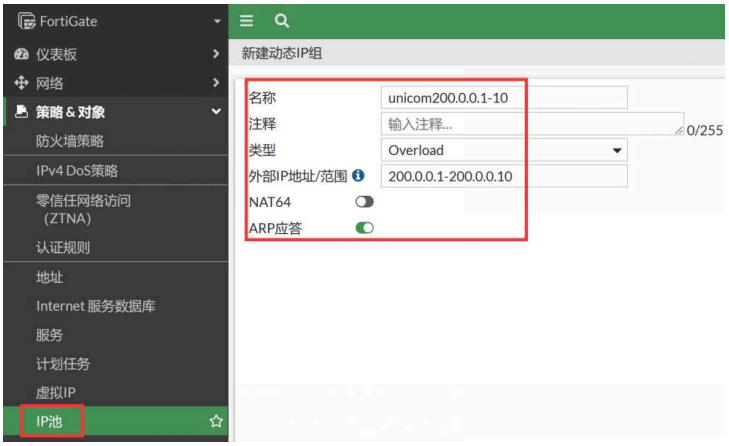
```
config firewall ippool
    edit xxxx
        set associated-interface port2
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

IPPool配置中的外部IP范围不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置IPPool后，IPPool中的地址属于FortiGate自身的IP地址，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。



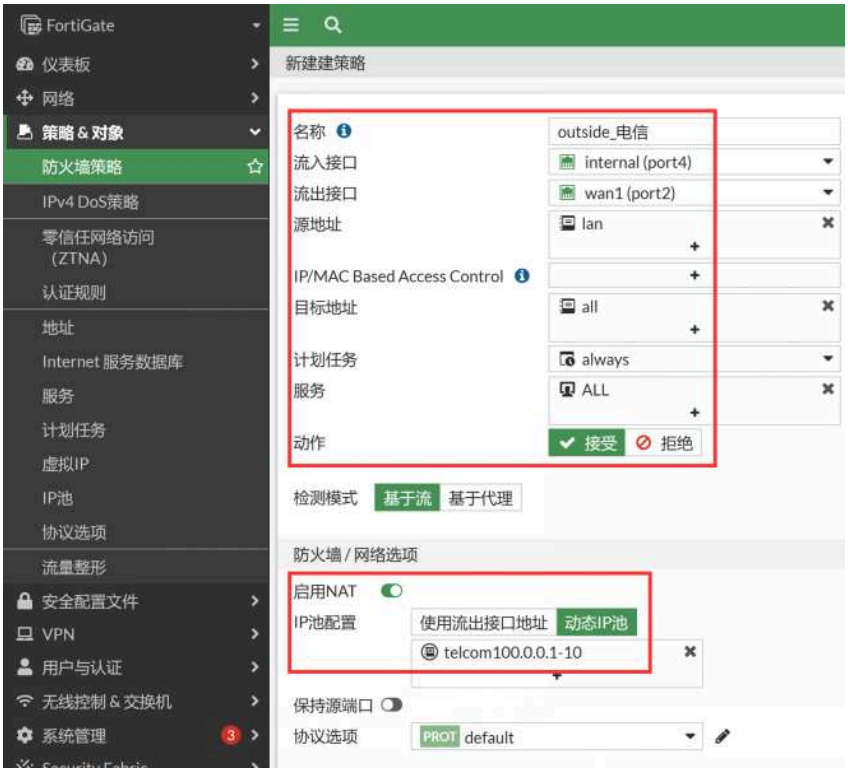


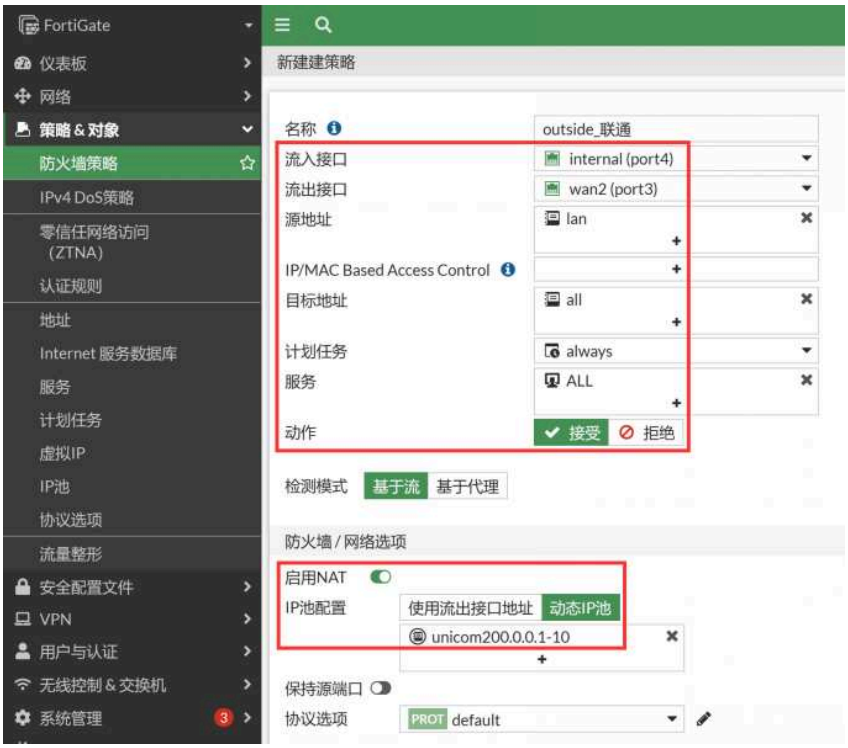
- 类型："超载"，动态的从地址池中分配
- 外部IP范围/子网：NAT转换后的源地址池
- 地址解析协议回复：启用，地址池会回应ARP请求

```
config firewall ippool
    edit "telcom100.0.0.1-10"
        set startip 100.0.0.1
        set endip 100.0.0.10
    next
    edit "unicom200.0.0.1-10"
        set startip 200.0.0.1
        set endip 200.0.0.10
    next
end
```

5. 配置上网放通策略，进入策略&对象→防火墙策略，新建安全策略。分别创建internal到wan1和internal到wan2的上网策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
config firewall policy
    edit 1
        set name "outside_电信"
        set srcintf "port4"
        set dstintf "port2"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set ippool enable
        set poolname "telcom100.0.0.1-10"
    next
    edit 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set name "outside_联通"
        set srcintf "port4"
        set dstintf "port3"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set ippool enable
        set poolname "unicom200.0.0.1-10"
    next
end

```

- 流入接口：选择internal
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：wan1或wan2
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 勾选" 动态IP地址池"，并选择相应的地址池进行互联网访问
- 点击确定按钮后，系统自动保存配置，策略生效
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

结果验证

客户端上网测试，通过tracert命令，检测去往不同运营IP的路径是否正确。

注意事项

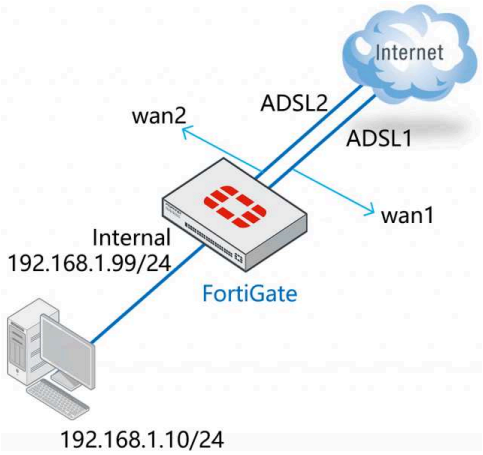
1. **IPPool配置中的外部IP范围不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置IPPool后，IPPool中的地址属于FortiGate自身的IP地址，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。**
2. 如果在SD-WAN中使用ippool的方式做SNAT，一定要在ippool下配置绑定接口，防止ippool在SD-WAN成员中转换错误。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

双线路ADSL

1. 使用两条ADSL拨号接入互联网，内网为192.168.1.0/24网段。
2. 通过策略路由，192.168.1.128/25网段单独使用一条ADSL2线路上网，其他人在ADSL1和ADSL2之间负载。

网络拓扑



配置要点

- wan1（port2）口、wan2（port3）口：接ADSL的接口，务必开启“从服务器重新获得网关”，这样ADSL拨号成功后设备会自动生成默认路由，无需手动配置默认路由
- internal（port4）口: IP地址设置格式为：192.168.1.99/24，可选择性地开启接口的管理功能
- 配置地址对象"lan"内容为：192.168.1.0/24， "lan1"内容为: 192.168.1.128/25。
- 配置从internal到wan1口的策略，并开启NAT
- 配置从internal到wan2口的策略，并开启NAT
- 配置策略路由，强制 lan1地址段使用wan2口访问互联网

配置步骤

1. 配置wan1口和wan2口的PPPoE，建议在CLI下配置PPPoE接口，使用此方式配置获取到IP后会自动添加默认路由到运营商。

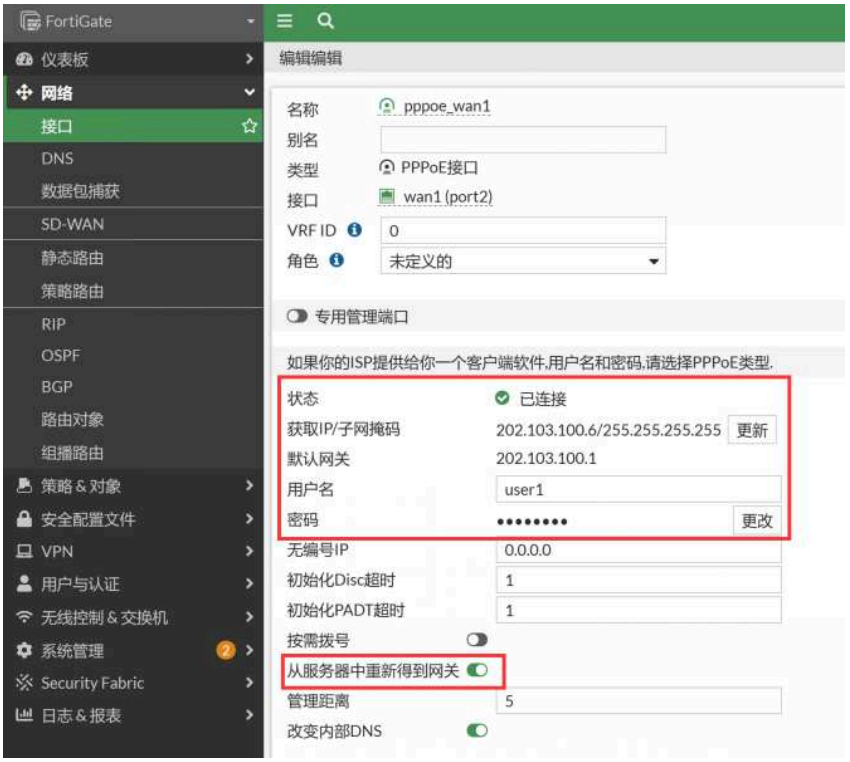
> **重要**
>
> 建议通过CLI的方式新建PPPoE虚拟接口，参考：部署前注意事项→PPPoE接口 ↗配置章节。

```
config system pppoe-interface
    edit "pppoe_wan1"
        set device "port2"
        set username "user1"
        set password ENC
iPUwfhZvvT1T1+v3UPEiPkxLa7RArisivypVqKeSgnPpEGbxLuddF05fEn962jPWkP+PyJBPoKRJcigI+8qvIuzFdBwFW2Mn/EF3Dq6zkcQqTfBT=
    next
    edit "pppoe_wan2"
        set device "port3"
        set username "user2"
        set password ENC
1ZwM5cq6bHbQbaIYXw89RBaYTCvlGH3TVghDsO0OMj1WdIEi/jCtnSTdvG3WfL9Iy9/r0C+D/CGI4hplaN2I/ga3Fp2x/dXfeQnQ2Xf82A6FGZ1R=
    next
end

以上命令执行后，会自动在system interface下创建同名接口，其中包含“从服务器中重新得到网关”的配置
FortiGate # show full sys int pppoe
config system interface
    edit "pppoe_wan1"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set defaultgw enable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set interface "port2"
    next
        edit "pppoe_wan2"
        set vdom "root"
        set mode pppoe
        set type tunnel
        set defaultgw enable
        set interface "port3"
    next
end
```

2. 以上配置完成后，可以在GUI上看到wan1（port2）、wan2（port3）下分别多了个PPPoE接口，并获取到了运营商的IP。可以看到“从服务器中重新得到网关”已开启，路由表中两个运营商的默认路由等价负载。

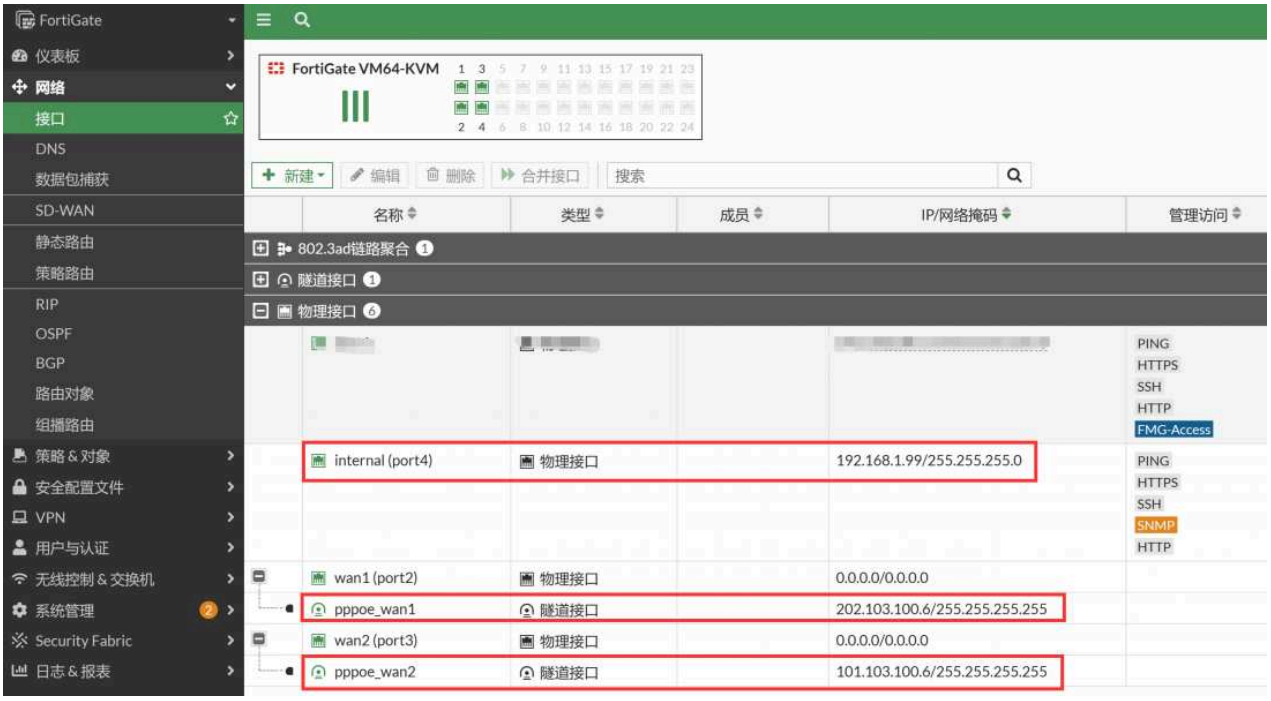




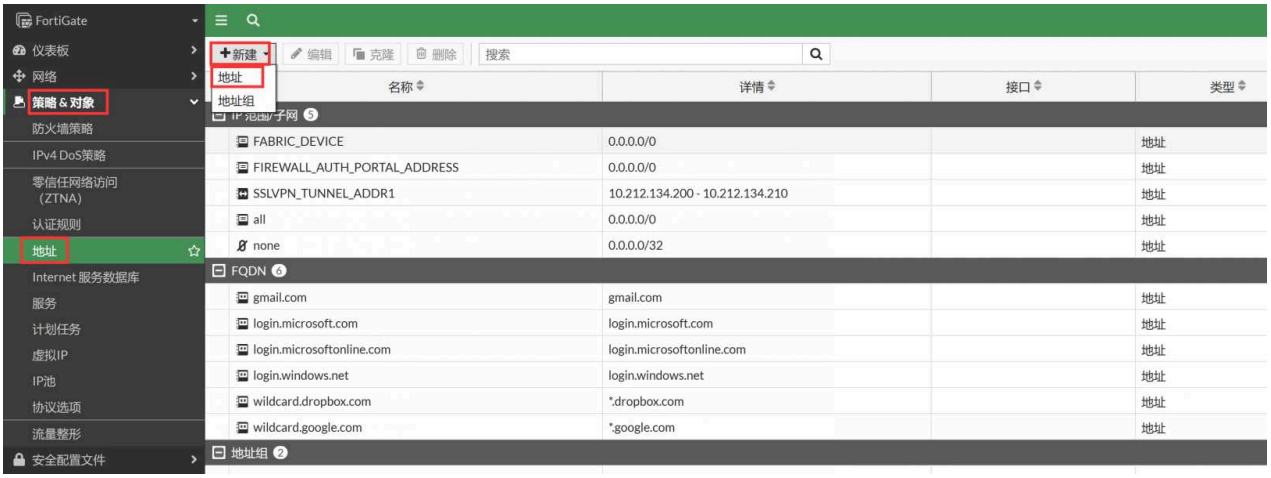
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 101.203.100.1, pppoe_wan2, [1/0]
                  [5/0] via 202.103.100.1, pppoe_wan1, [1/0]
C       101.103.100.6/32 is directly connected, pppoe_wan2
C       101.203.100.1/32 is directly connected, pppoe_wan2
C       202.103.100.1/32 is directly connected, pppoe_wan1
C       202.103.100.6/32 is directly connected, pppoe_wan1
```

3. 配置internal（port4）接口的IP为192.168.1.99/24。选择性地开启接口的管理功能，建议内部开启https、ssh、ping服务。

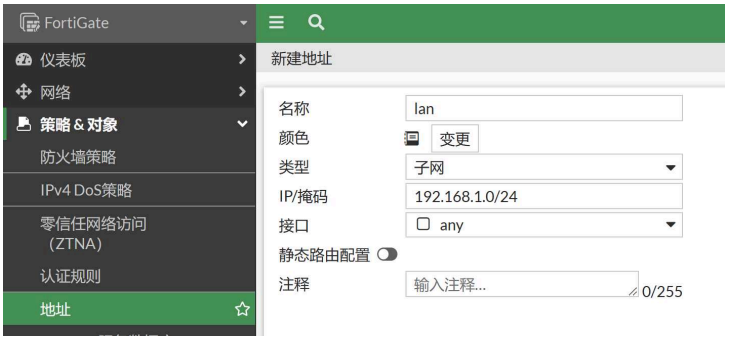


4. 配置地址资源，进入防火墙&对象→地址，点击新建地址按钮。



5. 名称配置为lan，地址节点选择子网：192.168.1.0/24，点击确认。

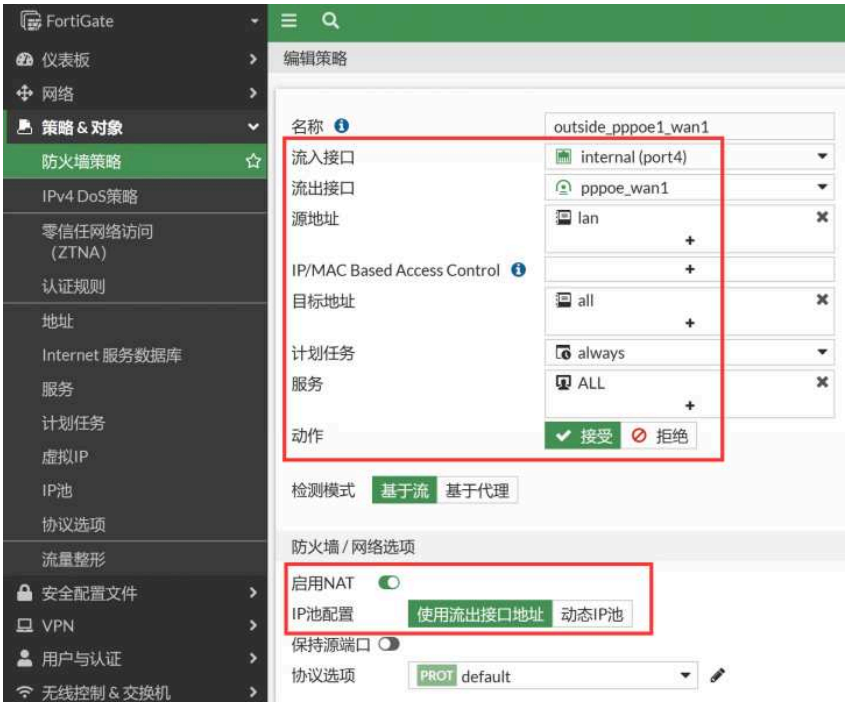
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

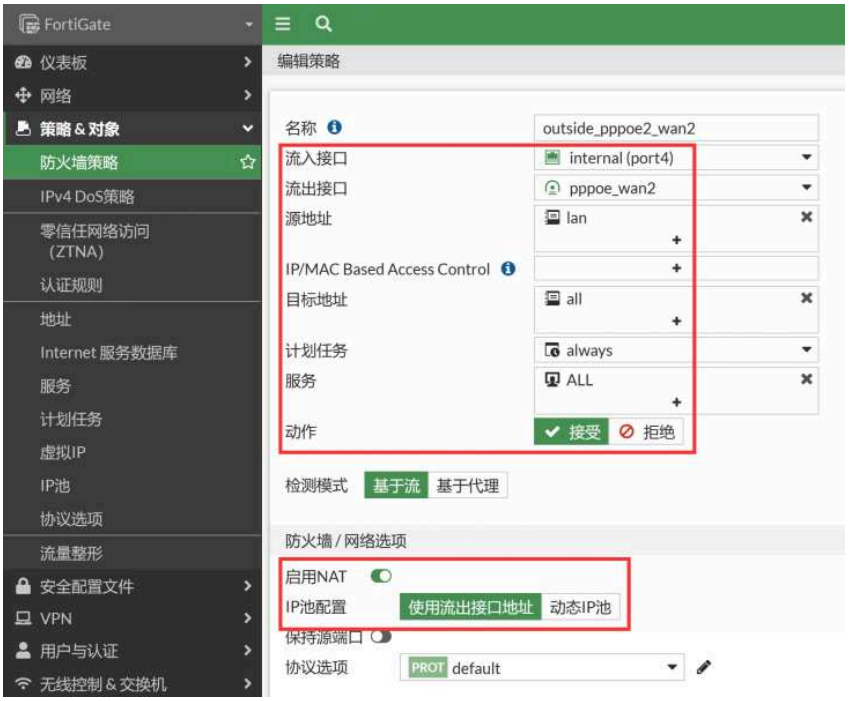



```
config firewall address
    edit "lan"
        set subnet 192.168.1.0 255.255.255.0
    next
end
```

6. 分别为wan1和wan2配置防火墙策略，放通内网到Internet的流量，并开启NAT，点击确定按钮后，系统自动保存配置，策略生效。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
config firewall policy
    edit 1
        set name "outside_pppoe1_wan1"
        set srcintf "port4"
        set dstintf "pppoe_wan1"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 2
        set name "outside_pppoe2_wan2"
        set srcintf "port4"
        set dstintf "pppoe_wan2"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

```

- 流入接口：internal（port4）
- 源地址：选择刚才定义的地址资源lan上网网段
- 流出接口：pppoe接口
- 目的地址选择: all，代表所有的地址
- 时间表：always
- 服务: ALL
- 动作：ACCEPT
- NAT：选择 "启用NAT"， 系统会自动将内网的lan地址段ip，转换为wan1接口地址，进行互联网访问
- 注意：启用"记录允许流量（记录流日志）"将会给系统带来额外的资源消耗，所以非必要情况下请不要启用记录日志

7. 配置策略路由，强制192.168.1.128/25网段单独使用一条ADSL2线路上网（需要在系统管理→可见功能中开启高级路由）。其他地址可以在ADSL1和ADSL两条链路上负载。




```
config router policy
    edit 1
        set input-device "port4"
        set src "192.168.1.128/255.255.255.128"
        set dstaddr "all"
        set output-device "pppoe_wan2"
    next
end
```

- 协议端口：协议类型，0为所有任何协议，可以指定6 tcp,17 udp,132 sctp等
- 流入接口：流量进入接口 ，internal
- 源地址掩码：数据包的源地址，192.168.1.128/25
- 目的地址掩码：数据包的目的地址, 默认全部
- 目的端口：目的端口，默认为所有。从1-65536
- 动作：流量采用的动作
- 流出接口：数据包的流出接口，pppoe_wan2

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 网关地址：流出接口的下一条网关地址， 由于是PPPoE拨号，不写下一跳地址，防火墙会根据静态路由表中的条目，自动使用PPPoE生成的静态路由的下一跳IP

结果验证

1. 将电脑IP地址设置为192.168.1.10/24，网关设置地为192.168.1.99，DNS配置为当地的DNS即可。电脑可通过wan1以及wan2访问互联网。

2. 更改主机IP为192.168.1.168/24，主机只能通过wan2口访问互联网。

3. 排障时可使用 tracert命令，或者抓包命令来查看数据包流出接口。

```
FortiGate#diagnose sniffer packet any 'icmp and host x.x.x.x' 4    //x.x.x.x为测试目标地址
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

端口映射应原理

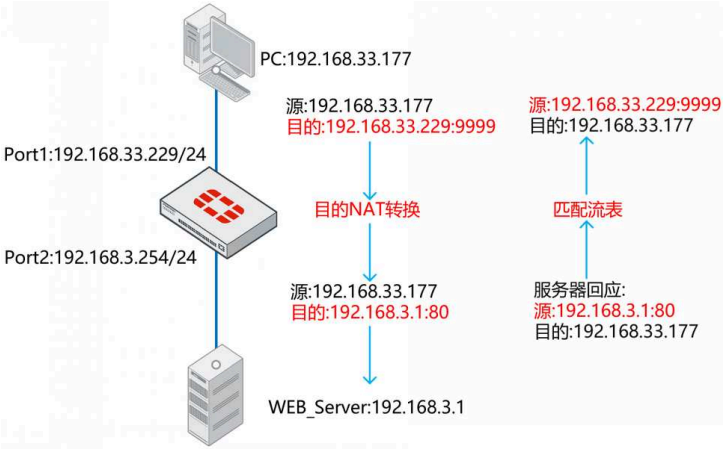
功能原理

数据从FortiGate通过时的处理流程：

1. 入接口收到数据包→新建流表或匹配流表→匹配目的NAT→查路由表→匹配安全策略→数据向出口转发→匹配源NAT→出接口转发数据包。
2. 源NAT转换通俗地讲即将源地址转换为另一个地址，目的地址不变。局域网的私网地址需要将源地址转换为公网地址才能访问外网。
3. 目的NAT转换通俗地讲即将目的地址转换为另一个地址，源地址不变。公网地址访问私网地址的服务器首先是将数据发给服务器所在的局域网的公网地址，再由设备将目的地址转换为服务器地址。

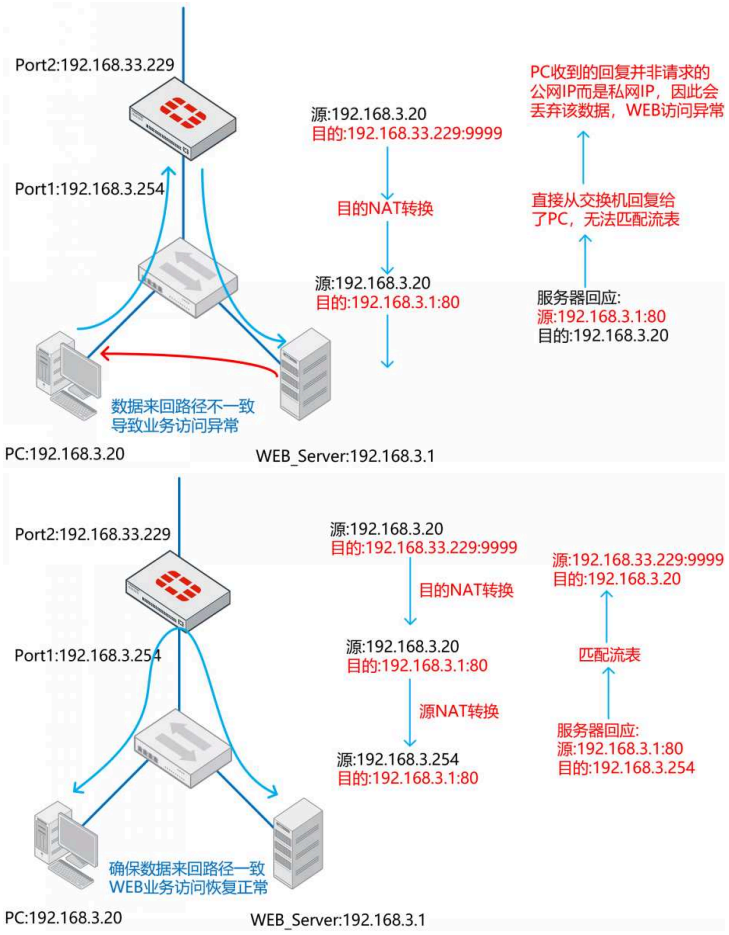
端口映射流程举例

1. 外网地址192.168.33.177访问服务器192.168.3.1的过程为：
   - 外网访问服务器的源IP为192.168.33.177，目的地址为192.168.33.229，目的端口为9999，经过FortiGate的目的NAT转换，将目的IP转换为192.168.3.1，目的端口转换为80。
   - 服务器回应时源IP为192.168.3.1，源端口为80，目的地址为192.168.33.177，匹配刚才目的NAT转换所建的流表将源IP地址转换为192.168.33.229，源端口转换为9999。



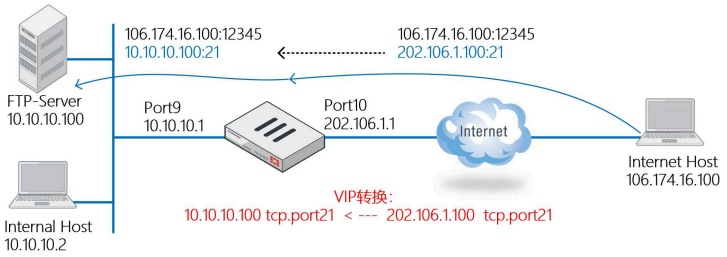
2. 内网用户192.168.3.20通过公网地址192.168.33.229访问服务器的数据过程需保证来回路径一致，所以需要配置源NAT转换也需要配置目的NAT转换：
   - 内网PC发出的源IP为192.168.3.20，目的IP为192.168.33.229，数据到FortiGate后，将源IP转换为内网口IP地址192.168.3.254，目的IP转换为192.168.3.1（注意目的端口也由9999变为80）。
   - 服务器收到数据后回应的源IP为192.168.3.1，目的IP为192.168.3.254，数据到FortiGate后，匹配刚才源NAT转换和目的NAT转换的流表，将192.168.3.1变为192.168.33.229，192.168.3.254变为192.168.3.20，则此时源IP地址变为192.168.33.229（注意源端口也由80变为9999），目的IP地址变为192.168.3.20，发送给内网PC。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



配置举例

网络拓扑



配置步骤

1. 新建VIP映射，将公网地址从port10映射到内部的FTP服务器私网IP。

```
config firewall vip
    edit VIP-FTP-server-port10
        set extip 202.106.1.100
        set extintf "port10"
        set portforward enable
        set mappedip 10.10.10.100
        set extport 21
        set mappedport 21
end
```

2. 创建安全策略引用该VIP。

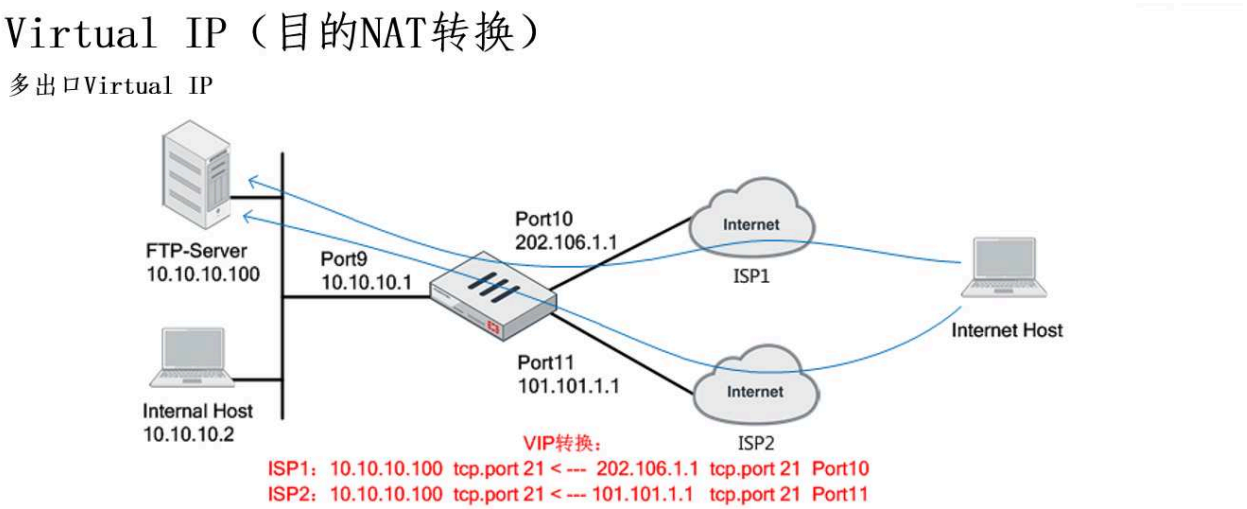
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall policy
    edit 0
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr VIP-ETP-Server-port10
        set action accept
        set schedule "always"
        set service "ALL"
end
```

3. 使用Internet PC访问VIP的FTP服务，查看会话表项。

```
FG1000D # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT          DESTINATION       DESTINATION-NAT
tcp     3551   106.174.16.100:4063 -                202.106.1.100:21  10.10.10.100:21  //Dnat转换session
icmp    59     10.10.10.100:512 202.106.1.1:62464  202.106.1.2:8     -                // 服务器OUT 走普通Snat
icmp    60     10.10.10.100:512 202.106.1.1:62464  106.174.16.100:8  -
FG1000D # diagnose sys session list
session info: proto=6 proto_state=01 duration=285 expire=3315 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=128/3/1 reply=130/2/1 tuples=2
orgin->sink: org pre->post, reply pre->post dev=17->16/16->17 gwy=10.10.10.100/202.106.1.2
hook=pre dir=org act=dnat 106.174.16.100:4063->202.106.1.100:21(10.10.10.100:21)
hook=post dir=reply act=snat 10.10.10.100:21->106.174.16.100:4063(202.106.1.100:21)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=2 auth_info=0 chk_client_info=0 vd=0
serial=015d9e27 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0
```

4. 多出口Virtual IP的场景。



双出口的VIP配置只需正常添加另外一条VIP条目和另外一个策略即可，但要特别主要在双出口环境下的RPF（反向路由检查）问题，如果双出口做负载均衡的情况下无需注意RPF检查问题，但是如果想要做浮动路由主备，需修改路由的优先级大小而非管理距离大小，以保证两条默认路由同时存在于路由表中。

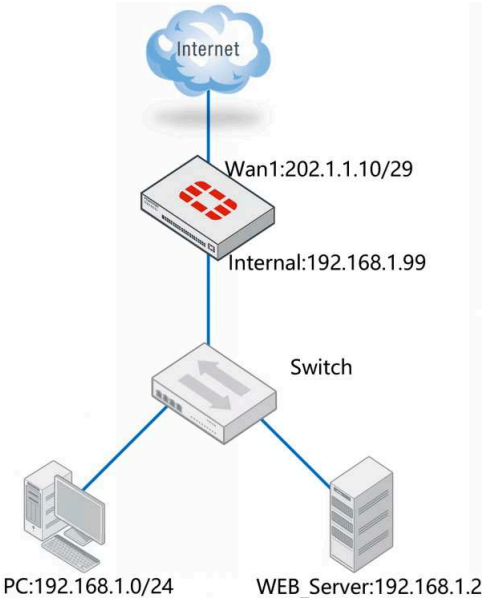
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

地址映射（一对一IP映射）

网络需求

用户已完成了防火墙基础配置，现在需要将内网的一台web服务器需要将HTTPS服务全映射到外网口的地址，让外网的用户能访问到此服务器。

网络拓扑



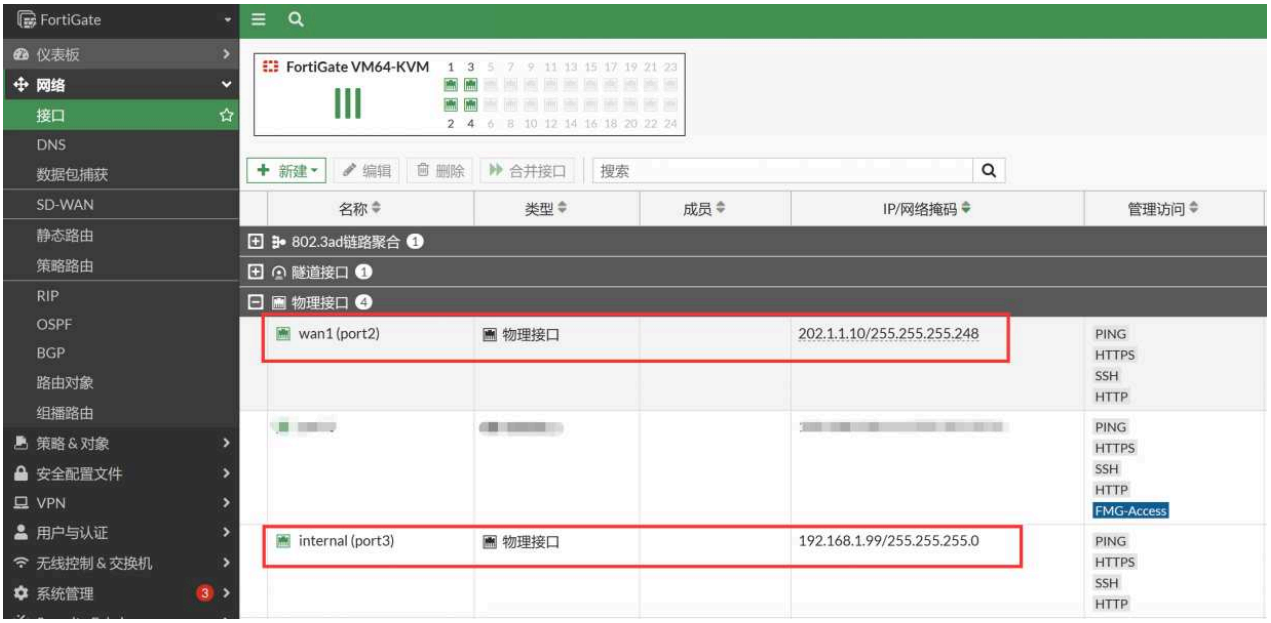
配置要点

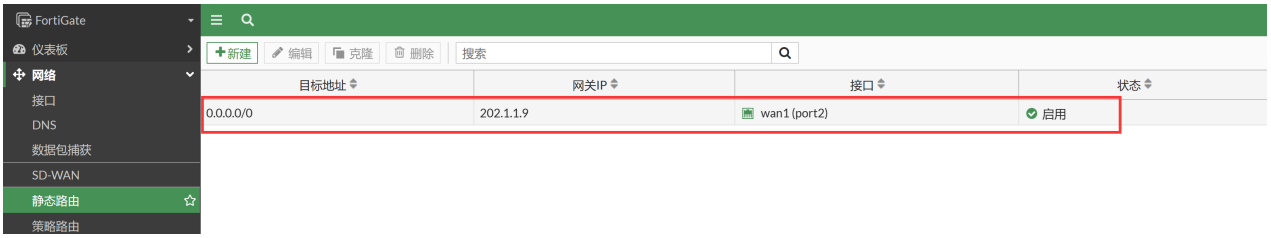
- 基础上网配置
- 配置虚拟IP（DNAT）
- 配置安全策略

配置步骤

1. 基础上网配置，请参照网络管理→路由模式→静态地址上网方式↗章节，接口IP、静态路由配置如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 进入策略&对象→虚拟IP，新建虚拟IP。

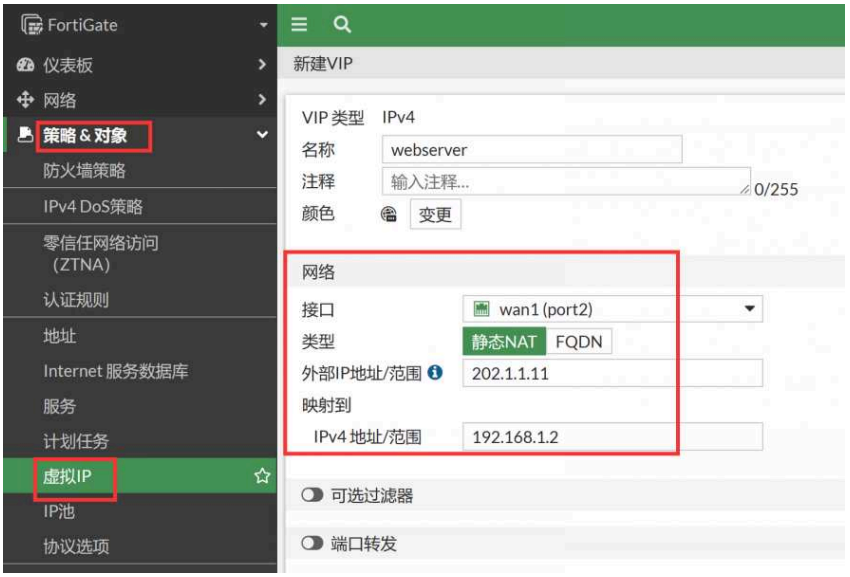
3. 配置VIP，名称为webserver，用于wan1接口。

重要

VIP配置中的外部IP不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP后，extip属于FortiGate自身的IP地址，即使VIP没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。

重要

强烈建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。



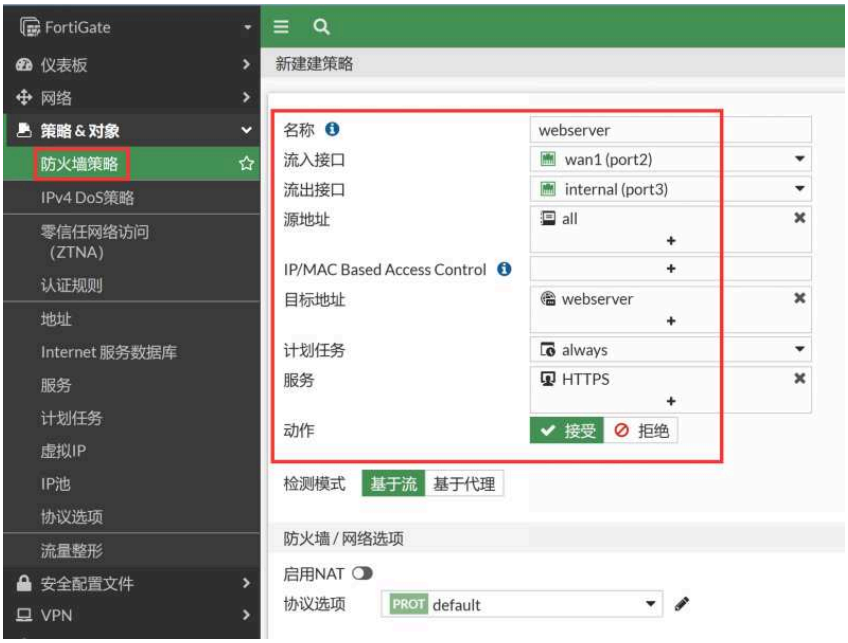
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall vip
    edit "webserver"
        set extip 202.1.1.11
        set mappedip "192.168.1.2"
        set extintf "port2"
    next
end
```

重要

“外部的IP地址/范围”和“映射的IPv4地址/范围”数量是对应，一对一映射，可以只写一个IP对一个IP的映射关系，也可以写一个映射范围。比如202.1.1.3-202.1.1.10，内部映射必须是192.168.1.2-192.168.1.9，对应映射关系也是对应的，202.1.1.3对应192.168.1.2，202.1.1.14对应192.168.1.3，依此类推。

4. 配置安全策略引用VIP。




```
config firewall policy
    edit 1
        set name "webserver"
        set srcintf "port2"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "webserver"
        set schedule "always"
        set service "HTTPS"
    next
end
```

- 流入接口：wan1 //如内网用户也需通过虚拟IP访问，需将此处设置为any
- 源地址：all
- 流出接口： internal
- 目的地址: webserver //定义好的虚拟IP映射对象
- 服务: HTTPS //只允许进行HTTPS服务访问
- 注意：如内网用户也需通过虚拟IP访问，有2种方式可实现：
  - 需将原策略的【流入接口】设置为any，并在该策略上开启NAT
  - 或者添加一条【流入接口】为internal的内到内策略，并在该策略上开启NAT
- NAT：根据需求开启，如果内网服务器到源客户端公网IP没有路由可达，仅有到达FortiGate内网口的路由，则需要开启NAT，在做DNAT之后再做一次源NAT，将源IP转换为FortiGate内网口IP
- 动作：接受

结果验证

从外部进行访问https://202.1.1.11 ↗ ，如果需要测试映射是否有效可以在策略的服务临时添加ping服务进行测试。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

1. **VIP配置中的外部IP不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP后，extip属于FortiGate自身的IP地址，即使VIP没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。**
2. 强烈建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。

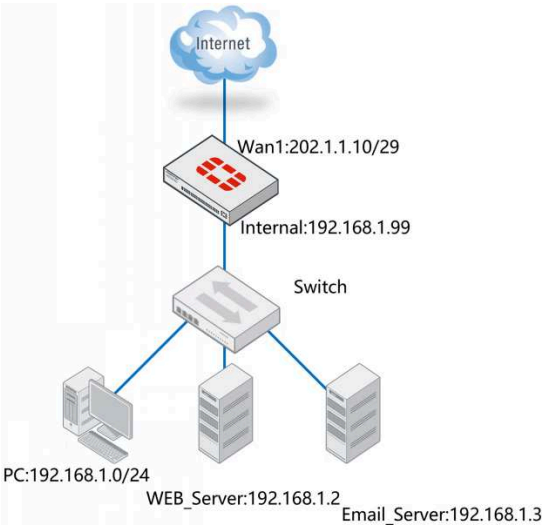
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

端口映射（一对多端口映射）

网络需求

1. 现在需要将内网的一台web服务器（192.168.1.2）的80端口映射到外网口的地址（202.1.1.11）的8080端口（内网端口与外网映射端口不一致）。
2. 将内网的一台email服务器（192.168.1.3）的25端口映射到外网口的地址（202.1.1.11）的25端口。
3. 案例意义：了解FortiGate的关键功能处理模块的匹配顺序：DNAT→路由→安全策略→源NAT。

网络拓扑



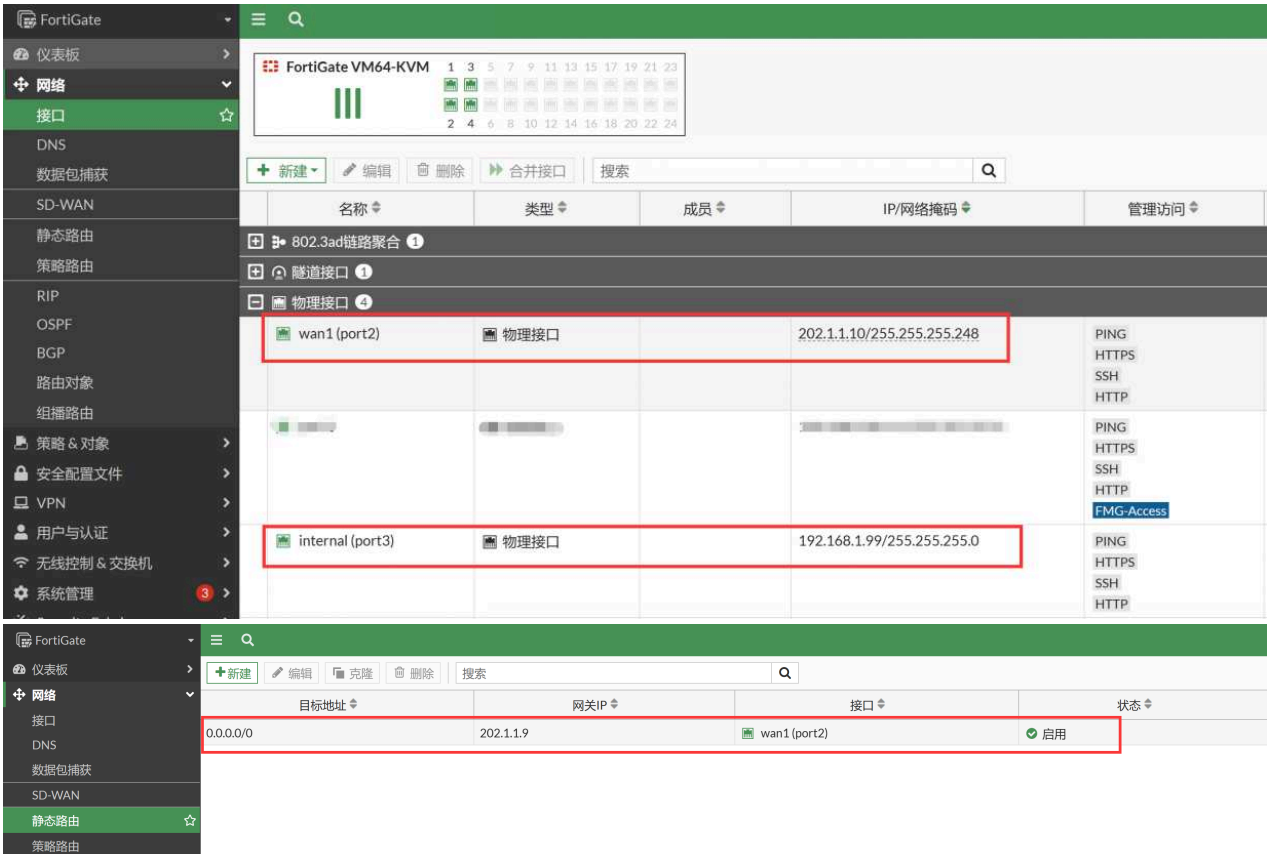
配置要点

- 基础上网配置
- 配置虚拟IP（DNAT）
- 配置安全策略

配置步骤

1. 基础上网配置，请参照网络管理→路由模式→静态地址上网方式↗章节，接口IP、静态路由配置如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 进入策略&对象→虚拟IP，新建虚拟IP。

3. 配置VIP1，名称为webserver:80，对HTTP服务器进行映射，用于wan1接口。

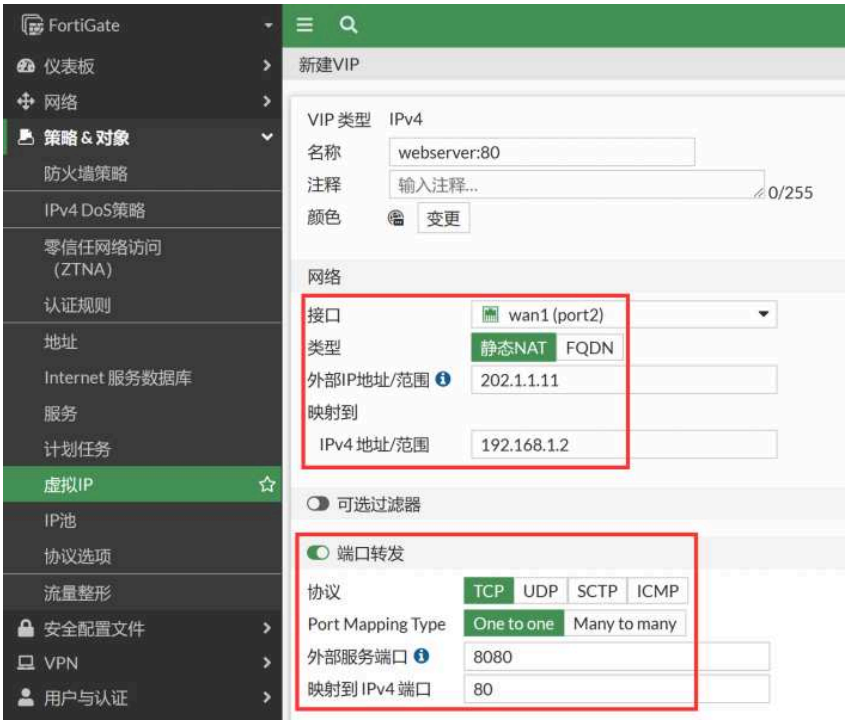
重要

VIP配置中的外部IP不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP后，extip属于FortiGate自身的IP地址，即使VIP没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。

重要

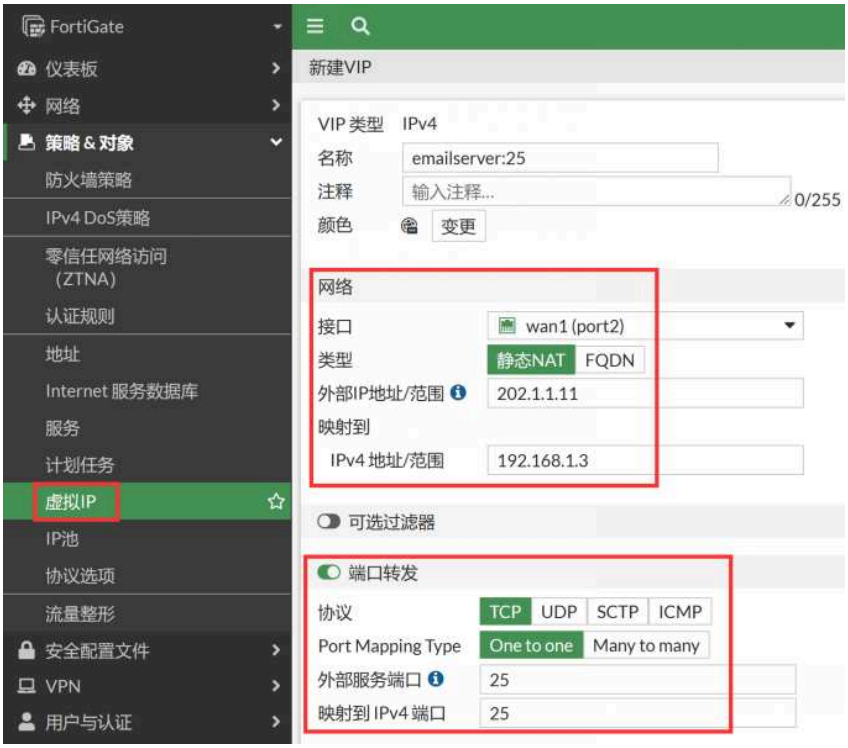
强烈建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置VIP2，名称为emailserver:25，对smtp服务器进行映射，用于wan1接口。

> **重要**
>
> 建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。




```
config firewall vip
    edit "webserver:80"
        set extip 202.1.1.11
        set mappedip "192.168.1.2"
        set extintf "port2"
        set portforward enable
        set extport 8080
        set mappedport 80
    next
```

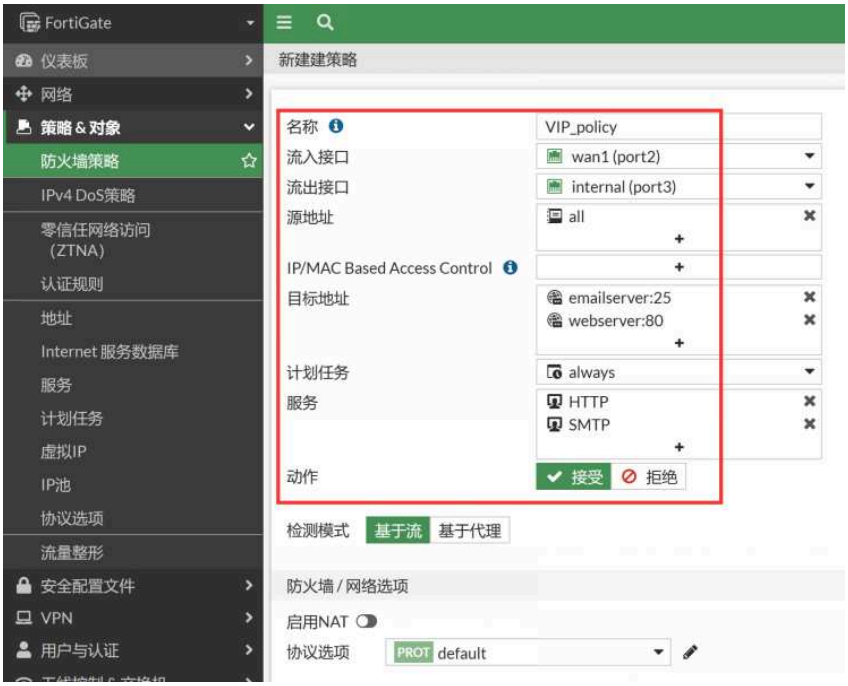

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    edit "emailserver:25"
        set extip 202.1.1.11
        set mappedip "192.168.1.3"
        set extintf "port2"
        set portforward enable
        set extport 25
        set mappedport 25
    next
end
```

重要

“外部的IP地址/范围”和“映射的IPv4地址/范围”数量是对应，一对一映射，可以只写一个IP对一个IP的映射关系，也可以写一个映射范围。比如202.1.1.3-202.1.1.10，内部映射必须是192.168.1.2-192.168.1.9，对应映射关系也是对应的，202.1.1.3对应192.168.1.2，202.1.14对应192.168.1.3，依此类推

5. 配置安全策略引用两个VIP。




```
FortiGate # show firewall policy
config firewall policy
    edit 1
        set name "VIP_policy"
        set srcintf "port2"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "emailserver:25" "webserver:80"
        set schedule "always"
        set service "HTTP" "SMTP"
    next
end
```

- 流入接口：wan1 //如内网用户也需通过虚拟IP访问，需将此处设置为any
- 源地址：all
- 流出接口： internal
- 目的地址: webserver:80和emailserver:25 //定义好的虚拟IP映射对象
- 服务: HTTP和SMTP //只允许进行HTTP和SMTP服务访问
- 注意：如内网用户也需通过虚拟IP访问，有2种方式可实现：
  - 需将原策略的【流入接口】设置为any，并在该策略上开启NAT
  - 或者添加一条【流入接口】为internal的内到内策略，并在该策略上开启NAT
- NAT：根据需求开启，如果内网服务器到源客户端公网IP没有路由可达，仅有到达FortiGate内网口的路由，则需要开启NAT，在做DNAT之后再做一次源NAT，将源IP转换为FortiGate内网口IP
- 动作：接受

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

1. 从外部进行访问http://202.1.1.11 。
2. 从外部访问202.1.1.11的SMTP服务。

注意事项

1. **VIP配置中的外部IP不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP后，extip属于FortiGate自身的IP地址，即使VIP没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。**
2. 强烈建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP、VIP映射的服务器在做SNAT时源地址转换错误等网络问题。

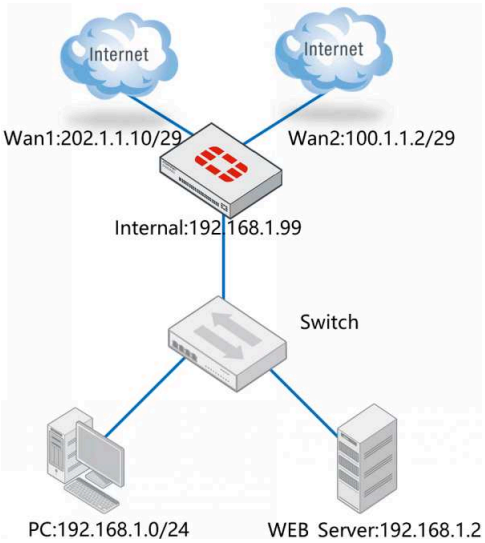
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

多线路端口映射

网络需求

- 将内网中的一台WEB服务器，分别映射到电信和联通２个互联网出口的公网IP上：
  - WEB服务器地址： 192.168.1.2/24 网关：192.168.1.99
  - 电信出口: 202.1.1.2/29 , 网关202.1.1.1，服务器公网地址202.1.1.3
  - 联通出口: 100.1.1.2/29 , 网关100.1.1.1，服务器公网地址100.1.1.3
  - 内部网段192.168.1.0/24需要上互联网
- 案例意义：
  - FortiGate支持数据流源进源出
  - 防火墙会对会话进行跟踪，从电信接口进入的访问，会优先从电信接口返回
  - 从联通接口进入的访问，会优先从联通接口返回
  - 条件是防火墙的路由表内，分别拥有能够匹配返回数据流的路由表，所以只需要配置电信和网通的两条默认路由即可

网络拓扑



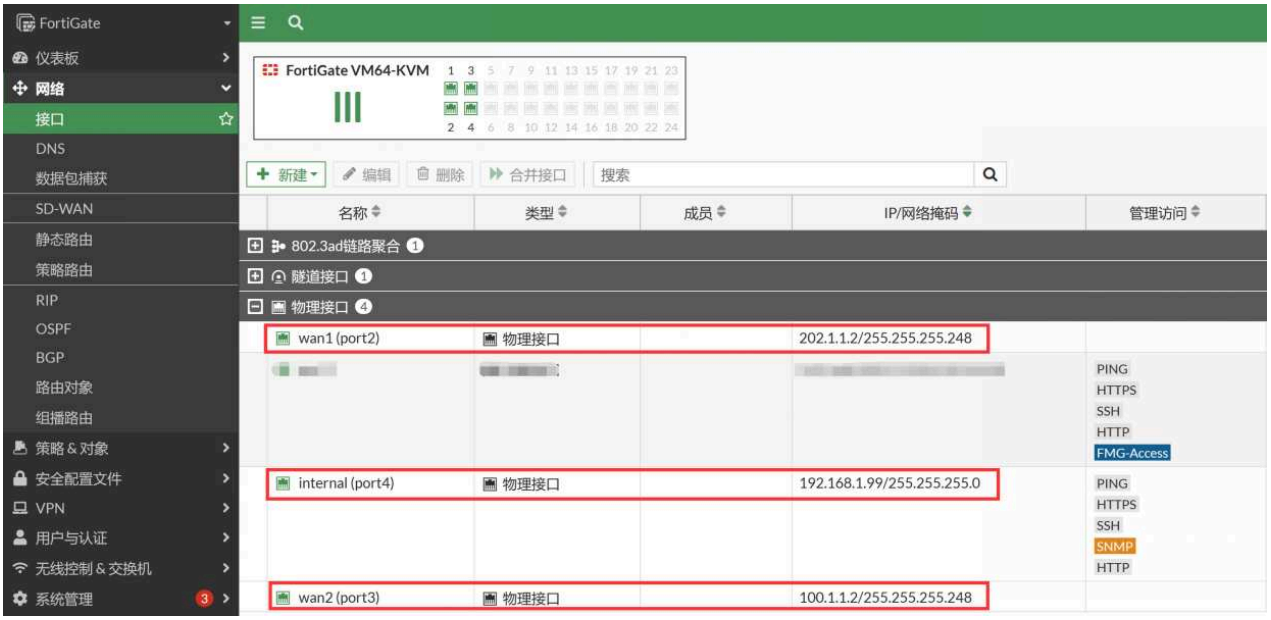
配置要点

- 配置接口IP
- 配置虚拟IP（DNAT）
- 配置安全策略

配置步骤

1. 基础上网配置，请参照策略与对象→多线路上网配置→双线路同运营商上网配置↗章节，接口IP、静态路由配置如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





重要

防火墙会对会话进行跟踪，从电信接口进入的访问，会优先从电信接口返回；从联通接口进入的访问，会优先从联通接口返回。条件是防火墙的路由表内，分别拥有能够匹配返回数据流的路由表。所以只需要配置电信和网通的两条默认路由即可。

2. 查看路由表，存在两条等价默认路由。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port3, [1/0]
                  [10/0] via 202.1.1.1, port2, [1/0]
C       100.1.1.0/29 is directly connected, port3
C       192.168.1.0/24 is directly connected, port4
C       202.1.1.0/29 is directly connected, port2
```

3. 进入策略&对象→虚拟IP，新建虚拟IP。

重要

建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。

4. 配置VIP1，名称为web1，对HTTP服务器进行映射，用于wan1（电信）接口。

重要

VIP配置中的外部IP不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP后，extip属于FortiGate自身的IP地址，即使VIP没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

强烈建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。



5. 配置VIP2，名称为web2，对HTTP服务器进行映射，用于wan2（联通）接口。



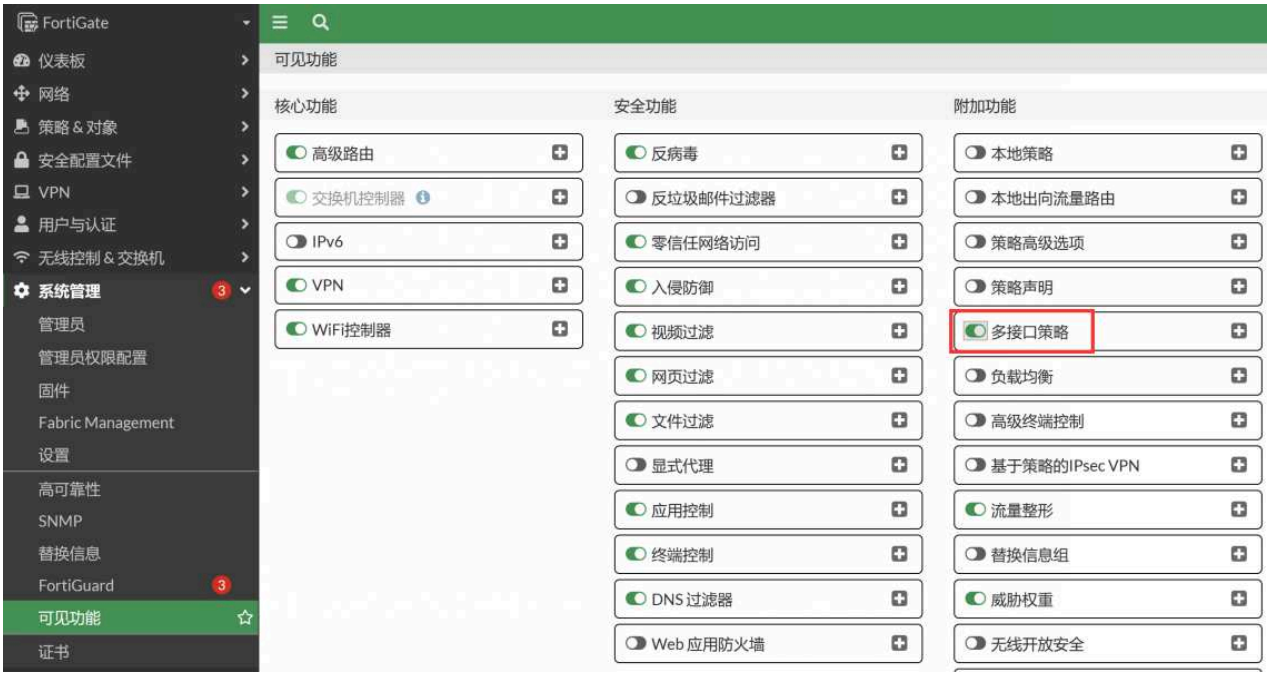

```
config firewall vip
    edit "web1"
        set extip 202.1.1.3
        set mappedip "192.168.1.2"
        set extintf "port2"
    next
    edit "web2"
        set extip 100.1.1.3
        set mappedip "192.168.1.2"
        set extintf "port3"
    next
end
```

重要

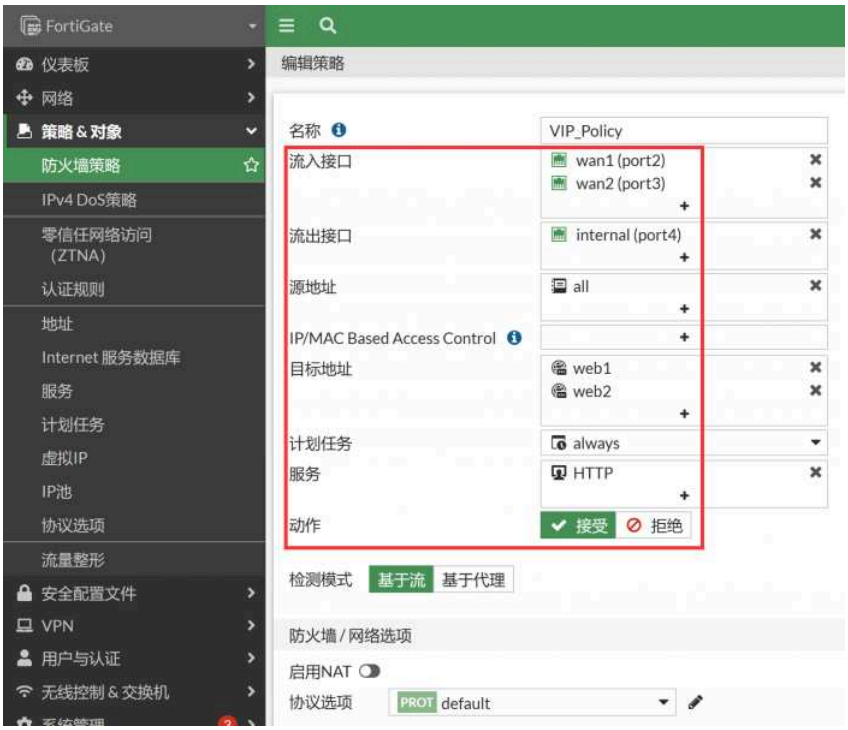
“外部的IP地址/范围”和“映射的IPv4地址/范围”数量是对应，一对一映射，可以只写一个IP对一个IP的映射关系，也可以写一个映射范围。比如202.1.1.3-202.1.1.10，内部映射必须是192.168.1.2-192.168.1.9，对应映射关系也是对应的，202.1.1.3对应192.168.1.2，202.1.1.14对应192.168.1.3，依此类推。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

6. 配置安全策略引用两个VIP，默认配置下，两条链路需要针对两个VIP配置两条防火墙策略，这里我们可以通过一条策略实现，打开系统管理→可见功能，开启“多接口策略”功能，这样我们就可以在防火墙策略的流入接口和流出接口中选择多个接口。



7. 配置安全策略引用两个VIP，入接口可以选择多个接口，同时选择wan1和wan2。

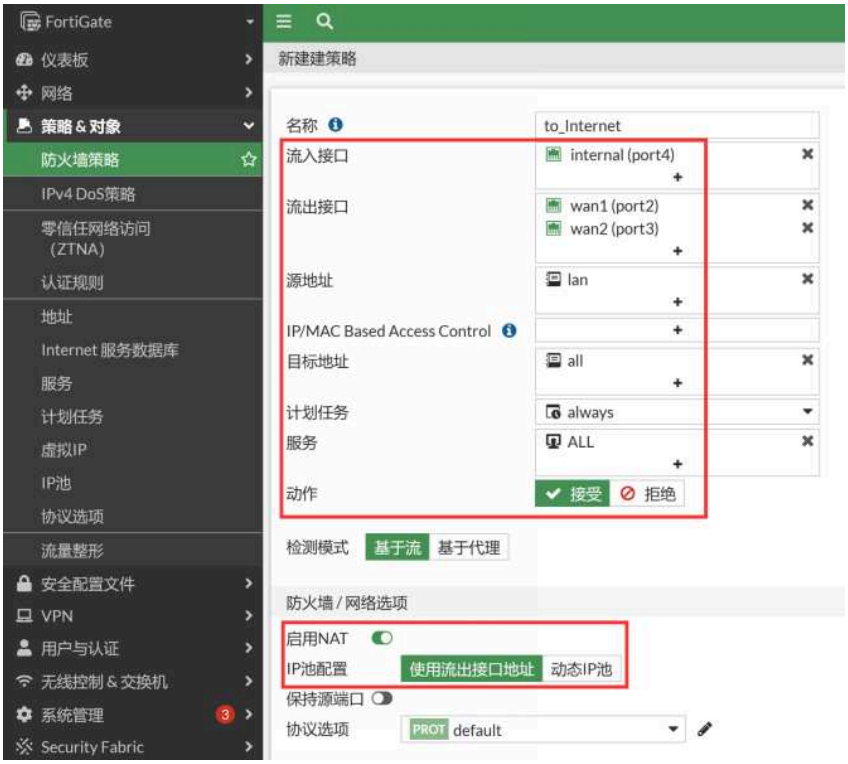



```
config firewall policy
    edit 1
        set name "VIP_Policy"
        set srcintf "port2" "port3"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "web1" "web2"
        set schedule "always"
        set service "HTTP"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 流入接口：wan1、wan2 //如内网用户也需通过虚拟IP访问，需将此处设置为any
- 源地址：all
- 流出接口： internal
- 目的地址: web1和web2 //定义好的虚拟IP映射对象
- 服务: HTTP //只允许进行HTTP服务访问
- 注意：如内网用户也需通过虚拟IP访问，有2种方式可实现：
  - 需将原策略的【流入接口】设置为any，并在该策略上开启NAT
  - 或者添加一条【流入接口】为internal的内到内策略，并在该策略上开启NAT
- NAT：根据需求开启，如果内网服务器到源客户端公网IP没有路由可达，仅有到达FortiGate内网口的路由，则需要开启NAT，在做DNAT之后再做一次源NAT，将源IP转换为FortiGate内网口IP
- 动作：接受

8. 配置内网网段访问两条互联网线路的放通策略。




```
config firewall policy
    edit 2
        set name "to_Internet"
        set srcintf "port4"
        set dstintf "port2" "port3"
        set action accept
        set srcaddr "lan"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

结果验证

1. 分别从2个运营商接口访问202.1.1.3和100.1.1.3两个IP的80端口。
2. 内网用户可以通过两条线路访问Internet。

注意事项

1. VIP配置中的外部IP不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP后，extip属于FortiGate自身的IP地址，即使VIP没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。
2. 强烈建议在配置VIP时，选择绑定接口，这样可以防止VIP在其他接口响应ARP导致的网络问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

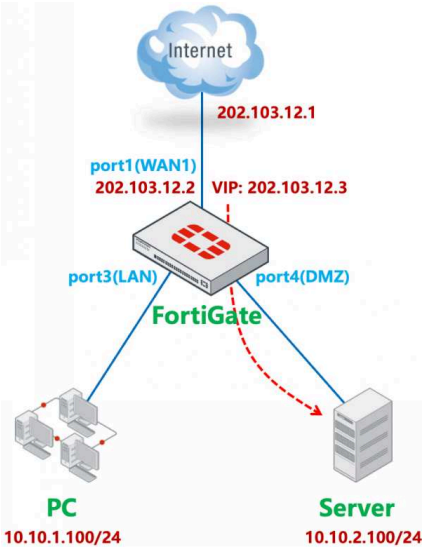
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VIP映射的主机访问Internet

网络需求

某用户使用VIP一对一映射了一个公网IP到内网服务器，同时又需要此服务器通过FortiGate的SNAT访问Internet。

网络拓扑



1. 在port1（WAN1）上通过VIP将202.103.12.3映射到内网Server 10.10.2.100。
2. 内网PC和Server都通过port1（WAN1）做SNAT访问Internet，SNAT策略配置转换的源IP为借用出接口地址202.103.12.2。

配置步骤

1. 配置VIP映射，将202.103.12.3映射到内网Server 10.10.2.100。

> **重要**
>
> 建议在配置 VIP 时绑定对应的接口，详情见“结果验证”的第2步。




```bash
config firewall vip
    edit "VIP_to_Server"
        set extip 202.103.12.3
        set mappedip "10.10.2.100"
        set extintf "port1"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    next
end
```

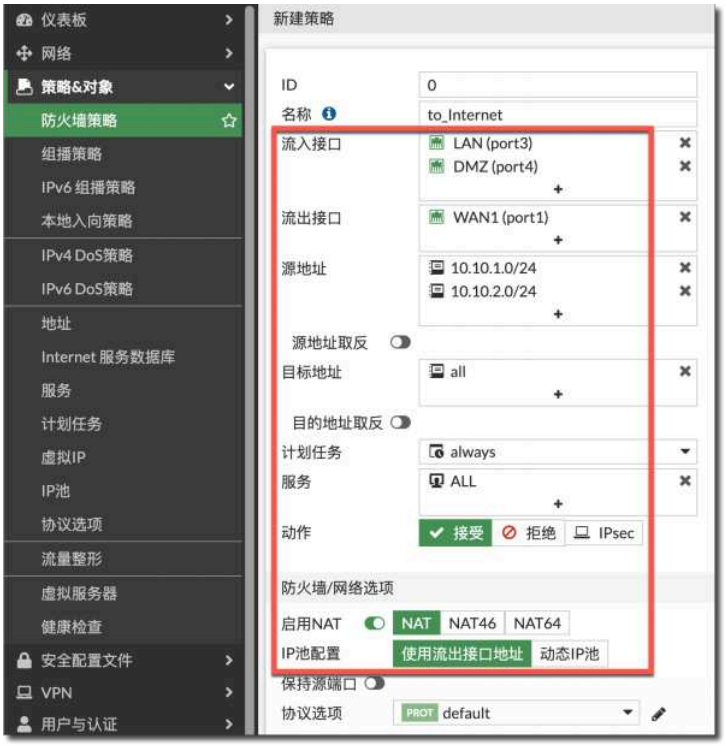
2. 使用安全策略放通Internet到VIP的访问。




```bash
config firewall policy
    edit 1
        set name "VIP_to_Server"
        set srcintf "port1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP_to_Server"
        set schedule "always"
        set service "ALL"
    next
end
```

3. 配置上网策略，允许内网PC和Server访问Internet，并开启SNAT，SNAT IP池选择使用流出接口地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 2
        set name "to_Internet"
        set srcintf "port3" "port4"
        set dstintf "port1"
        set action accept
        set srcaddr "10.10.1.0/24" "10.10.2.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

结果验证

1. 内网PC可以访问Internet时，SNAT转换的源地址正确地转换为出接口port1（WAN1）的IP地址202.103.12.2。

```
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
10.314895 port3 in 10.10.1.100 -> 110.242.68.3: icmp: echo request
10.314955 port1 out 202.103.12.2 -> 110.242.68.3: icmp: echo request
10.329378 port1 in 110.242.68.3 -> 202.103.12.2: icmp: echo reply
10.329411 port3 out 110.242.68.3 -> 10.10.1.100: icmp: echo reply
11.329278 port3 in 10.10.1.100 -> 110.242.68.3: icmp: echo request
11.329294 port1 out 202.103.12.2 -> 110.242.68.3: icmp: echo request
11.342086 port1 in 110.242.68.3 -> 202.103.12.2: icmp: echo reply
11.342098 port3 out 110.242.68.3 -> 10.10.1.100: icmp: echo reply
```

2. Server也可以正常访问Internet，但是经过SNAT后，转换的源地址不是出接口port1（WAN1）的IP地址202.103.12.2，而是VIP配置的extip地址202.103.12.3。

> **重要**
>
> 在多公网出口环境中，VIP 配置必须按照上述配置步骤绑定对应的公网接口，否则映射的 Server 主动访问 Internet 并执行 SNAT 时，可能会选错 SNAT 源地址。

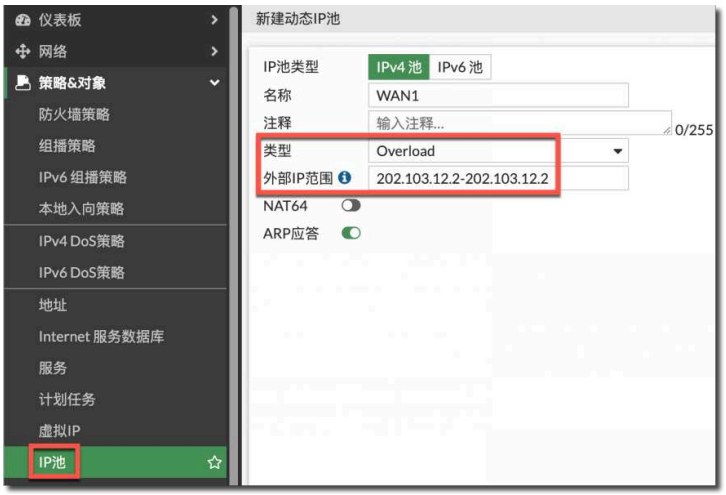
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
6.055136 port4 in 10.10.2.100 -> 110.242.68.4: icmp: echo request
6.055191 port1 out 202.103.12.3 -> 110.242.68.4: icmp: echo request
6.068436 port1 in 110.242.68.4 -> 202.103.12.3: icmp: echo reply
6.068471 port4 out 110.242.68.4 -> 10.10.2.100: icmp: echo reply
7.063159 port4 in 10.10.2.100 -> 110.242.68.4: icmp: echo request
7.063176 port1 out 202.103.12.3 -> 110.242.68.4: icmp: echo request
7.075904 port1 in 110.242.68.4 -> 202.103.12.3: icmp: echo reply
7.075913 port4 out 110.242.68.4 -> 10.10.2.100: icmp: echo reply
```

3. 默认配置下，当访问Internet的SNAT策略使用流出接口地址作为IP池配置时，有VIP映射的服务器访问Internet，会优先使用VIP的extip（202.103.12.3）作为SNAT的源地址，而不是流出接口地址（202.103.12.2）。

解决方法

1. 如果要求VIP映射的服务器访问Internet时，按照上网策略的配置使用流出接口地址作为SNAT的源地址，则需要将上网策略的SNAT池改为“动态IP池”方式。新建IP池，范围配置为出接口port1（WAN1）的IP。




```bash
config firewall ippool
    edit "WAN1"
        set startip 202.103.12.2
        set endip 202.103.12.2
    next
end
```

2. 编辑上网策略，将“IP池配置”修改为“动态IP池”，选择上步创建的IP池。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 2
        set name "to_Internet"
        set srcintf "port3" "port4"
        set dstintf "port1"
        set action accept
        set srcaddr "10.10.1.0/24" "10.10.2.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set ippool enable
        set poolname "WAN1"
    next
end
```

3. 再次使用Server访问Internet，可以看到FortiGate使用出接口port1（WAN1）作为SNAT的源地址。

```
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
1.358499 port4 in 10.10.2.100 -> 110.242.68.3: icmp: echo request
1.358517 port1 out 202.103.12.2 -> 110.242.68.3: icmp: echo request
1.372310 port1 in 110.242.68.3 -> 202.103.12.2: icmp: echo reply
1.372331 port4 out 110.242.68.3 -> 10.10.2.100: icmp: echo reply
2.364802 port4 in 10.10.2.100 -> 110.242.68.3: icmp: echo request
2.364819 port1 out 202.103.12.2 -> 110.242.68.3: icmp: echo request
2.377127 port1 in 110.242.68.3 -> 202.103.12.2: icmp: echo reply
2.377137 port4 out 110.242.68.3 -> 10.10.2.100: icmp: echo reply
```

4. 如果上网策略配置了“动态IP池”，但VIP映射的Server又想使用VIP的extip作为SNAT的源地址，那么可以通过如下配置实现。在VIP的配置中开启nat-source-vip后，即使上网策略的SNAT使用了“动态IP池”，VIP映射的主机依然会使用VIP的extip作为SNAT的源地址。

```bash
config firewall vip
    edit "VIP_to_Server"
        set nat-source-vip enable
    next
end
```

5. 开启nat-source-vip后，Server再次访问Internet，SNAT转换的源地址是VIP配置的extip地址202.103.12.3。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose sniffer packet any icmp 4
Using Original Sniffing Mode
interfaces=[any]
filters=[icmp]
2.769121 port4 in 10.10.2.100 -> 110.242.68.3: icmp: echo request
2.769275 port1 out 202.103.12.3 -> 110.242.68.3: icmp: echo request
2.782631 port1 in 110.242.68.3 -> 202.103.12.3: icmp: echo reply
2.782670 port4 out 110.242.68.3 -> 10.10.2.100: icmp: echo reply
3.781464 port4 in 10.10.2.100 -> 110.242.68.3: icmp: echo request
3.781469 port1 out 202.103.12.3 -> 110.242.68.3: icmp: echo request
3.795056 port1 in 110.242.68.3 -> 202.103.12.3: icmp: echo reply
3.795062 port4 out 110.242.68.3 -> 10.10.2.100: icmp: echo reply
```

总结

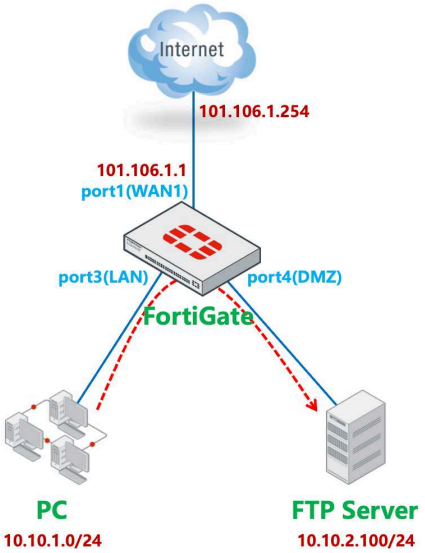
1. **上网策略的SNAT使用“流出接口地址”作为“IP池配置”时：**VIP映射的内网Server访问Internet，FortiGate使用VIP的extip作为SNAT的源IP，而不是上网策略的出接口地址（nat-source-vip不起任何作用）。
2. **上网策略的SNAT使用“动态IP池”作为“IP池配置”时：**
   - 默认情况下，VIP映射的内网Server访问Internet，FortiGate使用IP池范围中的地址作为SNAT的源IP，而不是VIP的extip。
   - 如果想使用VIP的extip作为SNAT的源IP，则需要在VIP配置中开启nat-source-vip。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

内网主机通过公网IP访问VIP

需求场景一

- *PC与Server对于FortiGate属于不同的接口、相同的网段。*
- *PC与Server属于不同网段。*



1. FortiGate的port1（WAN1）连接ISP。默认路由1指向port1（WAN1）。

> **重要**
>
> 如果通过策略路由来控制内网PC访问Internet，请参考本文注意事项章节中的说明。

```bash
FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.106.1.254, port1, [1/0]
C       10.10.1.0/24 is directly connected, port3
C       10.10.2.0/24 is directly connected, port4
C       101.106.1.0/24 is directly connected, port1
```

2. FortiGate通过配置VIP，在port1（WAN1）的公网IP 101.106.1.1上映射了FTP Server的21端口。

3. 内网PC通过port1（WAN1）做SNAT访问互联网。

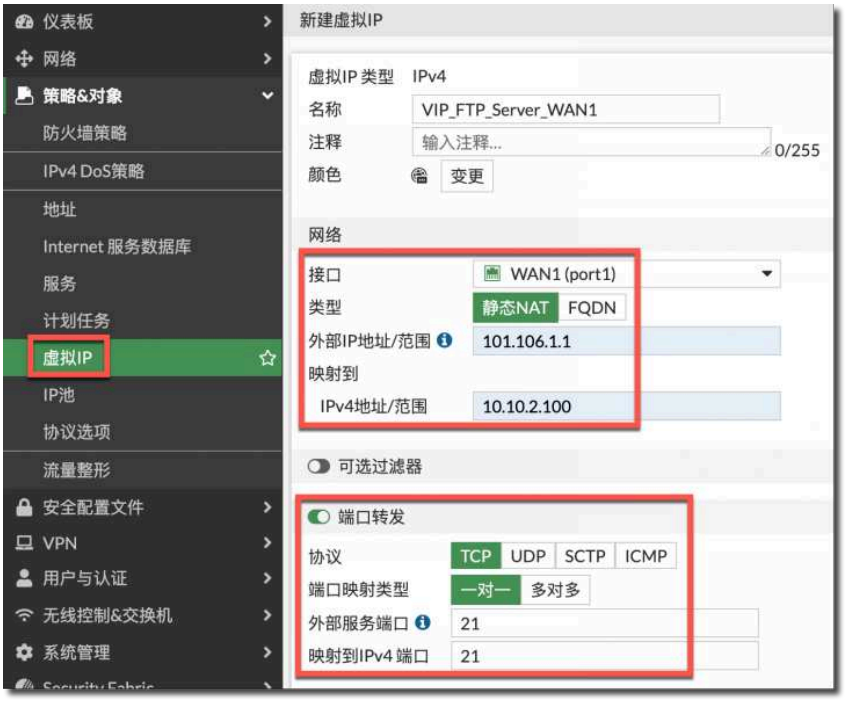
4. 内网PC和FTP Server位于不同的FortiGate内网口下，属于不同网段。

5. 内网PC需要通过FortiGate在port1（WAN1）上映射的公网IP 101.106.1.1（或通过域名解析得到此公网IP）的21端口访问FTP Server。

配置步骤

1. 正常配置属于外网接口port1（WAN1）的VIP条目，注意这里必须配置VIP的关联接口（此例中为port1），否则无法实现此功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall vip
    edit "VIP_FTP_Server_WAN1"
        set extip 101.106.1.1
        set mappedip "10.10.2.100"
        set extintf "port1"
        set portforward enable
        set extport 21
        set mappedport 21
    next
end
```

2. 配置安全策略放通外网port1（WAN1）到内网port4（DMZ）且目的IP为VIP条目的策略，注意这里不用开启SNAT。

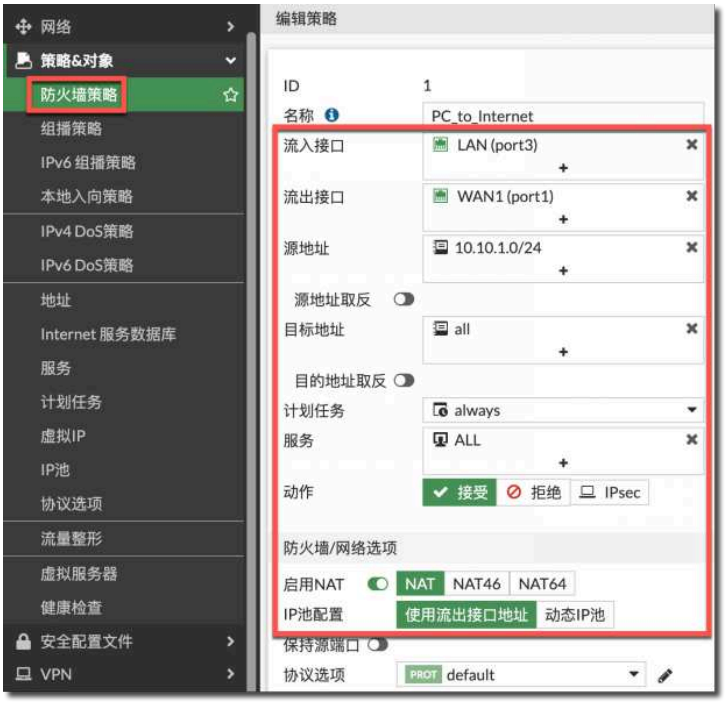
> **重要**
>
> VIP策略的“源地址”一定要包含PC所在网段，这里以“all”为例，既能包含外网访问VIP的流量，也包含PC所在网段。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall policy
    edit 2
        set name "VIP_FTP_Server_WAN1"
        set srcintf "port1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP_FTP_Server_WAN1"
        set schedule "always"
        set service "FTP"
    next
end
```

3. 正常配置放通内网port3（LAN）到外网port1（WAN1）的上网策略。

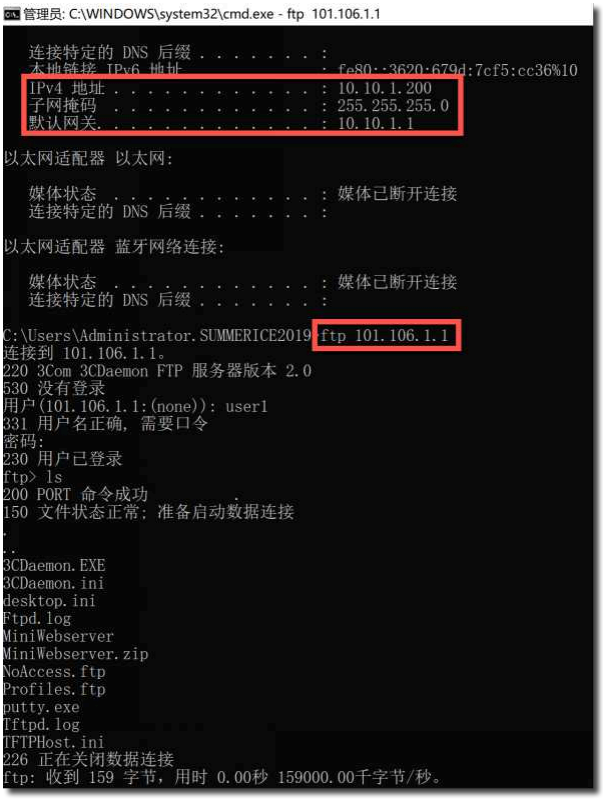



```bash
config firewall policy
    edit 1
        set name "PC_to_Internet"
        set srcintf "port3"
        set dstintf "port1"
        set action accept
        set srcaddr "10.10.1.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

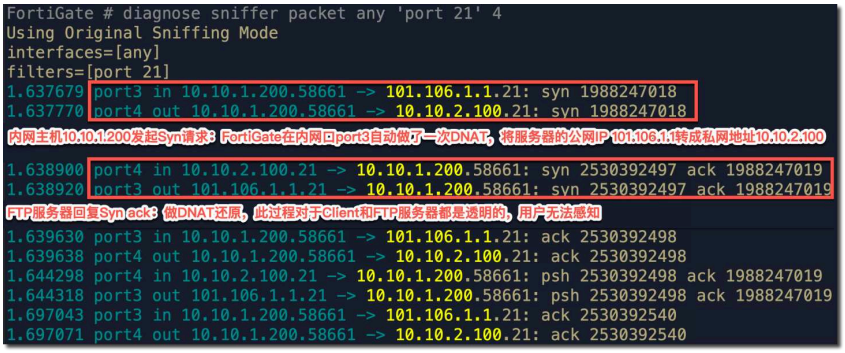
结果验证

内网PC就可以通过FTP服务器的VIP公网IP访问到DMZ区域的FTP服务器。

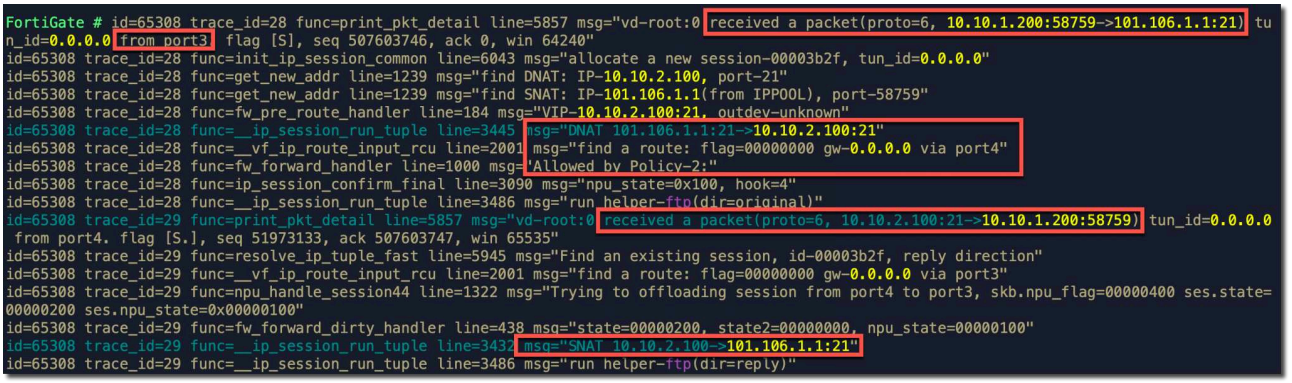
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



抓包分析



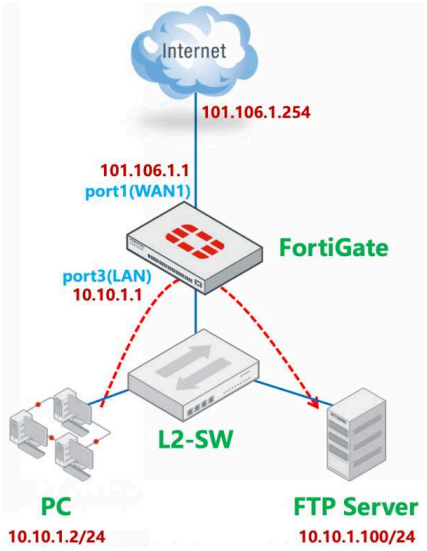
Debug Flow分析



需求场景二

- *PC与Server对于FortiGate属于相同的接口、相同的网段。*
- *PC与Server属于相同网段。*

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. FortiGate的port1（WAN1）连接ISP。默认路由1指向port1（WAN1）。

> **重要**
>
> 如果通过策略路由来控制内网PC访问Internet，请参考本文注意事项章节中的说明。

```bash
FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.106.1.254, port1, [1/0]
C       10.10.1.0/24 is directly connected, port3
C       101.106.1.0/24 is directly connected, port1
```

2. FortiGate通过配置VIP，在port1（WAN1）的公网IP 101.106.1.1上映射了FTP Server的21端口。

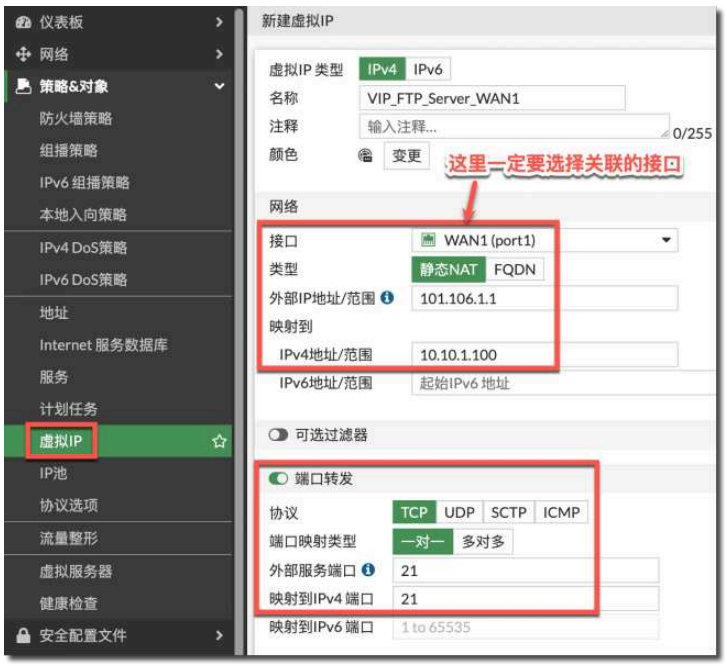
3. 内网PC通过port1（WAN1）做SNAT访问互联网。

4. 内网PC和FTP Server位于相同的二层交换机下，与FortiGate的port3（LAN）接口都属于同一网段。

5. 内网PC需要通过FortiGate在port1（WAN1）上映射的公网IP 101.106.1.1（或通过域名解析得到此公网IP）的21端口访问FTP Server。

配置步骤

1. 正常配置属于外网接口port1（WAN1）的VIP条目，注意这里必须配置VIP的关联接口（此例中为port1），否则无法实现此功能。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall vip
    edit "VIP_FTP_Server_WAN1"
        set extip 101.106.1.1
        set mappedip "10.10.1.100"
        set extintf "port1"
        set portforward enable
        set extport 21
        set mappedport 21
    next
end
```

2. 配置安全策略放通外网port1（WAN1）到内网port3（LAN）且目的IP为VIP条目的策略，注意这里不用开启SNAT。

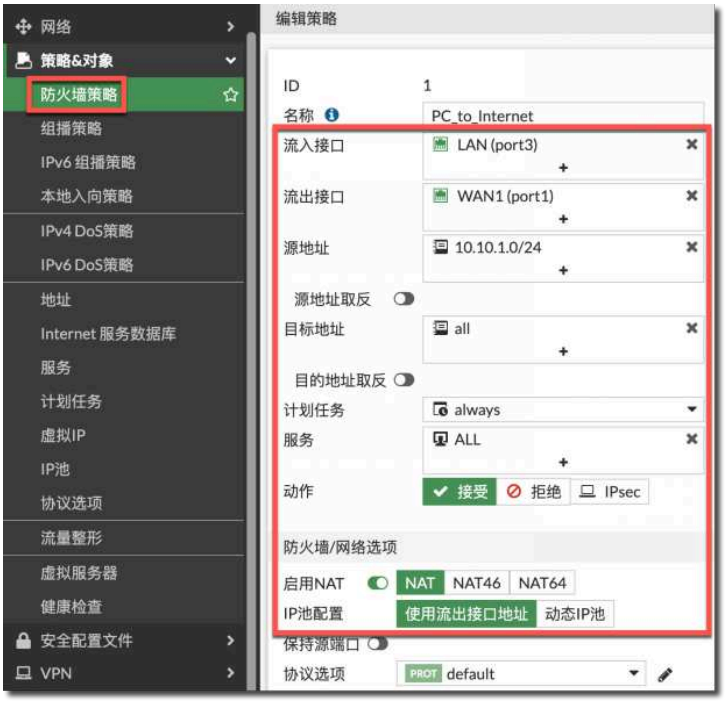
> **重要**
>
> VIP策略的“源地址”一定要包含PC所在网段，这里以“all”为例，既能包含外网访问VIP的流量，也包含PC所在网段。




```bash
config firewall policy
    edit 2
        set name "VIP_FTP_Server_WAN1"
        set srcintf "port1"
        set dstintf "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP_FTP_Server_WAN1"
        set schedule "always"
        set service "FTP"
    next
end
```

3. 正常配置放通内网port3（LAN）到外网port1（WAN1）的上网策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 1
        set name "PC_to_Internet"
        set srcintf "port3"
        set dstintf "port1"
        set action accept
        set srcaddr "10.10.1.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

结果验证

内网PC就可以通过FTP服务器的VIP公网IP访问到LAN区域的FTP服务器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
以太网适配器 Ethernet0:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::3620:679d:7cf5:cc36%10
   IPv4 地址 . . . . . . . . . . . . : 10.10.1.2
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.10.1.1

以太网适配器 以太网:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :

以太网适配器 蓝牙网络连接:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :

C:\Users\Administrator.SUMMERICE2019>ftp 101.106.1.1
连接到 101.106.1.1。
220 3Com 3CDaemon FTP 服务器版本 2.0
530 没有登录
用户(101.106.1.1:(none)): user1
331 用户名正确，需要口令
密码:
230 用户已登录
ftp> ls
200 PORT 命令成功
150 文件状态正常；准备启动数据连接
.
..
3CDaemon.EXE
3CDaemon.ini
desktop.ini
Ftpd.log
MiniWebserver
MiniWebserver.zip
NoAccess.ftp
Profiles.ftp
putty.exe
Tftpd.log
TFTPHost.ini
226 正在关闭数据连接
ftp: 收到 159 字节，用时 0.03秒 5.13千字节/秒。
```

抓包分析

```
FortiGate # diagnose sniffer packet any 'port 21' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 21]
2.240199 port3 in 10.10.1.2.58933 -> 101.106.1.1.21: syn 4029466216
2.240316 port3 out 10.10.1.1.58933 -> 10.10.1.100.21: syn 4029466216
内网主机10.10.1.2发起Syn请求；FortiGate在内网口port3自动做了一次DNAT，将公网IP 101.106.1.1转换成私网IP 10.10.1.100
同时做了一次SNAT，将源IP 10.10.1.2转换为内网口port3的IP 10.10.1.1
2.241016 port3 in 10.10.1.100.21 -> 10.10.1.1.58933: syn 3261134504 ack 4029466217
2.241037 port3 out 101.106.1.1.21 -> 10.10.1.2.58933: syn 3261134504 ack 4029466217
FTP服务器回复Syn ack；DNAT还原+SNAT还原，此过程对于Client和FTP服务器都是透明的，用户无法感知
2.241390 port3 in 10.10.1.2.58933 -> 101.106.1.1.21: ack 3261134505
2.241400 port3 out 10.10.1.1.58933 -> 10.10.1.100.21: ack 3261134505
2.245253 port3 in 10.10.1.100.21 -> 10.10.1.1.58933: psh 3261134505 ack 4029466217
2.245272 port3 out 101.106.1.1.21 -> 10.10.1.2.58933: psh 3261134505 ack 4029466217
2.296049 port3 in 10.10.1.2.58933 -> 101.106.1.1.21: ack 3261134547
2.296111 port3 out 10.10.1.1.58933 -> 10.10.1.100.21: ack 3261134547
2.304163 port3 in 10.10.1.2.58933 -> 101.106.1.1.21: psh 4029466217 ack 3261134547
2.304198 port3 out 10.10.1.1.58933 -> 10.10.1.100.21: psh 4029466217 ack 3261134547
2.307333 port3 in 10.10.1.100.21 -> 10.10.1.1.58933: psh 3261134547 ack 4029466231
2.307357 port3 out 101.106.1.1.21 -> 10.10.1.2.58933: psh 3261134547 ack 4029466231
2.357734 port3 in 10.10.1.2.58933 -> 101.106.1.1.21: ack 3261134566
2.357766 port3 out 10.10.1.1.58933 -> 10.10.1.100.21: ack 3261134566
```

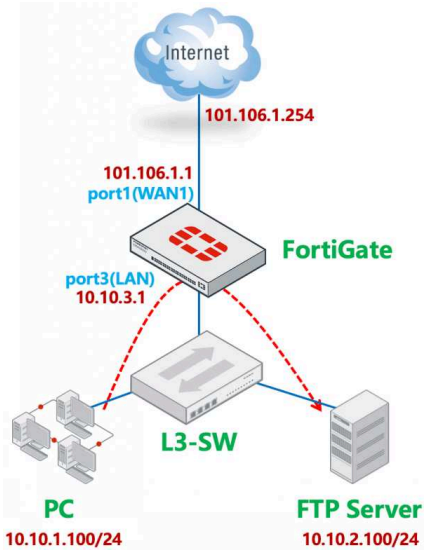
Debug Flow分析

```
FortiGate # id=65308 trace_id=86 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=6, 10.10.1.2:58945->101.106.1.1:21) tun_
id=0.0.0.0 from port3. flag [S], seq 2448638206, ack 0, win 8192"
id=65308 trace_id=86 func=init_ip_session_common line=6043 msg="allocate a new session-00004bdf, tun_id=0.0.0.0"
id=65308 trace_id=86 func=get_new_addr line=1239 msg="find DNAT: IP-10.10.1.100, port-21"
id=65308 trace_id=86 func=get_new_addr line=1239 msg="find SNAT: IP-101.106.1.1(from IPPOOL), port-58945"
id=65308 trace_id=86 func=fw_pre_route_handler line=184 msg="VIP-10.10.1.100:21, outdev-unknown"
id=65308 trace_id=86 func=__ip_session_run_tuple line=3445 msg="DNAT 101.106.1.1:21->10.10.1.100:21"
id=65308 trace_id=86 func=__vf_ip_route_input_rcu line=2001 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=86 func=fw_forward_handler line=1000 msg="Allowed by Policy-2: SNAT"
id=65308 trace_id=86 func=ip_session_confirm_final line=3000 msg="npu_state=0x100, hook=4"
id=65308 trace_id=86 func=__ip_session_run_tuple line=3432 msg="SNAT 10.10.1.2->10.10.1.1:58945"
id=65308 trace_id=86 func=__ip_session_run_tuple line=3486 msg="run helper-ftp(dir=original)"
id=65308 trace_id=87 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=6, 10.10.1.100:21->10.10.1.1:58945) tun_id=0.0.0.0 f
rom port3. flag [S.], seq 2750902401, ack 2448638207, win 65535"
id=65308 trace_id=87 func=resolve_ip_tuple_fast line=5945 msg="Find an existing session, id-00004bdf, reply direction"
id=65308 trace_id=87 func=__ip_session_run_tuple line=3445 msg="DNAT 10.10.1.1:58945->10.10.1.2:58945"
id=65308 trace_id=87 func=__vf_ip_route_input_rcu line=2001 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=87 func=npu_handle_session44 line=1322 msg="Trying to offloading session from port3 to port3, skb.npu_flag=00000400 ses.state=
00000200 ses.npu_state=0x00000101"
id=65308 trace_id=87 func=fw_forward_dirty_handler line=438 msg="state=00000200, state2=00000000, npu_state=00000101"
id=65308 trace_id=87 func=__ip_session_run_tuple line=3432 msg="SNAT 10.10.1.100->101.106.1.1:21"
id=65308 trace_id=87 func=__ip_session_run_tuple line=3486 msg="run helper-ftp(dir=reply)"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

需求场景三

- *PC与Server对于FortiGate属于相同的接口、不同的网段。*
- *PC与Server属于不同网段。*



1. FortiGate的port1（WAN1）连接ISP。默认路由1指向port1（WAN1）。

> **重要**
>
> 如果通过策略路由来控制内网PC访问Internet，请参考本文注意事项章节中的说明。

```bash
FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.106.1.254, port1, [1/0]
C       10.10.3.0/24 is directly connected, port3
C       101.106.1.0/24 is directly connected, port1
```

2. FortiGate通过配置VIP，在port1（WAN1）的公网IP 101.106.1.1上映射了FTP Server的21端口。

3. 内网PC通过port1（WAN1）做SNAT访问互联网。

4. 内网PC和FTP Server属于不同网段，网关位于同一个三层交换机下。

5. 内网PC、FTP Server与FortiGate的port3（LAN）接口属于不同网段。

6. 内网PC需要通过FortiGate在port1（WAN1）上映射的公网IP 101.106.1.1（或通过域名解析得到此公网IP）的21端口访问FTP Server。

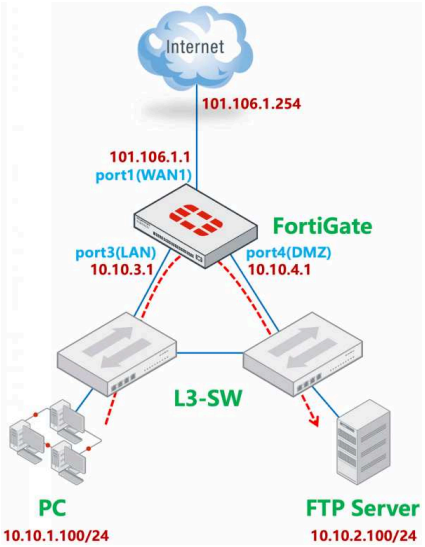
配置步骤

参考需求场景二的配置即可。

需求场景四

- *PC与Server对于FortiGate属于不同的接口、不同的网段。*
- *PC与Server属于不同网段。*

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. FortiGate的port1（WAN1）连接ISP。默认路由1指向port1（WAN1）。

> **重要**
>
> 如果通过策略路由来控制内网PC访问Internet，请参考本文注意事项章节中的说明。

```bash
FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.106.1.254, port1, [1/0]
S       10.10.1.0/24 [10/0] via 10.10.3.2, port3, [1/0]
S       10.10.2.0/24 [10/0] via 10.10.4.2, port4, [1/0]
C       10.10.3.0/24 is directly connected, port3
C       10.10.4.0/24 is directly connected, port4
C       101.106.1.0/24 is directly connected, port1
```

2. FortiGate通过配置VIP，在port1（WAN1）的公网IP 101.106.1.1上映射了FTP Server的21端口。

3. 内网PC通过port1（WAN1）做SNAT访问互联网。

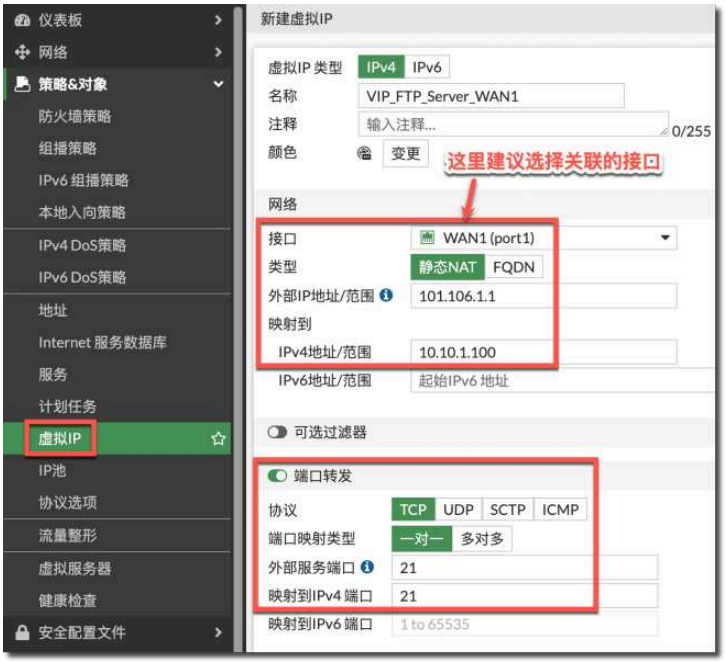
4. 内网PC和FTP Server位于不同的3层交换机下，属于不同网段，网关为各自相连的L3-SW，且PC可以和FTP Server通过两台L3-SW直接通信。两台L3-SW与FortiGate的2个接口分别三层互联，两台L3-SW的网关都指向FortiGate。

5. 内网PC需要通过FortiGate在port1（WAN1）上映射的公网IP 101.106.1.1（或通过域名解析得到此公网IP）的21端口访问FTP Server。

配置步骤

1. 正常配置属于外网接口port1（WAN1）的VIP条目，强烈建议配置VIP的关联接口（此例中为port1，不要配置为any），否则可能产生其他问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall vip
    edit "VIP_FTP_Server_WAN1"
        set extip 101.106.1.1
        set mappedip "10.10.2.100"
        set extintf "port1"
        set portforward enable
        set extport 21
        set mappedport 21
    next
end
```

2. 配置安全策略：公网port1（WAN1）到port4（DMZ），源地址为内网PC网段10.10.1.0/24，且目的IP为VIP条目的策略，注意这条策略开启SNAT，用于内网PC对VIP的访问。



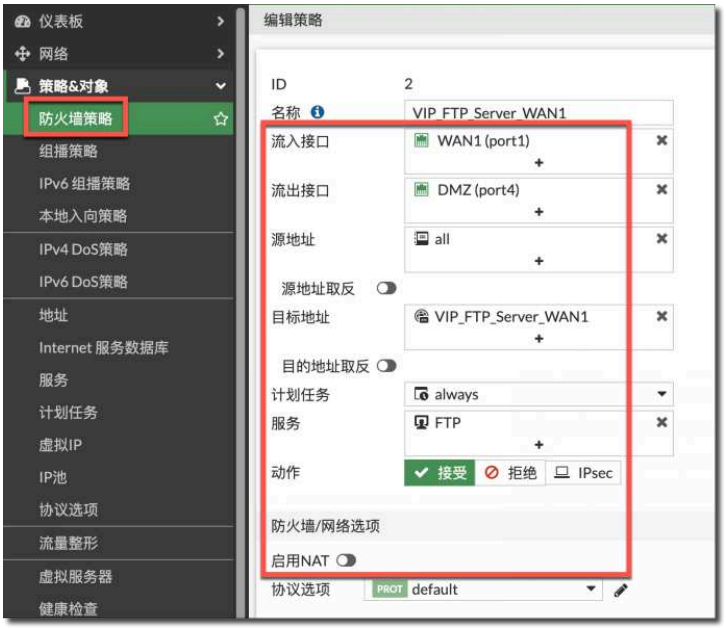

```bash
config firewall policy
    edit 3
        set name "LAN_to_VIP_FTP_Server"
        set srcintf "port1"
        set dstintf "port4"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set action accept
        set srcaddr "10.10.1.0/24"
        set dstaddr "VIP_FTP_Server_WAN1"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

3. 配置安全策略放通外网port1（WAN1）到内网port4（DMZ）且目的IP为VIP条目的策略，注意这里不用开启SNAT，用于外网客户端对VIP的访问。

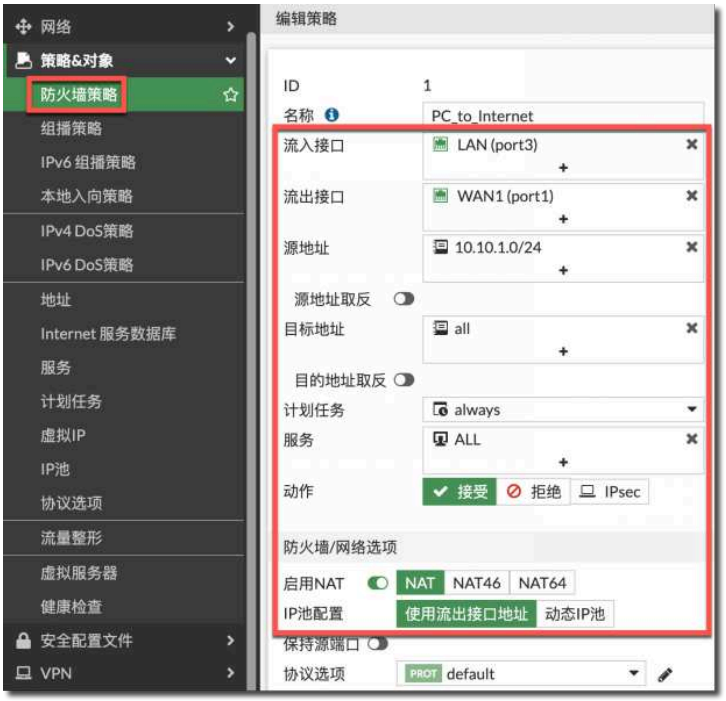
> **重要**
>
> VIP策略的“源地址”一定要包含PC所在网段，这里以“all”为例，既能包含外网访问VIP的流量，也包含PC所在网段。




```bash
config firewall policy
    edit 2
        set name "VIP_FTP_Server_WAN1"
        set srcintf "port1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP_FTP_Server_WAN1"
        set schedule "always"
        set service "FTP"
    next
end
```

4. 正常配置放通内网port3（LAN）到外网port1（WAN1）的上网策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 1
        set name "PC_to_Internet"
        set srcintf "port3"
        set dstintf "port1"
        set action accept
        set srcaddr "10.10.1.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

5. 注意策略顺序如下。



结果验证

内网PC就可以通过FTP服务器的VIP公网IP访问到DMZ区域的FTP服务器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
管理员: C:\WINDOWS\system32\cmd.exe - ftp 101.106.1.1

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::3620:679d:7cf5:cc36%10
   IPv4 地址 . . . . . . . . . . . . : 10.10.1.100
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.10.1.1

以太网适配器 以太网:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :

以太网适配器 蓝牙网络连接:

   媒体状态 . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :

C:\Users\Administrator.SUMMERICE2019>ftp 101.106.1.1
连接到 101.106.1.1。
220 3Com 3CDaemon FTP 服务器版本 2.0
530 没有登录
用户(101.106.1.1:(none)): user1
331 用户名正确，需要口令
密码:
230 用户已登录
ftp> ls
200 PORT 命令成功
150 文件状态正常；准备启动数据连接
.
..
3CDaemon.EXE
3CDaemon.ini
desktop.ini
Ftpd.log
MiniWebserver
MiniWebserver.zip
NoAccess.ftp
Profiles.ftp
putty.exe
Tftpd.log
TFTPHost.ini
226 正在关闭数据连接
ftp: 收到 159 字节，用时 0.05秒 3.46千字节/秒。
```

抓包分析

```
FortiGate # diagnose sniffer packet any 'port 21' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[port 21]
1.311118 port3 in 10.10.1.100.63731 -> 101.106.1.1.21: syn 742153841
1.311238 port4 out 10.10.4.1.63731 -> 10.10.2.100.21: syn 742153841
内网主机10.10.1.100发起Syn请求：FortiGate在内网口port3自动做了一次DNAT，将公网IP 101.106.1.1转换为10.10.2.100
同时做了一次SNAT，将源IP 10.10.1.100转换为DMZ接口port4的IP 10.10.4.1
1.311953 port4 in 10.10.2.100.21 -> 10.10.4.1.63731: syn 2547098373 ack 742153842
1.311967 port3 out 101.106.1.1.21 -> 10.10.1.100.63731: syn 2547098373 ack 742153842
FTP服务器回复Syn ack：DNAT还原+SNAT还原，此过程对于Client和FTP服务器是透明的，用户无法感知
1.312845 port3 in 10.10.1.100.63731 -> 101.106.1.1.21: ack 2547098374
1.312854 port4 out 10.10.4.1.63731 -> 10.10.2.100.21: ack 2547098374
1.317986 port4 in 10.10.2.100.21 -> 10.10.4.1.63731: psh 2547098374 ack 742153842
1.317994 port3 out 101.106.1.1.21 -> 10.10.1.100.63731: psh 2547098374 ack 742153842
1.358954 port3 in 10.10.1.100.63731 -> 101.106.1.1.21: psh 742153842 ack 2547098416
1.359010 port4 out 10.10.4.1.63731 -> 10.10.2.100.21: psh 742153842 ack 2547098416
1.363297 port4 in 10.10.2.100.21 -> 10.10.4.1.63731: psh 2547098416 ack 742153856
1.363321 port3 out 101.106.1.1.21 -> 10.10.1.100.63731: psh 2547098416 ack 742153856
1.427952 port3 in 10.10.1.100.63731 -> 101.106.1.1.21: ack 2547098435
1.428009 port4 out 10.10.4.1.63731 -> 10.10.2.100.21: ack 2547098435
```

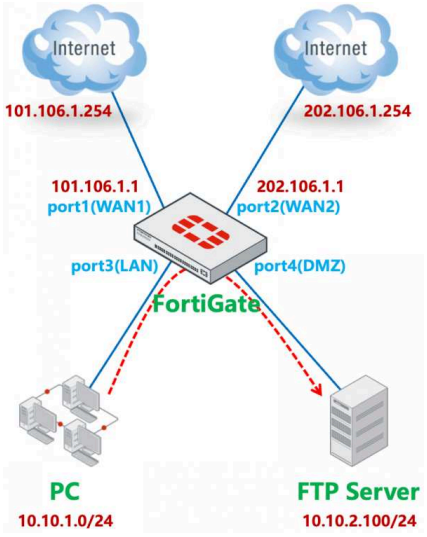
Debug Flow分析

```
FortiGate # id=65308 trace_id=1 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=6, 10.10.1.100:63737->101.106.1.1:21) tun
_id=0.0.0.0 from port3. flag [S], seq 1515674373, ack 0, win 8192"
id=65308 trace_id=1 func=init_ip_session_common line=6043 msg="allocate a new session-00000811, tun_id=0.0.0.0"
id=65308 trace_id=1 func=get_new_addr line=1239 msg="find DNAT: IP-10.10.2.100, port-21"
id=65308 trace_id=1 func=get_new_addr line=1239 msg="find SNAT: IP-101.106.1.1(from IPPOOL), port-63737"
id=65308 trace_id=1 func=fw_pre_route_handler line=184 msg="VIP-10.10.2.100:21, outdev-unknown"
id=65308 trace_id=1 func=__ip_session_run_tuple line=3445 msg="DNAT 101.106.1.1:21->10.10.2.100:21"
id=65308 trace_id=1 func=__vf_ip_route_input_rcu line=2001 msg="find a route: flag=00000000 gw-10.10.4.2 via port4"
id=65308 trace_id=1 func=get_new_addr line=1239 msg="find SNAT: IP-10.10.4.1(from IPPOOL), port-63737"
id=65308 trace_id=1 func=fw_forward_handler line=1000 msg="Allowed by Policy-3: SNAT"
id=65308 trace_id=1 func=ip_session_confirm_final line=3090 msg="npu_state=0x100, hook=4"
id=65308 trace_id=1 func=__ip_session_run_tuple line=3432 msg="SNAT 10.10.1.100->10.10.4.1:63737"
id=65308 trace_id=1 func=__ip_session_run_tuple line=3486 msg="run helper-ftp(dir=original)"
id=65308 trace_id=2 func=print_pkt_detail line=5857 msg="vd-root:0 received a packet(proto=6, 10.10.2.100:21->10.10.4.1:63737) tun_id=0.0.0.0 fr
om port4. flag [S.], seq 3648687917, ack 1515674374, win 65535"
id=65308 trace_id=2 func=resolve_ip_tuple_fast line=5945 msg="Find an existing session, id-00000811, reply direction"
id=65308 trace_id=2 func=__ip_session_run_tuple line=3445 msg="DNAT 10.10.4.1:63737->10.10.1.100:63737"
id=65308 trace_id=2 func=__vf_ip_route_input_rcu line=2001 msg="find a route: flag=00000000 gw-10.10.3.2 via port3"
id=65308 trace_id=2 func=npu_handle_session44 line=1322 msg="Trying to offloading session from port4 to port3, skb.npu_flag=00000400 ses.state=0
0000200 ses.npu_state=0x00000101"
id=65308 trace_id=2 func=fw_forward_dirty_handler line=438 msg="state=00000200, state2=00000000, npu_state=00000101"
id=65308 trace_id=2 func=__ip_session_run_tuple line=3432 msg="SNAT 10.10.2.100->101.106.1.1:21"
id=65308 trace_id=2 func=__ip_session_run_tuple line=3486 msg="run helper-ftp(dir=reply)"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

需求场景五

- *PC与Server对于FortiGate属于不同的接口、相同的网段。*
- *PC与Server属于不同网段。*



1. FortiGate的port1（WAN1）和port2（WAN2）分别连接两个ISP。默认路由1指向port1（WAN1），路由优先级为10，默认路由2指向port2（WAN2），路由优先级为20。

> **重要**
>
> 如果通过策略路由来控制内网PC访问Internet，请参考本文注意事项章节中的说明。

```bash
FortiGate # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 101.106.1.254, port1, [10/0]
                  [10/0] via 202.106.1.254, port2, [20/0]
C       10.10.1.0/24 is directly connected, port3
C       10.10.2.0/24 is directly connected, port4
C       101.106.1.0/24 is directly connected, port1
C       202.106.1.0/24 is directly connected, port2
```

2. FortiGate通过配置VIP，在port2（WAN2）的公网IP 202.106.1.1上映射了FTP Server的21端口。

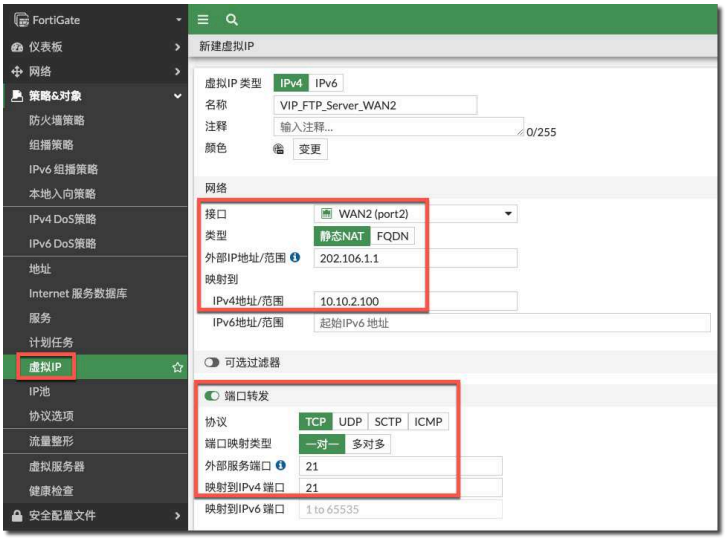
3. 内网PC通过port1（WAN1）做SNAT访问互联网（备用通过port2上网）。

4. 内网PC需要通过FortiGate在port2（WAN2）上映射的公网IP 202.106.1.1（或通过域名解析得到此公网IP）的21端口访问FTP Server。

配置步骤

1. 正常配置属于外网接口port2（WAN2）的VIP条目，强烈建议配置VIP的关联接口（此例中为port2，不要配置为any），否则可能引起其他问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall vip
    edit "VIP_FTP_Server_WAN2"
        set extip 202.106.1.1
        set mappedip "10.10.2.100"
        set extintf "port2"
        set portforward enable
        set extport 21
        set mappedport 21
    next
end
```

2. 配置安全策略放通外网port2（WAN2）到内网port4（DMZ）且目的IP为VIP条目的策略，注意这里不用开启SNAT。

> **重要**
>
> VIP策略的“源地址”一定要包含PC所在网段，这里以“all”为例，既能包含外网访问VIP的流量，也包含PC所在网段。

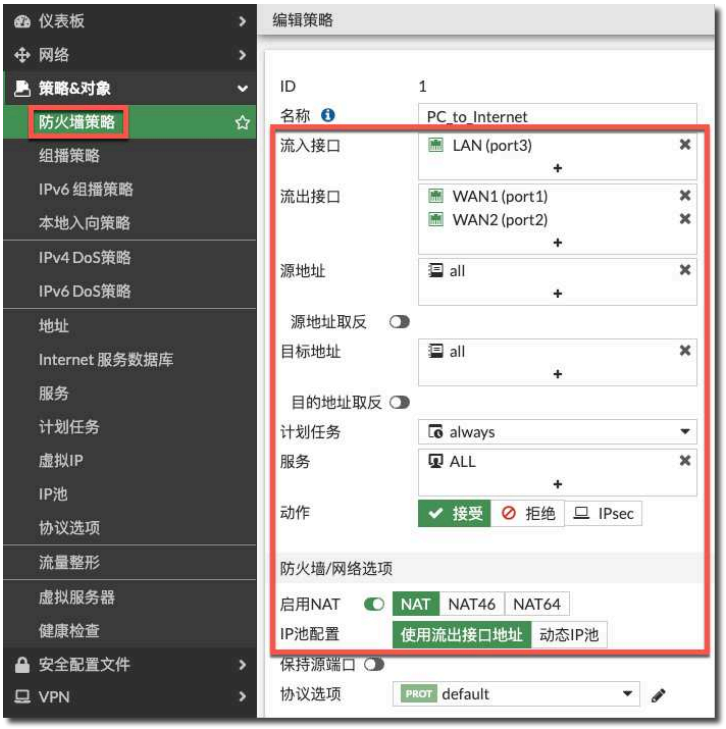



```bash
config firewall policy
    edit 2
        set name "VIP_FTP_Server_WAN1"
        set srcintf "port2"
        set dstintf "port4"
        set action accept
        set srcaddr "all"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstaddr "VIP_FTP_Server_WAN2"
        set schedule "always"
        set service "FTP"
    next
end
```

3. 正常配置放通内网port3（LAN）到外网port1（WAN1）、port2（WAN2）的上网策略。

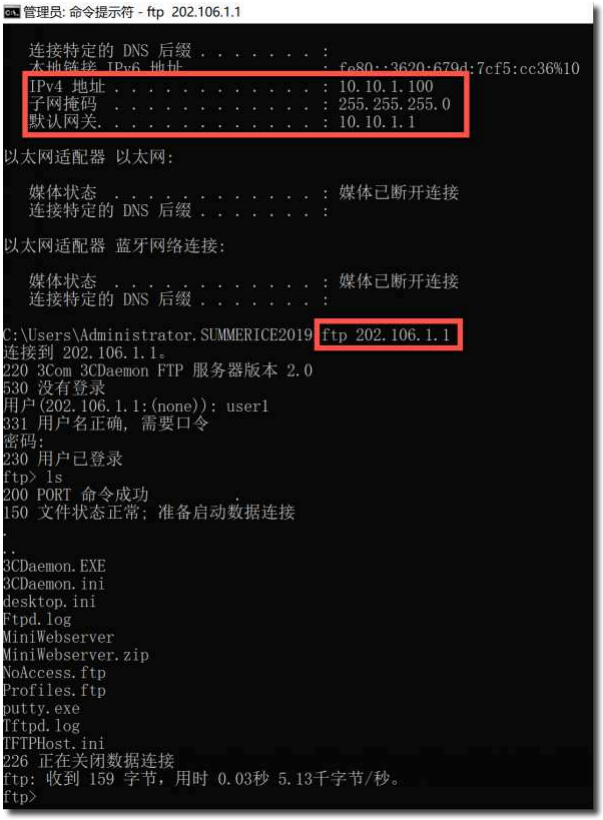



```bash
config firewall policy
    edit 1
        set name "PC_to_Internet"
        set srcintf "port3"
        set dstintf "port1" "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

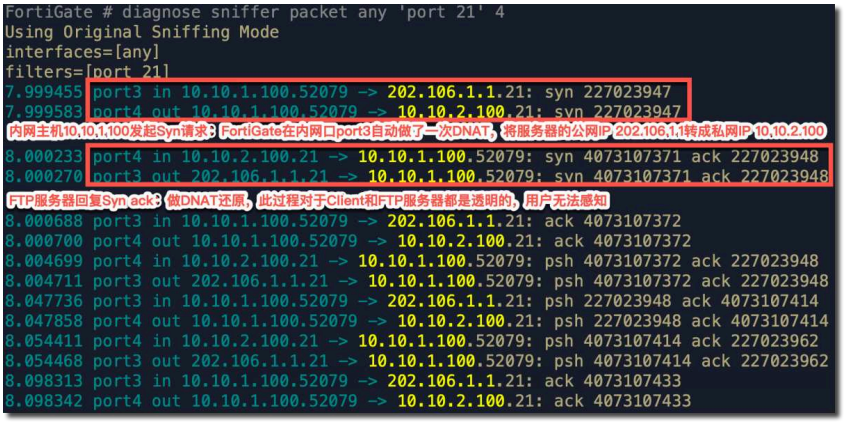
结果验证

内网PC就可以通过FTP服务器的VIP公网IP访问到DMZ区域的FTP服务器。

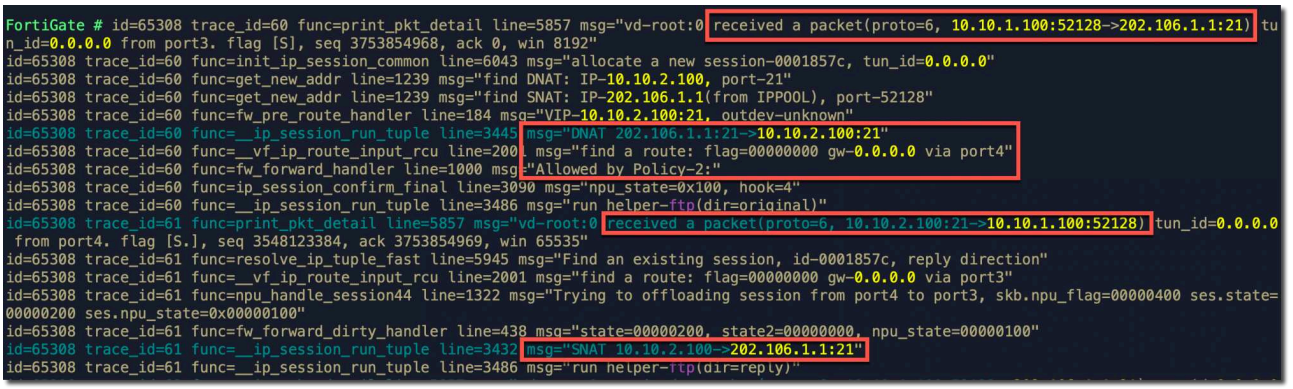
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



抓包分析



Debug Flow分析



总结

内网PC通过VIP的公网地址访问内部服务器时，对于FortiGate来说：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 如果发起访问的内网PC和VIP映射的真实服务器在FortiGate的同一个内网口下（与网段无关），FortiGate会自动做DNAT+SNAT。
- 如果发起访问的内网PC和VIP映射的真实服务器不在FortiGate的同一个内网口下（与网段无关），FortiGate会自动做DNAT，但不会做SNAT。如果内网服务器和PC的内网IP可以不通过FortiGate直接访问，则需要像场景三的步骤2那样额外配置一条源为内网PC网段，目标为VIP的开启SNAT的策略，否则服务器返回的Syn ack会从下游交换机直接返回，而不会经过FortiGate。

注意事项

如果通过策略路由来控制内网PC访问Internet，则需要额外的策略路由配置。

问题现象

1. 在需求场景2的配置基础上，FortiGate通过配置策略路由来控制PC网段访问Internet。

```bash
config router policy
    edit 1
        set input-device "port3"
        set src "10.10.1.0/255.255.255.0"
        set gateway 101.106.1.254
        set output-device "port1"
    next
end

FortiGate # diagnose firewall proute list
list route policy info(vf=root):
id=1(0x01) dscp_tag=0xfc 0xfc flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-0 iif=5(port3) dport=0-65535
path(1) oif=3(port1) gwy=101.106.1.254
source wildcard(1): 10.10.1.0/255.255.255.0
destination wildcard(1): 0.0.0.0/0.0.0.0
hit_count=2649 last_used=2024-05-07 09:35:17
```

2. 此时使用内网PC就无法通过FTP服务器的VIP公网IP访问到LAN区域的FTP服务器。抓包查看内网PC访问FTP服务器的VIP公网IP的流量只有in，没有out。

```bash
FortiGate # diagnose sniffer packet any 'port 21' 4 0 l

2024-05-06 14:57:40.855316 port3 in 10.10.1.100.51646 → 101.106.1.1.21: syn 1097509905
2024-05-06 14:57:41.872411 port3 in 10.10.1.100.51646 → 101.106.1.1.21: syn 1097509905
2024-05-06 14:57:43.872568 port3 in 10.10.1.100.51646 → 101.106.1.1.21: syn 1097509905
```

3. 相关Debug Flow显示TCP SYN报文经过DNAT转换后，匹配上网的策略路由，出接口为port1（WAN1），下一跳为运营商网关。但没有可以匹配的防火墙策略，被隐式策略（0）丢弃。

```
FortiGate # id=65308 trace_id=1 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=6, 10.10.1.2:63185->101.106.1.1:21) tun_id
=0.0.0.0 from port3. flag [S], seq 2162673907, ack 0, win 8192"
id=65308 trace_id=1 func=init_ip_session_common line=6080 msg="allocate a new session-00000b70, tun_id=0.0.0.0"
id=65308 trace_id=1 func=get_new_addr line=1213 msg="find DNAT: IP-10.10.1.100, port-21"
id=65308 trace_id=1 func=__iprope_tree_check line=535 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=1 func=get_new_addr line=1213 msg="find SNAT: IP-101.106.1.1(from IPPOOL), port-63185"
id=65308 trace_id=1 func=fw_pre_route_handler line=184 msg="VIP-10.10.1.100:21, outdev-unknown"
id=65308 trace_id=1 func=__ip_session_run_tuple line=3471 msg="DNAT 101.106.1.1:21->10.10.1.100:21"
id=65308 trace_id=1 func=rpdb_srv_match_input line=1040 msg="Match policy routing id=1: to 101.106.1.254 via ifindex-3"
id=65308 trace_id=1 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-101.106.1.254 via port1"
id=65308 trace_id=1 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=27, len=1"
id=65308 trace_id=1 func=fw_forward_handler line=837 msg="Denied by forward policy check (policy 0)"
```

解决方法1

1. 在上网的策略路由之前添加一条新的策略路由（如下配置中的ID 2）。流入接口为port3（LAN），源地址为内网PC网段（10.10.1.0/24），目的地址为FTP Server的内网IP，动作为停止策略路由（deny）。

```bash
config router policy
    edit 2
        set input-device "port3"
        set src "10.10.1.0/255.255.255.0"
        set dst "10.10.1.100/255.255.255.255"
        set action deny
    next
end
    edit 1
        set input-device "port3"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set src "10.10.1.0/255.255.255.0"
        set gateway 101.106.1.254
        set output-device "port1"
    next
end
```

2. 此时使用内网PC可以正常通过FTP服务器的VIP公网IP访问到LAN区域的FTP服务器，Debug Flow信息显示不会匹配策略路由，流程与场景二中的Debug Flow一致：

```
FortiGate # id=65308 trace_id=43 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=6, 10.10.1.2:63205->101.106.1.1:21) tun_"
id=65308 trace_id=43 func=init_ip_session_common line=6080 msg="allocate a new session-00000dcd, tun_id=0.0.0.0"
id=65308 trace_id=43 func=get_new_addr line=1213 msg="find DNAT: IP-10.10.1.100, port-21"
id=65308 trace_id=43 func=__iprope_tree_check line=535 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=43 func=get_new_addr line=1213 msg="find SNAT: IP-101.106.1.1(from IPPOOL), port-63205"
id=65308 trace_id=43 func=fw_pre_route_handler line=184 msg="VIP-10.10.1.100:21, outdev-unknown"
id=65308 trace_id=43 func=__ip_session_run_tuple line=3471 msg="DNAT 101.106.1.1:21->10.10.1.100:21"
id=65308 trace_id=43 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=43 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=29, len=2"
id=65308 trace_id=43 func=fw_forward_handler line=989 msg="Allowed by Policy-2: SNAT"
id=65308 trace_id=43 func=ip_session_confirm_final line=3113 msg="npu_state=0x100, hook=4"
id=65308 trace_id=43 func=__ip_session_run_tuple line=3458 msg="SNAT 10.10.1.2->10.10.1.1:63205"
id=65308 trace_id=43 func=__ip_session_run_tuple line=3512 msg="run helper-ftp(dir=original)"
id=65308 trace_id=44 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=6, 10.10.1.100:21->10.10.1.1:63205) tun_id=0.0.0.0 f"
id=65308 trace_id=44 func=resolve_ip_tuple_fast line=5982 msg="Find an existing session, id-00000dcd, reply direction"
id=65308 trace_id=44 func=__ip_session_run_tuple line=3471 msg="DNAT 10.10.1.1:63205->10.10.1.2:63205"
id=65308 trace_id=44 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=44 func=npu_handle_session44 line=1327 msg="Trying to offloading session from port3 to port3, skb.npu_flag=00000400 ses.state="
id=65308 trace_id=44 func=fw_forward_dirty_handler line=439 msg="state=00000200, state2=00000000, npu_state=00000101"
id=65308 trace_id=44 func=__ip_session_run_tuple line=3458 msg="SNAT 10.10.1.100->101.106.1.1:21"
id=65308 trace_id=44 func=__ip_session_run_tuple line=3512 msg="run helper-ftp(dir=reply)"
```

3. 其他场景下使用策略路由上网时，均可以参考此配置。

解决方法2

1. 在上网的策略路由之前添加一条新的策略路由（如下配置中的ID 2）。流入接口为port3（LAN），源地址为内网PC网段（10.10.1.0/24），目的地址为FTP Server的内网IP。流出接口为内网接口port3（LAN），网关地址为去往FTP Server的下一跳IP（此例需求场景2中的下一跳IP就是FTP Server的内网IP）。

> **重要**
>
> 在此例（需求场景2）中，策略路由ID 2的目的地址一定要填写具体的Server内网IP，防止Server返回的流量匹配到策略路由。

bash

```
config router policy
    edit 2
        set input-device "port3"
        set src "10.10.1.0/255.255.255.0"
        set dst "10.10.1.100/255.255.255.255"
        set gateway 10.10.1.100
        set output-device "port3"
    next
    edit 1
        set input-device "port3"
        set src "10.10.1.0/255.255.255.0"
        set gateway 101.106.1.254
        set output-device "port1"
    next
end
```

2. 此时使用内网PC可以正常通过FTP服务器的VIP公网IP访问到LAN区域的FTP服务器，Debug Flow信息显示如下：

```
FortiGate # id=65308 trace_id=32 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=6, 10.10.1.2:63197->101.106.1.1:21) tun_"
id=65308 trace_id=32 func=init_ip_session_common line=6080 msg="allocate a new session-00000ce2, tun_id=0.0.0.0"
id=65308 trace_id=32 func=get_new_addr line=1213 msg="find DNAT: IP-10.10.1.100, port-21"
id=65308 trace_id=32 func=__iprope_tree_check line=535 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=32 func=get_new_addr line=1213 msg="find SNAT: IP-101.106.1.1(from IPPOOL), port-63197"
id=65308 trace_id=32 func=fw_pre_route_handler line=184 msg="VIP-10.10.1.100:21, outdev-unknown"
id=65308 trace_id=32 func=__ip_session_run_tuple line=3471 msg="DNAT 101.106.1.1:21->10.10.1.100:21"
id=65308 trace_id=32 func=rpdb_srv_match_input line=1040 msg="Match policy routing id=2: to 10.10.1.100 via ifindex-5"
id=65308 trace_id=32 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=32 func=__iprope_tree_check line=524 msg="gnum-100004, use int hash, slot=29, len=2"
id=65308 trace_id=32 func=fw_forward_handler line=989 msg="Allowed by Policy-2: SNAT"
id=65308 trace_id=32 func=ip_session_confirm_final line=3113 msg="npu_state=0x100, hook=4"
id=65308 trace_id=32 func=__ip_session_run_tuple line=3458 msg="SNAT 10.10.1.2->10.10.1.1:63197"
id=65308 trace_id=32 func=__ip_session_run_tuple line=3512 msg="run helper-ftp(dir=original)"
id=65308 trace_id=33 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=6, 10.10.1.100:21->10.10.1.1:63197) tun_id=0.0.0.0 f"
id=65308 trace_id=33 func=resolve_ip_tuple_fast line=5982 msg="Find an existing session, id-00000ce2, reply direction"
id=65308 trace_id=33 func=__ip_session_run_tuple line=3471 msg="DNAT 10.10.1.1:63197->10.10.1.2:63197"
id=65308 trace_id=33 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=33 func=npu_handle_session44 line=1327 msg="Trying to offloading session from port3 to port3, skb.npu_flag=00000400 ses.state="
id=65308 trace_id=33 func=fw_forward_dirty_handler line=439 msg="state=00000200, state2=00000000, npu_state=00000101"
id=65308 trace_id=33 func=__ip_session_run_tuple line=3458 msg="SNAT 10.10.1.100->101.106.1.1:21"
id=65308 trace_id=33 func=__ip_session_run_tuple line=3512 msg="run helper-ftp(dir=reply)"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- TCP SYN到达FortiGate后先做DNAT转换（目的地址转换为FTP Server IP），然后匹配策略路由ID 2（步骤4新增的策略路由），出接口为port3（LAN）下一跳为FTP Server，随后执行SNAT，将源地址转换为port3（LAN）接口IP。
- FTP Server返回TCP SYN ACK时，做DNAT和SNAT还原，返回客户端PC。

3. 其他场景下使用策略路由上网时，均可以参考此配置。

特殊情况

如果FortiGate开启了异步路由（asymroute），且针对内网PC和服务器配置了用于上网的策略路由。客户端访问服务器后，服务器返回的流量也会查找策略路由，有可能匹配上上网的策略路由从公网口发出，从而导致返回的流量无法到达客户端。

所以这种情况下一定要针对服务器→客户端反向的流量配置策略路由，出接口配置为内网口，并放置在上网策略路由的前边。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VIP46映射

请参考：IPv6→NAT46映射章节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VIP64映射

请参考：IPv6→NAT64→NAT64映射、IPv6→NAT64→Embedded模式的NAT64和IPv6→NAT64→NAT64+DNS64上网章节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

同一接口进出的三层转发

本文介绍了FortiGate在数据包进出为同一逻辑接口（三层转发）时的处理机制。

默认行为

在默认配置下，数据包在穿越FortiGate做三层转发时，如果FortiGate查找路由表后确定从**同一接口in**的数据包也应通过**同一接口out（不更改VLAN tag、不做NAT、不进行IPSec封装/解封装）**，数据包就会直接从同一出接口发出，**不需要相应防火墙策略放通，也不会产生会话和流量日志**。

该默认行为可以通过如下CLI命令修改（默认为enable）。修改为disable后，必须配置明确的防火墙策略放通，流量才会被转发。

> **重要**
>
> - 对于公有云FortiGate-VM的单臂（one-arm）流量，始终建议将 `allow-traffic-redirect` 状态设置为 `disable` 。
> - 对于需要做NAT、日志审计的流量，建议将 `allow-traffic-redirect` 状态设置为 `disable` 。

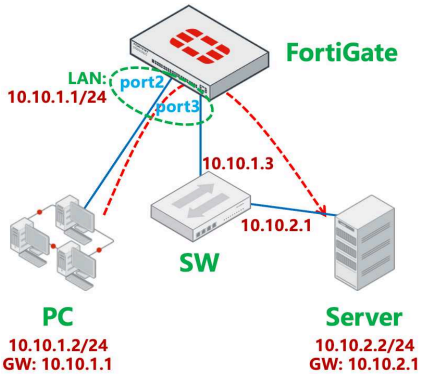
```bash
config system global
    set allow-traffic-redirect [enable | disable]
    set ipv6-allow-traffic-redirect [enable | disable]
end
```

不同流量场景的效果

对于不同类型的流量/版本组合， `allow-traffic-redirect` 的开启和关闭可能导致不同的效果。

源IP与转发接口在同一网段

网络拓扑



- FortiGate的port2和port3组成一个交换接口LAN。
- PC源IP `10.10.1.2` 与FortiGate的转发接口LAN的IP `10.10.1.1` 在同一网段。PC的网关为FortiGate的LAN接口IP，Server的网关为SW 10.10.2.1。
- PC访问Server，流量从FortiGate的LAN接口进，查路由表从LAN接口出（三层转发），下一跳为SW的地址10.10.1.3。

转发行为

- `set allow-traffic-redirect enable` （默认配置）：数据包就会按照路由（或策略路由）转发，直接从同一出接口发出，**不需要**相应防火墙策略放通，流量穿过FortiGate时，**不会创建会话，也不会产生流量日志**。
- `set allow-traffic-redirect disable` ： 必须有相应的防火墙策略放通。如果没有策略放通，流量将匹配隐式拒绝策略被丢弃。流量穿过FortiGate时，**会创建会话，可以产生流量日志，可以根据策略配置做NAT。**以上图拓扑为例，需要配置的放通策略如下所示。

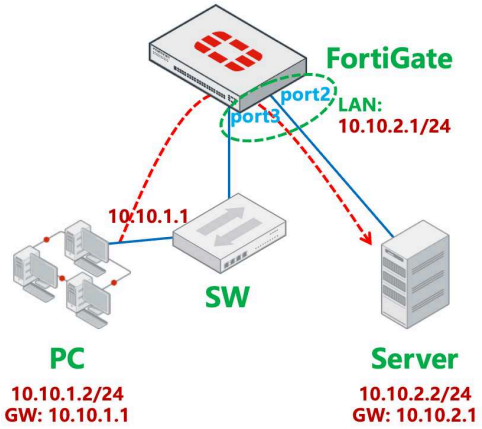
> **重要**
>
> 对于TCP流量，必须在策略中关闭 `anti-replay` ，这样TCP流量就不会作为重放流量被丢弃。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall policy
    edit 0
        set srcintf "LAN"
        set dstintf "LAN"
        set action accept
        set srcaddr "10.10.1.2/32"
        set dstaddr "10.10.2.2/32"
        set schedule "always"
        set service "ALL"
        set anti-replay disable    //针对TCP流量必须关闭//
    next
end
```

源IP与转发接口在不同网段

网络拓扑



- FortiGate的port2和port3组成一个交换接口LAN。
- PC源IP `10.10.1.2` 与FortiGate的转发接口LAN的IP `10.10.2.1` 不在同一网段。PC的网关为SW 10.10.1.1，Server的网关为FortiGate的LAN接口10.10.2.1。
- PC访问Server，流量从FortiGate的LAN接口进，查路由表从LAN接口出（三层转发），下一跳为SW的地址10.10.1.3。

转发行为

- **FortiOS版本 < 7.0.16/7.2.11/7.4.4：**无论 `allow-traffic-redirect` 启用还是禁用，流量都必须与防火墙策略进行匹配。**会创建会话，也可以产生流量日志。**
- **FortiOS版本 ≥ 7.0.16/7.2.11/7.4.4：**
  - `set allow-traffic-redirect enable` （默认配置）：数据包就会按照路由（或策略路由）转发，直接从同一出接口发出，**不需要**相应防火墙策略放通，流量穿过FortiGate时，**不会创建会话，也不会产生流量日志。**
  - `set allow-traffic-redirect disable`：必须有相应的防火墙策略放通。如果没有策略放通，流量将匹配隐式拒绝策略被丢弃。流量穿过FortiGate时，**会创建会话，可以产生流量日志，可以根据策略配置做NAT。**以上图拓扑为例，需要配置的放通策略如下所示。

> **重要**
>
> 对于TCP流量，必须在策略中关闭 `anti-replay` ，这样TCP流量就不会作为重放流量被丢弃。

```bash
config firewall policy
    edit 0
        set srcintf "LAN"
        set dstintf "LAN"
        set action accept
        set srcaddr "10.10.1.2/32"
        set dstaddr "10.10.2.2/32"
        set schedule "always"
        set service "ALL"
        set anti-replay disable    //针对TCP流量必须关闭//
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

导出策略为CSV或JSON

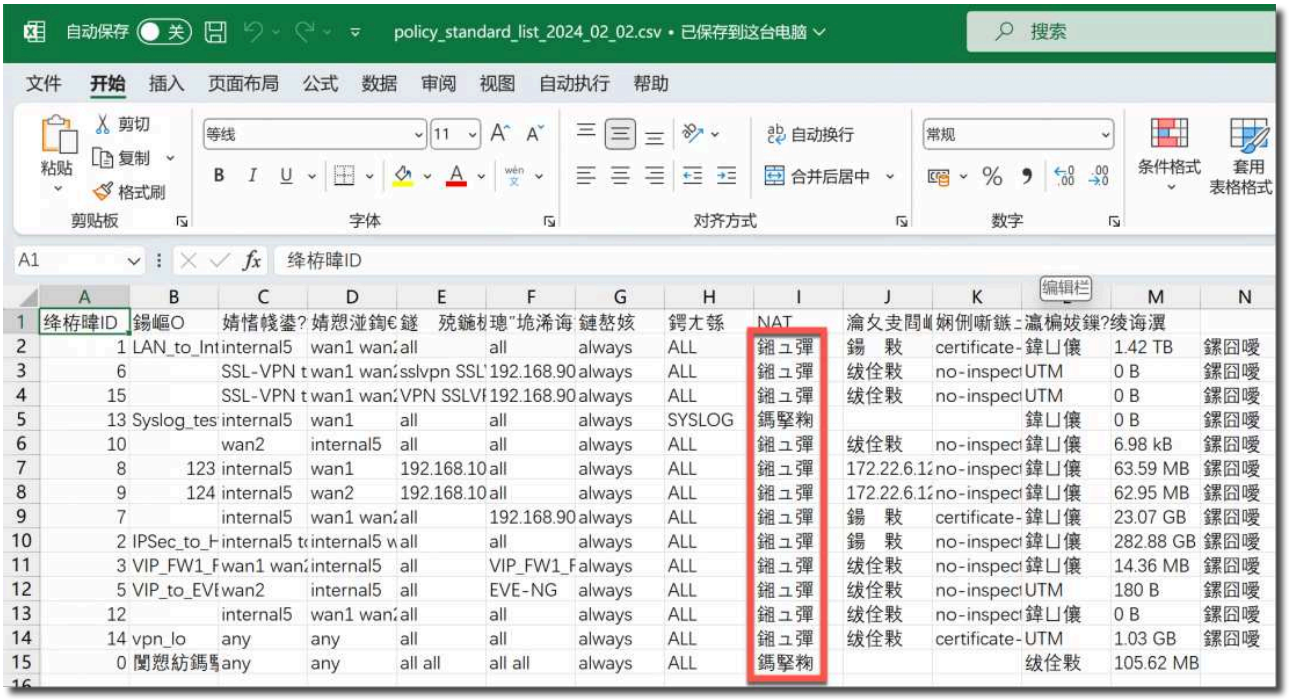
导出方法

在防火墙策略、组播策略、IPv6组播策略、IPv4 DoS策略、IPv6 DoS策略页面，点击页面右上角的导出按钮，可以导出CSV或JSON格式的策略列表。



导出CSV乱码

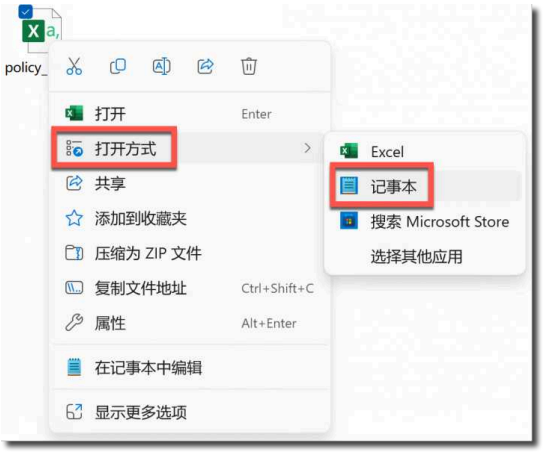
导出的策略内容中如果包含中文，导出的CSV文件中，中文字符会显示为乱码。这是由于CSV文件默认中文支持ANSI编码，且没有预留修改编码的选项。



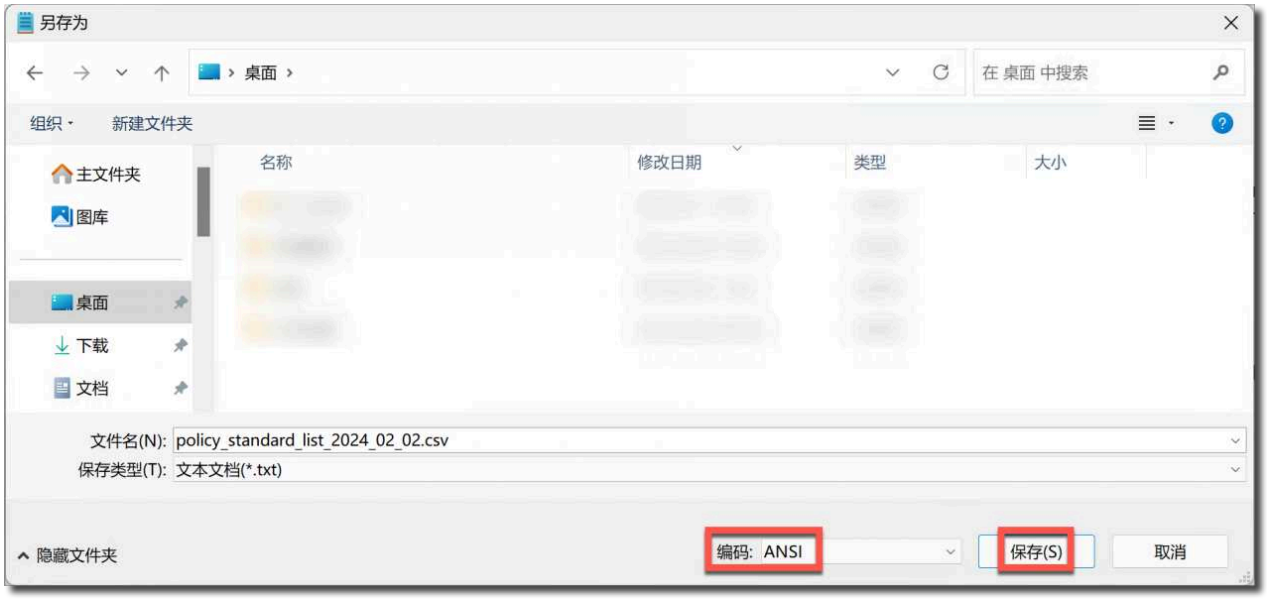
CSV乱码解决方法

1. 右键点击导出的CSV文件，使用记事本打开该文件。

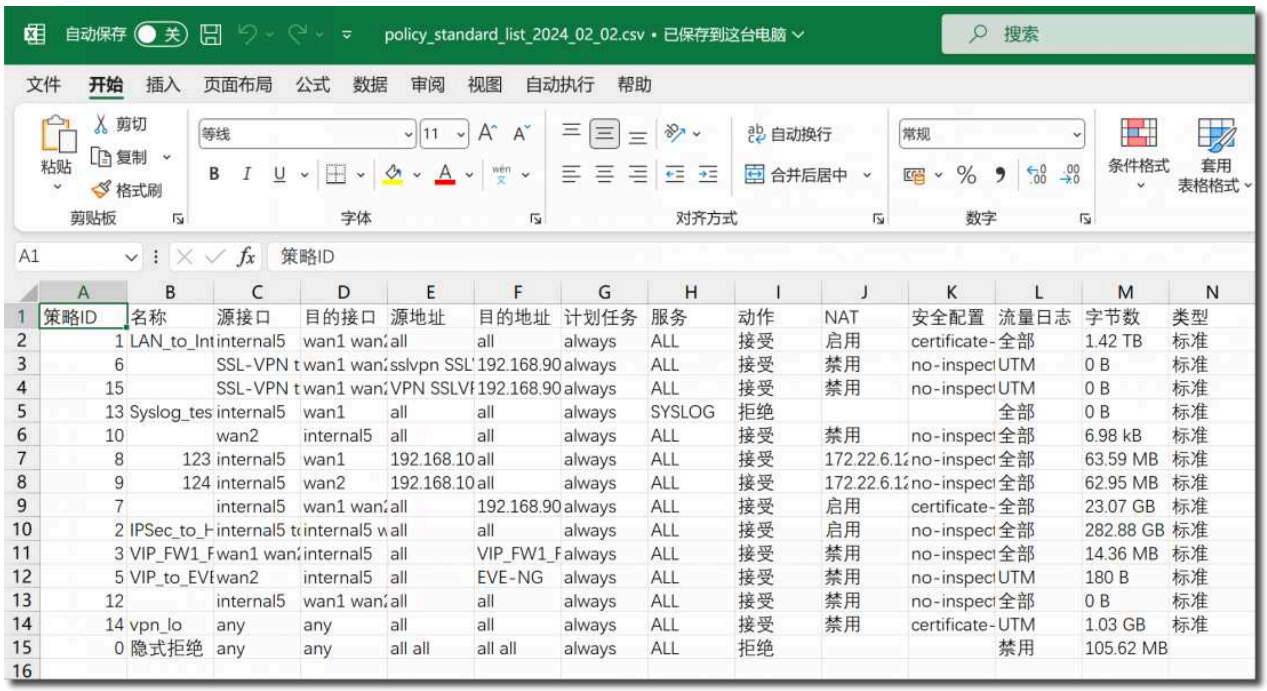
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在打开的记事本中点击文件→另存为，编码选择ANSI，并保存文件。



3. 打开保存的CSV文件，乱码已经可以正常显示为中文。



策略ID	名称	源接口	目的接口	源地址	目的地址	计划任务	服务	动作	NAT	安全配置	流量日志	字节数	类型
1	LAN_to_Int	internal5	wan1 wan2	all	all	always	ALL	接受	启用	certificate-	全部	1.42 TB	标准
6		SSL-VPN t	wan1 wan2	sslvpn SSL	192.168.90	always	ALL	接受	禁用	no-inspect	UTM	0 B	标准
15		SSL-VPN t	wan1 wan2	VPN SSLVI	192.168.90	always	ALL	接受	禁用	no-inspect	UTM	0 B	标准
13	Syslog_tes	internal5	wan1	all	all	always	SYSLOG	拒绝			全部	0 B	标准
10		wan2	internal5	all	all	always	ALL	接受	禁用	no-inspect	全部	6.98 kB	标准
8	123	internal5	wan1	192.168.10	all	always	ALL	接受	172.22.6.12	no-inspect	全部	63.59 MB	标准
9	124	internal5	wan2	192.168.10	all	always	ALL	接受	172.22.6.12	no-inspect	全部	62.95 MB	标准
7		internal5	wan1 wan2	all	192.168.90	always	ALL	接受	启用	certificate-	全部	23.07 GB	标准
2	IPSec_to_H	internal5 t	internal5 w	all	all	always	ALL	接受	启用	no-inspect	全部	282.88 GB	标准
3	VIP_FW1_F	wan1 wan2	internal5	all	VIP_FW1_F	always	ALL	接受	禁用	no-inspect	全部	14.36 MB	标准
5	VIP_to_EVE	wan2	internal5	all	EVE-NG	always	ALL	接受	禁用	no-inspect	UTM	180 B	标准
12		internal5	wan1 wan2	all	all	always	ALL	接受	禁用	no-inspect	全部	0 B	标准
14	vpn_lo	any	any	all	all	always	ALL	接受	禁用	certificate-	UTM	1.03 GB	标准
0	隐式拒绝	any	any	all all	all all	always	ALL	拒绝			禁用	105.62 MB	

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置Session TTL

功能介绍

1. 会话生存时间，即会话建立后无任何数据传送情况下的存活时间，默认为3600秒，当该会话在超时之前有任何数据匹配该会话，则该会话ttl计时器复位到该数值，如3600秒。有的服务如数据库。需要长连接，尽可能能将其TCP的会话超时时间设置得较大。
2. session-ttl配置有4种不同的类型，分为全局session-ttl 、全局自定义的session-ttl、策略session-ttl 、服务对象session-ttl。session-ttl必须在CLI下配置。

> **重要**
>
> 配置session-ttl时间只对状态为“已建立”的会话TTL时间生效。

配置方法

1. 配置全局session-ttl。

```
config system session-ttl
    set default 3600    //TCP会话的老化时间，300-2764800秒(最大为32天)，默认为3600s
end

config system global
    set udp-idle-timer 180    //UDP会话的老化时间，1-86400秒(最大为1天)，默认为180s
end
```

2. 全局自定义session-ttl，可自由定义协议、端口与会话超时时间。

```
config system session-ttl
    config port
        edit 1
            set protocol 6
            set timeout 86400
            set start-port 5000
            set end-port 5000
        next
        edit 2
            set protocol 17
            set timeout 360
            set start-port 4500
            set end-port 4500
        next
        edit 3
            set protocol 1
            set timeout 60
        next
    end
end
```

3. 基于策略的session-ttl，针对匹配该策略的所有协议的会话生效。

```
config firewall policy
    edit 1
        set srcintf lan
        set dstintf wan1
        set srcaddr all
        set dstaddr all
        set action accept
        set schedule always
        set service ANY
        set session-ttl 604800    //针对匹配该策略的所有协议/端口的会话生效
        set nat enable
    next
end
```

4. 基于服务对象的session-ttl，定义不同的对象，虽然同为23端口，可以配置指定不同协议的session-ttl时间，被策略引用后才会生效。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall service custom
    edit telnet
        set protocol TCP
        set tcp-portrange 23
        set session-ttl 7200
    next
    edit "telnetnew"
        set protocol UDP
        set tcp-portrange 23
        set session-ttl 3600
    next
end
```

Session TTL优先级

全局session-ttl（低）< 全局自定义session-ttl < 策略session-ttl < 被策略引用的服务对象session-ttl（高）。优先级高的session-ttl优先被使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

会话dirty机制

简介

会话Dirty状态

当FortiGate接收到新会话的首个数据包（如TCP SYN）时，设备会执行路由查询，并根据防火墙策略判断是否允许该流量通过，然后创建对应的会话。对首个响应数据包（如TCP SYN ACK）仅执行路由查找（不检查防火墙策略）。

FortiGate会将路由查询信息（出接口与网关）、防火墙策略ID及其他信息（如地址转换、UTM检测、认证、日志记录等）保存至会话中，并将其状态标记为 `may_dirty` 。其中本文主要关注其中的 `state=` 字段中的会话dirty状态，如下所示，该会话的状态为 `may_dirty` 。

```bash
session info: proto=6 proto_state=11 duration=2 expire=3597 timeout=3600 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty ndr npu f00     ←——这里的会话状态为may_dirty
statistic(bytes/packets/allow_err): org=116/2/1 reply=60/1/1 tuples=3
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=40→7/7→40 gwy=10.10.12.1/192.168.100.177
hook=post dir=org act=snat 192.168.100.177:54449→223.5.5.5:443(10.10.12.2:54449)
hook=pre dir=reply act=dnat 223.5.5.5:443→10.10.12.2:54449(192.168.100.177:54449)
hook=post dir=reply act=noop 223.5.5.5:443→192.168.100.177:54449(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=0c:37:96:06:d7:5d
misc=0 policy_id=1 pol_uuid_idx=661 auth_info=0 chk_client_info=0 vd=0
serial=00172c91 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×003c94 ips_offload ofld-O ofld-R
npu info: flag=0×81/0×81, offload=8/8, ips_offload=1/1, epid=16/16, ipid=95/66, vlan=0×0000/0×0000
vlifid=95/66, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=2/0, ha_divert=0/0
```

会话dirty状态有如下2种：

- `may_dirty` ：如果流量被防火墙策略允许，且设备没有发生任何策略、路由等变化，会话保持 `may_dirty` 状态。
- `dirty` ：如果防火墙策略中的参数（如源、目的）发生变化，或其他可能触发状态变更的条件（如路由变化），现有会话的 `may_dirty` 标记将被修改为 `dirty` 状态。随后FortiGate需要重新评估下一个匹配该会话数据包的路由、策略等信息：
  - 如果流量仍被防火墙策略允许，则移除 `dirty` 标志并恢复 `may_dirty` 标志，更新会话中的NAT、网关、策略ID等信息。
  - 若流量经重新评估后被判定为拒绝，则标记为 `block` 标志，并保留在会话表中直至过期。任何匹配带有 `block` 标志会话的数据包均会被丢弃。
  - 只要会话的状态没有被标记为 `dirty` ，FortiGate就不会对该会话执行重新评估。

会话dirty原因

以下是可能导致会话被标记为 `dirty` 的原因：

- 防火墙策略变化。
- 路由变化。
- 网络相关的配置变更。
- 执行FortiGuard计划更新（仅当下载新定义且策略关联了相关安全配置文件时）。
- 若会话通过FGSP协议进行同步。

会话dirty相关配置

firewall-session-dirty

防火墙策略配置发生变化后，相关会话的dirty状态变化会根据 `firewall-session-dirty` 配置决定。

- **VDOM级别配置**

```bash
config system settings
    set firewall-session-dirty { check-all | check-new | check-policy-option }
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- `check-all`（默认）：所有被编辑的防火墙策略影响的会话状态被标记为`dirty`，无论是匹配原有会话的流量还是新创建的流量，重新评估为新会话。
- `check-new`：现有会话不会被标记为`dirty`，而是被标记为`persistent`，原有匹配该会话的流量也不会被重新评估（直至该会话老化），仅检查新创建的流量。
- `check-policy-option`：使用防火墙策略级别汇总的配置。

- **策略级别配置**

```bash
config firewall policy
    edit <id>
        set firewall-session-dirty < check-all | check-new >
    next
end
```

  - `check-all`（默认）：所有被编辑的防火墙策略影响的会话状态被标记为`dirty`，无论是匹配原有会话的流量还是新创建的流量，重新评估为新会话。
  - `check-new`：现有会话不会被标记为`dirty`，而是被标记为`persistent`，原有匹配该会话的流量也不会被重新评估（直至该会话老化），仅检查新创建的流量。

fqdn-session-check

FQDN地址对象解析的IP发生变化后，相关会话的dirty状态变化会根据`fqdn-session-check`配置决定。

```bash
config system settings
    set fqdn-session-check { enable | disable }
end

FQDN地址示例:
config firewall address
    edit "www.fortinet.com"
        set type fqdn
        set fqdn "www.fortinet.com"
    next
end
```

- `disable`（默认）：现有会话不会被标记为`dirty`，而是被标记为`persistent`，原有匹配该会话的流量也不会被重新评估（直至该会话老化），仅检查新创建的流量。
- `enable`：现有相关会话被标记为`dirty`，无论是匹配原有会话的流量还是新创建的流量，重新评估为新会话。

snat-route-change

该参数决定路由变化后，SNAT的会话表是否跟随着一起变化更新。

```bash
config system settings
    set snat-route-change { enable | disable }
end
```

- `disable`（默认）：会话表项不变化，继续保持该会话，保持原有出口。
- `enable`：会话表项变化，会话状态会置位为`dirty`，并且后续同一会话的数据将会重新上送CPU查询策略/路由等参数，重新进行策略的匹配，一旦路由变化将会匹配新的出口进行数据的转发。

preserve-session-route

该参数基于路由出接口，决定路由变化后，非SNAT的会话表是否跟随着一起变化更新。

```
config system interface
    edit "port2"
        set preserve-session-route { enable | disable }
    next
end
```

- `disable`（默认）：不保持会话，立刻将会话标记为`dirty`，并重新评估后续流量。
- `enable`：强制保持会话，不会主动的更新会话中路由的下一跳地址。
- 这个命令的优先级更高，只要开启了接口的会话保持，无论`snat-route-change`是否开启，会话还是为会优先保持，会话/流量不会更变出接口信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ext-resource-session-check

外部威胁源对象（如IP、域名、Web分类等）的内容发生变化后，相关会话的dirty状态变化会根据`ext-resource-session-check`配置决定。

> **重要**
>
> 外部威胁源的配置请参考：Security Fabric→威胁情报源↗章节。

```bash
config system settings
    set fqdn-session-check { enable | disable }
end
```

- `disable`（默认）：现有会话不会被标记为`dirty`，而是被标记为`persistent`，原有匹配该会话的流量也不会被重新评估（直至该会话老化），仅检查新创建的流量。
- `enable`：现有相关会话被标记为`dirty`，无论是匹配原有会话的流量还是新创建的流量，重新评估为新会话。

dyn-addr-session-check

动态地址（如从SDN连接器获取地址）对象中的地址内容发生变化后，相关会话的dirty状态变化会根据`dyn-addr-session-check`配置决定。

```
config system settings
    set dyn-addr-session-check { enable | disable }
end
```

- `disable`（默认）：现有会话不会被标记为`dirty`，而是被标记为`persistent`，原有匹配该会话的流量也不会被重新评估（直至该会话老化），仅检查新创建的流量。
- `enable`：现有相关会话被标记为`dirty`，无论是匹配原有会话的流量还是新创建的流量，重新评估为新会话。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

iprope列表

简介

iprope 表是 FortiGate 内部用于表示管理员所配置防火墙策略的结构化数据形式。 iprope 将所有策略条目按功能划分为多个策略组，每组条目从上到下依次匹配，一旦命中即执行相应动作，不再继续检查同组的后续条目。

匹配依据包括：

- 源/目的地址
- 端口范围
- 协议类型

可能的动作包括：

- drop：丢弃数据包，不建立会话。
- accept：放行数据包，建立会话。
- redirect：将数据包交付内部处理逻辑。

> **提示**
>
> iprope 表中不存在 GUI 防火墙策略的“隐式拒绝”，所有条目均为显式策略。

常用命令

用于查看不同策略组的命令：

```bash
diagnose firewall iprope list 100002   # 静态 SNAT 策略
diagnose firewall iprope list 100000   # VIP（DNAT）策略
diagnose firewall iprope list 100004   # 普通 Forward 策略
diagnose firewall iprope list 10000e   # 系统生成的 Local-In 策略
diagnose firewall iprope list 100015   # Traffic Shaping 策略
diagnose firewall iprope list 100017   # 简单 ZTNA 策略
```

输出示例及字段说明

```bash
FortiGate # diagnose firewall iprope show 00100004

Policy Group 00100004

policy index=1 uuid_idx=14 action=accept
flag (8050108): redir nat master use_src pol_stats
flag2 (4000): resolve_sso
flag3 (20): schedule(always)
cos_fwd=255 cos_rev=255
group=00100004 av=00004e20 au=00000000 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0

zone(1): 3 -> zone(1): 6
source(1): 10.0.1.0-10.0.1.255, uuid_idx=12,
dest(1): 192.0.2.0-192.0.2.255, uuid_idx=13,
service(1):
[0:0x0:0/(0,65535)->(0,65535)]
helper:auto
```

字段含义说明：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

字段	含义
policy index	策略条目索引
action	动作类型
flag/flag2/flag3	启用的处理能力标识，如 NAT、SSL、策略统计等
zone	入/出口 zone 标识
source/dest	源/目的地址范围和 UUID
service	协议与端口匹配范围
helper	ALG（会话助手）配置方式

策略组列表

Group ID	名称	说明
00000003	AUTH_DEFAULT	Authentication 策略
00000005	CAPTIVE_PORTAL	配置 security-mode 的接口
00004e20	SESS_HELPER	Session Helper 相关
00100001	CUST_LOCAL_IN	自定义 Local-In 策略
00100002	STATIC_SNAT	静态 SNAT 或地址池 SNAT
00100003	DEC_FWD	IPsec 解密后策略匹配
00100004	ENC_FWD	所有 Forward 策略
0010000a	MULTICAST	组播策略
0010000c	EP_REDIR	Endpoint Control 相关策略
0010000d	CENTRAL_NAT	Central NAT 策略
0010000e	IMPLICIT_IN	系统生成的 Local-In 策略（例如管理协议）
0010000f	ADMIN_IN	管理面流量的基于接口放行策略
00100011	ZTNA_PROXY	ZTNA 策略
00100015	Traffic Shaper	Forward 整形策略
00100018	Traffic Shaper	Local-In 整形策略
00100019	Traffic Shaper	Local-Out 整形策略

提示

如果某功能在设备中启用，则对应策略组中可能包含默认策略条目。

注意事项

- 策略组具有固定的 Group ID。
- 每条策略使用 policy index 标识。
- 出厂配置中若某功能默认启用，则可能存在预置条目。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 所有策略检查在数据平面内部完成，不在 GUI 中显示。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

流量到达FortiGate后无法转发

问题现象

1. 某用户通过FortiGate访问Internet，但发现部分Internet服务无法访问，对应的IP也无法Ping通。

2. 检查防火墙上网策略配置全部正确，路由也无异常。

3. 抓包发现流量到达FortiGate后没有转发到Internet（只有in，没有out）。

```bash
FortiGate # diagnose sniffer packet any 'host 223.5.5.5' 4
interfaces=[any]
filters=[host 223.5.5.5]
0.400011 lan in 192.168.100.178 → 223.5.5.5: icmp: echo request
1.405165 lan in 192.168.100.178 → 223.5.5.5: icmp: echo request
2.410579 lan in 192.168.100.178 → 223.5.5.5: icmp: echo request
3.412497 lan in 192.168.100.178 → 223.5.5.5: icmp: echo request
```

4. Debug Flow看到该流量查找路由表的出接口为root，随后被丢弃。

```bash
id=65308 trace_id=1 func=print_pkt_detail line=5795 msg="vd-root:0 received a packet(proto=1,
192.168.100.178:65060→223.5.5.5:2048) tun_id=0.0.0.0 from lan. type=8, code=0, id=65060, seq=744."
id=65308 trace_id=1 func=init_ip_session_common line=5980 msg="allocate a new session-0000139d, tun_id=0.0.0.0"
id=65308 trace_id=1 func=vf_ip_route_input_common line=2611 msg="find a route: flag=80000000 gw-223.5.5.5 via
root"
id=65308 trace_id=1 func=fw_local_in_handler line=606 msg="iprope_in_check() check failed on policy 0, drop"
```

问题原因

1. 用户错误的配置了IPPool的地址范围为客户端要正常访问的IP地址，不论是否为防火墙策略引用。

```bash
config firewall ippool
    edit "IPPool"
        set startip 223.5.5.5
        set endip 223.5.5.5
    next
end
```

2. 或是用户错误的配置了VIP的extip地址为客户端要正常访问的IP地址，不论是否为防火墙策略引用。

```bash
config firewall vip
    edit "VIP"
        set extip 223.5.5.5
        set mappedip "10.10.2.1"
        set extintf "wan1"
    next
end
```

3. VIP配置中的外部IP和IPPool中配置的地址范围不能配置为现有网络中其他设备的IP、FortiGate的网关IP，也不能配置为内网客户端正常上网可能访问的IP地址。这是由于FortiGate配置VIP或IPPool后，extip、IPPool地址范围属于FortiGate自身的IP地址，即使VIP或IPPool没有被防火墙策略引用，所有访问该IP的流量经过FortiGate时都会被FortiGate引流到自身，影响正常的业务。

解决方法

1. 遇到以上问题时首先使用Sniffer抓包和Debug Flow排查，如果显示流量被路由到root接口，则有可能是以上配置导致。
2. 修改VIP中的extip或IPPool中的地址范围为正确的地址，或删除错误配置的VIP、IPPool。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VIP流量无法匹配防火墙策略

问题描述

1. 用户在防火墙策略中配置了一条引用VIP作为目标的防火墙策略（ID 6），源接口为wan1，目标接口为lan。

```bash
config firewall vip
    edit "VIP_192.168.100.77"
        set extip 10.10.12.5
        set mappedip "192.168.100.77"
        set extintf "wan1"
    next
end

config firewall policy
    edit 6
        set name "VIP_ADC"
        set srcintf "wan1"
        set dstintf "lan"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP_192.168.100.77"
        set schedule "always"
        set service "ALL"
    next
end
```

2. 用户想要暂时禁止从wan1到lan的流量（包括VIP流量），在上述策略前创建了一条从wan1到lan禁止所有流量的策略（ID 8）。

```bash
config firewall policy
    edit 8
        set name "Deny_wan1_to_lan"
        set srcintf "wan1"
        set dstintf "lan"
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic disable
    next
    edit 6
        set name "VIP_ADC"
        set srcintf "wan1"
        set dstintf "lan"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP_192.168.100.77"
        set schedule "always"
        set service "ALL"
    next
end
```

3. 此时外部流量访问VIP时，仍然可以通过VIP映射正常访问到内网服务器，流量会话匹配的Policy ID为6，拒绝策略的Policy ID 8在Policy ID 6之上，但仍然匹配了Policy ID 6。

```bash
session info: proto=6 proto_state=01 duration=14 expire=3585 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=ftp vlan_cos=0/255
state=may_dirty npu npd
statistic(bytes/packets/allow_err): org=164/3/1 reply=154/2/1 tuples=2
tx speed(Bps/kbps): 10/0 rx speed(Bps/kbps): 10/0
orgin->sink: org pre->post, reply pre->post dev=7->48/48->7 gwy=192.168.100.77/10.10.12.1
hook=pre dir=org act=dnat 10.10.12.1:13034->10.10.12.5:21(192.168.100.77:21)
hook=post dir=reply act=snat 192.168.100.77:21->10.10.12.1:13034(10.10.12.5:21)
pos/(before,after) 0/(0,0), 0/(0,0)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
dst_mac=00:e0:4c:b9:97:7c
misc=0 //policy_id=6// pol_uuid_idx=590 auth_info=0 chk_client_info=0 vd=0
serial=00002ee8 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4100000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  offload-denied helper
```

解决方法

1. 默认配置下（FortiOS 7.2.4之前的版本），仅当防火墙策略引用的目标地址为VIP时，访问VIP的流量才会匹配该策略。如果目标为“all”，则流量不会匹配该策略，所以上述场景下，访问VIP的流量只会匹配Policy ID 6。
2. 通过在Policy ID 8下开启`match-vip`，可以使访问VIP的流量匹配目标为“all”的策略Policy ID 8，从而被丢弃。

```bash
config firewall policy
    edit 8
        set match-vip enable
    next
end
```

3. 外部流量访再次问VIP时，虽然也执行了VIP的DNAT转换，但最后会匹配Policy ID 8被丢弃。

```bash
id=65308 trace_id=13 func=print_pkt_detail line=5795 msg="vd-root:0 received a packet(proto=6, 10.10.12.1:14317->10.10.12.5:21) tun_id=0.0.0.0 from wan1. flag [S], seq 987682832, ack 0, win 65535"
id=65308 trace_id=13 func=init_ip_session_common line=5980 msg="allocate a new session-00003270, tun_id=0.0.0.0"
id=65308 trace_id=13 func=get_new_addr line=1231 msg="find DNAT: IP-192.168.100.77, port-0(fixed port)"
id=65308 trace_id=13 func=fw_pre_route_handler line=180 msg="VIP-192.168.100.77:21, outdev-wan1"
id=65308 trace_id=13 func=__ip_session_run_tuple line=3402 msg="DNAT 10.10.12.5:21→192.168.100.77:21"
id=65308 trace_id=13 func=vf_ip_route_input_common line=2611 msg="find a route: flag=04000000 gw-192.168.100.77 via lan"
id=65308 trace_id=13 func=__iprope_tree_check line=539 msg="gnum-100004, use addr/intf hash, len=4"
id=65308 trace_id=13 func=fw_forward_handler line=825 msg="Denied by forward policy check (policy 8)"
```

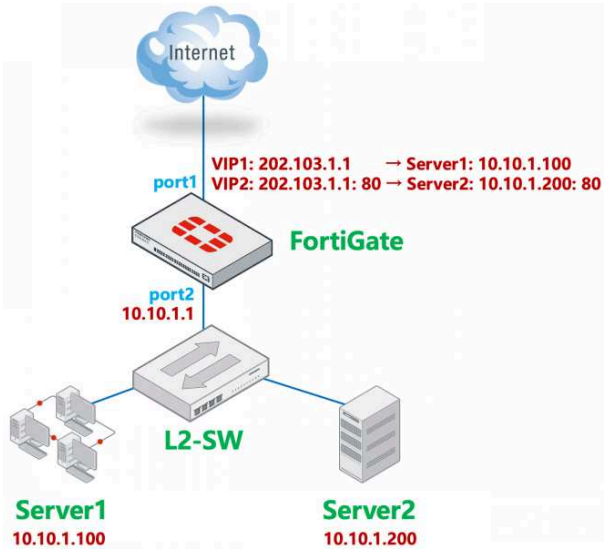
注意事项

- 在FortiOS 7.2.4及以后版本中，防火墙策略中的`match-vip`选项默认为`enable`状态。
- 在FortiOS 7.2.4之前的版本中，防火墙策略中的`match-vip`选项默认为`disable`状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VIP 匹配顺序

网络拓扑



- 初始状态下，FortiGate的公网接口port1上配置了1个VIP：从公网IP 202.103.1.1全映射到Server1 10.10.1.100（VIP1）。

```bash
config firewall vip
    edit "VIP1"
        set extip 202.103.1.1
        set mappedip "10.10.1.100"
        set extintf "port1"
    next
end
```

- 创建1条防火墙策略（VIP1_Policy）引用VIP1，公网客户端通过VIP1_Policy策略访问Server1。

```bash
config firewall policy
    edit 1
        set name "VIP1_Policy"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP1"
        set schedule "always"
        set service "ALL"
    next
end
```

问题现象

1. 由于业务需求，需要增加与VIP1相同的公网IP 202.103.1.1的80端口映射到Server2 10.10.1.100的80端口（VIP2），创建后VIP2位于VIP1后边。

```bash
config firewall vip
    edit "VIP1"
        set extip 202.103.1.1
        set mappedip "10.10.1.100"
        set extintf "port1"
    next
    edit "VIP2"
        set extip 202.103.1.1
        set mappedip "10.10.1.200"
        set extintf "port1"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set portforward enable
        set extport 80
        set mappedport 80
    next
end
```

2. 创建防火墙策略VIP2_Policy，引用VIP2，将VIP2_Policy移动到VIP1_Policy之前。当前的需求是，按照防火墙策略的顺序：

   - 访问VIP 202.103.1.1的80端口的流量应该优先匹配VIP2_Policy。
   - 访问VIP 202.103.1.1的其他端口的流量应该匹配VIP1_Policy。

```bash
config firewall policy
    edit 2
        set name "VIP2_Policy"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP2"
        set schedule "always"
        set service "ALL"
    next
    edit 1
        set name "VIP1_Policy"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr "VIP1"
        set schedule "always"
        set service "ALL"
    next
end
```

3. 但实际情况是：公网客户端（202.103.1.200）访问VIP（202.103.1.1）的80端口（或其他任意端口），流量经过DNAT后，目标地址仍然被转换为VIP1对应的Server1 IP 10.10.1.100，会话匹配策略为VIP1_Policy（ID 1）。这不符合预期。

```bash
session info: proto=6 proto_state=01 duration=10 expire=3589 timeout=3600 refresh_dir=both flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
......
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 202.103.1.200:50883->202.103.1.1:80(10.10.1.100:80) <———DNAT的地址仍为VIP1映射的Server1
hook=post dir=reply act=snat 10.10.1.100:80->202.103.1.200:50883(202.103.1.1:80)
......
misc=0 policy_id=1 pol_uuid_idx=15851 auth_info=0 chk_client_info=0 vd=0
......
```

4. 查看策略VIP2_Policy（ID 2）的匹配计数，始终为0。

```bash
FortiGate # diagnose firewall iprope show 100004 2
idx:2
pkts:0 (0 0 0 0 0 0 0 0)
bytes:0 (0 0 0 0 0 0 0 0)
asic_pkts:0 (0 0 0 0 0 0 0 0)
asic_bytes:0 (0 0 0 0 0 0 0 0)
flag:0x0
```

5. 查看策略VIP1_Policy（ID 1）的匹配计数，持续增长。

```bash
FortiGate # diagnose firewall iprope show 100004 1
idx:1
pkts:282 (282 0 0 0 0 0 0 0)
bytes:15921 (15921 0 0 0 0 0 0 0)
asic_pkts:0 (0 0 0 0 0 0 0 0)
asic_bytes:0 (0 0 0 0 0 0 0 0)
flag:0x0
hit count:54 (54 0 0 0 0 0 0 0)
    first hit:2025-11-05 14:52:19 last hit:2025-11-05 16:27:38
established session count:0
    first est:2025-11-05 15:02:00 last est:2025-11-05 15:53:55
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

6. 通过如下 CLI 命令查看 iprope 表特定流量的防火墙策略匹配情况，可以看到以上访问 VIP 80 端口的流量匹配的就是防火墙策略 VIP1_Policy（ID 1）。

```bash
diagnose firewall iprope lookup <src ip> <src port> <dst ip> <dst port> <protocol> <device>

FortiGate # diagnose firewall iprope lookup 202.103.1.200 0 202.103.1.1 80 6 port1
<src [202.103.1.200-0] dst [202.103.1.1-80] proto 6 dev port1> matches policy id: 1
```

问题原因

- 由于FortiGate内核设计，VIP转换始终优于防火墙策略进行处理：
  - 首先流量到达FortiGate后，VIP按照顺序从上向下依次匹配，并执行DNAT转换。
  - 然后防火墙策略才会按照DNAT转换后的流量特征，顺序从上向下依次匹配。
- 当全映射 VIP（VIP1）排在 80 端口映射 VIP（VIP2）上方时，所有目标为该公网 IP 的流量均命中全映射 VIP（VIP1），并按照VIP1进行DNAT转换，导致转换后的流量无法匹配VIP2_Policy。
- 通过观察防火墙 iprope 的 VIP 策略组（100000）也可以看到，VIP1 在 VIP2 之前：

> **相关信息**
>
> iprope 的相关解释请参考：策略与对象→iprope列表 ↗章节。

```bash
FortiGate # diagnose firewall iprope list 100000

policy index=15849 uuid_idx=15849 action=accept ←——VIP1在前
flag (8000104): f_p nat pol_stats
schedule()
cos_fwd=0  cos_rev=0
group=00100000 av=00000000 au=00000000 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0
zone(1): 0 -> zone(1): 0
source(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
dest(1): 202.103.1.1-202.103.1.1, uuid_idx=15849,
service(1):
        [0:0x0:0/(0,0)->(0,0)] flags:0 helper:auto
nat(1): flag=0 base=202.103.1.1:0 10.10.1.100-10.10.1.100(0:0)

policy index=15850 uuid_idx=15850 action=accept ←——VIP2在后
flag (8000100): nat pol_stats
schedule()
cos_fwd=0  cos_rev=0
group=00100000 av=00000000 au=00000000 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0
zone(1): 0 -> zone(1): 0
source(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
dest(1): 202.103.1.1-202.103.1.1, uuid_idx=15850,
service(1):
        [6:0x0:0/(0,65535)->(80,80)] flags:0 helper:auto
nat(1): flag=0 base=202.103.1.1:80 10.10.1.200-10.10.1.200(80:80)
......
```

解决方法

1. 调整 VIP 顺序，让映射 80 端口的 VIP（VIP2）排在全映射的 VIP （VIP1）之前，防火墙策略的顺序不需要调整。

```bash
config firewall vip
    move VIP2 before VIP1
end

config firewall vip
    edit "VIP2"
        set extip 202.103.1.1
        set mappedip "10.10.1.200"
        set extintf "port1"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set portforward enable
        set extport 80
        set mappedport 80
    next
    edit "VIP1"
        set extip 202.103.1.1
        set mappedip "10.10.1.100"
        set extintf "port1"
    next
end
```

2. 公网客户端（202.103.1.200）再次访问VIP（202.103.1.1）的80端口，流量经过DNAT后，目标地址被转换为VIP2对应的Server2 IP 10.10.2.100，会话匹配策略为VIP2_Policy（ID 2）。符合预期。

```bash
session info: proto=6 proto_state=01 duration=4 expire=3595 timeout=3600 refresh_dir=both flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
......
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 202.103.1.200:58372->202.103.1.1:80(10.10.1.200:80) <———DNAT的地址变为VIP2映射的Server2
hook=post dir=reply act=snat 10.10.1.200:80->202.103.1.200:58372(202.103.1.1:80)
......
misc=0 policy_id=2 pol_uuid_idx=15852 auth_info=0 chk_client_info=0 vd=0
......
```

3. 公网客户端（202.103.1.200）再次访问VIP（202.103.1.1）的其他端口（如443），流量经过DNAT后，目标地址被转换为VIP1对应的Server1 IP 10.10.1.100，会话匹配策略为VIP1_Policy（ID 1）。符合预期。

```bash
session info: proto=6 proto_state=06 duration=0 expire=4 timeout=3600 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
......
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=dnat 202.103.1.200:58617->202.103.1.1:443(10.10.1.100:443) <———DNAT的地址为VIP1映射的Server1
hook=post dir=reply act=snat 10.10.1.100:443->202.103.1.200:58617(202.103.1.1:443)
......
misc=0 policy_id=1 pol_uuid_idx=15851 auth_info=0 chk_client_info=0 vd=0
......
```

4. 查看策略VIP2_Policy（ID 2）已经开始有匹配计数。

```bash
FortiGate # diagnose firewall iprope show 100004 2
idx:2
pkts:46 (46 0 0 0 0 0 0 0)
bytes:2029 (2029 0 0 0 0 0 0 0)
asic_pkts:0 (0 0 0 0 0 0 0 0)
asic_bytes:0 (0 0 0 0 0 0 0 0)
flag:0x0
hit count:3 (3 0 0 0 0 0 0 0)
    first hit:2025-11-05 16:44:31 last hit:2025-11-05 16:50:40
established session count:1
    first est:2025-11-05 16:44:31 last est:2025-11-05 16:50:40
```

5. 查询iprope表特定流量的防火墙策略匹配情况，可以看到访问 VIP 80 端口的流量匹配的是防火墙策略 VIP2_Policy（ID 2）。

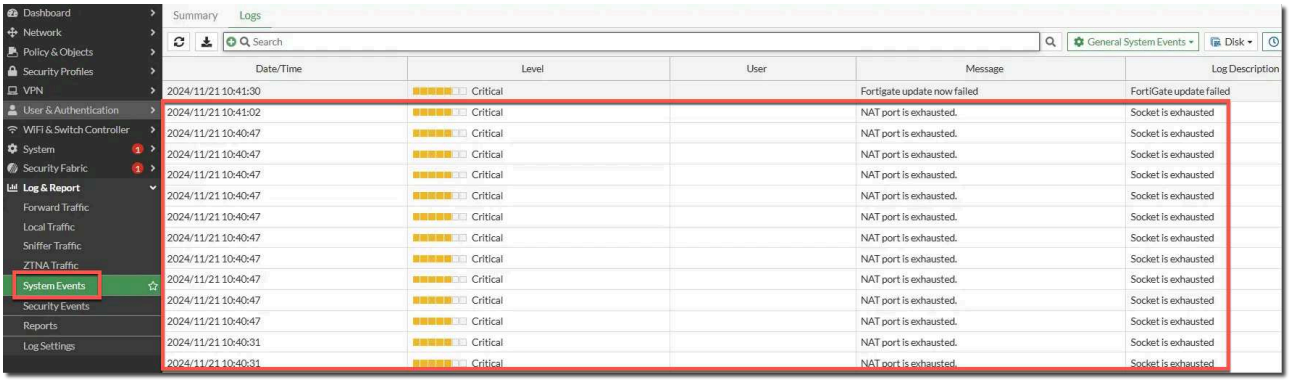
```bash
diagnose firewall iprope lookup <src ip> <src port> <dst ip> <dst port> <protocol> <device>

FortiGate # diagnose firewall iprope lookup 202.103.1.200 0 202.103.1.1 80 6 port1
<src [202.103.1.200-0] dst [202.103.1.1-80] proto 6 dev port1> matches policy id: 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NAT端口耗尽

问题现象

FortiGate部署在Internet出口，并开启NAT功能实现内部用户上网。在使用过程中FortiGate产生了`NAT port is exhausted. Socket is exhausted`的系统事件日志。




```bash
date="2024-11-27" time="11:20:32" devid="FG101FTK2000XXXX" vd="root" type="event" subtype="system" bid=540114651
devname="FG101FTK2000XXXX" dstepid=3 dsteuid=3 dstip="8.8.8.8" dstport=53 dvid=2147 epid=3 euid=3
eventtime=1732492832315428126 id=7242716162855799960 level="critical" logdesc="Socket is exhausted"
logid="0100020007" logver=604065868 msg="NAT port is exhausted." nat="33.43.111.222" proto=17 service="kernel"
srcip="10.200.100.50" srcport=15651 status="failure" tz="-0500" vrf=0
```

问题原因

在FortiGate上使用`同一SNAT IP + 同一目的IP + 同一协议 + 同一目的端口`（以下简称**四元组**）时，支持60416个连接。如果同一**四元组**已经存在了60416个连接，此时需要多一个连接，那么就会出现NAT端口耗尽的情况，新的连接无法建立，并产生以上日志。

对于其他连接，只要**四元组**没有达到60416个连接，就不会产生以上问题。所以只要其他流量中的SNAT IP、目的IP、协议、目的端口有任意一项与已耗尽的**四元组**不同，业务就不会受到影响。

FortiGate端口使用规则

1. FortiOS使用以上**四元组**来确定NAT可用池的原因是FortiGate是基于会话的防火墙。 流量通过FortiGate设备进行连接时，会创建一个会话，并为该会话创建两个索引。 FortiGate设备使用这些索引将匹配流量引导至匹配的会话。
2. 使用这些属性来确定池的原因是 FortiOS 防火墙基于会话的设计。 通过 FortiGate 设备进行 TCP 连接时，会创建一个会话，并为该会话创建2个索引， FortiGate设备使用这2个索引将匹配流量引导至会话：
   - **索引1**，用于流量发起方向的会话标识。

     ```
     src-ip: 10.10.1.1
     dst-ip: 202.1.1.1
     proto: TCP
     src-port: 10240
     dst-port: 443
     ```

   - **索引2**，用于返回流量的会话标识。

     ```
     src-ip: 202.1.1.1
     dst-ip: 101.1.1.1
     proto: TCP
     src-port: 80
     dst-port: 46372
     ```

   - 其中46372是发起方向流量SNAT后FortiGate分配的端口。有了这2个索引，当流量与其中任一索引匹配时，流量所属的会话就能被唯一匹配。
3. FortiGate在分配NAT端口时，只需确保所选NAT端口与**四元组**相结合是唯一的，以便唯一标识会话。
4. 举例，在以上流量已经创建会话的情况下，内网同一客户端10.10.1.1再与同一公网服务器202.1.1.1的443端口建立连接，此时FortiGate将创建另一个会话，返回方向上的索引如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
src-ip: 202.1.1.1
dst-ip: 10.10.1.1
proto: TCP
src-port: 443
dst-port: NP
```

5. NP 的值可以是任何值，只要五个值加起来是唯一的。 例如，FortiGate可以再次选择46372，因为`src-port`不一样。

```
src-ip: 202.1.1.1
dst-ip: 10.10.1.1
proto: TCP
src-port: 443
dst-port: 46372
```

6. 所以同一**四元组**的情况下FortiGate可以建立的连接数，取决于`src-port`的数量，FortiGate支持的最大值为60416。

7. 举例，如果访问的目的IP有3个，那么`同一SNAT IP + 同一目的端口`最多可以在FortiGate上产生多少个连接？答案是`60416 * 3 = 181248`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

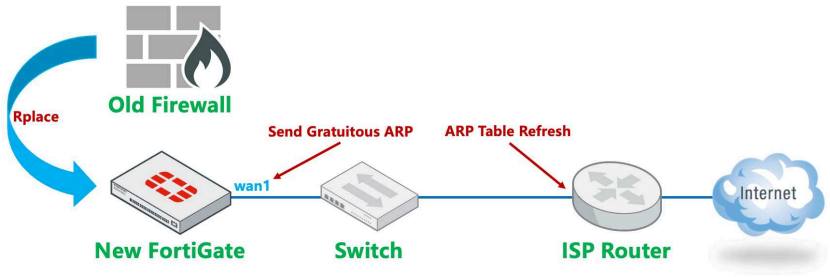
地址池ARP刷新

背景

在网络设备替换场景中（例如原厂商设备被FortiGate替换），如果设备的SNAT使用了IP Pool（地址池），可能会出现如下问题：

- 新防火墙上线后，IP Pool不会主动发送Gratuitous ARP（免费ARP）。
- 上游路由器或交换机的ARP缓存仍保留旧防火墙的MAC。
- 因此下行流量仍发往旧MAC，新防火墙收到后直接丢弃。表现为：上行能通，下行不通。
- 割接时无法联系运营商关闭路由器接口，导致无法更新运营商路由器的ARP表。

网络环境



- 使用FortiGate替换原有旧防火墙。
- FortiGate上线后，上游ISP路由器的ARP缓存仍保留旧防火墙的MAC。
- 新FortiGate通过IP Pool配置SNAT，使内网客户端访问Internet。

```bash
config system interface
    edit wan1
        set ip 192.168.1.2/24
        set allowaccess ping
    next
end

config firewall ippool
    edit "pool1"
        set startip 192.168.1.11
        set endip   192.168.1.20
        set associated-interface wan1
    next
end

config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "lan"
        set dstintf "wan1"
        set action accept
        set srcaddr "LAN"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set ssl-ssh-profile "certificate-inspection"
        set nat enable
        set ippool enable
        set poolname "pool1"
    next
end
```

方法1-HA切换

如果设备为HA组网，HA主备切换会触发ARP更新，FortiGate会对所有VIP、接口IP、IP Pool地址广播Gratuitous ARP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

1. 确认HA已启用Gratuitous ARP（默认即启用）。

```bash
config system ha
    set gratuitous-arps enable
    set arps 5
    set arps-interval 8
end
```

2. 在当前HA主设备上手动触发一次HA切换。

```bash
diagnose sys ha reset-uptime
```

3. 切换完成后，在新的HA主设备上抓包验证，可以看到设备根据IP Pool中的地址发送了对应的Gratuitous ARP。

```bash
FortiGate # diagnose sniffer packet port3 "arp" 4 0 l

2025-10-13 20:57:17.298321 port3 -- arp who-has 192.168.1.11 tell 192.168.1.11
2025-10-13 20:57:17.298331 port3 -- arp who-has 192.168.1.12 tell 192.168.1.12
2025-10-13 20:57:17.298340 port3 -- arp who-has 192.168.1.13 tell 192.168.1.13
 ...
2025-10-13 20:57:49.206136 port3 -- arp who-has 192.168.1.18 tell 192.168.1.18
2025-10-13 20:57:49.206143 port3 -- arp who-has 192.168.1.19 tell 192.168.1.19
2025-10-13 20:57:49.206149 port3 -- arp who-has 192.168.1.20 tell 192.168.1.20
```

方法2-临时创建VIP

FortiGate的VIP支持参数`gratuitous-arp-interval`，可主动周期性广播Gratuitous ARP。可临时将IP Pool地址段配置为VIP对象，以此强制发送Gratuitous ARP来刷新上游路由器ARP表项。

1. 创建VIP对象，地址范围包含IP Pool中的地址（可根据IP Pool数量配置多个VIP）。

重要

- `extip`：填写IP Pool中的地址。
- `mappedip`：可随意填写。
- `extintf`：填写连接运营商侧的接口。
- `gratuitous-arp-interval`：Gratuitous ARP的更新间隔，范围5~86400s，设置为0表示不发送Gratuitous ARP。注意间隔设置过小可能触发上游安全告警。

```bash
config firewall vip
    edit arp-refresh
        set extip 192.168.1.11-192.168.1.20
        set mappedip 192.168.3.11-192.168.3.20
        set extintf wan1
        set portforward enable
        set gratuitous-arp-interval 5
        set extport 12345
        set mappedport 12345
    next
end
```

2. 配置完成后抓包验证，设备根据VIP中的地址发送了对应的Gratuitous ARP。

```bash
FortiGate # diagnose sniffer packet wan1 'arp' 4 0 l
interfaces=[port3]
filters=[arp]
2025-10-13 21:50:46.230249 port3 -- arp who-has 192.168.1.11 tell 192.168.1.11
2025-10-13 21:50:46.230257 port3 -- arp who-has 192.168.1.12 tell 192.168.1.12
2025-10-13 21:50:46.230262 port3 -- arp who-has 192.168.1.13 tell 192.168.1.13
 ...
```

3. 确认上游路由器ARP更新完成后，删除该VIP。

```bash
config firewall vip
    delete arp-refresh
end
```

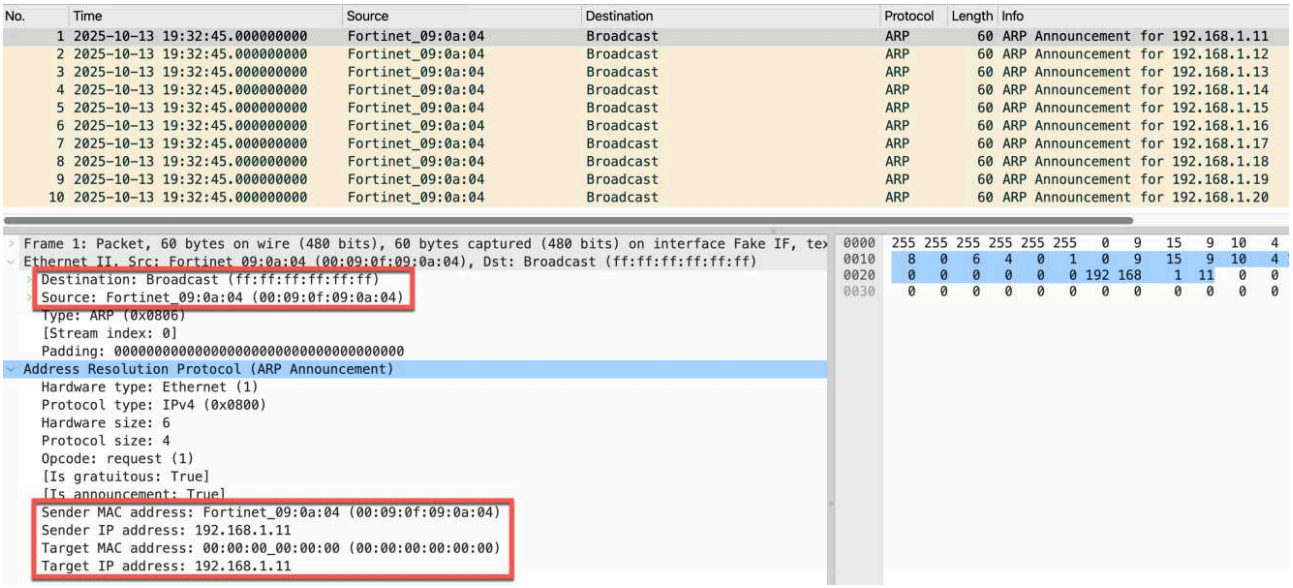

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Gratuitous ARP原理

报文示例

Gratuitous ARP的报文示例（gratuitous_arp.pcap ↗）。

报文特征：Gratuitous ARP = Sender IP == Target IP 且 Destination MAC == FF:FF:FF:FF:FF:FF。



主要作用

- 刷新上游交换机或路由器的ARP表。
- 通知邻居设备该IP地址的MAC已变更。
- 检测IP冲突（同网段若有重复地址，会收到响应）。

字段	特征	说明
操作码（Opcode）	1 (request) 或2 (reply)	GratuitousARP可为Request或Reply形式
Sender IP (SPA)	本机IP	表示自己拥有的IP地址
Target IP (TPA)	与Sender IP相同	这是Gratuitous ARP的关键特征之一
目标MAC (THA)	全0 (00:00:00:00:00:00)	因为不是响应任何主机，所以目标MAC为空
源MAC (SHA)	本机MAC地址	通常是接口的真实MAC
以太网目标地址	FF:FF:FF:FF:FF:FF（广播）	告知整个二层网段的所有设备
以太网类型 (Ethertype)	0x0806	表示这是一个ARP报文

Gratuitous ARP的两种类型

类型	Opcode	特点	主要用途
ARP Request型	1	“谁有我的地址？”	通知邻居更新ARP表
ARP Reply型	2	“我就是这个地址”	某些厂商采用这种形式广播自己的存在

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

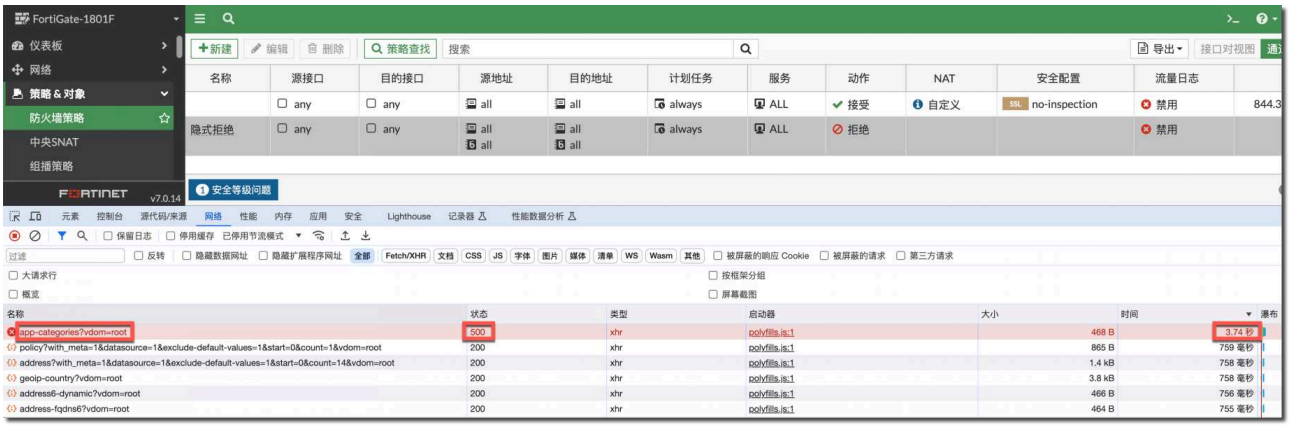
策略页面加载慢

问题现象

> **重要**
>
> 该问题仅存在于FortiOS 7.0.X版本，FortiOS 7.2和7.4版本不存在此问题。

访问FortiGate的防火墙策略（Firewall Policy）、中央SNAT（Central SNAT）、IPv4访问控制列表（IPv4 Access Control List）、零信任网络（ZTNA）、组播策略（Multicast Policy）、代理策略（Proxy Policy）、流量整形策略（Traffic Shaping Policies）、应用签名（Application Signatures）等策略相关页面时加载较慢，需要3~5秒才可以加载出来。

使用浏览器的开发者工具可以看到导致页面加载缓慢的资源是`/api/v2/monitor/fortiguard/app-categories?vdom=root`，并返回HTTP 500错误。



问题原因

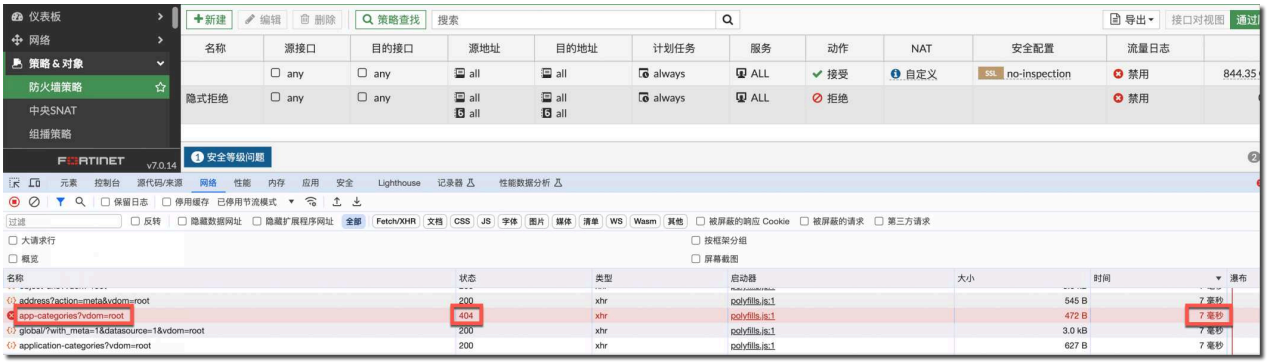
这个问题是由于通过Web方式访问这些页面时，需要从FortiGuard加载`app-categories`资源，如果FortiGate此时无法访问FortiGuard，则会花费3~5秒等待回应，直至返回HTTP 500（Internal Server Error）错误后才能显示页面。

解决方法

1. 确认FortiGate可以正常访问Internet，解决FortiGate与FortiGuard之间的连通性。
2. 如果FortiGate无法访问Internet或与FortiGuard通讯存在问题，可以在CLI下配置如下功能，关闭`gui-fortiguard-resource-fetch`后，访问这些页面时FortiGate不再会向FortiGuard请求`app-categories`资源，直接显示相关页面。

```bash
config system global
    set gui-fortiguard-resource-fetch disable
end
```

3. 再次访问FortiGate的防火墙策略页面，`app-categories`资源可以迅速加载（直接返回HTTP 404）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Local-in策略

Local-in Policy介绍

普通的防火墙策略仅能针对穿越防火墙接口的流量生效，针对目标是FortiGate自身地址（且未穿越FortiGate接口）的流量是不起作用的。Local-in Policy可以控制发送到FortiGate接口的入方向（未穿越FortiGate接口）流量。

> **重要**
>
> 即使流量的目标是FortiGate自身接口的地址，但穿越了FortiGate的接口，就不算Local-in流量，可以被普通防火墙策略控制，例如穿越FortiGate的WAN接口访问设备的内网口的流量。

管理流量（如HTTPS、PING、SSH等）可以在接口中配置允许或拒绝。受信任的管理主机可以在管理员选项中配置，以限制可以访问管理服务的主机。Local-in Policy可以自定义Local-in流量的源地址、目的地址、接口和服务。以控制以上功能无法控制的入方向本地流量：

- 可用于限制管理员访问或其他服务，例如SSL VPN服务，定义源地址或地址组来限制访问。例如，通过使用地理位置类型的地址，限制某个特定地理区域的IP访问FortiGate。也可以将“Security Fabric→外部连接器”中配置的“IP地址威胁来源”用作源地址或目的地址。
- 可以使用虚拟补丁（Virtual Patch）来减少针对FortiGate的已知漏洞的攻击。漏洞规则会在指定接口上对本地入方向流量进行扫描，并丢弃所有匹配攻击特征的流量。关于虚拟补丁（Virtual Patch）的使用方法，请参考虚拟补丁↗章节。

Local-in Policy配置

> **重要**
>
> - Local-in Policy不像普通的防火墙策略，普通防火墙策略默认隐含策略的动作为deny all，而Local-in Policy默认隐含策略的动作为permit all。
> - 在FortiOS 7.4.6、7.6.1及以后版本中，如果接口加入了SD-WAN区域，Local-in Policy只能引用接口所属的SD-WAN区域，不能引用独立的接口；如果之前的版本已经配置了Local-in Policy并引用属于SD-WAN区域的某个成员接口，升级到FortiOS 7.4.6、7.6.1及以后版本后，需要重新配置Local-in Policy才能生效。

```bash
config firewall {local-in-policy | local-in-policy6}
    edit <policy_number>
        set intf <interface>
        set srcaddr <source_address> [source_address] ...
        set srcaddr-negate {enable | disable}    //enable表示排除选择的源地址，默认为disable//
        set dstaddr <destination_address> [destination_address] ...
        set dstaddr-negate {enable | disable}    //enable表示排除选择的目标地址，默认为disable//
        set action {accept | deny}
        set service <service_name> [service_name] ...
        set schedule <schedule_name>
        set virtual-patch {enable | disable}
        set comments <string>
    next
end
```

配置步骤

举例1

用户在公网口port1上开启了SSL VPN功能。发现某些异常IP地址段经常尝试登录SSL VPN，但登录失败，并产生SSL VPN相关日志。用户想要禁止这些IP地址段尝试登录SSL VPN，不要产生SSL VPN登录日志。

1. 配置异常IP地址段的地址对象和地址组对象，例如尝试登录的异常源IP段为117.53.1.0/24、27.1.5.0/24和113.25.0.0/16，并使用地址组引用。

```bash
config firewall address
    edit "117.53.1.0/24"
        set subnet 117.53.1.0 255.255.255.0
    next
    edit "27.1.5.0/24"
        set subnet 27.1.5.0 255.255.255.0
    next
    edit "113.25.0.0/16"
        set subnet 113.25.0.0 255.255.0.0
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end

config firewall addrgrp
    edit "SSL_VPN_Deny_IP"
        set member "117.53.1.0/24" "27.1.5.0/24" "113.25.0.0/16"
    next
end
```

2. 配置用户使用的SSL VPN端口的服务对象，例如用户配置的SSL VPN端口为10443。

```bash
config firewall service custom
    edit "SSL_VPN_10443"
        set tcp-portrange 10443
    next
end
```

3. 配置Local-in Policy禁止这些异常IP访问FortiGate的SSL VPN服务。

```bash
config firewall local-in-policy
    edit 1
        set intf "port1"
        set srcaddr "SSL_VPN_Deny_IP"
        set dstaddr "all"
        set action deny
        set service "SSL_VPN_10443"
        set schedule "always"
    next
end
```

4. 使用Debug Flow查看限制网段发起的SSL VPN访问，流量被Local-in Policy（ID 1）阻断，且不再触发SSL VPN日志生成。

```bash
id=65308 trace_id=12 func=print_pkt_detail line=5888 msg="vd-root:0 received a packet(proto=6, 117.53.1.37:16008->202.103.12.2:10443) tun_id=0.0.0.0 from port1. flag [S], seq 4019479492, ack 0, win 29200"
id=65308 trace_id=12 func=init_ip_session_common line=6073 msg="allocate a new session-0000004e"
id=65308 trace_id=12 func=__vf_ip_route_input_rcu line=1999 msg="find a route: flag=80000000 gw-0.0.0.0 via root"
id=65308 trace_id=12 func=fw_local_in_handler line=618 msg="iprope_in_check() check failed on policy 1, drop"
```

5. 使用Debug Flow查看非限制网段的IP访问SSL VPN服务，可以正常访问TCP 10443端口。

```bash
id=65308 trace_id=39 func=print_pkt_detail line=5888 msg="vd-root:0 received a packet(proto=6, 202.103.12.1:16204->202.103.12.2:10443) tun_id=0.0.0.0 from port1. flag [S], seq 2461158975, ack 0, win 29200"
id=65308 trace_id=39 func=init_ip_session_common line=6073 msg="allocate a new session-0000003d"
id=65308 trace_id=39 func=__vf_ip_route_input_rcu line=1999 msg="find a route: flag=80000000 gw-0.0.0.0 via root"
id=65308 trace_id=39 func=ip_session_confirm_final line=3111 msg="npu_state=0×0, hook=1"
id=65308 trace_id=40 func=print_pkt_detail line=5888 msg="vd-root:0 received a packet(proto=6, 202.103.12.2:10443->202.103.12.1:16204) tun_id=0.0.0.0 from local. flag [S.], seq 1646480095, ack 2461158976, win 28960"
id=65308 trace_id=40 func=resolve_ip_tuple_fast line=5976 msg="Find an existing session, id-0000003d, reply direction"
...
```

6. 查看相关Local-in会话。

```bash
session info: proto=6 proto_state=01 duration=2 expire=3597 timeout=3600 refresh_dir=both flags=00000000
socktype=3 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 50/0 rx speed(Bps/kbps): 27/0
orgin->sink: org pre->in, reply out->post dev=3->9/9->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 202.103.12.1:16208->202.103.12.2:10443(0.0.0.0:0)
hook=post dir=reply act=noop 202.103.12.2:10443->202.103.12.1:16208(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=4294967295 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=0
serial=00000042 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
no_ofld_reason:  local
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

举例2

用户在公网口port1上开启了SSH访问功能。发现经常有国外IP尝试通过SSH登录FortiGate，但登录失败。用户想要禁止国外的IP访问SSH，但允许国内IP访问SSH。

1. 配置基于地理位置的国内IP地址对象。

```bash
config firewall address
    edit "China"
        set type geography
        set country "CN"
    next
end
```

2. 配置Local-in Policy允许国内IP的客户端访问FortiGate的SSH服务，但不允许其他IP访问FortiGate的SSH服务。

```bash
config firewall local-in-policy
    edit 1
        set intf "port1"
        set srcaddr "China"
        set dstaddr "all"
        set action accept
        set service "SSH"
        set schedule "always"
    next
    edit 2
        set intf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action deny
        set service "SSH"
        set schedule "always"
    next
end
```

3. 使用Debug Flow查看国内IP的SSH访问，可以正常访问。

```bash
id=65308 trace_id=1 func=print_pkt_detail line=5888 msg="vd-root:0 received a packet(proto=6, 202.103.12.1:18768->202.103.12.2:22) tun_id=0.0.0.0 from port1. flag [S], seq 3436667351, ack 0, win 29200"
id=65308 trace_id=1 func=init_ip_session_common line=6073 msg="allocate a new session-0000005a"
id=65308 trace_id=1 func=__vf_ip_route_input_rcu line=1999 msg="find a route: flag=80000000 gw-0.0.0.0 via root"
id=65308 trace_id=1 func=ip_session_confirm_final line=3111 msg="npu_state=0×0, hook=1"
id=65308 trace_id=2 func=print_pkt_detail line=5888 msg="vd-root:0 received a packet(proto=6, 202.103.12.2:22->202.103.12.1:18768) tun_id=0.0.0.0 from local. flag [S.], seq 4214370010, ack 3436667352, win 28960"
id=65308 trace_id=2 func=resolve_ip_tuple_fast line=5976 msg="Find an existing session, id-0000005a, reply direction"
...
```

4. 查看相关Local-in会话。

```bash
session info: proto=6 proto_state=01 duration=9 expire=3590 timeout=3600 refresh_dir=both flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=164/3/1 reply=127/2/1 tuples=2
tx speed(Bps/kbps): 17/0 rx speed(Bps/kbps): 13/0
orgin->sink: org pre->in, reply out->post dev=3->9/9->3 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 202.103.12.1:18782->202.103.12.2:22(0.0.0.0:0)
hook=post dir=reply act=noop 202.103.12.2:22->202.103.12.1:18782(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
misc=0 policy_id=1 pol_uuid_idx=15846 auth_info=0 chk_client_info=0 vd=0
serial=00000092 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
no_ofld_reason:  local
```

5. 使用Debug Flow查看国外IP的SSH访问，流量被Local-in Policy（ID 2）阻断。

```bash
id=65308 trace_id=1 func=print_pkt_detail line=5888 msg="vd-root:0 received a packet(proto=6, 35.1.2.3:10648->35.1.2.1:22) tun_id=0.0.0.0 from port1. flag [S], seq 891389291, ack 0, win 29200"
id=65308 trace_id=1 func=init_ip_session_common line=6073 msg="allocate a new session-0000008c"
id=65308 trace_id=1 func=__vf_ip_route_input_rcu line=1999 msg="find a route: flag=80000000 gw-0.0.0.0 via root"
id=65308 trace_id=1 func=fw_local_in_handler line=618 msg="iprope_in_check() check failed on policy 2, drop"
```

举例3

在HA环境下，用户开启并配置了HA独立管理口，需要在HA独立管理口下配置Local-in Policy。

1. 查看FortiGate HA的独立管理口配置，独立管理口为internal1。

```bash
config system ha
    config ha-mgmt-interfaces
        edit 1
            set interface "internal1"
        next
    end
end
```

2. 在internal1上配置Local-in Policy，入接口无法选择HA独立管理口internal1。

```bash
FortiGate # config firewall local-in-policy
FortiGate (local-in-policy) # edit 1
new entry '1' added
FortiGate (1) # set intf ?
<string>    Please input string value.
any             Match any interface in the virtual domain.
dmz     interface
fortilink       interface
internal        interface
internal4       interface
internal5(to_FW2_90D_internal_12_13)    interface
l2t.root        interface
naf.root        interface
ssl.root(SSL VPN interface)     interface
to_Home_WAN1    interface
to_Home_WAN2    interface
wan1    interface
wan2    interface
```

3. 在HA独立管理口上配置Local-in Policy时，需要开启`ha-mgmt-intf-only`选项，配置为enable后，Local-in Policy可以在HA独立管理口上正常下发。

```bash
config firewall local-in-policy
    edit 1
        set ha-mgmt-intf-only enable
        set intf "internal1"
        set srcaddr "Beijing_LAB_88"
        set dstaddr "all"
        set service "HTTPS"
        set schedule "always"
    next
end
```

TTL Policy

通过配置TTL Policy，可以阻止具有较高TTL的攻击流量。此功能与Local-in Policy一样仅用于本地入向流量，不适用于穿越FortiGate接口的流量，使用srcintf设置本地入向流量命中的接口（不能用于HA独立管理口）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall ttl-policy
    edit <id>
        set status {enable | disable}
        set action {accept | deny}
        set srcintf <interface>
        set srcaddr <source_address> [source_address] ...
        set service <service_name> [service_name] ...
        set schedule <schedule_name>
        set ttl <value/range>
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Local-out流量控制

Local-out流量指的是源自FortiGate并发往外部目标地址的流量。这种流量可能来自Syslog、FortiAnalyzer日志记录、FortiGuard服务、远程认证等。默认情况下，Local-out流量根据当前路由表来查找用于流量的出接口。但有些情况下，查询路由表的结果可能是去往目标IP的路径有多个出接口负载，但只有其中一个接口可以正确的到达目标地址。这种情况下如果负载到了错误的出接口，那么业务就会出现问题。

很多类型的Local-out流量支持根据SD-WAN规则或手工指定的接口作为出接口。在手工指定出口接口时，也可以指定源IP地址。支持设置出接口的Local-out流量类型如下所示：

1. Security Fabric→外部连接器（External Resources）中的终端/身份（Endpoint/Identity，可通过CLI配置）、威胁来源等（Threat Feeds，可通过GUI和CLI配置）。
2. 日志中的FortiAnalyzer服务器、FortiAnalyzer Cloud服务器、FortiGate Cloud日志服务器、Syslog服务器等。（可通过GUI和CLI配置）
3. 系统DNS服务器、FortiGuard服务器、FortiSandbox服务器等。（可通过GUI和CLI配置）
4. LDAP服务器、TACACS+服务器、Radius服务器等。（可通过CLI配置）

> **重要**
>
> 如果FortiGate开启了多VDOM功能，以上内容中1、2、3需要在Global视图下配置，4需要在VDOM视图下配置。

Local-out流量配置

通过GUI配置

DNS流量

用户FortiGate设备路由表中有两条等价的默认路由，出接口分别为wan1和wan2，只有wan1可以正常到达DNS服务器，DNS流量默认情况下在wan1和wan2上负载，当负载到wan2时，DNS解析会失败。

```bash
FortiGate # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 172.22.5.1, wan2, [1/0]
                 [10/0] via 172.22.6.1, wan1, [1/0]
...
```

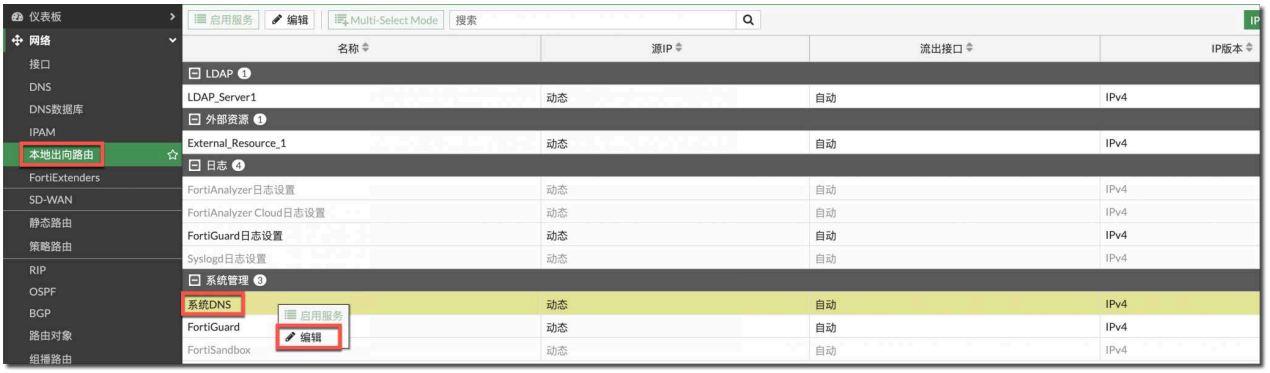
1. 在GUI上配置Local-out流量控制，首先要在“系统管理→可见功能”中开启“本地出向流量路由”。




```bash
config system global
    set gui-local-out enable
end
```

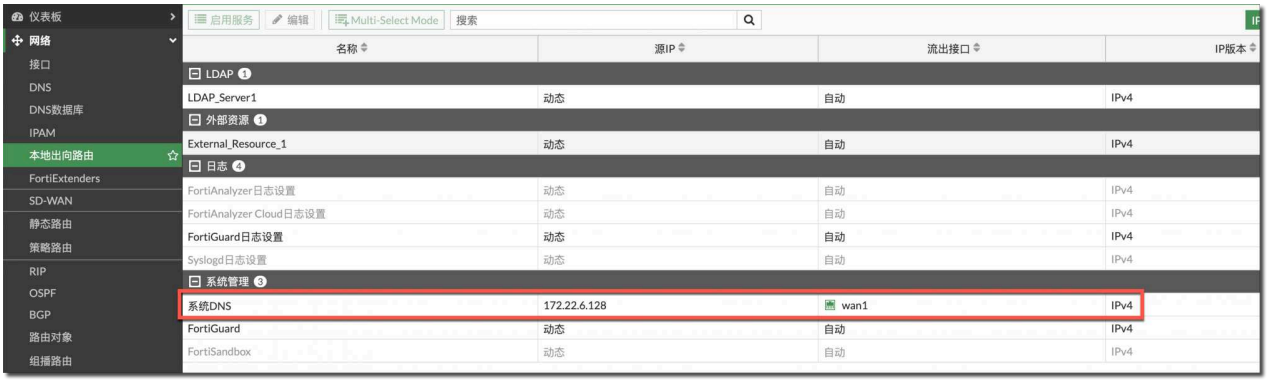
2. 进入网络→本地出向路由页面，编辑系统DNS选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置系统DNS的流出接口为指定模式，并选择wan1作为出接口（如果wan1上有多个IP，也可以修改源地址），点击确认下发配置。






```bash
config system dns
    set interface-select-method specify
    set interface "wan1"
end
```

LDAP流量

用户FortiGate设备路由表中有两条去往LDAP服务器所在网段的路由，出接口分别为internal4和internal5，只有internal5可以正常到达LDAP服务器，LDAP流量默认情况下在internal4和internal5上负载，当负载到internal4时，LDAP会无法访问。

```bash
FortiGate # get router info routing-table static

S       192.168.100.0/24 [10/0] via 10.10.12.2, internal4, [1/0]
                         [10/0] via 10.10.13.2, internal5, [1/0]
...
```

同时，LDAP服务器只允许FortiGate以10.10.12.111作为源IP访问。

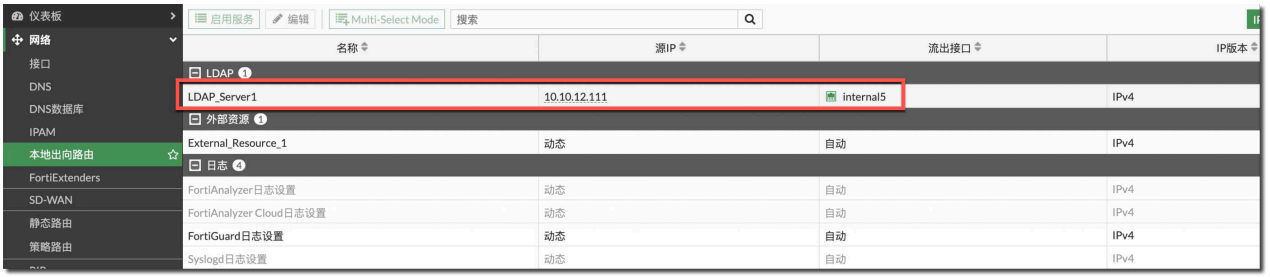
1. 进入网络→本地出向路由页面，编辑系统LDAP服务器选项（只有配置了LDAP/Radius/Tacacs+服务器后，才会在这里显示）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置系统LDAP服务器的流出接口为指定模式，并选择internal5作为出接口，选择源IP为手动模式，选择internal5接口的第二地址10.10.12.111，点击确认下发配置。






```bash
config user ldap
    edit "LDAP_Server1"
        set source-ip "10.10.12.111"
        set interface-select-method specify
        set interface "internal5"
    next
end
```

通过CLI配置

PING & Traceroute

ping和traceroute命令除了可以指定接口和源地址，也可以指定是否使用SD-WAN规则发送。

```bash
execute ping-options use-sdwan {yes | no}
execute ping6-options use-sd-wan {yes | no}
execute traceroute-options use-sdwan {yes | no}
```

集中管理

连接FortiManager进行集中管理的流量。

```bash
config system central-management
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
end
```

NTP服务器

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system ntp
    config ntpserver
        edit <id>
            set interface-select-method {auto | sdwan | specify}
            set interface <interface>
        next
    end
end
```

- `auto`：查找路由表进行转发。
- `sdwan`：查找SD-WAN规则或策略路由进行转发。
- `specify`：手工指定接口转发。
- `interface`：`interface-select-method`配置为`specify`时可用，用于手工指定流量的出接口。

DHCP代理

```bash
config system settings
    set dhcp-proxy-interface-select-method {auto | sdwan | specify}
    set dhcp-proxy-interface <interface>
end
```

DHCP中继

```bash
config system interface
    edit <interface>
        set dhcp-relay-interface-select-method {auto | sdwan | specify}
        set dhcp-relay-interface <interface>
    next
end
```

证书SCEP

```bash
config vpn certificate setting
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
    set source-ip <IP address>
end
```

IPS TLS协议探测

```bash
config ips global
    config tls-active-probe
        set interface-selection-method {auto | sdwan | specify}
        set interface <interface>
        set vdom <VDOM>
        set source-ip <IPv4 address>
        set source-ip6 <IPv6 address>
    end
end
```

- `VDOM`：当`interface-selection-method`设置为`sdwan`或`specify`时，可以指定流量的VDOM。

NetFlow/sFlow

```bash
NetFlow:
config system {netflow | vdom-netflow}
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
    set source-ip <IP address>
end

sFlow:
config system {sflow | vdom-sflow}
    config collectors
        edit <id>
            set interface-select-method {auto | sdwan | specify}
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set interface <interface>
            set source-ip <IP address>
        next
    end
end
```

FortiClient EMS

```bash
config endpoint-control fctems
    edit fctems1
        set interface-select-method {auto | sdwan | specify}
        set interface <interface>
        set source-ip <IP address>
    end
end
```

TACACS+

```bash
config log tacacs+accounting setting
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
    set source-ip <IP address>
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ISDB简介

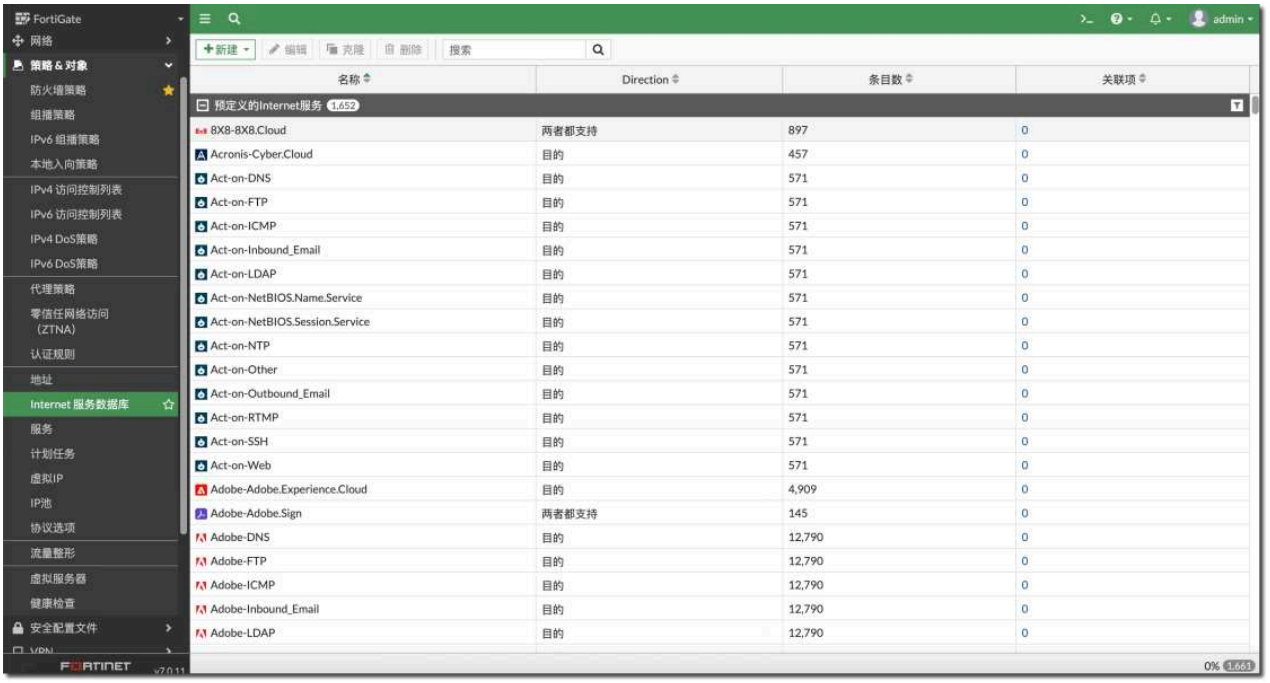
Internet Service Database（ISDB）是综合了IP地址范围、IP所有者、服务端口号、IP安全可信度的公网IP/服务数据库。该数据库来自FortiGuard系统，会定期更新，例如地理位置、IP声誉、知名度和DNS等。所有这些信息都有助于用户更有效地定义Internet安全，您可以使用数据库的内容作为策略中包含或排除的标准。

从 FortiOS 5.6开始，ISDB可以在防火墙策略中使用，但只能作为目标对象应用于策略。

从FortiOS 6.0开始，ISDB可以作为策略中的源对象和目标对象使用。您还可以将Internet服务应用于限速策略或SD-WAN策略。

您可以将三种类型的Internet服务应用于策略、静态路由、策略路由、SD-WAN规则：

- 预定义ISDB，进入FortiGate管理页面→策略&对象→Internet服务数据库，可以看到所有的预定义ISDB内容。



- 基于地址位置的ISDB，可在上述页面手动新建
- 自定义ISDB，只能通过CLI配置
- 扩展ISDB，只能通过CLI配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

预定义ISDB

本文主要介绍如何将预定义的ISDB条目应用到防火墙策略中。

配置步骤

重要

ISDB是一系列IP、协议、端口号的集合，所以配置后进行测试时，请使用ISDB中包含的协议、端口号进行测试，并不是只匹配到目标IP就会匹配到相关的ISDB。

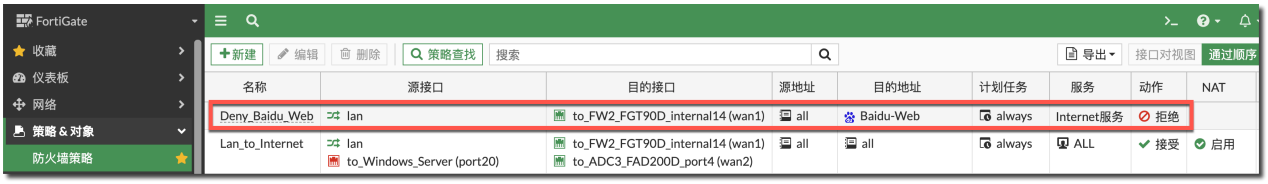
1. 通过Web方式访问防火墙的管理页面，进入“策略&对象→防火墙策略”页面，新建防火墙策略。
2. 配置流入接口和源地址，在“目标地址”选项中选择“Internet服务”，搜索“baidu”，选择“Baidu-Web”到目标地址中（该ISDB包含了所有百度的Web页面资源），动作选择“拒绝”，开启“记录拒绝流量”。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall policy
    edit 8
        set name "Deny_Baidu_Web"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "all"
        set internet-service enable
        set internet-service-name "Baidu-Web"
        set schedule "always"
        set logtraffic all
    next
end
```

3. 将该条策略移动至上网策略之前。

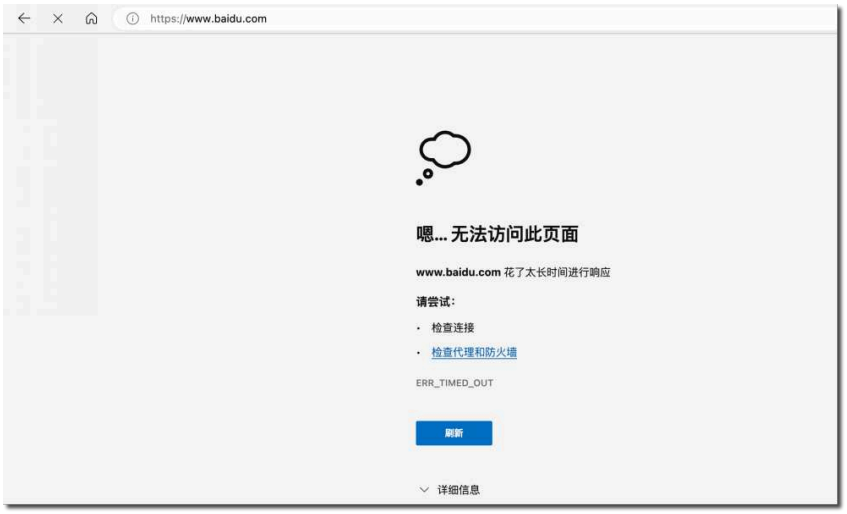


4. 使用“diagnose internet-service id 65646”可以看到该ISDB的详细信息，“diagnose internet-service id-summary 65646”可以看到该ISDB的简要信息。

```
diagnose internet-service id 65646
diagnose internet-service id-summary 65646
```

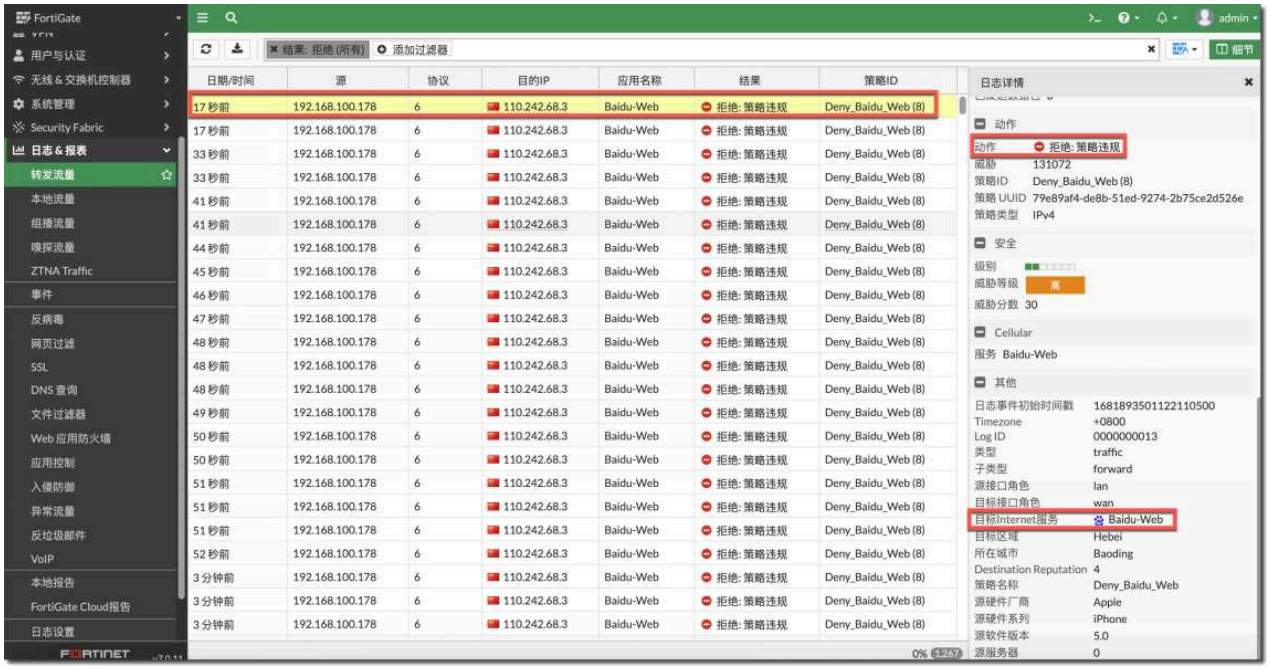
结果验证

1. 使用内网PC经过FortiGate访问网页https://www.baidu.com ↗ ，无法打开页面。



2. 查看防火墙的流量日志，可以看到客户端访问https://www.baidu.com ↗ 的流量被阻断，目标ISDB识别正确。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 由于策略中引用的ISDB Baidu-Web不包含ICMP服务，所以客户端仍然可以Ping通www.baidu.com ↗ 。

```
~ ifconfig en7
en7: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6467<RXCSUM,TXCSUM,VLAN_MTU,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 0c:37:96:06:d7:5d
        inet6 fe80::c9:55b5:f9f6:7b31%en7 prefixlen 64 secured scopeid 0xd
        inet 192.168.100.178 netmask 0xffffff00 broadcast 192.168.100.255
        inet 192.168.77.253 netmask 0xffffff00 broadcast 192.168.77.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (1000baseT <full-duplex>)
        status: active
~ ping www.baidu.com -c 5
PING www.a.shifen.com (110.242.68.4): 56 data bytes
64 bytes from 110.242.68.4: icmp_seq=0 ttl=51 time=10.831 ms
64 bytes from 110.242.68.4: icmp_seq=1 ttl=51 time=14.927 ms
64 bytes from 110.242.68.4: icmp_seq=2 ttl=51 time=10.963 ms
64 bytes from 110.242.68.4: icmp_seq=3 ttl=51 time=11.974 ms
64 bytes from 110.242.68.4: icmp_seq=4 ttl=51 time=10.716 ms

--- www.a.shifen.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 10.716/11.882/14.927/1.587 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

自定义ISDB

功能介绍

当预定义的ISDB中无法找到自己需要的ISDB时，可以使用自定义的ISDB（只能在CLI下配置），并应用在防火墙策略、限速策略、SD-WAN策略的目标中。

创建自定义的ISDB时，必须包含以下参数：

- IP地址或IP地址范围
- 协议号
- 端口号或端口号范围（如果是没有端口号的协议，则不需要填写，如ESP）
- 声誉级别（默认为3）

配置示例

```
config firewall internet-service-custom
    edit <name>
        set comment <comment>
        set reputation {1 | 2 | 3 | 4 | 5}
        config entry
            edit <ID>
                set protocol <protocol #>
                set dst <object_name>
                config port-range
                    edit <ID>
                        set start-port <port #>
                        set end-port <port #>
                    next
                end
            next
        end
    end
end
```

配置步骤

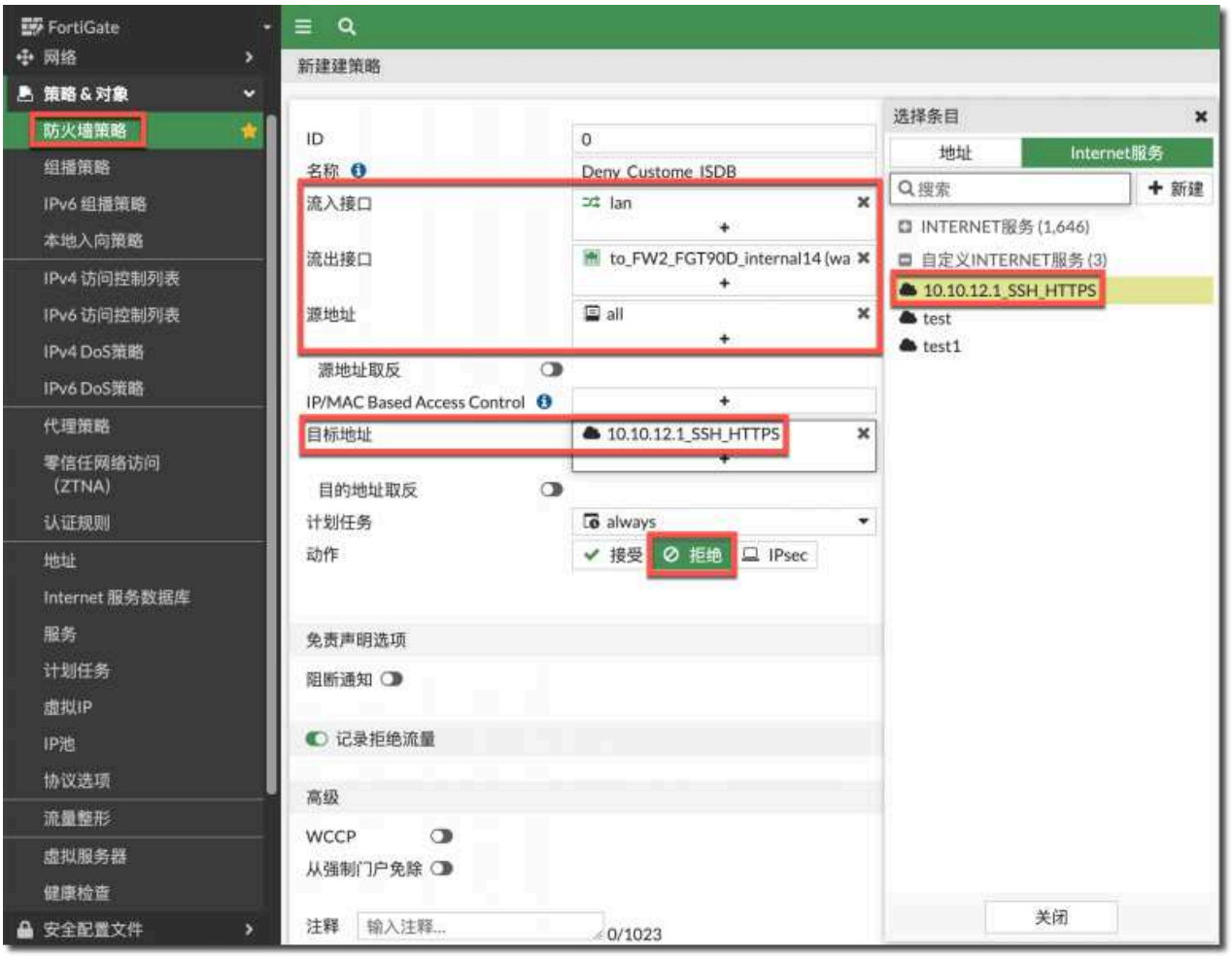
1. 配置目标的地址对象，并配置一条自定义的ISDB引用它们，协议为TCP的22端口和TCP的443端口。

```bash
config firewall address
    edit "10.10.12.1/32"
        set subnet 10.10.12.1 255.255.255.255
    next
end

config firewall internet-service-custom
    edit "10.10.12.1_SSH_HTTPS"
        set comment ''
        config entry
            edit 1
                set protocol 6
                config port-range
                    edit 1
                        set start-port 22
                        set end-port 22
                    next
                    edit 2
                        set start-port 443
                        set end-port 443
                    next
                end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

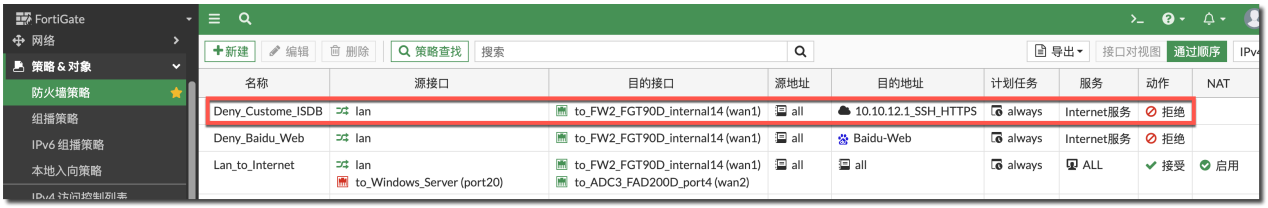
```
                set dst "10.10.12.1/32"
            next
        end
    next
end
```

2. 配置流入接口和源地址，在“目标地址”选项中选择“Internet服务”，在“自定义INTERNET服务”分类中，选择上步创建的自定义ISDB到目标地址中，动作选择“拒绝”，开启“记录拒绝流量”。




```
config firewall policy
    edit 9
        set name "Deny_Custome_ISDB"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "all"
        set internet-service enable
        set internet-service-custom "10.10.12.1_SSH_HTTPS"
        set schedule "always"
        set logtraffic all
    next
end
```

3. 将该条策略移动至上网策略之前。



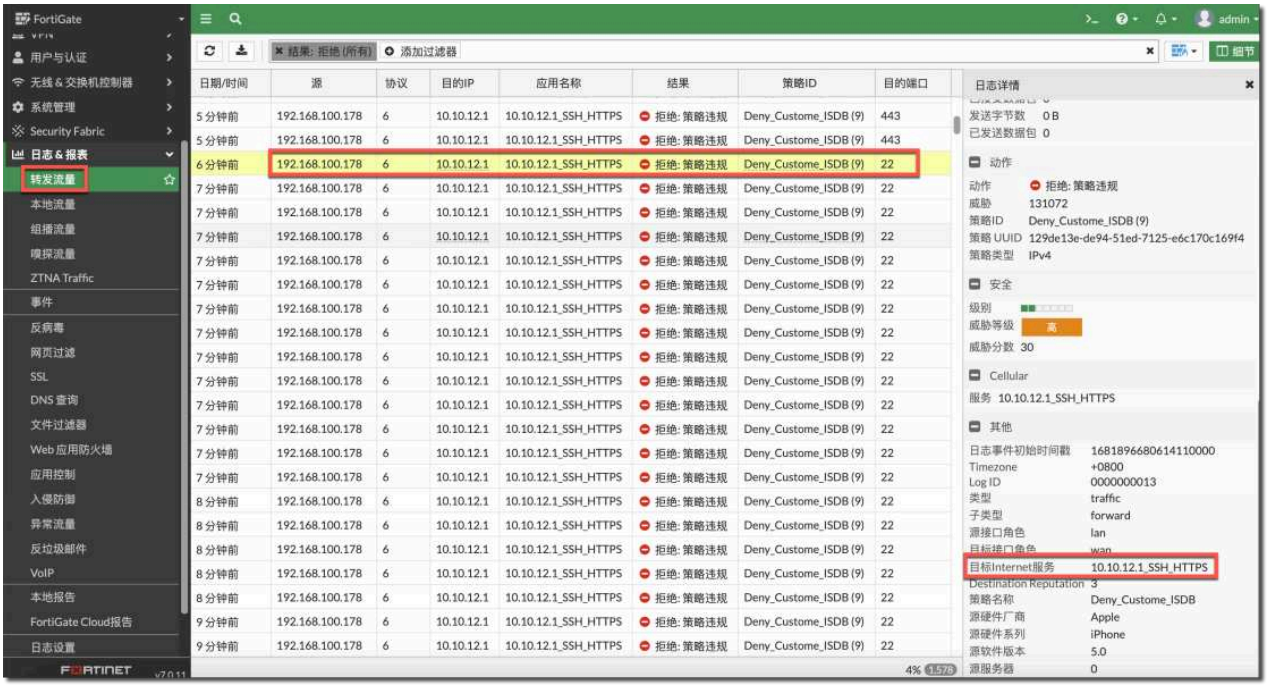
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

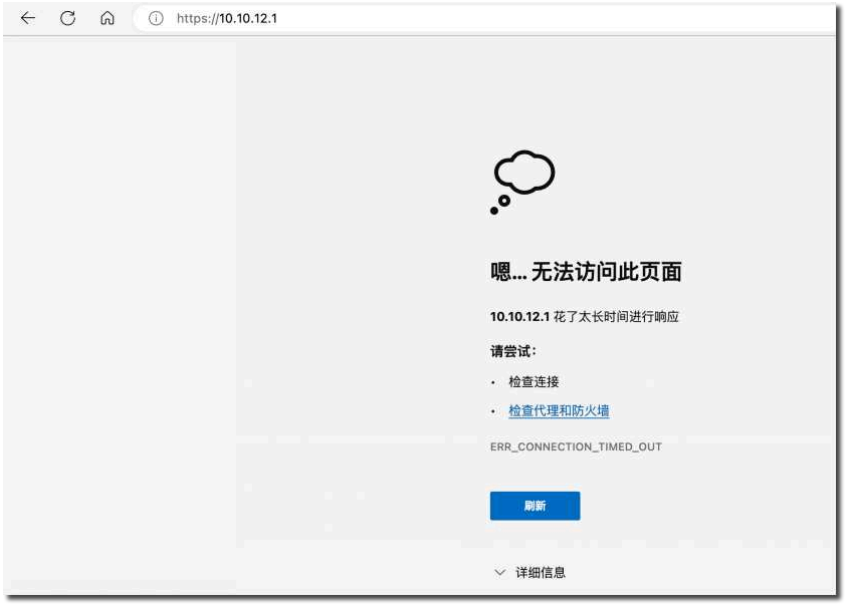
1. 使用内网PC经过FortiGate访问10.10.12.1的SSH（TCP port22）服务，无法访问。

```
✘ ~ ifconfig en7
en7: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6467<RXCSUM,TXCSUM,VLAN_MTU,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 0c:37:96:06:d7:5d
        inet6 fe80::c9:55b5:f9f6:7b31%en7 prefixlen 64 secured scopeid 0xd
        inet 192.168.100.178 netmask 0xffffff00 broadcast 192.168.100.255
        inet 192.168.77.253 netmask 0xffffff00 broadcast 192.168.77.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (1000baseT <full-duplex>)
        status: active
~ ssh admin@10.10.12.1
ssh: connect to host 10.10.12.1 port 22: Operation timed out
```

2. 查看防火墙的流量日志，可以看到客户端访问10.10.12.1的SSH流量被阻断，目标ISDB识别正确。

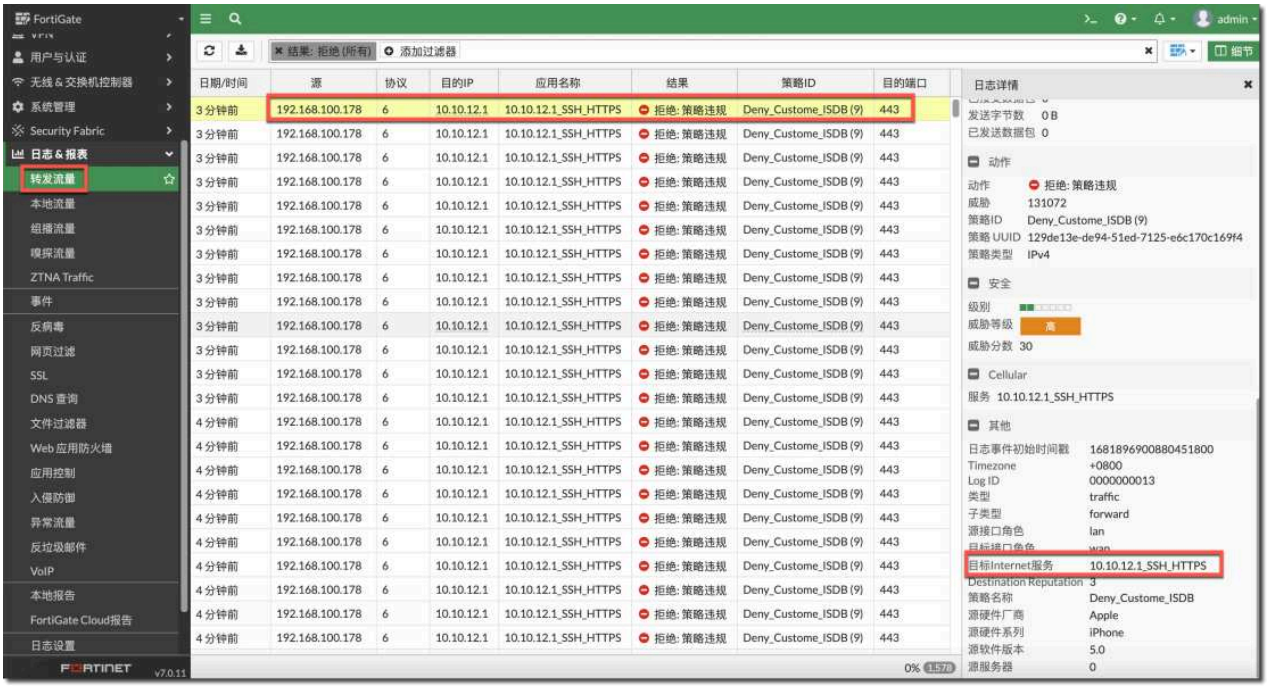


3. 使用内网PC经过FortiGate访问10.10.12.1的HTTPS（TCP port 443）服务，被阻断。



4. 查看防火墙的流量日志，可以看到客户端访问10.10.12.1的HTTPS流量被阻断，目标ISDB识别正确。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

扩展ISDB

功能介绍

扩展ISDB允许您对现有的预定义ISDB中配置的IP和端口范围进行增加，实际上是编辑预定义类型的ISDB条目，并向其添加IP地址和端口范围。

扩展ISDB必须在CLI下配置，创建扩展的ISDB时，必须包含以下参数：

- IP地址或IP地址范围
- 协议号
- 端口号或端口号范围（如果是没有端口号的协议，则不需要填写，如ESP）

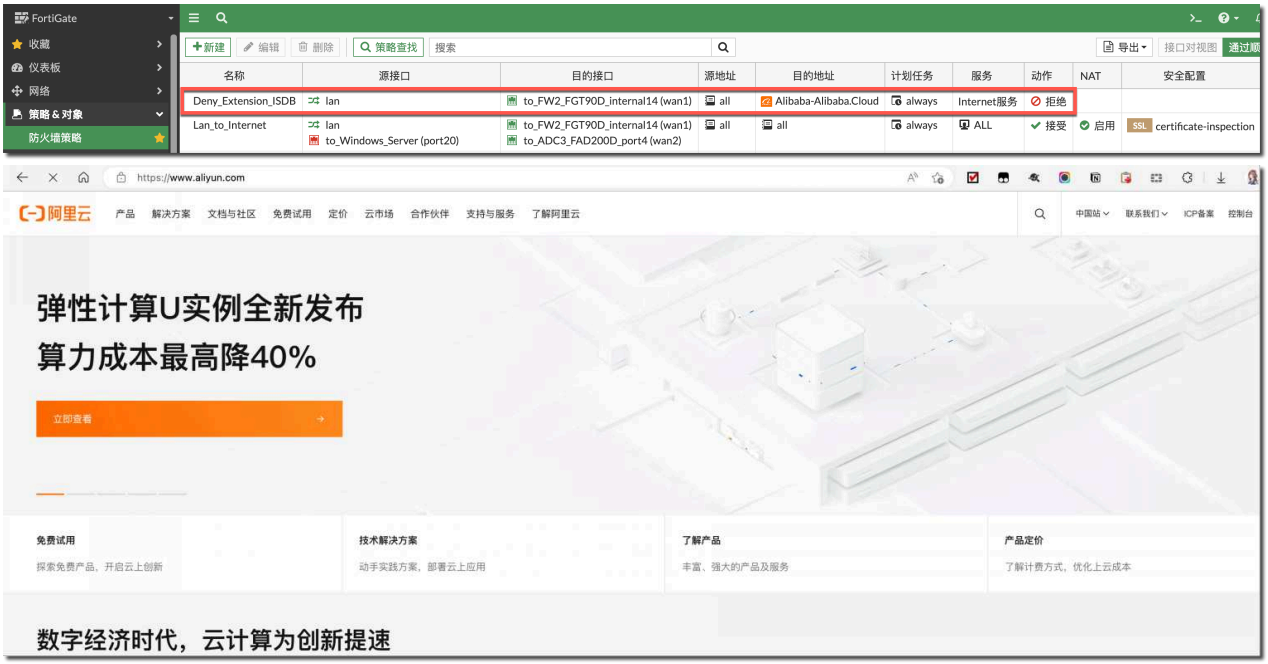
删除时必须从GUI的预定义ISDB中删除相关条目。

配置示例

```
config firewall internet-service-extension
    edit <ID #>
        set comment <comment>
        config entry
            edit <ID #>
                set protocol <number #>
                set dst <object_name>
                config port-range
                    edit <ID #>
                        set start-port <number #>
                        set end-port <number #>
                    next
                end
            next
        end
    end
end
```

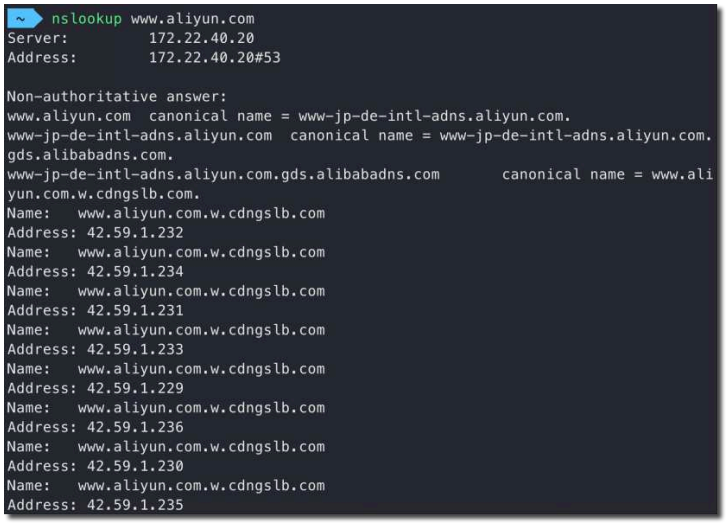
网络需求

1. 用户想禁止内网访问阿里云相关资源的流量，配置了安全策略阻断去往预定义ISDB“Alibaba-Alibaba.Cloud”的流量。
2. 但由于阿里云域名对应的IP一直在变化，预定义的ISDB还未来得及更新最新的IP地址和端口号，导致阿里云的个别资源仍然可以正常访问（如www.aliyun.com ↗ ）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 通过域名解析，找到仍然可以访问的资源为42.59.1.232、42.59.1.234、42.59.1.231、42.59.1.233、42.59.1.229、42.59.1.236、42.59.1.230、42.59.1.235的443端口。



4. 查看解析到的IP所属的预定义ISDB，可以看到没有属于任何一个预定义的ISDB。

```
FortiGate # diagnose internet-service info root 6 443 42.59.1.235
Can not find Internet Service ID and name. ret=-1
```

5. 解决方法是通过在预定义的ISDB上使用扩展ISDB，以扩充预定义的ISDB。

配置步骤

1. 配置需要在预定义的ISDB上扩展的IP资源的地址和地址组对象。

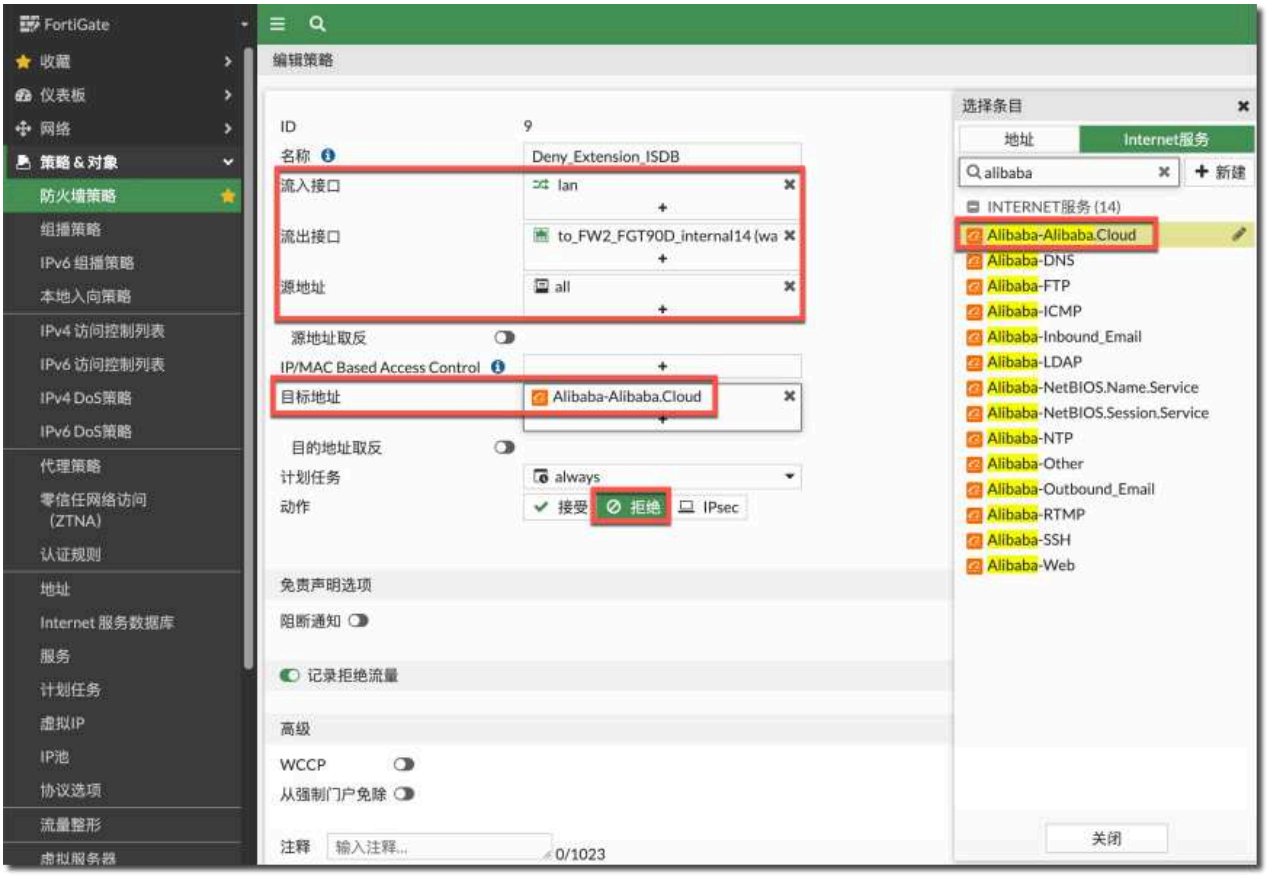
```
config firewall address
    edit "AliCloud_1"
        set subnet 42.59.1.232 255.255.255.255
    next
    edit "AliCloud_2"
        set subnet 42.59.1.234 255.255.255.255
    next
    edit "AliCloud_3"
        set subnet 42.59.1.231 255.255.255.255
    next
    edit "AliCloud_4"
        set subnet 42.59.1.233 255.255.255.255
    next
    edit "AliCloud_5"
        set subnet 42.59.1.229 255.255.255.255
    next
    edit "AliCloud_6"
        set subnet 42.59.1.236 255.255.255.255
    next
    edit "AliCloud_7"
        set subnet 42.59.1.230 255.255.255.255
    next
    edit "AliCloud_8"
        set subnet 42.59.1.235 255.255.255.255
    next
end
config firewall addrgrp
    edit "AliCloud_extension"
        set member "AliCloud_1" "AliCloud_2" "AliCloud_3" "AliCloud_4" "AliCloud_5" "AliCloud_6" "AliCloud_7"
"AliCloud_8"
    next
end
```

2. 配置一条扩展的ISDB，edit的ID填写预定义的ISDB“Alibaba-Alibaba.Cloud”的ID号（该ID号可以在GUI中查询），引用上步配置的地址组，协议为TCP，端口号为443端口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall internet-service-extension
    edit 6881402
        set comment ''
        config entry
            edit 1
                set protocol 6
                config port-range
                    edit 1
                        set start-port 443
                        set end-port 443
                    next
                end
                set dst "AliCloud_extension"
            next
        end
    next
end
```

3. 防火墙策略中配置流入接口和源地址，在“目标地址”选项中选择“Internet服务”，在“INTERNET服务”分类中，选择预定义的ISDB“Alibaba-Alibaba.Cloud”，动作选择“拒绝”，开启“记录拒绝流量”。




```
config firewall policy
    edit 9
        set name "Deny_Extension_ISDB"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "all"
        set internet-service enable
        set internet-service-name "Alibaba-Alibaba.Cloud"
        set schedule "always"
        set logtraffic all
    next
end
```

4. 将该条策略移动至上网策略之前。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

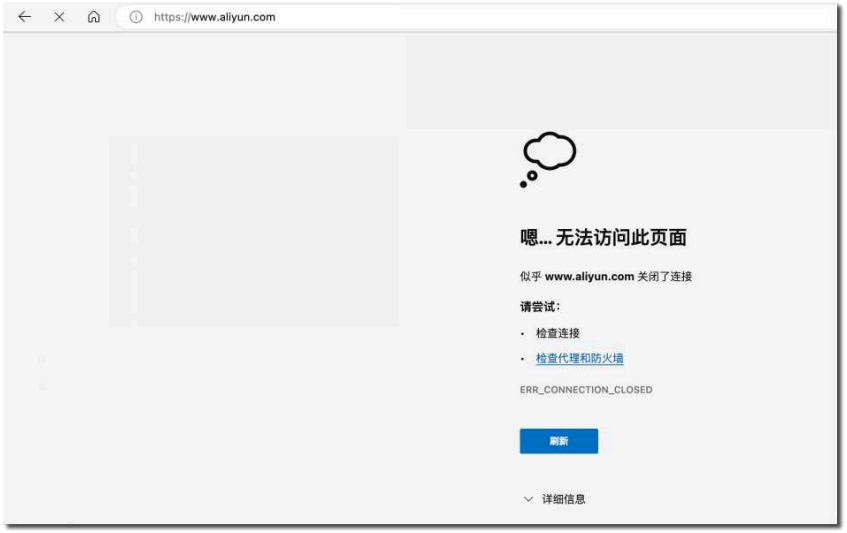


结果验证

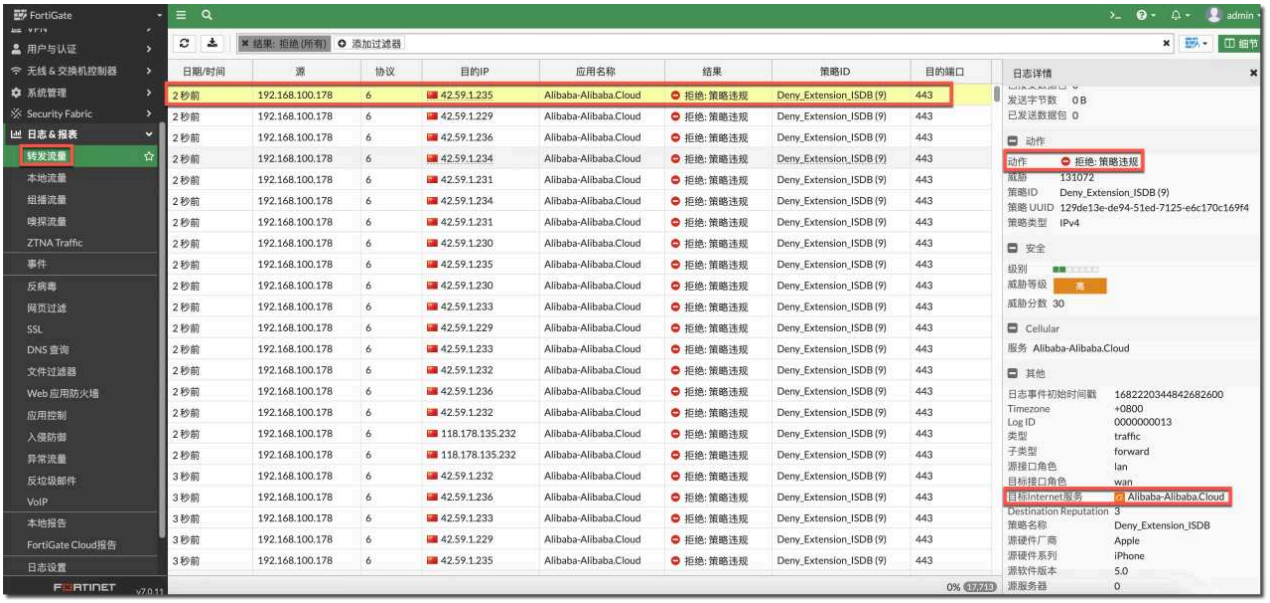
1. 查询手动扩展的IP和端口所属的ISDB，可以看到已被归类到预定义的ISDB“Alibaba-Alibaba.Cloud”中。

```
FortiGate # diagnose internet-service info root 6 443 42.59.1.235
Internet Service: 6881402(Alibaba-Alibaba.Cloud) country(0 Any) region(0 Any) city(0 Any)
```

2. 使用内网PC经过FortiGate访问www.aliyun.com，被阻断。



3. 查看防火墙的流量日志，可以看到客户端访问10.10.12.1的HTTPS流量被阻断，目标ISDB识别正确。



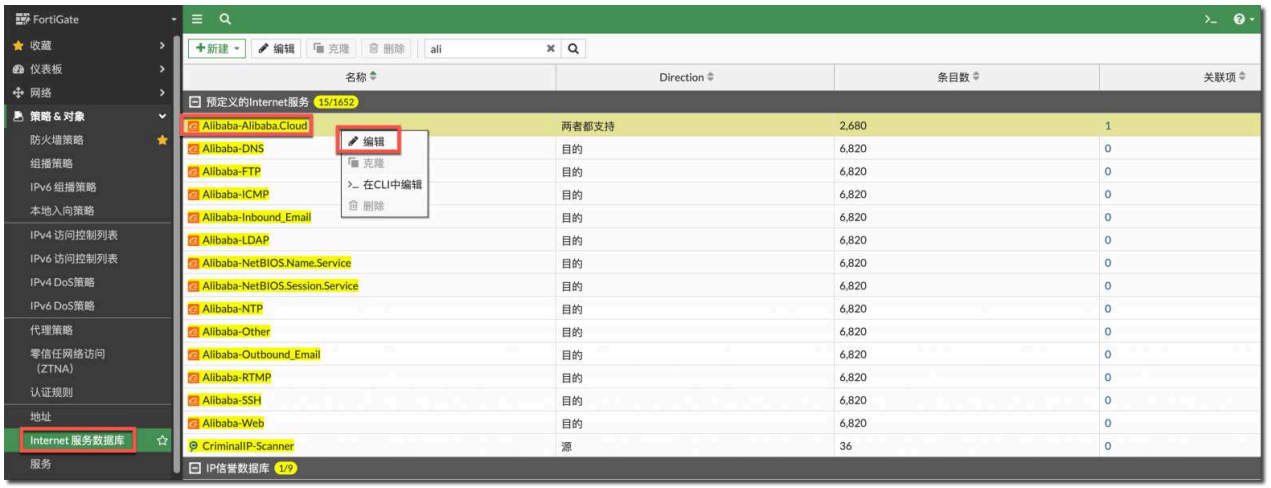
禁用预定义ISDB中的IP/端口

1. 首先查询某个属于预定义ISDB“Alibaba-Alibaba.Cloud”的IP/端口。

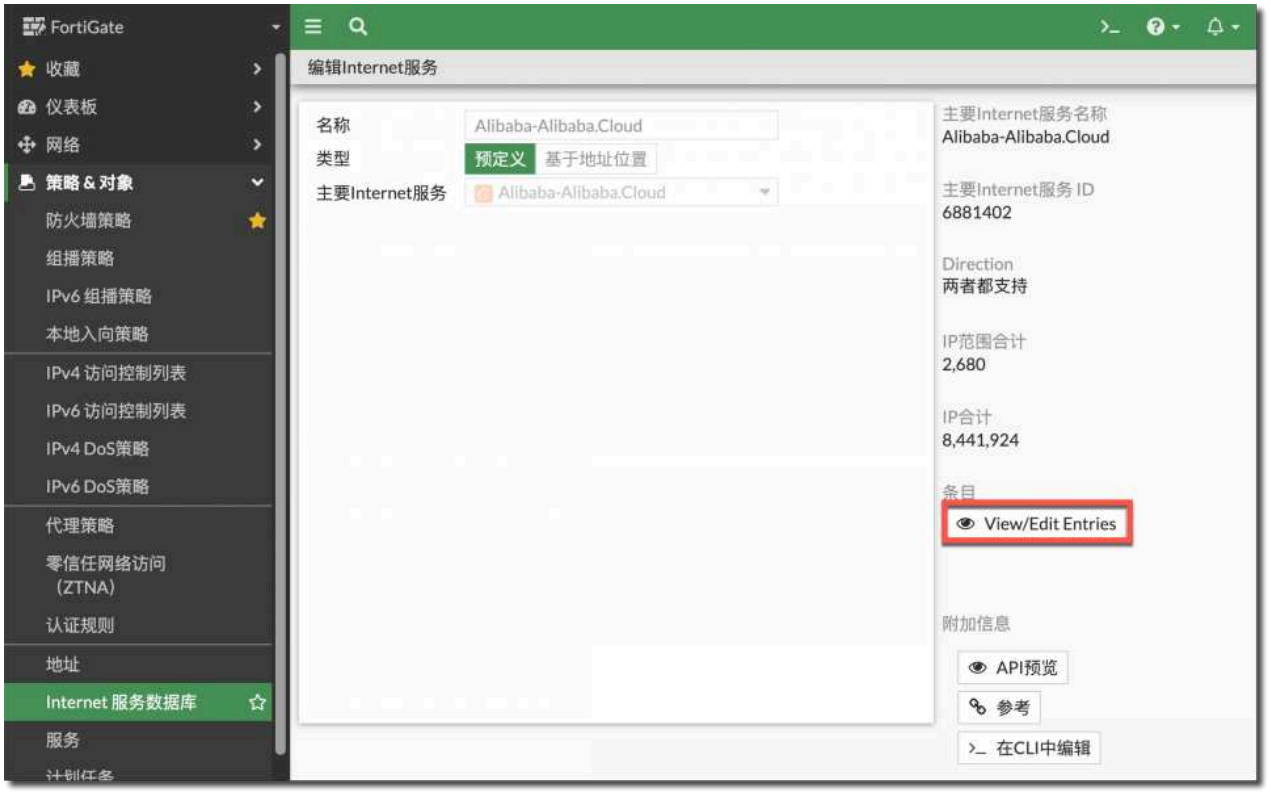
```
FortiGate # diagnose internet-service info root 6 443 223.109.11.27
Internet Service: 6881402(Alibaba-Alibaba.Cloud) country(156 China) region(801 Jiangsu) city(26800 Wuxi)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 进入“策略&对象→Internet服务数据库”，编辑要删除内容的预定义ISDB，这里以“Alibaba-Alibaba.Cloud”为例，双击或邮件选择“编辑”。

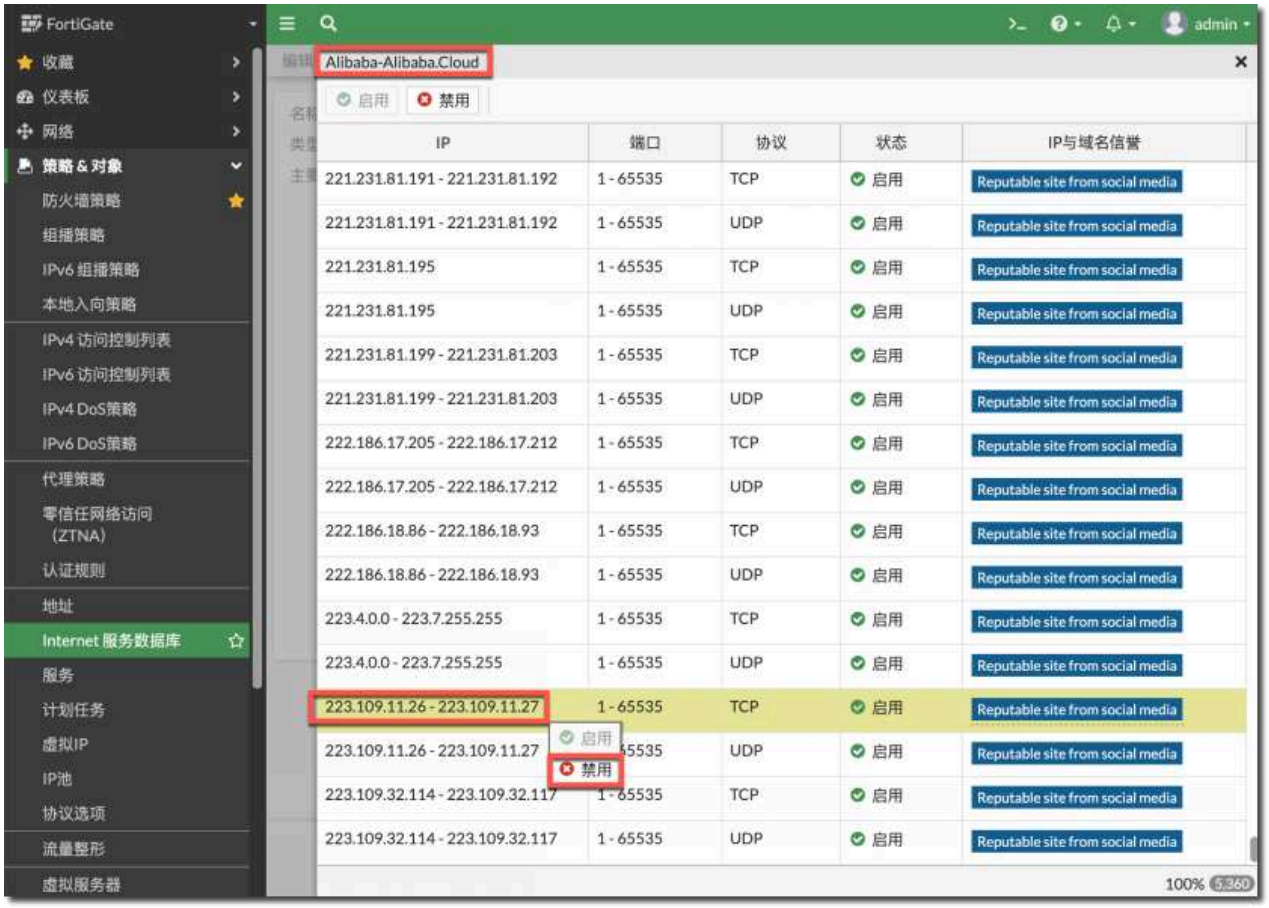


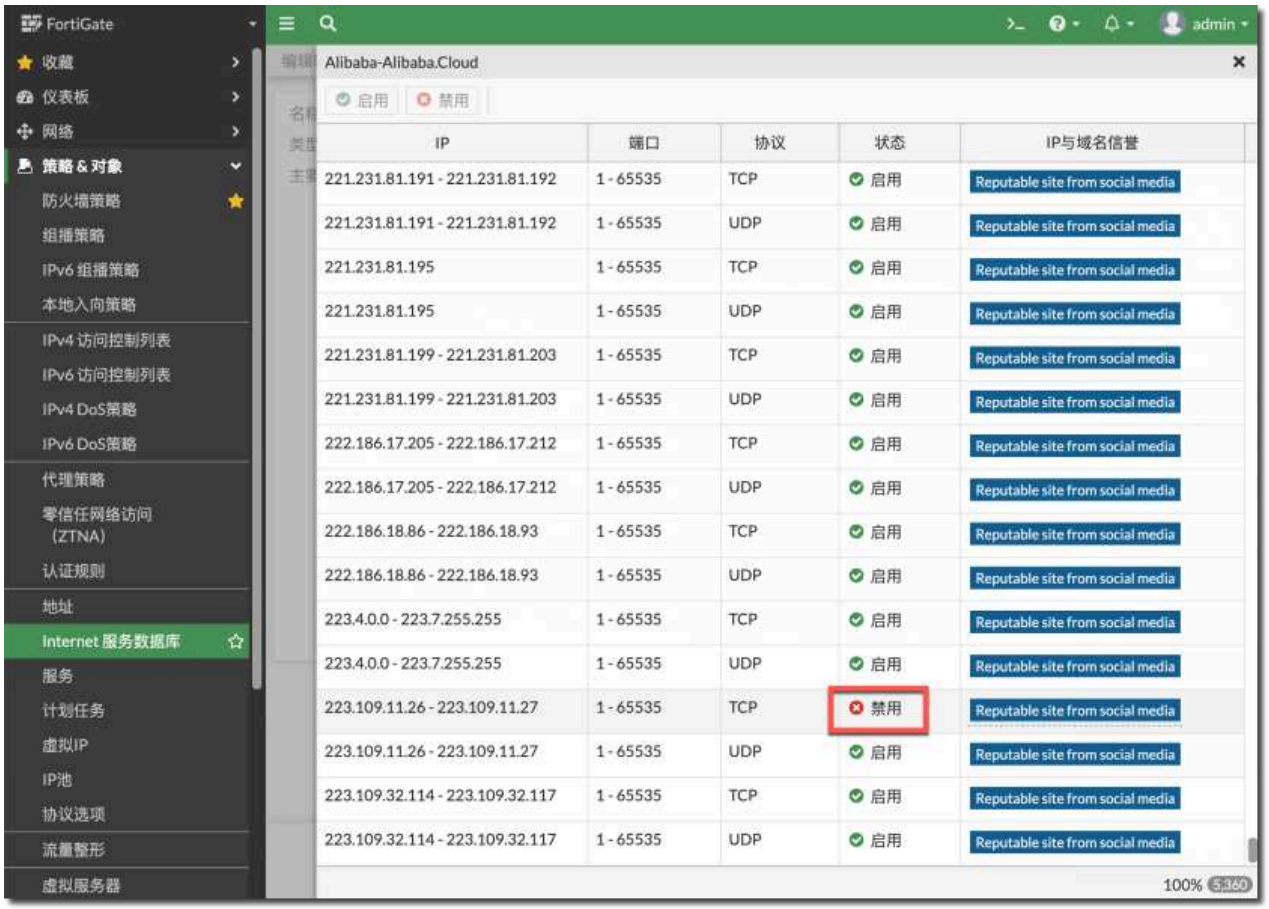
3. 点击页面右侧的“View/Edit Entries”，



4. 右键禁用IP/端口所属的条目。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





5. 再次查询该IP地址/端口所属的ISDB，可以看到没有属于任何ISDB。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose internet-service info root 6 443 223.109.11.27
Can not find Internet Service ID and name. ret=-1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IP信誉级别

功能介绍

ISDB中目前有五个信誉级别，可以在自定义ISDB中定义信誉级别。您可以配置防火墙策略以根据所需的信誉级别过滤流量。如果IP地址的信誉级别 ≥ 策略中设置的级别，则会转发数据包，否则将丢弃数据包。

五个信誉级别如下所示：

信誉级别	
1	已知的恶意站点，例如网络钓鱼站点或与僵尸网络服务器相关的站点
2	高风险服务站点，例如TOR、代理和P2P
3	未经证实的网站
4	信誉良好的社交媒体网站，如Facebook和Twitter
5	已知和经过验证的安全网站，例如Gmail、Amazon、eBay和淘宝

重要

防火墙策略中，默认最低信誉级别为0，表示未启用信誉过滤器。

对于未包含在ISDB中的IP地址，默认信誉级别为3。

默认信誉方向是基于目标IP的（可在策略中修改为基于源地址）。

配置举例

举例一

```
config firewall policy
    edit 1
        set srcintf "wan2"
        set dstintf "port1"
        set srcaddr “all”
        set dstaddr "all"
        set reputation-minimum 3
        set reputation-direction source
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

重要

来自信誉级别为3、4、5的源IP地址的数据包将匹配此策略。

举例二

```
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "wan2"
        set srcaddr “all”
        set dstaddr "all"
        set reputation-minimum 4
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set reputation-direction destination
        set action accept
        set schedule "always"
        set service "FTP"
        set nat enable
    next
end
```

重要

如果流量目标的IP信誉级别为4或5，且服务为FTP，则会匹配此策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于地理位置的ISDB

功能介绍

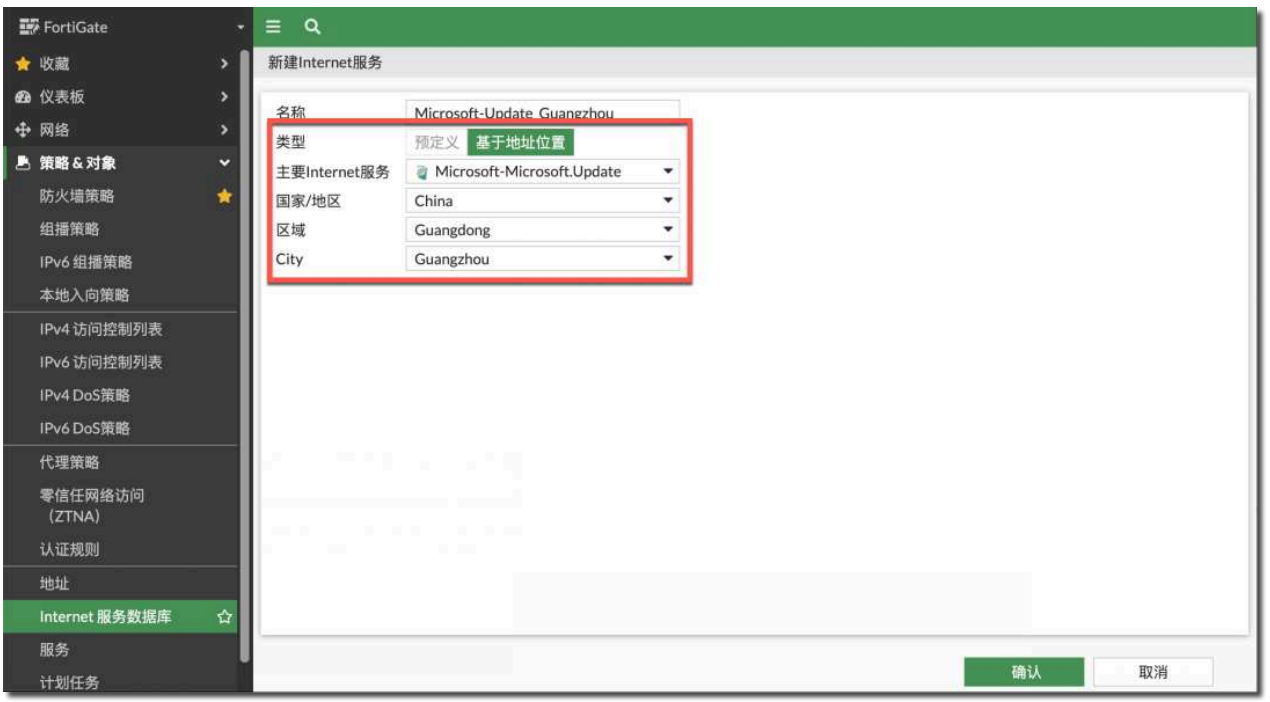
基于地理位置的ISDB允许用户定义国家/地区和城市。这些对象可以在防火墙策略、限速策略、SD-WAN规则中使用，以便对ISDB的位置进行更精细的控制。

配置步骤

1. 进入“策略&对象→Internet服务数据库”，点击“新建”按钮，选择“基于国家和地区的Internet”服务。



2. 按需配置主要的Internet服务，以及限定的国家/地区、区域和城市，下发配置。如下图所示为微软的更新服务ISDB，限定IP的地理位置在中国广东省广州市。

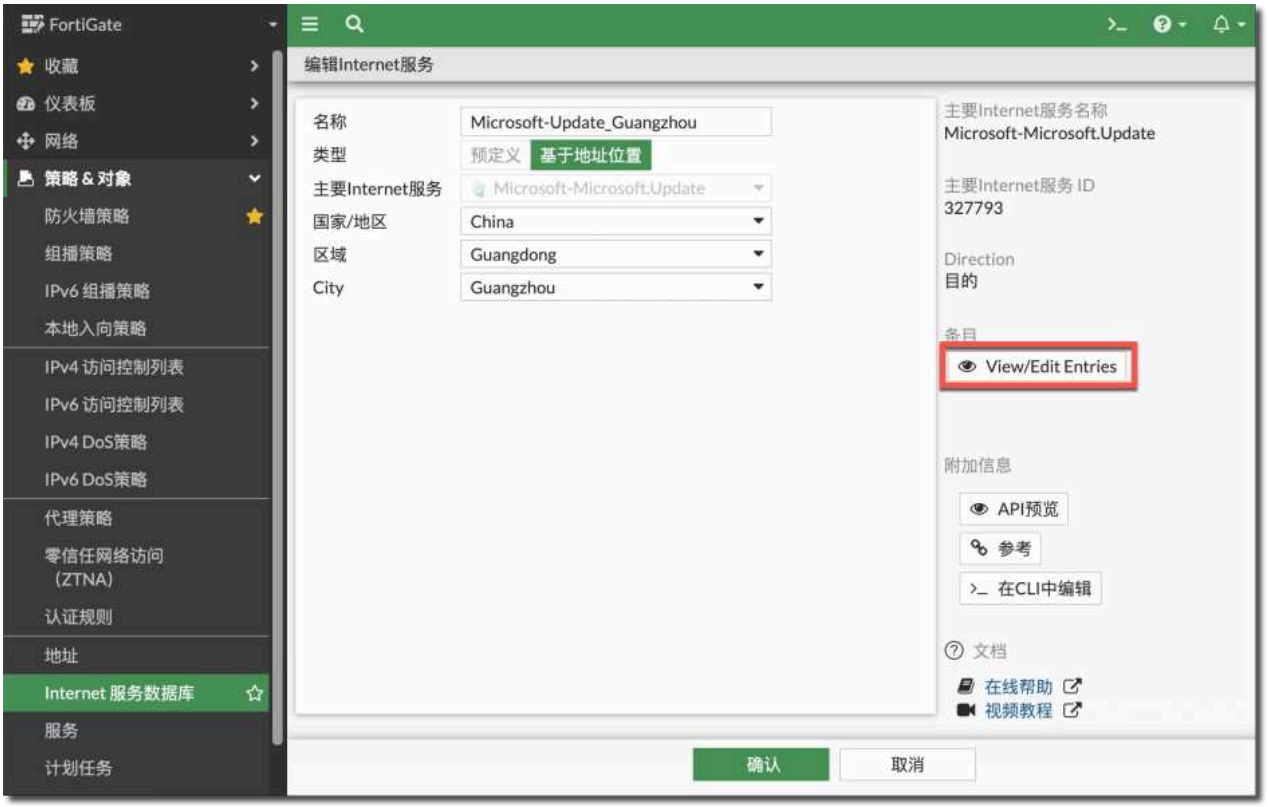


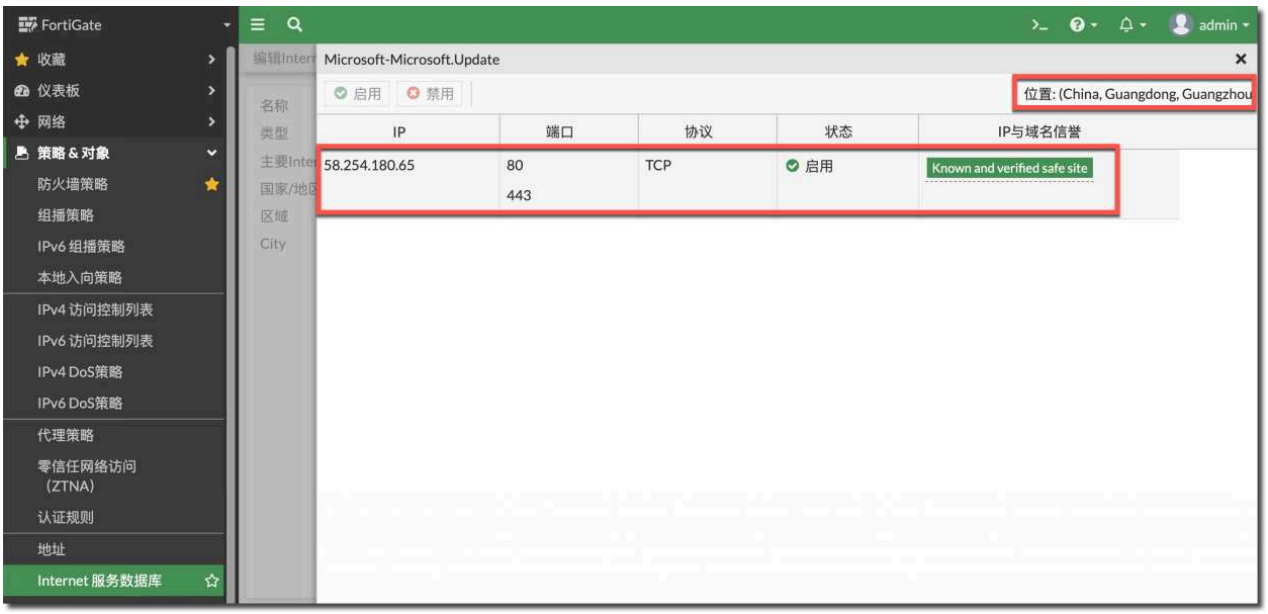

```
config firewall internet-service-name
    edit "Microsoft-Update_Guangzhou"
        set type location
        set internet-service-id 327793
        set country-id 156
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set region-id 628
        set city-id 9028
    next
end
```

3. 编辑上步配置的基于地理位置的ISDB，点击右侧的“View/Edit Entries”，可以查看该ISDB包含的IP/端口库。



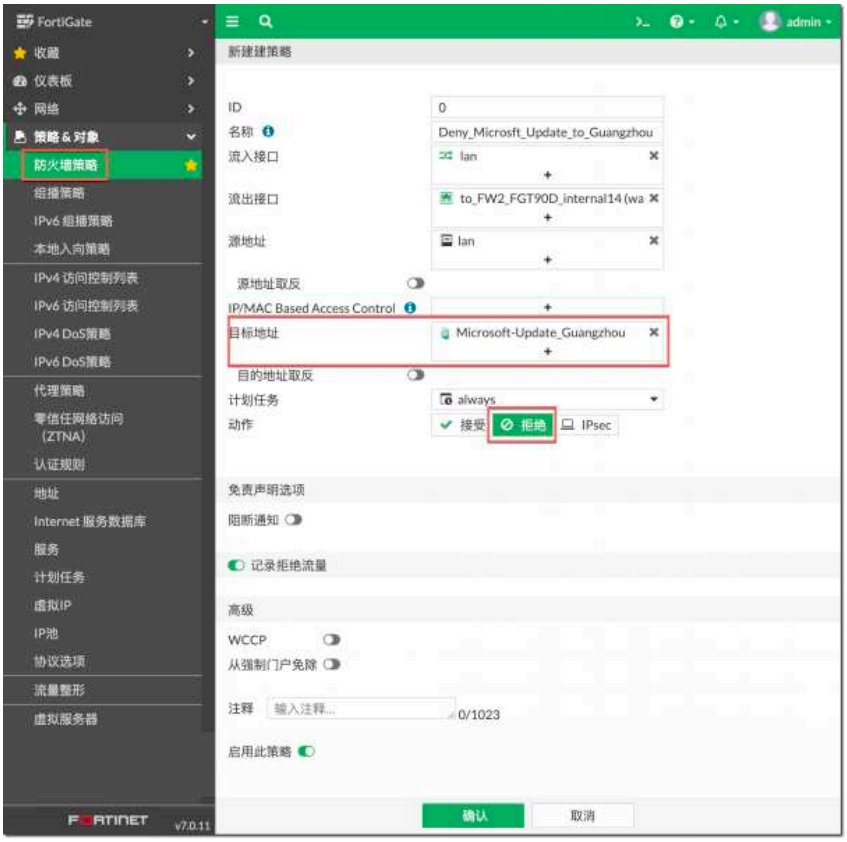


4. CLI下使用调试命令查看该ISDB属于广州的IP条目。

```
FortiGate # diagnose internet-service id 327793 | grep "country(156) region(628) city(9028)"
58.254.180.65-58.254.180.65 country(156) region(628) city(9028) blocklist(0×0) reputation(5), popularity(5)
domain(0) botnet(0) proto(6) port(80 443)
```

5. 新建防火墙安全策略，在目的中引用该ISDB，禁止访问该ISDB所属资源的流量。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall policy
    edit 6
        set name "Deny_Microsft_Update_to_Guangzhou"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "lan"
        set internet-service enable
        set internet-service-name "Microsoft-Update_Guangzhou"
        set schedule "always"
        set logtraffic all
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ISDB端口附加配置

功能介绍

1. 通过在CLI下配置“internet-service-append”，我们可以将包含指定端口的预定义ISDB服务，自动附加其他指定端口。
2. 举例：客户需要将所有包含443端口的ISDB中自动附加端口10443。

配置步骤

1. 配置前，查询某个IP + 端口的所属ISDB，可以看到110.242.68.4 + Port 443属于“Baidu-Web”，而110.242.68.4 + Port 10443属于“Baidu-Other”。

```
FortiGate # diagnose internet-service info root 6 443 110.242.68.4
Internet Service: 2883585(Baidu-Web) country(156 China) region(688 Hebei) city(1692 Baoding)

FortiGate # diagnose internet-service info root 6 10443 110.242.68.4
Internet Service: 2883584(Baidu-Other) country(156 China) region(688 Hebei) city(1692 Baoding)
```

2. 在CLI下配置“internet-service-append”，一下配置表示只要某个预定义的ISDB中包含的端口匹配“match-port”配置的端口443，则会将“append-port”配置的端口10443附加在这个ISDB中，该配置在全局的预定义ISDB中生效。

> **重要**
>
> 不包含具体端口的ISDB不会匹配“match-port”配置的端口。

```
config firewall internet-service-append
    set match-port 443
    set append-port 10443
end
```

3. 需要使用如下命令重载ISDB。

```
execute internet-service refresh
```

4. 再次查询110.242.68.4 + Port 10443端口所属的ISDB，已经变为“Baidu-Web”，但不再属于“Baidu-Other”。

```
FortiGate # diagnose internet-service info root 6 10443 110.242.68.4
Internet Service: 2883585(Baidu-Web) country(156 China) region(688 Hebei) city(1692 Baoding)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

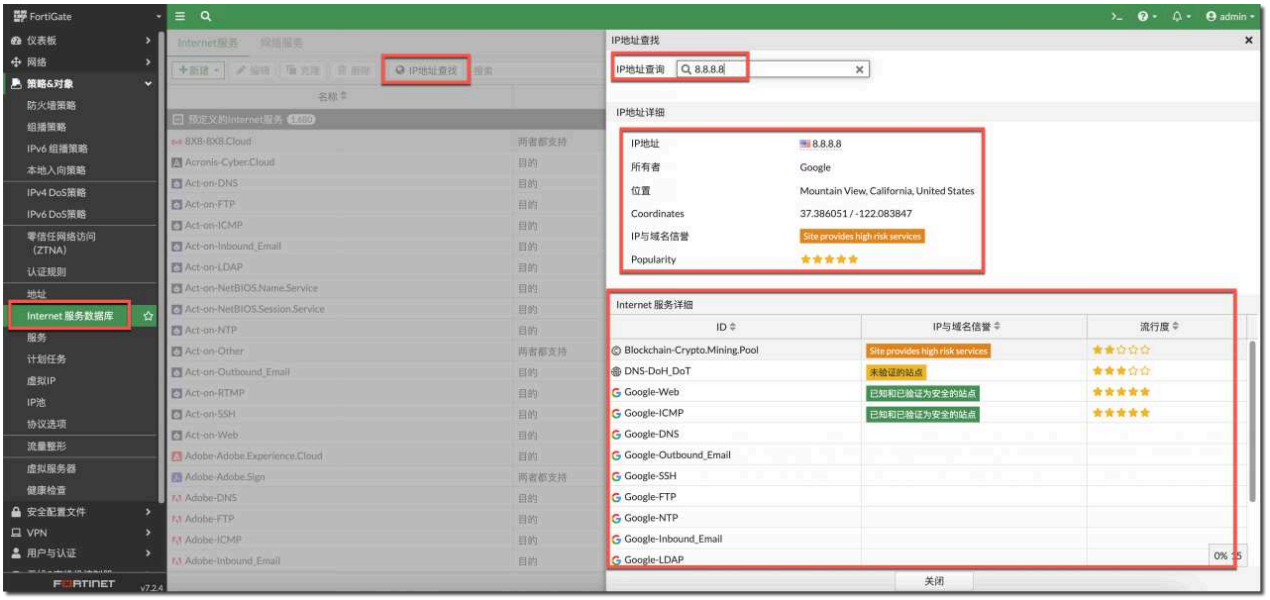
查询ISDB/地理位置信息

用户可以从ISDB库/GEO库中查找IP地址所属ISDB以及地理位置信息。返回的IP地址信息包括所属ISDB、位置、信誉和其他服务信息。

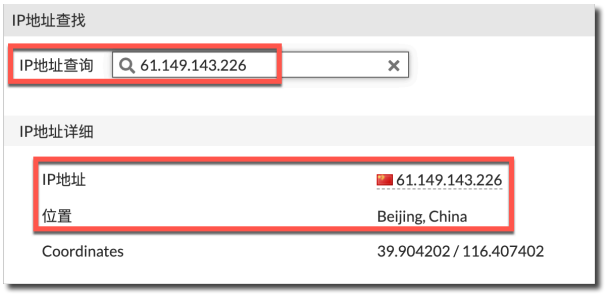
通过GUI查询

> **重要**
>
> GUI方式查询需FortiOS 7.2.0及更高版本支持。

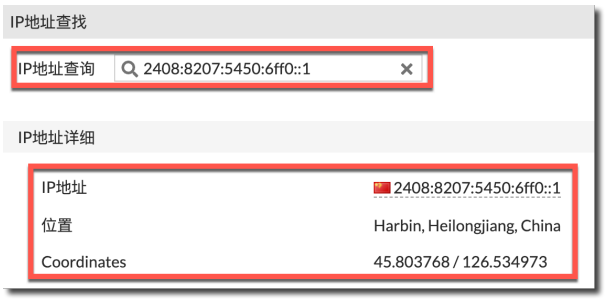
1. 进入“策略&对象→Internet服务数据库”，点击“IP地址查找”按钮，填写IPv4地址，可以查找到该IP所属的ISDB信息以及地理位置信息。



2. 查找一个不属于ISDB库的IP地址，也可以显示地理位置信息。



3. 同时也支持IPv6的查询。



通过CLI查询

1. 查询对应流量所属的ISDB，可以查询更精细的协议和端口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
diagnose internet-service info <vdname> <protocol> <port> <ip>
```

```
FortiGate # diagnose internet-service info root 6 443 110.242.68.4
Internet Service: 2883585(Baidu-Web) country(156 China) region(688 Hebei) city(1692 Baoding)
```

2. 查询某个ISDB ID包含的资源库具体列表，这里以Google.Web ↗（65537）为例。

```
diagnose internet-service id 65537
```

3. 查询某个ISDB的汇总信息，这里以Google.Web ↗（65537）为例。

```
FortiGate # diagnose internet-service id-summary 65537
Version: 00007.03214
Timestamp: 202305221646
Total number of IP ranges: 1192387
Number of Groups: 24
Group(0), Singularity(90), Number of IP ranges(2877)
Group(1), Singularity(89), Number of IP ranges(273689)
Group(2), Singularity(88), Number of IP ranges(49676)
Group(3), Singularity(87), Number of IP ranges(22743)
Group(4), Singularity(86), Number of IP ranges(16913)
Group(5), Singularity(85), Number of IP ranges(29777)
Group(6), Singularity(84), Number of IP ranges(5120)
Group(7), Singularity(83), Number of IP ranges(1290)
Group(8), Singularity(82), Number of IP ranges(266)
Group(9), Singularity(80), Number of IP ranges(93)
Group(10), Singularity(20), Number of IP ranges(886)
Group(11), Singularity(19), Number of IP ranges(990)
Group(12), Singularity(18), Number of IP ranges(7498)
Group(13), Singularity(17), Number of IP ranges(5855)
Group(14), Singularity(16), Number of IP ranges(10700)
Group(15), Singularity(15), Number of IP ranges(129919)
Group(16), Singularity(11), Number of IP ranges(412)
Group(17), Singularity(10), Number of IP ranges(197733)
Group(18), Singularity(9), Number of IP ranges(8129)
Group(19), Singularity(8), Number of IP ranges(3857)
Group(20), Singularity(7), Number of IP ranges(46816)
Group(21), Singularity(6), Number of IP ranges(183359)
Group(22), Singularity(5), Number of IP ranges(184276)
Group(23), Singularity(4), Number of IP ranges(9513)
Internet Service: 65537(Google-Web)
Number of IP ranges: 22984
Number of IP addresses: 19527487
Singularity: 6
Icon Id: 1
Direction: dst
Data source: isdb
```

4. 通过本地GEO库查询某个IP的地理位置信息。

```
FortiGate # diagnose internet-service id 65537 | grep 8.8.8.8

FortiGate # diagnose geoip ip2country 61.149.143.226
61.149.143.226 - China, is not anycast ip
```

5. 通过FortiGuard GEO库查询某个IP的地理位置信息（需要FortiGate可以连接到Internet），查询到的地理位置信息更为详细。

```
FortiGate # diagnose geoip geoip-query 61.149.143.226
IP:61.149.143.226
{
  "city":{
    "geoname_id":10175057,
    "names":{
      "en":"Beijing"
    }
  },
  "continent":{
    "code":"AS",
    "names":{
      "en":"Asia"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    }
  },
  "country":{
    "iso_code":"CN",
    "names":{
      "en":"China"
    }
  },
  "subdivisions":[
    {
      "names":{
        "en":"Beijing"
      }
    }
  ],
  "location":{
    "latitude":39.904202,
    "longitude":116.407402,
    "time_zone":"Asia\/Shanghai"
  }
}
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

按需模式的ISDB

功能介绍

默认情况下，FortiGate会使用全尺寸ISDB库文件放置在Flash盘分区中。在某些较低端的型号中（如FortiGate-30E、FortiGate-50E等），由于硬件Flash容量较小，使用全尺寸ISDB库可能会导致Flash分区异常。

ISDB按需模式将全尺寸ISDB文件替换为小得多的文件。此文件仅包含互联网服务的基本条目。在防火墙策略/限速策略/SD-WAN规则中使用某个ISDB服务时，FortiGate会查询FortiGuard以下载对应ISDB条目的IP地址/端口信息并将其存储在Flash驱动器上。防火墙策略中使用的 ISDB 条目的内容在重新启动后仍然存在。

> **重要**
>
> 该功能在FortiOS 7.2.4 GA及更新版本支持。

配置步骤

1. 在CLI下开启ISDB的on-demand模式，默认为standard模式，注意修改为on-demand模式后，已从FortiGuard下载的ISDB条目将会从Flash分区中删除，配置完成后，可以使用“execute update-ffdb-ondemand”下载on-demand模式的ISDB库，或者等待FortiGate的自动更新。

```
FortiGate # config sys global

FortiGate (global) # set internet-service-database ?
mini         Small sized Internet Service database with very limited IP addresses.
standard     Medium sized Internet Service database with most IP addresses.
full         Full sized Internet Service database with all IP addresses.
on-demand    Internet Service database with customer selected IP addresses.

FortiGate (global) # set internet-service-database on-demand
FortiGate (global) # end

Warning: Changing Internet Service database update mode will lead to the removal of all downloaded Internet
Service files.
Do you want to continue? (y/n)y

Please run "execute update-ffdb-ondemand" to do explicit download or wait for automatic schedule update for
configuration of Internet Service database
```

2. 此时查看FortiGate的ISDB库版本，Flash中的ISDB库已变为On-Demand模式，文件为空。

```
FortiGate # diagnose autoupdate versions | grep Internet -A 6
Internet-service On-Demand Database
————————
Version: 0.00000
Contract Expiry Date: n/a
Last Updated using scheduled update on Wed May 24 10:53:22 2023
Last Update Attempt: Wed May 24 17:23:10 2023
Result: No Updates
```

3. 使用“execute update-ffdb-ondemand”下载on-demand模式的ISDB库，或者等待FortiGate的自动更新完成，再次查看FortiGate的ISDB库版本，可以看到FortiGate已经下载了On-Demand模式的ISDB文件。

```
FortiGate # diagnose autoupdate versions | grep Internet -A 6
Internet-service On-Demand Database
————————
Version: 7.03216
Contract Expiry Date: n/a
Last Updated using manual update on Wed May 24 17:27:11 2023
Last Update Attempt: Wed May 24 17:27:11 2023
Result: Updates Installed
```

4. 由于尚未将任何ISDB条目应用于防火墙策略/限速策略/SD-WAN策略，因此ISDB Summary信息中的IP范围数量和IP地址数量为空，这里以Google.Web ↗（65537）为例。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose internet-service id-summary 65537
Version: 00007.03216
Timestamp: 202305231647
Total number of IP ranges: 2858
Number of Groups: 1
Group(0), Singularity(90), Number of IP ranges(2858)
Internet Service: 65537(Google-Web)
Number of IP ranges: 0
Number of IP addresses: 0
Singularity: 0
Icon Id: 1
Direction: dst
Data source: isdb
Country:
Region:
City:
```

5. 将该ISDB应用于一条防火墙策略中。

```
config firewall policy
    edit 5
        set name "Google-Web"
        set srcintf "lan"
        set dstintf "wan"
        set action accept
        set srcaddr "all"
        set internet-service enable
        set internet-service-name "Google-Web"
        set schedule "always"
        set nat enable
    next
end
```

6. 再次查看Google.Web（65537）Summary信息，可以看到在防火墙策略引用该ISDB后，FortiGate自动从FortiGuard下载了该ISDB库。

```
FortiGate # diagnose internet-service id-summary 65537
Version: 00007.03216
Timestamp: 202305231647
Total number of IP ranges: 25767
Number of Groups: 2
Group(0), Singularity(90), Number of IP ranges(2858)
Group(1), Singularity(6), Number of IP ranges(22909)
Internet Service: 65537(Google-Web)
Number of IP ranges: 22909
Number of IP addresses: 19527416
Singularity: 6
Icon Id: 1
Direction: dst
Data source: isdb
Country: 4 8 10 12 16 20 24 28 31 32 36 40 44 48 50 51 52 56 60 64 68 70
        72 76 84 86 90 96 100 104 108 112 116 120 124 132 136 144 148 152 156 158 162
        166 170 175 178 180 184 188 191 192 196 203 204 208 212 214 218 222 226 231 232 233
        234 238 239 242 246 248 250 254 258 260 262 266 268 270 275 276 288 292 296 300 308
 ...
```

7. 查看其他ISDB的Summary信息，仍然为空。

```
FortiGate # diagnose internet-service id-summary 1245187
Version: 00007.03216
Timestamp: 202305231647
Total number of IP ranges: 25767
Number of Groups: 2
Group(0), Singularity(90), Number of IP ranges(2858)
Group(1), Singularity(6), Number of IP ranges(22909)
Internet Service: 1245187(Fortinet-DNS)
Number of IP ranges: 0
Number of IP addresses: 0
Singularity: 0
Icon Id: 19
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Direction: dst
Data source: isdb
Country:
Region:
City:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

什么是DoS

DoS&DDoS

1. 拒绝服务攻击（英语：denial-of-service attack，简称DoS攻击）亦称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。

2. 当黑客使用网络上两个或以上被攻陷的电脑作为“僵尸”向特定的目标发动“拒绝服务”式攻击时，称为分布式拒绝服务攻击（distributed denial-of-service attack，简称DDoS攻击）。

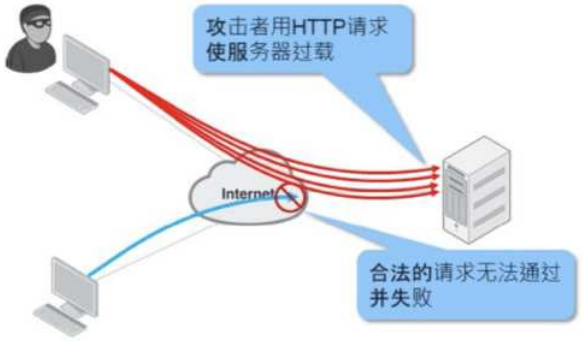
3. DoS侧重于通过对主机特定漏洞的利用攻击导致网络栈失效、系统崩溃、主机死机而无法提供正常的网络服务功能，从而造成拒绝服务，常见的DOS攻击手段有TearDrop、Land、Jolt、IGMP Nuker、Boink、Smurf、Bonk、OOB等；扫描也是网络攻击的一种，攻击者在发起网络攻击之前，通常会试图确定目标上开放的TCP/UDP端口，而一个开放的端口通常意味着某种应用。

4. DDoS的表现形式主要有两种，一种为流量攻击，主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机；另一种为资源耗尽攻击，主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或CPU被内核及应用程序占完而造成无法提供网络服务。 与DoS攻击相比，DDoS攻击更难以预防，因为黑客可能来自世界各地，DDoS攻击可以分为两个阶段：

    - 感染阶段：黑客将尝试开发并感染尽可能多的系统，受到感染和破坏的系统将称为Bot或Zombie，这些僵尸和僵尸分散在世界各地，所有这些僵尸或僵尸都将监听黑客的命令。
    - 攻击阶段：黑客向机器人或僵尸发出命令，以攻击目标系统，当这些僵尸程序或僵尸程序获得命令后，它们将开始攻击目标系统。从目标的角度来看，攻击将无处不在。

5. 拒绝服务的攻击也可能会导致目标计算机同一网络中的其他计算机被攻击，互联网和局域网之间的带宽会被攻击导致大量消耗，不但影响目标计算机，同时也影响局域网中的其他电脑。如果攻击的规模较大，整个地区的网络连接都可能会受到影响。

6. 攻击者的会话回消耗所有资源——RAM、CPU、端口号，减慢或使目标功能失效，直到不能响应合法的请求。



攻击现象

- 网络异常缓慢（打开文件或访问网站）
- 特定网站无法访问
- 无法访问任何网站
- 垃圾邮件的数量急剧增加
- 无线或有线网络连接异常断开
- 长时间尝试访问网站或任何互联网服务时被拒绝
- 服务器容易断线、卡顿、lag

攻击方式

DDoS攻击可分为3类：带宽消耗、资源匮乏、应用程序编程缺陷。

1. 带宽消耗：
    - 这种攻击试图使系统的带宽饱和。如果黑客可以用尽所有带宽，则黑客可以阻止合法用户访问系统。
    - 例如：客户从ISP订阅了10 Mbps的互联网带宽。如果黑客能够充分利用10 Mbps的Internet链接，则合法用户将不会留有带宽。由于没有足够的带宽供合法用户使用，因此他们将无法再访问系统。攻击的示例包括Smurf攻击，Fraggle攻击，Chargen攻击和放大攻击。
    - 使用FortiGate或FortiDDoS不能有效地缓解此类DDoS攻击。
2. 资源匮乏：
    - 该攻击试图使系统上的资源过载，使其无法使用，资源可以是会话表，CPU处理时间，磁盘空间等。
    - 攻击示例为TCP SYN Flood，SlowLoris等。
    - 可以使用Fortigate和FortiDDoS有效地缓解此类DDoS攻击。与Fortigate相比，FortiDDoS具有更先进和有效的缓解技术。
3. 应用程序编程缺陷：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 该攻击试图导致系统严重错误。黑客试图将格式错误的数据发送到系统，并且系统崩溃。通过对系统造成严重错误，这使系统无法使用。
- 攻击示例包括缓冲区溢出和编程逻辑错误。
- 使用FortiGate和FortiDDoS可以有效地缓解此类DDoS攻击。与FortiGate相比，FortiDDos具有更先进和有效的缓解技术。

攻击与防护方法

1. 防DoS攻击：
   - SYN Flood攻击：如果到一个目标IP地址的新TCP连接（包括重传）的SYN数据包速率超过配置的阈值，则执行配置的操作。
   - TCP Session攻击：如果来自一个源/去往一个目的IP地址的并发TCP连接数超过配置的阈值，则将执行配置的操作。
   - UDP Flood攻击：如果到一个目标IP地址的UDP会话速率超过配置的阈值，则将执行配置的操作。
   - UDP Session攻击：如果来自一个源/去往一个目的IP地址的并发UDP连接数超过配置的阈值，则将执行配置的操作。
   - ICMP Flood攻击：如果发送到一个目标IP地址的ICMP数据包的速率超过配置的阈值，则将执行配置的操作。
   - ICMP Session攻击：如果来自一个源/去往一个目的IP地址的并发ICMP连接数超过配置的阈值，则将执行配置的操作。
   - SCTP Flood攻击：如果发送到一个目标IP地址的SCTP数据包的速率超过配置的阈值，则将执行配置的操作。
   - CTP Session攻击：如果来自一个源/去往一个目的IP地址的并发SCTP连接数超过配置的阈值，则将执行配置的操作。
2. 抗扫描攻击：
   - TCP协议扫描：根据实际网络情况，当受到TCP扫描攻击时，可以配置防TCP扫描。 当一个源IP地址在1秒内将含有TCP SYN片段的IP 封包发送给位于相同目标IP地址的不同端口数量大于配置的门限值时，即认为其进行了端口扫描，系统将其标记为TCP SCAN，并在配置的阻断时间内拒绝来自于该台源主机的所有其它TCP SYN包。 启用防TCP扫描，可能会占用比较多的内存。
   - UDP协议扫描：根据实际网络情况，当受到UDP扫描攻击时，可以配置防UDP SCAN扫描。 当一个源IP地址在1秒内将含有UDP的IP 封包发送给位于相同目标IP地址的不同端口数量大于配置的门限值时，即进行了一次端口扫描，系统将其标记为UDP SCAN，并在配置的阻断时间内拒绝来自于该台源主机的所有其它UDP包。 启用防UDP扫描，可能会占用比较多的内存。
   - PING扫描：根据实际网络情况，当受到PING扫描攻击时，可以配置防PING扫描。 当一个源IP地址在1秒内发送给不同主机的ICMP 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将ICMP 封包(通常是应答请求) 发送给各个主机，以期获得至少一个回复，从而查明目标地址。NGFW设备在内部记录从某一远程源地点发往不同地址的ICMP 封包数目。当某个源IP被标记为地址扫描攻击，则系统在配置的阻断时间内拒绝来自该主机的其它更多ICMP 封包。 启用防PING扫描，可能会占用比较多的内存。
   - 主机抑制时长：设置防扫描功能的阻断时间，当系统检测到扫描攻击时，在配置的时长内拒绝来自于该台源主机的所有其它攻击包，缺省配置为20秒。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate DoS策略工作原理

DoS防护

1. 拒绝服务（DoS）策略会检查到达FortiGate接口的网络流量是否存在异常模式，这通常表明存在攻击。当攻击者启动与目标的异常大量会话时（穿过或到达FortiGate），将发生拒绝服务。大量会话会减慢或禁用目标系统，从而阻止合法用户使用它。
2. 在安全策略之前先检查DoS策略，以防止攻击触发更多的资源密集型安全保护并减慢FortiGate的速度。

DoS异常

FortiGate针对特定的异常流量设置了预定义的异常种类，用户无法添加自定义的DoS异常，以下是每个异常阈值的解释。

1. L3异常：
   - ip_src_session（并发）：如果来自一个源IP地址的并发IP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
   - ip_dst_session（并发）：如果到一个目标IP地址的并发IP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
2. L4异常
   - tcp_syn_flood（速率）：如果到一个目标IP地址的新TCP连接（包括重传）的SYN数据包速率超过配置的阈值，则执行配置的操作。建议值：2000/s。
   - tcp_port_scan（速率）：如果来自一个源IP地址的新TCP连接的SYN包速率（包括重传）超过了配置的阈值，则将执行配置的操作。建议值：1000/s。
   - tcp_src_session（并发）：如果来自一个源IP地址的并发TCP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
   - tcp_dst_session（并发）：如果到一个目标IP地址的并发TCP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
   - udp_flood（速率）：如果到一个目标IP地址的UDP会话速率超过配置的阈值，则将执行配置的操作。建议值：2000/s。
   - udp_scan（速率）：如果来自一个源IP地址的UDP会话速率超过配置的阈值，则将执行配置的操作。建议值：2000/s。
   - udp_src_session（并发）：如果来自一个源IP地址的并发UDP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
   - udp_dst_session（并发）：如果到一个目标IP地址的并发UDP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
   - icmp_flood（速率）：如果发送到一个目标IP地址的ICMP数据包的速率超过配置的阈值，则将执行配置的操作。建议值：250/s。
   - icmp_sweep（速率）：如果来自一个源IP地址的ICMP数据包的速率超过配置的阈值，则将执行配置的操作。建议值：100/s。
   - icmp_src_session（并发）：如果来自一个源IP地址的并发ICMP连接数超过配置的阈值，则将执行配置的操作。建议值：300。
   - icmp_dst_session（并发）：如果到一个目标IP地址的并发ICMP连接数超过配置的阈值，则将执行配置的操作。 建议值：1000。
   - sctp_flood（速率）：如果发送到一个目标IP地址的SCTP数据包的速率超过配置的阈值，则将执行配置的操作。建议值：2000/s。
   - sctp_scan（速率）：如果来自一个源IP地址的SCTP会话速率超过配置的阈值，则将执行配置的操作。建议值：1000/s。
   - sctp_src_session（并发）：如果来自一个源IP地址的并发SCTP连接数超过配置的阈值，则将执行配置的操作。建议值：5000。
   - sctp_dst_session（并发）：如果到一个目标IP地址的并发SCTP连接数超过配置的阈值，则执行配置的操作。 建议值：5000。

基于并发会话数的阈值

对于基于并发会话数的阈值，DoS策略会将超过设置阈值的连接阻断。这里举个例子：

1. 在FortiGate的DoS策略中，将icmp_src_session的阈值设置为10，攻击者发送了10条匹配异常条件的连接通过FortiGate。
2. 这10条连接将被放通，但第11条及以后匹配的连接将被阻断。此时，匹配异常条件的允许通过会话计数器变为10。
3. 之后，这10条连接没有后续报文传输，FortiGate针对ICMP流量的的老化时间为60s，那么60s的计时器到期后，匹配异常条件的允许通过会话计数器被重置为0。
4. 所以，如果在阻止之前允许进行10个会话，则在60秒后，将允许再进行10个会话。

基于速率的阈值

对于基于速率的阈值，其中阈值以每秒通过或到达的数据包为单位进行度量，“阻止”操作可通过两种方式防止异常流量瘫痪目标系统：

1. continuous：检测到异常后立即阻止数据包，并在速率高于阈值时继续阻止数据包。此为默认配置。

2. periodical：检测到异常后，允许每秒配置的数据包数量。

3. 这里举个例子：

   - 在FortiGate的DoS策略中，将icmp_flood的阈值设置为10/s，攻击者以20pps的速率启动1000个数据包的连续ping通过FortiGate。

   - 在continuous模式下，如果前10个数据包触发了DoS策略，则前10个数据包通过，阻断剩余的990个数据包。

   - 在periodical模式下，每秒钟允许通过10个数据包，所以会有500个数据包被阻断。（注：由于发包速率可能会发生波动，因此通过和阻止的数据包的实际数量可能不准确，但数量应接近定义的阈值。）

   - periodical模式需要在CLI下启动：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config ips global
    set anomaly-mode {continuous | periodical}
end
```

Quarantine

1. Quarantine用于阻止来自被认为是恶意行为者的源IP地址或对网络有害的流量源的任何其他流量。在隔离期间，将阻止来自源IP地址的流量，并将源IP地址添加到被禁止的用户列表中。禁止的用户列表保留在内核中，并由防病毒，数据泄漏防护（DLP），DoS和入侵防护系统（IPS）使用。使用任何这些功能的任何策略都将阻止来自攻击者IP地址的流量。该功能仅在CLI下可以配置，请参考“FortiGate DoS策略配置”。

2. 查看Quarantine用户列表：

```bash
# diagnose user quarantine list
src-ip-addr       created                 expires                 cause
192.168.118.77     Fri Jan 15 18:47:54 2021 Fri Jan 15 18:57:54 2021 DOS
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate DoS策略配置

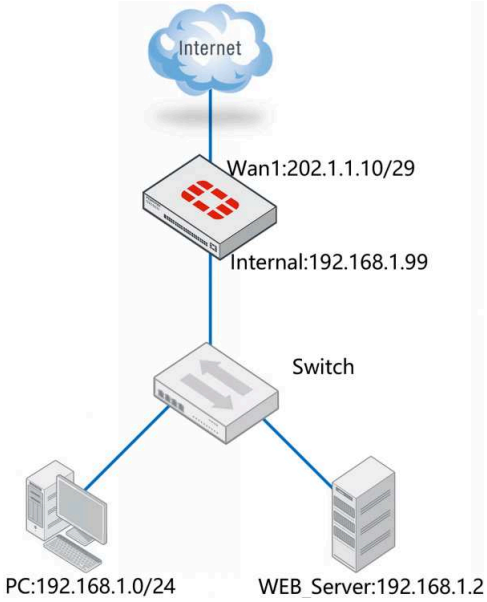
重要

要阻止DoS攻击，在位于攻击者和希望保护的所有资源之间的FortiGate设备上应用DoS策略。 DoS过滤比包处理过程更早完成，由内核处理。FortiGate的防SYN Flood攻击采用了业界最新的syncookie技术，在很少占用系统资源的情况下，可以有效地抵御SYN Flood等DDOS攻击对受保护服务器的攻击。从而阻止外部的恶意攻击，保护设备和内网，当检测到此类扫描探测时，向用户进行报警提示。

网络需求

Web服务器192.168.1.2，映射到外网地址202.1.1.11，对互联网开放HTTP服务，从而增加了服务器被攻击的风险，需要开启DDoS功能对服务器进行保护。对所有来自互联网的访问进行DDOS防护。

网络拓扑



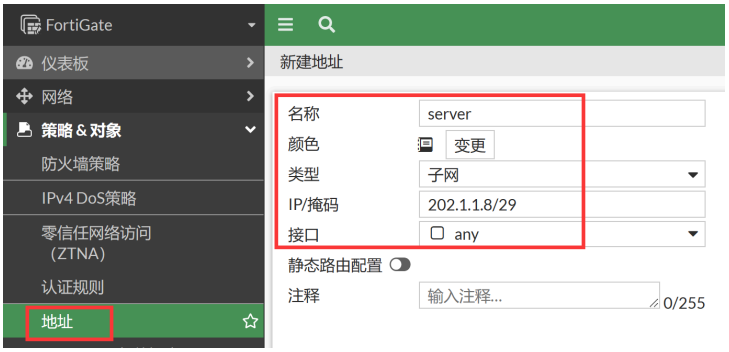
配置要点

- 定义服务器地址
- 定义DDoS策略

配置步骤

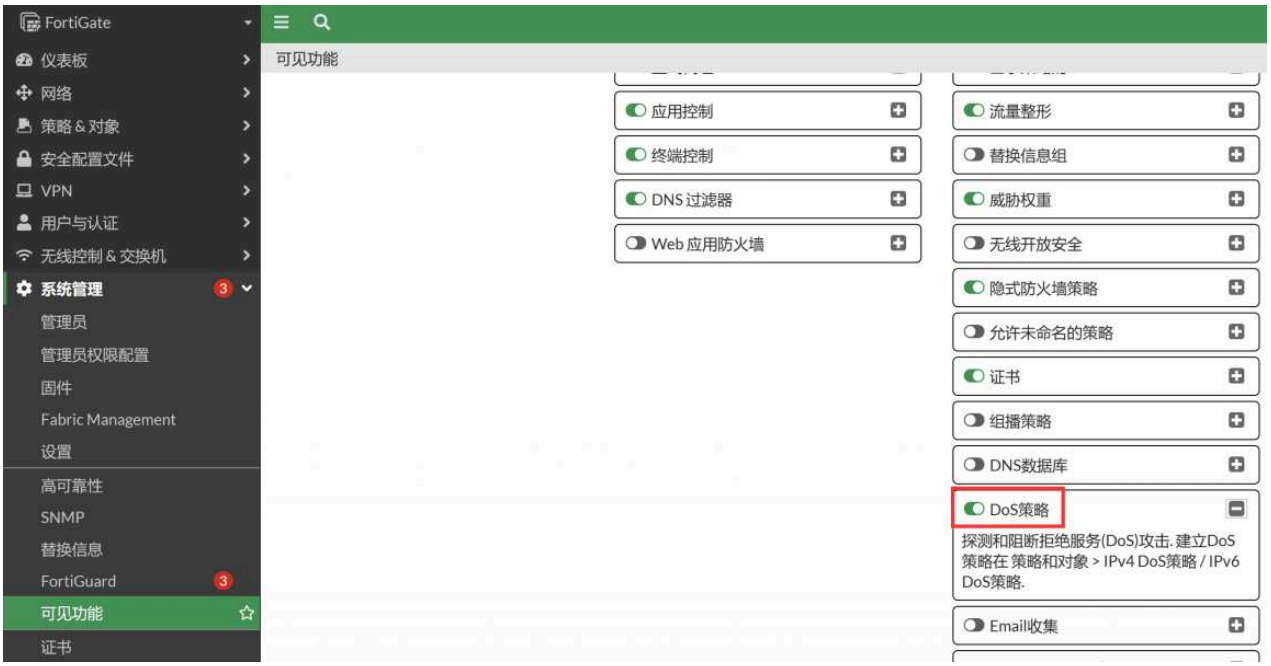
通过GUI配置

1. 定义服务器地址，进入策略&对象→地址，新建地址对象，名称配置为“server”，地址类型选择子网：ip/掩码为“202.1.1.8/29”，点击“确认”，该地址范围既包括了服务器地址（202.1.1.11）也包括了防火墙的外网口地址（202.1.1.10）。

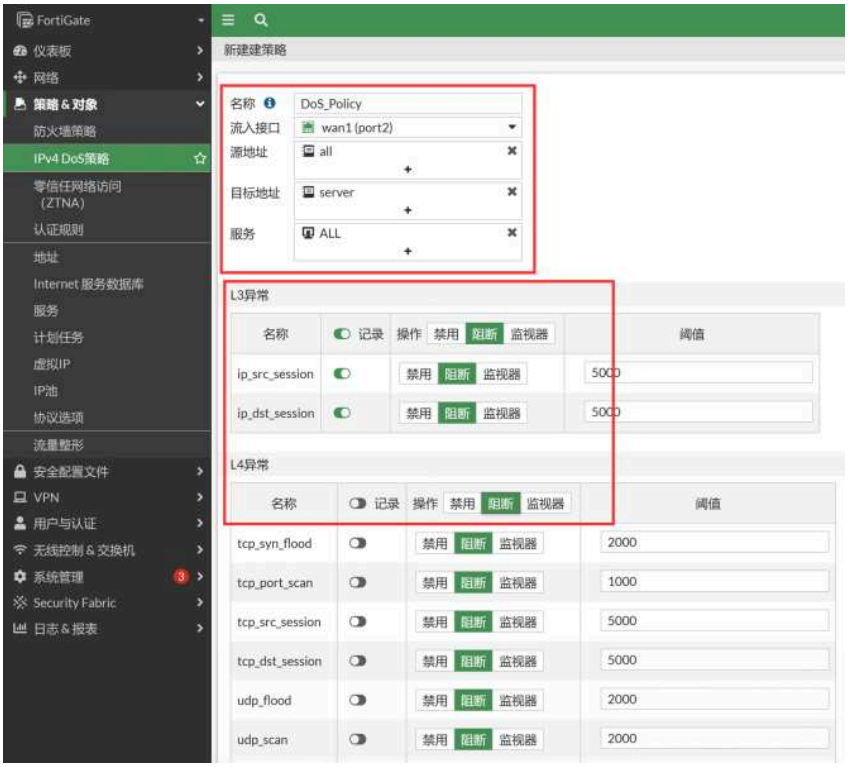


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置DoS策略齐前，需要确保在系统配置→可见功能中开启了DoS策略。



3. 一条DoS策略可以包含一个或多个异常配置，通过访问GUI的“策略 & 对象”→“IPv4 DoS策略”或“IPv6 DoS策略”页面，点击“新建”按钮，并配置参数。

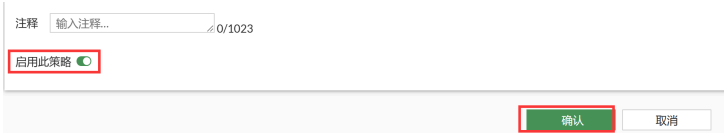


4. 具体参数可以参考如下表格。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

参数	说明
名称	输入策略名称。
流入接口	选择DoS策略工作的接口。
源地址	选择攻击流量的源地址。
目标地址	选择攻击流量的目标地址。 此处的地址应为与FortiGate接口相关联的地址，例如接口地址、接口第二地址、VIP地址。
服务	选择攻击流量的目标服务或服务组。 可以配置为ALL，或为了节省FortiGate资源，只选择FortiGate接口会应答的服务。
L3异常 L4异常	配置异常: Logging：启用/禁用特定异常或所有异常的日志记录。当操作为“阻断”或“监视器”时，将记录异常流量。 动作：选择达到阈值时需要执行的操作： 禁用：不检查异常流量。 阻断：阻断异常流量。 监视器：允许异常流量，但是如果启用了logging，则记录日志信息。 Threshold：触发异常动作需要达到的流量速率或并发数阈值。
注释	可选项。

5.启用此策略，然后点击确认。



通过CLI配置

1. 相关CLI命令。

```
config firewall DoS-policy
    edit 1
        set name "DoS_Policy"
        set interface "port2"
        set srcaddr "all"
        set dstaddr "server"
        set service "ALL"
        config anomaly
            edit "tcp_syn_flood"
                set status enable
                set action block
                set threshold 2000
            next
            edit "tcp_port_scan"
                set status enable
                set action block
                set threshold 1000
            next
            edit "tcp_src_session"
                set status enable
                set action block
                set threshold 5000
            next
            edit "tcp_dst_session"
                set status enable
                set action block
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set threshold 5000
            next
            edit "udp_flood"
                set status enable
                set action block
                set threshold 2000
            next
            edit "udp_scan"
                set status enable
                set action block
                set threshold 2000
            next
            edit "udp_src_session"
                set status enable
                set action block
                set threshold 5000
            next
            edit "udp_dst_session"
                set status enable
                set action block
                set threshold 5000
            next
            edit "icmp_flood"
                set status enable
                set action block
                set threshold 250
            next
            edit "icmp_sweep"
                set status enable
                set action block
                set threshold 100
            next
            edit "icmp_src_session"
                set status enable
                set action block
                set threshold 300
            next
            edit "icmp_dst_session"
                set status enable
                set action block
                set threshold 1000
            next
            edit "ip_src_session"
                set status enable
                set log enable
                set action block
                set threshold 5000
            next
            edit "ip_dst_session"
                set status enable
                set log enable
                set action block
                set threshold 5000
            next
            edit "sctp_flood"
                set status enable
                set action block
                set threshold 2000
            next
            edit "sctp_scan"
                set status enable
                set action block
                set threshold 1000
            next
            edit "sctp_src_session"
                set status enable
                set action block
                set threshold 5000
            next
            edit "sctp_dst_session"
                set status enable
                set action block
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set threshold 5000
            next
        end
    next
end
```

2. 具体参数可以参考如下表格。

参数	说明
`name <string>`	策略名称。
`interface <string>`	DoS策略工作的接口。
`srcaddr <string>`	攻击流量的源地址。
`dstaddr <string>`	攻击流量的目标地址。 此处的地址应为与FortiGate接口相关联的地址，例如接口地址、接口第二地址、VIP地址。
`service <string>`	攻击流量的目标服务或服务组。 可以配置为ALL，或为了节省FortiGate资源，只选择FortiGate接口会应答的服务。
status {enable or disable}	启用或关闭该异常。
log {enable or disable}	启用/禁用特定异常或所有异常的日志记录。当操作为“阻断”或“监视器”时，将记录异常流量。
action {pass or block}	选择达到阈值时需要执行的操作： pass：允许异常流量，但是如果启用了logging，则记录日志信息。 block：阻断异常流量。
quarantine {none or attacker}	Quarantine方法： none：关闭Quarantine功能。 attacker：阻断所有来自攻击者IP的流量，然后将攻击者IP加入用户黑名单。
quarantine-expiry <###d##h##m>	设置Quarantine的时长，格式为天、分钟、分钟（###d##h##m），范围1m - 364d23h59m, 默认为5m）。 该配置仅在Quarantine被配置为attacker时可用。
quarantine-log {enable or disable}	启用或禁用Quarantine日志（默认禁用），该配置仅在Quarantine被配置为attacker时可用。
`threshold <integer>`	触发异常动作需要达到的流量速率或并发数阈值。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate DoS策略调整

1. 应该如何调整DoS策略以防误报或阻止正常流量？DoS策略不依赖于会话状态，所以FortiGate的出站和入站流量都会被处理。例如如下流量抓包：

```
# di sniff pack Vlan_11 'port 80 and tcp[tcpflags] == tcp-syn' 1 25
interfaces=[Vlan_11]
filters=[port 80 and tcp[tcpflags] == tcp-syn]
0.876904 10.95.13.204.24088 → 10.95.136.204.80: syn 3585436935
0.894848 10.95.4.223.7273 → 10.95.128.117.80: syn 2436279189
0.947586 10.95.10.90.5871 → 10.95.132.100.80: syn 1124757321
0.972220 10.95.5.29.26781 → 10.95.128.217.80: syn 2500978264
```

2. 基于这一点，你需要使用如下推荐的配置。

从Internet保护内网服务器

1. 确保仅将内网服务器映射的IP（比如VIP）配置为DoS策略的目的地址。

2. 在被保护的服务器上开启需要的服务。在DoS策略的服务中仅配置服务器对外开启的服务。

3. DoS策略中仅配置与服务器开启的服务有关的异常。例如服务器只开启了SMTP服务，那么在配置DoS策略时，只配置tcp_syn_flood、tcp_src_session或ip_src_session异常。

4. 将这些异常配置到一个DoS策略中，根据实际使用情况，阈值设置为正常的值。例如配置tcp_src_session异常，对于单个源客户端来说，最大的并发会话数为100，则使用如下配置（对于每一个异常，都有一个“正常”的阈值，需要根据实际情况进行配置）：

```
config firewall DoS-policy
    edit 1
        set interface "wan1"
        set srcaddr "all"
        set dstaddr "200.201.202.1"
        set service "SMTP"
            config anomaly
                edit "tcp_src_session"
                    set status enable
                    set action block
                    set quarantine attacker
                    set quarantine-expiry 10
                    set quarantine-log enable
                    set threshold 100
                next
            end
    next
end
```

5. 如果使用tcp_dst_session或ip_dst_session，则DoS策略将限制服务器处理的并发会话数，不建议这么使用。

从内网保护FortiGate

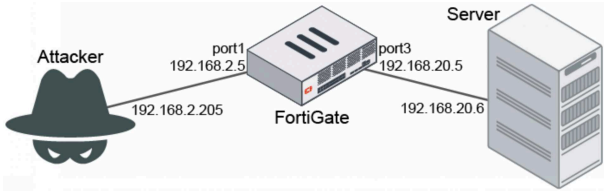
1. 将DoS策略的源配置为本地网络的网段（不要使用any）。
2. 将DoS策略的目的配置为any（攻击流量会通过默认路由到达防火墙），服务配置为ALL。
3. 开启这些异常：tcp_syn_flood、tcp_dst_session、ip_dst_session、tcp_port_scan，并根据平时使用情况配置正常的阈值。
4. 需要注意的是，在UDP相关异常和tcp_src异常的情况下，某些流量可能是由torrent（P2P）或Skype软件导致的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate DoS策略排错

DoS策略排错最好的办法就是查看分析异常日志与IPS异常信息。

网络拓扑



icmp_flood测试

1. Attacker向FortiGate以50pps的速率发送总共3000个icmp报文。

2. 在FortiGate上配置阈值为30pps的icmp_flood的DoS策略。

```
config firewall DoS-policy
    edit 1
        set name icmpFlood
        set interface "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "ALL"
        config anomaly
            edit "icmp_flood"
                set status enable
                set log enable
                set action block
                set threshold 30
            next
        end
    next
end
```

3. 配置debug filter，过滤icmp_flood攻击的debug信息。

```
# diagnose ips anomaly config
DoS sensors in kernel vd 0:
DoS id 1 proxy 0
  0 tcp_syn_flood status 0 log 0 nac 0 action 0 threshold 2000
  ...
  7 udp_dst_session status 0 log 0 nac 0 action 0 threshold 5000
  8 icmp_flood status 1 log 1 nac 0 action 7 threshold 30
  9 icmp_sweep status 0 log 0 nac 0 action 0 threshold 100
  ...
total # DoS sensors: 1.
# diagnose ips anomaly filter id 8
```

4. 使用Mac OS或Linux发起icmp_flood攻击，这里使用hping3工具为例（需要自行安装）。

```
summerice@Summerice ~ % sudo hping3 --icmp -i u20000（发包间隔20000微秒，即50pps） -c 3000 192.168.2.50

HPING 192.168.2.50 (en11 192.168.2.50): icmp mode set, 28 headers + 0 data bytes

...

--- 192.168.2.50 hping statistic ---

3000 packets tramitted, 30 packets received, 99% packet loss

round-trip min/avg/max = 0.4/0.5/0.8 ms
```

5. 由以上hping3发包结果可知，只有30个包通过，剩余icmp包被阻断，符合icmp_flood防护工作原理。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

6. 在攻击期间，在FortiGate查看异常列表。

```
# diagnose ips anomaly list

list nids meter:

id=icmp_flood         ip=192.168.2.50 dos_id=1 exp=1000 pps=46 freq=50

total # of nids meters: 1.
```

参数	说明
id=icmp_flood	攻击名称。
ip=192.168.2.50	触发异常的被攻击对象的IP地址，可能是服务器，也可能是客户端。 对于icmp_flood攻击，IP地址为攻击目标IP地址。如果是icmp_sweep攻击，该IP应为攻击源IP。
dos_id=1	匹配的DoS策略ID。
exp=998	剩余过期时间，单位为秒。
pps=46	命令执行时，已经收到的数据包pps。
freq=50	对于基于并发会话数的异常，freq为并发会话数。 对于基于速率的异常（flood、scan）： continuous模式：freq为pps中的最大数值，或者时最后一秒收到的数据包的总数。 periodic模式：freq为pps数值。

日志分析

1. 在GUI中访问“日志 & 报告”→异常，下载DoS的异常日志，这里截取攻击刚开始的两条日志举例。

2. 第一条日志中的字段分析。

```
date=2021-1-15 time=18:38:39 eventtime=1605911919824184594 tz="-0800" logid="0720018433" type="utm"
subtype="anomaly" eventtype="anomaly" level="alert" vd="root" severity="critical" srcip=192.168.2.205
srccountry="Reserved" dstip=192.168.2.50 srcintf="port1" srcintfrole="undefined" sessionid=0
action="clear_session" proto=1 service="PING" count=1307 attack="icmp_flood" icmpid="0x2195" icmptype="0x08"
icmpcode="0x00" attackid=16777316 policyid=1 policytype="DoS-policy" ref="http://www.fortinet.com/ids/VID16777316"
msg="anomaly: icmp_flood, 31 > threshold 30, repeats 28 times" crscore=50 craction=4096 crlevel="critical"
```

参数	说明
msg="anomaly: icmp_flood, 31 > threshold 30	在攻击的刚开始，第一条日志记录了攻击流量超过了30pps的阈值。
repeats 28 times	自上次记录日志以来超过阈值的数据包数。
srcip=192.168.2.205 dstip=192.168.2.50	攻击流量的源目IP。
action="clear_session"	清除相关会话，即阻断动作。 如果动作设置为“监视器”且“logging”开启，这里会显示“detected”。

3.第二条日志中的字段分析。

```
date=2021-1-15 time=18:39:09 eventtime=1605911949826224056 tz="-0800" logid="0720018433" type="utm"
subtype="anomaly" eventtype="anomaly" level="alert" vd="root" severity="critical" srcip=192.168.2.205
srccountry="Reserved" dstip=192.168.2.50 srcintf="port1" srcintfrole="undefined" sessionid=0 action="clear_session"
proto=1 service="PING" count=1497 attack="icmp_flood" icmpid="0x2195" icmptype="0x08" icmpcode="0x00"
attackid=16777316 policyid=1 policytype="DoS-policy" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly:
icmp_flood, 50 > threshold 30, repeats 1497 times" crscore=50 craction=4096 crlevel="critical"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

参数	说明
msg="anomaly: icmp_flood, 50 > threshold 30	在日志生成的前一秒，检测到了50个匹配异常的数据包，超过了配置的阈值30。
repeats 1497 times	自上次记录日志以来超过阈值的数据包数。

- 由于是持续的攻击流量，FortiGate为多个数据包每30s生成一次日志（注意第二条日志和第一条日志的间隔为30s）。
- 以下情况FortiGate不会再次生成DoS异常日志：
  - 相同的攻击ID在5s内发生了多次。
  - 相同的攻击ID在30s内发生了多次，且匹配的异常策略动作一致，并且拥有相同的源目IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

流量整形介绍

功能介绍

FortiGate通过对网络流量进行带宽限制和优先级排序来提供服务质量（QoS）。流量整形是FortiGate用来提供QoS的一种技术。流量整形的方法是在流量拥堵期间，将高优先级的流量优先转发。为重要业务流量保证稳定效果，同时对不太重要的流量进行限制。

FortiGate的NP6流量整形可配置为policing和queuing两种模式。两者的区别如下：

- Policing：当流量超过配置的带宽限制时，流量将被丢弃。
- Quening：当流量超过配置的带宽限制时，流量会延迟传输并存放在队列中，直到带宽释放。如果队列已满，流量会被丢弃。

Policing和Quening模式都可以通过设置带宽限制来确定流量的优先级，并提供带宽保证和最大带宽服务。但实现方式不同，因为Quening使用队列，而Policing不使用队列：

- 在Quening模式下，数据包从接口发送之前，要使用RED或FIFO等算法将其排入队列。内核根据HTB算法对数据包进行去队列，然后再将其发送出去。
- 在Policing模式下，如果流量超过了分配的带宽，会被直接丢弃。

配置方法

在FortiGate上配置流量整形有3种方法。如下列出了3种方法及其功能。

> **重要**
>
> 如果3种方法都配置了，则第1种优先于第2种，第2种优先于第3种。

方法	Policing		Quening
	流量优先级	带宽保证保证与最大带宽	流量队列
Traffic shaping profile 流量整形配置文件	支持	支持，基于出接口带宽的百分比	支持
Traffic shaper 流量整形器	支持	支持，基于速率	不支持
Global traffic prioritization 全局流量优先级	支持	不支持	不支持

其中“Traffic shaping profile”方式可配置为Policing或Quening模式。Quening模式可以在配置流量整形时提供队列相关选项。每种方法的实现方式略有不同，下文主要介绍Policing模式的功能和使用方法。

流量优先级

FortiGate可以将数据包划分为不同的优先级，以便优先处理某些流量，不同的流量整形方法，划分优先级的方法如下：

- Traffic shaping profile（流量整形配置文件）：不同的流量可以配置被分到不同的本地Class，最多可以配置30个Class。每个Class的流量可配置为5个优先级。
- Traffic shaper（流量整形器）：流量优先级可分为high（2）、medium（3）或low（4）级别。被带宽保证的流量会自动使用critical（1）级别。
- Global traffic prioritization（全局流量优先级）：根据流量报文IP头中携带的ToS（服务类型）或DSCP值，流量优先级分为high（2）、medium（3）或low（4）。

带宽保证与最大带宽

配置带宽保证的目的是分配总带宽的一部分优先给特定流量，以保证特定流量优先传输。每种流量整形的带宽保证方法的配置方法和处理方式都不同：

- Traffic shaping profile（流量整形配置文件）应用于设备流量出接口。如上文所属，Traffic shaping profile通过为不同的流量分配不同的Class来区分流量优先级，每个Class配置的保证带宽为出接口总带宽（需要配置）的百分比（而不是具体带宽数值），所有Class共同使用接口最大配置带宽的100%（也可小于100%，但不能大于100%）。每个Class中配置的优先级并不重要，保证带宽配置始终会生效。
- Traffic shaper（流量整形器）对带宽保证没有硬性限制。管理员需要了解分配给所有流量整形器的保证带宽，以免超过出接口的总带宽。被流量整形器带宽保证的流量优先级为1。如果优先级为1的总流量超过了总出口带宽，流量就会被丢弃。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 配置接口最大带宽限定了出接口可使用的最大带宽。它被配置为流量整形配置文件中外带宽的百分比。它被配置为流量整形器的速率。

配置出接口带宽

流量整形通常是为离开FortiGate的出口流量配置的。因此，在所有流量整形配置方法中，都必须定义出接口带宽，以便进行流量优先级排序。在Traffic shaping profile中定义保证带宽和最大带宽时，也需要定义出接口带宽。

对于Traffic shaper，配置出接口带宽不是应用最大带宽限制的必要条件；但对于保证带宽，配置外带宽则是必要条件。流量整形器上保证带宽限制下的流量优先级为1。如果未配置外带宽，则不会进行流量优先级排序，优先级也毫无意义。

Traffic shaping policy

流量整形配置文件和流量整形器是监控流量的方法。流量整形策略用于将流量映射到流量整形器或将其分配到一个类。 流量整形策略是根据特定 IP 头字段和/或上层标准匹配流量的规则。例如，它可以根据源和目标 IP、服务、应用程序和 URL 类别来匹配流量。一种常见的用例是根据 IP 标头中的 ToS 或 DS（差异化服务）字段匹配流量。这允许从下游设备的流量中读取服务类型或差异化服务（DiffServ）标签，并在 FortiGate 上进行相应的优先级排序。

DSCP matching and DSCP marking

DSCP匹配和DSCP标记可在防火墙整形策略和常规防火墙策略上执行。DSCP匹配用于匹配入口流量的DSCP标记，DSCP标记用于更改出口流量的DSCP标记。

在防火墙整形策略和常规防火墙策略中，使用`tos`和`tos-mask`字段执行DSCP匹配。使用`diffserv-forward`和`diffserv-reverse`字段执行DSCP标记。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

穿越流量

施工中……

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

本地流量

施工中……

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

流量整形配置文件

施工中……

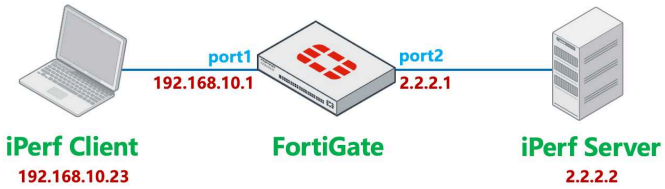
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

共享流量整形器

网络需求

基于多IP共享进行限速，限制Iperf Client传输速度，上行和下行速度分别为5Mbps。

网络拓扑



配置步骤

1. 进入策略&对象→流量整形→流量整形器，分别新建上传和下载的流量整形器，选择类型为共享的，最大带宽配置为5Mbps。





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall shaper traffic-shaper
    edit "share-5M-upload"
        set maximum-bandwidth 5
        set bandwidth-unit mbps
    next
    edit "share-5M-download"
        set maximum-bandwidth 5
        set bandwidth-unit mbps
    next
end
```

2. 进入策略&对象→流量整形→流量整策略，新建流量整形策略，源接口为内网口port1，出接口为port2，服务配置为iperf打流使用的端口，这里以UDP 5001为例。开启Apply Shaper，开启共享流量整形器，引用上传限速5M，开启反向整形器，引用下载5M。




```
config firewall shaping-policy
    edit 1
        set name "5001"
        set service "udp_5001"
        set srcintf "port1"
        set dstintf "port2"
        set traffic-shaper "share-5M-upload"
        set traffic-shaper-reverse "share-5M-download"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

结果验证

1. 客户端IPerf打流测试打30M流（上传）。

2. 客户端端观察。

```
C:\iperf-3.1.3-win64>iperf3.exe -c 2.2.2.2 -p 5001 -u -b 30M -l 1K
Connecting to host 2.2.2.2, port 5001
[  4] local 192.168.10.23 port 49590 connected to 2.2.2.2 port 5001
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[ 4]   0.00-1.00   sec 3.30 MBytes  27.7 Mbits/sec  3380
[ 4]   1.00-2.00   sec 3.61 MBytes  30.2 Mbits/sec  3692
[ 4]   2.00-3.00   sec 3.69 MBytes  30.9 Mbits/sec  3774
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[ 4]   3.00-4.00   sec 3.66 MBytes  30.7 Mbits/sec  3748
[ 4]   4.00-5.00   sec 3.46 MBytes  29.0 Mbits/sec  3546
[ 4]   5.00-6.00   sec 3.66 MBytes  30.7 Mbits/sec  3745
[ 4]   6.00-7.00   sec 3.39 MBytes  28.4 Mbits/sec  3468
[ 4]   7.00-8.00   sec 3.53 MBytes  29.6 Mbits/sec  3612
[ 4]   8.00-9.00   sec 3.62 MBytes  30.3 Mbits/sec  3705
[ 4]   9.00-10.00  sec 3.66 MBytes  30.7 Mbits/sec  3743
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[ 4]   0.00-10.00  sec 35.6 MBytes  29.8 Mbits/sec  0.196 ms 29694/36412 (82%)
[  4] Sent 36412 datagrams
iperf Done.
```

3. 服务器端观察，接收速率被限制在5Mbps左右。

```
C:\iperf-3.1.3-win64>iperf3.exe -s -p 5001
-----------------------------------------------------------
Server listening on 5001
-----------------------------------------------------------
Accepted connection from 2.2.2.1, port 61655
[ 5] local 2.2.2.2 port 5001 connected to 2.2.2.1 port 49590
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[ 5]   0.00-1.00  sec  1.08 MBytes  9.05 Mbits/sec  0.205 ms 2219/3325 (67%)
[ 5]   1.00-2.00   sec  628 KBytes  5.14 Mbits/sec  0.155 ms 3072/3700 (83%)
[ 5]   2.00-3.00   sec  641 KBytes  5.25 Mbits/sec  0.154 ms 3118/3759 (83%)
[ 5]   3.00-4.00   sec  627 KBytes  5.13 Mbits/sec  0.175 ms 2952/3579 (82%)
[ 5]   4.00-5.00   sec  610 KBytes  5.00 Mbits/sec  0.132 ms 3093/3703 (84%)
[ 5]   5.00-6.00   sec  635 KBytes  5.20 Mbits/sec  0.199 ms 3044/3679 (83%)
[ 5]   6.00-7.00  sec   591 KBytes  4.84 Mbits/sec  0.192 ms 2924/3515 (83%)
[ 5]   7.00-8.00   sec  616 KBytes  5.04 Mbits/sec  0.190 ms 3060/3676 (83%)
[ 5]   8.00-9.00   sec  628 KBytes  5.15 Mbits/sec  0.202 ms 3041/3669 (83%)
[ 5]   9.00-10.00  sec  635 KBytes  5.20 Mbits/sec  0.172 ms 3077/3712 (83%)
[ 5]  10.00-10.03  sec 1.00 KBytes   286 Kbits/sec  0.196 ms 94/95 (99%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[ 5]   0.00-10.03  sec 0.00 Bytes  0.00 bits/sec  0.196 ms 29694/36412 (82%)
-----------------------------------------------------------
```

4. 查看会话状态，可以看到共享限速的标识信息。

```
session info: proto=17 proto_state=01 duration=11 expire=179 timeout=0 flags=00000000 sockflag=00000000 sockport=0
av_idx=0 use=4
origin-shaper=share-5M-upload    //应用的共享限速
prio=2 guarantee 0Bps max 655360Bps traffic 655739Bps drops 36587508B
reply-shaper=
per_ip_shaper=
class_id=0 shaping_policy_id=3 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty os route_preserve
statistic(bytes/packets/allow_err): org=8138304/7737/1 reply=32/1/1 tuples=2
tx speed(Bps/kbps): 694987/5559 rx speed(Bps/kbps): 2/0
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 192.168.10.23:49768->2.2.2.2:5001(2.2.2.1:49768)
hook=pre dir=reply act=dnat 2.2.2.2:5001->2.2.2.1:49768(192.168.10.23:49768)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00001102 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000 ngfwid=n/a
dd_type=0 dd_mode=0

FGT-1 # diagnose  firewall shaper  traffic-shaper  list
name share-5M-upload
maximum-bandwidth 640 KB/sec
guaranteed-bandwidth 0 KB/sec
current-bandwidth 640 KB/sec
priority 2
overhead 0
tos ff
packets dropped 965353
bytes dropped 1015551356

FGT-1 # diagnose  netlink interface list  port2
if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ref=17 state=off start fw_flags=0 flags=up broadcast run multicast
Qdisc=pfifo_fast hw_addr=00:0c:29:e1:7d:41 broadcast_addr=ff:ff:ff:ff:ff:ff
stat: rxp=21438 txp=465340 rxb=12605783 txb=478598536 rxe=0 txe=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=17

FGT-1 # diagnose netlink qlen get port2
TX queue length for interface port2 is 1000
```

注意事项

共享带宽限速上行和下行限速需要分别调用，彼此之间独立工作，特别注意别只限制了上传速度，而没有配置下载速度，然后测速的时候发现限速不准确，标准的上行、下行速度限制为下图所示。



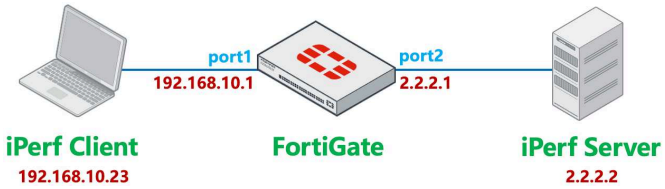
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

每IP整形器

网络需求

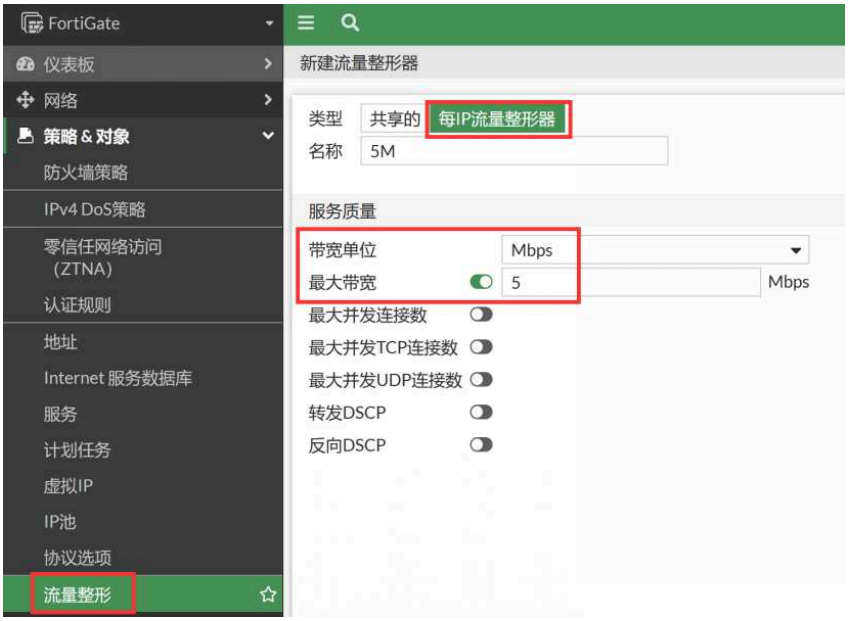
基于每IP对客户端进行限速，限制Iperf Client传输速度（包括上行和下行速度总和）为5Mbps。

网络拓扑



配置步骤

1. 进入策略&对象→流量整形→流量整形器，新建流量整形器，选择类型为每IP流量整形器，最大带宽配置为5Mbps。




```
config firewall shaper per-ip-shaper
    edit "5M"
        set max-bandwidth 5
        set bandwidth-unit mbps
    next
end
```

2. 进入策略&对象→流量整形→流量整策略，新建流量整形策略，源接口为内网口port1，出接口为port2，服务配置为iperf打流使用的端口，这里以UDP 5001为例。开启Apply Shaper，并引用上步配置的每IP限速整形器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config firewall shaping-policy
    edit 1
        set name "5M"
        set service "udp_5001"
        set srcintf "port1"
        set dstintf "port2"
        set per-ip-shaper "5M"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

结果验证

1. 客户端IPerf打流测试打30M流（上传）。

2. 客户端端观察。

```
C:\iperf-3.1.3-win64>iperf3.exe -c 2.2.2.2 -p 5001 -u -b 30M -l 1K
Connecting to host 2.2.2.2, port 5001
[  4] local 192.168.10.23 port 54998 connected to 2.2.2.2 port 5001
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[ 4]   0.00-1.00   sec 3.27 MBytes  27.4 Mbits/sec  3350
[ 4]   1.00-2.00   sec 3.53 MBytes  29.6 Mbits/sec  3619
[ 4]   2.00-3.00   sec 3.64 MBytes  30.6 Mbits/sec  3732
[ 4]   3.00-4.00   sec 3.77 MBytes  31.6 Mbits/sec  3860
[ 4]   4.00-5.00   sec 3.42 MBytes  28.7 Mbits/sec  3501
[ 4]   5.00-6.00   sec 3.57 MBytes  30.0 Mbits/sec  3660
[ 4]   6.00-7.00   sec 3.67 MBytes  30.8 Mbits/sec  3763
[  4]   7.00-8.00  sec  3.68 MBytes  30.8 Mbits/sec  3768
[ 4]   8.00-9.00   sec 3.34 MBytes  28.1 Mbits/sec  3421
[ 4]   9.00-10.00  sec 3.56 MBytes  29.8 Mbits/sec  3641
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[ 4]   0.00-10.00  sec 35.5 MBytes  29.7 Mbits/sec  0.180 ms 29610/36310 (82%)
[  4] Sent 36310 datagrams
iperf Done.
```

3. 服务器端观察，接收速率被限制在5Mbps左右。

```
C:\iperf-3.1.3-win64>iperf3.exe -s -p 5001
-----------------------------------------------------------
Server listening on 5001
-----------------------------------------------------------
Accepted connection from 2.2.2.1, port 61145
[ 5] local 2.2.2.2 port 5001 connected to 2.2.2.1 port 54998
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[ 5]  0.00-1.00   sec  1.07 MBytes 9.00 Mbits/sec  0.159 ms  2162/3262 (66%)
[ 5]   1.00-2.00   sec  616 KBytes  5.05 Mbits/sec  0.186 ms 3071/3687 (83%)
[ 5]   2.00-3.00   sec  635 KBytes  5.21 Mbits/sec  0.153 ms 3072/3707 (83%)
[ 5]   3.00-4.00   sec  654 KBytes  5.36 Mbits/sec  0.138 ms 3127/3781 (83%)
[ 5]   4.00-5.00   sec  597 KBytes  4.89 Mbits/sec  0.160 ms 2989/3586 (83%)
[ 5]   5.00-6.00   sec  621 KBytes  5.09 Mbits/sec  0.117 ms 3049/3670 (83%)
[ 5]   6.00-7.00   sec  642 KBytes  5.25 Mbits/sec  0.141 ms 3148/3790 (83%)
[ 5]   7.00-8.00   sec  632 KBytes  5.18 Mbits/sec  0.107 ms 3074/3706 (83%)
[ 5]   8.00-9.00   sec  587 KBytes  4.80 Mbits/sec  0.160 ms 2851/3438 (83%)
[ 5]   9.00-10.00  sec  615 KBytes  5.04 Mbits/sec  0.187 ms 2961/3576 (83%)
[ 5]  10.00-10.02  sec 1.00 KBytes   409 Kbits/sec  0.180 ms 106/107 (99%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[ 5]   0.00-10.02  sec 0.00 Bytes  0.00 bits/sec  0.180 ms 29610/36310 (82%)
-----------------------------------------------------------
```

4. 查看会话状态，可以看到每IP限速的标识信息。

```
session info: proto=17 proto_state=01 duration=33 expire=160 timeout=0 flags=00000000 sockflag=00000000 sockport=0
av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=5M    //被每IP限速标识
class_id=0 shaping_policy_id=3 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty per_ip route_preserve
statistic(bytes/packets/allow_err): org=9691056/9213/1 reply=32/1/1 tuples=2
tx speed(Bps/kbps): 291285/2330 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=3->4/4->3 gwy=0.0.0.0/0.0.0.0
hook=post dir=org act=snat 192.168.10.23:49631->2.2.2.2:5001(2.2.2.1:49631)
hook=pre dir=reply act=dnat 2.2.2.2:5001->2.2.2.1:49631(192.168.10.23:49631)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000e61 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000 ngfwid=n/a
dd_type=0 dd_mode=0

diagnose  firewall shaper  per-ip-shaper list
name 5M
maximum-bandwidth 640 KB/sec
maximum-concurrent-session 0
tos ff/ff
packets dropped 94884
bytes dropped 99717192
addr=192.168.10.23 status: bps=5250320 ses=3
```

注意事项

每IP带宽限速对上行和下行同时生效。只需要配置为5M，则上行和下行速度总和限速为5M。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

With per-IP traffic shaping, you can limit each IP address's behavior to avoid a situation where one user uses all of the available bandwidth. In addition to controlling the maximum bandwidth used per IP address, you can also define the maximum number of concurrent sessions for an IP address. For example, if you apply a per-IP shaper of 1 Mbps to your entire network, FortiOS allocates each user/IP address 1 Mbps of bandwidth. Even if the network consists of a single user, FortiOS allocates them 1 Mbps. If there are ten users, each user gets 1 Mbps of bandwidth, totaling 10 Mbps of outgoing traffic.

For shared shapers, all users share the set guaranteed and maximum bandwidths. For example, if you set a shared shaper for all PCs using an FTP service to 10 Mbps, all users uploading to the FTP server share the 10 Mbps.

Shared shapers affect upload speed. If you want to limit the download speed from the FTP server in the example, you must configure the shared shaper as a reverse shaper. Per-IP shapers apply the speed limit on both upload and download operations.

The following example shows how to apply a per-IP shaper to a traffic shaping policy. This shaper assigns each user a maximum bandwidth of 1 Mbps and allows each user to have a maximum of ten concurrent connections to the FTP server. In the example, FortiOS communicates with users using port10 and the FTP server using port9.

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NP7流量整形介绍

施工中……

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Policing模式

施工中……

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Shaping模式

施工中……

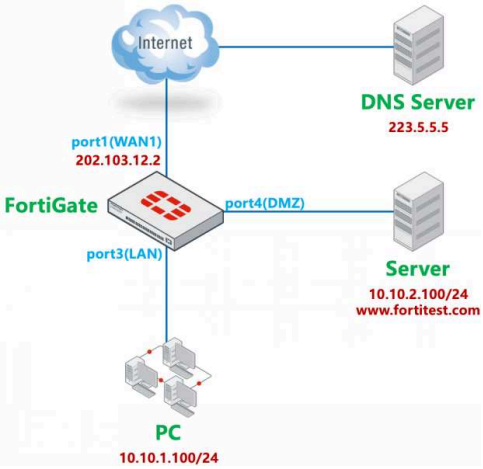
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

转换DNS解析结果

DNS Translation功能用于将穿越FortiGate的DNS解析结果替换为指定的结果。

具体适用场景请见如下网络拓扑与说明。

网络拓扑



1. DNS服务器位于Internet，内网PC填写的DNS服务器均为公网DNS服务器的IP 223.5.5.5。
2. FortiGate通过VIP将Server的端口映射到WAN1（port1）的202.103.12.2。
3. Server的域名为 `www.fortitest.com`，通过公网DNS服务器解析的结果为202.103.12.2。
4. 需要实现的效果：
   - 外网客户端访问Server时，直接通过 `www.fortitest.com` 解析到公网IP 202.103.12.2，通过FortiGate的VIP映射访问即可。
   - 内网客户端访问Server时，首先通过公网的DNS服务器223.5.5.5解析 `www.fortitest.com` 的IP地址，DNS Server会回复解析结果为202.103.12.2，FortiGate需要将解析结果修改为Server的内网IP 10.10.2.100，然后转发给内网客户端，内网客户端直接通过解析到的Server内网IP访问服务器。

配置步骤

1. 基础网络配置、上网策略、与Server的VIP配置（略）。

2. 在FortiGate上配置DNS Translation，将DNS请求结果为202.103.12.2的DNS响应报文中的IP地址修改为Server的内网IP 10.10.2.100。

```bash
config firewall dnstranslation
    edit 1
        set src 202.103.12.2
        set dst 10.10.2.100
    next
end
```

结果验证

1. 公网客户端PC使用DNS服务器223.5.5.5解析Server的域名（流量不经过FortiGate），得到结果为Server对应的VIP地址202.103.12.2。

```bash
C:\Users\Administrator.SUMMERICE2019>nslookup www.fortitest.com
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
名称:    www.fortitest.com
Address:  202.103.12.2
```

2. 内网客户端PC使用DNS服务器223.5.5.5解析Server的域名（流量经过FortiGate），得到结果为Server内网IP 10.10.2.100。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
C:\Users\Administrator.SUMMERICE2019>nslookup www.fortitest.com
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
名称:    www.fortitest.com
Address:  10.10.2.100
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

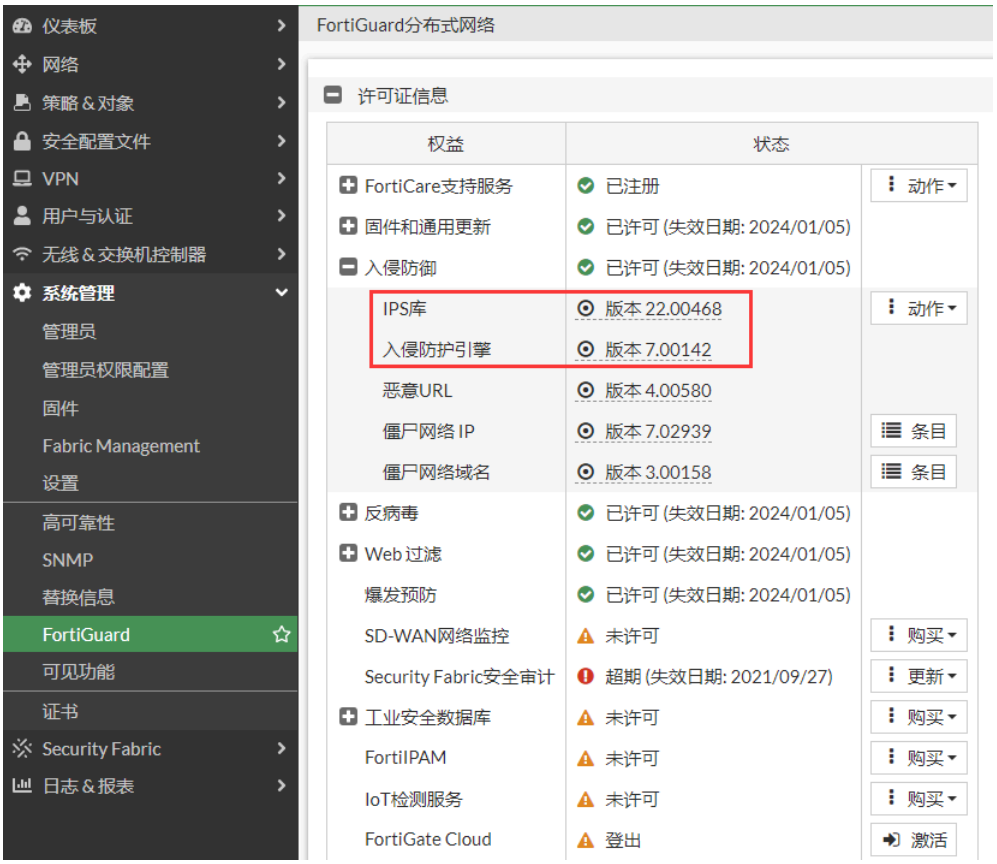
入侵防御简介

什么是IPS入侵防御系统

入侵防御系统 (IPS) 可帮助企业识别恶意流量并主动拦截此类流量进入企业网络。IPS通过特征库检测来识别流量中是否存在漏洞和漏洞利用程序；如果检测到威胁，则按照安全防御策略采取适当的措施，比如阻止访问。

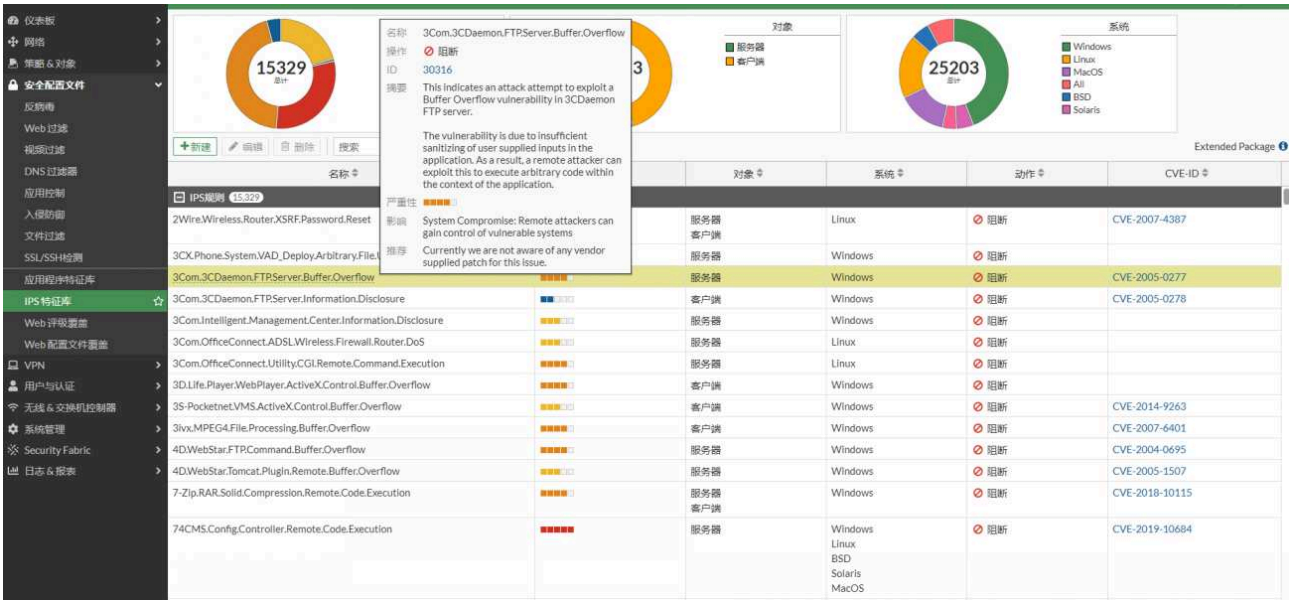
入侵防御特征库

选择“系统管理”-->“FortiGuard”-->“许可证信息”，在“入侵防御”菜单下可以查看IPS特种库的版本及IPS引擎的版本。



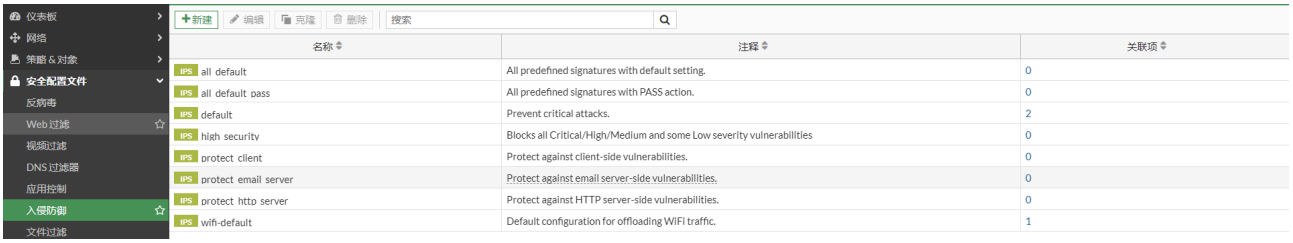
选择“安全配置文件”-->“IPS特征库”，可以查看具体的特征，将鼠标悬停在某一个特征上，可以查看该特征的详细信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

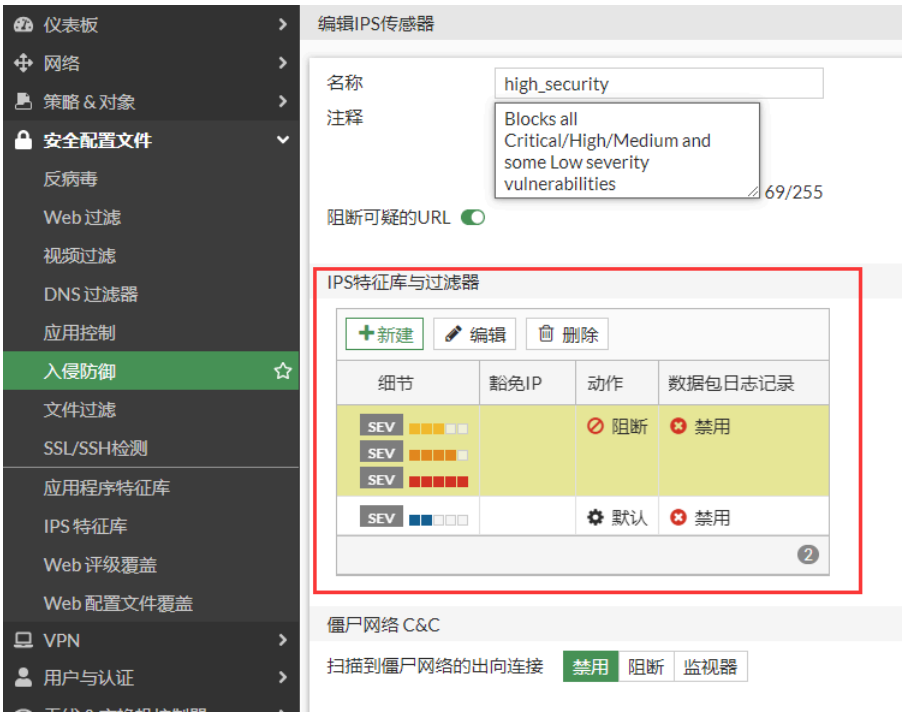


入侵防御配置文件

入侵防御默认有一些配置文件，这些配置文件应用的目标各有不同，也可以根据自身的业务需求创建新的配置文件。



在high_security配置文件中，IPS阻断严重级别是Critical/High/Medium的特征库，严重级别是Low的则是保持特征的默认动作。



在protect_http_server配置文件中，IPS将对象过滤器的属性设置为服务器，协议过滤器的属性设置为HTTP，因此过滤器仅包含适用于服务器的HTTP协议的签名，动作是使用特征默认的动作。

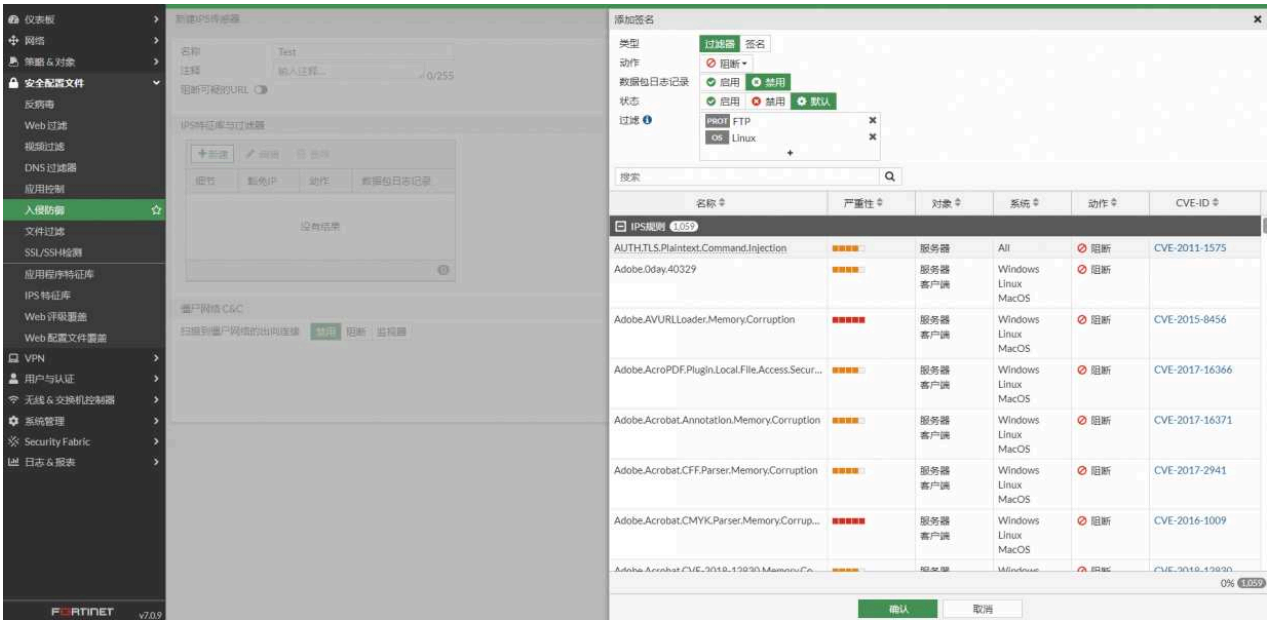
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



用户也可以根据自身的需求创建配置文件，选择“安全配置文件”-->“入侵防御”，点击“新建”，这里保护linux服务器的HTTP服务。

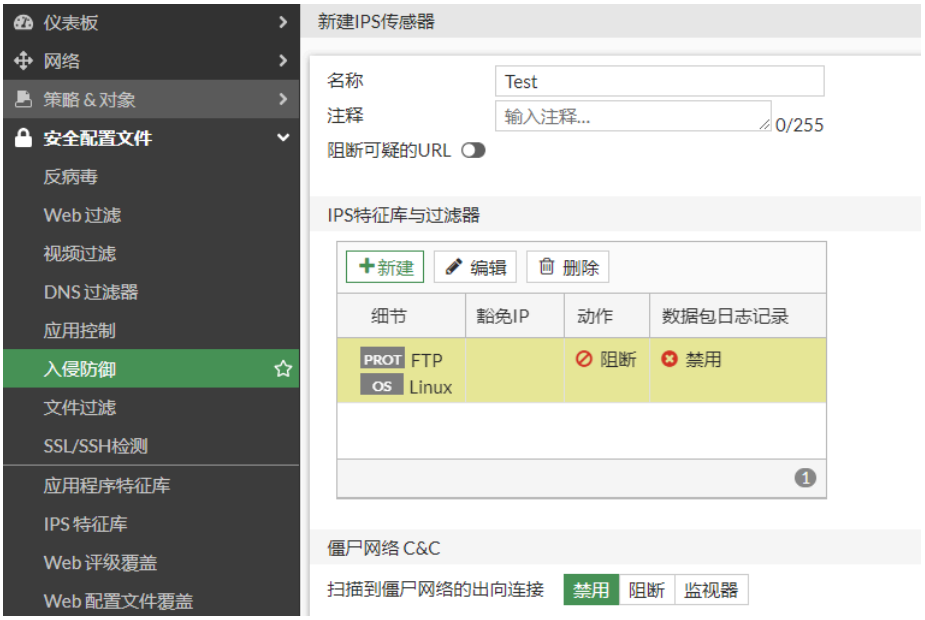
1. 创建IPS过滤器

在”IPS特征库与过滤器“选项下，点击“新建”，类型选择过滤器，动作设置为阻断，协议过滤器设置为FTP，OS过滤器设置为Linux。



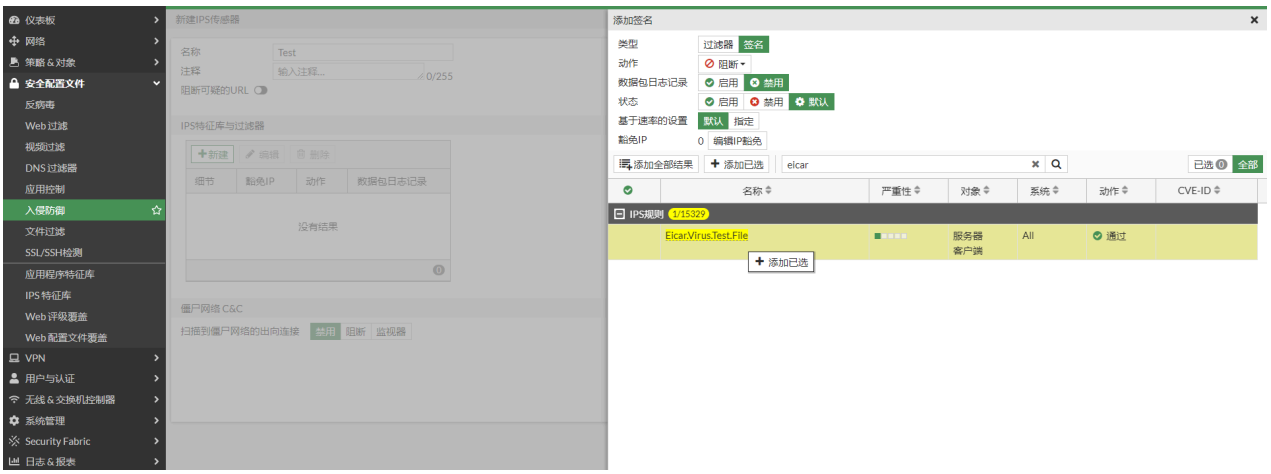
确定保存。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

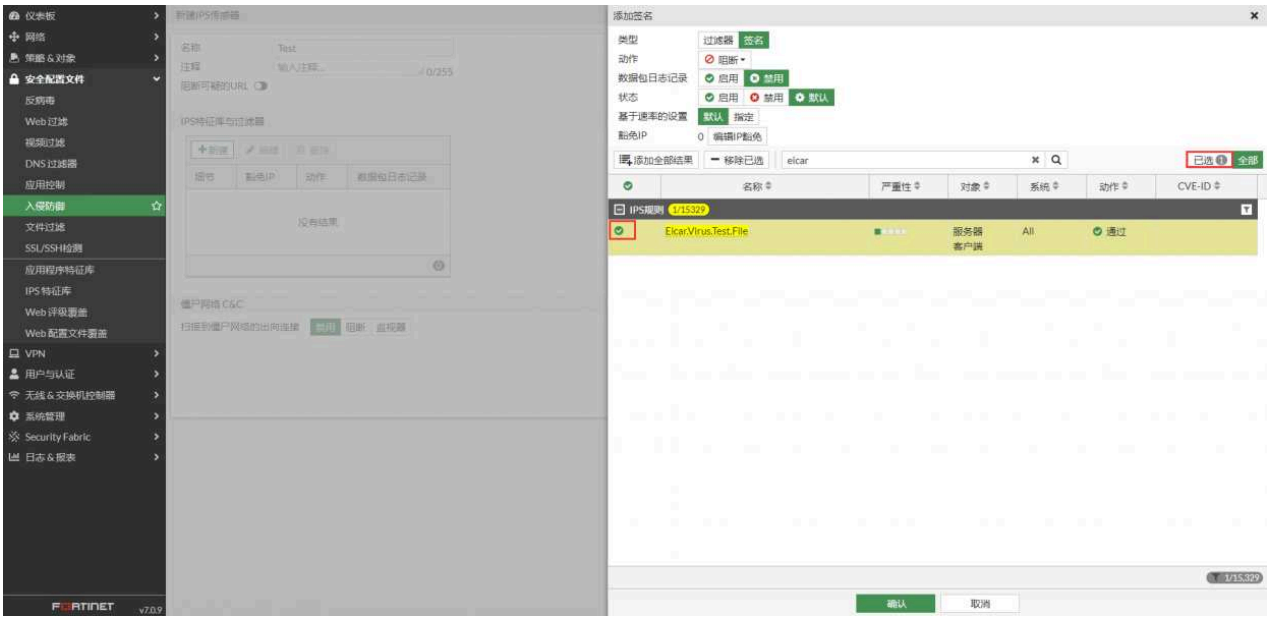


2. **指定某一个IPS具体的特征**

这里以eicar做测试。类型选择签名，动作设置为阻断，在搜索框中搜索eicar，将过滤出eicar的特征：Eicar.Virus.Test.File，然后右击该特征，点击“添加已选”，表示选中该特征。

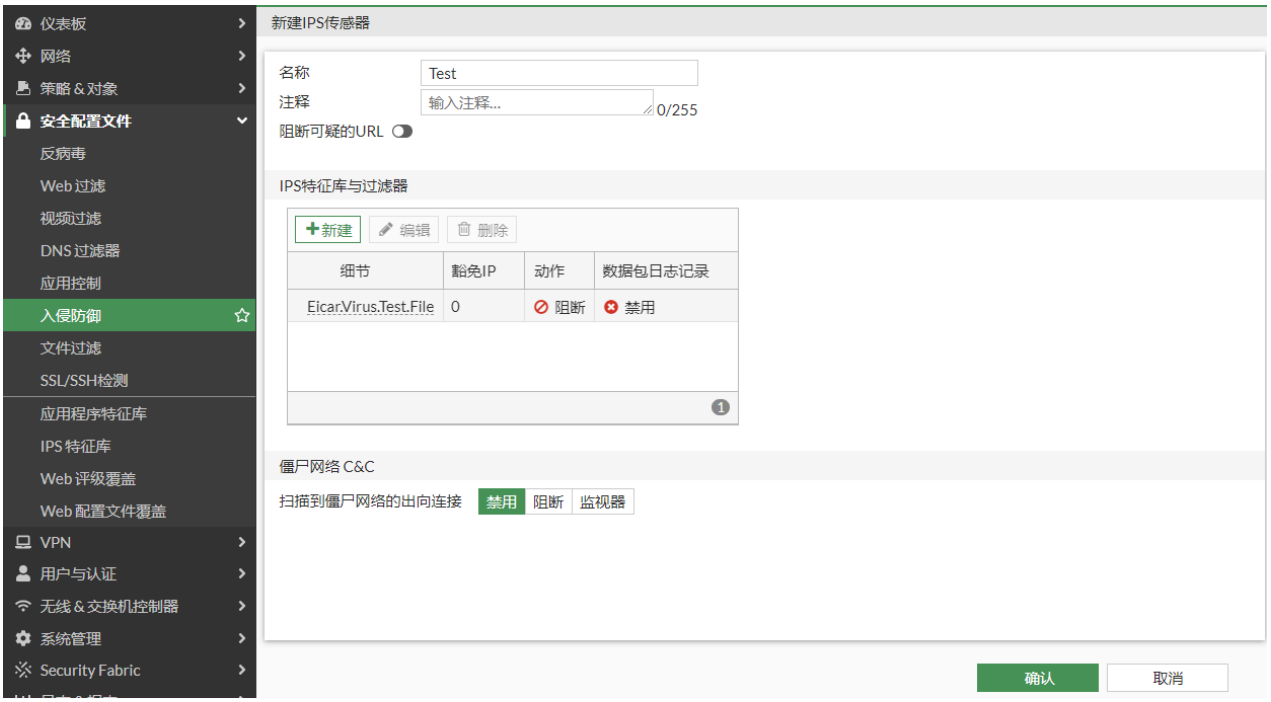


特征选中后，会有绿色勾选的标识，以及“已选”标签会标识出特征的数量，然后点击确认。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

确定保存。



3. **IPS规则的顺序**

如下图，严重级别过滤器设置为信息，该过滤器包含了eicar，动作是允许；单独设置eicar特征的动作是阻断；那么最终eicar的动作是允许。IPS规则是由上到下匹配的。



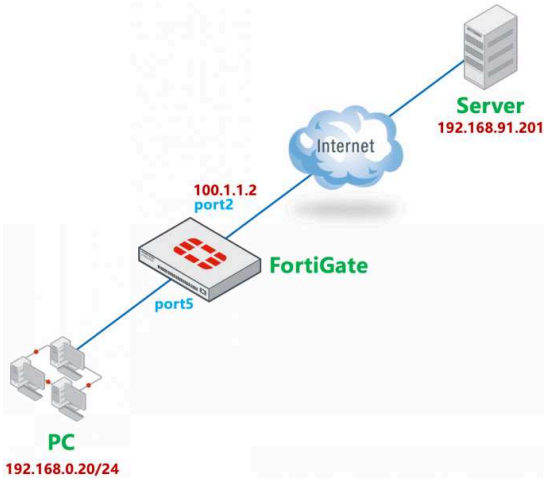
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

入侵防御配置

网络需求

客户使用IPS保护用户上网的流量。

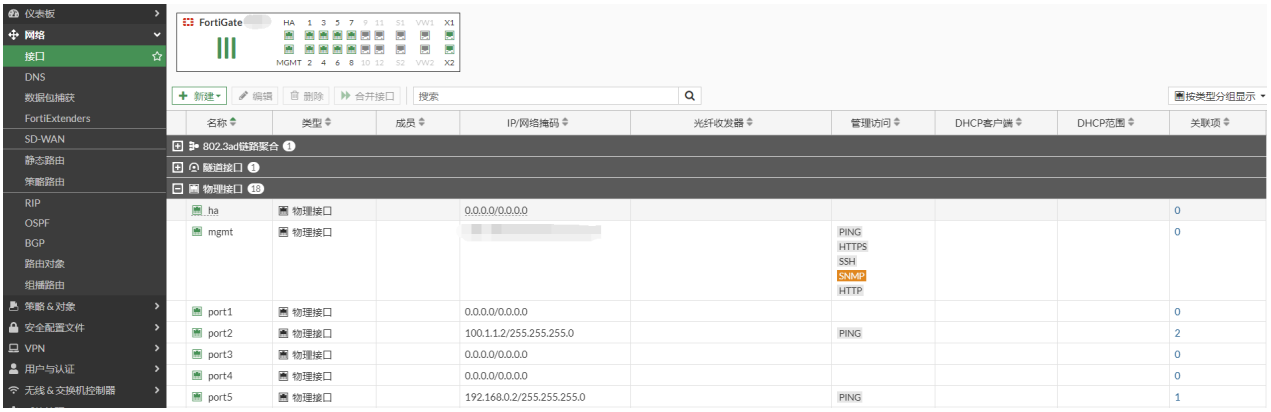
网络拓扑



配置步骤

1. **基本配置**

   配置接口IP和路由。





2. **配置IPS配置文件**

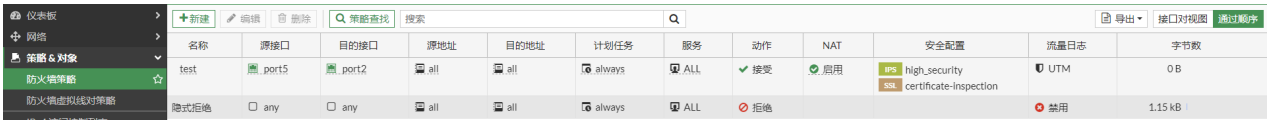
   这里直接使用默认的high_security配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



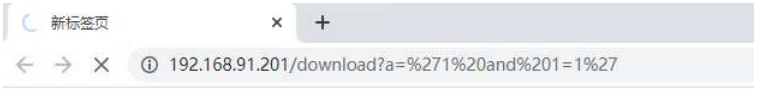
3. 配置策略

在策略中调用IPS配置文件。



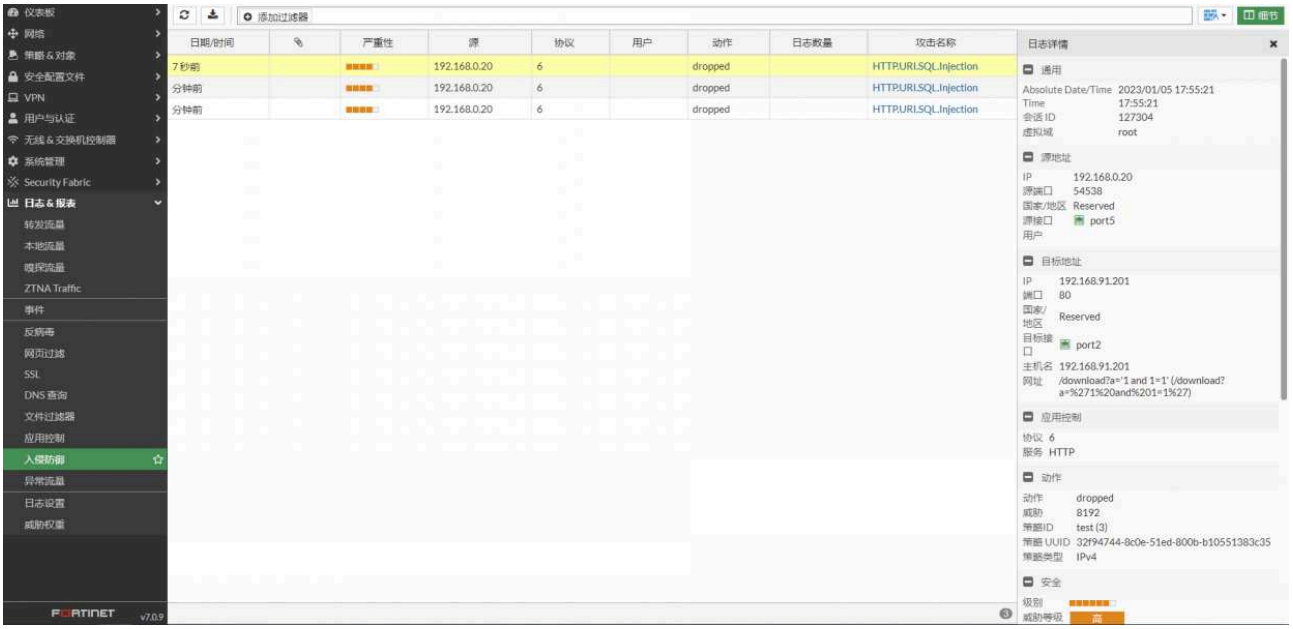
入侵防御测试

发起SQL注入攻击被IPS拦截。



查看IPS日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



安全

级别

威胁等级 高

威胁分数 30

Cellular

服务 HTTP

入侵防御

配置名称	high_security
攻击名称	HTTP.URI.SQL.Injection
攻击ID	15621
参考	http://www.fortinet.com/ids/VID15621
事件序列号	121635773
方向	outgoing
严重性	
消息	web_misc: HTTP.URI.SQL.Injection

其他

日志事件初始时间戳	1672912521315240700
Timezone	+0800
Log ID	0419016384
类型	utm
子类型	ips
事件类型	signature
源接口角色	undefined
目标接口角色	undefined

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

虚拟补丁

> **重要**
>
> 该功能在FortiOS 7.2.4及以后版本支持。

虚拟补丁介绍

虚拟补丁（Virtual Patch）是通过使用FortiGate的IPS Engine阻止已知漏洞来减轻漏洞攻击的方法。可以用在攻击目标为FortiGate自身的情况下，方法是使用FortiGate入接口上的Local-in Policy将FMWP（Firmware Virtual Patch）数据库应用到接口上。例如可以使用从FortiGuard推送的FMWP数据库来减轻针对GUI和SSL VPN的攻击，从而暂时地修补这些漏洞。

适用场景

适用于FortiGate自身存在漏洞，但暂时无法升级固件的情况（比如承载重要业务，短时间内不能升级重启）。当然，虚拟补丁只是权宜之计，最终仍然是推荐升级版本来解决漏洞问题。

实现原理

当在Local-in Policy中启用虚拟补丁时，IPS Engine会查询FortiGuard服务器，并执行如下动作：

- 获取针对当前FortiGate固件版本的漏洞列表。
- 根据Local-in会话中的服务（协议和端口号），确定流向FortiGate上本地入接口的会话是否需要扫描。目前，仅可以检查SSL VPN和Web GUI的本地流量。
- 如果经过检查，匹配Local-in Policy的会话所属功能没有包含在该FortiOS版本漏洞的功能类型中，则IPS Engine会绕过该会话（例如IPS Engine从FortiGuard获取的当前固件版本的漏洞只有关于SSL VPN的漏洞，没有关于GUI的漏洞，那么IPS Engine会自动Bypass所有GUI访问的Local-in会话流量）。IPS Engine仅扫描和丢弃可能正在利用漏洞的会话来优化性能。

配置方法

```bash
config firewall local-in-policy
    edit <id>
        set action accept
        set virtual-patch {enable | disable}
    next
end
```

配置步骤

举例1

虚拟补丁查询FortiGuard，此FortiOS版本只存在SSL VPN漏洞。IPS Engine会丢弃到FortiGate本地接口的SSL VPN的攻击流量，并绕过Web GUI流量。

1. 首先需要FortiGate具有FMWP License。

```bash
FortiGate # diagnose autoupdate versions | grep FMWP -A 6
FMWP Definitions
————————
Version: 24.00013 signed
Contract Expiry Date: Fri Feb  2 2024
Last Updated using scheduled update on Thu Feb  1 02:18:21 2024
Last Update Attempt: Thu Feb  1 16:48:12 2024
Result: No Updates
```

2. 在FortiGate的公网接口上，配置Local-in Policy，动作为accept，开启虚拟补丁，Service选择HTTPS和SSL VPN的端口（Service请根据您的FortiGate配置的HTTPS和SSL VPN端口来配置）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall local-in-policy
    edit 1
        set intf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSL_VPN_10443"
        set schedule "always"
        set virtual-patch enable
    next
end
```

3. 查看当前虚拟补丁从FortiGuard获取的漏洞信息，只包含SSL VPN漏洞，不包含GUI访问漏洞（7.4版本的CLI为`diagnose ips vpatch fmwp-status`）。

```
FortiGate # diagnose ips vpatch status
Enabled FMWP signatures: 1

  10002887 FortiOS.SSL-VPN.Heap.Buffer.Overflow.
```

4. 针对此漏洞进行攻击，攻击流量被IPS Engine拦截，如下为攻击的IPS拦截日志，GUI访问流量被IPS Engine bypass，不会产生IPS日志。

```bash
1: date=2023-11-07 time=14:53:44 eventtime=1699325624346021995 tz="+1200" logid="0419016384" type="utm"
subtype="ips" eventtype="signature" level="alert" vd="root" severity="critical" srcip=10.1.100.22
srccountry="Reserved" dstip=10.1.100.1 dstcountry="Reserved" srcintf="port2" srcintfrole="undefined"
dstintf="root" dstintfrole="undefined" sessionid=284 action="dropped" proto=6 service="HTTPS" policyid=1
attack="FortiOS.SSL-VPN.Heap.Buffer.Overflow." srcport=53250 dstport=11443 hostname="myfortigate.example"
url="/error" httpmethod="POST" direction="outgoing" attackid=10002887
ref="http://www.fortinet.com/ids/VID10002887" incidentserialno=99614721 msg="vPatch: FortiOS.SSL-
VPN.Heap.Buffer.Overflow." crscore=50 craction=4096 crlevel="critical"
```

举例2

虚拟补丁查询FortiGuard，此FortiOS版本只存在GUI访问漏洞。IPS Engine会丢弃到FortiGate本地接口的GUI访问的攻击流量，并绕过SSL VPN流量。

1. 在FortiGate的公网接口上，配置Local-in Policy，动作为accept，开启虚拟补丁，Service选择HTTPS和SSL VPN的端口（Service请根据您的FortiGate配置的HTTPS和SSL VPN端口来配置）。

```bash
config firewall local-in-policy
    edit 1
        set intf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSL_VPN_10443"
        set schedule "always"
        set virtual-patch enable
    next
end
```

2. 查看当前虚拟补丁从FortiGuard获取的漏洞信息，只包含SSL VPN漏洞，不包含GUI访问漏洞（7.4版本的CLI为`diagnose ips vpatch fmwp-status`）。

```bash
FortiGate # diagnose ips vpatch status
Enabled FMWP signatures: 2

  10002156 FortiOS.NodeJS.Proxy.Authentication.Bypass.
  10002890 FortiOS.HTTPD.Content-Length.Memory.Corruption.
```

3. 针对此漏洞进行攻击，攻击流量被IPS Engine拦截，如下为攻击的IPS拦截日志，SSL VPN访问流量被IPS Engine bypass，不会产生IPS日志。

```bash
1: date=2023-11-07 time=14:55:15 eventtime=1699325715311370215 tz="+1200" logid="0419016384" type="utm"
subtype="ips" eventtype="signature" level="alert" vd="root" severity="critical" srcip=10.1.100.22
srccountry="Reserved" dstip=10.1.100.1 dstcountry="Reserved" srcintf="port2" srcintfrole="undefined"
dstintf="root" dstintfrole="undefined" sessionid=304 action="dropped" proto=6 service="HTTPS" policyid=1
attack="FortiOS.NodeJS.Proxy.Authentication.Bypass." srcport=53622 dstport=443 hostname="127.0.0.1:9980"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
url="/api/v2/cmdb/system/admin" agent="Node.js" httpmethod="GET" direction="outgoing" attackid=10002156
ref="http://www.fortinet.com/ids/VID10002156" incidentserialno=99614722 msg="vPatch:
FortiOS.NodeJS.Proxy.Authentication.Bypass." crscore=50 craction=4096 crlevel="critical"
```

举例3

虚拟补丁查询FortiGuard，此FortiOS版本同时存在GUI访问漏洞和SSL VPN漏洞。IPS Engine会丢弃到FortiGate本地接口的GUI访问的攻击流量，并绕过SSL VPN流量。

1. 在FortiGate的公网接口上，配置Local-in Policy，动作为accept，开启虚拟补丁，Service选择HTTPS和SSL VPN的端口（Service请根据您的FortiGate配置的HTTPS和SSL VPN端口来配置）。

```bash
config firewall local-in-policy
    edit 1
        set intf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "HTTPS" "SSL_VPN_10443"
        set schedule "always"
        set virtual-patch enable
    next
end
```

2. 查看当前虚拟补丁从FortiGuard获取的漏洞信息，同时包含SSL VPN漏洞和GUI访问漏洞（7.4版本的CLI为`diagnose ips vpatch fmwp-status`）。

```bash
FortiGate # diagnose ips vpatch status
Enabled FMWP signatures: 3

  10002156 FortiOS.NodeJS.Proxy.Authentication.Bypass.
  10002887 FortiOS.SSL-VPN.Heap.Buffer.Overflow.
  10002890 FortiOS.HTTPD.Content-Length.Memory.Corruption.
```

3. 针对这些漏洞进行攻击，攻击流量被IPS Engine拦截，如下为攻击的IPS拦截日志，SSL VPN和GUI访问流量均会产生IPS日志。

```bash
1: date=2023-11-07 time=06:42:44 eventtime=1699296164649894963 tz="+1200" logid="0419016384" type="utm"
subtype="ips" eventtype="signature" level="alert" vd="root" severity="critical" srcip=10.1.100.22
srccountry="Reserved" dstip=10.1.100.1 dstcountry="Reserved" srcintf="port2" srcintfrole="undefined"
dstintf="root" dstintfrole="undefined" sessionid=1094 action="dropped" proto=6 service="HTTPS" policyid=1
attack="FortiOS.SSL-VPN.Heap.Buffer.Overflow." srcport=44164 dstport=10443 hostname="myfortigate.example"
url="/error" httpmethod="POST" direction="outgoing" attackid=10002887
ref="http://www.fortinet.com/ids/VID10002887" incidentserialno=116392250 msg="vPatch: FortiOS.SSL-
VPN.Heap.Buffer.Overflow." crscore=50 craction=4096 crlevel="critical"

2: date=2023-11-07 time=06:42:09 eventtime=1699296129458704870 tz="+1200" logid="0419016384" type="utm"
subtype="ips" eventtype="signature" level="alert" vd="root" severity="critical" srcip=10.1.100.22
srccountry="Reserved" dstip=10.1.100.1 dstcountry="Reserved" srcintf="port2" srcintfrole="undefined"
dstintf="root" dstintfrole="undefined" sessionid=1066 action="dropped" proto=6 service="HTTPS" policyid=1
attack="FortiOS.NodeJS.Proxy.Authentication.Bypass." srcport=42352 dstport=443 hostname="127.0.0.1:9980"
url="/api/v2/cmdb/system/admin" agent="Node.js" httpmethod="GET" direction="outgoing" attackid=10002156
ref="http://www.fortinet.com/ids/VID10002156" incidentserialno=116392236 msg="vPatch:
FortiOS.NodeJS.Proxy.Authentication.Bypass." crscore=50 craction=4096 crlevel="critical"
```

其他CLI命令

通过CLI查询特定版本的漏洞信息。

```bash
FortiGate # diagnose wad dev-vuln query vendor=fortinet&version=7.2.5&product=fortios
Dev-Vuln Lookup result: success, cache: found, fgd: unknown, item: 0x7fb474e0b4a0
Vulnerability details:
info entry (1):
        'vendor' = fortinet
       'product' = fortios
         'model' = N/A
   'version.min' = 7.2.0
   'version.max' = 7.2.5
      'firmware' = N/A
         'build' = N/A
    'date_added' = 2023-08-22T13:09:11
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  'date_updated' = 2023-08-22T13:09:11
       'sig_id' = 10004065
     'vuln_id' = 918630
    'severity' = 3
...
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

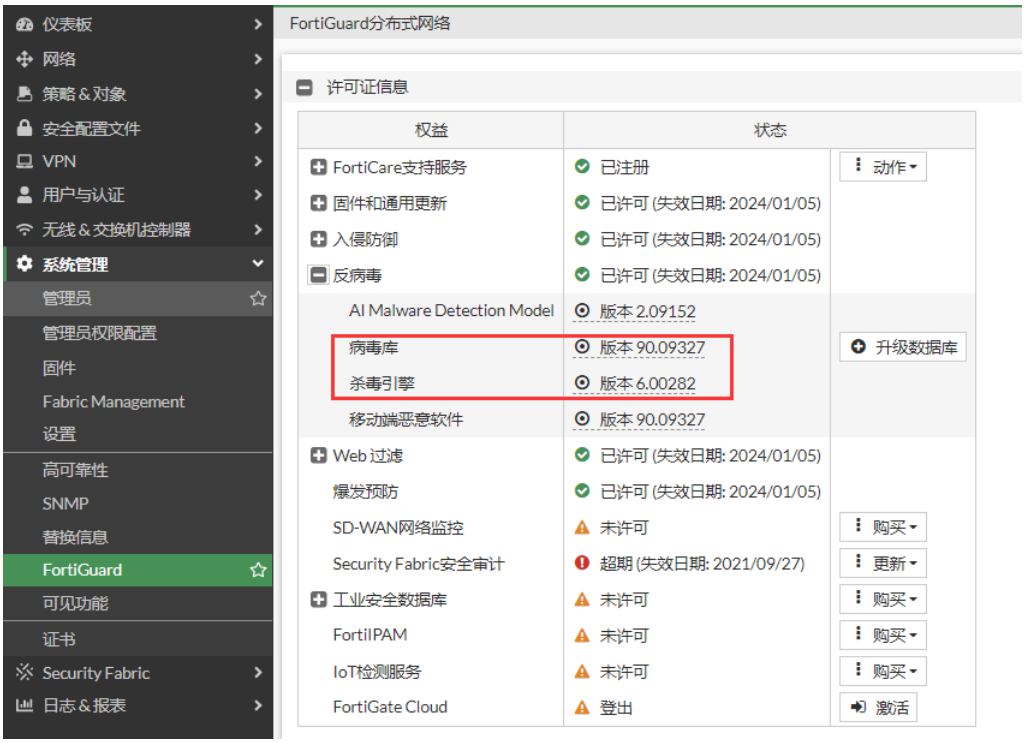
反病毒简介

什么是AV反病毒

AV反病毒功能凭借庞大且不断更新的病毒特征库有效保护企业内网用户和服务器免受病毒文件侵害。AV通过特征库检测来识别流量中的病毒文件， 如果检测到威胁，则按照安全防御策略采取适当的措施，比如阻止访问，避免由病毒文件而引起的数据破坏、权限更改和系统崩溃等情况的发生，保证网络的安全。

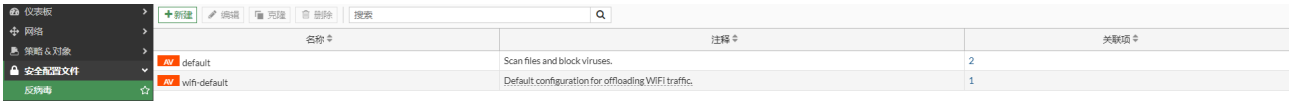
反病毒特征库

选择“系统管理”-->“FortiGuard”-->“许可证信息”，在“反病毒菜单”下可以查看AV特种库的版本及AV引擎的版本。



反病毒配置文件

反病毒默认自带两个配置文件，这两个配置文件设置是一样，只是描述性信息不一样。



默认使用default配置文件即可，动作默认是阻断，可根据实际情况调整。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



用户也可以根据自身的需求创建配置文件，选择“安全配置文件”-->“反病毒”，点击“新建”，这里保护HTTP服务。



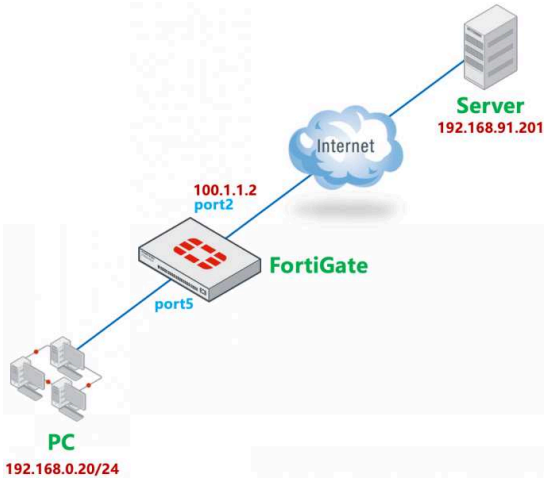
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

反病毒配置

网络需求

客户使用AV保护用户上网的流量。

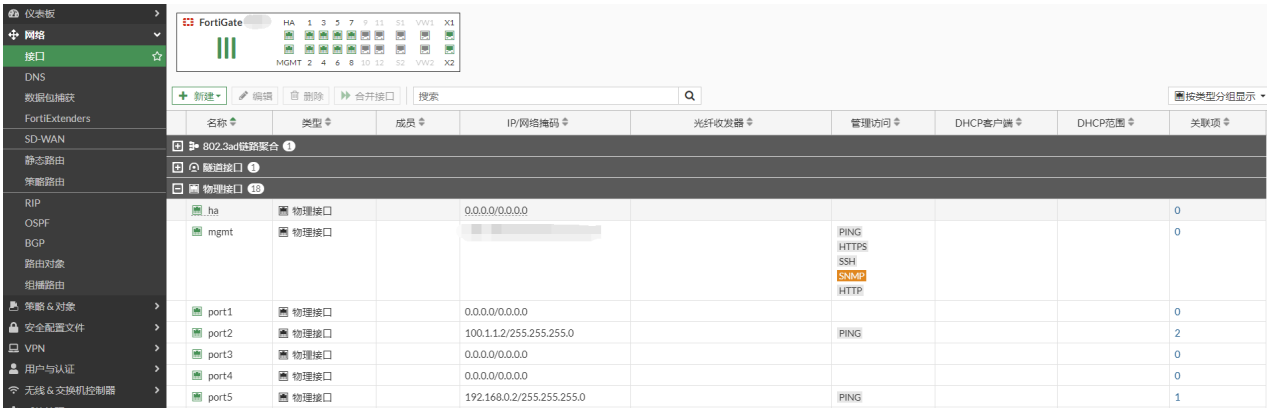
网络拓扑



配置步骤

1. 基本配置

   配置接口IP和路由。





2. 配置IPS配置文件

   这里使用默认的default配置文件。测试环境中使用eicar做测试。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



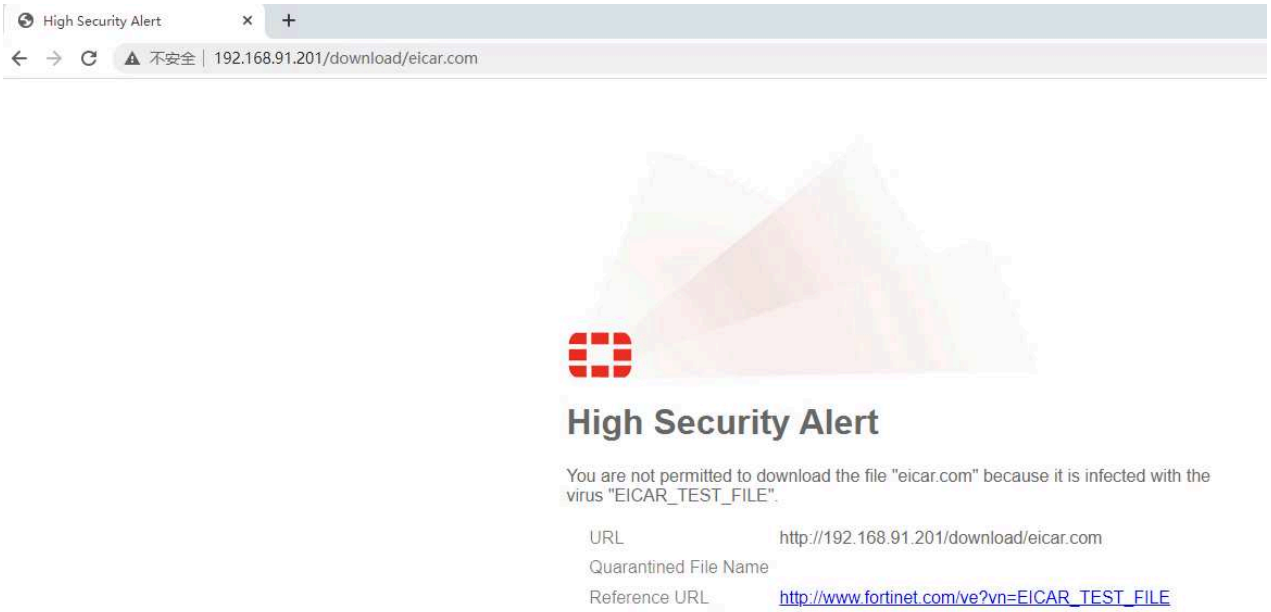
3. **配置策略**



反病毒测试

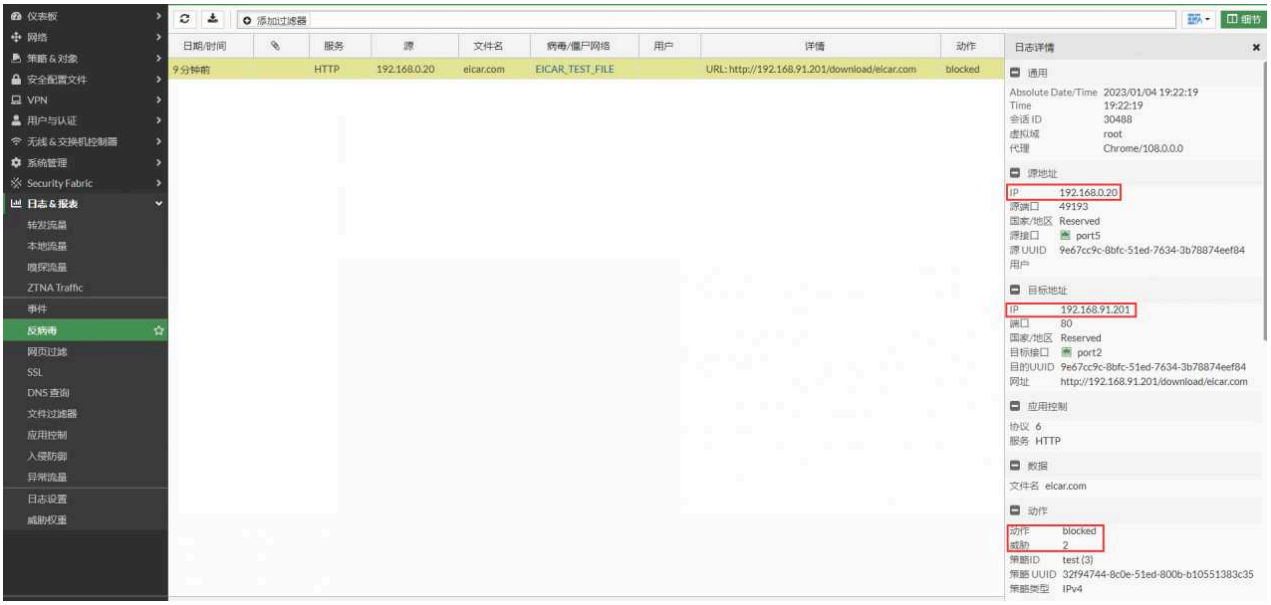
1. **使用PC下载eicar.com文件**

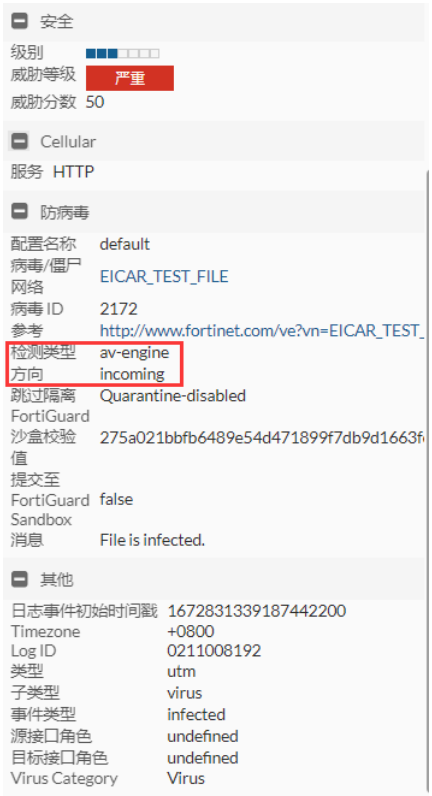
PC下载eicar.com时，被AV检测到并拦截。



查看反病毒日志。对于发起方192.168.0.20而言，攻击是从192.168.91.201到192.168.0.20，因此方向是incoming。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

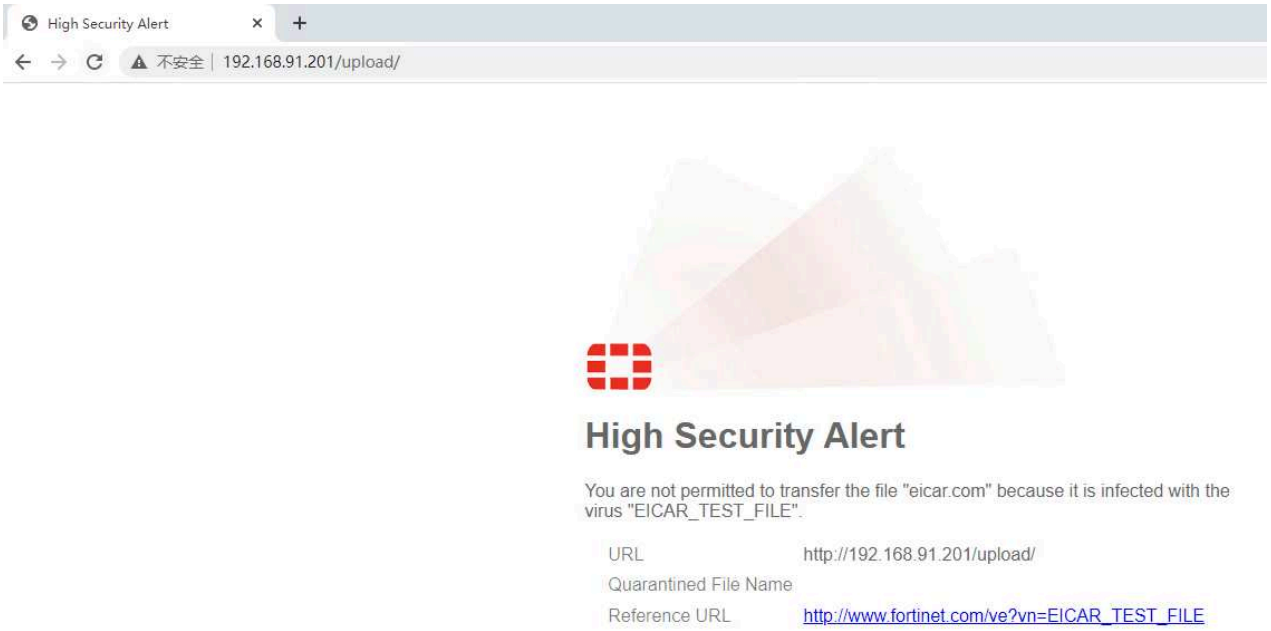




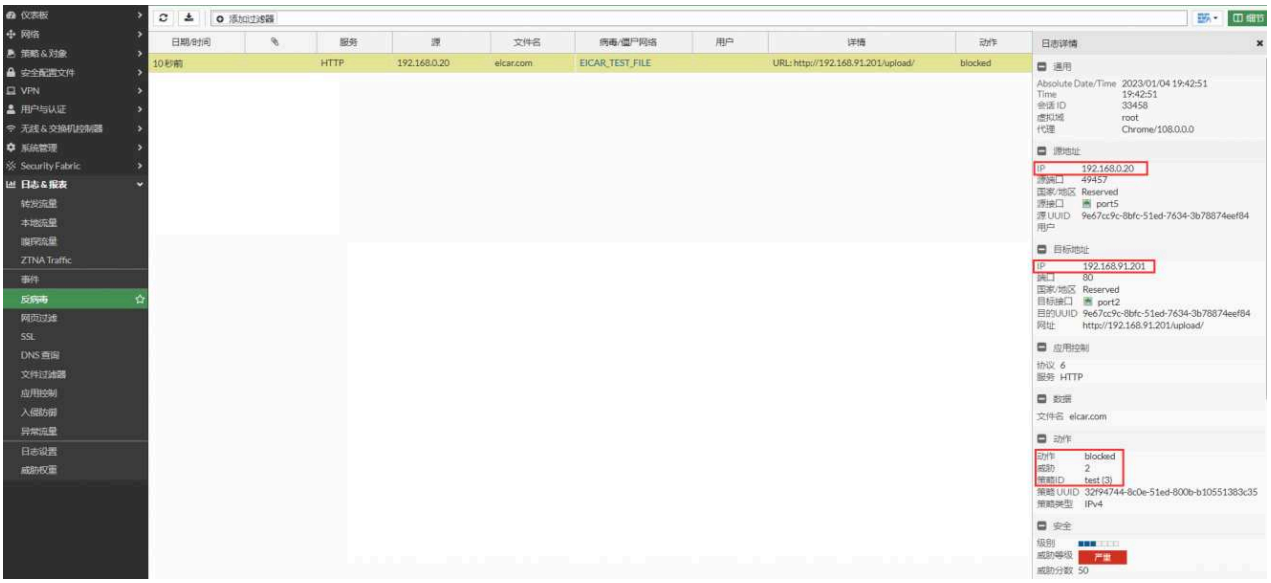
2. **使用PC上传eicar.com** ↗

   PC上传eicar.com时，被AV检测到并拦截。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看反病毒日志。对于发起方192.168.0.20而言，攻击是从192.168.0.20到192.168.91.201，因此方向是outgoing。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Cellular

服务	HTTP

防病毒

配置名称	default
病毒/僵尸网络	EICAR_TEST_FILE
病毒 ID	2172
参考	http://www.fortinet.com/ve?vn=EICAR_TEST_
检测类型	av-engine
方向	outgoing
跳过隔离	Quarantine-disabled
FortiGuard 沙盒校验值	275a021bbfb6489e54d471899f7db9d1663f
提交至 FortiGuard Sandbox	false
消息	File is infected.

其他

日志事件初始时间戳	1672832572227783400
Timezone	+0800
Log ID	0211008192
类型	utm
子类型	virus
事件类型	infected
源接口角色	undefined
目标接口角色	undefined
Virus Category	Virus

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于文件Hash的AV豁免

> **重要**
>
> 该功能在FortiOS 7.2.4及以上版本支持。

网络需求

在反病毒功能的使用中，如果有安全的文件被反病毒功能误判并阻止，用户需要向FortiGuard提交误报信息，然后等待官方确认和修复，需要等待一定的时间。需要可以对误判文件进行豁免操作，以允许即时传输该文件。

功能介绍

FortiGate允许对反病毒误判的文件进行豁免。用户可以指定文件的MD5、SHA1或SHA256哈希值进行匹配，当匹配FortiGate AV的白名单时，该文件会被Bypass。

> **重要**
>
> 豁免列表功能不适用于Outbreak Prevention、Machine-Learning、FortiNDR和FortiSandbox inline scans。

配置方法

此功能仅支持在CLI下配置。

```bash
config antivirus exempt-list
    edit <name>
        set hash-type {md5 | sha1 | sha256}
        set hash <string>
        set status {enable | disable}
    next
end
```

配置步骤与配置验证

1. 获取被误判文件的Hash值，这里以一个Eicar文件`csm-eicar.com`为例，该文件的MD5值为`44d88612fea8a8f36de82e1278abb02f`，该文件位于`www.csm-testcenter.org`网站。
2. 按需在“安全配置文件→反病毒”页面中配置反病毒配置文件，这里以“default”配置文件为例。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



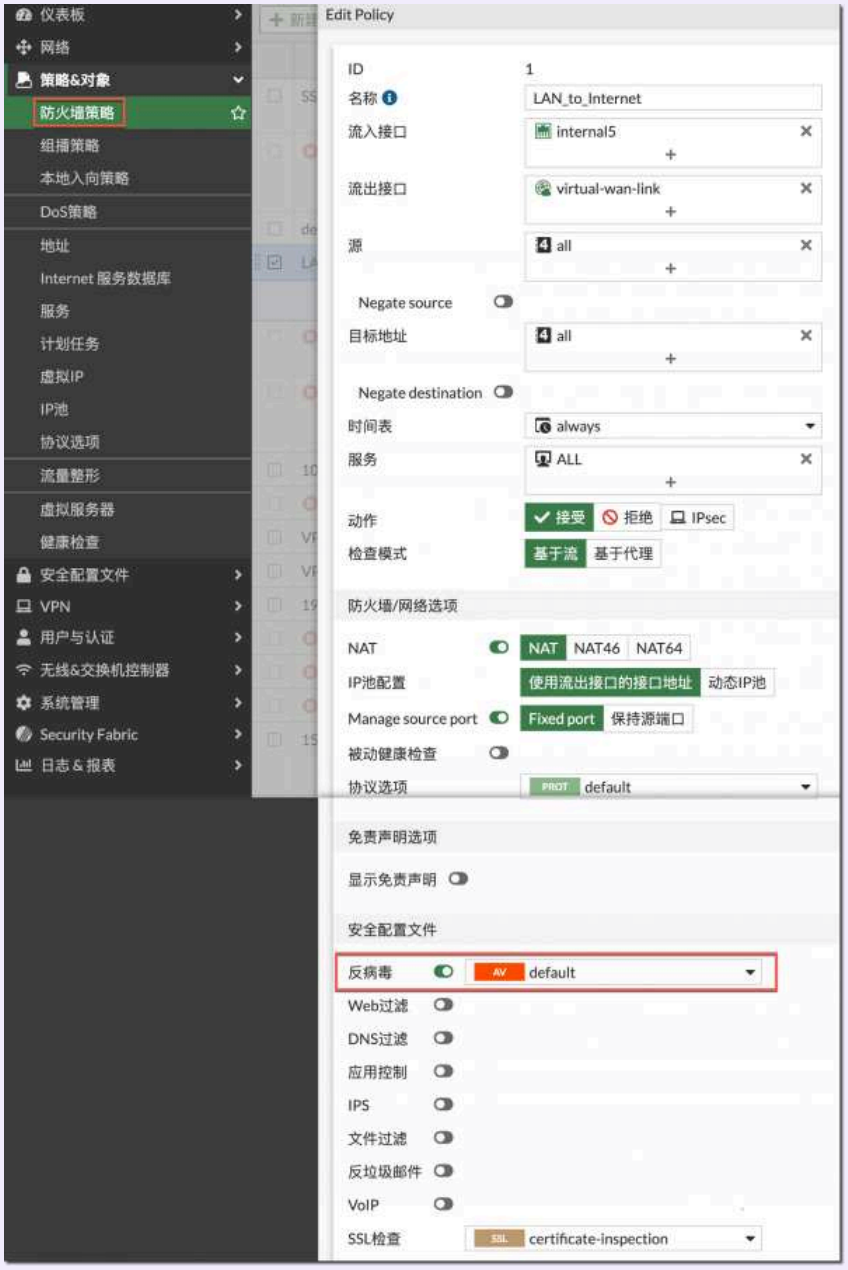
3. 在防火墙策略中引用该反病毒配置文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

- FortiOS 7.2.X版本需要防火墙策略的“检测模式”使用`proxy`（基于代理）模式才能生效。
- FortiOS 7.4.X版本的防火墙策略“检测模式”没有要求。

:::




```bash
config firewall policy
    edit 1
        set name "LAN_to_Internet"
        set srcintf "internal5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set nat enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 此时使用客户端PC使用HTTP穿过FortiGate下载该文件，下载失败。

```bash
root@Ubuntu # wget http://www.csm-testcenter.org/csm-eicar.com
--2025-11-11 16:03:51--  http://www.csm-testcenter.org/csm-eicar.com
正在解析主机 www.csm-testcenter.org (www.csm-testcenter.org)... 85.215.35.144
正在连接 www.csm-testcenter.org (www.csm-testcenter.org)|85.215.35.144|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：68 [application/octet-stream]
正在保存至："csm-eicar.com.1"
csm-eicar.com.1                 0%[                                                    ]       0  --.-KB/s  用时 0s
2025-11-11 16:03:52 (0.00 B/s) - 在 0/68 字节处发生读取错误 (Connection reset by peer)。重试中。
--2025-11-11 16:03:53--  (尝试次数： 2)  http://www.csm-testcenter.org/csm-eicar.com
正在连接 www.csm-testcenter.org (www.csm-testcenter.org)|85.215.35.144|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 403 Forbidden
2025-11-11 16:03:53 错误 403：Forbidden。
```

5. 该文件下载时被FortiGate的反病毒模块拦截，如下所示AV拦截日志。




```bash
date=2025-11-11 time=16:03:54 eventtime=1762848233896917415 tz="+0800" logid="0211008192" type="utm"
subtype="virus" eventtype="infected" level="warning" vd="root" policyid=1 poluuid="7933a8ea-da0e-51ee-d747-
443a0247aebe" policytype="policy" msg="File is infected." action="blocked" service="HTTP" sessionid=48151480
srcip=192.168.100.177 dstip=85.215.35.144 srcport=60122 dstport=80 srccountry="Reserved" dstcountry="Germany"
srcintf="internal5" srcintfrole="undefined" dstintf="wan1" dstintfrole="undefined" srcuuid="477325da-a1dc-51ed-
ecdd-9add8d1533e2" dstuuid="477325da-a1dc-51ed-ecdd-9add8d1533e2" proto=6 direction="incoming" filename="csm-
eicar.com" checksum="6851cf3c" quarskip="No-skip" virus="EICAR_TEST_FILE" viruscat="Virus" dtype="cached"
ref="https://fortiguard.com/encyclopedia/virus/2172" virusid=2172 url="http://www.csm-testcenter.org/csm-
eicar.com" profile="default" agent="Wget/1.21.4" httpmethod="GET"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f" analyticssubmit="false"
crscore=50 craction=2 crlevel="critical"
```

6. 在CLI下配置反病毒豁免列表，Hash类别为MD5，将该文件的MD5值填入其中。

```bash
config antivirus exempt-list
    edit "csm-eicar.com"
        set hash-type md5
        set hash "44d88612fea8a8f36de82e1278abb02f"
    next
end
```

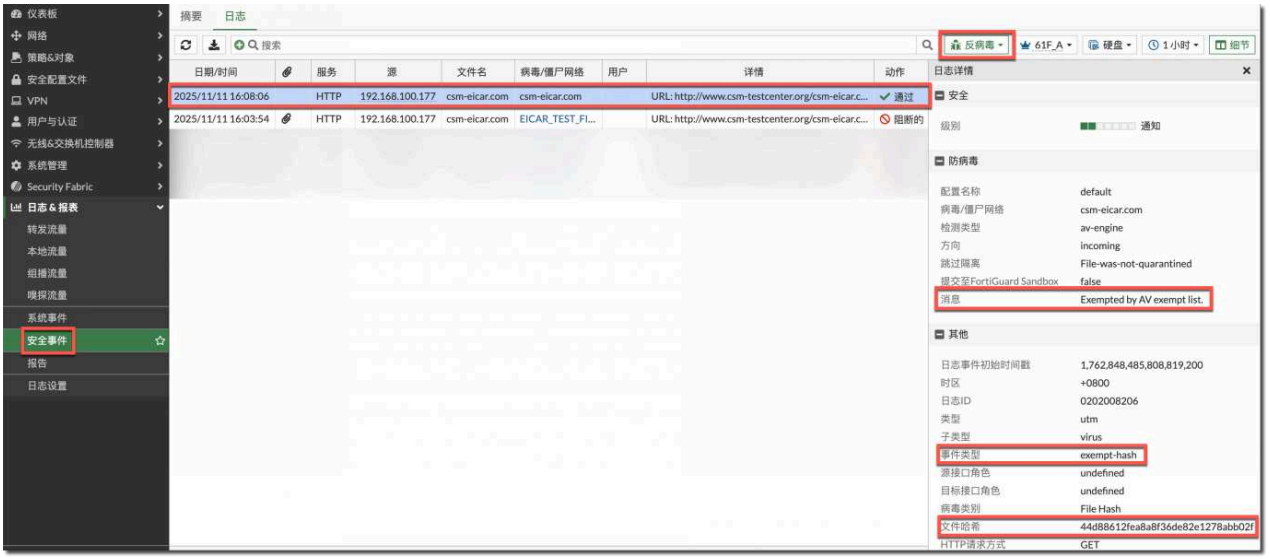
7. 再次使用客户端PC通过FortiGate下载该文件，下载成功。

```bash
root@Ubuntu # wget http://www.csm-testcenter.org/csm-eicar.com
--2025-11-11 16:08:04--  http://www.csm-testcenter.org/csm-eicar.com
正在解析主机 www.csm-testcenter.org (www.csm-testcenter.org)... 85.215.35.144
正在连接 www.csm-testcenter.org (www.csm-testcenter.org)|85.215.35.144|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：68 [application/octet-stream]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
正在保存至: “csm-eicar.com.2”

csm-eicar.com.2                100%[═══════════════════════════════════════════════════════⇒]      68   331 B/s  用时 0.2s

2025-11-11 16:08:05 (331 B/s) - 已保存 “csm-eicar.com.2” [68/68])
```

8. 该文件下载时被FortiGate的反病毒模块放通，如下所示AV拦截日志，日志中提示被该文件“Exempted by AV exempt list”。




```
date=2025-11-11 time=16:08:06 eventtime=1762848485808819095 tz="+0800" logid="0202008206" type="utm"
subtype="virus" eventtype="exempt-hash" level="notice" vd="root" policyid=1 poluuid="7933a8ea-da0e-51ee-d747-
443a0247aebe" policytype="policy" msg="Exempted by AV exempt list." action="passthrough" service="HTTP"
sessionid=48156818 srcip=192.168.100.177 dstip=85.215.35.144 srcport=62065 dstport=80 srccountry="Reserved"
dstcountry="Germany" srcintf="internal5" srcintfrole="undefined" dstintf="wan1" dstintfrole="undefined"
srcuuid="477325da-a1dc-51ed-ecdd-9add8d1533e2" dstuuid="477325da-a1dc-51ed-ecdd-9add8d1533e2" proto=6
direction="incoming" filename="csm-eicar.com" quarskip="File-was-not-quarantined" virus="csm-eicar.com"
viruscat="File Hash" dtype="av-engine" filehash="44d88612fea8a8f36de82e1278abb02f" url="http://www.csm-
testcenter.org/csm-eicar.com" profile="default" agent="Wget/1.21.4" httpmethod="GET" analyticssubmit="false"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

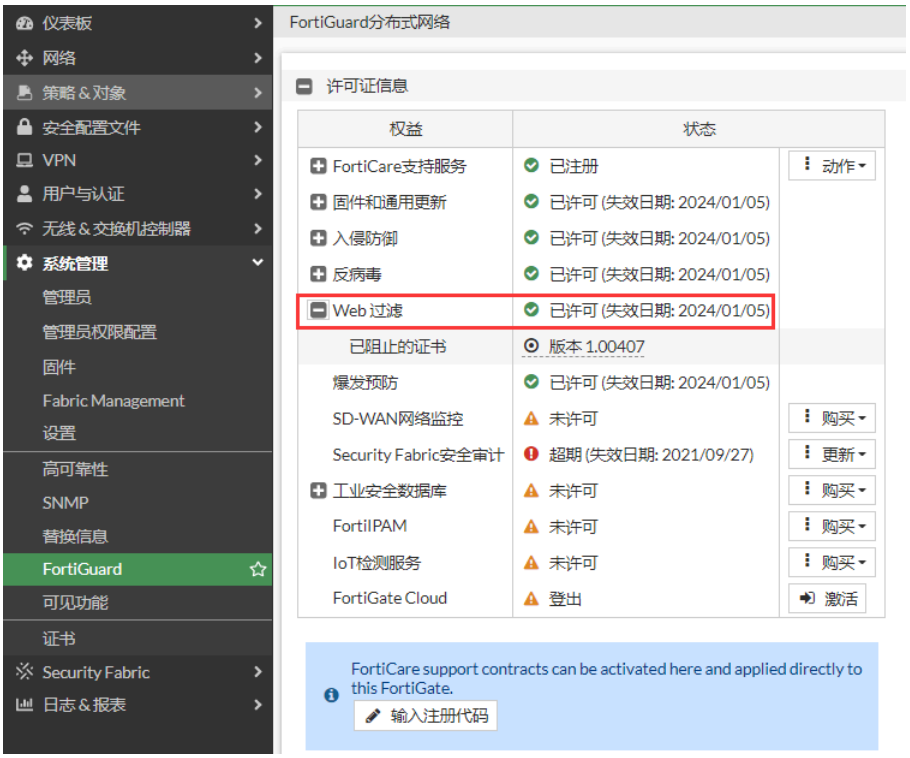
Web过滤简介

什么是Web过滤

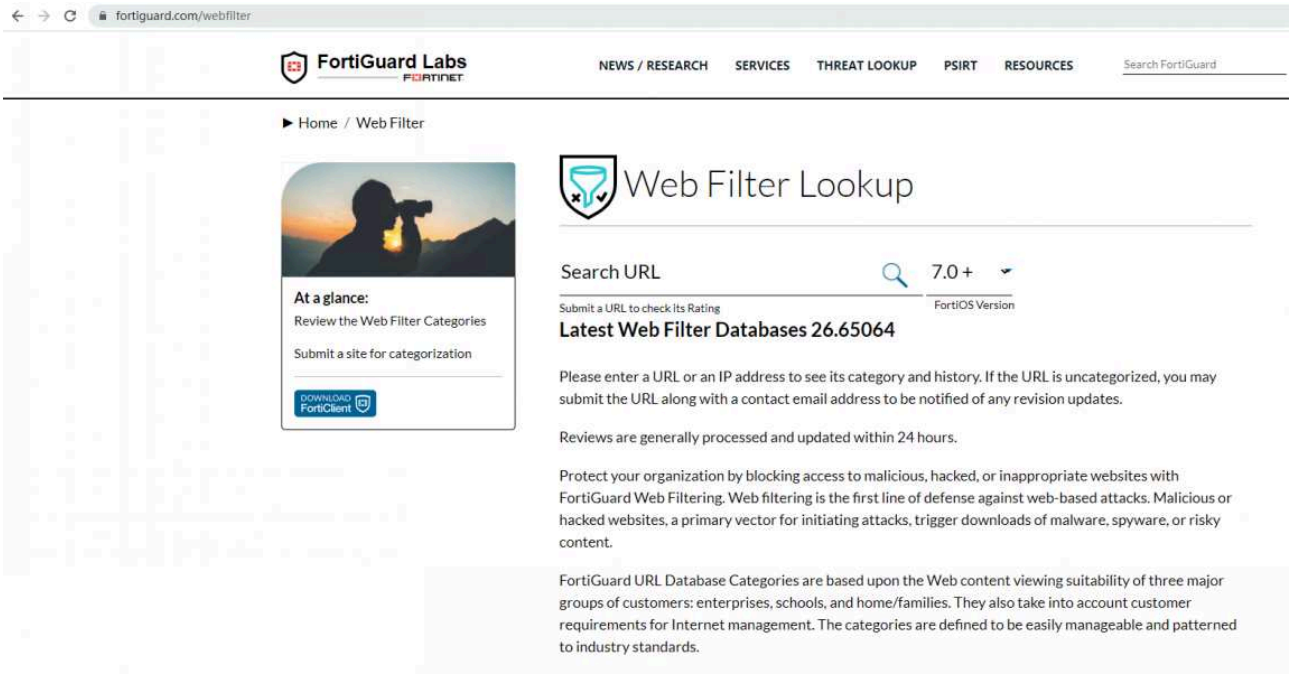
Web过滤是FortiGate对用户访问Web资源进行限制或控制的功能。

Web过滤特征库

选择“系统管理”-->“FortiGuard”-->“许可证信息”，查看Web过滤的状态是有license的。Web过滤的特征库在云端，不在FortiGate本地。

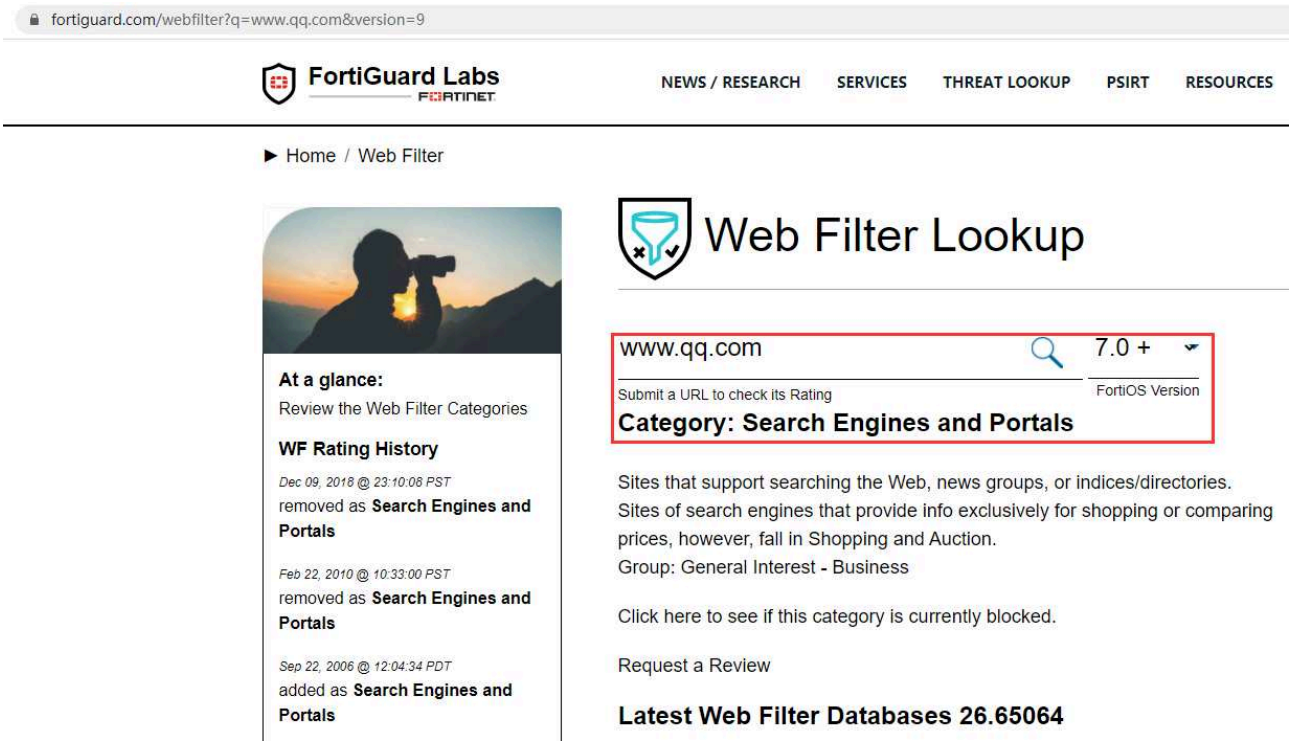


在FortiGuard上查看Webfilter特征库。



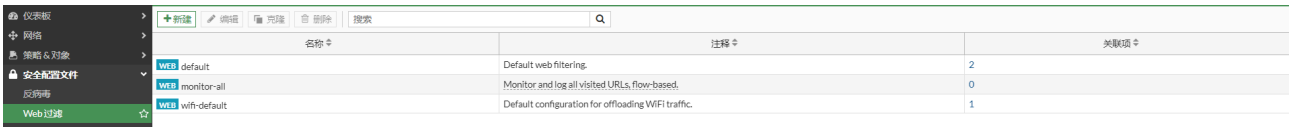
输入网站，可以查询该URL属于哪个分类。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



web过滤配置文件

web过滤默认有一些配置文件，这些配置文件应用的目标各有不同，也可以根据自身的业务需求创建新的配置文件。



default配置文件默认对成人内容，不安全的内容等进行阻断，对其他的内容进行监控。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



monitor-all配置文件对所有的内容都进行监控。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



用户也可以根据自身的需求创建配置文件，选择“安全配置文件”-->“Web过滤”，点击“新建”。如这里通过“URL过滤器”只允许用户访问 support.fortinet.com.cn ↗，其他网站都拒绝。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



URL过滤与WebFilter的执行顺序

1. 如果URL过滤的动作是允许或监视器，那么将继续执行WebFilter分类过滤（如果WebFilter通过查询FortiGuard的分类的匹配动作是拒绝，那么该URL仍然会被拒绝）。
2. 如果URL过滤的动作是拒绝，那么该URL将被直接拒绝。
3. 如果URL过滤的动作是例外，那么该URL直接放通，不会执行WebFilter分类过滤。

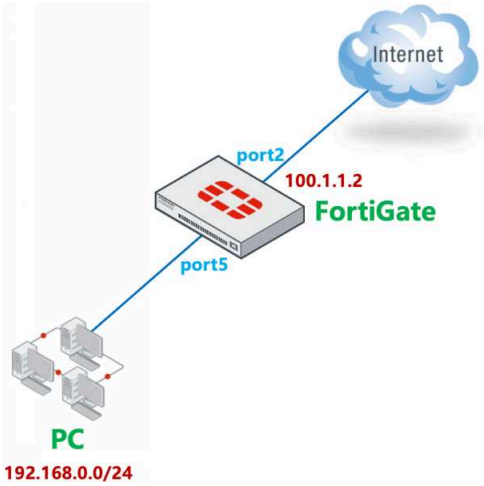
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Web过滤配置

网络需求

客户使用Webfilter限制用户访问Web资源。

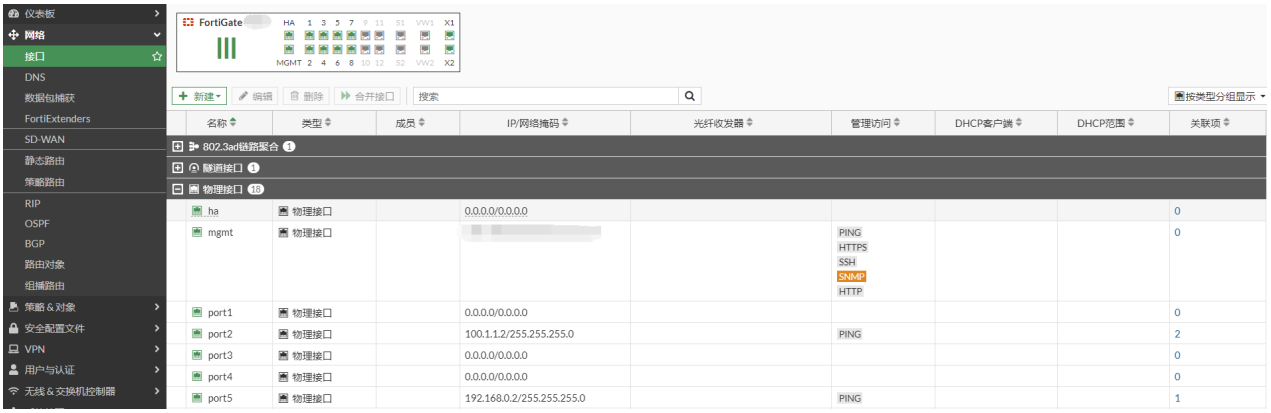
网络拓扑



配置步骤

1. **基本配置**

   配置接口IP和路由。





2. **配置Web过滤配置文件**

   这里直接使用Default配置文件，为了便于测试，这里阻断了用户访问”搜索引擎和门户网站“的URL分类。

   请勾选”当发生分级错误时允许的网站“。这是为了防止因网络延迟，丢包等原因导致FortiGate不能与FortiGuard webfilter通信而引起web站点无法评估，进而导致该站点不能访问；勾选后如果是由于无法评估引起的错误，将允许访问该站点。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



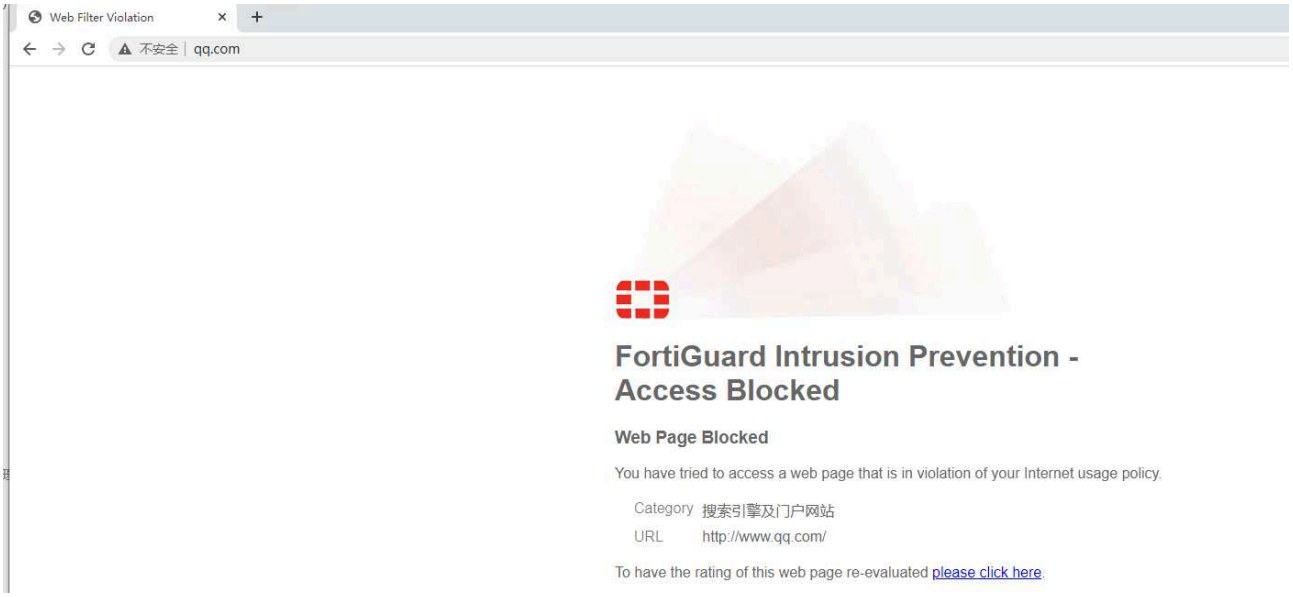
3. 配置策略



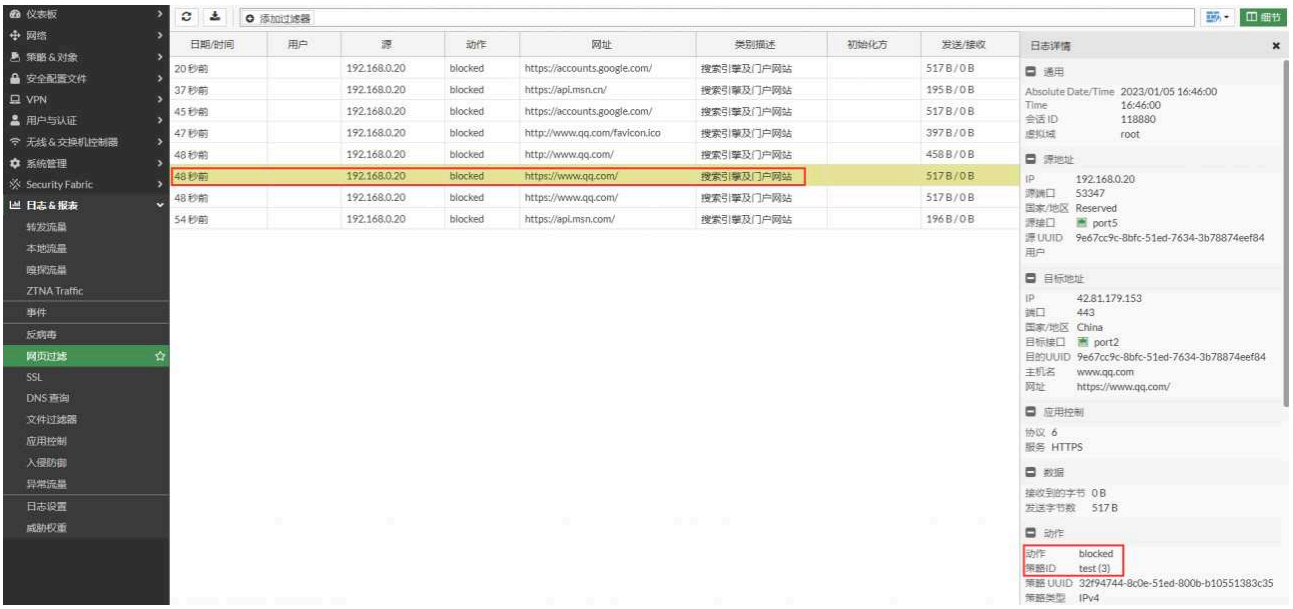
Web过滤测试

使用PC访问www.qq.com ↗ 被web过滤阻断。

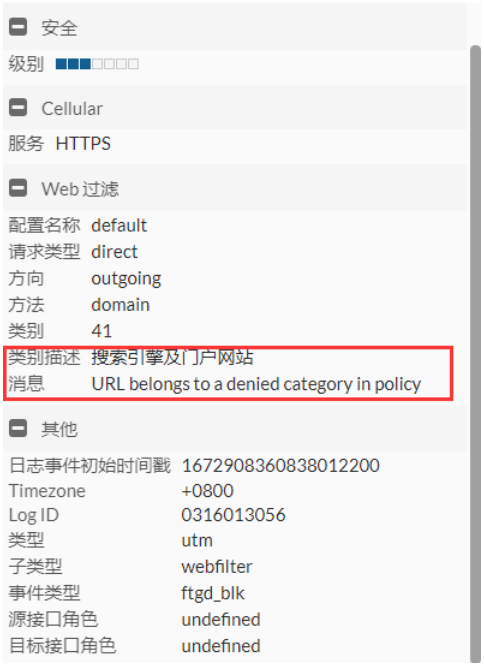
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看Web过滤日志



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

URL过滤

什么是URL过滤

在Web过滤中，除了根据FortiGuard分类执行监控或阻断动作外，还可以使用URL过滤来手动指定哪些网站被允许，哪些网站被阻断。



URL过滤与WebFilter的执行顺序

1. 如果URL过滤的动作是允许或监视器，那么将继续执行WebFilter分类过滤（如果WebFilter通过查询FortiGuard的分类的匹配动作是拒绝，那么该URL仍然会被拒绝）。
2. 如果URL过滤的动作是拒绝，那么该URL将被直接拒绝。
3. 如果URL过滤的动作是例外，那么该URL直接放通，不会执行WebFilter分类过滤。

URL过滤类型

简单：URL过滤器将执行完整的匹配；

如果网址设置为support.fortinet.com.cn ↗，那么URL过滤器将匹配support.fortinet.com.cn ↗，不会匹配www.fortinet.com.cn ↗；

如果网址设置为fortinet.com.cn ↗,那么URL过滤器将匹配support.fortinet.com.cn ↗，www.fortinet.com.cn ↗，fortinet.com.cn ↗，不会匹配fortinetxxx.com.cn ↗。

正则表达式：URL过滤器根据正则表达式执行匹配；

如果网址设置为fortinet（即.*fortinet.*），那么URL过滤器将匹配包含fortinet字符的网址，如www.fortinet.com ↗,www.xxxfortinetyyy.com ↗ 等；

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

如果网址设置为forti.*\.com，那么URL过滤器将匹配support.fortinet.com ↗，www.fortiguard.com ↗ 等。

通配符：URL过滤器根据通配符执行匹配；

如果网址设置为*，那么URL过滤器将匹配所有网址；

如果网址设置为*.fortinet.com，那么URL过滤器将匹配support.fortinet.com ↗，www.fortinet.com等；



URL过滤动作

例外：该UR直接被URL过滤器允许，不再执行后续的FortiGate过滤器，内容过滤器等；

阻断：该URL被URL过滤器阻断；

允许：该URL被URL过滤器允许，但仍然要执行FortiGuard过滤器，内容过滤器等；

监视器：动作和允许一样，但记录日志。



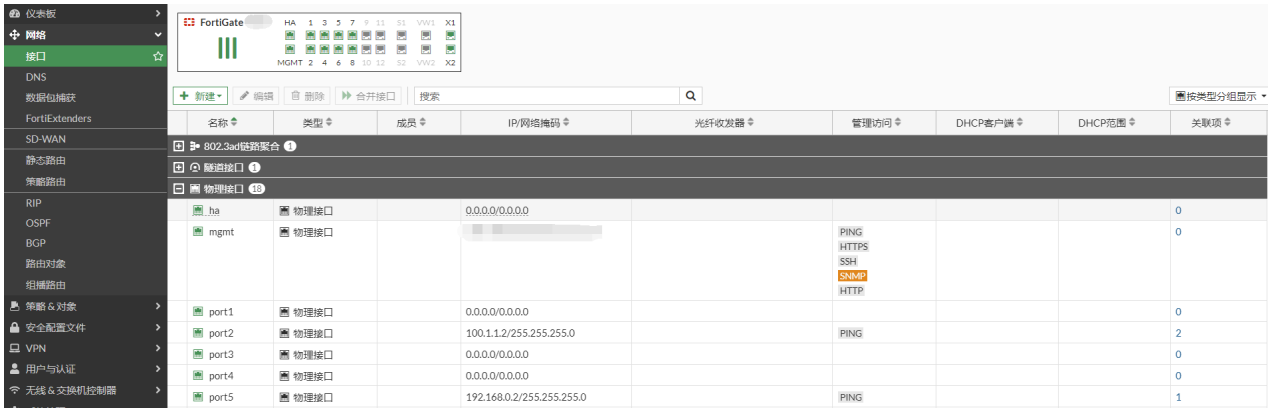
网络拓扑

PC----------(port5:192.168.0.2/24)FGT(port2:100.1.1.2)----------Internet

配置步骤

1. **基本配置**

   配置接口IP和路由。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **配置Web过滤配置文件**

这里直接使用Default配置文件，并使用URL过滤器只允许fortinet.com.cn域名的网站，阻止其他所有网站。

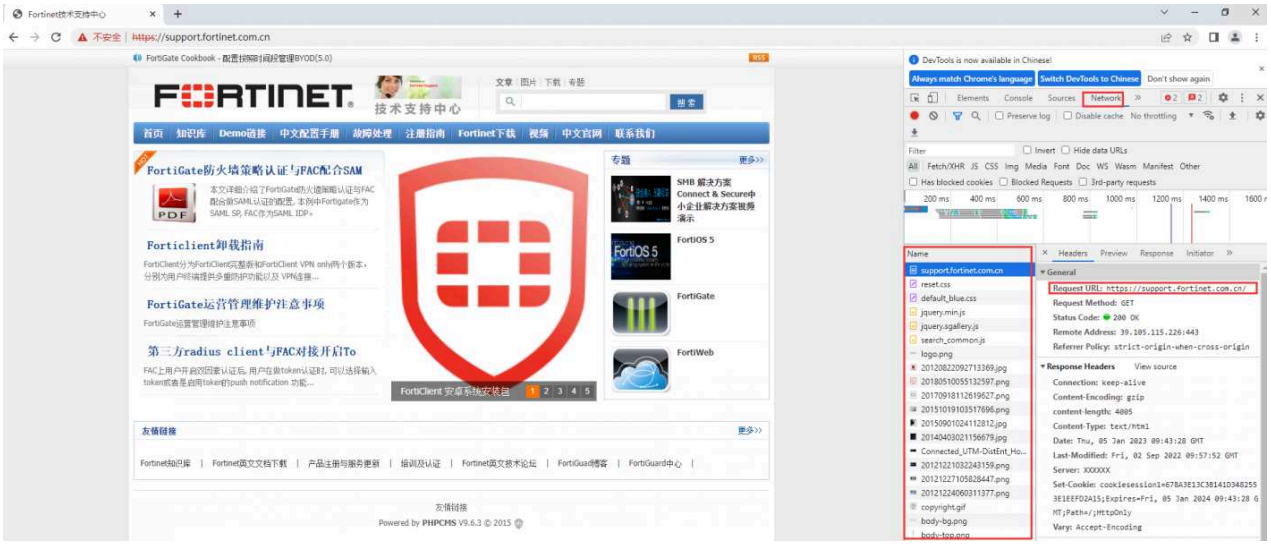
请勾选”当发生分级错误时允许的网站“。这是为了防止因网络延迟，丢包等原因导致FortiGate不能与FortiGuard webfilter通信而引起web站点无法评估，进而导致该站点不能访问；勾选后如果是由于无法评估引起的错误，将允许访问该站点。



重要

在浏览器访问一个网站中，浏览器不仅仅只是访问该域名本身。网站中有很多图片，js脚本等等都是需要加载的，因此在URL放通网站的时候，需要连那些浏览器内部访问的请求都要放通。浏览器访问一个域名时，通过F12，点击network可以查看到该域名加载了哪些内容。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

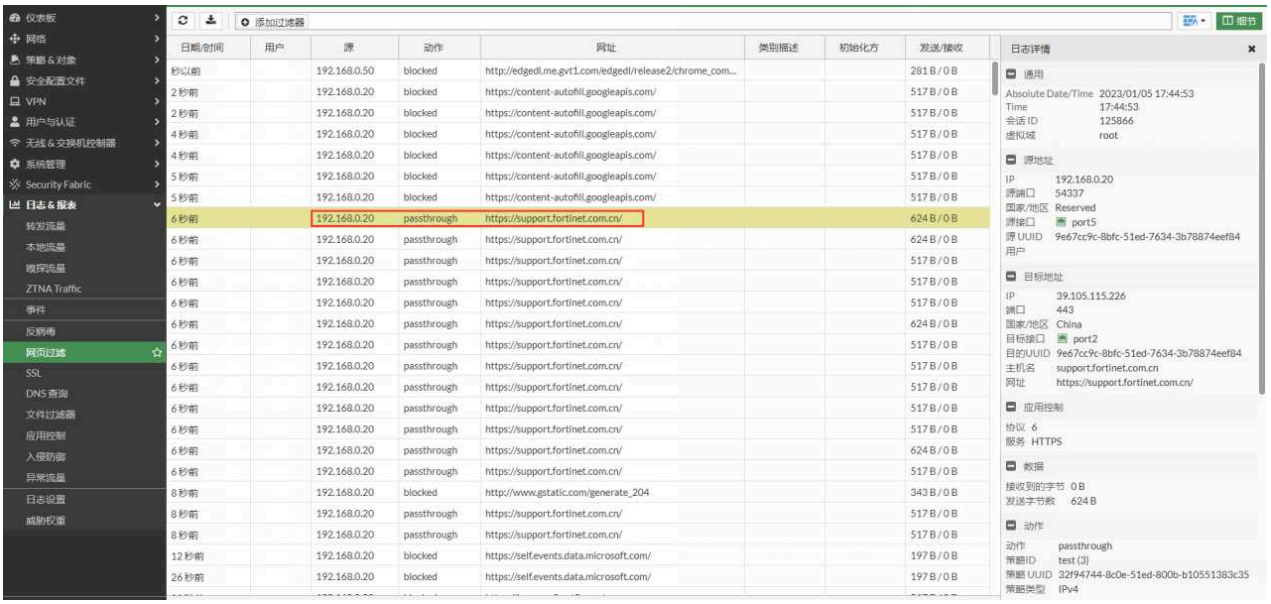


URL过滤测试

1. PC访问support.fortinet.com.cn是允许的。



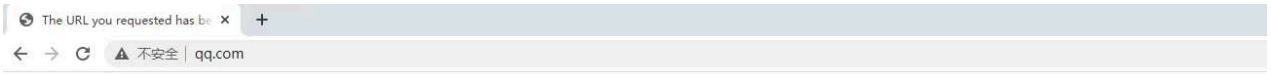
查看web过滤日志。

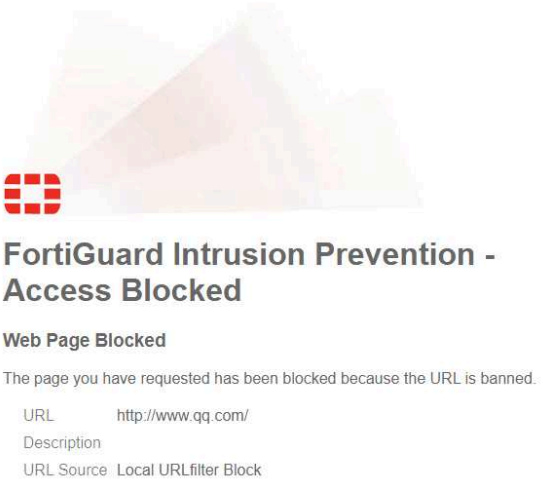


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



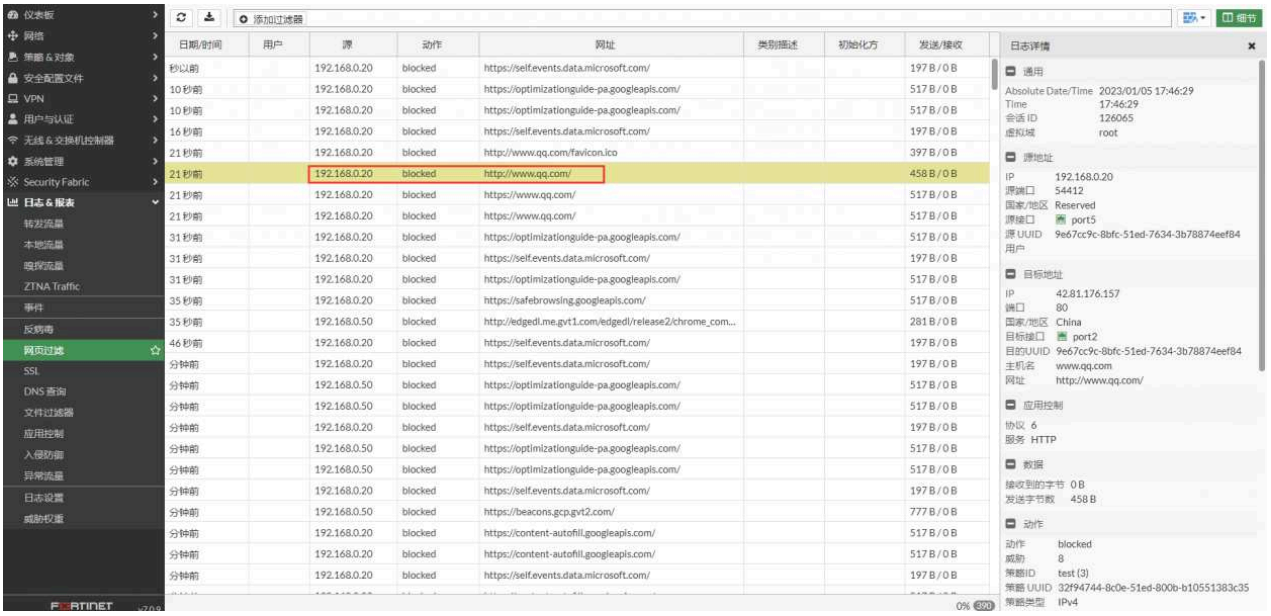
2. PC访问www.qq.com被URL过滤器阻止。





查看webfilter日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



安全

级别

威胁等级 高

威胁分数 30

Cellular

服务 HTTP

Web 过滤

配置名称	default
请求类型	direct
方向	outgoing
URL过滤器目录	1
URL过滤器列表	Auto-webfilter-urlfilter_8co7mmswt
消息	URL was blocked because it is in the URL filter list

其他

日志事件初始时间戳	1672911989973745400
Timezone	+0800
Log ID	0315012544
类型	utm
子类型	webfilter
事件类型	urlfilter
源接口角色	undefined
目标接口角色	undefined
URL源	Local URLfilter Block

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

URL过滤表达式

简介

本文介绍WebFilter在URL过滤时的三种表达式类型：

- 简单（Simple）
- 正则表达式（Regular Expression）
- 通配符（Wildcard）

简单（Simple）

简单（Simple）的URL过滤器条目必须采用标准URL格式，可以包含子域名和路径。

举例：`fortinet.com`，`fortinet.com/support`、`handbook.fortinet.com.cn`、`net.com`等。

当FortiGate的防火墙策略处于不同的检测模式（inspection-mode）时，Simple表达式的匹配方法会有所不同：

- 当防火墙策略配置为流模式（`set inspection-mode flow`，默认配置）时：只要simple表达式的字符串出现在实际访问的URL中（哪怕只是其中一部分），就会判定为匹配。
- 当防火墙策略配置为代理模式（`set inspection-mode proxy`）时：只有当实际访问的域名与simple表达式完全一致，或是simple表达式的子域名时，才会匹配。

防火墙策略检测模式	匹配规则说明	Simple表达式	匹配示例✅	不匹配示例❌

flow（默认）	只要Simple表达式的字符串出现在实际URL中任意位置，即判定为匹配	`net.com`	`net.com`
			`fortinet.com`
			`www.net.com`
			`www.fortinet.com`
				`net1.com`

		`net.com/prod`	`www.fortinet.com/products/doc`	

proxy	只有当访问的域名与 Simple 表达式完全一致，或是其子域名时，才算匹配（不检查后边）	`net.com`	`net.com`
			`www.net.com`
			`net.com.cn`
			`www.net.com.cn`
				`forinet.com`
				`www.fortinet.com`

		`net.com/prod`	`www.net.com/products/doc`	`www.fortinet.com/products/doc`

include-subdomains选项

从FortiOS 7.6.3版本开始，当防火墙策略的检测模式配置为代理模式（`set inspection-mode proxy`）时，可以在使用simple条目时控制子域名匹配的选项。

```bash
config webfilter urlfilter
    edit <id>
        set include-subdomains {enable/disable}
    next
end
```

- `enable`（默认）：simple表达式会匹配子域名。例如，`net.com`会匹配`www.net.com`、`www.net.com.cn`。
- `disable`：仅匹配确切的域名。例如，`net.com`只会会匹配`net.com`、`net.com.cn`，不会匹配`www.net.com`、`www.net.com.cn`。

通配符（Wildcard）

通配符（Wildcard）表达式可以根据指定的关键字灵活匹配多个URL，不需要严格的格式，比simple类型更灵活。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

匹配类型	匹配规则说明	Wildcard表达式	匹配示例✅	不匹配示例❌
基本匹配	URL开头左到右扫描，只要任意位置符合规则即匹配成功	`for*guard`	`fortiguard.com`	
中间匹配	若要匹配URL中间的字符，需要在开头加`*`	`*or*guard`	`www.fortiguard.com`	
		`or*guard`		`www.fortiguard.com`
结尾匹配	条目末尾不需要`*`，自动匹配末尾任意字符，`*fortinet`等效于`*fortinet*`	`*fortinet`	`www.fortinet.com` `support.fortinet.com` `handbook.fortinet.com.cn`	
子域名匹配	条目以`*.`开头，会匹配该域名和所有子域名	`*.fortinet.com`	`fortinet.com` `www.fortinet.com` `support.fortinet.com`	

正则表达式（Regex）

正则表达式（Regex）是一种类似Perl语法的规则，用来匹配一个或多个特定的URL，也可以用来排除不符合条件的 URL。

**正则符号 **	表达式含义	正则表达式	匹配示例✅	不匹配示例❌
`*`	匹配前一个字符出现0次或多次	`fortinet*.com`	`fortinetttttt.com`	`fortinetsupport.com`
`/i`	匹配时区分大小写	`/FORTINET/i`	`FORTINET`	`fortinet`
`^`	必须以特定字符串开头	`^fo`	`fortinet.com`	`support.fortinet.com` `notfortinet.com`
`$`	必须以特定字符串结尾	`\.com$`	`fortinet.com`	`fortinet.com.cn`
`.`	匹配任意单个字符	`fortinet.com`	`fortinetacom` `fortinetbcom` `fortinet.com`	`fortinetabccom`
`.*`	匹配任意字符	`forti.\*com`	`fortinet.com` `fortinetabccom` `fortinet-xyz-123com`	
`\`	转义特殊字符	`fortinet\.com`	`fortinet.com`	`fortinetacom` `fortinetbcom`
组合用法		`^fortinet\.com$`	`fortinet.com`	`www.fortinet.com` `fortinet.com.cn`
		`^forti.*\.com`	`fortiguard.com` `fortinet.com` `fortinet.com.cn`	`www.fortinet.com` `fortinet.net` `fortizcom`

附：

> **重要**
>
> [!NOTE]
>
> 正则表达式解释文档：https://perldoc.perl.org/perlre ↗ 正则表达式测试网站：https://regex101.com ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

带路径的URL识别

使用URL过滤功能时，如果需要识别的HTTPS网页携带目录（例如客户端访问的网页为`https://www.baidu.com/more/`），由于FQDN后的网站目录`/more/`是在TLS协商结束后客户端才会发起GET请求，访问`/more/`目录的HTTP GET请求被TLS加密，FortiGate需要开启防火墙策略中SSL检测模式需要使用`deep-inspection`模式才能识别到请求目录`/more`的HTTP报文。

HTTP网页不需要使用`deep-inspection`模式。

URL中携带#符号

当需要识别的URL中携带`#`字符，例如需要拦截的url为`http://yundisk.dwstock.com:8686/ksops/#/login`。

- 配置为Simple格式`http://yundisk.dwstock.com:8686/ksops/#/login`时无法保存ULR Filter配置，提示错误。
- 当使用通配符格式`http://yundisk.dwstock.com:8686/ksops/*/login`时无法实现拦截。

实际上客户端在请求URL`http://yundisk.dwstock.com:8686/ksops/#/login`时，`#`及之后的部分并不会发送给HTTP Server，如下抓包所示，客户端请求的URI并不包含`#`以及之后的字段`/login`。



`#`后的部分被称为URI fragment，仅在客户端本地浏览器生效，不会发送给Server（参考：https://en.wikipedia.org/wiki/URI_fragment ↗）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Chrome/Edge访问网页无法被拦截

问题现象

Web过滤针对部分网页配置了阻断动作，但Chrome/Edge浏览器发起的网页访问无法被阻断，Firefox浏览器发起的相同网页访问可以正确被Web过滤阻断。

使用基于FortiGuard的Web过滤或URL过滤均会出现此问题。

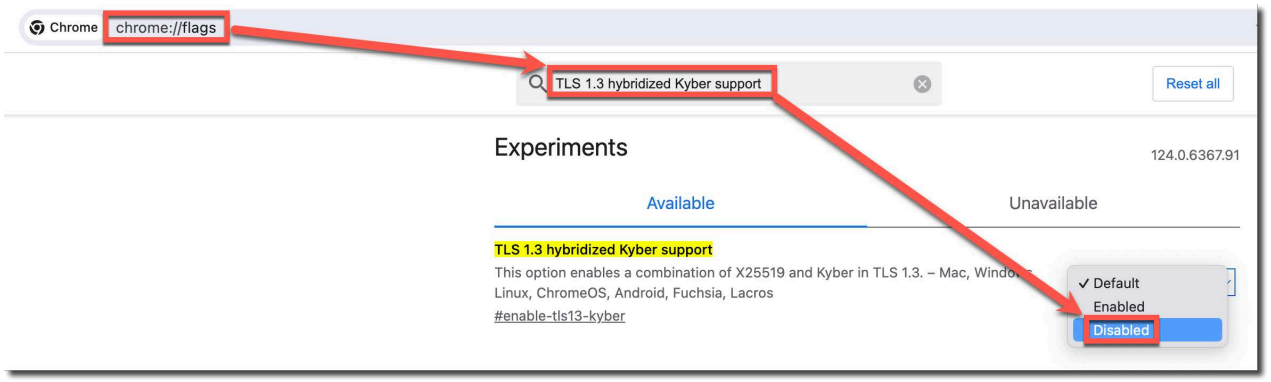
问题原因

从Chrome 116版本开始，引入了新特性“TLS 1.3 hybridized Kyber”。该特性默认开启，导致FortiGate的IPS Engine无法解密TLS交互流量，所以Web过滤功能失效。

解决方法1-修改Chrome配置

1. 在Chrome浏览器的地址栏，输入 `chrome://flags` （Edge为 `edge://flags` ），进入Experiments页面。

2. 在页面上方的搜索框中搜索 `TLS 1.3 hybridized Kyber support` ，并将其修改为Disabled。



3. 随后清除Chrome网页缓存，即可正常拦截Chrome的网页访问。

解决方法2-升级IPS Engine

升级FortiGate的IPS Engine到6.0.15:0171、IPSE 7.1.8:0178、IPSE 7.2.6:0331、IPSE 7.4.2:0519或更高版本后，即可正常拦截Chrome的网页访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

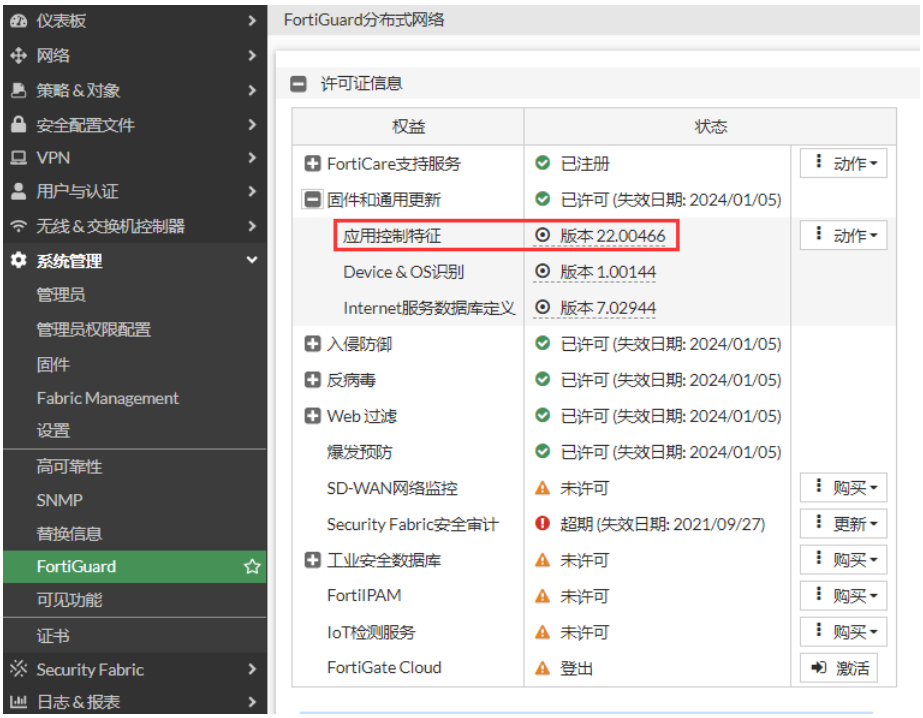
应用控制简介

什么是应用控制

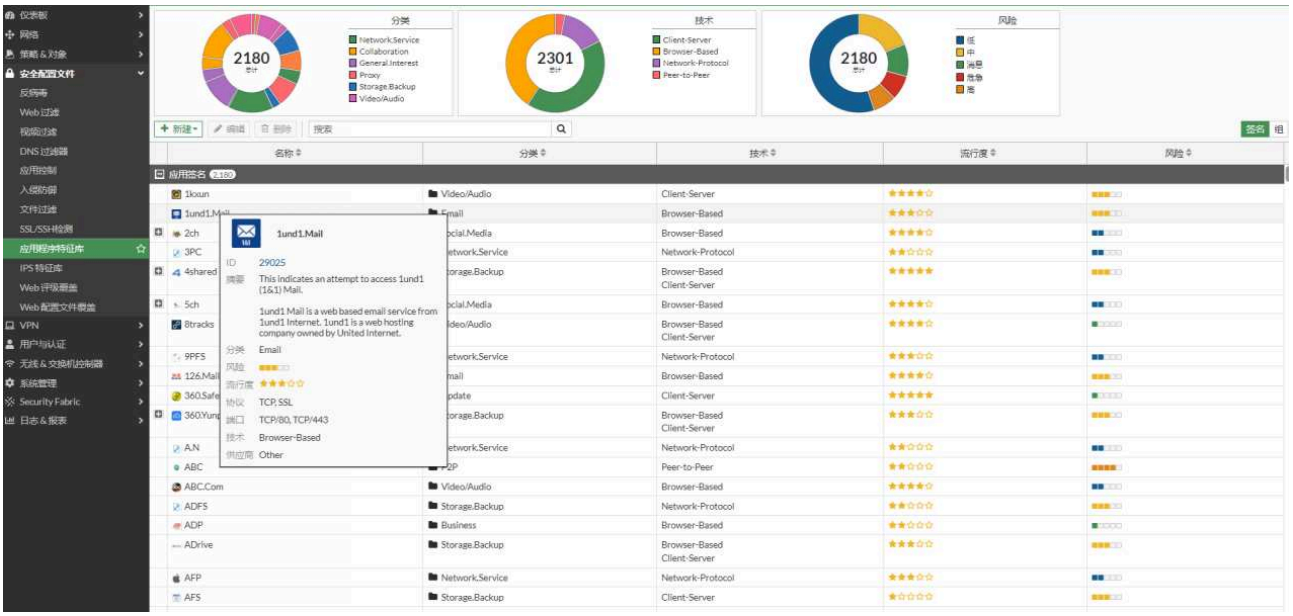
FortiGate通过扫描流量中的内容来检测应用程序，FortiGate应用控制可以检测二千多种不同的Web应用、软件程序、网络服务及通讯协议等特征，使企业重拾对应用程序的可视化和控制能力。

应用控制特征库

选择“系统管理”-->“FortiGuard”-->“许可证信息”，在”固件和通用更新“菜单下可以查看应用控制特征库的版本。



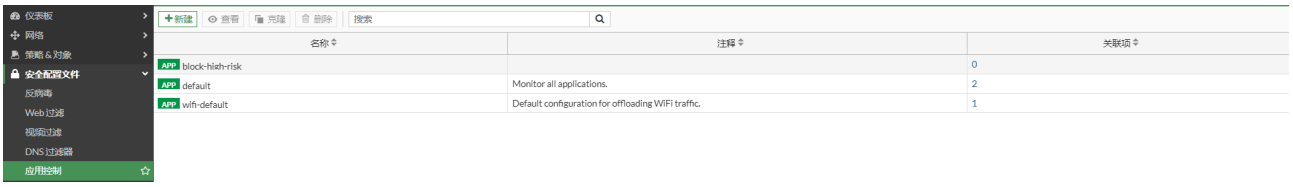
选择“安全配置文件”-->“应用控制特征库”，可以查看具体的特征，将鼠标悬停在某一个特征上，可以查看该特征的详细信息。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

应用控制配置文件

应用控制默认有一些配置文件，这些配置文件应用的目标各有不同，也可以根据自身的业务需求创建新的配置文件。



default配置文件，默认监控所有的应用。

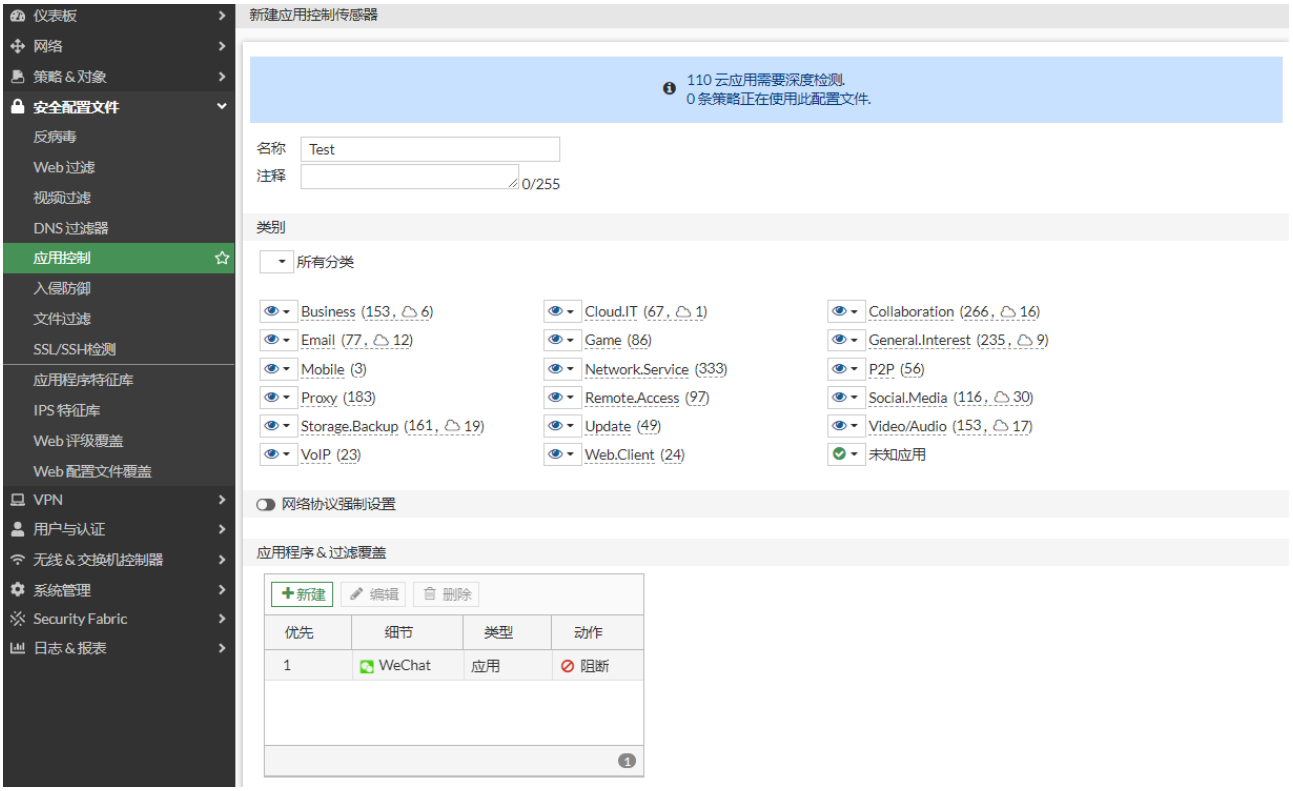


block-high-risk配置文件，阻断了Proxy和P2P类别的应用。



用户也可以根据自身的需求创建配置文件，选择“安全配置文件”-->“应用控制”，点击“新建”，如阻断微信。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



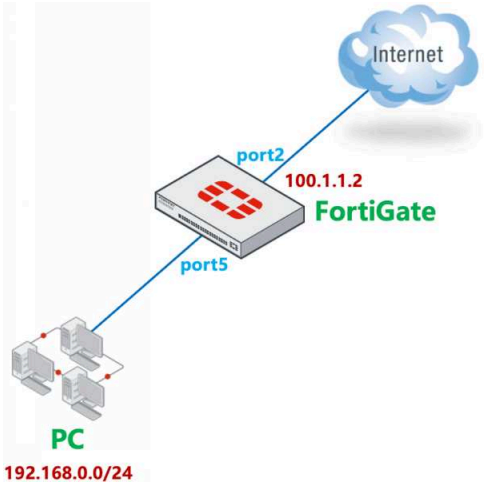
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置应用控制

网络需求

客户使用应用控监控和限制用户上网的流量。

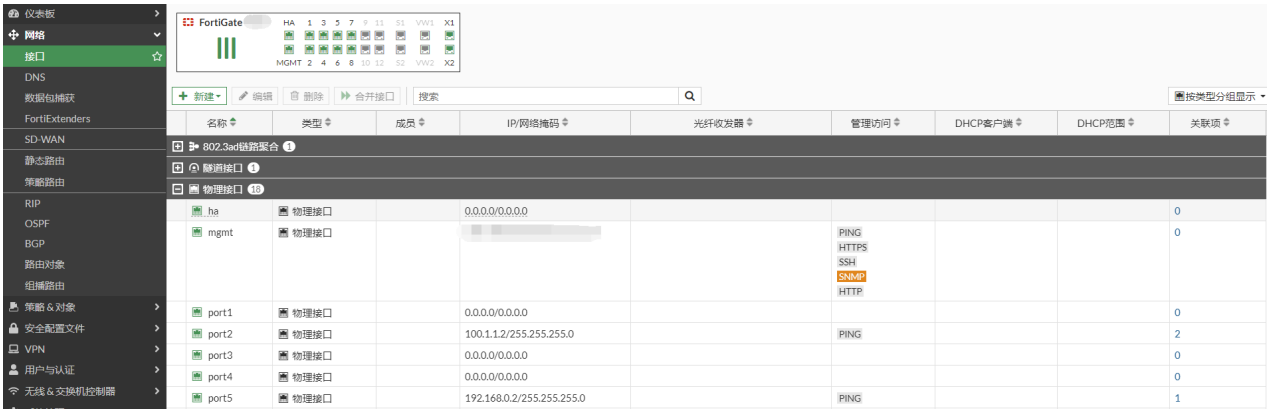
网络拓扑



配置步骤

1. **基本配置**

   配置接口IP和路由。

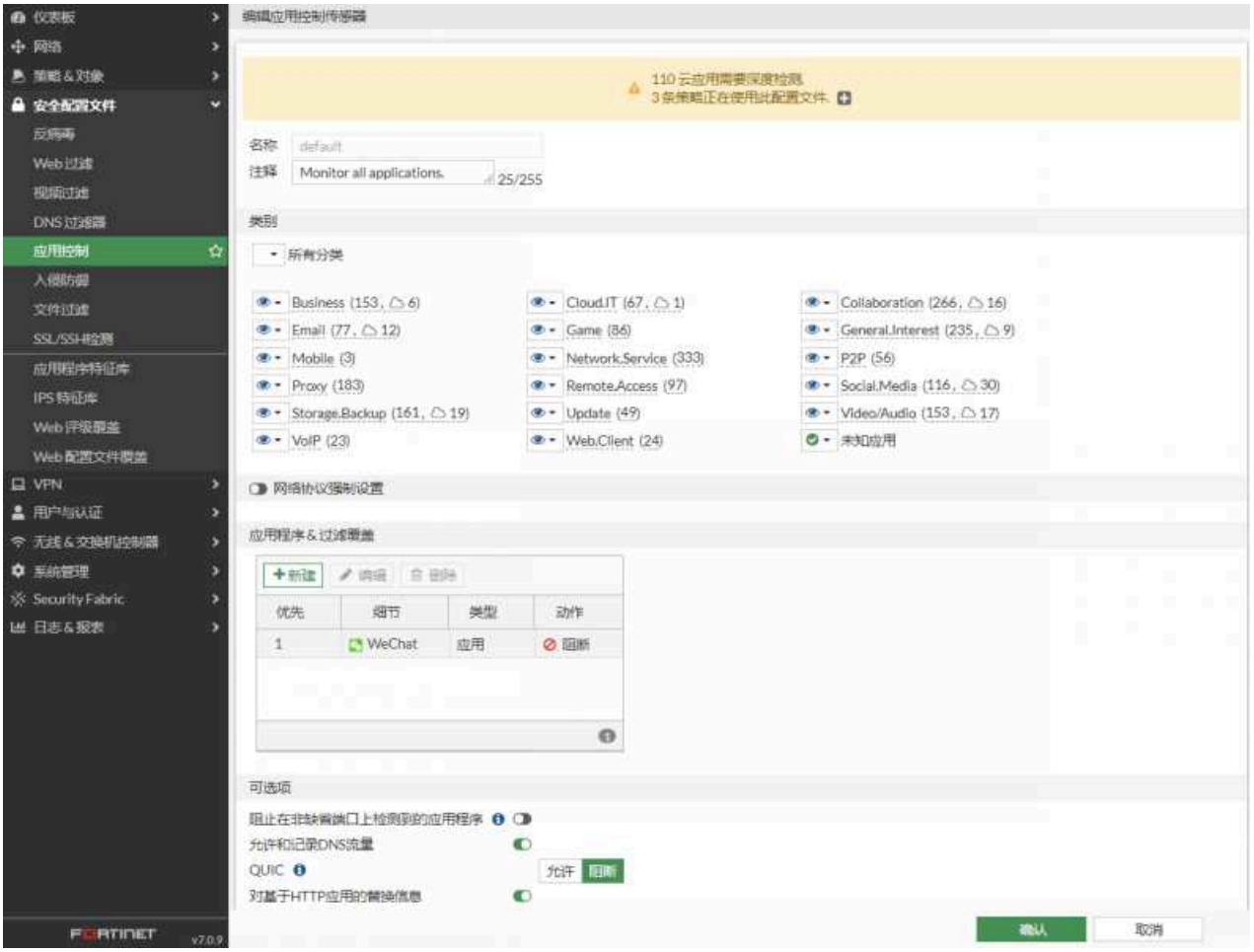




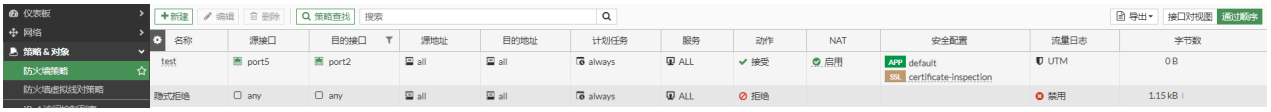
2. **配置应用控制配置文件**

   这里直接使用Default配置文件，并阻断了用户使用微信。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置策略



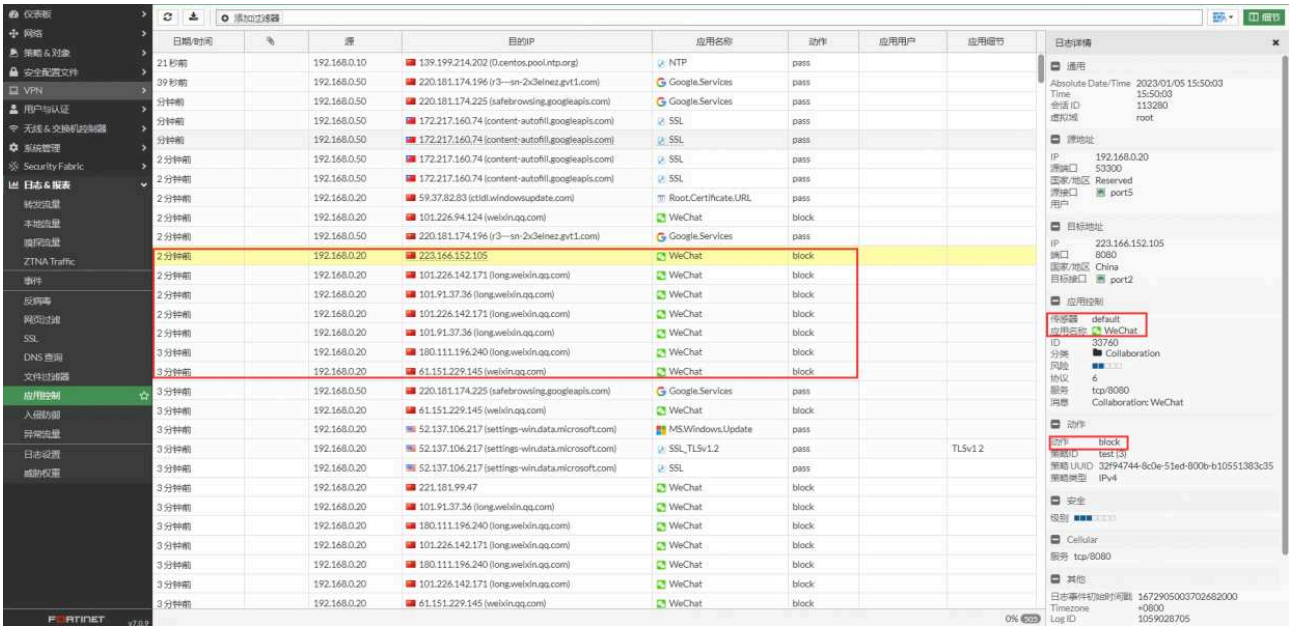
应用控制测试

PC登录微信被应用控制阻断。



查看应用控制日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



注意事项

有时会遇到开启应用控制后，腾讯相关的应用都是允许状态，但是微信或企业微信的图片无法发送（或发送缓慢），可能是由于微信/企业微信应用用到了QUIC协议，该协议在应用控制配置文件中默认是禁止的，修改为允许后，可以解决此问题。

> **重要**
>
> 在7.2及以后版本中，此开关被移除，请在应用控制过滤覆盖中对QUIC应用进行控制（QUIC位于Network.Service分类中，默认放通）。




```
config application list
    edit "default"
        set comment "Monitor all applications."
        set options allow-dns allow-quic
        config entries
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            edit 1
                set action pass
            next
        end
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

透明DNS转发器

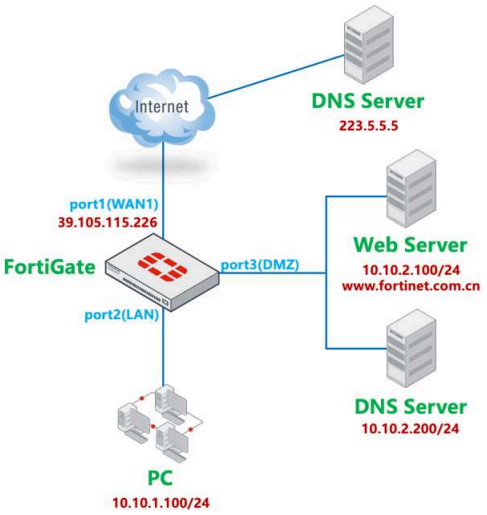
> **重要**
>
> 此功能在FortiOS 7.4.0及更新版本上支持。

功能介绍

FortiGate可以使用透明条件DNS转发器（Transparent conditional DNS forwarder）拦截特定域名的DNS查询并转发到特定DNS服务器，或是直接替换查询结果并回复给客户端。例如当客户端配置的DNS服务器位于公网时，为了将目标地址解析到本地的服务器IP，FortiGate可以拦截请求并将其重新路由到本地DNS服务器进行解析（如果配置了DNS数据库条目，也可以直接返回DNS结果）。

这样可以更好地控制DNS请求，尤其是管理员无法管理客户端设置的DNS服务器配置时。通过解析服务器的本地IP而不是公网IP来提高网络效率，也可以用于特定域名在公网DNS服务器的解析结果不符合用户预期的情况。

网络拓扑



1. 内网PC填写的DNS服务器均为公网DNS服务器的IP `223.5.5.5`。
2. FortiGate通过VIP将Web Server的端口映射到WAN1（port1）上。
3. Web Server的域名为 `www.fortinet.com.cn`，通过公网DNS服务器解析的结果为FortiGate配置的VIP地址。
4. 需要实现的效果：
   - 外网客户端访问Web Server时，直接通过 `www.fortinet.com.cn` 解析到FortiGate配置的VIP IP，通过FortiGate的VIP映射访问即可。
   - 内网客户端访问Server时：
     - 通过公网的DNS服务器223.5.5.5解析 `www.fortinet.com.cn` 的IP地址时，FortiGate拦截DNS请求，并直接回复DNS结果为Web Server的内网IP `10.10.2.100`，内网客户端直接通过解析到的Server内网IP访问服务器。
     - 其他 `fortinet.com.cn` 域的主机名（如 `support.fortinet.com.cn`）的DNS请求也会被FortiGate拦截，但转发到内网DNS Server `10.10.2.200` 进行解析，不直接回复DNS请求，也不通过外网的DNS服务器解析。

配置步骤

1. 基础网络配置、上网策略、与Server的VIP配置（略）。

2. 在FortiGate上配置DNS数据库（需要先在“系统管理→可见功能”中开启“DNS数据库”）。进入“网络→DNS数据库”页面，新建DNS数据库。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

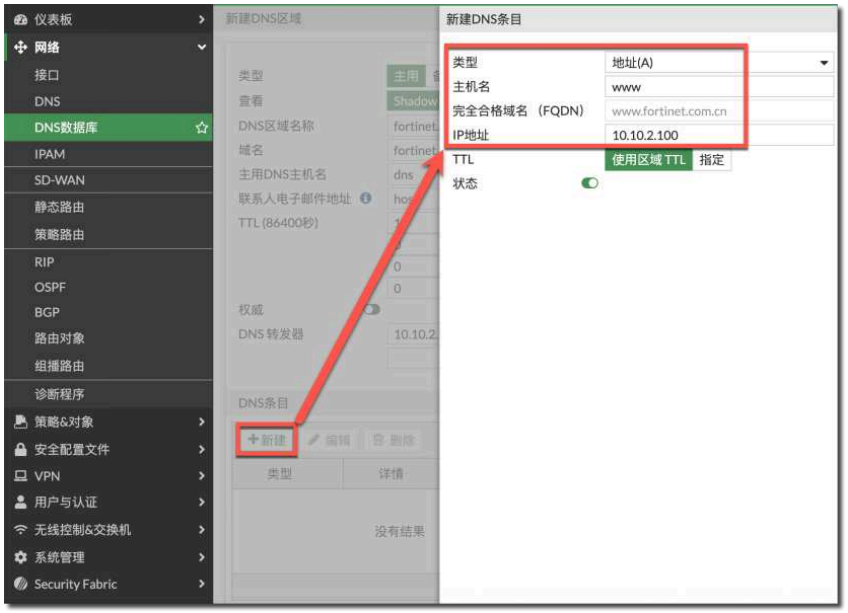


3. 在弹出的新建窗口中，配置区域名称，域名填写为 `fortinet.com.cn`，关闭“权威”选项，DNS转发器填写内网的DNS服务器 `10.10.2.200`（没有匹配上DNS数据库条目的主机名会被转发至此DNS服务器进行解析）。

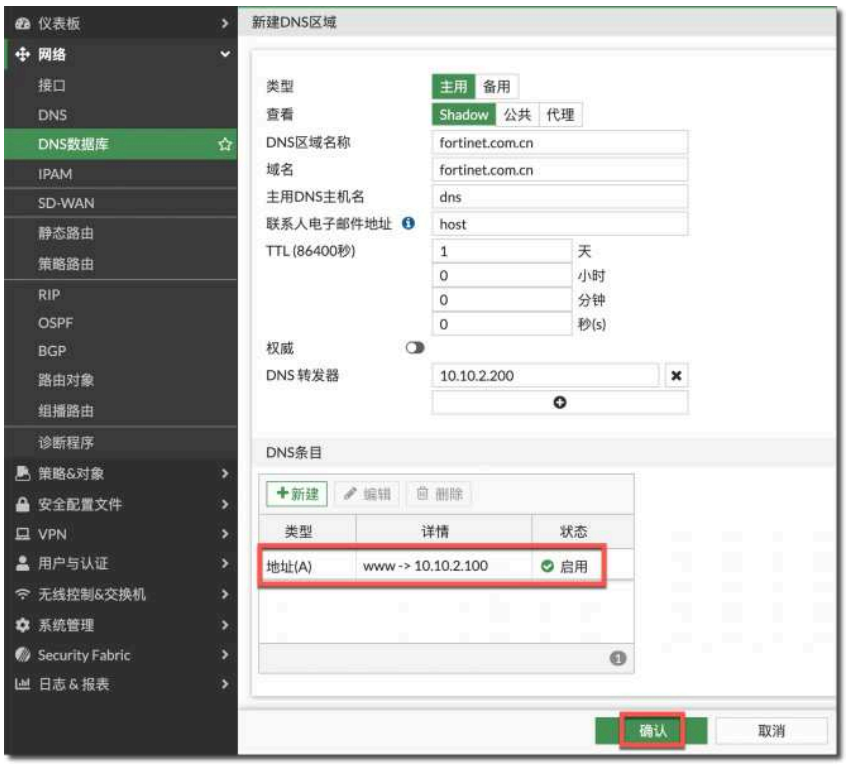


4. 在DNS条目中点击新建按钮，配置主机名为 `www`，IP地址为Web Server的内网IP `10.10.2.100`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 点击确认按钮下发DNS数据库配置。




```bash
config system dns-database
    edit "fortinet.com.cn"
        set domain "fortinet.com.cn"
        set authoritative disable
        set forwarder "10.10.2.200"
        config dns-entry
            edit 1
                set hostname "www"
                set ip 10.10.2.100
            next
        end
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose test application dnsproxy 8    //查看DNS数据库信息//
worker idx: 0
vfid=0 name=fortinet.com.cn domain=fortinet.com.cn ttl=86400 authoritative=0 view=shadow type=primary
serial=172498465 refresh=0
forwarder(s): 10.10.2.200
source-ip(s): 0.0.0.0 ::
    SOA: fortinet.com.cn (primary: dns.fortinet.com.cn, contact: host@fortinet.com.cn, serial: 172498465)(86400)
      A: www.fortinet.com.cn⟶10.10.2.100(86400)
```
bash

6. 如果需要指定DNS Database使用的源IP，例如在IPSec环境中，需要指定DNS的源IP为Tunnel接口的IP，需要在CLI中加入如下配置（此例中不需要配置）。

```
config system dns-database
    edit "fortinet.com.cn"
        set source-ip <IPv4_address>
    next
end
```
bash

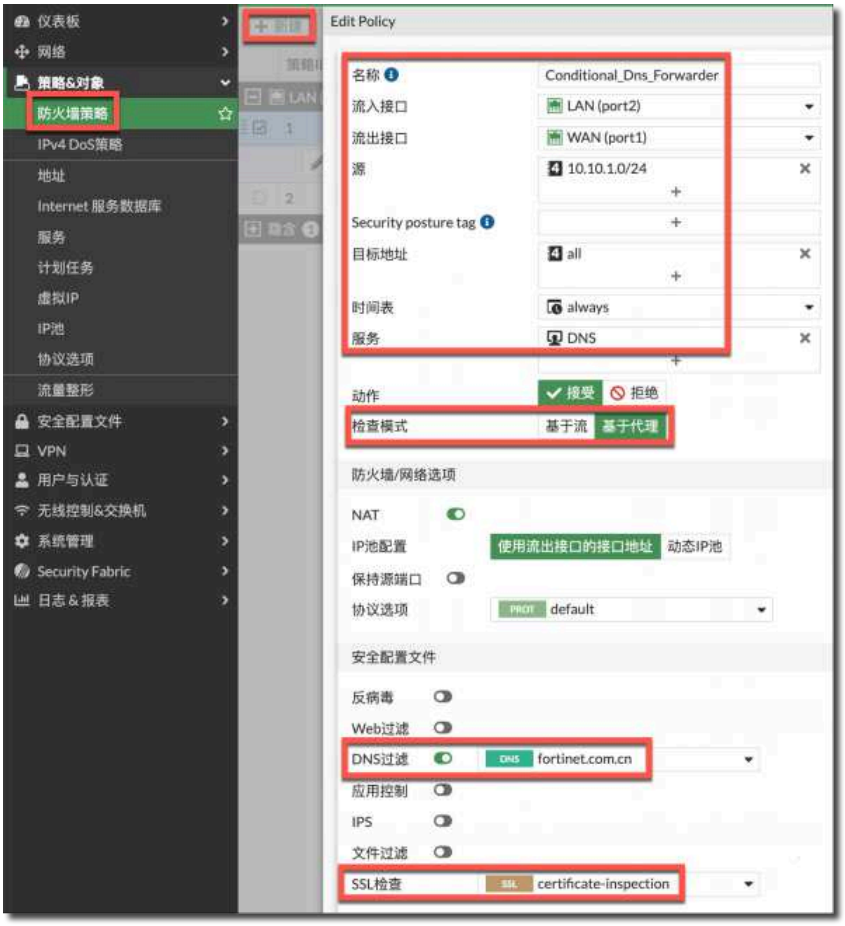
7. 新建DNS Filter配置文件，并通过`transparent-dns-database`功能引用上述配置的DNS Database（在此例中，我们仅使用`transparent-dns-database`功能，所以关闭了DNS Filter的其他过滤功能）。

> **重要**
>
> DNS Filter配置文件中的transparent-dns-database可以引用多个DNS Database。后续删除DNS Database时，需要先取消此处的引用。

```
config dnsfilter profile
    edit "fortinet.com.cn"
        config ftgd-dns
            set options ftgd-disable
        end
        set transparent-dns-database "fortinet.com.cn"
    next
end
```
bash

8. 在FortiGate上新建防火墙策略，源地址为内网PC网段，服务为DNS流量，**检查模式需要配置为“基于代理”**，DNS过滤器选择上步配置的DNS Filter配置文件，SSL检查选择“certificate-inspection”。注意此条策略放置在上网策略之前）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 1
        set name "Conditional_Dns_Forwarder"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "10.10.1.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "DNS"
        set utm-status enable
        set inspection-mode proxy
        set ssl-ssh-profile "certificate-inspection"
        set dnsfilter-profile "fortinet.com.cn"
        set nat enable
    next
end
```



结果验证

1. 公网客户端PC使用DNS服务器`223.5.5.5`解析Web Server的域名`www.fortinet.com.cn`（流量不经过FortiGate），得到结果为Server对应的VIP地址`39.105.115.226`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
::: important
nslookup www.fortinet.com.cn
:::
Server:     223.5.5.5
Address:    223.5.5.5#53

Non-authoritative answer:
Name:   www.fortinet.com.cn
Address: 39.105.115.226
```

2. 内网客户端PC使用DNS服务器`223.5.5.5`解析`www.fortinet.com.cn`的域名（流量经过FortiGate），得到结果为Web Server内网IP`10.10.2.100`。DNS流量被FortiGate拦截，由FortiGate代替公网DNS服务器回复DNS查询结果，这个过程对于客户端是透明的。

```bash
::: important
nslookup -type=a www.fortinet.com.cn 223.5.5.5
:::
服务器:  public1.alidns.com
Address:  223.5.5.5

非权威应答:
名称:    www.fortinet.com.cn
Address:  10.10.2.100
```

3. 内网客户端PC使用DNS服务器`223.5.5.5`解析`support.fortinet.com.cn`的域名（DNS数据库条目中不存在的主机名）：

   - DNS流量被FortiGate拦截，由FortiGate转发至内网DNS服务器`10.10.2.200`进行解析，这个过程对于客户端是透明的。

```bash
FortiGate # diagnose sniffer packet any 'host 223.5.5.5 or host 10.10.2.200' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 223.5.5.5 or host 10.10.2.200]
...
7.354793 port2 in 10.10.1.100.65195 → 223.5.5.5.53: udp 41
7.355069 port3 out 10.10.2.1.3313 → 10.10.2.200.53: udp 41
7.355655 port3 in 10.10.2.200.53 → 10.10.2.1.3313: udp 57
7.355764 port2 out 223.5.5.5.53 → 10.10.1.100.65195: udp 57
...
```

   - 解析结果为内网DNS服务器返回的结果`10.10.2.130`，这个结果是内网DNS服务器返回的。

```bash
C:\Users\Administrator.SUMMERICE2019>nslookup -type=a support.fortinet.com.cn
服务器:  public1.alidns.com
Address:  223.5.5.5

名称:    support.fortinet.com.cn
Address:  10.10.2.130
```

   - 查看FortiGate的DNS缓存，已经记录了`support.fortinet.com.cn`的DNS缓存信息，在TTL（最后一个`:`符号后的数字）结束前，客户端再次请求该域名时，FortiGate会直接响应DNS请求。

```bash
FortiGate # diagnose test application dnsproxy 7
worker idx: 0
...
vfid=0, name=support.fortinet.com.cn, ttl=86400:86250:1650
        10.10.2.130 (ttl=86400)
...
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec VPN原理

什么是IPSEC VPN

IPSec全称为Internet Protocol Security，是由Internet Engineering Task Force (IETF) 定义的安全标准框架，通过在公网上为两个或多个私有网络之间建立IPsec隧道，并通过加密和验证算法保证VPN连接的安全。IPSEC协议工作在IP层，在IP层对数据包进行加密和验证：

- 数据的机密性：IPSec的发送方对发给对端的数据进行加密；
- 数据的完整性：IPSec的接收方对接收到的数据进行验证以保证数据在传送的过程中没有被修改；
- 数据来源的认证：IPSec接收方验证数据的起源；
- 抗重播：IPSec的接收方可以检测并拒绝到重播的IP包；

SA安全关联

SA（security association）安全关联分为两种：ISAKMP/IKE SA和IPsec SA。

ISAKMP/IKE SA：对等体之间的ISAKMP/IKE SA用于控制IPsec协商数据流，如协商对IKE数据流进行加密以及对对等体进行验证的算法，确保协商过程中的安全。

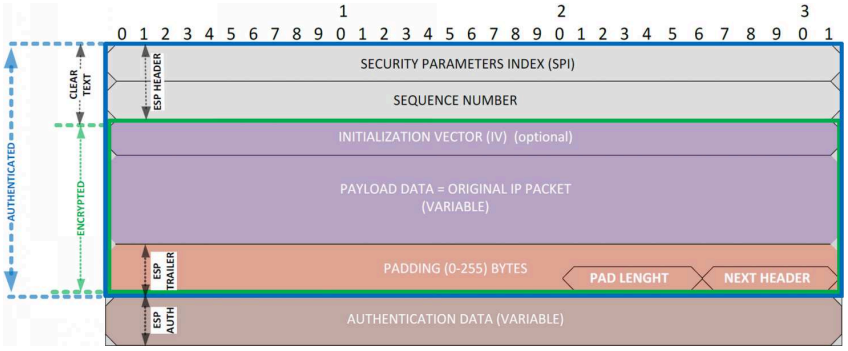
IPsec SA：IPSec SA用于协商对等体之间真正需要通信的IP数据流进行加密的算法，IPSec SA是单向的，因此至少需要两个:一个用于入站数据流，另一个用于出站数据流。

IPSEC安全协议

FortiGate IPSEC VPN只使用ESP，不支持AH。

ESP：ESP（Encapsulating Security Payload），协议号50，支持认证和加密功能。ESP在每一个数据包的标准IP报头后面添加一个ESP报文头，并在数据包后面追加一个ESP尾（ESP Trailer和ESP Auth data）。

ESP报文结构如下图：



- **SPI**：安全参数索引，用于标识IPSEC SA；
- **SEQUENCE NUMBER**：序列号，长度32bit，从1开始的递增的计数器，唯一地标识每一个数据包，用于防止重放攻击；
- **INITIALIZATION VECTOR (IV)**：初始向量，一些算法如 AES-GCM、AES-CCM 和 ChaCha20-Poly1305，采用 IV 生成一个随机数，用作加密和解密的输入参数；
- **PAYLOAD DATA**：负载数据，原始包中可变长的数据内容；
- **PADDING**：填充字段，需要加密的明文长度（也就是ESP报文的结构中，IV + Payload Data + Padding + Pad Length + Next Header的长度）必须是块长度的整数倍，事实是无法保证最后一个块的大小正好为块长度要求，因此信息必须填充至满足要求。只要是使用对称密钥的块密码工作模式，均可能需要Padding字段进行填充；
- **PAD LENGHT**：填充字段的长度，0表示没有填充；
- **NEXT HEADER**：下一头部，标识ESP报文头后的负载类型。传输模式下，是被保护的上层协议（TCP或UDP）的编号；隧道模式下，是IP协议的编号；
- **AUTHENTICATION DATA**：认证数据，包含数据完整性校验值ICV，用于接收方进行完整性校验；

ESP报文抓包示例：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
No.  Time      Source          Destination     Protocol  Length  Info
     8.644528  192.168.89.34   192.168.89.35   ESP          166  ESP (SPI=0xe68f324b)
     8.645259  192.168.89.35   192.168.89.34   ESP          166  ESP (SPI=0x51b93fc6)

> Frame 10: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits)
> Ethernet II, Src: Fortinet_ee:e2:fa (e8:1c:ba:ee:e2:fa), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
v Internet Protocol Version 4, Src: 192.168.89.34, Dst: 192.168.89.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 152
    Identification: 0x0300 (768)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: Encap Security Payload (50)
    Header Checksum: 0x449e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.89.34
    Destination Address: 192.168.89.35
v Encapsulating Security Payload
    ESP SPI: 0xe68f324b (3868144203)
    ESP Sequence: 2
```

AH：AH（Authentication Header），协议号51，只提供认证功能，不提供加密功能。

封装模式

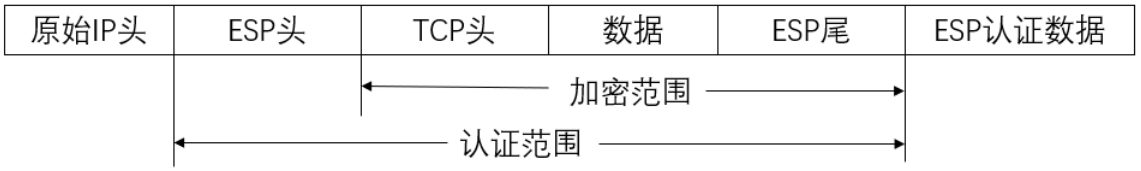
IPSEC隧道模式

在隧道模式下，ESP头被插到原始IP头之前，重新生成一个新的报文头放到ESP头之前，保护IP头和负载。隧道模式主要应用于VPN网关之间或主机与VPN网关之间的通信，用来保护VPN网关后面的网络。



IPSEC传输模式

在传输模式下，ESP头被插入到IP头与传输层协议头之间，保护TCP/UDP/ICMP的负载。传输模式没有添加额外的IP头，因此原始报文中的IP地址在加密后报文的IP头中是可见的。一般用于IPsec加密点等于IPsec通信点的环境下或GRE over IPsec的环境中。

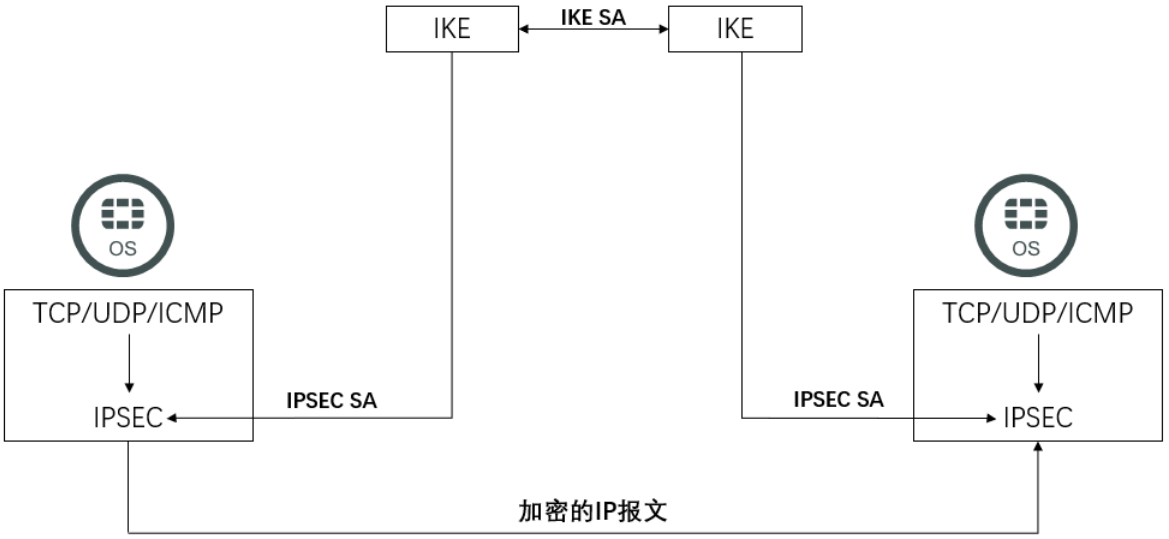


IKE协议

IKE协议与IPSEC的关系

因特网密钥交换IKE（Internet Key Exchange）协议建立在Internet安全关联和密钥管理协议ISAKMP定义的框架上，是基于UDP的应用层协议，分IKEv1和IKEv2两个版本。它为IPsec协商建立SA，并把协商好的参数交给IPsec，IPsec使用IKE建立的SA对IP报文加密或认证。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



IKE的安全机制

- **DH秘钥交换算法**：DH是一种公共密钥交换算法，它用于产生密钥材料，并通过ISAKMP消息在发送和接收端之间进行密钥材料交换。然后，两端各自计算出完全相同的对称密钥，该对称密钥用于计算加密和验证的密钥。DH使用密钥组定义自己产生密钥的长度。

DH Group	Description
1	More Modular Exponential (MODP) DH Group with a 768-bit modulus
2	MODP with a 1024-bit modulus
5	MODP with a 1536-bit modulus
14	MODP with a 2048-bit modulus
15	MODP with a 3027-bit modulus
16	MODP with a 4096-bit modulus
17	MODP with a 6144-bit modulus
18	MODP with a 8192-bit modulus
19	256-bit random elliptic curve group
20	384-bit random elliptic curve group
21	521-bit random elliptic curve group
27	Brainpool 224-bit elliptic curve group
28	Brainpool 256-bit elliptic curve group
29	Brainpool 384-bit elliptic curve group
30	Brainpool 512-bit elliptic curve group
31	Curve25519 128-bit elliptic curve group

- **身份认证**

  通过IP地址或者名称确定双方的身份，有两种身份认证方式：预共享秘钥和数字证书认证。

  - 在预共享密钥认证中，通信双方采用共享的密钥对报文进行Hash计算，判断双方的计算结果是否相同。如果相同，则认证通过；否则认证失败。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 在数字证书认证中，通信双方使用CA证书进行数字证书合法性验证，双方各有自己的公钥（网络上传输）和私钥（本地存储）。发送方对报文进行Hash计算，并用自己的私钥对报文计算结果进行加密，生成数字签名。接收方使用发送方的公钥对数字签名进行解密，并对报文进行Hash计算，判断计算结果与解密后的结果是否相同。如果相同，则认证通过；否则认证失败。

IKE支持的认证算法有：MD5、SHA1、SHA2-256、SHA2-384、SHA2-512。（MD5和SHA1认证算法不安全）

- **数据加密**

身份数据在密钥产生之后加密传送，实现了对身份数据的保护。

IKE支持的加密算法有：DES、3DES、AES-128、AES-192、AES-256。（DES和3DES加密算法不安全）

- **PFS**

PFS（Perfect Forward Secrecy），即完善的前向安全性，是指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。IPSec SA的密钥是从IKE SA的密钥导出的，由于一个IKE SA协商生成一对或多对IPSec SA，当IKE的密钥被窃取后，攻击者将可能收集到足够的信息来导出IPSec SA的密钥，PFS通过执行一次额外的DH交换，保证IPSec SA密钥的安全。

IKEv1秘钥协商过程

IKEv1秘钥协商分为两个阶段：

第一阶段：通信双方协商和建立IKE协议本身的使用的安全通道，即建立IKE SA。

第二阶段：利用第一阶段建立的安全通道建立一对用于数据安全传输的IPSEC SA。

IKEv1第一阶段

IKEv1第一阶段协商支持两种协商模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。

主模式

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.89…	192.168.89.…	ISAKMP	614	Identity Protection (Main Mode)
2	0.000096	192.168.89…	192.168.89.…	ISAKMP	234	Identity Protection (Main Mode)
3	0.000148	192.168.89…	192.168.89.…	ISAKMP	422	Identity Protection (Main Mode)
4	0.000424	192.168.89…	192.168.89.…	ISAKMP	422	Identity Protection (Main Mode)
5	0.000676	192.168.89…	192.168.89.…	ISAKMP	150	Identity Protection (Main Mode)
6	0.000746	192.168.89…	192.168.89.…	ISAKMP	134	Identity Protection (Main Mode)

野蛮模式

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.89.35	192.168.89.34	ISAKMP	698	Aggressive
2	0.000228	192.168.89.34	192.168.89.35	ISAKMP	570	Aggressive
3	0.000458	192.168.89.35	192.168.89.34	ISAKMP	214	Aggressive

主模式

主模式包含3次双向交换，用到了6条ISAKMP信息。

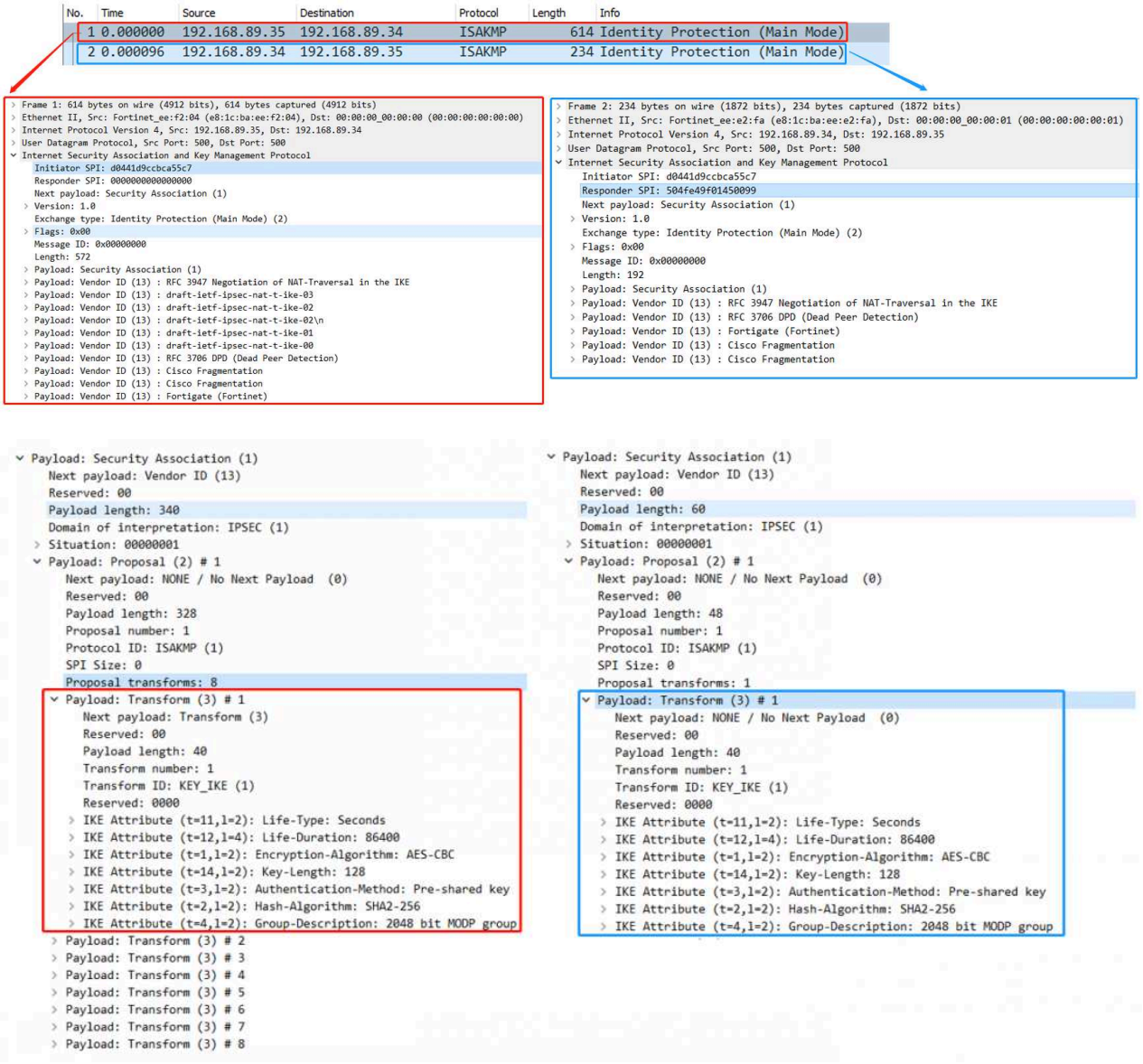
1. **第1和2个包用于安全提议交换。**

a. 在第1个包中，发起方SPI设置为随机值，而响应方SPI设置为0；在第2个数据包中，响应方SPI必须用新值回复，并且整个协商保持相同的SPI值。

b. 对Vendor ID进行处理，以确定对等体是否支持NAT-T、DPD等。

c. 协商安全协商加密和验证的算法。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **第3和4个包用于密钥信息交换**

通过DH公钥值和nonce值，两个对等体将生成一个名为SKEYID的种子密钥。为了不同的目的，将使用该种子密钥生成另外3个会话密钥：

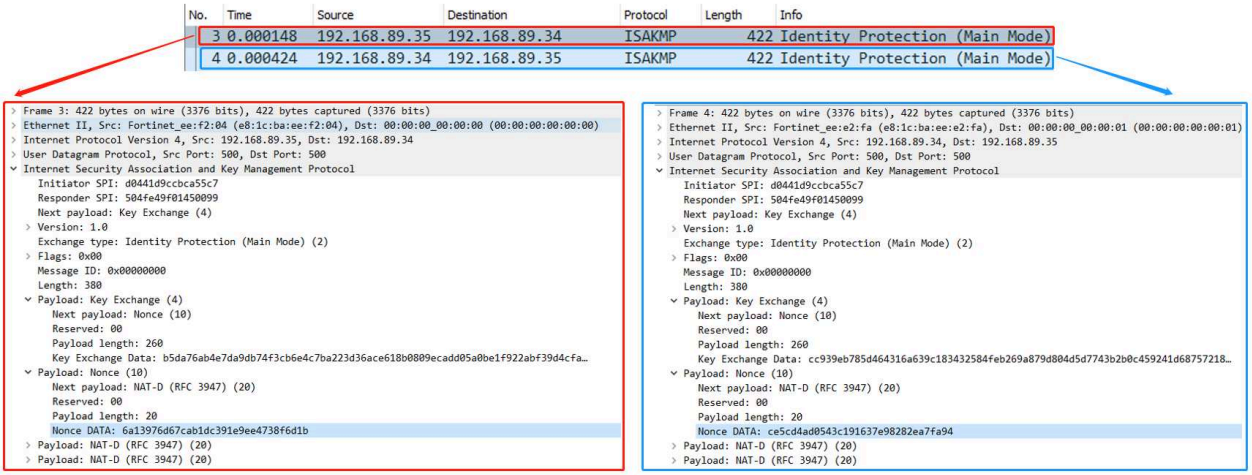
SKEYID_d：作为阶段2生成KEY的材料；

SKEYID_a：用来ISAKMP包完整性用的key；

SKEYID_e：用来加密ISAKMP包的key；

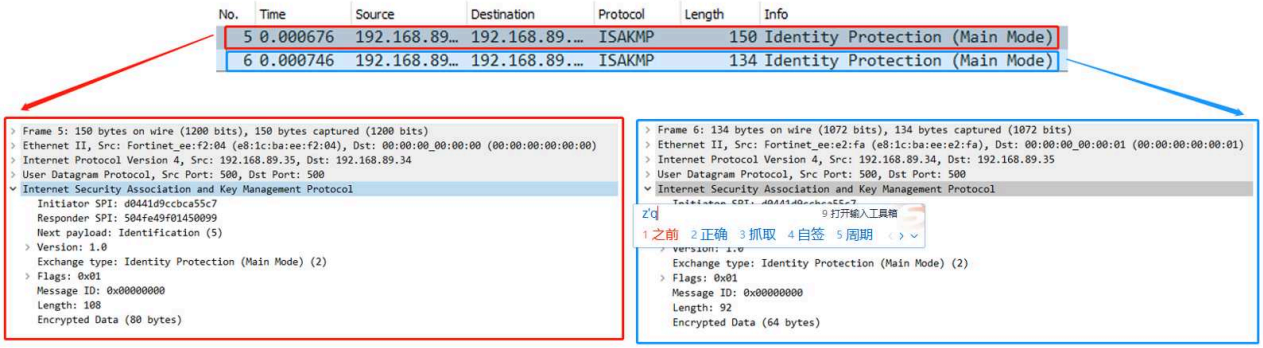
nonce：随机生成的数字，用于防重放攻击。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. **第5和6个包用于身份和认证信息交换**

第5和6个包是加密的，目的是确认对方的身份。如果是使用预共享密钥，那么验证包括检查双方是否有相同的预共享密钥。如果是证书，则对等体交换证书，并假设签署双方的CA是受信任的，则验证成功。

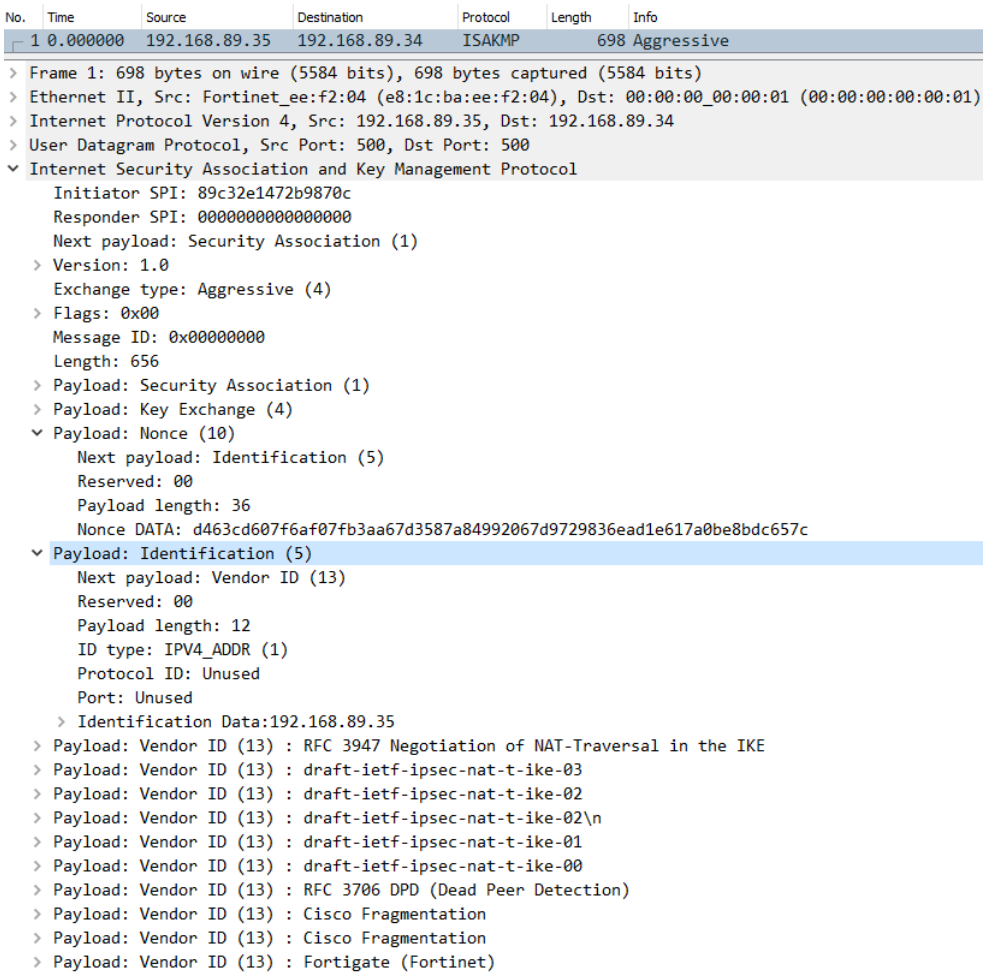


野蛮模式

野蛮模式只用到3个包。

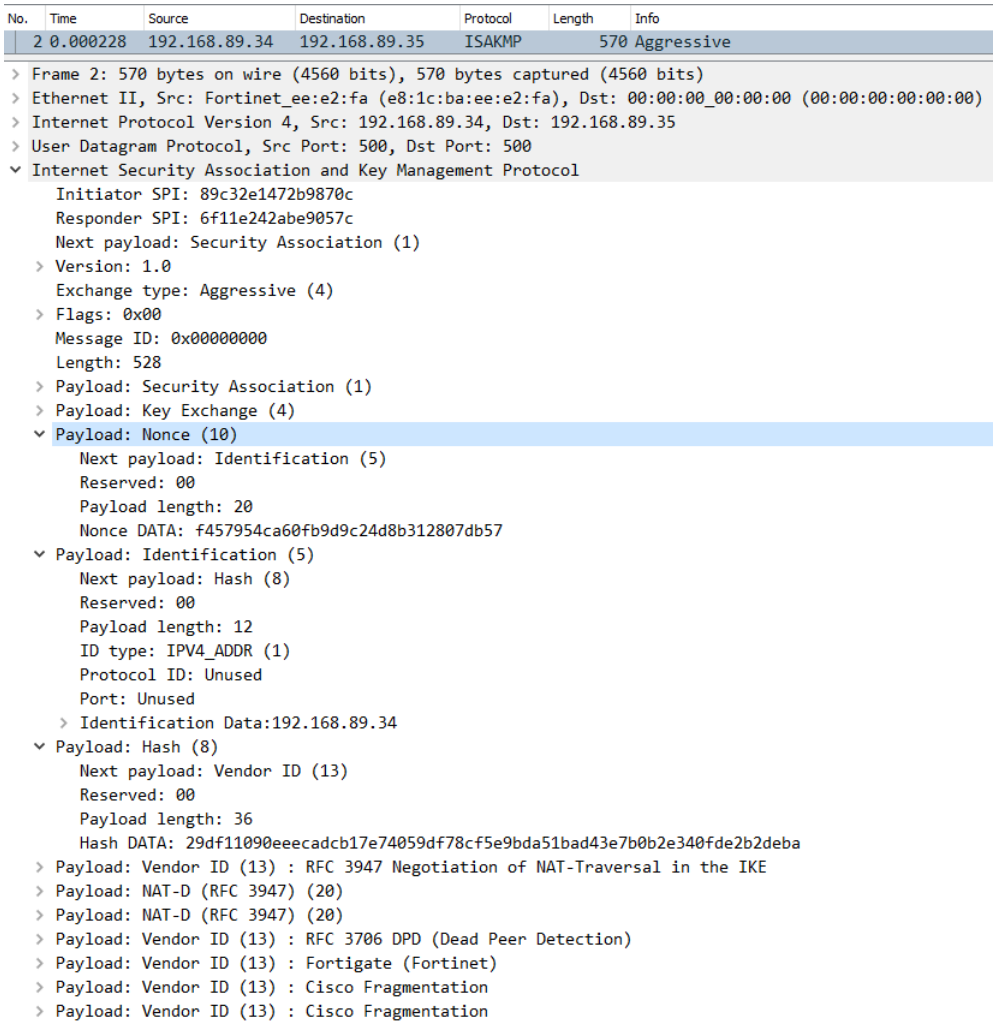
1. **第1个包，发起方发送安全提议、DH公开值、临时值(nonce)，以及身份ID供响应方验证。**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

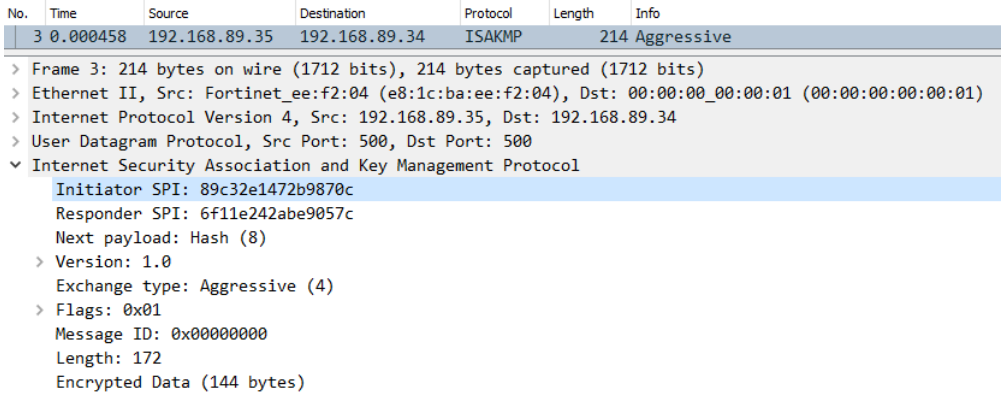


2. **第2个包，响应方用选定提议的所有参数，DH公开值进行应答，以及身份ID供发起方验证。**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. **第3个包，发起方发送验证数据。**



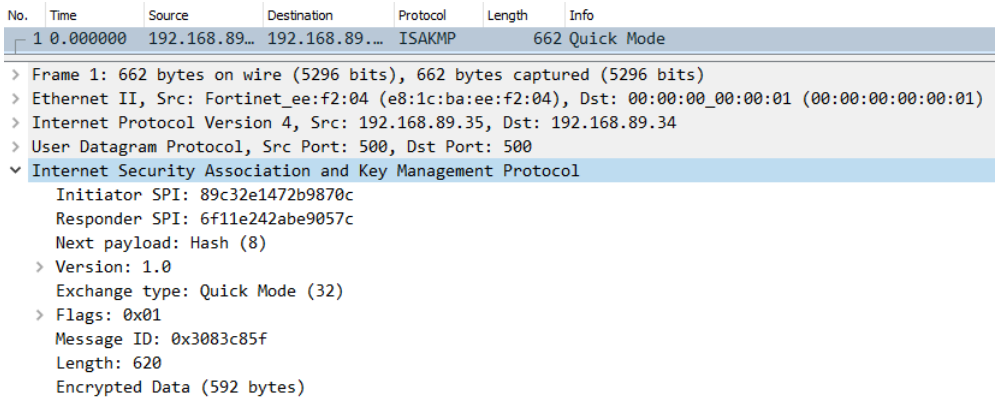
IKEv1第二阶段

IKEv1协商阶段二的目的就是建立用来安全传输数据的IPSec SA，并为数据传输衍生出密钥。该采用快速模式（Quick Mode），使用IKEv1协商阶段一中生成的密钥对ISAKMP消息的完整性和身份进行验证，并对ISAKMP消息进行加密，从而保证了数据交换的安全性。

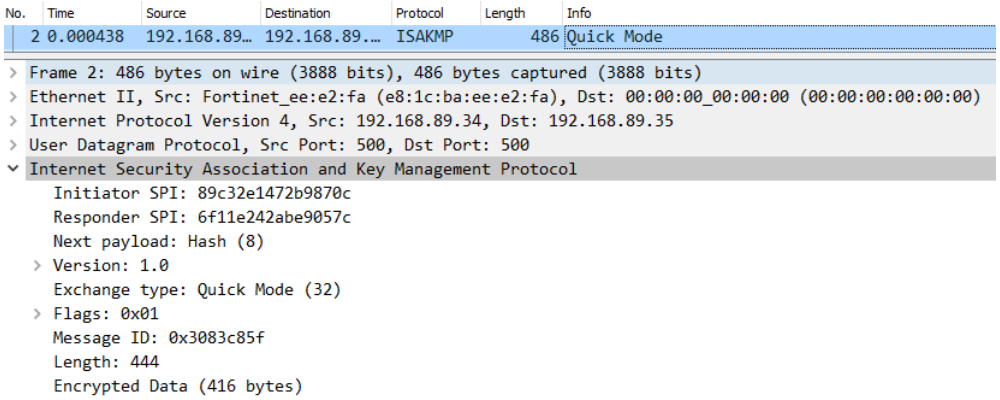
IKEv1第二阶段有3个包：

1. **第1个包，发起方发送本端的安全参数：被保护的数据流和IPSec安全提议等，以及身份认证信息。**

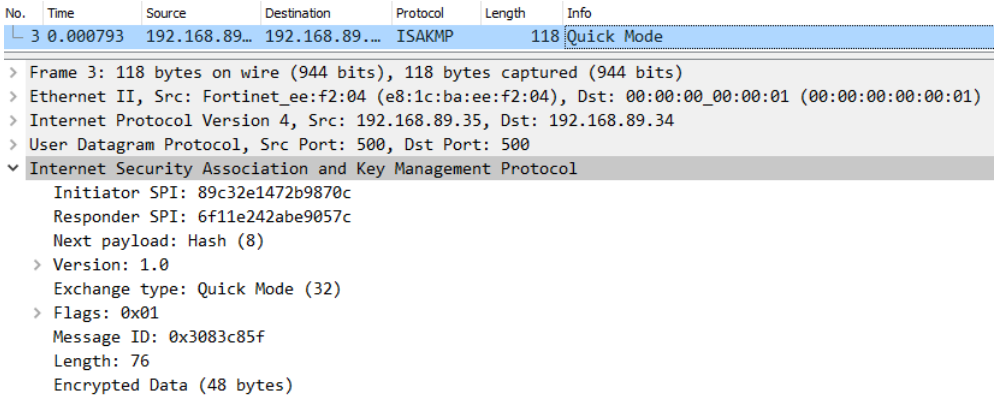
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **第2个包，响应方发送确认的安全参数和身份认证信息并生成IPSEC数据传输密钥。**



3. **发起方发送确认信息，确认与响应方可以通信，协商结束。**



IKEv2秘钥协商过程

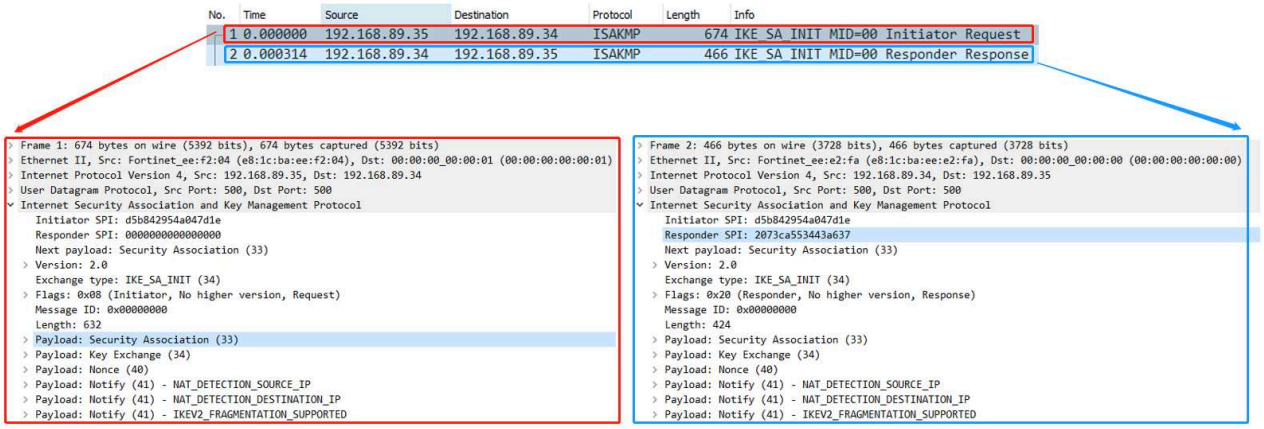
IKEv2使用2次交换共4个包就可以完成一对IPSec SA的建立，如果建立的IPSec SA大于一对时，每一对IPSec SA只需额外增加1次CREATE_CHILD_SA交换就可以完成。IKEv2定义了4种交换：初始交换（Initial Exchanges）、认证交换（IKE_AUTH）、创建子SA交换（Create_Child_SA Exchange）以及通知交换（Informational Exchange）。

初始交换

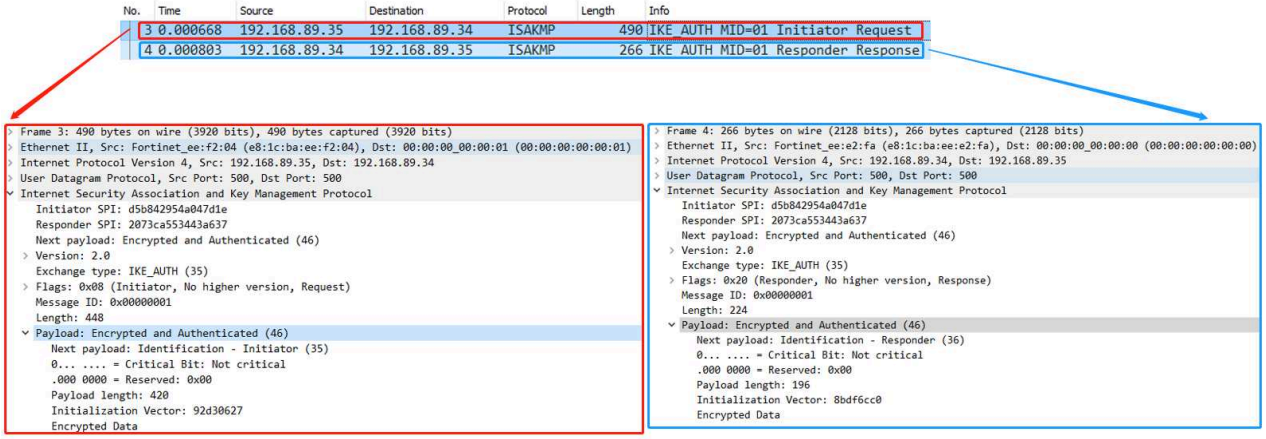
IKEv2通过初始交换就可以完成第一对IPSec SA的协商建立。

1. 第1和2个包，IKE_SA_INIT交换；协商IKE SA加密和验证算法，交换临时随机数和DH交换，然后生成一个共享密钥材料，通过这个共享密钥材料可以衍生出IPSec SA的所有密钥。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

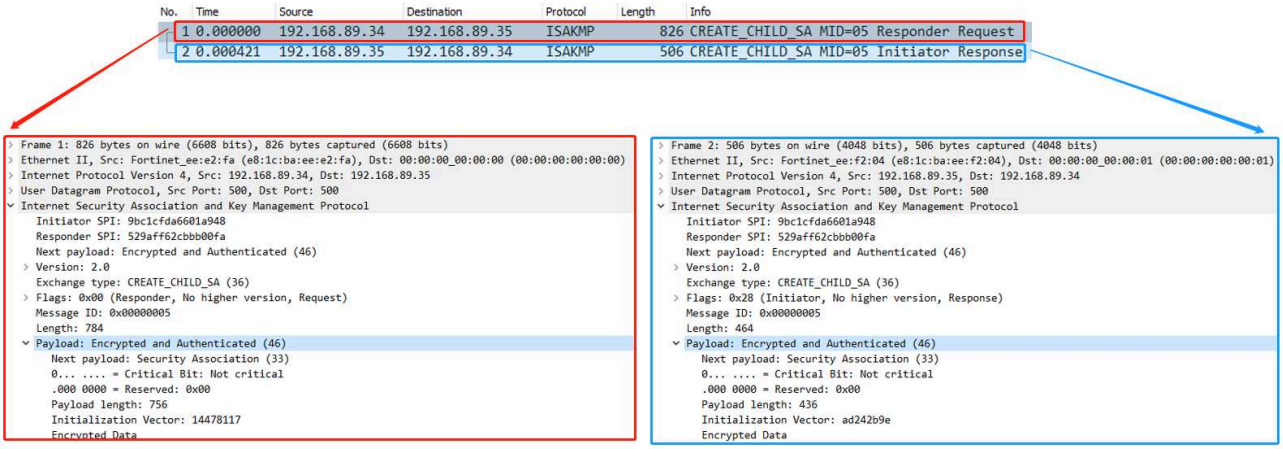


2. 第3和4个包，IKE_AUTH交换；完成身份认证、对前两条信息的认证和IPSec SA的参数协商，第3和4个包是加密的，其中可以包含一对用于ESP封装的IPSec SA。



创建子SA交换

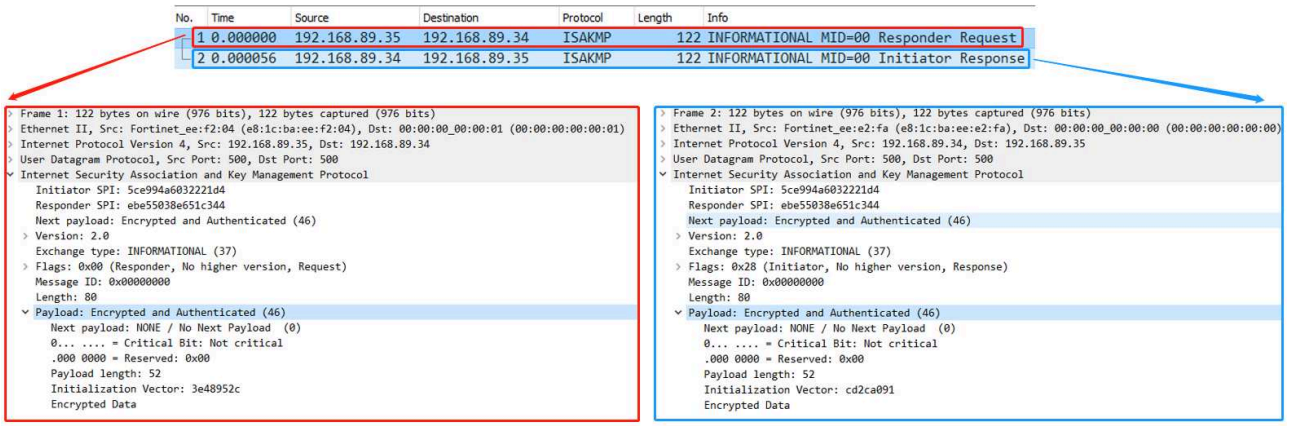
当一个IKE SA需要创建多对IPSEC SA时，则创建子SA交换来协商后续其他的IPSec SA。创建子SA交换还可以用于IKE SA的重协商。



通知交换

IPSEC两端有时会传递一些控制信息，例如错误信息或者通告信息，这些信息在IKEv2中是通过通知交换完成的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



NAT穿越

疑问：ESP隧道模式默认只支持一对一NAT转换，不支持PAT；ESP传输模式不支持NAT。如果FortiGate位于企业内部，运营商出口有单独的设备做NAT，那么IPSEC流量如何穿越NAT?

解决方案：

NAT-T技术，即在IP和ESP报文之间插入一个8个字节UDP头部(端口号默认为4500)，FortiGate默认enable NAT-T

新IP头	UDP头	ESP头	原始IP头	TCP头	数据	ESP尾	ESP认证数据

NAT-T由三部分组成：

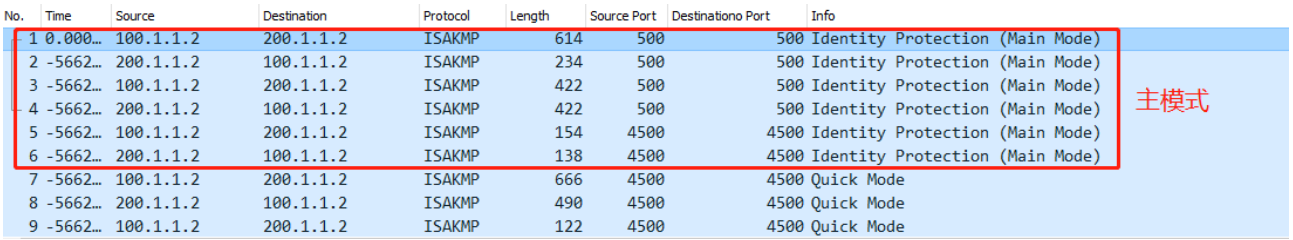
1. 首先是判断远程对等体是否支持NAT-T；

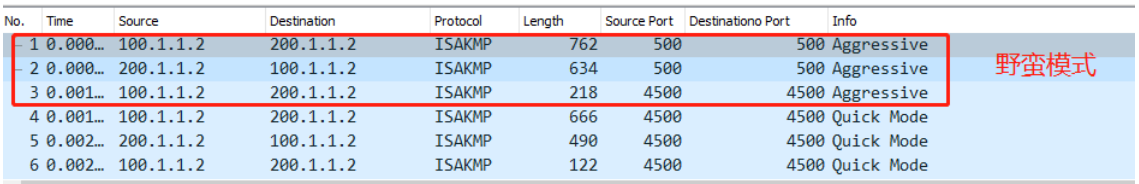
2. 其次是检测对等体之间的路径上是否有NAT；

3. 最后决定如何使用UDP封装来处理NAT。

IKEv1穿越NAT

IKEv1第一阶段协商支持两种协商模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。

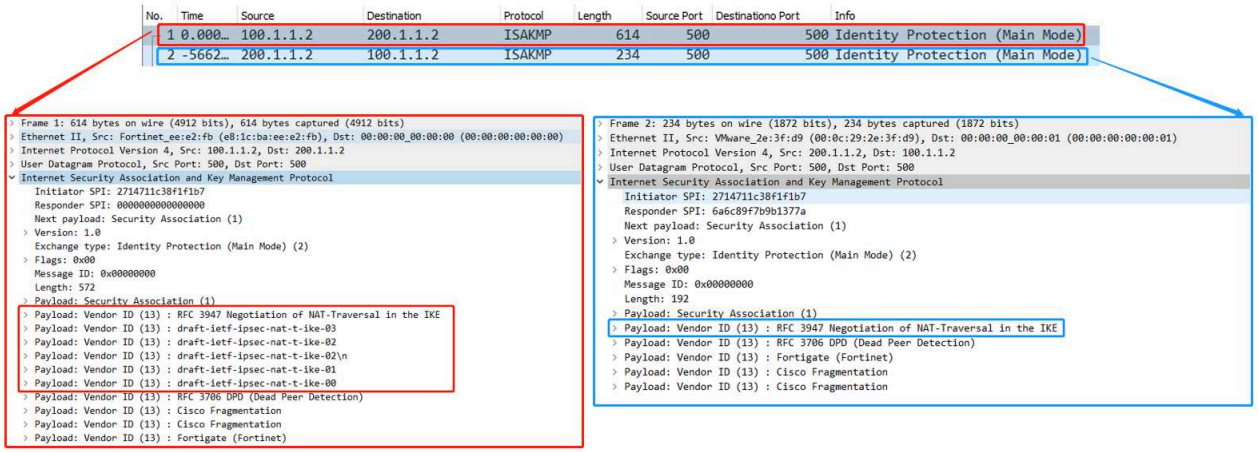




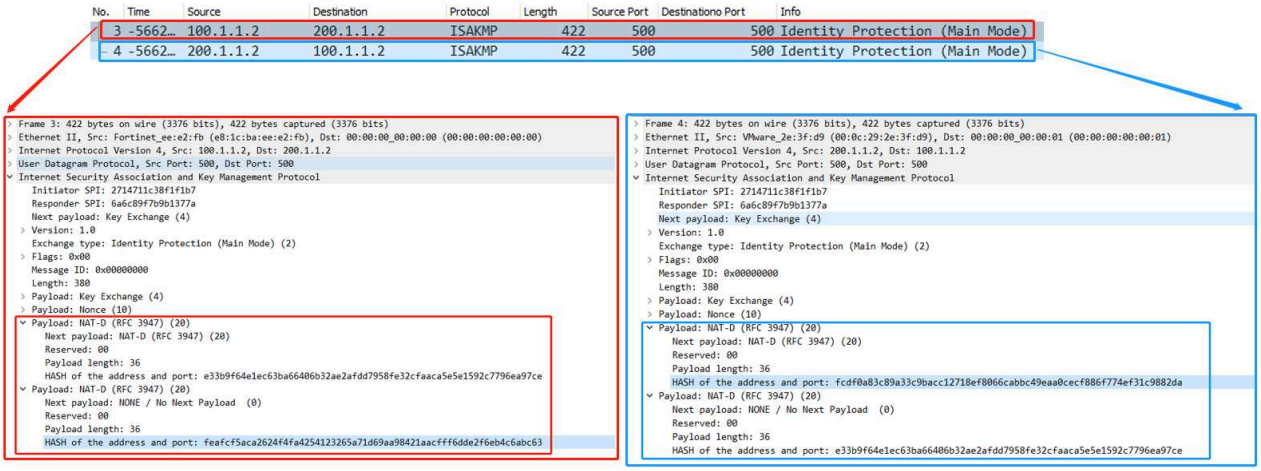
主模式

1. 第1和2个包协商是否支持NAT-T

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 第3和4个包，发起方插入了两个NAT-D载荷。第一个NAT-D载荷包含IKE对等体的IP地址和端口的Hash值，第二个NAT-D载荷包含本端的IP地址和端口的Hash值。响应方也计算这两个Hash值，两方计算的哪个Hash值不相等，表明哪个设备在NAT网关后面。



3. 完成NAT-T检测后，如果发现NAT网关，则后续UDP报文端口号修改为4500。

   当UDP封装的是ISAKMP消息，会增加一个non-ESP marker（为4个值为0的字节），以示跟封装ESP报文有区别。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

No.	Time	Source	Destination	Protocol	Length	Source Port	Destinationo Port	Info
5	-5662…	100.1.1.2	200.1.1.2	ISAKMP	154	4500	4500	Identity Protection (Main Mode)
6	-5662…	200.1.1.2	100.1.1.2	ISAKMP	138	4500	4500	Identity Protection (Main Mode)
7	-5662…	100.1.1.2	200.1.1.2	ISAKMP	666	4500	4500	Quick Mode
8	-5662…	200.1.1.2	100.1.1.2	ISAKMP	490	4500	4500	Quick Mode
9	-5662…	100.1.1.2	200.1.1.2	ISAKMP	122	4500	4500	Quick Mode

```
> Frame 5: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
> Ethernet II, Src: Fortinet_ee:e2:fb (e8:1c:ba:ee:e2:fb), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 100.1.1.2, Dst: 200.1.1.2
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
v UDP Encapsulation of IPsec Packets
    Non-ESP Marker
v Internet Security Association and Key Management Protocol
    Initiator SPI: 2714711c38f1f1b7
    Responder SPI: 6a6c89f7b9b1377a
    Next payload: Identification (5)
  > Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  > Flags: 0x01
    Message ID: 0x00000000
    Length: 108
    Encrypted Data (80 bytes)
```

```
0000  00 00 00 00 00 00 e8 1c  ba ee e2 fb 08 00 45 00   ........ ......E·
0010  00 8c 21 3f 00 00 40 11  2b 1c 64 01 01 02 c8 01   ··!?··@· +·d·····
0020  01 02 11 94 11 94 00 78  53 7c 00 00 00 00 27 14   ·······x S|····'·
0030  71 1c 38 f1 f1 b7 6a 6c  89 f7 b9 b1 37 7a 05 10   q·8···jl ····7z··
0040  02 01 00 00 00 00 00 00  00 6c db f6 30 43 06 5c   ········ ·l··0C·\
0050  aa eb 05 bd 1f 4f 15 1f  92 35 3a ed 71 b3 f1 06   ·····O·· ·5:·q···
0060  22 c5 36 43 cf 32 5e 78  4e 12 31 6c 4a 78 22 df   "·6C·2^x N·1lJx"·
0070  02 1e 87 cb ba fd 6e be  33 f0 e8 2d 6a 33 04 0d   ······n· 3··-j3··
0080  f8 4c f0 29 42 61 e9 ae  01 fe 44 61 95 f4 25 c4   ·L·)Ba·· ··Da··%·
0090  59 a1 49 fa d8 e5 d7 ae  66 85                     Y·I····· f·
```

野蛮模式

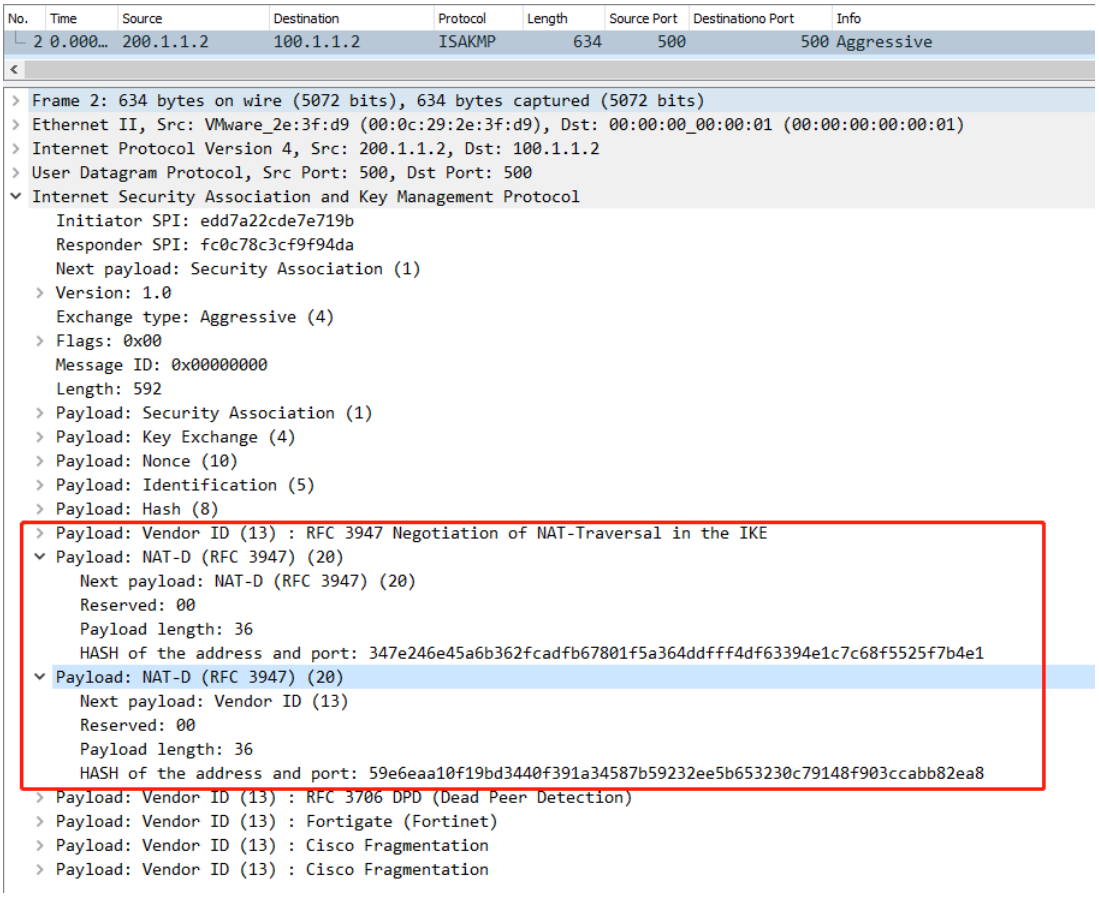
1. 第1个包，发起方在IKE消息中插入Vendor ID来告知对方自己支持NAT穿越。

No.	Time	Source	Destination	Protocol	Length	Source Port	Destinationo Port	Info
1	0.000…	100.1.1.2	200.1.1.2	ISAKMP	762	500	500	Aggressive

```
> Frame 1: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits)
> Ethernet II, Src: Fortinet_ee:e2:fb (e8:1c:ba:ee:e2:fb), Dst: 00:00:00_00:00:00 (00:00:00:00:00:
> Internet Protocol Version 4, Src: 100.1.1.2, Dst: 200.1.1.2
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: edd7a22cde7e719b
    Responder SPI: 0000000000000000
    Next payload: Security Association (1)
  > Version: 1.0
    Exchange type: Aggressive (4)
  > Flags: 0x00
    Message ID: 0x00000000
    Length: 720
  > Payload: Security Association (1)
  > Payload: Key Exchange (4)
  > Payload: Nonce (10)
  > Payload: Identification (5)
  > Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-01
  > Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-00
  > Payload: Vendor ID (13) : RFC 3706 DPD (Dead Peer Detection)
  > Payload: Vendor ID (13) : Cisco Fragmentation
  > Payload: Vendor ID (13) : Cisco Fragmentation
  > Payload: Vendor ID (13) : Fortigate (Fortinet)
```

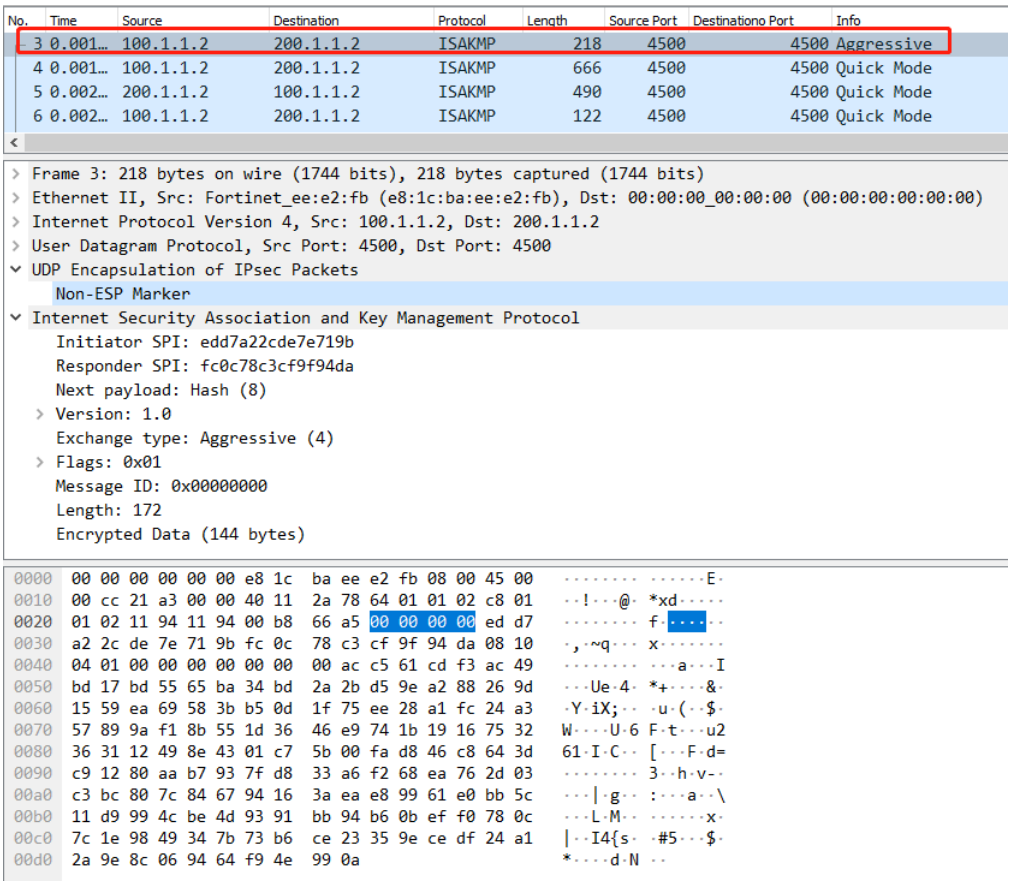
2. 第2个包，响应方确认支持NAT-T，并携带两个NAT-D载荷。第一个NAT-D载荷包含IKE对等体的IP地址和端口的Hash值，第二个NAT-D载荷包含本端的IP地址和端口的Hash值。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 第3个包，发起方同样携带自己的两个NAT-T载荷，响应方也计算这两个Hash值，两方计算的哪个Hash值不相等，表明哪个设备在NAT网关后面，但这个包的数据内容是加密的。完成NAT-T检测后，如果发现NAT网关，则从此UDP报文开始端口号修改为4500。

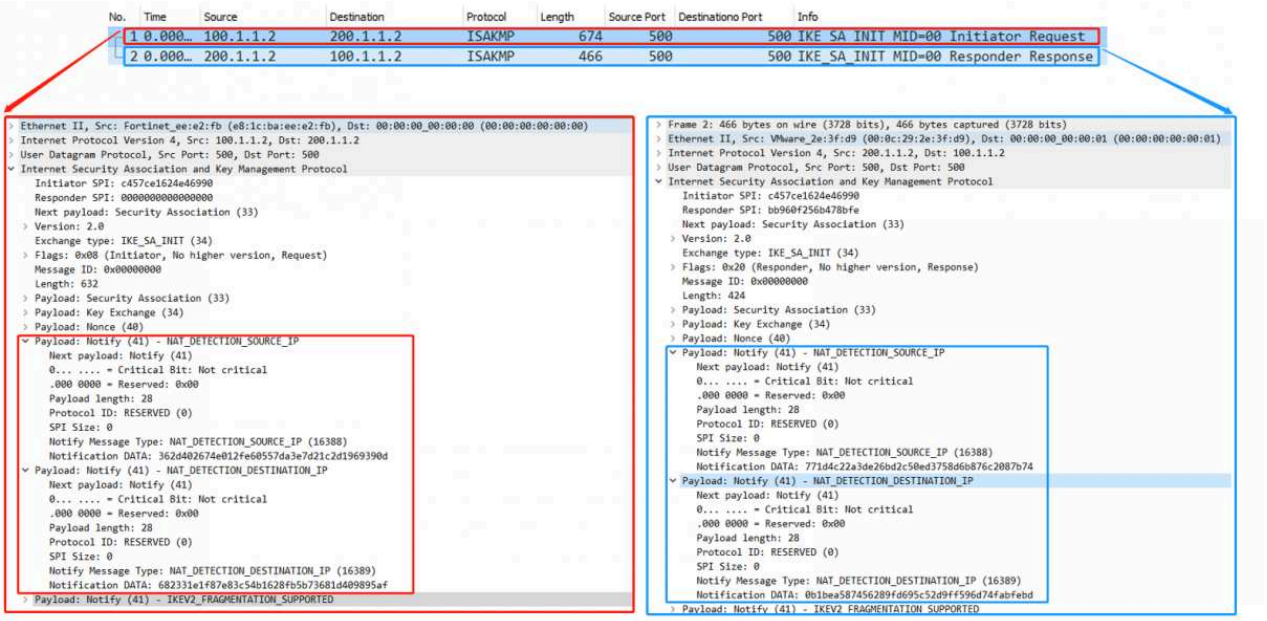
   当UDP封装的是ISAKMP消息，会增加一个non-ESP marker（为4个值为0的字节），以示跟封装ESP报文有区别。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

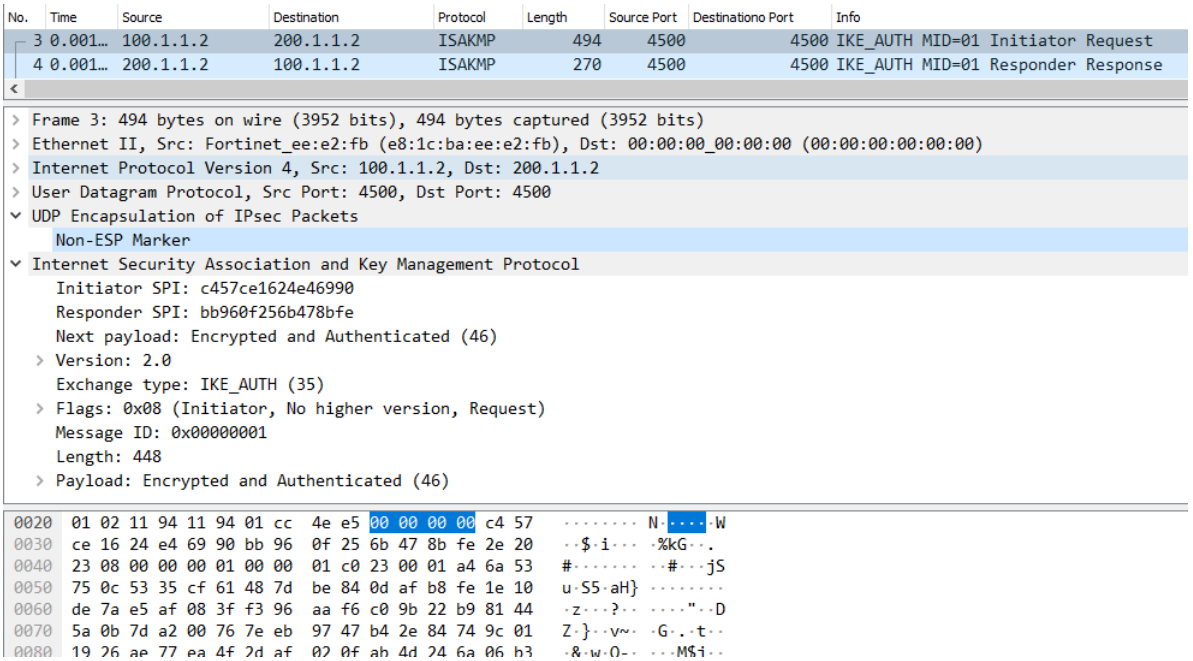
IKEv2穿越NAT

1. 第1和2个包，在IKE消息中插入两个载荷，第一个载荷NAT_DETECTION_SOURCE_IP包含本端的IP地址和端口的Hash值，第二个载荷NAT_DETECTION_DESTINATION_IP包含对端的IP地址和端口的Hash值。这两个通知载荷用于检测在将要建立IPSec隧道的两个网关之间是否存在NAT，如果接收到的NAT_DETECTION_SOURCE通知载荷没有匹配数据包IP头中的源IP和端口的Hash值，则说明对端位于NAT网关后面。如果接收到的NAT_DETECTION_DESTINATION_IP通知载荷没有匹配数据包IP头中的目的IP和端口的Hash值，则意味着本端位于NAT网关之后。



2. 第3和4个包，完成IKE_SA_INIT后，发现NAT设备，后续UDP报文端口号修改为4500。

   当UDP封装的是ISAKMP消息，会增加一个non-ESP marker（为4个值为0的字节），以示跟封装ESP报文有区别。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec DPD模式

DPD简介

1. Dead Peer Detection（DPD）是一种机制，用于检测远程对等方（peer）是否仍然活跃。在IPsec VPN中，两个端点之间的连接可能会由于网络问题或其他原因中断，为了及时发现并处理这种情况，就引入了DPD。
2. DPD通过在IPsec SA（安全关联）之间定期交换检测消息来实现。这些消息通常是在IKE（Internet Key Exchange）阶段协商的。如果一端在一定时间内没有收到来自对等方的DPD消息，就会认为对等方可能已经不再活跃，从而触发重新建立IKE通道或采取其他措施来恢复连接。
3. DPD参数不参与IKE协商，仅本地有效，本地的DPD配置决定自身的DPD探测机制。

DPD模式

FortiGate的DPD配置有3种模式：

- 禁用（disable）：任何情况下都不发送DPD探测报文。**一般情况下不建议选择此模式。**
- 空闲（on-idle）：IPSec隧道内一个方向上没有流量（即idle）时，在这个方向发送DPD探测报文；只有当IPSec隧道双向都有流量时，才不发DPD探测报文。**推荐使用，可以较快地发现隧道中断。**
- 按需（on-demand）：只有IPSec隧道内单向有流量时，在这个方向上发送DPD探测报文，其他情况（双向都有流量或双向都没有流量）下都不发送DPD探测报文。**较少的带宽占用和更少的CPU中断影响，但检测到隧道中断的速度较慢。**

隧道建立阶段	set dpd on-idle	set dpd on-demand
Tunnel建立前 （阶段1已建立，阶段2未建立）	有DPD probe	没有DPD probe
Tunnel建立后 （阶段2已建立，但没有IPSec流量）	有DPD probe	没有DPD probe
Ping over tunnel （Reques/Reply，IPSec双向有流量）	没有DPD probe	没有DPD probe
Ping over tunnel （Reques/no reply，IPSec单向流量）	Ping reply方向有DPD probe	Ping request方向有DPD probe

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec重协商机制

SA到期时间

FortiGate的IPSec关于SA的到期时间，有两个相关的时间概念：

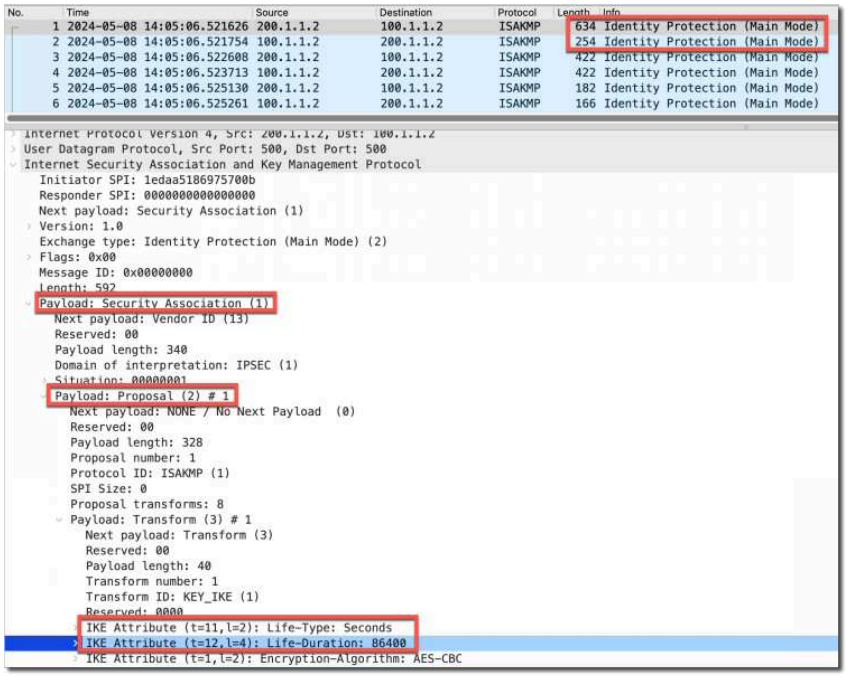
- **hard-timeout**：在IPSec的一阶段和二阶段中，均可以配置重协商超时时间（lifetime，下文我们用hard-timeout来表示配置的lifetime）。当hard-timeout到期后，FortiGate将结束当前一阶段/二阶段的SA。hard-timeout表示每一个一阶段/二阶段SA在本地的最大存在时间。默认配置下，FortiGate的IPSec一阶段重协商（hard-timeout）超时时间为86400s（24小时），二阶段重协商（hard-timeout）超时时间为43200s（12小时）。
- **soft-timeout**：实际的重协商间隔时间会小于hard-timeout，被称为soft-timeout。soft-timeout总是小于hard-timeout。在hard-timeout到期前，FortiGate会发起新的一阶段/二阶段协商并形成一对新的SA。同时，旧的一阶段/二阶段SA直到hard-timeout到期时才会消失，在（hard-timeout - soft-timeout）这个时间差（rekey-margin）内，会存在两对SA。soft-timeout是一种平滑机制，保证在旧SA的hard-timeout到期前协商出新的SA。在旧SA与新SA交替的过程中，IPSec业务不会中断。如果在SA的hard-timeout到期时才重协商新的SA，那么会导致IPSec业务在重协商期间中断。

> **重要**
>
> soft-timeout rekey机制需要在IPSec二阶段中开启 `keepalive` 功能才能生效，详情请参考：VPN→IPSec VPN→自动协商与 keepalive ↗章节。

hard-timeout交互

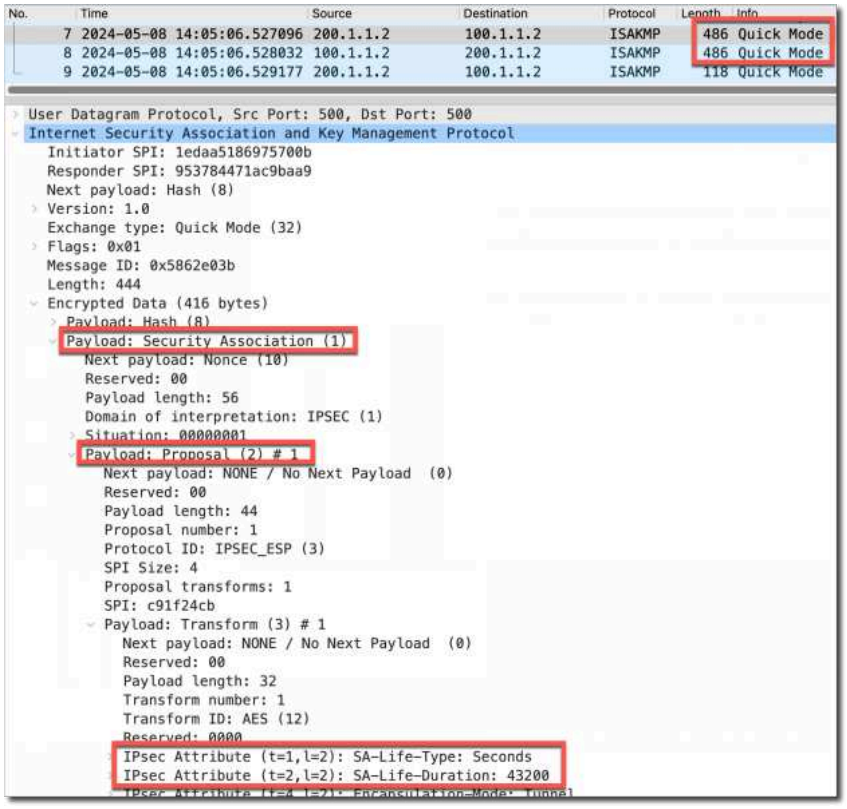
在IPSec一阶段/二阶段协商交互报文中，会携带已配置的重协商时间：

- IKEv1主模式：
  - 一阶段，位于第1、2个协商报文中：

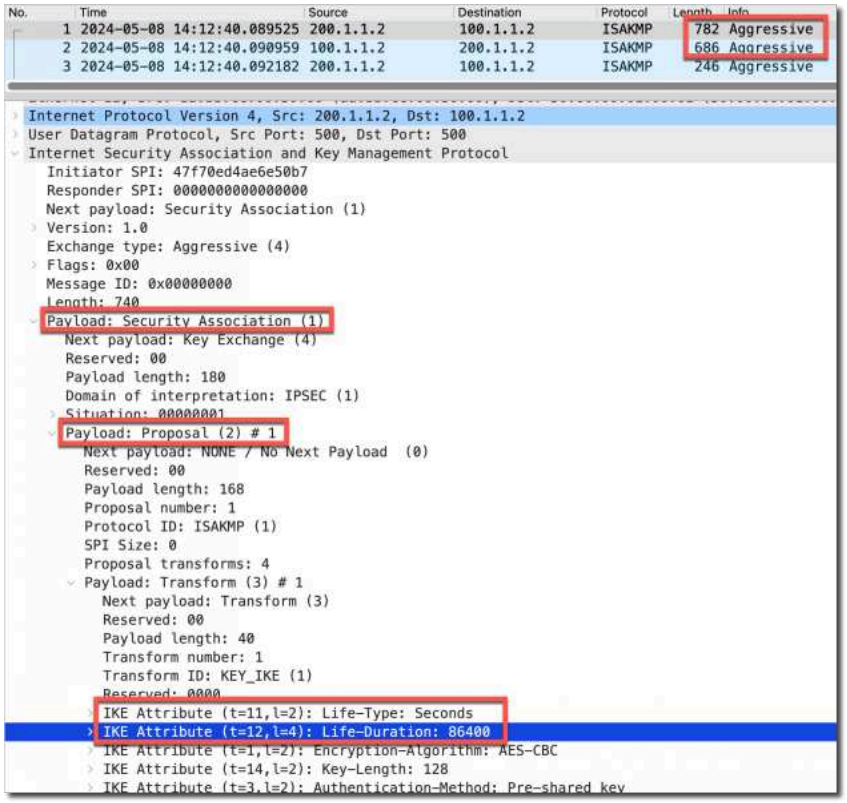


  - 二阶段，位于第1、2个协商报文中：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- IKEv1野蛮模式：
  - 一阶段，位于第1、2个协商报文中：



  - 二阶段：与IKEv1主模式相同，位于第1、2个协商报文中。
- IKEv2：FortiGate一阶段/二阶段协商时不携带hard-timeout参数。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

hard-timeout协商

IKEv1

如hard-timeout交互章节所示，IPSec IKEv1协商的双方会交互hard-timeout参数。但并不会因为双方配置的hard-timeout不一致而导致协商失败。**当IPSec IKEv1协商的双方配置的一阶段/二阶段hard-timeout不一致时，两端IPSec应以IPSec协商双方配置的较小的hard-timeout为准**。如下示例：

1. FW1与FW2之间建立IPSec IKEv1（主模式或野蛮模式）连接，FW1配置IPSec的一阶段/二阶段协商时间为3600s/1800s，FW2配置IPSec的一阶段/二阶段协商时间为1800s/3600s。

```bash
FW1:
config vpn ipsec phase1-interface
    edit "to_FW2"
        set interface "port2"
        set keylife 3600     ←——一阶段hard-timeout
        set net-device disable
        set remote-gw 201.1.1.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FW2"
        set phase1name "to_FW2"
        set keylifeseconds 1800     ←——二阶段hard-timeout
    next
end
```

```bash
FW2:
config vpn ipsec phase1-interface
    edit "to_FW1"
        set interface "port2"
        set keylife 1800     ←——一阶段hard-timeout
        set net-device disable
        set remote-gw 200.1.1.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FW1"
        set phase1name "to_FW1"
        set keylifeseconds 3600     ←——二阶段hard-timeout
    next
end
```

2. 两端IPSec建立后，查看IPSec一阶段的hard-timeout，可以看到FW1和FW2协商成功的一阶段hard-timeout以FW2配置（较小的hard-timeout）为准（1800s）。

```bash
FW1 # diagnose vpn ike gateway list name to_FW2 | grep "lifetime\|name"
name: to_FW2
  lifetime/rekey: 1800/1778     ←——“/”前为协商完成后生效的一阶段hard-timeout

FW2 # diagnose vpn ike gateway list name to_FW1 | grep "lifetime\|name"
name: to_FW1
  lifetime/rekey: 1800/1751     ←——“/”前为协商完成后生效的一阶段hard-timeout
```

3. 查看两端IPSec二阶段的hard-timeout，可以看到FW1和FW2协商成功的二阶段hard-timeout以FW1配置（较小的hard-timeout）为准（1800s）。

```bash
FW1 # get vpn ipsec tunnel name to_FW2 | grep "name\|lifetime"
  name: 'to_FW2'
    name: 'to_FW2'
      lifetime/rekey: 1800/1618     ←——“/”前为协商完成后生效的二阶段hard-timeout
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FW2 # get vpn ipsec tunnel name to_FW1 | grep "name\|lifetime"
  name: 'to_FW1'
    name: 'to_FW1'
      lifetime/rekey: 1800/1564     <———“/”前为协商完成后生效的二阶段hard-timeout
```

IKEv2

IKEv2的协商报文中，不包含任何hard-timeout参数，所以**IKEv2配置下IPSec双方的hard-timeout以本地配置为准，不会进行交互**。如下示例：

1. FW1与FW2之间建立IPSec IKEv2连接，FW1配置IPSec的一阶段/二阶段协商时间为3600s/1800s，FW2配置IPSec的一阶段/二阶段协商时间为1800s/3600s。

bash
```
FW1:
config vpn ipsec phase1-interface
    edit "to_FW2"
        set interface "port2"
        set ike-version 2
        set keylife 3600     <———一阶段hard-timeout
        set net-device disable
        set remote-gw 201.1.1.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FW2"
        set phase1name "to_FW2"
        set keylifeseconds 1800     <———二阶段hard-timeout
    next
end
```

bash
```
FW2:
config vpn ipsec phase1-interface
    edit "to_FW1"
        set interface "port2"
        set ike-version 2
        set keylife 1800     <———一阶段hard-timeout
        set net-device disable
        set remote-gw 200.1.1.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FW1"
        set phase1name "to_FW1"
        set auto-negotiate enable
        set keylifeseconds 3600     <———二阶段hard-timeout
    next
end
```

2. 两端IPSec建立后，查看IPSec一阶段的hard-timeout，可以看到FW1和FW2的一阶段hard-timeout以本地配置的为准，FW1为3600s，FW2为1800s。

bash
```
FW1 # diagnose vpn ike gateway list name to_FW2 | grep "hard-timeout\|name"
name: to_FW2
  lifetime/rekey: 3600/3313     <———“/”前为协商完成后生效的一阶段hard-timeout

FW2 # diagnose vpn ike gateway list name to_FW1 | grep "hard-timeout\|name"
name: to_FW1
  lifetime/rekey: 1800/1725     <———“/”前为协商完成后生效的一阶段hard-timeout
```

3. 查看两端IPSec二阶段的hard-timeout，可以看到FW1和FW2的二阶段hard-timeout以本地配置的为准，FW1为1800s，FW2为3600s。

bash
```
FW1 # get vpn ipsec tunnel name to_FW2 | grep "name\|lifetime"
  name: 'to_FW2'
    name: 'to_FW2'
      lifetime/rekey: 1800/1648     <———“/”前为协商完成后生效的二阶段hard-timeout
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FW2 # get vpn ipsec tunnel name to_FW1 | grep "name\|lifetime"
  name: 'to_FW1'
    name: 'to_FW1'
      lifetime/rekey: 3600/3299     <——“/”前为协商完成后生效的二阶段hard-timeout
```

soft-timeout数值

如上文介绍，soft-timeout会比hard-timeout减小一定的数值（rekey-margin），根据hard-timeout设置的大小以及IPSec连接建立的会话方向是发起方（initiator）还是响应方（responder），这个减去的值会相应变化，总结如下：

重要

- initiator：IPSec一阶段建立成功的发起方，也就是IKE成功协商过程中第1个IKE报文的发起者。
- responder：IPSec一阶段建立成功的响应方，也就是IKE成功协商过程中第2个IKE报文的响应者。

hard-timeout配置	发起方soft-timeout - hard-timeout (rekey-margin)	响应方soft-timeout - hard-timeout (rekey-margin)
hard-timeout < 3600s	-30s	-20s
hard-timeout ⩾ 3600s	-300s	-270s

无论是发起方（initiator）还是响应方（responder），当soft-timeout到期时（hard-timeout还未到期），会主动与对端IPSec协商出一个新的一阶段/二阶段SA，在（hard-timeout - soft-timeout = rekey-margin）这个时间差内，会与旧的SA共存。如下示例：

1. FW1与FW2之间建立IPSec IKEv1（主模式或野蛮模式）连接，FW1配置IPSec的一阶段/二阶段协商时间为120s/120s，FW2配置IPSec的一阶段/二阶段协商时间为120s/120s。为了测试时使FW1一直为响应方（Responder），开启FW1 IPSec一阶段中的`passive-mode`功能（不会主动发起IKE协商）。

```bash
FW1:
config vpn ipsec phase1-interface
    edit "to_FW2"
        set interface "port2"
        set keylife 120     <——一阶段hard-timeout
        set net-device disable
        set passive-mode enable     <——开启passive-mode，不会主动发起IKE协商
        set remote-gw 201.1.1.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FW2"
        set phase1name "to_FW2"
        set keylifeseconds 120     <——二阶段hard-timeout
    next
end
```

```bash
FW2:
config vpn ipsec phase1-interface
    edit "to_FW1"
        set interface "port2"
        set keylife 120     <——一阶段hard-timeout
        set net-device disable
        set remote-gw 200.1.1.2
        set psksecret xxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "to_FW1"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set phase1name "to_FW1"
        set auto-negotiate enable    ←——开启二阶段自动发起协商
        set keylifeseconds 120    ←——二阶段hard-timeout
    next
end
```

2. 两端IPSec建立后，立即查看IPSec一阶段的hard-timeout与soft-timeout，可以看到响应方（responder）FW1的soft-timeout比hard-timeout小20s，发起方（initiator）FW2的soft-timeout比hard-timeout小30s，符合本章节开头的总结。

```bash
FW1 # diagnose vpn ike gateway list name to_FW2 | grep "name\|lifetime\|status\|direction"
name: to_FW2
  direction: responder    ←——FW1为IKE会话的响应方
  status: established 0-0s ago = 0ms    ←——SA已建立时间
  lifetime/rekey: 120/100    ←——作为Responder，soft-timeout比hard-timeout小20s

FW2 # diagnose vpn ike gateway list name to_FW1 | grep "name\|lifetime\|status\|direction"
name: to_FW1
  direction: initiator    ←——FW2为IKE会话的发起方
  status: established 0-0s ago = 0ms    ←——SA已建立时间
  lifetime/rekey: 120/90    ←——作为Initiator，soft-timeout比hard-timeout小30s
```

3. 在连接刚建立时，立即查看IPSec二阶段的hard-timeout与soft-timeout，可以看到响应方（responder）FW1的soft-timeout比hard-timeout小20s，发起方（initiator）FW2的soft-timeout比hard-timeout小30s，符合本章节开头的总结。

```bash
FW1 # get vpn ipsec tunnel name to_FW2 | grep "name\|lifetime"
  name: 'to_FW2'
    name: 'to_FW2'
      lifetime/rekey: 120/100    ←——作为Responder，soft-timeout比hard-timeout小20s

FW2 # get vpn ipsec tunnel name to_FW1 | grep "name\|lifetime"
  name: 'to_FW1'
    name: 'to_FW1'
      lifetime/rekey: 120/90    ←——作为Initiator，soft-timeout比hard-timeout小30s
```

4. 所以理论上，发起方FW2（initiator）的soft-timeout总是比响应方FW1（responder）的soft-timeout先到期。

5. 等待发起方FW2（initiator）的一阶段soft-timeout到期，发起方FW2（initiator）会主动与FW1协商一个新的SA（soft-timeout从90s开始倒计时），旧SA的soft-timeout虽然变为0，但会重新从30s（hard-timeout - soft-timeout）开始倒计时，旧SA的倒计时参数从`rekey`变为`expiry`。

```bash
FW2 # diagnose vpn ike gateway list name to_FW1 | grep "name\|lifetime\|status\|direction"
name: to_FW1
  direction: initiator
  lifetime/rekey: 120/0    ←——FW2(initiator)的soft-timeout倒计时结束

FW2 # diagnose vpn ike gateway list name to_FW1 | grep "name\|lifetime\|status\|direction"
name: to_FW1
  direction: initiator
  lifetime/rekey: 120/90    ←——新的SA生成，rekey时间从90s开始倒计时
  direction: initiator
  hard-timeout/expiry: 120/30    ←——FW2(initiator)的旧SA，soft-timeout到期后，剩余的hard-timeout倒计时
```

6. 30s后，FW2旧SA的`expiry`倒计时结束，旧SA彻底删除，只剩下新的SA。

```bash
FW2 # diagnose vpn ike gateway list name to_FW1 | grep "name\|lifetime\|status\|direction"
name: to_FW1
  direction: initiator
  lifetime/rekey: 120/59    ←——新SA的soft-timeout倒计时，旧SA删除
```

7. 二阶段的情况与一阶段一致，所以在这种soft-timeout机制下，由于旧SA与新SA有共同存在时间差（hard-timeout - soft-timeout），只要网络状态正常，IPSec业务不会产生中断。

Rekey报文交互

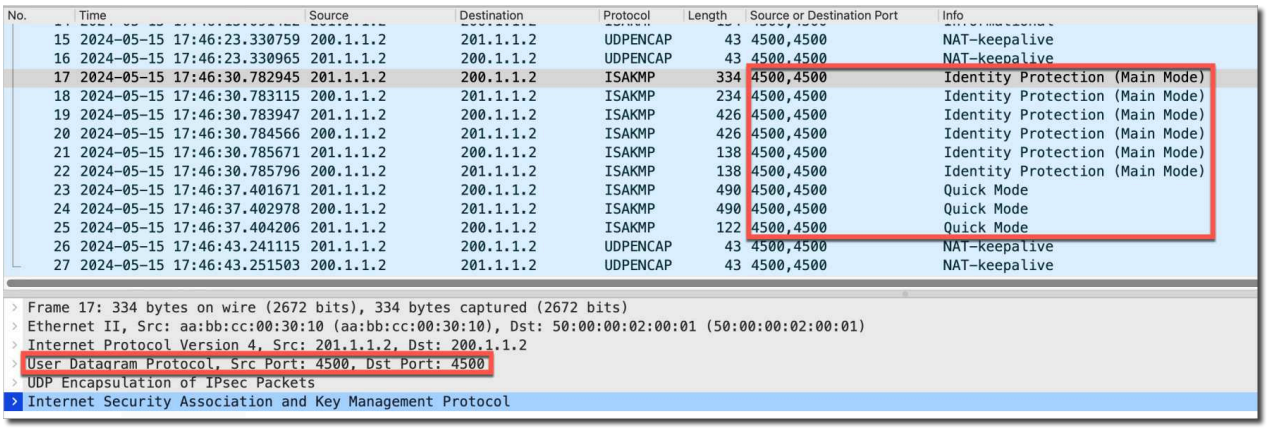
IKEv1主模式

FW2的SA soft-timeout到期时发起的新的SA协商，新的SA协商正常使用IKEv1主模式报文（一阶段6个包，二阶段3个包）交互，根据是否为NAT-T环境，Rekey协商报文所使用的端口有所不同：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- NAT-T：使用Rekey方式协商的IKEv1报文，所有协商报文将使用UDP 4500端口进行协商，报文内容不变。

> **重要**
>
> 而新发起（非Rekey方式）的IKEv1主模式协商第一阶段前4个报文使用UDP 500端口，后2个报文才开始使用UDP 4500端口）。



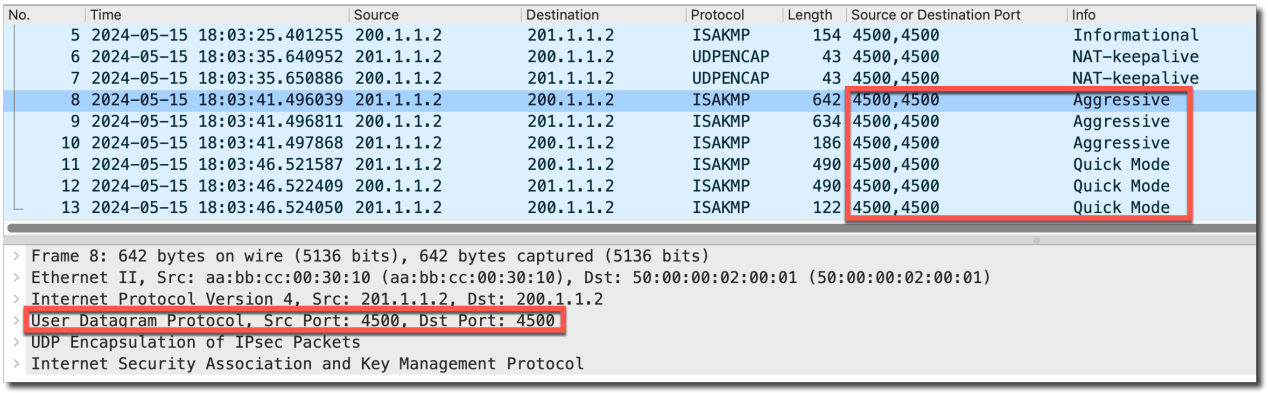
- 非NAT-T：无论是Rekey方式还是新发起的IKEv1主模式协商，都是用UDP 500端口。

IKEv1野蛮模式

FW2的SA soft-timeout到期时发起的新的SA协商，新的SA协商正常使用IKEv1野蛮模式报文（一阶段3个包，二阶段3个包）交互，根据是否为NAT-T环境，Rekey协商报文所使用的端口有所不同：

- NAT-T：使用Rekey方式协商的IKEv1报文，所有协商报文将使用UDP 4500端口进行协商，报文内容不变。

> **重要**
>
> 而新发起（非Rekey方式）的IKEv1野蛮模式协商第一阶段前2个报文使用UDP 500端口，最后1个报文才开始使用UDP 4500端口）。



- 非NAT-T：无论是Rekey方式还是新发起的IKEv1野蛮模式协商，都是用UDP 500端口。

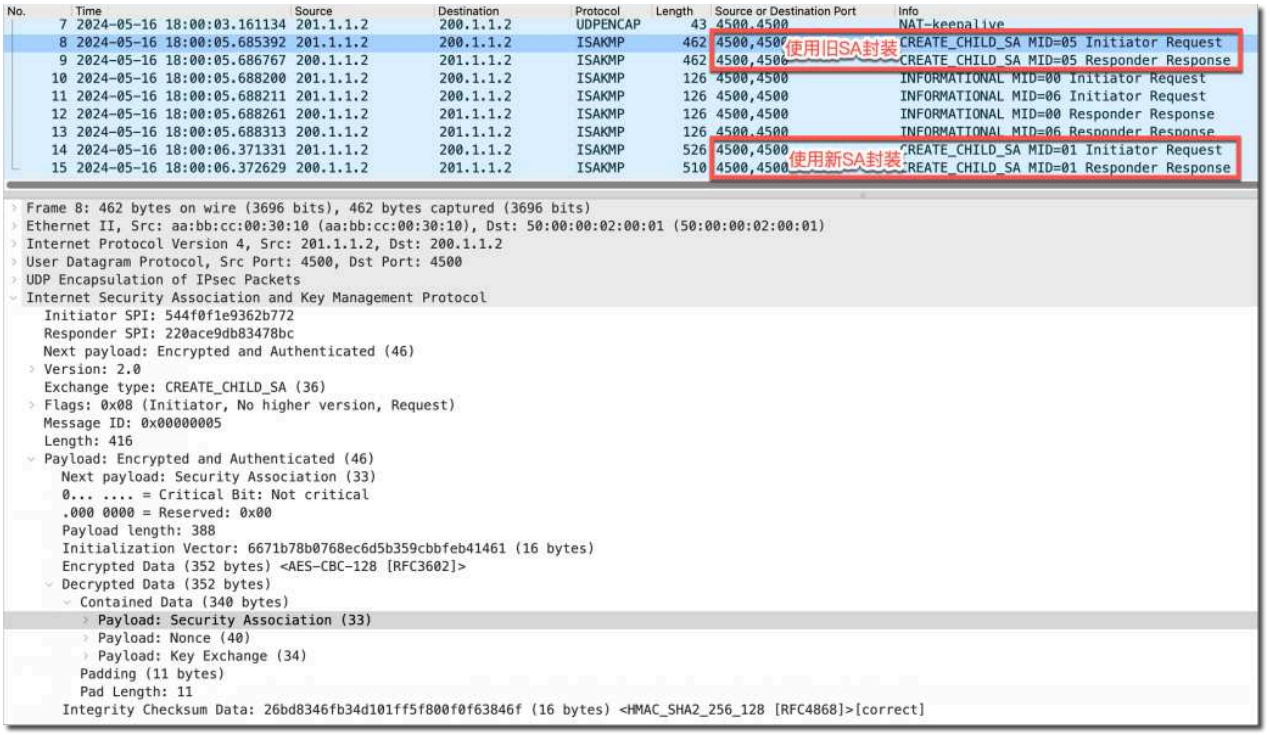
IKEv2

FW2的SA soft-timeout到期时发起的新的SA协商，新的一阶段SA协商包（原IKE_SA_INIT）使用旧的一阶段SA进行加密/验证，使用CREATE_CHILD_SA封装发送，新的二阶段SA协商包（原IKE_AUTH）使用新的一阶段SA进行加密/验证，使用CREATE_CHILD_SA封装发送。所以对于IKEv2的Rekey过程，均是被加密/验证保护的：

- NAT-T：使用Rekey方式协商的IKEv2报文，所有协商报文将使用UDP 4500端口进行协商，报文内容不变。

> **重要**
>
> 而新发起（非Rekey方式）的IKEv2协商IKE_SA_INIT的2个报文使用UDP 500端口，IKE_AUTH的2个报文才开始使用UDP 4500端口）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 非NAT-T：无论是Rekey方式还是新发起的IKEv2协商，都是用UDP 500端口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

自动协商与 keepalive

提示

- 本文主要讨论IPSec 二阶段中的 `auto-negotiate` 和 `keepalive` 。
- IPSec 一阶段中的 `keepalive` 配置是用于保持 NAT-T 环境下的 UDP 4500 会话，不属于本文讨论范围。

配置方法

提示

若IPSec一阶段开启了 `passive-mode` ，二阶段的 `auto-negotiate` 与 `keepalive` 将无法开启。

`auto-negotiate` 与 `keepalive` 是 IPSec 二阶段配置中用于隧道保持在线的机制。二者独立工作，又可搭配使用。

- `auto-negotiate` ：二阶段 SA 不存在时主动发起协商，默认关闭（dynamic 模式的隧道无法配置），无需流量触发。

```bash
config vpn ipsec phase2-interface
    edit <phase2_interface_name>
        set phase1name <phase1_interface_name>
        set auto-negotiate [enable | disable]
    next
end
```

- `keepalive` ：在已经有二阶段 SA 存在的情况下，决定二阶段 SA 达到 soft-timeout 时是否立即 rekey，防止隧道在 hard-timeout 到期时再进行 rekey，导致隧道中断。

相关信息

soft-timeout = hard-timeout – rekey-margin

soft-timeout、hard-timeout、rekey-margin 的相关信息请参考 VPN → IPSec VPN → IPSec重协商机制 ↗章节。

重要

`auto-negotiate` 开启后， `keepalive` 会被强制开启，且 `keepalive` 相关命令消失。只有在 `auto-negotiate` 关闭时才可以控制 `keepalive` 的开关。

```bash
config vpn ipsec phase2-interface
    edit <phase2_interface_name>
        set phase1name <phase1_interface_name>
        set auto-negotiate disable
        set keepalive [enable | disable]
    next
end
```

工作机制

不能将 `auto-negotiate` 和 `keepalive` 混淆，这是两个完全独立的功能。简单来说：

- `auto-negotiate` ：没有二阶段隧道时 → 主动协商建立，无需流量触发。
- `keepalive` ：有二阶段隧道的前提下 → 在soft-timeout 到期时发起rekey防止隧道中断。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

功能	生效条件	开启行为	关闭行为
`auto-negotiate`	二阶段 SA 不存在	持续主动发起二阶段协商，直到 SA 建立，无需流量触发	不会主动发起协商，需流量触发或对端发起
`keepalive`	二阶段 SA 达到 soft-timeout	立即发起二阶段 rekey，需要已建立的二阶段 SA	若最近 2 分钟内无流量，在 hard-timeout 到期时删除 SA，但不会 rekey 若最近 2 分钟内有流量，在 hard-timeout 到期时 rekey

组合行为

`auto-negotiate`	`keepalive`	对应行为
开启	强制开启	二阶段隧道会自动建立，无需流量触发 二阶段 soft-timeout 到期时发起 rekey
关闭	开启	二阶段隧道不会自动建立，需流量触发或对端发起 二阶段 soft-timeout 到期时发起 rekey
关闭	关闭	二阶段隧道不会自动建立，需流量触发 若最近 2 分钟内无流量，在 hard-timeout 到期时删除 SA，但不会 rekey 若最近 2 分钟内有流量，在 hard-timeout 到期时 rekey

配置建议

- `auto-negotiate`：通常建议开启，如有流量付费或性能考虑可设置为关闭。
- `keepalive`：始终建议保持开启，防止二阶段隧道在 hard-timeout 到期后发生中断。

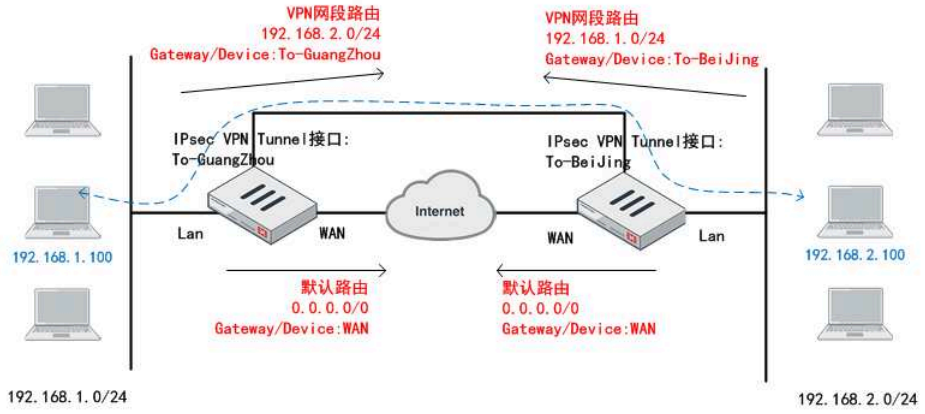
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec的两种配置模式

FortiGate IPsec VPN的两种配置模式

接口模式（默认，推荐使用）：

接口模式作为默认的IPsec VPN方式，FortiGate会自动创建一个IPsec VPN Tunnel接口，然后通过路由将感兴趣流指向IPsec VPN Tunnel，什么样的感兴趣流走IPsec VPN，由路由来决定，配置简单易懂，使用非常灵活，推荐使用。

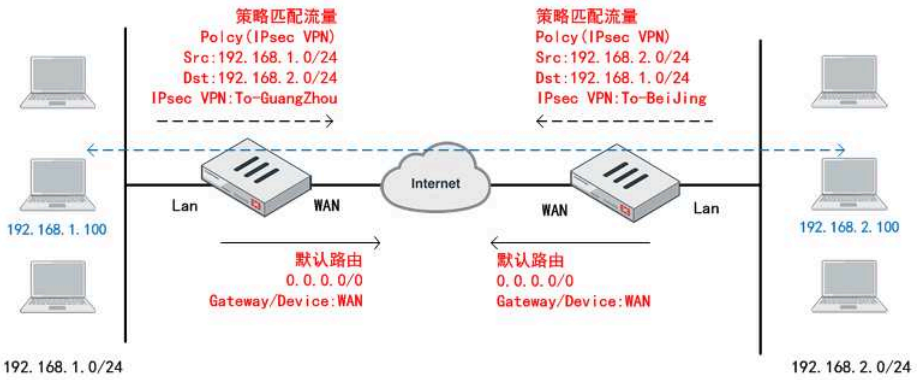


LAN和To-GuangZhou的接口之间通信需满足：

- IPsec VPN隧道UP
- 路由正确
- 策略放通

策略模式（默认隐藏，需要在Features中开启才能使用，不推荐使用）：

通过策略匹配出感兴趣流，然后再策略中调用IPsec VPN，是一种较为传统的IPsec VPN连接方式，一般较少使用，通常推荐使用接口模式IPsec VPN。



IPsec VPN建立起来之后，通过策略将流量匹配，只有感兴趣流才走IPsec VPN，而其他普通数据则走普通的路由从WAN口出去，不会自动生成IPsec tunnel接口，因此不再需要也不能配置指向VPN tunnel的路由。

接口模式 VS 策略模式

为什么FGT默认把策略模式隐藏，而推荐大家使用接口模式呢？

- 策略模式能实现的，几乎接口模式都能实现；
- 接口模式能实现的，策略模式不一定能够实现，例如：GRE OVER IPSEC、隧道上直接跑动态路由协议（RIP/OSPF/BGP）；
- 对于安全设备来说，生成一个VPN-Tunnel接口，策略配置起来的时候，思路更加简单清晰；
- 第二阶段感兴趣流可以配置为any_to_any，感兴趣流量通过路由来引导，而不需要定义与配置复杂的第二阶段感兴趣流；
- 接口模式支持ADVPN，更加适应各种复杂的组网环境；
- 接口模式支持IPv4和IPv6，而策略模式仅支持IPv4。

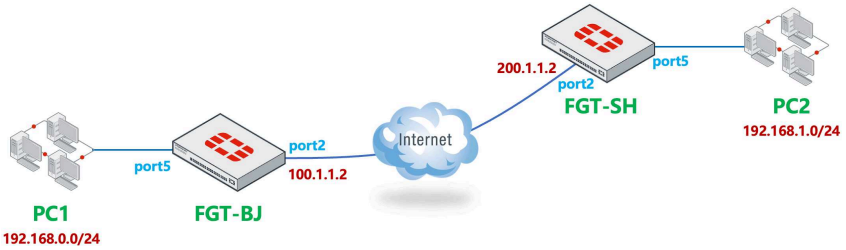
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

接口模式

网络需求

通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信。

网络拓扑



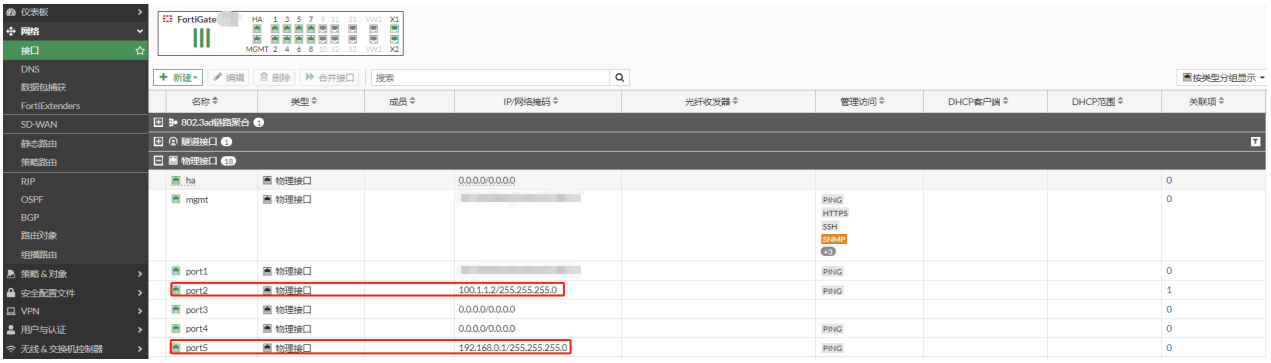
配置步骤

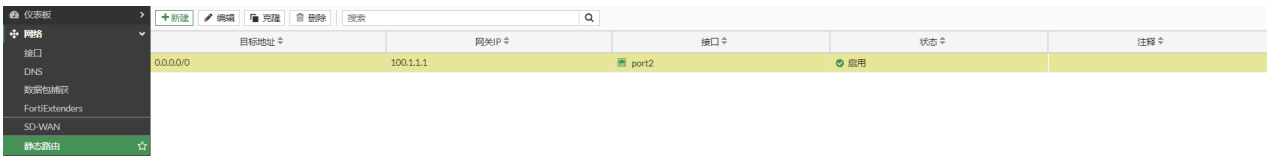
IPSec配置

以FGT-BJ配置步骤为例，FGT-SH同理。

1. 基本配置

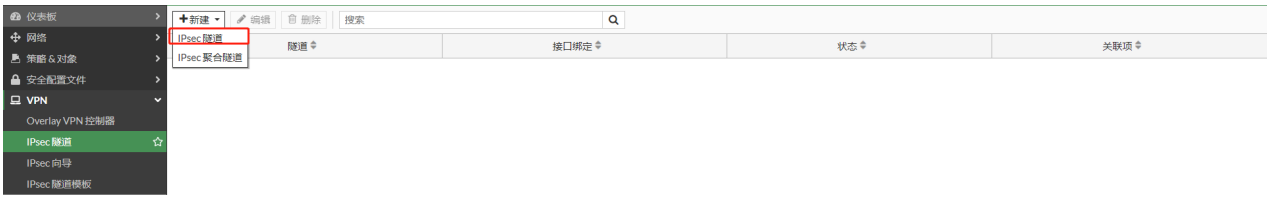
配置接口IP和路由





2. 配置IPSEC VPN

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。

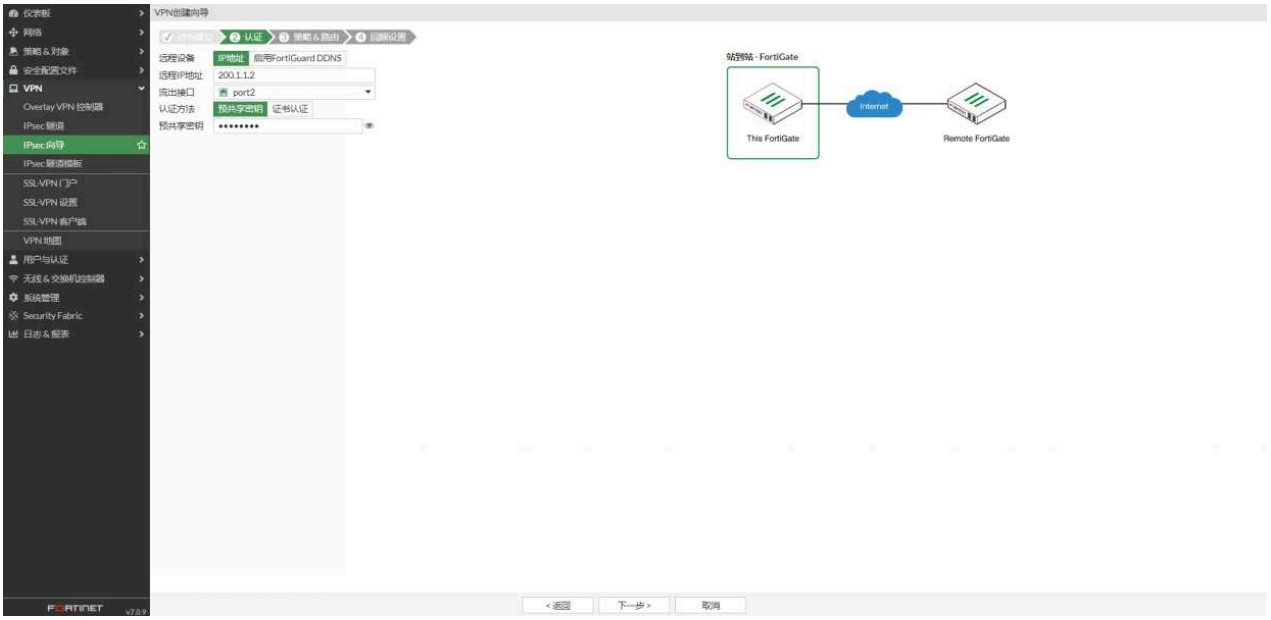


根据“VPN创建向导”进行VPN模板配置，输入名称，拓扑中没有NAT，这里选择“站点之间没有NAT”，并点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

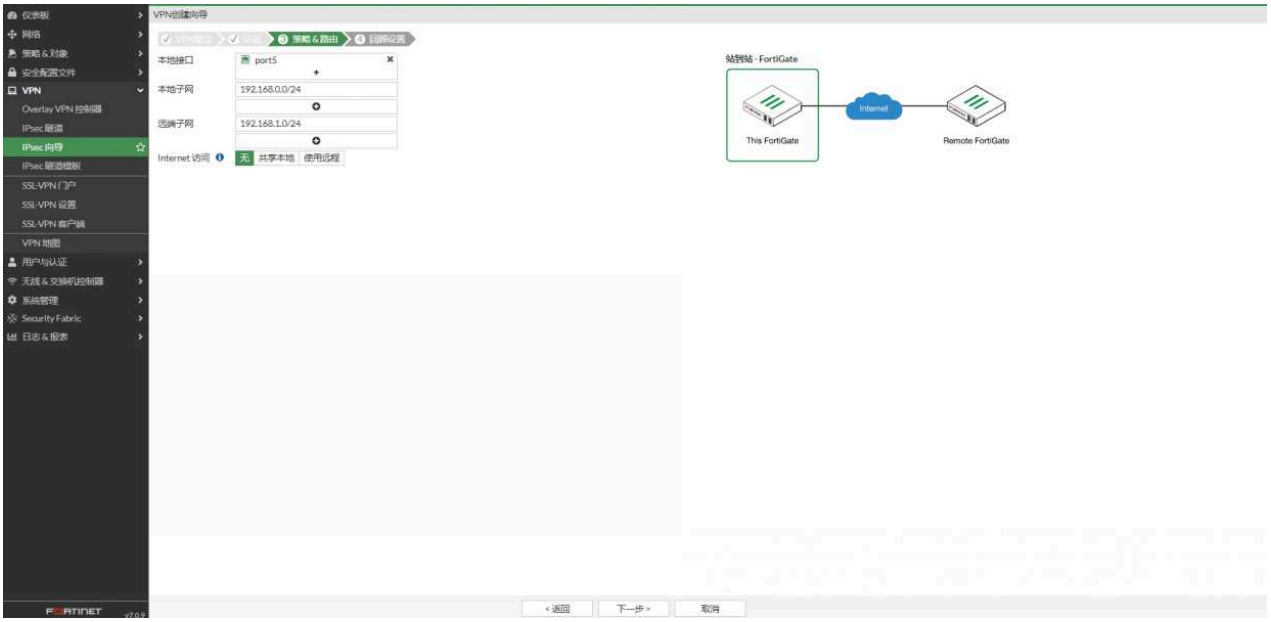


输入对端设备的IP地址（流出接口会根据路由自动选择），以及预共享秘钥。

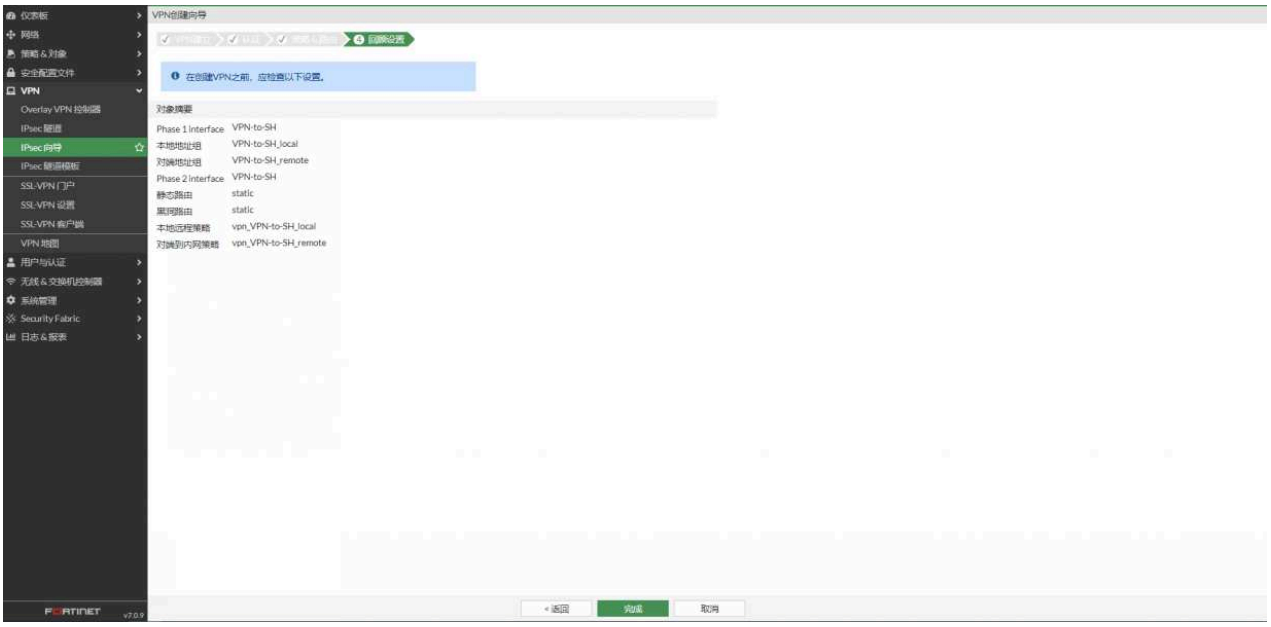


选择“本地接口”，即需要被IPSEC保护的内网的接口，这里是port5接口，本地子网会自动写为该接口的IP所在的IP网段（如果被保护的是其他网段，可以根据实际网络需求修改），输入“远端子网”，即远端需要被保护的网络。然后点击“下一步”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建向导提示即将创建的内容，然后点击完成。



VPN创建成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

如果最后完成模板部署的时候报错，那么需要注意，不要有旧的配置存在，比如相关VPN的策略、VPN的路由、VPN的IP地址对象，因为会冲突，所以需要把这些内容删除干净才可以顺利的部署向导模板，一般第一次部署不会遇到报错。

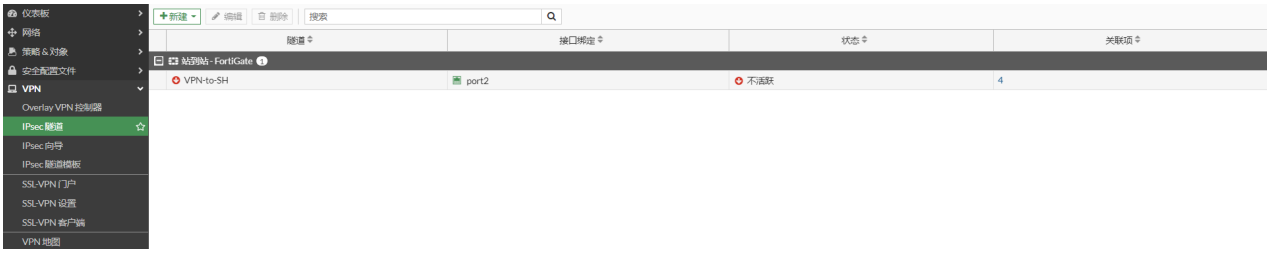
查看IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建地址对象和地址对象组



2. 创建IPSEC隧道



对应的命令行如下：

```bash
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: VPN-to-SH (Created by VPN wizard)"
        set wizard-type static-fortigate
        set remote-gw 200.1.1.2
        set psksecret ENC
feA2LOY0w7mUVHbFI06AZkRjLX80Di1eIIk+FiRIezwPpWU/5oSuf/2LUOIRtrDxOIoyTN+kj5TYADnJOL/K6zQ82ektaS146SvvvZQ9umHQTJJSW7
HtDfDqic1tZAImYJ+APdWC090tUIyc3z5qgcarmPUALfbDSZkmpzY6AtSLMJGHcGVkY4rVTl0GPNekUB/gUg==
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

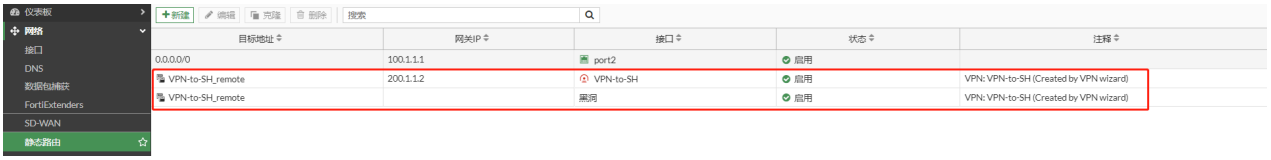
```
end
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set phase1name "VPN-to-SH"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: VPN-to-SH (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN-to-SH_local"
        set dst-name "VPN-to-SH_remote"
    next
end
```

3. 创建路由

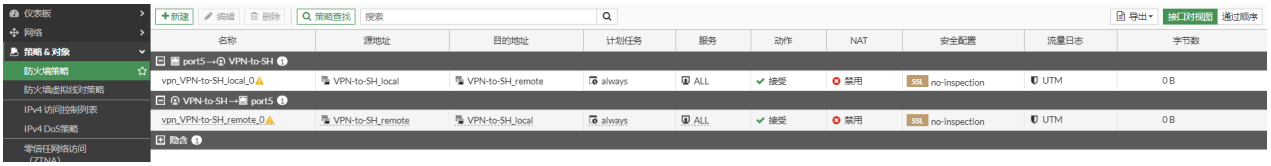
这里到对端的子网创建了两条路由：一条下一跳是VPN-to-SH接口的路由，一条黑洞路由。

> **重要**
>
> IPsec VPN隧道的路由下一跳只是一个隧道ID标识，并不是真正的路由下一跳IP，这和我们普通的路由下一跳不同，如这里的200.1.1.2是隧道的ID。

黑洞路由的目的：VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量会因为查询到了默认路由而走向了port2（Internet），从而产生了不期望的会话，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，业务流量会匹配不期望的会话而走向port2，从而引起该业务异常。因此有了这条黑洞路由就不会产生这条不期望的会话。

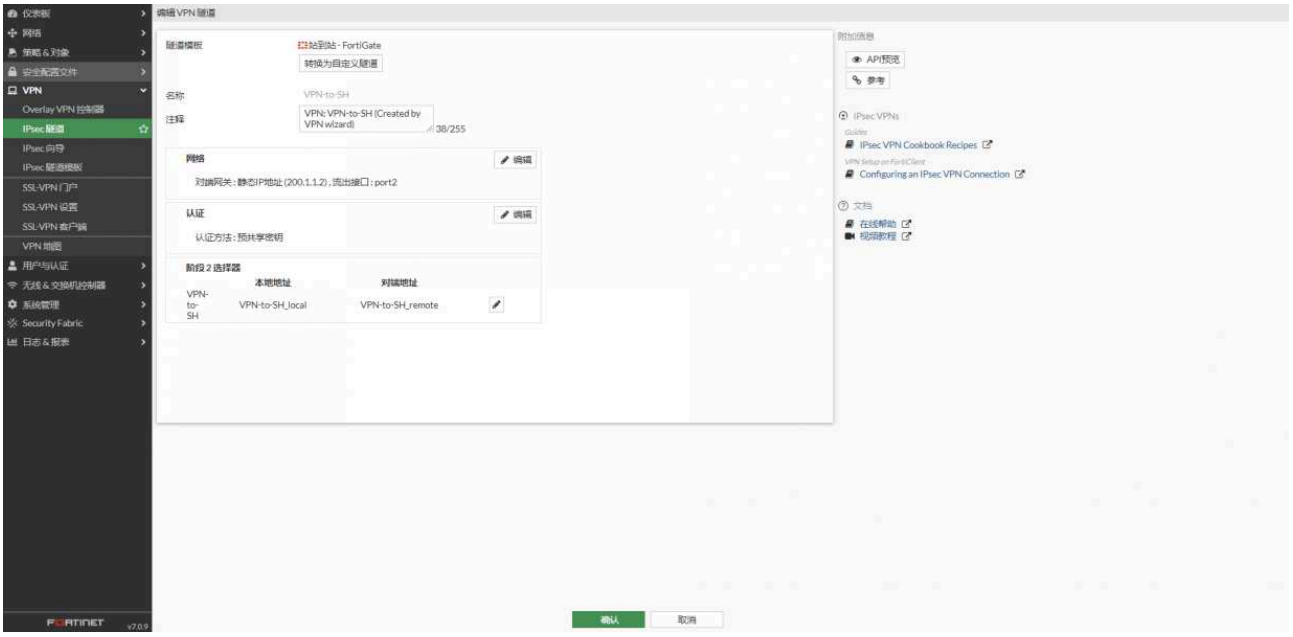


4. 创建策略



修改IPSEC VPN配置

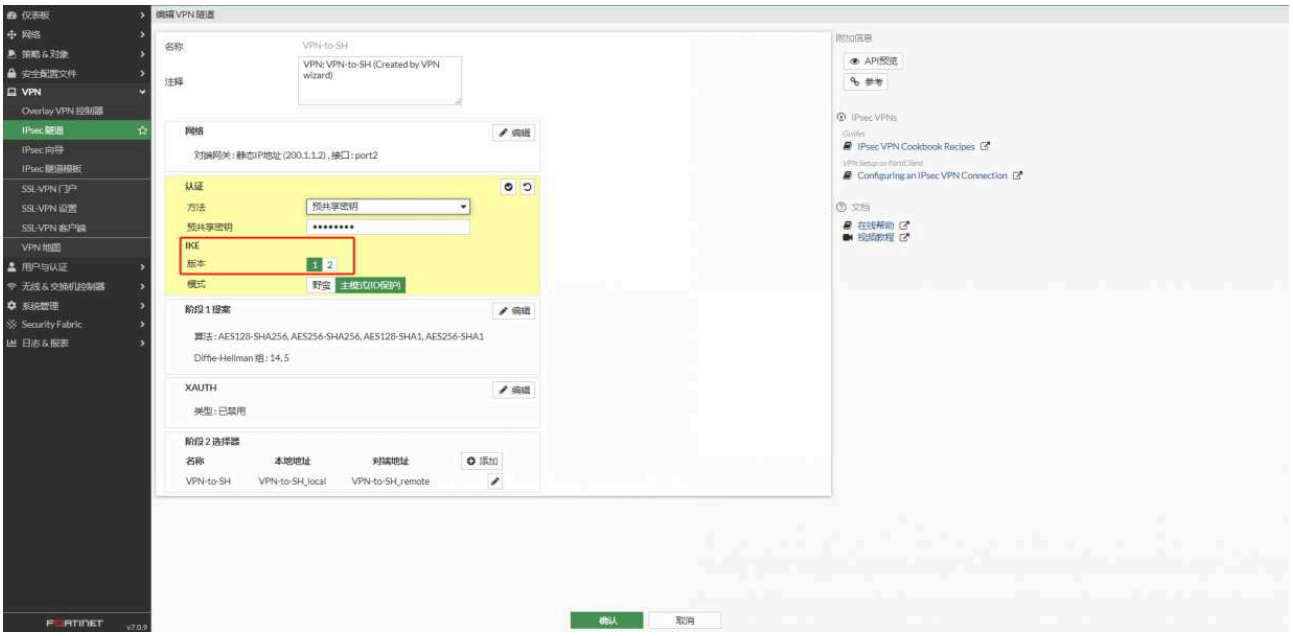
编辑VPN隧道如下图



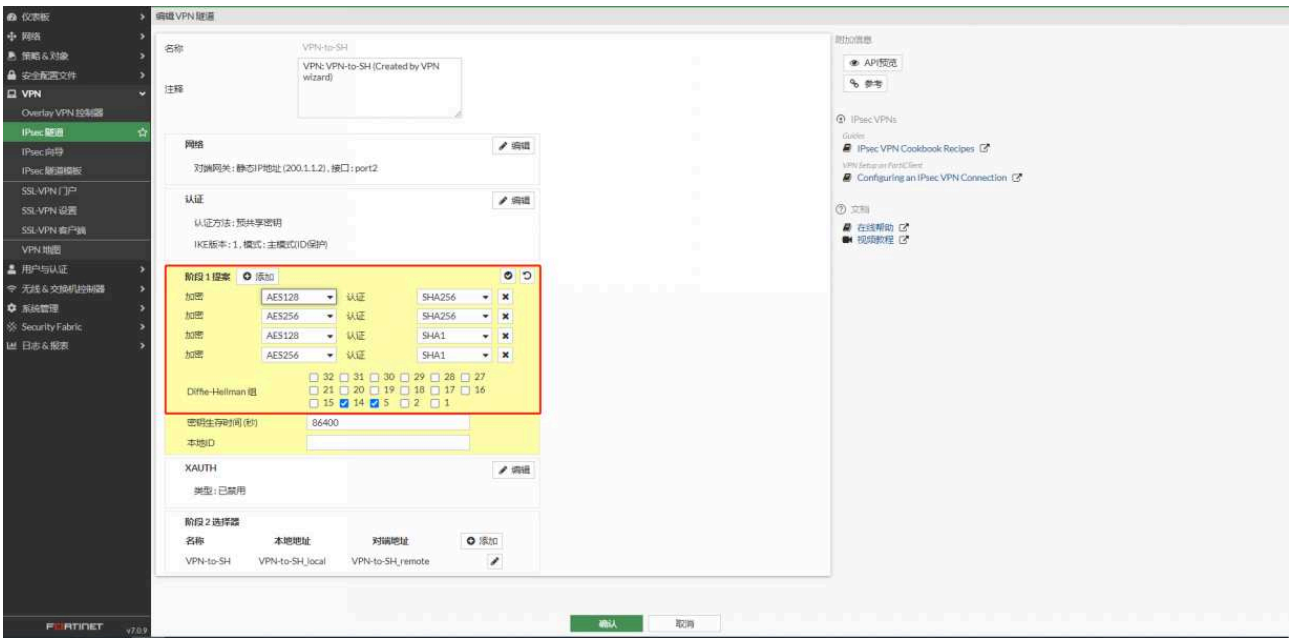
通过点击“转换为自定义隧道”可以在GUI界面设置的更多，是否需要修改可以根据实际网络需求决定。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

如IKE版本（默认使用IKEv1）



如修改阶段一加密和HASH算法



针对向导配置的优化建议

1. 在第一阶段中配置DPD模式为“空闲”（on-idle）（IPSec隧道内没有流量时发DPD探测，只有当IPSec隧道内双向有流量时，才不发DPD探测），实现快速的检测并切换VPN隧道的目的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的命令行

```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

2. 开启自动协商，主动让隧道UP起来，而非使用VPN业务的时候再去触发VPN的协商，这样可以减少业务的丢包。在VPN主动发起方开启即可。

IPSEC VPN阶段一自动协商是默认开启的。

```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

IPSEC VPN阶段二自动协商默认关闭，需要开启。

```
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

查看IPSEC状态

GUI查看IPSEC状态



CLI查看IPSEC状态

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# diagnose vpn ike gateway list

vd: root/0
name: VPN-to-SH
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 200.1.1.2/::200.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 1547s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/2  established 1/1  time 0/0/0 ms

  id/spi: 1428 5264c8b1b5ea006d/587ec20848be628f
  direction: initiator
  status: established 1547-1547s ago = 0ms
  proposal: aes128-sha256
  key: 7646944159f3ebe9-5eb6656064941ede
  lifetime/rekey: 86400/84552
  DPD sent/recv: 000000ec/00000000

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-SH ver=1 serial=3 100.1.1.2:0→200.1.1.2:0 tun_id=200.1.1.2 tun_id6=::200.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=9 olast=9 ad=/0
stat: rxp=1 txp=13 rxb=84 txb=17290
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=236
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-SH proto=0 sa=1 ref=2 serial=3 auto-negotiate
  src: 0:192.168.0.0-192.168.0.255:0
  dst: 0:192.168.1.0-192.168.1.255:0
  SA:  ref=6 options=18227 type=00 soft=0 mtu=1438 expire=41368/0B replaywin=2048
       seqno=e esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=0df9349a esp=aes key=16 6d4d64a051d4c6e4b1dce3c019e9c6c7
       ah=sha1 key=20 f307e4af948aed97e217c89295f50edd78166092
  enc: spi=58e500e1 esp=aes key=16 e751f770f16484e877dd63dd86576d76
       ah=sha1 key=20 3a38ffe6cacee7cae62d04c70aeeb82c9b6a91ff
  dec:pkts/bytes=2/168, enc:pkts/bytes=26/19266
  npu_flag=03 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=9 dec_npuid=1 enc_npuid=1
run_tally=0
```

查看路由

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
S       192.168.1.0/24 [10/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]        ←——到192.168.1.0/24走IPSEC VPN
```

指定IPSec本端的协商IP

如果IPSec绑定在WAN1接口上，但是想使用Loopback接口的IP与对端建立IPSec，应该怎么办呢？这种需求可以通过配置local-gw来实现。如下示例中：

1. FortiGate创建的IPSec绑定在WAN1口上，但wan1口的地址无法和IPSec对端设备直接通信，只有设备上的Loopback接口可以与对端设备通信。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system interface
    edit "wan1"
        set vdom "root"
        set ip 192.168.1.100 255.255.255.255
        set allowaccess ping
    next
    edit "Loopback1"
        set vdom "root"
        set ip 172.22.6.155 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

2. 配置IPSec隧道时，通过local-gw来指定本端协商IPSec时所使用的源IP地址。

> **重要**
>
> 在硬件FortiGate上，接口（Interface）不要选择Loopback接口，会导致IPSec流量无法被NP加速，本地网关（local-gw）可以选择Loopback接口。




```bash
config vpn ipsec phase1-interface
    edit "to_Home_WAN1"
        set interface "wan1"
        set local-gw 172.22.6.129
    next
end
```

3. IPSec协商与业务流量仍然从wan1接口发出，但源IP会使用Loopback1接口的IP。

```bash
FortiGate # diagnose sniffer packet any 'host 123.112.245.210 and udp' 4
interfaces=[any]
filters=[host 123.112.245.210 and udp]
18.804385 wan1 out 172.22.6.129.500 → 123.112.245.210.500: udp 649
18.816603 wan1 in 123.112.245.210.500 → 172.22.6.129.500: udp 432
18.819713 wan1 out 172.22.6.129.4500 → 123.112.245.210.4500: udp 276
18.828528 wan1 in 123.112.245.210.4500 → 172.22.6.129.4500: udp 244
18.974296 wan1 out 172.22.6.129.4500 → 123.112.245.210.4500: udp 120
21.877118 wan1 in 123.112.245.210.4500 → 172.22.6.129.4500: udp 104
21.877318 wan1 out 172.22.6.129.4500 → 123.112.245.210.4500: udp 104
21.882354 wan1 in 123.112.245.210.4500 → 172.22.6.129.4500: udp 104
...
```

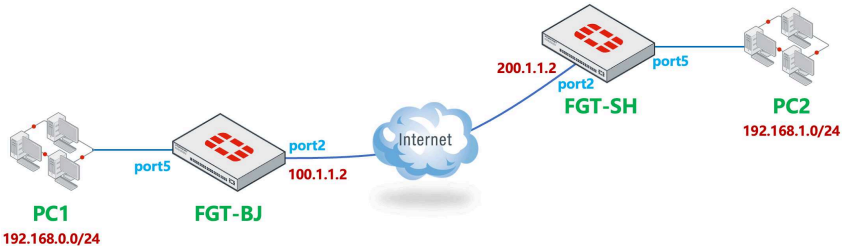

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

PKI证书认证

网络需求

通过IPsec VPN将2个局域网连接起来，IPsec VPN隧道需要采用证书认证方式来协商，实现192.168.0.0/24与192.168.1.0/24两个网段的通信。

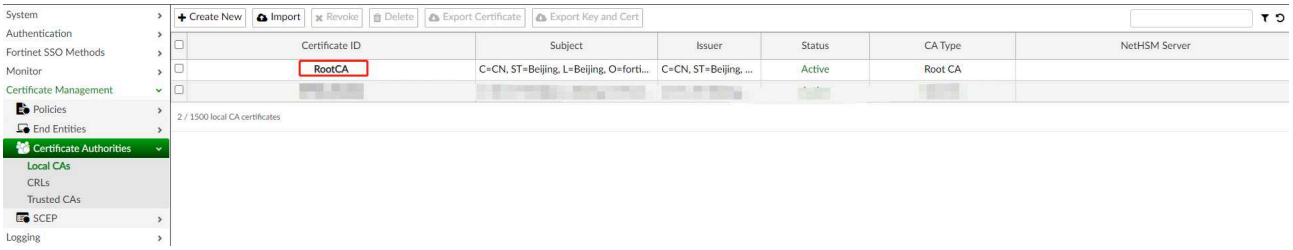
网络拓扑



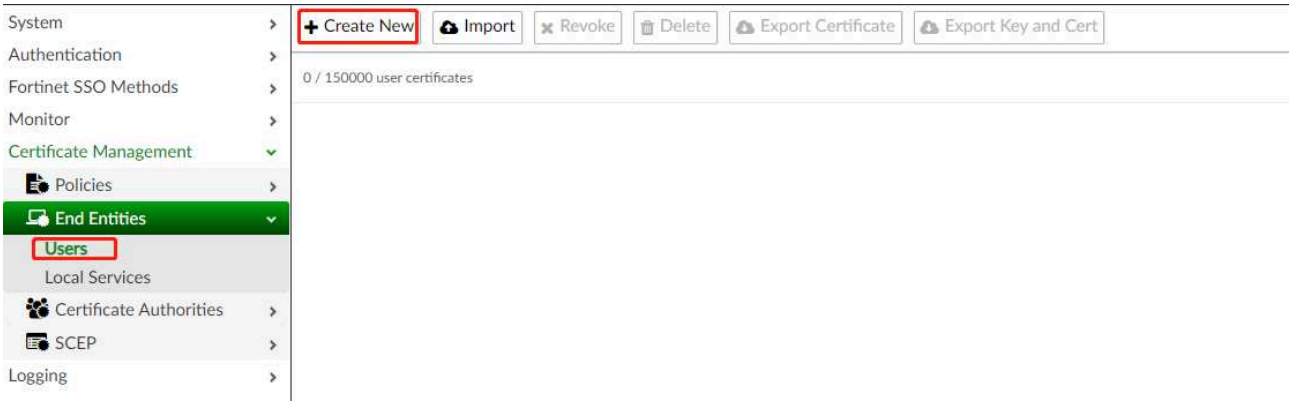
配置步骤

使用FortiAuthenticator为FGT-BJ和FGT-SH颁发证书

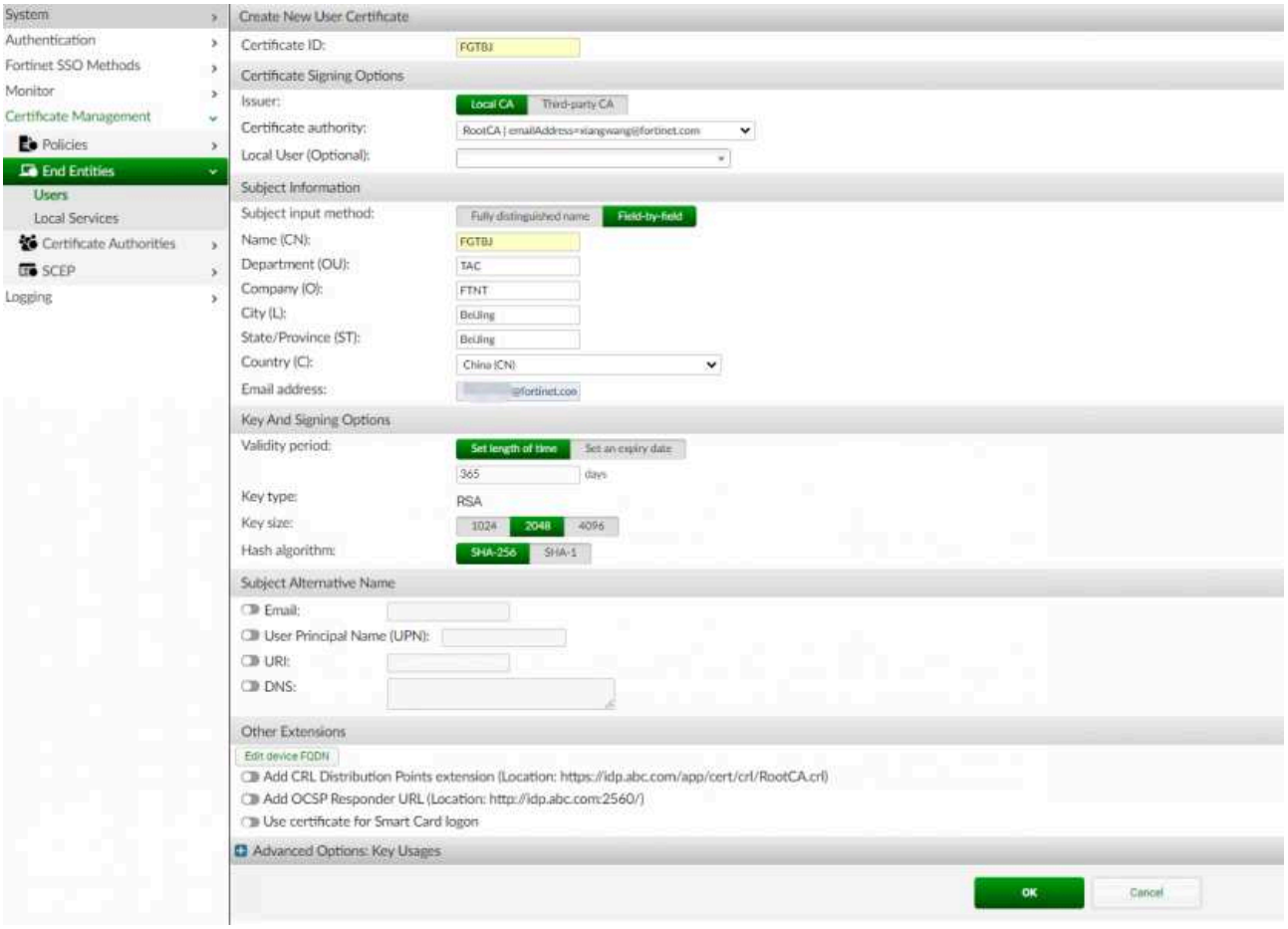
FortiAuthenticator可以做为证书服务器，RootCA是已创建好的根证书，这里使用RootCA为这两台FortiGate签发证书。（也可以使用其他证书服务器）



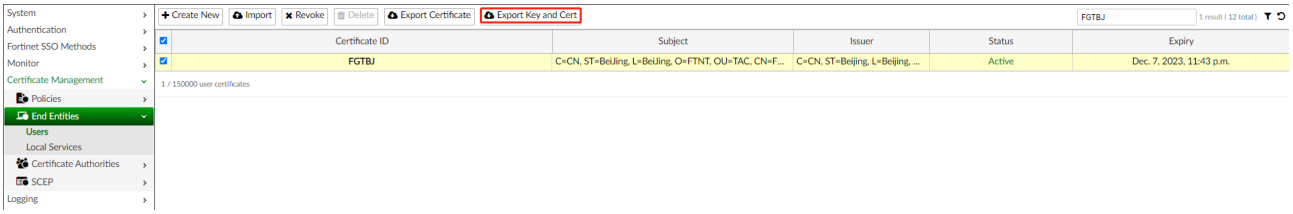
为FGT-BJ创建证书，FGT-SH同理。选择“End Entities”-->"User"，点击“Create New”，输入证书相关信息，并点击完成。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击“Export Key and Cert”导出FGTBJ证书的私钥和公钥。



输入一个密码保护私钥



下载证书

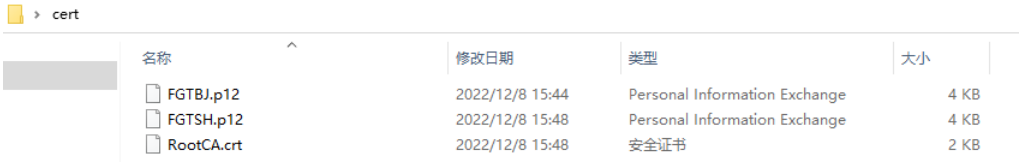
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiGate导入证书

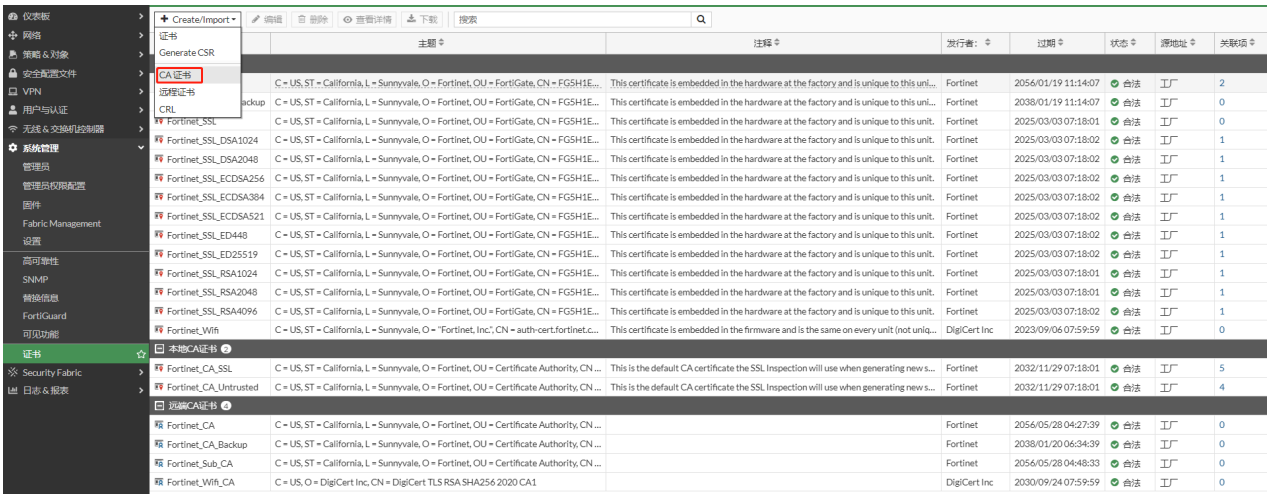
将根证书RootCA.crt和证书FGTBJ.p12导入到FGT_BJ。同理将根证书RootCA.crt和证书FGTSH.p12导入到FGT_SH。

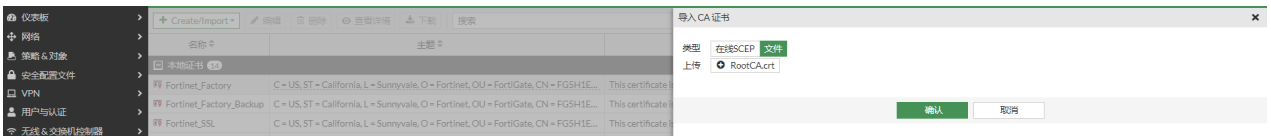
在数字证书认证中，通信双方使用CA证书进行数字证书合法性验证，双方各有自己的公钥（网络上传输）和私钥（本地存储）。发送方对报文进行Hash计算，并用自己的私钥对报文计算结果进行加密，生成数字签名。接收方使用发送方的公钥对数字签名进行解密，并对报文进行Hash计算，判断计算结果与解密后的结果是否相同。如果相同，则认证通过；否则认证失败。



1. 导入CA证书

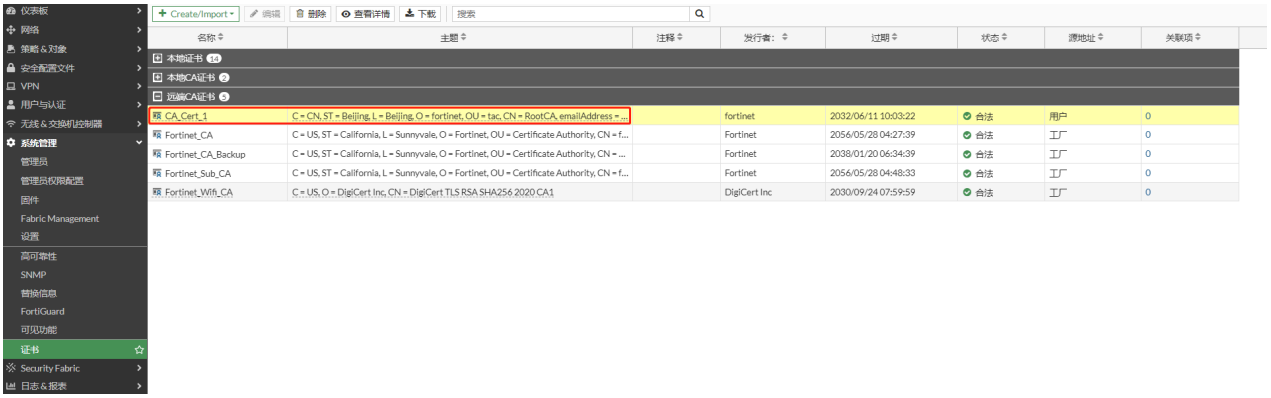
选择“系统管理”-->“证书”，点击“Create/Import”，选择CA证书。





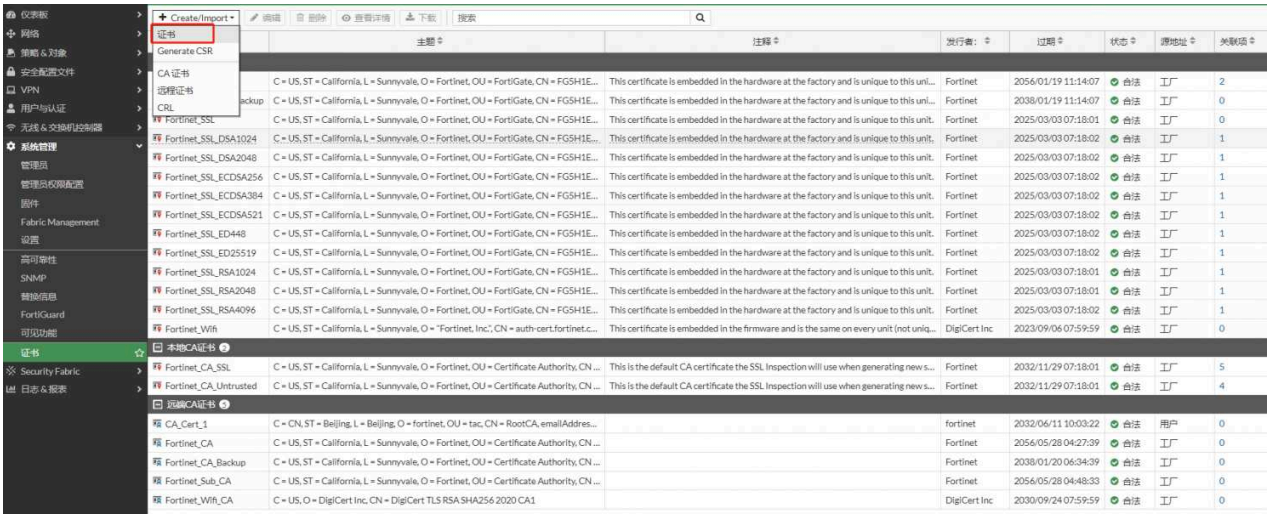
查看导入的CA证书

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

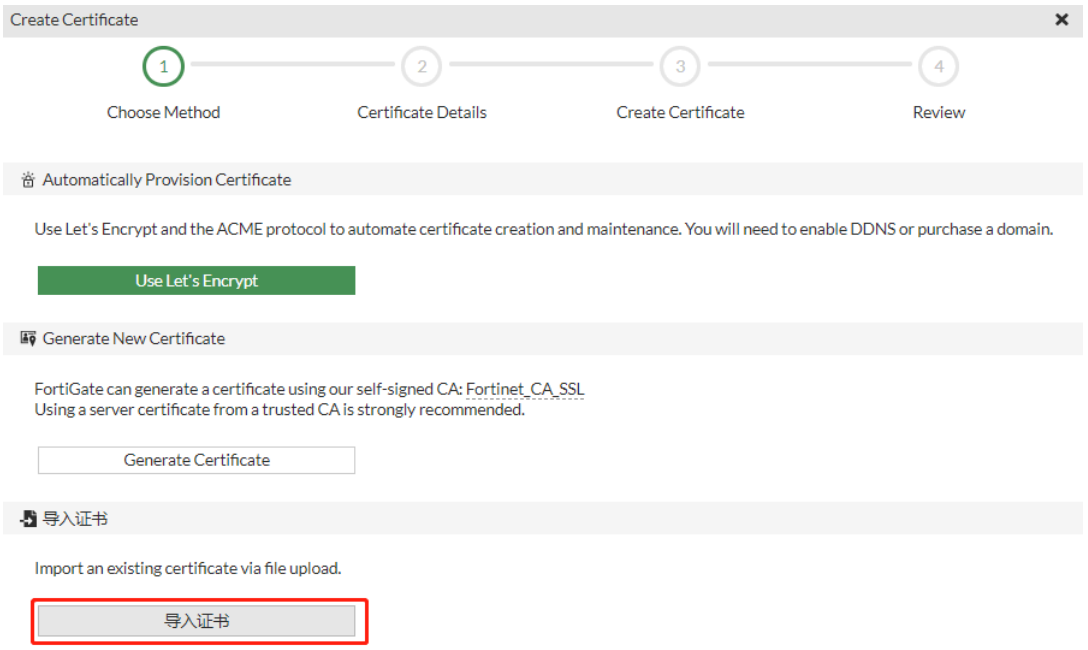


2. 导入本地证书

选择“系统管理”-->“证书”，点击“Create/Import”，选择“证书”。

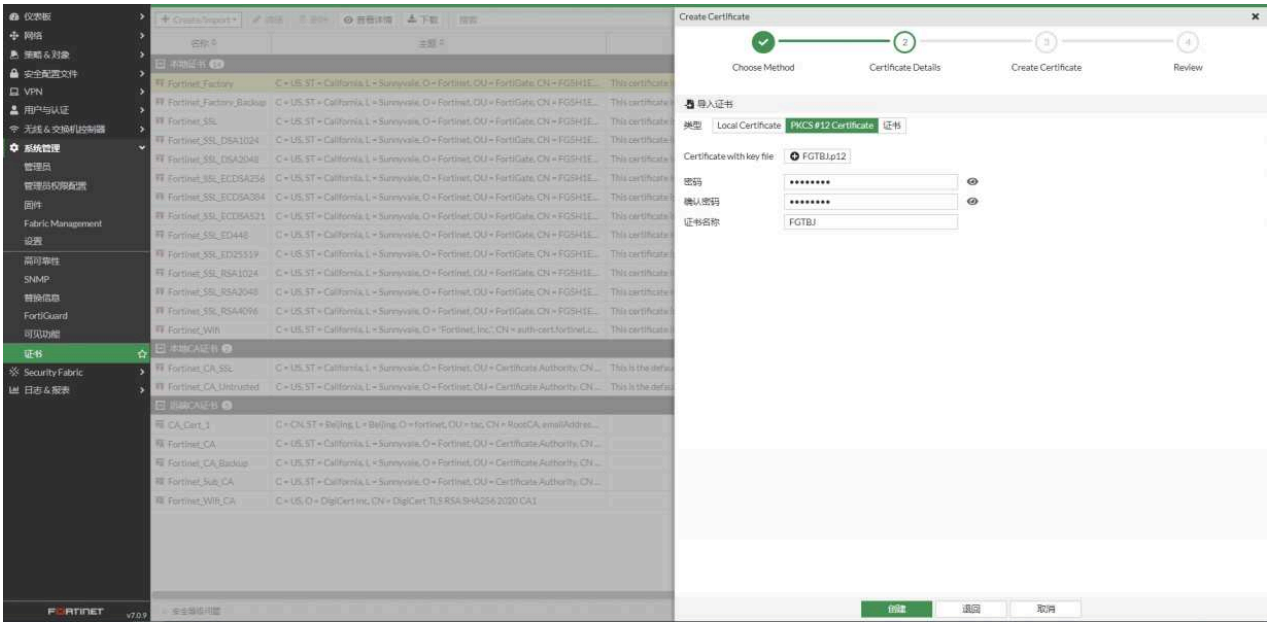


点击导入证书

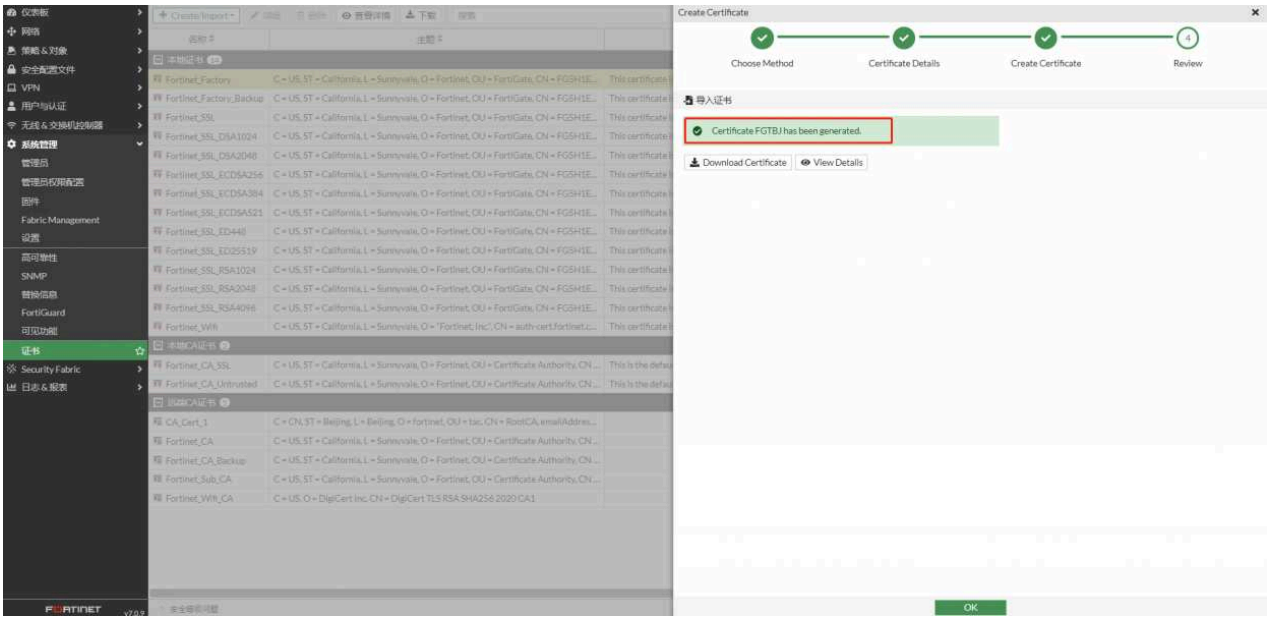


输入证书的密码，点击“创建”

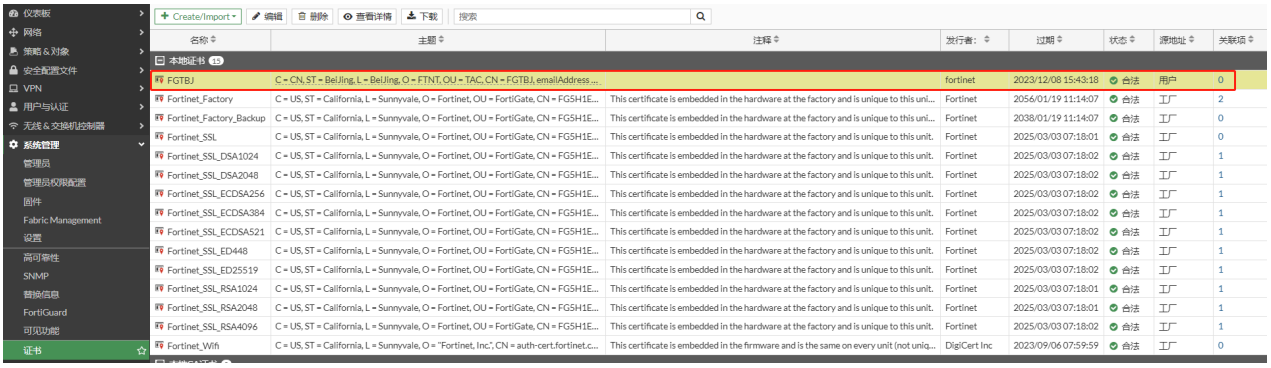
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



提示证书已成功导入



查看导入的本地证书



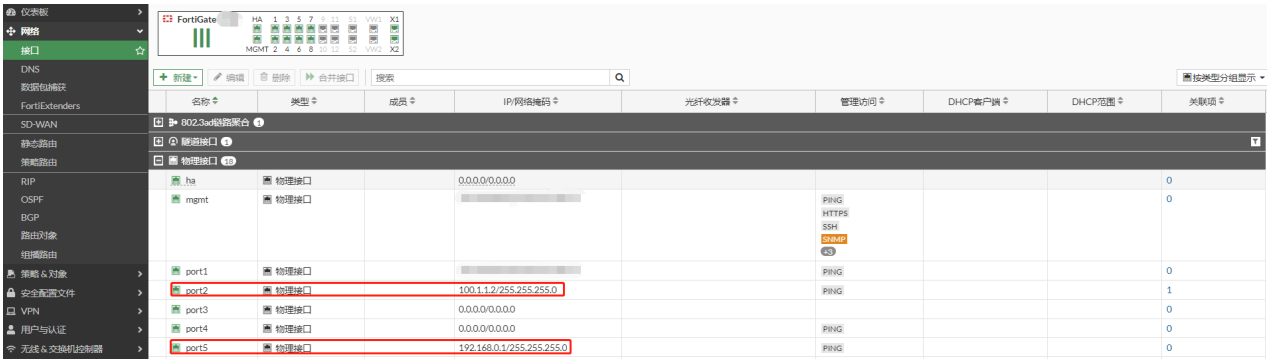
配置IPSec

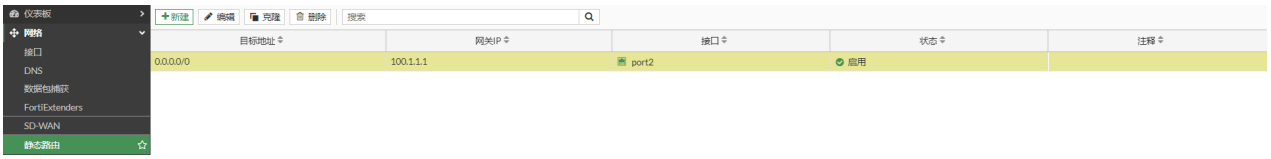
以FGT-BJ配置步骤为例，FGT-SH同理。

1. 基本配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

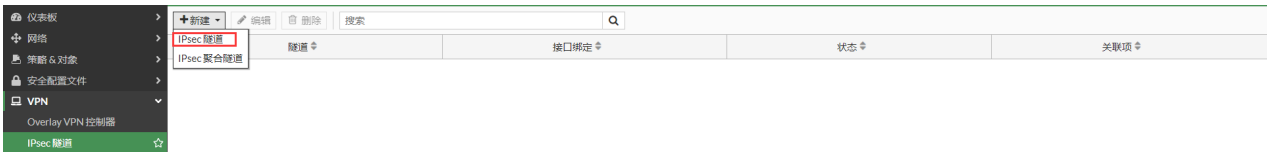
配置接口IP和路由





2. 配置IPSEC VPN

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



根据“VPN创建向导”进行VPN模板配置，输入名称，拓扑中没有NAT，这里选择“站点之间没有NAT”，并点击下一步。

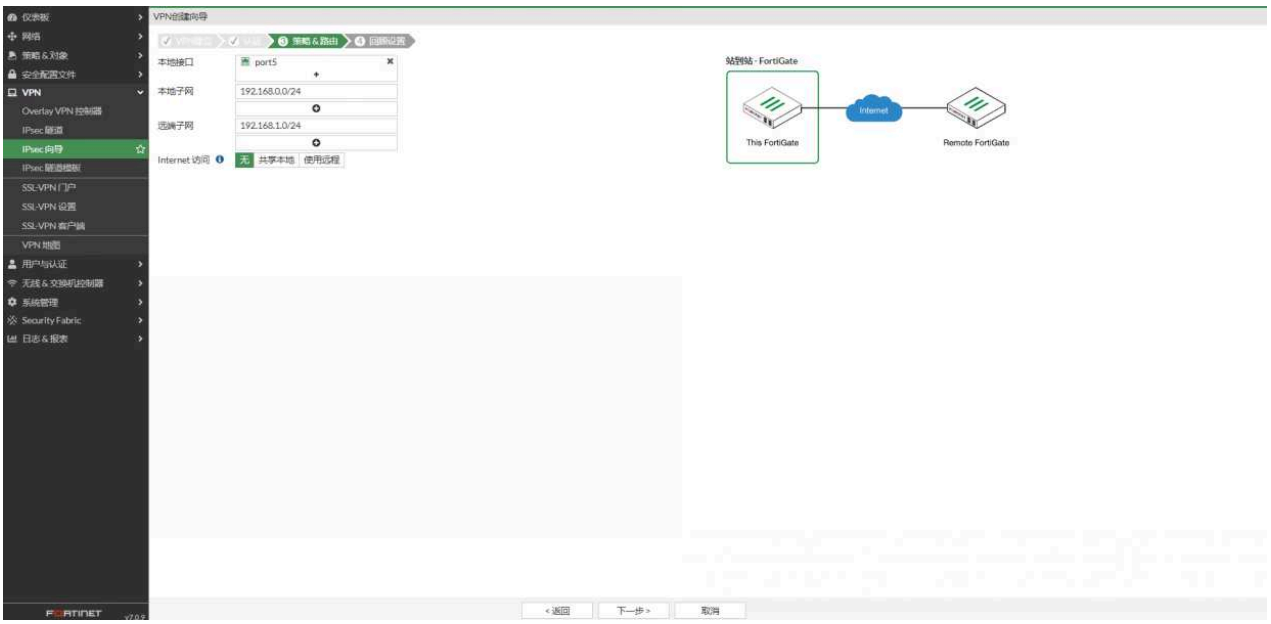


输入对端设备的IP地址（流出接口会根据路由自动选择），在证书认证中选择导入的本地证书“FGTBJ”，对端证书CA选择导入的CA证书“CA_Cert_1”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

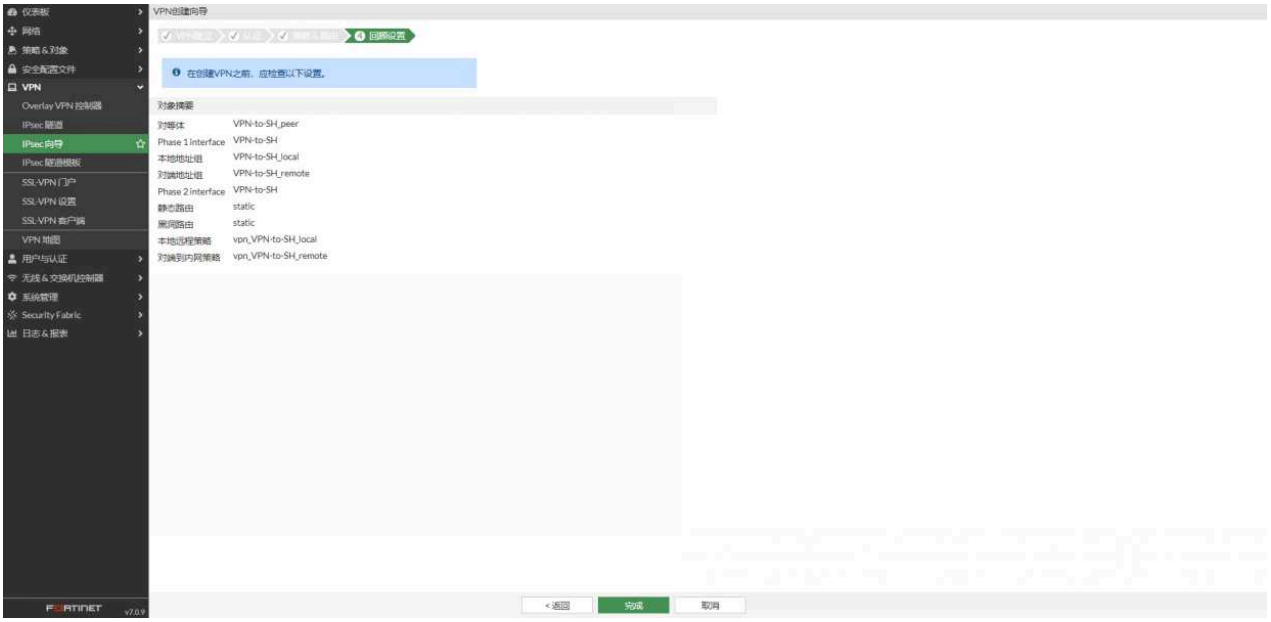


选择“本地接口”，即需要被IPSEC保护的内网的接口，这里是port5接口，本地子网会自动写为该接口的IP所在的IP网段（如果被保护的是其他网段，可以根据实际网络需求修改），输入“远端子网”，即远端需要被保护的网络。然后点击“下一步”。

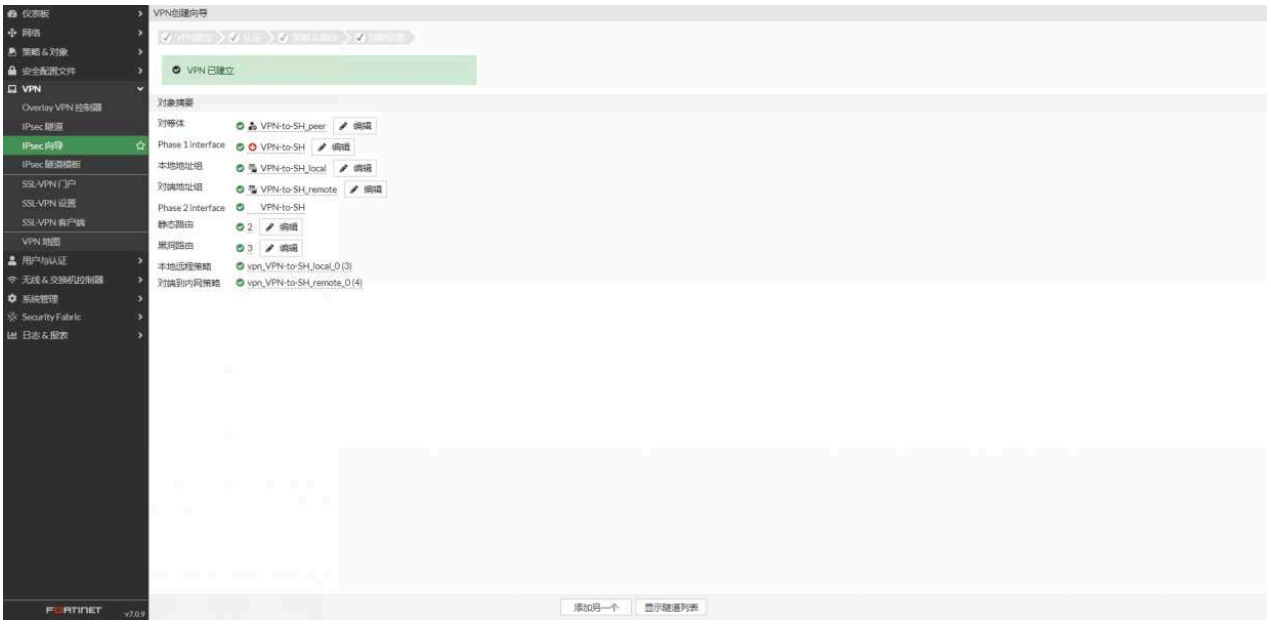


VPN创建向导提示即将创建的内容，然后点击完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建成功。



重要

如果最后完成模板部署的时候报错，那么需要注意，不要有旧的配置存在，比如相关VPN的策略、VPN的路由、VPN的IP地址对象，因为会冲突，所以需要把这些内容删除干净才可以顺利的部署向导模板，一般第一次部署不会遇到报错。

查看IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建地址对象和地址对象组

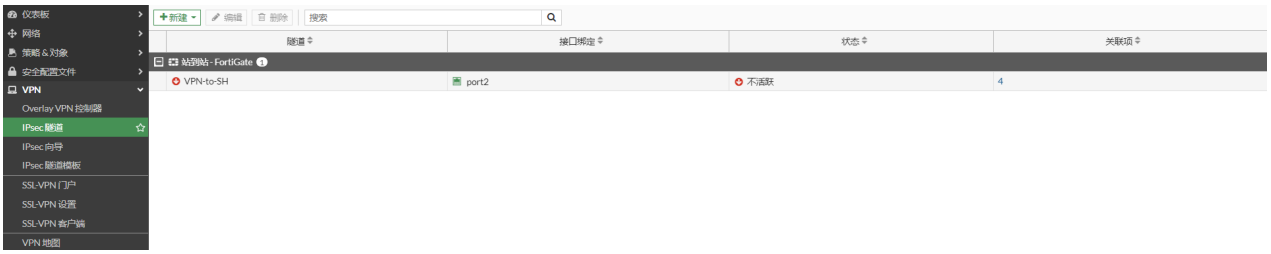


2. 创建PKI用户

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config user peer
    edit "VPN-to-SH_peer"
        set ca "CA_Cert_1"
    next
end
```

3. 创建IPSEC隧道



对应的命令行如下：

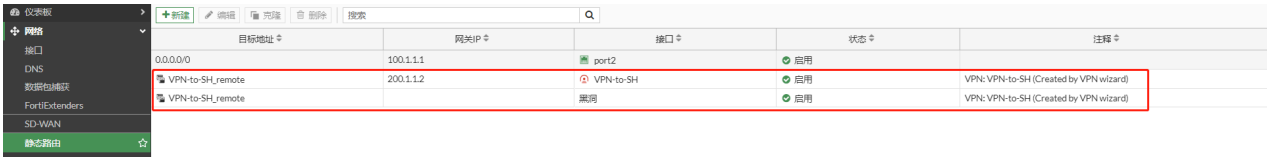
```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set interface "port2"
        set authmethod signature
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: VPN-to-SH (Created by VPN wizard)"
        set wizard-type static-fortigate
        set remote-gw 200.1.1.2
        set certificate "FGTBJ"
        set peer "VPN-to-SH_peer"
    next
end
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set phase1name "VPN-to-SH"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: VPN-to-SH (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN-to-SH_local"
        set dst-name "VPN-to-SH_remote"
    next
end
```

4. 创建路由

这里到对端的子网创建了两条路由：一条下一跳是VPN-to-SH接口的路由，一条黑洞路由。

> **重要**
>
> IPsec VPN隧道的路由下一跳只是一个隧道ID标识，并不是真正的路由下一跳IP，这和我们普通的路由下一跳不同，如这里的200.1.1.2是隧道的ID。

黑洞路由的目的：VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量会因为查询到了默认路由而走向了port2（Internet），从而产生了不期望的会话，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，业务流量会匹配不期望的会话而走向port2，从而引起该业务异常。因此有了这条黑洞路由就不会产生这条不期望的会话。



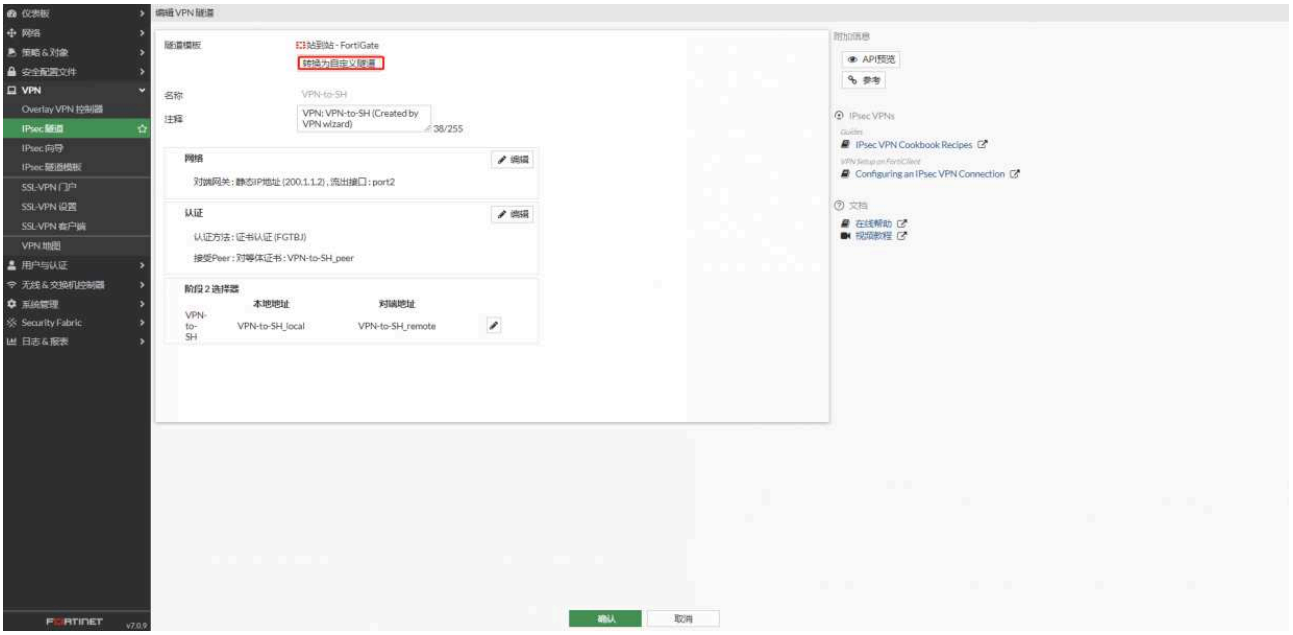
5. 创建策略

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



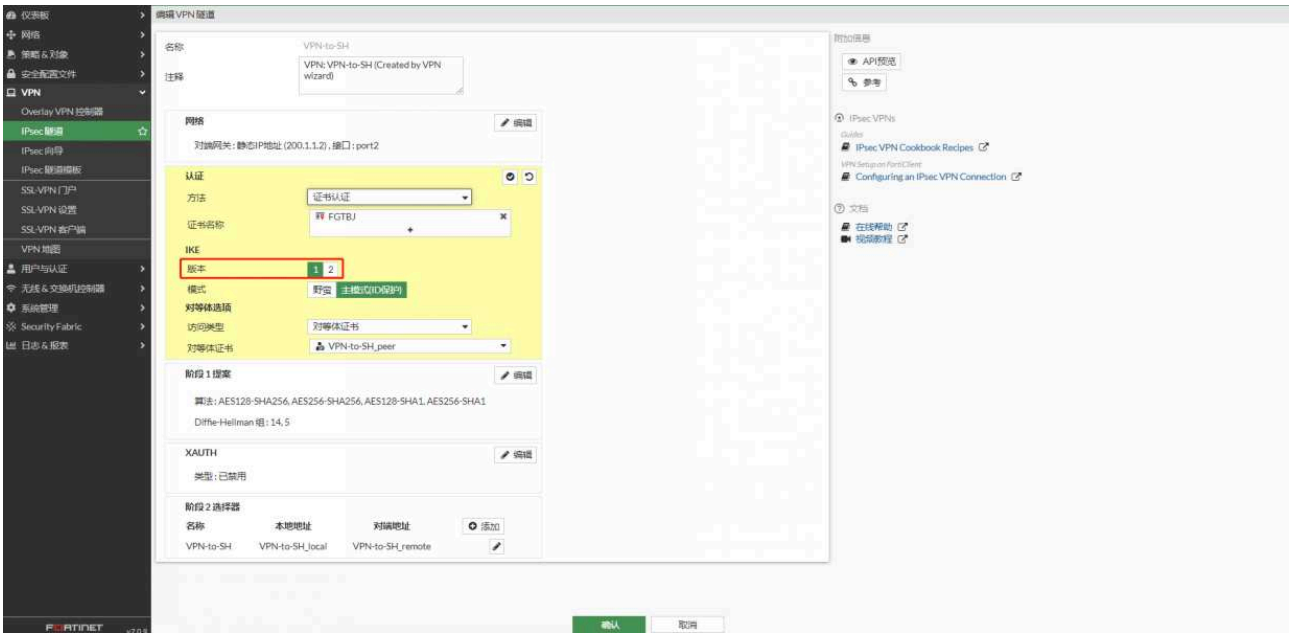
修改IPSEC VPN配置

编辑VPN隧道如下图



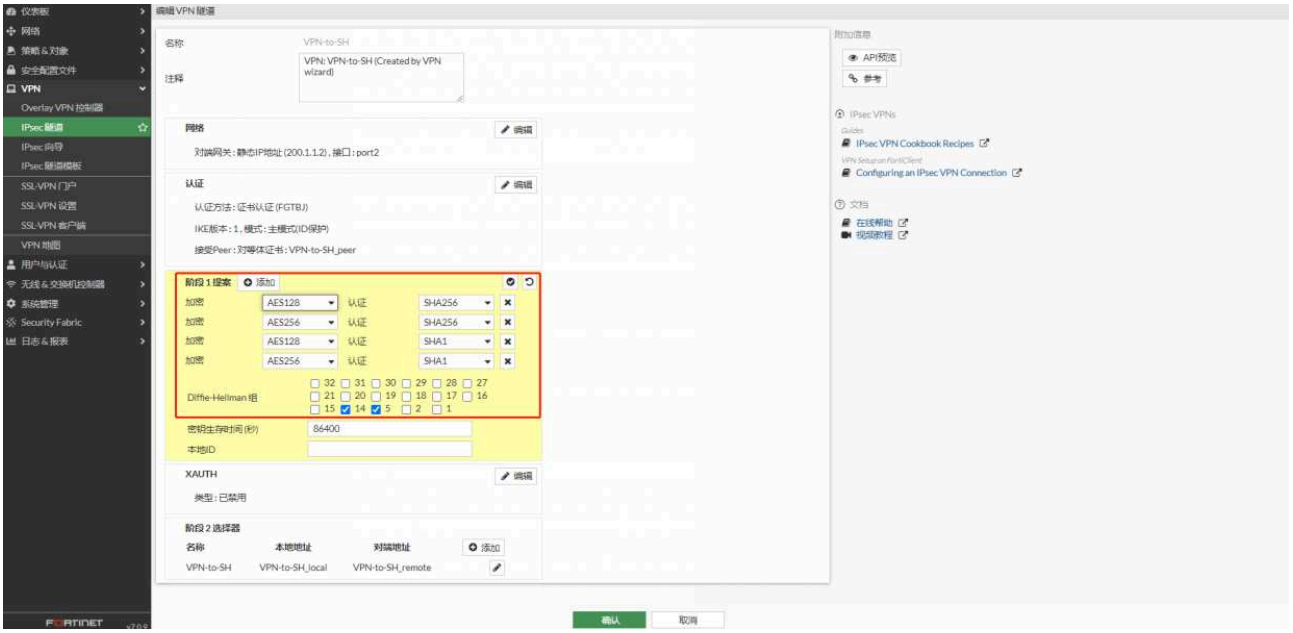
通过点击“转换为自定义隧道”可以在GUI界面设置的更多，是否需要修改可以根据实际网络需求决定。

如IKE版本（默认使用IKEv1）



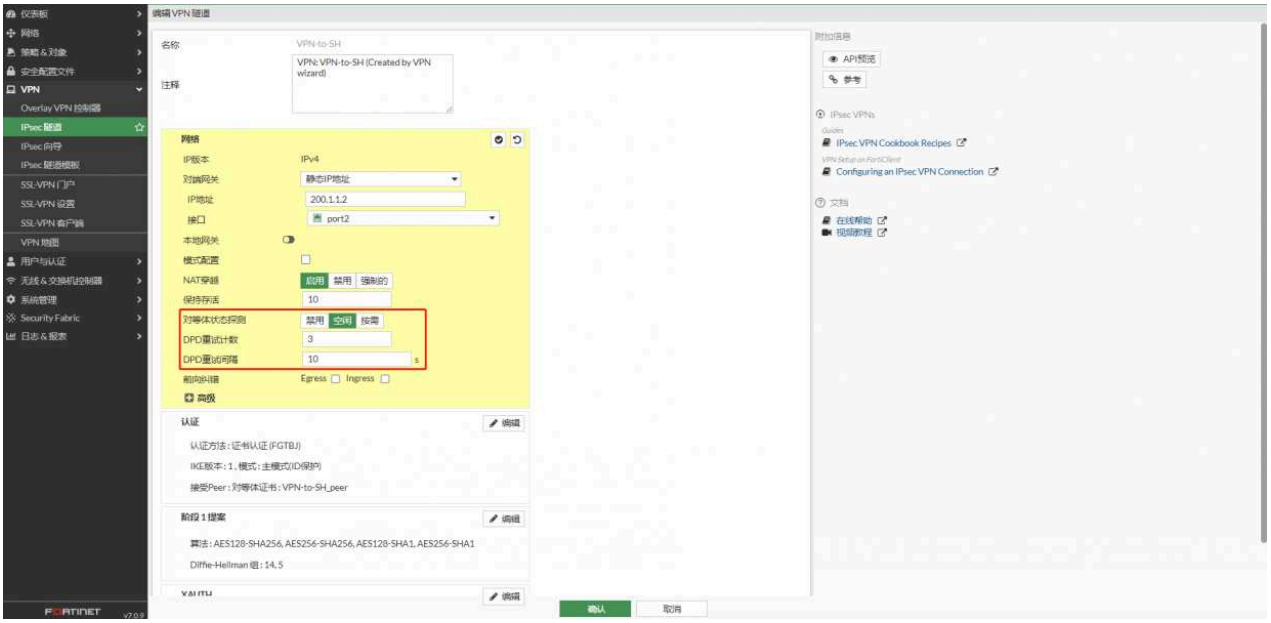
如修改阶段一加密和HASH算法

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



针对向导配置的优化建议

1. 在第一阶段中配置DPD模式为“空闲”（on-idle）（IPSec隧道内没有流量时发DPD探测，只有当IPSec隧道内双向有流量时，才不发DPD探测），实现快速的检测并切换VPN隧道的目的。



对应的命令行

```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

2. 开启自动协商，主动让隧道UP起来，而非使用VPN业务的时候再去触发VPN的协商，这样可以减少业务的丢包。在VPN主动发起方开启即可。

   IPSEC VPN阶段一自动协商是默认开启的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

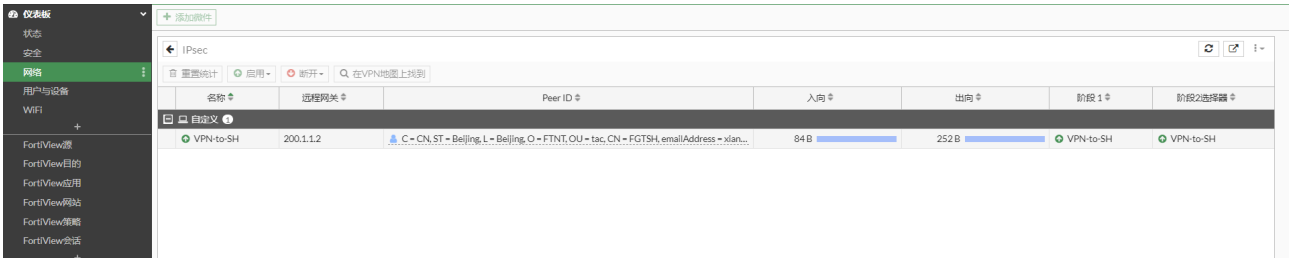
```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

IPSEC VPN阶段二自动协商默认关闭，需要开启。

```
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

查看IPSEC状态

GUI查看IPSEC状态



CLI查看IPSEC状态

```
# diagnose vpn ike gateway list

vd: root/0
name: VPN-to-SH
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 200.1.1.2/::200.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 95s ago
peer-id: C = CN, ST = Beijing, L = Beijing, O = FTNT, OU = tac, CN = FGTSH, emailAddress = xxxxxx@fortinet.com
peer-id-auth: yes
IKE SA: created 2/2  established 2/2  time 0/10500/21000 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 261 36a40a780f6e5a26/5c8a58382858d1c5
  direction: responder
  status: established 81-81s ago = 0ms
  proposal: aes128-sha256
  key: 4d17bfee50a67591-97e10ab6c738e5c1
  lifetime/rekey: 86400/86048
  DPD sent/recv: 00000000/00000000
  peer-id: C = CN, ST = Beijing, L = Beijing, O = FTNT, OU = tac, CN = FGTSH, emailAddress = xxxxxx@fortinet.com

  id/spi: 259 6fdf66aa8c4d7016/d499a5bf9b7784e0
  direction: initiator
  status: established 95-74s ago = 21000ms
  proposal: aes128-sha256
  key: fb35b9a59b37285f-0f48bef12a92b99a
  lifetime/rekey: 86400/86025
  DPD sent/recv: 00000008/00000000
  peer-id: C = CN, ST = Beijing, L = Beijing, O = FTNT, OU = tac, CN = FGTSH, emailAddress = xxxxxx@fortinet.com

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-SH ver=1 serial=4 100.1.1.2:0→200.1.1.2:0 tun_id=200.1.1.2 tun_id6=::200.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=4 olast=4 ad=/0
stat: rxp=1 txp=3 rxb=84 txb=252
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=8
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-SH proto=0 sa=1 ref=3 serial=1
  src: 0:192.168.0.0-192.168.0.255:0
  dst: 0:192.168.1.0-192.168.1.255:0
  SA:  ref=6 options=10226 type=00 soft=0 mtu=1438 expire=42837/0B replaywin=2048
       seqno=4 esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=0e81b327 esp=aes key=16 71d5090574a275127b9127ecc28d36a7
       ah=sha1 key=20 6389a6da9137a9d1b26d272d3919f2d218e6c0ce
  enc: spi=58e500e2 esp=aes key=16 447dd0e3a482ed893fea4aa549597dc4
       ah=sha1 key=20 1895ccc38badbf93caa77c9cbae424f4bd26e483
  dec:pkts/bytes=2/168, enc:pkts/bytes=6/708
  npu_flag=03 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=a dec_npuid=1 enc_npuid=1
```

查看路由

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
S       192.168.1.0/24 [10/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]        <———到192.168.1.0/24走IPSEC VPN
```

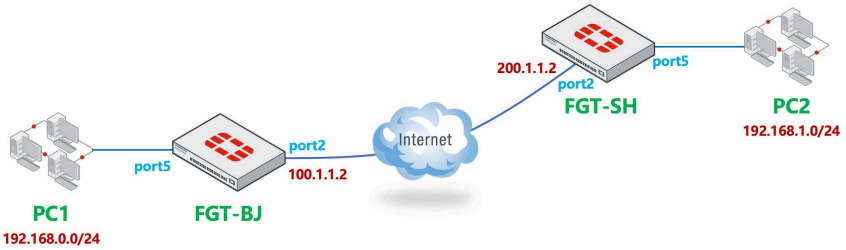

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

VPN隧道上运行OSPF或BGP

网络需求

通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信。FGT-BJ和FGT-SH通过OSPF或者BGP协议动态的学习到对方的路由。

网络拓扑

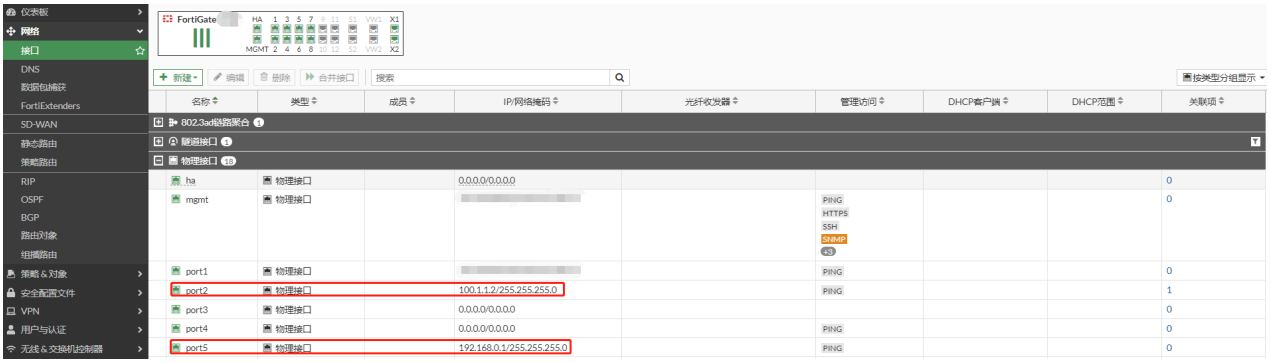


配置步骤

以FGT-BJ配置步骤为例，FGT-SH同理。

1. 基本配置

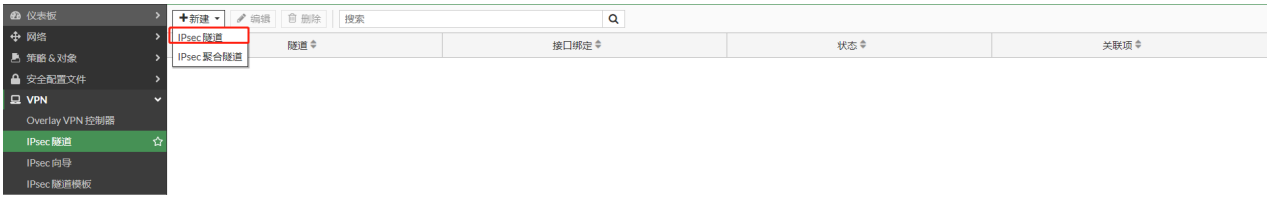
配置接口IP和路由





2. 配置IPSEC VPN

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



选择“自定义”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

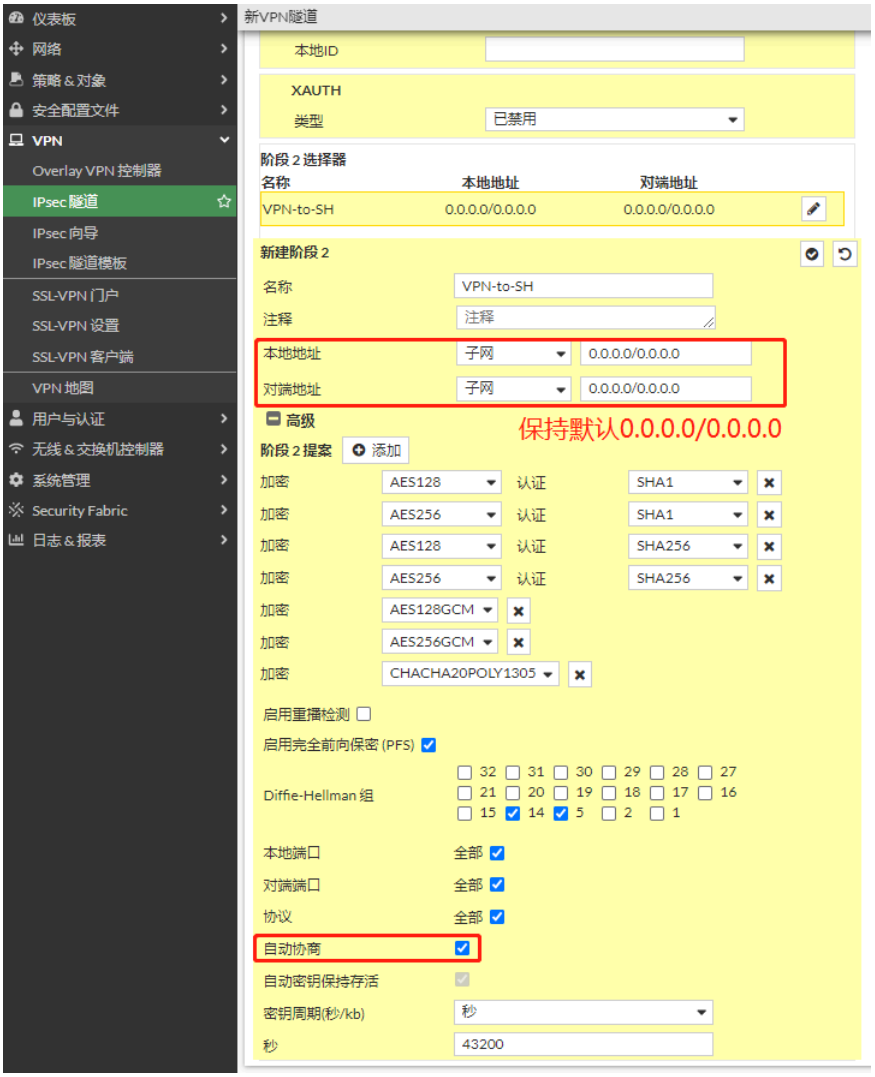


IPSEC VPN阶段一配置



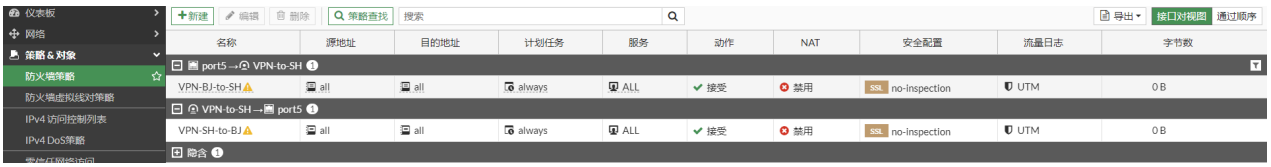
IPSEC VPN阶段二配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



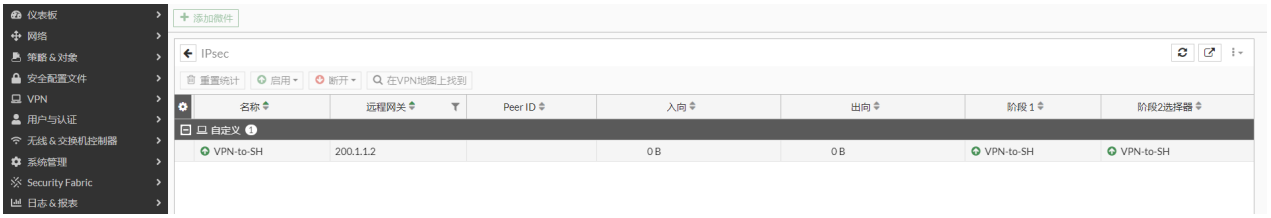


3. 配置IPSEC策略



4. 查看IPSEC状态

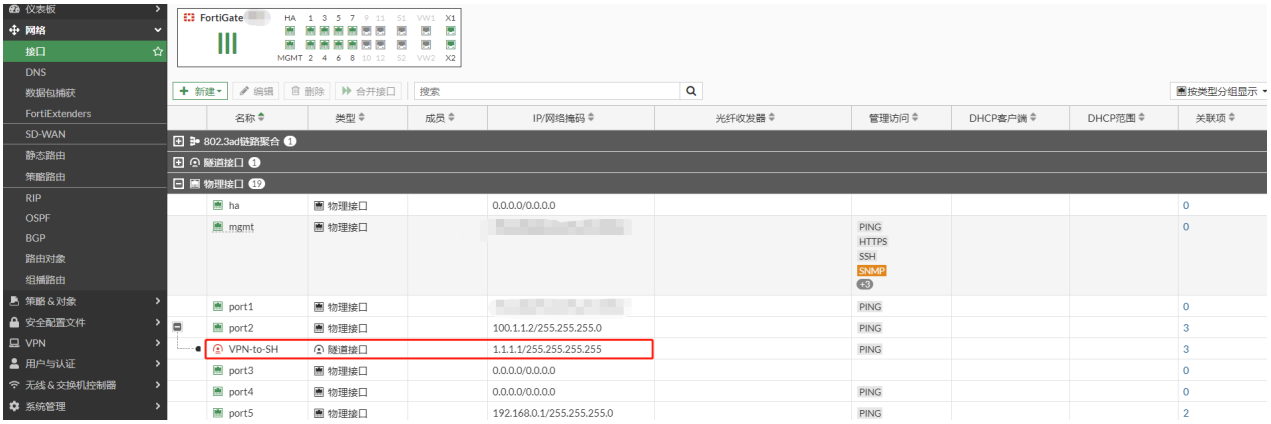
如果对端配置已配置完成，此时IPSEC状态是UP的。

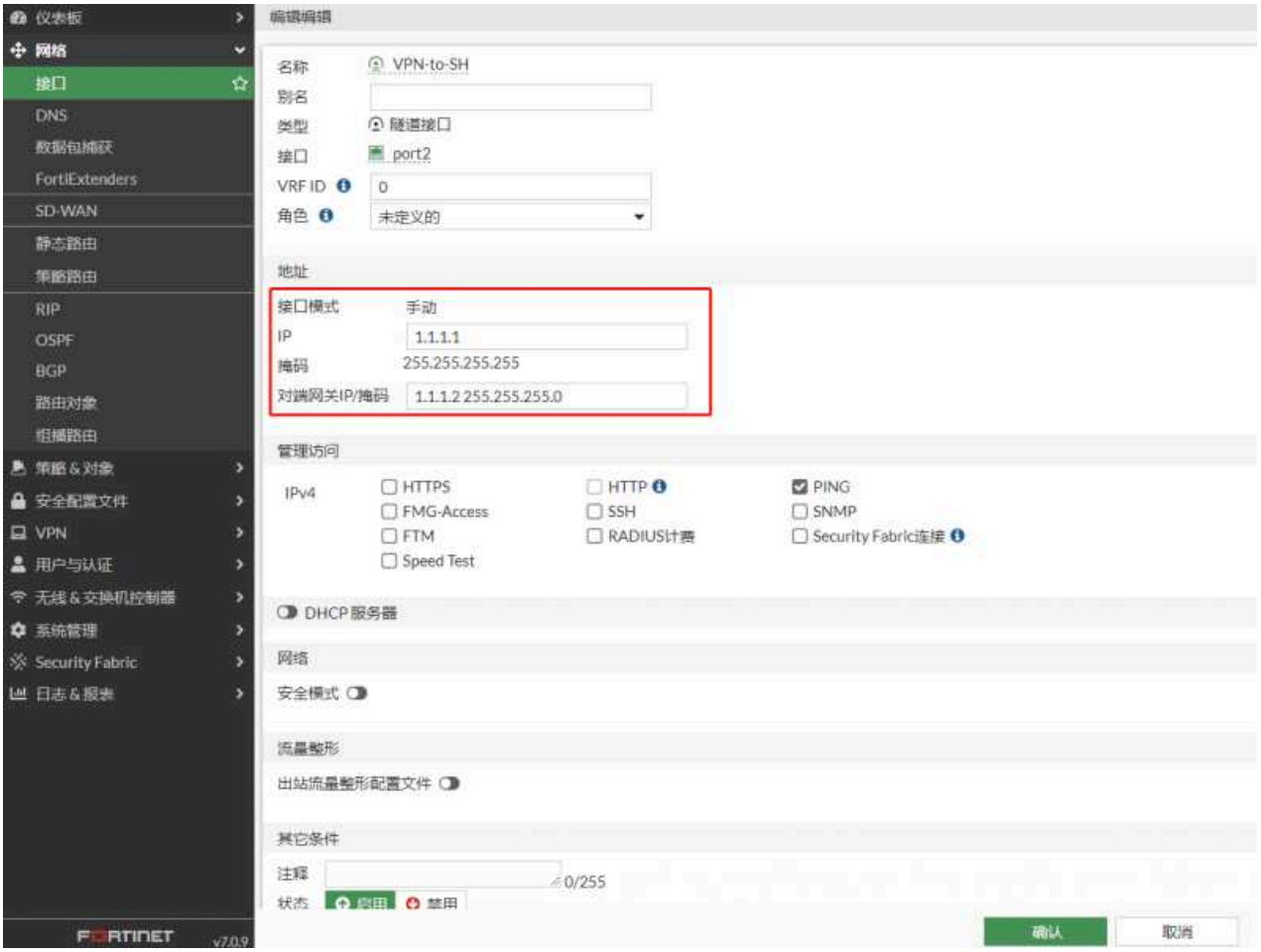


5. 配置IPSEC接口IP

为隧道接口分配IP用于动态路由协议

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





对应的命令行

```
config system interface
    edit "VPN-to-SH"
        set vdom "root"
        set ip 1.1.1.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 1.1.1.2 255.255.255.0
        set interface "port2"
    next
end
```

查看路由表

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

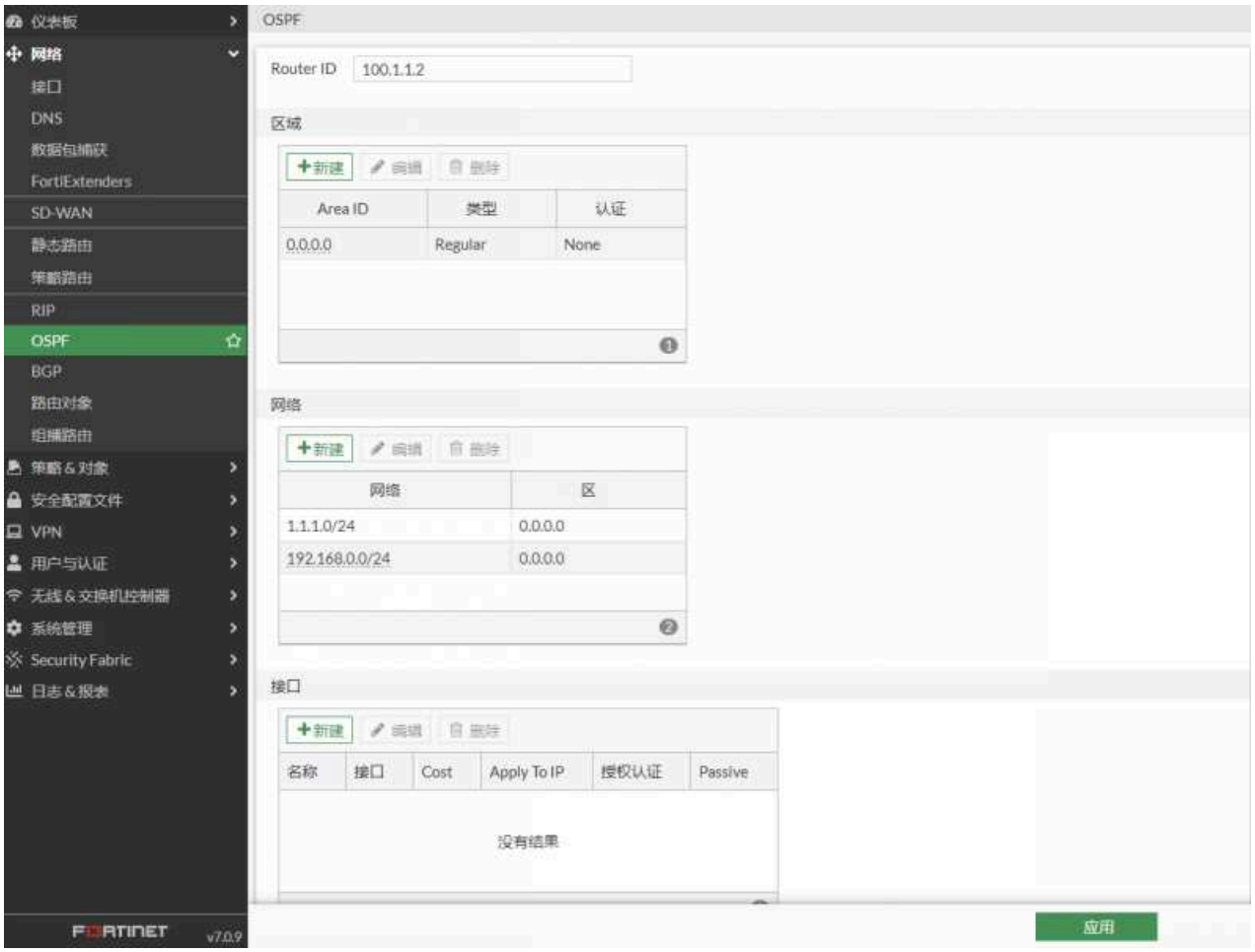
```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
S       1.1.1.0/24 [5/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]
C       1.1.1.1/32 is directly connected, VPN-to-SH
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
```

ping测试，能够正常ping通对端的IPSEC接口地址

```
# execute ping-options source 1.1.1.1
# execute ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
64 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=0.6 ms
64 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=0.5 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.6 ms
```

6. **使用OSPF或者BGP学习路由**

   配置OSPF

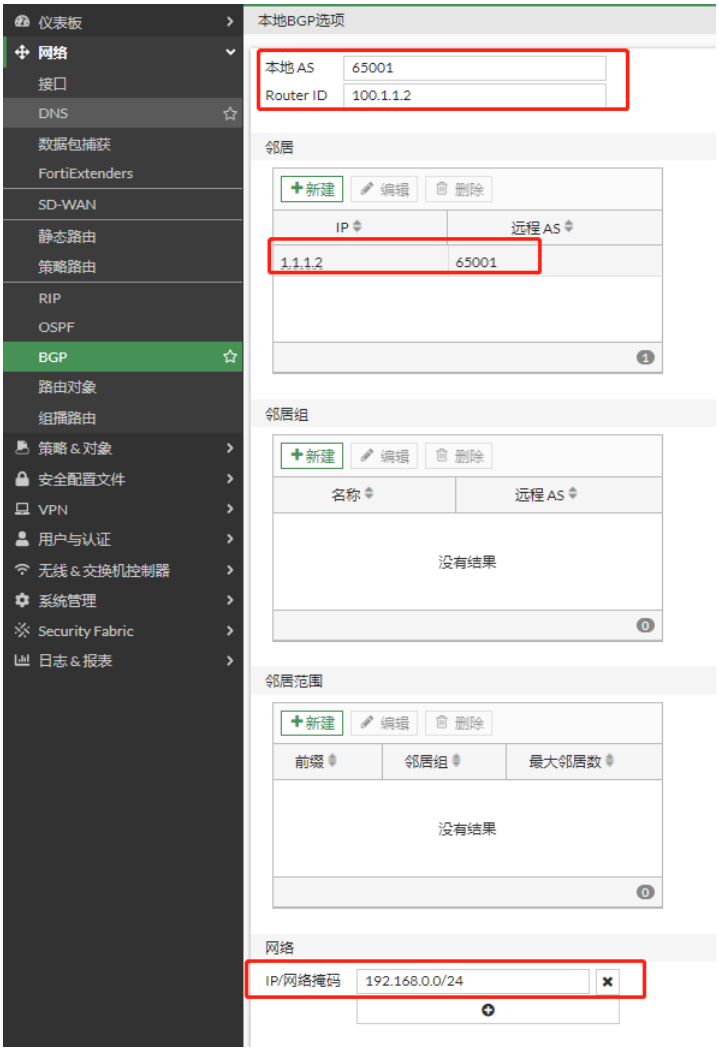


当对端也配置完成后，则可以建立OSPF邻居，并学习到对端的路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
200.1.1.2         1   Full/ -         00:00:39    1.1.1.2         VPN-to-SH(tun-id:200.1.1.2)

# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
S       1.1.1.0/24 [5/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]
C       1.1.1.1/32 is directly connected, VPN-to-SH
O       1.1.1.2/32 [110/100] via VPN-to-SH tunnel 200.1.1.2, 00:01:44
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
O       192.168.1.0/24 [110/101] via VPN-to-SH tunnel 200.1.1.2, 00:01:4
```

配置BGP



当对端也配置完成后，则可以建立BGP邻居，并学习到对端的路由。

```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 1.1.1.2, remote AS 65001, local AS 65001, internal link
  BGP version 4, remote router ID 200.1.1.2
  BGP state = Established, up for 00:08:37
  Last read 00:00:03, hold time is 180, keepalive interval is 60 seconds
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  Configured hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 12 messages, 0 notifications, 0 in queue
  Sent 12 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds
  Update source is VPN-to-SH
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Inbound soft reconfiguration allowed
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  0 accepted prefixes, 0 prefixes in rib
  1 announced prefixes
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes, 0 prefixes in rib
  0 announced prefixes
 Connections established 1; dropped 0
Local host: 1.1.1.1, Local port: 179
Foreign host: 1.1.1.2, Foreign port: 15455
Egress interface: 41
Nexthop: 1.1.1.1
Nexthop interface: VPN-to-SH
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

```

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
S       1.1.1.0/24 [5/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]
C       1.1.1.1/32 is directly connected, VPN-to-SH
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5

```

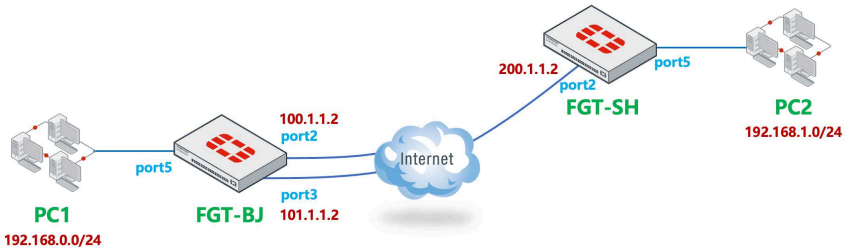

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

多路负载/主备IPSec VPN

网络需求

通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信，并实现多路负载或者主备切换。

网络拓扑



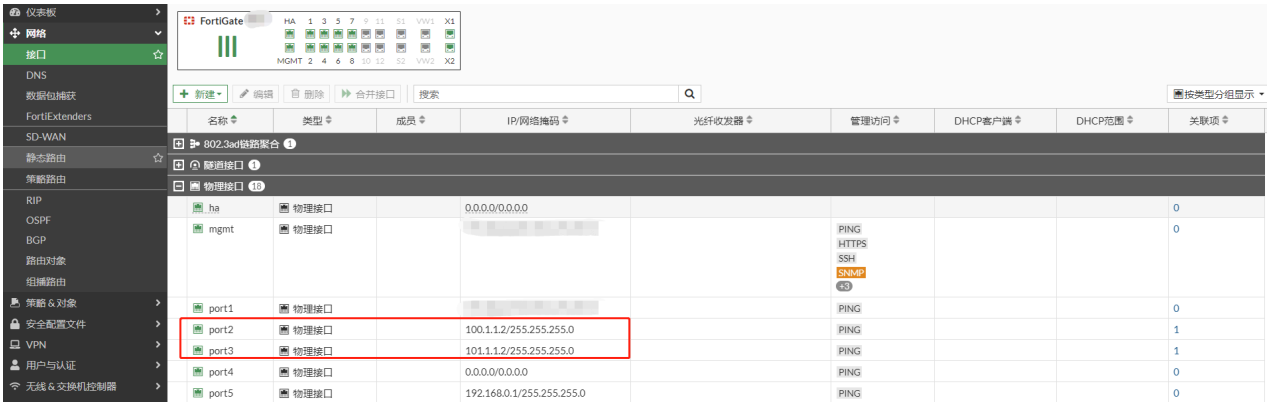
1. FGT-BJ port2和port3接口分别与FGT-SH port2 200.1.1.2建立两条IPSec VPN。
2. FGT-SH配置同理，FGT-SH使用port2接口分别与FGT-BJ 100.1.1.2和101.1.1.2建立两条IPSec VPN。

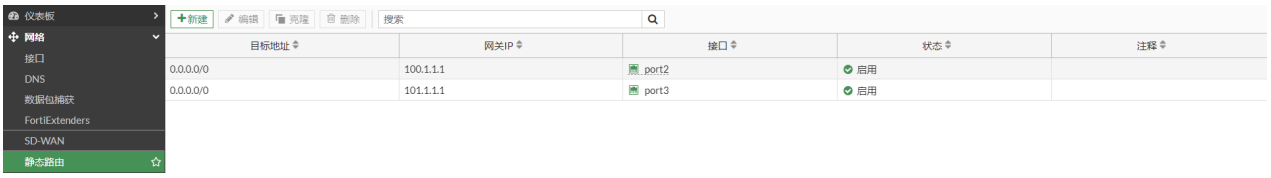
配置步骤

配置IPSec

1. **基本配置**

   配置接口IP和路由

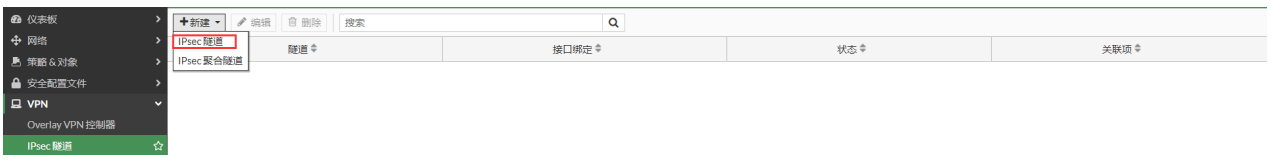




2. 配置IPSEC VPN

   FGT-BJ使用port2接口与FGT-SH port2 200.1.1.2建立IPSEC VPN

   选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



   根据“VPN创建向导”进行VPN模板配置，输入名称，拓扑中没有NAT，这里选择“站点之间没有NAT”，并点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



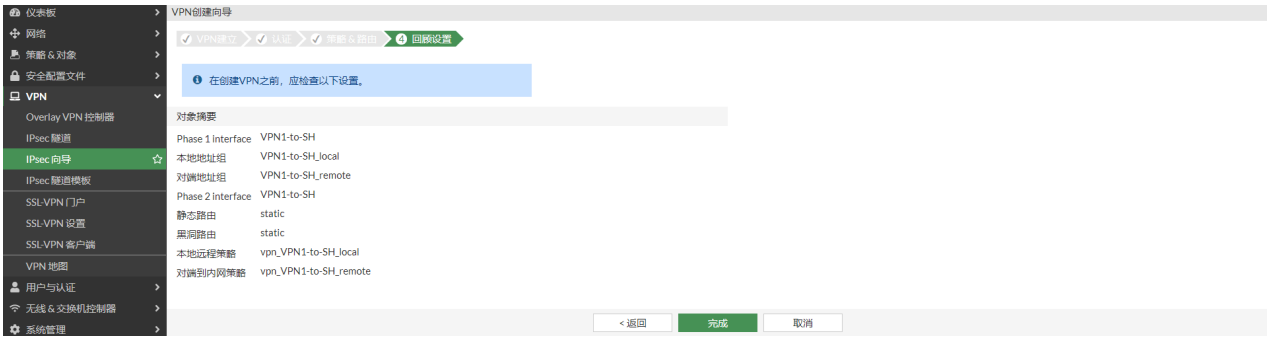
输入对端设备的IP地址（流出接口会根据路由自动选择），以及预共享秘钥。



选择“本地接口”，即需要被IPSEC保护的内网的接口，这里是port5接口，本地子网会自动写为该接口的IP所在的IP网段（如果被保护的是其他网段，可以根据实际网络需求修改），输入“远端子网”，即远端需要被保护的网络。然后点击“下一步”。



VPN创建向导提示即将创建的内容，然后点击完成。

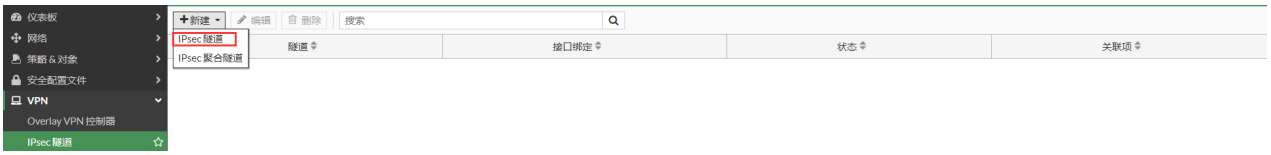


VPN创建成功。



FGT-BJ使用port3接口与FGT-SH port2 200.1.1.2建立IPSEC VPN

选择“VPN” --> “IPsec隧道”，点击“新建”，选择“IPsec隧道”。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

根据“VPN创建向导”进行VPN模板配置，输入名称，拓扑中没有NAT，这里选择“站点之间没有NAT”，并点击下一步。



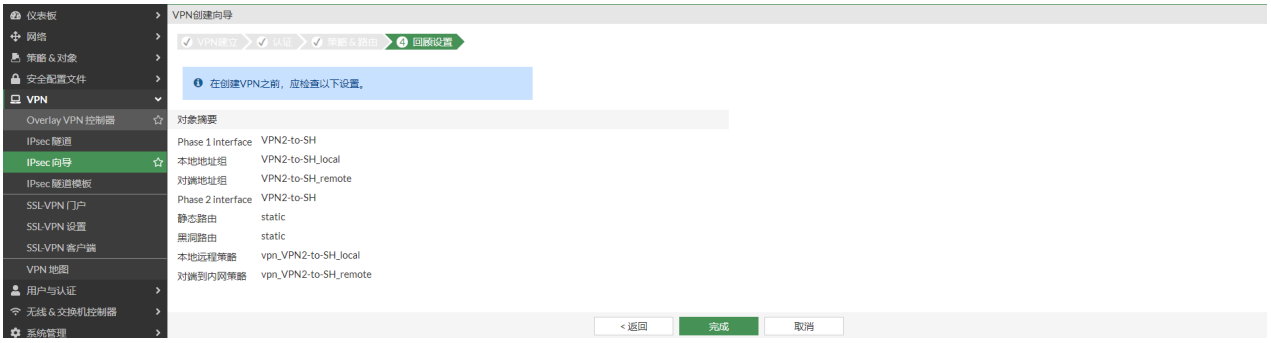
输入对端设备的IP地址（流出接口会根据路由自动选择），以及预共享秘钥。



选择“本地接口”，即需要被IPSEC保护的内网的接口，这里是port5接口，本地子网会自动写为该接口的IP所在的IP网段（如果被保护的是其他网段，可以根据实际网络需求修改），输入“远端子网”，即远端需要被保护的网络。然后点击“下一步”。



VPN创建向导提示即将创建的内容，然后点击完成。



VPN创建成功。



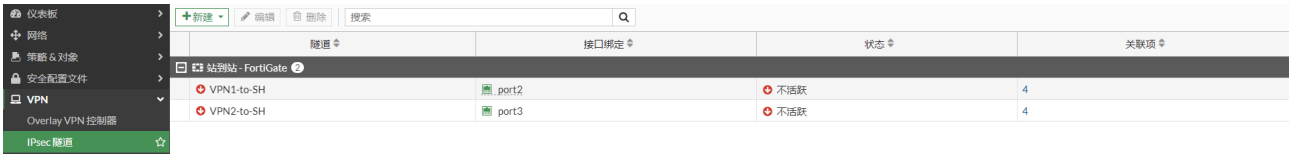
重要

如果最后完成模板部署的时候报错，那么需要注意，不要有旧的配置存在，比如相关VPN的策略、VPN的路由、VPN的IP地址对象，因为会冲突，所以需要把这些内容删除干净才可以顺利的部署向导模板，一般第一次部署不会遇到报错。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

查看IPSEC配置

已创建两条IPSEC VPN。

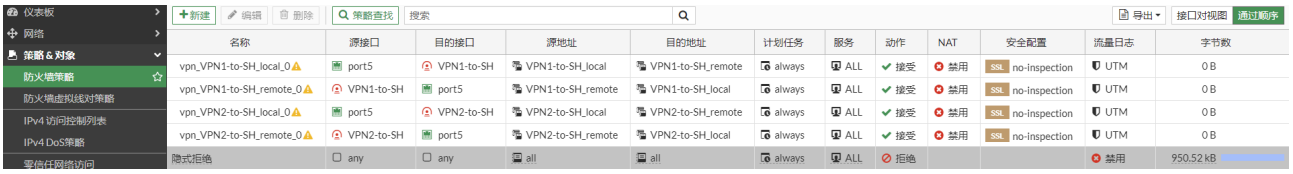


已创建IPSEC路由。

> **重要**
>
> IPsec VPN隧道的路由下一跳只是一个隧道ID标识，并不是真正的路由下一跳IP，这和我们普通的路由下一跳不同，如这里的200.1.1.2是隧道的ID；隧道ID通常是隧道的远程网关，对于具有相同远程网关的隧道，其他隧道id将随机分配（10.0.0.x），如第VPN2-to-SH隧道ID 10.0.0.1。

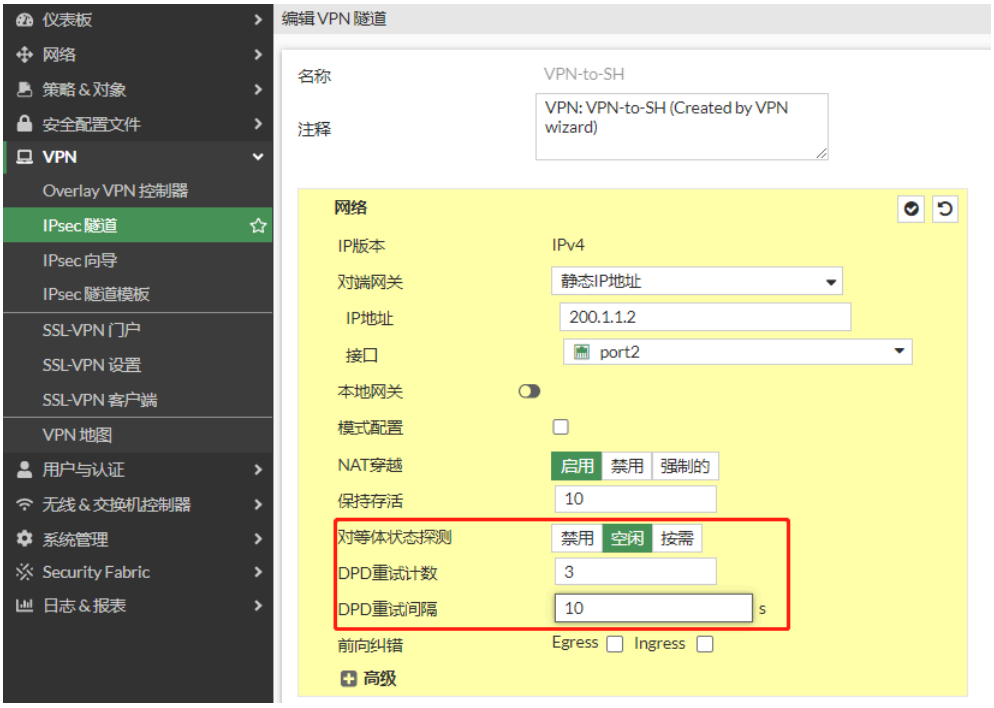


已创建防火墙策略。



针对向导配置的优化建议

1. 在第一阶段中配置DPD模式为“空闲”（on-idle）（IPSec隧道内没有流量时发DPD探测，只有当IPSec隧道内双向有流量时，才不发DPD探测），实现快速的检测并切换VPN隧道的目的。



对应的命令行

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN1-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
    edit "VPN2-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

2. 开启自动协商，主动让隧道UP起来，而非使用VPN业务的时候再去触发VPN的协商，这样可以减少业务的丢包。在VPN主动发起方开启即可。

IPSEC VPN阶段一自动协商是默认开启的。

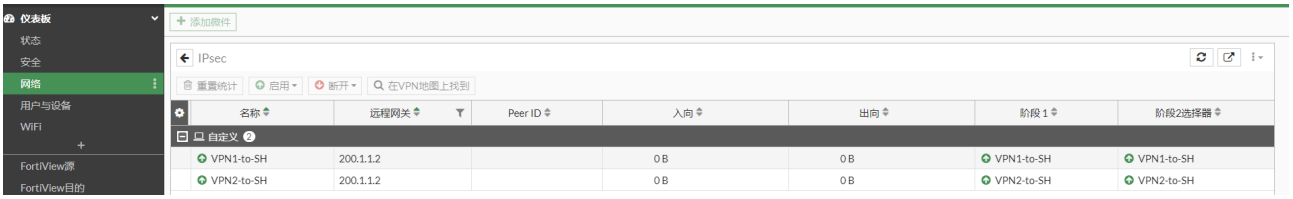
```
config vpn ipsec phase1-interface
    edit "VPN1-to-SH"
        set auto-negotiate enable
    next
    edit "VPN2-to-SH"
        set auto-negotiate enable
    next
end
```

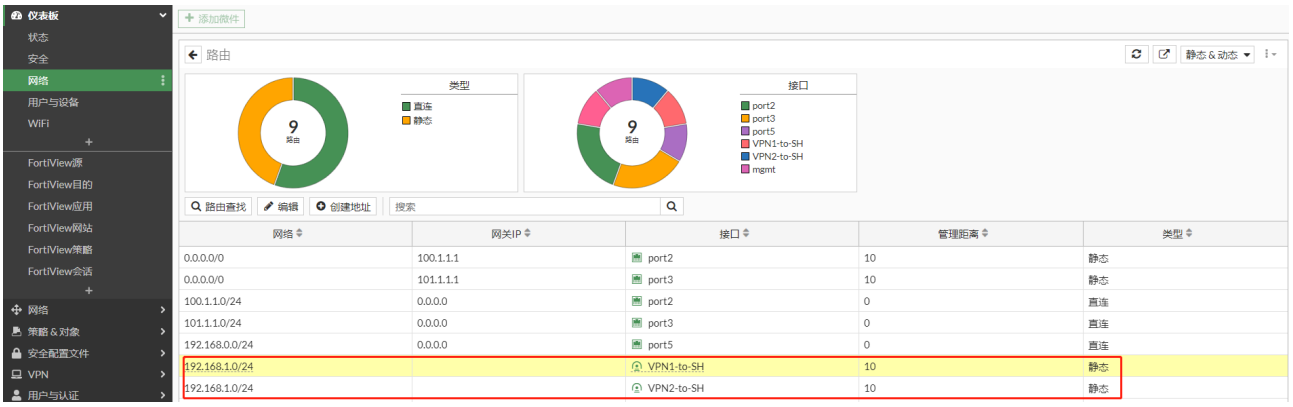
IPSEC VPN阶段二自动协商默认关闭，需要开启。

```
config vpn ipsec phase2-interface
    edit "VPN1-to-SH"
        set auto-negotiate enable
    next
    edit "VPN2-to-SH"
        set auto-negotiate enable
    next
end
```

多路负载IPSEC VPN

按照上述方式配置完成后，两条IPSEC VPN隧道的会UP起来，并且已通过静态路由实现负载均衡。





主备IPSEC VPN

有两种方法实现主备IPSEC VPN，这里VPN1-to-SH作为主，VPN2-to-SH作为备。

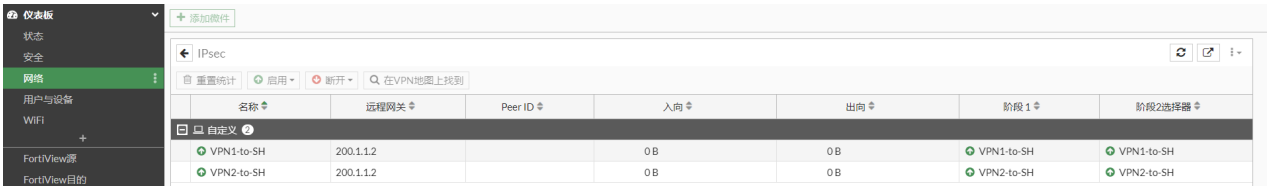
1. 使用路由的方法。通过静态路由的优先级控制IPSEC VPN主备。（动态路由也可以）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

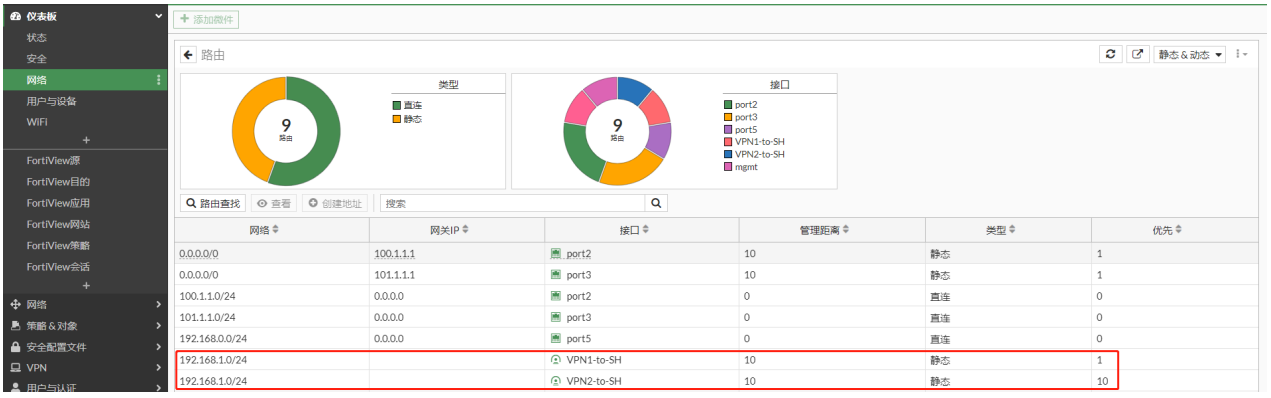
将VPN2-to-SH路由的优先级设置为10，默认是1，值越低优先级越高。



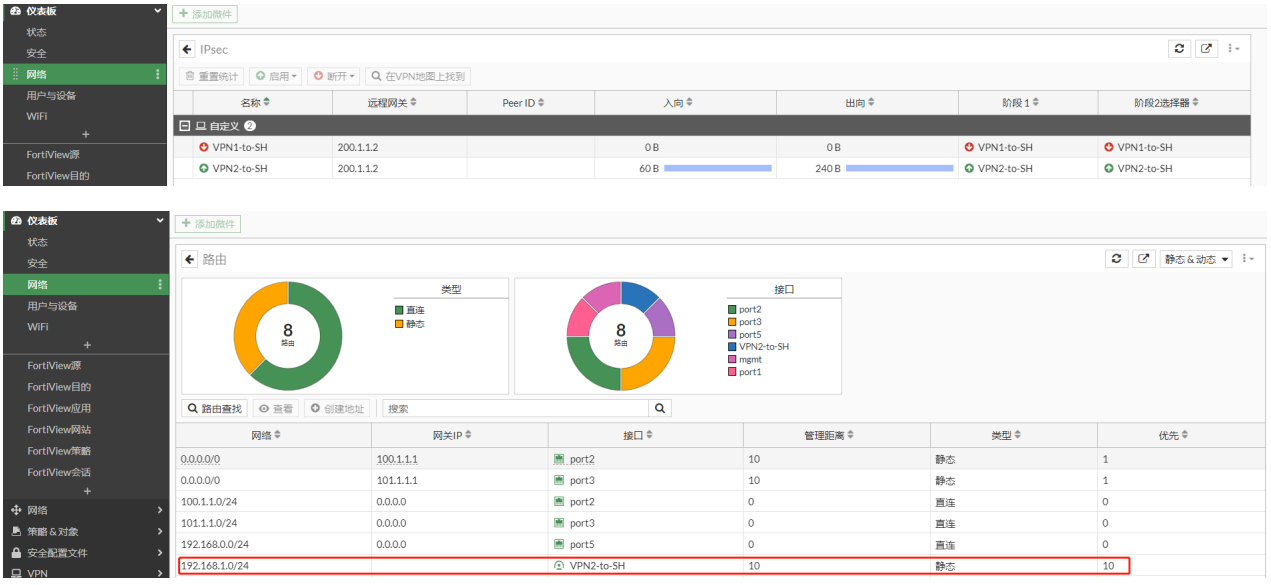
两条IPSEC VPN都能UP。



从路由表可以看出，VPN1-to-SH优先。



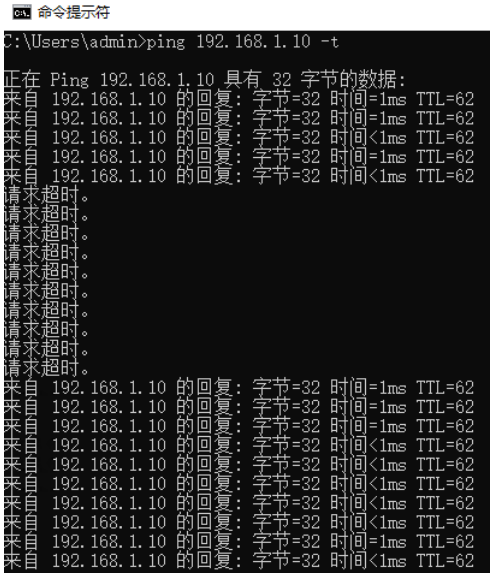
当VPN1-to-SH DOWN后，路由指向VPN2-to-SH。



当dpd设置重试次数为3，重试时间间隔为10s时，主备切换丢10个包。

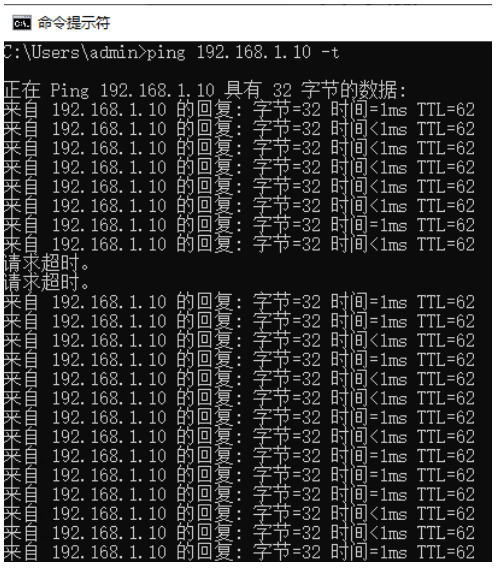
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN1-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```



当dpd设置重试次数为3，重试时间间隔为1s时，主备切换丢2个包。

```
config vpn ipsec phase1-interface
    edit "VPN1-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 1
    next
end
```



2. 使用IPSEC monitor的方法

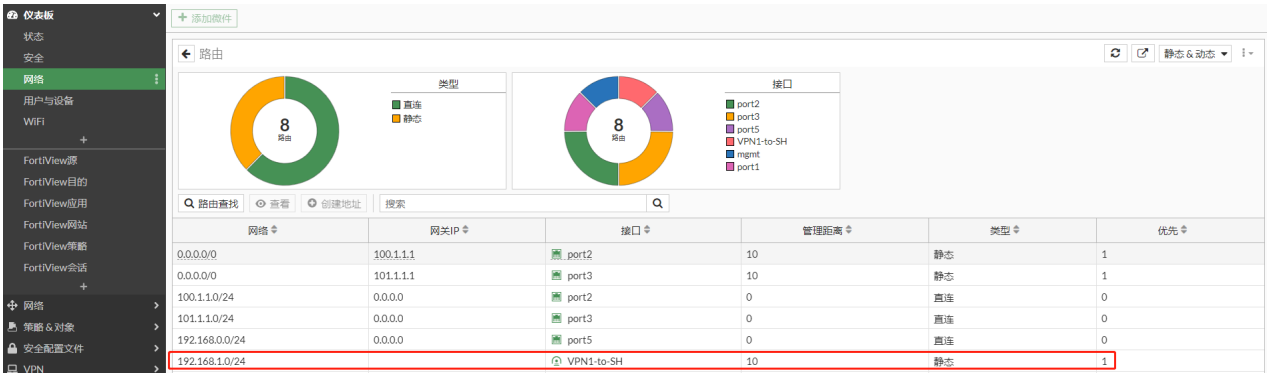
VPN1-to-SH作为主VPN UP起来，VPN2-to-SH作为备VPN则处于监听模式，一旦检测到主VPN隧道故障，则将备份的VPN协商起来，接替主VPN的工作。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN2-to-SH"
        set monitor "VPN1-to-SH"
    next
end
```

配置完成后，VPN1-to-SH是UP的，VPN2-to-SH是down的。





当port2的链路故障，VPN1-to-SH DOWN后，VPN2-to-SH会协商UP起来。



当dpd设置重试次数为3，重试时间间隔为10s时，主备切换丢10个包。

```
config vpn ipsec phase1-interface
    edit "VPN1-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

命令提示符

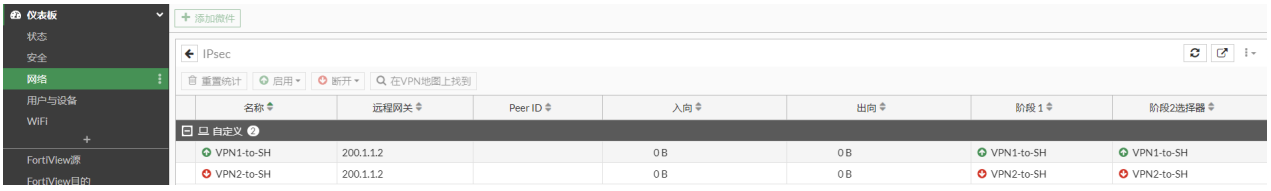
```
C:\Users\admin>ping 192.168.1.10 -t

正在 Ping 192.168.1.10 具有 32 字节的数据:
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
```

当dpd设置重试次数为3，重试时间间隔为1s时，主备切换丢2个包。

```
config vpn ipsec phase1-interface
    edit "VPN1-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 1
    next
end
```

```
C:\Users\admin>ping 192.168.1.10 -t

正在 Ping 192.168.1.10 具有 32 字节的数据:
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
请求超时。
请求超时。
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间<1ms TTL=62
来自 192.168.1.10 的回复: 字节=32 时间=1ms TTL=62
```

当port2的链路恢复后，VPN1-to-SH会抢回来，VPN1-to-SH协商UP起来，VPN2-to-SH DOWN。



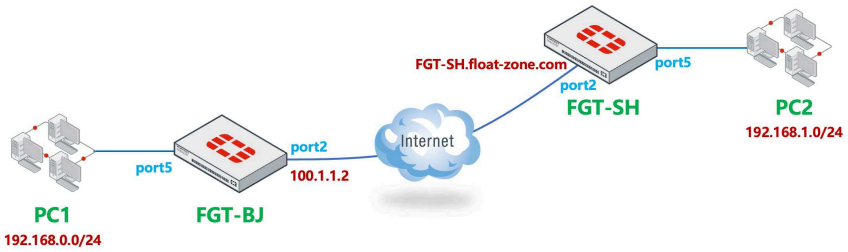
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGuard DDNS方式建立IPSec VPN

网络需求

FGT-BJ port2为静态固定IP地址，FGT-SH port2为PPPOE/DHCP动态拨号获取的IP地址，需要通过IPsec VPN将两个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信。

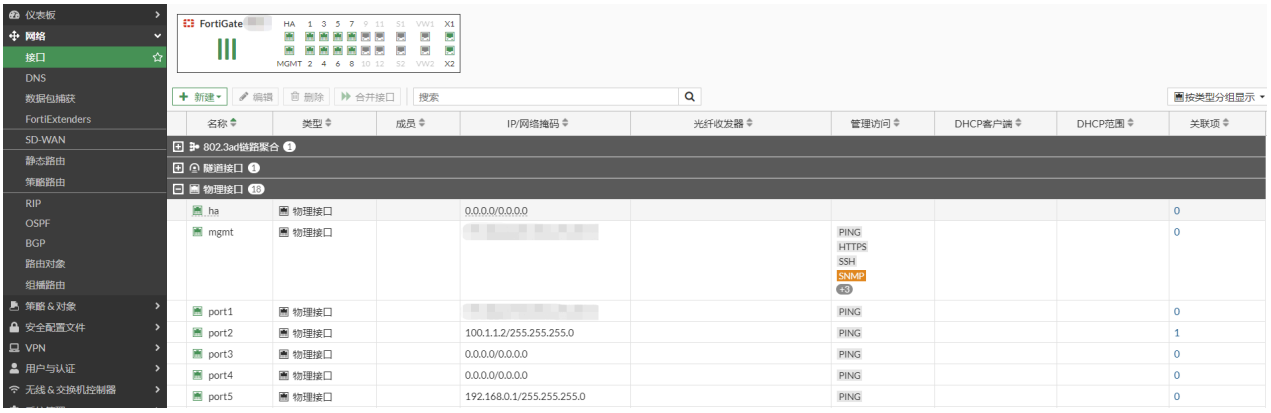
网络拓扑



配置步骤

FGT-BJ配置

1. 基本配置





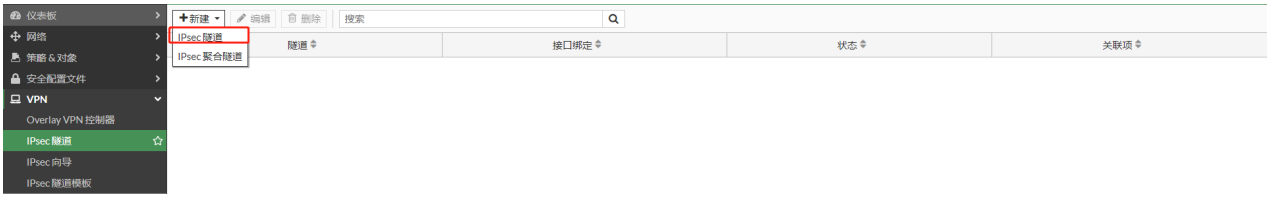
2. 配置IPSEC VPN

FGT-BJ使用域名FGT-SH.float-zone.com与对端发起连接，在配置IPSEC VPN前，先从FGT-BJ上测试是否能解析该域名。

```
# execute ping FGT-SH.float-zone.com
PING FGT-SH.float-zone.com (200.1.1.2): 56 data bytes
64 bytes from 200.1.1.2: icmp_seq=0 ttl=254 time=0.4 ms
64 bytes from 200.1.1.2: icmp_seq=1 ttl=254 time=0.3 ms
64 bytes from 200.1.1.2: icmp_seq=2 ttl=254 time=0.6 ms
64 bytes from 200.1.1.2: icmp_seq=3 ttl=254 time=0.4 ms
64 bytes from 200.1.1.2: icmp_seq=4 ttl=254 time=0.5 ms

--- FGT-SH.float-zone.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.4/0.6 ms
```

选择“VPN” --> “IPsec隧道”，点击“新建”，选择“IPsec隧道”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



选择“自定义”

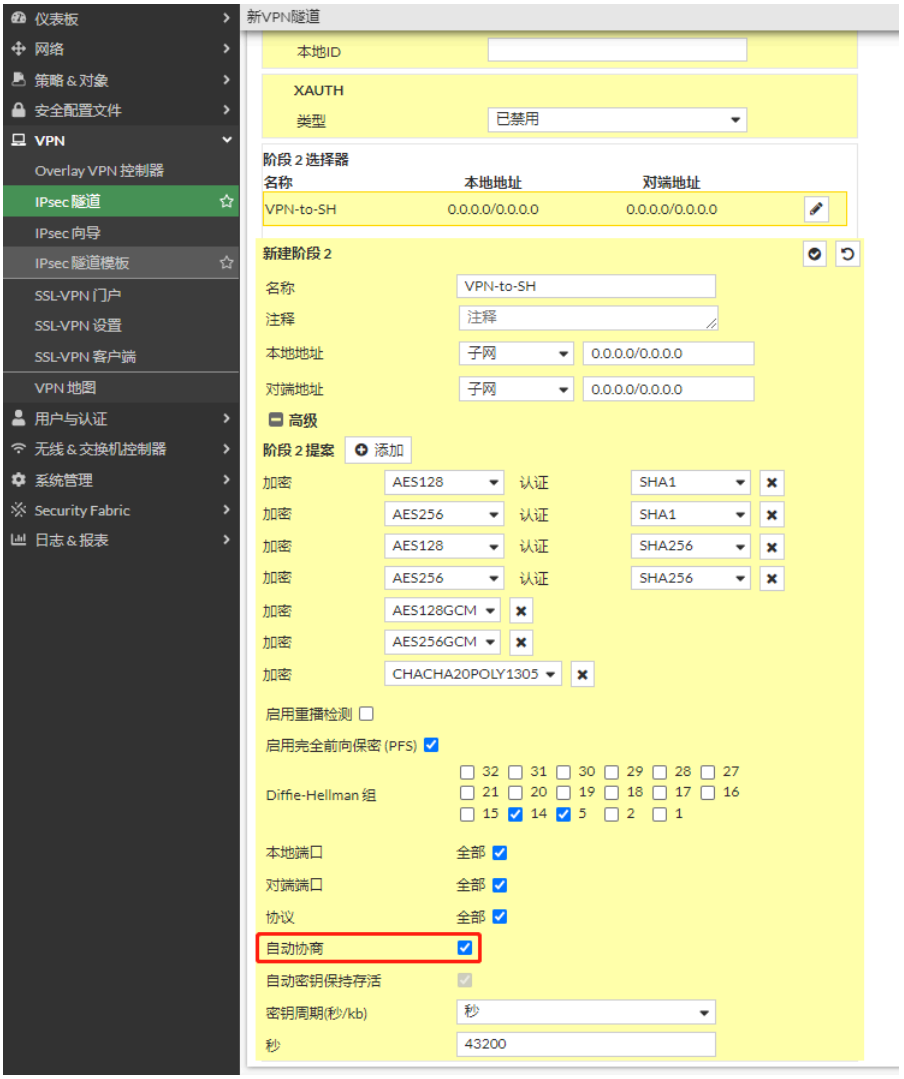


IPSEC VPN阶段一配置



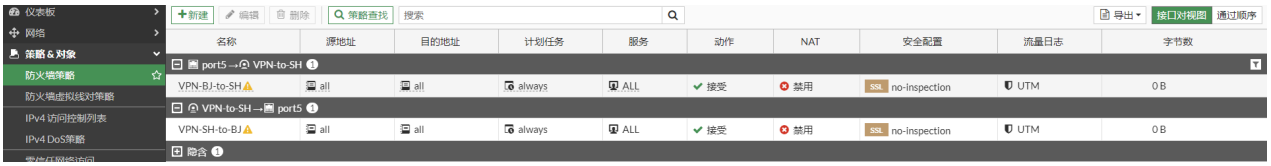
IPSEC VPN阶段二配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

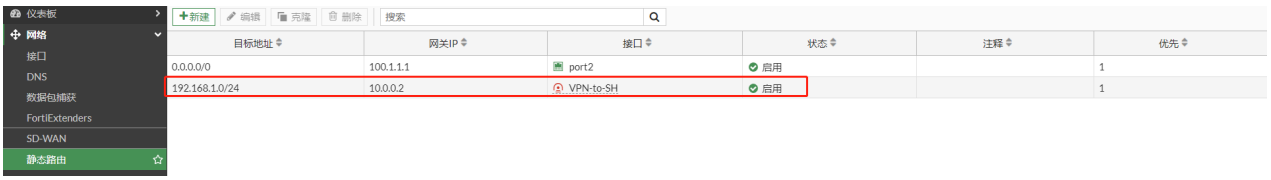




3. 配置IPSEC策略



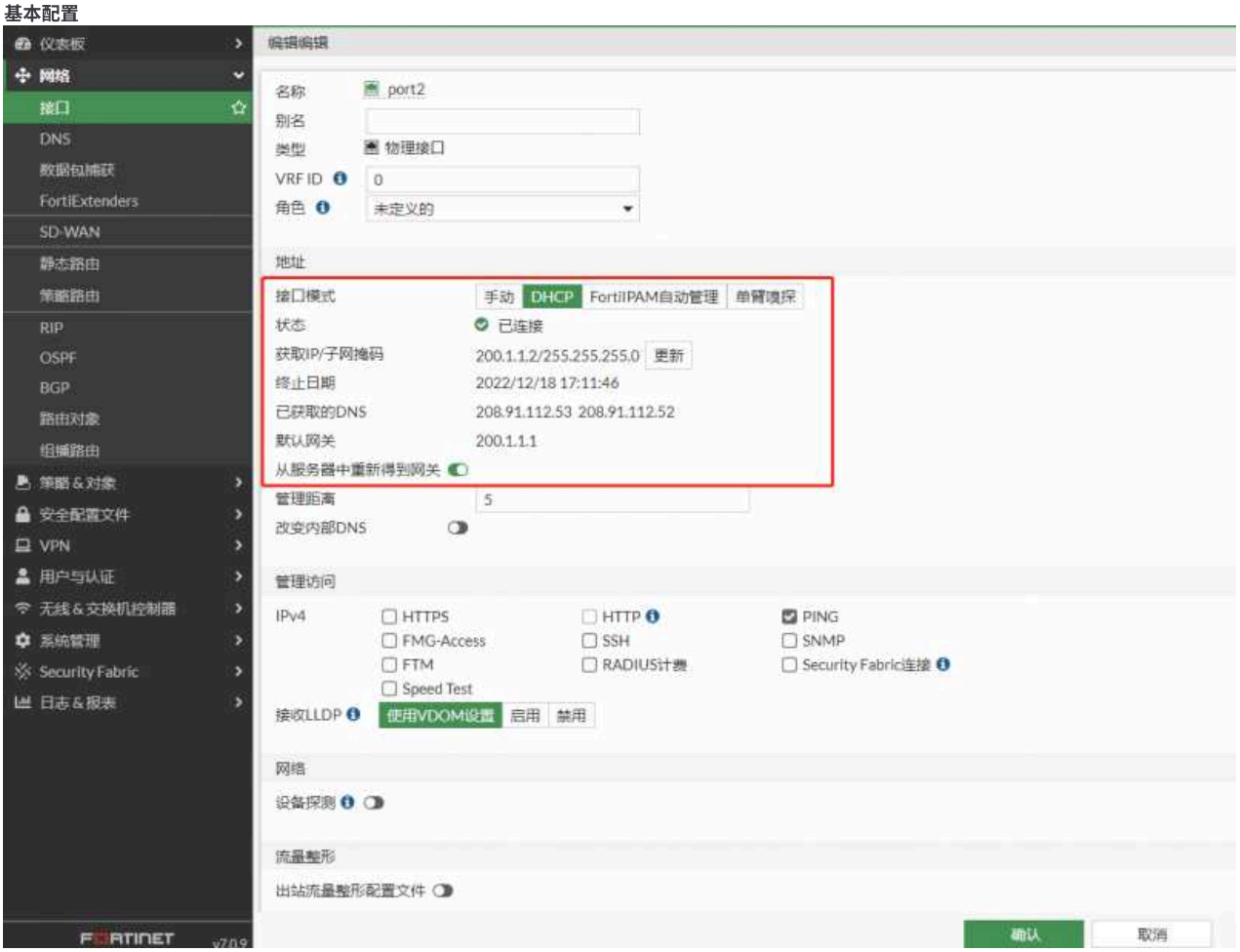
4. 配置路由

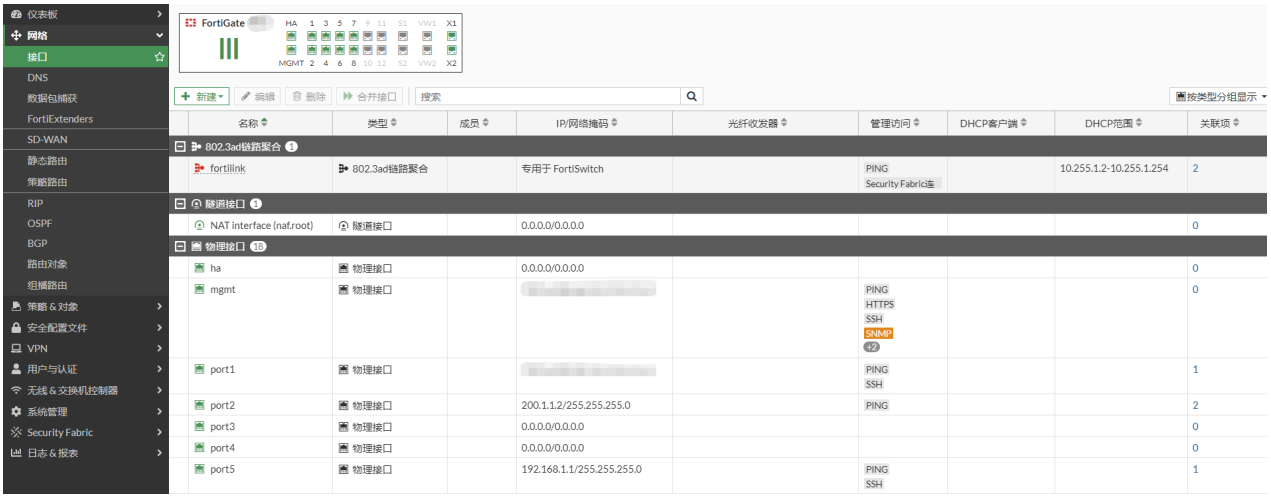


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FGT-SH配置

1. 基本配置

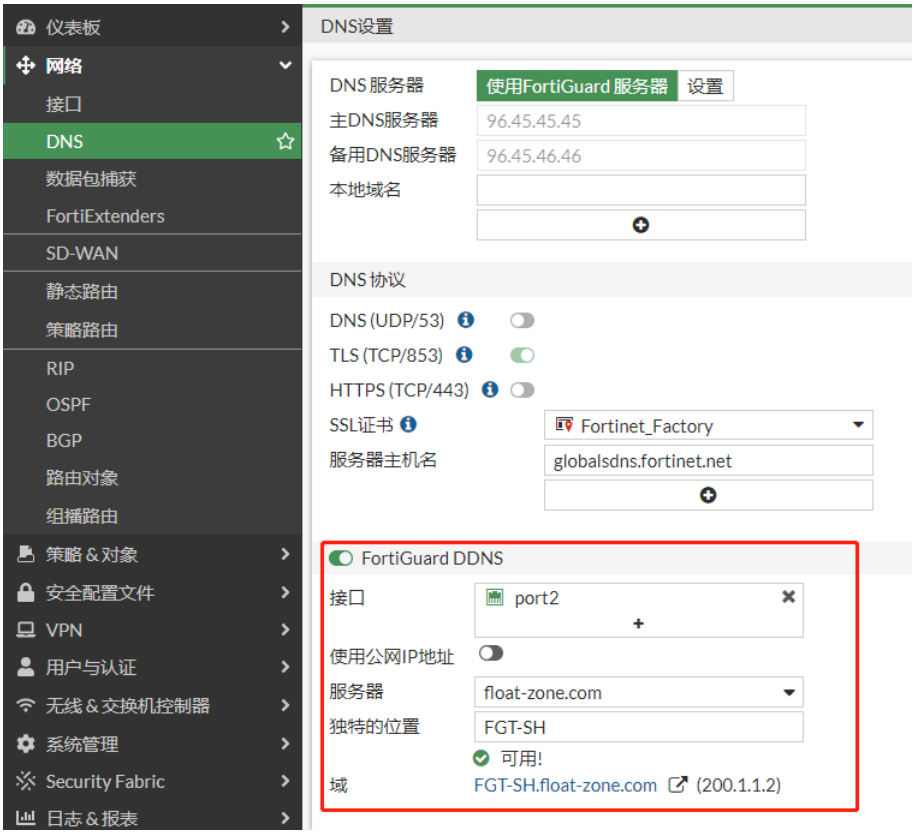




2. 配置FortiGuard DDNS

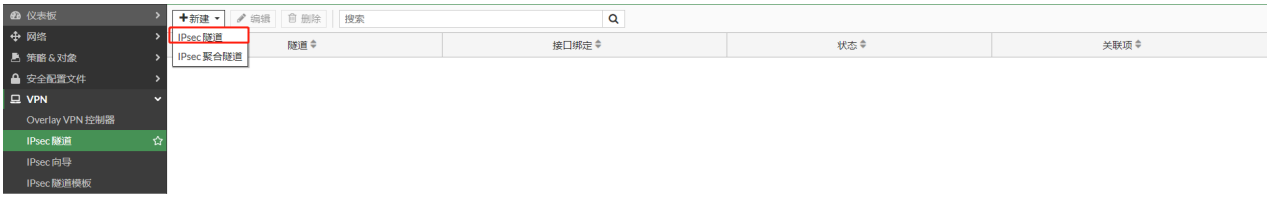
FGT-SH port2接口使用DHCP获取地址，地址是会变化的，但建立IPSEC VPN时，对端需要一个固定的地址，因此使用域名替代port2接口的IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. **配置IPSEC VPN**

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



这里依然使用自定义



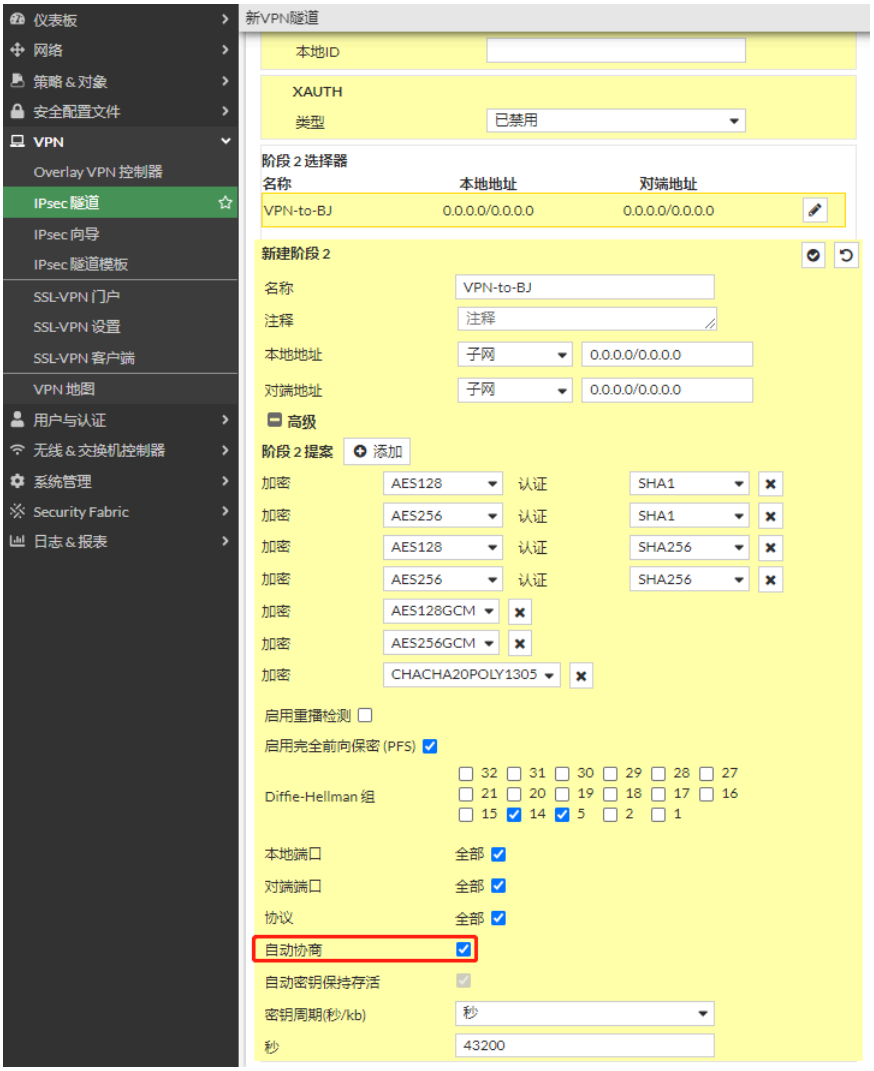
IPSEC VPN阶段一配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



IPSEC VPN阶段二配置

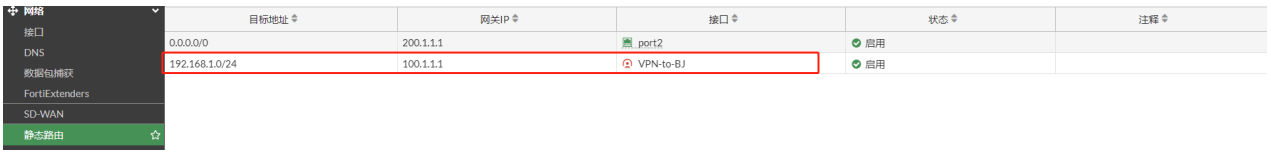
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置防火墙策略

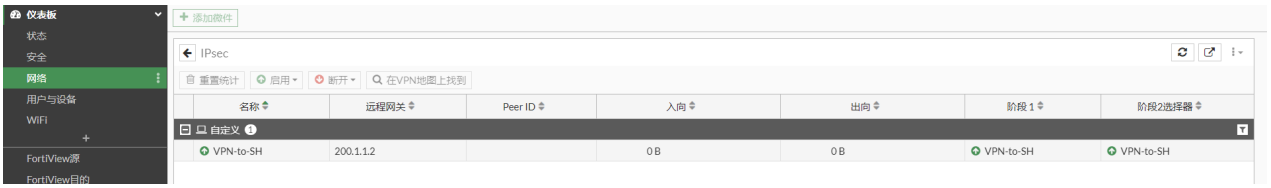


5. 配置路由



查看IPSEC VPN状态

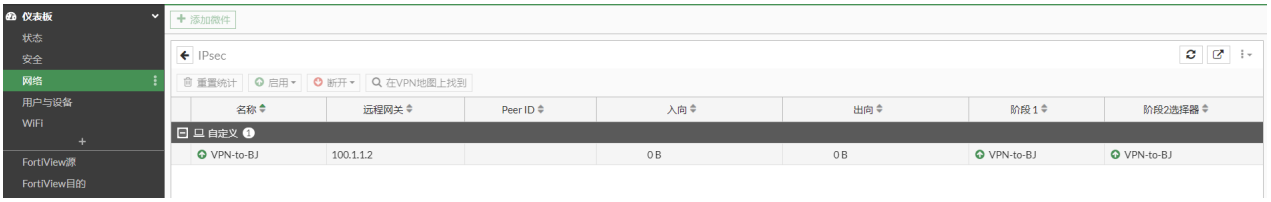
1. FGT-BJ IPSEC VPN状态



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# diagnose vpn ike gateway list

vd: root/0
name: VPN-to-SH
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 10.0.0.2/::10.0.0.2
remote_location: 0.0.0.0
network-id: 0
created: 195s ago
IKE SA: created 2/2  established 2/2  time 0/10500/21000 ms
IPsec SA: created 1/2  established 1/1  time 0/0/0 ms

  id/spi: 10 e3498ed0f017b22b/a19990e821f3733e
  direction: responder
  status: established 177-177s ago = 0ms
  proposal: aes128-sha256
  key: c9c4dd7d0bdea34b-e9425ad0fe0a17bc
  lifetime/rekey: 86400/85952
  DPD sent/recv: 00000000/00000000

  id/spi: 9 d46c45f0f50d9ce8/fcaf35fab405c65a
  direction: initiator
  status: established 195-174s ago = 21000ms
  proposal: aes128-sha256
  key: 27f09a3f144bf8da-85d9c19874786059
  lifetime/rekey: 86400/85925
  DPD sent/recv: 00000000/00000012

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-SH ver=1 serial=b 100.1.1.2:0→200.1.1.2:0 tun_id=10.0.0.2 tun_id6=::10.0.0.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=3 olast=3 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-SH proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=18225 type=00 soft=0 mtu=1438 expire=42750/0B replaywin=0
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42933/43200
  dec: spi=03ff1e97 esp=aes key=16 e44c72247f93456bb0191fb24eee8a8f
       ah=sha1 key=20 884f93d1f1212a08eb7e99fe6153408554d1e7f2
  enc: spi=a7236c3f esp=aes key=16 712b50eed56e1d231956ed11c595220b
       ah=sha1 key=20 0bede372f1a608d05df1c793d25c8939afb995a4
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=16 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. **FGT-SH IPSEC VPN状态**




```
# diagnose vpn ike gateway  list

vd: root/0
name: VPN-to-BJ
version: 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
interface: port2 10
addr: 200.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.1/::100.1.1.1
remote_location: 0.0.0.0
network-id: 0
created: 261s ago
IKE SA: created 2/2  established 2/2  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 59 d46c45f0f50d9ce8/fcaf35fab405c65a
  direction: responder
  status: established 258-258s ago = 0ms
  proposal: aes128-sha256
  key: 27f09a3f144bf8da-85d9c19874786059
  lifetime/rekey: 86400/85871
  DPD sent/recv: 0000001b/00000000

  id/spi: 58 e3498ed0f017b22b/a19990e821f3733e
  direction: initiator
  status: established 261-261s ago = 0ms
  proposal: aes128-sha256
  key: c9c4dd7d0bdea34b-e9425ad0fe0a17bc
  lifetime/rekey: 86400/85838
  DPD sent/recv: 00000000/00000000

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-BJ ver=1 serial=d 200.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.1 tun_id6=::100.1.1.1 dst_mtu=1500 dpd-
link=on weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=3 olast=3 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=27
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-BJ proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=18225 type=00 soft=0 mtu=1438 expire=42637/0B replaywin=0
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=a7236c3f esp=aes key=16 712b50eed56e1d231956ed11c595220b
       ah=sha1 key=20 0bede372f1a608d05df1c793d25c8939afb995a4
  enc: spi=03ff1e97 esp=aes key=16 e44c72247f93456bb0191fb24eee8a8f
       ah=sha1 key=20 884f93d1f1212a08eb7e99fe6153408554d1e7f2
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.1.1.2 npu_lgwy=200.1.1.2 npu_selid=f dec_npuid=0 enc_npuid=0
run_tally=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

GRE over IPSec

应用场景

传统的策略模式IPSec VPN无法运行组播、广播等数据，因此像OSPF/RIP等协议无法通过IPSec VPN直接运行，而需要借用GRE协议的辅助，GRE协议可封装组播、广播等数据，而IPSec又可将GRE协议封装在里面并且安全的加密，这样实现了通过互联网VPN安全的跑组播、广播等数据。

> **重要**
>
> 飞塔的接口模式IPSec VPN可以直接运行OSPF/RIP协议，因此如果都是FortiGate设备则无需使用GRE over IPSec，而直接使用接口模式的IPSec VPN即可实现GRE over IPSec一样的功能。与友商对接的时候也应该优先选择接口模式，部分友商有类似FortiGate接口模式的IPSec VPN（例如思科叫VTI，Virtual Tunnel Interface模式的IPSec VPN），而不需要再选择的GRE over IPSec，可以被接口模式替代。

那么什么时候需要用到GRE over IPSec呢?

1. 替换友商设备运行了GRE over IPSec的设备

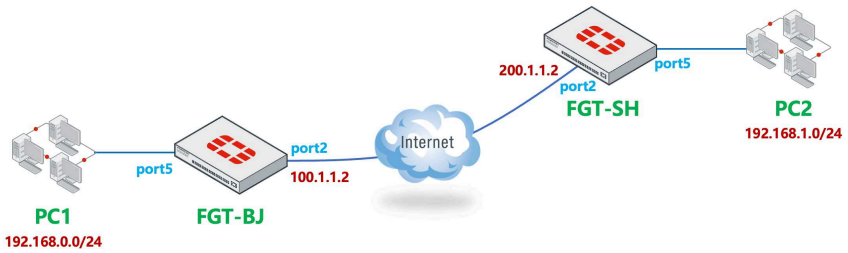
2. 对端设备为友商设备，且只能用GRE over IPSec进行对接

如果全部都是飞塔防火墙，则推荐使用接口模式IPSec VPN直接运行路由协议即可。如果存在友商设备场景下，且必须用 GRE over IPSec，那就选择此方式进行对接和部署。

网络需求

通过GRE over IPSec VPN（接口模式）将2个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信，FGT-BJ和FGT-SH之间运行OSPF协议。

网络拓扑



配置步骤

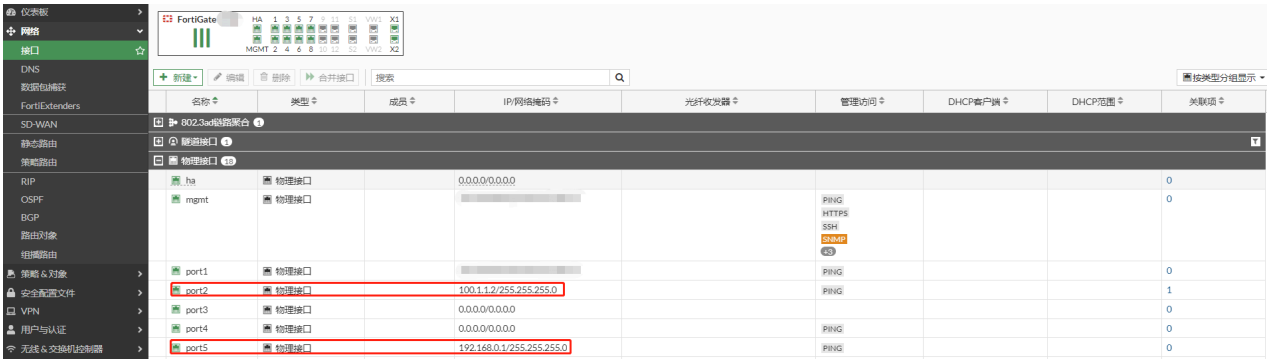
以FGT-BJ配置步骤为例，FGT-SH同理。

> **重要**
>
> 以下配置方法为Fortinet独有，不需要手动创建GRE tunnel接口，而是通过在IPSec tunnel接口上直接封装GRE的方式实现GRE over IPSec，配置较为方便。而官方Docs文档介绍的GRE over IPSec配置为较旧的方法（不推荐），推荐使用本文方法进行配置（如果对端不是Fortinet的设备，请在对端设备上使用传输模式，并配置第二阶段的感兴趣流为GRE Tunnel的源目IP，协议号为47）。旧版配置方法可参考：
> https://docs.fortinet.com/document/fortigate/7.0.11/administration-guide/799752/gre-over-ipsec ↗

1. **基本配置**

   配置接口IP和路由

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 配置GRE over IPSEC VPN

GRE over IPSEC VPN只能通过命令行配置（一阶段中需要配置“set encapsulation gre”，二阶段封装模式选择传输模式：“set encapsulation transport-mode”）

```
VPN第一阶段配置：
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 200.1.1.2
        set psksecret fortinet
        set dpd-retrycount 3
        set dpd-retryinterval 10
        set encapsulation gre
    next
end

VPN第二阶段的配置：
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set phase1name "VPN-to-SH"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set encapsulation transport-mode
        set protocol 47
    next
end
```

3. 配置防火墙策略



4. 查看IPSEC VPN状态

此时VPN状态是UP的

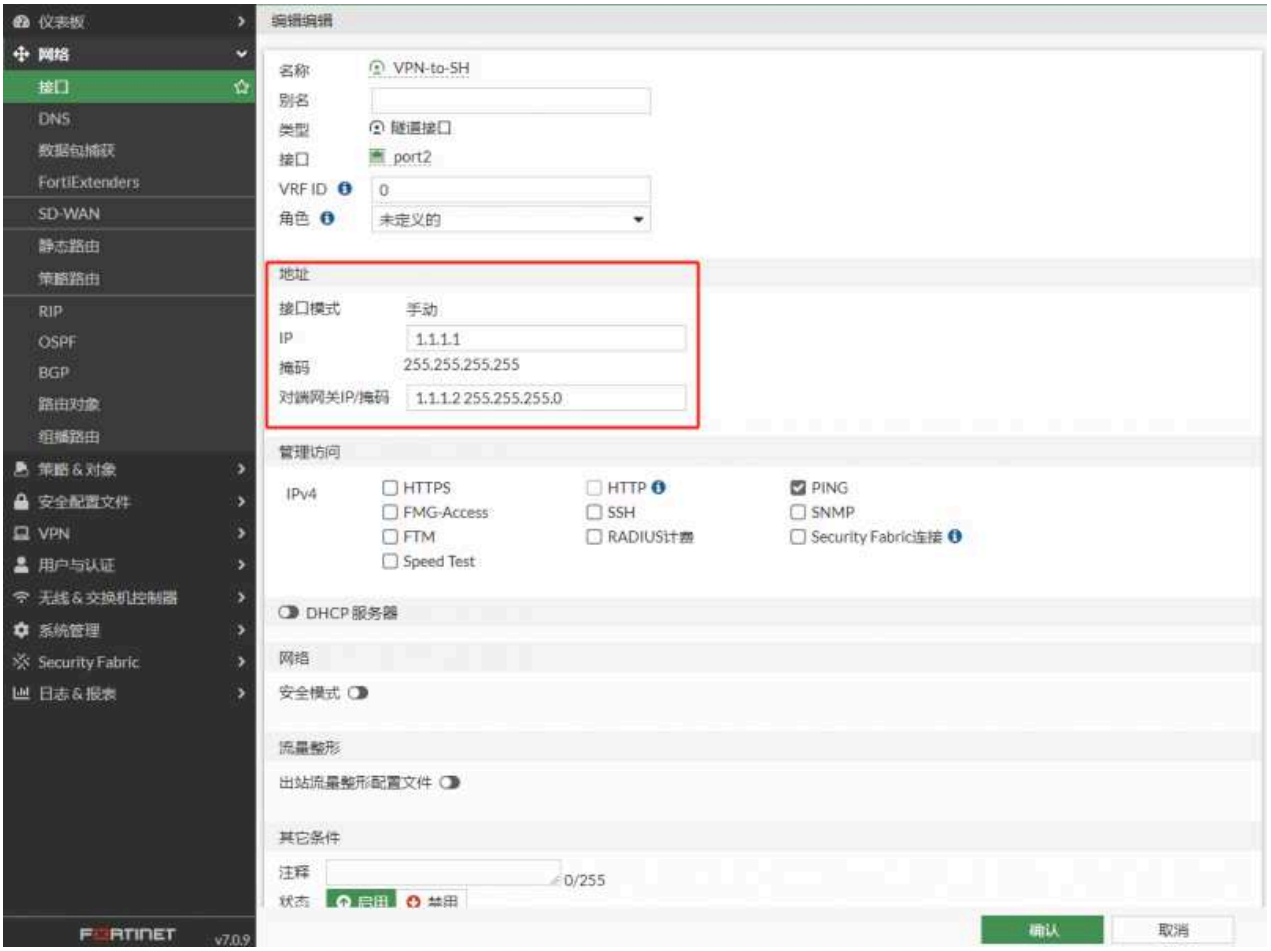


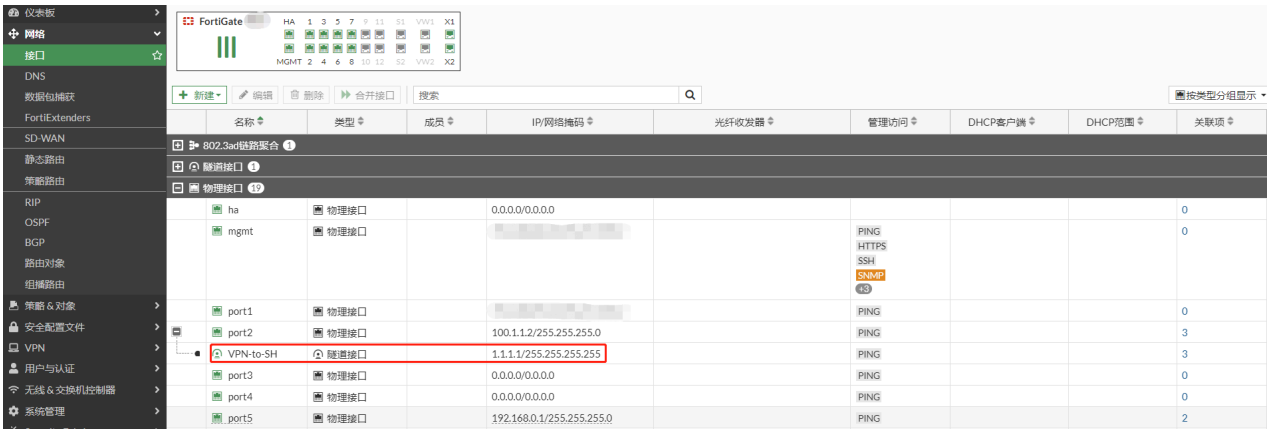
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# diagnose vpn ike gateway list

vd: root/0
name: VPN-to-SH
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 200.1.1.2/::200.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 5s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPSec SA: created 2/2  established 2/2  time 0/0/0 ms

  id/spi: 35 5aefc0a3874aef73/d1fa063796f38bbb
  direction: initiator
  status: established 5-5s ago = 0ms
  proposal: aes128-sha256
  key: 35cc029e92fafcd2-1eb88678a2dd3d93
  lifetime/rekey: 86400/86094
  DPD sent/recv: 00000000/00000000

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-SH ver=1 serial=9 100.1.1.2:0→200.1.1.2:0 tun_id=200.1.1.2 tun_id6=::200.1.1.2 dst_mtu=1500 dpd-
link=on weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=GRE/549 options[0225]=edg frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

encap-addr: 100.1.1.2→200.1.1.2
proxyid_num=1 child_num=0 refcnt=4 ilast=6 olast=6 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=42
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-SH proto=47 sa=2 ref=3 serial=1 auto-negotiate transport-mode
  src: 47:0.0.0.0-255.255.255.255:0
  dst: 47:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=8327 type=00 soft=0 mtu=1438 expire=42890/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42899/43200
  dec: spi=d4fb6a41 esp=aes key=16 a8da8882351e6d6f0a07ca6a8e9990fa
       ah=sha1 key=20 30e87d9cdb0ec7883005cd21c70cb75b41333a74
  enc: spi=9265e023 esp=aes key=16 8255103778ec791deb6dd576decb6859
       ah=sha1 key=20 479dd7e310e013112dcb9b4f9367c9686389efc5
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=14 dec_npuid=0 enc_npuid=0
  SA:  ref=3 options=8327 type=00 soft=0 mtu=1438 expire=42918/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42927/43200
  dec: spi=d4fb6a42 esp=aes key=16 3ef3be2fdb220fc740c3df3eb6955714
       ah=sha1 key=20 e1b9972a81d688cc32d160b0fc6060b57c42ccac
  enc: spi=9265e022 esp=aes key=16 a247b6207b2244b0ff7822fae3fab091
       ah=sha1 key=20 1c89fa4c89e197efa0886b23eaf722760c63b574
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=14 dec_npuid=0 enc_npuid=0
run_tally=0
```

5. **配置IPSEC VPN接口地址（此环境中，IPSec接口将充当GRE Tunnel接口使用）**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





接口地址通过GRE over IPSEC能通互ping成功。

重要

配置IPSec接口的remote-gw后，路由表中会产生remote-gw对应的直连路由，该路由可以将GRE封装后的流量送入IPSec隧道中。

```
# execute ping-options source 1.1.1.1
# execute ping 1.1.1.2
PING 1.1.1.2 (1.1.1.2): 56 data bytes
64 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=0.4 ms
64 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=0.6 ms

--- 1.1.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.5/0.7 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
S       1.1.1.0/24 [5/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]
C       1.1.1.1/32 is directly connected, VPN-to-SH
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
C       192.168.88.0/24 is directly connected, mgmt
C       192.168.89.0/24 is directly connected, port1
```

6. 配置OSPF



查看OSPF邻居和路由

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
200.1.1.2         1   Full/ -         00:00:34    1.1.1.2         VPN-to-SH(tun-id:200.1.1.2)

# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
S       1.1.1.0/24 [5/0] via VPN-to-SH tunnel 200.1.1.2, [1/0]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
20  C       1.1.1.1/32 is directly connected, VPN-to-SH
    O       1.1.1.2/32 [110/100] via VPN-to-SH tunnel 200.1.1.2, 00:00:01
    C       100.1.1.0/24 is directly connected, port2
    C       192.168.0.0/24 is directly connected, port5
    O       192.168.1.0/24 [110/101] via VPN-to-SH tunnel 200.1.1.2, 00:00:01
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

修改IPSec协商端口

1. 某些ISP会阻断UDP端口500或UDP端口4500，导致IPsec VPN无法协商和建立。FortiGate支持修改IPsec的协商端口来避免该问题。

```
config system settings
    set ike-port 10000    //默认udp port 500，端口范围udp port <1024> to <65535>
end
```

2. 修改后所有的隧道将使用指定的端口来协商。

3. 对于业务层面：

- 非NAT-T环境下仍然使用ESP封装。
- NAT-T下使用上述配置的IKE port来封装UDP Header。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与友商对接IPSec的注意事项

1. 由于每个厂商的地址组在IPSec协商中封装的格式可能不一致（FortiGate使用地址组时，二阶段只使用一个SA包含多个网段，不会切割为多个SA），可能导致协商失败或隧道翻转等现象，二阶段感兴趣流如果存在多对网段，请不要使用地址组作为第二阶段感兴趣流。请使用多个Subnet的作为二阶段感兴趣流的模式。

2. 由于每个厂商对两端SA重协商时间不一致时的处理方法不一致（FortiGate会使用双方SA重协商较小的时间作为自己的SA重协商时间），两端的一、二阶段SA重协商时间请尽量配置为相同的时间。

3. 如果IPSec与友商对接时选择证书认证，可能会出现连接无法建立的情况。

   - 在FortiGate的IPSec Debug信息中，如果看到如下报错：

```bash
FortiGate # diagnose debug application ike -1
FortiGate # diagnose debug enable

RenHangNewVPN: 7913020: received p1 notify type INITIAL-CONTACT
//RenHangNewVPN: 7913020: peer identifier IPV4_ADDR 54.121.33.6//
RenHangNewVPN: 7913020: Validating X.509 certificate
//RenHangNewVPN: 7913020: peer cert, subject='IPSECVPN', issuer='CFIT'//
//RenHangNewVPN: 7913020: peer ID does not match cert//
RenHangNewVPN: 7913020: certificate validation failed
RenHangNewVPN: 7913020: info_send_n1, type 20
......
```

   - 这是由于FortiGate选择证书认证时，默认会开启证书ID（subject或称为CN）与对端ID的一致性检查（符合RFC 4945）。当对端IPSec设备发送的ID（此例中为IPv4 54.121.33.6）与对端发送的证书的subject（此例中为“IPSECVPN”）不一致时，会认证失败。

```bash
config vpn ipsec phase1-interface
    edit "FGT110"
        set cert-id-validation enable    //使用证书认证后默认开启//
    next
end
```

   - 当然，FortiGate在开启IPSec证书认证时，会自动将本端ID修改为“asn1dn”类型，并将本端证书的subject复制到本端ID中，不会使用默认的本端IPv地址作为本端ID（符合RFC 4945）。

```bash
config vpn ipsec phase1-interface
    edit "FGT110"
        set interface "port8"
        set authmethod signature
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set localid "FGT200”    //配置locaid-type asn1dn后自动从本端证书的subject中读取后配置//
        set localid-type asn1dn    //开启证书认证后自动配置//
        set comments "VPN: FGT110 (Created by VPN wizard)"
        set remote-gw 192.168.8.111
        set certificate "FGT200"
    next
end
```

   - 所以当IPSec两端均为FortiGate时，如果没有手工更改ID配置，连接是可以正常建立的。但如果对端设备为友商设备，可能不会遵守RFC 4945，仍然使用IP地址作为ID发送至FortiGate，这样就会导致协商失败。

   - 解决办法：

     - 是在FortiGate上关闭证书ID与对端ID的一致性检查。

```bash
config vpn ipsec phase1-interface
    edit "FGT110"
        set cert-id-validation disable
    next
end
```

     - 或是在对端友商设备上配置ID类型为asn1dn，ID内容为其证书的subject（如果友商设备支持此配置）。

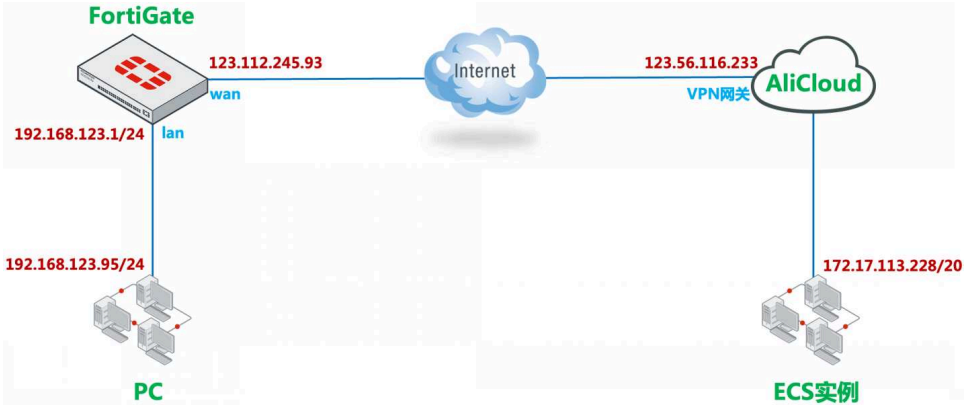
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与阿里云建立IPSec VPN

网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与172.17.112.0/20两个网段的通信。与阿里云进行IPsec VPN（IKE v1）对接。

组网拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置阿里云VPN
  - 配置VPN网关
  - 配置IPsec VPN连接
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略

注意事项

1. 在阿里云IPSec的工作机制中，阿里云IPSec一二阶段并没有关联，当阿里云的一阶段到期后，并不会重新发起一阶段的重协商，也不会删除对应的二阶段，而是需要满足一二阶段同时到期后才会发起一阶段的重协商。而对于FortiGate来说，只要一阶段的SA到期，就会删除二阶段的SA连接（FortiGate作为安全设备，这是正常的操作）。如下图为阿里云工程师对于阿里云IPSec协商工作机制的解释。



2. 这样就会导致当FortiGate为IPSec协商的响应方，而阿里云为IPSec协商的发起方时，可能会出现一阶段协商到期后，FortiGate将自己的一阶段和关联的二阶段连接删除，阿里云IPSec仅将自己的一阶段删除，保留二阶段直到二阶段倒计时结束，才会重新发起一阶段连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 此时FortiGate重新发起一阶段协商，阿里云是不响应的。会出现FortiGate端IPSec连接已经断开，而阿里云端仍然显示连接存在的情况，此时业务是不通的，需要等到阿里云残留的二阶段到期后，才会重新发起协商，如果两端二阶段配置的时间较长，则会中断较长的时间。

4. **想要规避此问题，需要FortiGate始终作为IPSec VPN的发起方，阿里云作为响应方，这样在一阶段到期前（30s或300s），FortiGate总能主动重新发起新的一阶段和二阶段连接。**

5. 由于阿里云端的IPSec协商机制无法配置修改，**Workaround是在FortiGate侧配置Local-in Policy**，在没有IKE会话建立的情况下，丢弃对端发来的IKE协商包（另外，FortiGate在IPSec连接建立后会删除IKE会话，也会丢弃在连接建立后对端发送的IKE协商包，避免自己成为响应方）。详情见配置步骤。

配置步骤

配置FortiGate

1. 基本上网配置。





2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置网络、认证、第一阶段。

> **重要**
>
> 这里的安全提议（阶段1提案）建议只保留一组，与阿里云测配置一致，不要选择多个算法组合。



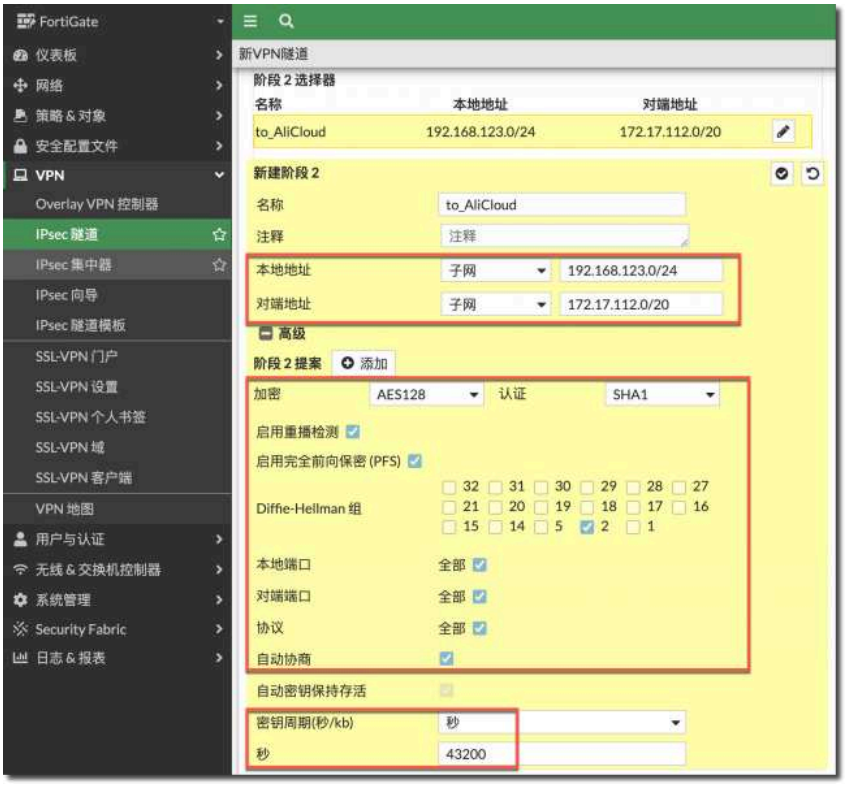

```
config vpn ipsec phase1-interface
    edit "to_AliCloud"
        set interface "wan"
        set peertype any
        set net-device disable
        set proposal aes128-sha1
        set dpd on-idle
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dhgrp 2
        set remote-gw 123.56.116.233
        set psksecret xxxxxx
    next
end
```

5. 配置第二阶段。

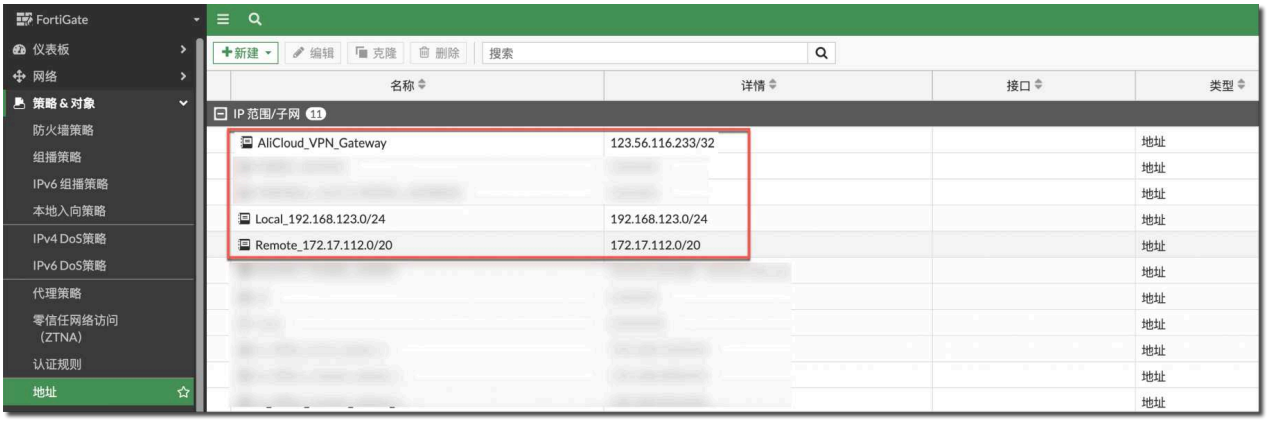
> **重要**
>
> 这里的安全提议（阶段2提案）建议只保留一组，与阿里云测配置一致，不要选择多个算法组合。

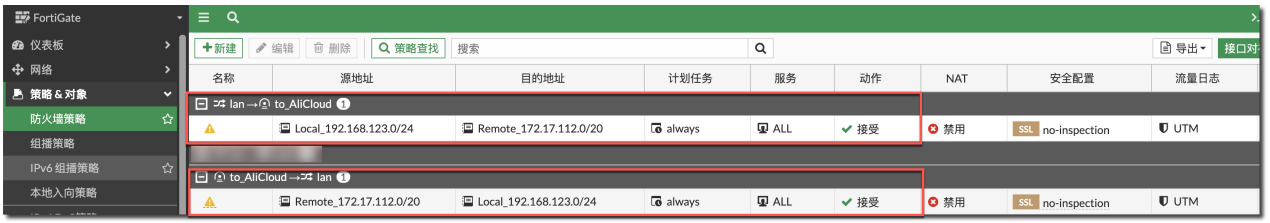



```
config vpn ipsec phase2-interface
    edit "to_AliCloud"
        set phase1name "to_AliCloud"
        set proposal aes128-sha1
        set dhgrp 2
        set auto-negotiate enable
        set src-subnet 192.168.123.0 255.255.255.0
        set dst-subnet 172.17.112.0 255.255.240.0
    next
end
```

6. 配置VPN相关的网段地址对象、阿里云VPN网关地址对象和防火墙策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
config firewall address
    edit "Local_192.168.123.0/24"
        set subnet 192.168.123.0 255.255.255.0
    next
    edit "Remote_172.17.112.0/20"
        set subnet 172.17.112.0 255.255.240.0
    next
    edit "AliCloud_VPN_Gateway"
        set subnet 123.56.116.233 255.255.255.255
    next
end

config firewall policy
    edit 4
        set srcintf "lan"
        set dstintf "to_AliCloud"
        set action accept
        set srcaddr "Local_192.168.123.0/24"
        set dstaddr "Remote_172.17.112.0/20"
        set schedule "always"
        set service "ALL"
    next
    edit 5
        set srcintf "to_AliCloud"
        set dstintf "lan"
        set action accept
        set srcaddr "Remote_172.17.112.0/20"
        set dstaddr "Local_192.168.123.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

7. 配置VPN业务网段的静态路由。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config router static
    edit 3
        set dst 172.17.112.0 255.255.240.0
        set device "to_AliCloud"
    next
    edit 4
        set dst 172.17.112.0 255.255.240.0
        set distance 254
        set blackhole enable
    next
end
```

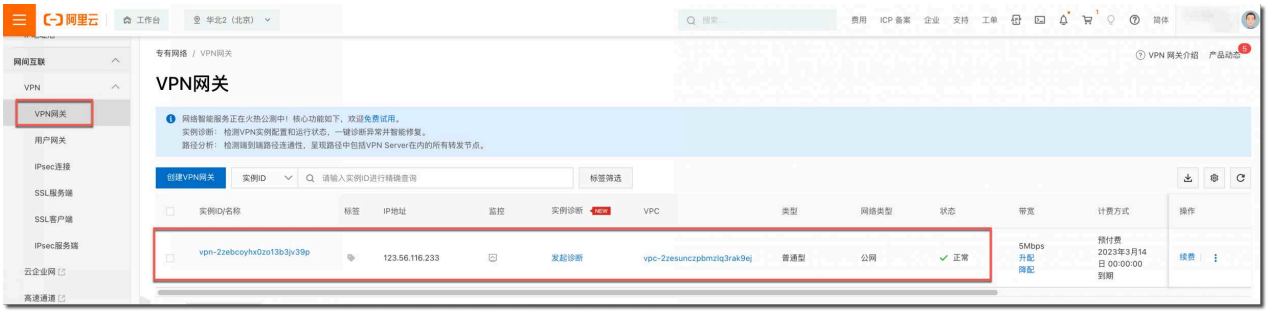
8. **为FortiGate配置Local-in Policy，在没有IKE会话建立的情况下，丢弃阿里云侧发来的IKE协商包。**

> **重要**
>
> 此步非常重要，不配置很可能出现与阿里云IPSec连接中断后无法重新建立的情况。

```
config firewall local-in-policy
    edit 1
        set intf "wan"
        set srcaddr "AliCloud_VPN_Gateway"
        set dstaddr "all"
        set service "IKE"
        set schedule "always"
        set action deny
    next
end
```

配置阿里云IPSec VPN

1. 进入网间互联→VPN→VPN网关页面，创建VPN网关，注意选择正确的与实例互通的交换机。



2. 进入用户网关页面，创建用户网关，即FortiGate的公网地址。



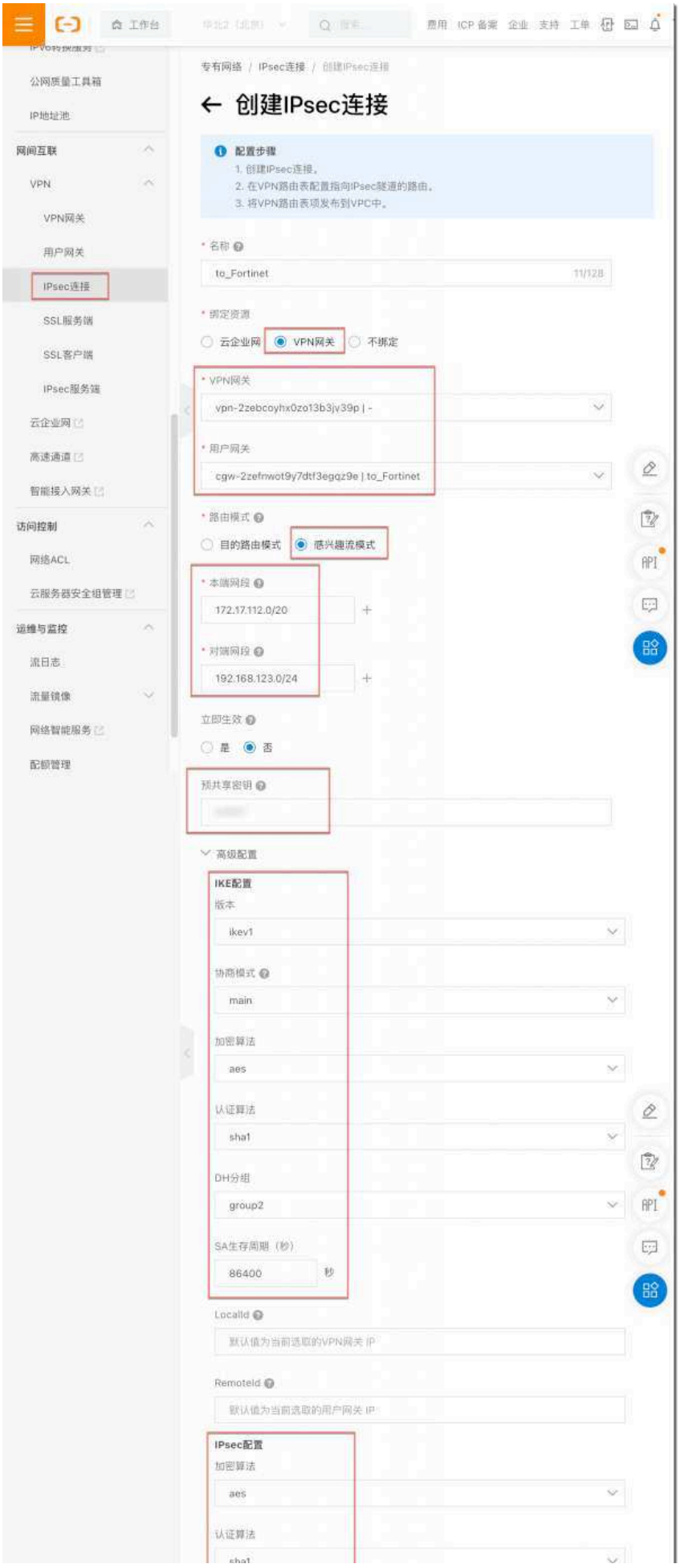
3. 进入IPSec连接页面，创建IPSec连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

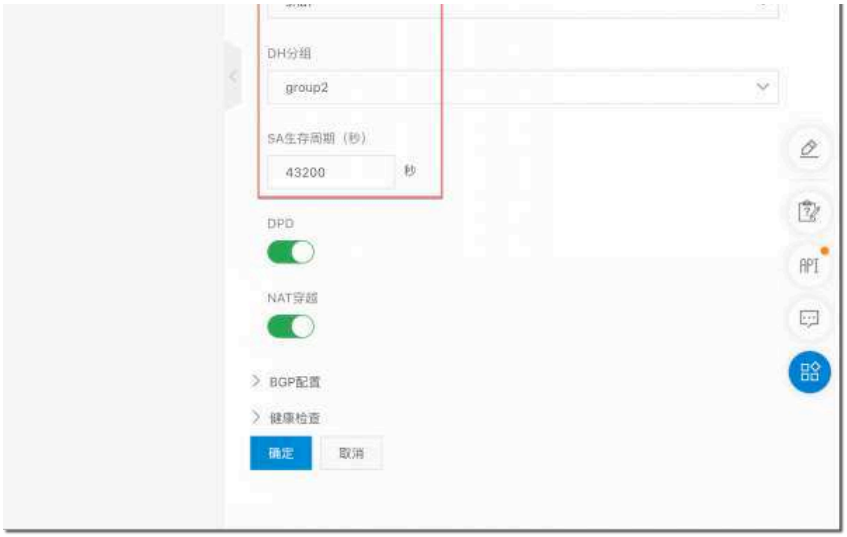


4. 选择绑定资源为VPN网关，分别选择第2步和第3步创建的VPN网关和用户网关，路由模式选择感兴趣流，填写本端和对端的感兴趣流网段，一二阶段算法与重协商时间与FortiGate保持一致。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



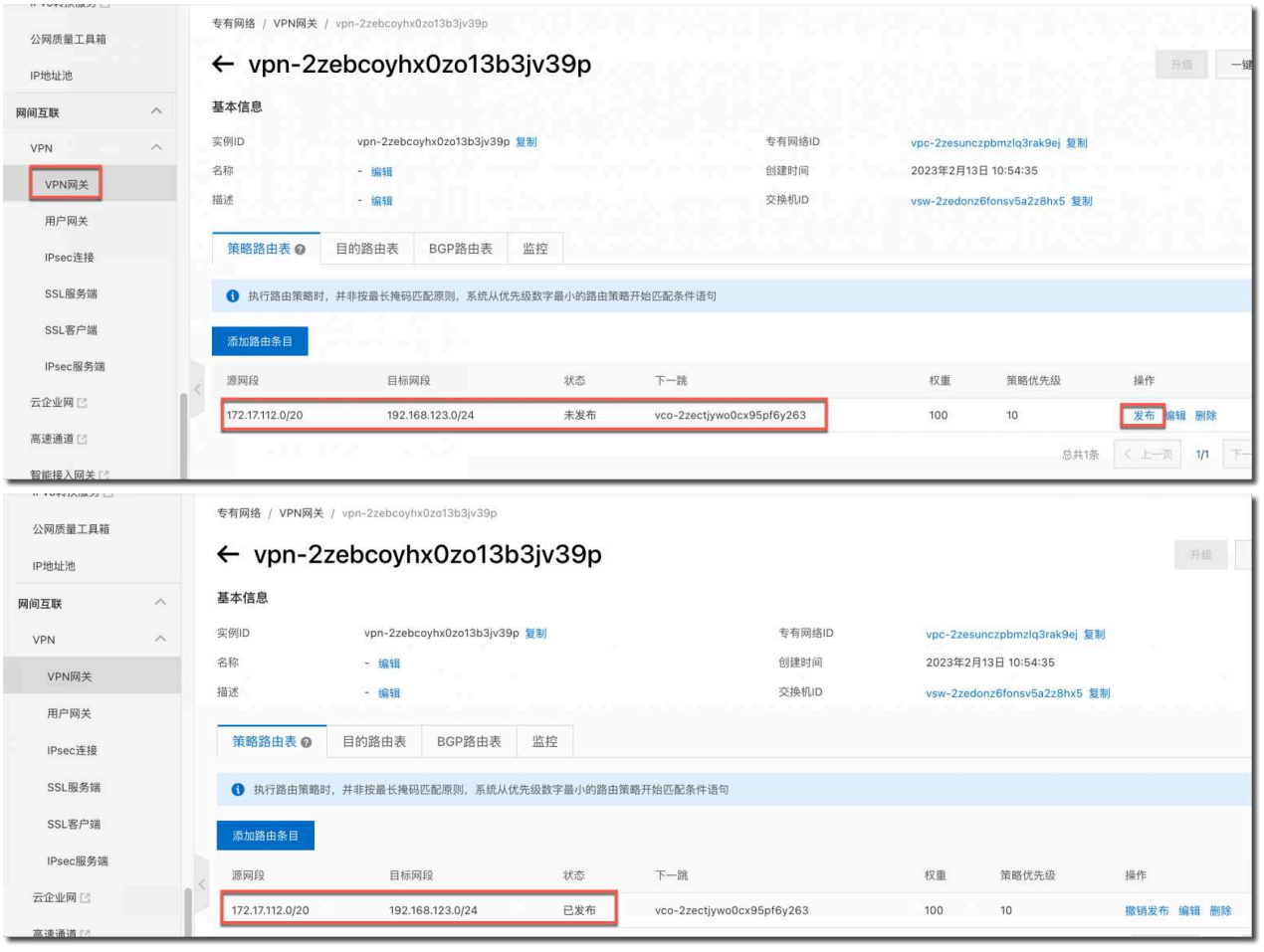
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 点击确定按钮，会弹出是否去VPN网关中发布路由的提示，选择确定，则会根据感兴趣流自动添加路由到VPN网关。

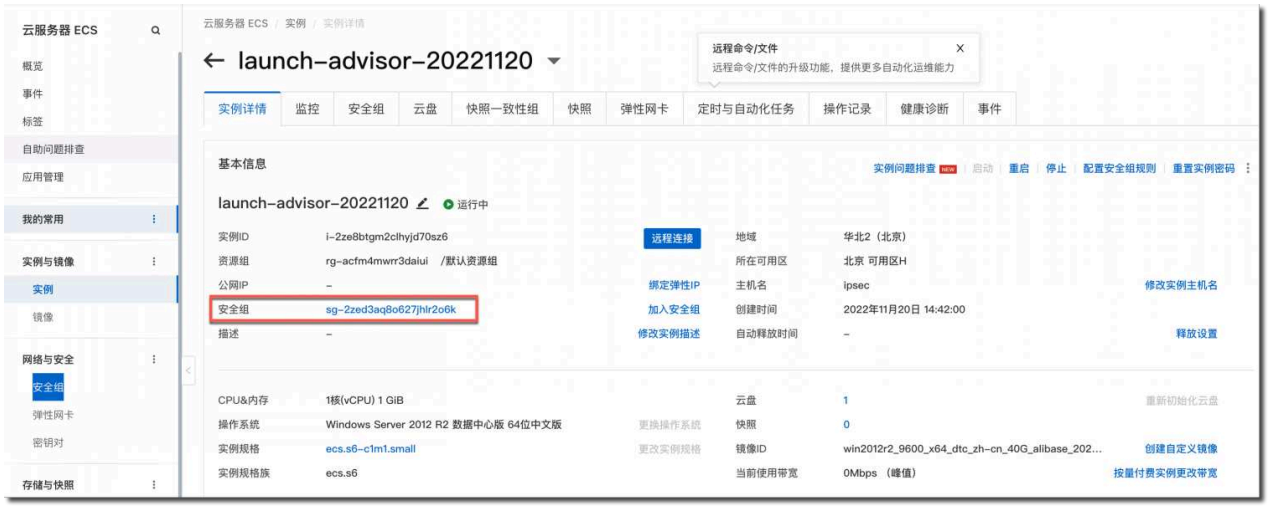


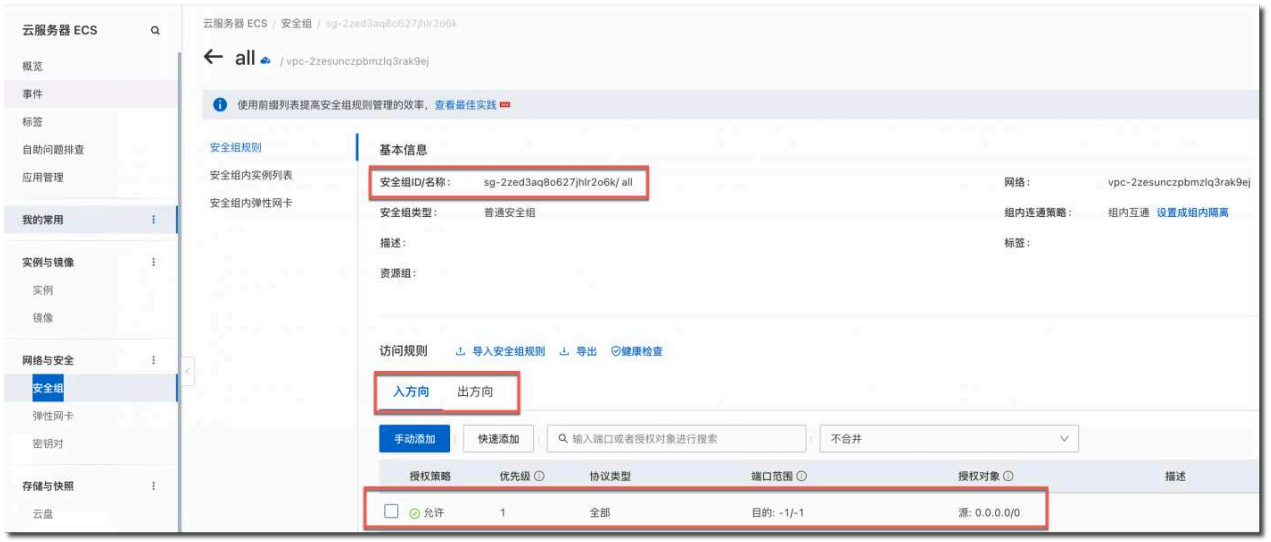
6. 进入VPN网关，编辑第1步中创建的VPN网关，在下方的策略路由表中可以看到针对VPN感兴趣流的策略路由，点击发布按钮发布路由，使其状态变为已发布。



7. 配置ECS实例的安全组，允许出方向和入方向的流量（根据实际需求配置）。

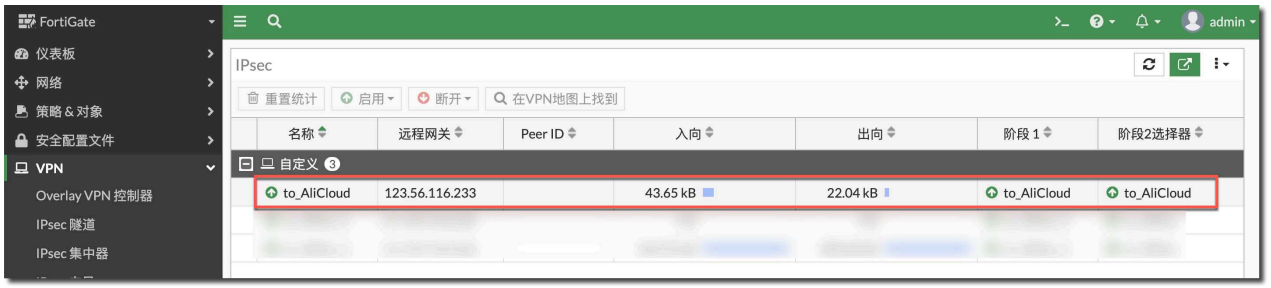
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。

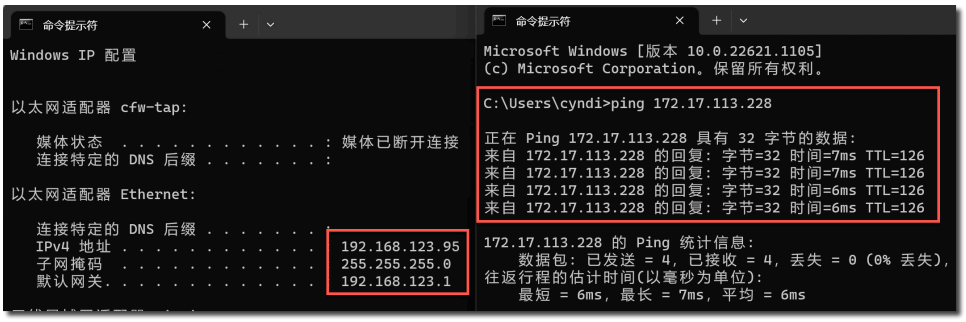


2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 123.112.245.1, wan, [1/0]
C       192.168.123.0/24 is directly connected, lan
S       172.17.112.0/20 [10/0] via to_AliCloud tunnel 123.56.116.233, [1/0]
C       123.112.245.0/24 is directly connected, wan
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. FortiGate侧PC业务测试。



4. FortiGate查看隧道建立状态，可以看到，FortiGate成为了initiator，这是正确的状态，如果成为responder，则会出现注意事项中提到的问题（配置Local-in Policy就是为了防止FortiGate成为responder）。

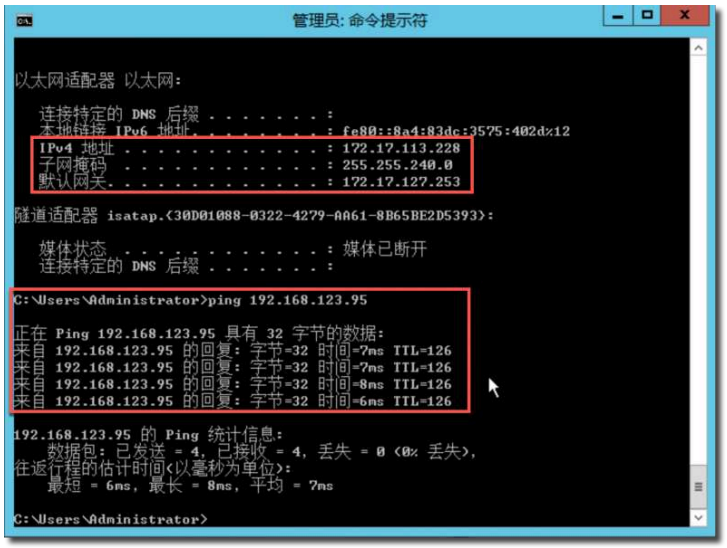
```
FortiGate # diagnose vpn ike gateway list name to_AliCloud

vd: root/0
name: to_AliCloud
version: 1
interface: wan 5
addr: 123.112.245.93:500 → 123.56.116.233:500
tun_id: 123.56.116.233/::123.56.116.233
remote_location: 0.0.0.0
network-id: 0
created: 9s ago
nat: me peer
IKE SA: created 1/1  established 1/1  time 40/40/40 ms
IPsec SA: created 1/1  established 1/1  time 70/70/70 ms

  id/spi: 1544 dd588fcaa7cdae73/f47afb7c48f8e129
  direction: initiator
  status: established 9-9s ago = 40ms
  proposal: aes128-sha1
  key: b12f333e43d7d263-03a98c2d39015ba5
  lifetime/rekey: 86400/86090
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list name to_AliCloud
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=to_AliCloud ver=1 serial=18 123.112.245.93:500→123.56.116.233:500 tun_id=123.56.116.233
tun_id6=::123.56.116.233 dst_mtu=1500 dpd-link=on weight=1
bound_if=5 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=6 ilast=7 olast=1 ad=/0
stat: rxp=116 txp=129 rxb=16390 txb=9310
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=5
natt: mode=keepalive draft=32 interval=10 remote_port=500
proxyid=to_AliCloud proto=0 sa=1 ref=3 serial=1 auto-negotiate
  src: 0:192.168.123.0-192.168.123.255:0
  dst: 0:172.17.112.0-172.17.127.255:0
  SA:  ref=6 options=18227 type=00 soft=0 mtu=1422 expire=42774/0B replaywin=2048
       seqno=80 esn=0 replaywin_lastseq=00000073 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=688c1754 esp=aes key=16 2d9485697de2a31671bffbd55a97d91d
       ah=sha1 key=20 ccd0cdfea070180dabba59888f50d6470aaef88d
  enc: spi=4cba32a0 esp=aes key=16 495332b764e20e44523f5de593c14806
       ah=sha1 key=20 a3880ddf07c940ccc18ec827d0f1329094389c16
  dec:pkts/bytes=117/16450, enc:pkts/bytes=131/9566
  npu_flag=03 npu_rgwy=123.56.116.233 npu_lgwy=192.168.123.175 npu_selid=19 dec_npuid=1 enc_npuid=1
run_tally=0
```

5. 阿里云侧查看IPSec隧道建立状态，可以看到第二阶段已经建立成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 阿里云侧ECS实例业务测试。



7. FortiGate侧抓包查看。

```
FortiGate # dia sni pa any "host 172.17.113.228 or host 123.56.116.223" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 172.17.113.228 or host 123.56.116.223]
2.729115 to_AliCloud out 192.168.123.95 → 172.17.113.228: icmp: echo request
2.729136 wan out 123.112.245.93 → 123.56.116.223: ESP(spi=0×4cba32a0,seq=0×7a)
2.730083 wan in 123.56.116.223 → 123.112.245.93: ESP(spi=0×688c1754,seq=0×74)
2.730098 to_AliCloud in 172.17.113.228 → 192.168.123.95: icmp: echo reply
3.729410 to_AliCloud out 192.168.123.95 → 172.17.113.228: icmp: echo request
3.729430 wan out 123.112.245.93 → 123.56.116.223: ESP(spi=0×4cba32a0,seq=0×7b)
3.730364 wan in 123.56.116.223 → 123.112.245.93: ESP(spi=0×688c1754,seq=0×75)
3.730382 to_AliCloud in 172.17.113.228 → 192.168.123.95: icmp: echo reply
4.729580 to_AliCloud out 192.168.123.95 → 172.17.113.228: icmp: echo request
4.729600 wan out 123.112.245.93 → 123.56.116.223: ESP(spi=0×4cba32a0,seq=0×7c)
4.730377 wan in 123.56.116.223 → 123.112.245.93: ESP(spi=0×688c1754,seq=0×76)
4.730397 to_AliCloud in 172.17.113.228 → 192.168.123.95: icmp: echo reply
5.729921 to_AliCloud out 192.168.123.95 → 172.17.113.228: icmp: echo request
5.729941 wan out 123.112.245.93 → 123.56.116.223: ESP(spi=0×4cba32a0,seq=0×7d)
5.731016 wan in 123.56.116.223 → 123.112.245.93: ESP(spi=0×688c1754,seq=0×77)
5.731031 to_AliCloud in 172.17.113.228 → 192.168.123.95: icmp: echo reply
6.730170 to_AliCloud out 192.168.123.95 → 172.17.113.228: icmp: echo request
6.730191 wan out 123.112.245.93 → 123.56.116.223: ESP(spi=0×4cba32a0,seq=0×7e)
6.731200 wan in 123.56.116.223 → 123.112.245.93: ESP(spi=0×688c1754,seq=0×78)
6.731219 to_AliCloud in 172.17.113.228 → 192.168.123.95: icmp: echo reply
```

其他说明

1. 请注意与阿里云建立IPSec VPN时，如果FortiGate位于NAT后（接口为私网地址），则需要在FortiGate的IPSec一阶段中指定Local-id，id类型为address，地址为FortiGateNAT后的公网地址。

```
config vpn ipsec phase1-interface
        edit to_AliCloud
                set localid-type address
                set localid 123.112.245.93    //此处填写NAT后的公网地址
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
6   end
```

2. 如果要使用IKEv2，只需要将两端一阶段配置中的IKE版本修改为IKEv2即可，同样的，需要保证两端的安全算法一致。

3. 关于sniffer抓VPN业务和ESP的包：

   - 抓取IPsec VPN的IKE协商包：

     ```
     1   diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
     ```

   - 抓取IPsec VPN的ESP加密数据包：

     ```
     1   diagnose sniffer packet any "host 101.1.1.1 and esp" 4
     ```

   - 抓取IPsec VPN的明文业务数据包：

     ```
     1   diagnose sniffer packet any "host 172.17.113.228 and icmp" 4
     ```

   - 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭（VPN流量较大的情况下谨慎开启）：

     ```
     1   FortiGate # config vpn ipsec phase1-interface
     2   FortiGate (phase1-interface) # edit to_AliCloud
     3   FortiGate (to_AliCloud) # set npu-offload disable
     4   FortiGate (to_AliCloud) # end
     ```

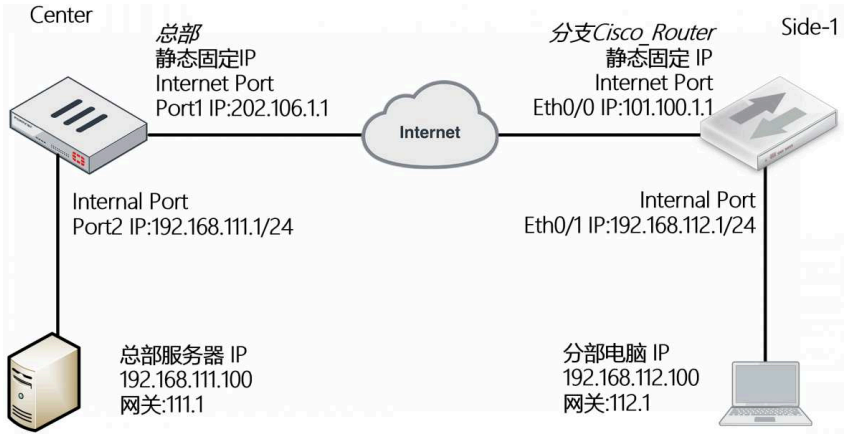

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与思科路由器建立IPSec VPN(IKE v1)

网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.111.0/24与192.168.112.0/24两个网段的通信。与思科路由器进行IPsec VPN（IKE v1）对接。

网络拓扑



配置要点

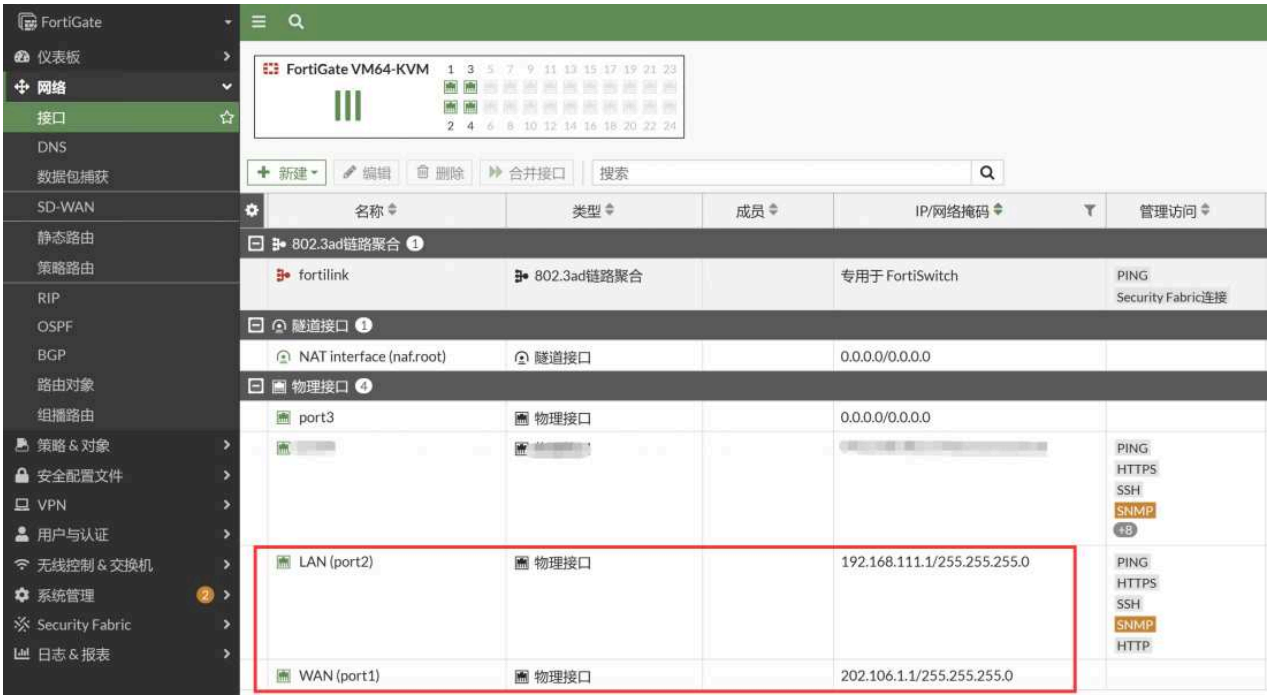
- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Cisco_Router
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 配置网络、认证、第一阶段。

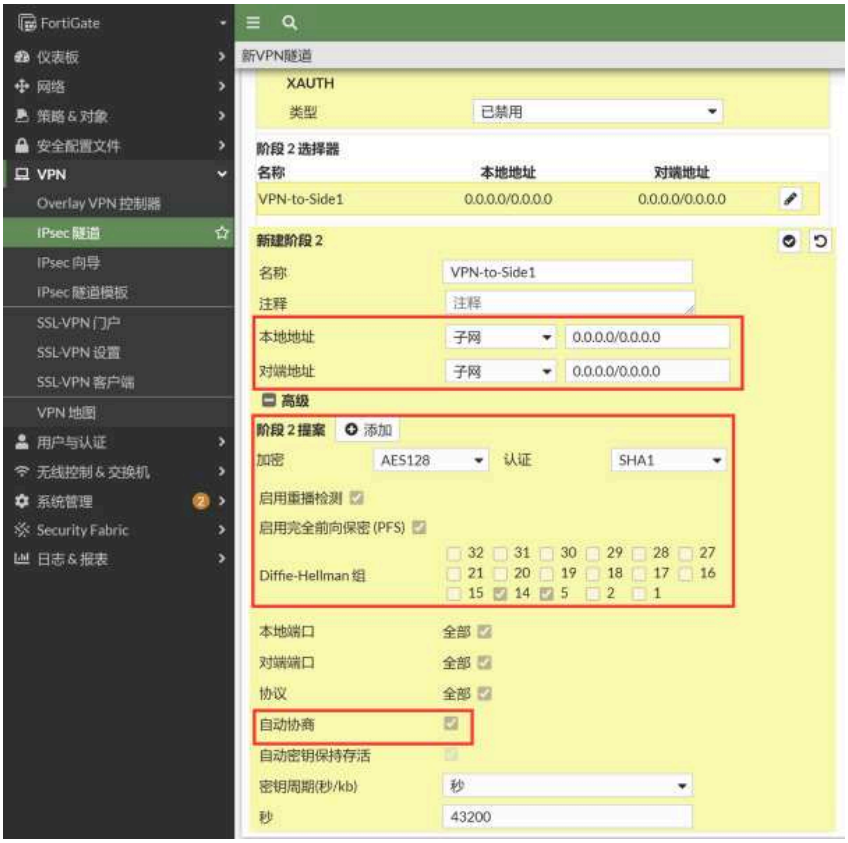
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase1-interface
    edit "VPN-to-Side1"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes256-sha1
        set dpd on-idle
        set dhgrp 14 5 2
        set remote-gw 101.100.1.1
        set psksecret ENC
/HISpjoxUQ1RoRXahwT2OpZmuyYsDY818arB4Q93PztlW0oynlDWuKIk1WIAXFLNldoVFlgOOjBk9Bf9tc6LdI/BeD6CmRvgokNIKa5fVnVgxXLzHM
9fPGvtRXb362jpxZkMxuKHcNGVrJCimmjVGAS+gixHgh8mRLj5kaMAbyhNX1odwNNgxYcxqap5iAwncL3ZzQ==
    next
end
```

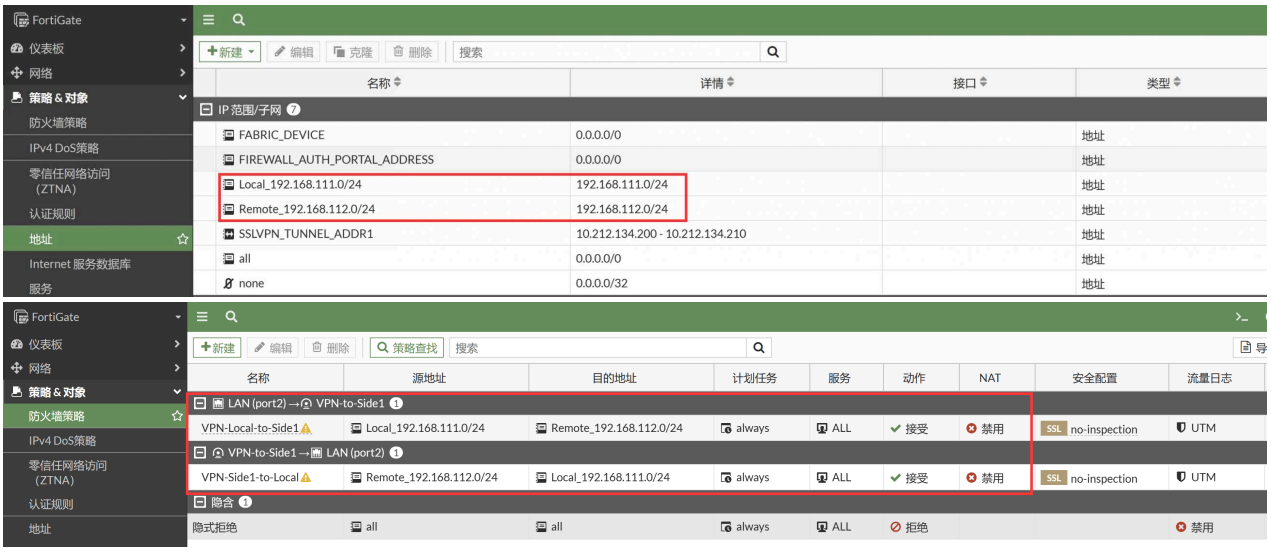
5. 配置第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase2-interface
    edit "VPN-to-Side1"
        set phase1name "VPN-to-Side1"
        set proposal aes128-sha1
        set auto-negotiate enable
    next
end
```

6. 配置VPN相关的网段地址对象和防火墙策略。

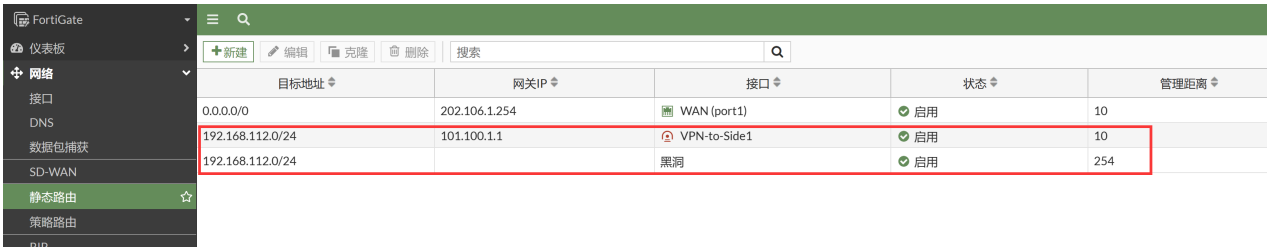



```
config firewall address
    edit "Local_192.168.111.0/24"
        set uuid 3bff7c90-8e7b-51ed-5311-ca9abc900a91
        set subnet 192.168.111.0 255.255.255.0
    next
    edit "Remote_192.168.112.0/24"
        set uuid 4647b500-8e7b-51ed-ea6f-c0ec2647bb42
        set subnet 192.168.112.0 255.255.255.0

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    next
end

config firewall policy
    edit 1
        set name "VPN-Local-to-Side1"
        set uuid 7d1e7ce4-8e7b-51ed-19ea-001e373a03f3
        set srcintf "port2"
        set dstintf "VPN-to-Side1"
        set action accept
        set srcaddr "Local_192.168.111.0/24"
        set dstaddr "Remote_192.168.112.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "VPN-Side1-to-Local"
        set uuid 96c924d2-8e7b-51ed-f2d1-a61215d677f8
        set srcintf "VPN-to-Side1"
        set dstintf "port2"
        set action accept
        set srcaddr "Remote_192.168.112.0/24"
        set dstaddr "Local_192.168.111.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

7. 配置VPN业务网段的静态路由。




```
config router static
    edit 1
        set gateway 202.106.1.254
        set device "port1"
    next
    edit 2
        set dst 192.168.112.0 255.255.255.0
        set device "VPN-to-Side1"
    next
    edit 3
        set dst 192.168.112.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

Cisco Router

1. 基本上网配置。

```
 interface Ethernet0/0
 ip address 101.100.1.1 255.255.255.0
 ip nat outside
 no shutdown
 !
 interface Ethernet0/1
 ip address 192.168.112.1 255.255.255.0
 ip nat inside
 no shutdown

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

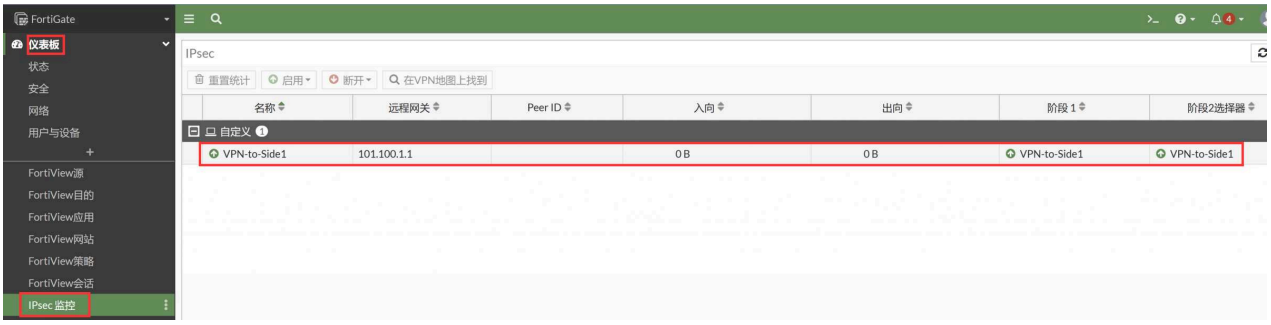
```
 !
 ip nat inside source list 101 interface Ethernet0/0 overload
 ip route 0.0.0.0 0.0.0.0 101.100.1.254
 !
 access-list 101 permit ip any any
```

2. IPsec IKE v1的配置。

```
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 5
 !
 crypto isakmp key Fortinet123# address 202.106.1.1
 crypto isakmp keepalive 10 periodic
 !
 crypto ipsec transform-set MY-Trans esp-aes esp-sha-hmac
  mode tunnel
 !
 crypto ipsec profile MY-IPsec-Pro
  set transform-set MY-Trans
  set pfs group5
 !
 interface Tunnel0
  ip address 1.1.1.2 255.255.255.0
  ip mtu 1400
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel destination 202.106.1.1
  tunnel protection ipsec profile MY-IPsec-Pro
 !
 ip route 192.168.111.0 255.255.255.0 Tunnel0 1.1.1.1
```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。



2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.106.1.254, port1, [1/0]
C       192.168.111.0/24 is directly connected, port2
S       192.168.112.0/24 [10/0] via VPN-to-Side1 tunnel 101.100.1.1, [1/0]
C       202.106.1.0/24 is directly connected, port1
```

3. FortiGate侧业务测试。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # execute ping-options source 192.168.111.1
FortiGate # execute ping 192.168.112.1
PING 192.168.112.1 (192.168.112.1): 56 data bytes
64 bytes from 192.168.112.1: icmp_seq=0 ttl=255 time=1.0 ms
64 bytes from 192.168.112.1: icmp_seq=1 ttl=255 time=1.2 ms
64 bytes from 192.168.112.1: icmp_seq=2 ttl=255 time=0.9 ms
64 bytes from 192.168.112.1: icmp_seq=3 ttl=255 time=1.1 ms
64 bytes from 192.168.112.1: icmp_seq=4 ttl=255 time=1.0 ms
--- 192.168.112.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.0/1.2 ms
```

4. FortiGate查看隧道建立状态。

```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Side1
version: 1
interface: port1 3
addr: 202.106.1.1:500 → 101.100.1.1:500
tun_id: 101.100.1.1/::101.100.1.1
remote_location: 0.0.0.0
network-id: 0
created: 449s ago
IKE SA: created 1/2  established 1/1  time 0/0/0 ms
IPsec SA: created 2/2  established 1/1  time 0/0/0 ms
  id/spi: 58 584e6c9052795a25/a433e7123ece6706
  direction: responder
  status: established 423-423s ago = 0ms
  proposal: aes256-sha1
  key: 447062de7f9b419b-37148f8d51b0e3be-dab2d73c40ed2fcc-48619811c9f95b96
  lifetime/rekey: 86400/85706
  DPD sent/recv: 00000000/6f07eaf6

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Side1 ver=1 serial=1 202.106.1.1:0→101.100.1.1:0 tun_id=101.100.1.1 tun_id6=::101.100.1.1
dst_mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overla0
proxyid_num=1 child_num=0 refcnt=4 ilast=5 olast=5 ad=/0
stat: rxp=110 txp=115 rxb=10840 txb=11260
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=2
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Side1 proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=2905/0B replaywin=2048
       seqno=74 esn=0 replaywin_lastseq=0000006e qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3333/3600
  dec: spi=148a81f0 esp=aes key=16 810f57e8981275c305be8c7fe3e6231d
       ah=sha1 key=20 7f9b004e1340ab3614dc359e50bf1ba5110ca6b6
  enc: spi=41a02d8a esp=aes key=16 81e238bdfb77856910326d4b40ac4bef
       ah=sha1 key=20 8785688516cc98c13b79d0008333db7b0a6f6dc7
  dec:pkts/bytes=220/21680, enc:pkts/bytes=230/30340
  npu_flag=00 npu_rgwy=101.100.1.1 npu_lgwy=202.106.1.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

5. Cisco_Router侧业务测试。

```
Router#ping 192.168.111.1 source 192.168.112.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.111.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.112.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/7 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
202.106.1.1     101.100.1.1     QM_IDLE           1002 ACTIVE
```

6. FortiGate侧抓包查看。

```
FortiGate # dia sni pa any "host 192.168.112.1 or host 101.100.1.1" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.112.1 or host 101.100.1.1]
2.729115 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
2.729136 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×41a02d8a,seq=0×7a)
2.730083 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a81f0,seq=0×74)
2.730098 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
3.729410 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
3.729430 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×41a02d8a,seq=0×7b)
3.730364 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a81f0,seq=0×75)
3.730382 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
4.729580 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
4.729600 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×41a02d8a,seq=0×7c)
4.730377 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a81f0,seq=0×76)
4.730397 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
5.729921 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
5.729941 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×41a02d8a,seq=0×7d)
5.731016 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a81f0,seq=0×77)
5.731031 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
6.730170 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
6.730191 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×41a02d8a,seq=0×7e)
6.731200 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a81f0,seq=0×78)
6.731219 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

   - 抓取IPsec VPN的IKE协商包：

     ```
     diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
     ```

   - 抓取IPsec VPN的ESP加密数据包：

     ```
     diagnose sniffer packet any "host 101.1.1.1 and esp" 4
     ```

   - 抓取IPsec VPN的明文业务数据包：

     ```
     diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
     ```

   - 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

     ```
     FortiGate # config vpn ipsec phase1-interface
     FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
     FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
     FortiGate (BJ-OSPF-TO-SH) # end
     ```

2. 附Cisco Router IPsec VPN传统的Crypto MAP的配置方式（上述为VTI方式的IPsec VPN）。

```
FortiGate二阶段配置：

config vpn ipsec phase2-interface
    edit "VPN-TO-Side1"
        set phase1name "VPN-TO-Side1"
        set proposal 3des-md5 aes128-sha1
        set auto-negotiate enable
        set src-subnet 192.168.111.0 255.255.255.0
        set dst-subnet 192.168.112.0 255.255.255.0
    next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
end

Cisco_Router 配置:

hostname Side_Router
!
interface Ethernet0/0
ip address 101.100.1.1 255.255.255.0
ip nat outside
crypto map MY_MAP
!
interface Ethernet0/1
ip address 192.168.112.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 101.100.1.254

access-list 101 deny ip 192.168.112.0 0.0.0.255 192.168.111.0 0.0.0.255  //NAT Bypass掉VPN的流量
access-list 101 permit ip any any

ip nat inside source list 101 interface Ethernet0/0 overload
!
!
crypto isakmp policy 10
 encr aes 256
 hash sha
 authentication pre-share
 group 5

crypto isakmp key Fortinet123# address 202.106.1.1
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set MY-Trans esp-aes esp-sha-hmac
 mode tunnel
!
access-list 102 permit ip 192.168.112.0 0.0.0.255 192.168.111.0 0.0.0.255
!
crypto map MY_MAP 10 ipsec-isakmp
 set peer 202.106.1.1
 set transform-set MY-Trans
 set pfs group5
 match address 102
```

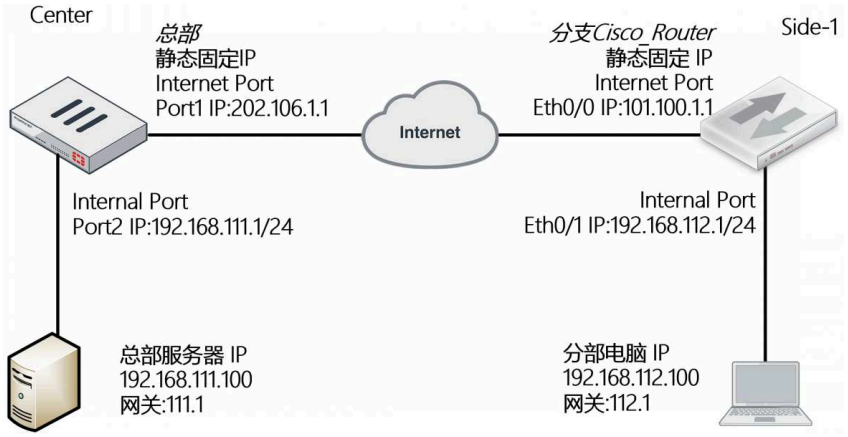

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与思科路由器建立IPSec VPN(IKE v2)

网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.111.0/24与192.168.112.0/24两个网段的通信。与思科路由器进行IPsec VPN（IKE v2）对接。

网络拓扑



配置要点

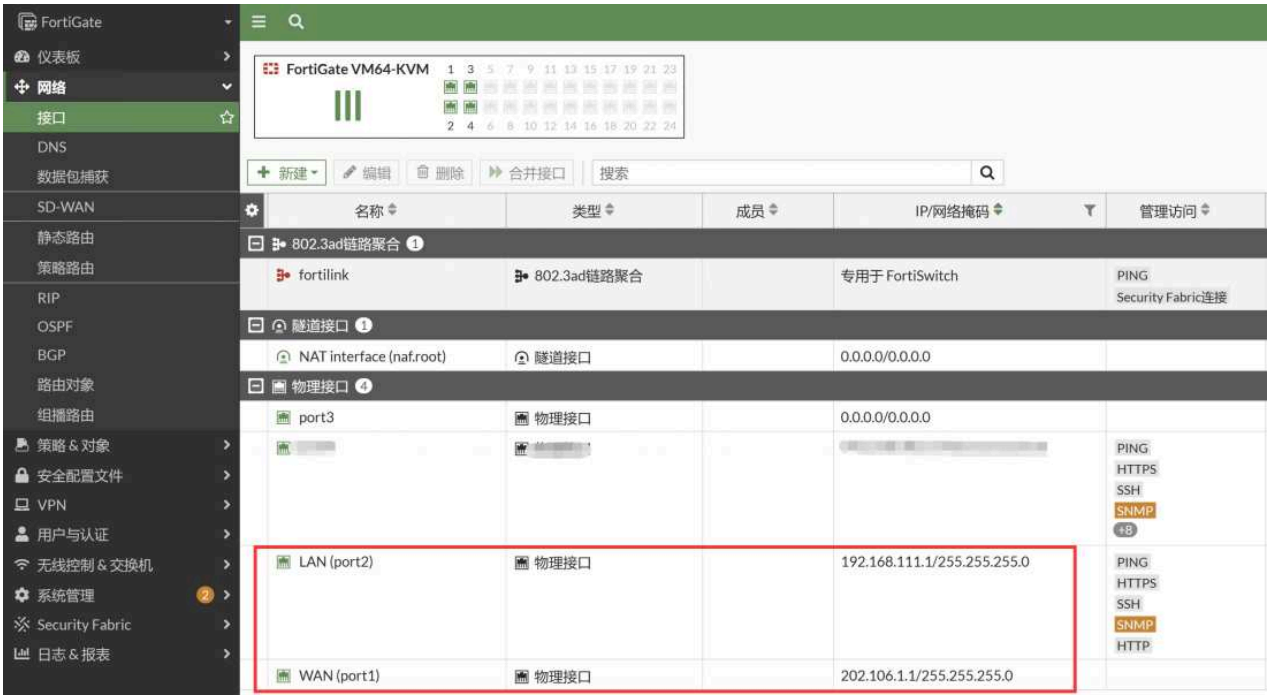
- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Cisco_Router
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。

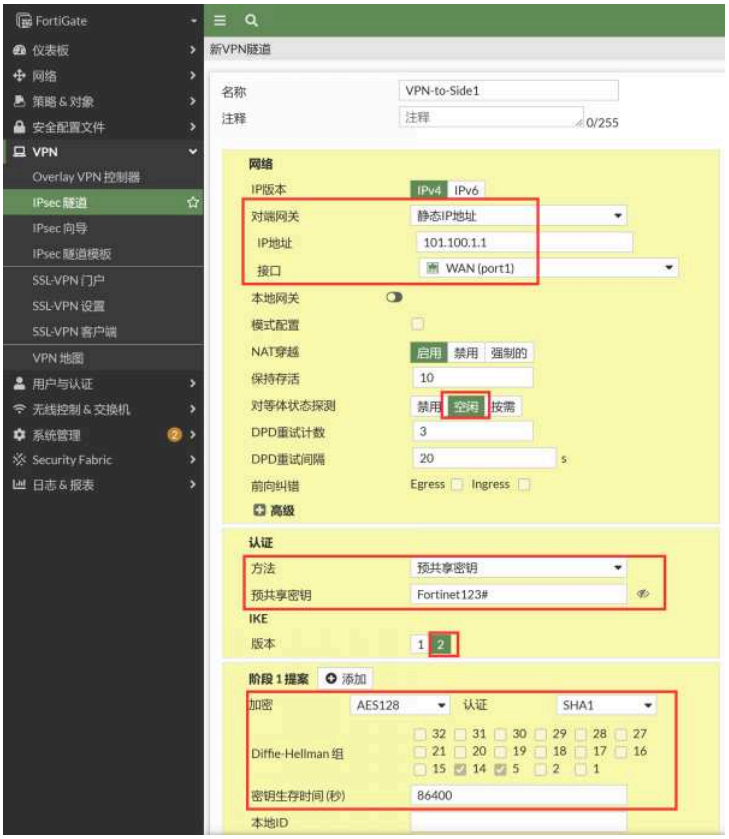


3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 配置网络、认证、第一阶段。

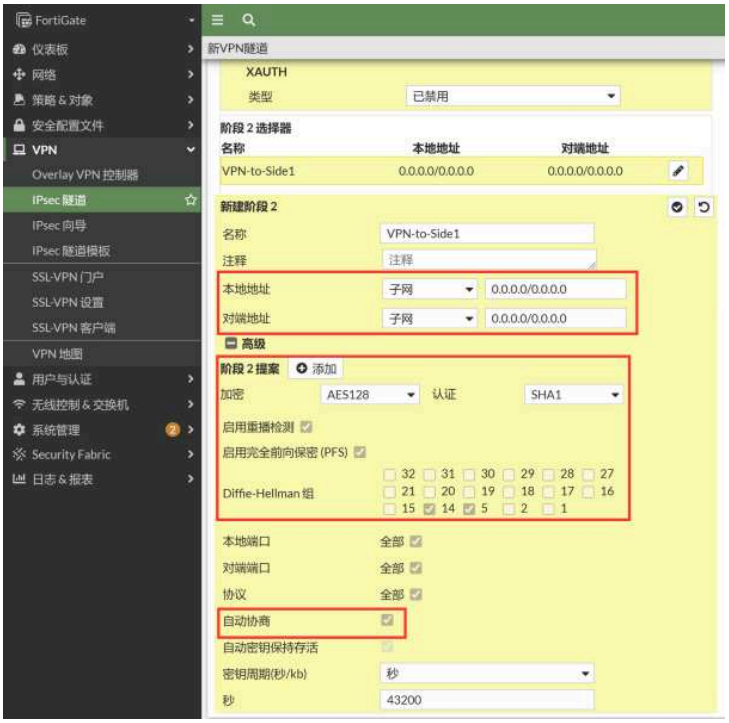
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase1-interface
    edit "VPN-to-Side1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha1
        set dpd on-idle
        set remote-gw 101.100.1.1
        set psksecret ENC
/HISpjoxUQ1RoRXahwT2OpZmuyYsDY818arB4Q93PztlW0oynlDWuKIk1WIAXFLNldoVFlgOOjBk9Bf9tc6LdI/BeD6CmRvgokNIKa5fVnVgxXLzHM
9fPGvtRXb362jpxZkMxuKHcNGVrJCimmjVGAS+gixHgh8mRLj5kaMAbyhNX1odwNNgxYcxqap5iAwncL3ZzQ==
    next
end
```

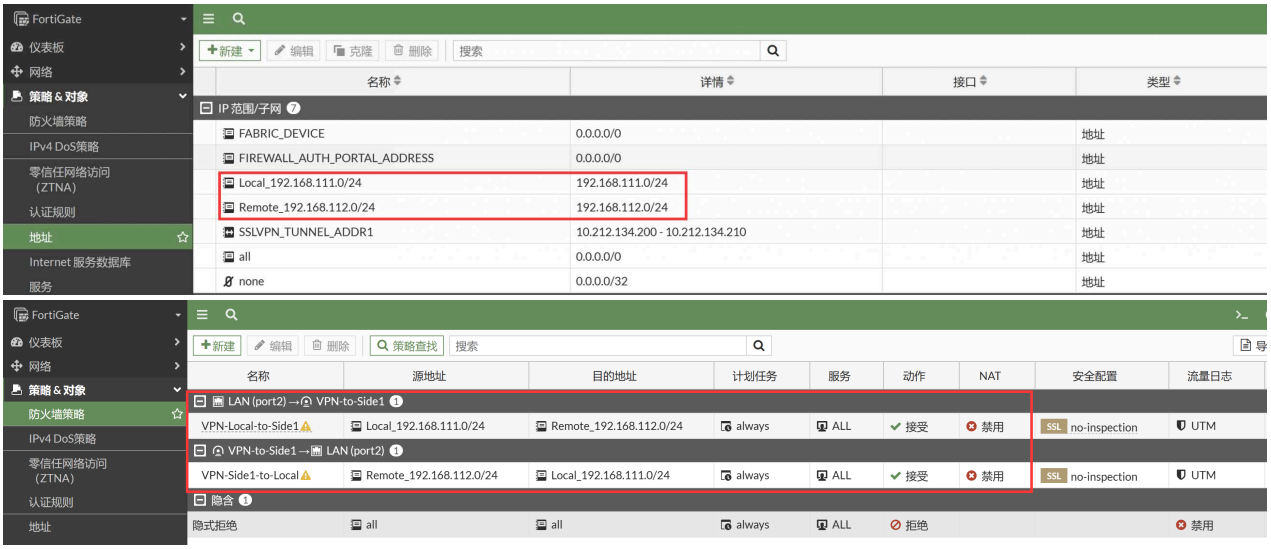
5. 配置第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase2-interface
    edit "VPN-to-Side1"
        set phase1name "VPN-to-Side1"
        set proposal aes128-sha1
        set auto-negotiate enable
    next
end
```

6. 配置VPN相关的网段地址对象和防火墙策略。




```
config firewall address
    edit "Local_192.168.111.0/24"
        set uuid 3bff7c90-8e7b-51ed-5311-ca9abc900a91
        set subnet 192.168.111.0 255.255.255.0
    next
    edit "Remote_192.168.112.0/24"
        set uuid 4647b500-8e7b-51ed-ea6f-c0ec2647bb42
        set subnet 192.168.112.0 255.255.255.0
    next
end

config firewall policy
    edit 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set name "VPN-Local-to-Side1"
        set uuid 7d1e7ce4-8e7b-51ed-19ea-001e373a03f3
        set srcintf "port2"
        set dstintf "VPN-to-Side1"
        set action accept
        set srcaddr "Local_192.168.111.0/24"
        set dstaddr "Remote_192.168.112.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "VPN-Side1-to-Local"
        set uuid 96c924d2-8e7b-51ed-f2d1-a61215d677f8
        set srcintf "VPN-to-Side1"
        set dstintf "port2"
        set action accept
        set srcaddr "Remote_192.168.112.0/24"
        set dstaddr "Local_192.168.111.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

7. 配置VPN业务网段的静态路由。




```
config router static
    edit 1
        set gateway 202.106.1.254
        set device "port1"
    next
    edit 2
        set dst 192.168.112.0 255.255.255.0
        set device "VPN-to-Side1"
    next
    edit 3
        set dst 192.168.112.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

Cisco Router

1. 基本上网配置。

```
interface Ethernet0/0
ip address 101.100.1.1 255.255.255.0
ip nat outside
no shutdown
!
interface Ethernet0/1
ip address 192.168.112.1 255.255.255.0
ip nat inside
no shutdown
!
ip nat inside source list 101 interface Ethernet0/0 overload
ip route 0.0.0.0 0.0.0.0 101.100.1.254
!
access-list 101 permit ip any any
```

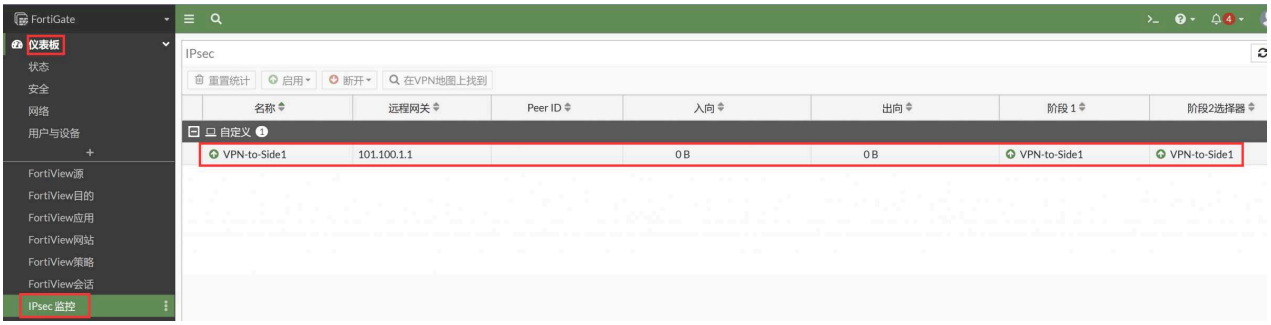

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. IPsec IKE v2的配置。

```
crypto ikev2 proposal MY-IKEV2-Proposal
 encryption aes-cbc-128
 integrity sha1
 group 5 14
 !
 crypto ikev2 policy MY_IKEV2_Policy
 proposal MY-IKEV2-Proposal
 !
 crypto ikev2 keyring MY_Keyring
 peer Center
   address 202.106.1.1
   pre-shared-key Fortinet123#
 !
 crypto ikev2 profile MY_IKEV2_Pro
 match identity remote address 202.106.1.1 255.255.255.255
 identity local address 101.100.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local MY_Keyring
 !
 crypto isakmp keepalive 10 periodic
 !
 crypto ipsec transform-set MY_Trans esp-aes esp-sha-hmac
 mode tunnel
 !
 crypto ipsec profile MY_IPsec_Pro
 set transform-set MY_Trans
 set pfs group5
 set ikev2-profile MY_IKEV2_Pro
 !
 interface Tunnel0
 ip address 1.1.1.2 255.255.255.0
 ip mtu 1400
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination 202.106.1.1
 tunnel protection ipsec profile MY_IPsec_Pro
 !
 ip route 192.168.111.0 255.255.255.0 Tunnel0 1.1.1.1
```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。



2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.106.1.254, port1, [1/0]
C       192.168.111.0/24 is directly connected, port2
S       192.168.112.0/24 [10/0] via VPN-to-Side1 tunnel 101.100.1.1, [1/0]
C       202.106.1.0/24 is directly connected, port1
```

3. FortiGate侧业务测试。

```
FortiGate # execute ping-options source 192.168.111.1

FortiGate # execute ping 192.168.112.1
PING 192.168.112.1 (192.168.112.1): 56 data bytes
64 bytes from 192.168.112.1: icmp_seq=0 ttl=255 time=1.0 ms
64 bytes from 192.168.112.1: icmp_seq=1 ttl=255 time=1.2 ms
64 bytes from 192.168.112.1: icmp_seq=2 ttl=255 time=0.9 ms
64 bytes from 192.168.112.1: icmp_seq=3 ttl=255 time=1.1 ms
64 bytes from 192.168.112.1: icmp_seq=4 ttl=255 time=1.0 ms

--- 192.168.112.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.0/1.2 ms
```

4. 查看FortiGate隧道状态。

```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Side1
version: 2
interface: port1 3
addr: 202.106.1.1:500 -> 101.100.1.1:500
tun_id: 101.100.1.1/::101.100.1.1
remote_location: 0.0.0.0
network-id: 0
created: 189s ago
PPK: no
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms
  id/spi: 371 c9520b1c2bc0e6c8/6aade7b829009948
  direction: initiator
  status: established 189-189s ago = 10ms
  proposal: aes128-sha1
  child: no
  SK_ei: 75237437cff25754-cf7db509c4681115
  SK_er: b32740a409713752-dee1a9e800220c20
  SK_ai: a51d7711574f8d4a-44ccb29646bb5227-6ea8727f
  SK_ar: 4e8c3e430012d7d7-bc227ae5d10bf045-205b82e5
  PPK: no
  message-id sent/recv: 11/0
  lifetime/rekey: 86400/85910
  DPD sent/recv: 0000000c/0000000c

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Side1 ver=2 serial=1 202.106.1.1:0->101.100.1.1:0 tun_id=101.100.1.1 tun_id6=::101.100.1.1
dst_mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overla0
proxyid_num=1 child_num=0 refcnt=4 ilast=3 olast=3 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=13
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Side1 proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=42694/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42898/43200
  dec: spi=148a8320 esp=aes key=16 2c299d148b78322997ffe3948ea8a426
       ah=sha1 key=20 c713f9ec7cecb6b6ffc80ce6fc407e8dc565a56f

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  enc: spi=2e03e37b esp=aes key=16 ef6e6e604f710a27393927db2be5c431
       ah=sha1 key=20 d80fc71d9b6947366693bff2a3c205b6b8b3b95d
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=101.100.1.1 npu_lgwy=202.106.1.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

5. Cisco_Router侧业务测试。

```
Router#ping 192.168.111.1 source 192.168.112.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.111.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.112.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/7 ms

Router#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
2         101.100.1.1/500       202.106.1.1/500       none/none            READY
      Encr: AES-CBC, keysize: 128, PRF: SHA1, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/261 sec
```

6. FortiGate侧抓包查看。

```
FortiGate # dia sni pa any "host 192.168.112.1 or host 101.100.1.1" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.112.1 or host 101.100.1.1]
1.980972 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
1.981265 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×2e03e37b,seq=0×2)
1.982549 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a8320,seq=0×1)
1.982619 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
2.981743 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
2.981768 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×2e03e37b,seq=0×3)
2.982852 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a8320,seq=0×2)
2.982869 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
3.982291 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
3.982312 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×2e03e37b,seq=0×4)
3.983316 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a8320,seq=0×3)
3.983333 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
4.983018 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
4.983039 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×2e03e37b,seq=0×5)
4.984193 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a8320,seq=0×4)
4.984212 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
5.983838 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
5.983860 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×2e03e37b,seq=0×6)
5.984866 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×148a8320,seq=0×5)
5.984884 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```

2. Cisco Router IPsec VPN传统的Crypto MAP的配置方式（上述为VTI方式的IPsec VPN）。

```
FortiGate 只需要修改IPsec VPN的第二阶段（添加明确的感兴趣流即可），其他的所有配置不变：
config vpn ipsec phase2-interface
    edit "VPN-TO-Side1"
        set phase1name "VPN-TO-Side1"
        set proposal 3des-md5 aes128-sha1
        set auto-negotiate enable
        set src-subnet 192.168.111.0 255.255.255.0
        set dst-subnet 192.168.112.0 255.255.255.0
    next
end

Cisco_Router配置：
hostname Side_Router
!
interface Ethernet0/0
ip address 101.100.1.1 255.255.255.0
ip nat outside
crypto map MY_MAP
!
interface Ethernet0/1
ip address 192.168.112.1 255.255.255.0
ip nat inside
!
ip route 0.0.0.0 0.0.0.0 101.100.1.254
access-list 101 deny ip 192.168.112.0 0.0.0.255 192.168.111.0 0.0.0.255 //NAT需bypass掉VPN流量
access-list 101 permit ip any any
ip nat inside source list 101 interface Ethernet0/0 overload
crypto ikev2 proposal MY-IKEV2-Proposal
encryption aes-cbc-128
integrity sha1
group 5 14
!
crypto ikev2 policy MY_IKEV2_Policy
proposal MY-IKEV2-Proposal
!
crypto ikev2 keyring MY_Keyring
peer Center
  address 202.106.1.1
  pre-shared-key Fortinet123#
!
crypto ikev2 profile MY_IKEV2_Pro
match identity remote address 202.106.1.1 255.255.255.255
identity local address 101.100.1.1
authentication remote pre-share
authentication local pre-share
keyring local MY_Keyring
!
crypto isakmp keepalive 10 periodic
!
crypto ipsec transform-set MY_Trans esp-aes esp-sha-hmac
mode tunnel
!
access-list 102 permit ip 192.168.112.0 0.0.0.255 192.168.111.0 0.0.0.255
!
crypto map MY_MAP 10 ipsec-isakmp
set peer 202.106.1.1
set transform-set MY_Trans
set pfs group5
set ikev2-profile MY_IKEV2_Pro
match address 102
```

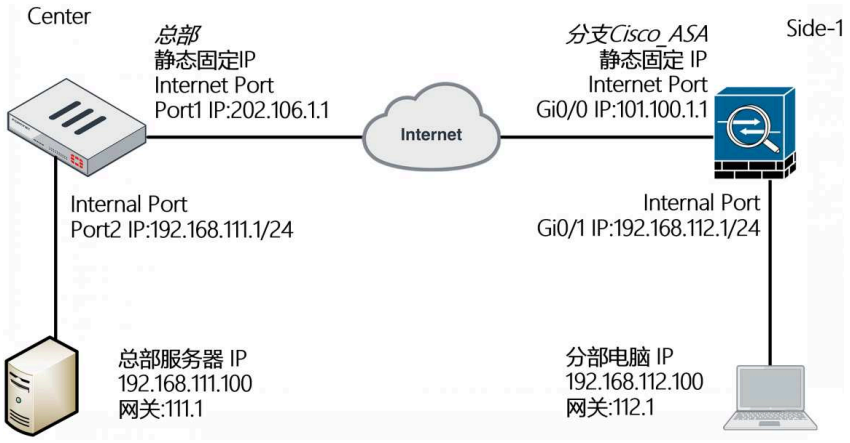

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与思科ASA防火墙建立IPSec VPN(IKE v1)

网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.111.0/24与192.168.112.0/24两个网段的通信。与思科ASA防火墙进行IPsec VPN（IKE v1）对接。

网络拓扑



配置要点

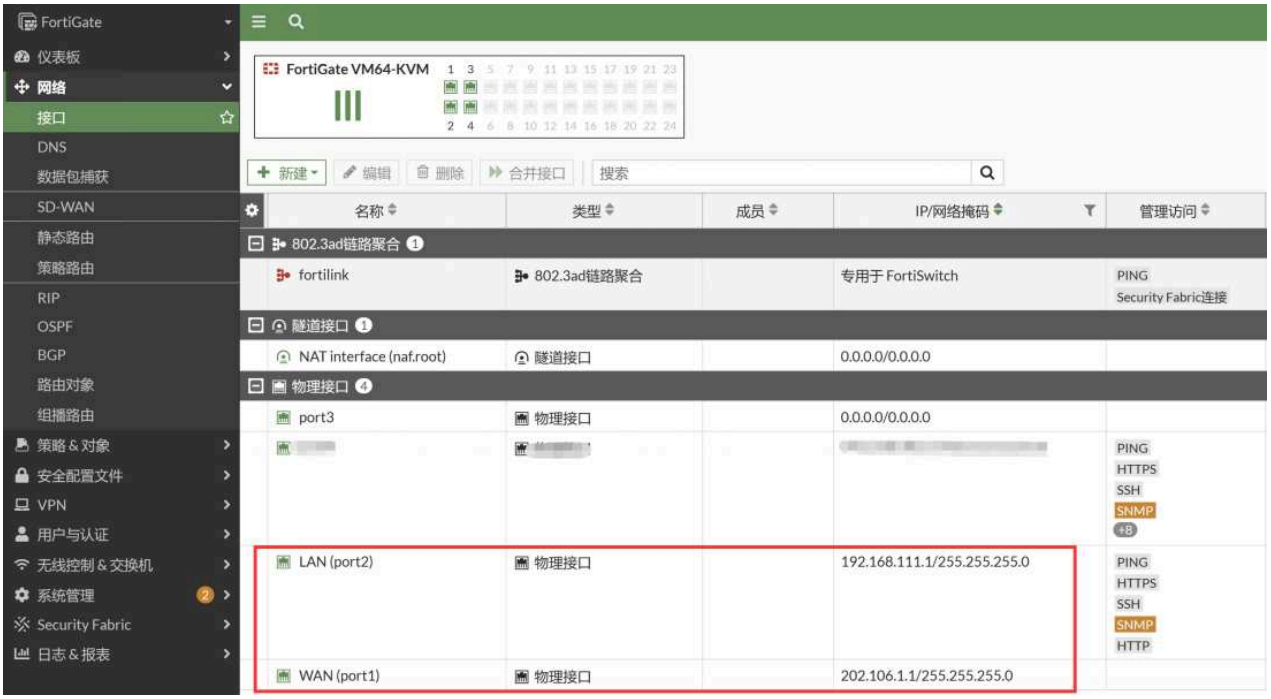
- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Cisco_ASA防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 配置网络、认证、第一阶段。

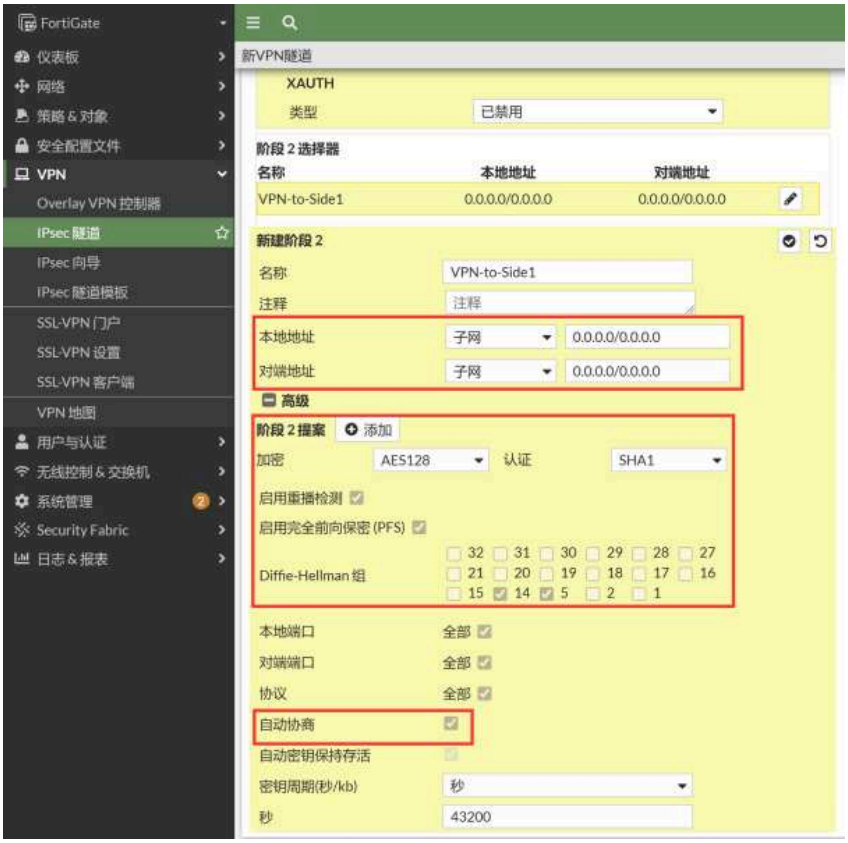
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase1-interface
    edit "VPN-to-Side1"
        set interface "port1"
        set peertype any
        set net-device disable
        set proposal aes256-sha1
        set dpd on-idle
        set dhgrp 14 5 2
        set remote-gw 101.100.1.1
        set psksecret ENC
/HISpjoxUQ1RoRXahwT2OpZmuyYsDY818arB4Q93PztlW0oynlDWuKIk1WIAXFLNldoVFlgOOjBk9Bf9tc6LdI/BeD6CmRvgokNIKa5fVnVgxXLzHM
9fPGvtRXb362jpxZkMxuKHcNGVrJCimmjVGAS+gixHgh8mRLj5kaMAbyhNX1odwNNgxYcxqap5iAwncL3ZzQ==
    next
end
```

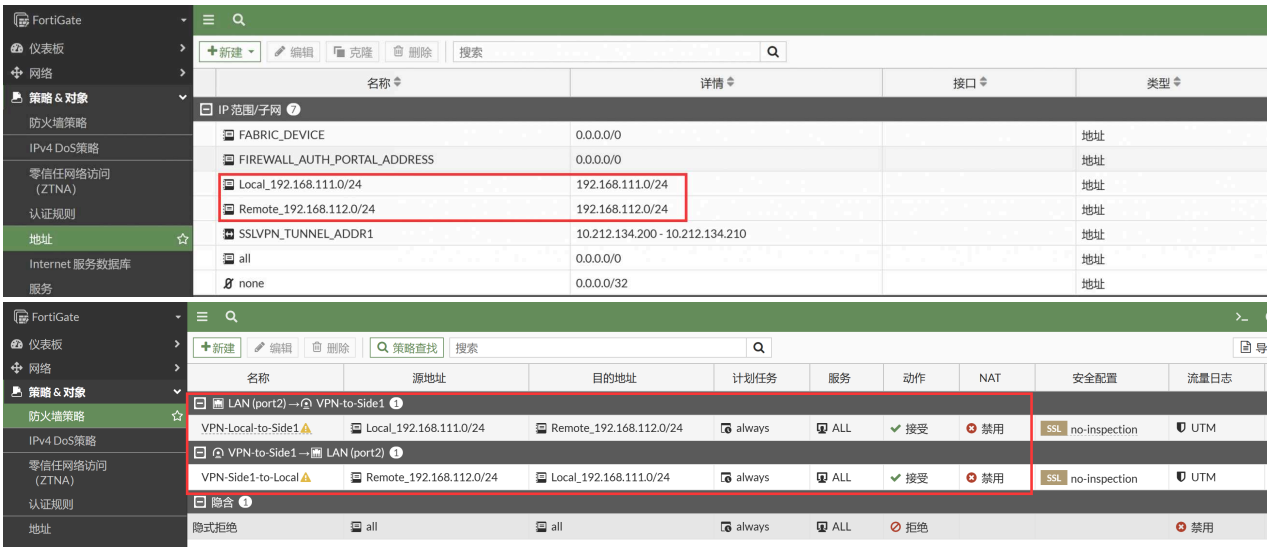
5. 配置第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase2-interface
    edit "VPN-to-Side1"
        set phase1name "VPN-to-Side1"
        set proposal aes128-sha1
        set auto-negotiate enable
    next
end
```

6. 配置VPN相关的网段地址对象和防火墙策略。

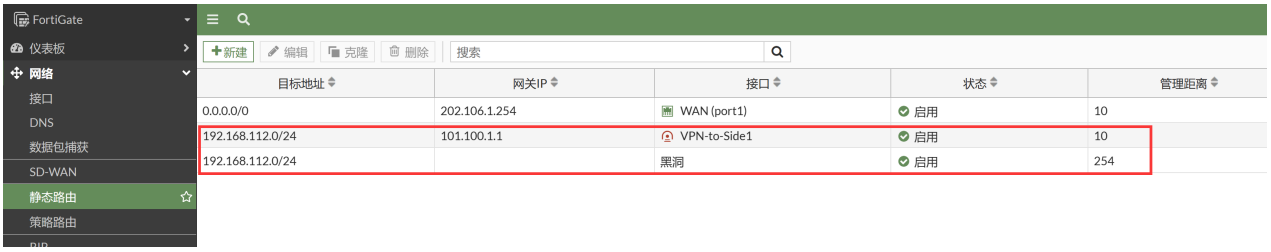



```
config firewall address
    edit "Local_192.168.111.0/24"
        set uuid 3bff7c90-8e7b-51ed-5311-ca9abc900a91
        set subnet 192.168.111.0 255.255.255.0
    next
    edit "Remote_192.168.112.0/24"
        set uuid 4647b500-8e7b-51ed-ea6f-c0ec2647bb42
        set subnet 192.168.112.0 255.255.255.0

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    next
end

config firewall policy
    edit 1
        set name "VPN-Local-to-Side1"
        set uuid 7d1e7ce4-8e7b-51ed-19ea-001e373a03f3
        set srcintf "port2"
        set dstintf "VPN-to-Side1"
        set action accept
        set srcaddr "Local_192.168.111.0/24"
        set dstaddr "Remote_192.168.112.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "VPN-Side1-to-Local"
        set uuid 96c924d2-8e7b-51ed-f2d1-a61215d677f8
        set srcintf "VPN-to-Side1"
        set dstintf "port2"
        set action accept
        set srcaddr "Remote_192.168.112.0/24"
        set dstaddr "Local_192.168.111.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

7. 配置VPN业务网段的静态路由。




```
config router static
    edit 1
        set gateway 202.106.1.254
        set device "port1"
    next
    edit 2
        set dst 192.168.112.0 255.255.255.0
        set device "VPN-to-Side1"
    next
    edit 3
        set dst 192.168.112.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

Cisco Router

1. 基本上网配置。

```
 interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 101.100.1.1 255.255.255.0
 no shutdown
 !
 interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 192.168.112.1 255.255.255.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

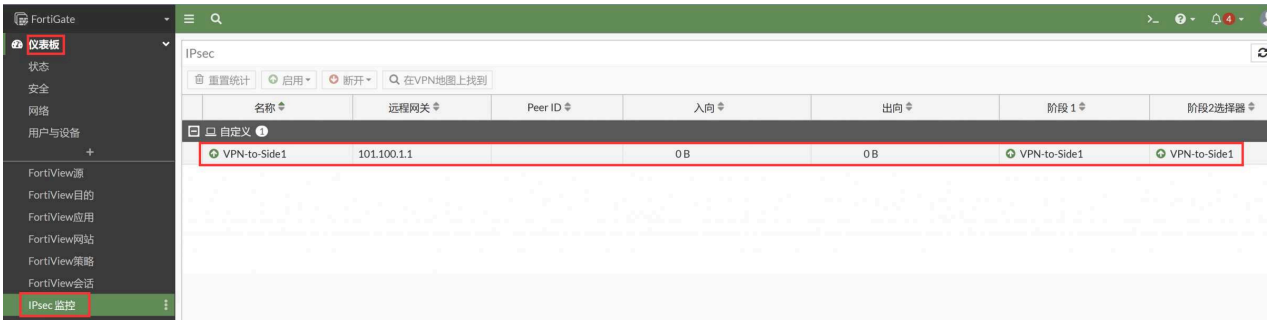
```
 no shutdown
 !
 route Outside 0.0.0.0 0.0.0.0 101.100.1.254

 object network Inside_Net_192.168.112.0
 subnet 192.168.112.0 255.255.255.0

 object network Inside_Net_192.168.112.0
 nat (Inside,Outside) dynamic interface

 policy-map global_policy
 class inspection_default
   inspect icmp
   inspect icmp error
```

2. IPsec IKE v1的配置。

```
crypto ikev1 enable Outside

 crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 86400

 tunnel-group 202.106.1.1 type ipsec-l2l
 tunnel-group 202.106.1.1 ipsec-attributes
 ikev1 pre-shared-key Fortinet123#
 !
 crypto ipsec ikev1 transform-set MY_Trans esp-aes esp-sha-hmac

 crypto ipsec profile MY_IPsec_Pro
 set ikev1 transform-set MY_Trans
 set security-association lifetime seconds 43200
 set security-association lifetime kilobytes unlimited
 set pfs group5
 !
 interface Tunnel0
 nameif VPN
 ip address 1.1.1.2 255.255.255.0
 tunnel source interface Outside
 tunnel destination 202.106.1.1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile MY_IPsec_Pro
 !
 management-access Inside    //为了可以让Inside接口可以被ping通
 !
 route VPN 192.168.111.0 255.255.255.0 1.1.1.1
```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。



2. 查看FortiGate的路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.106.1.254, port1, [1/0]
C       192.168.111.0/24 is directly connected, port2
S       192.168.112.0/24 [10/0] via VPN-to-Side1 tunnel 101.100.1.1, [1/0]
C       202.106.1.0/24 is directly connected, port1
```

3. FortiGate侧业务测试。

```
FortiGate # execute ping-options source 192.168.111.1

FortiGate # execute ping 192.168.112.1
PING 192.168.112.1 (192.168.112.1): 56 data bytes
64 bytes from 192.168.112.1: icmp_seq=0 ttl=255 time=1.0 ms
64 bytes from 192.168.112.1: icmp_seq=1 ttl=255 time=1.2 ms
64 bytes from 192.168.112.1: icmp_seq=2 ttl=255 time=0.9 ms
64 bytes from 192.168.112.1: icmp_seq=3 ttl=255 time=1.1 ms
64 bytes from 192.168.112.1: icmp_seq=4 ttl=255 time=1.0 ms

--- 192.168.112.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.0/1.2 ms
```

4. 查看FortiGate隧道状态。

```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Side1
version: 1
interface: port1 3
addr: 202.106.1.1:500 → 101.100.1.1:500
tun_id: 101.100.1.1/::101.100.1.1
remote_location: 0.0.0.0
network-id: 0
created: 142s ago
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms
  id/spi: 71 e412d996a3f9731b/a23fe38afa532c1b
  direction: initiator
  status: established 142-142s ago = 10ms
  proposal: aes256-sha1
  key: 608f0ca220d02d6c-cd0af89676672e4a-c534a6a6c28ef467-15adfbe008693366
  lifetime/rekey: 86400/85957
  DPD sent/recv: 00000000/702e146a

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Side1 ver=1 serial=1 202.106.1.1:0→101.100.1.1:0 tun_id=101.100.1.1 tun_id6=::101.100.1.1
dst_mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=3 olast=3 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=2
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Side1 proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=28338/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=28497/28800
  dec: spi=24c2aad2 esp=aes key=16 5568087b376e909df121ee5f0c0bcf6c
       ah=sha1 key=20 c423673ee77d191b93bea09089d120ab841bf14c
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  enc: spi=cd21cdff esp=aes key=16 60e173bbd4bff20493566a2e0209abfd
       ah=sha1 key=20 50122d2f90bbb2c02e875084e81d5e1960995b8a
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=101.100.1.1 npu_lgwy=202.106.1.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

5. Cisco_Router侧业务测试。

```
Router#ping 192.168.111.1 source 192.168.112.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.111.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.112.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/7 ms

ciscoasa# show crypto ikev1 sa
IKEv1 SAs:
   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1   IKE Peer: 202.106.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

6. FortiGate侧抓包查看。

```
FortiGate # dia sni pa any "host 192.168.112.1 or host 101.100.1.1" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.112.1 or host 101.100.1.1]
2.692454 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
2.692475 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×cd21cdff,seq=0×16)
2.694379 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2aad2,seq=0×15)
2.694394 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
3.692845 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
3.692865 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×cd21cdff,seq=0×17)
3.694116 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2aad2,seq=0×16)
3.694130 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
4.693332 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
4.693356 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×cd21cdff,seq=0×18)
4.695841 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2aad2,seq=0×17)
4.695863 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
5.693612 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
5.693634 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×cd21cdff,seq=0×19)
5.695531 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2aad2,seq=0×18)
5.695548 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
6.694338 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
6.694359 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×cd21cdff,seq=0×1a)
6.696289 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2aad2,seq=0×19)
6.696307 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```

2. 附Cisco ASA IPsec VPN传统的Crypto MAP的配置方式（上述为VTI方式的IPsec VPN）。

```
FortiGate 只需要修改IPsec VPN的第二阶段（添加明确的感兴趣流即可），其他的所有配置不变：
config vpn ipsec phase2-interface
    edit "VPN-TO-Side1"
        set phase1name "VPN-TO-Side1"
        set proposal 3des-md5 aes128-sha1
        set auto-negotiate enable
        set src-subnet 192.168.111.0 255.255.255.0
        set dst-subnet 192.168.112.0 255.255.255.0
    next
end

Cisco_ASA配置：
hostname ASA-FW
!
interface GigabitEthernet0/0
nameif Outside
security-level 0
ip address 101.100.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif Inside
security-level 100
ip address 192.168.112.1 255.255.255.0
!
route Outside 0.0.0.0 0.0.0.0 101.100.1.254 1

object network Inside_Net_192.168.112.0
subnet 192.168.112.0 255.255.255.0

object network Remote_VPN_Net_192.168.111.0
subnet 192.168.111.0 255.255.255.0

object network Inside_Net_192.168.112.0
nat (Inside,Outside) dynamic interface

policy-map global_policy
class inspection_default
  inspect icmp
  inspect icmp error

crypto ikev1 enable Outside

crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 86400

tunnel-group 202.106.1.1 type ipsec-l2l
tunnel-group 202.106.1.1 ipsec-attributes
 ikev1 pre-shared-key Fortinet123#

crypto ipsec ikev1 transform-set MY_Trans_1 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set MY_Trans_2 esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set MY_Trans_3 esp-aes-192 esp-sha-hmac

access-list VPN-Traffic extended permit ip object Inside_Net_192.168.112.0 object Remote_VPN_Net_192.168.111.0

crypto map MY_IPsec_MAP 10 match address VPN-Traffic
crypto map MY_IPsec_MAP 10 set pfs group5
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
crypto map MY_IPsec_MAP 10 set peer 202.106.1.1
crypto map MY_IPsec_MAP 10 set ikev1 transform-set MY_Trans_1 MY_Trans_2 MY_Trans_3
crypto map MY_IPsec_MAP interface Outside

nat (Inside,Outside) source static Inside_Net_192.168.112.0 Inside_Net_192.168.112.0 destination static
Remote_VPN_Net_192.168.111.0 Remote_VPN_Net_192.168.111.0 //使用Twice NAT将VPN流量在NAT中Bypass掉
```

注意事项

1. 默认配置下，FortiGate只使用时间到期作为二阶段rekey的条件，当二阶段配置的时间倒计时结束，则发起二阶段的rekey。



2. FortiGate可以使用流量作为rekey的条件，也可以同时使用时间（秒）和流量（KB）同时作为rekey的条件，当其中一个条件达到配置的数量时，则发起二阶段rekey。



3. 对于Cisco ASA防火墙，默认配置下同时使用时间（秒）和流量（KB）同时作为rekey的条件，默认的配置为4608000 KB和3600秒。当其中一个条件达到配置的数量时，则发起二阶段rekey。这样可能会导致IPSec隧道二阶段频繁的rekey。

4. 通过如下命令配置Cisco ASA只使用时间作为二阶段rekey条件。

```
crypto ipsec profile MY_IPsec_Pro
set security-association lifetime kilobytes unlimited
```

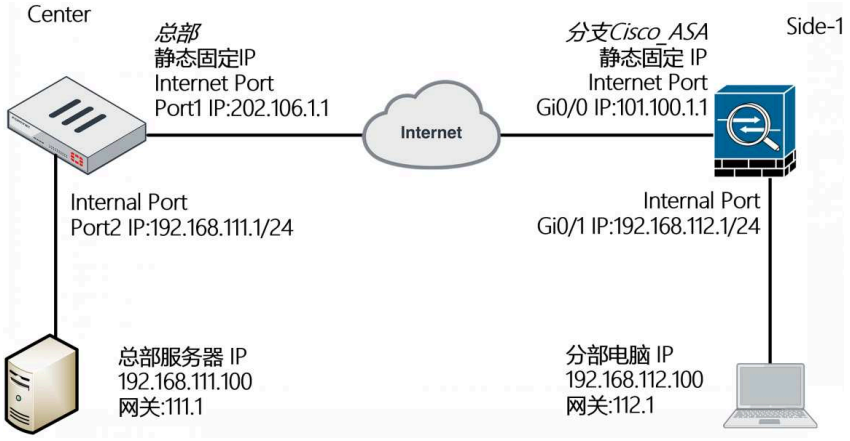

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与思科ASA防火墙建立IPSec VPN(IKE v2)

网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.111.0/24与192.168.112.0/24两个网段的通信。与思科ASA防火墙进行IPsec VPN（IKE v2）对接。

网络拓扑



配置要点

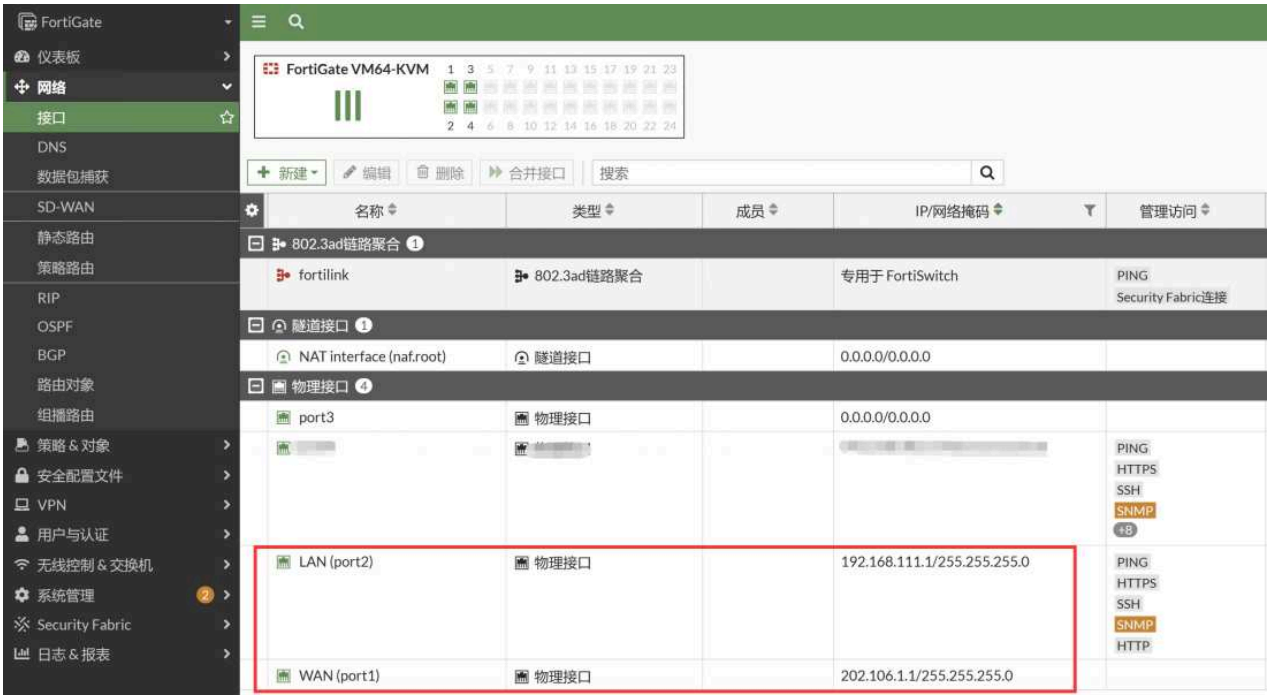
- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Cisco_ASA防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。

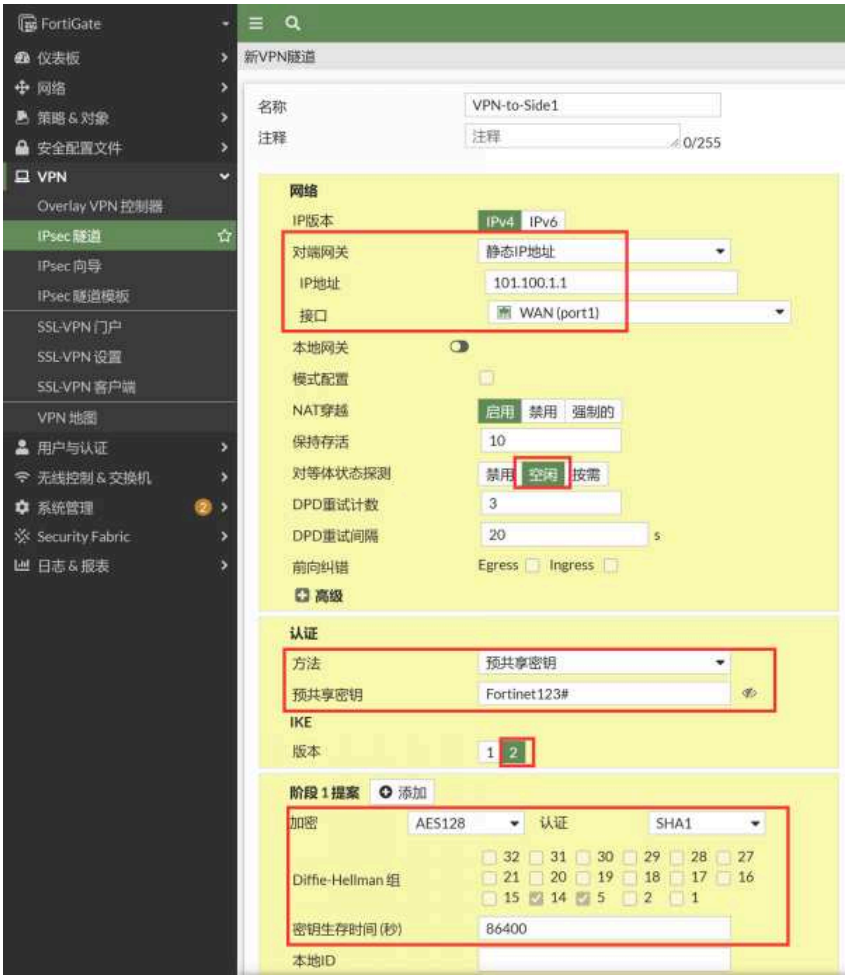


3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 配置网络、认证、第一阶段。

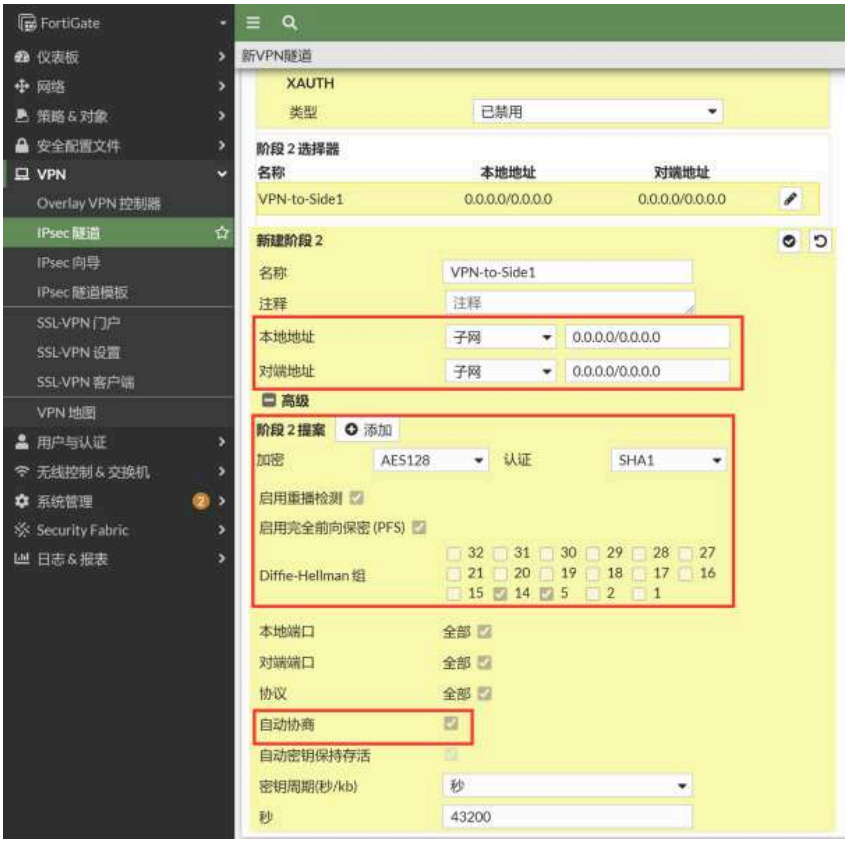
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase1-interface
    edit "VPN-to-Side1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha1
        set dpd on-idle
        set remote-gw 101.100.1.1
        set psksecret ENC
/HISpjoxUQ1RoRXahwT2OpZmuyYsDY818arB4Q93PztlW0oynlDWuKIk1WIAXFLNldoVFlgOOjBk9Bf9tc6LdI/BeD6CmRvgokNIKa5fVnVgxXLzHM
9fPGvtRXb362jpxZkMxuKHcNGVrJCimmjVGAS+gixHgh8mRLj5kaMAbyhNX1odwNNgxYcxqap5iAwncL3ZzQ==
    next
end
```

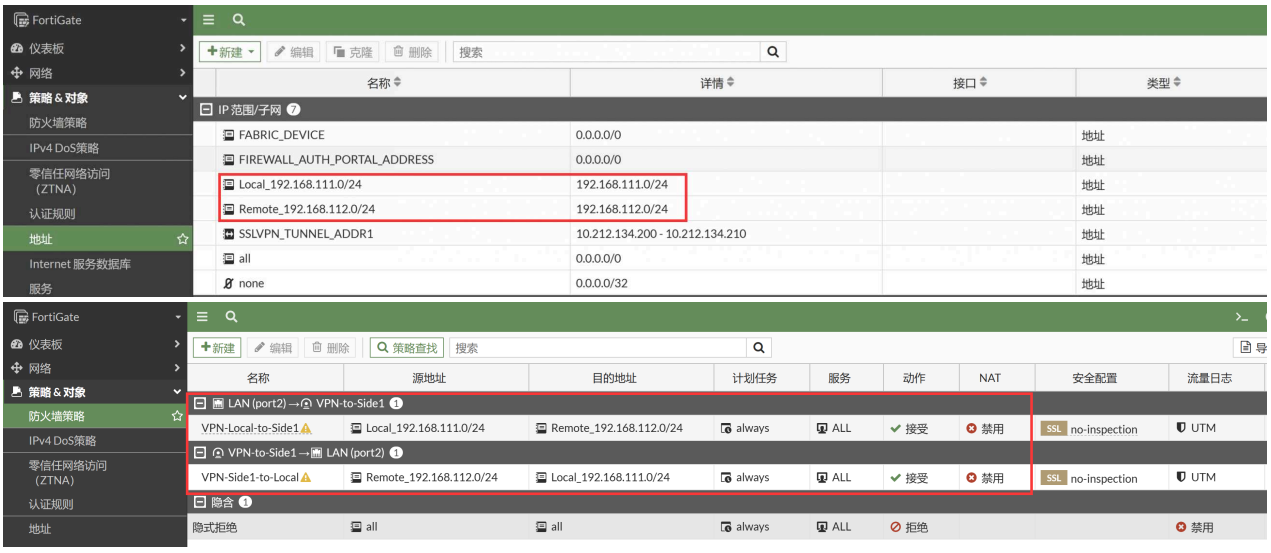
5. 配置第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config vpn ipsec phase2-interface
    edit "VPN-to-Side1"
        set phase1name "VPN-to-Side1"
        set proposal aes128-sha1
        set auto-negotiate enable
    next
end
```

6. 配置VPN相关的网段地址对象和防火墙策略。




```
config firewall address
    edit "Local_192.168.111.0/24"
        set subnet 192.168.111.0 255.255.255.0
    next
    edit "Remote_192.168.112.0/24"
        set subnet 192.168.112.0 255.255.255.0
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall policy
    edit 1
        set name "VPN-Local-to-Side1"
        set srcintf "port2"
        set dstintf "VPN-to-Side1"
        set action accept
        set srcaddr "Local_192.168.111.0/24"
        set dstaddr "Remote_192.168.112.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "VPN-Side1-to-Local"
        set srcintf "VPN-to-Side1"
        set dstintf "port2"
        set action accept
        set srcaddr "Remote_192.168.112.0/24"
        set dstaddr "Local_192.168.111.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

7. 配置VPN业务网段的静态路由。




```
config router static
    edit 1
        set gateway 202.106.1.254
        set device "port1"
    next
    edit 2
        set dst 192.168.112.0 255.255.255.0
        set device "VPN-to-Side1"
    next
    edit 3
        set dst 192.168.112.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

Cisco Router

1. 基本上网配置。

```
 interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 101.100.1.1 255.255.255.0
 no shutdown
 !
 interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 192.168.112.1 255.255.255.0
 no shutdown
 !
 route Outside 0.0.0.0 0.0.0.0 101.100.1.254
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

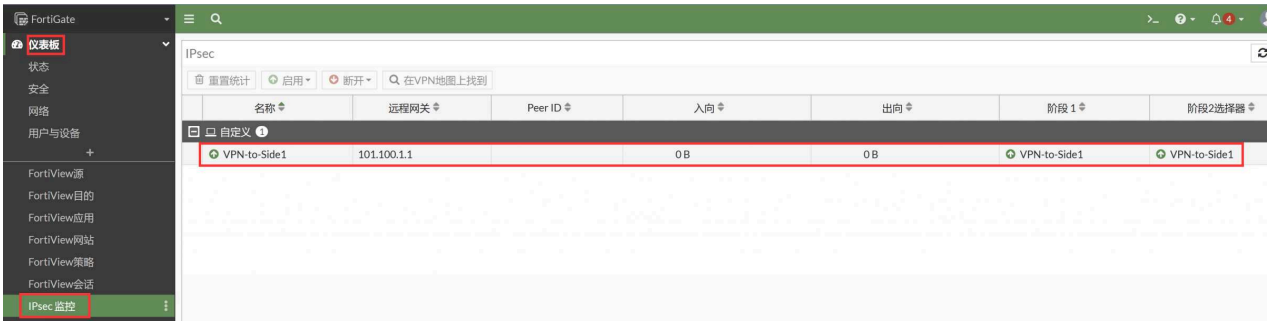
```
object network Inside_Net_192.168.112.0
subnet 192.168.112.0 255.255.255.0

object network Inside_Net_192.168.112.0
nat (Inside,Outside) dynamic interface

policy-map global_policy
class inspection_default
  inspect icmp
  inspect icmp error
```

2. IPsec IKEv2的配置。

```
crypto ikev2 enable Outside

crypto ikev2 policy 10
 encryption aes-256 aes-192 aes 3des
 integrity sha256 sha md5
 group 14 5
 prf sha256 sha md5
 lifetime seconds 86400
!
tunnel-group 202.106.1.1 type ipsec-l2l
tunnel-group 202.106.1.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Fortinet123#
 ikev2 local-authentication pre-shared-key Fortinet123#
!
crypto ipsec ikev2 ipsec-proposal MY_IPsec_Proposal
 protocol esp encryption aes-256 aes-192 aes 3des
 protocol esp integrity sha-256 sha-1 md5

crypto ipsec profile MY_IPsec_Profile
 set ikev2 ipsec-proposal MY_IPsec_Proposal
 set security-association lifetime seconds 43200
 set security-association lifetime kilobytes unlimited
 set pfs group5

interface Tunnel0
nameif VPN
ip address 1.1.1.2 255.255.255.0
tunnel source interface Outside
tunnel destination 202.106.1.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile MY_IPsec_Profile
!
management-access Inside     //为了可以让Inside接口可以被ping通。
!
route VPN 192.168.111.0 255.255.255.0 1.1.1.1
```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。



2. 查看FortiGate的路由表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.106.1.254, port1, [1/0]
C       192.168.111.0/24 is directly connected, port2
S       192.168.112.0/24 [10/0] via VPN-to-Side1 tunnel 101.100.1.1, [1/0]
C       202.106.1.0/24 is directly connected, port1
```

3. FortiGate侧业务测试。

```
FortiGate # execute ping-options source 192.168.111.1

FortiGate # execute ping 192.168.112.1
PING 192.168.112.1 (192.168.112.1): 56 data bytes
64 bytes from 192.168.112.1: icmp_seq=0 ttl=255 time=1.0 ms
64 bytes from 192.168.112.1: icmp_seq=1 ttl=255 time=1.2 ms
64 bytes from 192.168.112.1: icmp_seq=2 ttl=255 time=0.9 ms
64 bytes from 192.168.112.1: icmp_seq=3 ttl=255 time=1.1 ms
64 bytes from 192.168.112.1: icmp_seq=4 ttl=255 time=1.0 ms

--- 192.168.112.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.0/1.2 ms
```

4. 查看FortiGate隧道状态。

```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Side1
version: 2
interface: port1 3
addr: 202.106.1.1:500 → 101.100.1.1:500
tun_id: 101.100.1.1/::101.100.1.1
remote_location: 0.0.0.0
network-id: 0
created: 36s ago
PPK: no
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms
  id/spi: 134 11aa3d39fcd93c44/852e6b5523a3345d
  direction: initiator
  status: established 36-36s ago = 0ms
  proposal: aes256-sha1
  child: no
  SK_ei: 88ce24e4a2611994-bffb25c2d0ba869b-57e6a55b89508df1-b570966836823c48
  SK_er: 0dadc56cac99ad39-b507dff27d037bb1-33c8ef3555410c03-7e8383322010cb35
  SK_ai: 7481bc53c4d20b62-c9770a0695f2a2a1-0209ff70
  SK_ar: 150cadb3c206c29d-49f33c62d553fb0c-f87d3bf1
  PPK: no
  message-id sent/recv: 2/3
  lifetime/rekey: 86400/86063
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Side1 ver=2 serial=1 202.106.1.1:0→101.100.1.1:0 tun_id=101.100.1.1 tun_id6=::101.100.1.1
dst_mtu=1500 dpd-link=on weight=1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=12 olast=12 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=37
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Side1 proto=0 sa=1 ref=2 serial=1 auto-negotiate
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=42847/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=24c2ab68 esp=aes key=16 3de80d9ea806f7d02167116ef729d135
       ah=sha1 key=20 f05476e4cee8fab25811105c92ea6e5ccf8fd1e4
  enc: spi=0dd3fc4c esp=aes key=16 def29e57dd9b54801a3f31b9a6a920cb
       ah=sha1 key=20 adbfb39e5fe95fb385215da6a73113902bed6c4f
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=101.100.1.1 npu_lgwy=202.106.1.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

5. Cisco_Router侧业务测试。

```
ciscoasa#ping 192.168.111.1 source 192.168.112.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.111.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.112.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/7 ms

ciscoasa(config)# show crypto ikev2 sa
IKEv2 SAs:
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                                           Remote
Status         Role
 38557965 101.100.1.1/500                                 202.106.1.1/500
READY    RESPONDER
      Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/73 sec
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0×dd3fc4c/0×24c2ab68
```

6. FortiGate侧抓包查看。

```
FortiGate # dia sni pa any "host 192.168.112.1 or host 101.100.1.1" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.112.1 or host 101.100.1.1]
9.068586 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
9.068748 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×0dd3fc4c,seq=0×2)
9.072619 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2ab68,seq=0×1)
9.072669 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
10.069075 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
10.069097 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×0dd3fc4c,seq=0×3)
10.071135 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2ab68,seq=0×2)
10.071155 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
11.069398 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
11.069418 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×0dd3fc4c,seq=0×4)
11.071456 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2ab68,seq=0×3)
11.071483 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
12.069674 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
12.069695 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×0dd3fc4c,seq=0×5)
12.071430 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2ab68,seq=0×4)
12.071450 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
13.069841 VPN-to-Side1 out 192.168.111.1 → 192.168.112.1: icmp: echo request
13.069861 port1 out 202.106.1.1 → 101.100.1.1: ESP(spi=0×0dd3fc4c,seq=0×6)
13.071790 port1 in 101.100.1.1 → 202.106.1.1: ESP(spi=0×24c2ab68,seq=0×5)
13.071809 VPN-to-Side1 in 192.168.112.1 → 192.168.111.1: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```

2. Cisco Router IPsec VPN传统的Crypto MAP的配置方式（上述为VTI方式的IPsec VPN）。

```
FortiGate 只需要修改IPsec VPN的第二阶段（添加明确的感兴趣流即可），其他的所有配置不变：
config vpn ipsec phase2-interface
    edit "VPN-TO-Side1"
        set phase1name "VPN-TO-Side1"
        set proposal 3des-md5 aes128-sha1
        set auto-negotiate enable
        set src-subnet 192.168.111.0 255.255.255.0
        set dst-subnet 192.168.112.0 255.255.255.0
    next
end

Cisco_ASA配置：
hostname ASA-FW
!
interface GigabitEthernet0/0
nameif Outside
security-level 0
ip address 101.100.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif Inside
security-level 100
ip address 192.168.112.1 255.255.255.0
!
route Outside 0.0.0.0 0.0.0.0 101.100.1.254 1
object network Inside_Net_192.168.112.0
subnet 192.168.112.0 255.255.255.0
object network Inside_Net_192.168.112.0
nat (Inside,Outside) dynamic interface
object network Remote_VPN_Net_192.168.111.0
subnet 192.168.111.0 255.255.255.0
policy-map global_policy
class inspection_default
  inspect icmp
  inspect icmp error
crypto ikev2 enable Outside
crypto ikev2 policy 10
 encryption aes-256 aes-192 aes 3des
 integrity sha256 sha md5
 group 14 5
 prf sha256 sha md5
 lifetime seconds 86400
tunnel-group 202.106.1.1 type ipsec-l2l
tunnel-group 202.106.1.1 ipsec-attributes
 ikev2 remote-authentication pre-shared-key Fortinet123#
 ikev2 local-authentication pre-shared-key Fortinet123#
crypto ipsec ikev2 ipsec-proposal MY_IPsec_Proposal
 protocol esp encryption aes-256 aes-192 aes 3des
 protocol esp integrity sha-256 sha-1 md5
access-list VPN-Traffic extended permit ip object Inside_Net_192.168.112.0 object Remote_VPN_Net_192.168.111.0
crypto map MY_IPsec_MAP 10 match address VPN-Traffic
crypto map MY_IPsec_MAP 10 set pfs group5
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
crypto map MY_IPsec_MAP 10 set peer 202.106.1.1
crypto map MY_IPsec_MAP 10 set ikev2 ipsec-proposal MY_IPsec_Proposal
crypto map MY_IPsec_MAP interface Outside
nat (Inside,Outside) source static Inside_Net_192.168.112.0 Inside_Net_192.168.112.0 destination static
Remote_VPN_Net_192.168.111.0 Remote_VPN_Net_192.168.111.0 //使用Twice NAT将VPN流量在NAT中Bypass掉
```

注意事项

1. 默认配置下，FortiGate只使用时间到期作为二阶段rekey的条件，当二阶段配置的时间倒计时结束，则发起二阶段的rekey。



2. FortiGate可以使用流量作为rekey的条件，也可以同时使用时间（秒）和流量（KB）同时作为rekey的条件，当其中一个条件达到配置的数量时，则发起二阶段rekey。



3. 对于Cisco ASA防火墙，默认配置下同时使用时间（秒）和流量（KB）同时作为rekey的条件，默认的配置为4608000 KB和3600秒。当其中一个条件达到配置的数量时，则发起二阶段rekey。这样可能会导致IPSec隧道二阶段频繁的rekey。

4. 通过如下命令配置Cisco ASA只使用时间作为二阶段rekey条件。

```
crypto ipsec profile MY_IPsec_Pro
set security-association lifetime kilobytes unlimited
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与华为USG6000V防火墙建立IPSec VPN

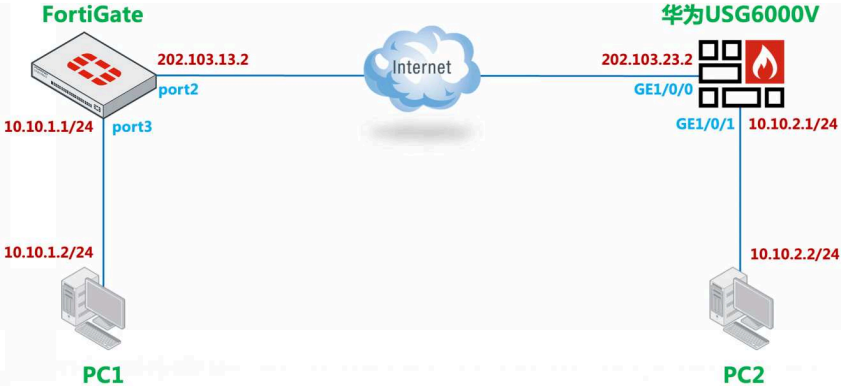
网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与10.10.2.0/24两个网段的通信。与华为USG6000V防火墙进行IPsec VPN（IKE v1）对接。

华为USG6000V防火墙版本：

```bash
<USG6000V2>display version
2023-04-06 17:43:15.520 +08:00
Huawei Versatile Routing Platform Software
VRP (R) Software, Version 5.170 (USG6000V2 V500R005C00SPC100)
Copyright (C) 2014-2018 Huawei Technologies Co., Ltd.
USG6000V2 uptime is 0 week, 0 day, 2 hours, 40 minutes
IPS Signature Database Version   : 2018070605
IPS Engine Version               : V200R005C00SPC037
AV Signature Database Version    :
SA Signature Database Version    : 2018062700
C&C Domain Name Database Version :
FILE Reputation Database Version :
Location Database Version        : 2014010414
```

网络拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置华为USG6000V防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略。

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 如图配置网络、认证、第一阶段、第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

不像和Cisco/PA/Juniper/山石使用虚拟接口创建IPSec，感兴趣流是全0。华为防火墙通常都是使用物理口创建IPSec，需要写明细的感兴趣流，所以FortiGate也要对应的写明细感兴趣数据流，不能写全0。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

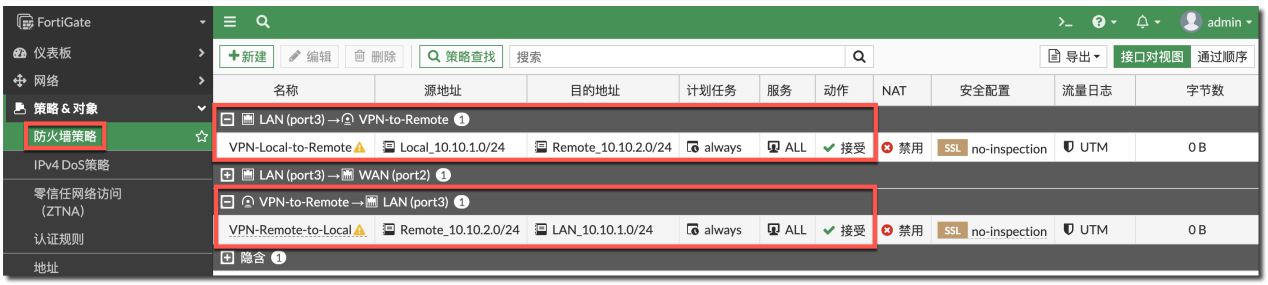


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config vpn ipsec phase1-interface
    edit "VPN-to-Remote"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 202.103.23.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-Remote"
        set phase1name "VPN-to-Remote"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 10.10.1.0 255.255.255.0
        set dst-subnet 10.10.2.0 255.255.255.0
    next
end
```

5. 配置VPN相关的网段地址对象和防火墙策略。






```bash
config firewall address
    edit "Local_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Remote_10.10.2.0/24"
        set subnet 10.10.2.0 255.255.255.0
    next
end

config firewall policy
    edit 2
        set name "VPN-Local-to-Remote"
        set srcintf "port3"
        set dstintf "VPN-to-Remote"
        set action accept
        set srcaddr "Local_10.10.1.0/24"
        set dstaddr "Remote_10.10.2.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-Remote-to-Local"
        set srcintf "VPN-to-Remote"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_10.10.2.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置VPN业务网段的静态路由。

重要

相关VPN的路由配置中“黑洞路由的意义：

你可能会遇到以下的VPN业务问题：通过VPN的SIP电话，时不时中断，无法向服务器成功注册？通过VPN的Radius认证无法经常会无法认证成功？ 通过VPN的AP注册到总部时不时会中断？持续的PRGT监控ping总部的服务器，时不时会显示中断？

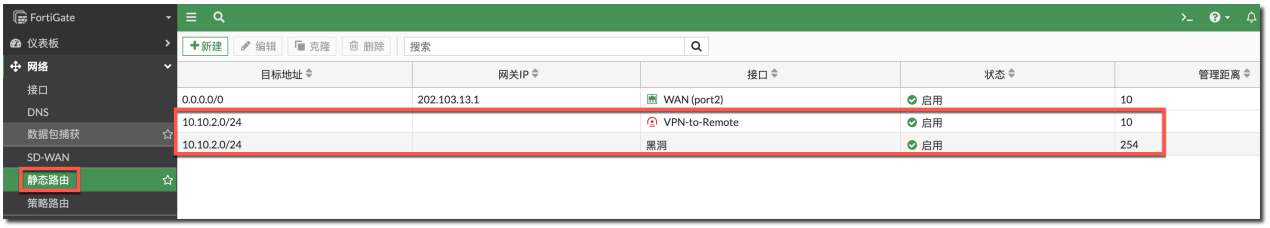
VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量（SIP注册请求/Radius/Capwap/ICMP）会因为查询到了默认路由而走向了WAN（Internet），从而产生了错误的UDP-NAT-Seesion，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，SIP等VPN旧的业务流量依旧会走到错误的Session上去，从而引起该业务异常。

解决方法：

- 方法一：配置去往VPN业务网段的“黑洞路由”，管理距离为254，VPN正常的情况下此黑洞路由不生效，而当VPN中断的时候，黑洞路由浮起来并且生效，将VPN中断时候的VPN流量丢弃，避免将流量转发到互联网而产生错误的session。配置VPN的备份黑洞路由的意义在此。
- 方法二：配置源接口：LAN，目的接口：WAN，源IP：本地内网网段，目的IP：对端内网网段，动作：丢包的策略。将此去往Internet的私网（无用的）流量丢弃掉，避免FGT产生这种错误的session，从而避免了UDP业务时不时中断的问题。
- 方法三：在全局下开启“set snat-route-change enable”，一旦路由发生变化，将相关的会话flag置位为“Dirty”，清除路由缓存并重新查找目的IP的下一跳地址，这样VPN隧道恢复的时候，流量也会相应的切换到VPN隧道里面来。

```
FortiGate # config system global
FortiGate (global) # set snat-route-change enable
FortiGate (global) # end
```

三种方式任意选择一种即可。推荐使用黑洞路由方式。




```bash
config router static
    edit 1
        set gateway 202.103.12.1
        set device "port2"
    next
    edit 2
        set dst 10.10.2.0 255.255.255.0
        set device "VPN-to-Remote"
    next
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

华为USG6000V

1. 基本IP与路由配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```bash
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 202.103.23.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.10.2.1 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet1/0/0
#
ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet1/0/0 202.103.23.1
```

2. 地址对象、策略、NAT配置。





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
ip address-set Local_10.10.2.0/24 type object
 address 0 10.10.2.0 mask 24
#
ip address-set Remote_10.10.1.0/24 type object
 address 0 10.10.1.0 mask 24
#
security-policy
 default action permit
 rule name to_Internet
  source-zone trust
  destination-zone untrust
  source-address address-set Local_10.10.2.0/24
  action permit
#
nat-policy
 rule name to_Internet
  source-zone trust
  destination-zone untrust
  source-address address-set Local_10.10.2.0/24
  action source-nat easy-ip
```

3. 配置IPSec，新建IPSec VPN策略。



4. 如下图参数配置，注意与FortiGate端的安全提议要一致（注意加密数据流不要选择地址对象，需要手动输入，否则第二阶段可能无法建立），开启反向路由注入。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

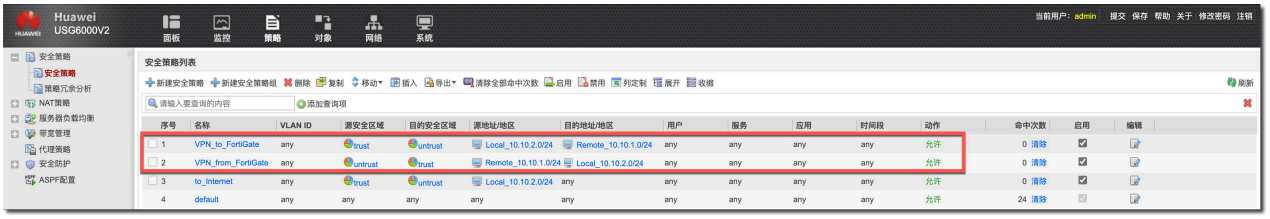



```bash
acl number 3000
 rule 5 permit ip source 10.10.2.0 0.0.0.255 destination 10.10.1.0 0.0.0.255
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
#
ike peer ike64165343931
 pre-shared-key %^%#GFRw6k/f}&DP2(A}Sh*9",ym@xVr%!NO~3!N]5u!%^%#
 ike-proposal 1
 remote-id-type none
 dpd type periodic
 remote-address 202.103.13.2
#
ipsec policy ipsec6416534390 1 isakmp
 security acl 3000
 pfs dh-group14
 ike-peer ike64165343931
 proposal prop64165343931
 tunnel local applied-interface
 alias to_FortiGate
 sa trigger-mode auto
 sa duration traffic-based 10485760
 sa duration time-based 43200
 route inject dynamic
```

5. 配置IPSec VPN相关网段放通的安全策略，并将他们移动至上网策略之前。




```
security-policy
 default action permit
 rule name VPN_to_FortiGate
  source-zone trust
  destination-zone untrust
  source-address address-set Local_10.10.2.0/24
  destination-address address-set Remote_10.10.1.0/24
  action permit
 rule name VPN_from_FortiGate
  source-zone untrust
  destination-zone trust
  source-address address-set Remote_10.10.1.0/24
  destination-address address-set Local_10.10.2.0/24
  action permit
 rule name to_Internet
  source-zone trust
  destination-zone untrust
  source-address address-set Local_10.10.2.0/24
  action permit
```

bash

6. 华为防火墙的转发流程是先做SNAT，再做IPsec VPN，也就是说，如果按照我们之前配置的SNAT规则，VPN的流量10.10.2.2去访问10.10.1.2的流量会被SNAT成公网IP 202.103.23.2，然后再进入到IPsec VPN流程，这个时候是无法匹配到感兴趣流的，因此流量将无法成功被IPSec加密。所以需要再配置一个VPN流量bypass的SNAT规则，让VPN流量不做SNAT转换，然后将其放置到最前面，优先匹配即可。



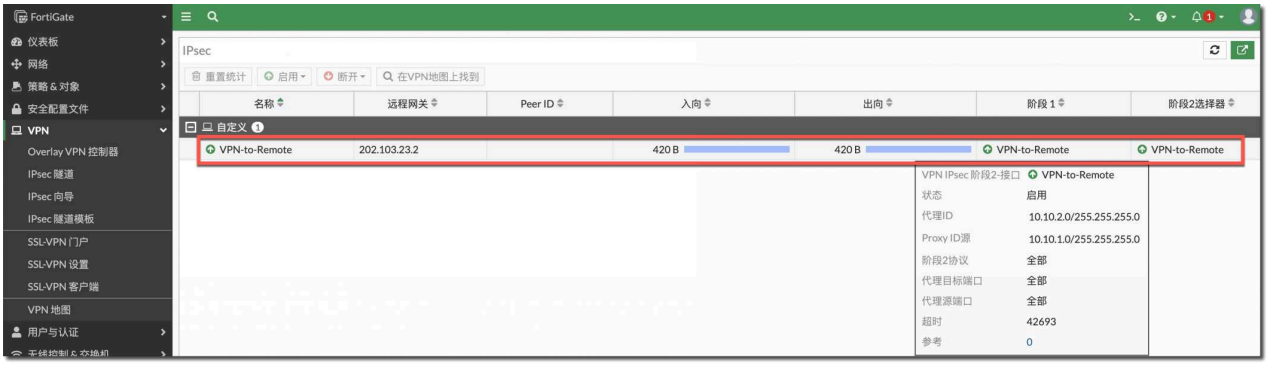

```
nat-policy
 rule name VPN_to_FortiGate
  source-zone trust
  destination-zone untrust
  source-address address-set Local_10.10.2.0/24
  destination-address address-set Remote_10.10.1.0/24
  action no-nat
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
 rule name to_Internet
  source-zone trust
  destination-zone untrust
  source-address address-set Local_10.10.2.0/24
  action source-nat easy-ip

```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: VPN-to-Remote
version: 1
interface: port2 4
addr: 202.103.13.2:500 → 202.103.23.2:500
tun_id: 202.103.23.2/::202.103.23.2
remote_location: 0.0.0.0
network-id: 0
created: 490s ago
IKE SA: created 1/1  established 1/1  time 210/210/210 ms
IPsec SA: created 1/2  established 1/1  time 390/390/390 ms
  id/spi: 257 05b470e04dc4363a/7f25ce9c15e94de3
  direction: initiator
  status: established 490-490s ago = 210ms
  proposal: aes256-sha256
  key: 9b5842bda3877c51-ebbc39ba4a960fde-f76d2defdebe67bd-de35bd7bc5720ec2
  lifetime/rekey: 86400/85609
  DPD sent/recv: 0000004d/135cb4c9

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Remote ver=1 serial=1 202.103.13.2:0→202.103.23.2:0 tun_id=202.103.23.2 tun_id6=::202.103.23.2
dst_mtu=1500 dpd-link=1
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=10
proxyid_num=1 child_num=0 refcnt=4 ilast=15 olast=15 ad=/0
stat: rxp=12 txp=12 rxb=1008 txb=1008
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=77
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Remote proto=0 sa=1 ref=4 serial=1 auto-negotiate
  src: 0:10.10.1.0-10.10.1.255:0
  dst: 0:10.10.2.0-10.10.2.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=42436/0B replaywin=2048
       seqno=d esn=0 replaywin_lastseq=0000000d qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42929/43200
  dec: spi=34dc8977 esp=aes key=32 947441e7c4d219ad7c0cb909942e17d2c8e25b42346ea53f301ba37161d2fdef
       ah=sha256 key=32 df58345781028ba4ac18cc037ce667e974941e4ff544b7368f523307c83d4ea4
  enc: spi=0b11f21b esp=aes key=32 d5dcfee82b332abf9bb62c620c3e42ee42c0f6c990fa380204b02b83f0acdbff
       ah=sha256 key=32 16b2afbcec0b0feb10cf4dedba31d99e3c59ce020823a88b9b99122b02bedf65
  dec:pkts/bytes=24/2016, enc:pkts/bytes=24/2880
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.13.2 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

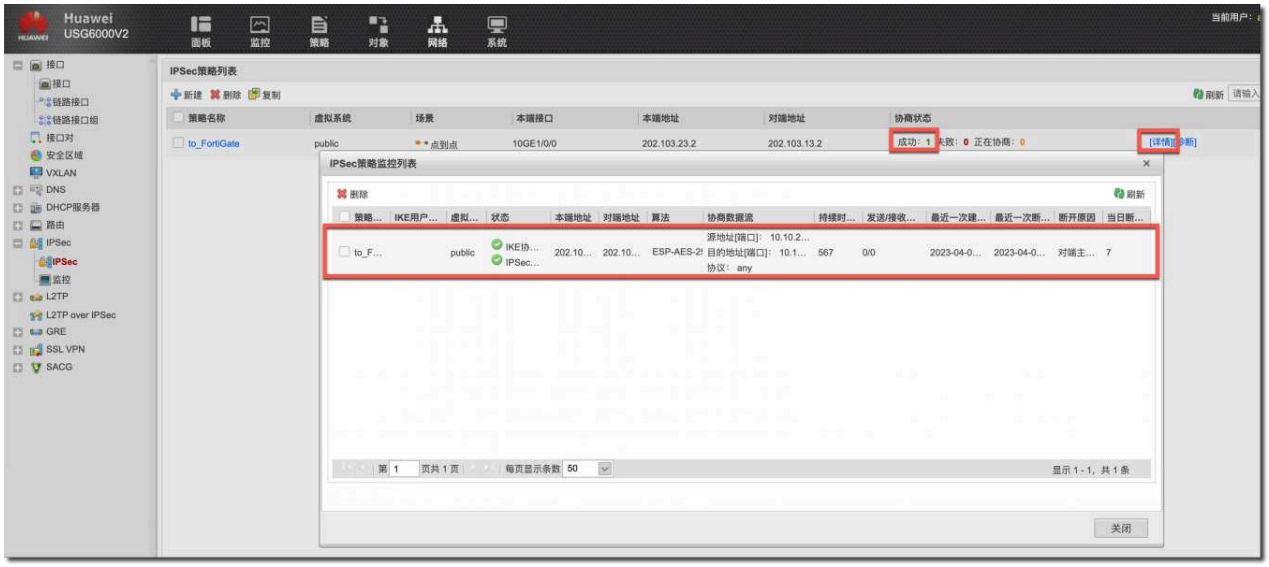
2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.103.13.1, port2, [1/0]
C       10.10.1.0/24 is directly connected, port3
S       10.10.2.0/24 [10/0] via VPN-to-Remote tunnel 202.103.23.2, [1/0]
C       192.168.100.0/24 is directly connected, port1
C       202.103.13.0/24 is directly connected, port2
```

3. FortiGate侧PC1业务测试。

```
VPCS> show
NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.1.2/24         10.10.1.1
       fe80::250:79ff:fe66:6804/64

VPCS> ping 10.10.2.2
84 bytes from 10.10.2.2 icmp_seq=1 ttl=62 time=5.413 ms
84 bytes from 10.10.2.2 icmp_seq=2 ttl=62 time=2.511 ms
84 bytes from 10.10.2.2 icmp_seq=3 ttl=62 time=2.242 ms
84 bytes from 10.10.2.2 icmp_seq=4 ttl=62 time=1.902 ms
84 bytes from 10.10.2.2 icmp_seq=5 ttl=62 time=2.080 ms
```

4. 华为防火墙查看IPSec连接状态。




```
<USG6000V2>display ike sa verbose remote 202.103.13.2
2023-04-06 17:27:29.590 +08:00
Ike sa verbose information :
-------------------------------------------------------------------------
Ike Sa phase   : 1
Establish Time : 2023-04-06 17:16:56
PortCfg Index  : 0x6
IKE Peer Name  : ike64165343931
Connection Id  : 347
Version        : v1
Exchange Mode  : Main
Flow VPN       :
Peer VPN       :
-------------------------------------------------------------------------
Intiator Cookie                        : 0x05b470e04dc4363a
Responder Cookie                       : 0x7f25ce9c15e94de3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Local Address                          : 202.103.23.2
Remote Address                         : 202.103.13.2:500
Encryption Algorithm                   : AES-256
Authentication Algorithm               : SHA2-256
Authentication Method                  : Pre-Shared key
DPD Capability                         : Yes
DPD Enable                             : Yes
Remaining Duration                     : 85766
Reference Counter                      : 1
Flags                                  : RD|A
Remote Id Type                         : IP
Remote Id                              : 202.103.13.2
DH Group                               : 14
NAT Traversal Version                  : RFC3947
ModeCfg IP                             : -
-------------------------------------------------------------------------

  Number of IKE SA : 1
```

```
<USG6000V2> display ipsec sa remote 202.103.13.2
2023-04-06 17:28:30.260 +08:00
ipsec sa information:
=============================
Interface: GigabitEthernet1/0/0
=============================
  -------------------------------
  IPSec policy name: "ipsec6416534390"
  Sequence number  : 1
  Acl group        : 3000
  Acl rule         : 5
  Mode             : ISAKMP
  -------------------------------
    Connection ID     : 350
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 11m 32s
    Tunnel local      : 202.103.23.2:500
    Tunnel remote     : 202.103.13.2:500
    Flow source       : 10.10.2.0/255.255.255.0 0/0-65535
    Flow destination  : 10.10.1.0/255.255.255.0 0/0-65535
    [Outbound ESP SAs]
      SPI: 886868343 (0×34dc8977)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 10485759/42508
      Max sent sequence-number: 18
      UDP encapsulation used for NAT traversal: N
      SA encrypted packets (number/bytes): 17/1428
    [Inbound ESP SAs]
      SPI: 185725467 (0×b11f21b)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 10485759/42508
      Max received sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      SA decrypted packets (number/bytes): 17/1428
      Anti-replay : Enable
      Anti-replay window size: 1024
```

5. 查看华为防火墙的路由表，可以看到自动添加了到FortiGate内网的路由。

```
[USG6000V2]display ip routing-table
2023-04-06 17:32:20.280 +08:00
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
        0.0.0.0/0   Static  60   0           D   202.103.23.1    GigabitEthernet1/0/0
      10.10.1.0/24  Unr     70   0           D   202.103.13.2    GigabitEthernet1/0/0
      10.10.2.0/24  Direct  0    0           D   10.10.2.1       GigabitEthernet1/0/1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
      10.10.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   202.103.23.0/24  Direct  0    0           D   202.103.23.2    GigabitEthernet1/0/0
   202.103.23.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
```

6. 华为防火墙侧PC2业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.2.2/24         10.10.2.1
       fe80::250:79ff:fe66:6805/64

VPCS> ping 10.10.1.2

84 bytes from 10.10.1.2 icmp_seq=1 ttl=62 time=3.139 ms
84 bytes from 10.10.1.2 icmp_seq=2 ttl=62 time=2.126 ms
84 bytes from 10.10.1.2 icmp_seq=3 ttl=62 time=2.508 ms
84 bytes from 10.10.1.2 icmp_seq=4 ttl=62 time=2.257 ms
84 bytes from 10.10.1.2 icmp_seq=5 ttl=62 time=1.767 ms
```

7. FortiGate侧抓包查看。

```
FortiGate # diagnose sniffer packet any 'host 10.10.2.2 and host 10.10.1.2 and icmp' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.2 and host 10.10.1.2 and icmp]
2023-04-06 17:30:20.440445 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:20.441055 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:20.441296 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:20.441308 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:21.444661 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:21.444753 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:21.444962 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:21.444969 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:22.447197 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:22.447332 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:22.447520 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:22.447527 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:23.451289 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:23.451454 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:23.451667 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:23.451676 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:24.453906 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:24.453939 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-06 17:30:24.454165 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-06 17:30:24.454176 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
```

说明

关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与H3C SecPath防火墙建立IPSec VPN

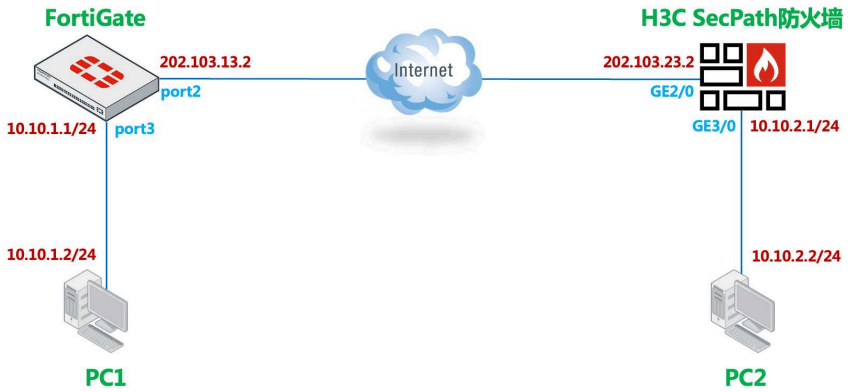
网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与10.10.2.0/24两个网段的通信。与H3C SecPath防火墙进行IPsec VPN（IKE v1）对接。

H3C SecPath防火墙版本：

```
<H3C>display version
H3C Comware Software, Version 7.1.064, ESS 1185P29
Copyright (c) 2004-2022 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath vFW1000 uptime is 0 weeks, 0 days, 0 hours, 7 minutes
Last reboot reason : Power on
Boot image: flash:/vFW1000-CMW710-BOOT-E1185P29-X64.bin
Boot image version: 7.1.064, ESS 1185P29
  Compiled Oct 31 2022 14:00:00
System image: flash:/vFW1000-CMW710-SYSTEM-E1185P29-X64.bin
System image version: 7.1.064, ESS 1185P29
  Compiled Oct 31 2022 14:00:00
```

网络拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置H3C SecPath防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略。

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 如图配置网络、认证、第一阶段、第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

不像和Cisco/PA/Juniper/山石使用虚拟接口创建IPSec，感兴趣流是全0。H3C防火墙通常都是使用物理口创建IPSec，需要写明细的感兴趣流，所以FortiGate也要对应的写明细感兴趣数据流，不能写全0。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

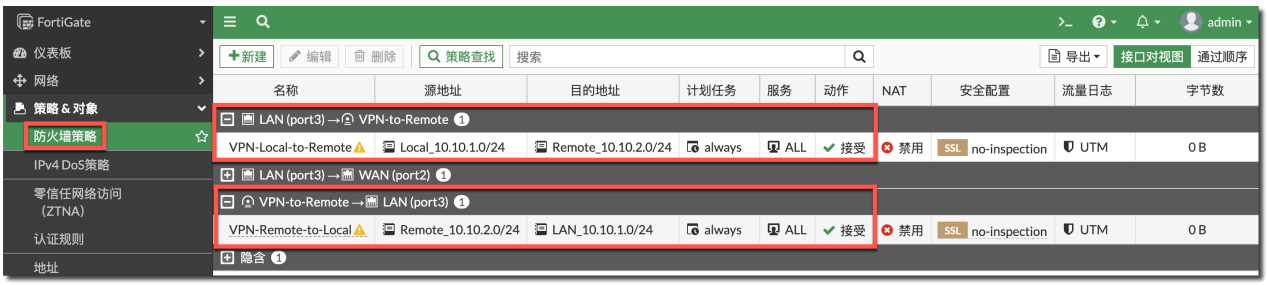


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN-to-Remote"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 202.103.23.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-Remote"
        set phase1name "VPN-to-Remote"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 10.10.1.0 255.255.255.0
        set dst-subnet 10.10.2.0 255.255.255.0
    next
end
```

5. 配置VPN相关的网段地址对象和防火墙策略。






```
config firewall address
    edit "Local_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Remote_10.10.2.0/24"
        set subnet 10.10.2.0 255.255.255.0
    next
end

config firewall policy
    edit 2
        set name "VPN-Local-to-Remote"
        set srcintf "port3"
        set dstintf "VPN-to-Remote"
        set action accept
        set srcaddr "Local_10.10.1.0/24"
        set dstaddr "Remote_10.10.2.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-Remote-to-Local"
        set srcintf "VPN-to-Remote"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_10.10.2.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置VPN业务网段的静态路由。

重要

相关VPN的路由配置中“黑洞路由的意义：

你可能会遇到以下的VPN业务问题：通过VPN的SIP电话，时不时中断，无法向服务器成功注册？通过VPN的Radius认证无法经常会无法认证成功？通过VPN的AP注册到总部时不时会中断？持续的PRGT监控ping总部的服务器，时不时会显示中断？

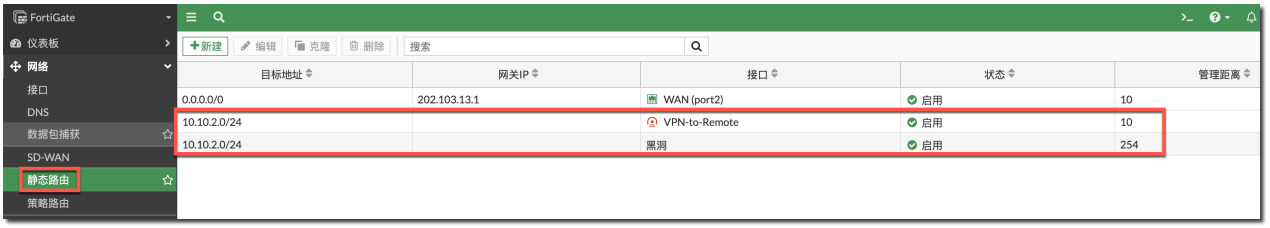
VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量（SIP注册请求/Radius/Capwap/ICMP）会因为查询到了默认路由而走向了WAN（Internet），从而产生了错误的UDP-NAT-Seesion，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，SIP等VPN旧的业务流量依旧会走到错误的Session上去，从而引起该业务异常。

解决方法：

- 方法一：配置去往VPN业务网段的“黑洞路由”，管理距离为254，VPN正常的情况下此黑洞路由不生效，而当VPN中断的时候，黑洞路由浮起来并且生效，将VPN中断时候的VPN流量丢弃，避免将流量转发到互联网而产生错误的session。配置VPN的备份黑洞路由的意义在此。
- 方法二：配置源接口：LAN，目的接口：WAN，源IP：本地内网网段，目的IP：对端内网网段，动作：丢包的策略。将此去往Internet的私网（无用的）流量丢弃掉，避免FGT产生这种错误的session，从而避免了UDP业务时不时中断的问题。
- 方法三：在全局下开启“set snat-route-change enable”，一旦路由发生变化，将相关的会话flag置位为“Dirty”，清除路由缓存并重新查找目的IP的下一跳地址，这样VPN隧道恢复的时候，流量也会相应的切换到VPN隧道里面来。

```
FortiGate # config system global
FortiGate (global) # set snat-route-change enable
FortiGate (global) # end
```

三种方式任意选择一种即可。推荐使用黑洞路由方式。

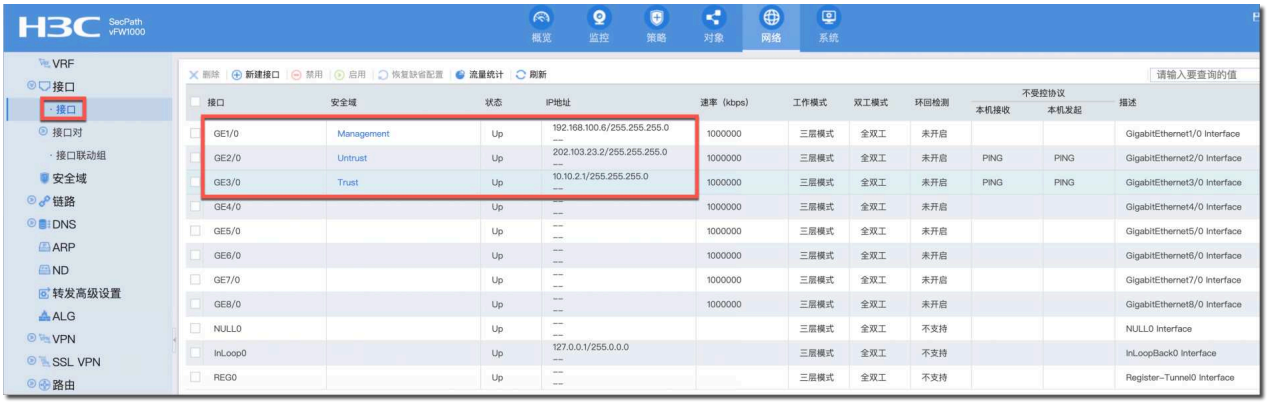


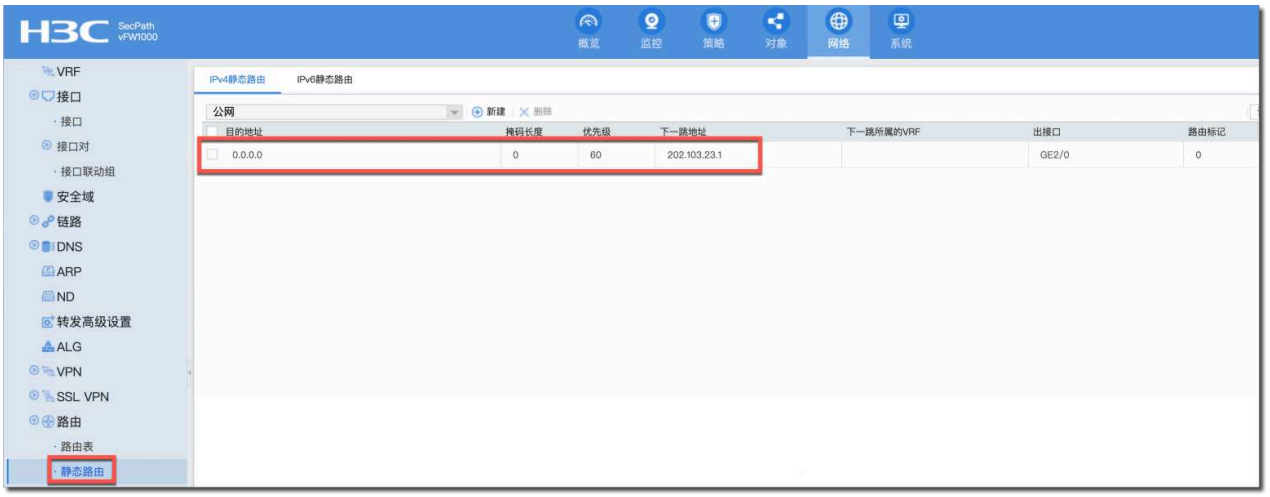

```
config router static
    edit 1
        set gateway 202.103.12.1
        set device "port2"
    next
    edit 2
        set dst 10.10.2.0 255.255.255.0
        set device "VPN-to-Remote"
    next
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

H3C SecPath

1. 基本IP与路由配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

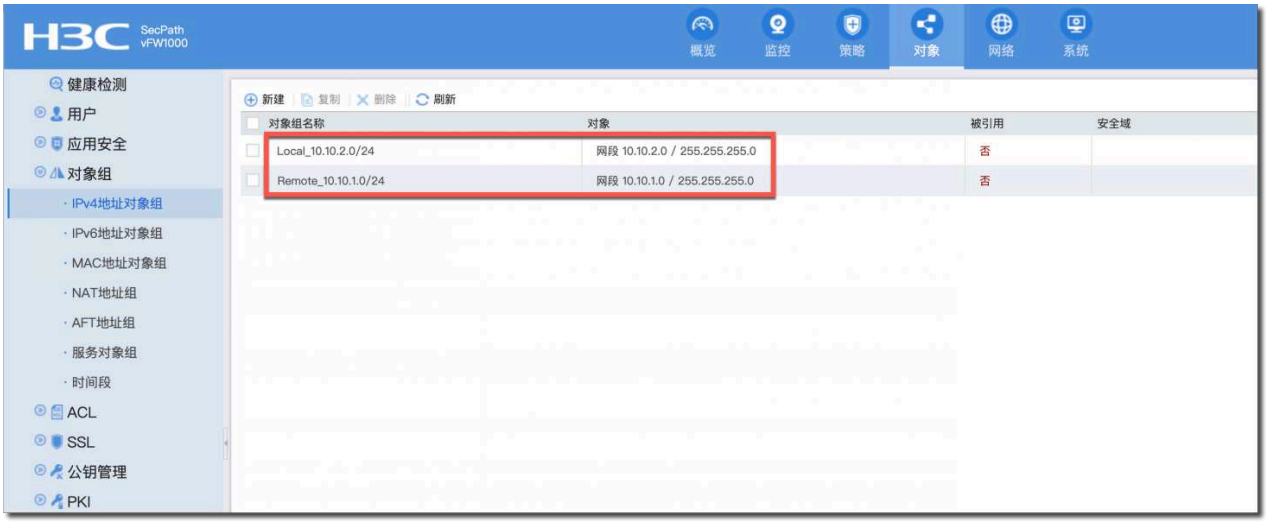




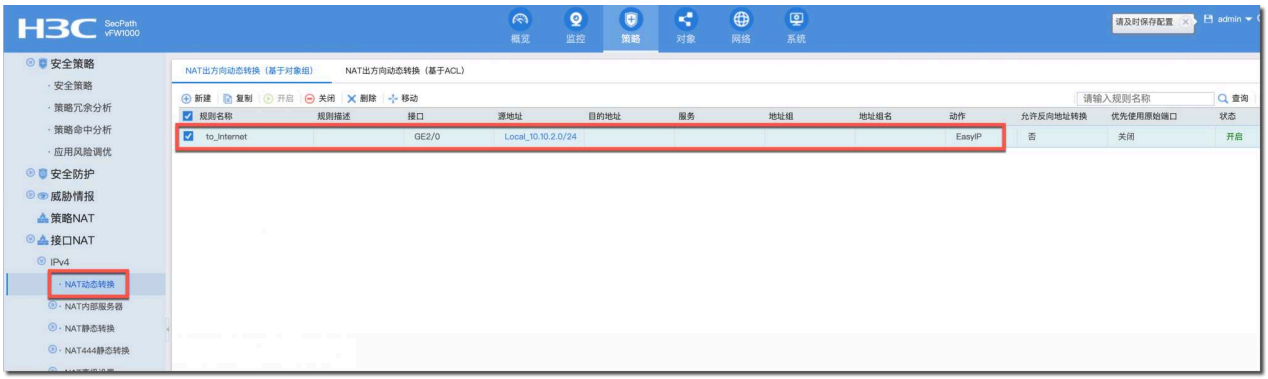

```
interface GigabitEthernet2/0
 port link-mode route
 ip address 202.103.23.2 255.255.255.0
 manage ping inbound
 manage ping outbound
#
interface GigabitEthernet3/0
 port link-mode route
 ip address 10.10.2.1 255.255.255.0
 manage ping inbound
 manage ping outbound
#
security-zone name Trust
 import interface GigabitEthernet3/0
#
security-zone name Untrust
 import interface GigabitEthernet2/0
#
 ip route-static 0.0.0.0 0 GigabitEthernet2/0 202.103.23.1
```

2. 地址对象、策略、NAT配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.








```
object-group ip address Local_10.10.2.0/24
 0 network subnet 10.10.2.0 255.255.255.0
#
object-group ip address Remote_10.10.1.0/24
 0 network subnet 10.10.1.0 255.255.255.0
#
security-policy ip
 rule 2 name to_Internet
  action pass
  source-zone Trust
  destination-zone Untrust
  source-ip Local_10.10.2.0/24
#
nat policy
 rule name to_Internet
  source-ip Local_10.10.2.0/24
  outbound-interface GigabitEthernet2/0
  action easy-ip
```

3. 配置IPSec，新建IKE提议，按照如图安全提议配置，点击确定下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 新建IPSec策略，如下图参数配置，注意与FortiGate端的安全提议要一致，注意对端ID选择“IPv4地址”，内容填写为FortiGate的公网口IP地址，如果FortiGate的地址是动态的，可以选择FQDN形式的ID，FortiGate侧本地ID也要对应修改为FQDN形式，开启“自动触发”和“DPD”，勾选“自动生成安全策略”（这里自动创建的策略是允许IPSec协商的发起和接受）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
acl advanced name IPsec_to_FortiGate_IPv4_1
 rule 0 permit ip source 10.10.2.0 0.0.0.255 destination 10.10.1.0 0.0.0.255
#
ipsec transform-set to_FortiGate_IPv4_1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
 pfs dh-group14
#
ipsec policy to_FortiGate 1 isakmp
 transform-set to_FortiGate_IPv4_1
 security acl name IPsec_to_FortiGate_IPv4_1
 local-address 202.103.23.2
 remote-address 202.103.13.2
 ike-profile to_FortiGate_IPv4_1
 sa trigger-mode auto
 sa duration time-based 43200
 sa idle-time 60
#
ike profile to_FortiGate_IPv4_1
 keychain to_FortiGate_IPv4_1
 dpd interval 20 on-demand
 match remote identity address 202.103.13.2 255.255.255.255
 match local address GigabitEthernet2/0
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain to_FortiGate_IPv4_1
 match local address GigabitEthernet2/0
 pre-shared-key address 202.103.13.2 255.255.255.255 key cipher $c$3$OAC3tjUo2G+AOc7w0iW8jeQvV2wpRj96iHSZ
#
interface GigabitEthernet2/0
 ipsec apply policy to_FortiGate
#
security-policy ip
 rule 4 name IPsec_to_FortiGate_1_20230407151324_IN
  action pass
  destination-zone Local
  service ike
  service nat-t-ipsec
  service ipsec-ah
  service ipsec-esp
 rule 3 name IPsec_to_FortiGate_1_20230407151324_OUT
  action pass
  source-zone Local
  service ike
  service nat-t-ipsec
  service ipsec-ah
  service ipsec-esp
```

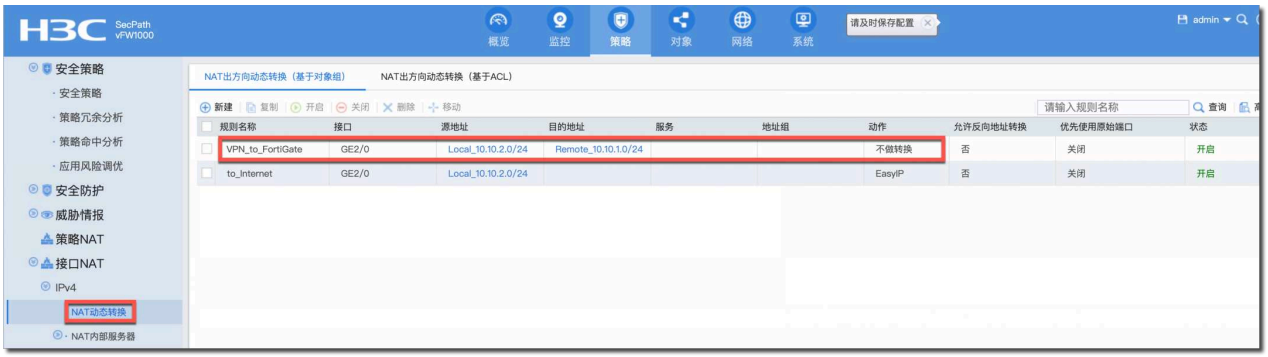
5. 配置IPSec VPN相关网段放通的安全策略，并将他们移动至上网策略之前。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
security-policy ip
 rule 6 name VPN_from_FortiGate
  action pass
  source-zone Untrust
  destination-zone Trust
  source-ip Remote_10.10.1.0/24
  destination-ip Local_10.10.2.0/24
 rule 5 name VPN_to_FortiGate
  action pass
  source-zone Trust
  destination-zone Untrust
  source-ip Local_10.10.2.0/24
  destination-ip Remote_10.10.1.0/24
 rule 4 name IPsec_to_FortiGate_1_20230407151324_IN
  action pass
  destination-zone Local
  service ike
  service nat-t-ipsec
  service ipsec-ah
  service ipsec-esp
 rule 3 name IPsec_to_FortiGate_1_20230407151324_OUT
  action pass
  source-zone Local
  service ike
  service nat-t-ipsec
  service ipsec-ah
  service ipsec-esp
 rule 2 name to_Internet
  action pass
  source-zone Trust
  destination-zone Untrust
  source-ip Local_10.10.2.0/24
```

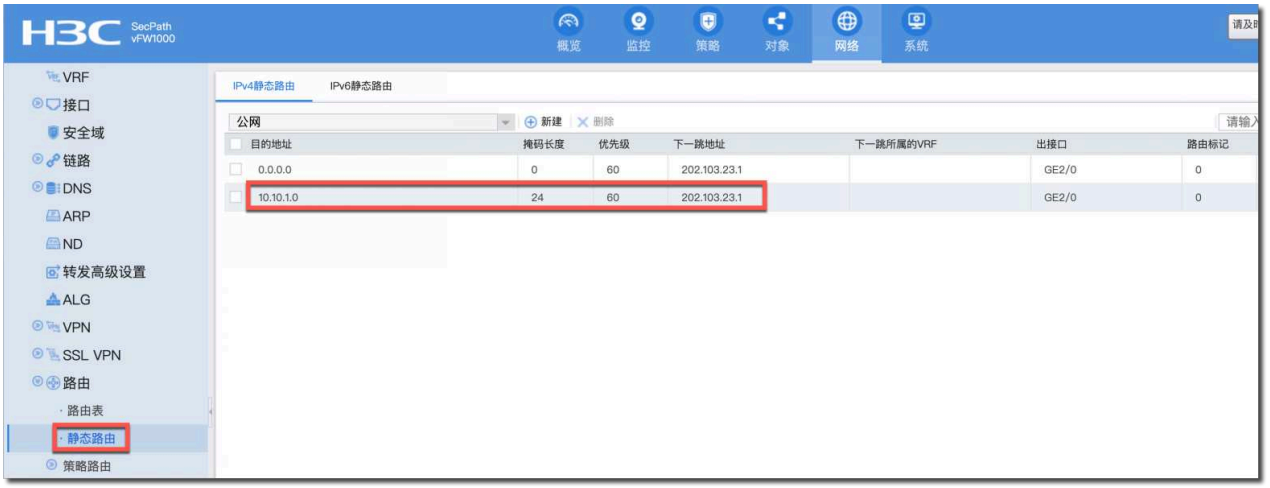
6. H3C防火墙的转发流程是先做SNAT，再做IPsec VPN，也就是说，如果按照我们之前配置的SNAT规则，VPN的流量10.10.2.2去访问10.10.1.2的流量会被SNAT成公网IP 202.103.23.2，然后再进入到IPsec VPN流程，这个时候是无法匹配到感兴趣流的，因此流量将无法成功被IPSec加密。所以需要再配置一个VPN流量bypass的SNAT规则，让VPN流量不做SNAT转换，然后将其放置到最前面，优先匹配即可。




```
nat policy
 rule name VPN_to_FortiGate
  source-ip Local_10.10.2.0/24
  destination-ip Remote_10.10.1.0/24
  outbound-interface GigabitEthernet2/0
  action no-nat
 rule name to_Internet
  source-ip Local_10.10.2.0/24
  outbound-interface GigabitEthernet2/0
  action easy-ip
```

7. 添加去往FortiGate内网VPN网段的静态路由（由于已经配置了默认路由从IPSec绑定的物理口出去，其实这里不需要配置，但如果没有默认路由或默认路由是其他接口，可以参考此配置）。

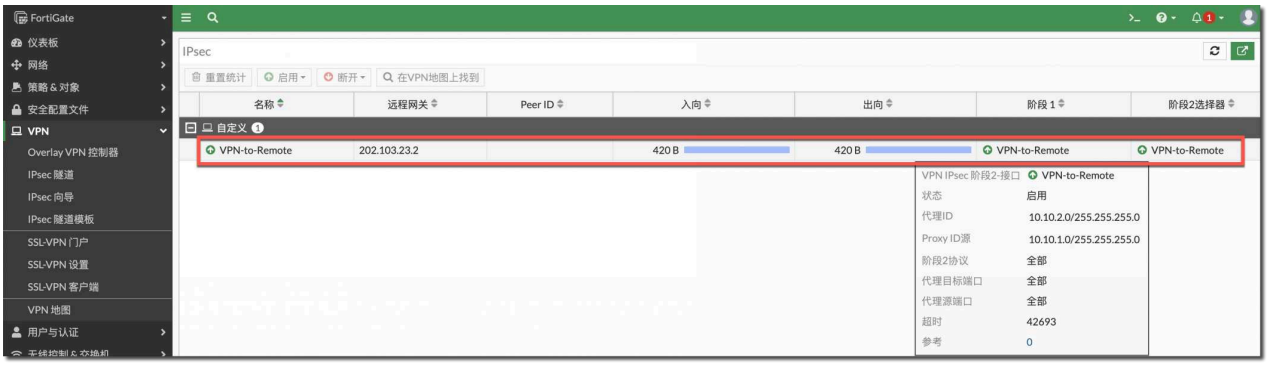
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
ip route-static 10.10.1.0 24 GigabitEthernet2/0 202.103.23.1
```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。




```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Remote
version: 1
interface: port2 4
addr: 202.103.13.2:500 → 202.103.23.2:500
tun_id: 202.103.23.2/::202.103.23.2
remote_location: 0.0.0.0
network-id: 0
created: 2435s ago
IKE SA: created 1/1  established 1/1  time 20/20/20 ms
IPsec SA: created 1/38  established 1/38  time 20/75/2030 ms
  id/spi: 365 3f178bf07066db5b/4bc6621ed12c3030
  direction: initiator
  status: established 2435-2435s ago = 20ms
  proposal: aes256-sha256
  key: 2f13f4b81d3eb4c1-575e1272457cc854-d37978c764f9a778-cd5724cdc244f07a
  lifetime/rekey: 86400/83664
  DPD sent/recv: 00000a61/000030dd

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Remote ver=1 serial=1 202.103.13.2:0→202.103.23.2:0 tun_id=202.103.23.2 tun_id6=::202.103.23.2
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=13 olast=13 ad=/0
stat: rxp=10 txp=15 rxb=840 txb=1260
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=2658
natt: mode=none draft=0 interval=0 remote_port=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
proxyid=VPN-to-Remote proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:10.10.1.0-10.10.1.255:0
  dst: 0:10.10.2.0-10.10.2.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=42881/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42901/43200
  dec: spi=34dc89a0 esp=aes key=32 9ebf3ec4affd4b4a57b18fe15c1c505184622c2cdcba87d788887f569cfaa23e
       ah=sha256 key=32 c3efca48ffbcd7fb0e8013fef745576010a71ec3c9a02a32f333c380de01e2a6
  enc: spi=bc07e7b7 esp=aes key=32 660dedaa1a6d145b94073c031a3e9f1587dcb44d3b50b9683382b27ecd5562ce
       ah=sha256 key=32 308adc9899b8775255c59053ed4a5edc3df8231135007d2a26614097619361de
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.13.2 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.103.13.1, port2, [1/0]
C       10.10.1.0/24 is directly connected, port3
S       10.10.2.0/24 [10/0] via VPN-to-Remote tunnel 202.103.23.2, [1/0]
C       192.168.100.0/24 is directly connected, port1
C       202.103.13.0/24 is directly connected, port2
```

3. FortiGate侧PC1业务测试。

```
VPCS> show
NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.1.2/24         10.10.1.1
       fe80::250:79ff:fe66:6804/64

VPCS> ping 10.10.2.2
84 bytes from 10.10.2.2 icmp_seq=1 ttl=62 time=4.769 ms
84 bytes from 10.10.2.2 icmp_seq=2 ttl=62 time=2.769 ms
84 bytes from 10.10.2.2 icmp_seq=3 ttl=62 time=2.194 ms
84 bytes from 10.10.2.2 icmp_seq=4 ttl=62 time=3.881 ms
84 bytes from 10.10.2.2 icmp_seq=5 ttl=62 time=2.335 ms
```

4. H3C防火墙查看IPSec连接状态。




```
<H3C>display ike sa verbose remote 202.103.13.2
    ------------------------------------------------------------
    Connection ID: 2
    Outside VPN:
    Inside VPN:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    Profile: to_FortiGate_IPv4_1
    Transmitting entity: Responder
    Initiator cookie: 3f178bf07066db5b
    Responder cookie: 4bc6621ed12c3030
    ------------------------------------------------
    Local IP/port: 202.103.23.2/500
    Local ID type: IPV4_ADDR
    Local ID: 202.103.23.2

    Remote IP/port: 202.103.13.2/500
    Remote ID type: IPV4_ADDR
    Remote ID: 202.103.13.2

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: SHA256
    Encryption-algorithm: AES-CBC-256

    Life duration(sec): 86400
    Remaining key duration(sec): 83791
    Exchange-mode: Main
    Diffie-Hellman group: Group 14
    NAT traversal: Not detected

    Extend authentication: Disabled
    Assigned IP address:
    Vendor ID index:0×ffffffff
    Vendor ID sequence number:0×0
```

```
<H3C> display ipsec sa remote 202.103.13.2
-----------------------------
Interface: GigabitEthernet2/0
-----------------------------

  -----------------------------
  IPsec policy: to_FortiGate
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy: dh-group14
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Responder
    Path MTU: 1424
    Tunnel:
        local  address: 202.103.23.2
        remote address: 202.103.13.2
    Flow:
        sour addr: 10.10.2.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 10.10.1.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1271313254 (0×4bc6b366)
      Connection ID: 347892350977
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA idle time: 60
      SA duration (kilobytes/sec): 1843200/43200
      SA remaining duration (kilobytes/sec): 1843200/43177
      Max received sequence-number: 0
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 886868385 (0×34dc89a1)
      Connection ID: 347892350976
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA idle time: 60
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
      SA duration (kilobytes/sec): 1843200/43200
      SA remaining duration (kilobytes/sec): 1843200/43177
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

5. 查看H3C防火墙的路由表，可以看到包含了手动配置的到FortiGate内网的路由。

```
<H3C>display ip routing-table
Destinations : 18       Routes : 18
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/0          Static  60  0           202.103.23.1    GE2/0
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
10.10.1.0/24       Static  60  0           202.103.23.1    GE2/0
10.10.2.0/24       Direct  0   0           10.10.2.1       GE3/0
10.10.2.1/32       Direct  0   0           127.0.0.1       InLoop0
10.10.2.255/32     Direct  0   0           10.10.2.1       GE3/0
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.100.0/24   Direct  0   0           192.168.100.6   GE1/0
192.168.100.6/32   Direct  0   0           127.0.0.1       InLoop0
192.168.100.255/32 Direct  0   0           192.168.100.6   GE1/0
202.103.23.0/24    Direct  0   0           202.103.23.2    GE2/0
202.103.23.2/32    Direct  0   0           127.0.0.1       InLoop0
202.103.23.255/32  Direct  0   0           202.103.23.2    GE2/0
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

6. H3C防火墙侧PC2业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.2.2/24         10.10.2.1
       fe80::250:79ff:fe66:6805/64

VPCS> ping 10.10.1.2

84 bytes from 10.10.1.2 icmp_seq=1 ttl=62 time=3.529 ms
84 bytes from 10.10.1.2 icmp_seq=2 ttl=62 time=2.741 ms
84 bytes from 10.10.1.2 icmp_seq=3 ttl=62 time=2.472 ms
84 bytes from 10.10.1.2 icmp_seq=4 ttl=62 time=2.250 ms
84 bytes from 10.10.1.2 icmp_seq=5 ttl=62 time=2.193 ms
```

7. FortiGate侧抓包查看。

```
FortiGate # diagnose sniffer packet any 'host 10.10.2.2 and host 10.10.1.2 and icmp' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.2 and host 10.10.1.2 and icmp]
2023-04-07 16:07:08.123477 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:08.123667 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:08.123902 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:08.123914 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:09.127191 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:09.127380 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:09.127691 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:09.127700 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:10.131278 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:10.131445 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:10.131618 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:10.131624 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:11.134468 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:11.134502 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:11.134737 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
2023-04-07 16:07:11.134744 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:12.137190 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:12.137220 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-07 16:07:12.137409 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-07 16:07:12.137416 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
```

说明

关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与山石SG6000防火墙建立IPSec VPN

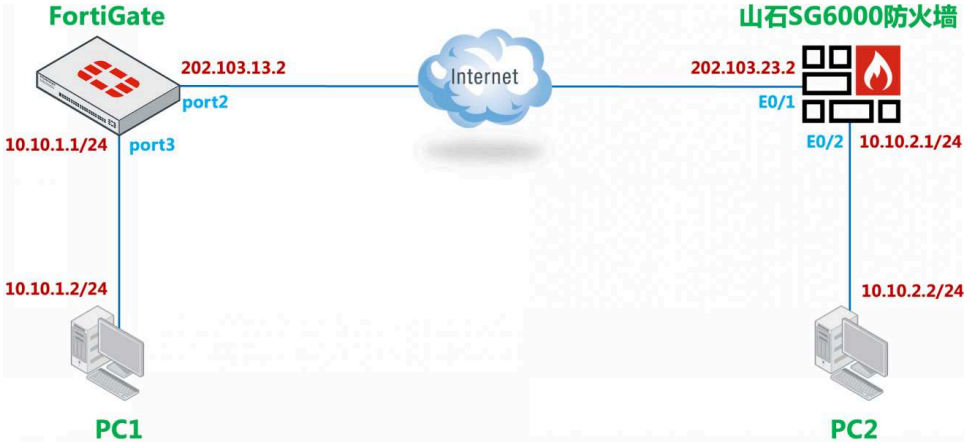
网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与10.10.2.0/24两个网段的通信。与山石SG6000-CloudEdge防火墙进行IPsec VPN（IKE v1）对接。

山石防火墙版本：

```
SG-6000# show version
Hillstone Networks StoneOS software, Version 5.5
Copyright (c) 2009-2023 by Hillstone Networks

Product name: SG-6000-VM00 S/N: 0010082687152785 Assembly number: 0000
Boot file is SG6000-CloudEdge-5.5R10P1-v6
Storage UUID is 2a771694-c137-483a-a7e2-ff93722c32ee
Instance UUID is iid-datasource-none
Update magic: 002300130532f202d5
Built by buildmaster8 2023/03/14 07:04:14
```

网络拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置山石SG6000防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略。

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 如图配置网络、认证、第一阶段、第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

和山石/Juniper/Palo Alto防火墙对接IPSec推荐使用全0的感兴趣流，这些厂商设备与FortiGate一致，创建IPSec时会创建虚拟的IPSec接口，通过路由对VPN流量进行引流，将需要加密的数据送到IPSec接口（当然写细化的感兴趣流也是可以的）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

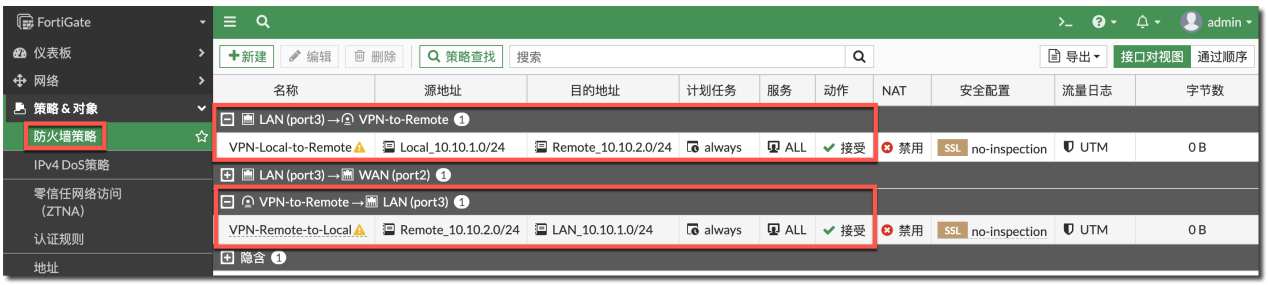


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN-to-Remote"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set dhgrp 14 5 2
        set remote-gw 202.103.23.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-Remote"
        set phase1name "VPN-to-Remote"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
end
```

5. 配置VPN相关的网段地址对象和防火墙策略。






```
config firewall address
    edit "Local_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Remote_10.10.2.0/24"
        set subnet 10.10.2.0 255.255.255.0
    next
end

config firewall policy
    edit 2
        set name "VPN-Local-to-Remote"
        set srcintf "port3"
        set dstintf "VPN-to-Remote"
        set action accept
        set srcaddr "Local_10.10.1.0/24"
        set dstaddr "Remote_10.10.2.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-Remote-to-Local"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set srcintf "VPN-to-Remote"
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_10.10.2.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置VPN业务网段的静态路由。

重要

相关VPN的路由配置中“黑洞路由的意义：

你可能会遇到以下的VPN业务问题：通过VPN的SIP电话，时不时中断，无法向服务器成功注册？通过VPN的Radius认证无法经常会无法认证成功？ 通过VPN的AP注册到总部时不时会中断？持续的PRGT监控ping总部的服务器，时不时会显示中断?

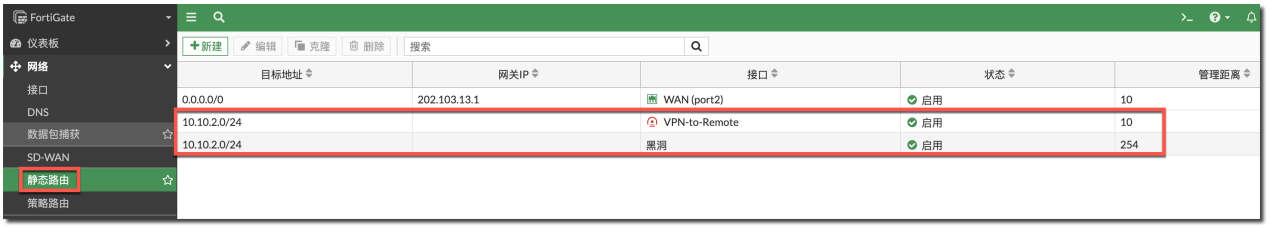
VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量（SIP注册请求/Radius/Capwap/ICMP）会因为查询到了默认路由而走向了WAN（Internet），从而产生了错误的UDP-NAT-Seesion，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，SIP等VPN旧的业务流量依旧会走到错误的Session上去，从而引起该业务异常。

解决方法：

- 方法一：配置去往VPN业务网段的“黑洞路由”，管理距离为254，VPN正常的情况下此黑洞路由不生效，而当VPN中断的时候，黑洞路由浮起来并且生效，将VPN中断时候的VPN流量丢弃，避免将流量转发到互联网而产生错误的session。配置VPN的备份黑洞路由的意义在此。
- 方法二：配置源接口：LAN，目的接口：WAN，源IP：本地内网网段，目的IP：对端内网网段，动作：丢包的策略。将此去往Internet的私网（无用的）流量丢弃掉，避免FGT产生这种错误的session，从而避免了UDP业务时不时中断的问题。
- 方法三：在全局下开启“set snat-route-change enable”，一旦路由发生变化，将相关的会话flag置位为“Dirty”，清除路由缓存并重新查找目的IP的下一跳地址，这样VPN隧道恢复的时候，流量也会相应的切换到VPN隧道里面来。

```
FortiGate # config system global
FortiGate (global) # set snat-route-change enable
FortiGate (global) # end
```

三种方式任意选择一种即可。推荐使用黑洞路由方式。



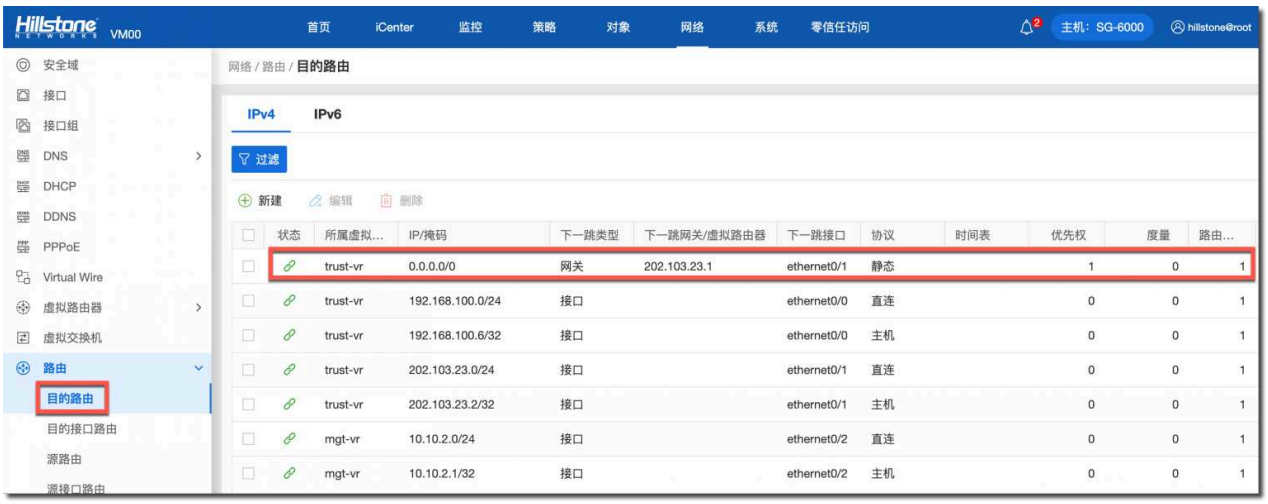

```
config router static
    edit 1
        set gateway 202.103.12.1
        set device "port2"
    next
    edit 2
        set dst 10.10.2.0 255.255.255.0
        set device "VPN-to-Remote"
    next
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

山石SG6000

1. 基本IP与路由配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



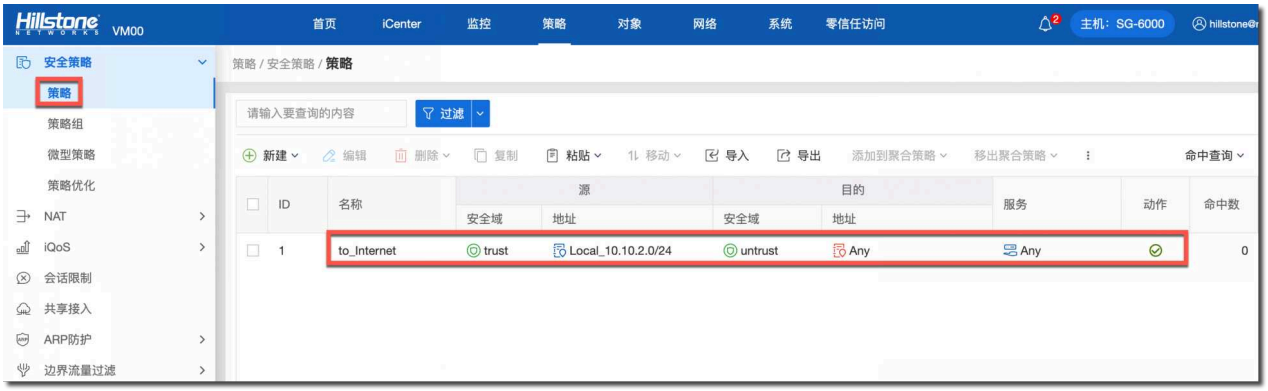



```
interface ethernet0/1
  zone  "untrust"
  ip address 202.103.23.2 255.255.255.0
  manage ping
exit
interface ethernet0/2
  zone  "trust"
  ip address 10.10.2.1 255.255.255.0
  manage ping
exit

ip vrouter "trust-vr"
  ip route 0.0.0.0/0 202.103.23.1
exit
```

2. 地址对象、策略、NAT配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.








```
address "Local_10.10.2.0/24"
  ip 10.10.2.0/24
exit
address "Remote_10.10.1.0/24"
  ip 10.10.1.0/24
exit

rule id 1
  action permit
  src-zone "trust"
  dst-zone "untrust"
  src-addr "Local_10.10.2.0/24"
  dst-addr "Any"
  service "Any"
  name "to_Internet"
exit

ip vrouter "trust-vr"
  snatrule id 1 from-zone "trust" to-zone "untrust" from address-book "Local_10.10.2.0/24" to address-book "Any"
service "Any" trans-to eif-ip mode dynamicport
exit
```

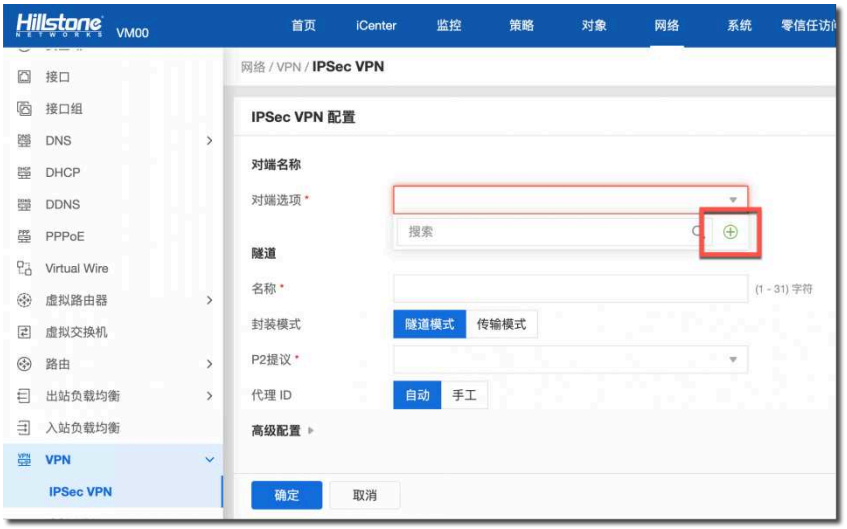
3. 在IPSec VPN页面点击新建按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 点击对端选项，点击右侧的“+”，创建新的对端选项，如下图配置VPN对端的相关配置，这里配置的是第一阶段安全提议，注意与FortiGate配置一致，并开启DPD，点击确定下发对端配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

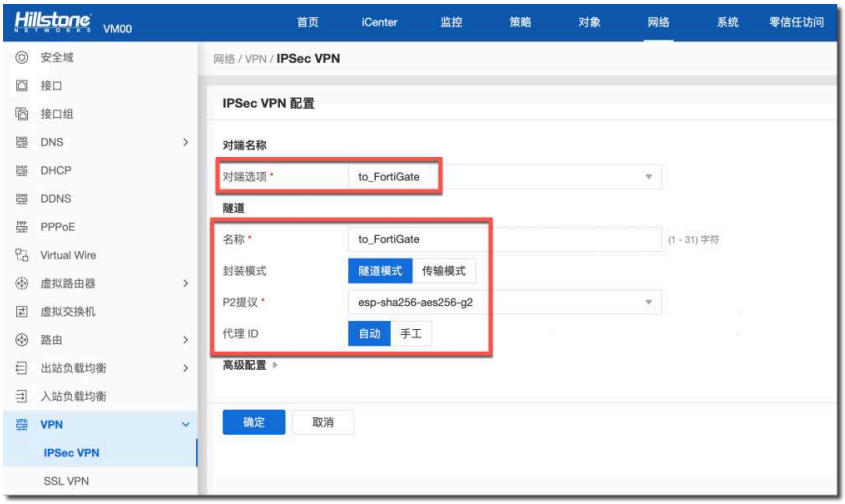





```
isakmp peer "to_FortiGate"
  isakmp-proposal "psk-sha256-aes256-g2"
  pre-share "$01011NMr$XE3F0ui+whYFfilc+Fx6mDJ7I8Y="
  peer 202.103.13.2
  accept-all-peer-id
  dpd interval 10 retry 3 periodic
  interface ethernet0/1
exit
```

5. “VPN对端配置”创建完成后，继续配置IPSec VPN，对端选项选择上步创建的“to_FortiGate”，配置二阶段安全提议与FortiGate端一致，高级配置中无需配置。

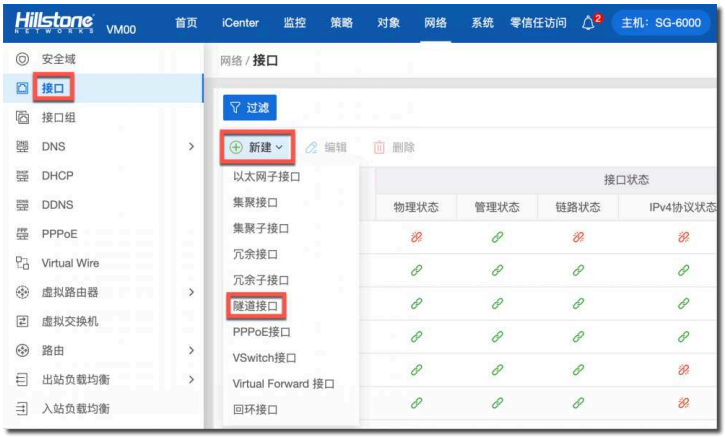
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

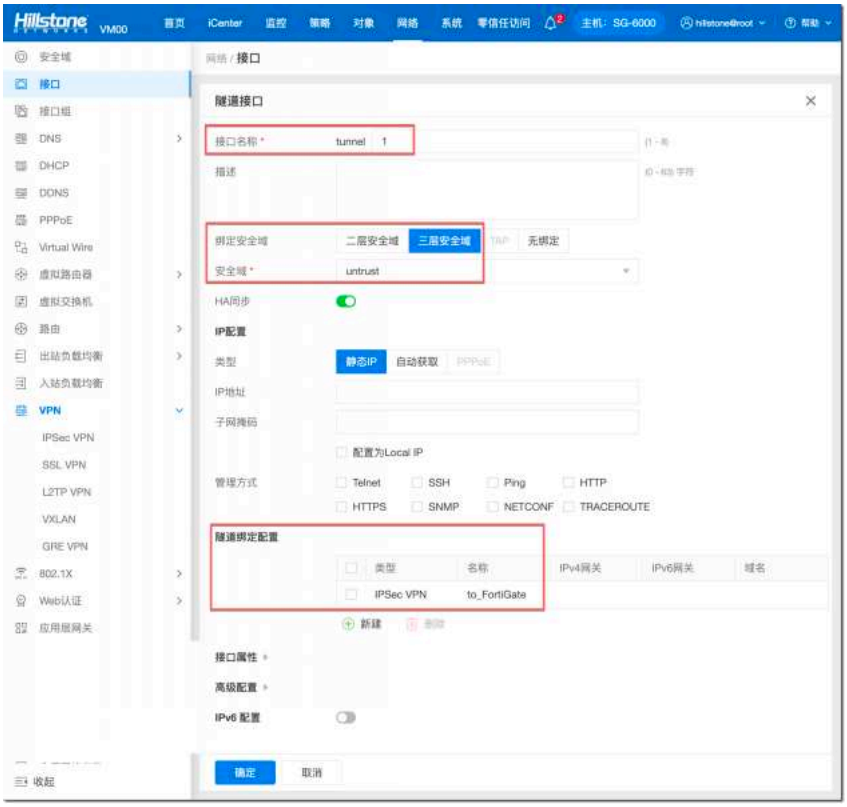



```
tunnel ipsec "to_FortiGate" auto sa-index 2
  ipsec-proposal "esp-sha256-aes128-g2"
  isakmp-peer "to_FortiGate"
exit
```

6. 创建隧道接口，并将IPSec VPN连接绑定至IPSec接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
interface tunnel1
  zone  "untrust"
  tunnel ipsec "to_FortiGate"
exit
```

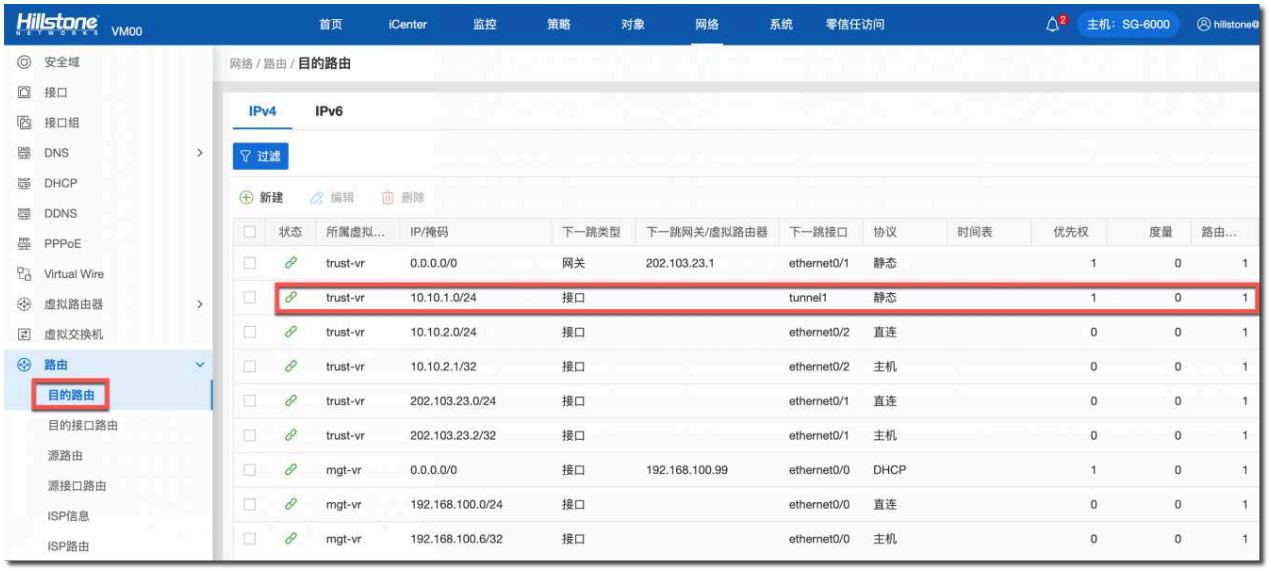
7. 配置IPSec VPN相关网段放通的安全策略，并将他们移动至上网策略之前。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
rule id 2
  action permit
  src-zone "untrust"
  dst-zone "trust"
  src-addr "Remote_10.10.1.0/24"
  dst-addr "Local_10.10.2.0/24"
  service "Any"
  name "VPN_from_FortiGate"
exit
rule id 3
  action permit
  src-zone "trust"
  dst-zone "untrust"
  src-addr "Local_10.10.2.0/24"
  dst-addr "Remote_10.10.1.0/24"
  service "Any"
  name "VPN_to_FortiGate"
exit
rule id 1
  action permit
  src-zone "trust"
  dst-zone "untrust"
  src-addr "Local_10.10.2.0/24"
  dst-addr "Any"
  service "Any"
  name "to_Internet"
exit
```

8. 添加去往FortiGate内网VPN网段的静态路由，出接口为tunnel接口。

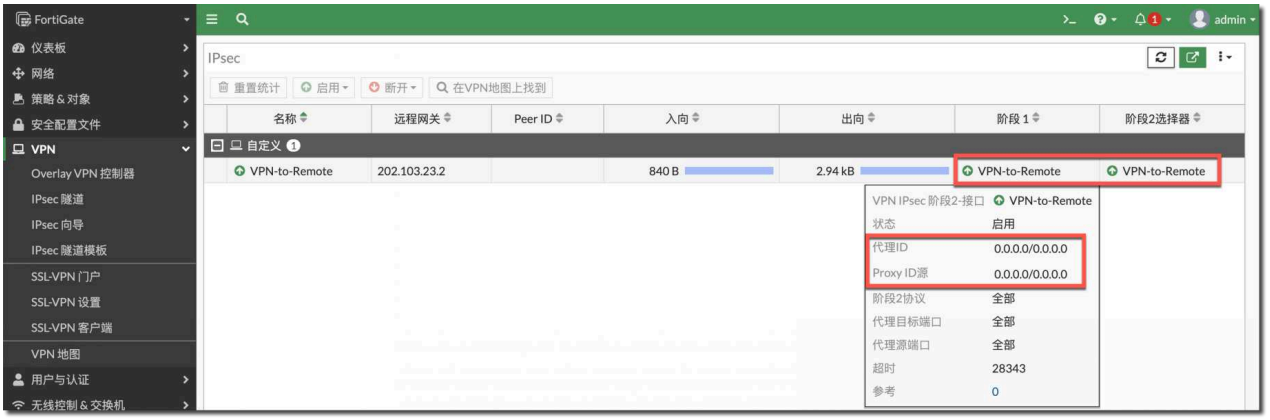



```
ip vrouter "trust-vr"
  ip route 10.10.1.0/24 "tunnel1"
exit
```

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Remote
version: 1
interface: port2 4
addr: 202.103.13.2:500 → 202.103.23.2:500
tun_id: 202.103.23.2/::202.103.23.2
remote_location: 0.0.0.0
network-id: 0
created: 1254s ago
IKE SA: created 1/1  established 1/1  time 120/120/120 ms
IPsec SA: created 1/7  established 1/2  time 0/65/130 ms
  id/spi: 6 682ffbe3bdcd7130/bca06b5547f0a164
  direction: initiator
  status: established 1254-1254s ago = 120ms
  proposal: aes256-sha256
  key: a45c9a51ac96f767-98ce117bc21328d4-431c2a6eeceb933e-af19239a1116dd28
  lifetime/rekey: 86400/84845
  DPD sent/recv: 00000000/000003bd

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Remote ver=1 serial=2 202.103.13.2:0→202.103.23.2:0 tun_id=202.103.23.2 tun_id6=::202.103.23.2
dst_mtu=1500 dpd-link=on weig1
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overla0
proxyid_num=1 child_num=0 refcnt=4 ilast=6 olast=6 ad=/0
stat: rxp=10 txp=35 rxb=840 txb=2940
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Remote proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=28252/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=28503/28800
  dec: spi=92c2ead0 esp=aes key=32 22c824606a1f39ec9f9ce853b7e78f0bceacf61695360474d5365d4df8448f0b
       ah=sha256 key=32 f501d221d046169419833ad4c6f6aa6d90155700048590023024a6e48dc12e3b
  enc: spi=2008ef27 esp=aes key=32 fbc3d717c22ec085dac575010867f28b798f13b0f95d92f37ebe1eb9baf9d997
       ah=sha256 key=32 4dc43f2f80f5b212cb399272a4fc2b765351b7c835bce4fe56370a06692b6b67
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.13.2 npu_selid=1 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

```

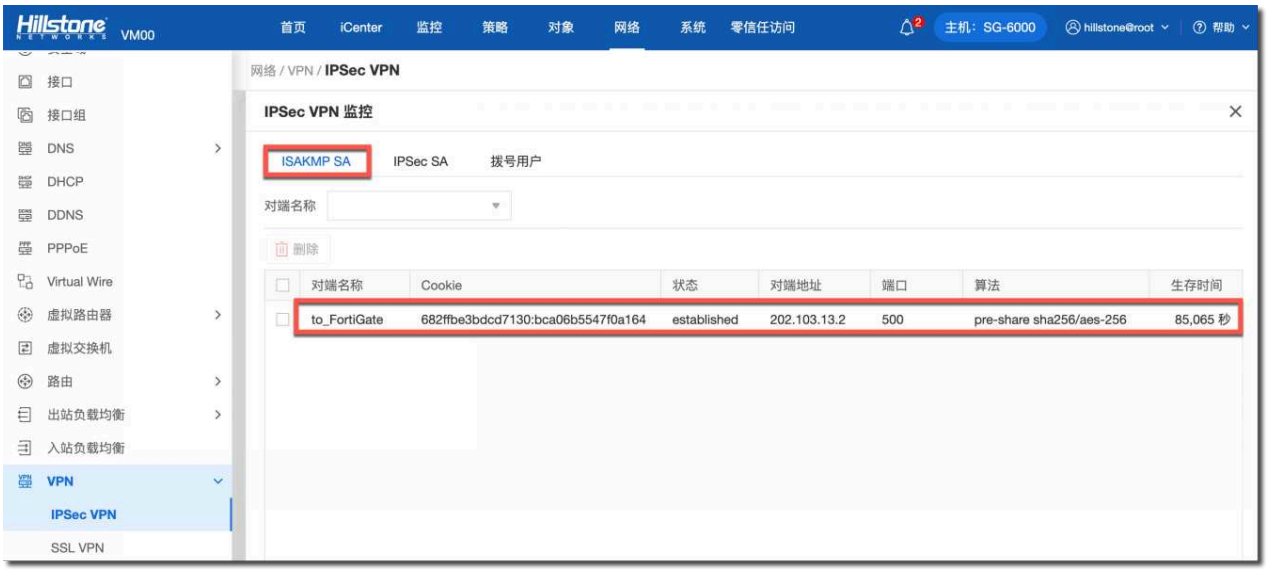

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.103.13.1, port2, [1/0]
C       10.10.1.0/24 is directly connected, port3
S       10.10.2.0/24 [10/0] via VPN-to-Remote tunnel 202.103.23.2, [1/0]
C       192.168.100.0/24 is directly connected, port1
C       202.103.13.0/24 is directly connected, port2
```

3. FortiGate侧PC1业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.1.2/24         10.10.1.1
       fe80::250:79ff:fe66:6805/64

VPCS> ping 10.10.2.2

84 bytes from 10.10.2.2 icmp_seq=1 ttl=62 time=3.442 ms
84 bytes from 10.10.2.2 icmp_seq=2 ttl=62 time=4.599 ms
84 bytes from 10.10.2.2 icmp_seq=3 ttl=62 time=1.291 ms
84 bytes from 10.10.2.2 icmp_seq=4 ttl=62 time=1.419 ms
84 bytes from 10.10.2.2 icmp_seq=5 ttl=62 time=1.397 ms
```

4. 山石防火墙查看IPSec连接状态。





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
SG-6000(config)# show isakmp sa
Total: 1
═══════════════════════════════════════════════════════════════════════════════════════
Cookies                            Gateway              Port      Algorithms                Lifetime
───────────────────────────────────────────────────────────────────────────────────────
682ffbe3bdcd7130:bca06b5547f0a164  202.103.13.2         500       pre-share  sha256/aes-256 84848
═══════════════════════════════════════════════════════════════════════════════════════

SG-6000(config)# show ipsec sa
Total: 1
S - Status, I - Inactive, A - Active;
═══════════════════════════════════════════════════════════════════════════════════════
Id    VPN                             Peer IP           Port Algorithms           SPI      Life(s) S
───────────────────────────────────────────────────────────────────────────────────────
3     to_FortiGate                    >202.103.13.2      500 esp:aes256/sha256/-  92c2ead0 28243   A
3     to_FortiGate                    <202.103.13.2      500 esp:aes256/sha256/-  2008ef27 28243   A
═══════════════════════════════════════════════════════════════════════════════════════
```

5. 查看山石防火墙的路由表，可以看到包含了手动配置的到FortiGate内网的路由。

```
SG-6000(config)# show ip route
Codes: K - kernel route, C - connected, S - static, N - Domain, Z - ISP, R - RIP, O - OSPF,
       B - BGP, D - DHCP, P - PPPoE, W - wireless, H - HOST, G - SCVPN, V - VPN, M - IMPORT,
       I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, * - FIB route, b - BFD enable

Routing Table for Virtual Router <trust-vr>
═══════════════════════════════════════════════════════════════════════
S>* 0.0.0.0/0 [1/0/1] via 202.103.23.1, ethernet0/1
S>* 10.10.1.0/24 [1/0/1] is directly connected, tunnel1
C>* 10.10.2.0/24 is directly connected, ethernet0/2
H>* 10.10.2.1/32 [0/0/1] is local address, ethernet0/2
C>* 202.103.23.0/24 is directly connected, ethernet0/1
H>* 202.103.23.2/32 [0/0/1] is local address, ethernet0/1
```

6. 山石防火墙侧PC2业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.2.2/24         10.10.2.1
       fe80::250:79ff:fe66:6806/64

VPCS> ping 10.10.1.2

84 bytes from 10.10.1.2 icmp_seq=1 ttl=62 time=1.715 ms
84 bytes from 10.10.1.2 icmp_seq=2 ttl=62 time=1.710 ms
84 bytes from 10.10.1.2 icmp_seq=3 ttl=62 time=7.731 ms
84 bytes from 10.10.1.2 icmp_seq=4 ttl=62 time=2.330 ms
84 bytes from 10.10.1.2 icmp_seq=5 ttl=62 time=1.684 ms
```

7. FortiGate侧抓包查看。

```
FortiGate # diagnose sniffer packet any 'host 10.10.2.2 and host 10.10.1.2 and icmp' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.2 and host 10.10.1.2 and icmp]
2023-04-10 16:27:56.023973 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:56.024029 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:56.026679 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:56.026698 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:57.029816 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:57.029855 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:57.030097 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:57.030109 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:58.031820 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:58.031856 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:58.032037 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:58.032049 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:59.033955 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:27:59.033988 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
2023-04-10 16:27:59.034145 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:27:59.034151 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:28:00.036548 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:28:00.036586 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-10 16:28:00.036803 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-10 16:28:00.036816 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```

2. 山石SG6000防火墙IPsec VPN Debug：

```
SG-6000[DBG]# debug vpn
SG-6000[DBG]# show logging debug
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与Palo Alto防火墙建立IPSec VPN

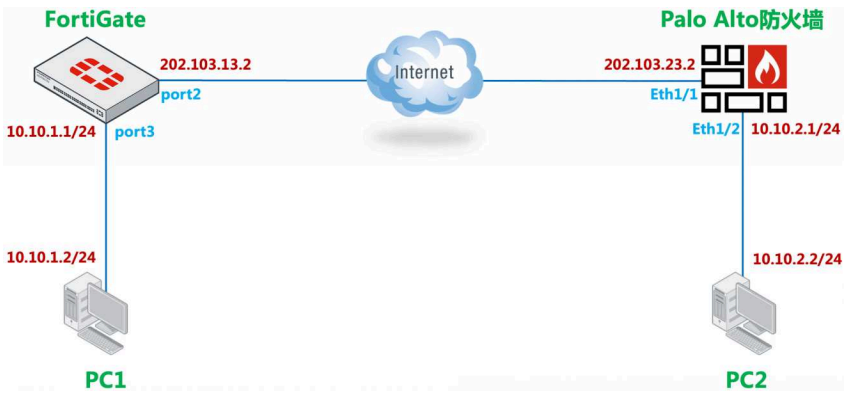
网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与10.10.2.0/24两个网段的通信。与Palo Alto防火墙进行IPsec VPN（IKE v1）对接。

Palo Alto防火墙版本信息：

```
admin@PA-VM> show system info

hostname: PA-VM
ip-address: 192.168.100.3
public-ip-address: unknown
netmask: 255.255.255.0
default-gateway: 192.168.100.99
ip-assignment: dhcp
ipv6-address: unknown
ipv6-link-local-address: fe80::5200:ff:fe01:0/64
ipv6-default-gateway:
mac-address: 50:00:00:01:00:00
time: Tue Apr 11 19:13:23 2023
uptime: 0 days, 0:10:21
family: vm
model: PA-VM
serial: unknown
vm-mac-base: BA:DB:EE:FB:AD:00
vm-mac-count: 255
vm-uuid: A42F5C9E-B1D9-4A19-B229-D959AF933A2B
vm-cpuid: KVM:63060000FDFB8B07
vm-license: none
vm-cap-tier: unknown
vm-cpu-count: 2
vm-memory: 4031324
vm-mode: KVM
cloud-mode: non-cloud
sw-version: 10.1.0
global-protect-client-package-version: 0.0.0
device-dictionary-version: 1-211
device-dictionary-release-date:
```

网络拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Palo Alto防火墙
  - 基本上网配置
  - 配置IPsec VPN

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略。

配置步骤

FortiGate

1. 基本上网配置。







2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 如图配置网络、认证、第一阶段、第二阶段。

重要

和山石/Palo Alto防火墙对接IPSec推荐使用全0的感兴趣流，这些厂商设备与FortiGate一致，创建IPSec时会创建虚拟的IPSec接口，通过路由对VPN流量进行引流，将需要加密的数据送到IPSec接口（当然写细化的感兴趣流也是可以的）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

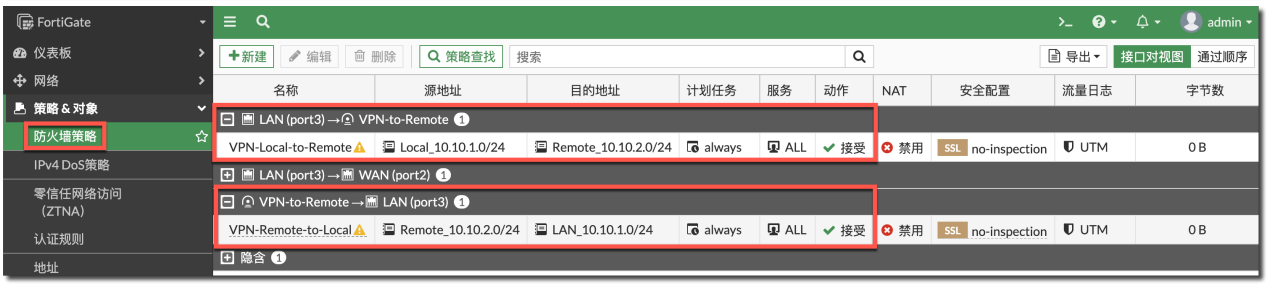


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN-to-Remote"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set dhgrp 14 5 2
        set remote-gw 202.103.23.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-Remote"
        set phase1name "VPN-to-Remote"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
end
```

5. 配置VPN相关的网段地址对象和防火墙策略。






```
config firewall address
    edit "Local_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Remote_10.10.2.0/24"
        set subnet 10.10.2.0 255.255.255.0
    next
end

config firewall policy
    edit 2
        set name "VPN-Local-to-Remote"
        set srcintf "port3"
        set dstintf "VPN-to-Remote"
        set action accept
        set srcaddr "Local_10.10.1.0/24"
        set dstaddr "Remote_10.10.2.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-Remote-to-Local"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set srcintf "VPN-to-Remote"
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_10.10.2.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置VPN业务网段的静态路由。

重要

相关VPN的路由配置中“黑洞路由的意义：

你可能会遇到以下的VPN业务问题：通过VPN的SIP电话，时不时中断，无法向服务器成功注册？通过VPN的Radius认证无法经常会无法认证成功？ 通过VPN的AP注册到总部时不时会中断？持续的PRGT监控ping总部的服务器，时不时会显示中断？

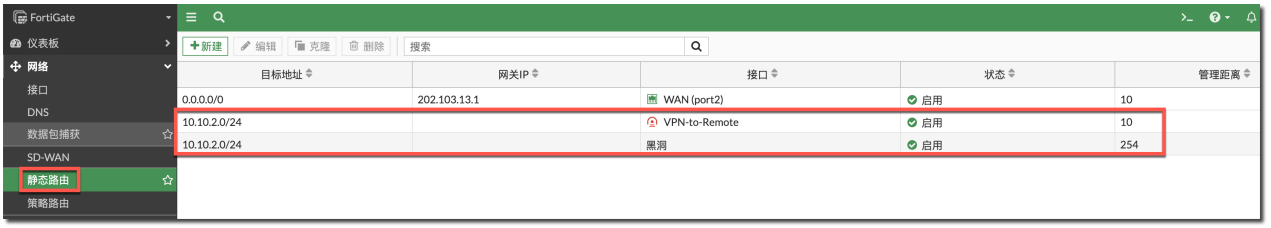
VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量（SIP注册请求/Radius/Capwap/ICMP）会因为查询到了默认路由而走向了WAN（Internet），从而产生了错误的UDP-NAT-Seesion，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，SIP等VPN旧的业务流量依旧会走到错误的Session上去，从而引起该业务异常。

解决方法：

- 方法一：配置去往VPN业务网段的“黑洞路由”，管理距离为254，VPN正常的情况下此黑洞路由不生效，而当VPN中断的时候，黑洞路由浮起来并且生效，将VPN中断时候的VPN流量丢弃，避免将流量转发到互联网而产生错误的session。配置VPN的备份黑洞路由的意义在此。
- 方法二：配置源接口：LAN，目的接口：WAN，源IP：本地内网网段，目的IP：对端内网网段，动作：丢包的策略。将此去往Internet的私网（无用的）流量丢弃掉，避免FGT产生这种错误的session，从而避免了UDP业务时不时中断的问题。
- 方法三：在全局下开启“set snat-route-change enable”，一旦路由发生变化，将相关的会话flag置位为“Dirty”，清除路由缓存并重新查找目的IP的下一跳地址，这样VPN隧道恢复的时候，流量也会相应的切换到VPN隧道里面来。

```
FortiGate # config system global
FortiGate (global) # set snat-route-change enable
FortiGate (global) # end
```

三种方式任意选择一种即可。推荐使用黑洞路由方式。

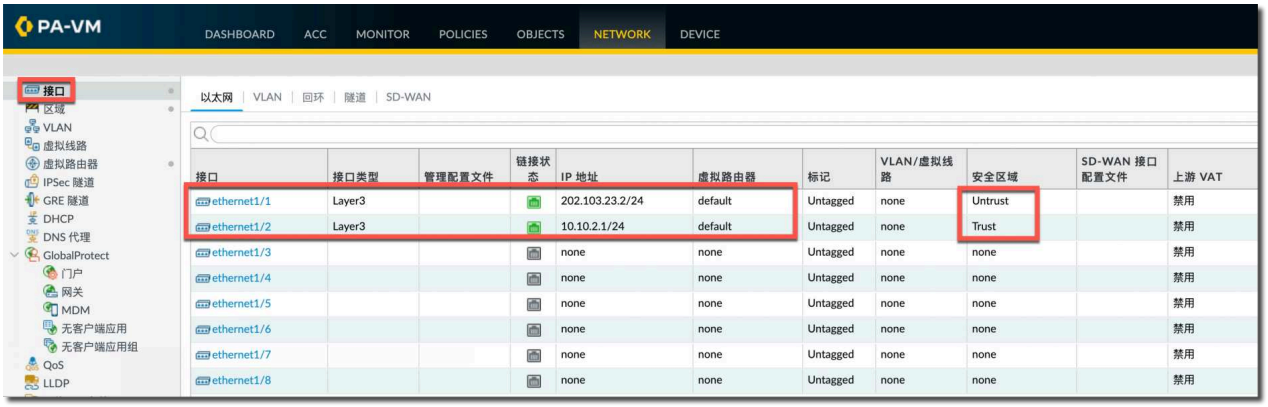


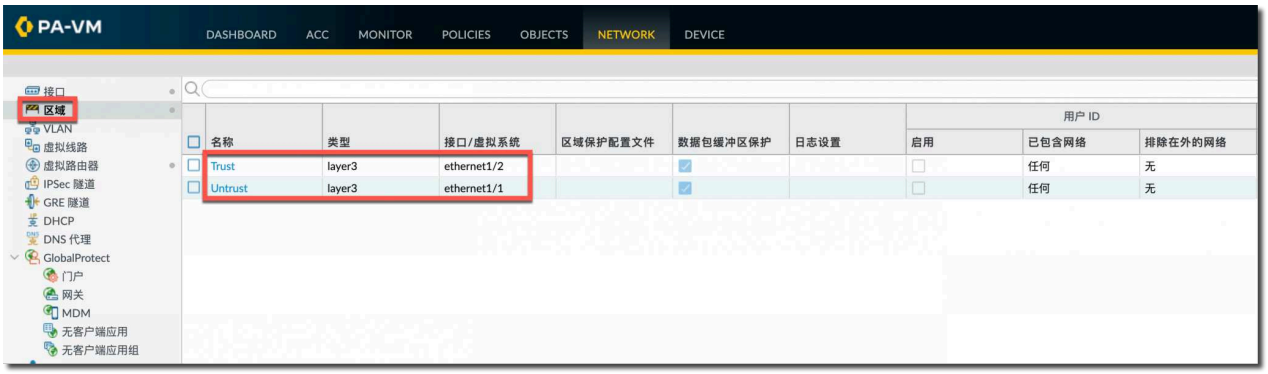

```
config router static
    edit 1
        set gateway 202.103.12.1
        set device "port2"
    next
    edit 2
        set dst 10.10.2.0 255.255.255.0
        set device "VPN-to-Remote"
    next
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

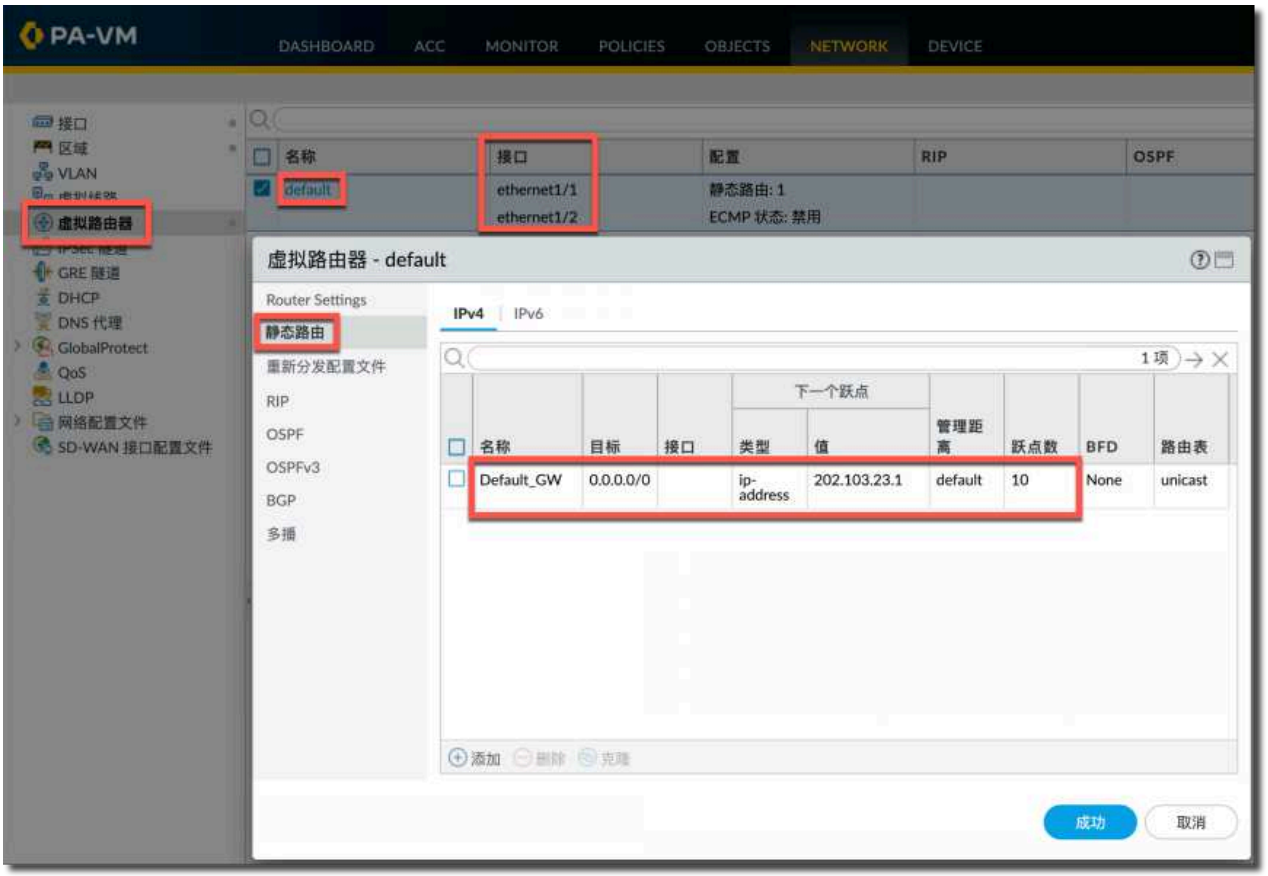
Palo Alto

1. 基本IP与路由配置，请注意一定要将接口加入安全域和虚拟路由器，否则接口无法通信。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.








```
network {
  interface {
    ethernet {
      ethernet1/1 {
        layer3 {
          ip {
            202.103.23.2/24;
          }
        }
```

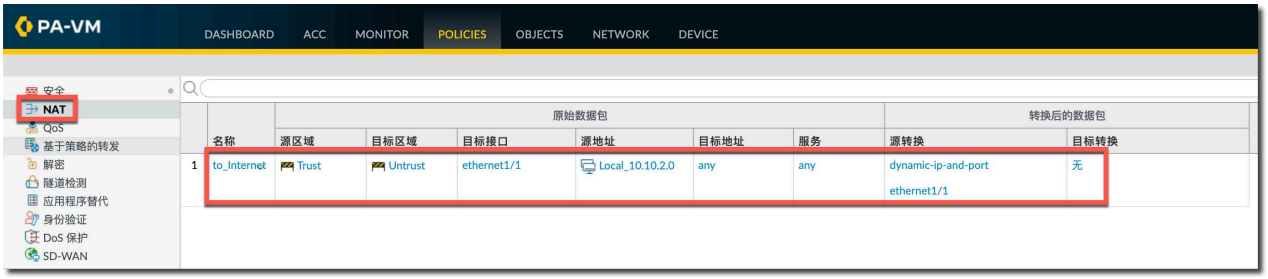

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
      }
      ethernet1/2 {
        layer3 {
          ip {
            10.10.2.1/24;
          }
        }
      }
    }
  }
  virtual-router {
    default {
      routing-table {
        ip {
          static-route {
            Default_GW {
              nexthop {
                ip-address 202.103.23.1;
              }
              metric 10;
              destination 0.0.0.0/0;
              route-table {
                unicast;
              }
            }
          }
        }
      }
      interface [ ethernet1/1 ethernet1/2];
    }
  }
}
```

2. 地址对象、策略、NAT配置。







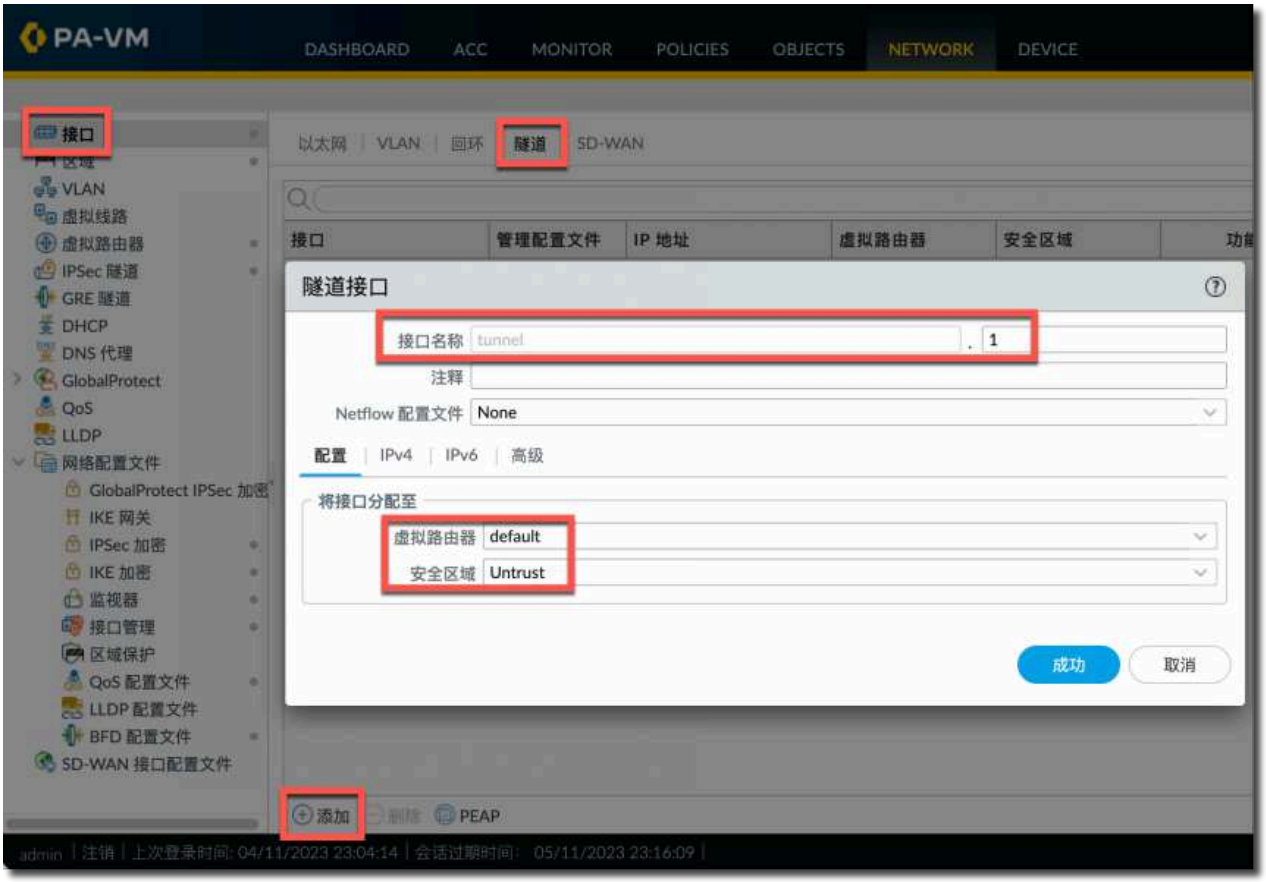

```
address {
  Local_10.10.2.0 {
    ip-netmask 10.10.2.0/24;
  }
  Remote_10.10.1.0 {
    ip-netmask 10.10.1.0/24;
  }
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
}

rulebase {
  security {
    rules {
      to_Internet {
        to Untrust;
        from Trust;
        source Local_10.10.2.0;
        destination any;
        source-user any;
        category any;
        application any;
        service application-default;
        source-hip any;
        destination-hip any;
        action allow;
      }
    }
  }
  nat {
    rules {
      to_Internet {
        source-translation {
          dynamic-ip-and-port {
            interface-address {
              interface ethernet1/1;
            }
          }
        }
        to Untrust;
        from Trust;
        source Local_10.10.2.0;
        destination any;
        service any;
        to-interface ethernet1/1;
      }
    }
  }
}
```

3. 创建IPSec隧道接口，并加入安全域和虚拟路由器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```
network {
  interface {
    tunnel {
      units {
        tunnel.1;
      }
    }
  }
  virtual-router {
    default {
      interface [ ethernet1/1 ethernet1/2 tunnel tunnel.1];
    }
  }
}

zone {
  Untrust {
    network {
      layer3 [ ethernet1/1 tunnel tunnel.1];
    }
  }
}
```

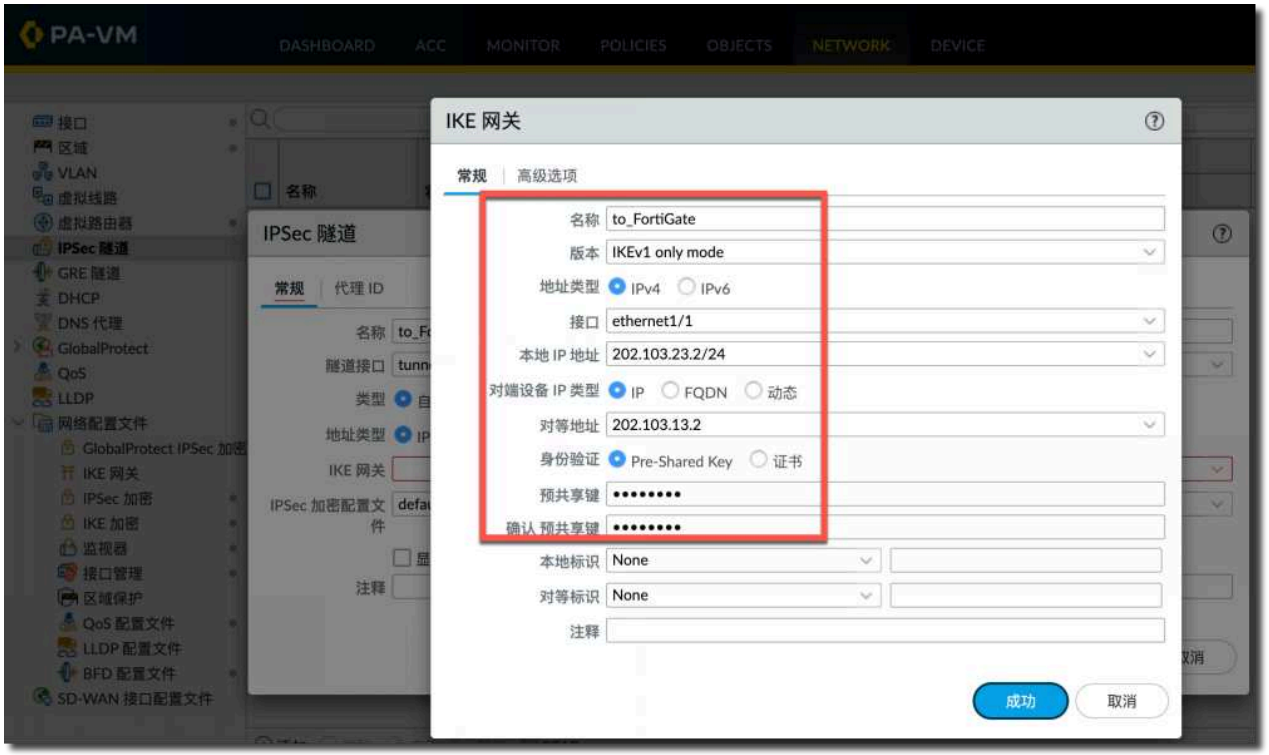

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

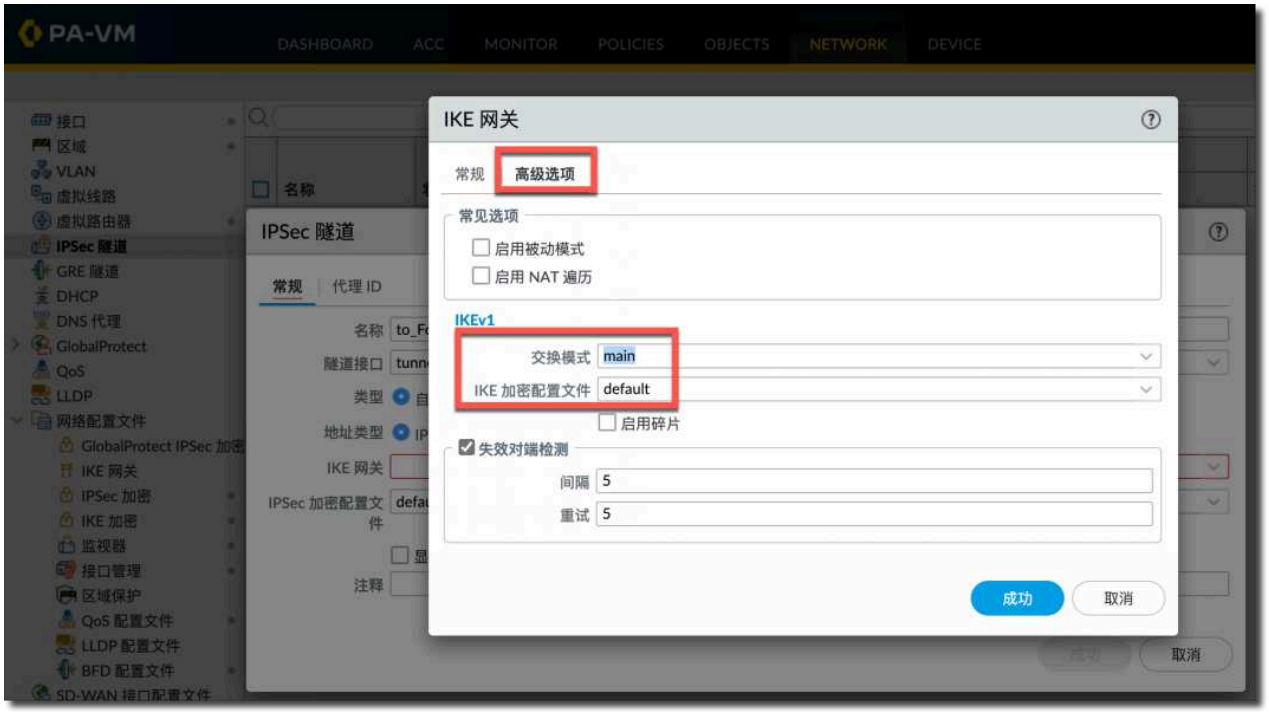
4. 在IPSec隧道页面点击添加按钮，输入隧道名称，隧道接口选择上步创建的“tunnel.1”。在“IKE网关”中选择“新IKE网关”。



5. 在弹出的“IKE网关”页面中，填写名称，版本选择IKEv1，接口选择自身用于建立IPSec的接口，对端VPN网关地址，预共享密钥。在“高级选项”中，配置交换模式为main，可以修改默认的一阶段安全提议，注意要和FortiGate端保持一致，此例中FortiGate的安全算法已配置为和Palo Alto中“default”包含的算法一致，所以不再进行修改（自定义的一阶段安全提议可以到“NETWORK→网络配置文件→IKE加密”中创建）。随后下发“IKE网关”的配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





6. “IKE网关”配置下发后，返回“IPSec隧道”窗口，确认“IKE网关”选择为上步创建的IKE网关，IPSec加密配置文件（二阶段安全提议）选择“default”（注意要和FortiGate端保持一致，此例中FortiGate的安全算法已配置为和Palo Alto中“default”包含的算法一致，所以不再进行修改，自定义的二阶段安全提议可以到“NETWORK→网络配置文件→IPSec加密”中创建）。“代理ID”选项卡无需配置（默认为0.0.0.0/0↔0.0.0.0/0）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
network {
  ike {
    crypto-profiles {
      ike-crypto-profiles {
        default {
          encryption [ aes-128-cbc 3des];
          hash sha1;
          dh-group group2;
          lifetime {
            hours 8;
          }
        }
      }
      ipsec-crypto-profiles {
        default {
          esp {
            encryption [ aes-128-cbc 3des];
            authentication sha1;
          }
          dh-group group2;
          lifetime {
            hours 1;
          }
        }
      }
    }
    gateway {
      to_FortiGate {
        authentication {
          pre-shared-key {
            key -AQ==pkKner19T1G/kibOr4kfy7Wymbg=sg4ErcrrUBiaoIjlTToVEA==;
          }
        }
        protocol {
          ikev1 {
            dpd {
              enable yes;
            }
            exchange-mode main;
          }
        }
        local-address {
          ip 202.103.23.2/24;
          interface ethernet1/1;
        }
        protocol-common {
          nat-traversal {
            enable no;
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
          }
          fragmentation {
            enable no;
          }
        }
        peer-address {
          ip 202.103.13.2;
        }
      }
    }
  }
  tunnel {
    ipsec {
      to_FortiGate {
        auto-key {
          ike-gateway {
            to_FortiGate;
          }
        }
        tunnel-monitor {
          enable no;
        }
        tunnel-interface tunnel;
      }
    }
  }
}
```

7. 配置IPSec VPN相关网段放通的安全策略，并将他们移动至上网策略之前。

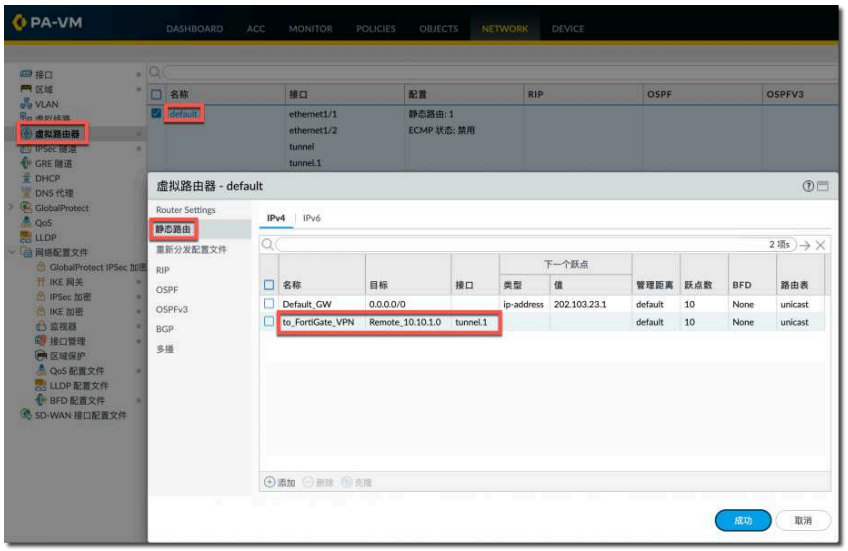



```
rulebase {
  security {
    rules {
      VPN_to_FortiGate {
        to Untrust;
        from Trust;
        source Local_10.10.2.0;
        destination Remote_10.10.1.0;
        source-user any;
        category any;
        application any;
        service application-default;
        source-hip any;
        destination-hip any;
        action allow;
      }
      VPN_from_FortiGate {
        to Trust;
        from Untrust;
        source Remote_10.10.1.0;
        destination Local_10.10.2.0;
        source-user any;
        category any;
        application any;
        service application-default;
        source-hip any;
        destination-hip any;
        action allow;
      }
      to_Internet {
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        to Untrust;
        from Trust;
        source Local_10.10.2.0;
        destination any;
        source-user any;
        category any;
        application any;
        service application-default;
        source-hip any;
        destination-hip any;
        action allow;
      }
    }
  }
}
```

8. 添加去往FortiGate内网VPN网段的静态路由，出接口为tunnel.1接口，下一跳配置为“None”即可。




```
network {
  virtual-router {
    default {
      routing-table {
        ip {
          static-route {
            to_FortiGate_VPN {
              path-monitor {
                enable no;
                failure-condition any;
                hold-time 2;
              }
              interface tunnel.1;
              metric 10;
              destination Remote_10.10.1.0;
              route-table {
                unicast;
              }
            }
          }
        }
      }
      interface [ ethernet1/1 ethernet1/2 tunnel tunnel.1];
    }
  }
}
```

9. 最后，点击右上角的commit按钮提交所有配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。




```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Remote
version: 1
interface: port2 4
addr: 202.103.13.2:500 → 202.103.23.2:500
tun_id: 202.103.23.2/::202.103.23.2
remote_location: 0.0.0.0
network-id: 0
created: 1403s ago
IKE SA: created 1/1  established 1/1  time 120/120/120 ms
IPsec SA: created 1/3  established 1/1  time 140/140/140 ms
  id/spi: 0 d73a6ee8d0baf991/db995f50650cc6b5
  direction: initiator
  status: established 1403-1403s ago = 120ms
  proposal: aes128-sha1
  key: fd7f588b849be1d4-d63993f074d6b8f8
  lifetime/rekey: 86400/84697
  DPD sent/recv: 0000003e/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Remote ver=1 serial=3 202.103.13.2:0→202.103.23.2:0 tun_id=202.103.23.2 tun_id6=::202.103.23.2
dst_mtu=1500 dpd-link=on weig1
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overla0
proxyid_num=1 child_num=0 refcnt=4 ilast=2 olast=2 ad=/0
stat: rxp=12 txp=17 rxb=1008 txb=1484
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=63
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Remote proto=0 sa=1 ref=2 serial=2 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=2205/0B replaywin=2048
       seqno=12 esn=0 replaywin_lastseq=0000000c qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3300/3600
  dec: spi=35f11fb3 esp=aes key=16 2aba5fd6c7959ed2ee4dbd4653f2e42f
       ah=sha1 key=20 78b303176925e02007e758e1b4f3b2a43fcaab7e
  enc: spi=b5d1ae56 esp=aes key=16 a5d0f8ace26a19dd6c5e1089c0b4f755
       ah=sha1 key=20 c99af8e83adcd0b435fca71d0b25302ca84cc4f1
  dec:pkts/bytes=24/2016, enc:pkts/bytes=34/4132
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.13.2 npu_selid=3 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. 查看FortiGate的路由表。

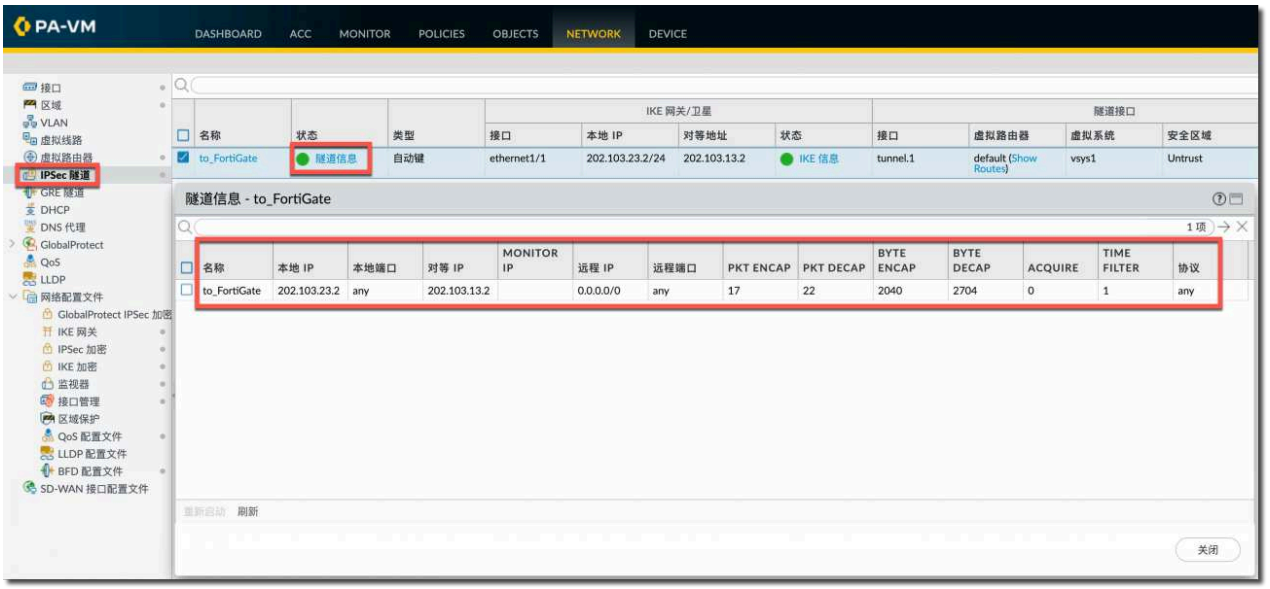
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.103.13.1, port2, [1/0]
C       10.10.1.0/24 is directly connected, port3
S       10.10.2.0/24 [10/0] via VPN-to-Remote tunnel 202.103.23.2, [1/0]
C       192.168.100.0/24 is directly connected, port1
C       202.103.13.0/24 is directly connected, port2
```

3. FortiGate侧PC1业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.1.2/24         10.10.1.1
       fe80::250:79ff:fe66:6804/64

VPCS> ping 10.10.2.2

84 bytes from 10.10.2.2 icmp_seq=1 ttl=62 time=4.250 ms
84 bytes from 10.10.2.2 icmp_seq=2 ttl=62 time=2.122 ms
84 bytes from 10.10.2.2 icmp_seq=3 ttl=62 time=2.039 ms
84 bytes from 10.10.2.2 icmp_seq=4 ttl=62 time=1.824 ms
84 bytes from 10.10.2.2 icmp_seq=5 ttl=62 time=2.243 ms
```

4. Palo Alto防火墙查看IPSec连接状态。




```
admin@PA-VM> show vpn ike-sa
IKEv1 phase-1 SAs
GwID/client IP  Peer-Address          Gateway Name                                                  Role Mode
Algorithm             Established     Expiration      V  ST Xt Phase2
_______________  ____________          ____________                                                  ____ ____ -
________              ___________     __________      -  -- -- ______
1               202.103.13.2          to_FortiGate                                                  Resp Main
PSK/ DH2/A128/SHA1    Apr.12 00:11:29 Apr.12 08:11:29 v1 13 1  1
Show IKEv1 IKE SA: Total 1 gateways found. 1 ike sa found.
IKEv1 phase-2 SAs
Gateway Name                                                  TnID     Tunnel                GwID/IP
Role Algorithm          SPI(in)  SPI(out) MsgID    ST Xt
____________                                                  ____     ______                _______          -
--- _________          _______  ________ _____    -- --
to_FortiGate                                                  1        to_FortiGate          1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Resp ESP/ DH2/tunl/SHA1 B5D1AE56 35F11FB3 689E6AC0 9  1
Show IKEv1 phase2 SA: Total 1 gateways found. 1 ike sa found.

admin@PA-VM> show vpn ipsec-sa
GwID/client IP  TnID   Peer-Address           Tunnel(Gateway)
Algorithm          SPI(in)  SPI(out) life(Sec/KB)             remain-time(Sec)
———————————   ———   ———————————           ———————————————
———————————          ———————  ———————— ———————————           ———————————————
1               1      202.103.13.2           to_FortiGate(to_FortiGate)
ESP/A128/SHA1      B5D1AE56 35F11FB3 3600/Unlimited           2152
Show IPSec SA: Total 1 tunnels found. 1 ipsec sa found.

admin@PA-VM> show vpn flow
total tunnels configured:                                   1
filter - type IPSec, state any
total IPSec tunnel configured:                              1
total IPSec tunnel shown:                                   1
id    name                                                          state   monitor local-ip
peer-ip                     tunnel-i/f                                  ————    ———————  ————————
--    ———————————————                                                 ————    ———————  ————————
————————                    ——————————
1     to_FortiGate                                                  active  off     202.103.23.2
202.103.13.2                tunnel.1
```

5. 查看Palo Alto防火墙的路由表，可以看到包含了手动配置的到FortiGate内网的路由。

```
admin@PA-VM> show routing route

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2, E:ecmp, M:multicast
VIRTUAL ROUTER: default (id 1)
  ==========
destination                             nexthop                             metric flags      age
interface          next-AS
0.0.0.0/0                               202.103.23.1                        10     A S
ethernet1/1
10.10.1.0/24                            0.0.0.0                             10     A S
tunnel.1
10.10.2.0/24                            10.10.2.1                           0      A C
ethernet1/2
10.10.2.1/32                            0.0.0.0                             0      A H
202.103.23.0/24                         202.103.23.2                        0      A C
ethernet1/1
202.103.23.2/32                         0.0.0.0                             0      A H
total routes shown: 6
```

6. Palo Alto防火墙侧PC2业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.2.2/24         10.10.2.1
       fe80::250:79ff:fe66:6805/64

VPCS> ping 10.10.1.2

84 bytes from 10.10.1.2 icmp_seq=1 ttl=62 time=2.099 ms
84 bytes from 10.10.1.2 icmp_seq=2 ttl=62 time=2.617 ms
84 bytes from 10.10.1.2 icmp_seq=3 ttl=62 time=2.074 ms
84 bytes from 10.10.1.2 icmp_seq=4 ttl=62 time=2.024 ms
84 bytes from 10.10.1.2 icmp_seq=5 ttl=62 time=1.944 ms
```

7. FortiGate侧抓包查看。

```
FortiGate # diagnose sniffer packet any 'host 10.10.2.2 and host 10.10.1.2 and icmp' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.2 and host 10.10.1.2 and icmp]
2023-04-12 15:38:12.130447 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:12.130504 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:12.130732 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
2023-04-12 15:38:12.130746 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:13.134398 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:13.134471 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:13.134728 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:13.134745 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:14.137358 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:14.137391 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:14.137592 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:14.137600 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:15.140135 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:15.140174 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:15.140321 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:15.140334 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:16.143326 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:16.143362 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-12 15:38:16.143547 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-12 15:38:16.143560 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

   - 抓取IPsec VPN的IKE协商包：

     ```
     diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
     ```

   - 抓取IPsec VPN的ESP加密数据包：

     ```
     diagnose sniffer packet any "host 101.1.1.1 and esp" 4
     ```

   - 抓取IPsec VPN的明文业务数据包：

     ```
     diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
     ```

   - 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

     ```
     FortiGate # config vpn ipsec phase1-interface
     FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
     FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
     FortiGate (BJ-OSPF-TO-SH) # end
     ```

2. Palo Alto防火墙IPsec VPN Debug：

```
debug ike global on debug
less mp-log ikemgr.log
debug ike pcap on
view-pcap no-dns-lookup yes no-port-lookup yes debug-pcap ikemgr.pcap
debug ike pcap off
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与Check Point防火墙建立IPSec VPN

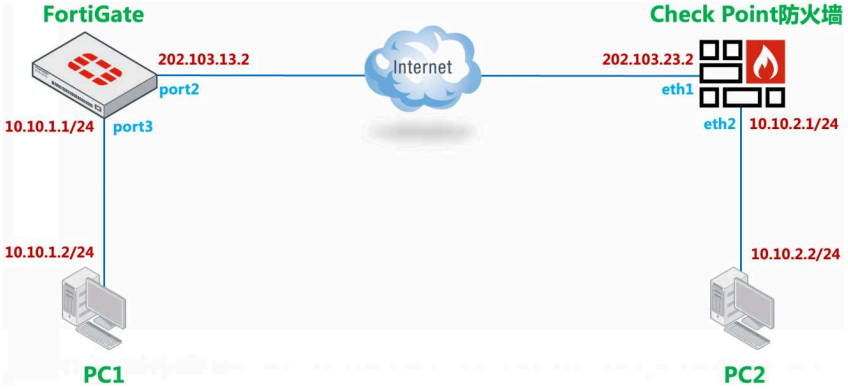
网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与10.10.2.0/24两个网段的通信。与Check Point防火墙进行IPsec VPN（IKE v1）对接。

Check Point防火墙版本：

```
gw-000100> ver
Product version Check Point Gaia R81.10
OS build 335
OS kernel version 3.10.0-957.21.3cpx86_64
OS edition 64-bit
```

网络拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Check Point防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略。

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 如图配置网络、认证、第一阶段、第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

由于Check Point的IPSec配置需要配置明细的感兴趣流，FortiGate与Check Point防火墙对接IPSec需要对应使用明细的感兴趣流。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

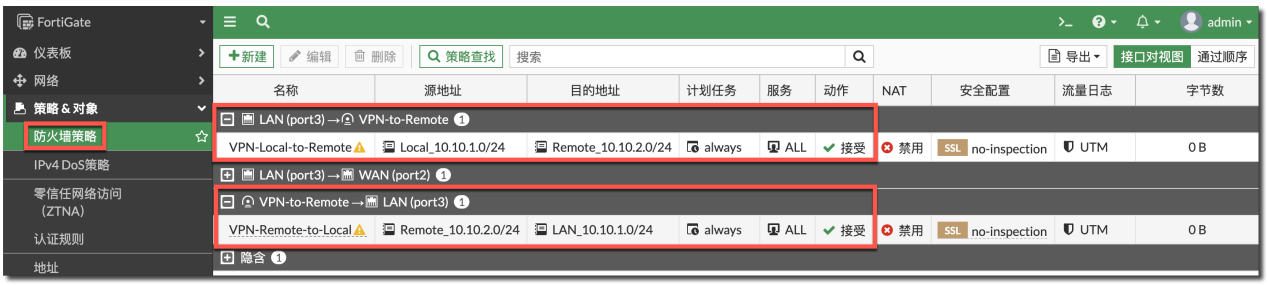


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN-to-Remote"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set dhgrp 14 5 2
        set remote-gw 202.103.23.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-Remote"
        set phase1name "VPN-to-Remote"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
end
```

5. 配置VPN相关的网段地址对象和防火墙策略。






```
config firewall address
    edit "Local_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Remote_10.10.2.0/24"
        set subnet 10.10.2.0 255.255.255.0
    next
end

config firewall policy
    edit 2
        set name "VPN-Local-to-Remote"
        set srcintf "port3"
        set dstintf "VPN-to-Remote"
        set action accept
        set srcaddr "Local_10.10.1.0/24"
        set dstaddr "Remote_10.10.2.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-Remote-to-Local"
        set srcintf "VPN-to-Remote"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_10.10.2.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置VPN业务网段的静态路由。

重要

相关VPN的路由配置中“黑洞路由的意义：

你可能会遇到以下的VPN业务问题：通过VPN的SIP电话，时不时中断，无法向服务器成功注册？通过VPN的Radius认证无法经常会无法认证成功？通过VPN的AP注册到总部时不时会中断？持续的PRGT监控ping总部的服务器，时不时会显示中断？

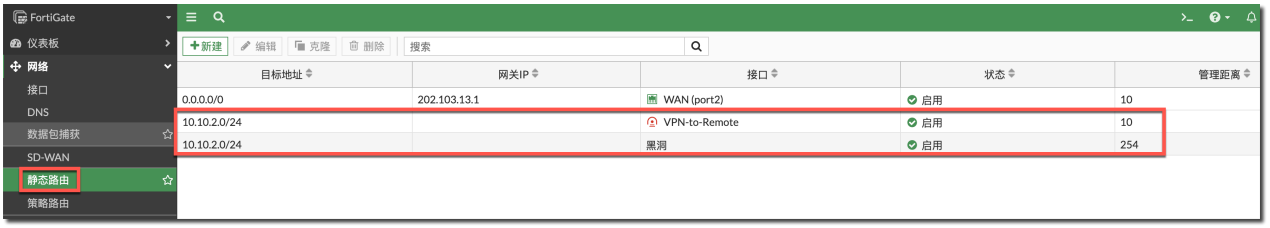
VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量（SIP注册请求/Radius/Capwap/ICMP）会因为查询到了默认路由而走向了WAN（Internet），从而产生了错误的UDP-NAT-Seesion，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，SIP等VPN旧的业务流量依旧会走到错误的Session上去，从而引起该业务异常。

解决方法：

- 方法一：配置去往VPN业务网段的“黑洞路由”，管理距离为254，VPN正常的情况下此黑洞路由不生效，而当VPN中断的时候，黑洞路由浮起来并且生效，将VPN中断时候的VPN流量丢弃，避免将流量转发到互联网而产生错误的session。配置VPN的备份黑洞路由的意义在此。
- 方法二：配置源接口：LAN，目的接口：WAN，源IP：本地内网网段，目的IP：对端内网网段，动作：丢包的策略。将此去往Internet的私网（无用的）流量丢弃掉，避免FGT产生这种错误的session，从而避免了UDP业务时不时中断的问题。
- 方法三：在全局下开启“set snat-route-change enable”，一旦路由发生变化，将相关的会话flag置位为“Dirty”，清除路由缓存并重新查找目的IP的下一跳地址，这样VPN隧道恢复的时候，流量也会相应的切换到VPN隧道里面来。

```
FortiGate # config system global
FortiGate (global) # set snat-route-change enable
FortiGate (global) # end
```

三种方式任意选择一种即可。推荐使用黑洞路由方式。

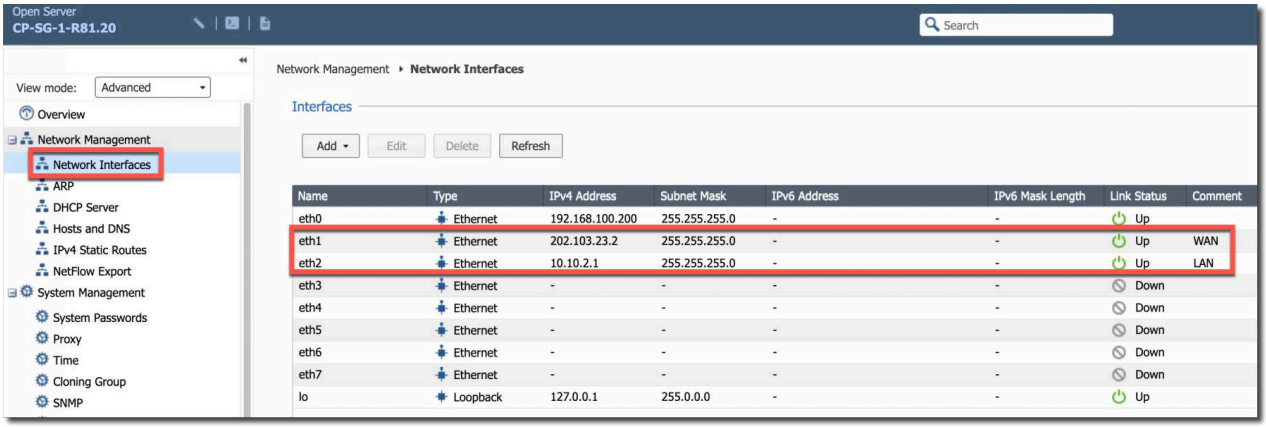


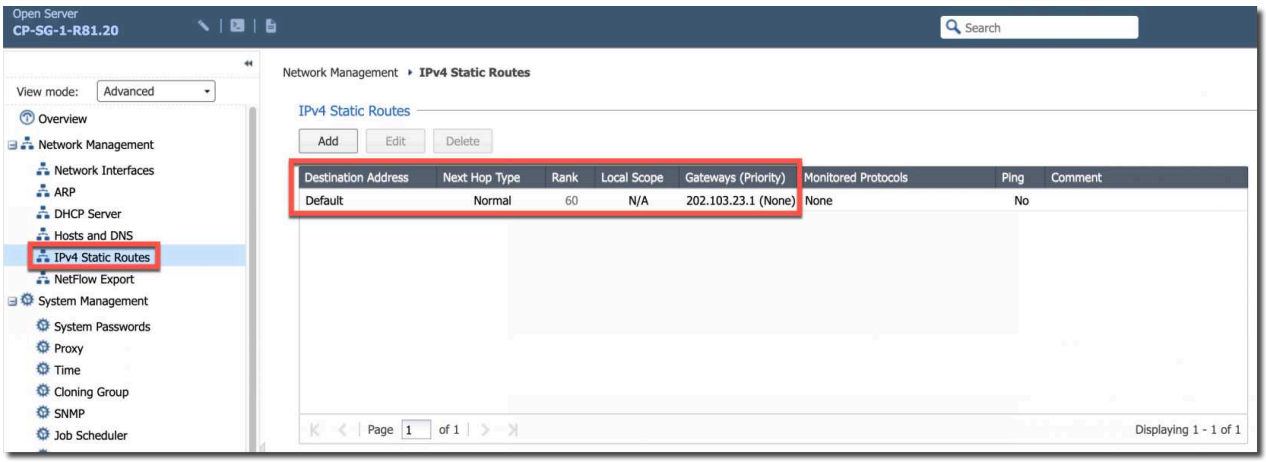

```
config router static
    edit 1
        set gateway 202.103.12.1
        set device "port2"
    next
    edit 2
        set dst 10.10.2.0 255.255.255.0
        set device "VPN-to-Remote"
    next
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

Check Point防火墙

1. 进入Check Point防火墙的Web管理页面，配置基本IP与路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



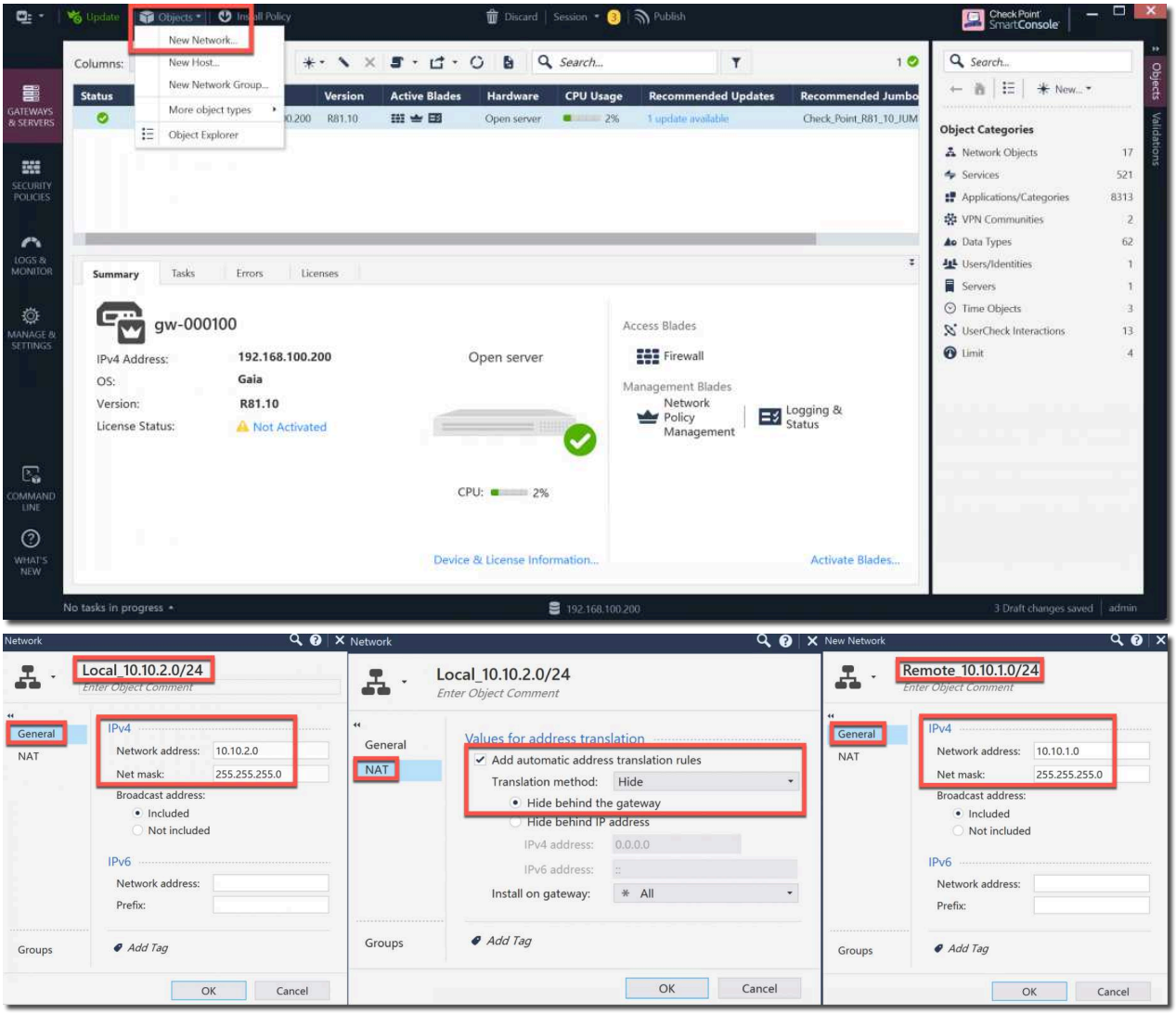



```
set interface eth1 comments "WAN"
set interface eth1 link-speed 1000M/full
set interface eth1 state on
set interface eth1 auto-negotiation on
set interface eth1 mtu 1500
set interface eth1 ipv4-address 202.103.23.2 mask-length 24
set interface eth2 comments "LAN"
set interface eth2 link-speed 1000M/full
set interface eth2 state on
set interface eth2 auto-negotiation on
set interface eth2 mtu 1500
set interface eth2 ipv4-address 10.10.2.1 mask-length 24

set static-route default nexthop gateway address 202.103.23.1 on
```

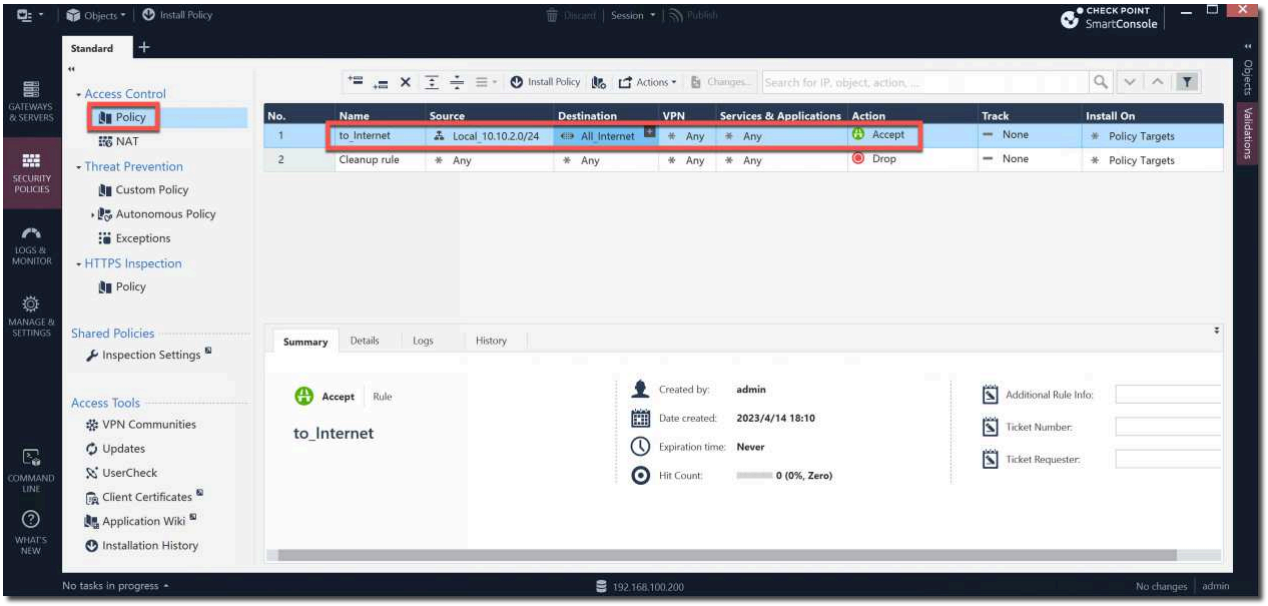
2. 在Check Point防火墙的CLI下使用“save config”命令保存配置。

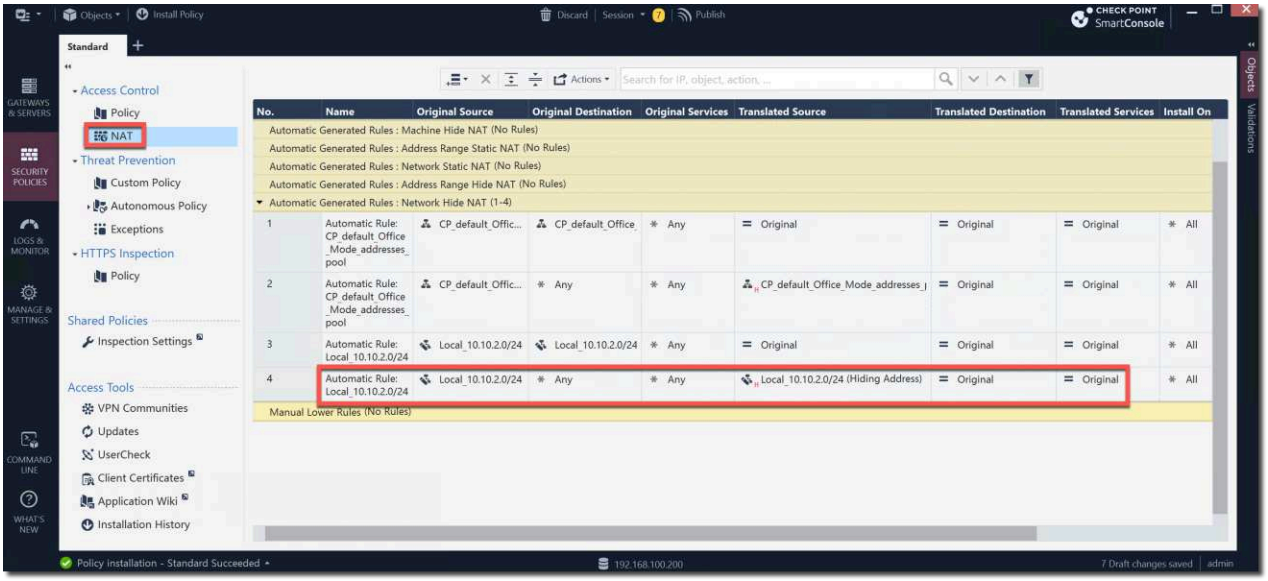
3. 使用SmartConsole连接Check Point防火墙，配置地址对象（在本地网段的地址对象中开启NAT，并选择Hide模式的NAT，地址对象创建完成后会自动创建对应的SNAT策略），创建上网的安全策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



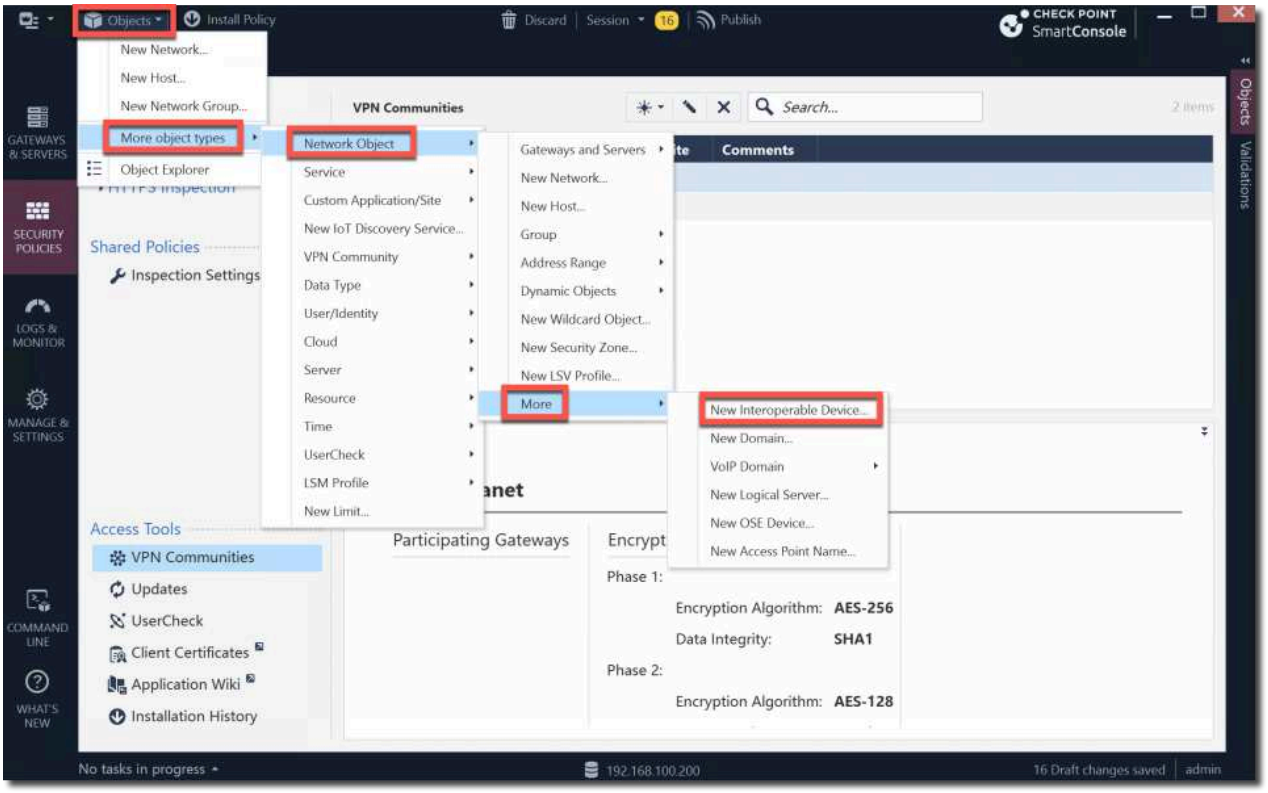
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



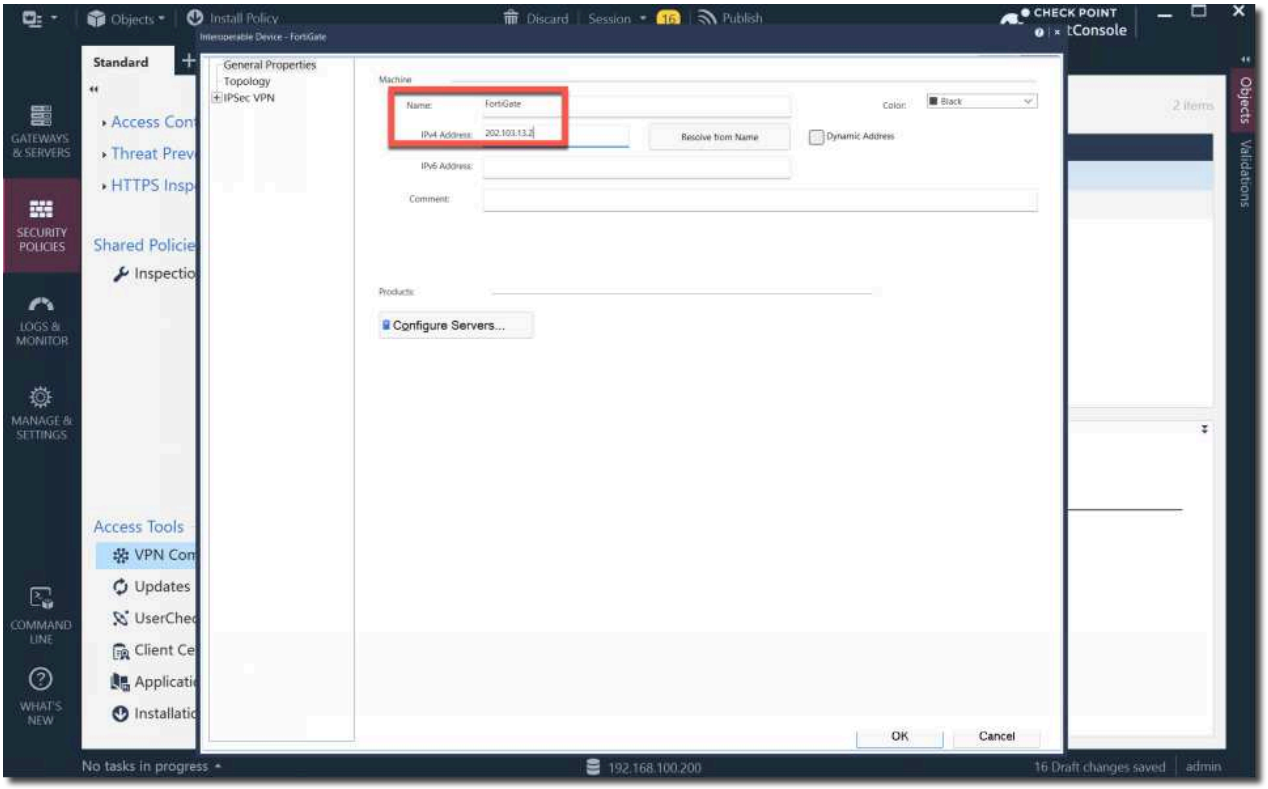


4. 创建“Interoperable Device”对象（IPSec远程网关）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

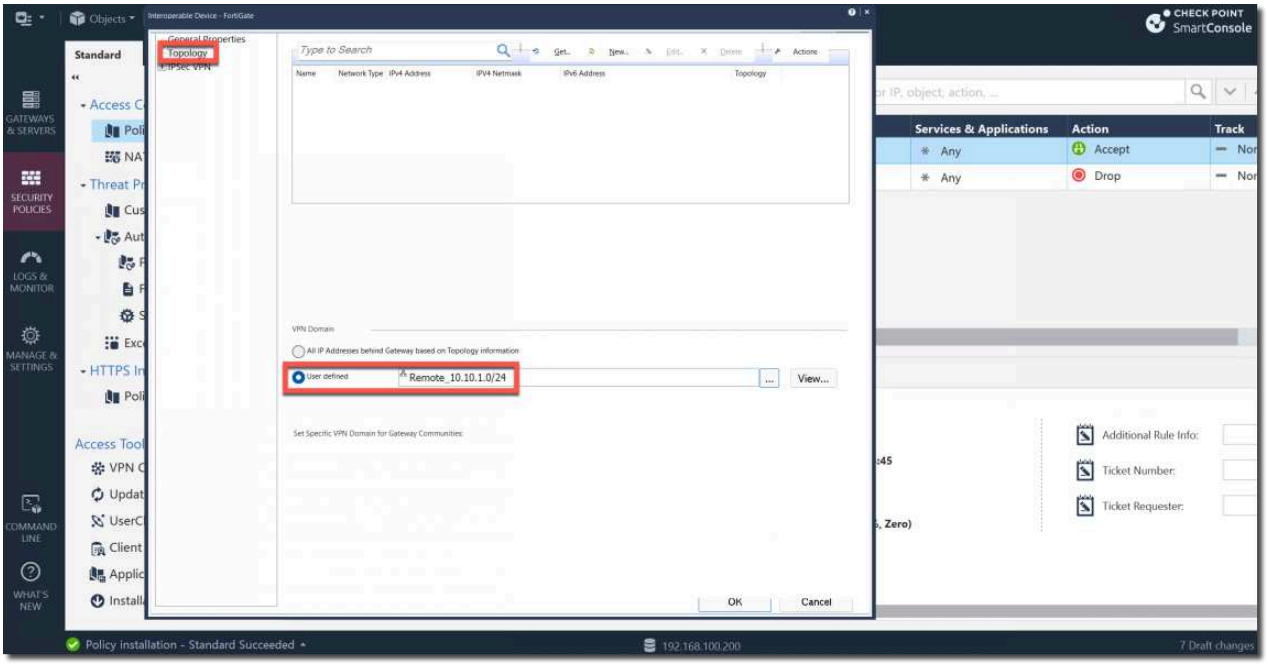


5. 在弹出的“Interoperable Device”的“General Properties”中的“Machine”处，填入FortiGate的VPN网关地址。

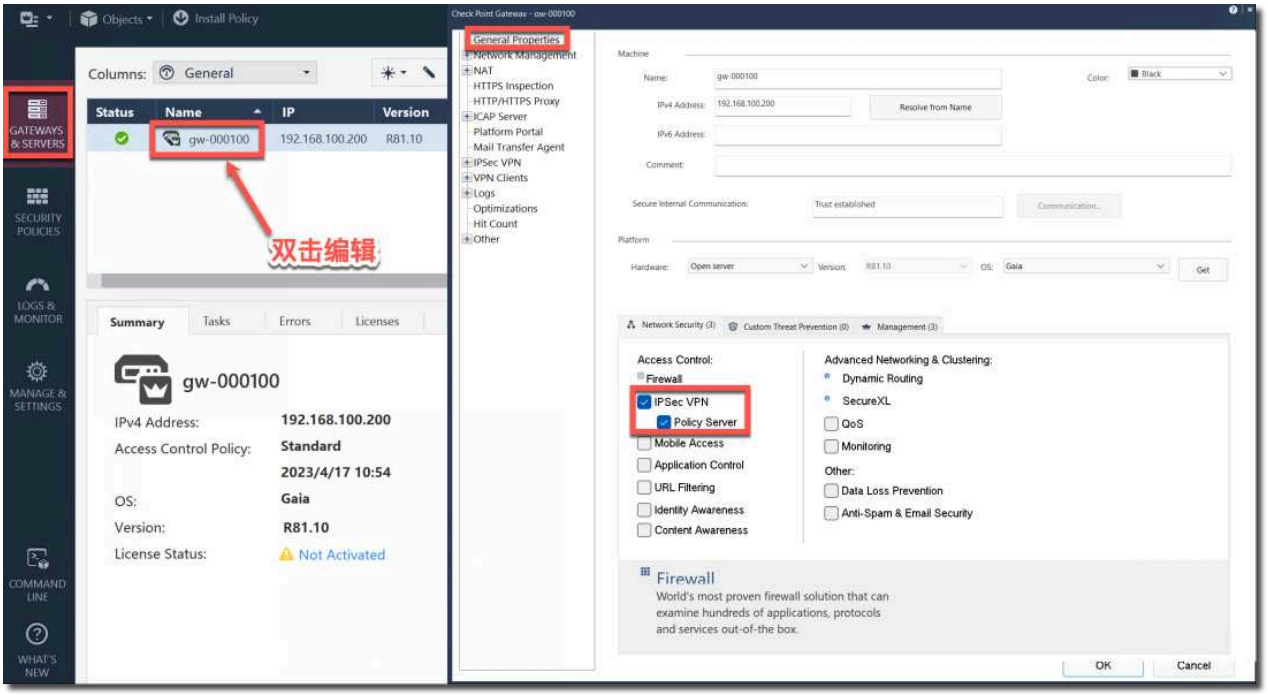


6. 在“Topology”中配置“VPN Domain”为“User defined”，并选择对端（FortiGate侧）VPN感兴趣流的地址对象，点击OK完成创建。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

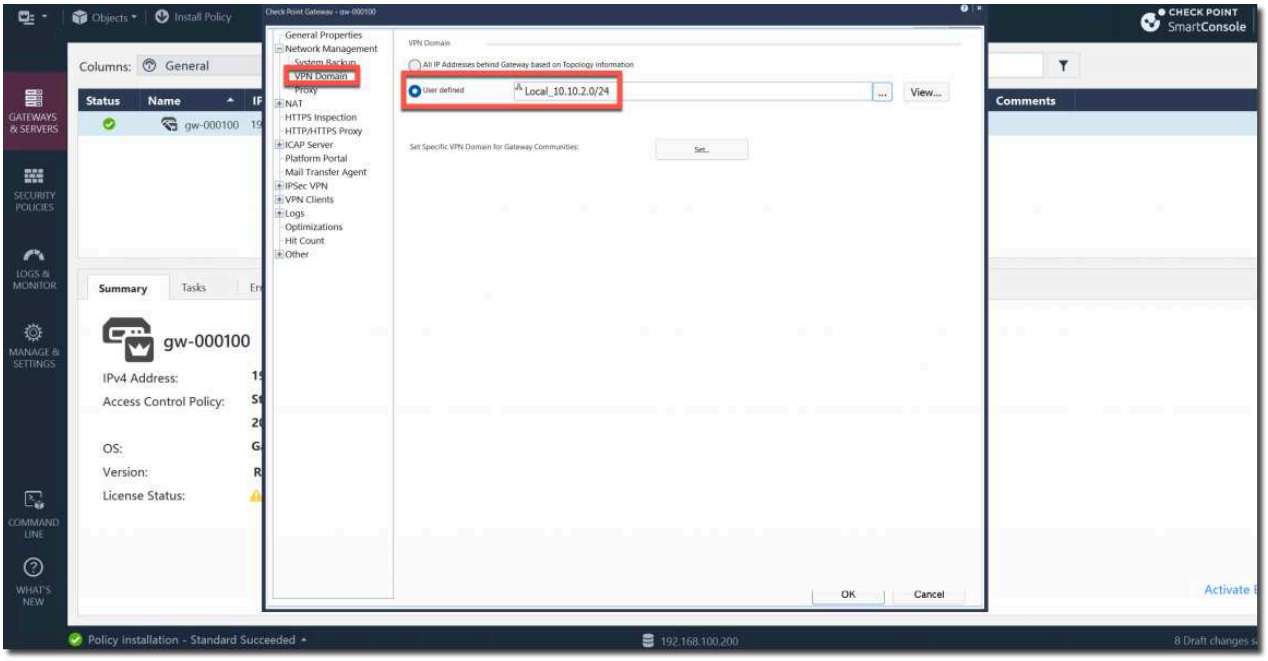


7. 进入“GATEWAYS & SERVERS”选项卡，双击管理的防火墙设备，在弹出的页面中的“General Properties”中开启IPSec VPN服务。

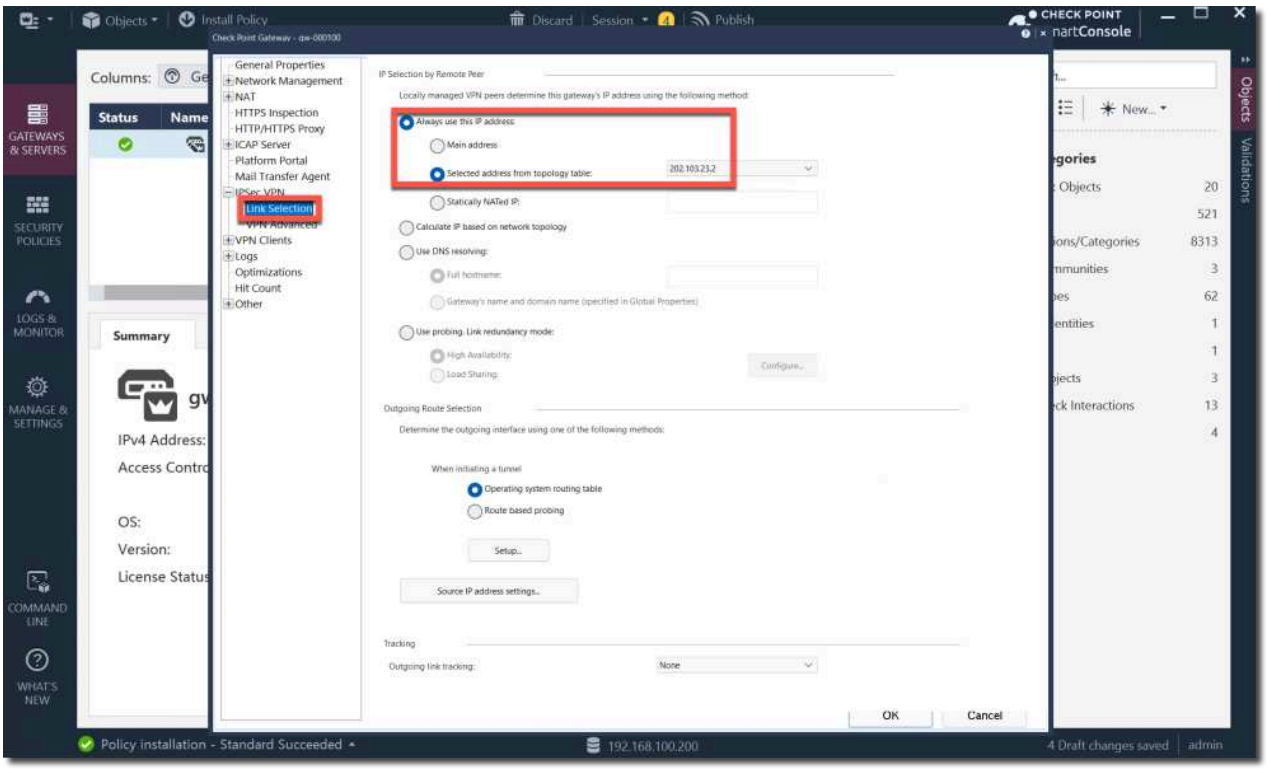


8. 在“Network Domain→VPN Domain”中，配置“User defined”为本地VPN保护网段的地址对象。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

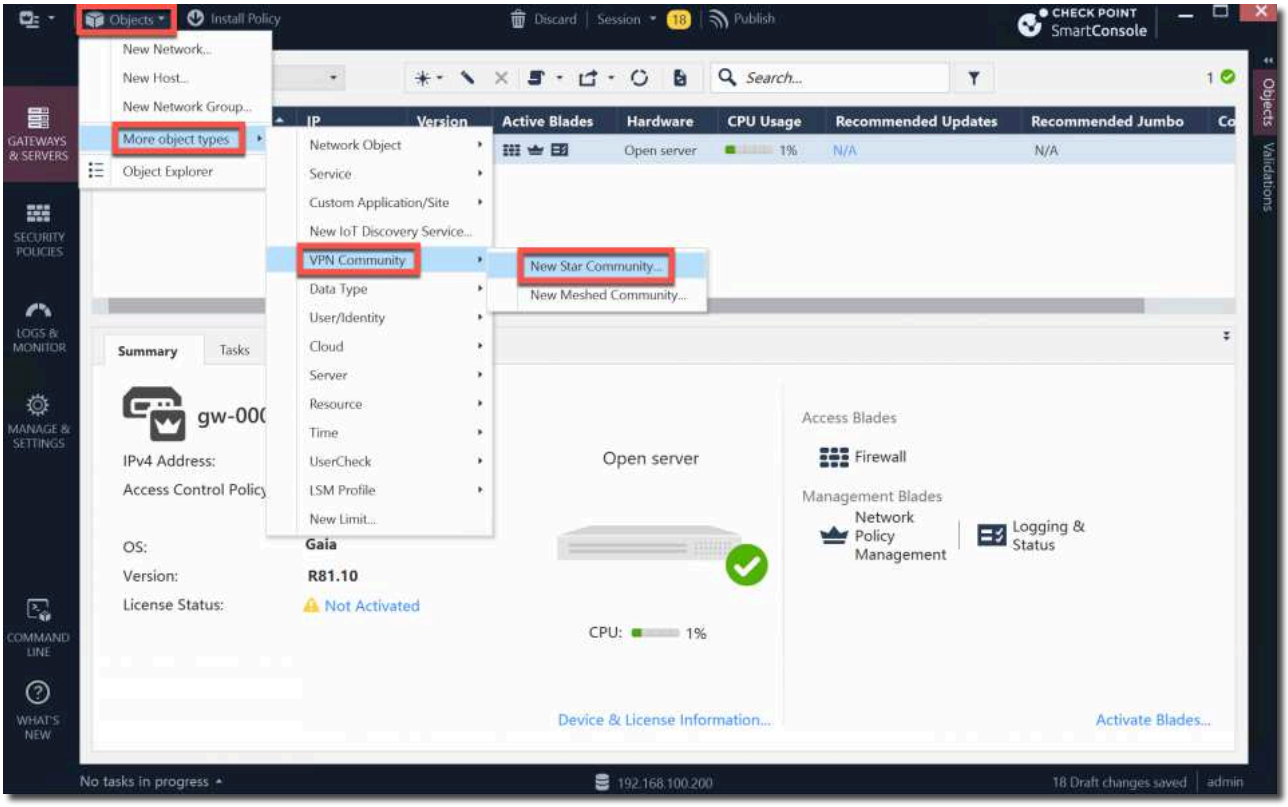


9. 在“IPSec VPN→Link Selection”中，配置“Always use this IP address”为“Selected address from topology table”，并选择eth1（本地VPN网关）的接口IP，点击OK下发配置。

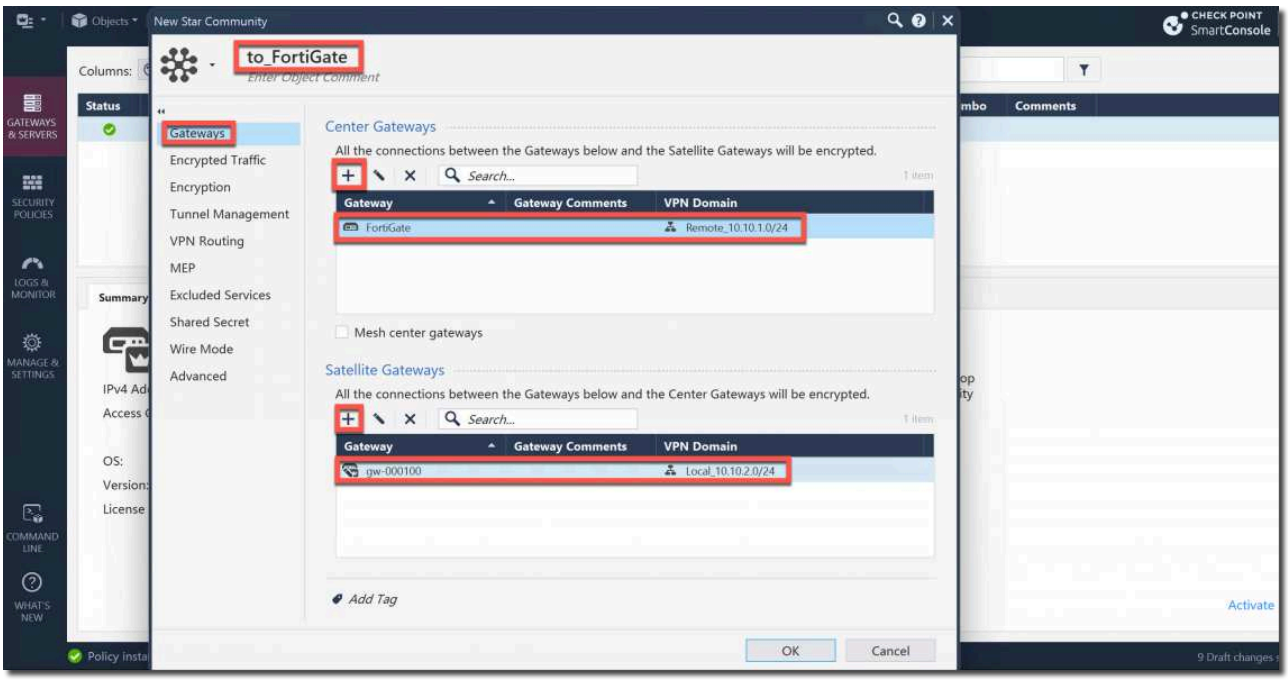


.0. 创建“VPNCommunity”对象。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

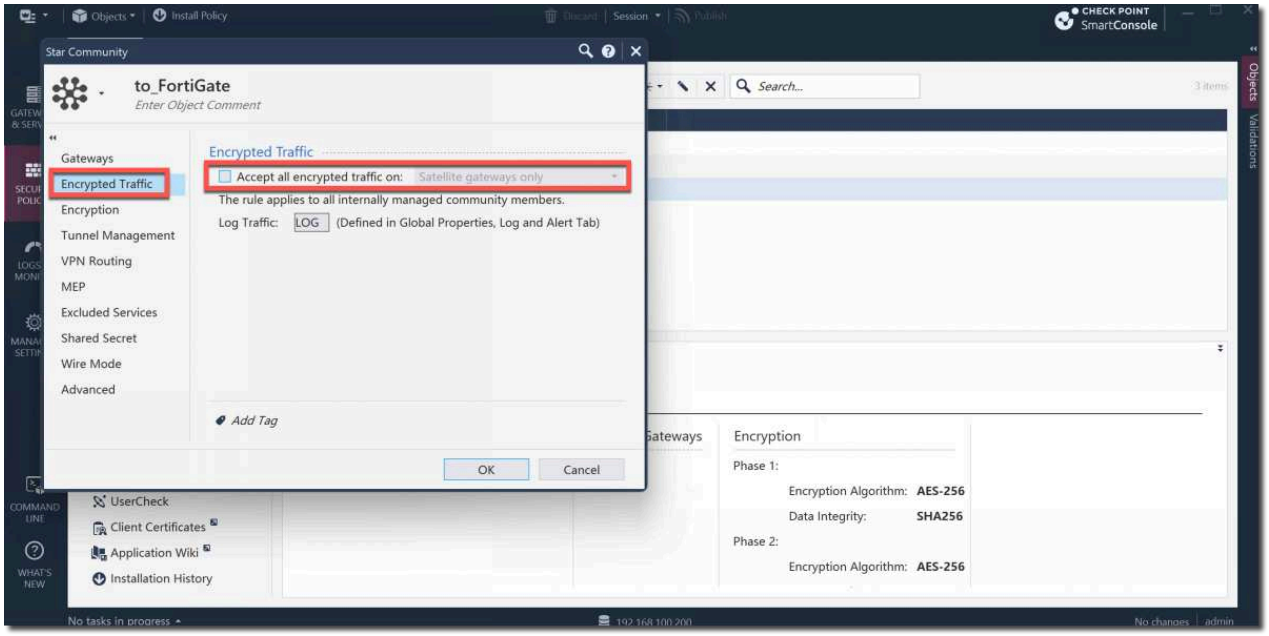


1. 在弹出的页面中，配置Gateway，“Center Gateways”添加上步创建的“Interoperable Device”，“Satellite Gateways”添加本地Gateway。

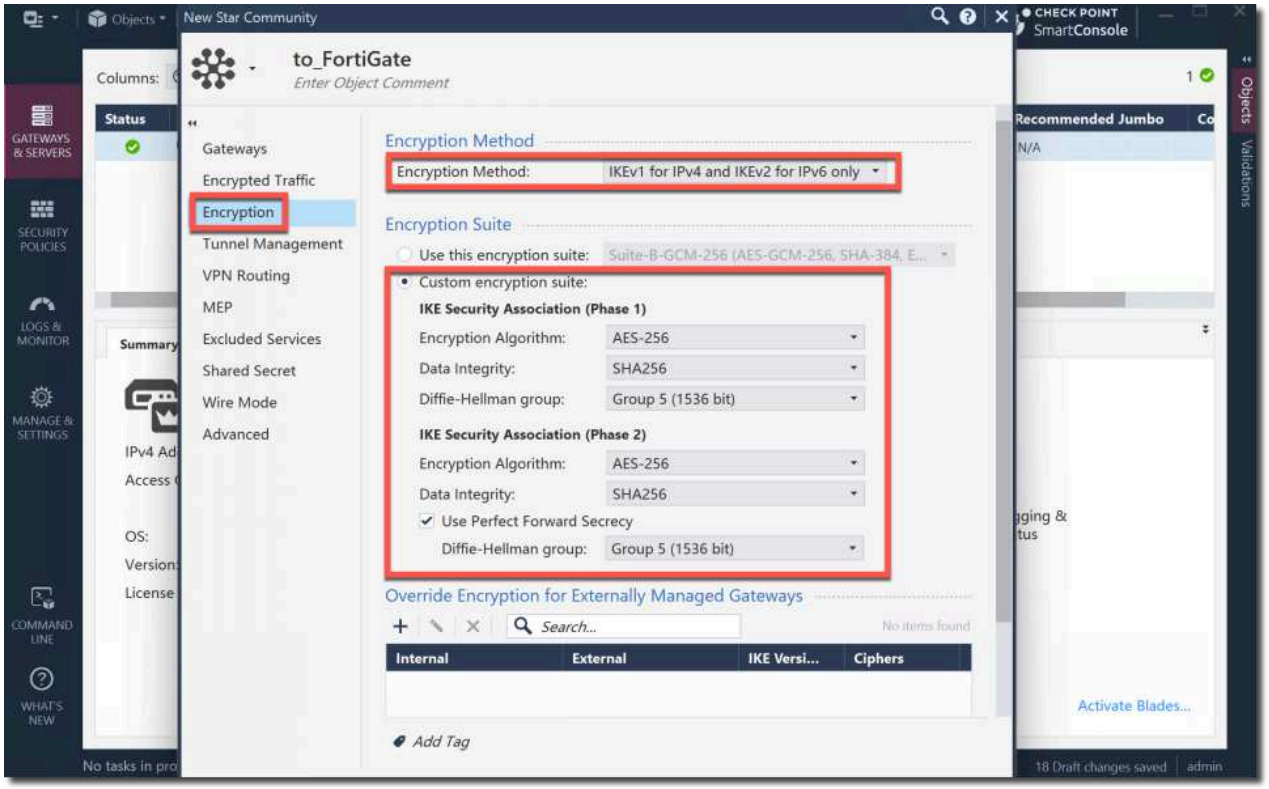


1. 在“Encrypted Traffic”中，不勾选“Accept all encrypted Traffic on”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

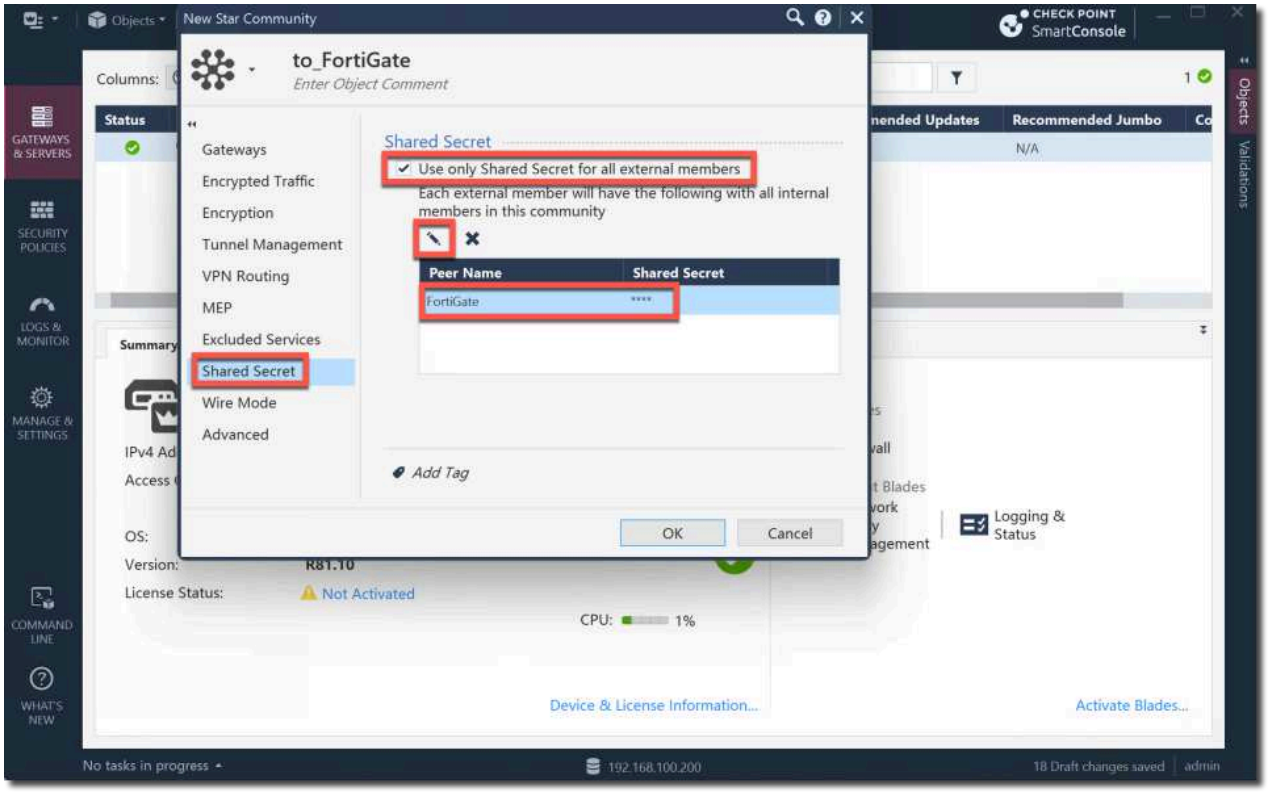


2. 在“Encryption”中配置一阶段和二阶段的安全提议，注意与FortiGate端保持一致。

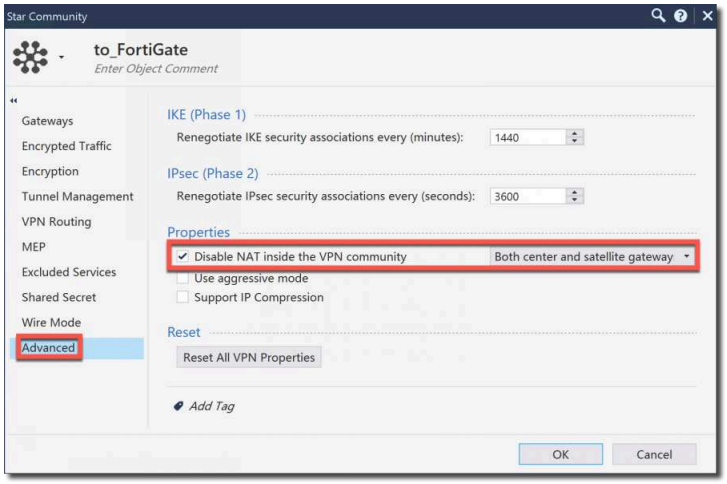


3. 在“Shared Secret”中开启“Use only Shared Secret for all external members”，编辑预共享密钥与FortiGate端一致。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

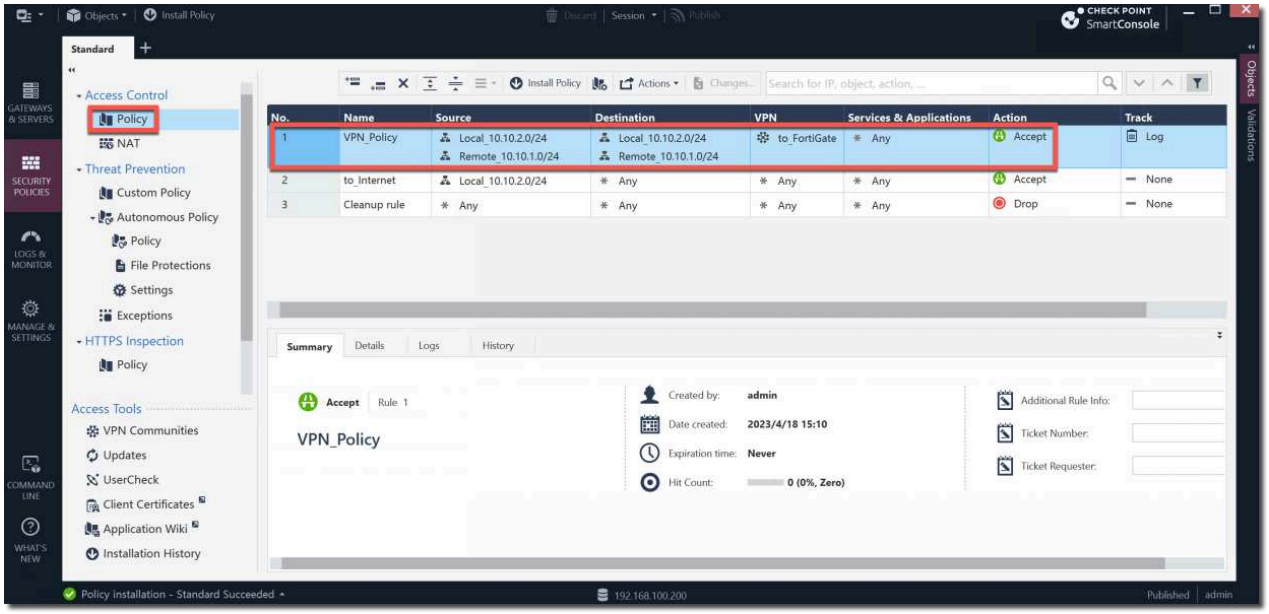


4. 由于Check Point的IPSec绑定在实际链路口，而不是虚拟tunnel接口，在出方向上，SNAT动作优先于IPSec封装，VPN流量经过SNAT后会匹配不上感兴趣流，所以需要配置IPSec流量不被SNAT处理。在“Advanced”选项卡中，勾选“Disable NAT inside the VPN Community”，开启后，进入VPN隧道的流量不会匹配NAT策略。点击OK下发配置。

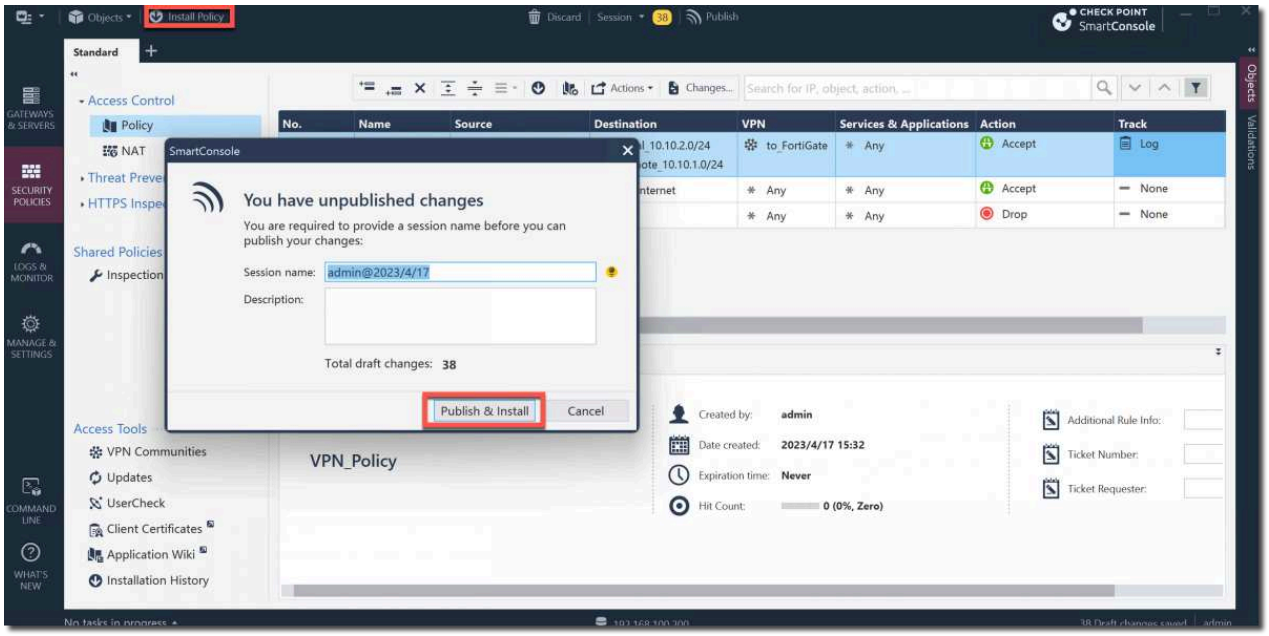


5. 在上网策略之前配置IPSec VPN相关网段放通的安全策略。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 最后，点击“Install Policy”安装所有策略。



结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Remote
version: 1
interface: port2 4
addr: 202.103.13.2:500 → 202.103.23.2:500
tun_id: 202.103.23.2/::202.103.23.2
remote_location: 0.0.0.0
network-id: 0
created: 127s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms
  id/spi: 508 d0481e88ec264101/908a37e3aa3e43be
  direction: initiator
  status: established 127-127s ago = 0ms
  proposal: aes256-sha256
  key: 39c34495a79b54ca-cdd33b755c2150e9-2b31e3f2ace9c0a2-5b9307e2ee57ee63
  lifetime/rekey: 1400/1242
  DPD sent/recv: 0000006e/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Remote ver=1 serial=1 202.103.13.2:0→202.103.23.2:0 tun_id=202.103.23.2 tun_id6=::202.103.23.2
dst_mtu=1500 dpd-link=on1
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 o0
proxyid_num=1 child_num=0 refcnt=4 ilast=31 olast=31 ad=/0
stat: rxp=10 txp=10 rxb=840 txb=840
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=110
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Remote proto=0 sa=1 ref=10 serial=2 auto-negotiate
  src: 0:10.10.1.0-10.10.1.255:0
  dst: 0:10.10.2.0-10.10.2.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=3166/0B replaywin=2048
       seqno=b esn=0 replaywin_lastseq=0000000a qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3297/3600
  dec: spi=daad030c esp=aes key=32 71ddf0ef357e7828acaffcbb4678daa04020591c56c2e6b3371643d4d5c0d1f5
       ah=sha256 key=32 cc7d15cad39ce576d9a1656e51c1b0e870aec41cf5d5e39c7ffcead1750363bd
  enc: spi=ccc51a59 esp=aes key=32 43d629dbc1e0bdb045772b7d5f42f6400a9ae5544be14b52312d7d7543bfb96b
       ah=sha256 key=32 5fdff7bce9562ae578488bbb78e9f050f91cfc137871c947056232114e017b93
  dec:pkts/bytes=20/1680, enc:pkts/bytes=20/2400
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.13.2 npu_selid=1 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. 查看FortiGate的路由表。

```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.103.13.1, port2, [1/0]
C       10.10.1.0/24 is directly connected, port3
S       10.10.2.0/24 [10/0] via VPN-to-Remote tunnel 202.103.23.2, [1/0]
C       192.168.100.0/24 is directly connected, port1
C       202.103.13.0/24 is directly connected, port2
```

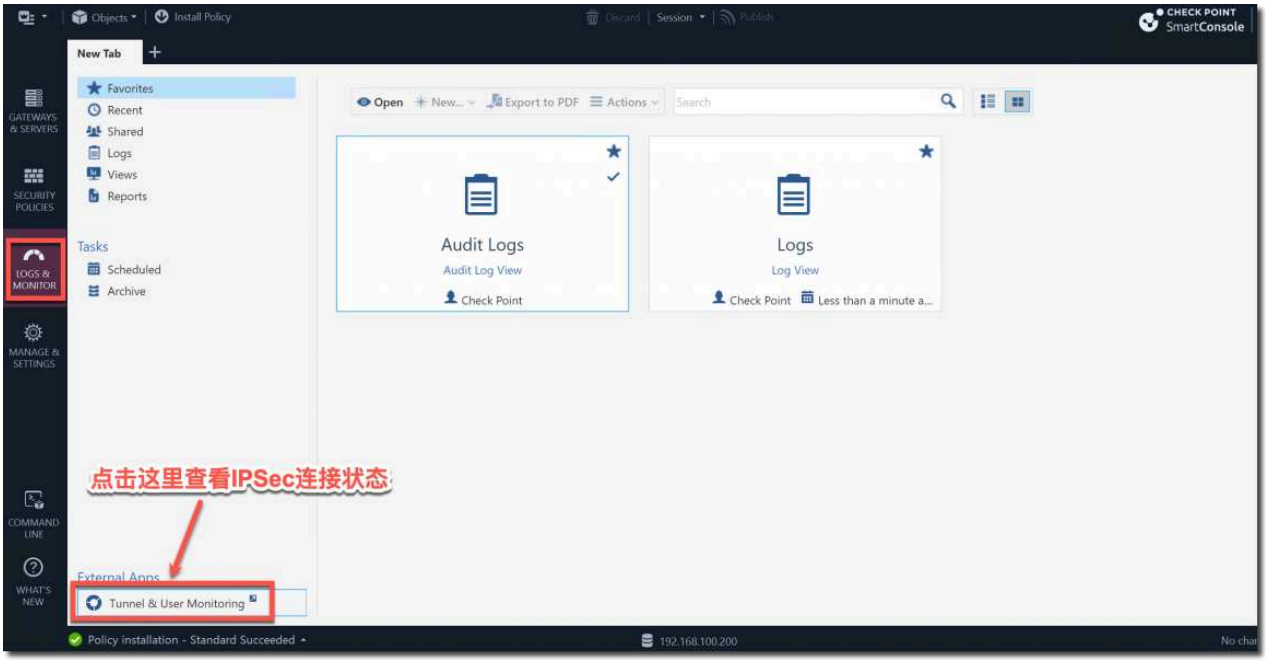
3. FortiGate侧PC1业务测试。

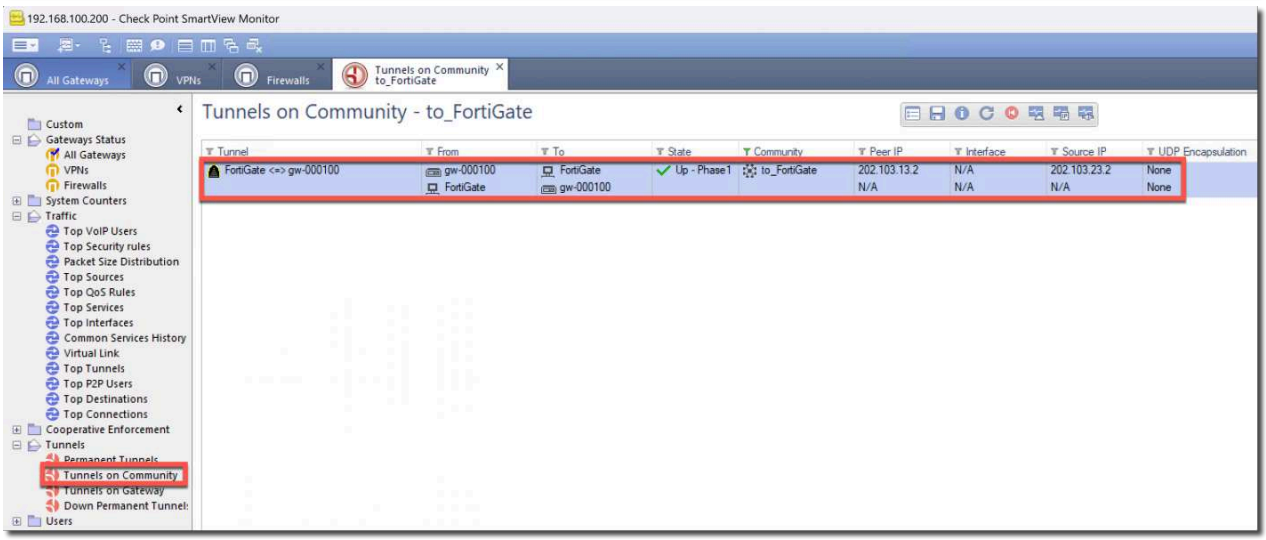
```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.1.2/24         10.10.1.1
       fe80::250:79ff:fe66:6805/64

VPCS> ping 10.10.2.2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
84 bytes from 10.10.2.2 icmp_seq=1 ttl=62 time=5.727 ms
84 bytes from 10.10.2.2 icmp_seq=2 ttl=62 time=2.354 ms
84 bytes from 10.10.2.2 icmp_seq=3 ttl=62 time=4.145 ms
84 bytes from 10.10.2.2 icmp_seq=4 ttl=62 time=2.402 ms
84 bytes from 10.10.2.2 icmp_seq=5 ttl=62 time=3.445 ms
```

4. Check Point防火墙查看IPSec连接状态。





5. 查看Check Point防火墙的路由表，可以看到VPN流量匹配了默认路由，送往本地VPN网关接口eth1（如果默认路由指向的不是本地VPN网关接口，请自行配置细化的VPN路由指向VPN网关接口）。

```
gw-000100> show route
Codes: C - Connected, S - Static, R - RIP, B - BGP (D - Default),
       O - OSPF IntraArea (IA - InterArea, E - External, N - NSSA),
       A - Aggregate, K - Kernel Remnant, H - Hidden, P - Suppressed,
       NP - NAT Pool, U - Unreachable, i - Inactive

S               0.0.0.0/0           via 202.103.23.1, eth1, cost 0, age 12890
C               10.10.2.0/24        is directly connected, eth2
C               127.0.0.0/8         is directly connected, lo
C               192.168.100.0/24    is directly connected, eth0
C               202.103.23.0/24     is directly connected, eth1
```

6. Check Point防火墙侧PC2业务测试。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.2.2/24         10.10.2.1
       fe80::250:79ff:fe66:6806/64

VPCS> ping 10.10.1.2

84 bytes from 10.10.1.2 icmp_seq=1 ttl=62 time=2.687 ms
84 bytes from 10.10.1.2 icmp_seq=2 ttl=62 time=2.235 ms
84 bytes from 10.10.1.2 icmp_seq=3 ttl=62 time=2.130 ms
84 bytes from 10.10.1.2 icmp_seq=4 ttl=62 time=2.225 ms
84 bytes from 10.10.1.2 icmp_seq=5 ttl=62 time=2.170 ms
```

7. FortiGate侧抓包查看。

```
FortiGate # diagnose sniffer packet any 'host 10.10.2.2 and host 10.10.1.2 and icmp' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.2 and host 10.10.1.2 and icmp]
2023-04-18 15:18:07.196766 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:07.196805 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:07.197221 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:07.197240 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:08.200924 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:08.200964 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:08.201134 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:08.201143 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:09.204488 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:09.204523 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:09.204736 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:09.204749 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:10.208678 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:10.208715 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:10.209058 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:10.209069 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:11.212295 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:11.212330 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-18 15:18:11.212521 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-18 15:18:11.212534 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

   - 抓取IPsec VPN的IKE协商包：

     ```
     diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
     ```

   - 抓取IPsec VPN的ESP加密数据包：

     ```
     diagnose sniffer packet any "host 101.1.1.1 and esp" 4
     ```

   - 抓取IPsec VPN的明文业务数据包：

     ```
     diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
     ```

   - 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

     ```
     FortiGate # config vpn ipsec phase1-interface
     FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
     FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
     FortiGate (BJ-OSPF-TO-SH) # end
     ```

2. Check Point防火墙IPsec VPN Debug请参考：
   https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SitetoSiteVPN_AdminGuide/Topics-VPNSG/CLI/vpn-debug.htm ↗ 。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
vpn debug
      on [<Debug_Topic>=<Debug_Level>]
      off
      ikeon [-s <Size_in_MB>]
      ikeoff
      trunc [<Debug_Topic>=<Debug_Level>]
      truncon [<Debug_Topic>=<Debug_Level>]
      truncoff
      timeon [<Seconds>]
      timeoff
      ikefail [-s <Size_in_MB>]
      mon
      moff
      say ["String"]
      tunnel [<Level>]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与Juniper SRX防火墙建立IPSec VPN

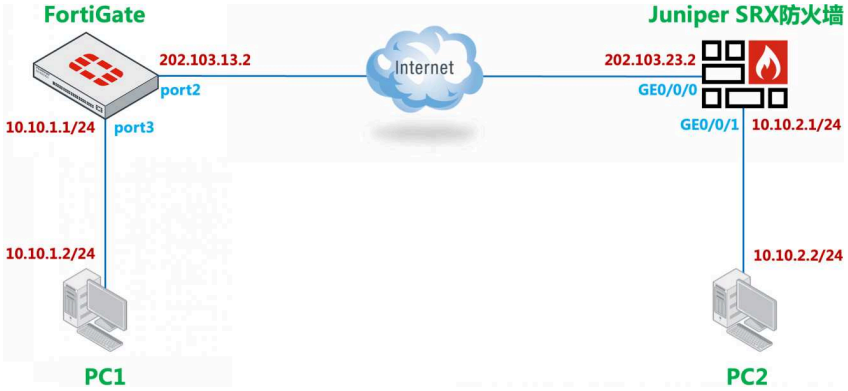
网络需求

如图所示，通过IPsec VPN（接口模式）将2个局域网连接起来，实现10.10.1.0/24与10.10.2.0/24两个网段的通信。与Juniper SRX防火墙进行IPsec VPN（IKE v1）对接。

Juniper SRX防火墙版本：

```
root# show version
## Last changed: 2023-04-11 03:02:08 UTC
version 23.1R1.8;
```

网络拓扑



配置要点

- 配置FortiGate
  - 基本上网配置
  - 配置IPsec VPN
- 配置Juniper SRX防火墙
  - 基本上网配置
  - 配置IPsec VPN
- 说明：如果要删除IPSEC VPN第一阶段、第二阶段时，需要先删除被调用的路由与防火墙安全策略。

配置步骤

FortiGate

1. 基本上网配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







2. 配置IPSec VPN，进入VPN→IPSec隧道，点击新建→IPSec隧道按钮。



3. 选择IPsec VPN自定义模板进行配置，点击下一步。



4. 如图配置网络、认证、第一阶段、第二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

由于Juniper的IPSec配置向导会创建明细的感兴趣流，FortiGate与Juniper防火墙对接IPSec推荐对应使用明细的感兴趣流。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

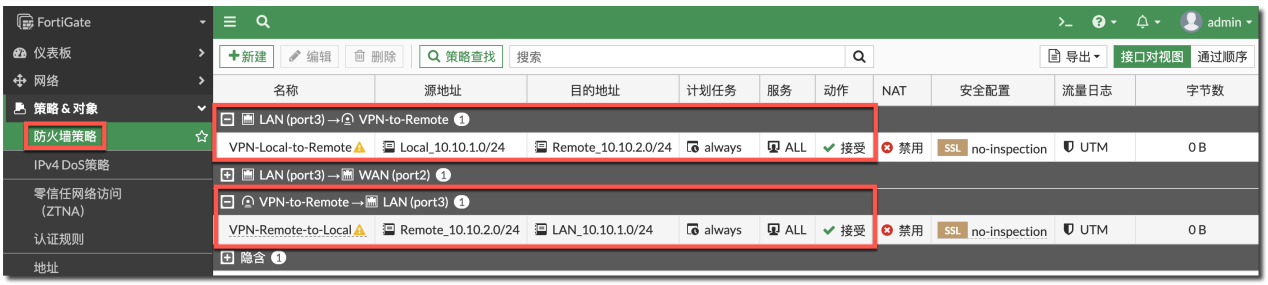


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN-to-Remote"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 202.103.23.2
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "VPN-to-Remote"
        set phase1name "VPN-to-Remote"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 10.10.1.0 255.255.255.0
        set dst-subnet 10.10.2.0 255.255.255.0
    next
end
```

5. 配置VPN相关的网段地址对象和防火墙策略。






```
config firewall address
    edit "Local_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "Remote_10.10.2.0/24"
        set subnet 10.10.2.0 255.255.255.0
    next
end

config firewall policy
    edit 2
        set name "VPN-Local-to-Remote"
        set srcintf "port3"
        set dstintf "VPN-to-Remote"
        set action accept
        set srcaddr "Local_10.10.1.0/24"
        set dstaddr "Remote_10.10.2.0/24"
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "VPN-Remote-to-Local"
        set srcintf "VPN-to-Remote"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_10.10.2.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

6. 配置VPN业务网段的静态路由。

重要

相关VPN的路由配置中“黑洞路由的意义：

你可能会遇到以下的VPN业务问题：通过VPN的SIP电话，时不时中断，无法向服务器成功注册？通过VPN的Radius认证无法经常会无法认证成功？ 通过VPN的AP注册到总部时不时会中断？持续的PRGT监控ping总部的服务器，时不时会显示中断？

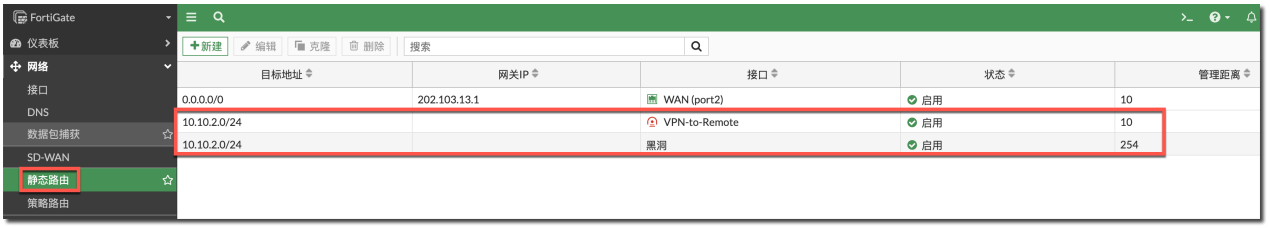
VPN有时候会因为各种原因重新连接，比如互联网不稳定，PPPOE重新连接更换公网IP地址等，VPN tunnel此时会出现短暂的DOWN，而去往对方的VPN业务网段的路由也会短暂消失，此时VPN的业务流量（SIP注册请求/Radius/Capwap/ICMP）会因为查询到了默认路由而走向了WAN（Internet），从而产生了错误的UDP-NAT-Seesion，此时即便VPN tunnel再次UP，VPN业务网段的路由再次恢复，SIP等VPN旧的业务流量依旧会走到错误的Session上去，从而引起该业务异常。

解决方法：

- 方法一：配置去往VPN业务网段的“黑洞路由”，管理距离为254，VPN正常的情况下此黑洞路由不生效，而当VPN中断的时候，黑洞路由浮起来并且生效，将VPN中断时候的VPN流量丢弃，避免将流量转发到互联网而产生错误的session。配置VPN的备份黑洞路由的意义在此。
- 方法二：配置源接口：LAN，目的接口：WAN，源IP：本地内网网段，目的IP：对端内网网段，动作：丢包的策略。将此去往Internet的私网（无用的）流量丢弃掉，避免FGT产生这种错误的session，从而避免了UDP业务时不时中断的问题。
- 方法三：在全局下开启“set snat-route-change enable”，一旦路由发生变化，将相关的会话flag置位为“Dirty”，清除路由缓存并重新查找目的IP的下一跳地址，这样VPN隧道恢复的时候，流量也会相应的切换到VPN隧道里面来。

```
FortiGate # config system global
FortiGate (global) # set snat-route-change enable
FortiGate (global) # end
```

三种方式任意选择一种即可。推荐使用黑洞路由方式。

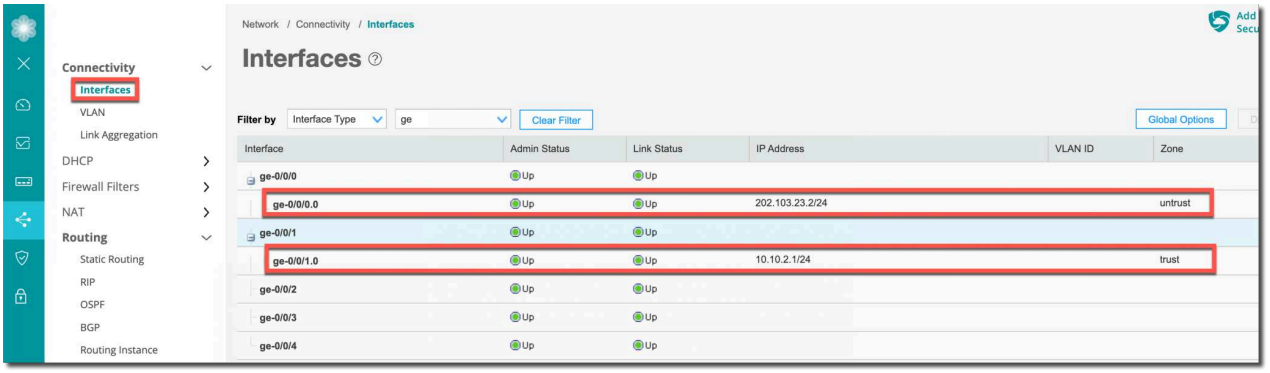


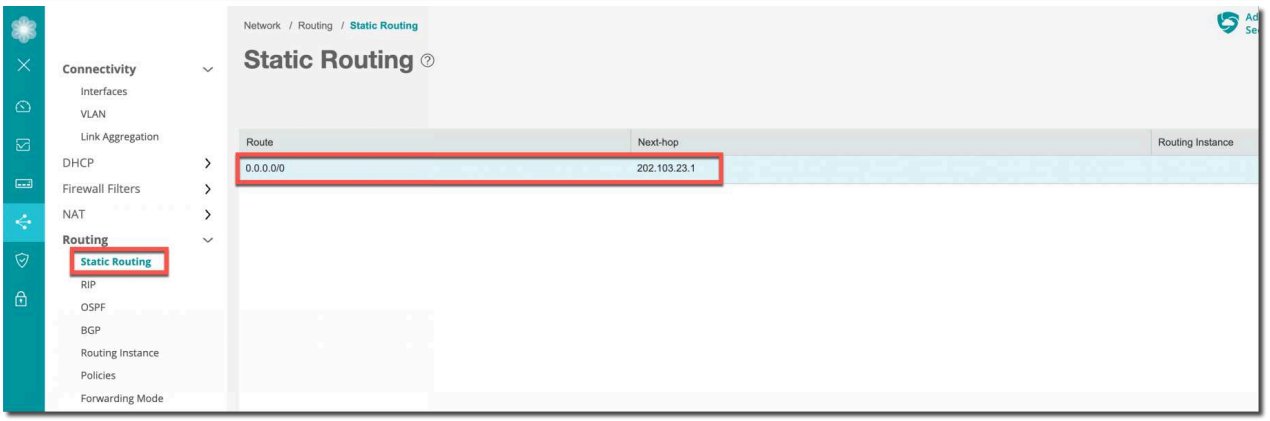

```
config router static
    edit 1
        set gateway 202.103.12.1
        set device "port2"
    next
    edit 2
        set dst 10.10.2.0 255.255.255.0
        set device "VPN-to-Remote"
    next
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 254
        set blackhole enable
    next
end
```

Juniper SRX

1. 基本IP与路由配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

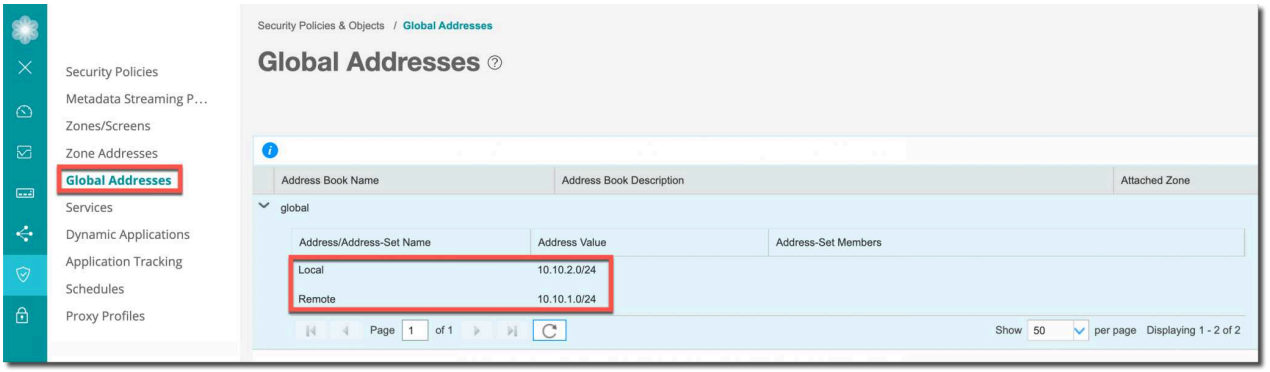


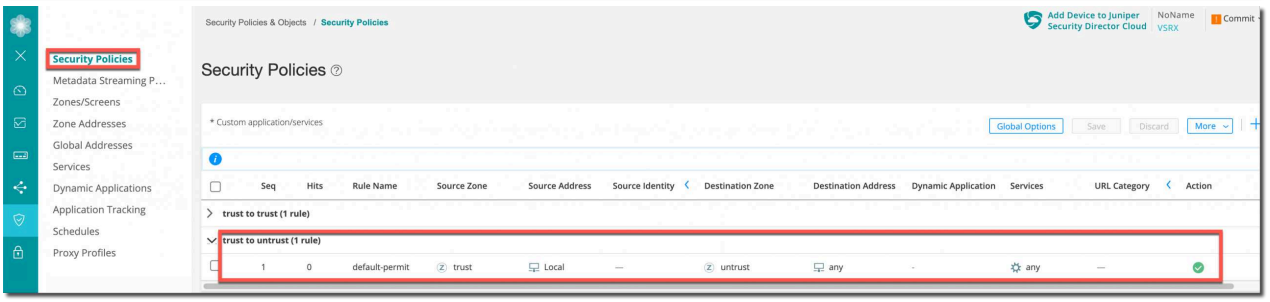


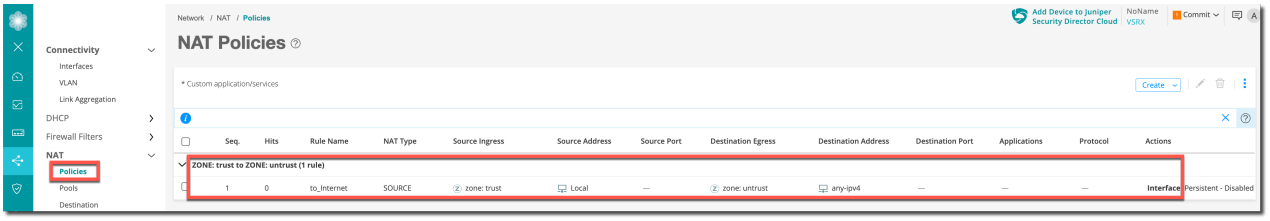

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 202.103.23.2/24;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 10.10.2.1/24;
            }
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 202.103.23.1;
    }
}
```

2. 地址对象、上网策略（默认存在）、上网NAT配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





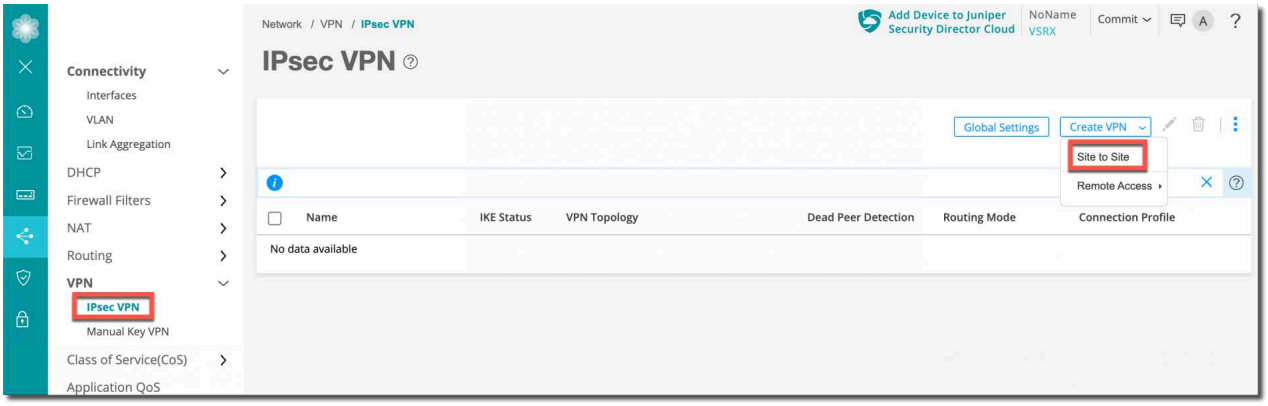



```
security {
    address-book {
        global {
            address Local 10.10.2.0/24;
            address Remote 10.10.1.0/24;
        }
    }
    nat {
        source {
            rule-set Zone_trust-Zone_untrust {
                from zone trust;
                to zone untrust;
                rule to_Internet {
                    match {
                        source-address-name Local;
                        destination-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy default-permit {
                match {
                    source-address Local;
                    destination-address any;
                    application any;
                }
                then {
                    permit;

```

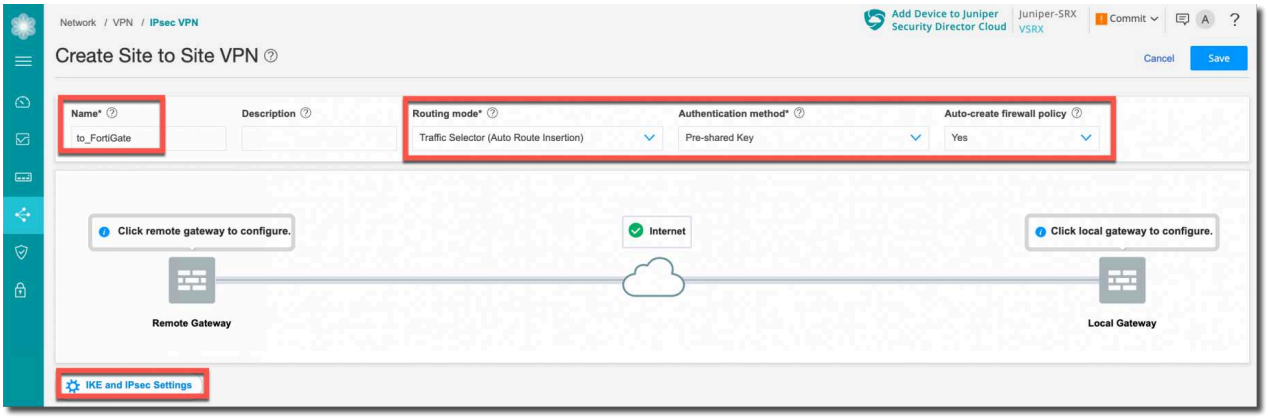

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                    }
                }
            }
        }
    }
```

3. 在IPSec VPN页面点击“Create VPN”按钮，并选择“Site to Site”模式。

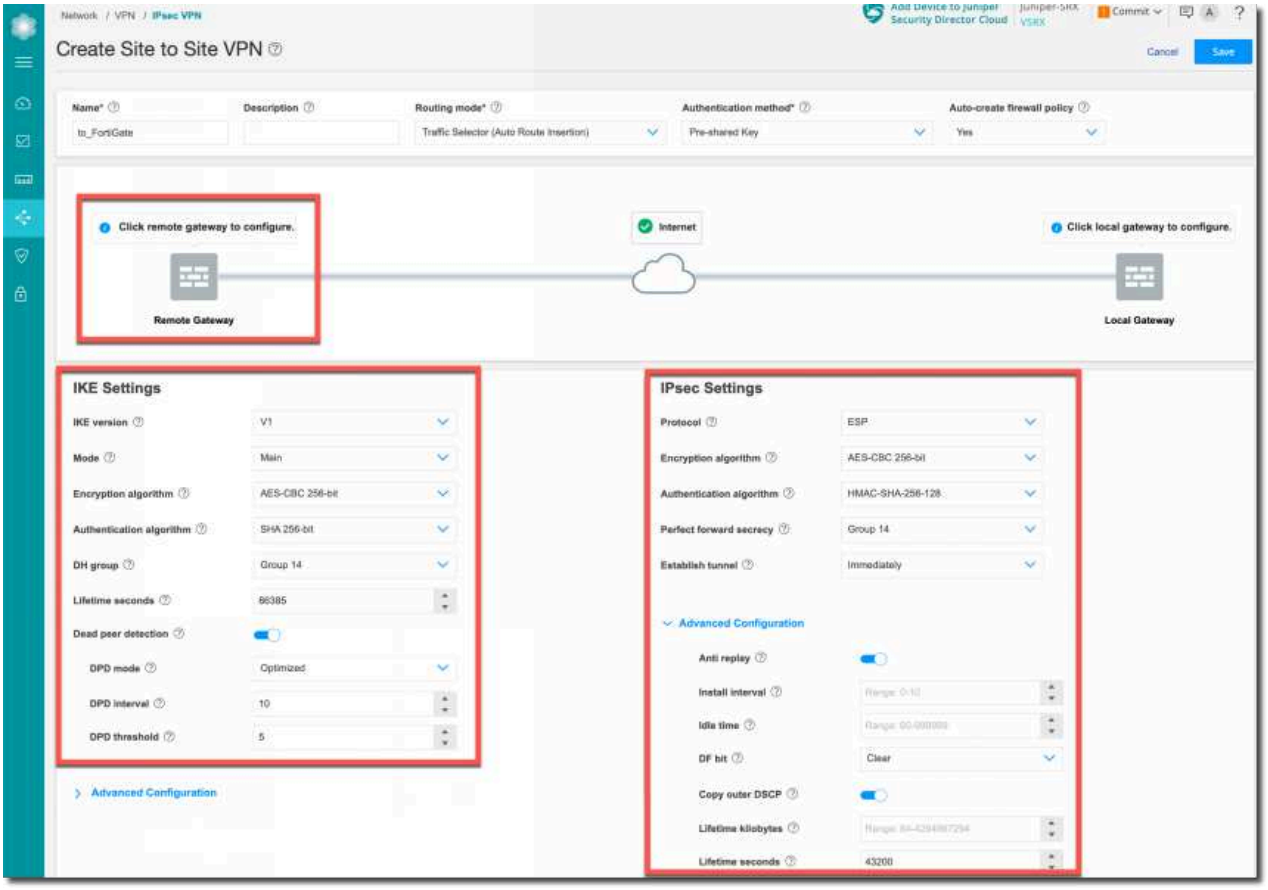


4. 填写IPSec VPN名称，“Routing mode”选择“Traffic Selector”（明细感兴趣流，并自动添加到对端VPN网段的路由），“Authentication method”选择“Pre-shared Key”，“Auto-create firewall policy”选择“Yes”（自动添加VPN网段之间的放通策略）。随后点击左下角的“IKE and IPSec Settings”。

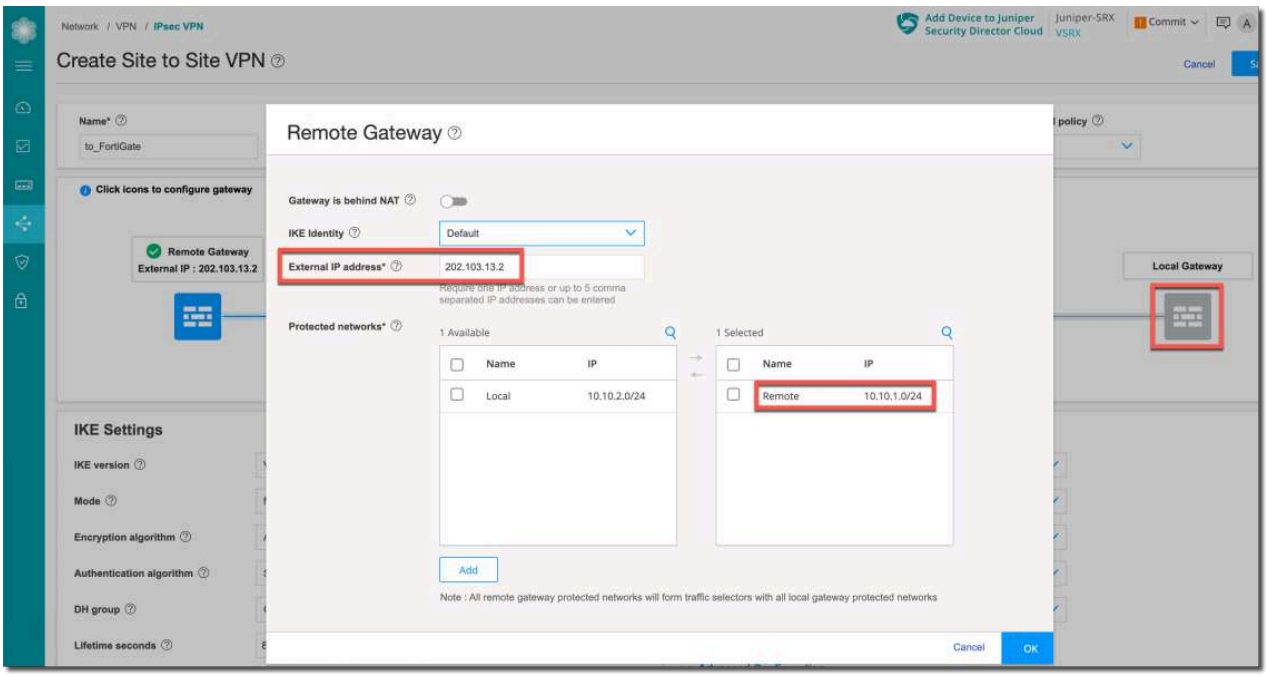


5. 配置IKE与IPSec协商参数，与FortiGate配置为一致，配置完成后，点击“Remote Gateway”配置远程网关。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

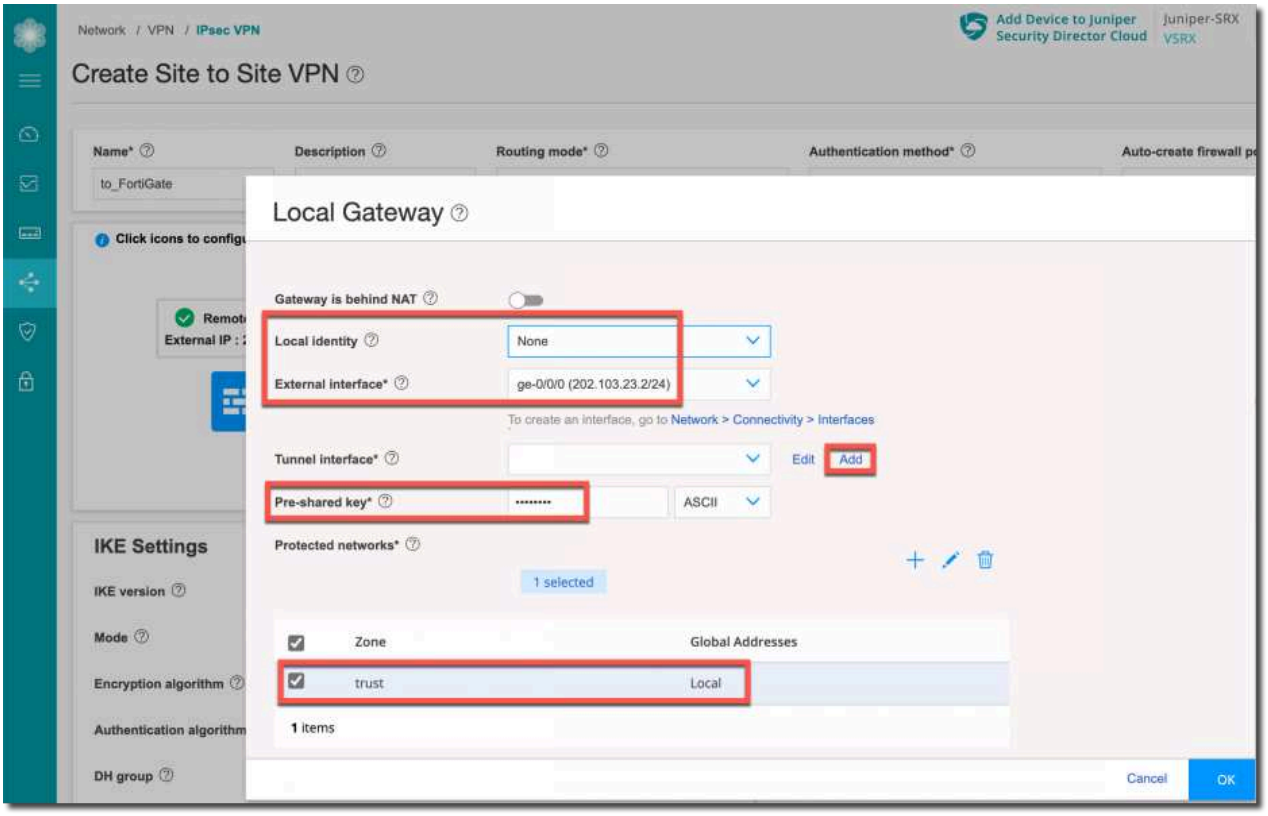


6. 根据实际情况选择是否修改“Gateway is behind NAT”以及ID配置。在“External IP address”中配置FortiGate侧的VPN网关地址，“Protected networks”选中FortiGate侧的VPN网段，点击OK下发配置。随后点击“Local Gateway”配置本地网关。

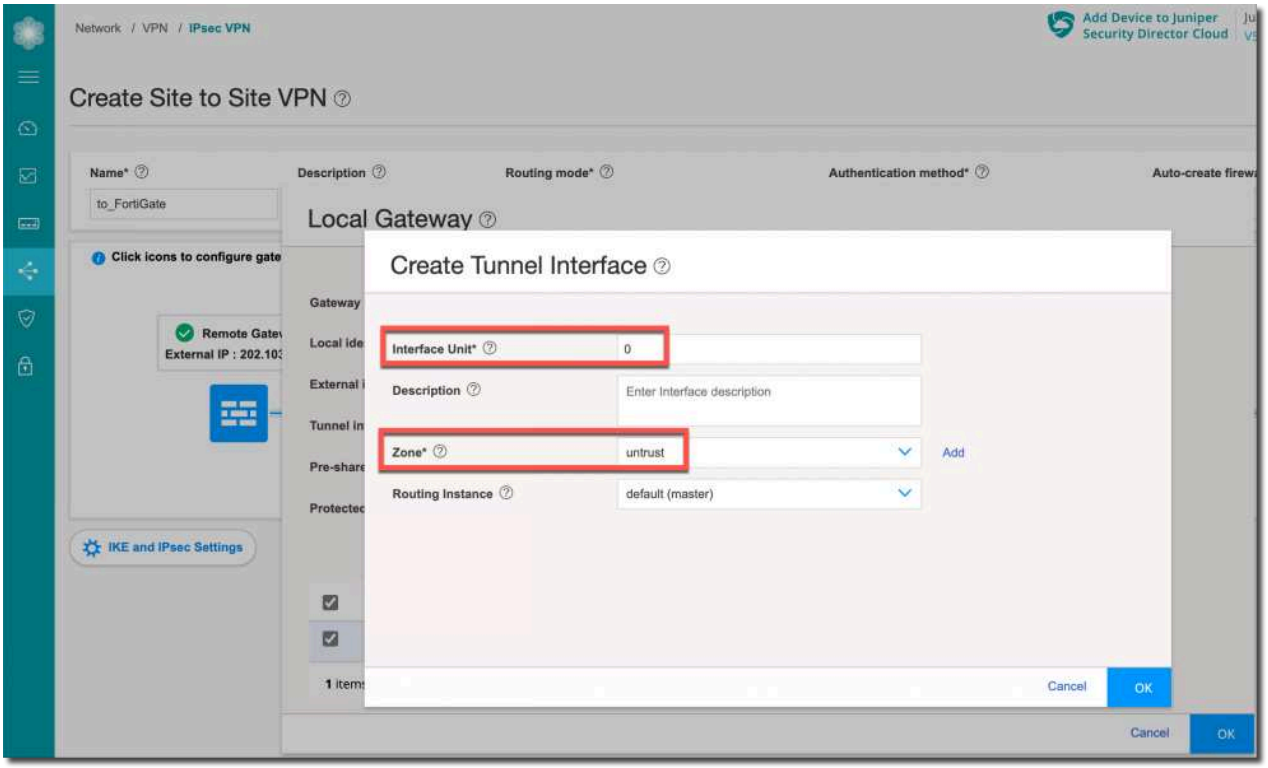


7. 点击“Local Gateway”配置本地网关，选择“External interface”为本地网关公网接口，填写预共享密钥，“Protected networks”选择本地的VPN网段，随后在“Tunnel interface”右侧点击“Add”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

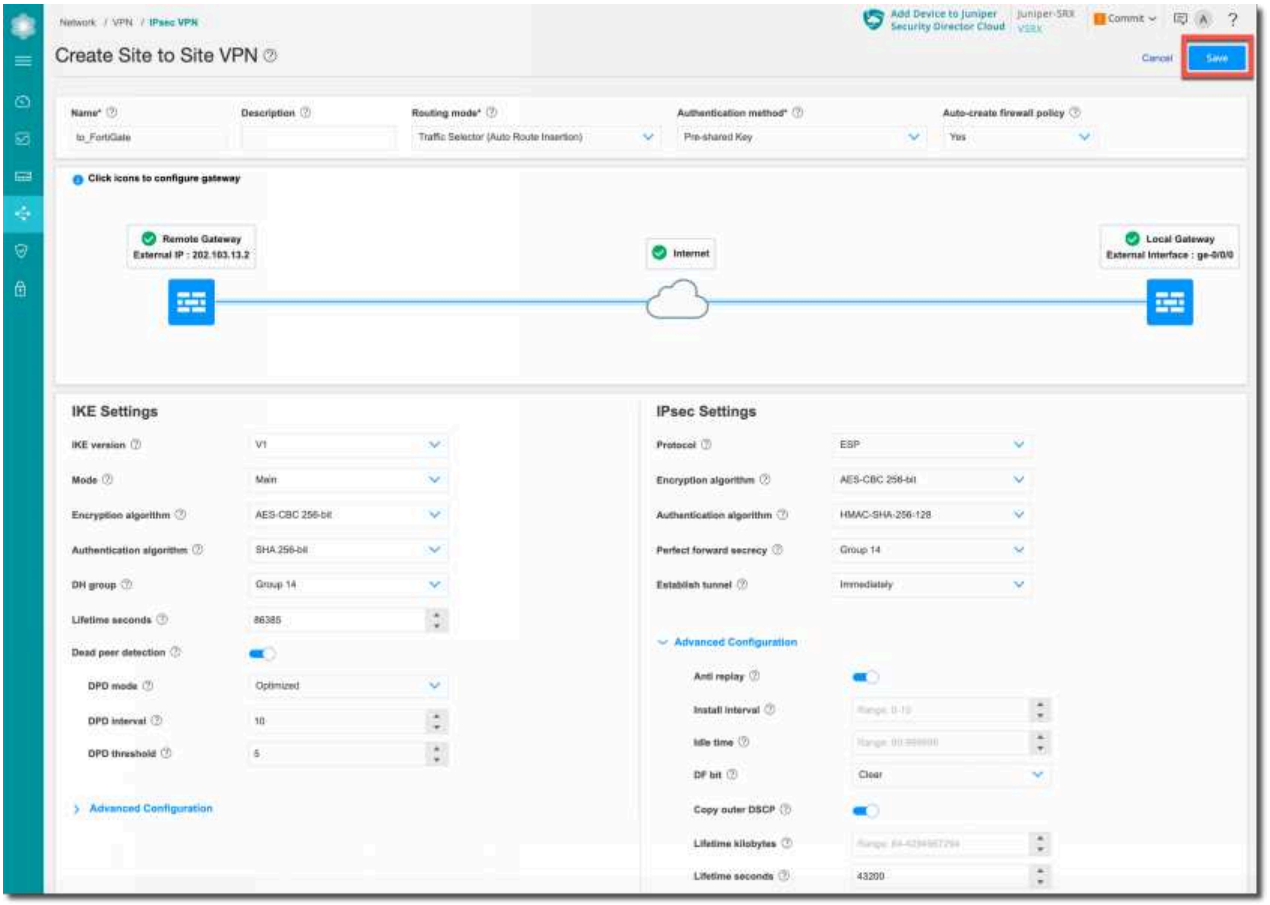


8. 新建Tunnel接口，配置Unit号与安全域信息，随后下发本地网关的配置。



9. 点击“Save”保存IPSec VPN配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

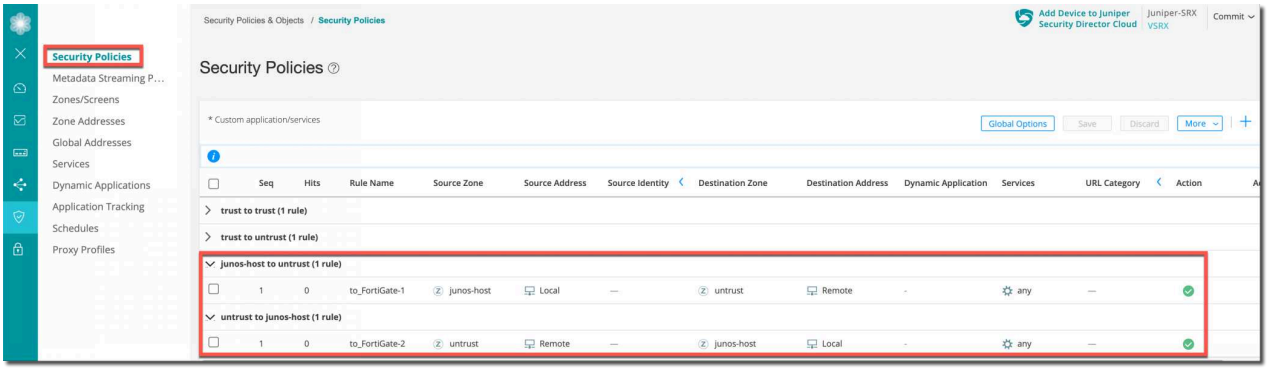



```
interfaces {
    st0 {
        unit 0 {
            family inet;
        }
    }
}
security {
    ike {
        proposal to_FortiGate {
            authentication-method pre-shared-keys;
            dh-group group14;
            authentication-algorithm sha-256;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 86385;
        }
        policy to_FortiGate {
            mode main;
            proposals to_FortiGate;
            pre-shared-key ascii-text "$9$KnSMxNdbs2oJx7Dikqf51REcev"; ## SECRET-DATA
        }
        gateway to_FortiGate {
            ike-policy to_FortiGate;
            address 202.103.13.2;
            dead-peer-detection {
                optimized;
                interval 10;
                threshold 5;
            }
            external-interface ge-0/0/0;
            local-address 202.103.23.2;
            version v1-only;
        }
    }
    ipsec {
        proposal to_FortiGate {
            protocol esp;
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            authentication-algorithm hmac-sha-256-128;
            encryption-algorithm aes-256-cbc;
            lifetime-seconds 43200;
        }
        policy to_FortiGate {
            perfect-forward-secrecy {
                keys group14;
            }
            proposals to_FortiGate;
        }
        vpn to_FortiGate {
            bind-interface st0.0;
            df-bit clear;
            copy-outer-dscp;
            ike {
                gateway to_FortiGate;
                ipsec-policy to_FortiGate;
            }
            traffic-selector ts-1 {
                local-ip 10.10.2.0/24;
                remote-ip 10.10.1.0/24;
            }
            establish-tunnels immediately;
        }
    }
}
```

.0. 查看自动添加的VPN网段安全策略。




```
security {
    policies {
            policy to_FortiGate-1 {
                match {
                    source-address Local;
                    destination-address Remote;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
        from-zone junos-host to-zone untrust {
            policy to_FortiGate-1 {
                match {
                    source-address Local;
                    destination-address Remote;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
```

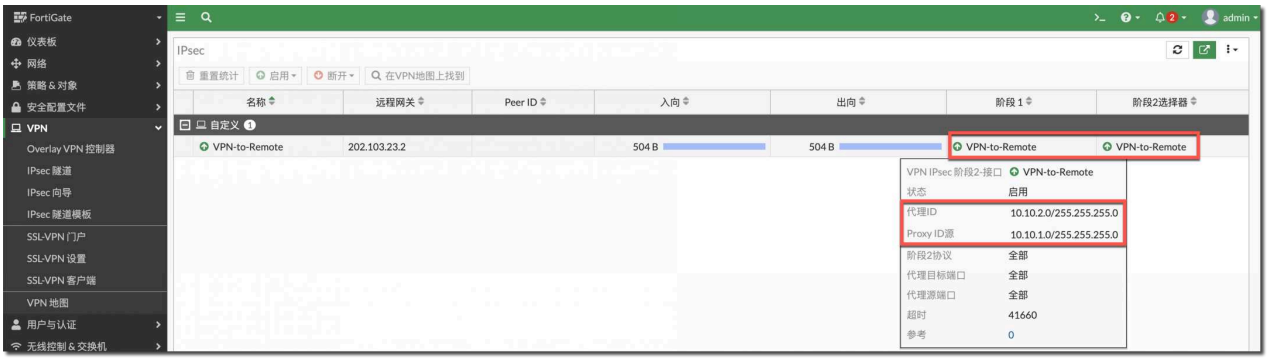

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                }
            }
        }
        from-zone untrust to-zone junos-host {
            policy to_FortiGate-2 {
                match {
                    source-address Remote;
                    destination-address Local;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
        from-zone untrust to-zone trust {
            policy to_FortiGate-2 {
                match {
                    source-address Remote;
                    destination-address Local;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-close;
                    }
                }
            }
        }
    }
}
```

1. 最后，点击页面右上角的Commit按钮提交所有配置。

结果验证

1. FortiGate上查看IPSec隧道建立，在仪表盘新建IPSec监控，可以看到IPSec建立成功。




```
FortiGate # diagnose vpn ike gateway list
vd: root/0
name: VPN-to-Remote
version: 1
interface: port2 4
addr: 202.103.13.2:500 → 202.103.23.2:500
tun_id: 202.103.23.2/::202.103.23.2
remote_location: 0.0.0.0
network-id: 0
created: 3s ago
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms
  id/spi: 84 81f7935c958dc231/0d50274a3603ed0c
  direction: initiator
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  status: established 3-3s ago = 10ms
  proposal: aes256-sha256
  key: 7617c0e9088a38f0-ba9b72527df54344-75a4f0b475a5c89a-ea60570f9f6a7f36
  lifetime/rekey: 86400/86096
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-Remote ver=1 serial=1 202.103.13.2:0->202.103.23.2:0 tun_id=202.103.23.2 tun_id6=::202.103.23.2
dst_mtu=1500 dpd-link=on weig1
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overla0
proxyid_num=1 child_num=0 refcnt=4 ilast=2 olast=2 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=65
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN-to-Remote proto=0 sa=1 ref=2 serial=2 auto-negotiate
  src: 0:10.10.1.0-10.10.1.255:0
  dst: 0:10.10.2.0-10.10.2.255:0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1438 expire=42888/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=0f3295e9 esp=aes key=32 1ef676bbce325c056b2bd2e7bdcc04b53d5493123ffff37734b92d7f0be650dc
       ah=sha256 key=32 1e0dd4317b3cf00168dad8528b820aadae59a09dac665d094324210b22abcadf
  enc: spi=06cf5a4d esp=aes key=32 06d4be5946563a9b7db6ad62c12625e61c18f83807abf62dbdf96d62f4dd2856
       ah=sha256 key=32 a11616829e581b70f3ec1e4fbecde7efb85a6da8cdb1718e34b40e12fbc5779f
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.13.2 npu_selid=1 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. 查看FortiGate的路由表。

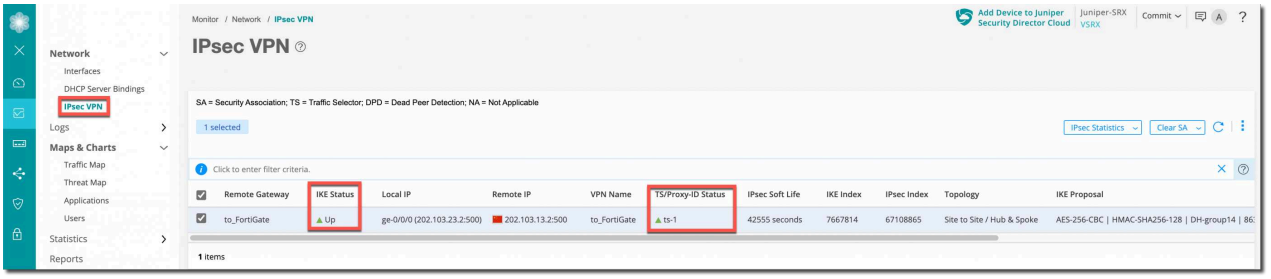
```
FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 202.103.13.1, port2, [1/0]
C       10.10.1.0/24 is directly connected, port3
S       10.10.2.0/24 [10/0] via VPN-to-Remote tunnel 202.103.23.2, [1/0]
C       192.168.100.0/24 is directly connected, port1
C       202.103.13.0/24 is directly connected, port2
```

3. FortiGate侧PC1业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.1.2/24         10.10.1.1
       fe80::250:79ff:fe66:6805/64

VPCS> ping 10.10.2.2

84 bytes from 10.10.2.2 icmp_seq=1 ttl=62 time=4.768 ms
84 bytes from 10.10.2.2 icmp_seq=2 ttl=62 time=1.770 ms
84 bytes from 10.10.2.2 icmp_seq=3 ttl=62 time=1.698 ms
84 bytes from 10.10.2.2 icmp_seq=4 ttl=62 time=2.116 ms
84 bytes from 10.10.2.2 icmp_seq=5 ttl=62 time=1.780 ms
```

4. Juniper防火墙查看IPSec连接状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
root@Juniper-SRX> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
7667814 UP     81f7935c958dc231  0d50274a3603ed0c  Main           202.103.13.2

root@Juniper-SRX>  show security ike security-associations 202.103.13.2 detail
IKE peer 202.103.13.2, Index 7667814, Gateway Name: to_FortiGate
  Role: Responder, State: UP
  Initiator cookie: 81f7935c958dc231, Responder cookie: 0d50274a3603ed0c
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 202.103.23.2:500, Remote: 202.103.13.2:500
  Lifetime: Expires in 86162 seconds
  Reauth Lifetime: Disabled
  IKE Fragmentation: Disabled, Size: 0
  Remote Access Client Info: Unknown Client
  Peer ike-id: 202.103.13.2
  AAA assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha256-128
   Encryption            : aes256-cbc
   Pseudo random function: hmac-sha256
   Diffie-Hellman group  : DH-group-14
  Traffic statistics:
   Input  bytes  :                 2996
   Output bytes  :                 2196
   Input  packets:                   15
   Output packets:                   14
   Input  fragmentated packets:       0
   Output fragmentated packets:       0
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 1
    Negotiation type: Quick mode, Role: Responder, Message ID: 0
    Local: 202.103.23.2:500, Remote: 202.103.13.2:500
    Local identity: 202.103.23.2
    Remote identity: 202.103.13.2
    Flags: IKE SA is created
```

```
root@Juniper-SRX> show security ipsec security-associations
  Total active tunnels: 1     Total Ipsec sas: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <67108865 ESP:aes-cbc-256/sha256 6cf5a4d 42899/ unlim - root 500 202.103.13.2
  ::: important
  67108865 ESP:aes-cbc-256/sha256 f3295e9 42899/ unlim - root 500 202.103.13.2
  :::

root@Juniper-SRX> show security ipsec security-associations vpn-name to_FortiGate detail
ID: 67108865 Virtual-system: root, VPN Name: to_FortiGate
  Local Gateway: 202.103.23.2, Remote Gateway: 202.103.13.2
  Traffic Selector Name: ts-1
  Local Identity: ipv4(10.10.2.0-10.10.2.255)
  Remote Identity: ipv4(10.10.1.0-10.10.1.255)
  Version: IKEv1
  DF-bit: clear, Copy-Outer-DSCP Enabled, Bind-interface: st0.0
  Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x2c608b29
  Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
  Tunnel events:
    Tue Apr 11 2023 15:42:30
    : IPSec SA negotiation successfully completed          (1 times)
    Tue Apr 11 2023 15:42:30
    : IKE SA negotiation successfully completed            (4 times)
    Tue Apr 11 2023 15:42:29
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    : IPSec SA delete payload received from peer, corresponding IPSec SAs cleared (1 times)
    Tue Apr 11 2023 15:42:25
    : IPSec SA negotiation successfully completed          (1 times)
    Tue Apr 11 2023 15:42:25
    : IPSec SA delete payload received from peer, corresponding IPSec SAs cleared (1 times)
    Tue Apr 11 2023 15:20:00
    : IPSec SA negotiation successfully completed          (1 times)
    Tue Apr 11 2023 15:20:00
    : Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)
  Direction: inbound, SPI: 6cf5a4d, AUX-SPI: 0
                             , VPN Monitoring: -
    Hard lifetime: Expires in 42865 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 42302 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
  Direction: outbound, SPI: f3295e9, AUX-SPI: 0
                             , VPN Monitoring: -
    Hard lifetime: Expires in 42865 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 42302 seconds
    Mode: Tunnel(0 0), Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64
```

5. 查看Juniper防火墙的路由表，可以看到包含了自动注入的到FortiGate内网的路由，出接口为Tunnel接口。

```
root@Juniper-SRX> show route

inet.0: 8 destinations, 9 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
0.0.0.0/0          *[Static/5] 00:58:27
                    ::: important
                     to 202.103.23.1 via ge-0/0/0.0
                    :::
                    [Access-internal/12] 00:59:24, metric 0
                    ::: important
                     to 192.168.100.99 via fxp0.0
                    :::
10.10.1.0/24       *[Static/5] 00:19:34
                    ::: important
                     via st0.0
                    :::
10.10.2.0/24       *[Direct/0] 00:58:27
                    ::: important
                     via ge-0/0/1.0
                    :::
10.10.2.1/32       *[Local/0] 00:58:27
                       Local via ge-0/0/1.0
192.168.100.0/24   *[Direct/0] 00:59:24
                    ::: important
                     via fxp0.0
                    :::
192.168.100.4/32   *[Local/0] 00:59:24
                       Local via fxp0.0
202.103.23.0/24    *[Direct/0] 00:58:27
                    ::: important
                     via ge-0/0/0.0
                    :::
202.103.23.2/32    *[Local/0] 00:58:27
                       Local via ge-0/0/0.0
```

6. Juniper防火墙侧PC2业务测试。

```
VPCS> show

NAME   IP/MASK              GATEWAY                           GATEWAY
VPCS1  10.10.2.2/24         10.10.2.1
       fe80::250:79ff:fe66:6806/64


```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
VPCS> ping 10.10.1.2

84 bytes from 10.10.1.2 icmp_seq=1 ttl=62 time=1.410 ms
84 bytes from 10.10.1.2 icmp_seq=2 ttl=62 time=1.547 ms
84 bytes from 10.10.1.2 icmp_seq=3 ttl=62 time=1.624 ms
84 bytes from 10.10.1.2 icmp_seq=4 ttl=62 time=2.176 ms
84 bytes from 10.10.1.2 icmp_seq=5 ttl=62 time=1.661 ms
```

7. FortiGate侧抓包查看。

```
FortiGate # diagnose sniffer packet any 'host 10.10.2.2 and host 10.10.1.2 and icmp' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.2 and host 10.10.1.2 and icmp]
2023-04-11 15:49:30.598552 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:30.598585 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:30.598754 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:30.598761 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:31.601426 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:31.601457 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:31.601769 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:31.601774 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:32.604474 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:32.604508 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:32.604694 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:32.604701 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:33.607589 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:33.607647 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:33.608105 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:33.608124 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:34.609922 VPN-to-Remote in 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:34.609955 port3 out 10.10.2.2 → 10.10.1.2: icmp: echo request
2023-04-11 15:49:34.610140 port3 in 10.10.1.2 → 10.10.2.2: icmp: echo reply
2023-04-11 15:49:34.610153 VPN-to-Remote out 10.10.1.2 → 10.10.2.2: icmp: echo reply
```

说明

1. 关于sniffer抓VPN业务和ESP的包：

- 抓取IPsec VPN的IKE协商包：

```
diagnose sniffer packet any "host 101.1.1.1 and (port 500 or port 4500)" 4
```

- 抓取IPsec VPN的ESP加密数据包：

```
diagnose sniffer packet any "host 101.1.1.1 and esp" 4
```

- 抓取IPsec VPN的明文业务数据包：

```
diagnose sniffer packet any "host 192.168.112.100 and icmp" 4
```

- 注意：由于硬件设备存在IPsec VPN芯片加速，因此可能数据包会抓不完全，主要指“ESP数据和明文业务数据”抓不全，因此有时候需要将VPN隧道的NP加速关闭：

```
FortiGate # config vpn ipsec phase1-interface
FortiGate (phase1-interface) # edit BJ-OSPF-TO-SH
FortiGate (BJ-OSPF-TO-SH) # set npu-offload disable
FortiGate (BJ-OSPF-TO-SH) # end
```

2. juniper防火墙相关：

- juniper防火墙IPsec VPN Debug：

```
# set system syslog file kmd-logs daemon info
# set system syslog file kmd-logs match KMD
# commit
show log kmd-logs
```

- 参考文档：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- https://supportportal.juniper.net/s/article/SRX-Resolution-Guide-How-to-troubleshoot-Problem-Scenarios-in-VPN-tunnels ↗
- https://supportportal.juniper.net/s/article/SRX-How-to-configure-syslog-to-display-VPN-status-messages ↗
- https://supportportal.juniper.net/s/article/SRX-IKE-Phase-1-VPN-status-messages ↗
- https://supportportal.juniper.net/s/article/SRX-How-to-troubleshoot-IKE-Phase-2-VPN-connection-issues ↗

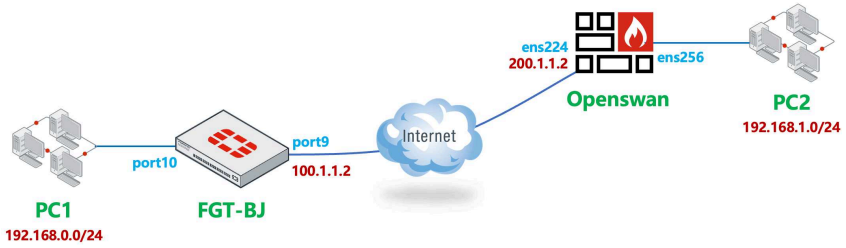
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与Openswan建立IPSec VPN

网络需求

通过IPsec VPN（接口模式）将2个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信。

网络拓扑



配置步骤

FortiGate IPSec配置

1. 基本配置

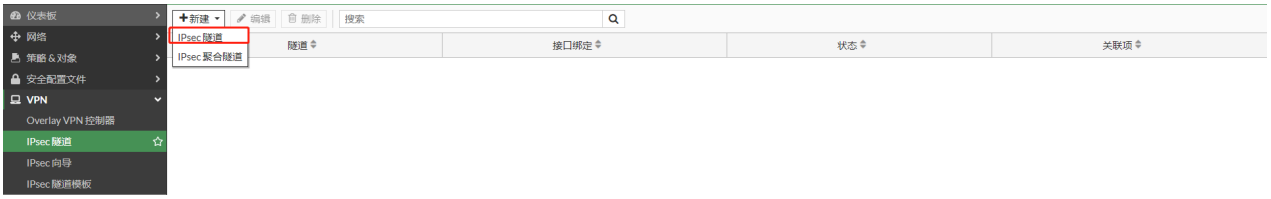
配置接口IP和路由。





2. 配置IPSEC

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



根据“VPN创建向导”进行VPN模板配置，输入名称，拓扑中没有NAT，这里选择“站点之间没有NAT”，并点击下一步。



输入对端设备的IP地址（流出接口会根据路由自动选择），以及预共享秘钥。

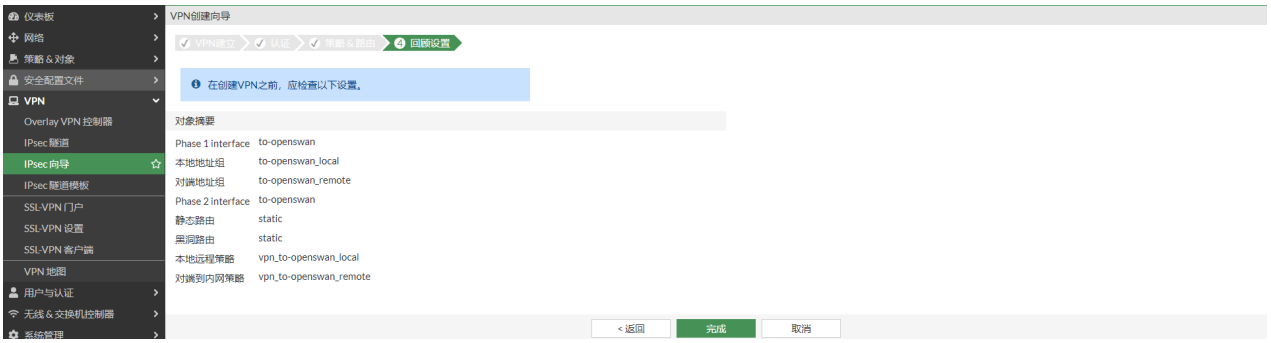
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



选择“本地接口”，即需要被IPSEC保护的内网的接口，这里是port10接口，本地子网会自动写为该接口的IP所在的IP网段（如果被保护的是其他网段，可以根据实际网络需求修改），输入“远端子网”，即远端需要被保护的网络。然后点击“下一步”。



VPN创建向导提示即将创建的内容，然后点击完成。



VPN创建成功。



3. 设置dpd和自动连接

在第一阶段中开启DPD周期性检测，每隔10s检测一次Peer状态。

```
config vpn ipsec phase1-interface
    edit "to-openswan"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

开启自动协商，主动让隧道UP起来，而非使用VPN业务的时候再去触发VPN的协商，这样可以减少业务的丢包。在VPN主动发起方开启即可。

IPSEC VPN阶段一自动协商是默认开启的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

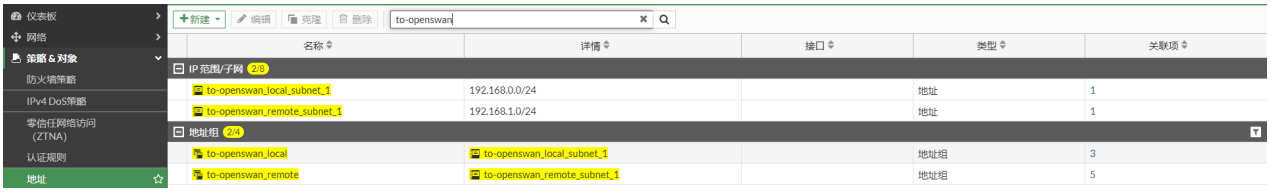
```
config vpn ipsec phase1-interface
    edit "to-openswan"
        set auto-negotiate enable
    next
end
```

IPSEC VPN阶段二自动协商默认关闭，需要开启。

```
config vpn ipsec phase2-interface
    edit "to-openswan"
        set auto-negotiate enable
    next
end
```

查看IPSEC向导所作的配置

1. 地址对象配置

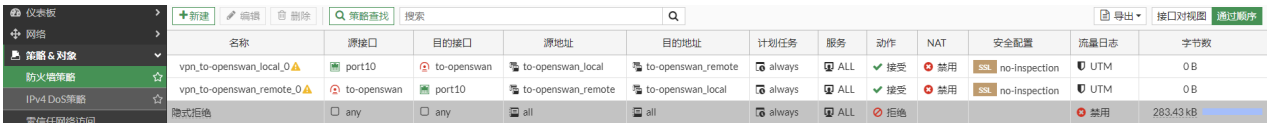


2. IPSEC配置




```
config vpn ipsec phase1-interface
    edit "to-openswan"
        set interface "port9"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set comments "VPN: to-openswan (Created by VPN wizard)"
        set wizard-type static-fortigate
        set remote-gw 200.1.1.2
        set psksecret ENC
p62NOSnHRHf0H/FDMjbdenLf9XFZ8AWBxxp4ztydCj8wqSRTiYDcbEBov4ZKf/5xUwzXl3tE3mUPLyRP9h6gq1YJGR2kocyO1hqc/Iy3hQa+LYORLl
znaMEKcxm6bKsNPeJHCe+FiOBatOW6pw9y8Vxwbp1yGvTkkKmyzfW3FWWzwbFHsa1AxigVRlZCsEKIzbW3dw==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "to-openswan"
        set phase1name "to-openswan"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set comments "VPN: to-openswan (Created by VPN wizard)"
        set src-addr-type name
        set dst-addr-type name
        set src-name "to-openswan_local"
        set dst-name "to-openswan_remote"
    next
end
```

3. 策略配置



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

4. 路由配置



配置openswan

1. 接口及路由配置

```
# ifconfig
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 200.1.1.2  netmask 255.255.255.0  broadcast 200.1.1.255
        inet6 fe80::2652:4dd7:5d0e:941d  prefixlen 64  scopeid 0x20<link>
        inet6 240e:604:109:39::216  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:37:f0:ac  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 2266 (2.2 KiB)
        RX errors 0  dropped 500  overruns 0  frame 0
        TX packets 18  bytes 2284 (2.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
ens256: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::227:594:d82:e098  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:37:f0:b6  txqueuelen 1000  (Ethernet)
        RX packets 2519  bytes 389134 (380.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 150  bytes 10928 (10.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         200.1.1.1       0.0.0.0         UG    106    0        0 ens224
192.168.1.0     0.0.0.0         255.255.255.0   U     105    0        0 ens256
200.1.1.0       0.0.0.0         255.255.255.0   U     106    0        0 ens224
```

2. 安装openswan

测试环境中centos版本

```
# rpm --query centos-release
centos-release-7-9.2009.1.el7.centos.x86_64

# uname -a
Linux centos7-3 3.10.0-1160.49.1.el7.x86_64 #1 SMP Tue Nov 30 15:51:32 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

安装openswan

```
yum install -y openswan
```

查看openswan安装的配置文件，libreswan即openswan。

```
# rpm -qc libreswan
/etc/ipsec.conf
/etc/ipsec.d/policies/block
/etc/ipsec.d/policies/clear
/etc/ipsec.d/policies/clear-or-private
/etc/ipsec.d/policies/portexcludes.conf
/etc/ipsec.d/policies/private
/etc/ipsec.d/policies/private-or-clear
/etc/ipsec.secrets
/etc/pam.d/pluto
```

3. 开启ipv4转发，关闭ICMP重定向

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
cat >> /etc/sysctl.conf << EOF
echo net.ipv4.ip_forward = 1
EOF

sysctl -a | egrep "ipv4.*(accept|send)_redirects" | awk -F "=" '{print$1"= 0"}'
sysctl -a | egrep "ipv4.*(accept|send)_redirects" | awk -F "=" '{print$1"= 0"}' >> /etc/sysctl.conf
sysctl -p /etc/sysctl.conf
```

4. **关闭SELINUX**

```
临时关闭：setenforce 0

永久关闭：
#vi /etc/selinux/config
SELINUX=disabled
```

5. **关闭防火墙或者开启IPSEC所需的端口UDP 500，UDP4500，ESP**

这里关闭防火墙

```
systemctl stop firewalld
systemctl disable firewalld
```

6. **配置openswan**

```
在/etc/ipsec.conf中默认包含如下配置，建议将IPsec连接作为单独的文件添加到/etc/ipsec.d/
include /etc/ipsec.d/*.conf
```

```
在/etc/ipsec.secrets中默认包含如下配置，建议将IPsec共享密钥作为单独的文件添加到/etc/ipsec.d/
include /etc/ipsec.d/*.secrets
```

配置IPSEC预共享密钥

```
vim /etc/ipsec.d/ipsec.secrets
100.1.1.2  : psk "ipsec-key"

格式：本地用于连接的IP+空格+远端网关IP+空格+英文冒号+空格+PSK+预共享密钥，冒号的两边都有空格，密钥用英文双引号。
```

配置IPSEC连接

```
vim /etc/ipsec.d/ipsec.conf
#ipsec连接名称
conn ipsec1

#phase1
#共享密钥
  authby=secret
#start表示ipsec服务启动后会主动发起IPSEC连接;add只表示添加，服务启动不会发起连接,使用ipsec auto --up ipsec名称发起连接
  auto=start
#阶段1密钥集
  ike=aes128-sha1;modp1536
#ike密钥交换方式
  keyexchange=ike
#阶段1生命周期
  ikelifetime=86400s
#默认为no主模式，野蛮模式为yes
  aggrmode=no

#phase2
#段2传输格式
  phase2=esp
#阶段2密钥集
  phase2alg=aes128-sha1;modp1536
#关闭压缩
  compress=no
#开启PFS
  pfs=yes
#阶段2生命周期
  salifetime=3600s
#隧道模式
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  type=tunnel
#本地IP
  left=200.1.1.2
#本地子网
  leftsubnet=192.168.1.0/24
#远端VPN网关IP
  right=100.1.1.2
#远端子网
  rightsubnet=192.168.0.0/24
#远端路由按缺省配置
  rightnexthop=%defaultroute
#开启dpd检查，每10s发起一次dpd检查，30s没有收到dpd响应，则清楚该ipsec连接
  dpddelay=10
  dpdtimeout=30
  dpdaction=clear

```

启动IPSEC服务

```
systemctl start ipsec
systemctl enable ipsec
```

通过ipsec verify进行配置项校验。如果回显信息全部为OK时，表示配置成功。

```
# ipsec verify
Verifying installed system and configuration files
Version check and ipsec on-path                         [OK]
Libreswan 3.25 (netkey) on 3.10.0-1160.49.1.el7.x86_64
Checking for IPsec support in kernel                    [OK]
 NETKEY: Testing XFRM related proc values
         ICMP default/send_redirects                    [OK]
         ICMP default/accept_redirects                  [OK]
         XFRM larval drop                               [OK]
Pluto ipsec.conf syntax                                 [OK]
Two or more interfaces found, checking IP forwarding    [OK]
Checking rp_filter                                      [OK]
Checking that pluto is running                          [OK]
 Pluto listening for IKE on udp 500                     [OK]
 Pluto listening for IKE/NAT-T on udp 4500              [OK]
 Pluto ipsec.secret syntax                              [OK]
Checking 'ip' command                                   [OK]
Checking 'iptables' command                             [OK]
Checking 'prelink' command does not interfere with FIPS [OK]
Checking for obsolete ipsec.conf options                [OK]
```

如果报如下错误：

```
Checking rp_filter                                      [ENABLED]
 /proc/sys/net/ipv4/conf/all/rp_filter                  [ENABLED]
 /proc/sys/net/ipv4/conf/ens192/rp_filter               [ENABLED]
 /proc/sys/net/ipv4/conf/ens224/rp_filter               [ENABLED]
 /proc/sys/net/ipv4/conf/ens256/rp_filter               [ENABLED]
 /proc/sys/net/ipv4/conf/ip_vti0/rp_filter              [ENABLED]
```

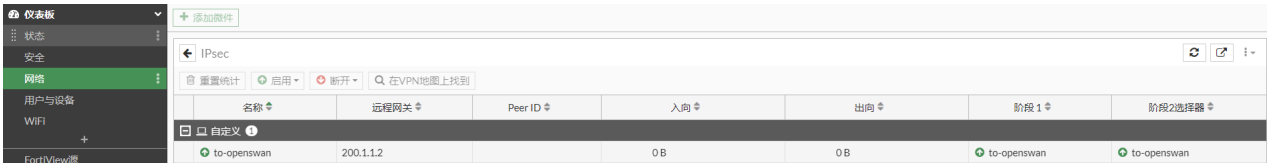
则通过如下命令解决：

```
 关闭源路由检查
 echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
 echo 0 > /proc/sys/net/ipv4/conf/ens192/rp_filter
 echo 0 > /proc/sys/net/ipv4/conf/ens224/rp_filter
 echo 0 > /proc/sys/net/ipv4/conf/ens256/rp_filter
 echo 0 > /proc/sys/net/ipv4/conf/ip_vti0/rp_filter
```

查看IPSEC状态

1. **查看FortiGate IPSEC状态**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
# diagnose vpn ike gateway  list

vd: root/0
name: to-openswan
version: 1
interface: port9 38
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 200.1.1.2/::200.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 19s ago
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 50/50/50 ms
  id/spi: 137 d69345dd761e35e1/0f7cdc8405b9cb8d
  direction: responder
  status: established 19-19s ago = 10ms
  proposal: aes128-sha1
  key: 82d396f4422ed9b5-2031250ed717f7f3
  lifetime/rekey: 86400/86110
  DPD sent/recv: 00000000/00003e85

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=to-openswan ver=1 serial=2 100.1.1.2:0→200.1.1.2:0 tun_id=200.1.1.2 tun_id6=::200.1.1.2 dst_mtu=1500 dpd-
link=on weight=1
bound_if=38 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=7 olast=7 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=158
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to-openswan proto=0 sa=1 ref=2 serial=3
  src: 0:192.168.0.0-192.168.0.255:0
  dst: 0:192.168.1.0-192.168.1.255:0
  SA:  ref=3 options=10226 type=00 soft=0 mtu=1438 expire=3312/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3330/3600
  dec: spi=dc629039 esp=aes key=16 257e01bac6998199e46bb81fcfea8ea7
       ah=sha1 key=20 ae77b59ee36fc4412db7c998b00513655ce05e44
  enc: spi=2d0f59d9 esp=aes key=16 3abe273778a50dd2e45708eaca1af809
       ah=sha1 key=20 5710a515c5a7d1a4bb857e1b62bce8a7ed8f0622
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=3 dec_npuid=0 enc_npuid=0
run_tally=0
```

2. 查看openswan IPSEC状态

```
# ipsec status
000 using kernel interface: netkey
000 interface lo/lo ::1@500
000 interface ens192/ens192 2022::231@500
000 interface ens224/ens224 240e:604:109:39::216@500
000 interface lo/lo 127.0.0.1@4500
000 interface lo/lo 127.0.0.1@500
000 interface ens192/ens192 192.168.88.231@4500
000 interface ens192/ens192 192.168.88.231@500
000 interface ens224/ens224 200.1.1.2@4500
000 interface ens224/ens224 200.1.1.2@500
000 interface ens256/ens256 192.168.1.1@4500
000 interface ens256/ens256 192.168.1.1@500
000
000
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
000 fips mode=disabled;
000 SElinux=disabled
000 seccomp=disabled
000
000 config setup options:
000
000 configdir=/etc, configfile=/etc/ipsec.conf, secrets=/etc/ipsec.secrets, ipsecdir=/etc/ipsec.d
000 nssdir=/etc/ipsec.d, dumpdir=/run/pluto, statsbin=unset
000 dnssec-rootkey-file=/var/lib/unbound/root.key, dnssec-trusted=<unset>
000 sbindir=/usr/sbin, libexecdir=/usr/libexec/ipsec
000 pluto_version=3.25, pluto_vendorid=OE-Libreswan-3.25
000 nhelpers=-1, uniqueids=yes, dnssec-enable=yes, perpeerlog=no, logappend=yes, logip=yes, shuntlifetime=900s,
xfrmlifetime=300s
000 ddos-cookies-threshold=50000, ddos-max-halfopen=25000, ddos-mode=auto
000 ikeport=500, ikebuf=0, msg_errqueue=yes, strictcrlpolicy=no, crlcheckinterval=0, listen=<any>, nflog-all=0
000 ocsp-enable=no, ocsp-strict=no, ocsp-timeout=2, ocsp-uri=<unset>
000 ocsp-trust-name=<unset>
000 ocsp-cache-size=1000, ocsp-cache-min-age=3600, ocsp-cache-max-age=86400, ocsp-method=get
000 secctx-attr-type=32001
000 debug: control
000
000 nat-traversal=yes, keep-alive=20, nat-ikeport=4500
000 virtual-private (%priv):
000 - allowed subnets: 10.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, 25.0.0.0/8, 100.64.0.0/10, fd00::/8, fe80::/10
000
000 ESP algorithms supported:
000
000 algorithm ESP encrypt: id=3, name=ESP_3DES, ivlen=8, keysizemin=192, keysizemax=192
000 algorithm ESP encrypt: id=6, name=ESP_CAST, ivlen=8, keysizemin=128, keysizemax=128
000 algorithm ESP encrypt: id=11, name=ESP_NULL, ivlen=0, keysizemin=0, keysizemax=0
000 algorithm ESP encrypt: id=12, name=ESP_AES, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=13, name=ESP_AES_CTR, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=14, name=ESP_AES_CCM_A, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=15, name=ESP_AES_CCM_B, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=16, name=ESP_AES_CCM_C, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=18, name=ESP_AES_GCM_A, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=19, name=ESP_AES_GCM_B, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=20, name=ESP_AES_GCM_C, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=22, name=ESP_CAMELLIA, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=23, name=ESP_NULL_AUTH_AES_GMAC, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=252, name=ESP_SERPENT, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm ESP encrypt: id=253, name=ESP_TWOFISH, ivlen=8, keysizemin=128, keysizemax=256
000 algorithm AH/ESP auth: id=1, name=AUTH_ALGORITHM_HMAC_MD5, keysizemin=128, keysizemax=128
000 algorithm AH/ESP auth: id=2, name=AUTH_ALGORITHM_HMAC_SHA1, keysizemin=160, keysizemax=160
000 algorithm AH/ESP auth: id=5, name=AUTH_ALGORITHM_HMAC_SHA2_256, keysizemin=256, keysizemax=256
000 algorithm AH/ESP auth: id=6, name=AUTH_ALGORITHM_HMAC_SHA2_384, keysizemin=384, keysizemax=384
000 algorithm AH/ESP auth: id=7, name=AUTH_ALGORITHM_HMAC_SHA2_512, keysizemin=512, keysizemax=512
000 algorithm AH/ESP auth: id=8, name=AUTH_ALGORITHM_HMAC_RIPEMD, keysizemin=160, keysizemax=160
000 algorithm AH/ESP auth: id=9, name=AUTH_ALGORITHM_AES_XCBC, keysizemin=128, keysizemax=128
000 algorithm AH/ESP auth: id=250, name=AUTH_ALGORITHM_AES_CMAC_96, keysizemin=128, keysizemax=128
000 algorithm AH/ESP auth: id=251, name=AUTH_ALGORITHM_NULL_KAME, keysizemin=0, keysizemax=0
000
000 IKE algorithms supported:
000
000 algorithm IKE encrypt: v1id=5, v1name=OAKLEY_3DES_CBC, v2id=3, v2name=3DES, blocksize=8, keydeflen=192
000 algorithm IKE encrypt: v1id=8, v1name=OAKLEY_CAMELLIA_CBC, v2id=23, v2name=CAMELLIA_CBC, blocksize=16,
keydeflen=128
000 algorithm IKE encrypt: v1id=-1, v1name=n/a, v2id=20, v2name=AES_GCM_C, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: v1id=-1, v1name=n/a, v2id=19, v2name=AES_GCM_B, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: v1id=-1, v1name=n/a, v2id=18, v2name=AES_GCM_A, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: v1id=13, v1name=OAKLEY_AES_CTR, v2id=13, v2name=AES_CTR, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: v1id=7, v1name=OAKLEY_AES_CBC, v2id=12, v2name=AES_CBC, blocksize=16, keydeflen=128
000 algorithm IKE encrypt: v1id=65004, v1name=OAKLEY_SERPENT_CBC, v2id=65004, v2name=SERPENT_CBC, blocksize=16,
keydeflen=128
000 algorithm IKE encrypt: v1id=65005, v1name=OAKLEY_TWOFISH_CBC, v2id=65005, v2name=TWOFISH_CBC, blocksize=16,
keydeflen=128
000 algorithm IKE encrypt: v1id=65289, v1name=OAKLEY_TWOFISH_CBC_SSH, v2id=65289, v2name=TWOFISH_CBC_SSH,
blocksize=16, keydeflen=128
000 algorithm IKE PRF: name=HMAC_MD5, hashlen=16
000 algorithm IKE PRF: name=HMAC_SHA1, hashlen=20
000 algorithm IKE PRF: name=HMAC_SHA2_256, hashlen=32
000 algorithm IKE PRF: name=HMAC_SHA2_384, hashlen=48
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
000 algorithm IKE PRF: name=HMAC_SHA2_512, hashlen=64
000 algorithm IKE PRF: name=AES_XCBC, hashlen=16
000 algorithm IKE DH Key Exchange: name=MODP1024, bits=1024
000 algorithm IKE DH Key Exchange: name=MODP1536, bits=1536
000 algorithm IKE DH Key Exchange: name=MODP2048, bits=2048
000 algorithm IKE DH Key Exchange: name=MODP3072, bits=3072
000 algorithm IKE DH Key Exchange: name=MODP4096, bits=4096
000 algorithm IKE DH Key Exchange: name=MODP6144, bits=6144
000 algorithm IKE DH Key Exchange: name=MODP8192, bits=8192
000 algorithm IKE DH Key Exchange: name=DH19, bits=512
000 algorithm IKE DH Key Exchange: name=DH20, bits=768
000 algorithm IKE DH Key Exchange: name=DH21, bits=1056
000 algorithm IKE DH Key Exchange: name=DH22, bits=1024
000 algorithm IKE DH Key Exchange: name=DH23, bits=2048
000 algorithm IKE DH Key Exchange: name=DH24, bits=2048
000
000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,3,64} trans={0,3,6936} attrs={0,3,4624}
000
000 Connection list:
000
000 "ipsec1": 192.168.1.0/24===200.1.1.2<200.1.1.2>...100.1.1.2<100.1.1.2>===192.168.0.0/24; erouted; eroute
owner: #3
000 "ipsec1":     oriented; my_ip=unset; their_ip=unset; my_updown=ipsec _updown;
000 "ipsec1":   xauth us:none, xauth them:none,  my_username=[any]; their_username=[any]
000 "ipsec1":   our auth:secret, their auth:secret
000 "ipsec1":   modecfg info: us:none, them:none, modecfg policy:push, dns:unset, domains:unset, banner:unset,
cat:unset;
000 "ipsec1":   labeled_ipsec:no;
000 "ipsec1":   policy_label:unset;
000 "ipsec1":   ike_life: 86400s; ipsec_life: 3600s; replay_window: 32; rekey_margin: 540s; rekey_fuzz: 100%;
keyingtries: 0;
000 "ipsec1":   retransmit-interval: 500ms; retransmit-timeout: 60s;
000 "ipsec1":   initial-contact:no; cisco-unity:no; fake-strongswan:no; send-vendorid:no; send-no-esp-tfc:no;
000 "ipsec1":   policy: PSK+ENCRYPT+TUNNEL+PFS+UP+IKEV1_ALLOW+IKEV2_ALLOW+SAREF_TRACK+IKE_FRAG_ALLOW+ESN_NO;
000 "ipsec1":   conn_prio: 24,24; interface: ens224; metric: 0; mtu: unset; sa_prio:auto; sa_tfc:none;
000 "ipsec1":   nflog-group: unset; mark: unset; vti-iface:unset; vti-routing:no; vti-shared:no; nic-offload:auto;
000 "ipsec1":   our idtype: ID_IPV4_ADDR; our id=200.1.1.2; their idtype: ID_IPV4_ADDR; their id=100.1.1.2
000 "ipsec1":   dpd: action:clear; delay:10; timeout:30; nat-t: encaps:auto; nat_keepalive:yes; ikev1_natt:both
000 "ipsec1":   newest ISAKMP SA: #2; newest IPsec SA: #3;
000 "ipsec1":   IKE algorithms: AES_CBC_128-HMAC_SHA1-MODP1536
000 "ipsec1":   IKE algorithm newest: AES_CBC_128-HMAC_SHA1-MODP1536
000 "ipsec1":   ESP algorithms: AES_CBC_128-HMAC_SHA1_96-MODP1536
000 "ipsec1":   ESP algorithm newest: AES_CBC_128-HMAC_SHA1_96; pfsgroup=MODP1536
000
000 Total IPsec connections: loaded 1, active 1
000
000 State Information: DDoS cookies not required, Accepting new IKE connections
000 IKE SAs: total(1), half-open(0), open(0), authenticated(1), anonymous(0)
000 IPsec SAs: total(1), authenticated(1), anonymous(0)
000
000 #2: "ipsec1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 85343s; newest ISAKMP;
lastdpd=3s(seq in:16011 out:0); idle; import:admin initiate
000 #3: "ipsec1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2784s; newest IPSEC;
eroute owner; isakmp#2; idle; import:admin initiate
000 #3: "ipsec1" esp.dc629039@100.1.1.2 esp.2d0f59d9@200.1.1.2 tun.0@100.1.1.2 tun.0@200.1.1.2 ref=0 refhim=0
Traffic: ESPin=0B ESPout=0B! ESPmax=4194303B
000
000 Bare Shunt list:
000
```

业务测试

1. 从FortiGate端PC ping OPENSWAN端的PC

```
PC1# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        ether 00:0c:29:0e:4e:c5  txqueuelen 1000  (Ethernet)
        RX packets 58117456  bytes 4943397966 (4.6 GiB)
        RX errors 0  dropped 183  overruns 0  frame 0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        TX packets 3346784  bytes 205418084392 (191.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC1# ping 192.168.1.10 -c 4
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=62 time=1.13 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=62 time=0.852 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=62 time=0.750 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=62 time=0.775 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.750/0.877/1.132/0.153 ms
```

2. 从 OPENSWAN端的PC ping FortiGate端PC

```
PC2# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6476393  bytes 1884675006 (1.7 GiB)
        RX errors 0  dropped 3749817  overruns 0  frame 0
        TX packets 184443  bytes 12303642 (11.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC2# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.681 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.715 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.801 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=0.771 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.681/0.742/0.801/0.046 ms
```

OPENSWAN debug查看

开启openswan debug

```
# /etc/ipsec.conf - Libreswan IPsec configuration file
# see 'man ipsec.conf' and 'man pluto' for more information
# For example configurations and documentation, see https://libreswan.org/wiki/
config setup
        # Normally, pluto logs via syslog.
        logfile=/var/log/pluto.log
        #
        # Do not enable debug options to debug configuration issues!
        #
        # plutodebug="control parsing"
        # plutodebug="all crypt"
        plutodebug=control
```

1. 阶段1密钥机不匹配时，openswan debug显示如下：

```
Feb  7 17:58:48.108027: | *received 332 bytes from 100.1.1.2:500 on ens224 (port=500)
Feb  7 17:58:48.108082: | processing: start from 100.1.1.2:500 (in process_md() at demux.c:392)
Feb  7 17:58:48.108103: |  processing version=1.0 packet with exchange type=ISAKMP_XCHG_IDPROT (2)
Feb  7 17:58:48.108119: | icookie table: hash icookie fc 65 ed f1  76 0e d2 08 to 15842219016969466431 slot
0x558680eded00
Feb  7 17:58:48.108126: | v1 state object not found
Feb  7 17:58:48.108148: | received Vendor ID payload [RFC 3947]
Feb  7 17:58:48.108160: | ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
Feb  7 17:58:48.108171: | ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
Feb  7 17:58:48.108179: | ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n]
Feb  7 17:58:48.108186: | ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-01]
Feb  7 17:58:48.108195: | ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
Feb  7 17:58:48.108205: | received Vendor ID payload [Dead Peer Detection]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Feb  7 17:58:48.108213: | received Vendor ID payload [FRAGMENTATION]
Feb  7 17:58:48.108224: | received Vendor ID payload [FRAGMENTATION c0000000]
Feb  7 17:58:48.108237: packet from 100.1.1.2:500: ignoring unknown Vendor ID payload
[8299031757a36082c6a621de00000000]
Feb  7 17:58:48.108251: | creating state object #2 at 0×558682efea98
Feb  7 17:58:48.108265: | processing: start state #2 connection "ipsec1" 100.1.1.2:500 (in main_inI1_outR1() at
ikev1_main.c:757)
Feb  7 17:58:48.108313: | inserting state object #2
Feb  7 17:58:48.108338: "ipsec1" #2: responding to Main Mode
Feb  7 17:58:48.108372: | started looking for secret for 200.1.1.2→100.1.1.2 of kind PKK_PSK
Feb  7 17:58:48.108384: | actually looking for secret for 200.1.1.2→100.1.1.2 of kind PKK_PSK
Feb  7 17:58:48.108397: | 1: compared key 100.1.1.2 to 200.1.1.2 / 100.1.1.2 → 4
Feb  7 17:58:48.108406: | 2: compared key 200.1.1.2 to 200.1.1.2 / 100.1.1.2 → 12
Feb  7 17:58:48.108413: | line 1: match=12
Feb  7 17:58:48.108422: | best_match 0>12 best=0×558682efd7c8 (line=1)
Feb  7 17:58:48.108430: | concluding with best_match=12 best=0×558682efd7c8 (lineno=1)
Feb  7 17:58:48.108441: "ipsec1" #2: WARNING: connection ipsec1 PSK length of 8 bytes is too short for sha2_256
PRF in FIPS mode (16 bytes required)
Feb  7 17:58:48.108461: "ipsec1" #2: Oakley Transform [AES_CBC (256), HMAC_SHA2_256, MODP2048] refused
Feb  7 17:58:48.108471: | started looking for secret for 200.1.1.2→100.1.1.2 of kind PKK_PSK
Feb  7 17:58:48.108478: | actually looking for secret for 200.1.1.2→100.1.1.2 of kind PKK_PSK
Feb  7 17:58:48.108486: | 1: compared key 100.1.1.2 to 200.1.1.2 / 100.1.1.2 → 4
Feb  7 17:58:48.108495: | 2: compared key 200.1.1.2 to 200.1.1.2 / 100.1.1.2 → 12
Feb  7 17:58:48.108505: | line 1: match=12
Feb  7 17:58:48.108512: | best_match 0>12 best=0×558682efd7c8 (line=1)
Feb  7 17:58:48.108522: | concluding with best_match=12 best=0×558682efd7c8 (lineno=1)
Feb  7 17:58:48.108533: "ipsec1" #2: WARNING: connection ipsec1 PSK length of 8 bytes is too short for sha2_256
PRF in FIPS mode (16 bytes required)
Feb  7 17:58:48.108541: "ipsec1" #2: Oakley Transform [AES_CBC (256), HMAC_SHA2_256, MODP1536] refused
Feb  7 17:58:48.108548: "ipsec1" #2: no acceptable Oakley Transform
Feb  7 17:58:48.108556: | complete v1 state transition with NO_PROPOSAL_CHOSEN
```

2. 当共享密钥错误时，openswan debug显示如下：

```
Feb  7 17:57:28.726151: | *received 108 bytes from 100.1.1.2:500 on ens224 (port=500)
Feb  7 17:57:28.726176: | processing: start from 100.1.1.2:500 (in process_md() at demux.c:392)
Feb  7 17:57:28.726186: |  processing version=1.0 packet with exchange type=ISAKMP_XCHG_IDPROT (2)
Feb  7 17:57:28.726197: | cookies table: hash icookie 2b 08 9f f0  ed 75 b2 1a rcookie 2e fa 5e f5  8a 50 a4 93 to
10219631855637370284 slot 0×558680ed9da0
Feb  7 17:57:28.726217: | v1 peer and cookies match on #1, provided msgid 00000000 == 00000000
Feb  7 17:57:28.726224: | v1 state object #1 found, in STATE_MAIN_R2
Feb  7 17:57:28.726232: | processing: start state #1 connection "ipsec1" 100.1.1.2:500 (in process_v1_packet() at
ikev1.c:1117)
Feb  7 17:57:28.726270: "ipsec1" #1: byte 2 of ISAKMP Identification Payload should have been zero, but was not
(ignored)
Feb  7 17:57:28.726283: "ipsec1" #1: length of ISAKMP Identification Payload is larger than can fit
Feb  7 17:57:28.726290: "ipsec1" #1: probable authentication failure (mismatch of preshared secrets?): malformed
payload in packet
Feb  7 17:57:28.726313: | processing: stop from 100.1.1.2:500 (BACKGROUND) (in process_md() at demux.c:394)
Feb  7 17:57:28.726322: | processing: stop state #1 connection "ipsec1" 100.1.1.2:500 (in process_md() at
demux.c:396)
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

与strongSwan建立IPsec VPN

配置请参考链接：FortiGate与strongSwan建立IPSec VPN ↗。

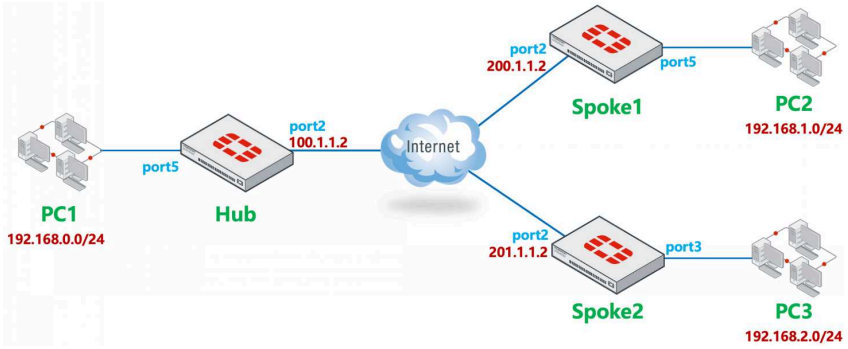
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Hub-and-spoke模式

网络需求

某公司总部内部有一台OA服务器，其余分2个支机构都需要通过vpn拨入总部内网对OA服务器进行访问，为了方便配置，总部不想有太多的配置，总部只建立一条vpn隧道，实现所有分支机构和总部的通讯，SPOKE之间的流量通过HUB进行中转。

网络拓扑

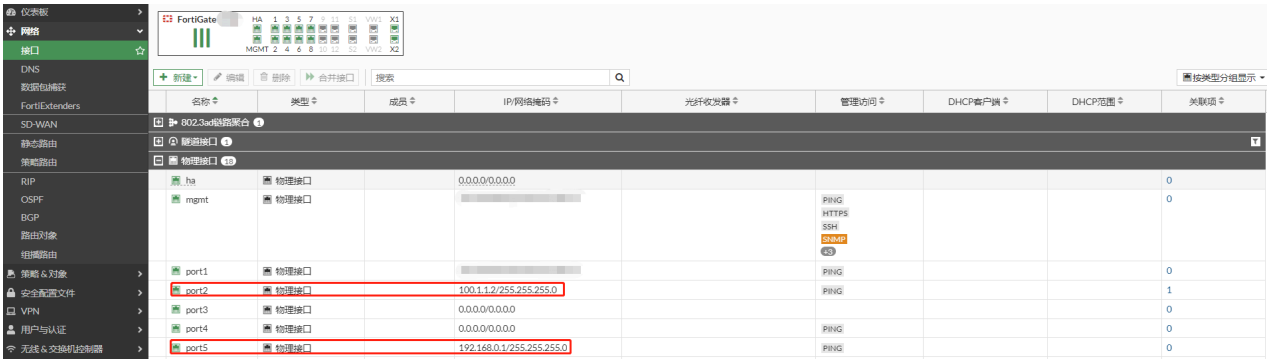


配置步骤

HUB配置

1. **基本配置**

   配置接口IP和路由





2. **配置IPSEC VPN**

   总部（HUB）IPsec VPN配置说明：

   - HUB使用动态拨号的VPN方式。 因为分支可能来自任意地方的IP，另外分支可能使用PPPOE拨号，公网IP随时会变更，因此没有办法确认对方的公网IP，只能动态拨号方式的IPsec VPN。
   - HUB使用主模式。

     其实HUB的阶段1使用主模式或野蛮模式二者都是可以工作的，只要hub和spoke之间使用相同的阶段1模式即可。

     如果HUB相同接口下（如wan1口）只有一条动态拨号的IPsec VPN，可以简单的直接使用主模式，接收Peer ID为any即可。

     如果HUB相同接口下（如wan1口）有两条或以上type是dynamic的阶段1，就必须使用野蛮模式，因为阶段1 type是dynamic的remote-gw为0.0.0.0，存在多个时会导致冲突，结果匹配到非预期的阶段1，这时候必须使用野蛮模式的Peer ID来区分/匹配）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

一条动态拨号VPN的场景下我们HUB选择最简单的主动模式+任意Peer ID+预共享密钥。这种选择优势是在SPOKE看来感觉就像是建立一个很普通的LAN-TO-LAN的IPsec VPN。

- HUB第二阶段感兴趣流保持默认的0.0.0.0/0.0.0.0↔0.0.0.0/0.0.0.0。

> **重要**
>
> 如果使用静态路由来转发Hub与Spoke之间的流量，由于Hub是被动的接受Spoke的协商，在没有协商之前Hub不知道Spoke的具体网段/感兴趣流，Hub保持默认0.0.0.0/0↔0.0.0.0/0即可，会自动学习分支的源保护网段，同时自动产生反向的去往感兴趣流的回程静态路由（一阶段开启了add-route功能），不要在Hub上手动配置去往Spoke内网的静态路由，否则会出现VPN技术→IPSec VPN→IPSec VPN排错→ Hub-Spoke静态路由问题 ↗章节的问题。
>
> 而Spoke是需要配置明细的源保护网段的，如192.168.1.0/24↔0.0.0.0/0，Hub通过add-route功能自动添加去往Spoke源保护网段（192.168.1.0/24）的静态路由。

创建IPSEC VPN。



IPSEC VPN阶段一配置。



IPSEC VPN阶段二配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建完成。



对应的命令行

```bash
config vpn ipsec phase1-interface
    edit "HUB"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route enable    //确保Hub的add-route开启，默认开启//
        set dpd on-idle
        set psksecret ENC
o00sB0EFtnTN9mJd5/xShv4v22vbn3NpgGIepVJSXGup1iQ++HB0zjDaOuj8jIyKjxZ3yhYqjtQXL9HJ5aoTQ4rlVRiBlw7jcxbSB8lzbU0As8YhUo
b3Z6T2StvFeRC1VUDac8wmjsPbkUkOq0YlRZ22DoQMe2t+lG6orUAgDlY6iko6mlodLfmMiRxOFNIASP5UNg==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "HUB"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set phase1name "HUB"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set keepalive enable
    next
end
```

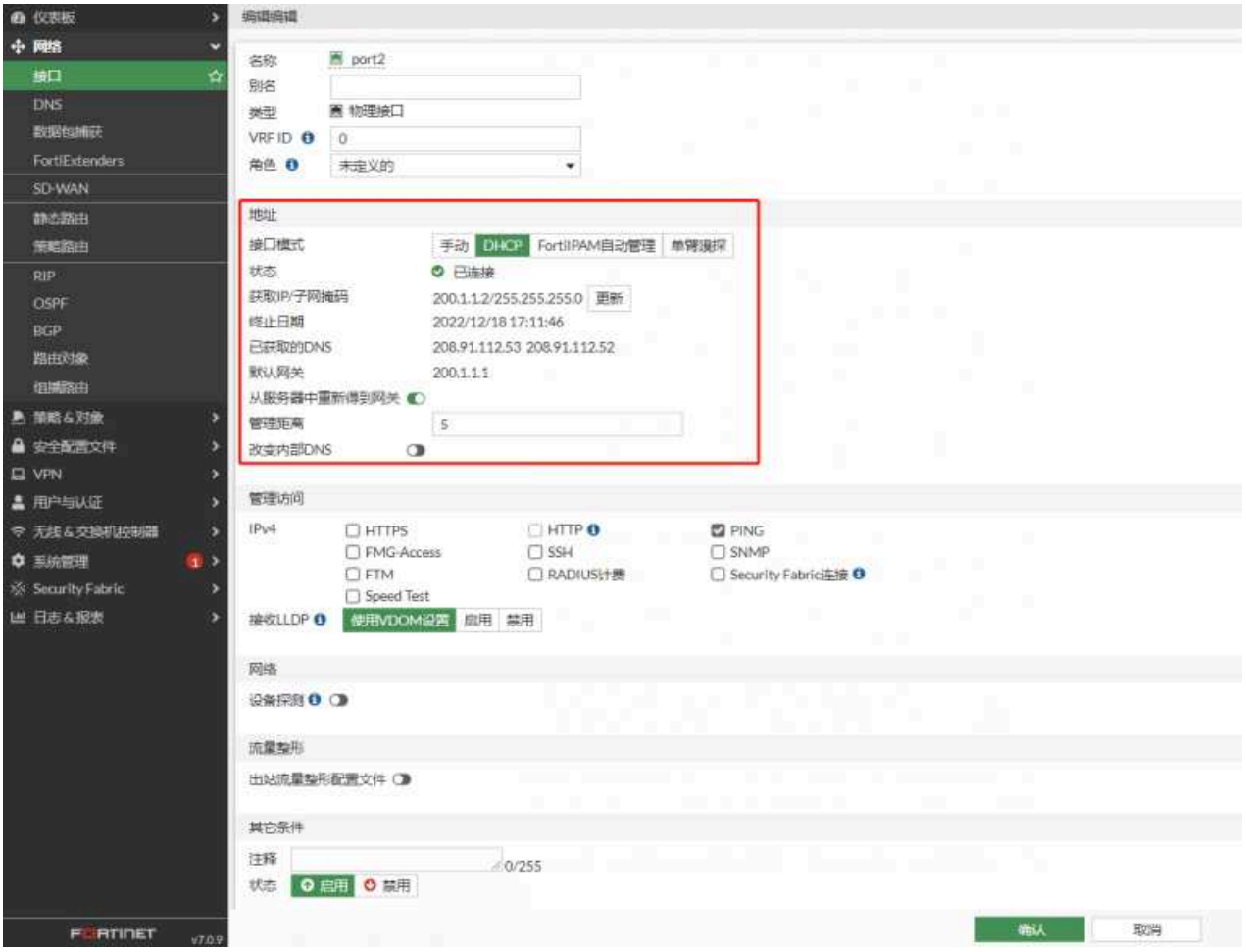
3. 配置策略

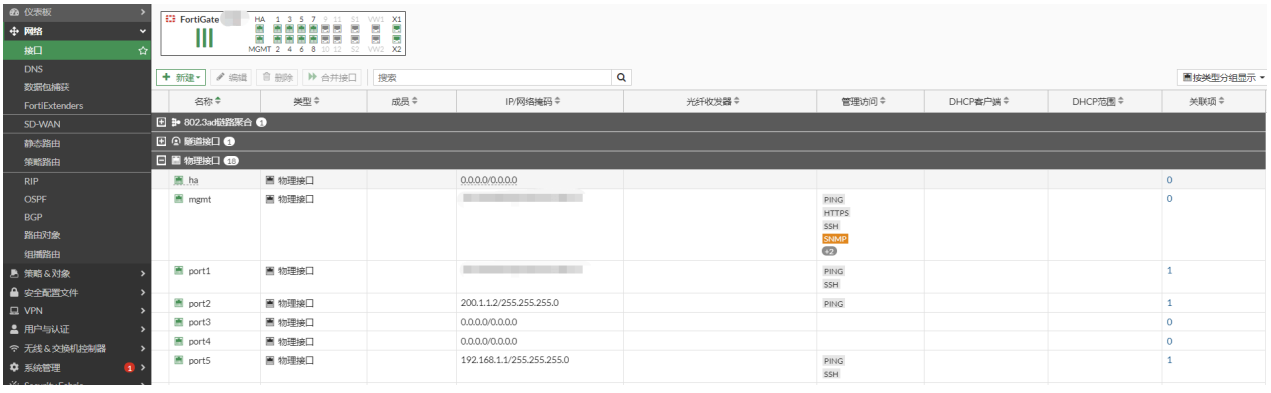
创建3条策略，从上到下分别是：分支到总部的放通策略；总部到分支的放通策略；分支到分支的放通策略。



SPOKE1配置

1. 基本配置





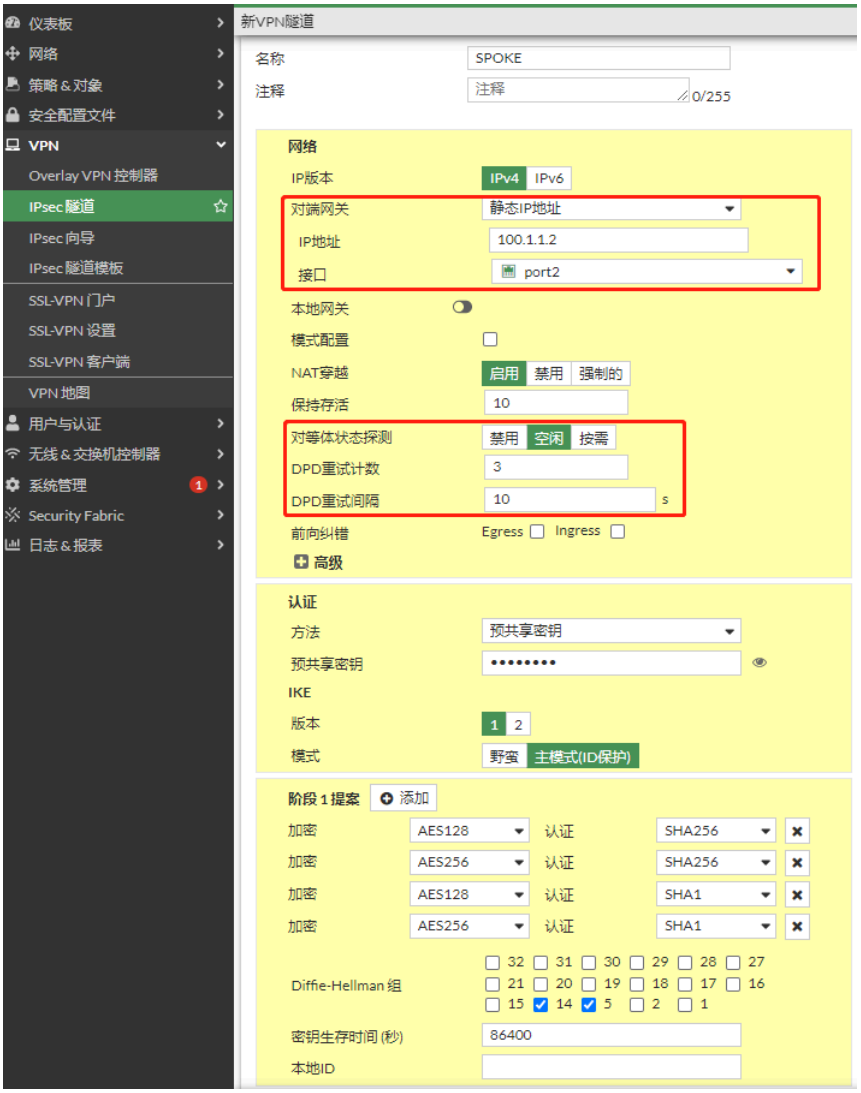
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置IPSEC VPN

创建IPSEC VPN。



IPSEC VPN阶段一配置



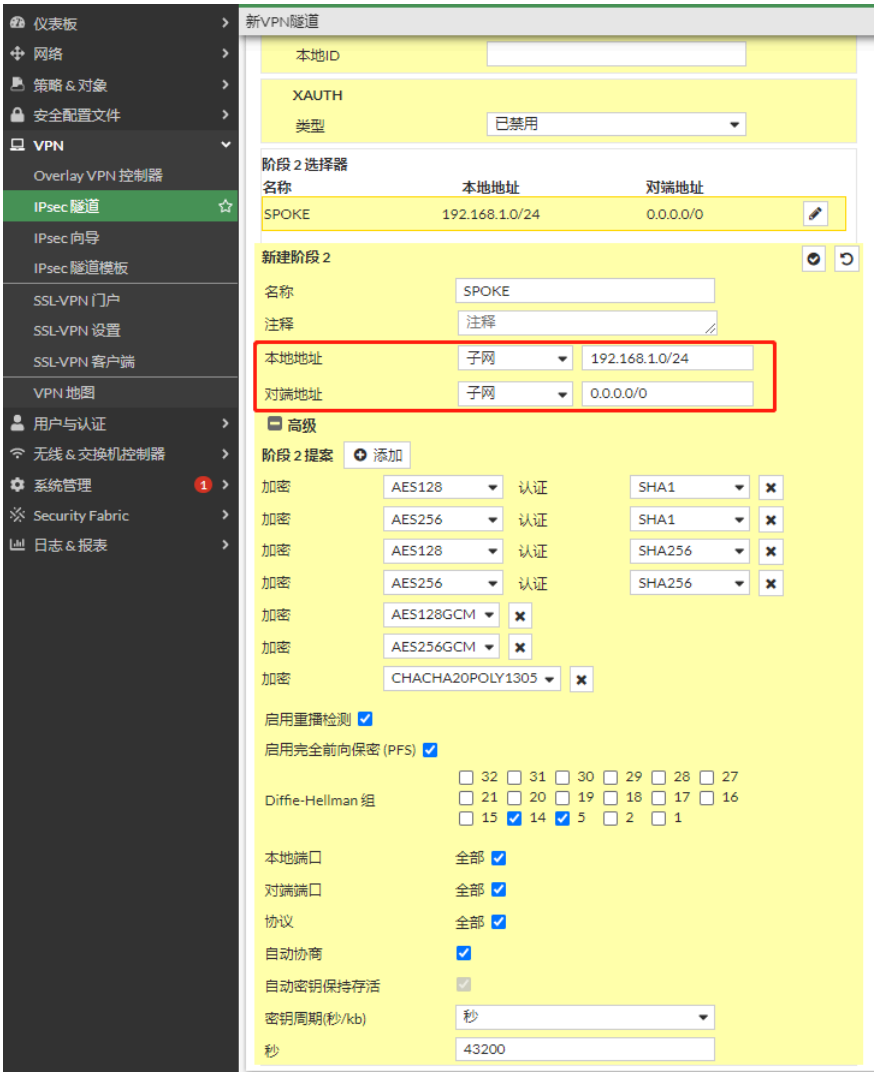
IPSEC VPN阶段二配置。

重要

如果使用静态路由来转发Hub与Spoke之间的流量，由于Hub是被动的接受Spoke的协商，在没有协商之前Hub不知道Spoke的具体网段/感兴趣流，Hub保持默认0.0.0.0/0↔0.0.0.0/0即可，会自动学习分支的源保护网段，同时自动产生反向的去往感兴趣流的回程静态路由（一阶段开启了add-route功能），不要在Hub上手动配置去往Spoke内网的静态路由，否则会出现VPN技术→IPSec VPN→IPSec VPN排错→ Hub-Spoke静态路由问题 ↗章节的问题。

而Spoke是需要配置明细的源保护网段的，如192.168.1.0/24↔0.0.0.0/0，Hub通过add-route功能自动添加去往Spoke源保护网段（192.168.1.0/24）的静态路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建完成。



对应的命令行

```
config vpn ipsec phase1-interface
    edit "SPOKE1"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 100.1.1.2
        set psksecret ENC
/nQqtlGc19JE/tKd0G4lHD1r7279qcDTpVAlNPW1djHDvxMhIuZctGGr1lw1l/Odi3WkvMrhEDydpVxEtvSWPBUp2+pbhB8fXowEkkoYtaGvvmA0oh
j+Bk7NOETHZKUQw9D7b8ibhF5HjbbEphvWb6QwDgI+pjwhp56AZp6sF05L3RLR2nLMEqJKCf6CBog5Se/MbA==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "SPOKE1"
        set phase1name "SPOKE1"
```

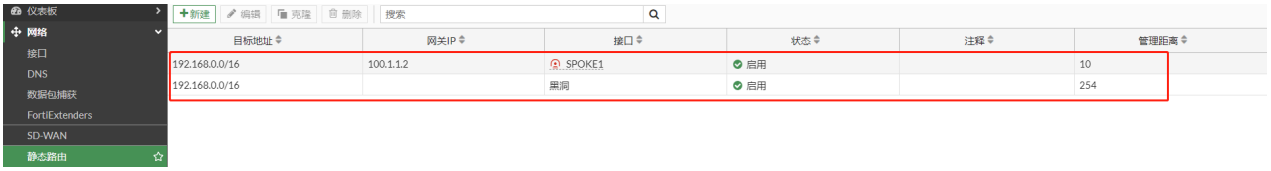

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 192.168.1.0 255.255.255.0
    next
end
```

3. 配置路由

这里路由的目标是192.168.0.0/16，是HUB和其他SPOKE的业务网段汇总（分支之间没有单独建立VPN，从HUB互通）。如果只需要访问总部，则写总部的明细网段即可，即192.168.0.0/24。

管理距离为254的黑洞路由是为了VPN中断的时候防止产生错误的NAT会话。



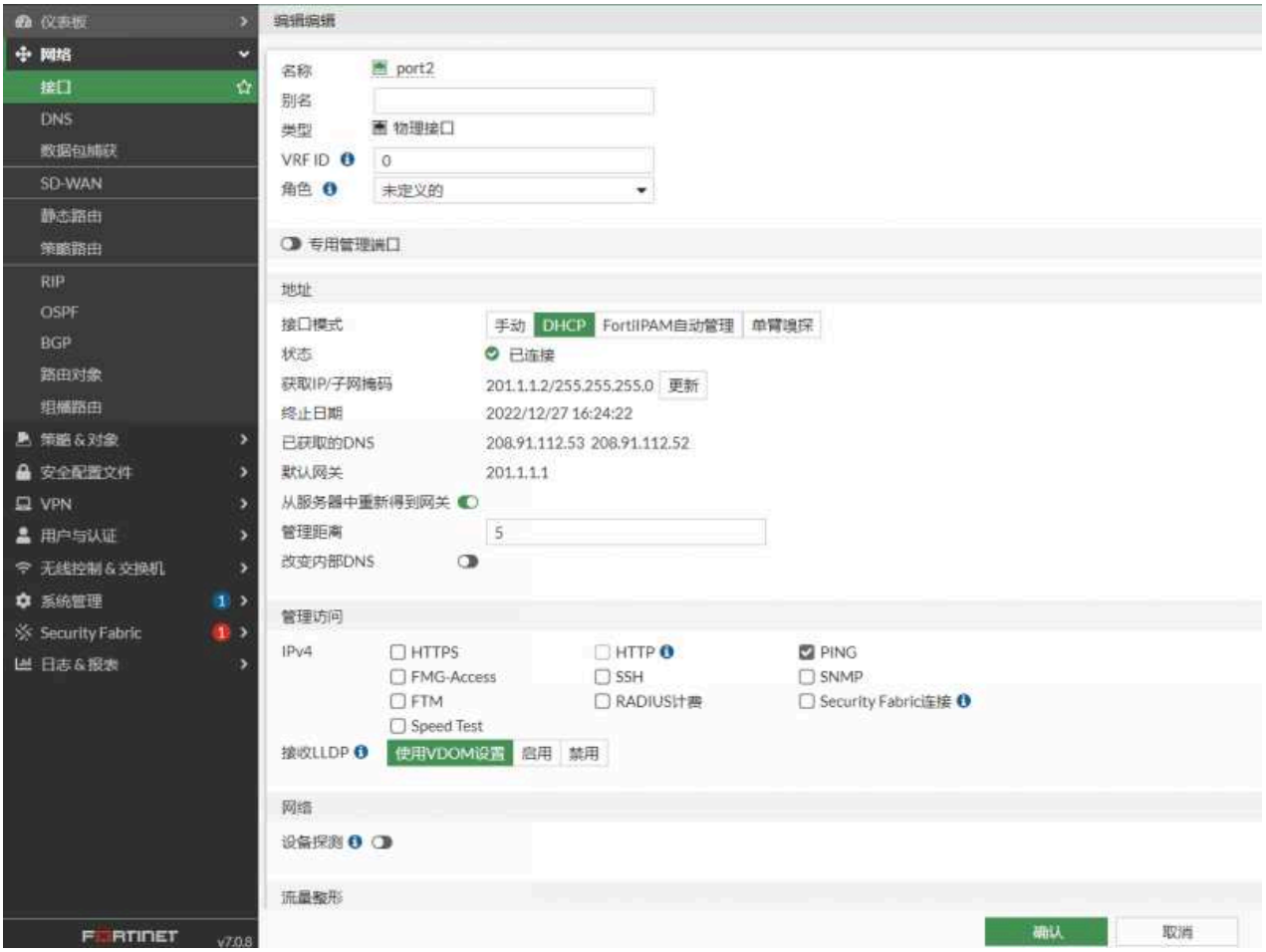
4. 配置策略

由于SPOKE1开启了自动连接，当配置策略后，就会主动与HUB协商，策略中的接口已经是绿色的，说明VPN接口已经UP。

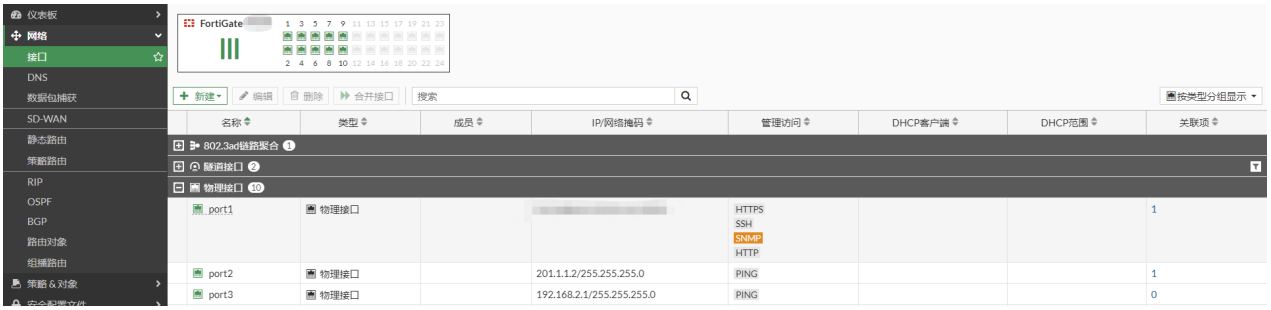


SPOKE2配置

1. 基本配置



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

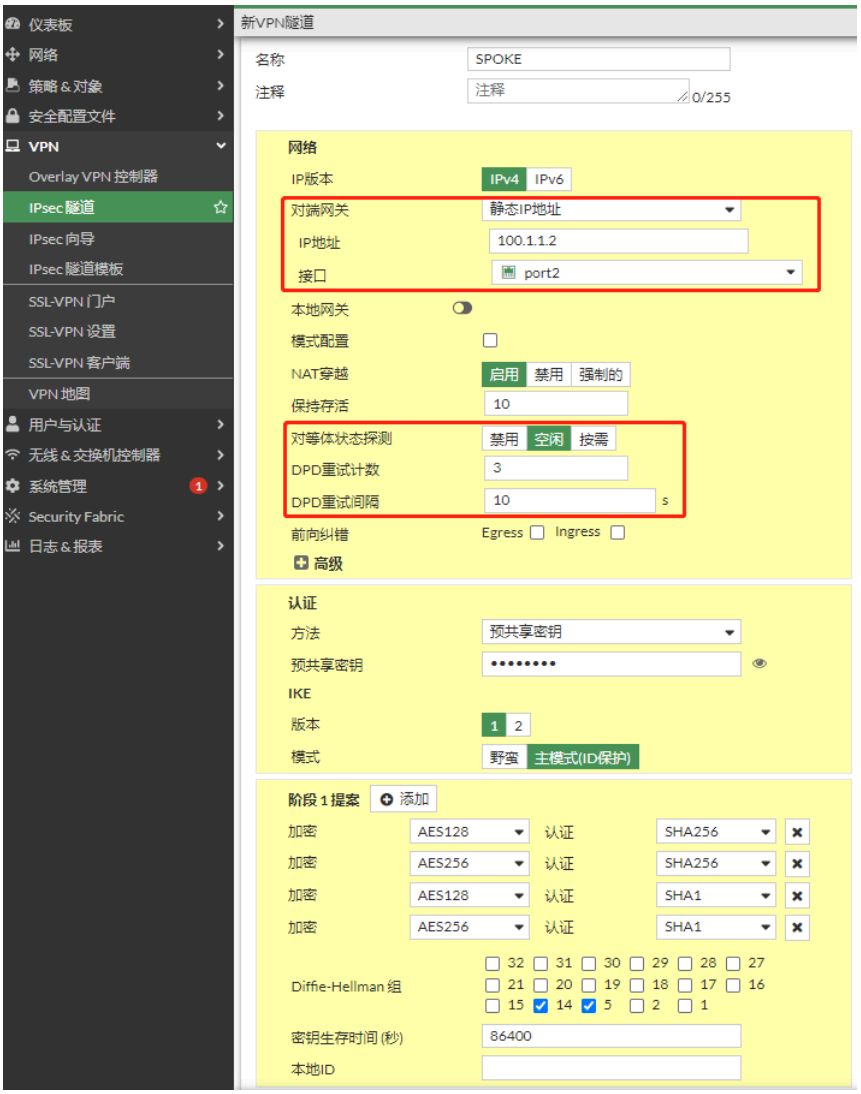


2. 配置IPSEC VPN

创建IPSEC VPN。



IPSEC VPN阶段一配置



IPSEC VPN阶段二配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

如果使用静态路由来转发Hub与Spoke之间的流量，由于Hub是被动的接受Spoke的协商，在没有协商之前Hub不知道Spoke的具体网段/感兴趣流，Hub保持默认0.0.0.0/0↔0.0.0.0/0即可，会自动学习分支的源保护网段，同时自动产生反向的去往感兴趣流的回程静态路由（一阶段开启了add-route功能），不要在Hub上手动配置去往Spoke内网的静态路由，否则会出现VPN技术→IPSec VPN→IPSec VPN排错→ Hub-Spoke静态路由问题 ↗章节的问题。

而Spoke是需要配置明细的源保护网段的，如192.168.1.0/24↔0.0.0.0/0，Hub通过add-route功能自动添加去往Spoke源保护网段（192.168.1.0/24）的静态路由。



完成VPN创建。



对应的命令行

```
config vpn ipsec phase1-interface
    edit "SPOKE2"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 100.1.1.2
        set psksecret ENC
tW+gF8+AfteBwl7HXJwMXlNTH3LGBMv0D0d1krXTNETF4/AFPUWOQvD96qoK7aQNOGOben9RUCqQ7BX2GT9lisno5ilp1zp1HlFaqkTe2l6BPL3rM1
```

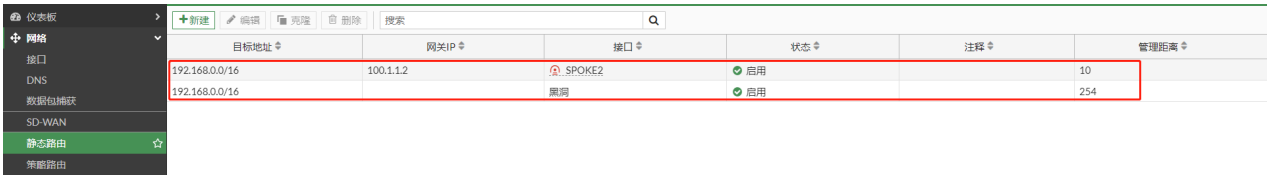

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
BLMVYF7kCW/ozSPHSXU14OIlZ+sNQioiskUhMk7RFHbkXALqDBDVMIIfM/odiP+kpHZmya3+mQDDYCjnEA3Q==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "SPOKE2"
        set phase1name "SPOKE2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 192.168.2.0 255.255.255.0
    next
end
```

3. 配置路由

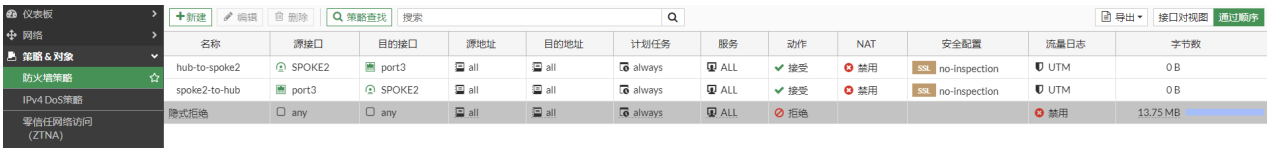
这里路由的目标是192.168.0.0/16，是HUB和其他SPOKE的业务网段汇总（分支之间没有单独建立VPN，从HUB互通）。如果只需要访问总部，则写总部的明细网段即可，即192.168.0.0/24。

管理距离为254的黑洞路由是为了VPN中断的时候防止产生错误的NAT会话。



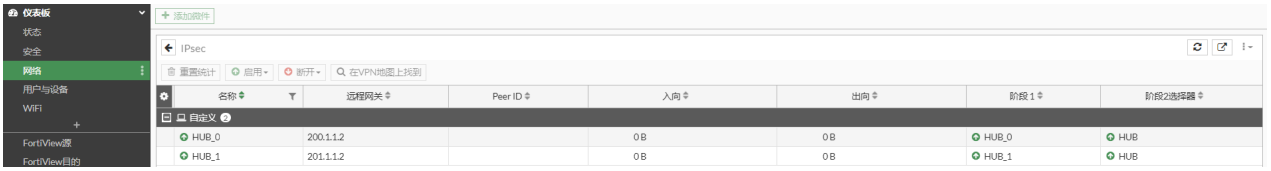
4. 配置策略

由于SPOKE2开启了自动连接，当配置策略后，就会主动与HUB协商，策略中的接口已经是绿色的，说明VPN接口已经UP。



查看VPN状态

1. HUB端VPN状态




```
# diagnose vpn  ike gateway list

vd: root/0
name: HUB_0
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 200.1.1.2/::10.0.0.38
remote_location: 0.0.0.0
network-id: 0
created: 222s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 5 9e99b894d5de25e7/f6f50471f8504b5c
  direction: responder
  status: established 222-222s ago = 0ms
  proposal: aes128-sha256
  key: 12b4b577207df3b1-72d0c8ab630bca42
  lifetime/rekey: 86400/85907
  DPD sent/recv: 00000017/00000000

vd: root/0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
name: HUB_1
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 201.1.1.2:500
tun_id: 201.1.1.2/::10.0.0.39
remote_location: 0.0.0.0
network-id: 0
created: 115s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 6 61a95053c4a2a7bc/283be8ae94d730cc
  direction: responder
  status: established 115-115s ago = 0ms
  proposal: aes128-sha256
  key: 29af7f5a8312e219-5b96fb7006b7bab6
  lifetime/rekey: 86400/86014
  DPD sent/recv: 0000000a/00000005

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=HUB_0 ver=1 serial=41 100.1.1.2:0→200.1.1.2:0 tun_id=200.1.1.2 tun_id6=::10.0.0.38 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=HUB index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=4 olast=4 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=23
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=HUB proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:192.168.1.0-192.168.1.255:0
  SA:  ref=3 options=2a6 type=00 soft=0 mtu=1438 expire=42969/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43191/43200
  dec: spi=14b71563 esp=aes key=16 8c3637326e7c38dbefc9bac5333125ca
       ah=sha1 key=20 a8fe40c940d8f4321d72ff9f0b0018c5b52d4f1e
  enc: spi=bcdbb5b1 esp=aes key=16 d24189aae387a6a13930e4998c7fc653
       ah=sha1 key=20 58cbd4a72ea1ad459c322ab483fe0c78f483c170
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=3e dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=HUB_1 ver=1 serial=42 100.1.1.2:0→201.1.1.2:0 tun_id=201.1.1.2 tun_id6=::10.0.0.39 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=HUB index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=7 olast=7 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=10
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=HUB proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:192.168.2.0-192.168.2.255:0
  SA:  ref=3 options=2a6 type=00 soft=0 mtu=1438 expire=43069/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=14b71564 esp=aes key=16 2a26ef846d7b8174388e862859ea7680
       ah=sha1 key=20 8915e7b5a2f18de14e3f239a7921653949a2c205
  enc: spi=1719f302 esp=aes key=16 1b704defe11ffdf2f26f4f2482f65eab
       ah=sha1 key=20 0b6a0e5d527eed61ca2b002ea8797b270a61eb87
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=201.1.1.2 npu_lgwy=100.1.1.2 npu_selid=3f dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=HUB ver=1 serial=3f 100.1.1.2:0→0.0.0.0:0 tun_id=10.0.0.15 tun_id6=::10.0.0.15 dst_mtu=0 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
proxyid_num=0 child_num=2 refcnt=4 ilast=44854899 olast=44854899 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=10000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

查看HUB端生成的路由

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
S       192.168.1.0/24 [15/0] via HUB tunnel 200.1.1.2, [1/0]
S       192.168.2.0/24 [15/0] via HUB tunnel 201.1.1.2, [1/0]
```

2. SPOKE1端VPN状态




```
# diagnose vpn ike gateway  list

vd: root/0
name: SPOKE1
version: 1
interface: port2 10
addr: 200.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 293s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 0 9e99b894d5de25e7/f6f50471f8504b5c
  direction: initiator
  status: established 293-293s ago = 0ms
  proposal: aes128-sha256
  key: 12b4b577207df3b1-72d0c8ab630bca42
  lifetime/rekey: 86400/85806
  DPD sent/recv: 00000000/0000001e

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=SPOKE1 ver=1 serial=17 200.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=5 olast=5 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE1 proto=0 sa=1 ref=2 serial=2 auto-negotiate
  src: 0:192.168.1.0-192.168.1.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=18227 type=00 soft=0 mtu=1438 expire=42607/0B replaywin=2048
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
      seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=bcdbb5b1 esp=aes key=16 d24189aae387a6a13930e4998c7fc653
       ah=sha1 key=20 58cbd4a72ea1ad459c322ab483fe0c78f483c170
  enc: spi=14b71563 esp=aes key=16 8c3637326e7c38dbefc9bac5333125ca
       ah=sha1 key=20 a8fe40c940d8f4321d72ff9f0b0018c5b52d4f1e
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.1.1.2 npu_lgwy=200.1.1.2 npu_selid=18 dec_npuid=0 enc_npuid=0
run_tally=0
```

查看SPOKE1端的路由

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0]
S       192.168.0.0/16 [10/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
C       192.168.1.0/24 is directly connected, port5
C       200.1.1.0/24 is directly connected, port2
```

3. SPOKE2端VPN状态




```
# diagnose vpn  ike gateway list

vd: root/0
name: SPOKE2
version: 1
interface: port2 6
addr: 201.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 302s ago
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 0 61a95053c4a2a7bc/283be8ae94d730cc
  direction: initiator
  status: established 302-302s ago = 10ms
  proposal: aes128-sha256
  key: 29af7f5a8312e219-5b96fb7006b7bab6
  lifetime/rekey: 86400/85797
  DPD sent/recv: 00000018/0000000a

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=SPOKE2 ver=1 serial=d 201.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=6 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=4 olast=4 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=24
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:192.168.2.0-192.168.2.255:0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=18203 type=00 soft=0 mtu=1438 expire=42596/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=1719f302 esp=aes key=16 1b704defe11ffdf2f26f4f2482f65eab
       ah=sha1 key=20 0b6a0e5d527eed61ca2b002ea8797b270a61eb87
  enc: spi=14b71564 esp=aes key=16 2a26ef846d7b8174388e862859ea7680
       ah=sha1 key=20 8915e7b5a2f18de14e3f239a7921653949a2c205
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.1.1.2 npu_lgwy=201.1.1.2 npu_selid=a dec_npuid=0 enc_npuid=0
run_tally=0
```

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 201.1.1.1, port2, [1/0]
S       192.168.0.0/16 [10/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected, port2
```

业务测试

1. HUB端业务测试

```
PC1# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6140132  bytes 1760274153 (1.6 GiB)
        RX errors 0  dropped 3749603  overruns 0  frame 0
        TX packets 51686  bytes 3833219 (3.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

访问SPOKE1
PC1# ping 192.168.1.10 -c 4
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=62 time=1.42 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=62 time=0.788 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=62 time=0.751 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=62 time=0.688 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.688/0.913/1.427/0.300 ms

访问SPOKE2
PC1# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=62 time=1.09 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=62 time=0.935 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=0.991 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=1.06 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.935/1.021/1.098/0.070 ms
```

2. SPOKE1端业务测试

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
PC2# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1a6c:e61:d2b9:a415  prefixlen 64  scopeid 0×20<link>
        inet6 2001::2  prefixlen 64  scopeid 0×0<global>
        ether 00:0c:29:0e:4e:c5  txqueuelen 1000  (Ethernet)
        RX packets 5904889  bytes 459674552 (438.3 MiB)
        RX errors 0  dropped 58  overruns 0  frame 0
        TX packets 3224540  bytes 205411564402 (191.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

访问HUB
PC2# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.746 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.765 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.862 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=0.677 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.677/0.762/0.862/0.071 ms

访问SPOKE2
PC2# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=61 time=1.14 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=61 time=0.952 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=61 time=1.51 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=61 time=0.886 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.886/1.124/1.519/0.248 ms
```

3. SPOKE2端业务测试

```
PC3# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.10  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::2652:4dd7:5d0e:941d  prefixlen 64  scopeid 0×20<link>
        inet6 240e:604:109:39::216  prefixlen 64  scopeid 0×0<global>
        ether 00:0c:29:37:f0:ac  txqueuelen 1000  (Ethernet)
        RX packets 9638867  bytes 205844622412 (191.7 GiB)
        RX errors 0  dropped 118  overruns 0  frame 0
        TX packets 5737914  bytes 378901312 (361.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

访问HUB
PC2# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.848 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.935 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.899 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=1.04 ms
--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.848/0.931/1.045/0.081 ms

访问SPOKE1
PC3# ping 192.168.1.10 -c 4
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=61 time=1.13 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=61 time=1.22 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=61 time=1.21 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=61 time=1.04 ms
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.043/1.151/1.220/0.075 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

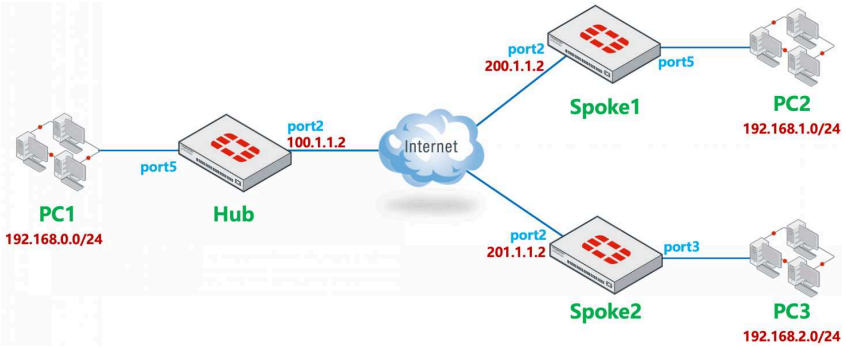
拨号VPN运行动态路由

网络需求

某公司总部内部有一台OA服务器，其余分2个支机构都需要通过vpn拨入总部内网对OA服务器进行访问，为了方便配置，总部不想有太多的配置，总部只建立一条vpn隧道，实现所有分支机构和总部的通讯。同时需要运行动态路由协议将总部和分支的路由全部打通，SPOKE之间的流量通过HUB进行中转。

网络拓扑

HUB and SPOKE通过动态路由学习到整网的业务网段路由，SPOKE之间相互的流量通过HUB进行中转。



VPN Tunnel IP地址分配，以及BGP的规划：

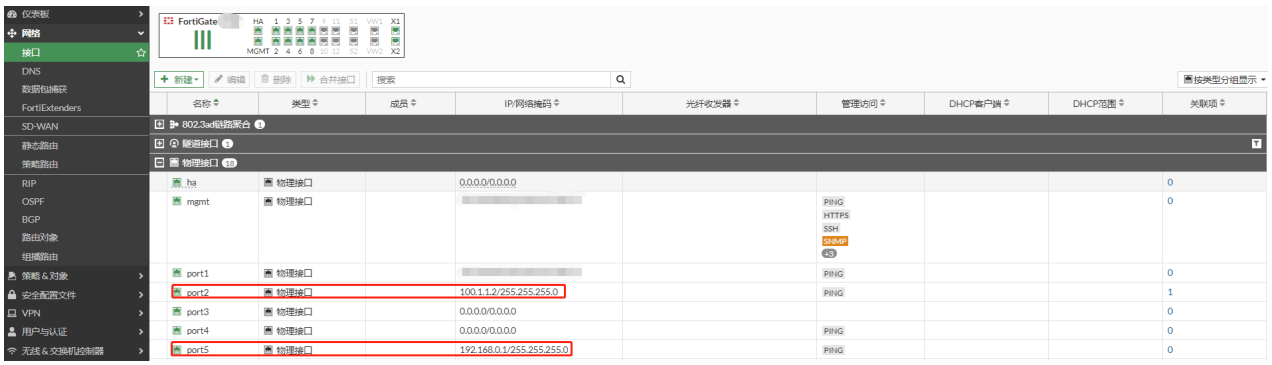
角色	公网IP	私网网段	VPN隧道IP	BGP信息
HUB	100.1.1.2	192.168.0.1/24	10.10.10.1	AS 65001 RR
SPOKE1	200.1.1.2	192.168.1.1/24	10.10.10.2	AS 65001 RR Client
SPOKE2	201.1.1.2	192.168.2.1/24	10.10.10.3	AS 65001 RR Client
SPOKE3	...	...	...	...
SPOKEX	...	...	...	...

配置步骤

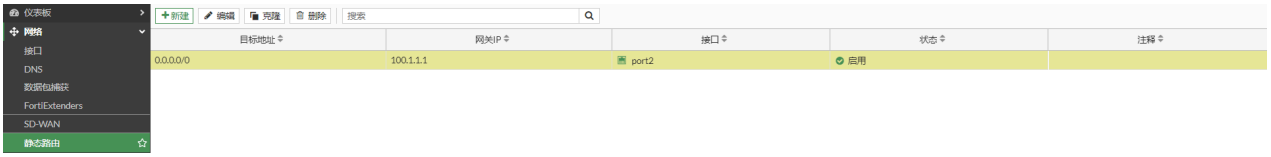
HUB端配置

1. **基本配置**

配置接口IP和路由



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



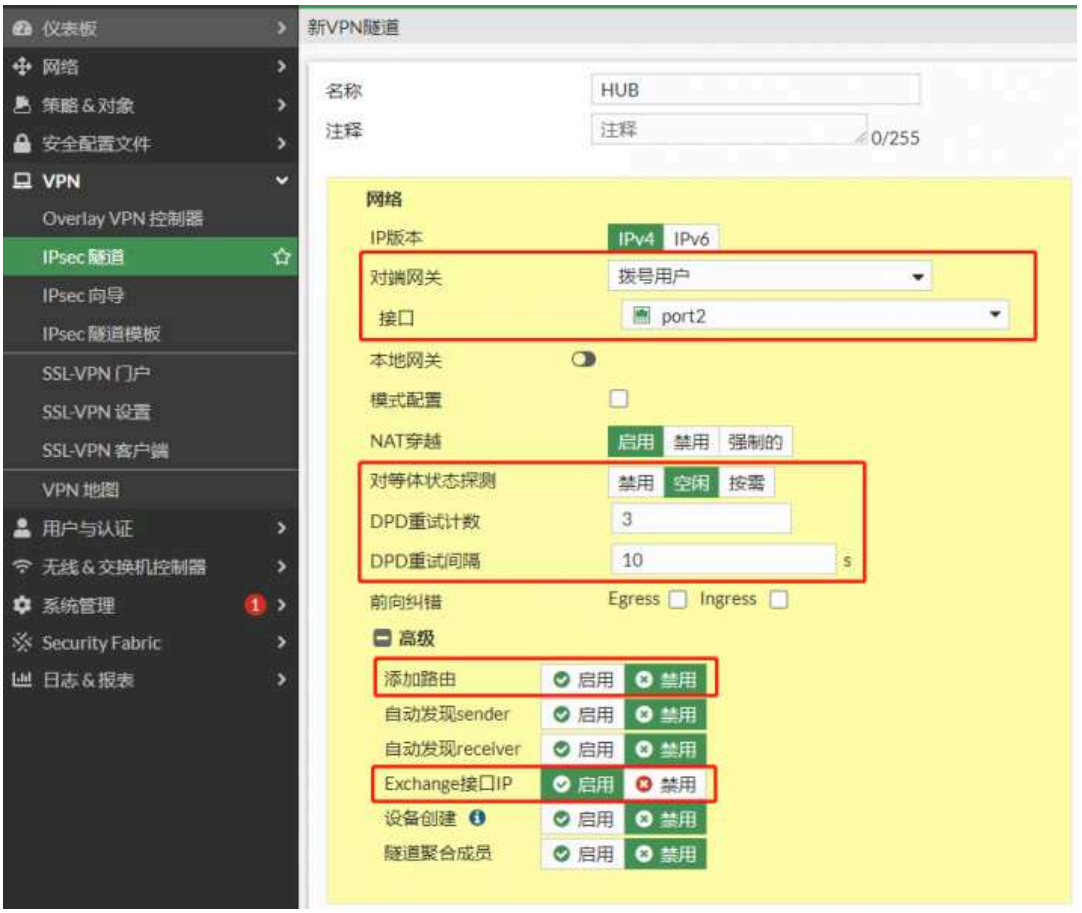
2. 配置IPSEC VPN

创建IPSEC VPN。

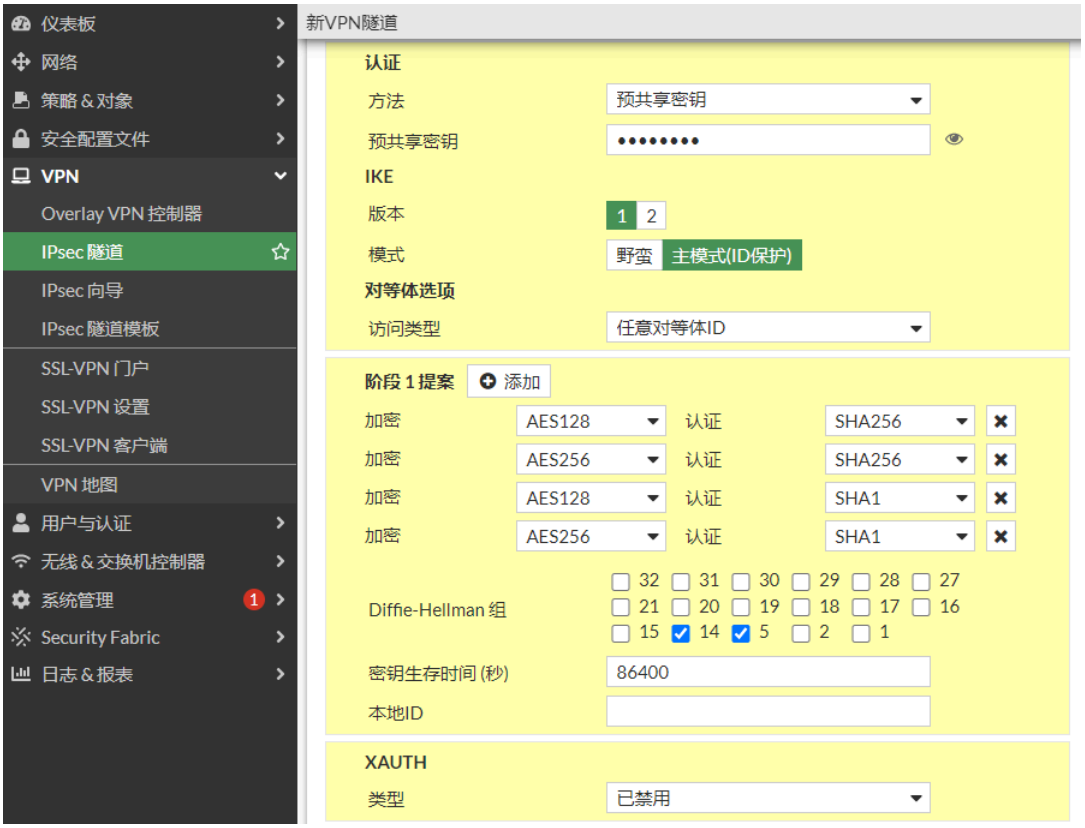


IPSEC VPN阶段一配置。

由于HUB和SPOKE之间是通过动态路由学习，因此“添加路由”选项禁用，不用HUB自动学习SPOKE的路由；Exchange接口IP打开，需要交换HUB和SPOKE之间VPN接口的IP。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



IPSEC VPN阶段二配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



创建完成。



对应的命令行

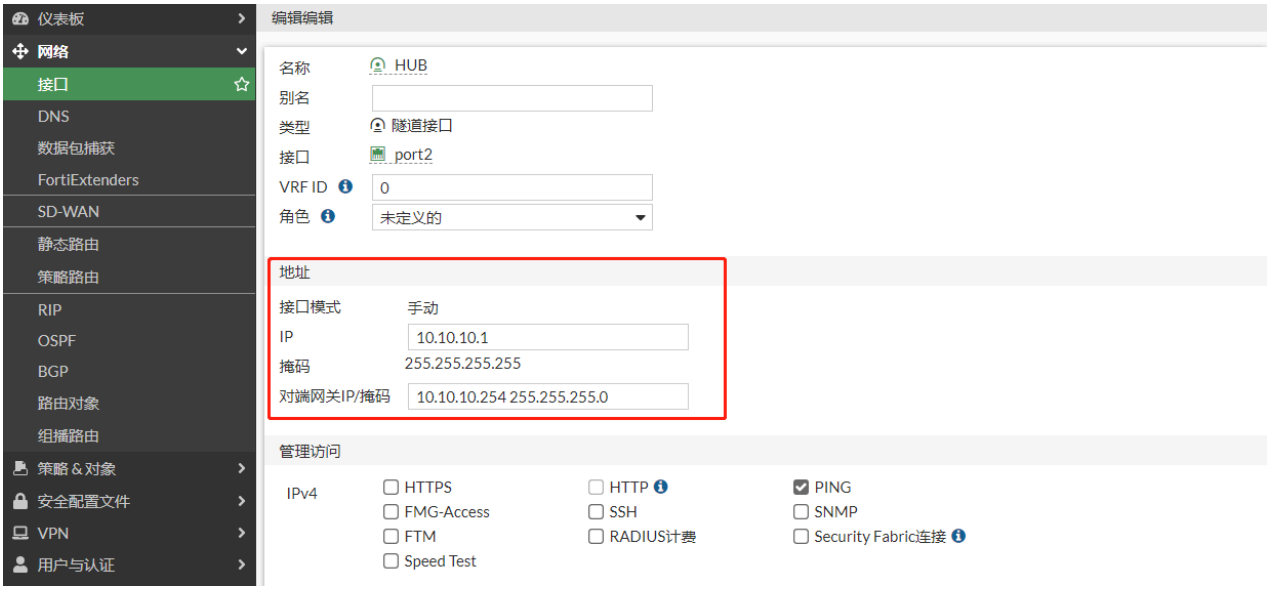
```
config vpn ipsec phase1-interface
    edit "HUB"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set psksecret ENC
m9c6Qk4uhwWLRTRDI2EzYQym02Uma0709h07KB2pmS0Ek+8ZUOpRTH6OZdFEZPdlZktXajf/KRkR6SNO7UwW27pYAWoRygwcWhvJrO67tIWl5AksoO
X3uy2YTjFX+kVbrw5WTVoLogqtJ4yPk7coZpMKUvqJkAv8flqIIi3EfY4TgY2avzSOkBVm8ZLgokTkmt3PMQ==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "HUB"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
21          set phase1name "HUB"
            set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
            set keepalive enable
        next
    end
```

3. 配置VPN接口IP

HUB端的”对端网关IP“ 10.10.10.254是不被Spoke所使用的预留IP，IPsec Tunnel是一个点对点的隧道，但是ADVPN中这条隧道需要同时对应多个SPOKE，因此不能将Remote IP写成一个存在的SPOKE端IP。



4. 配置策略

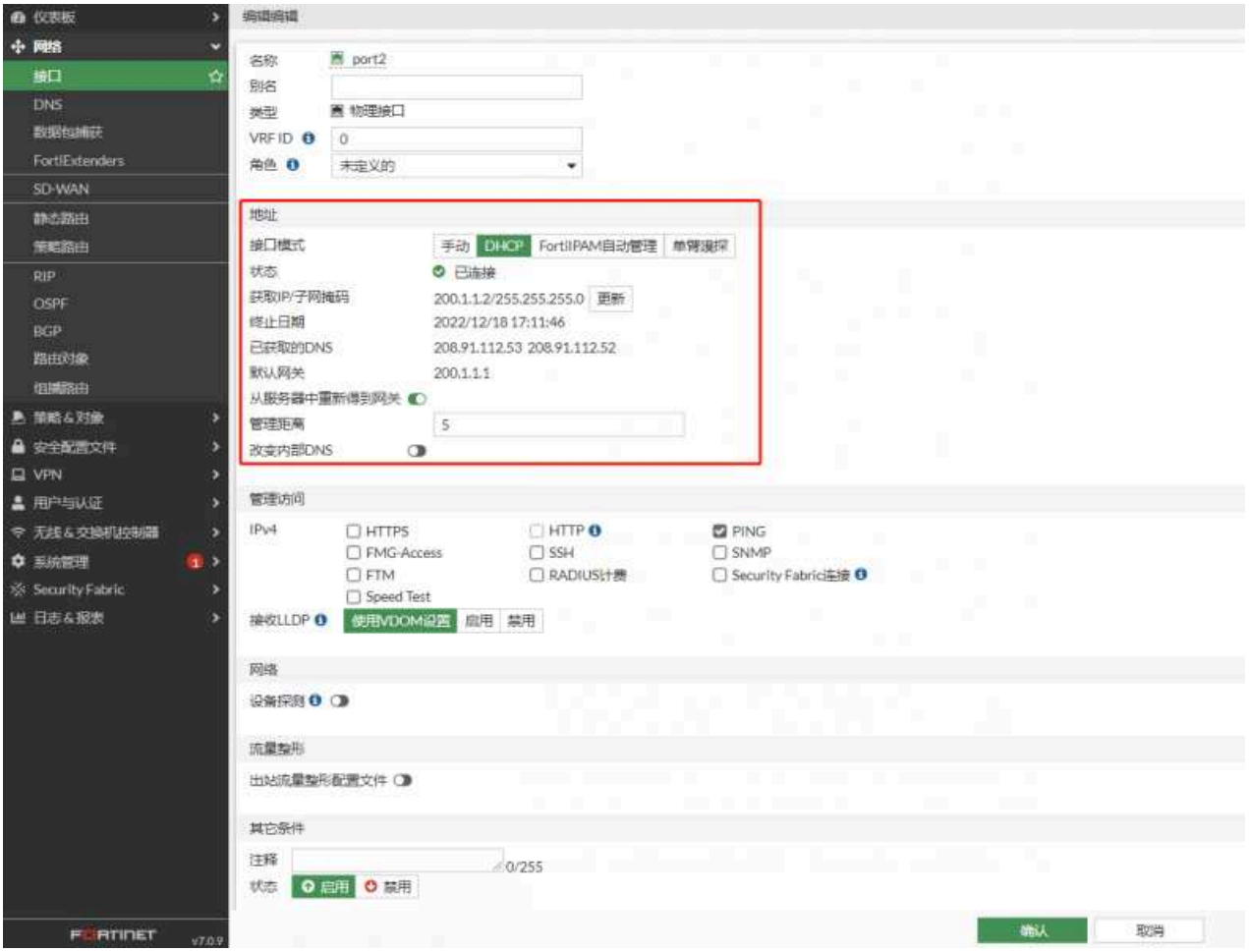
创建3条策略，从上到下分别是：分支到总部的放通策略；总部到分支的放通策略；分支到分支的放通策略。

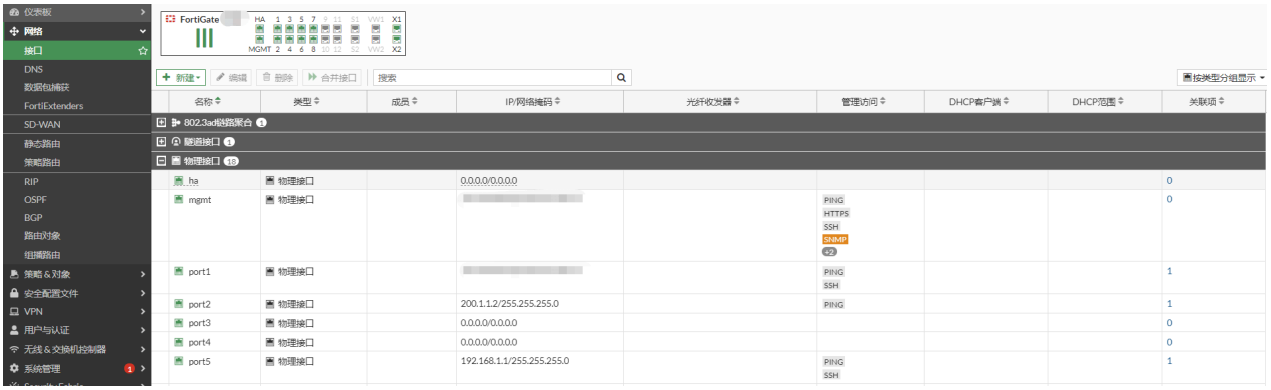


SPOKE1配置

1. 基本配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 配置IPSEC VPN

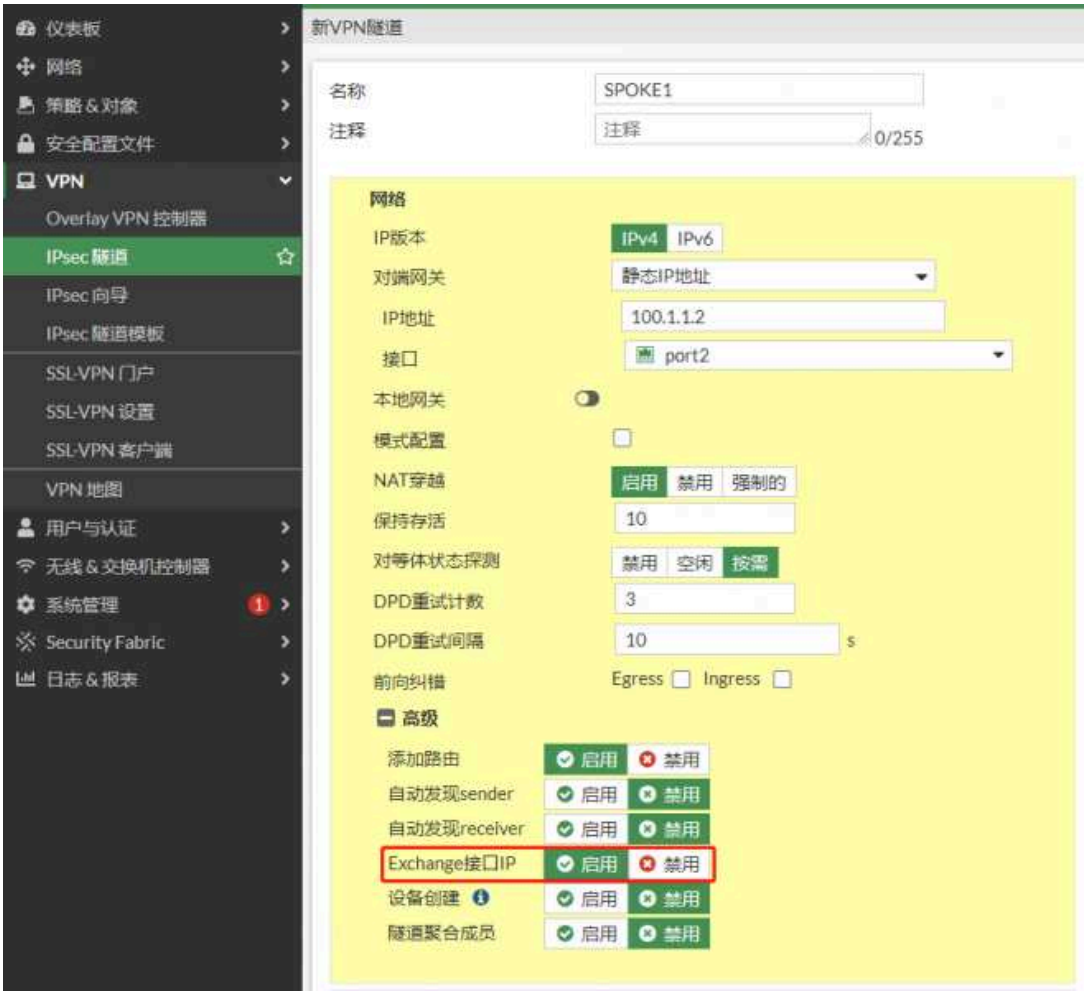
创建IPSEC VPN。

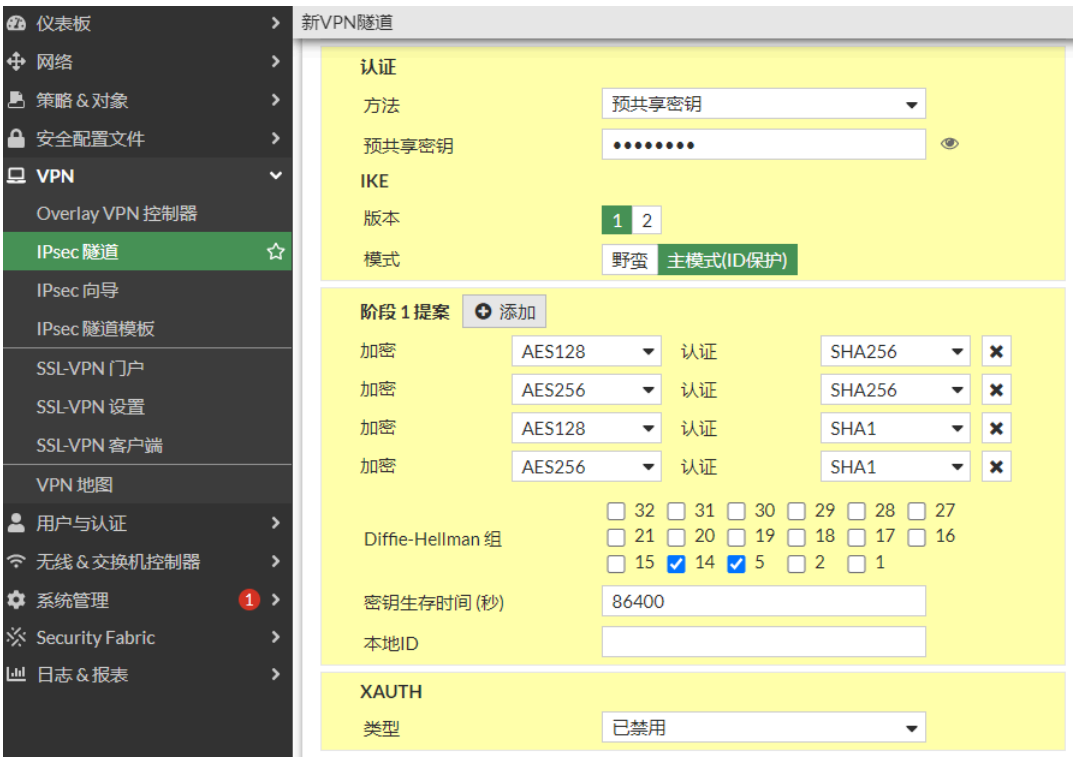


IPSEC VPN阶段一配置。

由于HUB和SPOKE之间是通过动态路由学习，因此Exchange接口IP打开，需要交换HUB和SPOKE之间VPN接口的IP；SPOKE1是静态IPSEC，所以“添加路由”选项对SPOKE1没有意义，不用关注。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

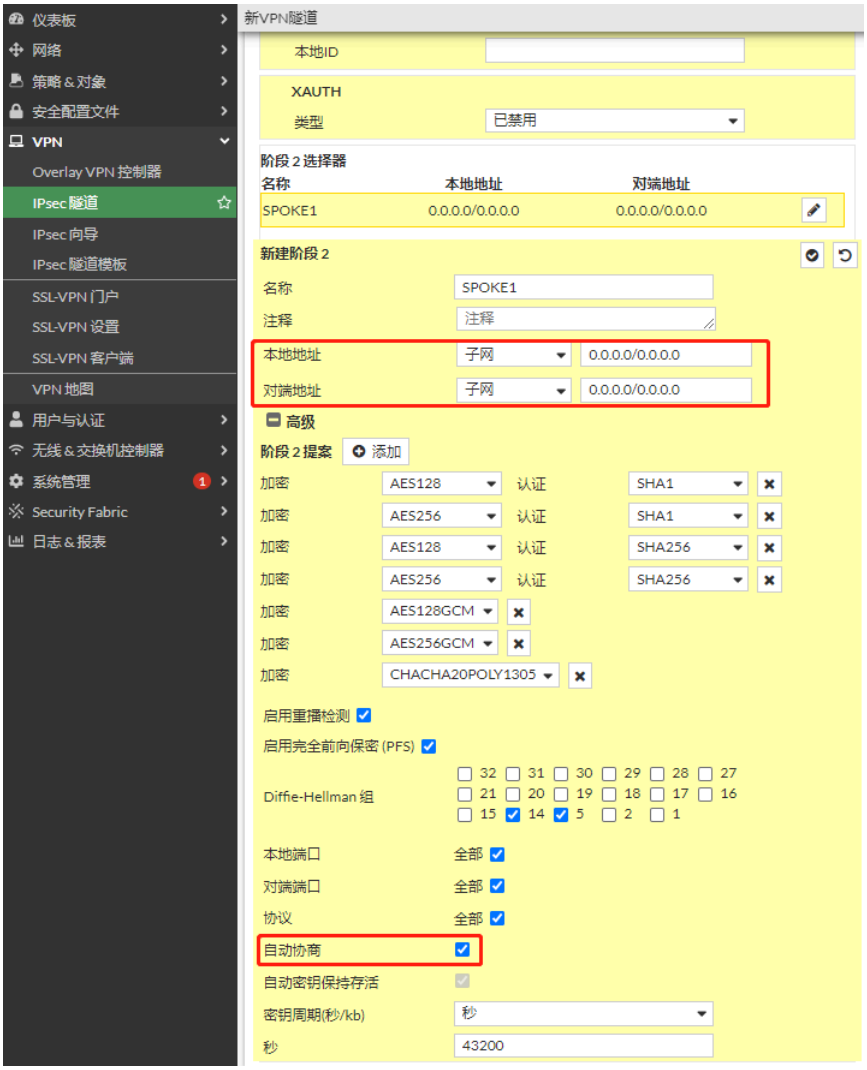




IPSEC VPN阶段二配置。

第二阶段感兴趣流配置为0.0.0.0/0.0.0.0，后续通过动态路由将流量指向VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建完成。



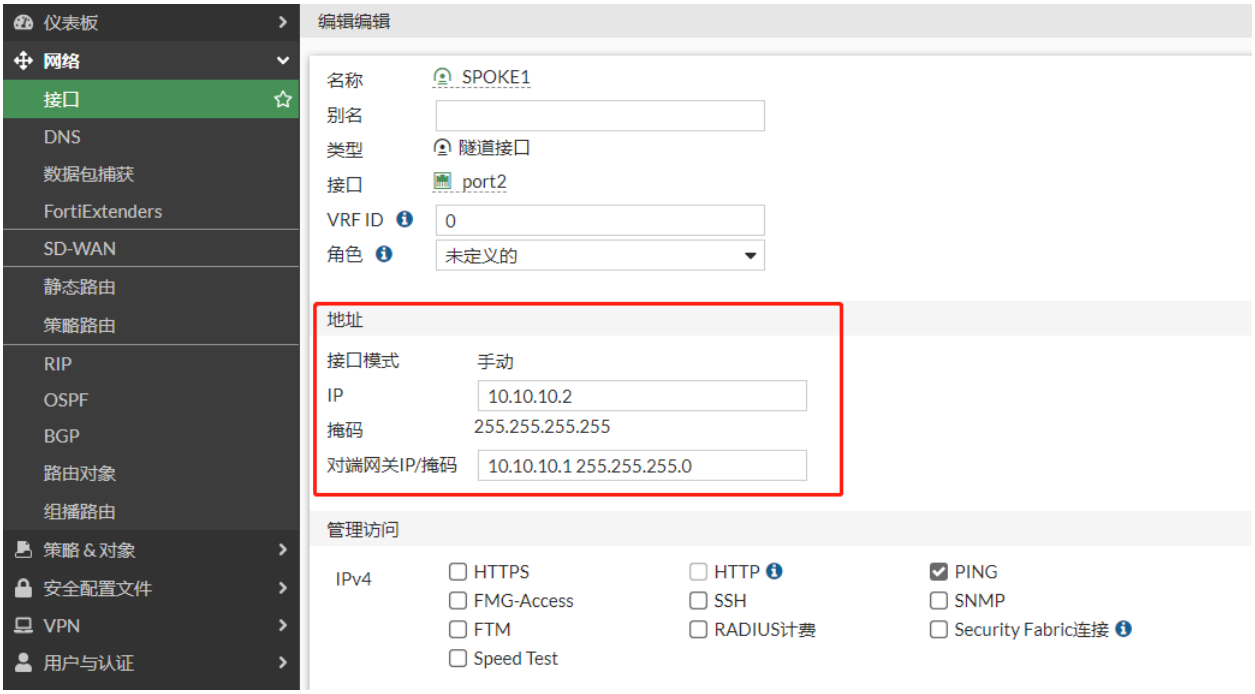
对应的命令行

```
config vpn ipsec phase1-interface
    edit "SPOKE1"
        set interface "port2"
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 100.1.1.2
        set psksecret ENC
SasMccP3qWqglxEV1I2Z8ESNcmdXyPqkxyIoMpEM3haEKdLyi6qcOoc9WtdukEH2zXuV/bcVW6HyYqi8rh+KZ533z7cH6zqNpXCrOicxBYDXrEPVU6
NXtp4UgL+bqiG6Vm1FzA62V+YN4RfchkuK49CuipVrer1xFqqIgXQVxM5GVuq+5wFvtWf5VBeuFbw+GHJlPQ==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "SPOKE1"
        set phase1name "SPOKE1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

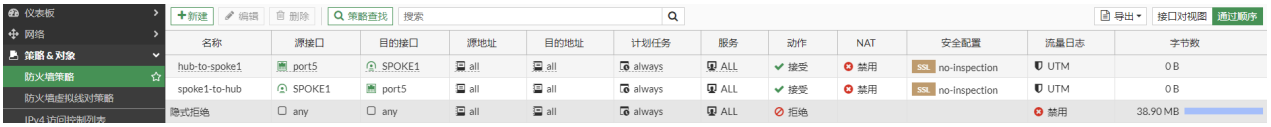
3. 配置VPN接口IP

SPOKE1的“对端网关IP”是指向HUB的。



4. 配置策略

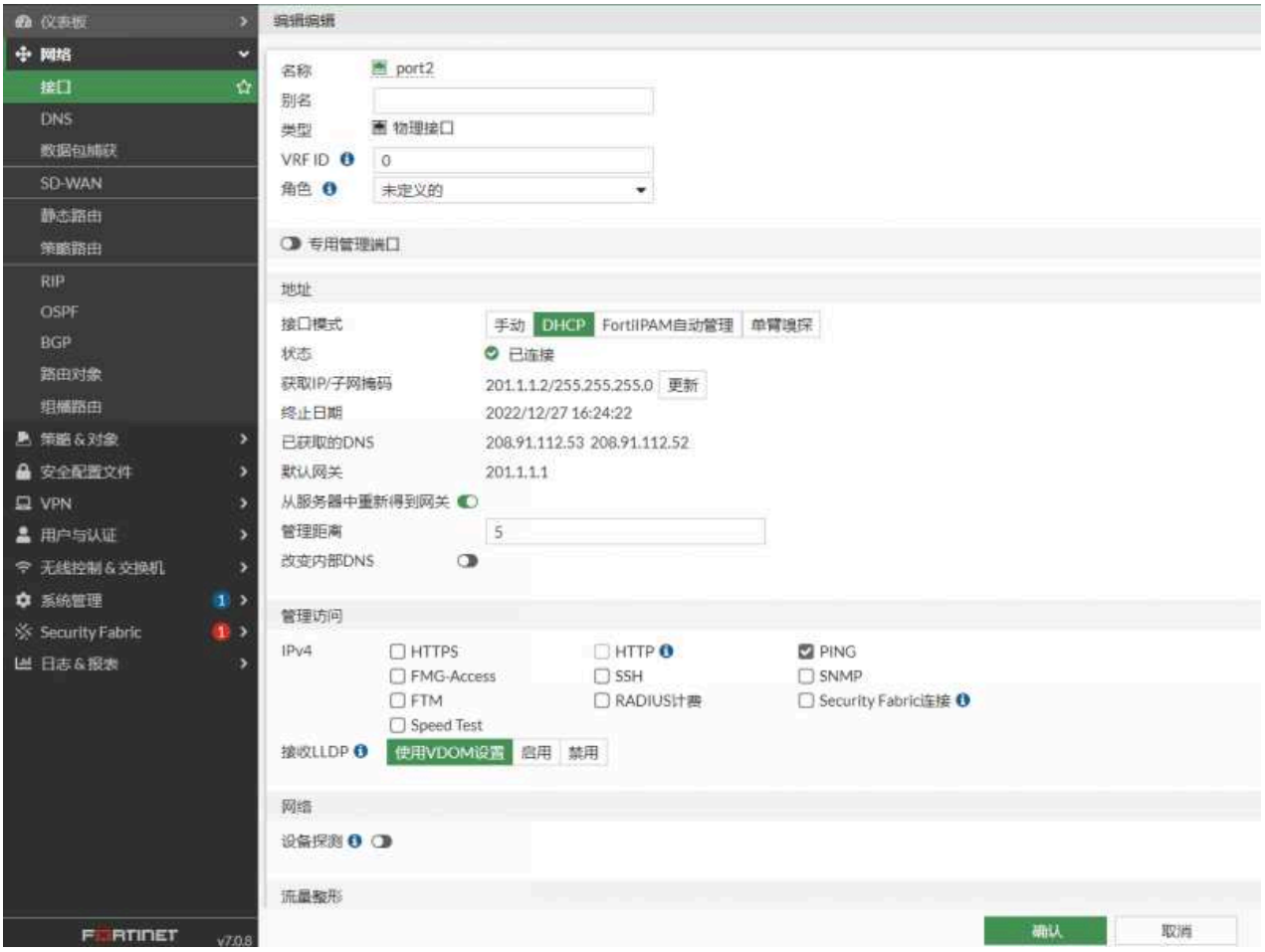
由于SPOKE1开启了自动连接，当配置策略后，就会主动与HUB协商，策略中的接口已经是绿色的，说明VPN接口已经UP。

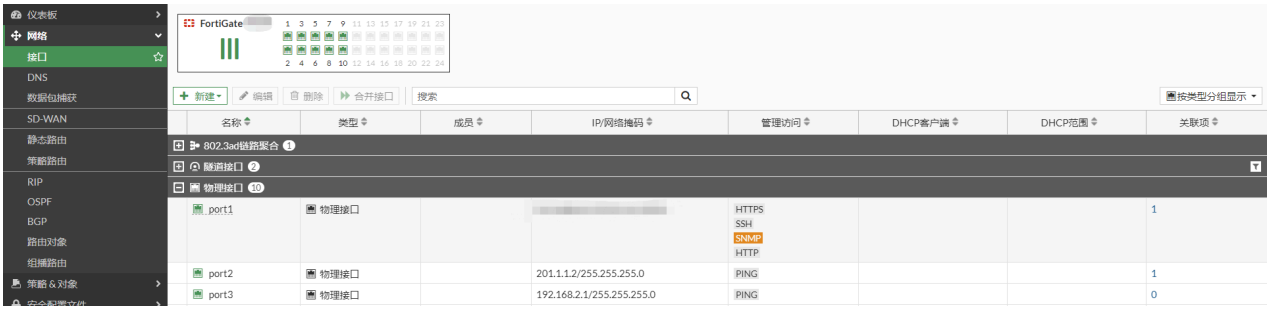


SPOKE2配置

1. 基本配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. **配置IPSEC VPN**

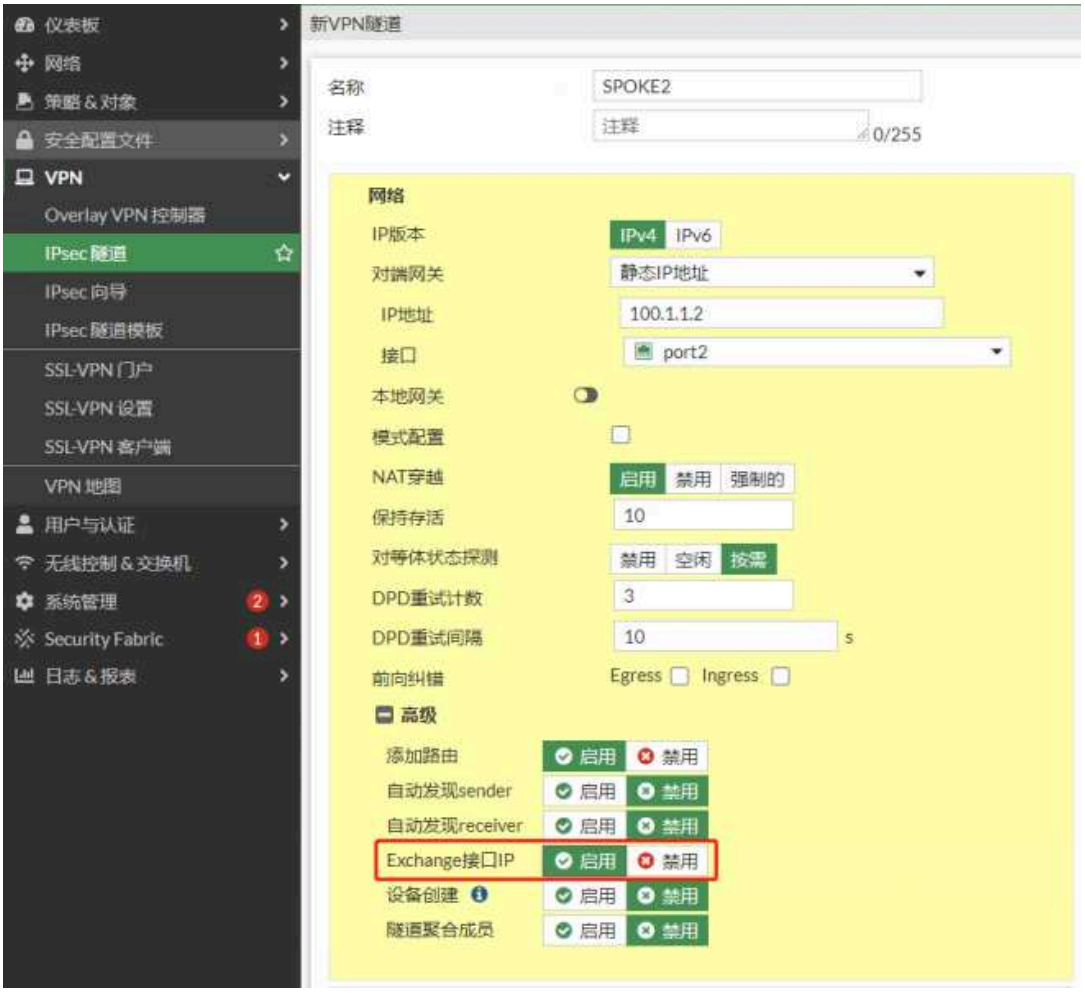
创建IPSEC VPN。

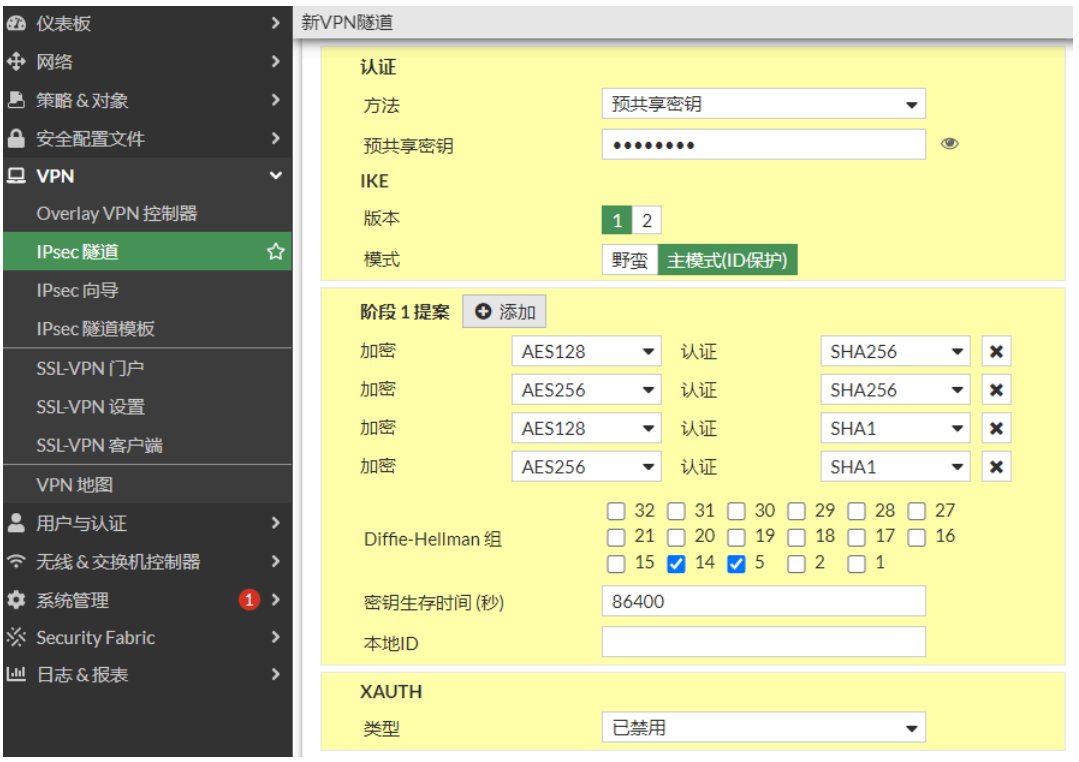


IPSEC VPN阶段一配置。

由于HUB和SPOKE之间是通过动态路由学习，因此Exchange接口IP打开，需要交换HUB和SPOKE之间VPN接口的IP；SPOKE2是静态IPSEC，所以“添加路由”选项对SPOKE2没有意义，不用关注。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

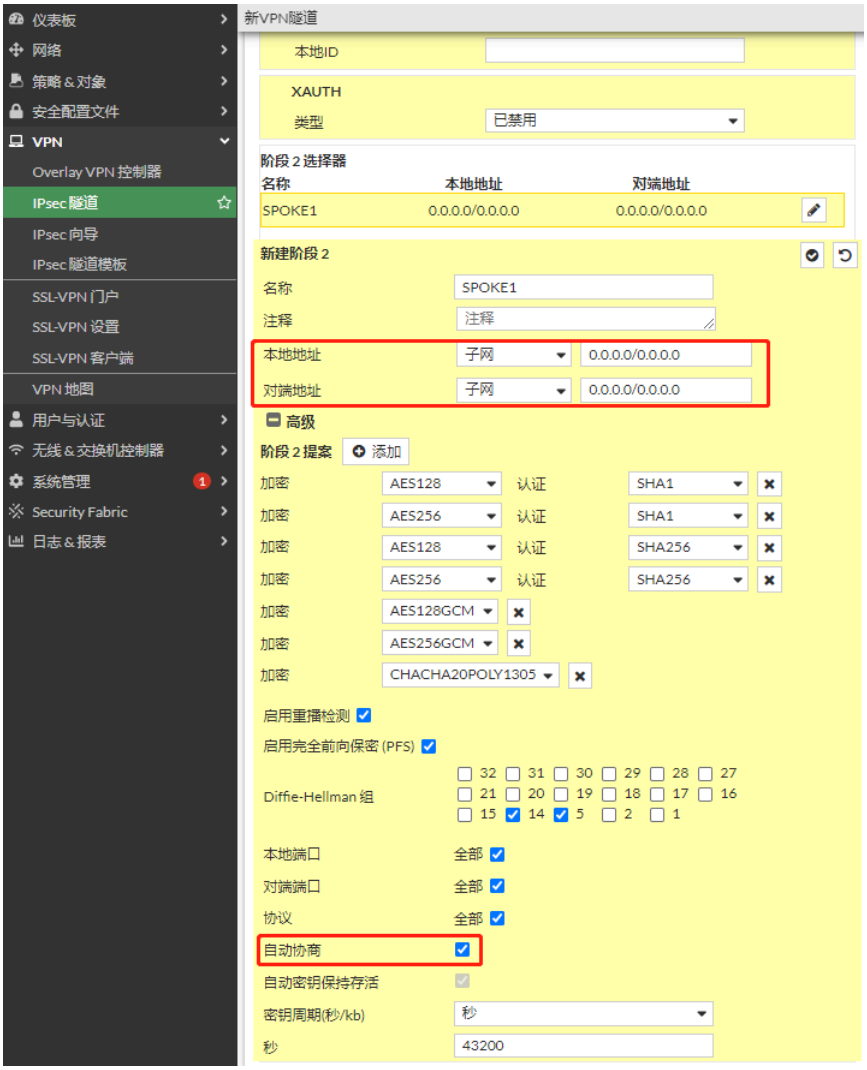




IPSEC VPN阶段二配置。

第二阶段感兴趣流配置为0.0.0.0/0.0.0.0，后续通过动态路由将流量指向VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建完成。



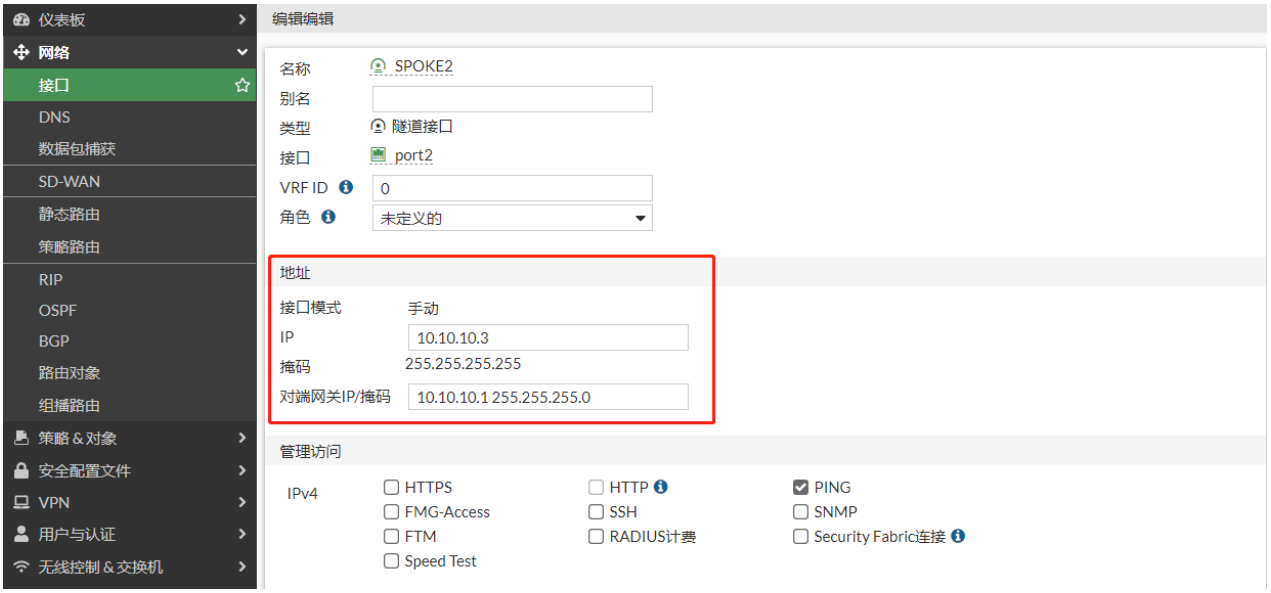
对应的命令行

```
config vpn ipsec phase1-interface
    edit "SPOKE2"
        set interface "port2"
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set remote-gw 100.1.1.2
        set psksecret ENC
H3nAayIN5AWs3FomZpZri+tl6IAqg3iVu66h3qNXTjw1oSkiHauyAa/IUNw4xeJxD5dmiLfcAd/zzDb6BVai19ekg0Qvejqy39Mxr9UaRniPKE4dvo
aoVLWy4OvamxRzf82+JAUYKlF0NvVlMQ/+0JUYOunFeUlLLtht4dW69X9VTXfEBdwav496AzfYgI4gRTFFSg==
        set dpd-retryinterval 10
    next
end
config vpn ipsec phase2-interface
    edit "SPOKE2"
        set phase1name "SPOKE2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

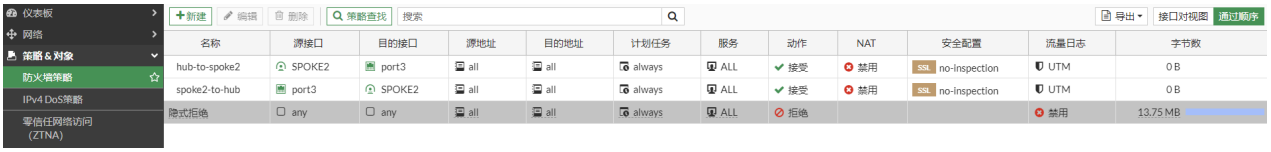
3. 配置VPN接口IP

SPOKE2的“对端网关IP”是指向HUB的。



4. 配置策略

由于SPOKE2开启了自动连接，当配置策略后，就会主动与HUB协商，策略中的接口已经是绿色的，说明VPN接口已经UP。



查看VPN状态和路由表

1. HUB端VPN状态和路由表




```
# diagnose vpn ike gateway  list

vd: root/0
name: HUB_0
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 200.1.1.2/::10.0.0.4
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.1 → 0.0.0.0
created: 33s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 2 b114b317daa486b7/29ede80ef4398500
  direction: responder
  status: established 33-33s ago = 0ms
  proposal: aes128-sha256
  key: 770b2cdeba34d096-8edcf542d0c07ef5
  lifetime/rekey: 86400/86096
  DPD sent/recv: 00000004/00000000

vd: root/0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
name: HUB_1
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 201.1.1.2:500
tun_id: 201.1.1.2/::10.0.0.5
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.1 → 0.0.0.0
created: 22s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 3 a0d49273057cb2d8/146f94f98305de8d
  direction: responder
  status: established 22-22s ago = 0ms
  proposal: aes128-sha256
  key: 4dc2b68b5795fd1c-0a400a810f439a19
  lifetime/rekey: 86400/86107
  DPD sent/recv: 00000000/00000008

FGT-wangxiang-used # diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=HUB_0 ver=1 serial=4 100.1.1.2:0→200.1.1.2:0 tun_id=200.1.1.2 tun_id6=::10.0.0.4 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=HUB index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=5 olast=5 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=HUB proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=226 type=00 soft=0 mtu=1438 expire=43155/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43191/43200
  dec: spi=d87e91b4 esp=aes key=16 f598636b2f6feb532e32f883300f4595
       ah=sha1 key=20 663bcb60b48c072daebdc011e27c35836e2f45eb
  enc: spi=d56f5619 esp=aes key=16 f3059875bf7c1915eb711a5355a603a8
       ah=sha1 key=20 f8d348a6abdb169781f2e1b3aae099c70d16ea92
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=2 dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=HUB_1 ver=1 serial=5 100.1.1.2:0→201.1.1.2:0 tun_id=201.1.1.2 tun_id6=::10.0.0.5 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=HUB index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=4 olast=4 ad=/0
stat: rxp=1 txp=0 rxb=60 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=2
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=HUB proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=4 options=226 type=00 soft=0 mtu=1438 expire=43162/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=d87e91b5 esp=aes key=16 f7229ae8b4fe965ea7346f41ffae201a
       ah=sha1 key=20 8ada15a3ef8a71fdb3037ee1f7014ca930009cdb
  enc: spi=c7b86106 esp=aes key=16 a6346a22cf40fba236f0cfaacc720261
       ah=sha1 key=20 e093aed38364b32892da5ae4f99413be54a7c635
  dec:pkts/bytes=2/120, enc:pkts/bytes=0/0
  npu_flag=02 npu_rgwy=201.1.1.2 npu_lgwy=100.1.1.2 npu_selid=3 dec_npuid=1 enc_npuid=0
------------------------------------------------------
name=HUB ver=1 serial=1 100.1.1.2:0→0.0.0.0:0 tun_id=10.0.0.1 tun_id6=::10.0.0.1 dst_mtu=0 dpd-link=on weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
proxyid_num=0 child_num=2 refcnt=4 ilast=42949600 olast=42949600 ad=/0
stat: rxp=3 txp=0 rxb=180 txb=0
dpd: mode=on-idle on=0 idle=10000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

查看路由表

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       10.10.10.0/24 is directly connected, HUB
C       10.10.10.1/32 is directly connected, HUB
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
```

从HUB端分别ping SPOKE1和SPOKE2的隧道接口地址。

```
# execute ping-options source 10.10.10.1
# execute ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2): 56 data bytes
64 bytes from 10.10.10.2: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 10.10.10.2: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=255 time=0.3 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=255 time=0.4 ms

--- 10.10.10.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.4/0.7 ms

# execute ping 10.10.10.3
PING 10.10.10.3 (10.10.10.3): 56 data bytes
64 bytes from 10.10.10.3: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 10.10.10.3: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.10.10.3: icmp_seq=2 ttl=255 time=0.4 ms
64 bytes from 10.10.10.3: icmp_seq=3 ttl=255 time=0.5 ms
64 bytes from 10.10.10.3: icmp_seq=4 ttl=255 time=0.2 ms

--- 10.10.10.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.5 ms
```

2. **SPOKE1端VPN状态**




```
# diagnose vpn  ike gateway  list

vd: root/0
name: SPOKE1
version: 1
interface: port2 10
addr: 200.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.2 → 10.10.10.1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
created: 139s ago
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 0 33b5335c7174437e/c89906c6196f3cd7
  direction: initiator
  status: established 139-139s ago = 0ms
  proposal: aes128-sha256
  key: ad3e41d87eb3b8b8-c97c621b25fe9a48
  lifetime/rekey: 86400/85960
  DPD sent/recv: 00000004/0000000a

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=SPOKE1 ver=1 serial=1 200.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=12 olast=12 ad=/0
stat: rxp=0 txp=6 rxb=0 txb=360
dpd: mode=on-demand on=1 idle=10000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE1 proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=5 options=18227 type=00 soft=0 mtu=1438 expire=42762/0B replaywin=2048
       seqno=7 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=1a45fdb4 esp=aes key=16 373c729e4164750638f8ff0d37dbdd12
       ah=sha1 key=20 323ffd35fb089657505202639ad92371df146881
  enc: spi=a7d1cc77 esp=aes key=16 6da00eca8e15572377040c982e206526
       ah=sha1 key=20 3ea0959e65417277e75bdc5f52bdbc768f33d9b0
  dec:pkts/bytes=0/0, enc:pkts/bytes=12/1080
  npu_flag=01 npu_rgwy=100.1.1.2 npu_lgwy=200.1.1.2 npu_selid=0 dec_npuid=0 enc_npuid=1
run_tally=0
```

查看路由表

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0]
S       10.10.10.0/24 [5/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
C       10.10.10.2/32 is directly connected, SPOKE1
C       192.168.1.0/24 is directly connected, port5
C       200.1.1.0/24 is directly connected, port2
```

从SPOKE1端ping HUB的隧道地址。

```
# execute ping-options source 10.10.10.2
# execute ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.4 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.6 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=0.4 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=0.6 ms

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.7 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. SPOKE2端VPN状态




```
# diagnose vpn ike gateway list

vd: root/0
name: SPOKE2
version: 1
interface: port2 6
addr: 201.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.3 → 10.10.10.1
created: 166s ago
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 0 712a042d8d25877d/437eb372be68f67e
  direction: initiator
  status: established 166-166s ago = 10ms
  proposal: aes128-sha256
  key: 48fb4b35b9a67aa3-f2f62d8949523c2d
  lifetime/rekey: 86400/85933
  DPD sent/recv: 0000000f/00000004

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=SPOKE2 ver=1 serial=1 201.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=6 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=8 olast=8 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=15
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=18203 type=00 soft=0 mtu=1438 expire=42730/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42899/43200
  dec: spi=99b97fa0 esp=aes key=16 6da0cd14244e96c9224fdfc526104c88
       ah=sha1 key=20 c15decb70b3de9678d1313b564ec2e6e912b9540
  enc: spi=a7d1cc78 esp=aes key=16 023a05cc8cd9224c781ca640b044c5b3
       ah=sha1 key=20 96da3fa1c8207a267200aac94db3718944574a1b
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.1.1.2 npu_lgwy=201.1.1.2 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

查看路由表

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 201.1.1.1, port2, [1/0]

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
S       10.10.10.0/24 [5/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
C       10.10.10.3/32 is directly connected, SPOKE2
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected, port2
```

从SPOKE2端ping HUB隧道接口地址。

```
# execute ping-options source 10.10.10.3
# execute ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=255 time=0.6 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=255 time=0.6 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=255 time=0.6 ms
64 bytes from 10.10.10.1: icmp_seq=4 ttl=255 time=0.4 ms

--- 10.10.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.6 ms
```

配置动态路由

1. HUB端BGP配置

利用BGP neighbor-group特性，只要匹配前缀列表10.10.10.0/24的BGP-Peer均可以和HUB建立BGP邻居。

将邻居设置为Route-Reflector-Client，自己即为路由反射器（Route-Reflector）,通过路由反射器原理实时同步整网路由。

```
config router bgp
    set as 65001
    set router-id 100.1.1.2
    config neighbor-group
        edit "group1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set interface "HUB"
            set remote-as 65001
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "group1"
        next
    end
    config network
        edit 1
            set prefix 192.168.0.0 255.255.255.0
        next
    end
end
```

2. SPOKE1端BGP配置

与HUB端建立BGP邻居

```
config router bgp
    set as 65001
    set router-id 200.1.1.2
    config neighbor
        edit "10.10.10.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set interface "SPOKE1"
            set remote-as 65001
        next
    end
    config network
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```

3. SPOKE2端BGP配置

与HUB端建立BGP邻居

```
config router bgp
    set as 65001
    set router-id 201.1.1.2
    config neighbor
        edit "10.10.10.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set interface "SPOKE2"
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
    config network6
        edit 1
            set prefix6 ::/128
        next
    end
end
```

查看路由表

1. HUB端路由表

```
FGT-wangxiang-used # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       10.10.10.0/24 is directly connected, HUB
C       10.10.10.1/32 is directly connected, HUB
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
B       192.168.1.0/24 [200/0] via 10.10.10.2 (recursive is directly connected, HUB), 00:21:21
B       192.168.2.0/24 [200/0] via 10.10.10.3 (recursive is directly connected, HUB), 00:21:21
```

2. SPOKE1端路由表

```
FGT-wangxiang-used # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0]
S       10.10.10.0/24 [5/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE1 tunnel 100.1.1.2, [1/0]

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
C       10.10.10.2/32 is directly connected, SPOKE1
C       200.1.1.0/24 is directly connected, port2
C       192.168.1.0/24 is directly connected, port5
B       192.168.0.0/24 [200/0] via 10.10.10.1 (recursive via SPOKE1 tunnel 100.1.1.2), 00:21:41
B       192.168.2.0/24 [200/0] via 10.10.10.3 (recursive via SPOKE1 tunnel 100.1.1.2), 00:21:18
```

3. SPOKE2端路由表

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0]
S       10.10.10.0/24 [5/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
C       10.10.10.3/32 is directly connected, SPOKE2
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected, port2
B       192.168.0.0/24 [200/0] via 10.10.10.1 (recursive via SPOKE2 tunnel 100.1.1.2), 00:22:27
B       192.168.1.0/24 [200/0] via 10.10.10.2 (recursive via SPOKE2 tunnel 100.1.1.2), 00:22:27
```

业务测试

1. HUB端业务测试

```
PC1# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6140132  bytes 1760274153 (1.6 GiB)
        RX errors 0  dropped 3749603  overruns 0  frame 0
        TX packets 51686  bytes 3833219 (3.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

访问SPOKE1
PC1# ping 192.168.1.10 -c 4
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=62 time=1.42 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=62 time=0.788 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=62 time=0.751 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=62 time=0.688 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.688/0.913/1.427/0.300 ms

访问SPOKE2
PC1# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=62 time=1.09 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=62 time=0.935 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=0.991 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=1.06 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.935/1.021/1.098/0.070 ms
```

2. SPOKE1端业务测试

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
PC2# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1a6c:e61:d2b9:a415  prefixlen 64  scopeid 0×20<link>
        inet6 2001::2  prefixlen 64  scopeid 0×0<global>
        ether 00:0c:29:0e:4e:c5  txqueuelen 1000  (Ethernet)
        RX packets 5904889  bytes 459674552 (438.3 MiB)
        RX errors 0  dropped 58  overruns 0  frame 0
        TX packets 3224540  bytes 205411564402 (191.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

访问HUB
PC2# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.746 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.765 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.862 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=0.677 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.677/0.762/0.862/0.071 ms

访问SPOKE2
PC2# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=61 time=1.14 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=61 time=0.952 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=61 time=1.51 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=61 time=0.886 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.886/1.124/1.519/0.248 ms
```

3. **SPOKE2端业务测试**

```
PC3# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.10  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::2652:4dd7:5d0e:941d  prefixlen 64  scopeid 0×20<link>
        inet6 240e:604:109:39::216  prefixlen 64  scopeid 0×0<global>
        ether 00:0c:29:37:f0:ac  txqueuelen 1000  (Ethernet)
        RX packets 9638867  bytes 205844622412 (191.7 GiB)
        RX errors 0  dropped 118  overruns 0  frame 0
        TX packets 5737914  bytes 378901312 (361.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

访问HUB
PC3# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.848 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.935 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.899 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=1.04 ms
--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.848/0.931/1.045/0.081 ms

访问SPOKE1
PC3# ping 192.168.1.10 -c 4
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=61 time=1.13 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=61 time=1.22 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=61 time=1.21 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=61 time=1.04 ms
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.043/1.151/1.220/0.075 ms
```

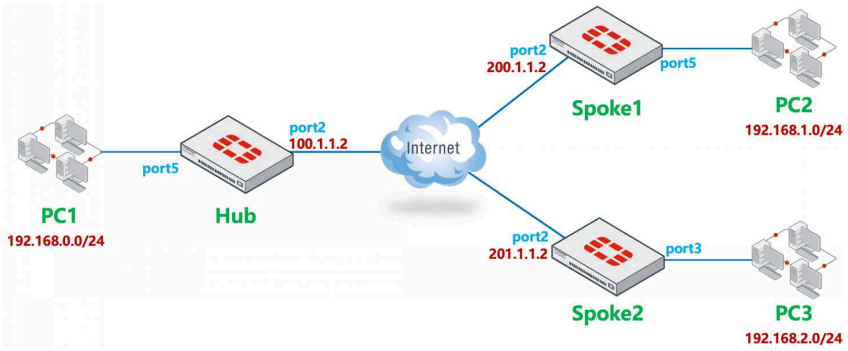

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ADVPN模式

网络需求

传统的Hub-Spoke方式中，Spoke只能和Hub建立永久隧道，Spoke之间的流量需要通过Hub来转发，这种方式减轻了Spoke的负担，增加了 Hub的性能要求，同时利于总部对分支间流量的监控；使用ADVPN技术实现的Full-Mesh方式中，Spoke之间可以建立动态直连隧道，分支间的流量可以直接转发。相比而言，Hub负担减轻，同时减少分支间流量的延迟，更有利于SPOKE之间的流量传输，在实际使用的过程中可按照自身需求进行选择。

网络拓扑



VPN Tunnel IP地址分配，以及BGP的规划：

角色	公网IP	私网网段	VPN隧道IP	BGP信息
HUB	100.1.1.2	192.168.0.1/24	10.10.10.1	AS 65001 RR反射器
SPOKE1	200.1.1.2	192.168.1.1/24	10.10.10.2	AS 65001 RR Client
SPOKE2	201.1.1.2	192.168.2.1/24	10.10.10.3	AS 65001 RR Client
SPOKE3	...	...	...	...
SPOKEX	...	...	...	...

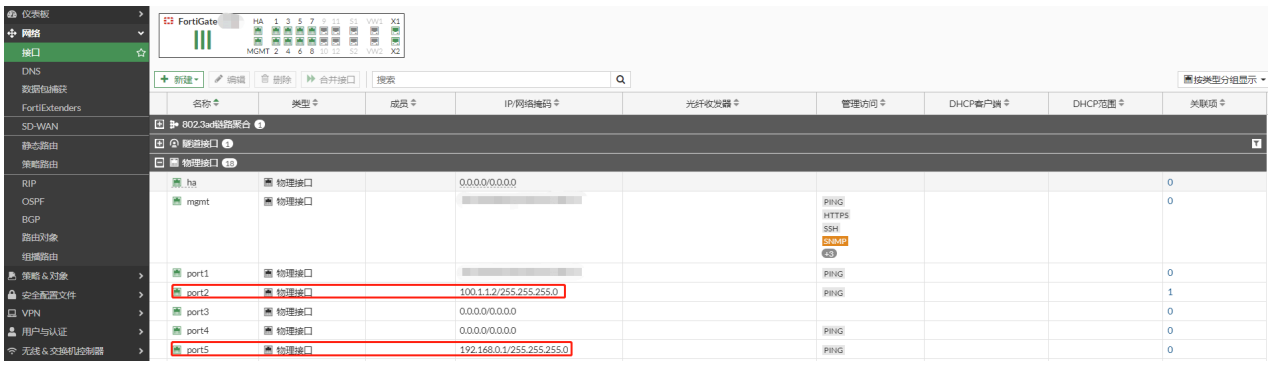
配置步骤

这里使用IPSEC “Hub and Spoke”模板创建ADVPN。

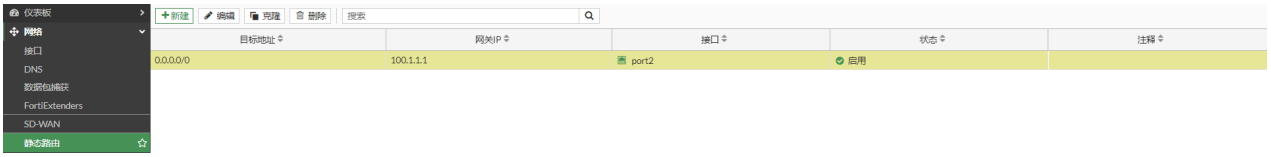
HUB端配置

1. **基本配置**

配置接口IP和路由

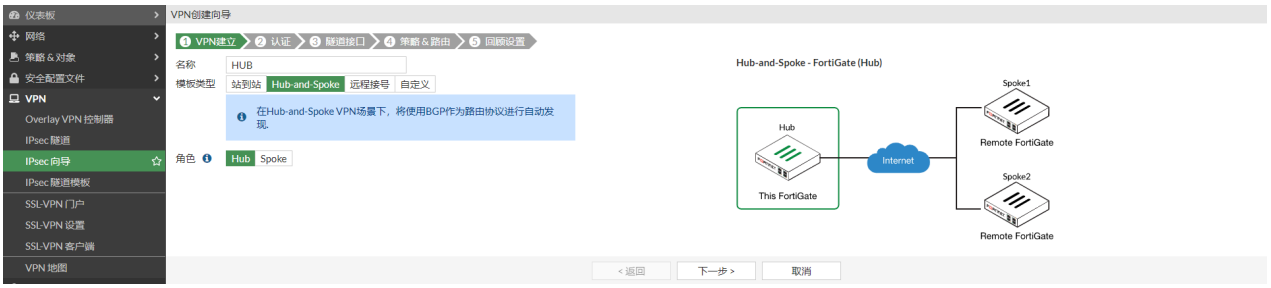


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

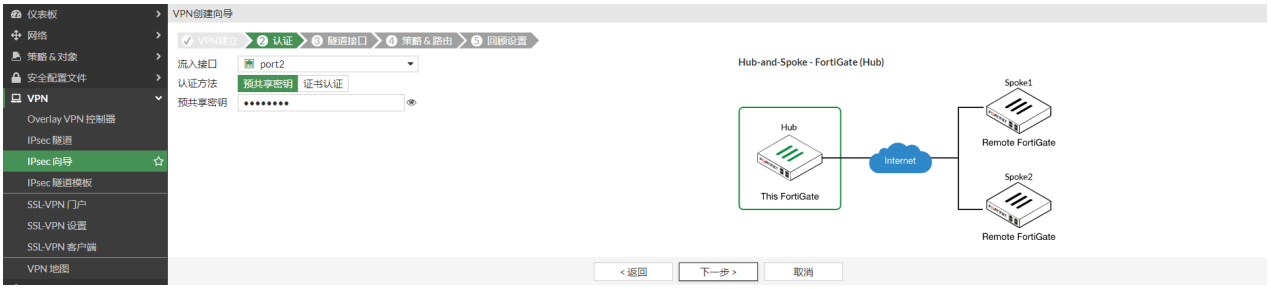


2. 配置IPSEC VPN

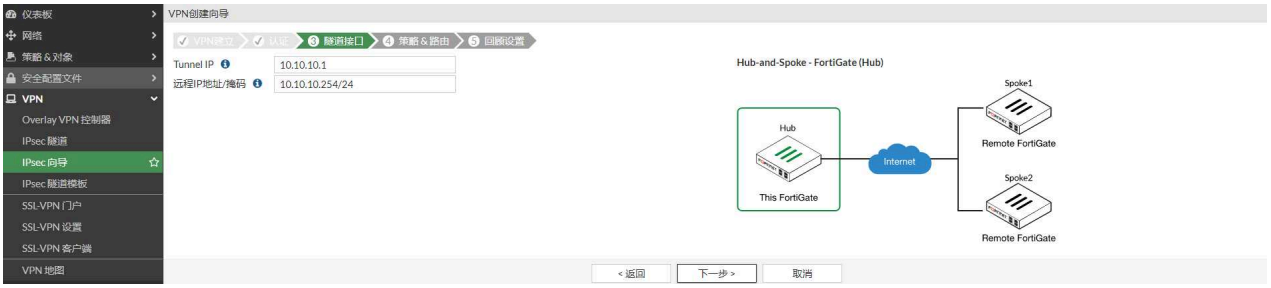
选择“Hub and Spoke”模板



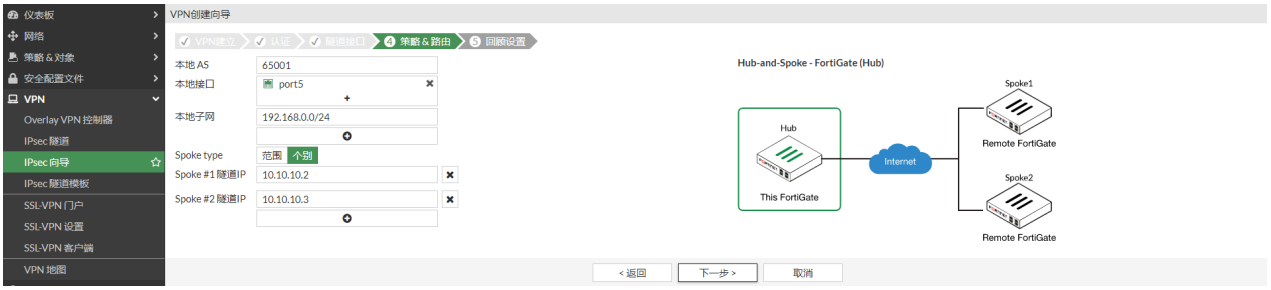
选择创建IPSEC的接口及预共享秘钥。



HUB端的tunnel ip是10.10.10.1，远程IP地址/掩码是10.10.10.254/24。10.10.10.254是不被Spoke所使用的预留IP，IPsec Tunnel是一个点对点的隧道，但是ADVPN中这条隧道需要同时对应多个SPOKE，因此不能将Remote IP写成一个存在的SPOKE端IP。



输入BGP AS号，本地的内网接口及本地的内网网段，这里有两个spoke，分别设置对应隧道IP。



VPN向导即将创建的内容。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



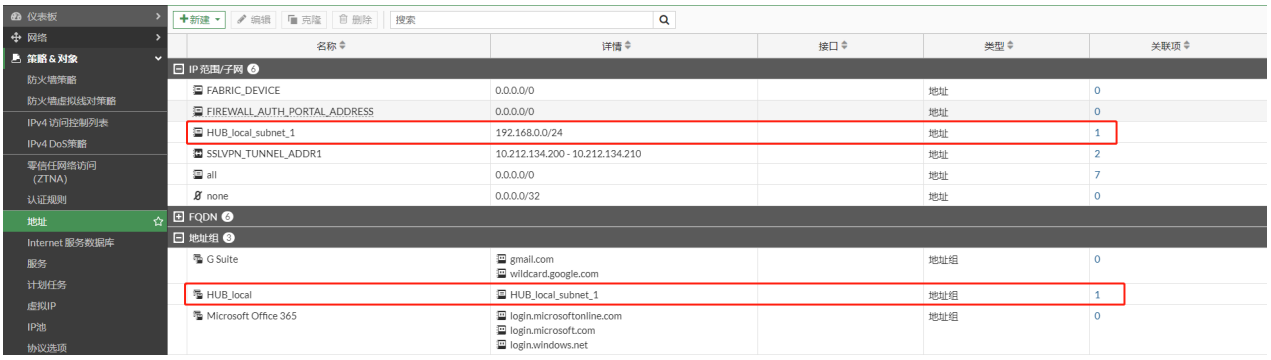
VPN创建完成，Spoke#1和Spoke#2需要复制下来用于SPOKE端创建VPN。



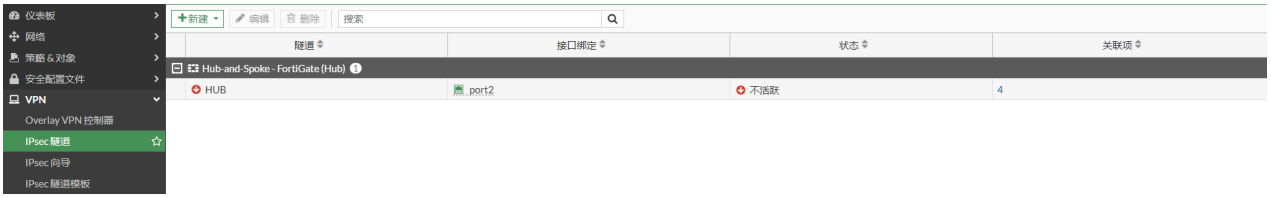
查看HUB端IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建地址对象和地址对象组



2. 创建IPSEC VPN



对应的命令行

```
config vpn ipsec phase1-interface
    edit "HUB"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

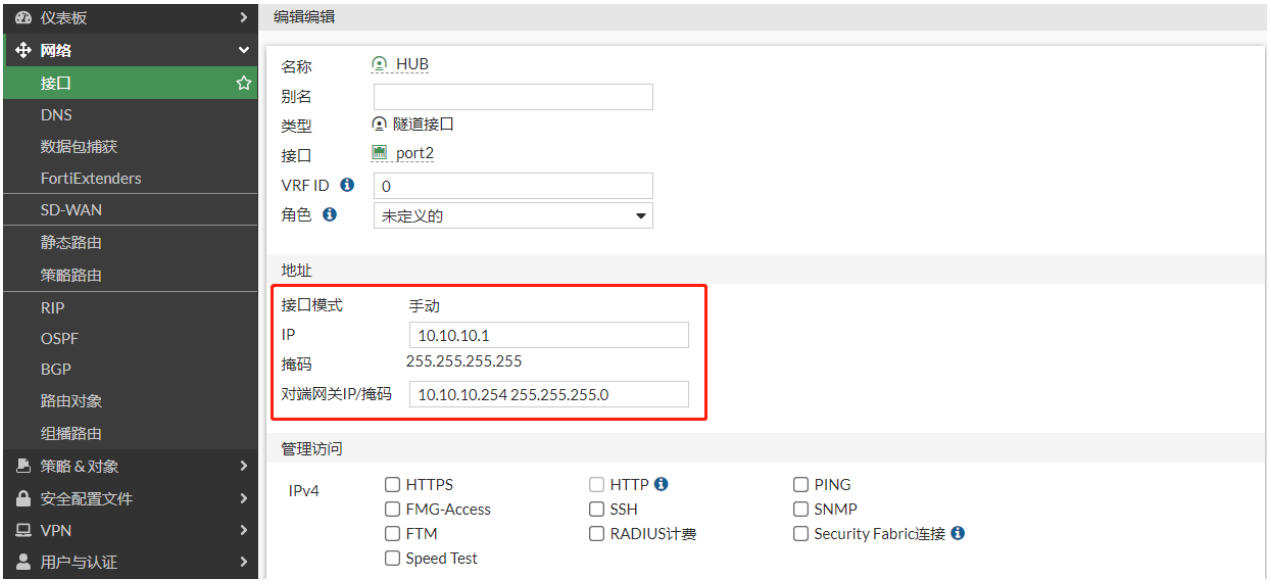
```
        set add-route disable
        set dpd on-idle
        set comments "VPN: HUB (Created by VPN wizard)"
        set wizard-type hub-fortigate-auto-discovery
        set auto-discovery-sender enable
        set psksecret ENC
SKVqWAT1K2iJB8U5T26IVmwtHjbLPes7VloWfh1ARXPGobKTYHruFIVEe/RjNKZrNj3j1GdXrvp1GlPLt7DExzLGKKyIoQ/1q5owciyhpLn753JL0k
RW86eR/C2h0aDcGZVKI8U9MagbU1pEy7RC71rtRr3dJjSd95eu6oeyq9FssYpAq9jCdyDbiSpbZoEVoYEwiw==
    next
end
config vpn ipsec phase2-interface
    edit "HUB"
        set phase1name "HUB"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: HUB (Created by VPN wizard)"
    next
end
```

3. 创建策略

> **重要**
>
> 模板中只创建了SPOKE到HUB端的策略以及SPOKE到SPOKE端的策略，没有创建HUB到SPOKE端的策略，可以根据业务的需求添加。



4. 创建VPN接口IP



5. 创建BGP

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



针对向导配置的优化建议

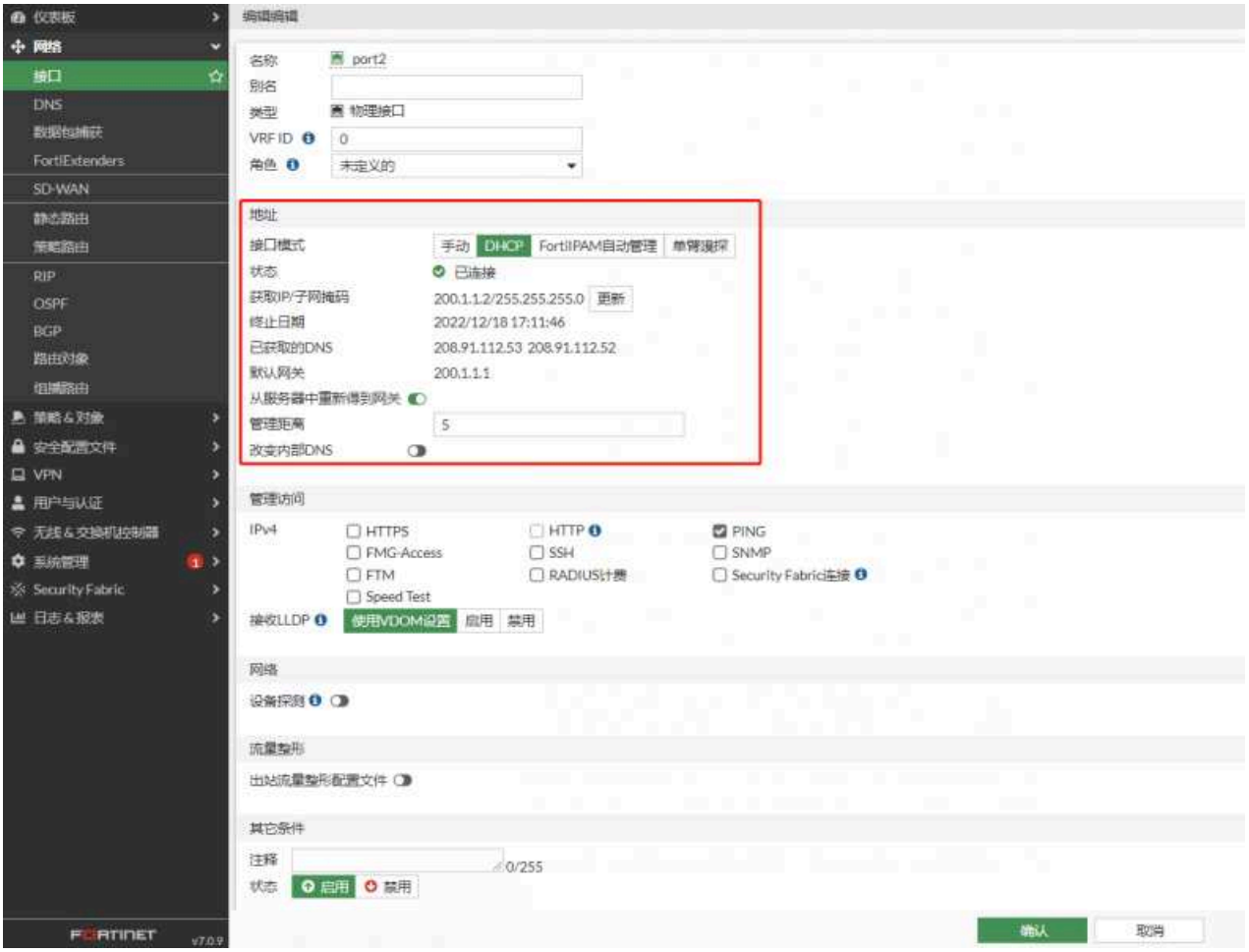
1. 在第一阶段中开启DPD周期性检测（每隔10s检测一次Peer状态），实现快速的检测并切换VPN隧道的目的。

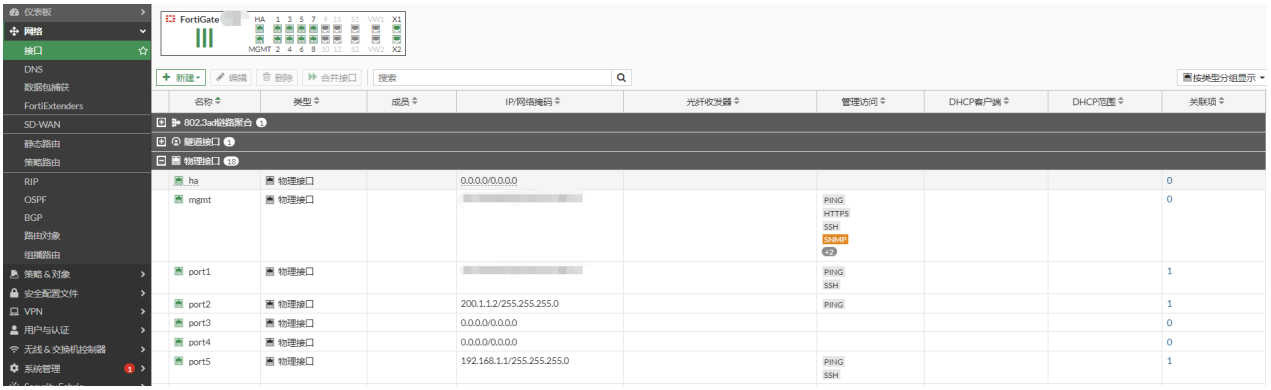
```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

SPOKE1端配置

1. **基本配置**

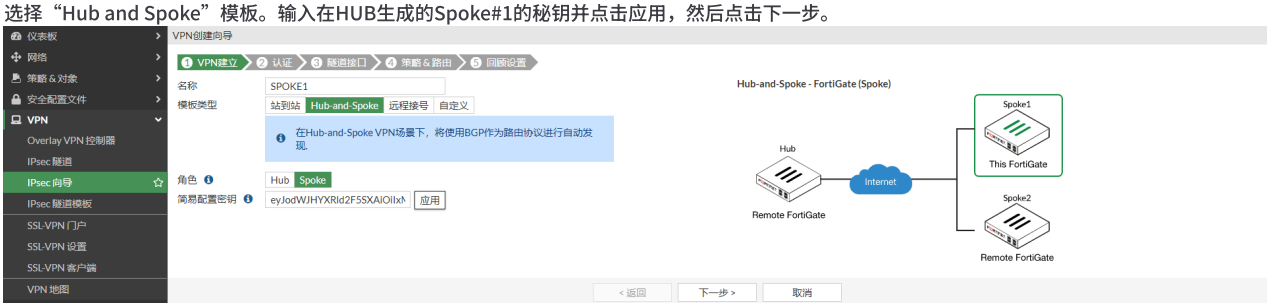
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





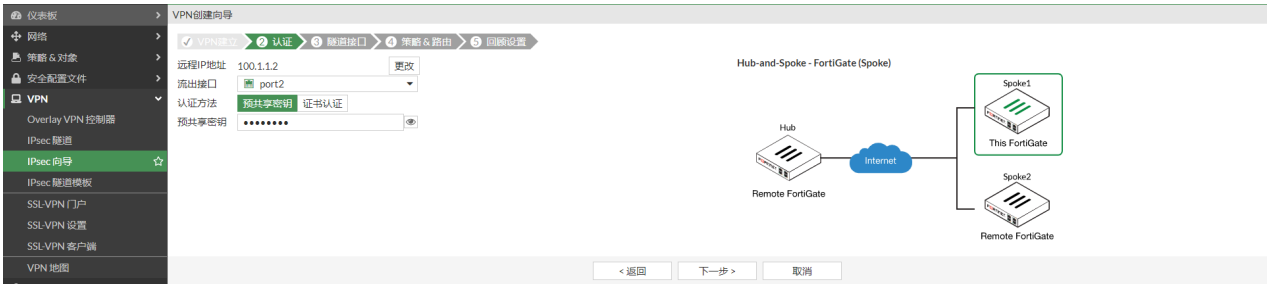
2. 配置IPSEC VPN

选择“Hub and Spoke”模板。输入在HUB生成的Spoke#1的秘钥并点击应用，然后点击下一步。

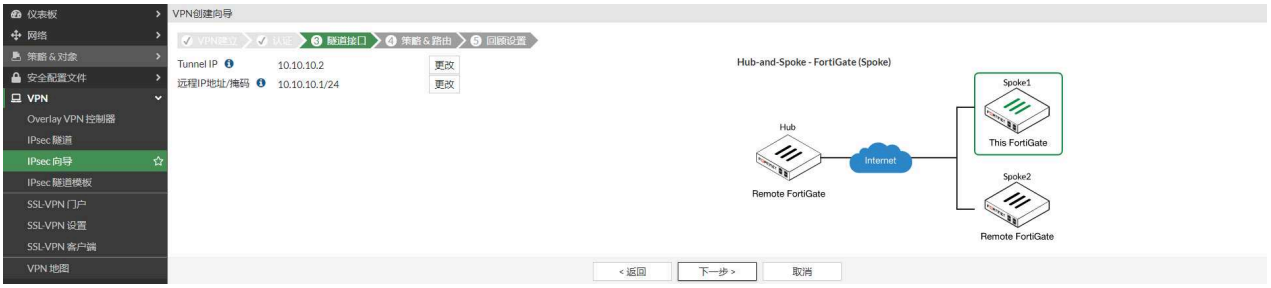


远程IP地址和流出接口会自动生成，需要输入预共享秘钥。点击下一步。

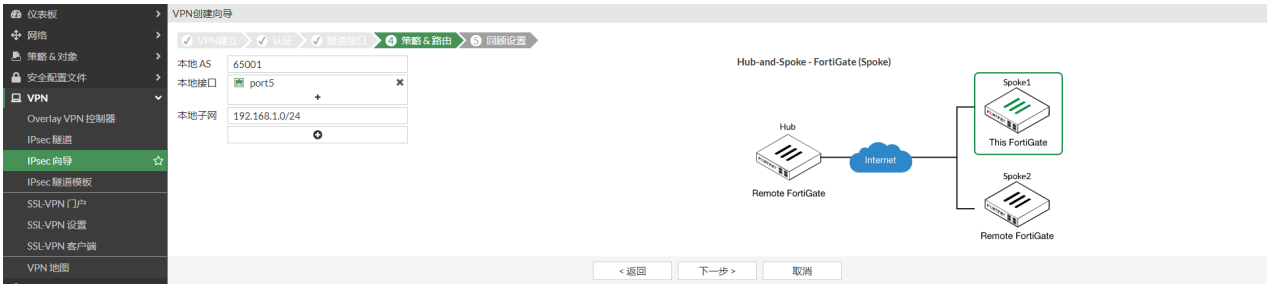
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



自动生成隧道IP，点击下一步。



自动生成本地AS号，需要生成SPOKE1本地的内网接口及需要保护的内网网段，点击下一步。



VPN向导即将创建的内容，点击完成。



VPN创建完成。

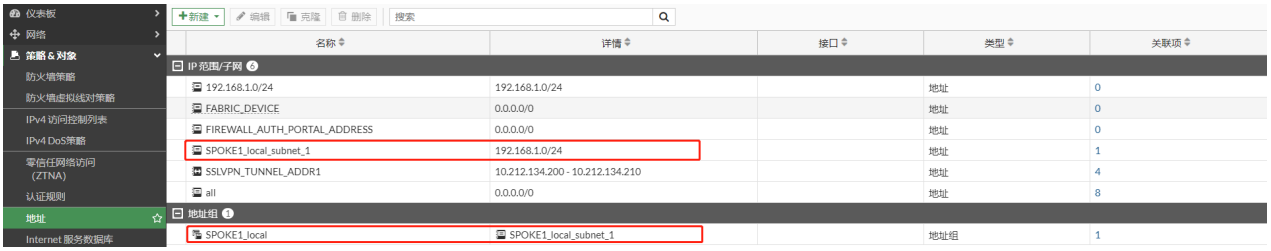


查看SPOKE1端IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建地址对象和地址对象组

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 创建VPN



对应的命令行

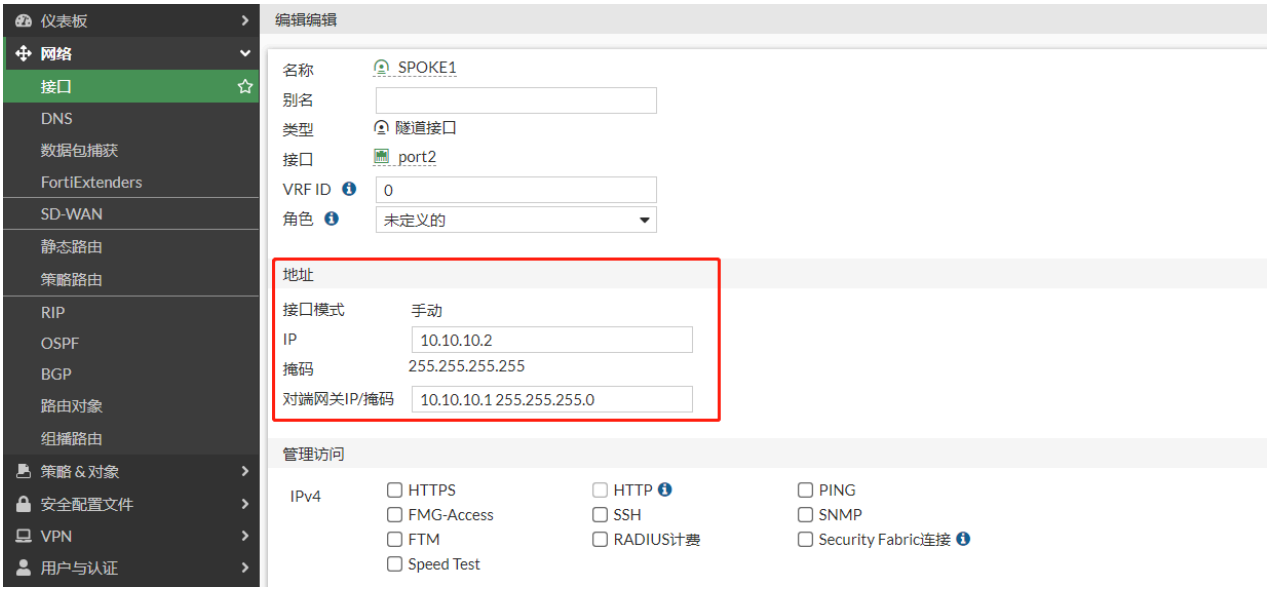
```bash
config vpn ipsec phase1-interface
    edit "SPOKE1"
        set interface "port2"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: SPOKE1 (Created by VPN wizard)"
        set wizard-type spoke-fortigate-auto-discovery
        set auto-discovery-receiver enable
        set remote-gw 100.1.1.2
        set psksecret ENC
zVXgULIXvCQPfG0ubZ8R36jhME7KanJ9V/NyV8zt5tXA5jlwPAli6alNN6g26Udtb04sWU/veKHuorIFmj9fO0J9vBi6Da6+pRlhnfSZ/f3fcxG7hj
7ydbk72PyXw2mDdDKsMty+27VVqTNG8OEyxdX+/vCG82iT5NjaLM84V/P1/YNUlIWqrnte2PEjuw9tzzbbDQ==
    next
end
config vpn ipsec phase2-interface
    edit "SPOKE1"
        set phase1name "SPOKE1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: SPOKE1 (Created by VPN wizard)"
    next
end
```

3. 创建策略



4. 创建VPN接口IP

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 创建BGP



针对向导配置的优化建议

1. 在第一阶段中开启DPD周期性检测（每隔10s检测一次Peer状态），实现快速的检测并切换VPN隧道的目的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

2. 开启自动协商，主动让隧道UP起来，而非使用VPN业务的时候再去触发VPN的协商，这样可以减少业务的丢包。在VPN主动发起方开启即可。

   IPSEC VPN阶段一自动协商是默认开启的。

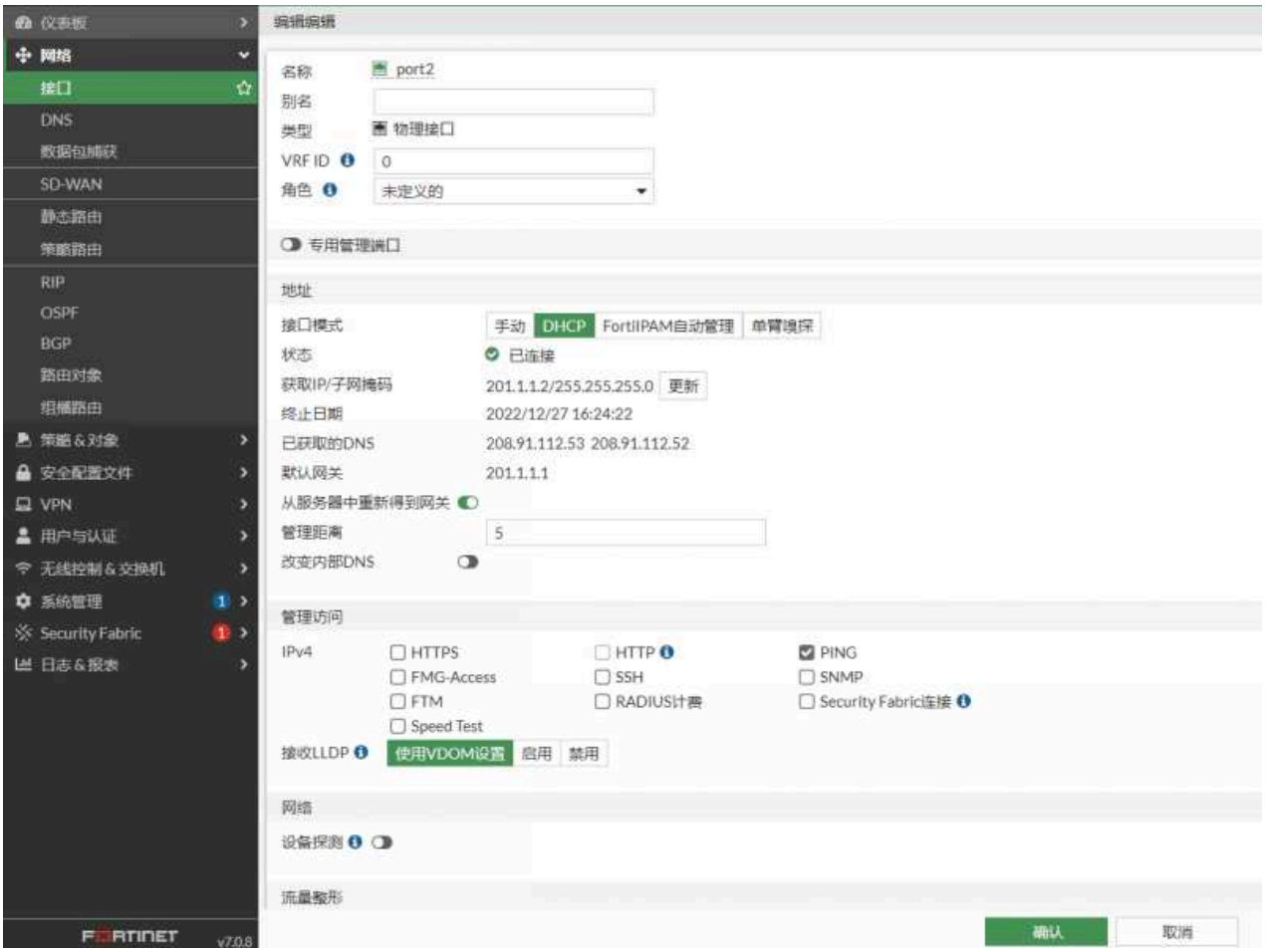
```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

IPSEC VPN阶段二自动协商默认关闭，需要开启。

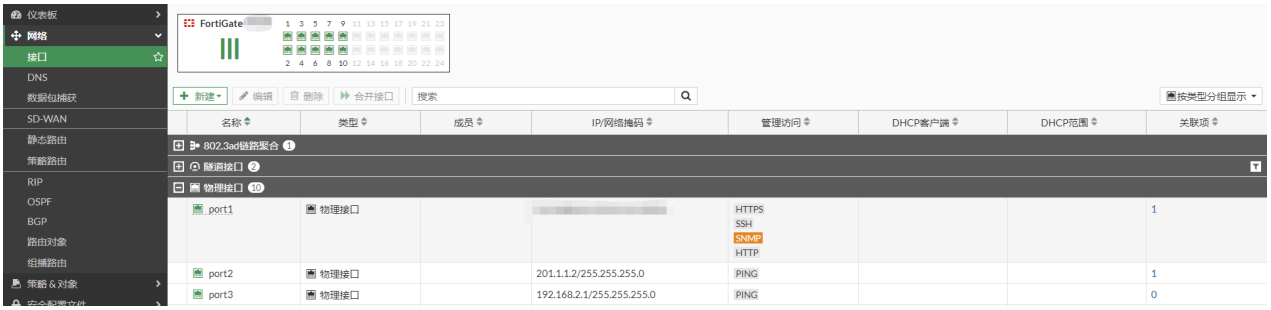
```
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

SPOKE2配置

1. 基本配置

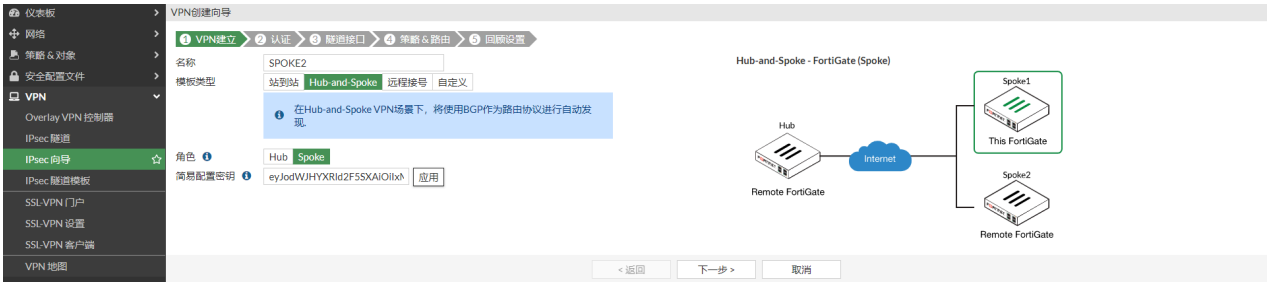


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

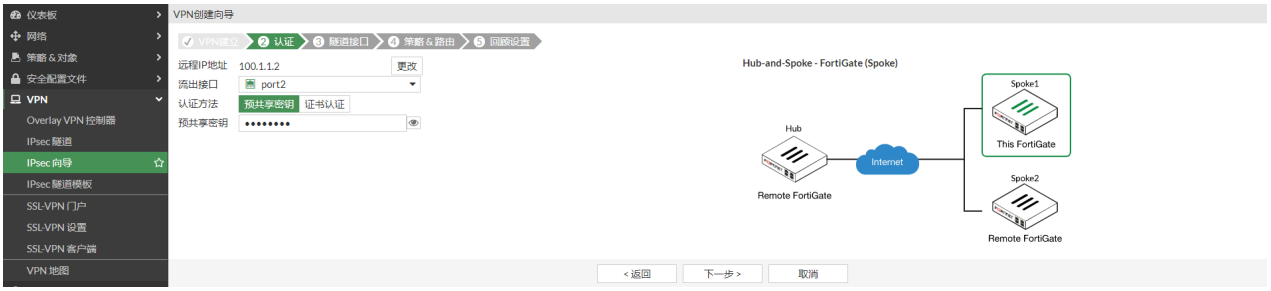


2. 配置IPSEC VPN

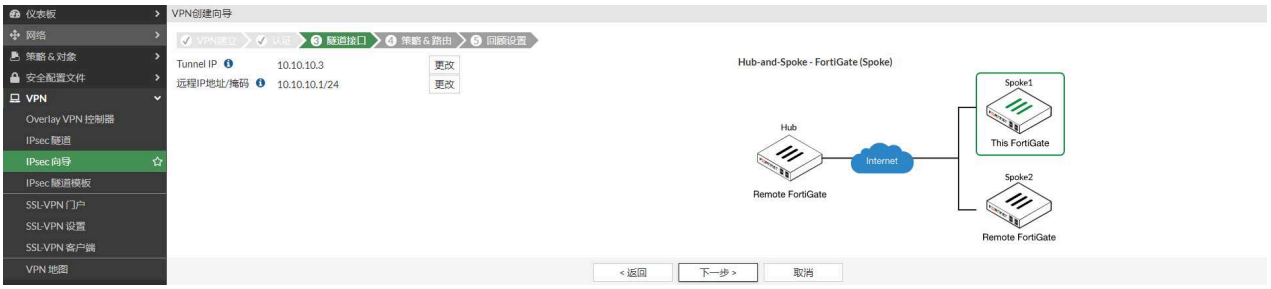
选择“Hub and Spoke”模板。输入在HUB生成的Spoke#2的秘钥并点击应用，然后点击下一步。



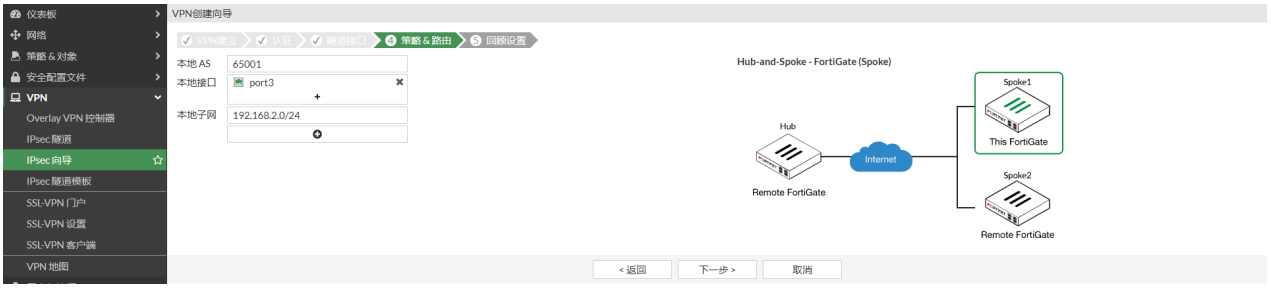
远程IP地址和流出接口会自动生成，需要输入预共享秘钥。点击下一步。



自动生成隧道IP，点击下一步。



自动生成本地AS号，需要生成SPOKE1本地的内网接口及需要保护的内网网段，点击下一步。



VPN向导即将创建的内容，点击完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



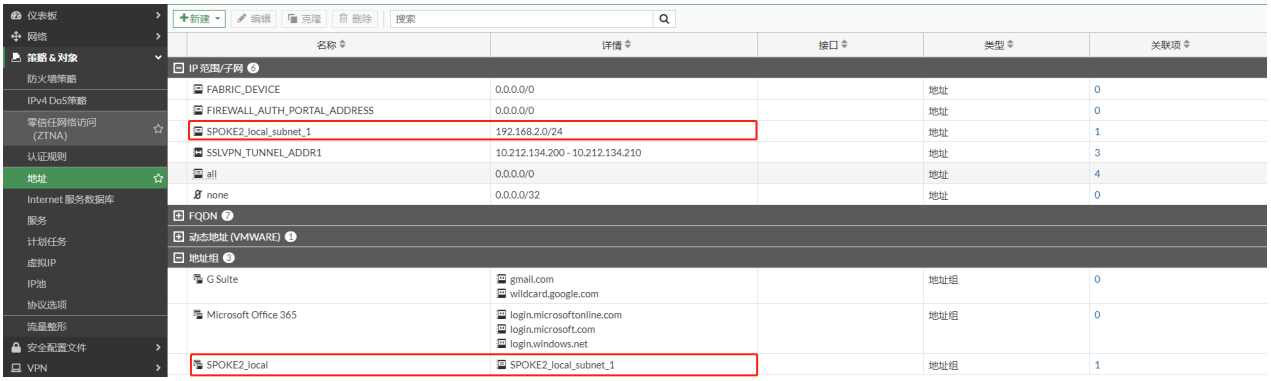
VPN创建成功。



查看SPOKE2端IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建地址对象和地址对象组



2. 创建VPN



对应的命令行

```
config vpn ipsec phase1-interface
    edit "SPOKE2"
        set interface "port2"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: SPOKE2 (Created by VPN wizard)"
        set wizard-type spoke-fortigate-auto-discovery
        set auto-discovery-receiver enable
        set remote-gw 100.1.1.2
        set psksecret ENC
```

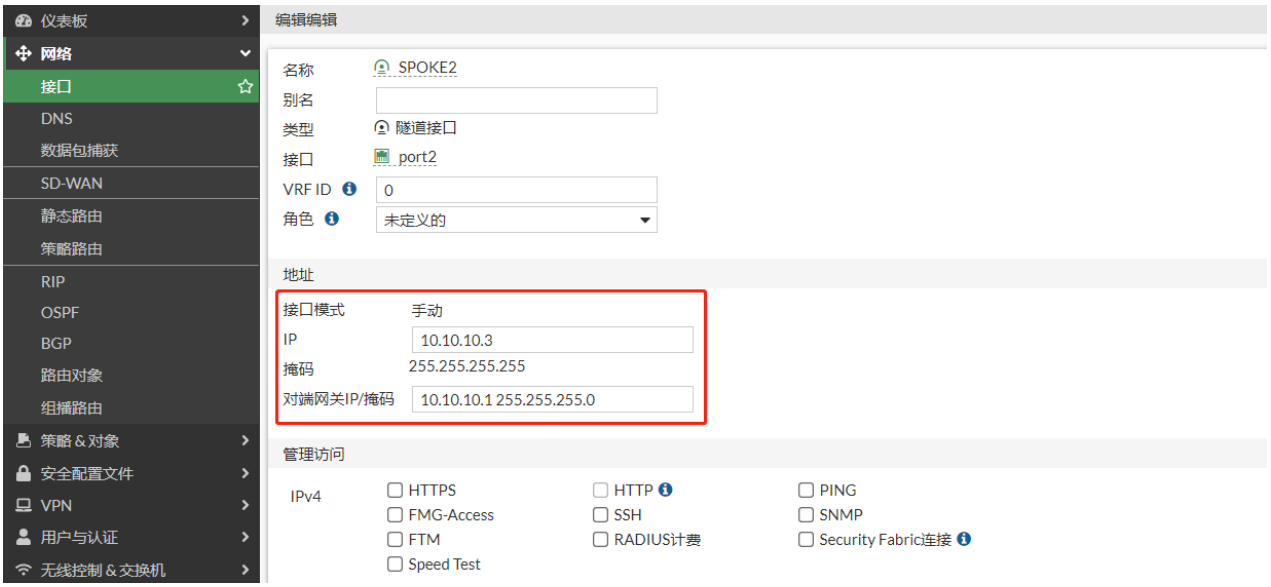

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Hhob5itx47wX/q8zqk2vgdQqbTGPVR3Ks4Bti+eH4AOK/4vS+a1JTnh4IwhyrQ8J8APUDv6ttVJDUV00lROhiXPy3XNqtZR1Vw8mlAv1I3KQTvEWV9
/AUZRWRqoEKN8uo98qbPR97LC5NPQ7OIiZYvsh8T5XQhHGzRNiQpL4sSWBRbJDTvKrxarnuJr8UIdzHqO7xA==
    next
end
config vpn ipsec phase2-interface
    edit "SPOKE2"
        set phase1name "SPOKE2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: SPOKE2 (Created by VPN wizard)"
    next
end
```

3. 创建策略



4. 创建VPN接口IP



5. 创建BGP

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



针对向导配置的优化建议

1. 在第一阶段中开启DPD周期性检测（隧道没有流量时，每隔10s检测一次Peer状态），实现快速的检测并切换VPN隧道的目的。

```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set dpd on-idle
        set dpd-retrycount 3
        set dpd-retryinterval 10
    next
end
```

2. 开启自动协商，主动让隧道UP起来，而非使用VPN业务的时候再去触发VPN的协商，这样可以减少业务的丢包。在VPN主动发起方开启即可。

   IPSEC VPN阶段一自动协商是默认开启的。

```
config vpn ipsec phase1-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```

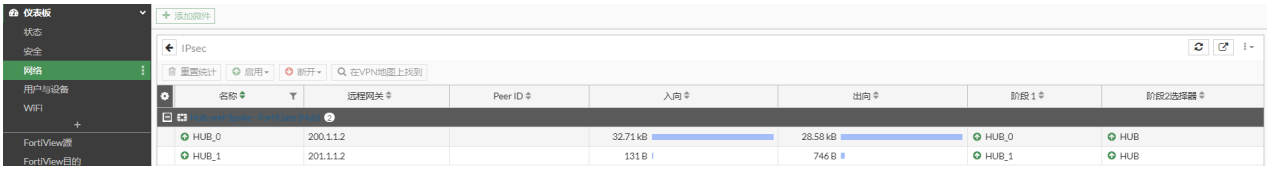
   IPSEC VPN阶段二自动协商默认关闭，需要开启。

```
config vpn ipsec phase2-interface
    edit "VPN-to-SH"
        set auto-negotiate enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

查看VPN和路由状态

1. HUB端VPN和路由状态




```
# diagnose vpn  ike gateway list

vd: root/0
name: HUB_0
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 200.1.1.2:500
tun_id: 10.10.10.2/::10.0.0.4
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.1 → 10.10.10.2
created: 212s ago
auto-discovery: 1 sender
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/2  established 1/2  time 0/0/0 ms

  id/spi: 0 1f454ba48eb31ef1/779d7de61a925ba5
  direction: responder
  status: established 212-212s ago = 0ms
  proposal: aes128-sha256
  key: 26b761298dff1684-03a1e6994809ae6d
  lifetime/rekey: 86400/85917
  DPD sent/recv: 00000000/00000000

vd: root/0
name: HUB_1
version: 1
interface: port2 10
addr: 100.1.1.2:500 → 201.1.1.2:500
tun_id: 10.10.10.3/::10.0.0.5
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.1 → 10.10.10.3
created: 155s ago
auto-discovery: 1 sender
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/2  established 1/2  time 0/0/0 ms

  id/spi: 1 4b28344cdc4862a2/c0f31569b4326560
  direction: responder
  status: established 155-155s ago = 0ms
  proposal: aes128-sha256
  key: 5e6660c76dfafef8-062dfbfdc7c83d2d
  lifetime/rekey: 86400/85974
  DPD sent/recv: 00000000/00000008

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=HUB_0 ver=1 serial=5 100.1.1.2:0→200.1.1.2:0 tun_id=10.10.10.2 tun_id6=::10.0.0.4 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=HUB index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=s/1
stat: rxp=2 txp=482 rxb=32710 txb=34637
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

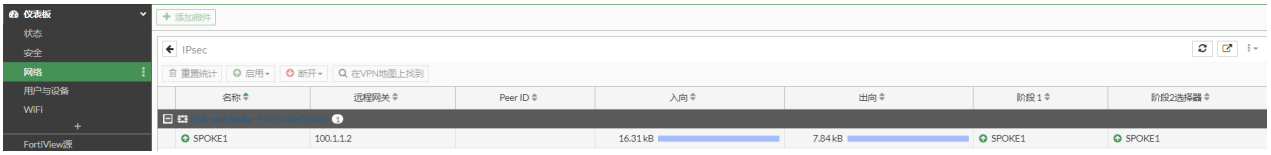
```
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=HUB proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1438 expire=43082/0B replaywin=2048
       seqno=f2 esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43186/43200
  dec: spi=9fbaba90 esp=aes key=16 a779f017a79a7e25bebcd73a8729ca4d
       ah=sha1 key=20 032444a21009bb1ed477c1b1c9fff594761031d5
  enc: spi=54b85815 esp=aes key=16 c4dcfc64ac2175b63e9e35198755e4ac
       ah=sha1 key=20 9b19cfd19c928ae8d12de4c6a76a7040e9baf274
  dec:pkts/bytes=2/16392, enc:pkts/bytes=482/47064
  npu_flag=03 npu_rgwy=200.1.1.2 npu_lgwy=100.1.1.2 npu_selid=2 dec_npuid=1 enc_npuid=1
--------------------------------------------------------------
name=HUB_1 ver=1 serial=6 100.1.1.2:0→201.1.1.2:0 tun_id=10.10.10.3 tun_id6=::10.0.0.5 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=HUB index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=s/1
stat: rxp=2 txp=12 rxb=131 txb=798
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=2
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=HUB proto=0 sa=1 ref=3 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1438 expire=43120/0B replaywin=2048
       seqno=4 esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43190/43200
  dec: spi=9fbaba91 esp=aes key=16 2670729ad842dd91c879db020170554b
       ah=sha1 key=20 1b6eb76171659fc431e7ffaed7e90bb9d7daa1fe
  enc: spi=f01e0450 esp=aes key=16 e4ed2f14faac5e5ddf7dec37ac8d6843
       ah=sha1 key=20 12f6d432f0a1ebef51de6e32d811dba066f54741
  dec:pkts/bytes=2/142, enc:pkts/bytes=6/551
  npu_flag=03 npu_rgwy=201.1.1.2 npu_lgwy=100.1.1.2 npu_selid=3 dec_npuid=1 enc_npuid=1
--------------------------------------------------------------
name=HUB ver=1 serial=4 100.1.1.2:0→0.0.0.0:0 tun_id=10.0.0.2 tun_id6=::10.0.0.2 dst_mtu=0 dpd-link=on weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0

proxyid_num=0 child_num=2 refcnt=4 ilast=42953655 olast=42953655 ad=/0
stat: rxp=4 txp=494 rxb=32841 txb=35435
dpd: mode=on-idle on=0 idle=10000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

查看路由表

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port2, [1/0]
C       10.10.10.0/24 is directly connected, HUB
C       10.10.10.1/32 is directly connected, HUB
C       100.1.1.0/24 is directly connected, port2
C       192.168.0.0/24 is directly connected, port5
B       192.168.1.0/24 [200/0] via 10.10.10.2 (recursive is directly connected, HUB), 00:50:01
B       192.168.2.0/24 [200/0] via 10.10.10.3 (recursive is directly connected, HUB), 00:29:13
```

2. SPOKE1端VPN和路由状态

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
# diagnose vpn ike gateway list

vd: root/0
name: SPOKE1
version: 1
interface: port2 10
addr: 200.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.2 → 10.10.10.1
created: 397s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/2  established 1/2  time 0/0/0 ms

  id/spi: 0 1f454ba48eb31ef1/779d7de61a925ba5
  direction: initiator
  status: established 397-397s ago = 0ms
  proposal: aes128-sha256
  key: 26b761298dff1684-03a1e6994809ae6d
  lifetime/rekey: 86400/85702
  DPD sent/recv: 00000004/00000000

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=SPOKE1 ver=1 serial=1 200.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/568 options[0238]=npu create_dev frag-rfc  role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=11 olast=11 ad=r/2
stat: rxp=2 txp=649 rxb=32678 txb=45413
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE1 proto=0 sa=1 ref=3 serial=2 auto-negotiate adr
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=42643/0B replaywin=2048
       seqno=1bf esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42933/43200
  dec: spi=54b85815 esp=aes key=16 c4dcfc64ac2175b63e9e35198755e4ac
       ah=sha1 key=20 9b19cfd19c928ae8d12de4c6a76a7040e9baf274
  enc: spi=9fbaba90 esp=aes key=16 a779f017a79a7e25bebcd73a8729ca4d
       ah=sha1 key=20 032444a21009bb1ed477c1b1c9fff594761031d5
  dec:pkts/bytes=2/16342, enc:pkts/bytes=892/90448
  npu_flag=03 npu_rgwy=100.1.1.2 npu_lgwy=200.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1
```

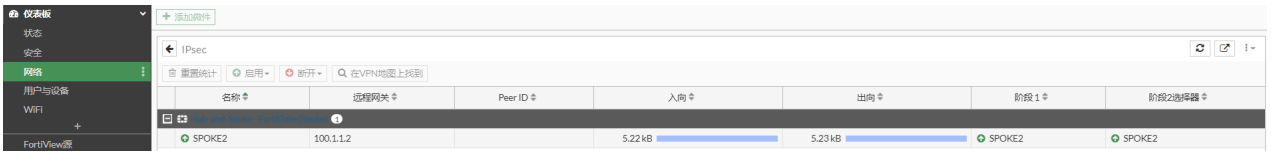
查看路由表

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0]
S       10.10.10.0/24 [5/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
C       10.10.10.2/32 is directly connected, SPOKE1
C       192.168.1.0/24 is directly connected, port5
C       200.1.1.0/24 is directly connected, port2
B       192.168.0.0/24 [200/0] via 10.10.10.1 (recursive via SPOKE1 tunnel 100.1.1.2), 00:52:00
B       192.168.2.0/24 [200/0] via 10.10.10.3 (recursive via SPOKE1 tunnel 100.1.1.2), 00:30:43
```

3. SPOKE2端VPN和路由状态




```
# diagnose vpn ike gateway list

vd: root/0
name: SPOKE2
version: 1
interface: port2 6
addr: 201.1.1.2:500 → 100.1.1.2:500
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.3 → 10.10.10.1
created: 429s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/2  established 1/2  time 0/0/0 ms

  id/spi: 0 4b28344cdc4862a2/c0f31569b4326560
  direction: initiator
  status: established 429-429s ago = 0ms
  proposal: aes128-sha256
  key: 5e6660c76dfafef8-062dfbfdc7c83d2d
  lifetime/rekey: 86400/85671
  DPD sent/recv: 00000017/00000003

# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=SPOKE2 ver=1 serial=2 201.1.1.2:0→100.1.1.2:0 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-link=on
weight=1
bound_if=6 lgwy=static/1 tun=intf mode=auto/1 encap=none/568 options[0238]=npu create_dev frag-rfc  role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=9 olast=9 ad=r/2
stat: rxp=27 txp=24 rxb=1863 txb=1536
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=23
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE2 proto=0 sa=1 ref=3 serial=2 auto-negotiate adr
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=1a203 type=00 soft=0 mtu=1438 expire=42552/0B replaywin=2048
       seqno=f esn=0 replaywin_lastseq=00000013 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42897/43200
  dec: spi=f01e0450 esp=aes key=16 e4ed2f14faac5e5ddf7dec37ac8d6843
       ah=sha1 key=20 12f6d432f0a1ebef51de6e32d811dba066f54741
  enc: spi=9fbaba91 esp=aes key=16 2670729ad842dd91c879db0201705546
       ah=sha1 key=20 1b6eb76171659fc431e7ffaed7e90bb9d7daa1fe
  dec:pkts/bytes=36/2480, enc:pkts/bytes=28/2653
  npu_flag=00 npu_rgwy=100.1.1.2 npu_lgwy=201.1.1.2 npu_selid=2 dec_npuid=0 enc_npuid=0
```

查看路由表

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0
S       10.10.10.0/24 [5/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
C       10.10.10.3/32 is directly connected, SPOKE2
C       192.168.2.0/24 is directly connected, port3
C       200.1.1.0/24 is directly connected, port2
B       192.168.0.0/24 [200/0] via 10.10.10.1 (recursive via SPOKE2 tunnel 100.1.1.2), 00:34:25
B       192.168.1.0/24 [200/0] via 10.10.10.2 (recursive via SPOKE2 tunnel 100.1.1.2), 00:34:25
```

业务测试

1. SPOKE1端访问HUB

```
PC2# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1a6c:e61:d2b9:a415  prefixlen 64  scopeid 0x20<link>
        inet6 2001::2  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:0e:4e:c5  txqueuelen 1000  (Ethernet)
        RX packets 5904889  bytes 459674552 (438.3 MiB)
        RX errors 0  dropped 58  overruns 0  frame 0
        TX packets 3224540  bytes 205411564402 (191.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC2# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.746 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.765 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.862 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=0.677 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.677/0.762/0.862/0.071 ms
```

2. SPOKE2端访问HUB

```
PC3# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.10  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::2652:4dd7:5d0e:941d  prefixlen 64  scopeid 0x20<link>
        inet6 240e:604:109:39::216  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:37:f0:ac  txqueuelen 1000  (Ethernet)
        RX packets 9638867  bytes 205844622412 (191.7 GiB)
        RX errors 0  dropped 118  overruns 0  frame 0
        TX packets 5737914  bytes 378901312 (361.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC3# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=62 time=0.848 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=62 time=0.935 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=62 time=0.899 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=62 time=1.04 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.848/0.931/1.045/0.081 ms
```

3. SPOKE之间访问

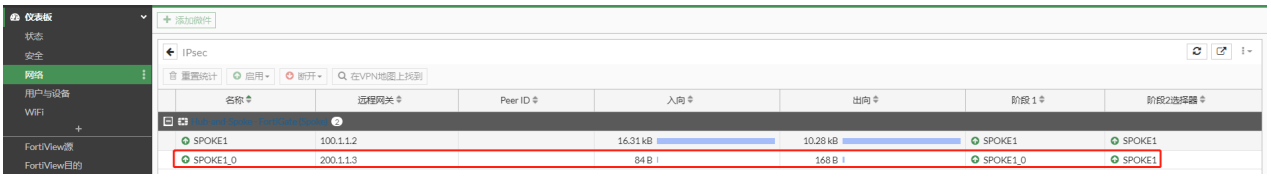
```
PC2# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1a6c:e61:d2b9:a415  prefixlen 64  scopeid 0x20<link>
        inet6 2001::2  prefixlen 64  scopeid 0x0<global>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        ether 00:0c:29:0e:4e:c5  txqueuelen 1000  (Ethernet)
        RX packets 5908666  bytes 460902918 (439.5 MiB)
        RX errors 0  dropped 58  overruns 0  frame 0
        TX packets 3225276  bytes 205411619294 (191.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

SPOKE1访问SPOKE2
PC2# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=61 time=1.27 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=0.925 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=0.812 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.812/1.004/1.276/0.199 ms
```

SPOKE之间访问时，会触发SPOKE之间创建单独的VPN。

在SPOKE1上查看与SPOKE2之间的VPN和路由。

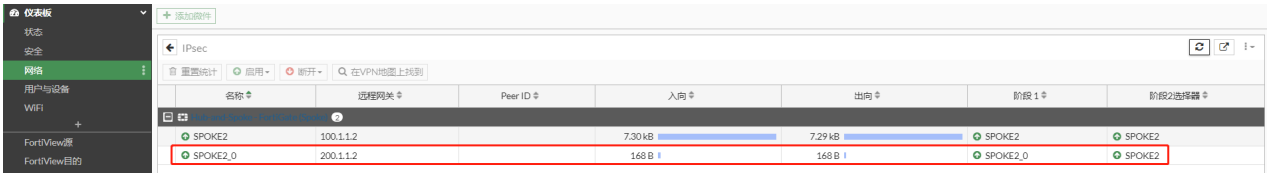



```
# diagnose vpn ike gateway list name SPOKE1_0

vd: root/0
name: SPOKE1_0
version: 1
interface: port2 10
addr: 200.1.1.2:500 → 201.1.1.2:500
tun_id: 201.1.1.2/::201.1.1.2
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.2 → 10.10.10.3
created: 30s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 2 c9a21426384683c3/9ec0d3e19cd425e1
  direction: initiator
  status: established 30-30s ago = 0ms
  proposal: aes128-sha256
  key: 8caa0db523816e6c-c1c1d43ab5961a5a
  lifetime/rekey: 86400/86069
  DPD sent/recv: 00000003/00000000

# diagnose vpn tunnel list name SPOKE1_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SPOKE1_0 ver=1 serial=3 200.1.1.2:0→201.1.1.2:0 tun_id=201.1.1.2 tun_id6=::201.1.1.2 dst_mtu=1500 dpd-
link=on weight=1
bound_if=10 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/760 options[02f8]=npu create_dev no-sysctl rgwy-chg
frag-rfc  role=primary accept_traffic=1 overlay_id=0

parent=SPOKE1 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=2 olast=2 ad=r/2
stat: rxp=1 txp=2 rxb=84 txb=168
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE1 proto=0 sa=1 ref=3 serial=1 auto-negotiate adr
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=42855/0B replaywin=2048
       seqno=3 esn=0 replaywin_lastseq=00000002 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42897/43200
  dec: spi=54b85816 esp=aes key=16 0478ea93933324f29cf01524e7d28ec4
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
       ah=sha1 key=20 5fb7754757facf499e85b1bdb314520d3cf10faa
  enc: spi=f01e0451 esp=aes key=16 183a97d565d45c86096969afeacd60ec
       ah=sha1 key=20 7f1cf1f622146d60453f68f35ed9804ab4566d46
  dec:pkts/bytes=2/168, enc:pkts/bytes=4/472
  npu_flag=03 npu_rgwy=201.1.1.2 npu_lgwy=200.1.1.2 npu_selid=3 dec_npuid=1 enc_npuid=1

  # get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 200.1.1.1, port2, [1/0]
S       10.10.10.0/24 [5/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE1 tunnel 100.1.1.2, [1/0]
C       10.10.10.2/32 is directly connected, SPOKE1
                      is directly connected, SPOKE1_0
C       10.10.10.3/32 is directly connected, SPOKE1_0
B       192.168.0.0/24 [200/0] via 10.10.10.1 (recursive via SPOKE1 tunnel 100.1.1.2), 00:07:22
B       192.168.2.0/24 [200/0] via 10.10.10.3 (recursive is directly connected, SPOKE1_0), 00:00:26
C       200.1.1.0/24 is directly connected, port2
C       192.168.1.0/24 is directly connected, port5
```

在SPOKE2上查看与SPOKE1之间的VPN。




```
# diagnose vpn ike gateway list name SPOKE2_0

vd: root/0
name: SPOKE2_0
version: 1
interface: port2 6
addr: 201.1.1.2:500 → 200.1.1.2:500
tun_id: 10.10.10.2/::10.0.0.1
remote_location: 0.0.0.0
network-id: 0
virtual-interface-addr: 10.10.10.3 → 10.10.10.2
created: 150s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 2 c9a21426384683c3/9ec0d3e19cd425e1
  direction: responder
  status: established 150-150s ago = 0ms
  proposal: aes128-sha256
  key: 8caa0db523816e6c-c1c1d43ab5961a5a
  lifetime/rekey: 86400/85979
  DPD sent/recv: 00000000/0000000f

# diagnose vpn  tunnel list name SPOKE2_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SPOKE2_0 ver=1 serial=3 201.1.1.2:0→200.1.1.2:0 tun_id=10.10.10.2 tun_id6=::10.0.0.1 dst_mtu=1500 dpd-
link=on weight=1
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/760 options[02f8]=npu create_dev no-sysctl rgwy-chg
frag-rfc  role=primary accept_traffic=1 overlay_id=0

parent=SPOKE2 index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=6 olast=6 ad=r/2
stat: rxp=2 txp=2 rxb=168 txb=168
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=SPOKE2 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=1a203 type=00 soft=0 mtu=1438 expire=43034/0B replaywin=2048
       seqno=3 esn=0 replaywin_lastseq=00000003 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43191/43200
  dec: spi=f01e0451 esp=aes key=16 183a97d565d45c86096969afeacd60ec
       ah=sha1 key=20 7f1cf1f622146d60453f68f35ed9804ab4566d46
  enc: spi=54b85816 esp=aes key=16 0478ea93933324f29cf01524e7d28ec4
       ah=sha1 key=20 5fb7754757facf499e85b1bdb314520d3cf10faa
  dec:pkts/bytes=4/336, enc:pkts/bytes=4/472
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=201.1.1.2 npu_selid=3 dec_npuid=0 enc_npuid=0

# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [5/0] via 201.1.1.1, port2, [1/0]
S       10.10.10.0/24 [5/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
S       10.10.10.1/32 [15/0] via SPOKE2 tunnel 100.1.1.2, [1/0]
C       10.10.10.2/32 is directly connected, SPOKE2_0
C       10.10.10.3/32 is directly connected, SPOKE2
                      is directly connected, SPOKE2_0
B       192.168.0.0/24 [200/0] via 10.10.10.1 (recursive via SPOKE2 tunnel 100.1.1.2), 00:13:13
B       192.168.1.0/24 [200/0] via 10.10.10.2 (recursive is directly connected, SPOKE2_0), 00:01:48
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected, port2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

野蛮模式/network-id适用场景

关于主模式中的Peer ID问题

1. 在主模式中，第3、4个包交互之后（DH公钥和随机数交换），需要使用到Pre-shared key（管理员配置的预共享密钥）值用于生成SHEYID（预共享密钥方式认证：SKEYID=hash (pre-shared key ,Ni | Nr) ），此时是无法通过Peer-ID查找到，因为Peer-ID参数在第5、6个包中，而且还是被加密的，解密需要使用到SHEYID为材料生成的密钥SHEYID_e，因此这个时候只能通过对方发起IKE协商的公网IP地址去查找Peer的Pre-shared key以确认其身份。
2. 如此将引出一个问题，在对方（分部）为PPPoE/DHCP等动态IP场景中时，总部无法配置明确的对方IP和Pre-shared key，而只能配置动态拨号方式的IPsec VPN，如果我们选择第一阶段为主模式，因为Peer-ID在第5、6包携带，并且是加密的，因此Hub在主模式中是无法提前获知到Peer-ID信息的，也没办法根据Peer-ID信息去查找到底用哪一个Pre-shared key，一般动态IP场景中主模式使用较少，而且就算使用主模式的话的Peer-ID配置为any的较多。
3. IKEv1主模式拨号连接的匹配条件顺序（所有匹配条件都一致时，Spoke发起的连接匹配Hub配置顺序的第一个拨号连接）：
   - local-gw：默认为拨号连接使用的接口Primary IP，可以手动更改为设备上其他接口的IP。
   - IKEv1 Main mode + PSK。
   - Proposal + DH group。

什么时候需要野蛮模式

1. Hub端同一个接口IP上存在多条动态拨号的IKEv1主模式IPsec VPN，且使用的算法、预共享密钥、DH组一致。此时由于拨号VPN的目的IP都是any（0.0.0.0），此时根本无法区分这两条IPsec VPN隧道，不知道拨号用户到底是匹配Dia_VPN1还是匹配Dia_VPN2（FGT的处理是优先匹配靠前的拨号VPN），因此为了区分本地的多条动态拨号VPN，则需要配置Peer ID参数，以便区分这本地的多条动态IPsec VPN隧道，例如：
   - Dia_VPN1（动态拨号VPN野蛮模式）：
     - Local ID：BJ
     - Peer ID：South-FGT
     - Dia_VPN2（动态拨号VPN野蛮模式）：
       - Local ID：BJ
       - Peer ID：North-FGT
2. 如果对方拨号用户1填写的Local ID是South-FGT则连接到Dia_VPN1，如果对方拨号用户2填写的Local ID是North-FGT则连接到Dia_VPN2。这样就可以将不通的拨号用户进行区分和分离，方便进行独立的VPN隧道、独立的策略进行控制。在这种需求的情况下：首先需要舍弃掉主模式，用野蛮模式，同时使用不同的Peer-ID来区分不同的动态VPN隧道。
3. IKEv1野蛮模式拨号连接的匹配条件顺序（所有匹配条件都一致时，Spoke发起的连接匹配Hub配置顺序的第一个拨号连接）：
   - local-gw：默认为拨号连接使用的接口Primary IP，可以手动更改为设备上其他接口的IP。
   - IKEv1 Main mode + PSK。
   - Proposal + DH group。
   - Peer ID（开启客户端用户认证时使用user.local.name ↗）。

什么时候需要network-id

1. 在IKEv2的协商报文中，ID信息包含在IKE_AUTH报文中，且被加密。所以会出现和IKEv1主模式一样的问题（同一个接口IP上存在多条动态拨号的IKEv1主模式IPsec VPN，且使用的算法、预共享密钥、DH组一致）。
2. Fortinet使用network-id属性来解决此问题，该字段包含在IKEv2协商的第1、2个报文（IKE_SA_INIT）中，没有被加密，**network-id为Fortinet私有**。

```bash
Hub:
config vpn ipsec phase1-interface
    edit "Hub_1"
        set ike-version 2
        set network-overlay enable
        set network-id 1
    next
end
config vpn ipsec phase1-interface
    edit "Spoke1"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set ike-version 2
        set network-overlay enable
        set network-id 1
    next
end
```

3. Hub在同一个接口IP上存在多条动态拨号的IKEv2 IPsec VPN，且使用的算法、预共享密钥、DH组一致，可以配置不同的network-id来区分不同的Spoke拨入连接。

```bash
config vpn ipsec phase1-interface
    edit "Hub_1"
        set type dynamic
        set interface "wan1"
        set ike-version 2
        set network-overlay enable
        set network-id 1
    next
        set type dynamic
        edit "Hub_2"
        set interface "wan1"
        set ike-version 2
        set network-overlay enable
        set network-id 2
    next
end
```

4. 每个Spoke配置不同的network-id来连接Hub上对应的拨号连接。

```bash
Spoke1:
config vpn ipsec phase1-interface
    edit "Spoke1"
        set interface "port2"
        set ike-version 2
        set network-overlay enable
        set network-id 1
    next
end

Spoke2:
config vpn ipsec phase1-interface
    edit "Spoke1"
        set interface "port2"
        set ike-version 2
        set network-overlay enable
        set network-id 2
    next
end
```

5. IKEv2拨号连接的匹配条件顺序（所有匹配条件都一致时，Spoke发起的连接匹配Hub配置顺序的第一个拨号连接）：

- local-gw：默认为拨号连接使用的接口Primary IP，可以手动更改为设备上其他接口的IP。
- IKEv1 Main mode + PSK。
- Proposal + DH group。
- network-id。

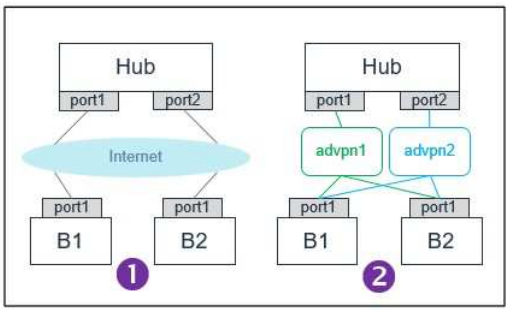
ADVPN下的network-id或野蛮模式ID

在ADVPN部署模式下，如果每个Spoke与Hub建立两条IPSec隧道，Spoke与Spoke创建shortcut隧道前，需要注意配置IKEv2的network-id或野蛮模式ID。如下举例的ADVPN环境，所有IPSec连接使用IKEv2建立。

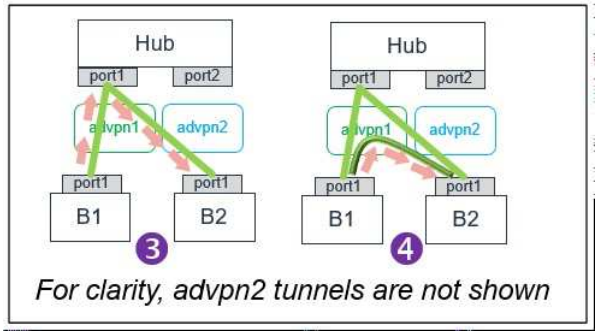
1. ADVPN部署，B1和B2只有一条运营商线路接入，Hub有两条运营商线路。

2. B1和B2的单线路与Hub的两个线路接口分别创建overlay IPSec隧道advpn1和advpn2。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

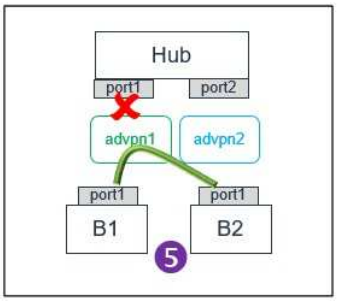


3. 初始状态下，B1访问B2的流量将经过B1→advpn1→Hub→advpn1→B2。然后Hub将通过advpn1协助B1和B2之间协商建立Shortcut隧道。



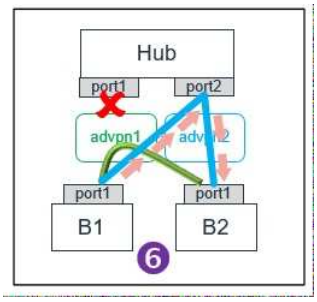
- B1和B2之间建立基于advpn1上的Shortcut。
- 随后从B1访问B2的流量将经过Shortcut _advpn1。

4. 如果Hub的port1线路出现故障。



- Hub（port1）和B1之间的父隧道将关闭，Hub（port1）和B2之间也会发生同样的情况。
- 同时，B1和B2之间创建的Shortcut_advpn1会维持建立状态，因为ADVPN Shortcut的lifetime与其父隧道（advpn1）的lifetime无关。
- B1↔Hub和B2↔Hub通过advpn1隧道建立的BGP邻居中断。

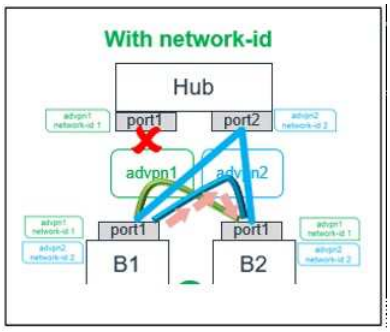
5. 之后B1和B2之间的BGP路由通过Hub的advpn2收敛。从B1主动访问B2的流量会先经过Hub转发，因为B1和B2之间还没有通过advpn2创建Shortcut。



6. Hub将尝试通过Advpn2在B1和B2之间建立Shortcut隧道。

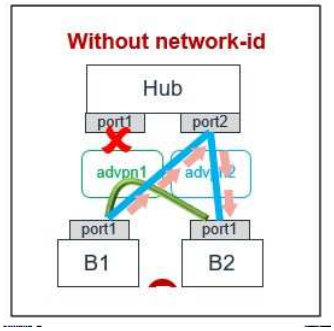
- **如果B1上的两条IPSec隧道配置了不同的Network-id：**将在Advpn2上的B1和B2之间建立advpn2上的Shortcut。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- advpn2和advpn1上的Shortcut隧道都建立在相同Underlay线路IP上：B1(port1) ↔ B2(port1)。
- 这两个相同Underlay源目IP的Shortcut隧道可以同时建立，因为每个Overlay IPSec隧道都配置了不同的network-id，B2可以根据不同的network-id来区分隧道并与之建立。
- BGP路由收敛后，B1访问B2的流量流经advpn2上的Shortcut传输。

- **如果B1上的两条IPSec隧道没有配置Network-id**：B2忽略B1在advpn2上的Shortcut隧道建立请求。



- 因为在相同的Underlay IP地址 B1(port1) ↔ B2(port1)上已经存在Shortcut隧道（基于advpn1）。如果不为每个Overlay隧道配置不同的Network-id，则B2无法区分两个advpn上的Shortcut并同时建立两个相同Underlay的Shortcut隧道。
- 只要B1对B2 Advpn1上的Shortcut隧道建立后，B1通过Advpn2向B2发送任何流量，都会通过Hub进行转发，因为此时advpn2上的Shortcut隧道无法建立。

7. 在Hub和Spoke上都要配置network-id，且每个线路上Hub和Spoke的network-id保持一致。

```bash
Hub:
config vpn ipsec phase1-interface
    edit "advpn1"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set network-overlay enable
        set network-id 1
         …
    next
    edit "advpn2"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set network-overlay enable
        set network-id 2
         …
    next
end

B1&B2:
config vpn ipsec phase1-interface
    edit "advpn1"
        set ike-version 2
        set interface "port1"
        set remote-gw x.x.x.x
        set network-overlay enable
        set network-id 1
         …
    next
 edit "advpn2"
        set ike-version 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set interface "port1"
        set remote-gw y.y.y.y
        set network-overlay enable
        set network-id 2
        ...
    next
end
```

8. 对于IKEv1，IKEv1并不支持network-id。但也可以通过如下两种方式部署上述的ADVPN场景：

   - ADVPN隧道可以部署为IKEv1的野蛮模式，Spoke之间相同Underlay IP的Shortcut可以通过配置不同的野蛮模式ID来进行区分。
   - 使用IKEv1的主模式/野蛮模式，并不配置ID。通过开启Shortcut隧道与父隧道的绑定关系，当Shortcut隧道的父隧道中断后，所有关联的Shortcut隧道会一起关闭。这样就不会出现上述Spoke之间同时存在两个Shortcut需要建立的情况，这个配置需要在Spoke上的IPSec一阶段配置（`set auto-discovery-shortcuts dependent`）：

```bash
config vpn ipsec phase1-interface
    edit "advpn1"
        set ike-version 1
        set interface "port1"
        set remote-gw x.x.x.x
        set auto-discovery-receiver enable
        set auto-discovery-shortcuts dependent    //Shortcut隧道状态依赖父隧道状态，默认为independent//
        ...
    next
 edit "advpn2"
        set ike-version 1
        set interface "port1"
        set remote-gw y.y.y.y
        set auto-discovery-receiver enable
        set auto-discovery-shortcuts dependent    //Shortcut隧道状态依赖父隧道状态，默认为independent//
        ...
    next
end
```

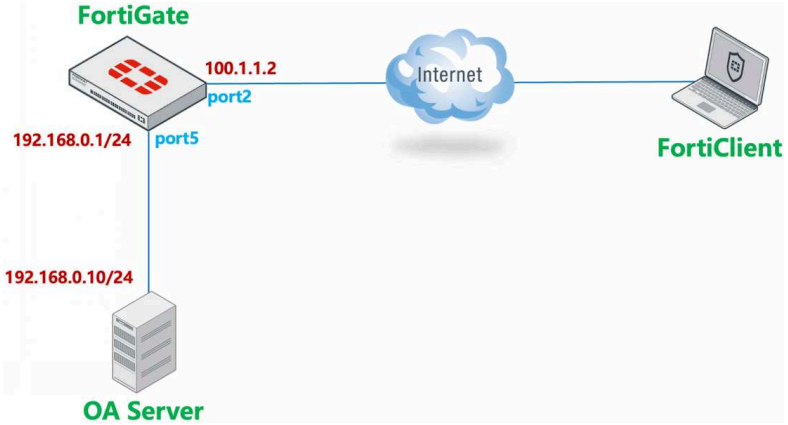

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiClient拨号

网络需求

某公司内部有一台OA服务器，在外移动办公的工作人员需要通过IPSEC VPN拨入到公司内网来对内网服OA服务器进行访问。

网络拓扑

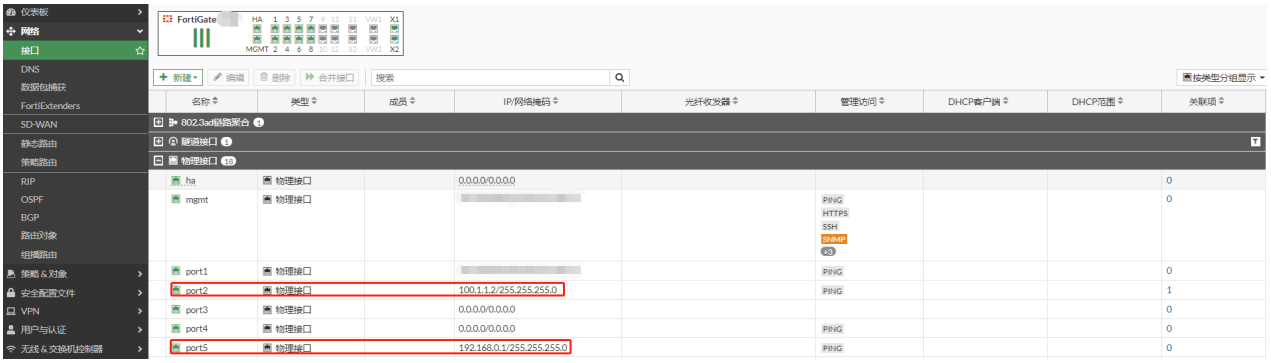


配置步骤

配置IPSec

1. 基本配置

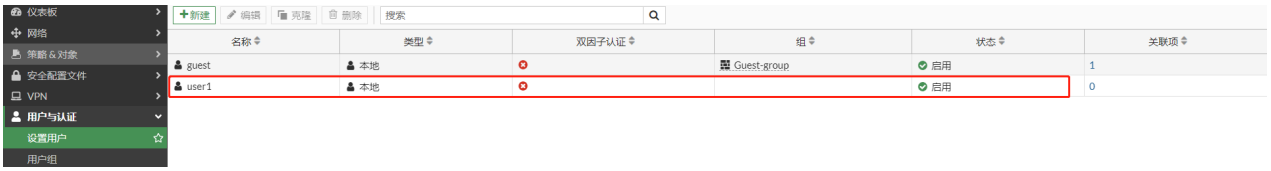
配置接口IP和路由





2. 创建用户

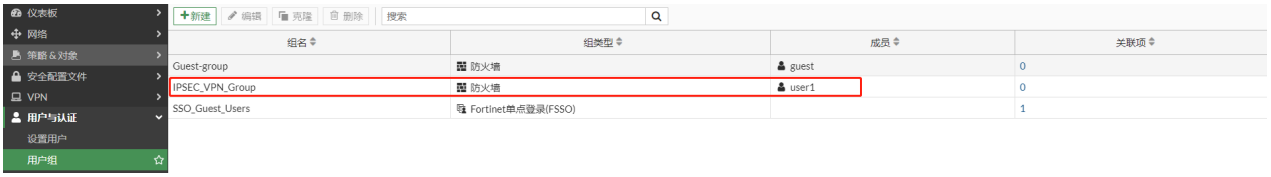
选择“用户与认证”-->“设置用户”，创建本地用户。



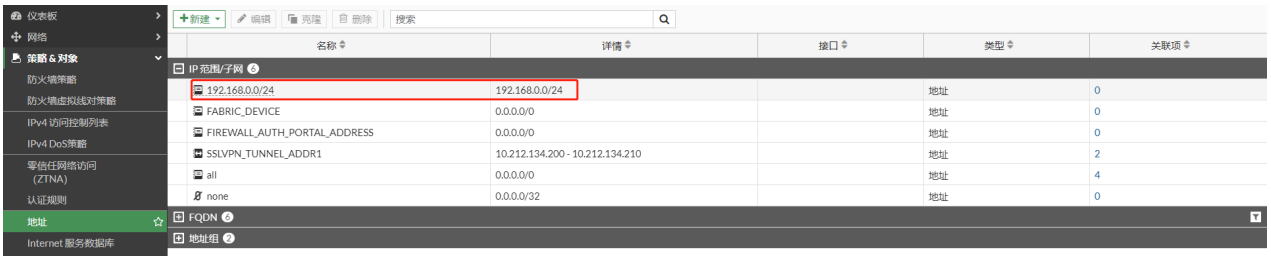
3. 创建用户组

选择“用户与认证”-->“用户组”，点击“新建”，创建本地用户组。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

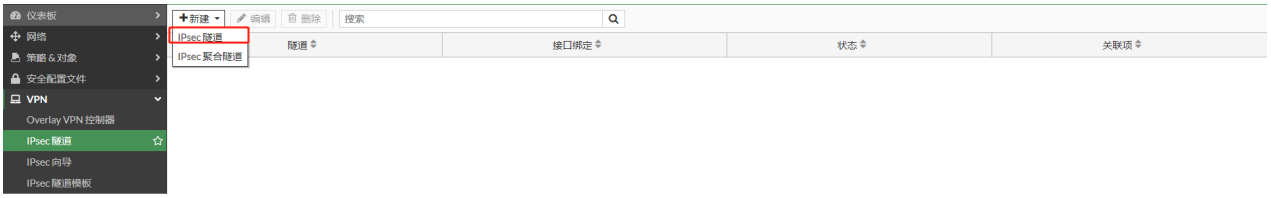


4. 创建子网



5. 配置IPSEC VPN

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



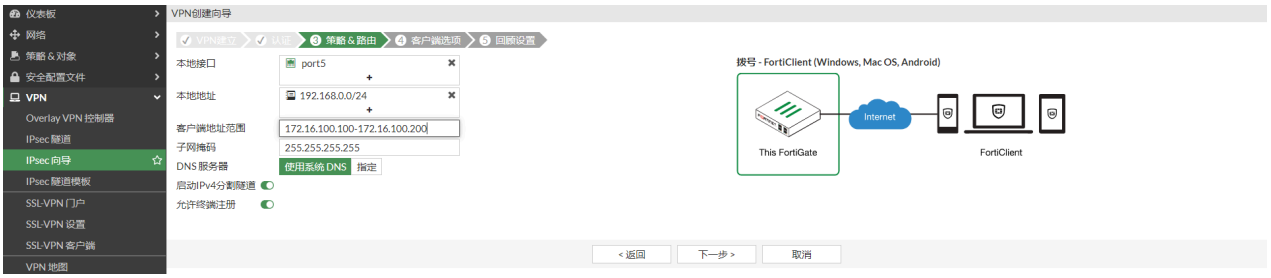
根据“VPN创建向导”进行VPN模板配置，输入名称，选择”远程接“-->"基于客户端"-->“FortiClient”，并点击下一步。



选择对外的接口，设置预共享秘钥和用户组，并点击下一步。



输入内网接口，允许访问的本地地址段，客户端拨号后获取的地址范围，并点击下一步。



保存密码，FortiClient第一次拨号成功后，FortiClient会显示“保存密码”的选项，默认勾选。

自动连接，FortiClient第一次拨号成功后，FortiClient会显示“自动连接”的选项，该功能是运行FortiClient会拨入该IPSEC VPN。

保持存活，FortiClient第一次拨号成功后，FortiClient会显示“保持连接”的选项，该功能是IPSEC VPN由于网络原因中断后，会自动重拨。

免费的FortiClient版本不支持自动连接和保持连接，需要完整版的FortiClient，需要购买EMS license。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN创建向导提示即将创建的内容，然后点击完成。



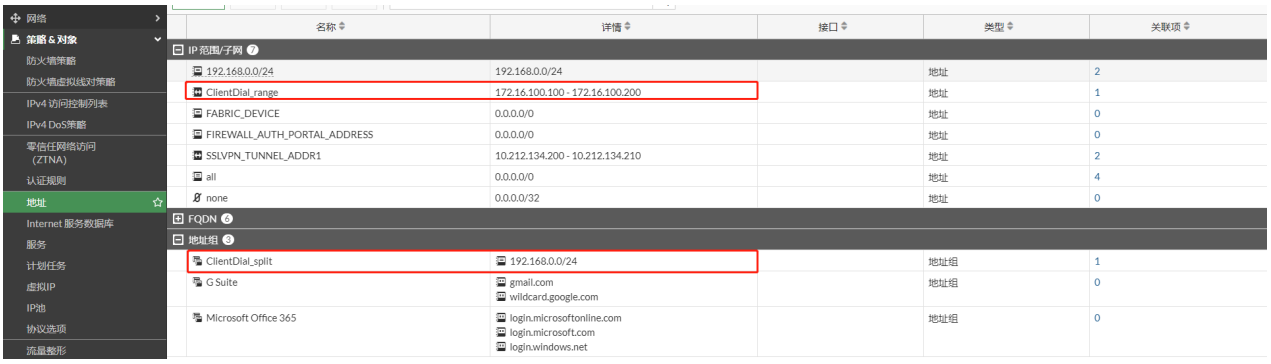
VPN创建成功。



查看IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建地址对象和地址对象组。



2. 创建IPSEC VPN



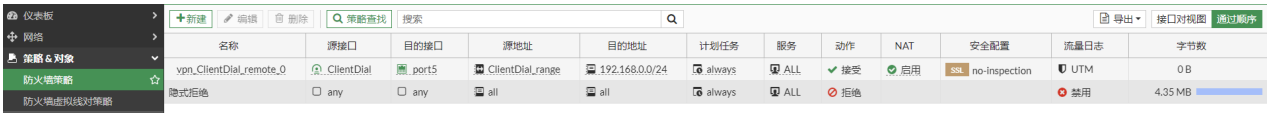
对应的命令行

```
config vpn ipsec phase1-interface
    edit "ClientDial"
        set type dynamic
        set interface "port2"
        set mode aggressive
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

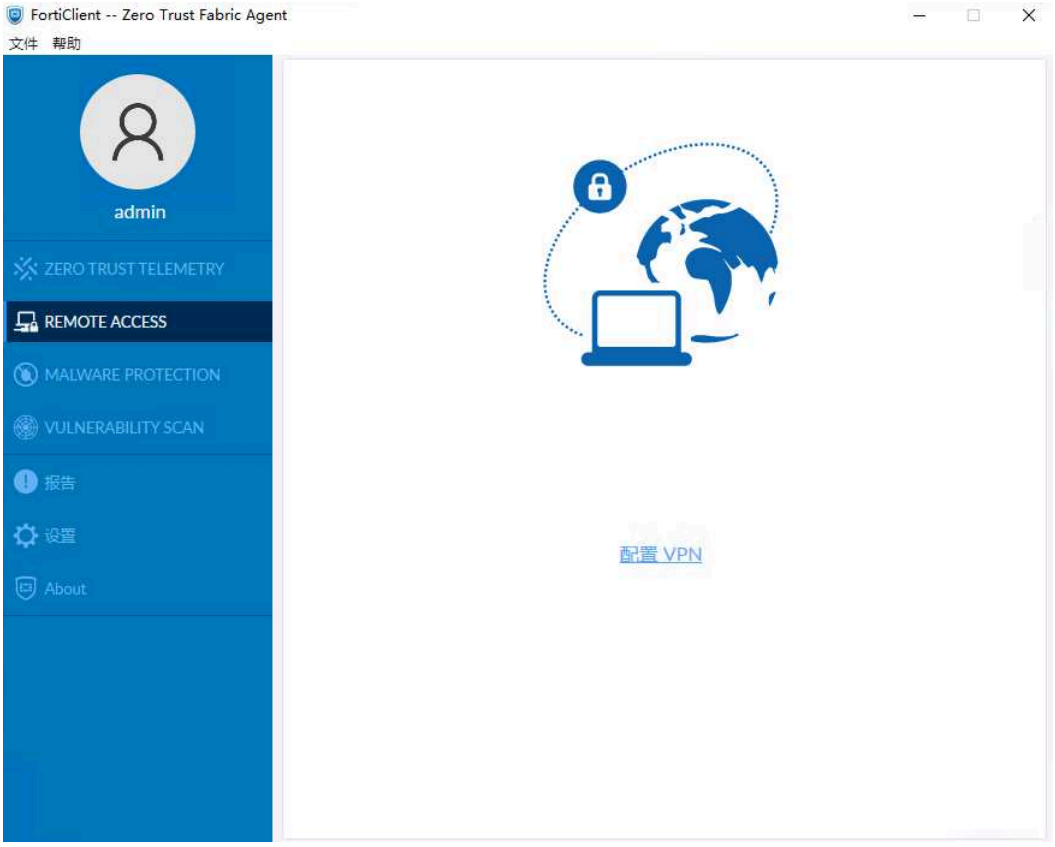
```
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: ClientDial (Created by VPN wizard)"
        set wizard-type dialup-forticlient
        set xauthtype auto
        set authusrgrp "IPSEC_VPN_Group"
        set ipv4-start-ip 172.16.100.100
        set ipv4-end-ip 172.16.100.200
        set dns-mode auto
        set ipv4-split-include "ClientDial_split"
        set save-password enable
        set psksecret ENC
cTt0jnn1i1wx0Elky0oa0pRS3I7Kb8UAUHRndju/6cI7nbcQ1IBcmXqdj9aJXjE/ZNUZgElJLwKARXoP3iJPBAkWJaYtQrEC+XfZC2QGr/Xsw72UQS
L0Rll8wIKAk7vPDIQXbn/eQSYPs7CH+2r64HiKJ91+zt3LzAlASNooXPKea8EK7f9qaUTfj/p/kxqrk9aN6A==
    next
end

config vpn ipsec phase2-interface
    edit "ClientDial"
        set phase1name "ClientDial"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: ClientDial (Created by VPN wizard)"
    next
end
```

3. 创建策略。



配置FortClient

1. 选择“Remote Access”，点击“配置VPN”。



2. 输入连接名，远程网关，共享秘钥，以及用户名，然后点击“保存”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



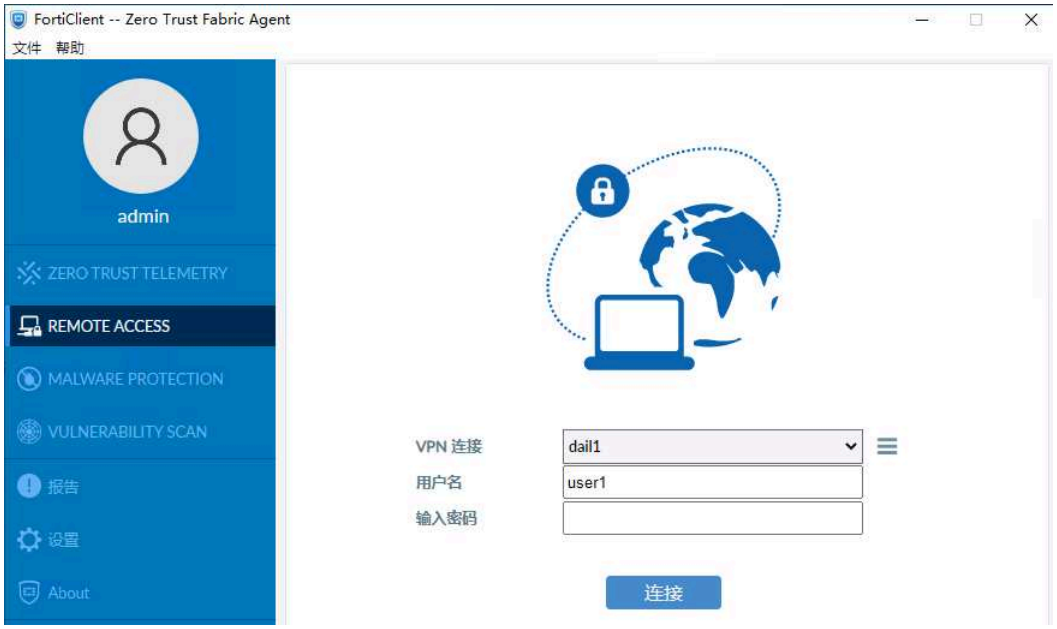
在”高级设置“有更多的选项，如ike版本，IKE阶段一和阶段二的加密集等，可以根据FortiGate的设置做对应的修改。





3. VPN配置完成

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortClient拨号测试

1. 在FortiClient中输入账号密码，点击“连接”，FortiClient拨号成功。



2. 查看终端路由表，192.168.0.0/24指向IPSEC VPN，并能成功访问OA Server。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

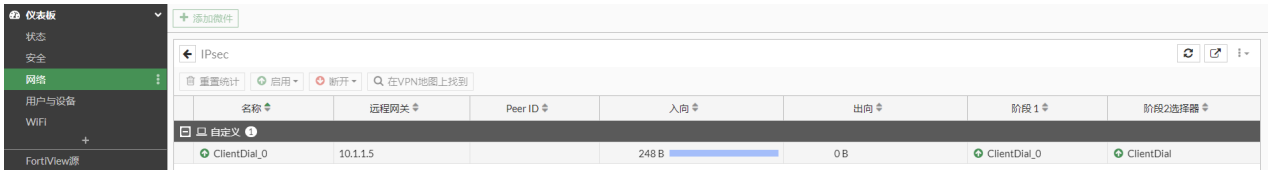
命令提示符

```
C:\Users\admin>route print
===========================================================================
接口列表
  5...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
  9...00 0c 29 a2 90 e0 ......Intel(R) 82574L Gigabit Network Connection
  4...00 0c 29 a2 90 ea ......Intel(R) 82574L Gigabit Network Connection #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0        10.1.1.1        10.1.1.5    281
         10.1.1.0    255.255.255.0         在链路上         10.1.1.5    281
         10.1.1.5  255.255.255.255         在链路上         10.1.1.5    281
       10.1.1.255  255.255.255.255         在链路上         10.1.1.5    281
        100.1.1.2  255.255.255.255        10.1.1.1        10.1.1.5     25
        127.0.0.0        255.0.0.0         在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
      169.254.1.1  255.255.255.255   172.16.100.101   172.16.100.100      1
    172.16.100.100  255.255.255.255         在链路上     172.16.100.100    257
      192.168.0.0    255.255.255.0   172.16.100.101   172.16.100.100      1
     192.168.89.0    255.255.255.0         在链路上      192.168.89.37    281
    192.168.89.37  255.255.255.255         在链路上      192.168.89.37    281
   192.168.89.255  255.255.255.255         在链路上      192.168.89.37    281
        224.0.0.0        240.0.0.0         在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上     172.16.100.100    257
        224.0.0.0        240.0.0.0         在链路上      192.168.89.37    281
        224.0.0.0        240.0.0.0         在链路上         10.1.1.5    281
  255.255.255.255  255.255.255.255         在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上     172.16.100.100    257
  255.255.255.255  255.255.255.255         在链路上      192.168.89.37    281
  255.255.255.255  255.255.255.255         在链路上         10.1.1.5    281
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址  跃点数
          0.0.0.0          0.0.0.0        10.1.1.1     默认
```

命令提示符

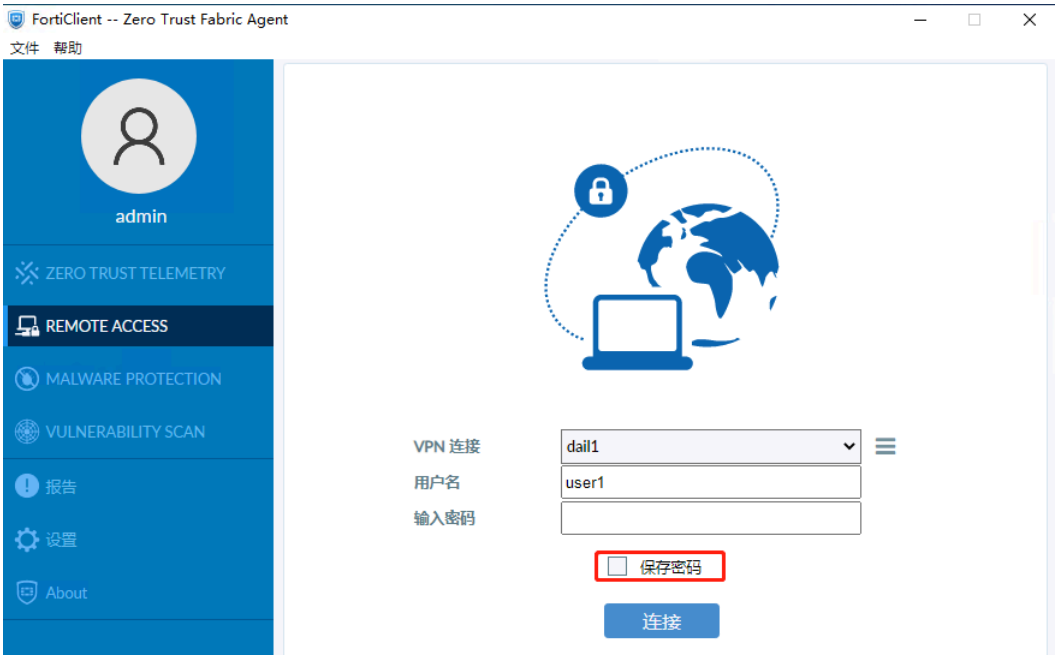
```
C:\Users\admin>ping 192.168.0.10

正在 Ping 192.168.0.10 具有 32 字节的数据:
来自 192.168.0.10 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.0.10 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.0.10 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.0.10 的回复: 字节=32 时间<1ms TTL=63

192.168.0.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

3. FortiGate查看client连接。



4. 点击“中断连接”，FortiClient就会显示“保存密码”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



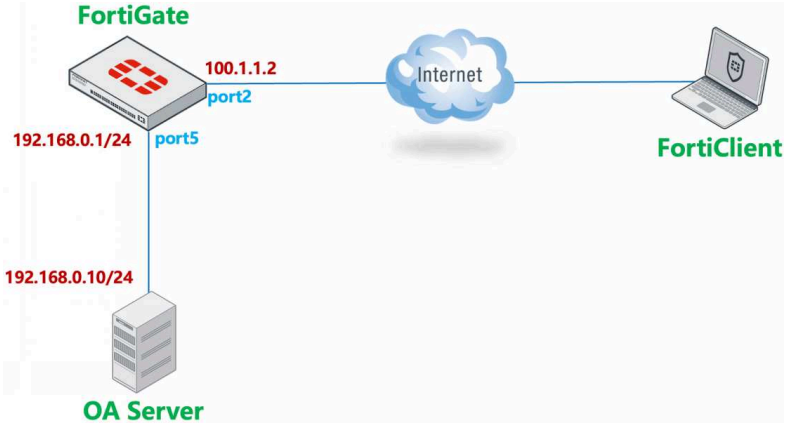
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiClient使用证书认证连接IPSec

网络需求

某公司内部有一台OA服务器，在外移动办公的工作人员需要通过vpn,拨入到公司内网来对内网服OA服务器进行访问，采用证书认证的方式。

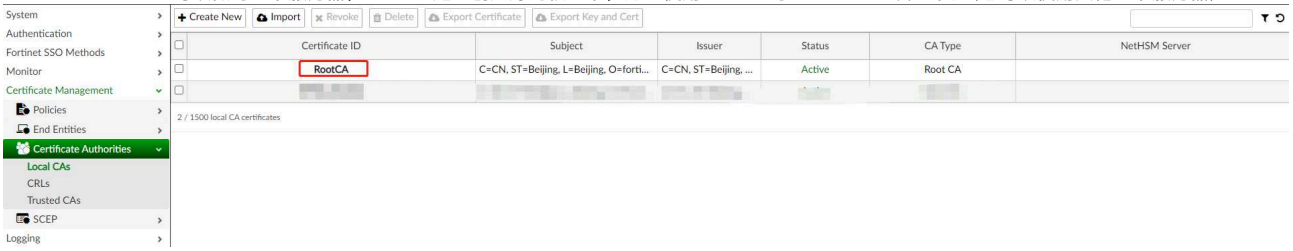
网络拓扑



配置步骤

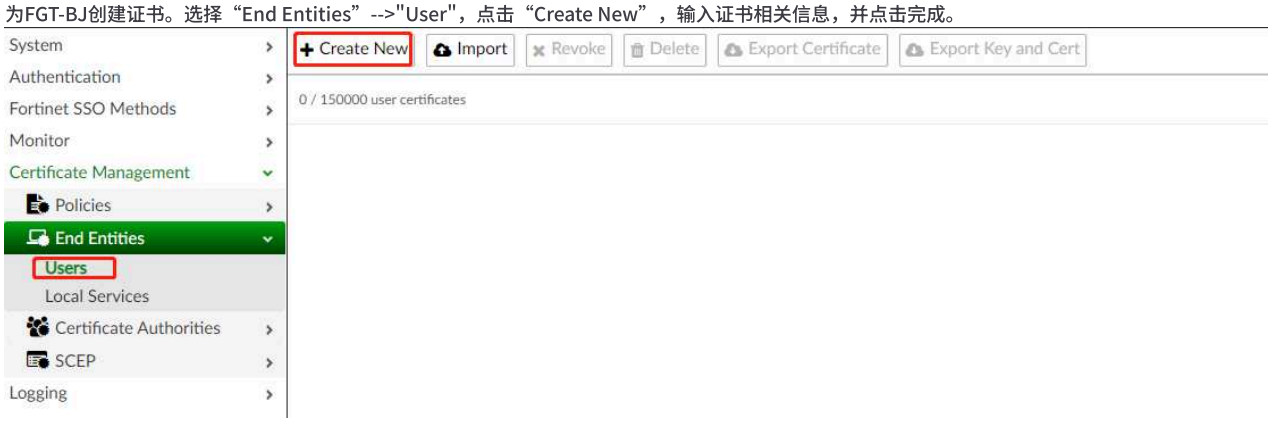
使用FortiAuthenticator为FGT-BJ和终端颁发证书

FortiAuthenticator可以做为证书服务器，RootCA是已创建好的根证书，这里使用RootCA为FortiGate签发证书。（也可以使用其他证书服务器）

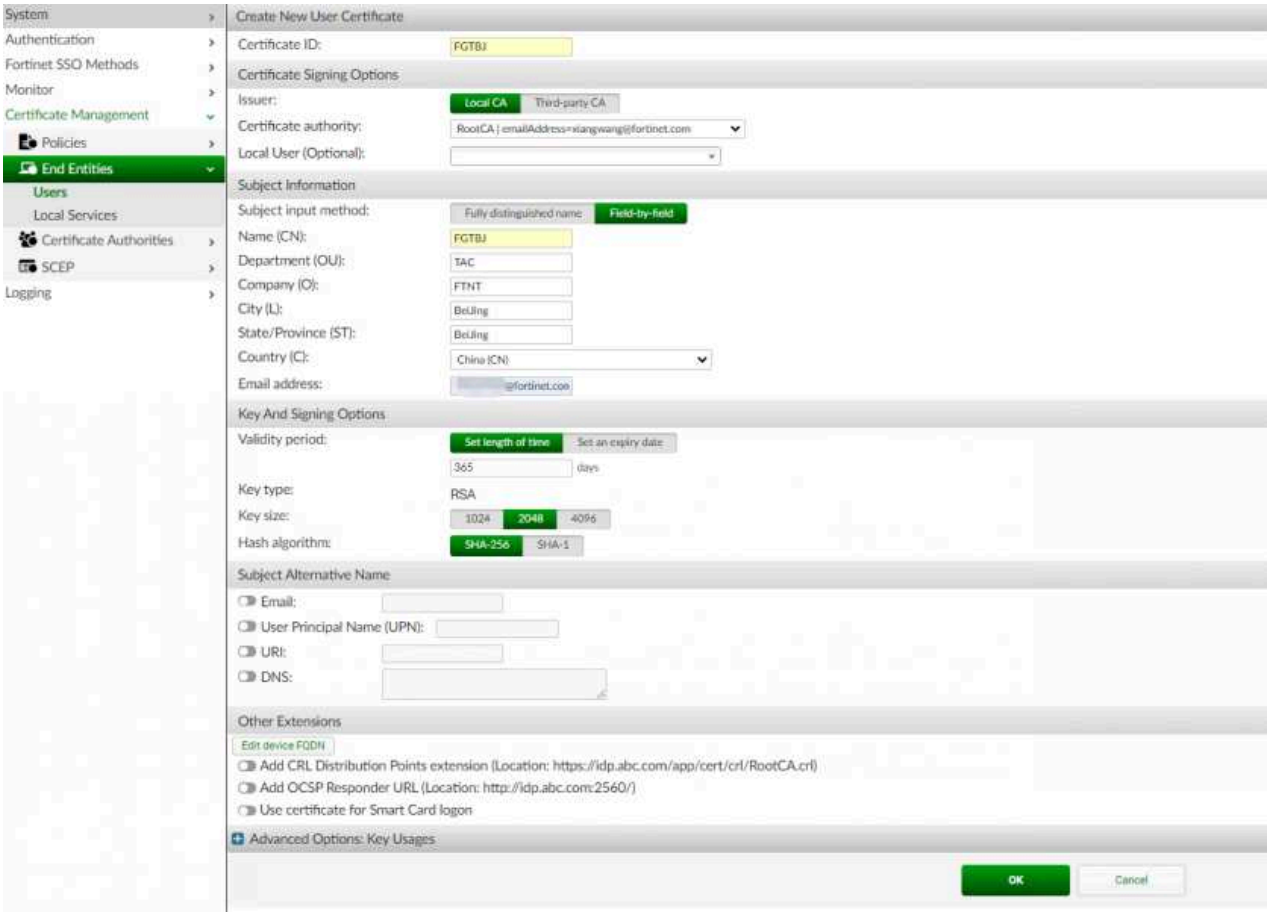


1. 为FGT-BJ颁发证书

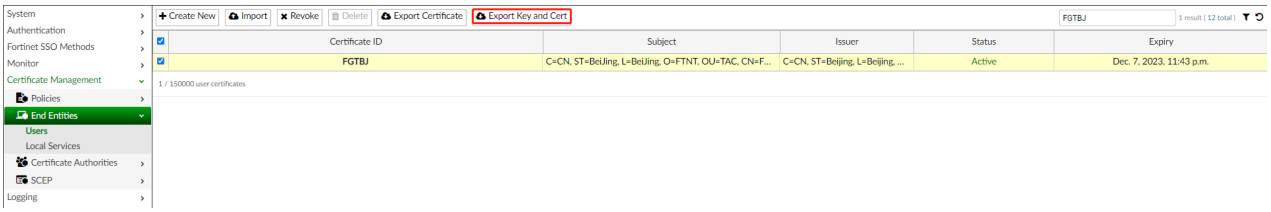
为FGT-BJ创建证书。选择“End Entities”-->"User"，点击“Create New”，输入证书相关信息，并点击完成。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击“Export Key and Cert”导出FGTBJ证书的私钥和公钥。



输入一个密码保护私钥



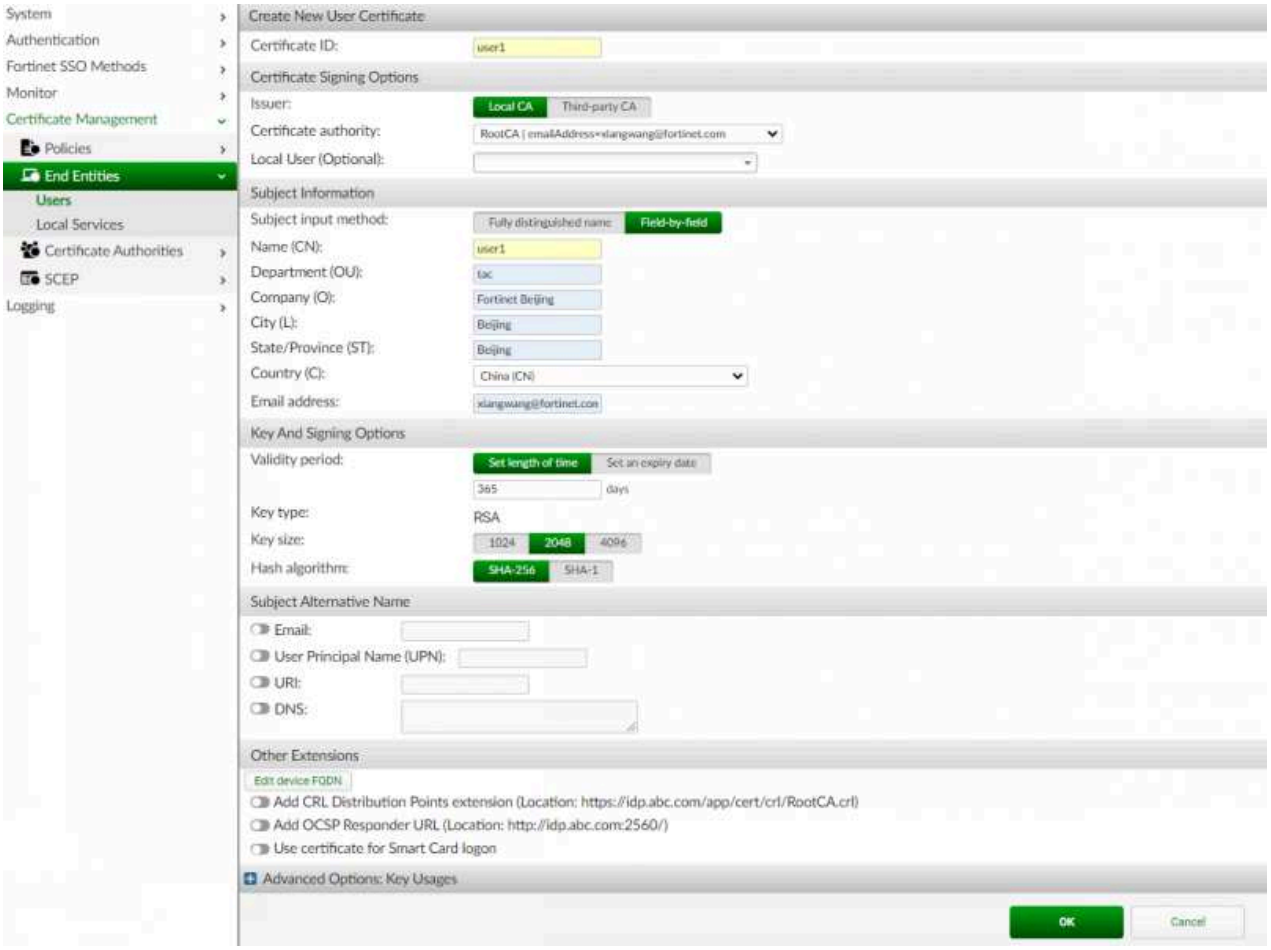
下载证书

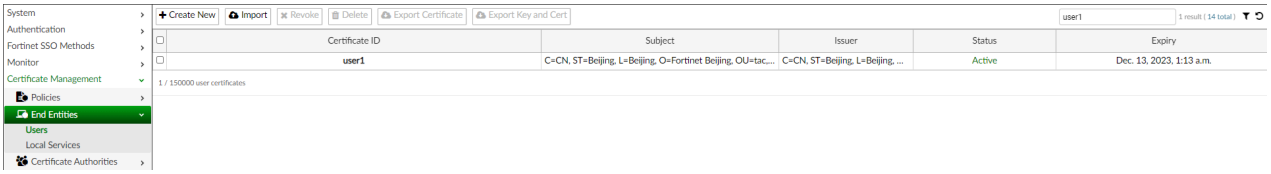
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 为终端颁发证书

为终端颁发证书和上述步骤是一样的。





FortiGate导入证书

将根证书RootCA.crt和证书FGTBJ.p12导入到FGT_BJ。

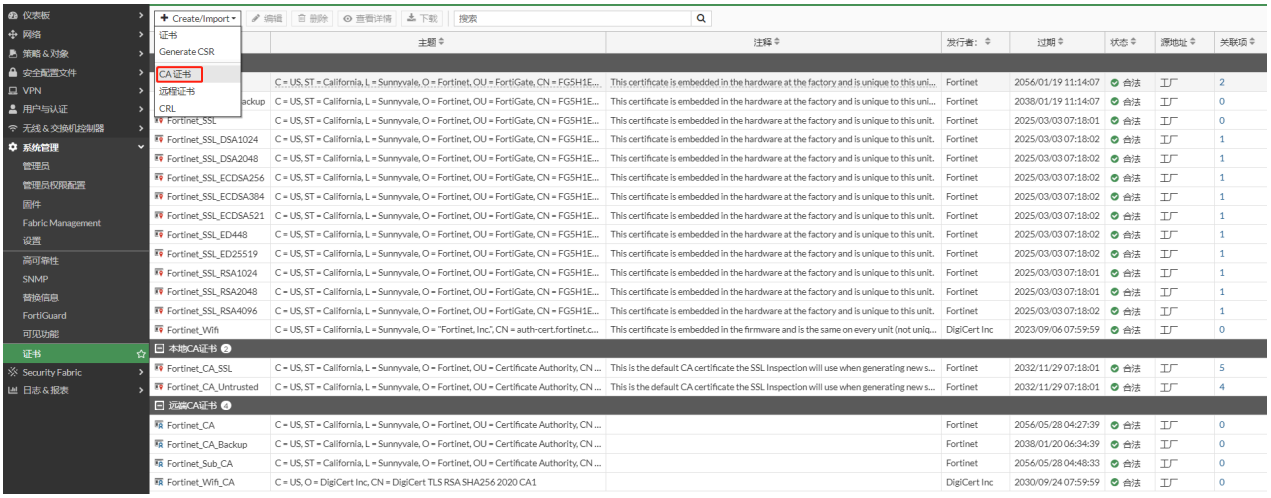
在数字证书认证中，通信双方使用CA证书进行数字证书合法性验证，双方各有自己的公钥（网络上传输）和私钥（本地存储）。发送方对报文进行Hash计算，并用自己的私钥对报文计算结果进行加密，生成数字签名。接收方使用发送方的公钥对数字签名进行解密，并对报文进行Hash计算，判断计算结果与解密后的结果是否相同。如果相同，则认证通过；否则认证失败。

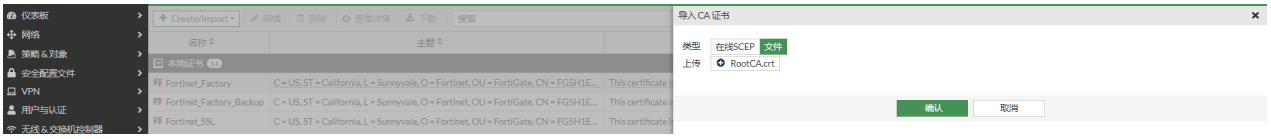
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



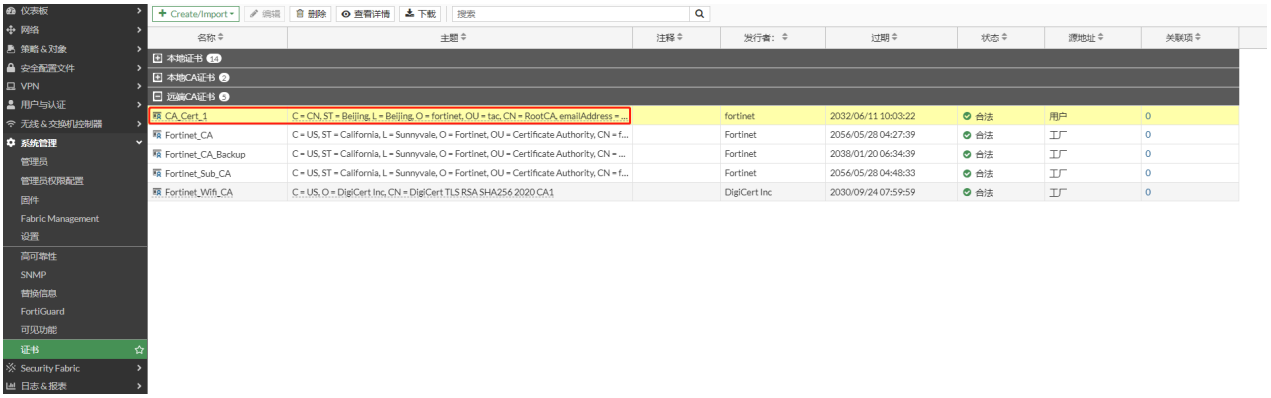
1. 导入CA证书

选择“系统管理”-->“证书”，点击“Create/Import”，选择CA证书。





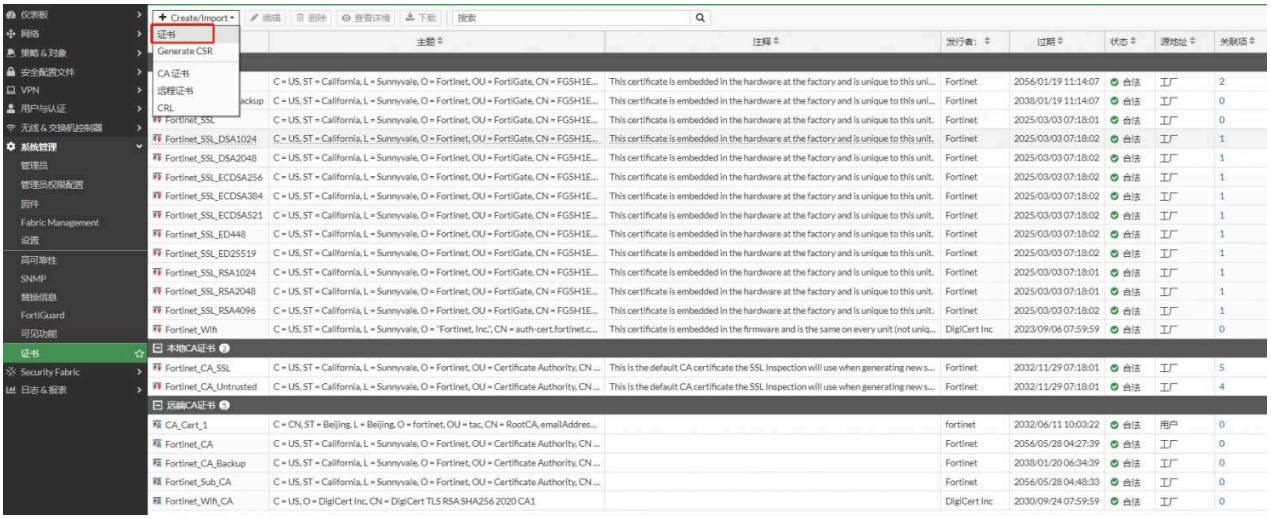
查看导入的CA证书



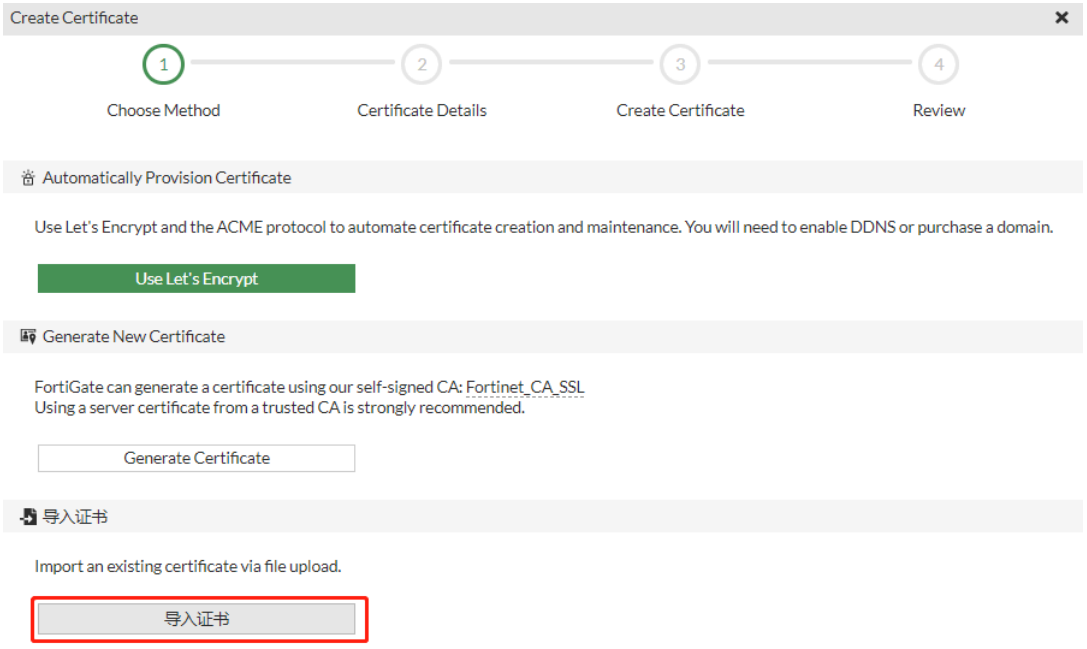
2. 导入本地证书

选择“系统管理”-->“证书”，点击“Create/Import”，选择“证书”。

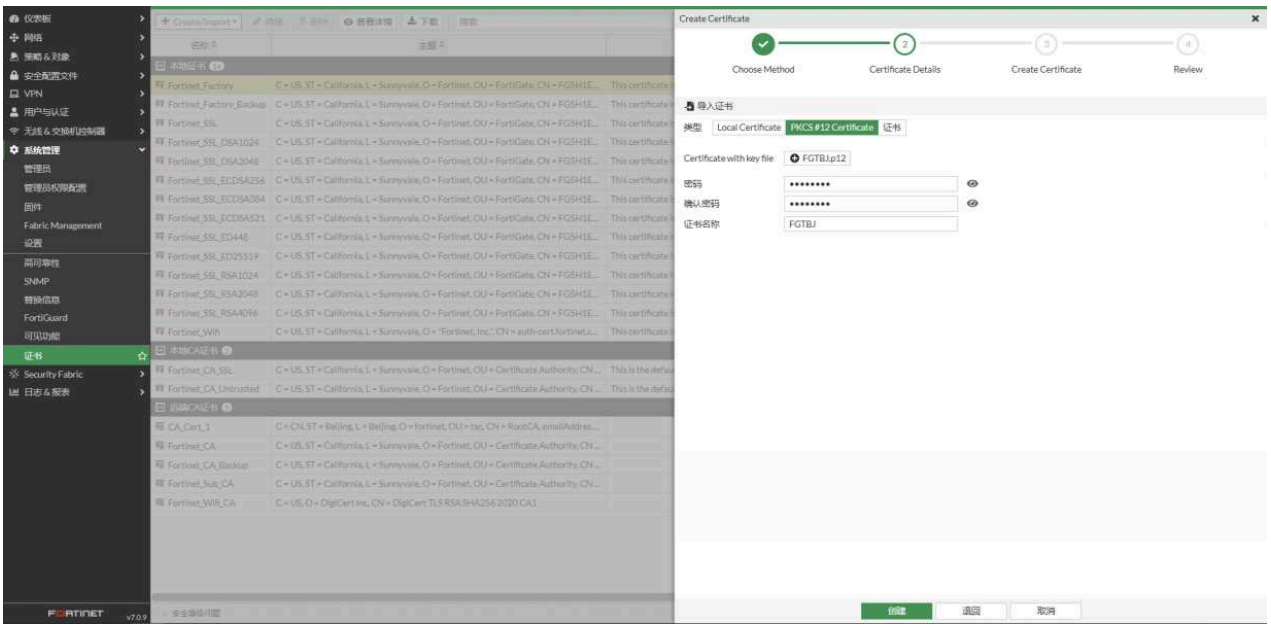
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击导入证书

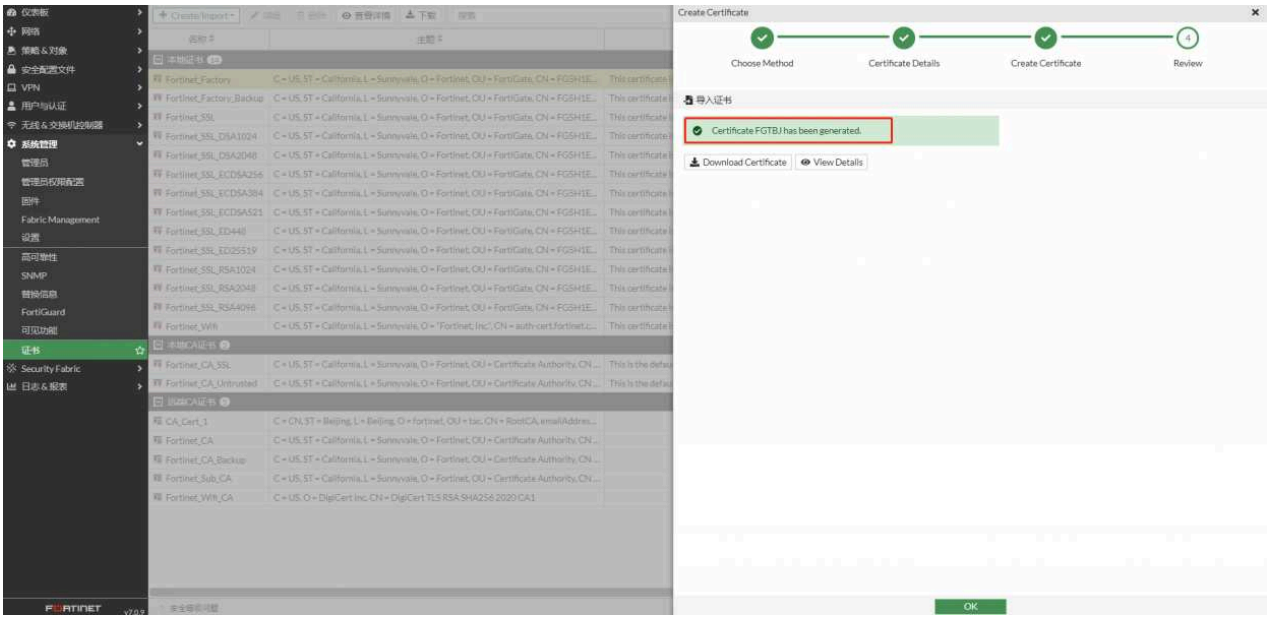


输入证书的密码，点击“创建”

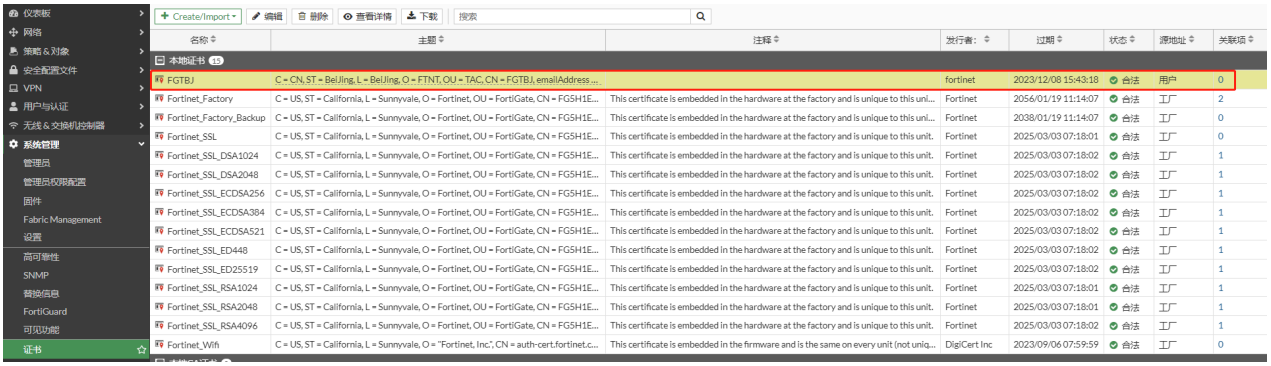


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

提示证书已成功导入



查看导入的本地证书



终端导入证书

将根证书RootCA.crt和证书user1.p12导入到终端。



1. 导入根证书RootCA.crt

双击RootCA.crt，点击“安装证书”。

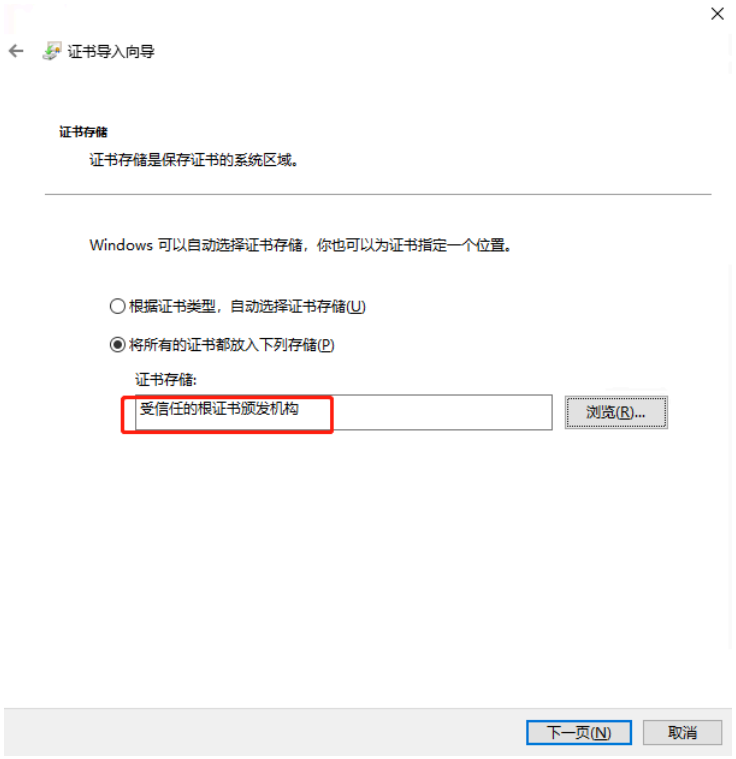
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

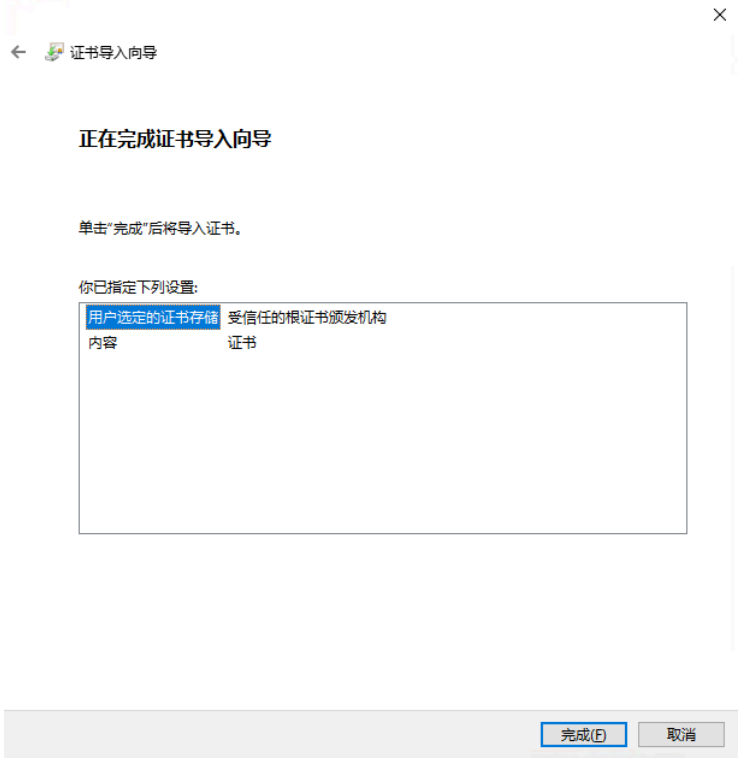




证书存入“受信任的根证书颁发机构”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

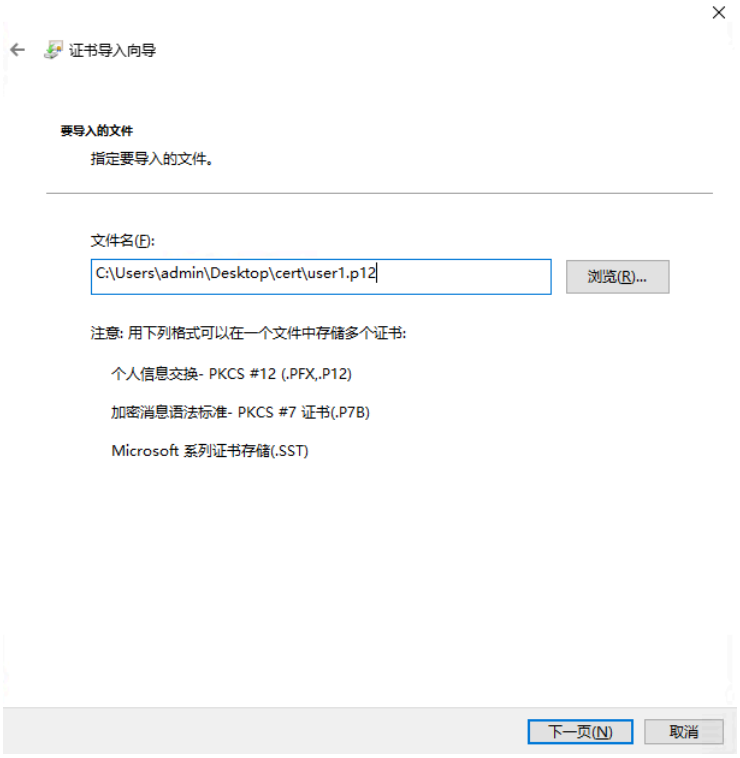




2. 导入个人证书user1.p12

   双击user1.p12，然后安装证书

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

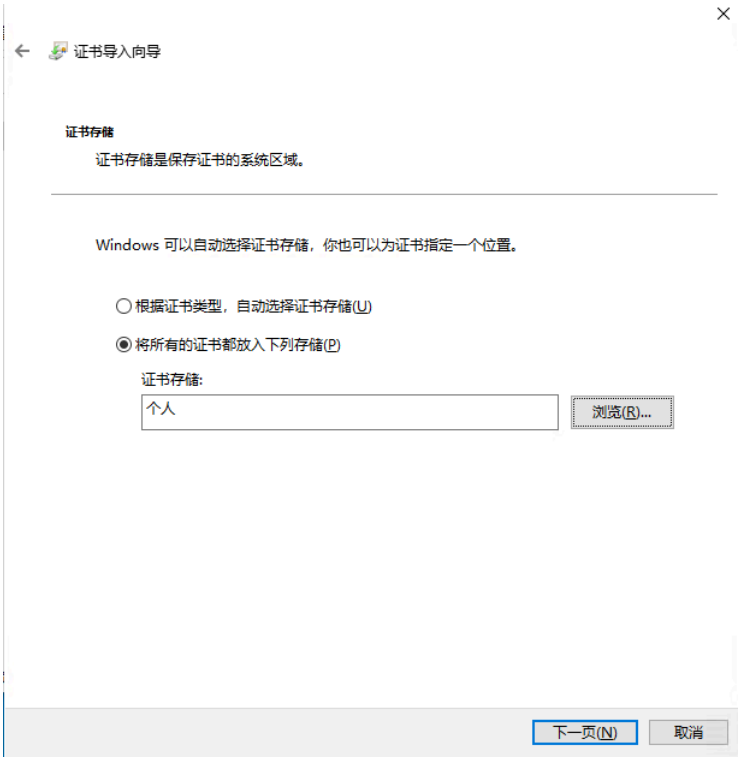


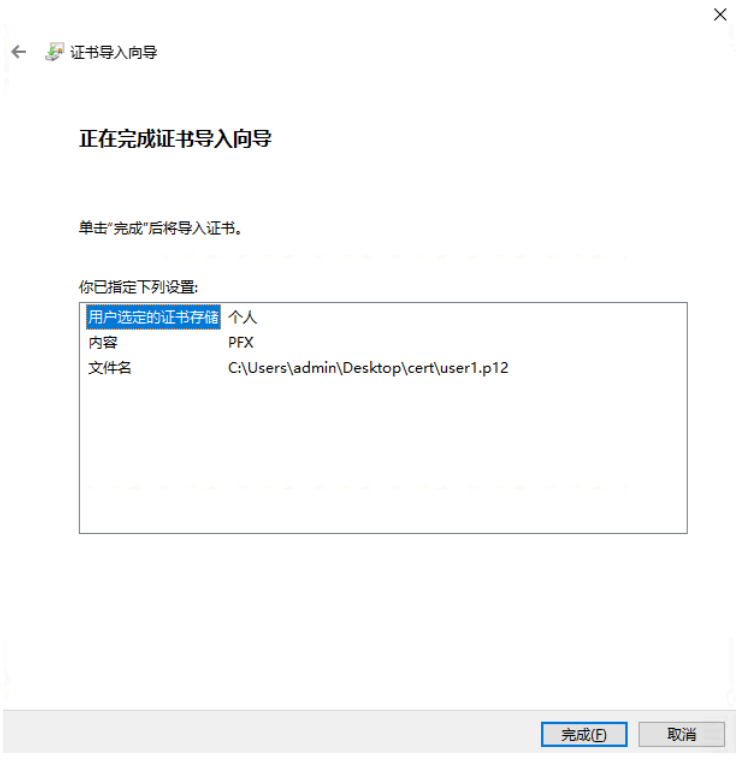
输入证书的密码



证书存入“个人”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



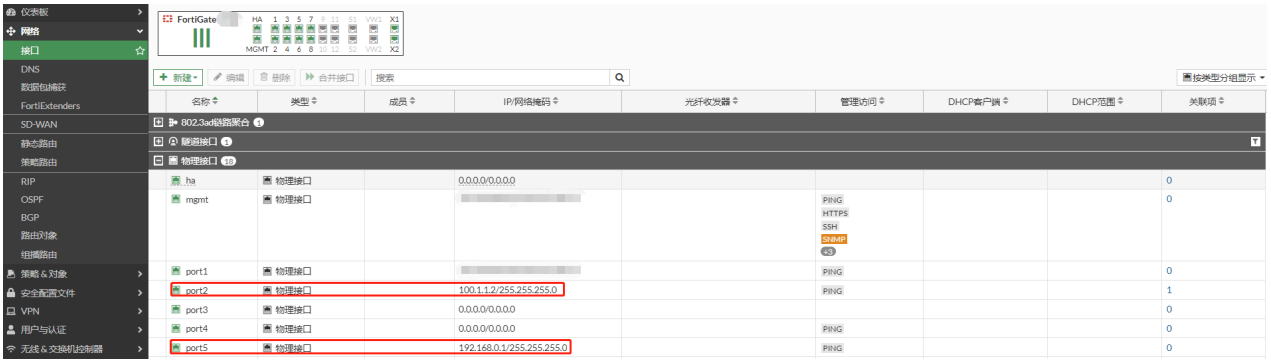


IPSEC VPN配置步骤

1. **基本配置**

   配置接口IP和路由

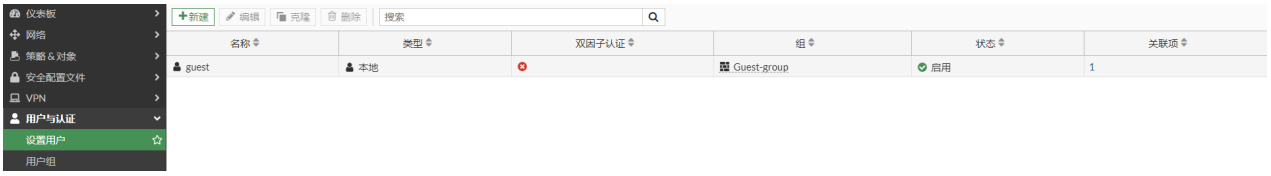
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 创建用户

选择“用户与认证”-->“设置用户”，点击“新建”。



选择“本地用户”，点击“下一步”。



输入用户名和密码，点击“下一步”。

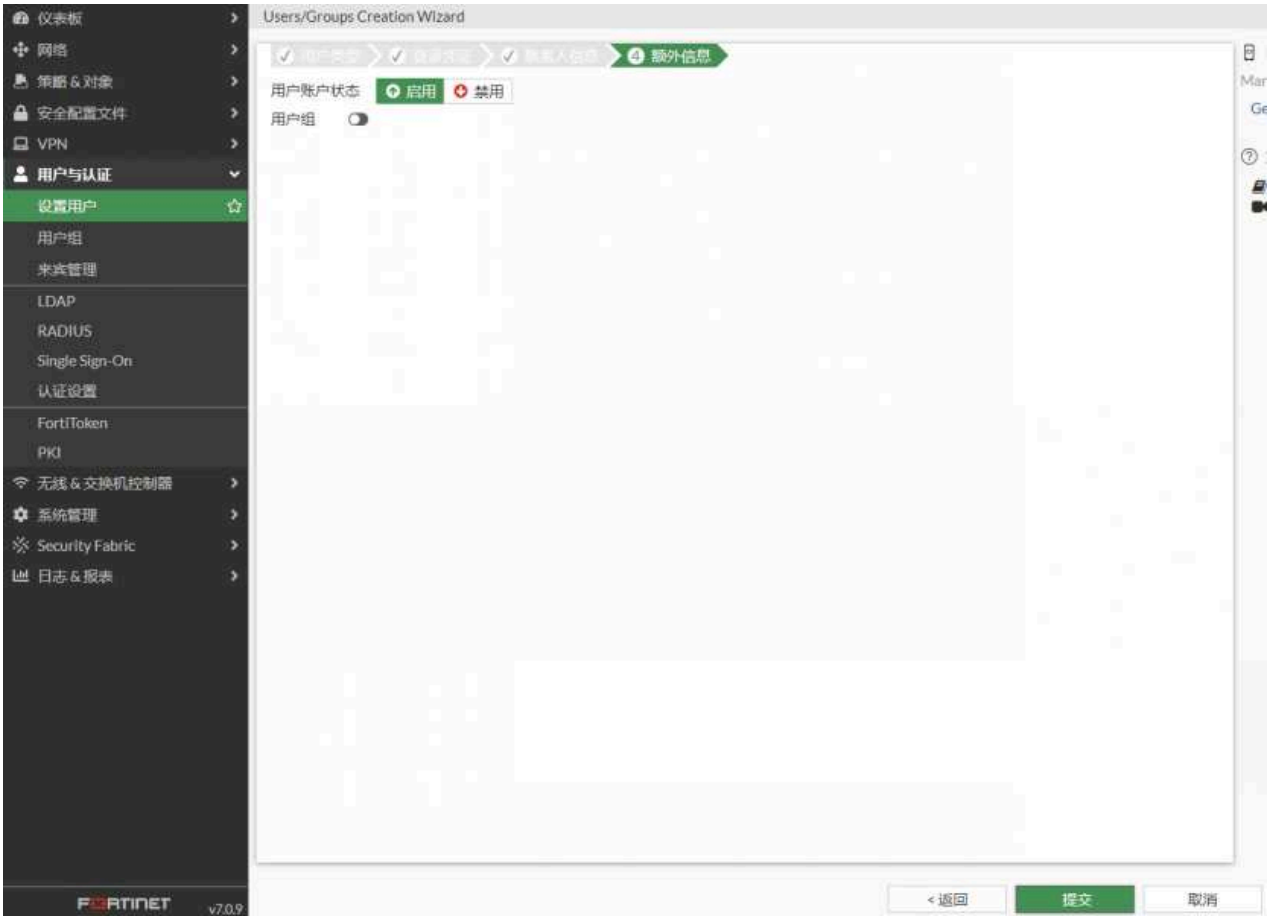


可根据需求选择启用。这里不启用，点击“下一步”。

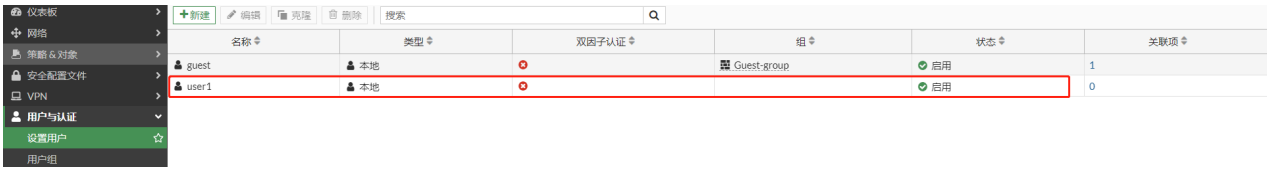


点击“提交”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

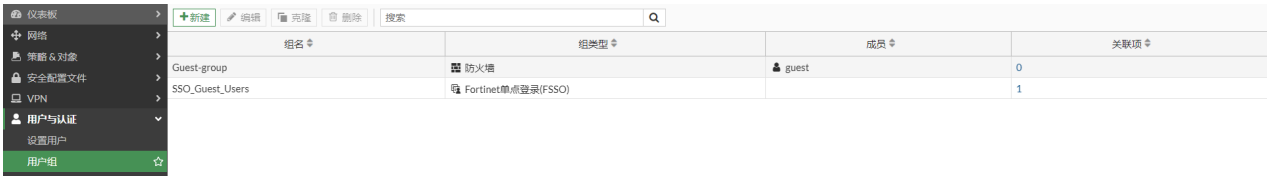


完成用户创建。



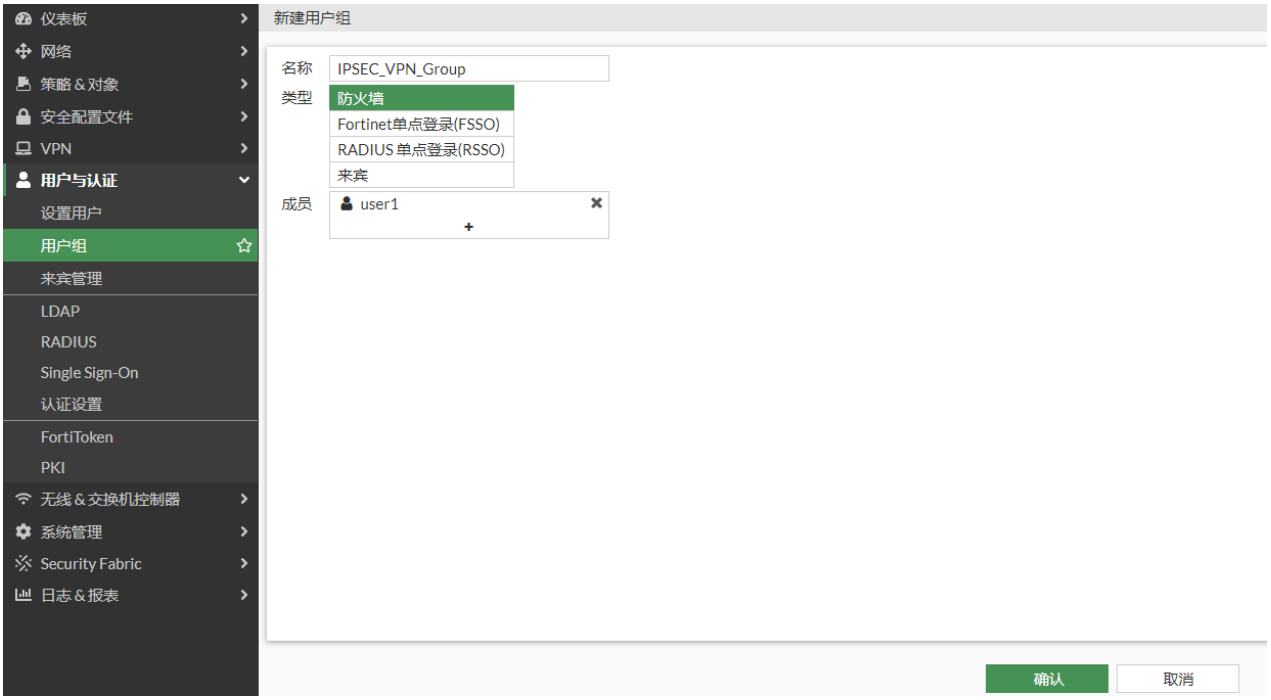
3. 创建用户组

选择“用户与认证”-->“用户组”，点击“新建”。

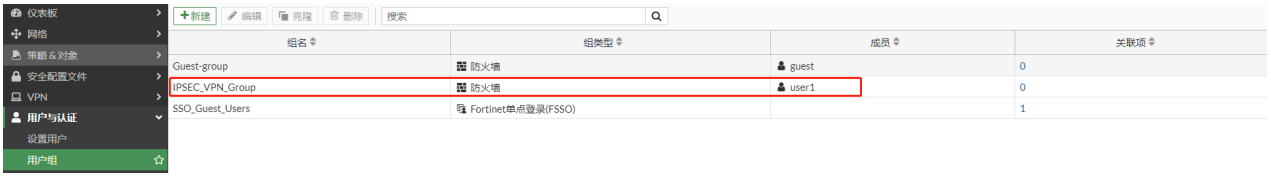


输入名称，即组名，并将用户加入用户组，点击“确认”。

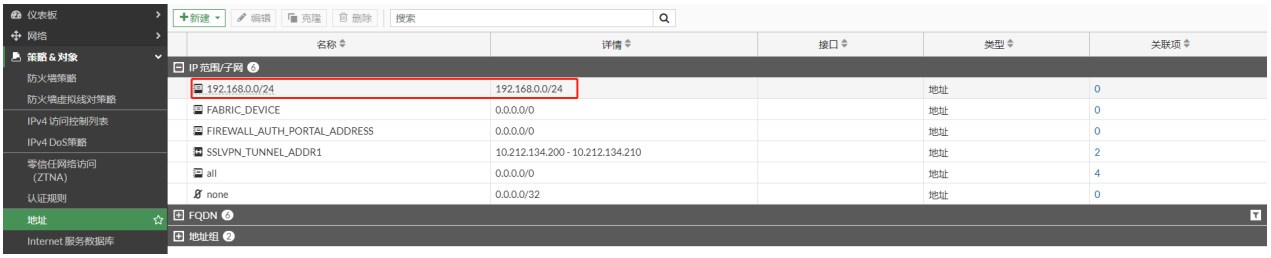
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



完成用户组创建。

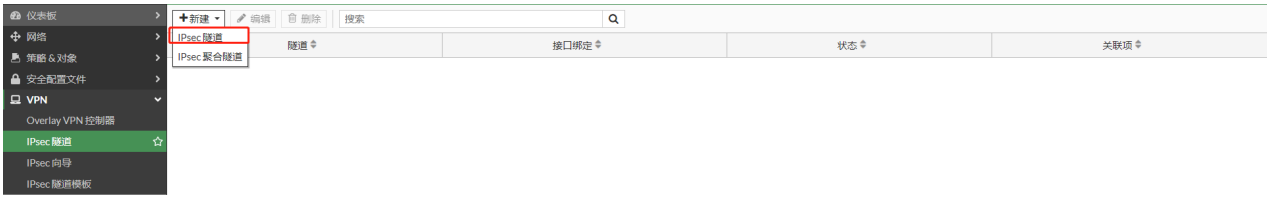


4. 创建子网



5. 配置IPSEC VPN

选择“VPN”-->“IPsec隧道”，点击“新建”，选择“IPsec隧道”。



根据“VPN创建向导”进行VPN模板配置，输入名称，选择”远程接“-->"基于客户端"-->“FortiClient”，并点击下一步。

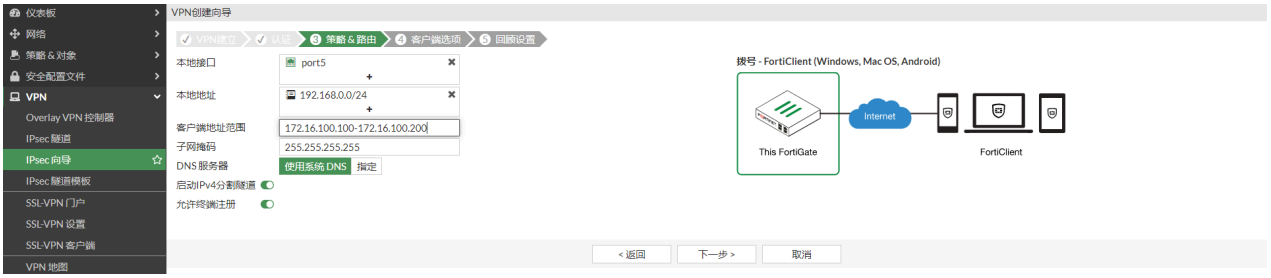


选择对外的接口，用户组，证书名是本地的证书FGTBJ，对端证书CA是导入的RootCA，即CA_Cert_1，并点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



输入内网接口，允许访问的本地地址段，客户端拨号后获取的地址范围，并点击下一步。



保存密码，FortiClient第一次拨号成功后，FortiClient会显示“保存密码”的选项，默认勾选。

自动连接，FortiClient第一次拨号成功后，FortiClient会显示“自动连接”的选项，该功能是运行FortiClient会拨入该IPSEC VPN。

保持存活，FortiClient第一次拨号成功后，FortiClient会显示“保持连接”的选项，该功能是IPSEC VPN由于网络原因中断后，会自动重拨。

免费的FortiClient版本不支持自动连接和保持连接，需要完整版的FortiClient，需要购买EMS license。



VPN创建向导提示即将创建的内容，然后点击完成。



VPN创建成功。

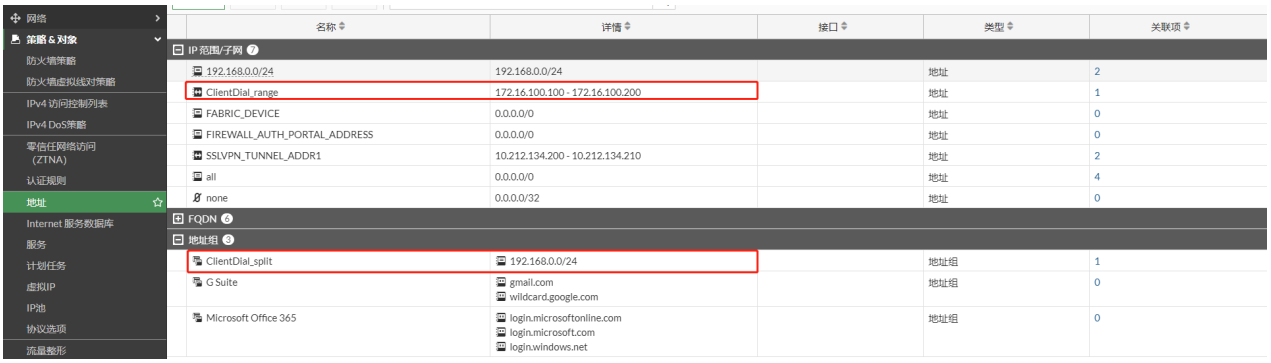


查看IPSEC向导创建的配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

1. 创建地址对象和地址对象组。



2. 创建PKI对象

```
config user peer
    edit "ClientDial_peer"
        set ca "CA_Cert_1"
    next
end
```

3. 创建IPSEC VPN



对应的命令行

```
config vpn ipsec phase1-interface
    edit "ClientDial"
        set type dynamic
        set interface "port2"
        set authmethod signature
        set mode aggressive
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set comments "VPN: ClientDial (Created by VPN wizard)"
        set wizard-type dialup-forticlient
        set xauthtype auto
        set authusrgrp "IPSEC_VPN_Group"
        set certificate "FGTBJ"
        set peer "ClientDial_peer"
        set ipv4-start-ip 172.16.100.100
        set ipv4-end-ip 172.16.100.200
        set dns-mode auto
        set ipv4-split-include "ClientDial_split"
        set save-password enable
    next
end
config vpn ipsec phase2-interface
    edit "ClientDial"
        set phase1name "ClientDial"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set comments "VPN: ClientDial (Created by VPN wizard)"
    next
end
```

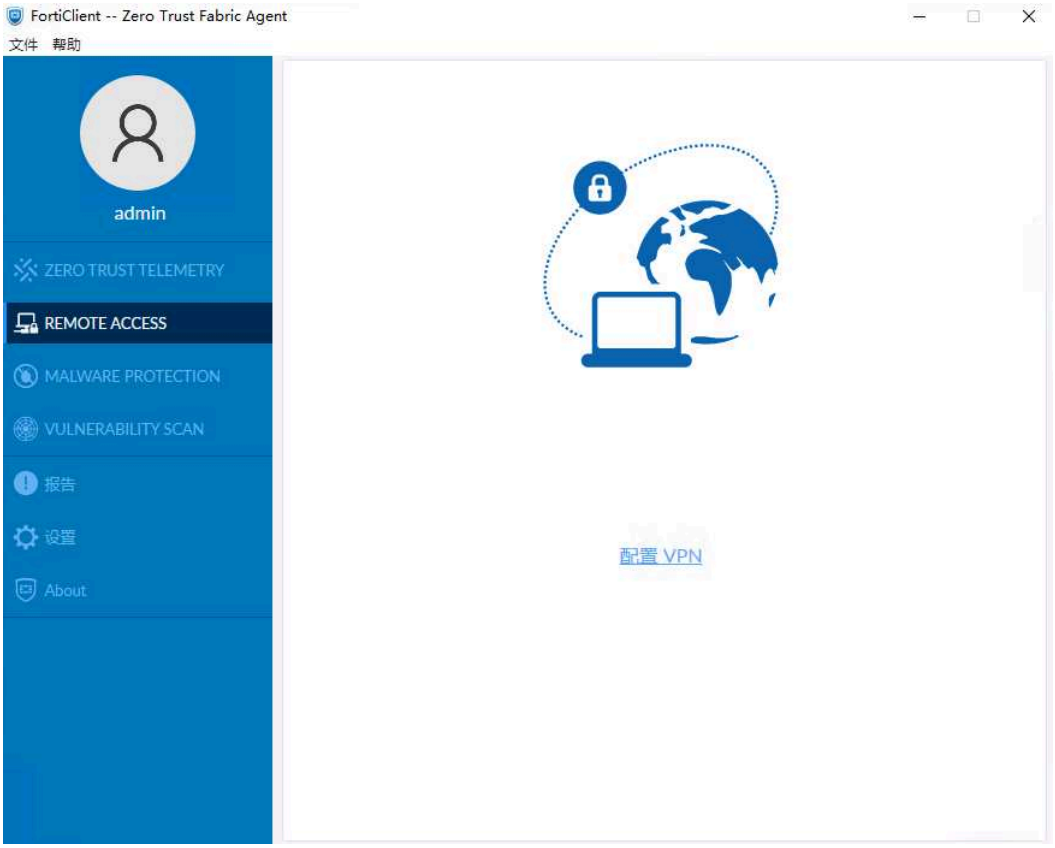
4. 创建策略



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置FortClient

1. 选择“Remote Access”，点击“配置VPN”。



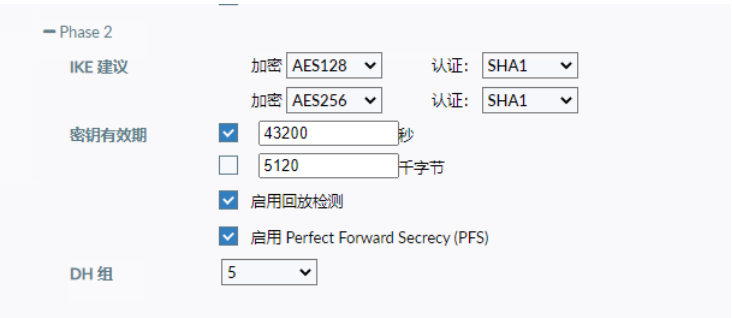
2. 选择IPSEC VPN，输入连接名，远程网关，个人证书，以及用户名，然后点击“保存”。



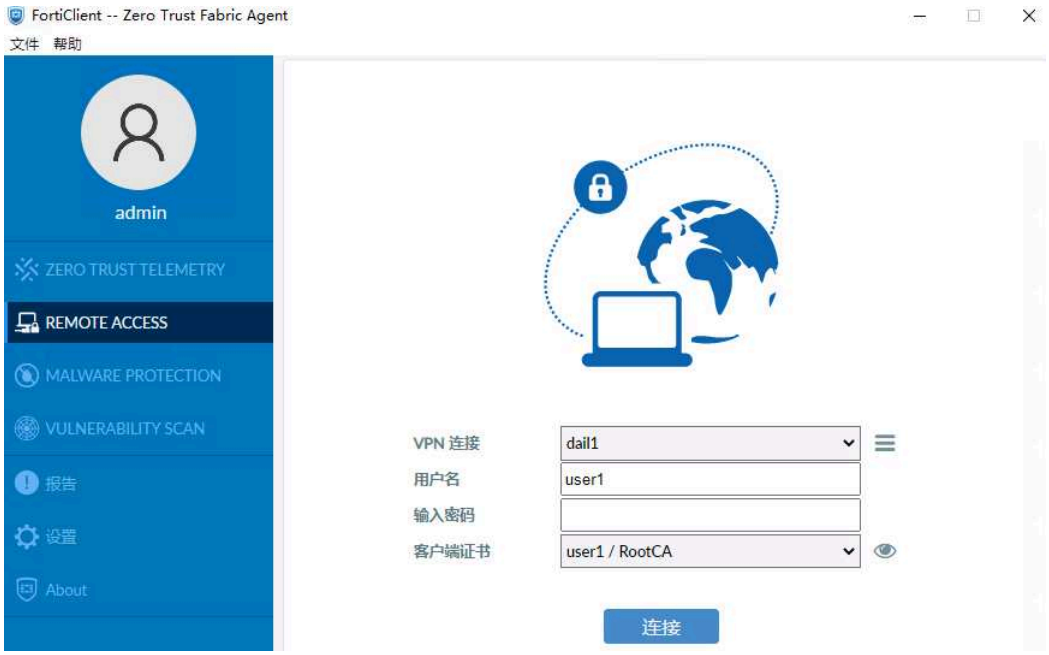
3. 在”高级设置“有更多的选项，如ike版本，IKE阶段一和阶段二的加密集等，可以根据FortiGate的设置做对应的修改。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





3. VPN配置完成



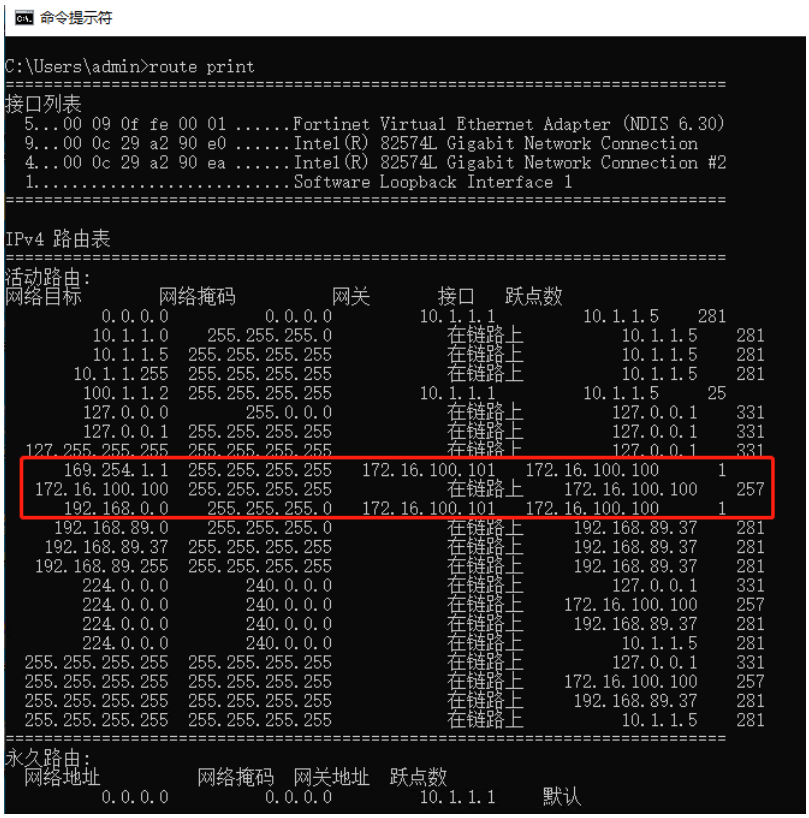
FortClient拨号测试

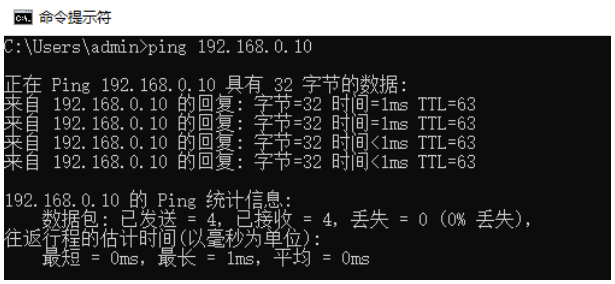
1. 在FortiClient中输入账号密码，点击“连接”，FortiClient拨号成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



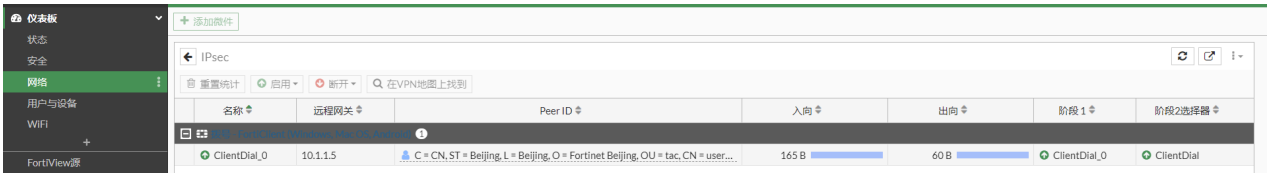
2. 查看终端路由表，192.168.0.0/24指向IPSEC VPN，并能成功访问OA Server。



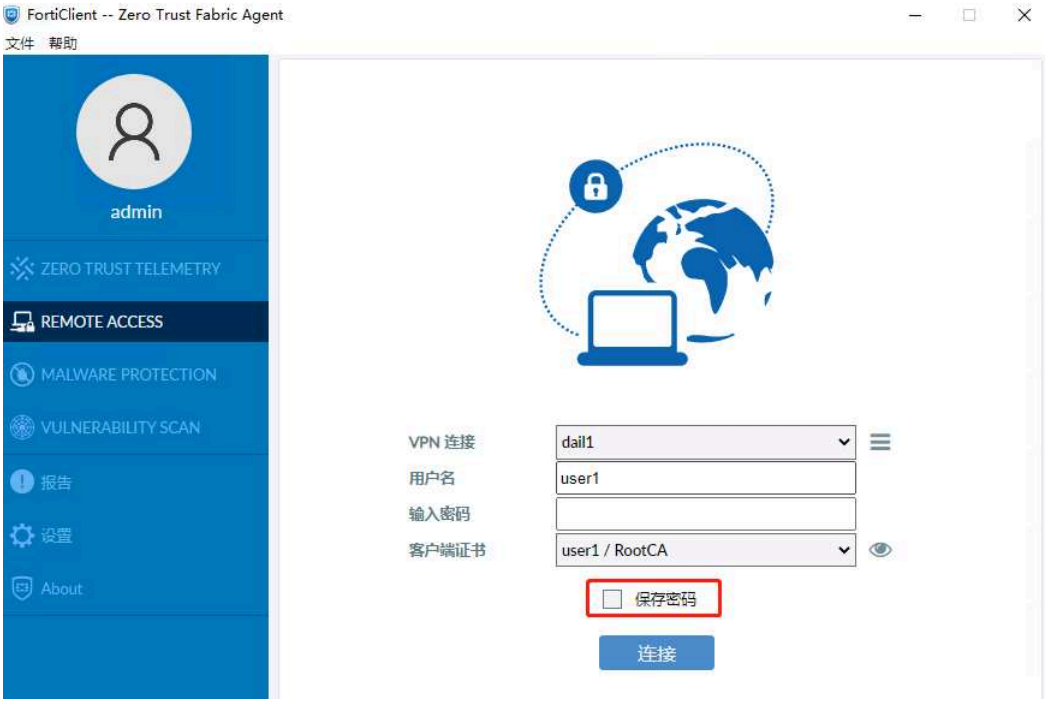


3. FortiGate查看Client的连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 点击“中断连接”，FortiClient就会显示“保存密码”选项。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于TCP的FortiClient拨号

重要

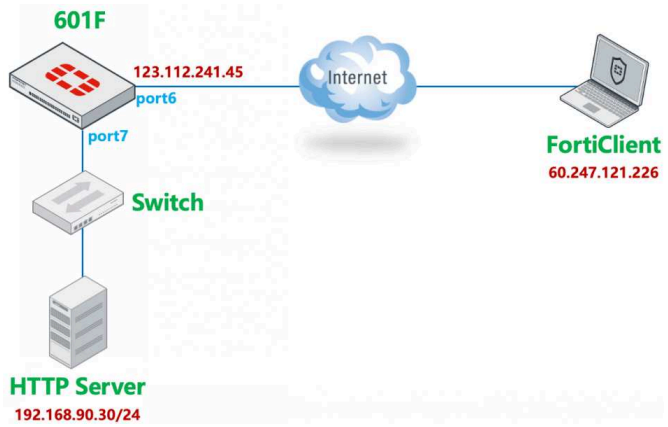
- 该功能在FortiOS 7.4.2、7.6.0及以上版本支持。
- 该功能要求FortiClient版本≥7.4.1。
- 该功能仅支持IKEv2。
- 使用基于TCP的FortiClient IPSec拨号模式，FortiGate暂不支持ESP流量的NP加速（但可以被CP芯片加速）。
- 在FortiClient 7.4.4及以后版本中，FortiClient VPN only版本（免费）将不再支持此功能，FortiClient ZTNA版本（需要EMS License）仍然支持此功能。

功能介绍

传统拨号IPsec VPN流量使用UDP或ESP协议，在FortiOS 7.4.3、7.6.0及以上版本可以通过TCP运行。出于以下考量，我们推荐将FortiClient拨号模式的SSL VPN/IPSec over UDP逐渐迁移至IPSec over TCP。

- 从FortiOS 7.6.3开始，FortiGate在所有型号上移除了SSL VPN Tunnel模式，需要使用IPSec VPN拨号模式替代SSL VPN的Tunnel模式（详情参考：VPN技术→SSL_VPN→开启SSL VPN ↗中的“SSL VPN移除情况”部分）。
- 在高延迟或拥塞的网络中，基于UDP的IPSec VPN连接可能会出现数据包丢失或性能下降。TCP具有错误检测和重传机制，可提高IPSec VPN连接在此类环境中的可靠性和稳定性。
- 部分运营商可能对UDP 500/4500、ESP流量实施策略性限速（如降低QoS优先级或设置带宽阈值）或阻断，尤其在高峰时段或跨境链路上。通过将IPSec VPN切换至TCP传输，可规避此类UDP限速策略，利用TCP的标准化流量特征获得更稳定的带宽分配，从而保障VPN隧道的吞吐量。

网络拓扑



- FortiGate-601F（NP7）配置基于TCP的IKEv2拨号IPsec服务器，自定义TCP端口为4443。
- IKEv2使用EAP进行用户身份验证。
- 客户端使用FortiClient 7.4.3版本，配置TCP目标端口4443连接FortiGate的IPsec。

基础配置

用户配置

1. 创建用于IPSec拨号认证的用户和用户组。

```bash
config user local
    edit "user1"
        set type password
        set passwd 1q2w3e4r
    next
    edit "user2"
        set type password
        set passwd 1q2w3e4r
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config user group
    edit "VPN"
        set member "user1" "user2"
    next
end
```

2. 配置用于隧道分割的地址对象，可以配置多个。

```bash
config firewall address
    edit "192.168.90.0/24"
        set subnet 192.168.90.0 255.255.255.0
    next
end
```

指定基于TCP的IPSec端口

1. 指定基于TCP的IPSec VPN使用的端口（`ike-tcp-port`），这里配置为TCP 4443。

> **重要**
>
> - 默认 `ike-tcp-port` 配置：
>   - FortiOS 7.4：4500。
>   - FortiOS 7.6：443。
> - 修改 `ike-tcp-port` 选项是基于当前VDOM生效的，该VDOM内所有基于TCP的IPSec连接都将使用指定端口封装IKE协商包和IPSec ESP报文。若需同时支持其他使用不同TCP端口的IPSec连接（如与其他FortiGate之间），建议通过新建VDOM实现。
> - 修改 `ike-tcp-port` 选项不会影响基于UDP的IPSec连接端口（`ike-port`，默认500）。

```bash
config system settings
    set ike-tcp-port 4443
end
```

2. 如果使用TCP 443端口，可能会与FortiGate的HTTPS管理端口或SSL VPN端口冲突，需要修改HTTPS管理端口/SSL VPN为其他端口，IPSec的TCP 443端口才能生效。

```bash
HTTPS管理端口：
config system global
    set admin-sport <port>
end

SSL VPN端口：
config vpn ssl settings
    set port <port>
end
```

FortiGate IPSec配置

> **重要**
>
> 通过GUI的配置步骤基于FortiOS 7.6.3，如果是7.4.X版本，请参考通过CLI命令配置的部分。

通过GUI配置（FortiOS 7.6）

1. 在FortiGate进入“VPN→VPN隧道”页面，点击“新建”按钮，选择“来自模板的IPSec隧道”。



2. 在弹出的“VPN向导”中，填写隧道名称，模板选择“远程访问”类型，然后点击“开始”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在“VPN隧道”页面填写“预共享密钥”，传输模式选择“TCP封装”，用户身份验证方法选择“阶段1接口”，选择已创建的VPN用户组，其他保持默认，点击“下一个”按钮。

重要

可选配置：

- 传输：
  - TCP封装：强制使用TCP封装IKE协商报文与IPSec ESP报文，TCP端口会使用已配置的 `ike-tcp-port` 。
  - 自动：优先使用UDP封装IKE协商报文，如果UDP连接超时（默认超时时间为15s）。
- 使用Fortinet封装：
  - 开启：使用Fake TCP头部封装ESP（RFC8229），仅适用于FortiGate之间建立的IPSec。
  - 关闭：使用标准TCP头部封装ESP（RFC9293），使用FortiClient连接时，一定要关闭此选项。
- 用户身份验证方法：
  - 阶段1接口：在IPSec阶段1配置中手动选择需要认证的用户组，只能选择一个用户组。
  - 从策略继承：在IPSec相关的防火墙策略中指定需要认证的用户组，适用于有多个用户组的情况。
- DNS服务器：
  - 使用系统DNS：分配系统配置的DNS服务器给FortiClient。
  - 指定：手工指定给FortiClient分配的DNS服务器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 在“远程端点”页面填写给FortiClient分配的地址池，关闭“EMS SN验证”，点击“下一个”按钮。



5. 在“本地FortiGate”页面选择用于接入IPSec连接的接口port6，IPSec拨号访问的目的接口port7，“本地地址”选择需要隧道分离的地址对象“192.168.90.0/24”（可选多个），点击“下一个”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. Comment页面提示会自动下发的地址对象（分配的地址池）、地址组（包含隧道分割的地址对象）、策略（远程到本地放通）的名称，可以点右侧的笔修改名称。



7. IPSec VPN连接创建完成。



8. 查看通过向导自动创建的地址和地址组对象。

```bash
地址（分配的IP地址池）：
config firewall address
    edit "TCP_Dialup_range"
        set type iprange
        set comment "VPN: TCP_Dialup -- Created by VPN wizard"
        set start-ip 10.100.1.100
        set end-ip 10.100.1.200
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
地址组（隧道分割网段）：
config firewall addrgrp
    edit "TCP_Dialup_split"
        set member "192.168.90.0/24"
        set comment "VPN: TCP_Dialup -- Created by VPN wizard"
    next
end
```

9. 查看通过向导创建的IPSec隧道一阶段和二阶段CLI配置。

```bash
config vpn ipsec phase1-interface
    edit "TCP_Dialup"
        set type dynamic
        set interface "port6"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set comments "VPN: TCP_Dialup -- Created by VPN wizard"
        set dhgrp 20 21
        set eap enable
        set eap-identity send-request
        set wizard-type dialup-forticlient
        set authusrgrp "VPN"
        set transport tcp
        set ipv4-start-ip 10.100.1.100
        set ipv4-end-ip 10.100.1.200
        set dns-mode auto
        set ipv4-split-include "TCP_Dialup_split"
        set save-password enable
        set psksecret ENC
iEMCQpp6y6RY3YqsG30txAPygrAppFQYI9fCj5fb/3SVQKJv4rQ4AkexsTC+z3KnXxUpDygDUCc8znjJQnx06jI0CKMHOR++uVgfEOAoMwwfnNQCHr
CBO+I479zBKhDC11kWOGp7IfOX2vWEsZ4LH/MXIuP+vzvD70RqPthkGGz+bnKMgjsr0fkVUwUghtV6PryzeFlmMjY3dkVA
    next
end

config vpn ipsec phase2-interface
    edit "TCP_Dialup"
        set phase1name "TCP_Dialup"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set dhgrp 20 21
        set comments "VPN: TCP_Dialup -- Created by VPN wizard"
    next
end
```

.0. 查看通过向导自动创建的防火墙策略，默认开启SNAT，可根据实际需求调整配置。

```bash
config firewall policy
    edit 22
        set name "vpn_TCP_Dialup_local_allow"
        set srcintf "TCP_Dialup"
        set dstintf "prot7"
        set action accept
        set srcaddr "TCP_Dialup_range"
        set dstaddr "192.168.90.0/24"
        set schedule "always"
        set service "ALL"
        set nat enable
        set comments "VPN: TCP_Dialup -- Created by VPN wizard"
    next
end
```

通过CLI配置（FortiOS 7.4）

1. 创建用于分配IP的地址对象和用于隧道分割的地址组对象。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
地址（分配的IP地址池）：
config firewall address
    edit "TCP_Dialup_range"
        set type iprange
        set start-ip 10.100.1.100
        set end-ip 10.100.1.200
    next
end

地址组（隧道分割网段）：
config firewall address
    edit "192.168.90.0/24"
        set subnet 192.168.90.0 255.255.255.0
    next
end

config firewall addrgrp
    edit "TCP_Dialup_split"
        set member "192.168.90.0/24"
    next
end
```

2. 配置IPSec VPN一阶段。

- `type`：dynamic，拨号模式。
- `interface`：port6，选择用于接入IPSec连接的接口。
- `ike-verison`：2，只有IKEv2支持基于TCP的IPSec模式。
- `mode-cfg`：enable，开启为客户端分配IP和DNS功能。
- `proposal` / `dhgrp`：一阶段安全提议，与FortiClient配置一致即可。
- `eap`：enable，IKEv2客户端认证使用EAP模式。
- `authusrgrp`：VPN，认证使用已创建的VPN用户组。
- `transport`：tcp，使用TCP封装IKE协商报文和ESP报文。
- `ipv4-start-ip` / `ipv4-end-ip`：为FortiClient分配IP的地址池。
- `dns-mode`：auto，使用系统DNS分配给FortiClient。
- `ipv4-split-include`：选择需要隧道分离的地址组对象“TCP_Dialup_split”，这里既可以选择地址组，也可以选择地址对象，但只能选择一个，所以这里以地址组为例，可以包含多个地址对象。
- `save-password`：enable，允许FortiClient保存密码。
- `psksecret`：预共享密钥。

```bash
config vpn ipsec phase1-interface
    edit "TCP_Dialup"
        set type dynamic
        set interface "port6"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set dhgrp 20 21
        set eap enable
        set eap-identity send-request
        set authusrgrp "VPN"
        set transport tcp
        set ipv4-start-ip 10.100.1.100
        set ipv4-end-ip 10.100.1.200
        set dns-mode auto
        set ipv4-split-include "TCP_Dialup_split"
        set save-password enable
        set psksecret 1q2w3e4r
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

可选配置：

- `transport`：
  - tcp：强制使用TCP封装IKE协商报文与IPSec ESP报文，TCP端口会使用已配置的`ike-tcp-port`。
  - auto：优先使用UDP封装IKE协商报文，如果UDP连接超时（默认超时时间为15s）。
- `fortinet-esp`：
  - enable：使用Fake TCP头部封装ESP（RFC8229），仅适用于FortiGate之间建立的IPSec。
  - disable：使用标准TCP头部封装ESP（RFC9293），使用FortiClient连接时，一定要关闭此选项。
- `authusrgrp`：
  - 配置用户组：在IPSec阶段1配置中手动选择需要认证的用户组，只能选择一个用户组。
  - 不配置：在IPSec相关的防火墙策略中指定需要认证的用户组，适用于有多个用户组的情况。
- `dns-mode`：
  - auto：分配系统配置的DNS服务器给FortiClient。
  - manual：手工指定给FortiClient分配的DNS服务器，然后通过`set ipv4-dns-server1 <ipv4_address>`、`set ipv4-dns-server2 <ipv4_address>`等命令设置手工指定的DNS服务器。

3. 配置IPSec VPN二阶段。

- `phase1name`：绑定的一阶段名称。
- `proposal` / `dhgrp`：二阶段安全提议，与FortiClient配置一致即可。

```bash
config vpn ipsec phase2-interface
    edit "TCP_Dialup"
        set phase1name "TCP_Dialup"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set dhgrp 20 21
    next
end
```

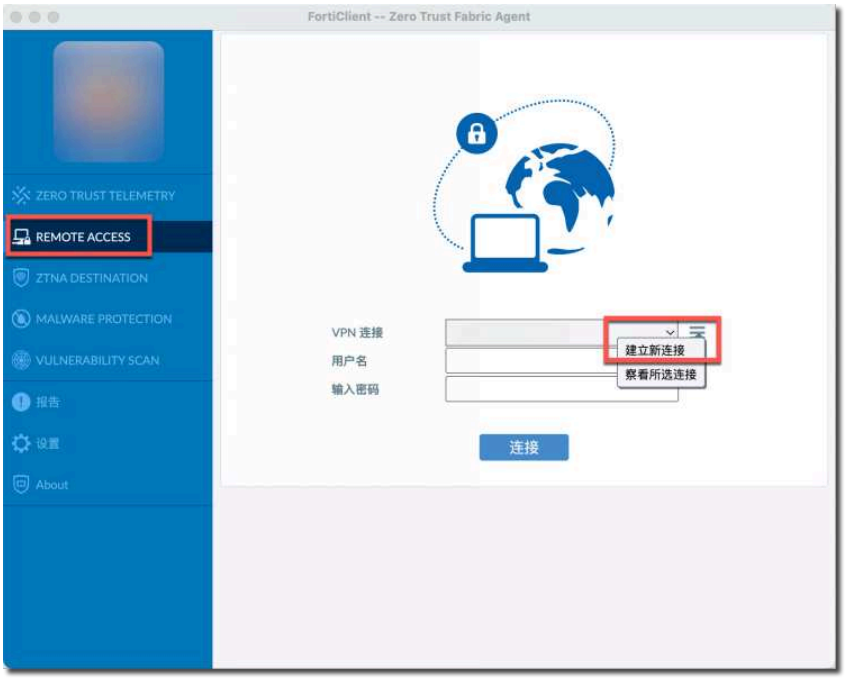
4. 创建防火墙策略，放通FortiClient到VPN资源的访问，可根据实际需求调整配置。

```bash
config firewall policy
    edit 22
        set name "vpn_TCP_Dialup_local_allow"
        set srcintf "TCP_Dialup"
        set dstintf "port7"
        set action accept
        set srcaddr "TCP_Dialup_range"
        set dstaddr "192.168.90.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

FortiClient配置

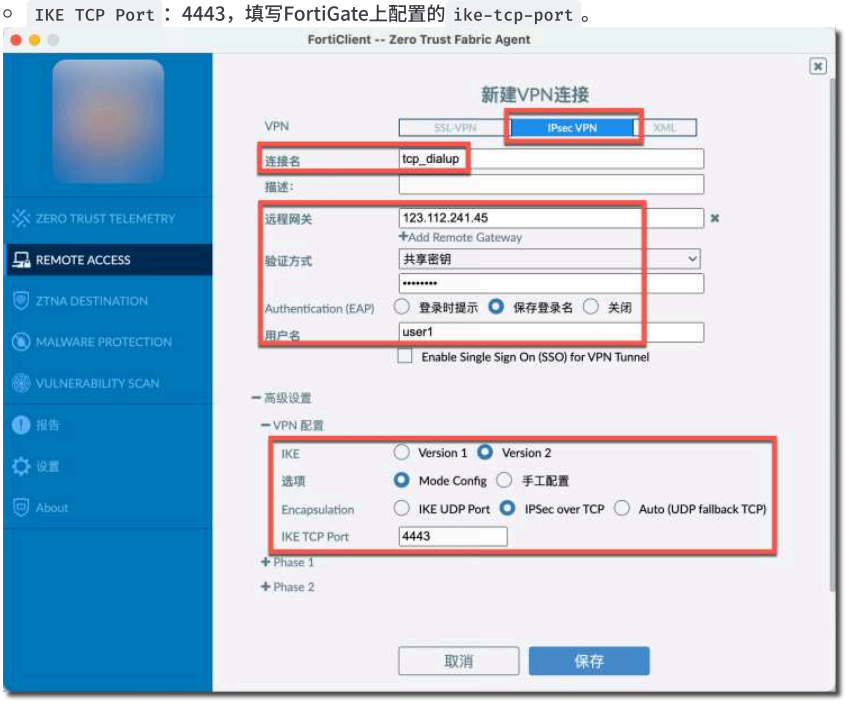
1. 在FortiClient的“Remote Access”界面新建连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 配置VPN连接的基本信息和“高级设置”中的“VPN配置”。

- `VPN类型`：IPSec VPN。
- `远程网关`：填写FortiGate侧接入IPSec的IP。
- `验证方式`：共享密钥，并填入FortiGate配置的IPSec预共享密钥。
- `Authentication` / `用户名`：保存登录名，填写用于EAP认证的用户名。
- `IKE`：Version2。
- `选项`：Mode Config。
- `Encapsulation`：IPSec over TCP。
- `IKE TCP Port`：4443，填写FortiGate上配置的 `ike-tcp-port` 。



重要

可选配置：

- `Encapsulation`：
  - Auto (UDP fallback TCP)：优先使用UDP封装IKE协商报文，如果UDP连接超时（默认超时时间为15s），需要FortiGate的IPSec一阶段中的 `transport` 也设置为 `auto` 才能使用。

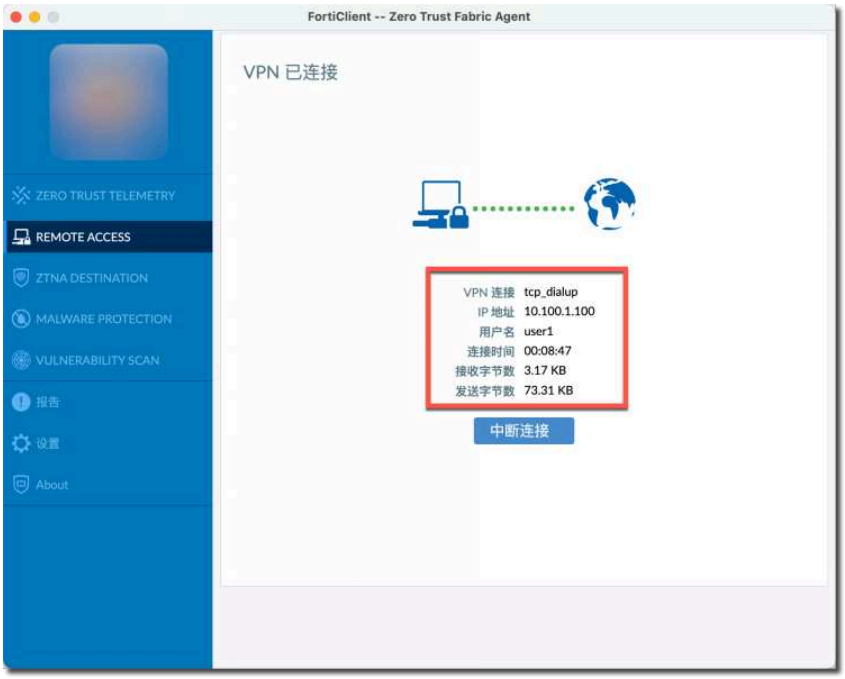
3. 配置IPSec一阶段与二阶段，配置的算法包含在FortiGate配置的安全提议中即可。点击“保存”按钮创建IPSec连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



结果验证

1. 在FortiClient中输入账号/密码，点击“连接”，FortiClient拨号成功。



2. FortiGate GUI显示IPSec一二阶段均建立成功。



3. 在FortiGate上查看IPSec一阶段状态，可以看到传输模式为TCP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # diagnose vpn ike gateway list name TCP_Dialup_0

vd: root/0
name: TCP_Dialup_0
version: 2
interface: port6 12
addr: 123.112.241.45:4443 -> 60.247.121.226:59961
tun_id: 10.100.1.100/::10.0.0.15
remote_location: 0.0.0.0
network-id: 0
transport: TCP    //传输协议为TCP//
created: 7s ago
eap-user: user1    //EAP认证的用户名//
2FA: no
peer-id: Summerices-MacBook-Pro.local
peer-id-auth: no
FortiClient UID: 20835405F599455B9842348F3C690201
assigned IPv4 address: 10.100.1.100/255.255.255.255    //分配的IP地址//
nat: me peer
pending-queue: 0
PPK: no
IKE SA: created 1/1  established 1/1  time 120/120/120 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 70 de71e2a0d62b8736/24365703d2c80d80
  direction: responder
  status: established 7-7s ago = 120ms
  proposal: aes128-sha256
  child: no
  SK_ei: 9e8bbde335eec3a5-885365f407bc0db2
  SK_er: 00eb55dc186eebfe-fba2d0f60debd94e
  SK_ai: 73c01df8a38dacbb-4d79c9eb83842232-affb78dcf6a39117-996de329f3049a45
  SK_ar: dd98c48c5201681a-b979d55de179487c-184da864964c75fa-8464b07fdc107016
  PPK: no
  message-id sent/recv: 0/6
  QKD: no
  PQC-KEM (IKE): no
  PQC-KEM (all IPsec): no
  lifetime/rekey: 86400/86122
  DPD sent/recv: 00000000/00000000
  peer-id: Summerices-MacBook-Pro.local
```

4. 在FortiGate上查看IPSec二阶段状态。

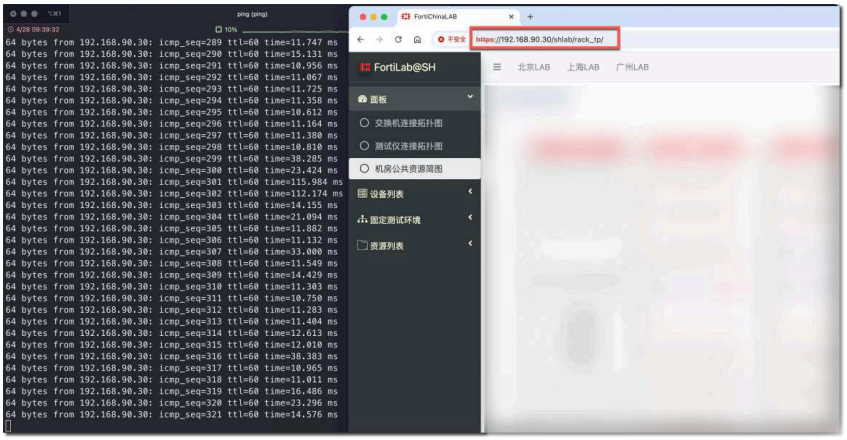
```bash
FortiGate # diagnose vpn tunnel list name TCP_Dialup_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=TCP_Dialup_0 ver=2 serial=1d 123.112.241.45:4443->60.247.121.226:59961 nexthop=123.112.241.1
tun_id=10.100.1.100 tun_id6=::10.0.0.15 status=up dst_mtu=1500 weight=1
bound_if=5 real_if=5 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-
chg frag-rfc  run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=TCP_Dialup index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=45 olast=231 ad=/0
stat: rxp=670 txp=519 rxb=58809 txb=43596
dpd: mode=on-demand on=1 status=ok idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=TCP_Dialup proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.100.1.100-10.100.1.100:0    //目标感兴趣流是为FortiClient分配的IP地址//
  SA:  ref=3 options=6a6 type=00 soft=0 mtu=1438 expire=42398/0B replaywin=2048
       seqno=208 esn=0 replaywin_lastseq=0000029e qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43190/43200
  dec: spi=1a0ea8ca esp=aes key=16 04866c80174edb4312e10f6b793f94c9
       ah=sha1 key=20 7d7024df2395a9861182343865a6d00d636cedbe
  enc: spi=0ac10c0a esp=aes key=16 0abce89fea1f16aaf2b6e5b7411f5bcc
       ah=sha1 key=20 195e92517ac09ed37e7de8ab851fd69d3ba61802
  dec:pkts/bytes=670/58809, enc:pkts/bytes=519/78888
  npu_flag=00 npu_rgwy=0.0.0.0 npu_lgwy=0.0.0.0 npu_selid=0
  dec_npuid=0 enc_npuid=0 dec_engid=-1 enc_engid=-1 dec_saidx=-1 enc_saidx=-1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

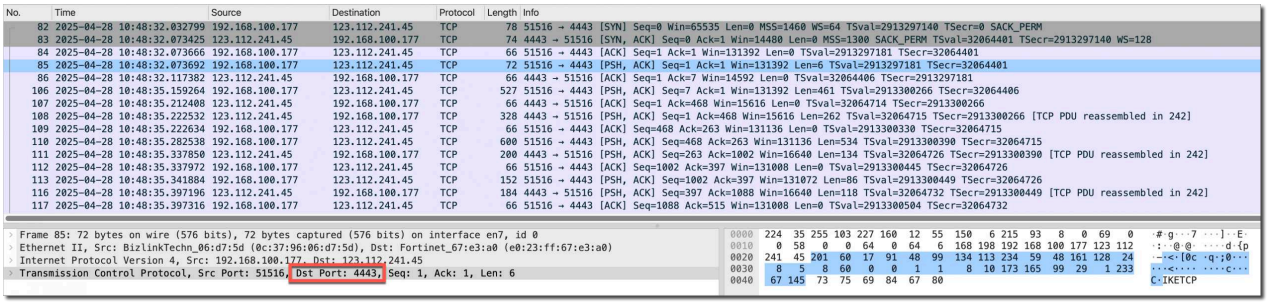
5. 查看FortiClient所在终端IPv4路由表（以下为macOS查看IPv4路由的命令，Windows可以使用`route print -4`查看），192.168.90.0/24指向FortiClient获取的地址10.100.1.100。

```bash
::: important
netstat -rn -f inet
:::
Routing tables

Internet:
Destination        Gateway            Flags               Netif Expire
......
10.100.1.100       10.100.1.100       UHr                 utun8
10.100.1.100/32    link#34            UCS                 utun8
192.168.90         10.100.1.100       UGSc                utun8
......
```

6. 使用FortiClient所在终端访问192.168.90.30，可以通过IPSec正常访问。



7. 抓包查看IPSec over TCP的协商过程与业务流量，可以看到IKEv2协商与ESP流量都被TCP 4500封装（RFC 9293）。



8. 查看FortiClient访问VPN资源的会话，基于TCP的IPSec流量（未开启`fortinet-esp`）无法被NP加速。

```bash
session info: proto=1 proto_state=00 duration=14 expire=59 timeout=0 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=0.0.0.0/10.100.1.100 vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=1260/15/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 83/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=53->13/13->53 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.100.1.100:44090->192.168.90.30:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.90.30:44090->10.100.1.100:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=1904 auth_info=0 chk_client_info=0 vd=0
serial=0000034d tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x000100
no_ofld_reason:  npu-flag-off    //流量无法被NP加速//
```

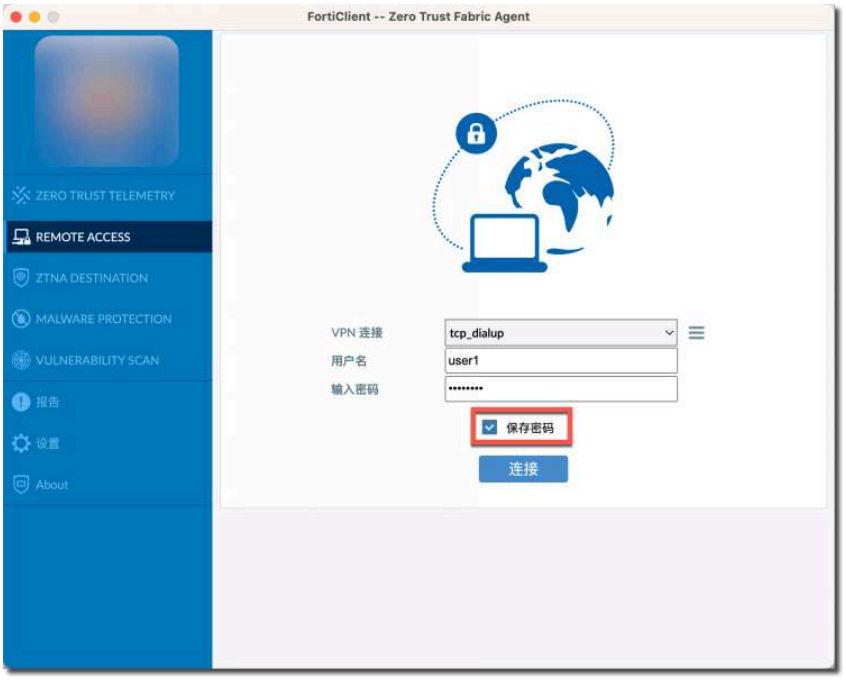
9. 查看FortiGate的硬件/软件加解密统计，可以看到基于TCP的IPSec流量（未开启`fortinet-esp`）虽然无法被NP加速，但可以被CP加速，CP芯片统计计数一直在增长，而SOFTWARE（CPU）统计计数一直为0。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # diagnose vpn ipsec status
All ipsec crypto devices in use:
np7_0:    //NP统计计数始终为0//
    Encryption (encrypted/decrypted)
        null             : 0                0
        des              : 0                0
        3des             : 0                0
        aes              : 0                0
        aes-gcm          : 0                0
        aria             : 0                0
        seed             : 0                0
        chacha20poly1305 : 0                0
    Integrity (generated/validated)
        null             : 0                0
        md5              : 0                0
        sha1             : 0                0
        sha256           : 0                0
        sha384           : 0                0
        sha512           : 0                0

......

CP9:    //CP统计计数一直在增长//
    Encryption (encrypted/decrypted)
        null             : 0                0
        des              : 0                0
        3des             : 0                0
        aes              : 47               464
        aes-gcm          : 0                0
        aria             : 0                0
        seed             : 0                0
        chacha20poly1305 : 0                0
    Integrity (generated/validated)
        null             : 0                0
        md5              : 0                0
        sha1             : 47               464
        sha256           : 0                0
        sha384           : 0                0
        sha512           : 0                0

......

SOFTWARE:    //CPU统计计数始终为0//
    Encryption (encrypted/decrypted)
        null             : 0                0
        des              : 0                0
        3des             : 0                0
        aes              : 0                0
        aes-gcm          : 0                0
        aria             : 0                0
        seed             : 0                0
        chacha20poly1305 : 0                0
    Integrity (generated/validated)
        null             : 0                0
        md5              : 0                0
        sha1             : 0                0
        sha256           : 0                0
        sha384           : 0                0
        sha512           : 0                0
```

.0. FortiClient第一次连接成功后点击“中断连接”，就会显示“保存密码”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



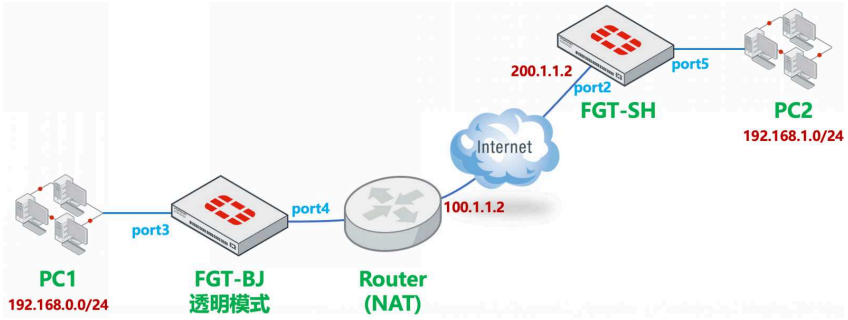
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

透明模式下的IPSec VPN

网络需求

在FortiGate透明模式下，通过IPsec VPN（策略模式）将2个局域网连接起来，实现192.168.0.0/24与192.168.1.0/24两个网段的通信。

网络拓扑



- FGT-BJ是透明模式，PC1的网关指向Router。
- FGT-SH是NAT/路由模式。

配置步骤

FGT-BJ配置

1. **基本配置**

为了便于测试，单独建立一个透明模式的vdom，将port3和port4划入tp1 vdom。



将设备修改为透明模式

> **重要**
>
> IPSec将使用透明模式配置的管理IP（manageip）作为IPSec的本地网关对IKE或ESP进行封装。
>
> 在此例中，FGT-BJ的IPSec本地网关地址为透明模式的管理IP 192.168.0.5，需要确保透明模式的管理IP与Router（NAT）之间的连通性。

```
config system settings
    set opmode transparent
    set manageip 192.168.0.5/255.255.255.0
    set gateway 192.168.0.2
end
```

2. **打开基于策略的IPSEC**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置IPSEC

“选择VPN”-->"IPSEC隧道"，点击“创建”

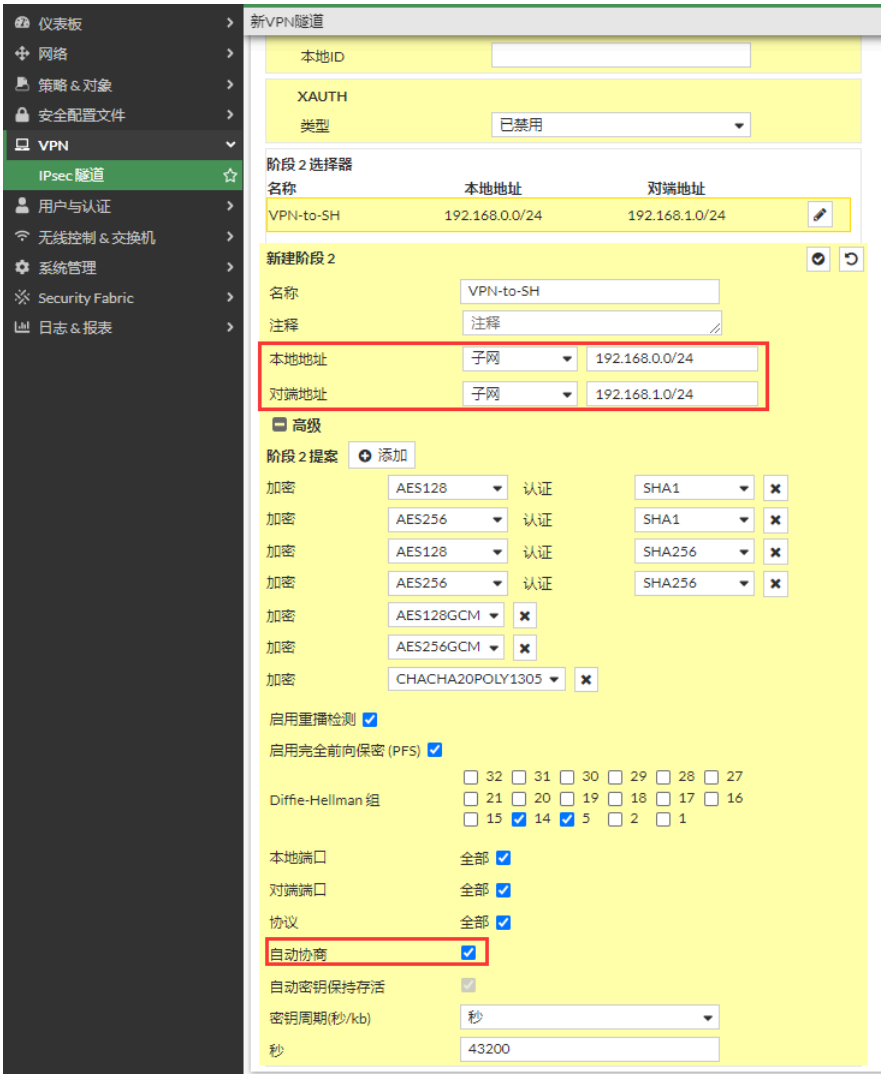


配置IPSEC VPN阶段一



配置IPSEC VPN阶段二

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



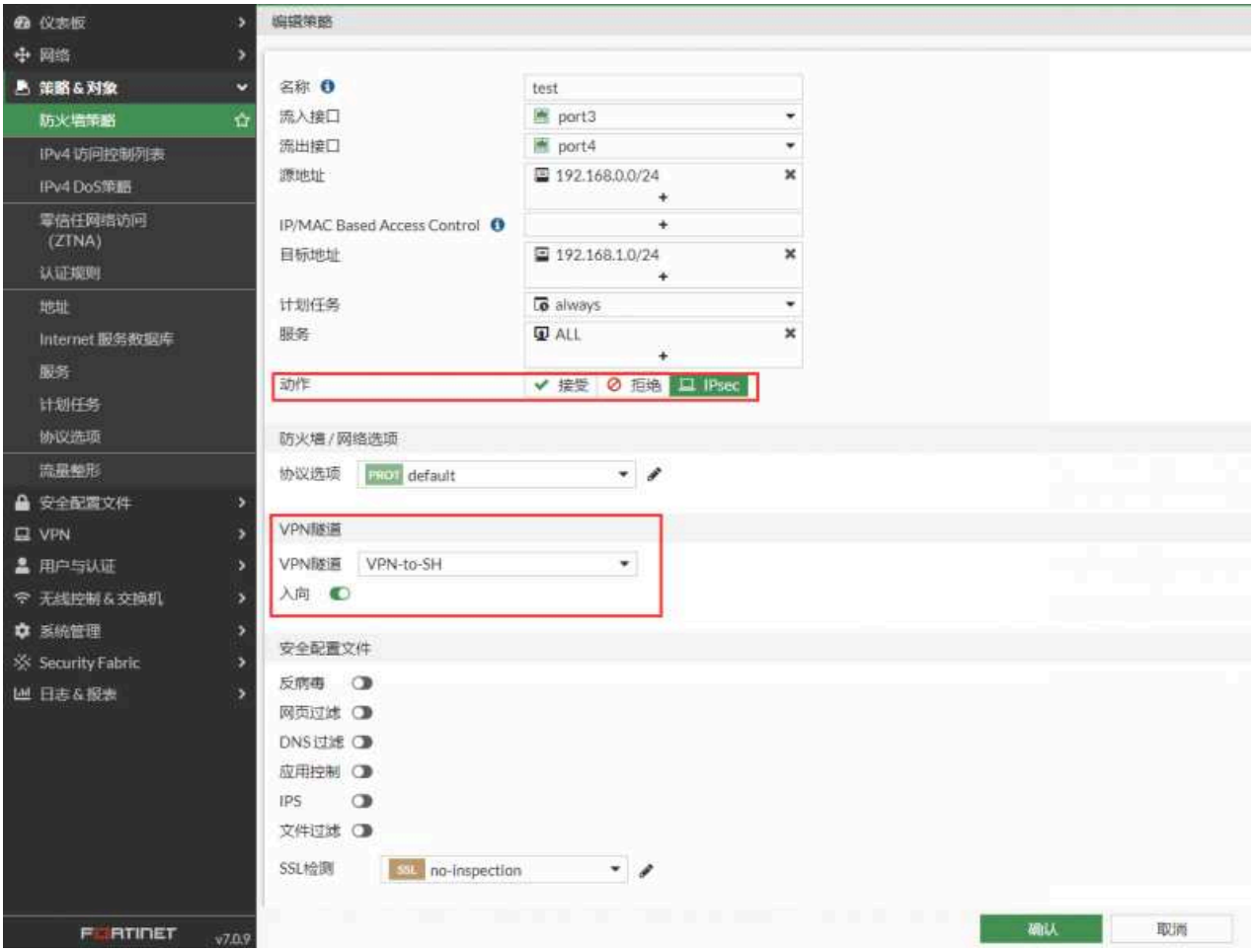
配置完成。

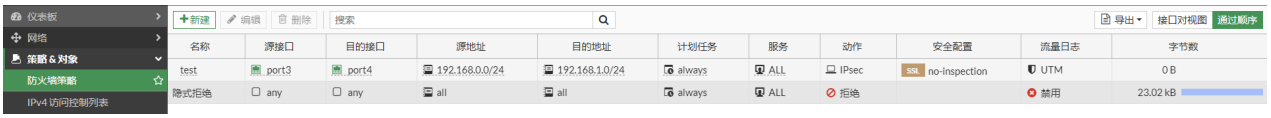


4. **配置策略**

新建策略时，动作要选择IPSEC，指定IPSEC 隧道，入向表示允许对端发起IPSEC流量，如果不勾选，对端发起的IPSEC流量将被拒绝。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





5. IPSEC配置对应的命令行

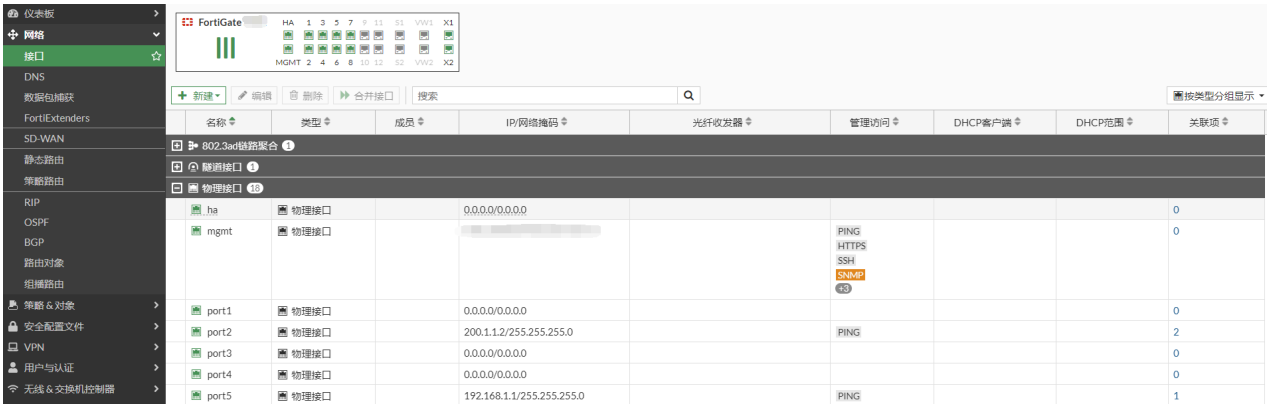
```
config vpn ipsec phase1
    edit "VPN-to-SH"
        set peertype any
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set remote-gw 200.1.1.2
        set psksecret ENC
51lISs3KQ4m+sXPI9G+hwY8ysQEZUNApjT3dLeudcNwE3/ESIDyHJMeUAIBaMZ6aL6lrBiwleBYoEKnP+8gUusyE2nKqVwGYSdzsKHbycQyezu8a9z
ESIu3CoVZA+FUiM+iUSDN0GHwZh6nMkl4g1rXYcLle5qzF0ybsKyYOIwmwovD0v9hBsw5HWMl06WcYnA5hVA==
        set dpd-retryinterval 10
    next
end

# show vpn ipsec phase2
config vpn ipsec phase2
    edit "VPN-to-SH"
        set phase1name "VPN-to-SH"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
        set src-subnet 192.168.0.0 255.255.255.0
        set dst-subnet 192.168.1.0 255.255.255.0
    next
end
```

FGT-SH配置

1. 基本配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置接口ip和路由。





2. 配置IPSEC

选择“VPN”-->“IPSEC隧道”，点击“创建”。



输入对端FortiGate的公网IP（在本文拓扑中为Router NAT后的公网地址100.1.1.2）及预共享秘钥。

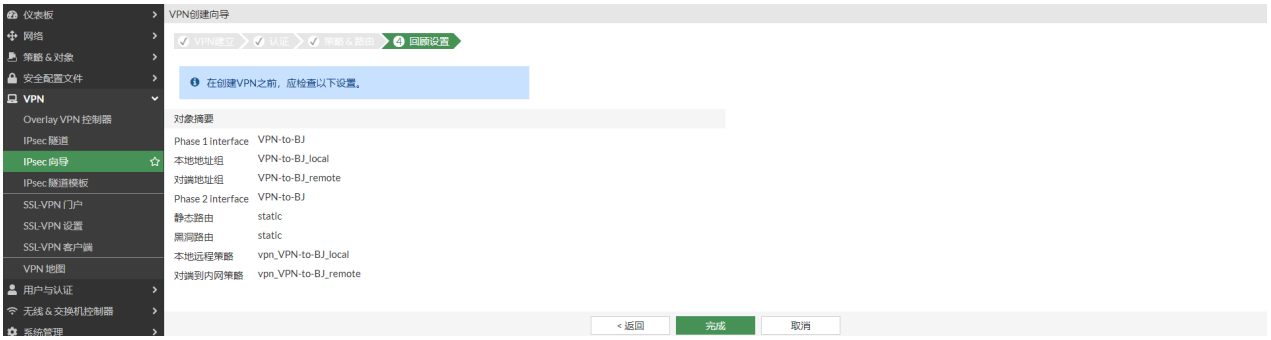


输入需要保护的网段和接口。

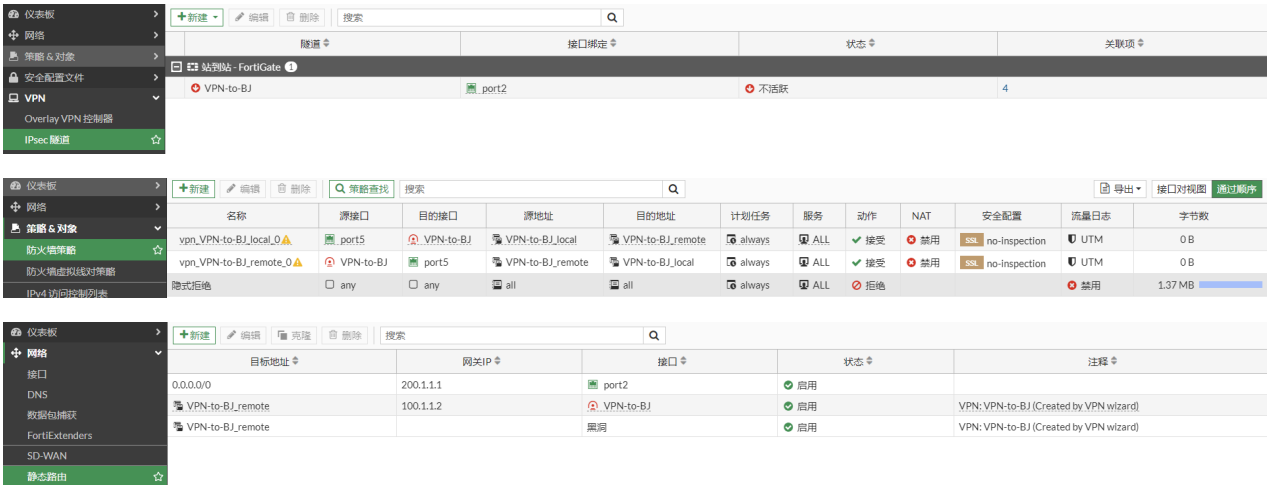


即将创建的内容。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



IPSEC模板创建IPSEC VPN隧道，策略，路由成功。



3. 针对向导配置的优化建议



4. IPSEC配置对应的命令行

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "VPN-to-BJ"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set dpd on-idle
        set comments "VPN: VPN-to-BJ (Created by VPN wizard)"
        set remote-gw 100.1.1.2
        set psksecret ENC
y6uhBx2lgYaxVJ4mkMu+Jf1M4a0a3XnIHULRXDaRBcvy6SVVyFksSsqg6ZdfXAp7okjT3btI8WATWijaxbM1T/1YHfU9gtI0vXFuBoc6Jij41ztBko
hof+OwhJnb+WILWrNIGrgThqN/Su3RtyNk/ruiiW4hs3INa5ku0ZlT7StMlJBRoZ4zQ2XjMXETmOgdZnQR9Q==
        set dpd-retryinterval 10
    next
end

wangxiang-used2 # show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "VPN-to-BJ"
        set phase1name "VPN-to-BJ"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN-to-BJ_local"
        set dst-name "VPN-to-BJ_remote"
    next
end
```

查看IPSEC状态

FGT-BJ IPSEC状态

GUI查看IPSEC状态。



CLI查看IPSEC状态

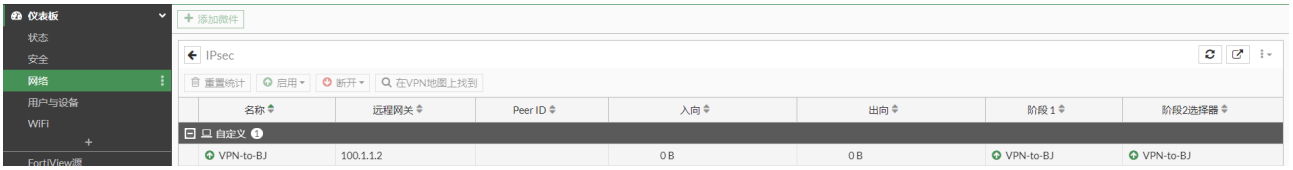
```
# diagnose vpn ike gateway list
vd: tp1/3
name: VPN-to-SH
version: 1
interface:  0
addr: 192.168.0.5:4500 → 200.1.1.2:4500
tun_id: 200.1.1.2/::200.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 522s ago
nat: me
IKE SA: created 1/1  established 1/1  time 9000/9000/9000 ms
IPsec SA: created 1/1  established 1/1  time 9000/9000/9000 ms

  id/spi: 88 df473084a6cd160a/fd52b18f1451abed
  direction: initiator
  status: established 522-513s ago = 9000ms
  proposal: aes128-sha256
  key: dbd02be2254a30c4-383ba553458819b3
  lifetime/rekey: 86400/85586
  DPD sent/recv: 00000009/0000002c

# diagnose vpn tunnel list
list all ipsec tunnel in vd 3
------------------------------------------------------
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
name=VPN-to-SH ver=1 serial=1 192.168.0.5:4500→200.1.1.2:4500 tun_id=200.1.1.2 tun_id6=::200.1.1.2 dst_mtu=1500
dpd-link=on weight=0
bound_if=0 lgwy=static/1 tun=tunnel mode=auto/1 encap=none/8 options[0008]=npu  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=7 ilast=4 olast=4 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=9
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=VPN-to-SH proto=0 sa=1 ref=2 serial=1 auto-negotiate
  src: 0:192.168.0.0-192.168.0.255:0
  dst: 0:192.168.1.0-192.168.1.255:0
  SA:  ref=3 options=18227 type=00 soft=0 mtu=1422 expire=42386/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=f77af5f3 esp=aes key=16 51994a2f09e97e1d834fba1454afce40
       ah=sha1 key=20 f75607ee1dde5d6a97d79d125fa2fbe77033e9d7
  enc: spi=e9cb7b26 esp=aes key=16 4c3df88982eb657c0ac2e851e26727b2
       ah=sha1 key=20 24392681766e619bcee614fb6e3b8318ae37d40e
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=200.1.1.2 npu_lgwy=192.168.0.5 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

FGT-SH IPSEC状态

GUI查看IPSEC状态。



CLI查看IPSEC状态。

```
# diagnose vpn ike gateway list

vd: root/0
name: VPN-to-BJ
version: 1
interface: port2 10
addr: 200.1.1.2:4500 → 100.1.1.2:64916
tun_id: 100.1.1.2/::100.1.1.2
remote_location: 0.0.0.0
network-id: 0
created: 563s ago
nat: peer
IKE SA: created 1/2  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 14 df473084a6cd160a/fd52b18f1451abed
  direction: responder
  status: established 544-544s ago = 0ms
  proposal: aes128-sha256
  key: dbd02be2254a30c4-383ba553458819b3
  lifetime/rekey: 86400/85585
  DPD sent/recv: 0000002f/00000009

# diagnose vpn  tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=VPN-to-BJ ver=1 serial=3 200.1.1.2:4500→100.1.1.2:64916 tun_id=100.1.1.2 tun_id6=::100.1.1.2 dst_mtu=1500 dpd-
link=on weight=1
bound_if=10 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0

proxyid_num=1 child_num=0 refcnt=4 ilast=4 olast=4 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=10000ms retry=3 count=0 seqno=47
natt: mode=silent draft=32 interval=10 remote_port=64916
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
proxyid=VPN-to-BJ proto=0 sa=1 ref=2 serial=1
  src: 0:192.168.1.0-192.168.1.255:0
  dst: 0:192.168.0.0-192.168.0.255:0
  SA:  ref=3 options=10226 type=00 soft=0 mtu=1422 expire=42386/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42933/43200
  dec: spi=e9cb7b26 esp=aes key=16 4c3df88982eb657c0ac2e851e26727b2
       ah=sha1 key=20 24392681766e619bcee614fb6e3b8318ae37d40e
  enc: spi=f77af5f3 esp=aes key=16 51994a2f09e97e1d834fba1454afce40
       ah=sha1 key=20 f75607ee1dde5d6a97d79d125fa2fbe77033e9d7
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.1.1.2 npu_lgwy=200.1.1.2 npu_selid=2 dec_npuid=0 enc_npuid=0
run_tally=0
```

业务测试

1. 从FGT-BJ端 ping FGT-SH端

```
# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6352519  bytes 1854154972 (1.7 GiB)
        RX errors 0  dropped 3749690  overruns 0  frame 0
        TX packets 130448  bytes 8786148 (8.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC1# ping 192.168.1.10 -c 4
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=63 time=0.717 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=63 time=0.853 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=63 time=0.720 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=63 time=0.752 ms

--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.717/0.760/0.853/0.061 ms
```

2. 从FGT-SH端 ping FGT-BJ端

```
# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1a6c:e61:d2b9:a415  prefixlen 64  scopeid 0x20<link>
        inet6 2001::2  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:0e:4e:c5  txqueuelen 1000  (Ethernet)
        RX packets 6040640  bytes 490806558 (468.0 MiB)
        RX errors 0  dropped 145  overruns 0  frame 0
        TX packets 3246663  bytes 205412788614 (191.3 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

# ping 192.168.0.10 -c 4
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=63 time=0.790 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=63 time=0.879 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=63 time=0.686 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=63 time=0.855 ms

--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.686/0.802/0.879/0.079 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec Debug命令

开启IPSEC Debug

```
输出所有IPSEC协商信息
diagnose debug application ike -1
diagnose debug enable

如果有多个IPSEC，则使用filter过滤指定的IPSEC对端，以便查看
diagnose vpn ike log filter dst-addr4 x.x.x.x

清除过滤条件
diagnose vpn ike log filter clear
```

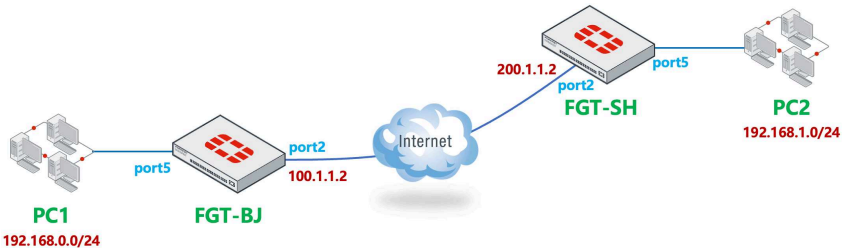
关闭IPSec Debug

```
diagnose debug reset
diagnose debug disable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSEC IKEv1主模式Debug分析

网络拓扑



IPSEC Debug分析

FGT-SH发起协商，FGT-BJ进行Debug查看，下面是FGT-BJ的debug输出

```
# diagnose debug application ike -1
# diagnose debug  enable

收到发起方的数据包，主模式第1个包
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=2f013665b867de80/0000000000000000 len=572 vrf=0
ike 0: in
2F013665B867DE80000000000000000000110020000000000000023C0D000154000000010000000100000148010100080300002801010000800B
0001000C000400015180800100078 00E00808003000180020004800400 0E0300002802010000800B0001000C000400015180800100078 00E0080
80030001800200048004000503000028030100008 00B0001000C000400015180800100078 00E0100800300018002000480040 00E030000280401
0000800B0001000C000400015180800100078 00E0100800300018002000480040005030000280501000080 0B0001000C000400015180800100 07
800E0080800300018002000280040 00E0300002806010000800B0001000C000400015180800100078 00E0080800300018002000280040005030 0
002807010000800B0001000C000400015180800100078 00E0100800300018002000280040 00E0000002808010000800B0001000C000400015180
80010007800E0100800300018002000280040005 0D0000144A131C81070358455C5728F20E95452F0D0000147D9419A65310CA6F2C179D921552
9D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F
0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7
DE7F00D6C2D30D0000184048B7D56EBCE88525E7DE7F00D6C2D3C0000000000000148299031757A36082C6A621DE00000000
ike 0:2f013665b867de80/0000000000000000:2: responder: main mode get 1st message...
ike 0:2f013665b867de80/0000000000000000:2: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:2f013665b867de80/0000000000000000:2: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:2f013665b867de80/0000000000000000:2: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
ike 0:2f013665b867de80/0000000000000000:2: VID draft-ietf-ipsec-nat-t-ike-02\n 90CB80913EBB696E086381B5EC427B1F
ike 0:2f013665b867de80/0000000000000000:2: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:2f013665b867de80/0000000000000000:2: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:2f013665b867de80/0000000000000000:2: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:2f013665b867de80/0000000000000000:2: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:2f013665b867de80/0000000000000000:2: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:2f013665b867de80/0000000000000000:2: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.
ike 0: cache rebuild done

VPN-to-SH有匹配的proposal
ike 0:2f013665b867de80/0000000000000000:2: negotiation result
ike 0:2f013665b867de80/0000000000000000:2: proposal id = 1:
ike 0:2f013665b867de80/0000000000000000:2:   protocol id = ISAKMP:
ike 0:2f013665b867de80/0000000000000000:2:      trans_id = KEY_IKE.
ike 0:2f013665b867de80/0000000000000000:2:      encapsulation = IKE/none
ike 0:2f013665b867de80/0000000000000000:2:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:2f013665b867de80/0000000000000000:2:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:2f013665b867de80/0000000000000000:2:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:2f013665b867de80/0000000000000000:2:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:2f013665b867de80/0000000000000000:2: ISAKMP SA lifetime=86400
ike 0:2f013665b867de80/0000000000000000:2: SA proposal chosen, matched gateway VPN-to-SH
ike 0:VPN-to-SH: created connection: 0×8272220 10 100.1.1.2→200.1.1.2:500.
ike 0:VPN-to-SH:2: DPD negotiated
ike 0:VPN-to-SH:2: peer is FortiGate/FortiOS (v0 b0)
ike 0:VPN-to-SH:2: selected NAT-T version: RFC 3947
ike 0:VPN-to-SH:2: cookie 2f013665b867de80/4878dfc8fee0cc14
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

响应方回复的数据包，主模式第2个包，回复选定的proposal

```
ike 0:VPN-to-SH:2: out
2F013665B867DE804878DFC8FEE0CC1401100200000000000000000C00D00003C0000000100000001000000300101000100000028010100000800B
0001000C000400015180800100078 00E008080030001800200048004000E0D0000144A131C81070358455C5728F20E95452F0D000014AFCAD713
68A1F1C96B8696FC775701000D0000148299031757A36082C6A621DE000000000D0000144048B7D56EBCE88525E7DE7F00D6C2D3000000184048
B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:VPN-to-SH:2: sent IKE msg (ident_r1send): 100.1.1.2:500→200.1.1.2:500, len=192, vrf=0,
id=2f013665b867de80/4878dfc8fee0cc14
```

收到发起方的数据包，主模式第3个包，DH秘钥交换

```
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=2f013665b867de80/4878dfc8fee0cc14 len=380 vrf=0
ike 0: in
2F013665B867DE804878DFC8FEE0CC1404100200000000000000017C0A0001045369DFD050FE4B83832486EB52226B86D1577173ACAF314808BC
CC85503E79B107B6A4A84FF35AAC33CD21A34B92B0F5DB386B7C1CA6EB8CA960C9F10BF634422EFB65A1F10C990178FF50F399D3F7C100739FD0
7180370CD8E8F453C3820719E6E1A93B05A82547D9C006171B4662D5F6957AA4EAF646E951149C7932F857FCFF65C3A08C33BAB87CCA8EFFEB77
2C3173FA598322DF3985D685274538422F7F6A8DEE06E7DD82D20903CA20351BA0ED72759E472228CD1F3CA1B4B3EFAE928024A9EEDD2518F558
B4642DBD8F6104C3C575D60EC18C42708D5BD62139AD4BEACA3EFAEF9C2D20F1E08ACC6383B5BBA423372457D1276AEB92EA44A578B12F031400
0014D72D6C2B0293D53F5100169A9B9FCD2C140000243D49DDDC234A0ECB8B6FB311024C90A47BA01F6F651CB35C0EFAD8EA92C1186600000024
86DF949862FBE5DACC6A16AF1D52082976C458B245B28165A65B4A6C8047F396
ike 0:VPN-to-SH:2: responder:main mode get 2nd message ...
ike 0:VPN-to-SH:2: received NAT-D payload type 20
ike 0:VPN-to-SH:2: received NAT-D payload type 20
ike 0:VPN-to-SH:2: NAT not detected
ike 0:VPN-to-SH:2: generate DH public value request queued
ike 0:VPN-to-SH:2: compute DH shared secret request queued
```

响应方回复的数据包，主模式第4个包，DH秘钥交换

```
ike 0:VPN-to-SH:2: out
2F013665B867DE804878DFC8FEE0CC1404100200000000000000017C0A000104C7C1AE93B18487170D87BCDE7C5CADB6EB6ECEAB1C79D43B5179
3B52005A64A8D481779209039910A037E5EC9E8601AD675F6FE02A9B17C534A68DF48B0290C898E47A0A5E64660501E1FB35BB995E337DC257B1
4F89B09CC5708EF7522767D911B69A99D20EAC47A1A95CF8E21887BEFCB2CEB0952D1F193108454325C82F43311DF030E4F48F830007A19C77AA
9B77EF98834B427DE9E1136EDF6C4F9FF48D5772C165E105B6278DBCBC220796E509FC0397DEBC694B7E975307B5B4505C9AC48F73E26EA60DB5
AD9705D9830347667D05BC59CE6E3662CA054EB1A01F9CB075CB3BCC292B982E931042EC6F6692BF624215179E6663F3B319E98E56CD59EA1400
001440B940F425F78C908561DB60981F79C71400002486DF949862FBE5DACC6A16AF1D52082976C458B245B28165A65B4A6C8047F39600000024
3D49DDDC234A0ECB8B6FB311024C90A47BA01F6F651CB35C0EFAD8EA92C11866
ike 0:VPN-to-SH:2: sent IKE msg (ident_r2send): 100.1.1.2:500→200.1.1.2:500, len=380, vrf=0,
id=2f013665b867de80/4878dfc8fee0cc14
ike 0:VPN-to-SH:2: ISAKMP SA 2f013665b867de80/4878dfc8fee0cc14 key 16:161F81D2B495911EF63B98D14AD53392
```

收到发起方的数据包，主模式第5个数据包

```
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=2f013665b867de80/4878dfc8fee0cc14 len=108 vrf=0
ike 0: in
2F013665B867DE804878DFC8FEE0CC1405100201000000000000006C300DBBB94A52BF9EBD32DAD36637AF3D01E12599D17FA31C11C0E84769FF
94BBB2E2B495567DA5BC9742A711CE425345CA3172FC40E6F780C6D7B5BA7C1335289E087ADE06F7BE1D7049A827E902B778
ike 0:VPN-to-SH:2: responder: main mode get 3rd message ...
ike 0:VPN-to-SH:2: dec
2F013665B867DE804878DFC8FEE0CC1405100201000000000000006C0800000C01000000C80101020B00002428BFF5F8227E569BC4138008FEFD
2446057302EEE6662B5CED771411A71FFB930000001C00000001011060022F013665B867DE804878DFC8FEE0CC14FE5CDC03
ike 0:VPN-to-SH:2: received p1 notify type INITIAL-CONTACT
```

主模式使用IPV4地址作为身份ID，预共享秘钥认证成功

```
ike 0:VPN-to-SH:2: peer identifier IPV4_ADDR 200.1.1.2
ike 0:VPN-to-SH:2: PSK authentication succeeded
ike 0:VPN-to-SH:2: authentication OK
ike 0:VPN-to-SH:2: enc
2F013665B867DE804878DFC8FEE0CC1405100201000000000000004C0800000C0100000064010102000000241328931A3FDD6ABABDF48A93D4C3
937D6151EA202121C6FAEAE55698A6F85A57
```

响应方回复的数据包，主模式第6个包，身份信息和认证信息确认

```
ike 0:VPN-to-SH:2: out
2F013665B867DE804878DFC8FEE0CC1405100201000000000000005C74BC93E1AB30646D580EC9F228CEAFA928ADC9EC53A454D6C7E3FA36CB5B
FCF1EEE6F13590EC2BFDA2299E25C9815B2AF528D0E8A6F441D22D4D5B70F98E3BA8
ike 0:VPN-to-SH:2: sent IKE msg (ident_r3send): 100.1.1.2:500→200.1.1.2:500, len=92, vrf=0,
id=2f013665b867de80/4878dfc8fee0cc14
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

第一阶段建立成功，生成IKE SA

```
ike 0:VPN-to-SH:2: established IKE SA 2f013665b867de80/4878dfc8fee0cc14
ike 0:VPN-to-SH:2: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0, mode_cfg=0
ike 0:VPN-to-SH:2: processing INITIAL-CONTACT
ike 0:VPN-to-SH: flushing
ike 0:VPN-to-SH: flushed
ike 0:VPN-to-SH:2: processed INITIAL-CONTACT
ike 0:VPN-to-SH: set oper up
ike 0:VPN-to-SH:2: no pending Quick-Mode negotiations
```

收到发起方的数据包，快速模式第1个包

```
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Quick id=2f013665b867de80/4878dfc8fee0cc14:31008365 len=620 vrf=0
ike 0: in
2F013665B867DE804878DFC8FEE0CC1408102001310083650000026C9DE34950B723760C49E4FC1522F510BF59FFD6880B3F2331E0948E049ED7
594508887D23676A0F646530D7BA6CFB3AEDD0C299727D1637970406D9A3092D2AE86918E3D126BCB320EC2E8B602D97A7FE10CF5AE7497746CF
0A56E8AA444F3CD5237C7AC30606E2E279E5E4271B4D2141907A99821BEDECA31CE8B5D36EDB61478B6E673853D952B6958DB25F2BA7EA95A67B
C7E259A0E823ACBA17C8C6F38003C4F79191F876DBC95B78A92A2473EF158A4CA04BABE1AB83BA5D3E026928B4CB9E68B884DF08D45C5EBC789B
41ACBD5106F9E7EF8A83DE6E9C5970D6158B88E2228B7424BE7020DE0920E9740531A00F1104517ECC0273E2BC19F201AC0487A7D05AF9D29FBB
3C9167565774CF17ACB103694B5EB96057B514C26B849773F0888333A8D28D70950BD54CA2980F6B80FB85990BC5154AB5A26D6F0C267B18F0AE
6BBC54FD1D94A2B66FC51F83247C2183050DE99262E6B829D7AAB266F4877F7AF64F0340DBE7D2BF3DD4E06201D0C54059471963AB9DD6C53DDE
84BD5144F281EEE1BD5B06B1A2C8E9700AA29BD150DAB64AD02C92D3711AB0EA27549C7FEEA9DD88C7F5D6C51CF6B4B8553F2BD90F1176D4F3B8
9A244F95DAF7B2F060B78F0255AE0A74D1444F9A484B90930BA66159EF203A8E476681C45A859B716D8C0BB17D1C24890A4624E72ECB5C4557BF
807D59352BF0B4ADA324DF70CF7537AD43D9138BCD7AE2705C05590828E3D1B1736BD348BE39C32D4EC50F790AB3C69EC66D7D95098DA090EABE
77C45CCB4E91510569033E985919B8873237DE59323B6B4DBBE391C220A016130C42EDF4681897FD
ike 0:VPN-to-SH:2:0: responder received first quick-mode message
ike 0:VPN-to-SH:2: dec
2F013665B867DE804878DFC8FEE0CC1408102001310083650000026C01000024C7EFFF7C6D036D232FFF690088223379 28B03AFD50F33CED859B
59D9AC9412950A0000EC0000000100000001000000E001030407DB38E2B303000020010C0000800100018002A8C0800400018006008080050002
8003000E03000020020C0000800100018002A8C0800400018006010080050002800 3000E03000020030C0000800100018002A8C0800400018006
0080800500058003000E03000020040C0000800100018002A8C0800400018006010080050005800 3000E0300001C0514000080010001800 2A8C0
8004000180060080800 3000E0300001C0614000080010001800 2A8C0800400018006010080050005800 3000E0000001C071C0000800100018002A8C08004
0001800601008003000E040000147D2BEB602046C003CC7C8078DB63B5A805000104712E6A9987254B0247F457E224710813BC36723BD07FDC6D
2420A3F8C1A6612EE12F0CB8FE7F18EA8318C03EB5B25AC803317615EAFA6600B18F97D90FB8D16928CA3A95AAE106C87A4E368B460882AE763A
E31D4484B18CFD50595144BD0BF7D748635590A8941EB4CCA7C6A25ADB532CE4807E08F3BFC6D781C1B3A4DF1CE59849CFEEF7A71E92FDB318C3
7EBDCBAFAEFE35670D1A9FCF77C818CD2708017E0482BAA42BF9951BD52E55C6CBD6AECF6985510D388FD04931532D5C932696885C6492C0F0CD
D3C3965DB1D5EA477A0416CA98692CC6EBA52142719D965CACBD1FB78574D33056E5EF1A5D7D5878CA209BF6C2DBA82526AE34503FEB58C1F777
0500001004000000C0A80100FFFFFF00000000 1004000000C0A80000FFFFFF00B09C916D1B008707
```

第二阶段有匹配的感兴趣流和proposal

```
ike 0:VPN-to-SH:2:0: peer proposal is: peer:0:192.168.1.0-192.168.1.255:0, me:0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:2:VPN-to-SH:0: trying
ike 0:VPN-to-SH:2:VPN-to-SH:0: matched phase2
ike 0:VPN-to-SH:2:VPN-to-SH:0: autokey
ike 0:VPN-to-SH:2:VPN-to-SH:0: my proposal:
ike 0:VPN-to-SH:2:VPN-to-SH:0: proposal id = 1:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   PFS DH group = 14
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0: proposal id = 2:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   protocol id = IPSEC_ESP:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:VPN-to-SH:2:VPN-to-SH:0:   PFS DH group = 5
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0: incoming proposal:
ike 0:VPN-to-SH:2:VPN-to-SH:0: proposal id = 1:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   PFS DH group = 14
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:2:VPN-to-SH:0: negotiation result
ike 0:VPN-to-SH:2:VPN-to-SH:0: proposal id = 1:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:2:VPN-to-SH:0:   PFS DH group = 14
ike 0:VPN-to-SH:2:VPN-to-SH:0:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:2:VPN-to-SH:0:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:2:VPN-to-SH:0:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:2:VPN-to-SH:0: set pfs=MODP2048
ike 0:VPN-to-SH:2:VPN-to-SH:0: using tunnel mode.
ike 0:VPN-to-SH:2:VPN-to-SH:0: generate DH public value request queued
ike 0:VPN-to-SH:2:VPN-to-SH:0: compute DH shared secret request queued
ike 0:VPN-to-SH:2:VPN-to-SH:0: replay protection enabled
ike 0:VPN-to-SH:2:VPN-to-SH:0: SA life soft seconds=42929.
ike 0:VPN-to-SH:2:VPN-to-SH:0: SA life hard seconds=43200.
ike 0:VPN-to-SH:2:VPN-to-SH:0: IPsec SA selectors #src=1 #dst=1
ike 0:VPN-to-SH:2:VPN-to-SH:0: src 0 4 0:192.168.0.0/255.255.255.0:0
ike 0:VPN-to-SH:2:VPN-to-SH:0: dst 0 4 0:192.168.1.0/255.255.255.0:0


生成IN和OUT方向的IPSEC SA
ike 0:VPN-to-SH:2:VPN-to-SH:0: add IPsec SA: SPIs=fe02f809/db38e2b3
ike 0:VPN-to-SH:2:VPN-to-SH:0: IPsec SA dec spi fe02f809 key 16:95A30E49CBCB4EFCBAA65C8CA9B0074C auth
20:C5E5A450DABB70B398CD151C67D3B30E2BC938EA
ike 0:VPN-to-SH:2:VPN-to-SH:0: IPsec SA enc spi db38e2b3 key 16:A4DDB950CCE7BAD17A48AAB32F61514A auth
20:10B16B53C56103A2036BF5308EB3DB30885DB220
```

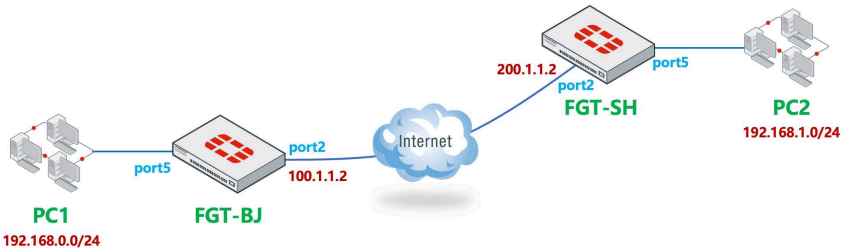

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:VPN-to-SH:2:VPN-to-SH:0: added IPsec SA: SPIs=fe02f809/db38e2b3

隧道UP
ike 0:VPN-to-SH:2:VPN-to-SH:0: sending SNMP tunnel UP trap
ike 0:VPN-to-SH:2: enc
2F013665B867DE804878DFC8FEE0CC1408102001310083650000001B001000024C308502AF541F30479F8C453637BADED887799A67B446206E205
F558A5BC077D0A000038000000010000000100000002C01030401FE02F80900000020010C0000800100018002A8C0800400018006008080050002
8003000E040000141451040EC380E31C646516A89096C12505000104890DB8BA0888142ACD3C99CBD3B57B71186093383DA57E60CE60308E0E9B
EB6B27C751FF683DC4FC56EAB5DECE51B3A52C085A0C477DEF0BAE3ACCA11764D4C49C0ADBF6E12A033929ADC01A1C6D7587C5BE571C7E637819
06FA124705430DBDDF477C238A27E9358A1A8C8FEF923702229F4C8F790847066853CF54E7AD9ED0C3B847C3ADB01A262FA03C3B36EEDDE140E5
975C509DB991A65764CD8F2E8569FE870118494C3735784B8F91AF3F82D296E04FA2C061D0BCC2B713115077AC2223402FEAA2DBA0E8530C10D0
33FEF9D150B30F77A26241B542A613E191590DB77FD0A9A9432C20B526FEAE06EE70920F382F9C49928D39118013ED6EC7697BB2050000100400
0000C0A80100FFFFFF00000000100400000C0A80000FFFFFF00

响应方回复的数据包，快速模式第2个包，发送确认的安全参数和身份认证信息
ike 0:VPN-to-SH:2: out
2F013665B867DE804878DFC8FEE0CC1408102001310083650000001BC5BF94023269A223BC47B8445F7F1DB5707F939EDAFF54CF75D4A3B1CFCF2
C256BFF1ACC1E94729AA344342A8D3C38849D3E7AD8827053E70BEF72D069A331301EBE135F7674951DB0D1B568F0C47D778E992FC25D61D0690
EB27AC0481CFC80317A30A7CF06A20635F53AA4EDD2B830C92E9EF5EAA3D1E3272ECEAB88CBC187A242D81B1F9DA053482D05FF4ACDB571F8F9B
9D675C4BFEC401E9E13AEEFF6A17F8689BDDAE83CFE363AFF24BA4D6C7D1617D0A7AA4C5A63E0C60BA40A7B92D020E494A35C7242308C437436D
AD7C015D43BF517F55FDD1207D9C4719B48D77DED72DA812899576009141D1F9E2307A279523EAF0850B7A3968BA3AD4E7EE48761EF8E11D046B
CB54BC4114E2E6A69E7B3A0CBE071D1A0A23BCA262AD92A9FD6BD193A935819B5BEE6067FBAA1FC9B087F84CA3641DA372AA27FE6A17B751A72F
263CE3D2FDED093809CB7CE6E7D3D2A6556E720147AD12D2D8861490A9E78EC213F5F155B93D6075AD26FE1177EDA152551EB1867B3B7C65EFA2
CB7387D780427B0662F9EC667139E17B9692F36060F0ECB8F8620EA1DEAB55488A5A6D4BD3AB
ike 0:VPN-to-SH:2: sent IKE msg (quick_r1send): 100.1.1.2:500→200.1.1.2:500, len=444, vrf=0,
id=2f013665b867de80/4878dfc8fee0cc14:31008365

收到发起方的数据包，快速模式第3个包，发起方的确认报文
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Quick id=2f013665b867de80/4878dfc8fee0cc14:31008365 len=76 vrf=0
ike 0: in
2F013665B867DE804878DFC8FEE0CC1408102001310083650000004CC37A67EFDA1D1385BAD16B7F1462D26C8510BEA49AD6681DA24219B2C2B9
B3CF5EC6577F1AE0051F2DBEC65F7BB65CD7
ike 0:VPN-to-SH:2: dec
2F013665B867DE804878DFC8FEE0CC1408102001310083650000004C000000249C86B516C45350E8D2254EE877DBFB8CF7B461D3454C9FD93BCE
FB177035802712E75AF0009C454FDB097C0B
ike 0:VPN-to-SH:VPN-to-SH:0: send SA_DONE SPI 0×db38e2b3
ike 0:VPN-to-SH: link is idle 10 100.1.1.2→200.1.1.2:0 dpd=1 seqno=1 rr=0


# diagnose debug  disable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec IKEv1野蛮模式Debug分析

网络拓扑



IPSEC Debug分析

FGT-SH发起协商，FGT-BJ进行Debug查看，下面是FGT-BJ的debug输出

```
# diagnose debug application ike -1
# diagnose debug  enable

收到对端的数据包，野蛮模式第1个包
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=d281703dcfc7fc74/0000000000000000 len=720 vrf=0
ike 0: in
D281703DCFC7FC7400000000000000000001100400000000000000002D0040000B400000001000000010000000A801010004030000280101000080 0
0001000C000400015180800100078 00E00808003000180020004800400 0E03000028030100000800B0001000C000400015180800100078 00E0100
80030001800200048004000E03000028050100000800B0001000C000400015180800100078 00E00808003000180020002800400 0E000000280701
0000800B0001000C000400015180800100078 00E01008003000180020002800400 0E0A00010453E290339EEA9422A4B4B1034821162393F25DC7
7AE0D24864206F06B8E7826733B2FD2DF5C70E86310C29F83A77057D630FF9F8C0CE6DBA3FB571D5D3960C9AAC7260FE6D8019E523508632E142
3CF657A462DCA2F4EFB96268E48003194A77D9D85C6A864F1366B7FDA693D1798DFBADCDF3797116C551F260BC03DFA9B7ADF795EAD145DE2ADD
68EDF20E87E67D8F2E90D3245D3A8ED9AB630134CA5F23158BFDA4A6DBC1E5F6C03FB6C3278A3209295A8C7558E93BBB66F115383B11CF7F4644
608A5E448B53F4B2BC3447064464455756 84CD0850FE9D6B47A981BBAEDD24D60F8424618B0F45E34B8C20FF7A48AF12192B44EED4DF2F333533
849321F505000024D612B8B99DFE002B24E032D5DA3AB863E9AC517913DE2F80658C3C0B3554A9190D00000C01000000C80101020D0000144A13
1C81070358455C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D000014
90CB80913EBB696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D00
0014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D30D0000184048B7D56EBCE88525E7DE7F00D6C2D3
C0000000000000148299031757A36082C6A621DE00000000
ike 0:d281703dcfc7fc74/0000000000000000:3: responder: aggressive mode get 1st message ...
ike 0:d281703dcfc7fc74/0000000000000000:3: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:d281703dcfc7fc74/0000000000000000:3: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:d281703dcfc7fc74/0000000000000000:3: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
ike 0:d281703dcfc7fc74/0000000000000000:3: VID draft-ietf-ipsec-nat-t-ike-02 90CB80913EBB696E086381B5EC427B1F
ike 0:d281703dcfc7fc74/0000000000000000:3: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:d281703dcfc7fc74/0000000000000000:3: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:d281703dcfc7fc74/0000000000000000:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:d281703dcfc7fc74/0000000000000000:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:d281703dcfc7fc74/0000000000000000:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:d281703dcfc7fc74/0000000000000000:3: VID FORTIGATE 8299031757A36082C6A621DE00000000

发起方使用IP地址作为身份ID
ike 0::3: peer identifier IPV4_ADDR 200.1.1.2
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.

VPN-to-SH有匹配的Proposal
ike 0: cache rebuild done
ike 0:d281703dcfc7fc74/0000000000000000:3: negotiation result
ike 0:d281703dcfc7fc74/0000000000000000:3: proposal id = 1:
ike 0:d281703dcfc7fc74/0000000000000000:3:   protocol id = ISAKMP:
ike 0:d281703dcfc7fc74/0000000000000000:3:      trans_id = KEY_IKE.
ike 0:d281703dcfc7fc74/0000000000000000:3:      encapsulation = IKE/none
ike 0:d281703dcfc7fc74/0000000000000000:3:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:d281703dcfc7fc74/0000000000000000:3:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:d281703dcfc7fc74/0000000000000000:3:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:d281703dcfc7fc74/0000000000000000:3:         type=OAKLEY_GROUP, val=MODP2048.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:d281703dcfc7fc74/0000000000000000:3: ISAKMP SA lifetime=86400
ike 0:d281703dcfc7fc74/0000000000000000:3: SA proposal chosen, matched gateway VPN-to-SH
ike 0:VPN-to-SH: created connection: 0×8291690 10 100.1.1.2→200.1.1.2:500.
ike 0:VPN-to-SH:3: DPD negotiated
ike 0:VPN-to-SH:3: peer is FortiGate/FortiOS (v0 b0)
ike 0:VPN-to-SH:3: selected NAT-T version: RFC 3947
ike 0:VPN-to-SH:3: generate DH public value request queued
ike 0:VPN-to-SH:3: compute DH shared secret request queued
ike 0:VPN-to-SH:3: cookie d281703dcfc7fc74/d07504953e9d8606
ike 0:VPN-to-SH:3: ISAKMP SA d281703dcfc7fc74/d07504953e9d8606 key 16:9F8B9F21828B2667E9F48941FAE1411C

响应方回复的数据包，野蛮模式第2个报文，响应方用选定提议的所有参数，DH公开值进行应答，以及身份ID供发起方验证
ike 0:VPN-to-SH:3: out
D281703DCFC7FC74D07504953E9D8606011004000000000000002500400003C0000000100000001000000300101000100000028010100008000B
0001000C000400015180800100078000E00808003000180020004800400 0E0A000104797A5665CD5074E082FADF617796BCD6769F2E25B6A03AB6
FDF9AF091A20F4695EE09AD2266A3F99D70C8EC1B470EFA5D2B768626C412AD2F6F3FB6D69FDD77C07FB9A275DC405328907BCF8D587D375C914
378C28788E4978BE85654DBBA2E9E057968A72A7B4B5FC460588F20130C54B4A041261E4DC38B01F10B4118C243ECC4BD50F2E1034879B7ED428
F2003DAE42C74A7479A20B3A2CEB082321F640F4BEC18FF6BA01E3E34600D713DEBD218A350ABE0ACC9F61904F2F43949BFDC43D0A6F3D656B15
22B16050D04205DF5E60118758106EF1852CF801163810164D3B7B2064C4A54185660E20493F81102B12FF4B88B1A447F34749178AE6CDB39185
050000140DA682516661FD4466ADF8F415C3423C0800000C01000000640101020D0000240A3F41A59BC6E3354F353985366B8D7148AF7B96F560
E33CBED1D86B8E28CB4C140000144A131C81070358455C5728F20E95452F14000024D3141A6A7D9320C4105437E65A9B4E60E653C68D9A71A5AF
FC24B06A49CED2EE0D0000244B1C68D360542FC9E16DC7867E8FC6CA8FC90FBDC591A2AC1F0B7B37CE0A6BA60D000014AFCAD71368A1F1C96B86
96FC775701000D0000148299031757A36082C6A621DE000000000D0000144048B7D56EBCE88525E7DE7F00D6C2D3000000184048B7D56EBCE885
25E7DE7F00D6C2D3C0000000
ike 0:VPN-to-SH:3: sent IKE msg (agg_r1send): 100.1.1.2:500→200.1.1.2:500, len=592, vrf=0,
id=d281703dcfc7fc74/d07504953e9d8606


收到发起方的数据包，野蛮模式第3个报文，发起方的确认信息，确认与响应方可以通信
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=d281703dcfc7fc74/d07504953e9d8606 len=172 vrf=0
ike 0: in
D281703DCFC7FC74D07504953E9D860608100401000000000000000AC07B95FFAA22F64125C7C69E4BE2CDAA9CF69581F048D1D9FF7526A143818
E59F1D59314B926251FAF7B80060D7317500A859CB66E64DE016BFC7E1C9D52DE71246F25B9959A6CE700EF95E28746F045B41AAE04299D7F39A
4C8C98BAB85AF3D842971CD2CDB280743677706CCD7A2D1D334D7F6A9CC59946388B50734290E8ECBBBFAA9E8198207007CADFB101184CBD
ike 0:VPN-to-SH:3: responder: aggressive mode get 2nd response...
ike 0:VPN-to-SH:3: dec
D281703DCFC7FC74D07504953E9D860608100401000000000000000AC14000024D90A7BBC0962B9E6192FA19BDAFDD607B0FDFBC19A05A019F225
9FC9D0EE6371140000244B1C68D360542FC9E16DC7867E8FC6CA8FC90FBDC591A2AC1F0B7B37CE0A6BA60B000024D3141A6A7D9320C4105437E6
5A9B4E60E653C68D9A71A5AFFC24B06A49CED2EE0000001C0000000101106002D281703DCFC7FC74D07504953E9D860628CB58CA69594207
ike 0:VPN-to-SH:3: received NAT-D payload type 20
ike 0:VPN-to-SH:3: received NAT-D payload type 20
ike 0:VPN-to-SH:3: received p1 notify type INITIAL-CONTACT

预共享秘钥认证成功
ike 0:VPN-to-SH:3: PSK authentication succeeded
ike 0:VPN-to-SH:3: authentication OK
ike 0:VPN-to-SH:3: NAT not detected


生成IKE SA
ike 0:VPN-to-SH:3: established IKE SA d281703dcfc7fc74/d07504953e9d8606
ike 0:VPN-to-SH:3: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0, mode_cfg=0
ike 0:VPN-to-SH:3: processing INITIAL-CONTACT
ike 0:VPN-to-SH: flushing
ike 0:VPN-to-SH: flushed
ike 0:VPN-to-SH:3: processed INITIAL-CONTACT
ike 0:VPN-to-SH: set oper up
ike 0:VPN-to-SH:3: no pending Quick-Mode negotiations


收到发起的数据包，快速模式第1个包
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Quick id=d281703dcfc7fc74/d07504953e9d8606:03b7f8e6 len=620 vrf=0
ike 0: in
D281703DCFC7FC74D07504953E9D86060810200103B7F8E60000026C407ACC496B7A31B516DCEBFC25D4C6C668B271C7969F0B1785DF58417ED3
99C37BD28D42CC804C33CDE204D57588C4354E4A4A421804B7160B020EEF914F7BC2368EBD8EB6D322359574E37DEFA2C255E7BAE94FF245859D
E7912F4A0C20F1594833582B0A40CE6D9D267ADE8CCDFB47F06B360CA48256F67D0834B6657C3A46C9DE785F0117A336F83810DF0F2F7CC2926B
D5757F093C453BB0AB32ACE53DF72C096045C5C5E0D0FE3E79D2DE5108D2AE0AE916E364D152A131AC2E8C980EEC1CCA7BAD7175739A4B09FF95
BA46C482D8149A9B3A7A2D0A1DDABEE65391070FEDB3497CF5436B0B9B8F9ED64F087CB601C6A871338BF756D28D8FA1B703D92BCC51643BF78B
CF156DF38046951B9D71108FD12F8D1A9EAFED83291E95BE22C2CAB810A10E00AA9B82EB4789270EF1CC3AA442A946A21E7FFDCBD85336AD8C87
73F231EB9669992CE37A8F9B069189103D59B587441485370D7260E8F61C1A94E9527C15FDEB26AE4D3AB69477F95892BB4429E0DBF2CA55A754
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
3664A11BC2643ABE7008D97B0D6A12F3827E0F9F2FD98DB4A92B846D8D366702F77523EA5F4CA6D4B6621A267623758C9C401C1A9C7FA595EDC7
89D0EAACBAB88FF66E6532381135B859609595B877D7661FDAF1B684733451FC63FCED3C1911FE14EB3906267CC24ECE199CB0DF7405C7D4C9D8
38AB44A0FD78AE099670A5724CDA917FD2333912E8012FC9BD51D393517FA78184BC5351B2883ABA8F6AA876D1327D6E79ACD13A921C56EF904E
29073200647A1DFA2228B0334AC8BF881814A612AF98637D691383A2D9FF3901FAF6ADF04FCEC55B
ike 0:VPN-to-SH:3:230: responder received first quick-mode message
ike 0:VPN-to-SH:3: dec
D281703DCFC7FC74D07504953E9D86060810200103B7F8E60000026C01000024F703EDB480571505460F14635B22E25FDFF7DF6B9E191863AA7E
B50C0E12D04F0A0000EC0000000100000001000000E001030407DB38E2B403000020010C0000800100018002A8C0800400018006008080050002
8003000E03000020020C0000800100018002A8C0800400018006010080050002800300 0E03000020030C0000800100018002A8C0800400018006
0080800500058003000E03000020040C0000800100018002A8C0800400018006010080050005800 3000E0300001C0514000080010001800 2A8C0
800400018006008080030 00E0300001C0614000080010001800 2A8C0800400018006010080030 00E0000001C071C0000800100018002A8C08004
0001800601008003000E040000149FD42C6D9B3DFD82CB79295C580709A305000104A2533113195DAEB243659EAF23432B20E32C34FDA0642C25
C1EE2B76EB5E2E6C2548A3B88F58251C805676AC034AB82D49AEE335AFA2F81D2CD91B85B7BA20A614C30C1A18BBFAD91A0096377FCD2B23EE36
457D337899F356C65A95EFC1510AB13F053C29A4110A046F7875F15CB6D9D7EE6839883A6BF2BAA63F50C121FAC79535E3473F8923779BEB886F
401A298ADDE0D158CA543089CDCF1724714916CD066A8135AB09BC90B19B3C5B11AC81A18CCD85A3FF06B205D0A053659596D46CD57809980095
C4BEC4F9256453E2F65857DD22E05A558466F54DB7A8F65DF67F6F7372CA2C9EBC88ACEBE89140D4B52538F79B73BA7B3EEE86AB669A455D0590
0500001004000000C0A80100FFFFFF0000000001004000000C0A80000FFFFFF0042BE359222C53C07

第二阶段有匹配的感兴趣流和proposal
ike 0:VPN-to-SH:3:230: peer proposal is: peer:0:192.168.1.0-192.168.1.255:0, me:0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:3:VPN-to-SH:230: trying
ike 0:VPN-to-SH:3:VPN-to-SH:230: matched phase2
ike 0:VPN-to-SH:3:VPN-to-SH:230: autokey
ike 0:VPN-to-SH:3:VPN-to-SH:230: my proposal:
ike 0:VPN-to-SH:3:VPN-to-SH:230: proposal id = 1:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   PFS DH group = 14
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230: proposal id = 2:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   PFS DH group = 5
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:VPN-to-SH:3:VPN-to-SH:230: incoming proposal:
ike 0:VPN-to-SH:3:VPN-to-SH:230: proposal id = 1:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   PFS DH group = 14
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=NULL
ike 0:VPN-to-SH:3:VPN-to-SH:230: negotiation result
ike 0:VPN-to-SH:3:VPN-to-SH:230: proposal id = 1:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:3:VPN-to-SH:230:   PFS DH group = 14
ike 0:VPN-to-SH:3:VPN-to-SH:230:      trans_id = ESP_AES_CBC (key_len = 128)
ike 0:VPN-to-SH:3:VPN-to-SH:230:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:3:VPN-to-SH:230:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:3:VPN-to-SH:230: set pfs=MODP2048
ike 0:VPN-to-SH:3:VPN-to-SH:230: using tunnel mode.
ike 0:VPN-to-SH:3:VPN-to-SH:230: generate DH public value request queued
ike 0:VPN-to-SH:3:VPN-to-SH:230: compute DH shared secret request queued
ike 0:VPN-to-SH:3:VPN-to-SH:230: replay protection enabled
ike 0:VPN-to-SH:3:VPN-to-SH:230: SA life soft seconds=42933.
ike 0:VPN-to-SH:3:VPN-to-SH:230: SA life hard seconds=43200.
ike 0:VPN-to-SH:3:VPN-to-SH:230: IPsec SA selectors #src=1 #dst=1
ike 0:VPN-to-SH:3:VPN-to-SH:230: src 0 4 0:192.168.0.0/255.255.255.0:0
ike 0:VPN-to-SH:3:VPN-to-SH:230: dst 0 4 0:192.168.1.0/255.255.255.0:0
```

生成IN和OUT方向的IPSEC SA

```
ike 0:VPN-to-SH:3:VPN-to-SH:230: add IPsec SA: SPIs=fe02f80a/db38e2b4
ike 0:VPN-to-SH:3:VPN-to-SH:230: IPsec SA dec spi fe02f80a key 16:EC236EB218FDFDB618A4F3F9365BC2A6 auth
20:87C419704D9037DF765191533D14EAD75985138F
ike 0:VPN-to-SH:3:VPN-to-SH:230: IPsec SA enc spi db38e2b4 key 16:DD0E65226AEB9DC29360DACD7874D604 auth
20:4E1E6ADE3A2BF7F38507D2FA5202121C9C8959D6
ike 0:VPN-to-SH:3:VPN-to-SH:230: added IPsec SA: SPIs=fe02f80a/db38e2b4
```

隧道UP

```
ike 0:VPN-to-SH:3:VPN-to-SH:230: sending SNMP tunnel UP trap
ike 0:VPN-to-SH:3: enc
D281703DCFC7FC74D07504953E9D86060810200103B7F8E6000001B001000024413D8E541E90DE2DD722E84C5DDB7A0305D221EA20A2D53D6762
ED25D74F6E930A000038000000010000000100000002C01030401FE02F80A00000020010C0000800100018002A8C08004000180060080800500028003000E04000014C56F0A2B71A119C8EAB36D97BAC4EEA305000104DEA2BDF7CD3559834DE23B8726D4DA4B2D898E9764AB0E2EAF160F491FE06241136B6F7AFACDC1D95C11A410F81873854CB58C6F01E57007899C8117E5A195E82A1026164307EDE5755191B9D04DABBC68F8ECD89C647AADD7930F8F2D0C8192BAD7B8972E909A799255B91DF75FC3A2520918C10D2FE3520BB242299E22B16E8640BD323AB7508B1F8FD29D10BCB164841CC8D93B4C9688280998F26DA9C19B0C5299A58AFBC55E8C56171FC17DA0ED6231550F37D9468CE6DC3D0FEDAAAC946916CEC1F2D81FC1FBBA2664810466BED343E7D5E441B63367B74CB7E6B33074BBBD538FE9DB46659F4D93E28A387CF33AF6B0448BE4F81D6FB01296E4616CD7050000100400
0000C0A80100FFFFFF00000000100400000C0A80000FFFFFF00
```

响应方回复的数据包，快速模式第2个包，发送确认的安全参数和身份认证信息

```
ike 0:VPN-to-SH:3: out
D281703DCFC7FC74D07504953E9D86060810200103B7F8E6000001BC10B04C4F733E257D73525EBEDB01FA1A25FC3BD684DD58F70CDA141AAC4F
133E03D65A9D3C6E8CE741F647E0342CEF07F0DF809D58566CFF017720EA9F27B873C28BBC35235E5B1B9F3A53EB0EC357AFAD729E146B7C3712
28FDE746E94EB35CB1D5D046C5CC736E5F193AFB4451B0D0FD7FD6D142BFF53BA3443A16B8FEA41FDD9BA2596CEA16FFEA245EA0B0860F565062
C6DEC2024E7E1B0BC2BB0FE7ECF49F5F5C721AD5E9E4C26107D1A3A6B2FCCC777E9D6B9DD5DF8A920417EC102E90E7CD7008437520568E9A0E5C
67E3D918F7EC16166B8E6092EE47811FFAF75A795A97C3625E23E6D94A17538C2B4645102E0058229D4C5F6B5656AEF34B231A8E5A3D9422C534
BC23F6D2CDAD5D1A17EE968D0C1B2ADD0EC1022EA1CFDAF758728C606C60CE27A4BB4DC54D76C6DBA1B208301D52F8E17759DED5F91A24A6C632
```

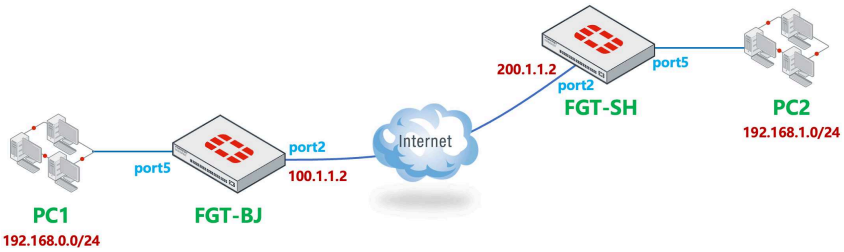

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
8D581FC6110E17FD6166C9EA1FC21791AB183E9A1F3068B3551949E5C8A3F15DFC0348EDD2485F428598BED1B3DE1BF2E7017989E03A5F37167F
64648EED3AF3F30447D5054A0AB7AD192BEA4AF625706283F673B2D93EA6D6B17537D86C1905
ike 0:VPN-to-SH:3: sent IKE msg (quick_r1send): 100.1.1.2:500→200.1.1.2:500, len=444, vrf=0,
id=d281703dcfc7fc74/d07504953e9d8606:03b7f8e6


收到发起方的数据包，快速模式第3个包，发起方的确认报文
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Quick id=d281703dcfc7fc74/d07504953e9d8606:03b7f8e6 len=76 vrf=0
ike 0: in
D281703DCFC7FC74D07504953E9D86060810200103B7F8E60000004CBFE7E9BC7B60005BC3C8AB90CACB6C5412DACDAAE36B845C34C802177DAD
5E1D0A243A6B8BA8770B920A75A6D68626C7
ike 0:VPN-to-SH:3: dec
D281703DCFC7FC74D07504953E9D86060810200103B7F8E60000004C0000002421BD4F317C5DD58943C142AE4186BE1BBE36FBC91C8600E924DC
42BD95107512E61AC8842070C9A16C994E0B
ike 0:VPN-to-SH:VPN-to-SH:230: send SA_DONE SPI 0×db38e2b4
ike 0:VPN-to-SH: link is idle 10 100.1.1.2→200.1.1.2:0 dpd=1 seqno=e5 rr=0

# diagnose debug  disable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSEC IKEv2 Debug分析

网络拓扑



IPSEC Debug分析

1. FGT-SH发起协商，FGT-BJ进行Debug查看，下面是FGT-BJ的debug输出。

```bash
diagnose debug application ike -1
diagnose debug  enable
```

2. 收到发起方的数据包，SA_INIT交互的第1个包。

```bash
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv2 exchange=SA_INIT id=0640897749c18520/0000000000000000 len=632
ike 0: in
0640897749C18520000000000000000000212022080000000000000278220000F0020000340101000503000000C0100000C800E00800300000802
0000050300000803000000C0300000804000005000000080400000E020000340201000503000000C0100000C800E0100030000080200000503000
00080300000C0300000804000005000000080400000E0200002C030100040300000C01000014800E008003000008020000050300000804000
0500000008040000E0200002C040100040300000C01000014800E0100030000080200000603000008040000050000000804000000E0000002C
0501000403000000C0100001C800E0100030000080200000503000008040000050000000804000000E28000108000E0000D7B68B7EF380848D23
3FF08CD57789166A356E53E982392A157953AE8939C833D28C94436514956B08E168503B92D5B09E97FBA36CBCC3B3CBCB5DC9640C6E6F073F
FC88B01DC668D8AF3B61AC2D46B71524B91ECD8CE68F1529986A43BB2E357CFDEE972FFBFCB2B5BC92A38BE6B9E8BEB47A923216AA3753346B
B764CF7760E526B1FD010A8FB51E7B1BB7F80782D53B8C6690852F4D03969CE4CFE8F2252360A4F5672A5C76BA16E45053259BF8E0A154E9BF
F1709B7A72ECF15ED1936E512288D639935CF8096D9F4B8527444CE4C13657F6B751371B6E183B688870C466D5E439DD1AA319306DBC2C6F5E
DC76A1F4EF5223F306E09B3F990FDFF6675B1D290000242941FAF7F9BCFBFA6A308624D8327BB7BDBA4C72BAAA79E27F5FE76580056BE82900
001C000040046248FDD09A0E5B87EFEE4EBE51267EFAA176C9692900001C00004005B85DCDB85885019864A547D5DB8E60946F538368000000
080000402E
```

3. VPN-to-SH有匹配的proposal。

```bash
ike 0:0640897749c18520/0000000000000000:8: responder received SA_INIT msg
ike 0:0640897749c18520/0000000000000000:8: received notify type NAT_DETECTION_SOURCE_IP
ike 0:0640897749c18520/0000000000000000:8: received notify type NAT_DETECTION_DESTINATION_IP
ike 0:0640897749c18520/0000000000000000:8: received notify type FRAGMENTATION_SUPPORTED
ike 0:0640897749c18520/0000000000000000:8: incoming proposal:
ike 0:0640897749c18520/0000000000000000:8: proposal id = 1:
ike 0:0640897749c18520/0000000000000000:8:   protocol = IKEv2:
ike 0:0640897749c18520/0000000000000000:8:      encapsulation = IKEv2/none
ike 0:0640897749c18520/0000000000000000:8:         type=ENCR, val=AES_CBC (key_len = 128)
ike 0:0640897749c18520/0000000000000000:8:         type=INTEGR, val=AUTH_HMAC_SHA2_256_128
ike 0:0640897749c18520/0000000000000000:8:         type=PRF, val=PRF_HMAC_SHA2_256
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP2048.
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP1536.
ike 0:0640897749c18520/0000000000000000:8: proposal id = 2:
ike 0:0640897749c18520/0000000000000000:8:   protocol = IKEv2:
ike 0:0640897749c18520/0000000000000000:8:      encapsulation = IKEv2/none
ike 0:0640897749c18520/0000000000000000:8:         type=ENCR, val=AES_CBC (key_len = 256)
ike 0:0640897749c18520/0000000000000000:8:         type=INTEGR, val=AUTH_HMAC_SHA2_256_128
ike 0:0640897749c18520/0000000000000000:8:         type=PRF, val=PRF_HMAC_SHA2_256
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP2048.
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP1536.
ike 0:0640897749c18520/0000000000000000:8: proposal id = 3:
ike 0:0640897749c18520/0000000000000000:8:   protocol = IKEv2:
ike 0:0640897749c18520/0000000000000000:8:      encapsulation = IKEv2/none
ike 0:0640897749c18520/0000000000000000:8:         type=ENCR, val=AES_GCM_16 (key_len = 128)
ike 0:0640897749c18520/0000000000000000:8:         type=PRF, val=PRF_HMAC_SHA2_256
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP2048.
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP1536.
ike 0:0640897749c18520/0000000000000000:8: proposal id = 4:
ike 0:0640897749c18520/0000000000000000:8:   protocol = IKEv2:
ike 0:0640897749c18520/0000000000000000:8:      encapsulation = IKEv2/none
ike 0:0640897749c18520/0000000000000000:8:         type=ENCR, val=AES_GCM_16 (key_len = 256)
ike 0:0640897749c18520/0000000000000000:8:         type=PRF, val=PRF_HMAC_SHA2_384
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP2048.
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP1536.
ike 0:0640897749c18520/0000000000000000:8: proposal id = 5:
ike 0:0640897749c18520/0000000000000000:8:   protocol = IKEv2:
ike 0:0640897749c18520/0000000000000000:8:      encapsulation = IKEv2/none
ike 0:0640897749c18520/0000000000000000:8:         type=ENCR, val=CHACHA20_POLY1305 (key_len = 256)
ike 0:0640897749c18520/0000000000000000:8:         type=PRF, val=PRF_HMAC_SHA2_256
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP2048.
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP1536.
ike 0:0640897749c18520/0000000000000000:8: matched proposal id 1
ike 0:0640897749c18520/0000000000000000:8: proposal id = 1:
ike 0:0640897749c18520/0000000000000000:8:   protocol = IKEv2:
ike 0:0640897749c18520/0000000000000000:8:      encapsulation = IKEv2/none
ike 0:0640897749c18520/0000000000000000:8:         type=ENCR, val=AES_CBC (key_len = 128)
ike 0:0640897749c18520/0000000000000000:8:         type=INTEGR, val=AUTH_HMAC_SHA2_256_128
ike 0:0640897749c18520/0000000000000000:8:         type=PRF, val=PRF_HMAC_SHA2_256
ike 0:0640897749c18520/0000000000000000:8:         type=DH_GROUP, val=MODP2048.
ike 0:0640897749c18520/0000000000000000:8: lifetime=86400
ike 0:0640897749c18520/0000000000000000:8: SA proposal chosen, matched gateway VPN-to-SH
ike 0:VPN-to-SH: created connection: 0×829cec0 10 100.1.1.2→200.1.1.2:500.
ike 0:VPN-to-SH:8: processing notify type NAT_DETECTION_SOURCE_IP
ike 0:VPN-to-SH:8: processing NAT-D payload
ike 0:VPN-to-SH:8: NAT not detected
ike 0:VPN-to-SH:8: process NAT-D
ike 0:VPN-to-SH:8: processing notify type NAT_DETECTION_DESTINATION_IP
ike 0:VPN-to-SH:8: processing NAT-D payload
ike 0:VPN-to-SH:8: NAT not detected
ike 0:VPN-to-SH:8: process NAT-D
ike 0:VPN-to-SH:8: processing notify type FRAGMENTATION_SUPPORTED
ike 0:VPN-to-SH:8: responder preparing SA_INIT msg
ike 0:VPN-to-SH:8: generate DH public value request queued
ike 0:VPN-to-SH:8: responder preparing SA_INIT msg
ike 0:VPN-to-SH:8: compute DH shared secret request queued
ike 0:VPN-to-SH:8: responder preparing SA_INIT msg
```

4. 响应方回复的数据包，SA_INIT交互的第2个包，回复选定的proposal，临时随机数。

```
ike 0:VPN-to-SH:8: out                                                
```

```bash
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv2 exchange=AUTH id=0640897749c18520/79d668275e8fab85:00000001 len=448
ike 0: in
0640897749C1852079D668275E8FAB852E2023080000000100000 1C0230001A4E1AC49EE91ACC84D384E33FC743CD8013E9CAC48143D241030
DFAF21A7349A62273BA50FB9FF55C8EA7DAC579275E067A8AF56F7982C4B09BC7838438CDA3A7E1922135D0025DFD7F875743BF4EFC02F139D
07A0DBE919ECDBCE30D2C703943CFCC76A587FC78A45CA0BC4AF9EFA50BFEA9E0BB9142944F32F0447B60648788C76A52C81F8EA155BAF403E
2B6E9CFED650E38EBD52F56C33D131ED95A1C812BAC7DE00FEC27E85BA265268086E144ADF658829BA388745E16C256E988A9F86C4B6206DBC
8F354C6DB2D708D2487174F41E3D5E4BF856E1461104858CCFE4FA217592DD616E15431ACB1E9DC0016A4F5D61A7E77B44425DE471512E9C42
CF92B8642E0C5DF0F2B5C605DAAF1BB2CCCA507F275BC4F68E6F263634FF8B66D7F5879329736025E32B14AE0E06C0D4483625F2C462DE381F
F0234A65E5E2E1F0A2D048EF0496B949F5357C76CC8496BF54E65D61011E069E8DD4038B18981DFD7D1BE41A70D76305361B72DB470F287C99
DE1ADC38B51796FF1E5E678387D66E8042BE112EF7EBE5847EB61EAAAAD105C0DF10257BEA8229AEF457366958F9181AE3
ike 0:VPN-to-SH:8: dec
0640897749C1852079D668275E8FAB852E2023080000000100000198230000042900000C01000000C80101022700000800004000290000280200000004C6DA8BCBDEB2583A8A9810615789489134006FEBCA456E407D70393DB45904821000008000040242C000104020000280103040 3DB38E2B90300000C0100000C800E008003000008030000020000000805000000020000280203040 3DB38E2B90300000C0100000C800E0100030000080300000200000008050000000200002803030403DB38E2B90300000C0100000C800E0100030000080300000C000000080500000002000028040304 03DB38E2B90300000C0100000C800E0100030000080300000C000000080500000002000020050304 02DB38E2B90300000C0100001480 0E008000000008050000000200002006030402DB38E2B90300000C01000014800E010000000008050000000000002007030402DB38E2B90300000C0100001C800E010000000008050000002D000018010000000700001000 00FFFFC0A80100C0A801FF000000180100000007000010000 0FFFFC0A80000C0A800FF
ike 0:VPN-to-SH:8: responder received AUTH msg
ike 0:VPN-to-SH:8: processing notify type INITIAL_CONTACT
ike 0:VPN-to-SH:8: processing notify type MESSAGE_ID_SYNC_SUPPORTED
```

7. 发起方使用IP作为自身的ID，认证成功。

```
ike 0:VPN-to-SH:8: peer identifier IPV4_ADDR 200.1.1.2
ike 0:VPN-to-SH:8: auth verify done
ike 0:VPN-to-SH:8: responder AUTH continuation
ike 0:VPN-to-SH:8: authentication succeeded
ike 0:VPN-to-SH:8: responder creating new child
```

8. 找到匹配的proposal和感兴趣流。

```bash
ike 0:VPN-to-SH:8:423: peer proposal:
ike 0:VPN-to-SH:8:423: TSi_0 0:192.168.1.0-192.168.1.255:0
ike 0:VPN-to-SH:8:423: TSr_0 0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:8:VPN-to-SH:423: comparing selectors
ike 0:VPN-to-SH:8:VPN-to-SH:423: matched by rfc-rule-2
ike 0:VPN-to-SH:8:VPN-to-SH:423: phase2 matched by subset
ike 0:VPN-to-SH:8:VPN-to-SH:423: accepted proposal:
ike 0:VPN-to-SH:8:VPN-to-SH:423: TSi_0 0:192.168.1.0-192.168.1.255:0
ike 0:VPN-to-SH:8:VPN-to-SH:423: TSr_0 0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:8:VPN-to-SH:423: autokey
ike 0:VPN-to-SH:8:VPN-to-SH:423: incoming child SA proposal:
ike 0:VPN-to-SH:8:VPN-to-SH:423: proposal id = 1:
ike 0:VPN-to-SH:8:VPN-to-SH:423:   protocol = ESP:
ike 0:VPN-to-SH:8:VPN-to-SH:423:      encapsulation = TUNNEL
ike 0:VPN-to-SH:8:VPN-to-SH:423:         type=ENCR, val=AES_CBC (key_len = 128)
ike 0:VPN-to-SH:8:VPN-to-SH:423:         type=INTEGR, val=SHA
ike 0:VPN-to-SH:8:VPN-to-SH:423:         type=ESN, val=NO
ike 0:VPN-to-SH:8:VPN-to-SH:423:         PFS is disabled
ike 0:VPN-to-SH:8:VPN-to-SH:423: matched proposal id 1
ike 0:VPN-to-SH:8:VPN-to-SH:423: proposal id = 1:
ike 0:VPN-to-SH:8:VPN-to-SH:423:   protocol = ESP:
ike 0:VPN-to-SH:8:VPN-to-SH:423:      encapsulation = TUNNEL
ike 0:VPN-to-SH:8:VPN-to-SH:423:         type=ENCR, val=AES_CBC (key_len = 128)
ike 0:VPN-to-SH:8:VPN-to-SH:423:         type=INTEGR, val=SHA
ike 0:VPN-to-SH:8:VPN-to-SH:423:         type=ESN, val=NO
ike 0:VPN-to-SH:8:VPN-to-SH:423:         PFS is disabled
ike 0:VPN-to-SH:8:VPN-to-SH:423: lifetime=43200
ike 0:VPN-to-SH:8: responder preparing AUTH msg
ike 0:VPN-to-SH:8: established IKE SA 0640897749c18520/79d668275e8fab85
ike 0:VPN-to-SH:8: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0, mode_cfg=0
ike 0:VPN-to-SH:8: processing INITIAL-CONTACT
ike 0:VPN-to-SH: flushing
ike 0:VPN-to-SH: flushed
ike 0:VPN-to-SH:8: processed INITIAL-CONTACT
ike 0:VPN-to-SH: set oper up
ike 0:VPN-to-SH:8:VPN-to-SH:423: replay protection enabled
ike 0:VPN-to-SH:8:VPN-to-SH:423: set sa life soft seconds=42930.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:VPN-to-SH:8:VPN-to-SH:423: set sa life hard seconds=43200.
ike 0:VPN-to-SH:8:VPN-to-SH:423: IPsec SA selectors #src=1 #dst=1
ike 0:VPN-to-SH:8:VPN-to-SH:423: src 0 7 0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:8:VPN-to-SH:423: dst 0 7 0:192.168.1.0-192.168.1.255:0
ike 0:VPN-to-SH:8:VPN-to-SH:423: add IPsec SA: SPIs=fe02f80f/db38e2b9

```

9. 生成IN和OUT方向的IPSEC SA。

```bash
ike 0:VPN-to-SH:8:VPN-to-SH:423: IPsec SA dec spi fe02f80f key 16:81DC7F6F04EF90B86ACD5DE389290829 auth
20:6ED062D0343F9A3905CB3DF496846DDE03A3F5ED
ike 0:VPN-to-SH:8:VPN-to-SH:423: IPsec SA enc spi db38e2b9 key 16:7AC6134E6A36AE792428800B79CC2DC2 auth
20:50EEC2F6F23A0AC711679F61DC3EE6928FC967B9
ike 0:VPN-to-SH:8:VPN-to-SH:423: added IPsec SA: SPIs=fe02f80f/db38e2b9
```

.0. 隧道UP。

```bash
ike 0:VPN-to-SH:8:VPN-to-SH:423: sending SNMP tunnel UP trap
ike 0:VPN-to-SH:8: enc
2700000C01000000640101022900002802000000C55D3BB2AD28F1C48AD025D070255A48E114948725D28D20941363F40BBCAFA62100000800
0040242C00002C0000002801030403FE02F80F0300000C0100000C800E00800300000803000002000000008050000002D000018010000000700
00100000FFFFC0A80100C0A801FF0000001801000000070000100000FFFFC0A80000C0A800FF0706050403020107
```

.1. 响应方回复的数据包，IKE_AUTH交互的第2个包，回复身份信息，感兴趣流，选定的proposal。

```bash
ike 0:VPN-to-SH:8: out
0640897749C1852079D668275E8FAB852E2023200000000010000000E0240000C44AD9A518699109640D1EA67962E73585E17D1269A94910B367
2BAAB5706F353F950D18963DB076624C38DCF0C3D3CDF8D3EC991CF4CEE93D0EFA461E9E23C9362FD0F06B42E6251BDB1C2064DC0E17A8E99F
E31AF55CB0E5A6786EA694DADE5CBBFA5037A0297F77F38B19891910F33430D50350FAD2A716BF45BD0493A7F2DD0E2A3FC09074C464DC2DA2
EFCB7CE00D94D4822D8C81C5A15841DEB46B7017E379643FF00BA34247C836CC8F32565A082E1226E3ABB10379865E18FBACC661FF
ike 0:VPN-to-SH:8: sent IKE msg (AUTH_RESPONSE): 100.1.1.2:500→200.1.1.2:500, len=224, vrf=0,
id=0640897749c18520/79d668275e8fab85:00000001
ike 0:VPN-to-SH: link is idle 10 100.1.1.2→200.1.1.2:0 dpd=1 seqno=16d rr=0
```

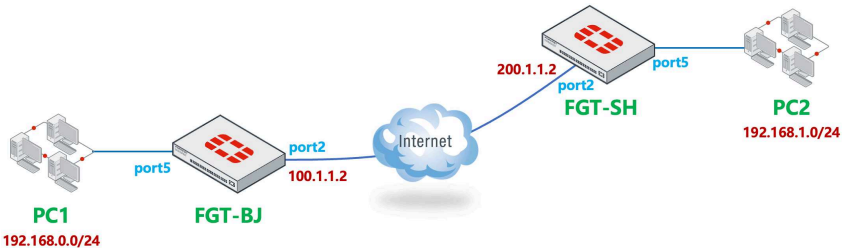
.2. 关闭Debug。

```bash
diagnose debug disable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSEC协商失败举例

网络拓扑



收不到对端IPSEC UDP port 500的协商报文

在FGT-BJ端抓包可以看出FGT-BJ已经发送IPSEC协商报文给FGT-SH，但是FGT-BJ没有收到FGT-SH的协商报文，因此问题可能是运营商阻断了UDP port 500端口的通信，也可能是FGT-SH的配置问题。同理可在FGT-SH端抓包查看。

```bash
FGT-BJ# diagnose sniffer packet any 'host 200.1.1.2 and udp port 500' 4
interfaces=[any]
filters=[host 200.1.1.2 and udp port 500]
8.239752 port2 out 100.1.1.2.500 → 200.1.1.2.500: udp 192
8.240249 port2 out 100.1.1.2.500 → 200.1.1.2.500: udp 380
8.240778 port2 out 100.1.1.2.500 → 200.1.1.2.500: udp 92
```

NAT环境下收不到对端IPSEC UDP port 4500的协商报文

在FGT-BJ端抓包可以看出两端有UDP port 500的IPSEC报文交互，但是FGT-BJ没有收到FGT-SH IPSEC UDP port 4500的协商报文，因此问题可能是运营商阻断了UDP port 4500端口的通信，也可能是FGT-SH的配置问题。同理可在FGT-SH端抓包查看。

```bash
FGT-BJ# diagnose sniffer packet any 'host 200.1.1.2 and (udp port 500 or udp port 4500)' 4
interfaces=[any]
filters=[host 200.1.1.2 and (udp port 500 or udp port 4500)]
6.097481 port2 out 100.1.1.2.500 → 200.1.1.2.500: udp 380
6.098041 port2 in 200.1.1.2.500 → 100.1.1.2.500: udp 380
6.098294 port2 out 100.1.1.2.4500 → 200.1.1.2.4500: udp 112
6.098780 port2 out 100.1.1.2.4500 → 200.1.1.2.4500: udp 624
```

阶段一Proposal秘钥集不匹配

从Debug显示ike Negotiate ISAKMP SA Error: ike 0:f0d8d95cbf3e993e/0000000000000000:13: no SA proposal chosen，对比incoming proposal和my proposal可以看出IPSEC阶段一（ike Negotiate ISAKMP SA）没有匹配的加密算法。

```bash
FGT-BJ# diagnose debug application ike -1
FGT-BJ# diagnose debug  enable

ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=f0d8d95cbf3e993e/0000000000000000 len=332 vrf=0
ike 0: in
F0D8D95CBF3E993E0000000000000000011002000000000000000014C0D0000640000000100000001000000580101000203000028010100000800B
0001000C000400015180800100078 00E00808003000180020006800400 0E0000002802010000800B0001000C000400015180800100078 00E0080
80030001800200068004000 50D0000144A131C81070358455C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60
464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F0AEAA8620D000014
4485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D30D00
00184048B7D56EBCE88525E7DE7F00D6C2D3C0000000000000148299031757A36082C6A621DE00000000
ike 0:f0d8d95cbf3e993e/0000000000000000:13: responder: main mode get 1st message ...
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID draft-ietf-ipsec-nat-t-ike-02 90CB80913EBB696E086381B5EC427B1F
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID DPD AFCAD71368A1F1C96B8696FC77570100
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:f0d8d95cbf3e993e/0000000000000000:13: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.
ike 0: cache rebuild done
ike 0:f0d8d95cbf3e993e/0000000000000000:13: incoming proposal:
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 0:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 0:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA2_512.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: my proposal, gw VPN-to-SH:
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: proposal id = 1:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:   protocol id = ISAKMP:
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      trans_id = KEY_IKE.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:      encapsulation = IKE/none
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_HASH_ALG, val=SHA.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f0d8d95cbf3e993e/0000000000000000:13:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:f0d8d95cbf3e993e/0000000000000000:13: ISAKMP SA lifetime=86400
ike 0:f0d8d95cbf3e993e/0000000000000000:13: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:f0d8d95cbf3e993e/0000000000000000:13: no SA proposal chosen
```

预共享秘钥不匹配

从Debug显示probable pre-shared secret mismatch，可以判断是预共享秘钥不匹配

bash

```
FGT-BJ# diagnose debug application ike -1
FGT-BJ# diagnose debug  enable

ike shrank heap by 163840 bytes
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=dd4a4831edc1e725/0000000000000000 len=332 vrf=0
ike 0: in
DD4A4831EDC1E725000000000000000000011002000000000000000014C0D0000640000000100000001000000580101000203000028010100008000B
0001000C000400015180800010007800E0080800300018002000480040000E0000002802010000800B0001000C000400015180800010007800E0080
800300018002000480040005 0D0000144A131C81070358455C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60
464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F0AEAA8620D000014
4485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D30D00
00184048B7D56EBCE88525E7DE7F00D6C2D3C00000000000001482990317 57A36082C6A621DE00000000
ike 0:dd4a4831edc1e725/0000000000000000:17: responder: main mode get 1st message...
ike 0:dd4a4831edc1e725/0000000000000000:17: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:dd4a4831edc1e725/0000000000000000:17: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:dd4a4831edc1e725/0000000000000000:17: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
ike 0:dd4a4831edc1e725/0000000000000000:17: VID draft-ietf-ipsec-nat-t-ike-02\n 90CB80913EBB696E086381B5EC427B1F
ike 0:dd4a4831edc1e725/0000000000000000:17: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:dd4a4831edc1e725/0000000000000000:17: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:dd4a4831edc1e725/0000000000000000:17: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:dd4a4831edc1e725/0000000000000000:17: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:dd4a4831edc1e725/0000000000000000:17: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:dd4a4831edc1e725/0000000000000000:17: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.
ike 0: cache rebuild done
ike 0:dd4a4831edc1e725/0000000000000000:17: negotiation result
ike 0:dd4a4831edc1e725/0000000000000000:17: proposal id = 1:
ike 0:dd4a4831edc1e725/0000000000000000:17:   protocol id = ISAKMP:
ike 0:dd4a4831edc1e725/0000000000000000:17:      trans_id = KEY_IKE.
ike 0:dd4a4831edc1e725/0000000000000000:17:      encapsulation = IKE/none
ike 0:dd4a4831edc1e725/0000000000000000:17:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:dd4a4831edc1e725/0000000000000000:17:         type=OAKLEY_HASH_ALG, val=SHA2_256.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:dd4a4831edc1e725/0000000000000000:17:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:dd4a4831edc1e725/0000000000000000:17:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:dd4a4831edc1e725/0000000000000000:17: ISAKMP SA lifetime=86400
ike 0:dd4a4831edc1e725/0000000000000000:17: SA proposal chosen, matched gateway VPN-to-SH
ike 0:VPN-to-SH: created connection: 0×9b57be0 10 100.1.1.2→200.1.1.2:500.
ike 0:VPN-to-SH:17: DPD negotiated
ike 0:VPN-to-SH:17: peer is FortiGate/FortiOS (v0 b0)
ike 0:VPN-to-SH:17: selected NAT-T version: RFC 3947
ike 0:VPN-to-SH:17: cookie dd4a4831edc1e725/7d0c610fb77157ce
ike 0:VPN-to-SH:17: out
DD4A4831EDC1E7257D0C610FB77157CE011002000000000000000C00D00003C000000010000000100000030010100010000002801010000800B
0001000C000400015180800100078 00E00808003000180020004800400 0E0D0000144A131C81070358455C5728F20E95452F0D000014AFCAD713
68A1F1C96B8696FC775701000D0000148299031757A36082C6A621DE000000000D0000144048B7D56EBCE88525E7DE7F00D6C2D3000000184048
B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:VPN-to-SH:17: sent IKE msg (ident_r1send): 100.1.1.2:500→200.1.1.2:500, len=192, vrf=0,
id=dd4a4831edc1e725/7d0c610fb77157ce
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=dd4a4831edc1e725/7d0c610fb77157ce len=380 vrf=0
ike 0: in
DD4A4831EDC1E7257D0C610FB77157CE04100200000000000000017C0A0001044FF0C6534555C243272FB0833E95A874D13A865B705BD1C94ED0
D0543A52972D5512DB656C442276401DC9FCFA3AA119208499DF00C5043FA108FE0BE3D38F2BF896E927F0E96454BC828886CC7CD8AB1022D19D
60A9811B25CD571A7E10188C6FD7E61CB9E64DE5D33A38F9BCF0B2C2E41C611D9AC5C047E2A03938BC6798683CE6208F43A6CA894407182B9CEE
9A3B41FB58BC3039326C180335E5044F7FA4D6A027426B609933E4B02BF09AA693AA64518B8050FD0ED70BC7AE87C0C88C09D58E68F4474F21E8
D6C3F7D66D3C7A423E91278F42D6B1BB014A53F215E8D1BEAFA2E1D1CD717DFA02A896BD83C525E5400993BA860A61A4207B66437C4EA6031400
0014657893D41BEBDBEA198635BC6A09EF9914000024A66B51CDA1E16E10A0B69659421DF4143EF4394DF3E6A08E9E5BAB9DEBC5292C00000024
06045FC70A8214BED832E183B81236F416DF5770C32F118AD2F38B9F3CD54606
ike 0:VPN-to-SH:17: responder:main mode get 2nd message...
ike 0:VPN-to-SH:17: received NAT-D payload type 20
ike 0:VPN-to-SH:17: received NAT-D payload type 20
ike 0:VPN-to-SH:17: NAT not detected
ike 0:VPN-to-SH:17: generate DH public value request queued
ike 0:VPN-to-SH:17: compute DH shared secret request queued
ike 0:VPN-to-SH:17: out
DD4A4831EDC1E7257D0C610FB77157CE04100200000000000000017C0A0001042354F77BA3782481818EFCA017482C82BE52A8F85A6E36AF8C31
1C80EA75EA9C3CAD3AB41C069BE71EFF4DFC076C72E0369E7C0B7668EF7A53B674B8E5CAE1755DEF61CB21927A45A1304EF0895714D3CB622F37
B435C9E7EA0C2D7980951C20CAA41CAEF5A44F61D30304B0C24EA82BB1FBBB20FF2C5245FBDCCC0D9102DAE56B2C8AA4E41DB5473AF7ADDA0CA5
C1EE43CAE6BB1D807379CECF73F8D70849EFB353D51805FE16EA186604E87CAC595040E42F65DF18CAF08373C3C2A81D7F0BB8025139B5AD3F94
239748EBB9FF337AE10C4FE415B5B93017A42D66B7574E406398BCBB7C235F88B382B94FC03638CB9BDB5F8A8D43764004B4B41EA86E381C1400
0014BDA49AFE0D6450572E7C41AE2BC3CEF51400002406045FC70A8214BED832E183B81236F416DF5770C32F118AD2F38B9F3CD5460600000024
A66B51CDA1E16E10A0B69659421DF4143EF4394DF3E6A08E9E5BAB9DEBC5292C
ike 0:VPN-to-SH:17: sent IKE msg (ident_r2send): 100.1.1.2:500→200.1.1.2:500, len=380, vrf=0,
id=dd4a4831edc1e725/7d0c610fb77157ce
ike 0:VPN-to-SH:17: ISAKMP SA dd4a4831edc1e725/7d0c610fb77157ce key 16:308FD68288AC676140E7228F0D38783A
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Identity Protection id=dd4a4831edc1e725/7d0c610fb77157ce len=108 vrf=0
ike 0: in
DD4A4831EDC1E7257D0C610FB77157CE05100201000000000000006C8FE002AE3B8049C7B1913FC10F2D97F44D646E05224E064DEC03481780B7
A238205D754F3E9D56715677EE1755456CB2A7065507E04FDCFB454ED3A7C7AC0A77E146380BED18595E4EC503A89EDB11C2
ike 0:VPN-to-SH:17: responder: main mode get 3rd message...
ike 0:VPN-to-SH:17: dec
DD4A4831EDC1E7257D0C610FB77157CE05100201000000000000006C553BDCD748E60ACBE00D989D77561C67934BDA836A49273085DDDE950D5F
328C845CF726C579351BED1BC286ED98D115D683ED3B0FB5FF6A97809437417B29D0B722E56F95A3EA9268565E3303B3C75D
ike 0:VPN-to-SH:17: parse error
ike 0:VPN-to-SH:17: probable pre-shared secret mismatch
```

Peer ID不匹配

从Debug显示ignoring IKE request, incorrect ID，可以判断FGT-BJ设置了对端的身份peer ID，由于对端不匹配，因此协商失败。

bash

```
FGT-BJ# diagnose debug application ike -1
FGT-BJ# diagnose debug  enable

ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=e6280452ac6300c3/0000000000000000 len=720 vrf=0
ike 0: in
E6280452AC6300C3000000000000000000011004000000000000002D0040000B400000001000000010000001A801010004030000280101000080 0B
0001000C000400015180800100078 00E00808003000180020004800400 0E0300002803010000800B0001000C000400015180800100078 00E0100
8003000180020004800400 0E0300002805010000800B0001000C000400015180800100078 00E00808003000180020002800400 0E000000280701
0000800B0001000C000400015180800100078 00E01008003000180020002800400 0E0A000104B6A00CB09789C8BC6146763CE20B649D18F4923F
D7C80543ED2EF0EF97667D1CFA0684F40AAE49A6734172BFDEB8594A7B8DF0D5BC9141C613DFC8D822AC73EAC167AB6412A1F22AE72A3B132822
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
4F5377C57F094B6D2A952A483A4B8C44787707C387C33EB7240CF5B3FB5B4C2144EF94B39E830D3EF2F2980C403A3817E0FBB2FC18425CD0498A
73419AFA2BF3CADCB520CA2583DE90F55E72E686898BF3177D3AEE60C7BC0F7AB35D7D7E06E2E319C8FAAD0E8822D81AAB7780EC837664E6A177
2420F20B3C80760169600CEBDDF5A2EAAC5741391218D4C104892F7823A400F837375AC6E86D811BCB68AA5D54C6463C4E609113C567E3CDE1E4
89A5A874050000245345D5C44232C8EA75FA163A9605835CB173327C00AA6B3C79B3D087F9BE7F410D00000C01000000C80101020D0000144A13
1C81070358455C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D000014
90CB80913EBB696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D00
0014AFCAD71368A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D30D0000184048B7D56EBCE88525E7DE7F00D6C2D3
C000000000000148299031757A36082C6A621DE00000000
ike 0:e6280452ac6300c3/0000000000000000:24: responder: aggressive mode get 1st message ...
ike 0:e6280452ac6300c3/0000000000000000:24: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:e6280452ac6300c3/0000000000000000:24: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:e6280452ac6300c3/0000000000000000:24: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
ike 0:e6280452ac6300c3/0000000000000000:24: VID draft-ietf-ipsec-nat-t-ike-02\n 90CB80913EBB696E086381B5EC427B1F
ike 0:e6280452ac6300c3/0000000000000000:24: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:e6280452ac6300c3/0000000000000000:24: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:e6280452ac6300c3/0000000000000000:24: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:e6280452ac6300c3/0000000000000000:24: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:e6280452ac6300c3/0000000000000000:24: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:e6280452ac6300c3/0000000000000000:24: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0::24: peer identifier IPV4_ADDR 200.1.1.2
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.
ike 0: cache rebuild done
ike 0:VPN-to-SH: ignoring IKE request, incorrect ID.
ike 0:e6280452ac6300c3/0000000000000000:24: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:e6280452ac6300c3/0000000000000000:24: no SA proposal chosen
```

阶段二Proposal秘钥集不匹配

从Debug显示ike Negotiate IPsec SA Error: ike 0:VPN-to-SH:28:23: no SA proposal chosen，对比incoming proposal和my proposal可以看出IPSEC阶段二（ike Negotiate IPsec SA Error）没有匹配的加密算法。

bash

```
FGT-BJ# diagnose debug application ike -1
FGT-BJ# diagnose debug  enable

ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=f7204652fa935744/0000000000000000 len=656 vrf=0
ike 0: in
F7204652FA935744000000000000000001100400000000000000290040000B400000001000000010000000A801010004030000280201000080B
0001000C000400015180800100078 00E00808003000180020004800400050300002804010000800B0001000C000400015180800100078 00E0100
8003000180020004800400050300002806010000800B0001000C000400015180800100078 00E00808003000180020002800400050000000280801
0000800B0001000C000400015180800100078 00E0100800300018002000280040005 0A0000C412447085117ADAC1FEBBD542C368680FEA237164
357F20442AFC40C2A589DBA7F32F33ED514F890D0E4FF2F6C7BEE902AE01CBB5CD541119097BB21863BADF1518CB892AA4A7F18FA33895136C38
CF1714E4CD91A84C885C3C4F5B623607469BFF4370460765FEF16583F0A53838A32668DD758252861C401EDAD583A882849DFAD20E37FC7446DF
38A7EB5D2A643726C99BDD7008293879D3623F8317E15C2334995A051081FB9626802B5C179F22EAFF570FCA3C09E1BD616BCE8C8DF587190500
00244E01F8ABA71441ECB0510C71D87D85DCEE37B3927DE27397AE61CA69B36E242D0D00000C01000000C80101020D0000144A131C8107035845
5C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB
696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD713
68A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D30D0000184048B7D56EBCE88525E7DE7F00D6C2D3C00000000000
00148299031757A36082C6A621DE00000000
ike 0:f7204652fa935744/0000000000000000:28: responder: aggressive mode get 1st message ...
ike 0:f7204652fa935744/0000000000000000:28: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:f7204652fa935744/0000000000000000:28: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:f7204652fa935744/0000000000000000:28: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
ike 0:f7204652fa935744/0000000000000000:28: VID draft-ietf-ipsec-nat-t-ike-02\n 90CB80913EBB696E086381B5EC427B1F
ike 0:f7204652fa935744/0000000000000000:28: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:f7204652fa935744/0000000000000000:28: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:f7204652fa935744/0000000000000000:28: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:f7204652fa935744/0000000000000000:28: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:f7204652fa935744/0000000000000000:28: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:f7204652fa935744/0000000000000000:28: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0::28: peer identifier IPV4_ADDR 200.1.1.2
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.
ike 0: cache rebuild done
ike 0:f7204652fa935744/0000000000000000:28: negotiation result
ike 0:f7204652fa935744/0000000000000000:28: proposal id = 1:
ike 0:f7204652fa935744/0000000000000000:28:   protocol id = ISAKMP:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:f7204652fa935744/0000000000000000:28:      trans_id = KEY_IKE.
ike 0:f7204652fa935744/0000000000000000:28:      encapsulation = IKE/none
ike 0:f7204652fa935744/0000000000000000:28:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:f7204652fa935744/0000000000000000:28:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:f7204652fa935744/0000000000000000:28:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:f7204652fa935744/0000000000000000:28:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:f7204652fa935744/0000000000000000:28: ISAKMP SA lifetime=86400
ike 0:f7204652fa935744/0000000000000000:28: SA proposal chosen, matched gateway VPN-to-SH
ike 0:VPN-to-SH: created connection: 0×9b57be0 10 100.1.1.2→200.1.1.2:500.
ike 0:VPN-to-SH:28: DPD negotiated
ike 0:VPN-to-SH:28: peer is FortiGate/FortiOS (v0 b0)
ike 0:VPN-to-SH:28: selected NAT-T version: RFC 3947
ike 0:VPN-to-SH:28: generate DH public value request queued
ike 0:VPN-to-SH:28: compute DH shared secret request queued
ike 0:VPN-to-SH:28: cookie f7204652fa935744/5b61d63b74cbb9f6
ike 0:VPN-to-SH:28: ISAKMP SA f7204652fa935744/5b61d63b74cbb9f6 key 16:0F91D8F5D8A2C9FA3A9088B189E03E25
ike 0:VPN-to-SH:28: out
F7204652FA9357445B61D63B74CBB9F60110040000000000000002110400003C0000000100000001000000300101000100000028020100008008
0001000C000400015180800100078000E00808003000180020004800400050A0000C4F4B3253B46BD6F0E6565ECEED05034971D80ECF4F3CDC60F
FDA3FEDB48C17FECCE8FF822AE90A5CCB6AF42639776B96DC37937512BC0A3F9BFFF2E928675A2C809A7EC994FD0EB20B67BE20D9B3BE4B67141
91F4F0C7367C5CD6426D044D32CAC8846133F49E58D54971E9A0AC21E87A84D89AE61272B054C00647076F653AF6C6C14169F85D90EA436DD94F
0C74BACAD6DBB6A8B1C3891F792351C7EB7DA6833B6B05882779827B8624D94F3B8CC9175C8CCE725AFAEB326D800797781699FE0500001448B6
599BE05DE8169526D5559B9F3C930800000D020000007465737431 0D0000240A540CEA1B861ABB4EE4E8A7BF1241860187DB76D929109FC58DD6
8ED39DB45F140000144A131C81070358455C5728F20E95452F140000249A6E313BA678326493465137F6BDA361E9B2381E17CE5CF19EE808B223
46E67C0D000024ACC52C4EFEC900F50AD8EEB8FE3C08EA6E18437072859ECC217AD6E29C5964A00D000014AFCAD71368A1F1C96B8696FC775701
000D000014829903175 7A36082C6A621DE000000000D0000144048B7D56EBCE88525E7DE7F00D6C2D3000000184048B7D56EBCE88525E7DE7F00
D6C2D3C0000000
ike 0:VPN-to-SH:28: sent IKE msg (agg_r1send): 100.1.1.2:500→200.1.1.2:500, len=529, vrf=0,
id=f7204652fa935744/5b61d63b74cbb9f6
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=f7204652fa935744/5b61d63b74cbb9f6 len=172 vrf=0
ike 0: in
F7204652FA9357445B61D63B74CBB9F6081004010000000000000AC4368B8C00750D9E5D4364D4C8C3E8741F5D66ADB8F2716593C3DB039D130
88AB5A2E4D38FEA304CAB222731BC854E4506D50ABAFC2D456FDEB620E7927D161A6FA9709F473EA4EB963799383B67C3F1E82076A68ED37501B
CC42E3BD01A211E2E5821A7785CE35C0527663C430D35266AF1BD1D8496ECFB32F5420C795F386B8C7F8D08611A2ECC3CF020C7D4D43D93E
ike 0:VPN-to-SH:28: responder: aggressive mode get 2nd response...
ike 0:VPN-to-SH:28: dec
F7204652FA9357445B61D63B74CBB9F6081004010000000000000AC140000246A0154E97988DFCFFB1D314FF8E895AE5C9ED93CB3B6FE44833A
8B423F639ED514000024ACC52C4EFEC900F50AD8EEB8FE3C08EA6E18437072859ECC217AD6E29C5964A00B0000249A6E313BA678326493465137
F6BDA361E9B2381E17CE5CF19EE808B22346E67C0000001C0000000101106002F7204652FA9357445B61D63B74CBB9F639536A88D14FCC07
ike 0:VPN-to-SH:28: received NAT-D payload type 20
ike 0:VPN-to-SH:28: received NAT-D payload type 20
ike 0:VPN-to-SH:28: received p1 notify type INITIAL-CONTACT
ike 0:VPN-to-SH:28: PSK authentication succeeded
ike 0:VPN-to-SH:28: authentication OK
ike 0:VPN-to-SH:28: NAT not detected
ike 0:VPN-to-SH:28: established IKE SA f7204652fa935744/5b61d63b74cbb9f6
ike 0:VPN-to-SH:28: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0, mode_cfg=0
ike 0:VPN-to-SH:28: processing INITIAL-CONTACT
ike 0:VPN-to-SH: flushing
ike 0:VPN-to-SH: flushed
ike 0:VPN-to-SH:28: processed INITIAL-CONTACT
ike 0:VPN-to-SH: set oper up
ike 0:VPN-to-SH:28: no pending Quick-Mode negotiations
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Quick id=f7204652fa935744/5b61d63b74cbb9f6:854d6010 len=476 vrf=0
ike 0: in
F7204652FA9357445B61D63B74CBB9F608102001854D6010000001DCD35083E7B123E3B5C7C5ECCE5C291BF2AB24505BA8045D3712FD03B3C692
1B8879E69C4F89C41ED3AA8F4D8C67F3CF1ED801F07862C20EE784387EF43372115C4C7ED2DE2269431C4D69AD61BE03C918555C69280EF4D9DE
81C058FBAC440D4FAF0B507CDE4779CE282A0D12E7CA0AC0EF1C13D9F100C6C4DD849A1E12E11AEB8141356C9231AA43667F07C9323266853197
1F3BA330804BD63D963699AB7DB0B046B938470F1082B30E1E52D5C1B2F3E23ECC8C19F0B7281FF51E7A06F39C83D1897A91E3D2BABA0233D115
4DAEAD2C5E15D7363063CB4BBB1125536368DD508F6CA3230FF80980D26A696B970B3CF5846974FC7F6AF48891A118EA8DAA9A5022FA69958095
DDF55BAC8A30676A780B99B398E9DDCC84A2E8DC79E68240437D7C28D7D6B76A4155BE29F3018195D8CF8B7CA339308F09C1744459F751A837DB
85A3BD7E3323745773 76EAA9662E5692439CFCB0AF2D06833CC88D9CC371854AE33272D9469971B48A4C62BD2413A6F814DAD70C4680B0942B67
E5EF8CC1F9158573B40B4B6B9BC5E8D7EC7B32285EFFE51935D5F011493CA822378ED42D1F04FEF702FB8371DAF7902BE30CFA6C0185A42145D0
DE9AA73C5ACB5C111CA8C9BB
ike 0:VPN-to-SH:28:23: responder received first quick-mode message
ike 0:VPN-to-SH:28: dec
F7204652FA9357445B61D63B74CBB9F608102001854D6010000001DC01000024EA4C99A2785B85A08F8AD5DAEDD8227E2E23F7157394766515BE
32574DF3324A0A000058000000010000000100000004C0103040236826FEB03000020010C0000800100018002A8C08004000180060100800500 02
8003000E00000020020C0000800100018002A8C08004000180060100800500058003000E04000014153BB1F0FE1EC2D16347F6E59D9279EE0500
01044B6A54A5DE7C5BF9DD546C32A28508FEFBC9056F465563F366A20AA5318FFC514DF0800CD028DC7422634E749A1B85A4CA414501B87DE19F
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
DF9F6674BFAB35E224D5460FDD6A26D11A800DF0386403F850876F93BE32971442E8E4F235F307FED3C53AF74294B6989BDF38438A5595A50942
3235B2B820D57B344870F03F999C712458DD13A2A36047370CB5917097D54D6B7E8D320BADD3B292FF2D089AD0923DE2AE9116B7CB98DFCAED4A
97D7DF7FA9391EAD63F121C4C24BA8E11FBD590F2459296C6B750745C67B165CE6A0D16A3A9E6CDC2621470412544C4C29BF6912EA9BFEB8811E
08459CF098E6C6401228568B632BB267E10593E6AF1A9272724A0500001004000000C0A80100FFFFFF0000000001004000000C0A80000FFFFFF00
2BDD3013B2168B798A40790B
ike 0:VPN-to-SH:28:23: peer proposal is: peer:0:192.168.1.0-192.168.1.255:0, me:0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:28:VPN-to-SH:23: trying
ike 0:VPN-to-SH:28:VPN-to-SH:23: matched phase2
ike 0:VPN-to-SH:28:VPN-to-SH:23: autokey
ike 0:VPN-to-SH:28:VPN-to-SH:23: my proposal:
ike 0:VPN-to-SH:28:VPN-to-SH:23: proposal id = 1:
ike 0:VPN-to-SH:28:VPN-to-SH:23:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:28:VPN-to-SH:23:   PFS DH group = 14
ike 0:VPN-to-SH:28:VPN-to-SH:23:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:28:VPN-to-SH:23:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:28:VPN-to-SH:23:         type = AUTH_ALG, val=SHA2_512
ike 0:VPN-to-SH:28:VPN-to-SH:23: proposal id = 2:
ike 0:VPN-to-SH:28:VPN-to-SH:23:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:28:VPN-to-SH:23:   PFS DH group = 5
ike 0:VPN-to-SH:28:VPN-to-SH:23:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:28:VPN-to-SH:23:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:28:VPN-to-SH:23:         type = AUTH_ALG, val=SHA2_512
ike 0:VPN-to-SH:28:VPN-to-SH:23: incoming proposal:
ike 0:VPN-to-SH:28:VPN-to-SH:23: proposal id = 1:
ike 0:VPN-to-SH:28:VPN-to-SH:23:   protocol id = IPSEC_ESP:
ike 0:VPN-to-SH:28:VPN-to-SH:23:   PFS DH group = 14
ike 0:VPN-to-SH:28:VPN-to-SH:23:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:28:VPN-to-SH:23:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:28:VPN-to-SH:23:         type = AUTH_ALG, val=SHA1
ike 0:VPN-to-SH:28:VPN-to-SH:23:      trans_id = ESP_AES_CBC (key_len = 256)
ike 0:VPN-to-SH:28:VPN-to-SH:23:      encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:VPN-to-SH:28:VPN-to-SH:23:         type = AUTH_ALG, val=SHA2_256
ike 0:VPN-to-SH:28:VPN-to-SH:23: negotiation failure
ike Negotiate IPsec SA Error: ike 0:VPN-to-SH:28:23: no SA proposal chosen
ike 0:VPN-to-SH:23: info_send_n2, type 14, peer SPI 36826feb
ike 0:VPN-to-SH:28: enc
F7204652FA9357445B61D63B74CBB9F608100501D001250C000000500B000024DA181A96FDB1E05A810C664047DA00EE6AC66F194C9549253F32
2B804C59869000000010000000010304000E36826FEB
ike 0:VPN-to-SH:28: out
F7204652FA9357445B61D63B74CBB9F608100501D001250C0000005C3A5150D6C379B62DDE5EB654F552CE2C5FB1022E78DE45FD65FA1FDE284B
57EA3AC4DD593068FECBE6A60DBADB418C54B61E2C9C2C415BB5323CB41283CFFA87
ike 0:VPN-to-SH:28: sent IKE msg (p2_notify_14): 100.1.1.2:500→200.1.1.2:500, len=92, vrf=0,
id=f7204652fa935744/5b61d63b74cbb9f6:d001250c
ike 0:VPN-to-SH:28: error processing quick-mode message from 200.1.1.2 as responder
ike shrank heap by 159744 bytes
```

感兴趣流不匹配

从Debug显示specified selectors mismatch，对比两端感兴趣流peer: type=7/7, local=0:192.168.0.0-192.168.0.255:0, remote=0:192.168.1.0-192.168.1.255:0和mine: type=7/7, local=0:192.168.0.0-192.168.0.255:0, remote=0:192.168.10.0-192.168.10.255:0是不匹配的，因此协商失败。

```bash
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=9bbf928209f22769/0000000000000000 len=656 vrf=0
ike 0: in
9BBF928209F22769000000000000000000011004000000000000000290040000B400000001000000010000000A801010004030000280101000080B
0001000C000400015180800100078 00E00808003000180020004800400050300002802010000800B0001000C000400015180800100078 00E0100
80030001800200048004000503000028030100008 00B0001000C000400015180800100078 00E00808003000180020002800400050000000280401
0000800B0001000C000400015180800100078 00E0100800300018002000280040005 0A0000C499A094C58E0633FF797B3EF770CB35722E912E05
33C5C6657BDC1883DB5EB8B8D704EE6D5405EAD5CAE35B54698AAB9E4B2B18D285BE7A0F3C4BF05DB4E86E8F080A723FE26C667B17D52F1C95F1
E8960A94377D36CBDBADC70D355E7BB3557D2BAF27572B634183ACA7914686E2B09871469BAF9DA137915F60C17DC1FABCA750E380641AB53665
BFA7D3CFB3037B8DD8600E92551B6733CE4A2DE9D528A39E495D23BEB48455FFD88570E68DA43E9318D348675FBB93AF3362B6DFBAC499C40500
0024EA3AFD1354F3F8794D04364A1DA75C09290F121FD2A23F751D01BE3635C3C1980D00000C01000000C80101020D0000144A131C8107035845
5C5728F20E95452F0D0000147D9419A65310CA6F2C179D9215529D560D000014CD60464335DF21F87CFDB2FC68B6A4480D00001490CB80913EBB
696E086381B5EC427B1F0D00001416F6CA16E4A4066D83821A0F0AEAA8620D0000144485152D18B6BBCD0BE8A8469579DDCC0D000014AFCAD713
68A1F1C96B8696FC775701000D0000144048B7D56EBCE88525E7DE7F00D6C2D30D0000184048B7D56EBCE88525E7DE7F00D6C2D3C00000000000
00148299031757A36082C6A621DE00000000
ike 0:9bbf928209f22769/0000000000000000:29: responder: aggressive mode get 1st message ...
ike 0:9bbf928209f22769/0000000000000000:29: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:9bbf928209f22769/0000000000000000:29: VID draft-ietf-ipsec-nat-t-ike-03 7D9419A65310CA6F2C179D9215529D56
ike 0:9bbf928209f22769/0000000000000000:29: VID draft-ietf-ipsec-nat-t-ike-02 CD60464335DF21F87CFDB2FC68B6A448
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ike 0:9bbf928209f22769/0000000000000000:29: VID draft-ietf-ipsec-nat-t-ike-02\n 90CB80913EBB696E086381B5EC427B1F
ike 0:9bbf928209f22769/0000000000000000:29: VID draft-ietf-ipsec-nat-t-ike-01 16F6CA16E4A4066D83821A0F0AEAA862
ike 0:9bbf928209f22769/0000000000000000:29: VID draft-ietf-ipsec-nat-t-ike-00 4485152D18B6BBCD0BE8A8469579DDCC
ike 0:9bbf928209f22769/0000000000000000:29: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:9bbf928209f22769/0000000000000000:29: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:9bbf928209f22769/0000000000000000:29: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:9bbf928209f22769/0000000000000000:29: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0::29: peer identifier IPV4_ADDR 200.1.1.2
ike 0: cache rebuild start
ike 0:VPN-to-SH: local:100.1.1.2, remote:200.1.1.2
ike 0:VPN-to-SH: cached as static-ddns.
ike 0: cache rebuild done
ike 0:9bbf928209f22769/0000000000000000:29: negotiation result
ike 0:9bbf928209f22769/0000000000000000:29: proposal id = 1:
ike 0:9bbf928209f22769/0000000000000000:29:   protocol id = ISAKMP:
ike 0:9bbf928209f22769/0000000000000000:29:      trans_id = KEY_IKE.
ike 0:9bbf928209f22769/0000000000000000:29:      encapsulation = IKE/none
ike 0:9bbf928209f22769/0000000000000000:29:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:9bbf928209f22769/0000000000000000:29:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:9bbf928209f22769/0000000000000000:29:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:9bbf928209f22769/0000000000000000:29:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:9bbf928209f22769/0000000000000000:29: ISAKMP SA lifetime=86400
ike 0:9bbf928209f22769/0000000000000000:29: SA proposal chosen, matched gateway VPN-to-SH
ike 0:VPN-to-SH: created connection: 0×9b57be0 10 100.1.1.2→200.1.1.2:500.
ike 0:VPN-to-SH:29: DPD negotiated
ike 0:VPN-to-SH:29: peer is FortiGate/FortiOS (v0 b0)
ike 0:VPN-to-SH:29: selected NAT-T version: RFC 3947
ike 0:VPN-to-SH:29: generate DH public value request queued
ike 0:VPN-to-SH:29: compute DH shared secret request queued
ike 0:VPN-to-SH:29: cookie 9bbf928209f22769/1912fc364606cdf2
ike 0:VPN-to-SH:29: ISAKMP SA 9bbf928209f22769/1912fc364606cdf2 key 16:6F0A5C5D7ABE1862A0754D4F67F6C309
ike 0:VPN-to-SH:29: out
9BBF928209F227691912FC364606CDF201100400000000000000002110400003C000000010000000100000030010100010000002801010000800B
0001000C000400015180800100078 00E00808003000180020004800400050A0000C4789B20D8E6155283C87B6C929A2CE7FC886FDB69F26FE13B
B5BCD92C73B0F2BDC7A495FB095CC5CED439F41DB332A22594A9128635D392BB8D511BA38FF3984BCD092FBC7AF4E22FC8CD25BF91FA6D0334B1
2D4ED2FAC4FD061A7C199BFC6C19613645D9729D57D80003CF347B5B51D545EE9B5560904DC8A071A9291F42F948A61CDDB99915C0757FE13411
153AF6CB42FB8BE04873F606280B3AFDCB7B817A1D4106364F934F64936DBB595681EEF360CC887FCBD456657FA8497FCA18471A05000014FAFD
06AA2EB8122B83A734FAF066A39F0800000D020000074657374310D0000249471A719861E95E1CBF1723784350CC0876E57B07E6FA74D06A0B3
F4F81AD3F2140000144A131C81070358455C5728F20E95452F1400002493E1BF9E618E0E5225FEE63AB09074A2ED8DADEDE66B1D79F009C96C00
6B13E60D000024CB2EC39A82D1FEE194284F072DA1FE064954BC8059215C114AE94739631B63C40D000014AFCAD71368A1F1C96B8696FC775701
000D0000148299031757A36082C6A621DE00000000D0000144048B7D56EBCE88525E7DE7F00D6C2D3000000184048B7D56EBCE88525E7DE7F00
D6C2D3C0000000
ike 0:VPN-to-SH:29: sent IKE msg (agg_r1send): 100.1.1.2:500→200.1.1.2:500, len=529, vrf=0,
id=9bbf928209f22769/1912fc364606cdf2
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Aggressive id=9bbf928209f22769/1912fc364606cdf2 len=172 vrf=0
ike 0: in
9BBF928209F227691912FC364606CDF208100401000000000000000ACF2D87D3D3C57A87AA9FBEEFD034859AFC9AF00BEBEB1BB1FA731127B48EA
D6C7AA5B0FA8D84E6446D502E242937B83F222A23BD25C31095752FEFF3C97C3095B698EE63122D4E47925CD95D7F1FF2B793BA587D4EC882D3D
10804C395C24CB12AEFC208B3C7DB4793889FB5CDAD64831290EAA5AE65FD7DE10AE60D80109162F1F9C769F1F57059FCED85A10BCA12E70
ike 0:VPN-to-SH:29: responder: aggressive mode get 2nd response ...
ike 0:VPN-to-SH:29: dec
9BBF928209F227691912FC364606CDF208100401000000000000000AC14000024A31F2CDD20D257FD8CB06D9FEA96472FD20E34599130F73928E0
E24B80D81FE914000024CB2EC39A82D1FEE194284F072DA1FE064954BC8059215C114AE94739631B63C40B00002493E1BF9E618E0E5225FEE63A
B09074A2ED8DADEDE66B1D79F009C96C006B13E60000001C00000001011060029BBF928209F227691912FC364606CDF279B09DF11828DE07
ike 0:VPN-to-SH:29: received NAT-D payload type 20
ike 0:VPN-to-SH:29: received NAT-D payload type 20
ike 0:VPN-to-SH:29: received p1 notify type INITIAL-CONTACT
ike 0:VPN-to-SH:29: PSK authentication succeeded
ike 0:VPN-to-SH:29: authentication OK
ike 0:VPN-to-SH:29: NAT not detected
ike 0:VPN-to-SH:29: established IKE SA 9bbf928209f22769/1912fc364606cdf2
ike 0:VPN-to-SH:29: check peer route: if_addr4_rcvd=0, if_addr6_rcvd=0, mode_cfg=0
ike 0:VPN-to-SH:29: processing INITIAL-CONTACT
ike 0:VPN-to-SH: flushing
ike 0:VPN-to-SH: flushed
ike 0:VPN-to-SH:29: processed INITIAL-CONTACT
ike 0:VPN-to-SH: set oper up
ike 0:VPN-to-SH:29: no pending Quick-Mode negotiations
ike 0: comes 200.1.1.2:500→100.1.1.2:500,ifindex=10,vrf=0....
ike 0: IKEv1 exchange=Quick id=9bbf928209f22769/1912fc364606cdf2:29a1bf3f len=412 vrf=0
ike 0: in
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
9BBF928209F227691912FC364606CDF20810200129A1BF3F0000019CA256FBF54CF315B0F0D3EBA8234DEF95082641935CBC5CF69FD677D3657F
B02E591720692F3706441317346555CA0F5FC750F4202A8459C159C3892443B4A1537AA863AD33883432E73F63C1406D12043F142C79E1BAAA33
10248865F52BE530725EA7DBF2A00E9E5E5A1C3942D96BD979F2FD4C43071680651F142C015A47351772636C667AD010EAA6A9971A9D52B2553E
954C9590FC03C7D252600CDBEB16E4CB8E913AA3992A2986EE68D44774CD5F1F253BF07FB7AF649189E2D8EF982FEC6EBFD89C0F2B6CBD5EDFDD
65A93353A3497AA73932C546DBDD94F900977EDCBF058144FA0B69508000E017A97BB075968D854547FC55ECFA841B356563E32D41413B3813B0
DB32B3E4C8CDE3DF159F96F6B887D2AB5480D0A36FBFD657A1F1D89868DC78860903A1CDA173B655022112B15F5DE6A14430D998F230F041355C
61D20829D9BA9CAF3CE57D58DD8425CD37E0A9BEE5514FDB7159AFB8398FDAFCB077499CA00FA4FCA9F1BC9A5B2208DFE69B2C041C85442669A6
A1D23E8133AD
ike 0:VPN-to-SH:29:25: responder received first quick-mode message
ike 0:VPN-to-SH:29: dec
9BBF928209F227691912FC364606CDF20810200129A1BF3F0000019C0100002458D9086AFB973BD12DB26A7870A43555F16C84F66FDA55240152
0C92832D79BE0A000058000000010000000100000004C0103040236826FEC03000020010C0000800100018002A8C0800400018006010080050002
8003000500000020020C0000800100018002A8C0800400018006010080050005800300050400001406 2F996DD325B8E32EB8B8EDDE3D48C40500
00C4D0A802E07811F15FB57E6A8DC7C46D9E4EC6BB5580F531B24787DCC36DB6A9B2D04B13A0FE462CC4348B4C3434CBFC3E887FCF6BD982ABF9
E06E24AB4B3A88C6416FCE8BC58A45F97226F2F59C63758AFC7112483C3C4BF357F35DF1351267ED3004C6A8CAE54F7FFAEC67482CD3FDC9CC4C
53A176B4A3C3DC6D62A2948C08071A8D5B616A55284CD82A1D89E021E67A5A05AFDD3B3F2FEB0DC8251B8E70D4ED71E83655B7E6E8CFB5BFF09E
433594BF8D4CE68CDC3656BAC89C067E84A3BA9A0500001004000000C0A80100FFFFFF00000000100400000C0A80000FFFFFF005F66F91E52BA
59DB99E4F90B
ike 0:VPN-to-SH:29:25: peer proposal is: peer:0:192.168.1.0-192.168.1.255:0, me:0:192.168.0.0-192.168.0.255:0
ike 0:VPN-to-SH:29:VPN-to-SH:25: trying
ike 0:VPN-to-SH:29:25: specified selectors mismatch
ike 0:VPN-to-SH:29:25: peer: type=7/7, local=0:192.168.0.0-192.168.0.255:0, remote=0:192.168.1.0-192.168.1.255:0
ike 0:VPN-to-SH:29:25: mine: type=7/7, local=0:192.168.0.0-192.168.0.255:0, remote=0:192.168.10.0-192.168.10.255:0
ike 0:VPN-to-SH:29:25: no matching phase2 found
ike 0:VPN-to-SH:29:25: failed to get responder proposal
ike 0:VPN-to-SH:29: error processing quick-mode message from 200.1.1.2 as responder
```

IKEv2重协商失败

1. 使用IKEv2，且感兴趣流只有一对保护网段时，一定要注意两端二阶段的PFS配置是否一致，如果不一致，可能会导致第一次IPSec协商成功，但后续重协商时失败。
2. 这是由于IKEv2在第一次协商时，二阶段的SA包含在IKE_AUTH报文中，而IKE_AUTH中携带的SA是无法使用PFS的，所以即使两端PFS配置不一致（例如一端开启另一端不开启，或配置的PFS DH组不一致），第一次协商连接也是可以正常建立的。
3. 但重协商（rekey）时，使用的是Create_Child_SA报文携带SA信息，Create_Child_SA会按照用户配置携带PFS信息，这时如果两端的PFS配置不一致，会导致IKEv2重协商时协商失败。
4. 使用如下命令（childless-ike）可以强制FortiGate使用Child SA携带二阶段SA（IKE_AUTH中不携带二阶段SA，所有二阶段SA必须通过Create_Child_SA协商，注意使用此功能时对端设备也必须支持并开启此功能）。

```bash
config vpn ipsec phase1-interface
    edit xxxx
        set ike-version 2
        set childless-ike enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec命名注意事项

注意事项1

ADVPN环境下，有时候会遇到所有Spoke与Hub的IPSec连接建立成功，但Spoke之间在流量触发后，Shortcut连接无法建立的情况。

问题现象

1. 检查Spoke与Hub间的IPSec连接状态是否正常。

2. 在Spoke上执行IKE Debug，检查输出日志，如下所示，Spoke已经收到了Hub返回的shortcut-offer：

```
# diagnose debug application ike -1
# diagnose debug enable
```

```
ike 0:FGT-ADVPN-HUB-1:17: notify msg received: SHORTCUT-OFFER
ike 0:FGT-ADVPN-HUB-1: shortcut-offer 172.26.22.22→172.10.10.1 psk 64 ppk 0 ver 1 mode 0
ike 0 looking up shortcut by addr 172.10.10.1, name FGT-ADVPN-HUB-1
```

3. 问题出现在另一个Spoke发送的shortcut-reply后，当Spoke收到另一个Spoke发送的shortcut-reply（经由Hub转发）后，准备与其建立Shortcut连接，但由于Shortcut连接的名字过长（Shortcut连接的名字是在与Hub的连接名称基础上加上字符“_[number]”，FGT-ADVPN-HUB-1_0），导致无法发起Shortcut连接。

```bash
ike 0:FGT-ADVPN-HUB-1:17: notify msg received: SHORTCUT-REPLY
ike 0:FGT-ADVPN-HUB-1: recv shortcut-reply 17386919350863387436 3d31b000f3a4cb20/918e5c255a8451ca 10.10.50.1 to
172.26.22.22 psk 64 ppk 0
 ver 1 mode 0 ext-mapping 0.0.0.0:0
ike 0:FGT-ADVPN-HUB-1: iif 28 172.10.10.1→172.26.22.22 route lookup oif 12 root
ike 0:FGT-ADVPN-HUB-1: shortcut-reply received from 10.10.50.1:500, local-nat=no, peer-nat=no
ike 0:FGT-ADVPN-HUB-1: created connection: 0×dd3cdb0 5 10.10.10.2→10.10.50.1:500.
ike 0:FGT-ADVPN-HUB-1: adding new dynamic tunnel for 10.10.50.1:500
ike 0:FGT-ADVPN-HUB-1: could not create dialup name FGT-ADVPN-HUB-1_0, too long
ike 0:FGT-ADVPN-HUB-1: deleting
ike 0:FGT-ADVPN-HUB-1: deleted
ike 0:FGT-ADVPN-HUB-1: schedule auto-negotiate
```

4. 检查Spoke端的IPSec一阶段配置，名称为FGT-ADVPN-HUB-1，总计15个字符。

```
# config vpn ipsec phase1-interface
    edit "FGT-ADVPN-HUB-1"
        set interface "wan1"
        set keylife 28800
        set peertype any
        set net-device enable
        set proposal aes256-sha256
        set add-route disable
        set dpd on-idle
        set dhgrp 14
        set auto-discovery-receiver enable
        set remote-gw x.x.x.x
        set psksecret ENC
        set dpd-retryinterval 5
    next
```

解决方法

1. 当配置IPSec VPN时，对名字的长度限制为15个字符，超过15个字符是无法配置的。
2. 但如果存在ADVPN的配置，当Spoke与Spoke之间触发Shortcut连接建立时，Shortcut连接的名称会在与Hub的连接名称的基础上加上字符`_`+数字（从0开始），例如以上示例中，Shortcut连接的名称为“FGT-ADVPN-HUB-1_0”，这已经超过了15个字符，这就导致Shortcut连接由于名字过长无法发起连接建立。
3. 如果是ADVPN部署环境，建议在Spoke上配置与Hub的IPSec连接时，名称长度建议小于12个字符（根据最多可以建立多少个Shortcut决定，例如需要建立2位数数量的Shortcut连接，使用13个字符的IPSec连接名称，从第10个Shortcut连接开始将无法建立）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项2

在同一个FortiGate上配置了一个IPSec连接的名称后，新增其他IPSec连接配置时，名称不要使用已创建的IPSec连接名称 + `_<number>` 的格式，例如：

- 第1个IPSec连接（拨号模式）：名称为 `CT` 。
- 第2个IPSec连接：不要配置名称为 `CT_0` （或 `CT_1` 、 `CT_2` 、 `CT_3` ……）。

这是由于第1个IPSec拨号连接有客户端拨号成功后，生成的动态IPSec隧道名称会被命名为 `CT_0` 、 `CT_1` 、 `CT_2` 、 `CT_3` ……这些名称中的 `CT_0` 与第2个IPSec连接的名称冲突，会导致第2个IPSec连接无法正常通信，即使两个IPSec连接在不同的VDOM（即使开启了VDOM，任何接口的名称也具有全局唯一性）。

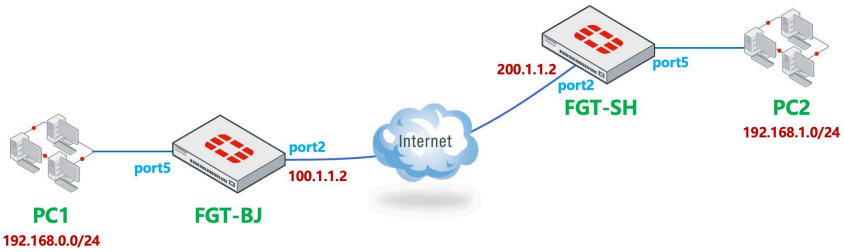
出现此问题时，受影响的IPSec接口的状态会出现异常，使用 `diagnose netlink interface list` 可以看到该接口（CT_1）的link≠0（接口的link只有等于0时才正常）。

```bash
Hub (VDOM2) # diagnose netlink interface list

......
if=CT_1 family=00 type=768 index=23 mtu=1420 link=24 master=0    //受影响的IPSec隧道名称，link≠0//
flags=up p2p run noarp multicast

if=CT family=00 type=768 index=24 mtu=1420 link=0 master=0
flags=up p2p run noarp multicast
......
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec业务不通问题

网络拓扑



隧道UP了，但是业务不通，如何排查

1. 抓包查看数据是否通过IPSEC接口转发

```
# diagnose sniffer packet any icmp 4
interfaces=[any]
filters=[icmp]
2.615008 port5 in 192.168.0.10 → 192.168.1.10: icmp: echo request
2.615030 VPN-to-SH out 192.168.0.10 → 192.168.1.10: icmp: echo request     #VPN-to-SH是IPSEC接口
2.615891 VPN-to-SH in 192.168.1.10 → 192.168.0.10: icmp: echo reply
2.616067 port5 out 192.168.1.10 → 192.168.0.10: icmp: echo reply
```

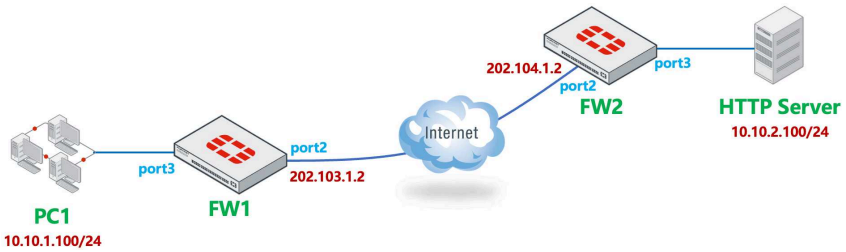
2. 通过Debug Flow查看匹配的策略和路由是否正确

```
#diagnose debug flow filter addr 192.168.1.10
#diagnose debug flow show function-name enable
#diagnose debug console timestamp enable
#diagnose debug flow trace start 5
#diagnose debug enable

从PC1 192.168.0.10 ping PC2 192.168.1.10 第1个数据包 echo request
2022-12-30 17:50:12 id=20085 trace_id=1 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
192.168.0.10:23728→192.168.1.10:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=23728, seq=1."
2022-12-30 17:50:12 id=20085 trace_id=1 func=init_ip_session_common line=6024 msg="allocate a new session-
00003fab, tun_id=0.0.0.0"
2022-12-30 17:50:12 id=20085 trace_id=1 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000
gw-200.1.1.2 via VPN-to-SH"
2022-12-30 17:50:12 id=20085 trace_id=1 func=fw_forward_handler line=881 msg="Allowed by Policy-4:"
2022-12-30 17:50:12 id=20085 trace_id=1 func=ipsecdev_hard_start_xmit line=669 msg="enter IPSec interface VPN-to-
SH, tun_id=0.0.0.0"
2022-12-30 17:50:12 id=20085 trace_id=1 func=_do_ipsecdev_hard_start_xmit line=229 msg="output to IPSec tunnel
VPN-to-SH"
2022-12-30 17:50:12 id=20085 trace_id=1 func=esp_output4 line=844 msg="IPsec encrypt/auth"
2022-12-30 17:50:12 id=20085 trace_id=1 func=ipsec_output_finish line=544 msg="send to 100.1.1.1 via intf-port2"

PC2到PC1的响应包 echo reply
2022-12-30 17:50:12 id=20085 trace_id=2 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
192.168.1.10:23728→192.168.0.10:0) tun_id=200.1.1.2 from VPN-to-SH. type=0, code=0, id=23728, seq=1."
2022-12-30 17:50:12 id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
00003fab, reply direction"
2022-12-30 17:50:12 id=20085 trace_id=2 func=vf_ip_route_input_common line=2605 msg="find a route: flag=00000000
gw-192.168.0.10 via port5"
2022-12-30 17:50:12 id=20085 trace_id=2 func=npu_handle_session44 line=1183 msg="Trying to offloading session from
VPN-to-SH to port5, skb.npu_flag=00000000 ses.state=00010200 ses.npu_state=0×05040000"
2022-12-30 17:50:12 id=20085 trace_id=2 func=fw_forward_dirty_handler line=410 msg="state=00010200,
state2=00000000, npu_state=05040000"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

ESP分片丢包

网络拓扑



网络配置

1. 基础网络配置（略）。

2. FW1的IPSec配置，静态模式的IPSec IKEv2连接，中间没有NAT穿越。

> **重要**
>
> 默认配置下IPSec的分片方式为post-encapsulation（后封装），IPSec隧道在收到任何需要ESP封装的报文时，不考虑IPSec Tunnel接口的MTU，先将明文封装到ESP中（如果明文已经是分片包，则会先重组明文分片），直接发送至公网接口。从公网接口发出时，再根据公网接口的MTU（默认为1500 Bytes）对ESP报文进行分片。这种post-encapsulation（后封装）方式符合RFC标准。

```bash
config vpn ipsec phase1-interface
    edit "VPN_to_FW2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set ip-fragmentation post-encapsulation    //默认配置//
        set dpd on-idle
        set remote-gw 202.103.13.2
        set psksecret ENC
A/oFySlyF2xkGInFX2pcoKpiQAgFb7xyVO4YaJ01IKQzYWPNOClbem+A/JpdLQUUaw+936tj6UC4LjW3Zivxgzl/9N3QZk8WlEBJUO/HrdWrUL=
    next
end

config vpn ipsec phase2-interface
    edit "VPN_to_FW2"
        set phase1name "VPN_to_FW2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

3. FW2的IPSec配置。

```bash
config vpn ipsec phase1-interface
    edit "VPN_to_FW1"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set ip-fragmentation post-encapsulation    //默认配置//
        set dpd on-idle
        set remote-gw 202.103.12.2
        set psksecret ENC
mBPuOPm3FhObt60JaaO6ac0T0YsD/8sYru2PKnbY5V1y/3ljX+fA22/WCKbqTAHzhd45dz9yTlZ/qQ/ajGemn+UuMcHnrdeVPEwTrbDi6oP0om=
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config vpn ipsec phase2-interface
    edit "VPN_to_FW1"
        set phase1name "VPN_to_FW1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set auto-negotiate enable
    next
end
```

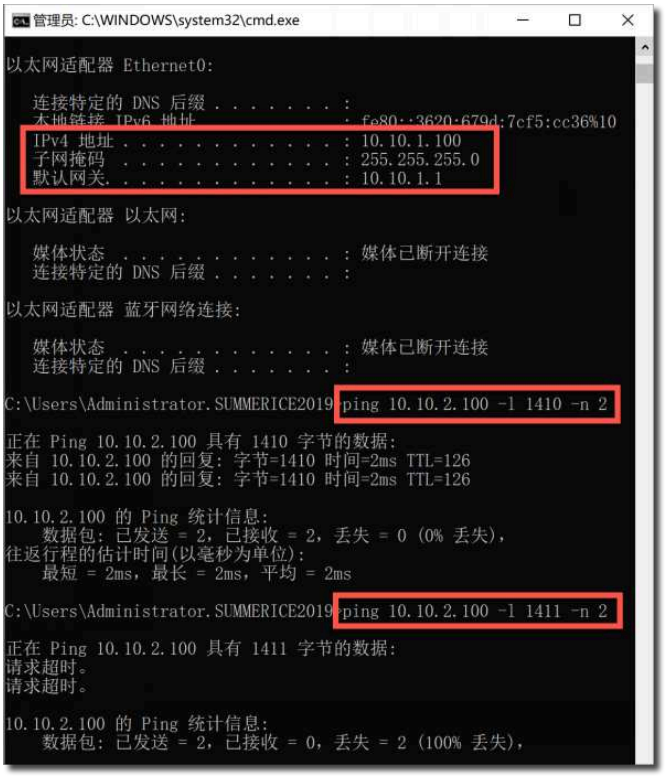
4. 查看IPSec二阶段状态，可以看到options中有`frag-rfc`标记，表示分片方式为RFC标准（post-encapsulation，后封装）。

```bash
FW1 # diagnose vpn tunnel list | grep options
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_state=0 role=primary
accept_traffic=1 overlay_id=0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1230 expire=42024/0B replaywin=2048
```

问题现象

1. PC1与HTTP Server可以互相Ping通，通过SMB传输文件也没有问题。

2. 当PC1和HTTP Server使用较大的data-size（当前IPSec算法 + 非NAT-T环境下，超过1410 Bytes）互Ping时，无法Ping通。



3. 较大的UDP报文（产生了分片）无法传输。

问题原因

1. 当较大的ICMP、UDP等报文无法通过IPSec隧道传输时，就要考虑运营商是否有丢弃ESP分片报文的动作了。

2. 以ICMP包为例，PC1 Ping HTTP Server，data-size=1600，无法Ping通。

```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
Windows IP 配置
以太网适配器 Ethernet0:
   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . : fe80::3620:679d:7cf5:cc36%10
   IPv4 地址 . . . . . : 10.10.1.100
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . : 10.10.1.1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

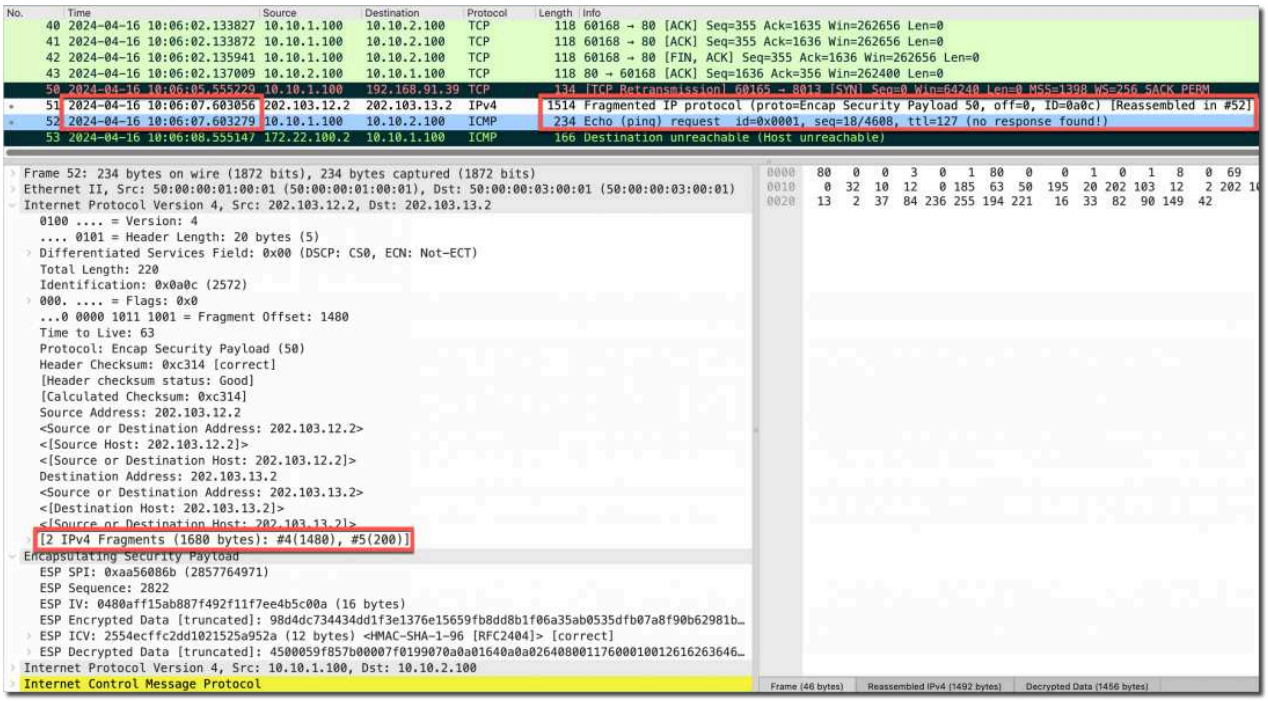
```
C:\Users\Administrator.SUMMERICE2019>ping 10.10.2.100 -t -l 1600 -n 1
正在 Ping 10.10.2.100 具有 1600 字节的数据:
请求超时。

10.10.2.100 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 0, 丢失 = 1 (100% 丢失)
```

3. 在FW1上抓取目标地址为10.10.2.100的数据包，PC1发出的Ping request报文被分为两片（第1片去掉IP头的长度为1480 Bytes，第2片去掉IP头的长度为128 Bytes），进入IPSec接口后，被重组为一个包（加上IP头部的总长度为1628 Bytes）。

> **重要**
>
> FortiGate默认的IP分片方式为后封装，即先重组分片报文，再封装ESP，然后从业务接口发出时根据接口MTU对ESP报文进行分片。

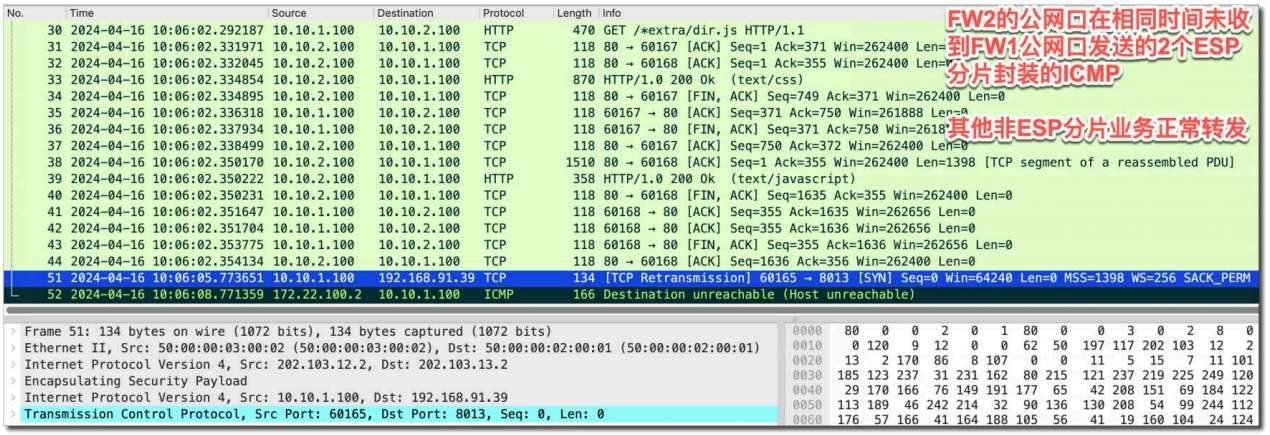
```bash
FW1 # diagnose sniffer packet any 'host 10.10.2.100' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.100]
2024-04-12 14:08:00.664087 port3 in 10.10.1.100 → 10.10.2.100: icmp: echo request (frag 36352:1480@0+)
2024-04-12 14:08:00.664107 port3 in 10.10.1.100 → 10.10.2.100:  ip-proto-1 (frag 36352:128@1480)
2024-04-12 14:08:00.664179 VPN_to_FW2 out 10.10.1.100 → 10.10.2.100: icmp: echo request
```

4. 同时在FW1的公网接口（port2）上抓取向FW2发送的ESP报文（如果是NAT-T环境，则需要抓取UDP 4500报文）并解密（抓取ESP及解密步骤请参考VPN技术→IPSec VPN→IPSec VPN排错→IPSec解密↗章节），可以看到步骤3中进入IPSec隧道并重组的ICMP报文被ESP封装，封装ESP后的总大小为1688 Bytes（包含IP头部），从port2发送时，由于port2的MTU为1500 Bytes（默认配置），需要分成2片后发出，这样就产生了ESP分片。其他的业务没有产生ESP分片。



5. 在FW2的公网接口（port2）抓取ESP报文（如果是NAT-T环境，则需要抓取UDP 4500报文）并解密（解密步骤请参考VPN技术→IPSec VPN→IPSec VPN排错→IPSec解密↗章节），没有收到步骤4中抓到的两片ESP报文（封装ICMP Request报文），只能收到没有分片的ESP报文（如下所示的被ESP封装且未分片的FTP业务正常转发和使用，但没有抓到步骤4中的两片封装ICMP的ESP）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 基本可以确定FW1发出的ESP分片在Internet上被丢弃，与FortiGate无关。

解决方法

- 联系运营商检查线路上的ESP分片丢包。
- 开启IPSec的预封装功能（pre-encapsulation），避免在Internet线路上出现ESP分片报文，本文着重介绍这种方法。

IPSec预封装

1. 在FW1和FW2的IPSec一阶段中将IP分片模式修改为预封装模式（pre-encapsulation），修改该配置后，隧道会发生重建。

> **重要**
>
> 将IPSec的分片方式修改为pre-encapsulation（预封装）后，IPSec隧道在收到任何需要ESP封装的报文时，会根据当前IPSec Tunnel接口的MTU，先将明文根据Tunnel接口的MTU进行分片（如果明文已经是分片包，则会先重组明文分片），对每一片明文分片封装ESP，然后从公网接口发出。
>
> 在IPSec绑定的公网接口MTU为1500（默认）的情况下，IPSec Tunnel接口的MTU被设置为1420 Bytes，确保封装ESP后的报文从IPSec绑定的公网接口发出时，不会超过1500 Bytes，从而避免了在公网线路上产生ESP分片（如果是AES256/SHA512算法 + NAT-T环境的组合，默认的1420是不行的，请参考这里 ↗ ）。
>
> 如果修改了公网接口的MTU值，IPSec Tunnel接口上的MTU值不会自动跟随修改。需要在Tunnel接口上手动跟随修改MTU值：
>
> - 例如使用AES128/SHA1算法组合，物理接口的MTU为1500，IPSec Tunnel接口的MTU为1420。
> - 客户因为网络需要将物理接口的MTU修改为1400，那么需要同步地将IPSec Tunnel接口的MTU修改为1320。
>
> 本文仅介绍物理口没有更改MTU的情况。

```bash
FW1:
config vpn ipsec phase1-interface
    edit "VPN_to_FW2"
        set ip-fragmentation pre-encapsulation
    next
end

FW2:
config vpn ipsec phase1-interface
    edit "VPN_to_FW1"
        set ip-fragmentation pre-encapsulation
    next
end
```

> **重要**
>
> 在“拨号用户（dynamic）”类型的IPSec一阶段配置中设置 `pre-encapsulation` 时：
>
> - 预封装功能不会立刻生效，必须重启设备或删除重配才能生效（在FortiOS 7.X上均存在此问题）。
> - 在新配置的IPSec一阶段中直接配置 `set ip-fragmentation pre-encapsulation` 可以直接生效。
>
> “静态IP地址（static）”模式的IPSec隧道不存在此问题。

2. 查看IPSec Tunnel接口的MTU值，IPSec Tunnel接口的MTU值为1420。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW1 # diagnose netlink interface list name VPN_to_FW2 | grep mtu
if=VPN_to_FW2 family=00 type=768 index=17 mtu=1420 link=0 master=0

FW2 # diagnose netlink interface list name VPN_to_FW1 | grep mtu
if=VPN_to_FW1 family=00 type=768 index=16 mtu=1420 link=0 master=0
```

3. 再次查看IPSec二阶段状态，可以看到options中的`frag-rfc`标记消失，表示分片方式为预封装（pre-encapsulation）。

```bash
FW1 # diagnose vpn tunnel list | grep options
bound_if=4 lgwy=static/1 tun=intf mode=auto/1 encap=none/40 options[0028]=npu  run_state=0 role=primary
accept_traffic=1 overlay_id=0
  SA:  ref=3 options=38203 type=00 soft=0 mtu=1230 expire=42899/0B replaywin=2048
```

4. 使用PC1 Ping HTTP Server，data-size=1600，这次可以Ping通了。

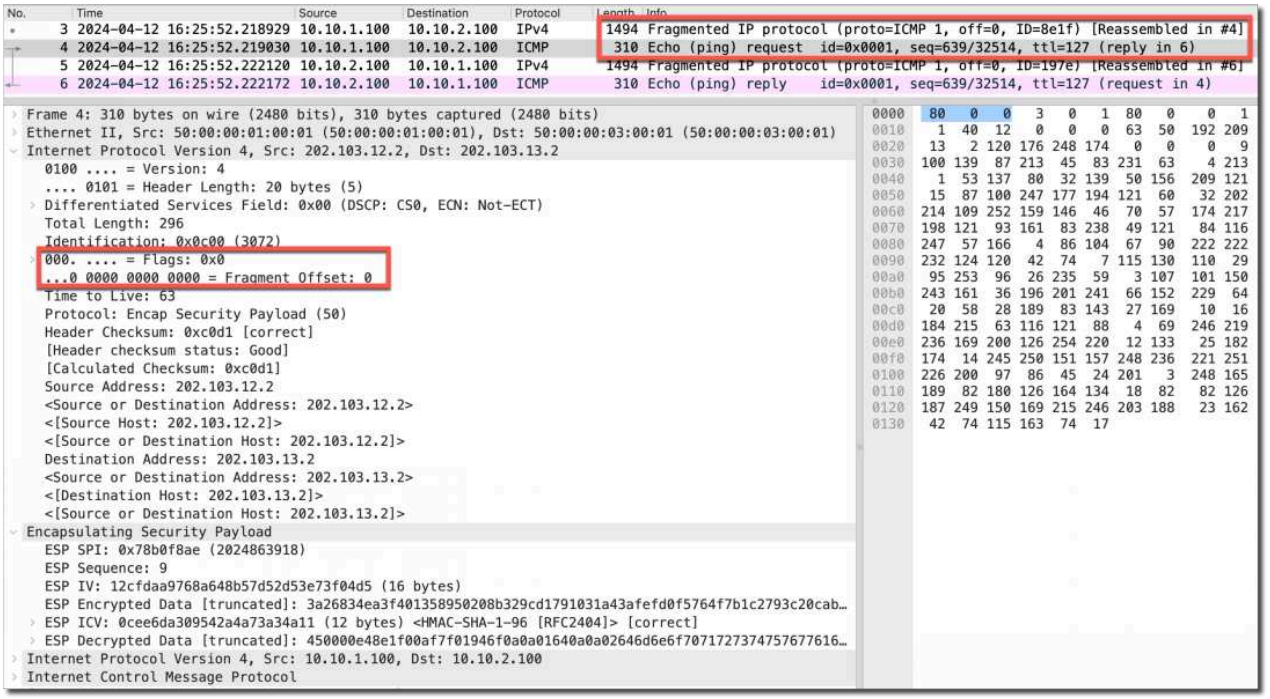
```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
Windows IP 配置
以太网适配器 Ethernet0:
   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::3620:679d:7cf5:cc36%10
   IPv4 地址 . . . . . . . . . . . . : 10.10.1.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.10.1.1

C:\Users\Administrator.SUMMERICE2019>ping 10.10.2.100 -t -l 1600 -n 1
正在 Ping 10.10.2.100 具有 1600 字节的数据:
来自 10.10.2.100 的回复: 字节=1600 时间=2ms TTL=126

10.10.2.100 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 2ms, 平均 = 2ms
```

5. 在FW1上抓取目标地址为10.10.2.100的数据包，PC1发出的Ping request报文被分为两片（第1片去掉IP头的长度为1480 Bytes，第2片去掉IP头的长度为128 Bytes），进入IPSec接口后，被重组为一个包（加上IP头部的总长度为1628 Bytes），随后根据IPSec Tunnel接口的MTU=1420 Bytes进行预分片，被分为两片（第1片去掉IP头的长度为1400 Bytes，第2片去掉IP头的长度为208 Bytes）。

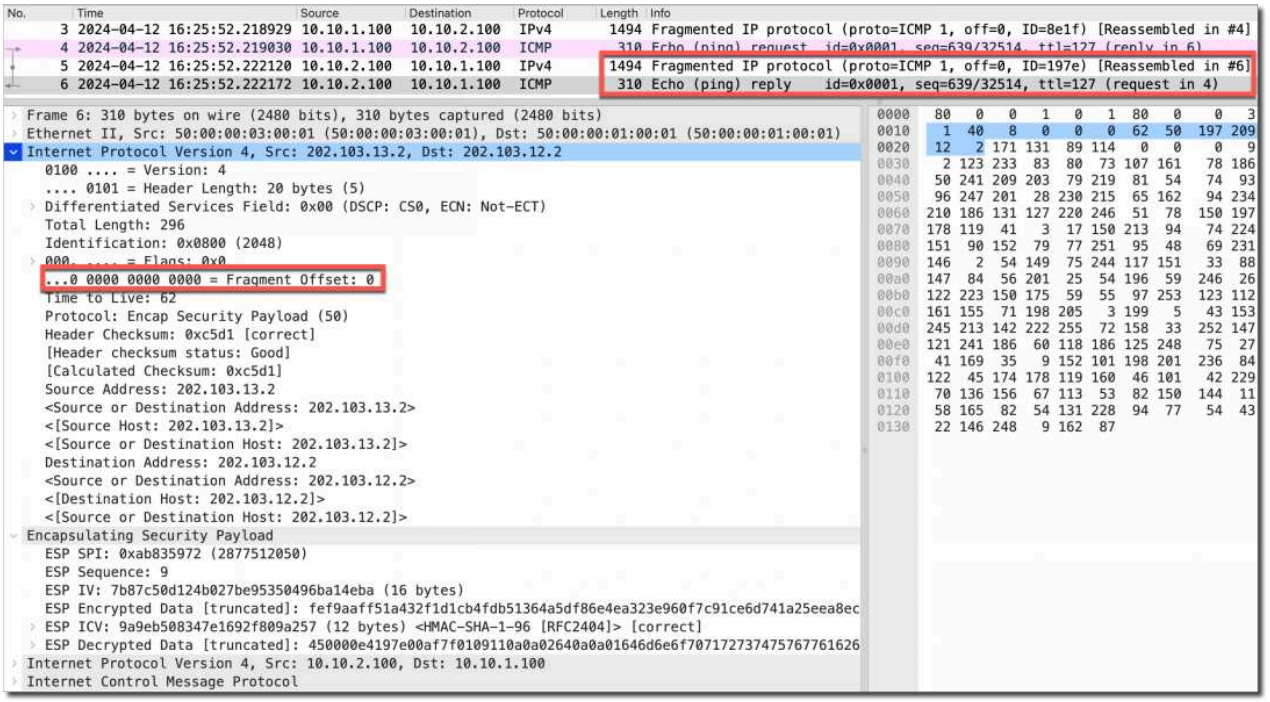
```bash
FW1 # diagnose sniffer packet any 'host 10.10.2.100' 4 0 l
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.100]
//Request方向//
2024-04-12 16:12:38.796118 port3 in 10.10.1.100 → 10.10.2.100: icmp: echo request (frag 36382:1480@0+)
2024-04-12 16:12:38.796139 port3 in 10.10.1.100 → 10.10.2.100:  ip-proto-1 (frag 36382:128@1480)
2024-04-12 16:12:38.796191 VPN_to_FW2 out 10.10.1.100 → 10.10.2.100: icmp: echo request (frag 36382:1400@0+)
2024-04-12 16:12:38.796271 VPN_to_FW2 out 10.10.1.100 → 10.10.2.100:  ip-proto-1 (frag 36382:208@1400)

//Reply方向//
2024-04-12 16:12:38.798245 VPN_to_FW2 in 10.10.2.100 → 10.10.1.100: icmp: echo reply (frag 6525:1400@0+)
2024-04-12 16:12:38.798297 VPN_to_FW2 in 10.10.2.100 → 10.10.1.100:  ip-proto-1 (frag 6525:208@1400)
2024-04-12 16:12:38.798317 port3 out 10.10.2.100 → 10.10.1.100: icmp: echo reply (frag 6525:1400@0+)
2024-04-12 16:12:38.798478 port3 out 10.10.2.100 → 10.10.1.100:  ip-proto-1 (frag 6525:208@1400)
```

6. 同时在FW1的公网接口（port2）上抓取向FW2发送的ESP报文（如果是NAT-T环境，则需要抓取UDP 4500报文）并解密（解密步骤请参考VPN技术→IPSec VPN→IPSec VPN排错→IPSec解密↗章节），可以看到步骤5中被预分片的2个ICMP分片报文分别被ESP封装，加密后的两个ESP包大小均未超过1500 Bytes（包含IP头部），从port2发送时，由于port2的MTU为1500 Bytes（默认配置），不需要进行分片，这样就不会产生ESP分片发送到Internet。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 返回的ICMP Reply也一样被FW2的IPSec进行预封装分片，没有在Internet线路上产生ESP分片。



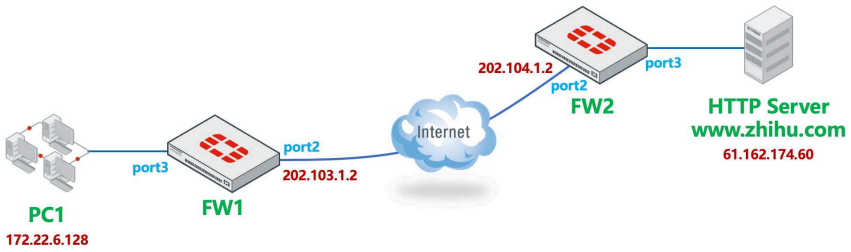
8. 这样就规避了Internet线路上丢弃ESP分片包导致的业务不通问题。

IPSec预封装对DF置位IP包的影响

问题现象

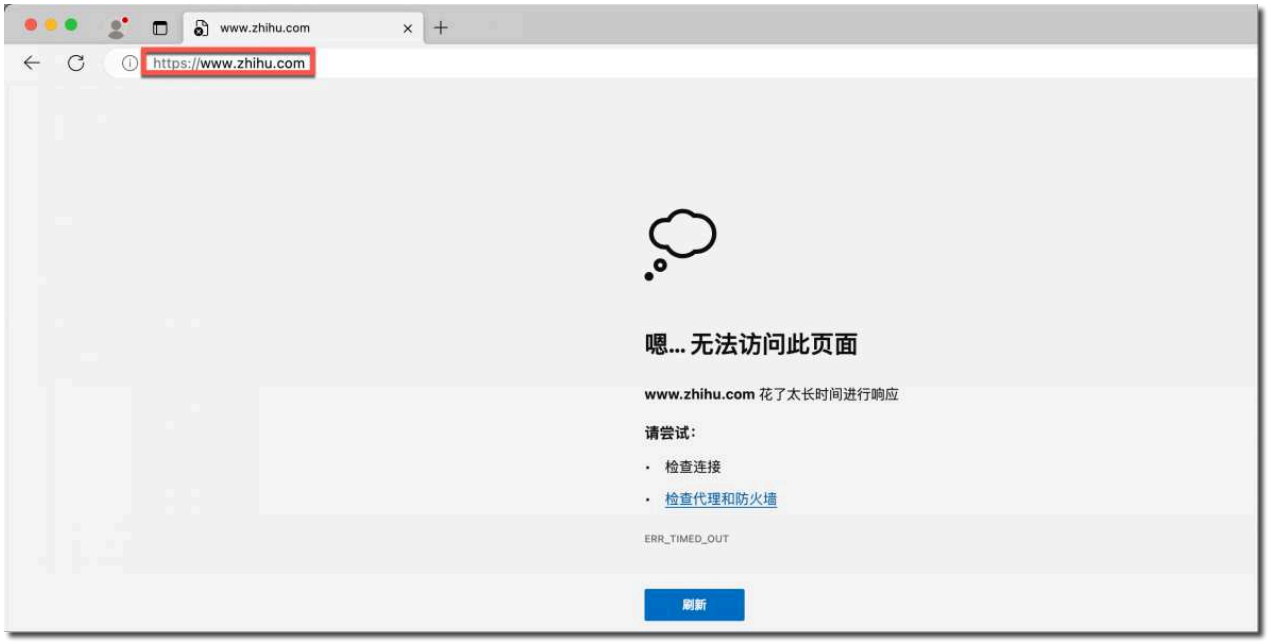
1. 修改拓扑如下，PC1通过FW1与FW2之间的IPSec隧道，从FW2的port3访问Internet，FW1和FW2的IPSec均开启预封装（pre-encapsulation）功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

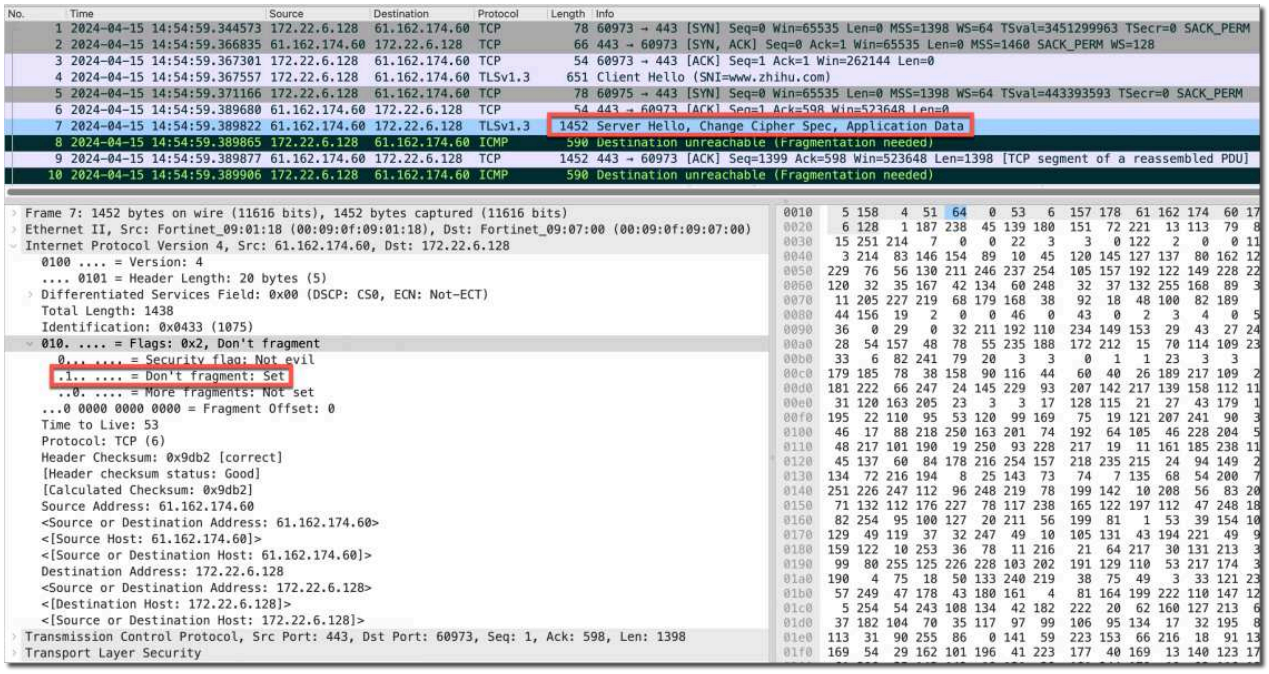


2. PC在日常访问HTTP应用时，TCP SYN中的TCP-MSS一般都为1460 Bytes。大部分HTTP服务器返回的TCP业务报文，IP头部中的DF（Don't fragment）选项都会置位，表示不允许传输路径上的设备对此报文进行分片。

3. 如上述拓扑所示PC1（10.10.1.100）通过IPSec隧道访问HTTP服务器（`www.zhihu.com`），无法打开该网站。

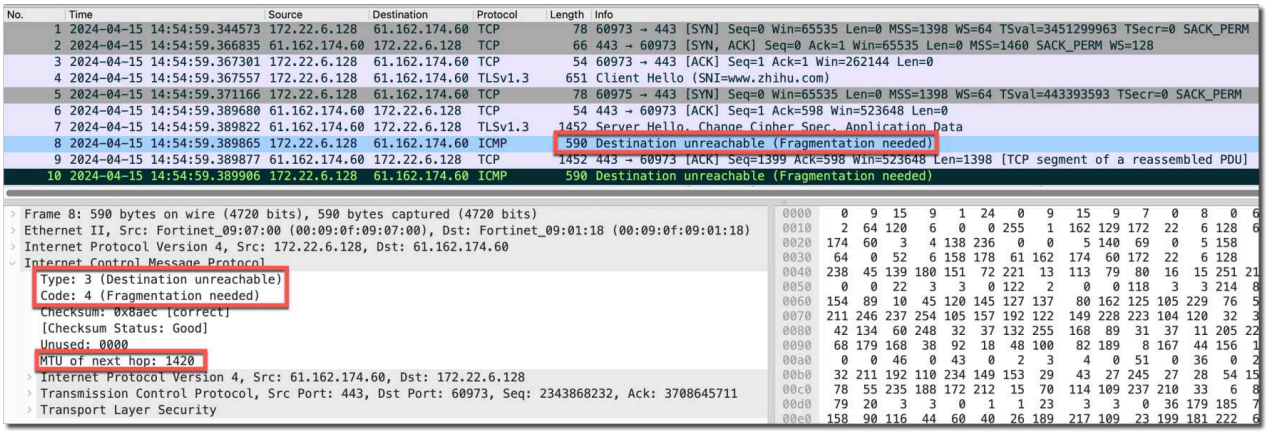


4. 在FW2的port3接口抓包，HTTP服务器向客户端返回的Server Hello报文较大，去除二层头部帧后的大小为1438 Bytes，这超过了此例中IPSec Tunnel默认的MTU 1420 Bytes。

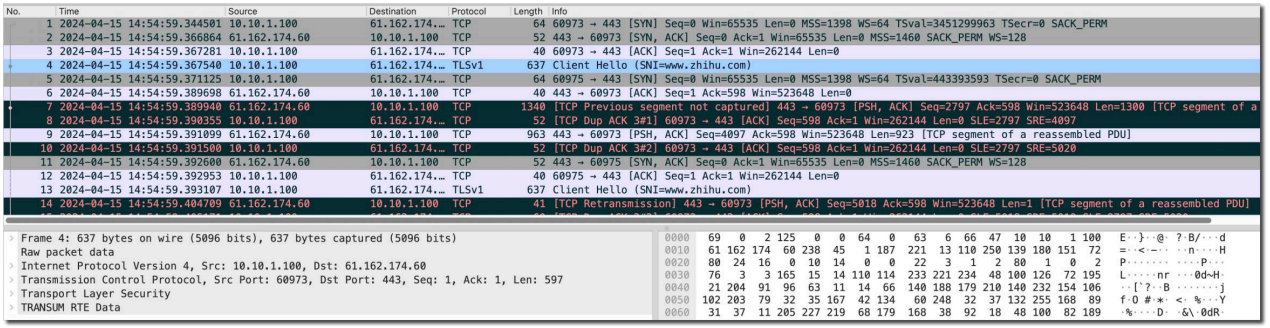


5. IPSec开启了预封装（pre-encapsulation）功能，需要根据此例中IPSec Tunnel接口的MTU 1420 Bytes进行预分片，但由于该Server Hello报文的IP头部的DF（Don't fragment）选项被置位，该报文无法被IPSec预分片，所以被FortiGate丢弃。FortiGate也会返回一个`fragmentation needed and DF set (Type3, Code4)`的ICMP消息给服务器端，携带了FortiGate IPSec Tunnel接口的MTU值1420 Bytes。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 同时在FW2的IPSec Tunnel接口上抓包，没有看到这个Server Hello报文，说明被FortiGate丢弃。



解决方法1-修改TCP-MSS

1. 在FW2或FW1的IPSec Tunnel接口或VPN策略中配置调低TCP握手时协商的TCP-MSS，修改TCP-MSS的大小根据IPSec接口的MTU决定，默认的IPSec Tunnel接口MTU为1420 Bytes，那么TCP-MSS建议修改为IPSec Tunnel接口的MTU减去20 Bytes的IP头部和20 Bytes的TCP头部，不同二阶段加密/验证算法和NAT-T环境下的建议IPSec Tunnel接口MTU和TCP-MSS如下：

> **重要**
>
> 一些特殊情况下TCP头部可能达到60 Bytes，如果修改TCP-MSS为1380 Bytes后仍然出现由于TCP头部超过20 Bytes导致的以上问题，请修改TCP-MSS为1340 Bytes。
>
> 以下IPSec Tunnel接口的MTU均建立在其绑定的业务接口的MTU为1500 Bytes的前提下，如果调整了业务接口的MTU（如此例中的port2），IPSec Tunnel接口的MTU以及TCP-MSS都要做相应修改。

算法组合	非NAT-T		NAT-T	
	建议Tunnel MTU	建议TCP-MSS	建议Tunnel MTU	建议TCP-MSS
3DES-SHA1	1420（默认，无需修改）	1380	1420（默认，无需修改）	1380
AES256-SHA256/AES256-SHA384/AES192-SHA256/AES192-SHA384/AES128-SHA1/AES128-SHA256	1420（默认，无需修改）	1380	1420（默认，无需修改）	1380
AES256-SHA512	1420（默认，无需修改）	1380	1406（需手工修改）	1366

2. 在FW2或FW1上修改IPSec Tunnel接口或VPN策略的TCP-MSS（仅需要在一台设备上修改，这里以FW2为例）为1380。

```bash
config system interface
    edit "VPN_to_FW1"
        set tcp-mss 1380
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
修改后可以使用如下CLI命令查看Tunnel接口的TCP-MSS：
FW2 # diagnose netlink dstmac list VPN_to_FW1
dev=VPN_to_FW1 mac=00:00:00:00:00:00 rx_tcp_mss=1380 tx_tcp_mss=1380 egress_overspill_threshold=0 egress_bytes=0
egress_over_bps=0 ingress_overspill_threshold=0 ingress_bytes=0 ingress_over_bps=0 sampler_rate=0
```

或基于策略的修改（两种方法取其一）：

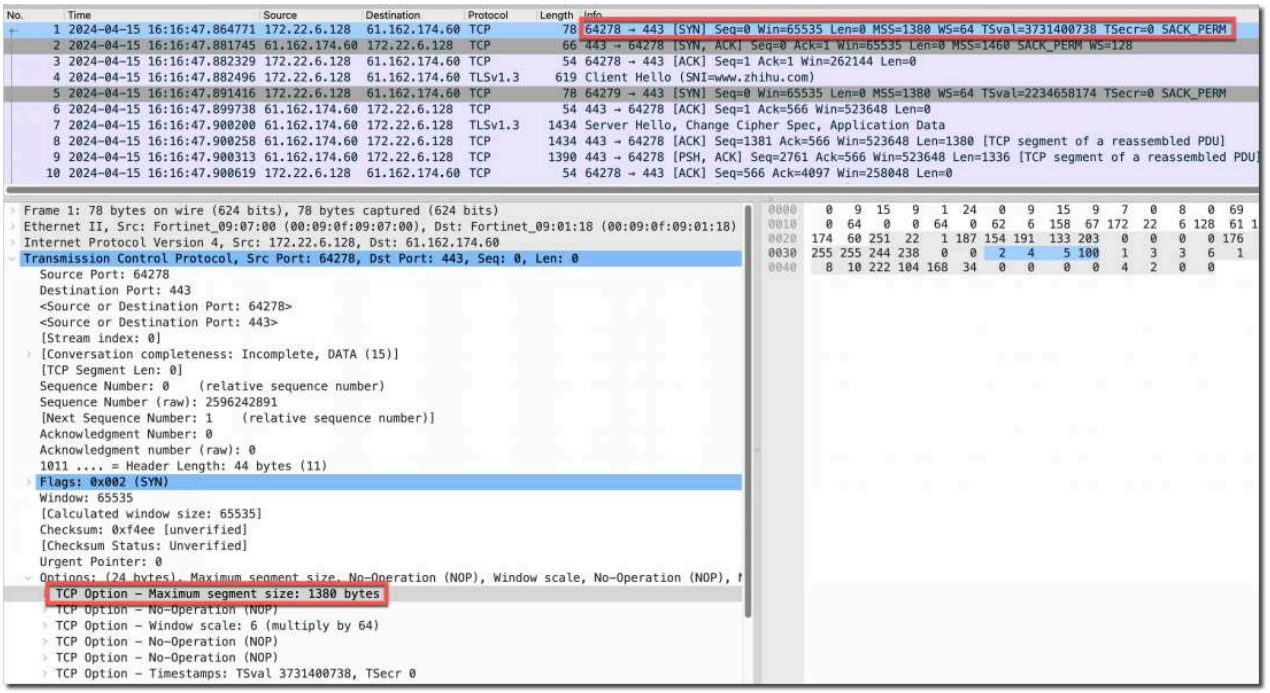
```bash
config firewall policy
    edit 2
        set name "VPN_to_FW1"
        set srcintf "port3" "VPN_to_FW1"
        set dstintf "VPN_to_FW1" "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set tcp-mss-sender 1380      //发送方向的TCP SYN报文修改TCP-MSS为1380//
        set tcp-mss-receiver 1380    //接收方向的TCP SYN报文修改TCP-MSS为1380//
    next
end
```

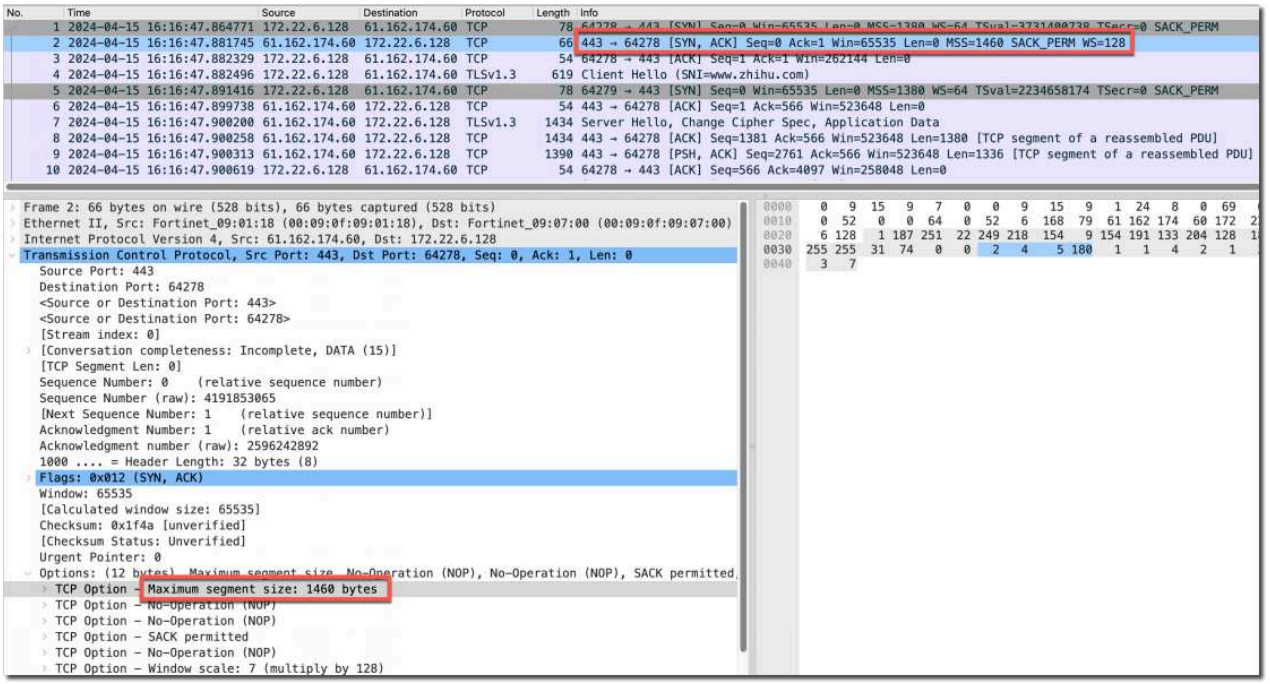
3. 再次使用PC1（10.10.1.100）通过IPSec隧道访问HTTP服务器（`www.zhihu.com`），可以正常打开该网站。



4. 在FW2的port3接口抓包，可以看到PC1访问HTTP服务器发出的TCP SYN报文中的TCP-MSS被FortiGate修改为了1380 Bytes。HTTP服务器返回的TCP-MSS为 14680 Bytes。

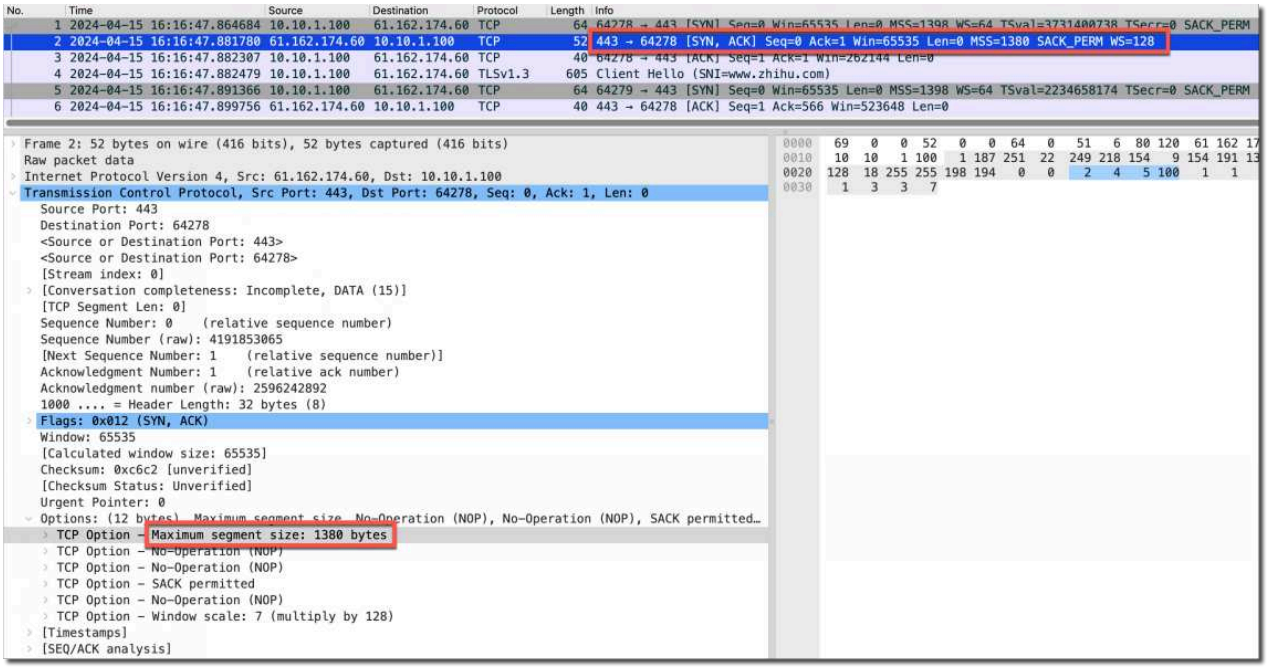
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



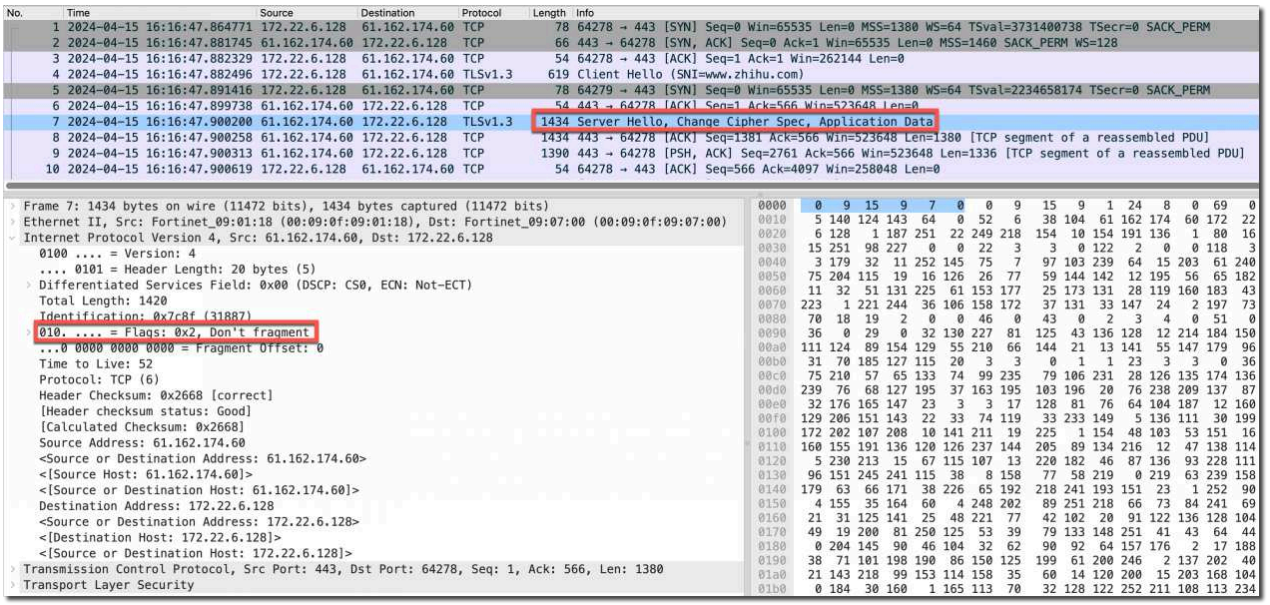


5. 在FW2的IPSec Tunnel接口抓包，可以看到HTTP服务器返回的SYN ACK的TCP-MSS被修改为1380 Bytes。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

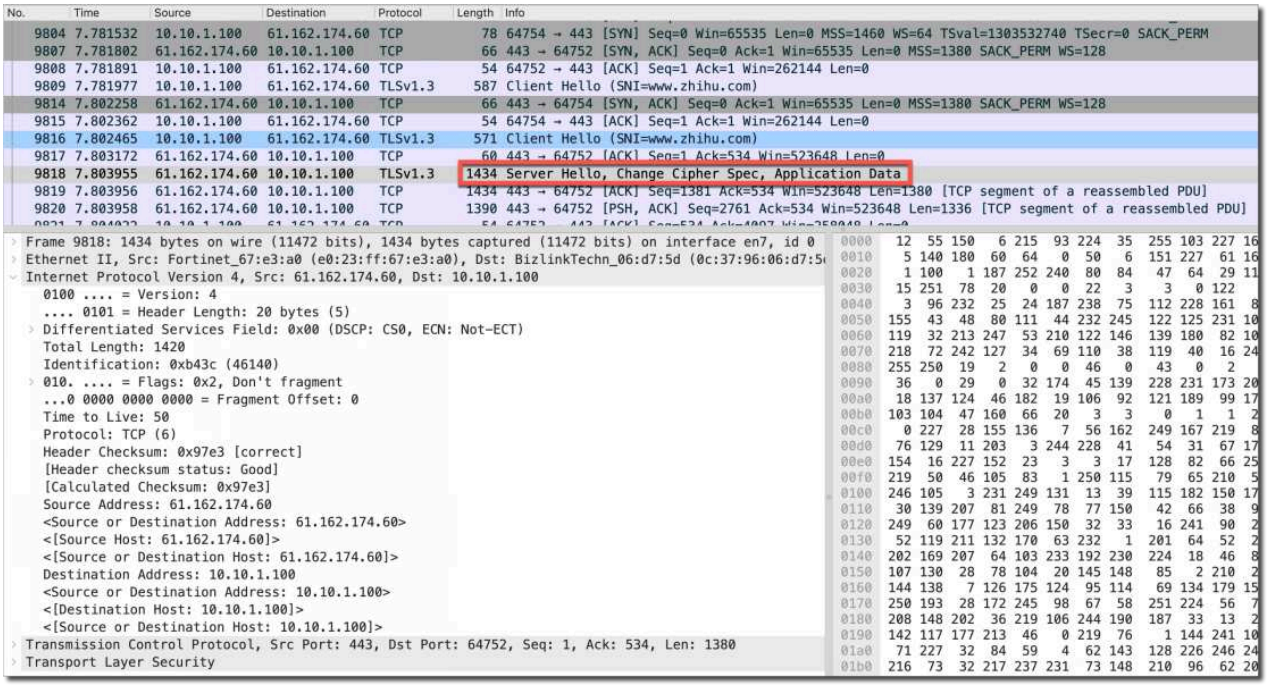


6. 在FW2的port3接口抓包，HTTP服务器向客户端返回的Server Hello这次去除二层头部帧后的大小为1420 Bytes，没有超过此例中IPSec Tunnel默认的MTU 1420 Bytes，所以即使IP头中仍然有DF置位，但不会被IPSec预分片。



7. 同时在PC1的网卡上抓包，可以收到这个Server Hello报文，说明没有被FortiGate丢弃，问题解决。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. Internet传输路径上未产生任何ESP分片。

解决方法2-关闭honor-df

1. 在FW1和FW2上的全局配置下关闭`honor-df`（默认开启），关闭后，将忽略任何IP头部中的DF位，对超过接口MTU的报文执行分片操作。

> **重要**
>
> 该配置不仅影响预封装模式的IPSec，也影响其他非VPN流量，请谨慎使用。

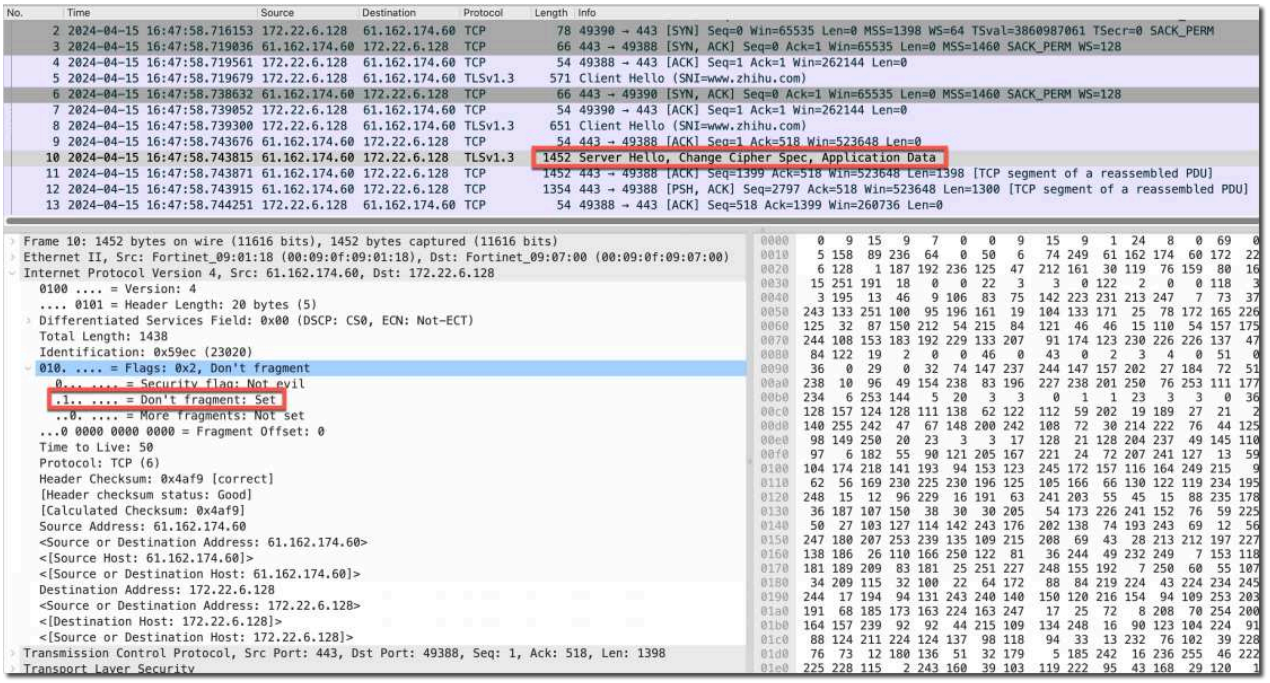
```bash
config system global
    set honor-df disable
end
```

2. 再次使用PC1（10.10.1.100）通过IPSec隧道访问HTTP服务器（`www.zhihu.com`），可以正常打开该网站。



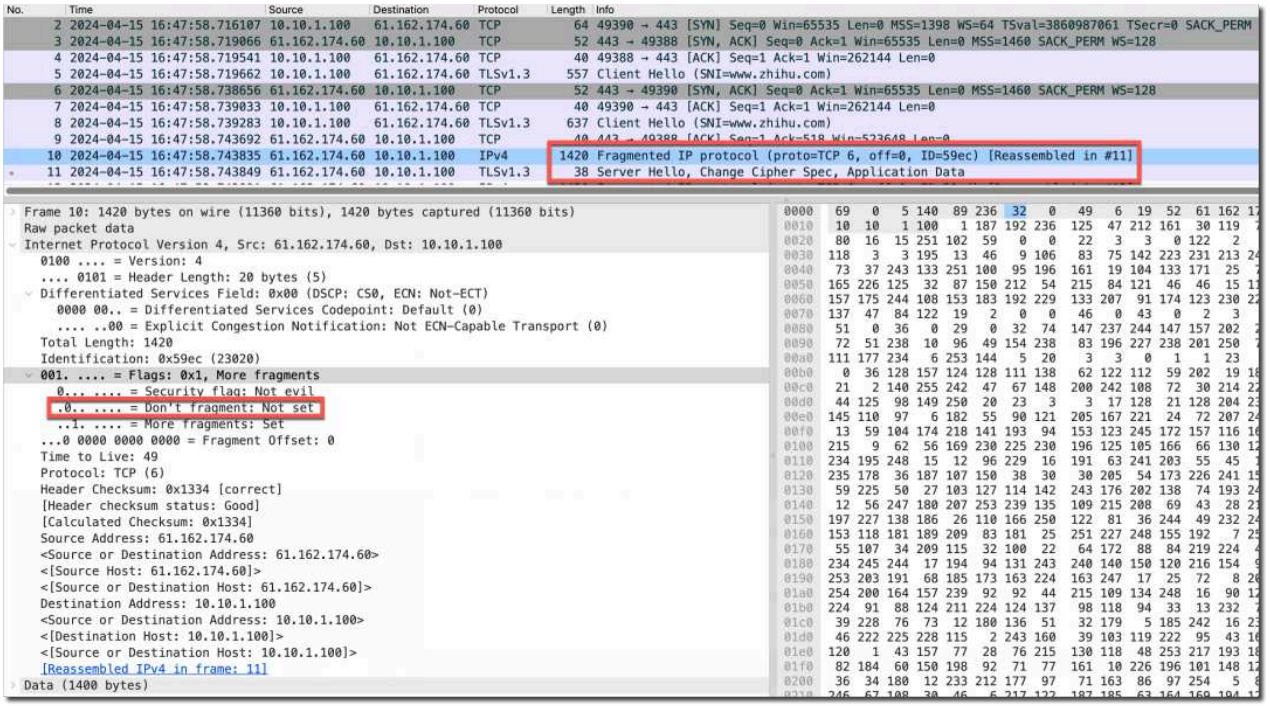
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在FW2的port3接口抓包，HTTP服务器向客户端返回的Server Hello报文较大，去除二层头部帧后的大小为1438 Bytes，这超过了此例中IPSec Tunnel默认的MTU 1420 Bytes，且IP头部中的DF置位。



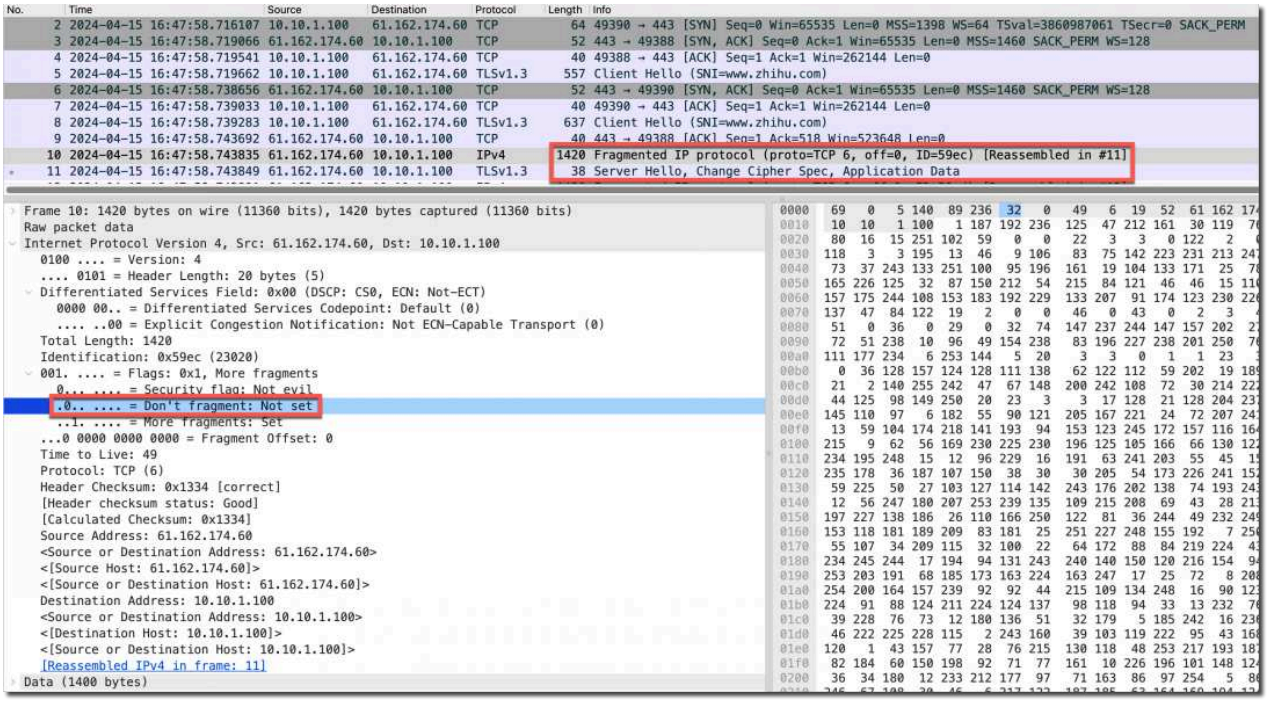
4. 同时在FW2的IPSec Tunnel接口抓包，可以看到FortiGate无视了这个Server Hello报文IP头部的DF标志位，执行了IPSec预封装功能，根据IPSec Tunnel接口的MTU 1420 Bytes将Server Hello报文分为2片，这两个分片IP包的DF选项均没有置位。

> **重要**
>
> 在Tunnel接口上抓取的报文没有2层帧头部，所以两个分片的大小为1420 Bytes和38 Bytes。



5. 同时在PC1的网卡上抓包，可以收到这个Server Hello报文的两个分片，问题解决。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. Internet传输路径上未产生任何ESP分片。

总结

1. 当遇到Internet线路上丢ESP分片的情况，可以使用FortiGate IPSec的预封装（pre-encapsulation）功能规避此问题：
   - IPSec后封装（post-encapsulation）：默认配置。IPSec隧道在收到任何需要ESP封装的报文时，不考虑IPSec Tunnel接口的MTU，先将明文封装到ESP中（如果明文已经是分片包，则会先重组明文分片），直接发送至公网接口。从公网接口发出时，再根据公网接口的MTU（默认为1500 Bytes）对ESP报文进行分片。这种post-encapsulation（后封装）方式符合RFC标准。
   - IPSec预封装（pre-encapsulation）：IPSec隧道在收到任何需要ESP封装的报文时，会根据当前IPSec Tunnel接口的MTU，先将明文根据Tunnel接口的MTU进行分片（如果明文已经是分片包，则会先重组明文分片），对每一片明文分片封装ESP，然后从公网接口发出。
2. 当使用IPSec预封装（pre-encapsulation）模式时，DF置位且超过IPSec Tunnel MTU的IP报文在IPSec隧道中传输会被丢弃，可以通过以下2种方法解决：
   - 解决方法1-修改TCP-MSS（推荐）。根据当前IPSec接口绑定的业务接口的MTU值决定IPSec Tunnel接口的MTU，根据IPSec Tunnel接口的MTU决定TCP-MSS的大小，适用于TCP报文。
   - 解决方法2-关闭honor-df。忽略任何IP头部中的DF置位，影响全局。对于DF置位的UDP或其他非TCP报文可以使用此种方法。
3. 更多关于IPSec分片的知识请参考：https://summerice.notion.site/376bdd5796914707b0560a8a0e429bde?v=033f688f25f34b5cacc6df3f21a7560b&pvs=4 ↗ 。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec无法修改隧道类型

问题现象

1. 当需要修改已创建的IPSec隧道类型时，例如已创建的IPSec隧道类型为静态模式，需要修改为拨号模式，页面会提示`-9999:-9999`的错误信息。



2. 通过CLI更改时也会失败，提示`Cannot change tunnel type once configured.`。

```bash
Spoke1 # config vpn ipsec phase1-interface
Spoke1 (phase1-interface) # edit VPN_to_CT
Spoke1 (VPN_to_CT) # set type dynamic
Spoke1 (VPN_to_CT) # next
Cannot change tunnel type once configured.
object set operator error, -9999, roll back the setting
Command fail. Return code 1
```

问题原因

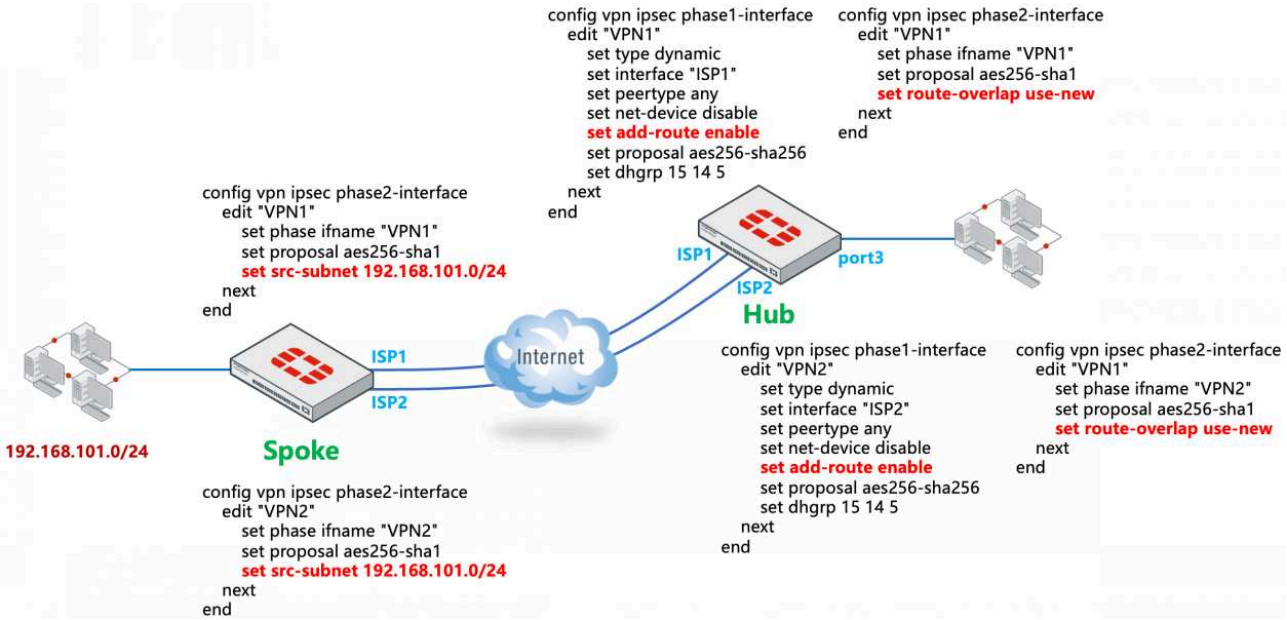
配置IPSec隧道后会生成“tun_id”，用于IPsec隧道的路由会使用“tun_id”进行匹配。因此无法修改IPSec隧道的类型，在静态、拨号、DDNS类型之间都无法进行修改。

解决方法为删除已有的IPSec隧道（以及相关联配置），并重新创建其他类型的IPSec隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Hub-Spoke双线路隧道抖动

网络拓扑



1. Spoke与Hub均有2条线路接入Internet。
2. Hub的ISP1和ISP2线路上分别创建一个拨号类型的IPSec连接：
   - Hub上的两条拨号IPSec隧道一阶段配置中，开启 `add-route` 功能，根据Spoke的源保护网段自动添加去往Spoke的路由。
   - 二阶段源目保护网段均为0.0.0.0/0，默认配置下， `route-overlap` 状态为 `use-new` 。
3. Spoke的ISP1线路与Hub1的ISP1线路建立IPSec连接，Spoke的ISP2线路与Hub1的ISP1线路建立IPSec连接。
   - Spoke上的两条IPSec隧道二阶段配置中，源保护网段均配置为明细的192.168.101.0/24，目的保护网段配置为0.0.0.0/0。
4. 由于Spoke两条线路的上的IPSec二阶段配置的源保护网段一样（192.168.101.0/24），所以理论上Hub在实现 `add-route` 时，应该添加2条目标为192.168.101.0/24的路由，并等价负载到两条拨号隧道上创建的子隧道。这也是用户想要实现的需求。

问题现象

> **重要**
>
> 在升级FortiOS 7.0.13、7.2.6、7.4.1及更新版本后，会出现此问题，这是正常情况，功能机制随版本发生了变化。

1. Spoke上的SD-WAN健康检查检测Hub端的资源，出现丢包现象。

```bash
Spoke # diagnose sys sdwan health-check
Health Check(Spoke1):
Seq(4 VPN1): state(dead), packet-loss(95.000%) sla_map=0x0
Seq(5 VPN2): state(alive), packet-loss(11.000%) latency(9.479), jitter(4.353), bandwidth-up(19999998), bandwidth-dw(19999998), bandwidth-bi(39999996) sla_map=0x0
```

2. 在Hub上查看IPSec一阶段（IKE）状态，多次执行查看命令，已创建时间一直处于很短的状态。

```bash
Hub # diagnose vpn ike gateway list | grep "name:\|created"
name: VPN2_0
//created: 1s ago//
IKE SA: created 1/1 established 1/1 time 10/10/10 ms
IPsec SA: created 2/2 established 2/2 time 0/0/0 ms
name: VPN1_0
//created: 1s ago//
IKE SA: created 1/1 established 1/1 time 10/10/10 ms
IPsec SA: created 1/1 established 1/1 time 10/10/10 ms
```

3. 查看Hub上通过 `add-route` 功能添加的路由，只有一条隧道上添加了去往Spoke内网的路由。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
Hub # get router info routing-table details 192.168.101.0

Routing table for VRF=0
Routing entry for 192.168.101.0/24
Known via "static", distance 15, metric 0, best
* via VPN1 tunnel 200.52.10.17, tun_id
```

问题原因

1. 通过 `diagnose debug application ike -1` 查看IPSec Debug信息，可以看到IPSec不停地在两条隧道上添加和删除去往Spoke的路由。

```bash
Hub # diagnose debug application ike -1
Hub # diagnose debug enable

ike 0:VPN1_0:562:1753: peer proposal is: peer:0:192.168.101.0-192.168.101.255:0, me:0:0.0.0.0-255.255.255.255:0
ike 0:VPN1_0:562:Spoke1LAN:1753: dst 0 7 0:192.168.101.0-192.168.101.255:0
ike 0:VPN2:1748: moving route 192.168.101.0/255.255.255.0 oif VPN2(32) metric 15 priority 1 to 0:VPN1:1753
ike 0:VPN2:1748: del route 192.168.101.0/255.255.255.0 tunnel 20.0.0.3 oif VPN2(32) metric 15 priority 1
ike 0:VPN1:1753: add route 192.168.101.0/255.255.255.0 gw 200.52.10.17 oif VPN1(31) metric 15 priority 1
ike 0:VPN2:563:1755: TSi_0 0:192.168.101.0-192.168.101.255:0
ike 0:VPN2:563:Spoke1-LAN_E:1755: TSi_0 0:192.168.101.0-192.168.101.255:0
ike 0:VPN2_0:563:Spoke1-LAN_E:1755: dst 0 7 0:192.168.101.0-192.168.101.255:0
ike 0:VPN1:1753: moving route 192.168.101.0/255.255.255.0 oif VPN1(31) metric 15 priority 1 to 0:VPN2:1755
ike 0:VPN1:1753: del route 192.168.101.0/255.255.255.0 tunnel 200.52.10.17 oif VPN1(31) metric 15 priority 1
ike 0:VPN2:1755: add route 192.168.101.0/255.255.255.0 gw 20.0.0.3 oif VPN2(32) metric 15 priority 1
ike 0:VPN1_0:564:1761: peer proposal is: peer:0:192.168.101.0-192.168.101.255:0, me:0:0.0.0.0-255.255.255.255:0
ike 0:VPN1_0:564:Spoke1LAN:1761: dst 0 7 0:192.168.101.0-192.168.101.255:0
ike 0:VPN2:1755: moving route 192.168.101.0/255.255.255.0 oif VPN2(32) metric 15 priority 1 to 0:VPN1:1761
ike 0:VPN2:1755: del route 192.168.101.0/255.255.255.0 tunnel 20.0.0.3 oif VPN2(32) metric 15 priority 1
ike 0:VPN1:1761: add route 192.168.101.0/255.255.255.0 gw 200.52.10.17 oif VPN1(31) metric 15 priority 1
```

2. 这是由于Hub端在执行 `add-route` 功能时，由于两条Spoke隧道使用的源保护网段一样，Hub认为这两个保护网段冲突：

- 当Hub的IPSec二阶段中的 `route-overlap` 状态为 `use-new` （默认配置）时：每个Spoke网段只能添加一条路由到路由表，后建立的IPSec隧道会导致前边已建立的IPSec隧道及其添加的相同路由被移除。这样就会出现两条隧道不停翻转（overlap）的情况。
- 当Hub的IPSec二阶段中的 `route-overlap` 状态为 `allow` 时：允许同时在两个隧道上添加去往Spoke内网的路由。

解决方法

1. 在Hub的两条IPSec拨号连接的二阶段配置中，将 `route-overlap` 状态配置为 `allow` 。

```bash
config vpn ipsec phase2-interface
    edit "VPN1"
        set route-overlap allow
    next
    edit "VPN2"
        set route-overlap allow
    next
end
```

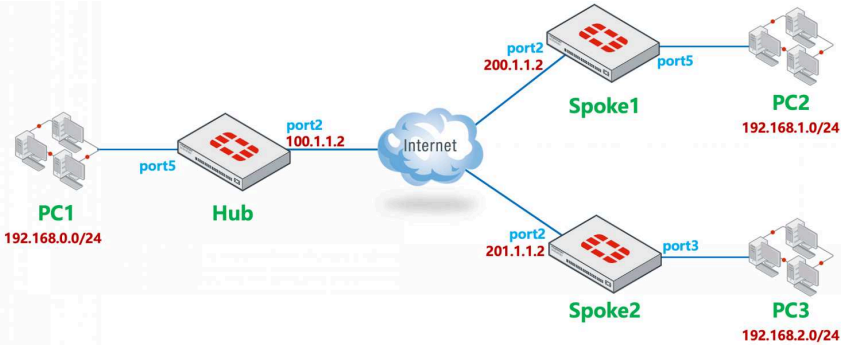
2. 查看Hub上通过 `add-route` 功能添加的路由，两条隧道上都添加了去往Spoke内网的路由，并等价负载。

```bash
Hub # get router info routing-table details 192.168.101.0

Routing table for VRF=0
Routing entry for 192.168.101.0/24
Known via "static", distance 15, metric 0, best
* via VPN2 tunnel 115.38.6.12, tun_id
* via VPN1 tunnel 200.52.10.17, tun_id
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Hub-Spoke静态路由问题

网络拓扑



1. Hub设备位于数据中心，配在port2配置“拨号用户（Dynamic）”模式的IPSec连接。
2. Spoke1与Spoke2均在port2上配置“静态IP地址（Static）”类型的IPSec连接，与Hub建立IPSec隧道。
3. Hub与Spoke之间通过静态路由进行通信。

配置信息

仅以Hub和Spoke1为例。基础网络IP、路由配置略。

Hub

1. IPSec隧道配置，隧道类型为dynamic，第二阶段保护网段为0.0.0.0/0↔0.0.0.0/0，`add-route`功能为关闭状态。

```bash
config vpn ipsec phase1-interface
    edit "Hub"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256
        set add-route disable
        set dpd on-idle
        set psksecret ENC
YsyLk34z2H6ffoT8QYhgsX5aS5FN4Vq3g9IpjKgh/7uBJdl+W3IMHDuXxXpT1a+ZyxR37cOfpB1Uzf0Vnv8D2Q0E+3259DPYr556hZRDGYo46f=
        set dpd-retryinterval 60
    next
end

config vpn ipsec phase2-interface
    edit "Hub"
        set phase1name "Hub"
        set proposal aes128-sha1
        set keepalive enable
    next
end
```

2. 配置IPSec Tunnel IP。

```bash
config system interface
    edit "Hub"
        set ip 10.10.10.1 255.255.255.255
        set type tunnel
        set remote-ip 10.10.10.254 255.255.255.0
        set interface "port2"
    next
end
```

3. 配置防火墙策略放通IPSec隧道与内网口port3之间的流量。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall policy
    edit 1
        set name "VPN_Hub"
        set srcintf "Hub" "port3"
        set dstintf "Hub" "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

4. 配置去往Spoke1内网网段（192.168.1.0/24）和Spoke2内网网段（192.168.2.0/24）的静态路由，出接口选择IPSec Tunnel接口。

```bash
config router static
    edit 2
        set dst 192.168.1.0 255.255.255.0
        set device "Hub"
    next
    edit 3
        set dst 192.168.2.0 255.255.255.0
        set device "Hub"
    next
end
```

Spoke1

1. IPSec隧道配置，隧道类型为static，第二阶段保护网段为0.0.0.0/0↔0.0.0.0/0。

```bash
config vpn ipsec phase1-interface
    edit "Spoke1"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal aes128-sha256
        set remote-gw 100.1.1.2
        set dpd on-idle
        set psksecret ENC
fDnGerNZb+ogGLimNoAdp/nQj8tOZRBwu91bMs1MqK4oB/t1Szc8C1Ma43Pga8cW8Qxdew7TgFECbvwq1nYxPqVU6pnbj/DkpT/nuGzvTietA0mjCB
ubl/1jPU8wkFWABfIXsivn0YOSyjHmQx5LSdbhjvM9FTI6CKjixMszGuC8T8kpczpL2h1FAX1SkytiKeztJg==
    next
end

config vpn ipsec phase2-interface
    edit "Spoke1"
        set phase1name "Spoke1"
        set proposal aes128-sha1
        set auto-negotiate enable
    next
end
```

2. 配置IPSec Tunnel IP。

```bash
config system interface
    edit "Spoke1"
        set ip 10.10.10.2 255.255.255.255
        set type tunnel
        set remote-ip 10.10.10.254 255.255.255.0
        set interface "port2"
    next
end
```

3. 配置防火墙策略放通IPSec隧道与内网口port3之间的流量。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config firewall policy
    edit 1
        set name "VPN_Spoke1"
        set srcintf "port3" "Spoke1"
        set dstintf "port3" "Spoke1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

4. 配置去往Hub内网网段（192.168.0.0/24）的静态路由，出接口选择IPSec Tunnel接口。

```bash
config router static
    edit 2
        set dst 192.168.0.0 255.255.255.0
        set device "Spoke1"
    next
end
```

Spoke2

略，与Spoke1一致。

问题现象

1. IPSec隧道建立后，查看Hub和Spoke的IPSec一阶段状态中的`tun_id`，可以看到Hub建立了两个动态子IPSec连接（Hub_0和Hub_1），Hub和Spoke显示已建立的隧道ID（`tun_id`）均为对端公网IP地址。

```bash
Hub # diagnose vpn ike gateway list | grep "name\|tun_id"
name: Hub_0
tun_id: 200.1.1.2/::10.0.0.5    <——隧道ID为Spoke1的公网IP
name: Hub_1
tun_id: 201.1.1.2/::10.0.0.7    <——隧道ID为Spoke2的公网IP
```

```bash
Spoke1 # diagnose vpn ike gateway list | grep "name\|tun_id"
name: Spoke1
tun_id: 100.1.1.2/::100.1.1.2    <——隧道ID为Hub的公网IP
```

```bash
Spoke2 # diagnose vpn ike gateway list | grep "name\|tun_id"
name: Spoke2
tun_id: 100.1.1.2/::100.1.1.2    <——隧道ID为Hub的公网IP
```

2. 使用PC2（Spoke1内网）访问PC1（Hub内网），可以正常通信。

```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
Windows IP 配置
以太网适配器 Ethernet0:
   IPv4 地址 . . . . . . . . . . . . : 192.168.1.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.1.1

C:\Users\Administrator.SUMMERICE2019>ping 192.168.0.100
正在 Ping 192.168.0.100 具有 32 字节的数据:
来自 192.168.0.100 的回复: 字节=32 时间=3ms TTL=126
来自 192.168.0.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.0.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.0.100 的回复: 字节=32 时间=2ms TTL=126
192.168.0.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 3ms, 平均 = 1ms
```

3. 使用PC1（Hub内网）访问PC2（Spoke1内网）或PC3（Spoke2内网），无法正常通信。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
Windows IP 配置
以太网适配器 Ethernet0:
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.0.1

C:\Users\Administrator.SUMMERICE2019>ping 192.168.1.100
正在 Ping 192.168.1.100 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
192.168.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

4. 在Hub上抓包显示ICMP Request报文已被送入IPSec Tunnel接口。Debug Flow虽然显示ICMP Request报文已被送入IPSec Tunnel接口，但路由查找的 `gw` （网关）为0.0.0.0，正确的 `gw` 应为步骤1中看到的Hub与Spoke1的IPSec子连接 `Hub_0` 的 `tun_id` 200.1.1.1。

```
Hub # id=65308 trace_id=5 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=1, 192.168.0.100:1->192.168.1.100:2048) tun_id=0
.0.0.0 from port3. type=8, code=0, id=1, seq=55735."
id=65308 trace_id=5 func=init_ip_session_common line=6080 msg="allocate a new session-0000019e, tun_id=0.0.0.0"
id=65308 trace_id=5 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via Hub"  路由查找网关为0.0.0.0
id=65308 trace_id=5 func=__iprope_tree_check line=535 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=5 func=fw_forward_handler line=989 msg="Allowed by Policy-1:"
id=65308 trace_id=5 func=ip_session_confirm_final line=3113 msg="npu_state=0x100, hook=4"
id=65308 trace_id=5 func=ipsecdev_hard_start_xmit line=662 msg="enter IPSec interface Hub, tun_id=0.0.0.0"  进入父隧道Hub后没有后续动作
```

5. 在Hub上查看IPSec Tunnel接口的统计信息，可以看到txe（发送错误）计数随着PC1访问PC2的流量在一直增长。

```bash
Hub # diagnose netlink interface list name Hub | grep "txe=\|if="
if=Hub family=00 type=768 index=16 mtu=1420 link=0 master=0
stat: rxp=15 txp=15 rxb=900 txb=900 rxe=0 txe=102 rxd=0 txd=0 mc=0 collision=0 @ time=1715074667

Hub # diagnose netlink interface list name Hub | grep "txe=\|^if="
if=Hub family=00 type=768 index=16 mtu=1420 link=0 master=0
stat: rxp=15 txp=15 rxb=900 txb=900 rxe=0 txe=108 <———txe计数增长 rxd=0 txd=0 mc=0 collision=0 @ time=1715074676
```

问题原因

1. 这是由于FortiOS 7.0新的IPSec内核设计导致的。FortiOS 7.0之前版本的Dynamic模式IPSec使用“route tree”功能查找流量应该匹配的子隧道。FortiOS 7.0之后将“route tree”功能移除，使用“tunn-id”用于标识Dynamic模式IPSec连接生成的每个子连接。当Dynamic模式的IPSec连接生成子连接（如Hub_0，Hub_1……）时，将自动分配一个 `tunn-id` 给这个子连接，默认配置下，使用对端的公网IP作为隧道的 `tunn-id` 。

2. 在Spoke1（Static类型的IPSec）上查看去往Hub内网网段（192.168.0.0/24）的路由，可以看到路由信息中有对应的 `tun_id` ，为Hub的公网地址100.1.1.2，所以Spoke内网PC去往Hub内外PC的流量可以正确送入对应 `tun_id` 的IPSec隧道。

```bash
Spoke1 # get router info routing-table all | grep 192.168.0.0
S       192.168.0.0/24 [10/0] via Spoke1 tunnel 100.1.1.2, [1/0]
```

3. 在Hub上查看路由表，可以看到已配置的Hub去往Spoke1和Spoke2的静态路由在路由表中显示为Tunnel接口的直连路由，并未显示对应的 `tun_id` （这里应为Spoke1和Spoke2的公网IP）。这是由于在Hub上配置的去往Spoke内网的静态路由并未指定出接口和下一跳为哪个IPSec子连接（Hub_0或Hub_1）。

```bash
Hub # get router info routing-table all | grep 192.168
C       192.168.0.0/24 is directly connected, port3
S       192.168.1.0/24 [10/0] is directly connected, Hub, [1/0]
S       192.168.2.0/24 [10/0] is directly connected, Hub, [1/0]
```

4. 当PC1（Hub内网）访问PC2（Spoke1内网）或PC3（Spoke2内网）时，发起流量进入Hub的IPSec隧道后，由于路由中没有 `tun_id` 标识，IPSec不知道应该将其送往哪个子IPSec连接（Hub_0或Hub_1）。

解决方法1-使用add-route

1. 在Spoke上的IPSec二阶段配置中，修改源保护网段为明细保护网段，目标保护网段仍为0.0.0.0/0。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
Spoke1:
config vpn ipsec phase2-interface
    edit "Spoke1"
        set src-subnet 192.168.1.0 255.255.255.0
    next
end

Spoke2:
config vpn ipsec phase2-interface
    edit "Spoke1"
        set src-subnet 192.168.2.0 255.255.255.0
    next
end
```

2. 将Hub上配置的去往Spoke内外的静态路由禁用或删除。

```bash
config router static
    edit 2
        set status disable
        set dst 192.168.1.0 255.255.255.0
        set device "Hub"
    next
    edit 3
        set status disable
        set dst 192.168.2.0 255.255.255.0
        set device "Hub"
    next
end
```

3. 在Hub上的IPSec一阶段配置中，将`add-route`功能开启，根据Spoke协商的源保护网段自动添加去往Spoke内网的路由。

```bash
config vpn ipsec phase1-interface
    edit "Hub"
        set add-route enable
    next
end
```

4. 在Hub上查看路由表，可以看到通过`add-route`功能添加的去往Spoke内网的路由自动添加了`tunn-id`标记，去往Spoke1内网的路由指定的是IPSec子连接Hub_0的`tunn-id`，去往Spoke2内网的路由指定的是IPSec子连接Hub_1的`tunn-id`。

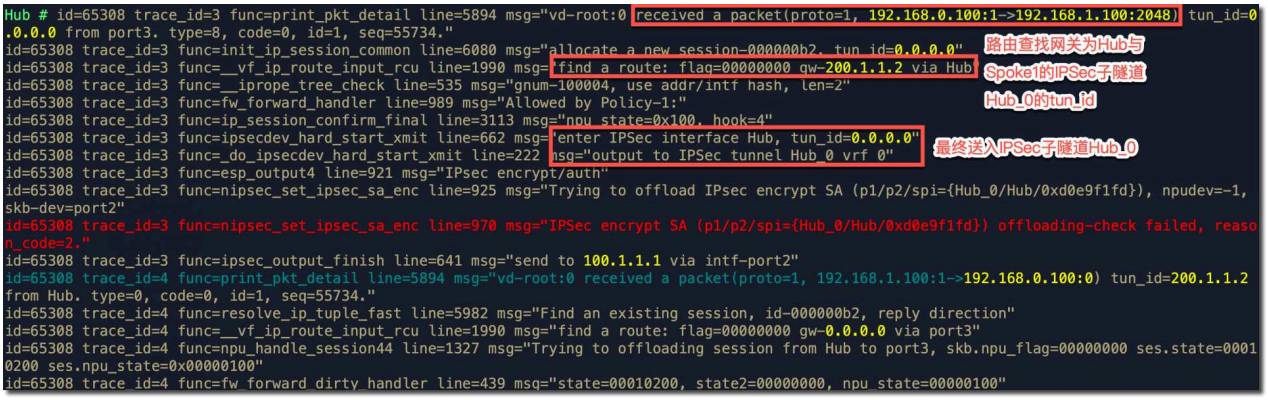
```bash
Hub # get router info routing-table all | grep 192.168
C       192.168.0.0/24 is directly connected, port3
S       192.168.1.0/24 [15/0] via Hub tunnel 200.1.1.2, [1/0]
S       192.168.2.0/24 [15/0] via Hub tunnel 201.1.1.2, [1/0]
```

5. 使用PC1（Hub内网）访问PC2（Spoke1内网）或PC3（Spoke2内网），可以正常通信。

```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
以太网适配器 Ethernet0:
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.0.1

C:\Users\Administrator.SUMMERICE2019>ping 192.168.1.100
正在 Ping 192.168.1.100 具有 32 字节的数据:
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=3ms TTL=126
192.168.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 3ms, 平均 = 1ms
```

6. Debug Flow显示ICMP Request报文到达FortiGate后，路由查找网关为Hub与Spoke1的IPSec子隧道Hub_0的`tun_id`200.1.1.2。该流量最终可以被送入IPSec子隧道Hub_0送往Spoke1。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



解决方法2-配置VPN路由下一跳

重要

此方法要求Spoke的公网IP不会变化。

1. Spoke IPSec二阶段仍然配置0.0.0.0↔0.0.0.0的保护网段，Hub关闭`add-route`功能。

2. 在Hub上修改去往Spoke的静态路由，配置下一跳为Spoke对应的公网IP（tun_id）。

重要

出接口为IPSec Tunnel时，相关路由的下一跳（gateway）只能在CLI下配置。

```bash
config router static
    edit 2
        set dst 192.168.1.0 255.255.255.0
        set gateway 200.1.1.2
        set device "Hub"
    next
    edit 3
        set dst 192.168.2.0 255.255.255.0
        set gateway 201.1.1.2
        set device "Hub"
    next
end
```

3. 在Hub查看路由表，去往Spoke内网的路由下一跳变为Spoke1和Spoke2的公网IP，对应相关已建立的IPSec子隧道Hub_0、Hub_1的`tun_id`。

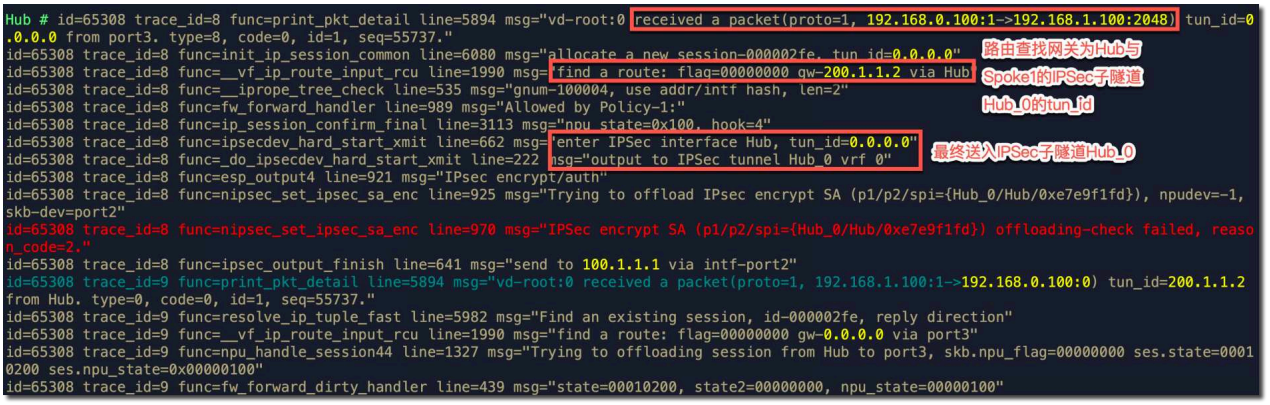
```bash
Hub # get router info routing-table all | grep 192.168
C       192.168.0.0/24 is directly connected, port3
S       192.168.1.0/24 [10/0] via Hub tunnel 200.1.1.2, [1/0]
S       192.168.2.0/24 [10/0] via Hub tunnel 201.1.1.2, [1/0]
```

4. 使用PC1（Hub内网）访问PC2（Spoke1内网）或PC3（Spoke2内网），可以正常通信。

```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
以太网适配器 Ethernet0:
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.0.1

C:\Users\Administrator.SUMMERICE2019>ping 192.168.1.100
正在 Ping 192.168.1.100 具有 32 字节的数据:
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=3ms TTL=126
192.168.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 3ms, 平均 = 1ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

5. Debug Flow显示ICMP Request报文到达FortiGate后，路由查找网关为Hub与Spoke1的IPSec子隧道Hub_0的`tun_id` 200.1.1.2。该流量最终可以被送入IPSec子隧道Hub_0送往Spoke1。




```
Hub # id=65308 trace_id=8 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=1, 192.168.0.100:1->192.168.1.100:2048) tun_id=0
.0.0.0 from port3. type=8, code=0, id=1, seq=55737."
id=65308 trace_id=8 func=init_ip_session_common line=6080 msg="allocate a new session-000002fe, tun_id=0.0.0.0"
id=65308 trace_id=8 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-200.1.1.2 via Hub"
id=65308 trace_id=8 func=__iprope_tree_check line=535 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=8 func=fw_forward_handler line=989 msg="Allowed by Policy-1:"
id=65308 trace_id=8 func=ip_session_confirm_final line=3113 msg="npu_state=0x100, hook=4"
id=65308 trace_id=8 func=ipsecdev_hard_start_xmit line=662 msg="enter IPSec interface Hub, tun_id=0.0.0.0"
id=65308 trace_id=8 func=_do_ipsecdev_hard_start_xmit line=222 msg="output to IPSec tunnel Hub_0 vrf 0"
id=65308 trace_id=8 func=esp_output4 line=921 msg="IPSec encrypt/auth"
id=65308 trace_id=8 func=nipsec_set_ipsec_sa_enc line=925 msg="Trying to offload IPsec encrypt SA (p1/p2/spi={Hub_0/Hub/0xe7e9f1fd}), npudev=-1,
skb-dev=port2"
id=65308 trace_id=8 func=nipsec_set_ipsec_sa_enc line=970 msg="IPSec encrypt SA (p1/p2/spi={Hub_0/Hub/0xe7e9f1fd}) offloading-check failed, reaso
n_code=2."
id=65308 trace_id=8 func=ipsec_output_finish line=641 msg="send to 100.1.1.1 via intf-port2"
id=65308 trace_id=9 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=1, 192.168.1.100:1->192.168.0.100:0) tun_id=200.1.1.2
from Hub. type=0, code=0, id=1, seq=55737."
id=65308 trace_id=9 func=resolve_ip_tuple_fast line=5982 msg="Find an existing session, id-000002fe, reply direction"
id=65308 trace_id=9 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=9 func=npu_handle_session44 line=1327 msg="Trying to offloading session from Hub to port3, skb.npu_flag=00000000 ses.state=0001
0200 ses.npu_state=0x00000100"
id=65308 trace_id=9 func=fw_forward_dirty_handler line=439 msg="state=00010200, state2=00000000, npu_state=00000100"
```

解决方法3-使用exchange-ip

1. Spoke IPSec二阶段仍然配置0.0.0.0↔0.0.0.0的保护网段，Hub关闭`add-route`功能。

2. 在所有Spoke上修改IPSec一阶段配置，开启`exchange-ip`功能，Spoke与Hub进行IKE协商时会发送对应隧道已配置的IPSec Tunnel IP地址，隧道建立完成后，Hub将使用Spoke发送的IPSec Tunnel IP作为对应的隧道ID（`tun_id`）。

```bash
Spoke1:
config vpn ipsec phase1-interface
    edit "Spoke1"
        set exchange-interface-ip enable
    next
end

Spoke2:
config vpn ipsec phase1-interface
    edit "Spoke2"
        set exchange-interface-ip enable
    next
end
```

重要

在本文“配置信息”章节中已为所有IPSec Tunnel接口配置了IP。

如果Spoke的IPSec Tunnel接口没有手动配置IP或没有通过mode-cfg获取IP，则需要手工指定`exchange-ip`要交换的IP地址（该地址可自定义，不需要是设备上已存在的地址）：

```bash
config vpn ipsec phase1-interface
    edit "Spoke2"
        set exchange-interface-ip enable
        set exchange-ip-addr4 10.10.10.2
    next
end
```

3. IPSec隧道建立后，查看Hub和Spoke的IPSec一阶段状态中的`tun_id`，可以看到Hub建立了两个动态子IPSec连接（Hub_0和Hub_1），Hub和Spoke显示已建立的隧道ID（tun_id）均为对端公网IP地址。

```bash
Hub # diagnose vpn ike gateway list | grep "name\|tun_id"
name: Hub_0
tun_id: 10.10.10.2/::10.0.0.50     <——隧道ID为Spoke1的IPSec Tunnel IP
name: Hub_1
tun_id: 10.10.10.3/::10.0.0.53     <——隧道ID为Spoke2的IPSec Tunnel IP
```

4. 在Hub上修改去往Spoke的静态路由，配置下一跳为Spoke对应的IPSec Tunnel接口IP。

重要

出接口为IPSec Tunnel时，相关路由的下一跳（gateway）只能在CLI下配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config router static
    edit 2
        set dst 192.168.1.0 255.255.255.0
        set gateway 10.10.10.2
        set device "Hub"
    next
    edit 3
        set dst 192.168.2.0 255.255.255.0
        set gateway 10.10.10.3
        set device "Hub"
    next
end
```

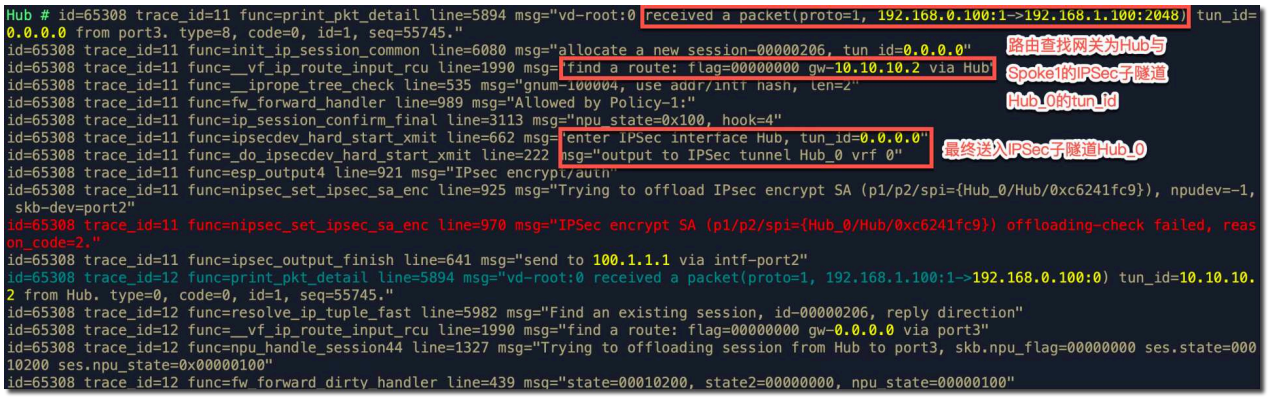
5. 在Hub查看路由表，去往Spoke内网的路由下一跳变为Spoke1和Spoke2的IPSec Tunnel IP，对应相关已建立的IPSec子隧道Hub_0、Hub_1的`tun_id`。

```bash
Hub # get router info routing-table all | grep 192.168
C       192.168.0.0/24 is directly connected, port3
S       192.168.1.0/24 [10/0] via Hub tunnel 10.10.10.2, [1/0]
S       192.168.2.0/24 [10/0] via Hub tunnel 10.10.10.3, [1/0]
```

6. 使用PC1（Hub内网）访问PC2（Spoke1内网）或PC3（Spoke2内网），可以正常通信。

```bash
C:\Users\Administrator.SUMMERICE2019>ipconfig
以太网适配器 Ethernet0:
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.100
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.0.1

C:\Users\Administrator.SUMMERICE2019>ping 192.168.1.100
正在 Ping 192.168.1.100 具有 32 字节的数据:
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=1ms TTL=126
来自 192.168.1.100 的回复: 字节=32 时间=3ms TTL=126
192.168.1.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 3ms, 平均 = 1ms
```

7. Debug Flow显示ICMP Request报文到达FortiGate后，路由查找网关为Hub与Spoke1的IPSec子隧道Hub_0的`tun_id`200.1.1.2。该流量最终可以被送入IPSec子隧道Hub_0送往Spoke1。

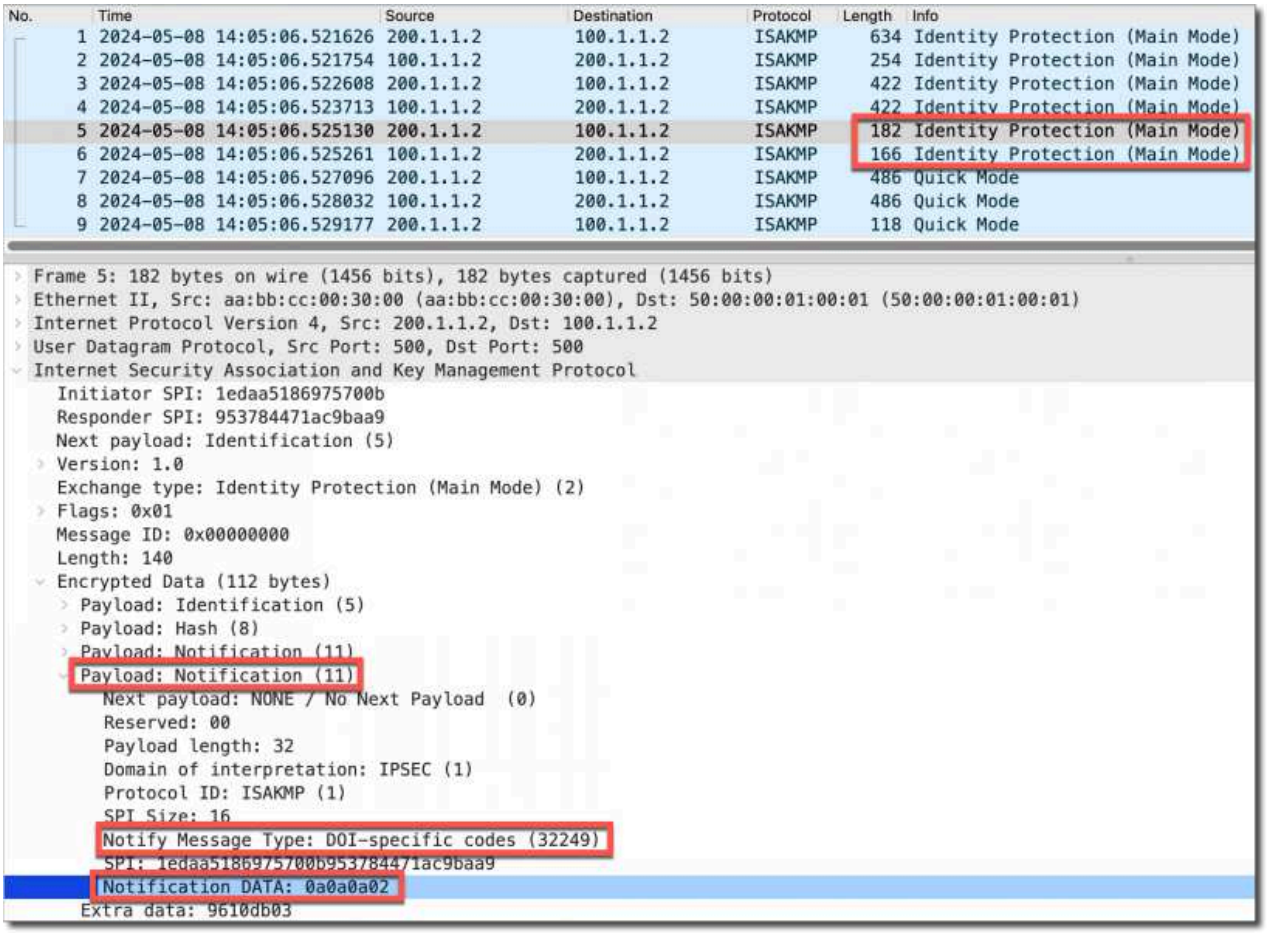



```
Hub # id=65308 trace_id=11 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=1, 192.168.0.100:1->192.168.1.100:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=1, seq=55745."
id=65308 trace_id=11 func=init_ip_session_common line=6080 msg="allocate a new session-00000206, tun_id=0.0.0.0"
id=65308 trace_id=11 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-10.10.10.2 via Hub"
id=65308 trace_id=11 func=__iprope_tree_check line=535 msg="gnum-100004, use addr/intf hash, len=2"
id=65308 trace_id=11 func=fw_forward_handler line=989 msg="Allowed by Policy-1:"
id=65308 trace_id=11 func=ip_session_confirm_final line=3113 msg="npu_state=0x100, hook=4"
id=65308 trace_id=11 func=ipsecdev_hard_start_xmit line=662 msg="enter IPSec interface Hub, tun_id=0.0.0.0"
id=65308 trace_id=11 func=_do_ipsecdev_hard_start_xmit line=222 msg="output to IPSec tunnel Hub_0 vrf 0"
id=65308 trace_id=11 func=esp_output4 line=921 msg="IPsec encrypt/auth"
id=65308 trace_id=11 func=nipsec_set_ipsec_sa_enc line=925 msg="Trying to offload IPsec encrypt SA (p1/p2/spi={Hub_0/Hub/0xc6241fc9}), npudev=-1, skb-dev=port2"
id=65308 trace_id=11 func=nipsec_set_ipsec_sa_enc line=970 msg="IPSec encrypt SA (p1/p2/spi={Hub_0/Hub/0xc6241fc9}) offloading-check failed, reason_code=2."
id=65308 trace_id=11 func=ipsec_output_finish line=641 msg="send to 100.1.1.1 via intf-port2"
id=65308 trace_id=12 func=print_pkt_detail line=5894 msg="vd-root:0 received a packet(proto=1, 192.168.1.100:1->192.168.0.100:0) tun_id=10.10.10.2 from Hub. type=0, code=0, id=1, seq=55745."
id=65308 trace_id=12 func=resolve_ip_tuple_fast line=5982 msg="Find an existing session, id-00000206, reply direction"
id=65308 trace_id=12 func=__vf_ip_route_input_rcu line=1990 msg="find a route: flag=00000000 gw-0.0.0.0 via port3"
id=65308 trace_id=12 func=npu_handle_session44 line=1327 msg="Trying to offloading session from Hub to port3, skb.npu_flag=00000000 ses.state=00010200 ses.npu_state=0x00000100"
id=65308 trace_id=12 func=fw_forward_dirty_handler line=439 msg="state=00010200, state2=00000000, npu_state=00000100"
```

Exchange IP交互报文

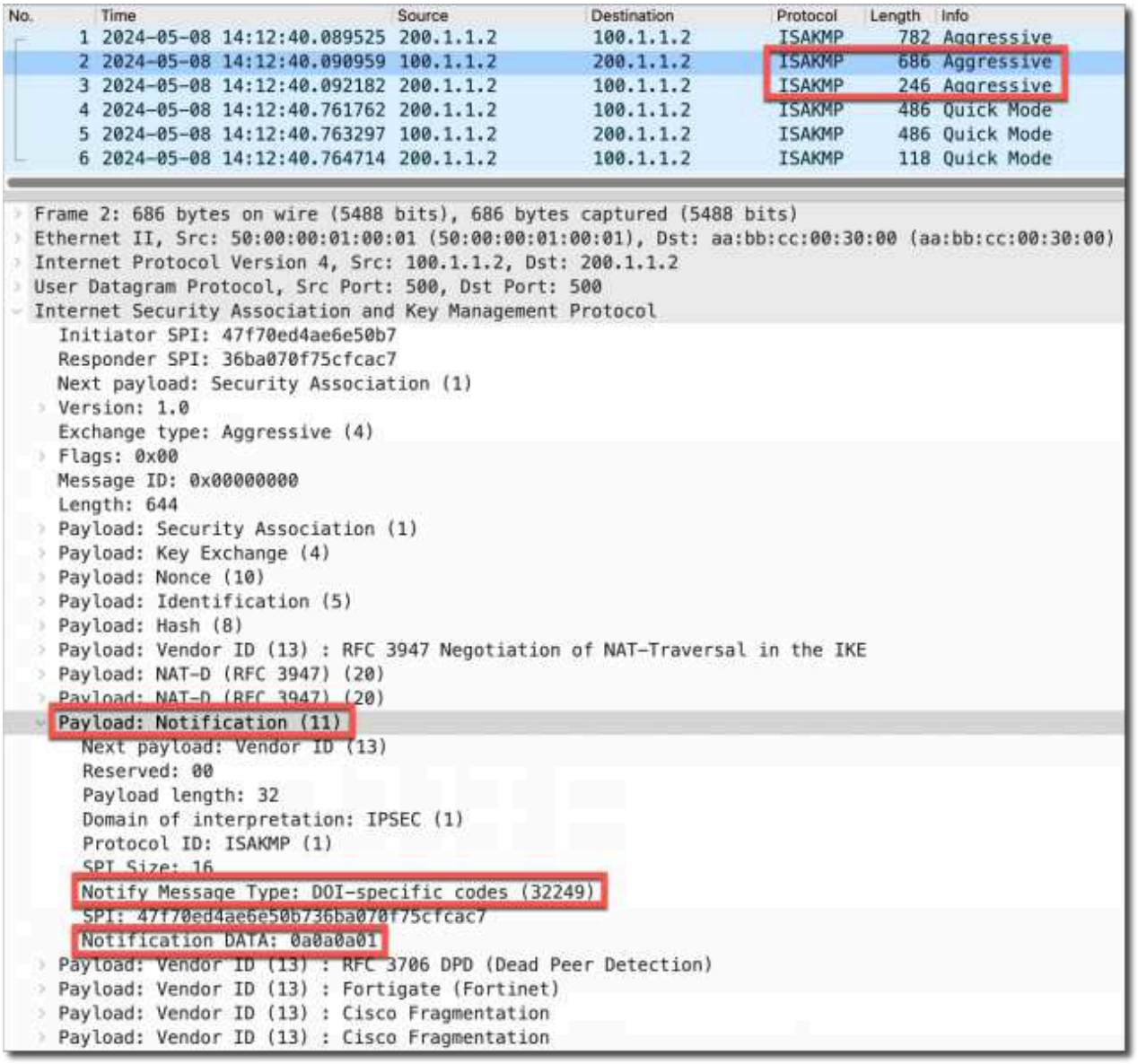
- IKEv1主模式：位于第一阶段第5、6个报文中`Payload: Notification (11)`（`Notify Message Type`为`DOI-specific codes (32249)`）的`Notification DATA`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



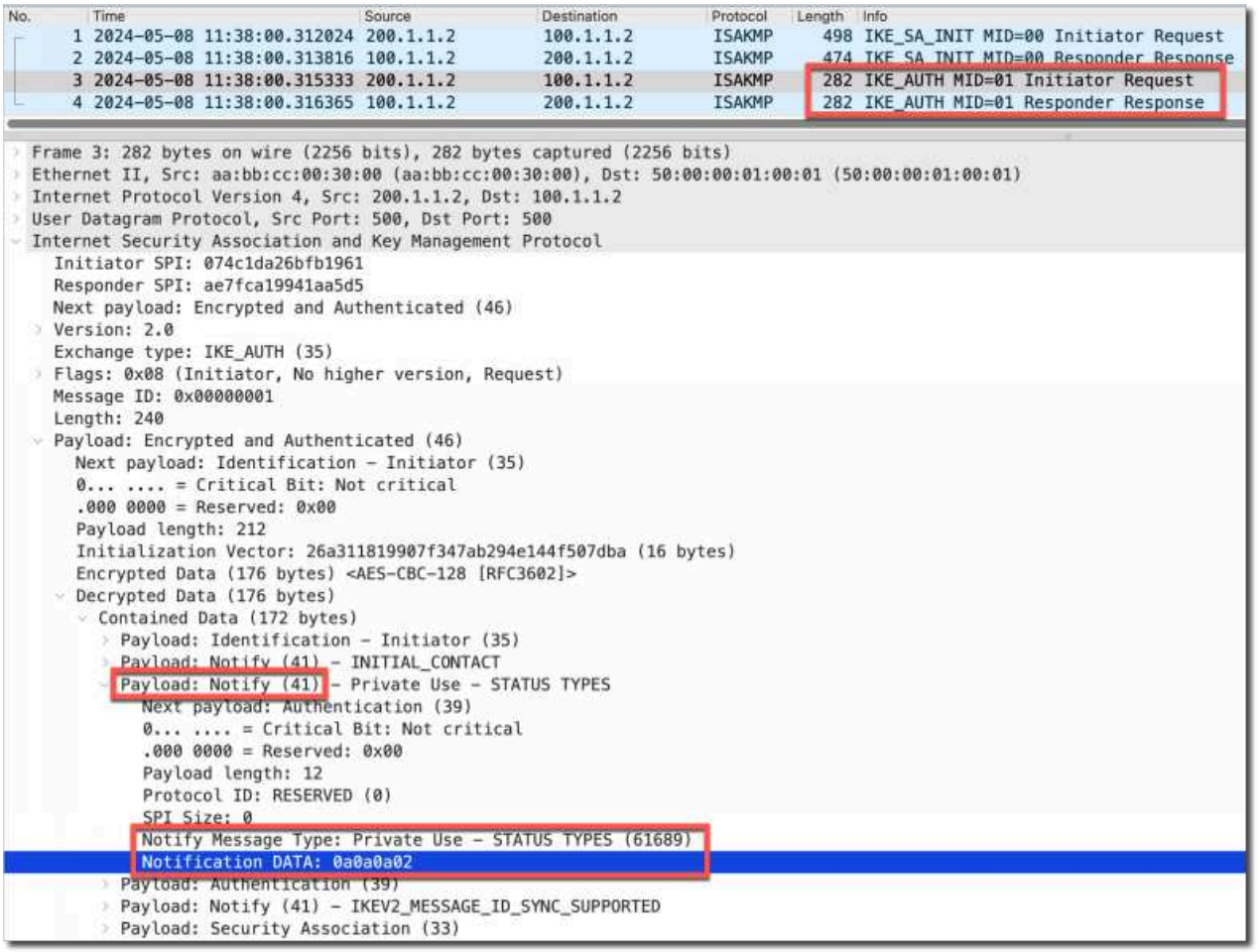
- IKEv1野蛮模式：位于第一阶段第2、3个报文中`Payload: Notification (11)`（`Notify Message Type`为`DOI-specific codes (32249)`）的`Notification DATA`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- IKEv2：位于IKE_AUTH报文中 `Payload: Notify (41)` （ `Notify Message Type` 为 `Private Use - STATUS TYPES (61689)` ）的 `Notification DATA` 。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



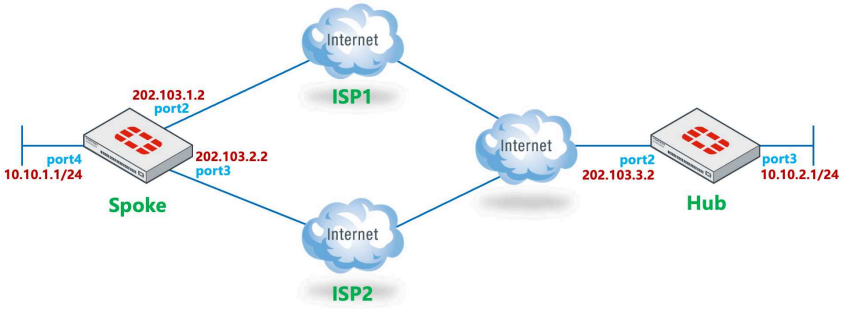
解决方法4-使用动态路由

使用BGP或OSPF等动态路由，自动学习去往Spoke内网网段的路由会携带对应的 `tun_id` 。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Hub 反向流量异步

网络拓扑



1. Spoke 有两条运营商线路 ISP1、ISP2，Hub 只有一条运营商线路。
2. Hub 创建 dynamic 模式的 IPSec VPN，Spoke 配置两条静态隧道与 Hub 建立 IPSec 连接。
3. Spoke 配置 SD-WAN，成员为两条 IPSec 隧道，并配置 SD-WAN 健康检查，检查源为 Spoke 内网口 port4 的 IP 地址，检查目标为 Hub 的内网口 port3 的 IP 地址。
4. 路由层面：
   - Spoke→Hub：Spoke 配置静态路由指向 SD-WAN 区域，IPSec 保护网段的源配置为明细网段 10.10.1.0/24。
   - Hub→Spoke：Hub 通过 IPSec 一阶段中的 `add-route` / 二阶段中的 `set route-overlap allow` 配置自动添加去往 Spoke 内网的路由，并在 Spoke 的两条隧道中负载。

配置信息

基础网络 IP、路由配置略。

Hub

1. 在公网接口 port2 上配置 IPSec 隧道，隧道类型为 dynamic，一阶段开启 `add-route`，二阶段保护网段为 0.0.0.0/0↔0.0.0.0/0，`route-overlap` 配置为 `allow`，`net-device` 为默认关闭状态。

> **相关信息**
>
> - `add-route` 的相关信息请参考：VPN→IPSec VPN→IPSec VPN排错→Hub-Spoke静态路由问题 ↗。
> - `route-overlap` 的相关信息请参考：VPN→IPSec VPN→IPSec VPN排错→Hub-Spoke双线路隧道抖动 ↗。

```bash
config vpn ipsec phase1-interface
    edit "Hub"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256
        set dpd on-idle
        set psksecret fortinet
        set dpd-retryinterval 60
    next
end

config vpn ipsec phase2-interface
    edit "Hub"
        set phase1name "Hub"
        set proposal aes128-sha1
        set route-overlap allow
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置防火墙策略放通 IPSec 隧道与内网口 port3 之间的流量。

```bash
config firewall policy
    edit 1
        set name "VPN_Hub"
        set srcintf "Hub" "port3"
        set dstintf "Hub" "port3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

Spoke

1. 在两条 ISP 线路接口 port2 和 port3 分别创建 IPSec 隧道配置，隧道类型为 static，第二阶段保护网段本端均使用明细的内网网段：10.10.1.0/24↔0.0.0.0/0。

```bash
config vpn ipsec phase1-interface
    edit "vpn_line1"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes128-sha256
        set dpd on-idle
        set remote-gw 202.103.3.3
        set psksecret fortinet
    next
    edit "vpn_line2"
        set interface "port3"
        set peertype any
        set net-device disable
        set proposal aes128-sha256
        set dpd on-idle
        set remote-gw 202.103.3.3
        set psksecret fortinet
    next
end

config vpn ipsec phase2-interface
    edit "vpn_line1"
        set phase1name "vpn_line1"
        set proposal aes128-sha1
        set auto-negotiate enable
        set src-subnet 10.10.1.0 255.255.255.0
    next
    edit "vpn_line2"
        set phase1name "vpn_line2"
        set proposal aes128-sha1
        set auto-negotiate enable
        set src-subnet 10.10.1.0 255.255.255.0
    next
end
```

2. 将两个 IPSec 接口加入 SD-WAN 区域，并配置 SD-WAN 健康检查，检查源为 Spoke 内网口 port4 的 IP 地址，检查目标为 Hub 的内网口 port3 的 IP 地址。

```bash
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "vpn_line1"
        next
        edit 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set interface "vpn_line2"
        next
    end
    config health-check
        edit "to_Hub"
            set server "10.10.2.1"
            set update-static-route disable
            set source 10.10.1.1
            set members 0
        next
    end
end
```

3. 配置防火墙策略放通 2 条 IPSec 隧道（SD-WAN 区域）与内网口 port4 之间的流量。

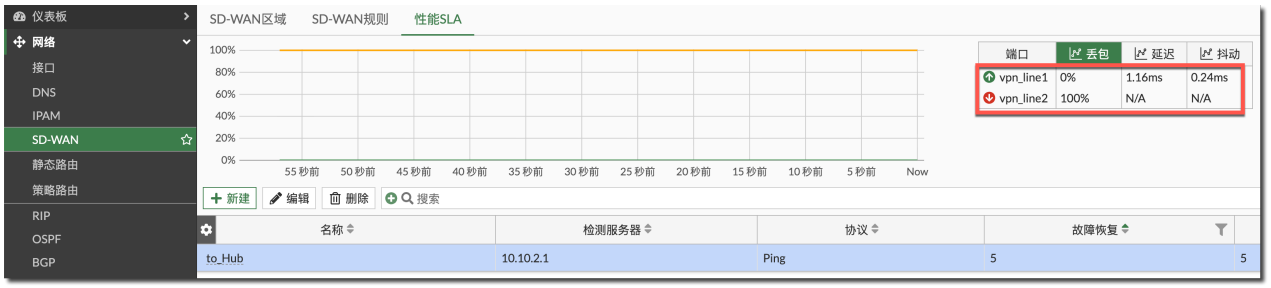
```bash
config firewall policy
    edit 1
        set name "all"
        set srcintf "virtual-wan-link" "port4"
        set dstintf "port4" "virtual-wan-link"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

4. 配置去往 Hub 内网网段（192.168.0.0/24）的静态路由，出接口选择 SD-WAN 区域。

```bash
config router static
    edit 3
        set dst 10.10.2.0 255.255.255.0
        set distance 1
        set sdwan-zone "virtual-wan-link"
    next
end
```

问题现象

1. Spoke 与 Hub 的两条 IPSec 隧道建立后，SD-WAN 健康检查工作异常，在 vpn_line1 隧道上显示 `alive`，vpn_line2 隧道显示 `dead`。




```bash
Spoke # diagnose sys sdwan health-check status
Health Check(to_Hub):
Seq(1 vpn_line1): state(alive), packet-loss(0.000%) latency(1.092), jitter(0.172), mos(4.404), bandwidth-up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x0
Seq(2 vpn_line2): state(dead), packet-loss(100.000%) sla_map=0x0
```

2. 在 Spoke 上抓包，可以看到健康检查从 Spoke 两条隧道 vpn_line1、vpn_line2 分别发送了 ICMP Request，但 ICMP Reply 都是从 vpn_line1 返回的。这说明 Hub 在返回 ICMP Reply 报文时送错了隧道，所以 Spoke 认定 vpn_line2 为 `dead` 状态。

```bash
Spoke # diagnose sniffer packet any 'host 10.10.2.1 and icmp' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.1 and icmp]
0.277013 vpn_line1 out 10.10.1.1 → 10.10.2.1: icmp: echo request
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
0.277148 vpn_line2 out 10.10.1.1 → 10.10.2.1: icmp: echo request
0.278120 vpn_line1 in 10.10.2.1 → 10.10.1.1: icmp: echo reply
0.278160 vpn_line1 in 10.10.2.1 → 10.10.1.1: icmp: echo reply
```

3. 在Hub上查看路由表，可以看到去往Spoke内网（10.10.1.0/24）的路由等价负载到了两条IPSec隧道（Hub_0、Hub_1）上。

```bash
Hub # get router info routing-table all
......
Routing table for VRF=0
S       10.10.1.0/24 [15/0] via Hub_1 tunnel 202.103.1.2, [1/0]
                     [15/0] via Hub_0 tunnel 202.103.2.2, [1/0]
......
```

4. 在 Hub 上查看 Spoke 发起的健康检查的 2 条会话，由于 Hub 未开启 `net-device`，所以两条会话的入接口均为 dynamic 模式的 IPSec 接口（Hub，index=16）。

```bash
Hub # diagnose netlink interface list Hub | grep index
if=Hub family=00 type=768 index=16 mtu=1420 link=0 master=0

session info: proto=1 proto_state=00 duration=6288 expire=59 timeout=0 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=0.0.0.0/202.103.1.2 vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=501840/12546/1 reply=501840/12546/1 tuples=2
tx speed(Bps/kbps): 79/0 rx speed(Bps/kbps): 79/0
orgin->sink: org pre->in, reply out->post dev=16->8/8->16 <---入接口为Hub接口 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.10.1.1:31400->10.10.2.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.2.1:31400->10.10.1.1:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=15849 auth_info=0 chk_client_info=0 vd=0
serial=0000a1ef tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
no_ofld_reason:  local

session info: proto=1 proto_state=00 duration=3401 expire=59 timeout=0 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=0.0.0.0/202.103.2.2 vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=271160/6779/1 reply=271160/6779/1 tuples=2
tx speed(Bps/kbps): 79/0 rx speed(Bps/kbps): 79/0
orgin->sink: org pre->in, reply out->post dev=16->8/8->16 <---入接口为Hub接口  gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.10.1.1:32554->10.10.2.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.2.1:32554->10.10.1.1:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=15849 auth_info=0 chk_client_info=0 vd=0
serial=0000a704 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
no_ofld_reason:  local
```

5. Hub 上显示 Spoke 与本端建立了两条 IPSec 隧道 Hub_0 和 Hub_1。Hub 的 Debug Flow 显示所有的 ICMP Reply 都被送进了 Hub_0 隧道，从 Hub_1 隧道收到的 ICMP Request 对应的 ICMP Reply 从 Hub_0 返回，流量没有源进源出。

```bash
Hub # get vpn ipsec tunnel summary
'Hub_0' 202.103.1.2:0  selectors(total,up): 1/1  rx(pkt,err): 158890/0  tx(pkt,err): 317780/0
'Hub_1' 202.103.2.2:0  selectors(total,up): 1/1  rx(pkt,err): 158890/0  tx(pkt,err): 0/0

Hub # diagnose debug flow filter daddr 10.10.1.1
Hub # diagnose debug flow filter proto 1
Hub # diagnose debug enable
Hub # diagnose debug flow trace start 200

↓↓↓↓第1个ICMP Reply（ICMP Request从Hub_0接收），从Hub_0返回↓↓↓↓
id=65308 trace_id=20 func=print_pkt_detail line=6005 msg="vd-root:0 received a packet(proto=1, 10.10.2.1:31400-
>10.10.1.1:0) tun_id=0.0.0.0 from local. type=0, code=0, id=31400, seq=981."
id=65308 trace_id=20 func=resolve_ip_tuple_fast line=6107 msg="Find an existing session, id-0000a1ef, reply
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
direction"
id=65308 trace_id=20 func=ip_session_core_in line=6732 msg="dir=1, tun_id=202.103.1.2"    ←——针对Hub_0收到的ICMP
Request返回的Reply，tun_id为Spoke的vpn_line1公网IP
id=65308 trace_id=20 func=ipsecdev_hard_start_xmit line=662 msg="enter IPSec interface Hub, tun_id=202.103.1.2"
id=65308 trace_id=20 func=_do_ipsecdev_hard_start_xmit line=222 msg="output to IPSec tunnel Hub_0,
tun_id=202.103.1.2, vrf 0"    ←——送到了Hub_0，这个送对了
id=65308 trace_id=20 func=esp_output4 line=917 msg="IPsec encrypt/auth"
id=65308 trace_id=20 func=ipsec_output_finish line=676 msg="send to 202.103.3.1 via intf-port2"

↓↓↓↓第2个ICMP Reply（ICMP Request从Hub_1接收），从Hub_0返回↓↓↓↓
id=65308 trace_id=19 func=print_pkt_detail line=6005 msg="vd-root:0 received a packet(proto=1, 10.10.2.1:31596-
>10.10.1.1:0) tun_id=0.0.0.0 from local. type=0, code=0, id=31596, seq=981."
id=65308 trace_id=19 func=resolve_ip_tuple_fast line=6107 msg="Find an existing session, id-0000a2bd, reply
direction"
id=65308 trace_id=19 func=ip_session_core_in line=6732 msg="dir=1, tun_id=202.103.2.2"    ←——针对Hub_1收到的ICMP
Request返回的Reply，tun_id为Spoke的vpn_line2公网IP
id=65308 trace_id=19 func=ipsecdev_hard_start_xmit line=662 msg="enter IPSec interface Hub, tun_id=202.103.2.2"
id=65308 trace_id=19 func=_do_ipsecdev_hard_start_xmit line=222 msg="output to IPSec tunnel Hub_0,
tun_id=202.103.1.2, vrf 0"    ←——送到了Hub_0，这个送错了
id=65308 trace_id=19 func=esp_output4 line=917 msg="IPsec encrypt/auth"
id=65308 trace_id=19 func=ipsec_output_finish line=676 msg="send to 202.103.3.1 via intf-port2"
```

问题原因

1. 默认配置下，Hub 的 dynamic 模式的 IPSec 连接的 `net-device` 配置为 `disable` 状态，来自同一 Spoke 的多条隧道共享一个 phase1-interface，Hub 做回包决策是：
   - 查路由（通常是 ECMP，指向同一 phase1）。
   - 匹配 selector/proxy-id，也就是感兴趣流。
2. 如果多条隧道的 selector（感兴趣流）相同，多条 SA 会同时匹配。而 Hub 没有 “入向隧道” 的绑定关系，于是回包会落到 “优先级更高 / 先匹配” 的那条路由对应的隧道，形成不对称回流。
3. 典型触发条件：
   - Hub 为 dynamic 模式隧道，`net-device` 为 `disable` 状态。
   - 同一 Spoke 多条隧道。
   - Spoke 多条隧道的 selector/proxy-id（感兴趣流）重复。
   - Hub 回程为 ECMP / 聚合隧道（多条候选路径同权重）。

解决方法 1-Spoke 配置 location-id

重要

- 配置要求：
  - 为每台 Spoke 配置唯一的 `location-id`。这样 Hub 会把来自同一 Spoke 的多条拨号隧道分为一组，**并缓存 “原始入向隧道”**。回包优先在该组里选入向那条隧道，保持对称。
  - `location-id` 只是用于 Hub 识别同一 Spoke 多条隧道的标识，并不是真实的 IP 地址，但建议配置为能标识该 Spoke 的 IP 地址，如 loopback 接口地址。
- 工作原理：
  - 分组：Hub 接收报文时，依据远端上报的 `location-id`，将相同 `location-id`、挂在同一 phase1-interface 的拨号隧道划为同一站点组。
  - 隧道绑定：Hub 会缓存流量的原始入向隧道，形成一个 “隧道组键”，基于 `phase1 + location-id + SPI` 的内部标识。
  - 回包选路：回包时优先在该组内直接选回入向那条隧道。若不可用，再在同组内切换，不会跨到其它 Spoke。

1. 在 Spoke 上配置 `location-id`（同一台 Spoke 的多条隧道用相同的 `location-id`）。

```bash
config system settings
    set location-id 10.10.1.1
end
```

2. 重建 Spoke 与 Hub 间的隧道，然后在 Hub 查看 IPSec 一阶段状态。可以看到 Spoke 将 `location-id` 传递给了 Hub，Hub 将 Spoke 建立的两条隧道标记了相同的 `remote_location: 10.10.1.1`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

提示

`location-id` 通过 IKE 协商传递：

- IKEv1：`Main Mode` 的第 5/6 个报文中的 Fortinet 私有字段。
- IKEv2：`IKE_AUTH` 报文中的 Fortinet 私有字段。

```bash
Hub # diagnose vpn ike gateway list

vd: root/0
name: Hub_0
version: 1
interface: port2 4
addr: 202.103.3.3:500 → 202.103.1.2:500
tun_id: 202.103.1.2/::10.0.0.62
remote_location: 10.10.1.1    ←——Spoke配置的location-id
network-id: 0
transport: UDP
created: 3s ago
peer-id: 202.103.1.2
peer-id-auth: no
pending-queue: 0
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms

  id/spi: 72 d1e24bba9ed24c5b/d31a2eaa6a2cec9f
  direction: responder
  status: established 3-3s ago = 0ms
  proposal: aes128-sha256
  key: 827f2d4a98e8918f-77fd9d748ea39e48
  QKD: no
  lifetime/rekey: 86400/86126
  DPD sent/recv: 00000000/00000000
  peer-id: 202.103.1.2

vd: root/0
name: Hub_1
version: 1
interface: port2 4
addr: 202.103.3.3:500 → 202.103.2.2:500
tun_id: 202.103.2.2/::10.0.0.63
remote_location: 10.10.1.1    ←——Spoke配置的location-id
network-id: 0
transport: UDP
created: 2s ago
peer-id: 202.103.2.2
peer-id-auth: no
pending-queue: 0
IKE SA: created 1/1  established 1/1  time 0/0/0 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 73 4324ed445892ef2b/c7efb986832df49b
  direction: responder
  status: established 2-2s ago = 0ms
  proposal: aes128-sha256
  key: b40c73f8b0deb162-7144c5911025e8fe
  QKD: no
  lifetime/rekey: 86400/86127
  DPD sent/recv: 00000000/00000000
  peer-id: 202.103.2.2
```

3. 在 Spoke 查看 SD-WAN 健康检查状态，两条隧道均为 `alive` 状态。

```bash
Spoke # diagnose sys sdwan health-check status
Health Check(to_Hub):
Seq(1 vpn_line1): state(alive), packet-loss(0.000%) latency(1.358), jitter(0.377), mos(4.403), bandwidth-
up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x0
Seq(2 vpn_line2): state(alive), packet-loss(0.000%) latency(1.194), jitter(0.249), mos(4.404), bandwidth-
up(9999999), bandwidth-dw(9999999), bandwidth-bi(19999998) sla_map=0x0
```

4. 在 Spoke 上抓包，可以看到 ICMP Reply 可以被 Hub 从正确的隧道送回。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
Spoke # diagnose sniffer packet any 'host 10.10.2.1 and icmp' 4
Using Original Sniffing Mode
interfaces=[any]
filters=[host 10.10.2.1 and icmp]
0.241158 vpn_line1 out 10.10.1.1 → 10.10.2.1: icmp: echo request
0.241283 vpn_line2 out 10.10.1.1 → 10.10.2.1: icmp: echo request
0.242357 vpn_line1 in 10.10.2.1 → 10.10.1.1: icmp: echo reply
0.242594 vpn_line2 in 10.10.2.1 → 10.10.1.1: icmp: echo reply
```

解决方法 2-Hub 开启 net-device

> **注意**
>
> 由于会带来 Hub 的性能问题，在 Spoke 数量较多的场景下不推荐此方法。

1. Hub 的 IPSec 一阶段开启 `net-device`，隧道会自动重建。

```bash
config vpn ipsec phase1-interface
    edit "Hub"
        set net-device enable
    next
end
```

2. 在 Hub 上查看 Spoke 发起的健康检查的 2 条会话，由于 Hub 开启了 `net-device`，所以两条会话的入接口为动态生成的 tunnel 接口（Hub_0：index=16，Hub_1：index=17）。此时源进源出特性可以直接根据会话生效。

```bash
Hub # diagnose netlink interface list | grep Hub
if=Hub family=00 type=768 index=16 mtu=1420 link=0 master=0
if=Hub_0 family=00 type=768 index=17 mtu=1420 link=16 master=0
if=Hub_1 family=00 type=768 index=18 mtu=1420 link=16 master=0

session info: proto=1 proto_state=00 duration=6836 expire=59 timeout=0 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=0.0.0.0/202.103.1.2 vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=545680/13642/1 reply=545680/13642/1 tuples=2
tx speed(Bps/kbps): 80/0 rx speed(Bps/kbps): 80/0
orgin->sink: org pre->in, reply out->post dev=17->8/8->17 <——入接口为Hub_0接口 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.10.1.1:31400->10.10.2.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.2.1:31400->10.10.1.1:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=15849 auth_info=0 chk_client_info=0 vd=0
serial=0000a1ef tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
no_ofld_reason:  local

session info: proto=1 proto_state=00 duration=3949 expire=59 timeout=0 refresh_dir=both flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ tun_id=0.0.0.0/202.103.2.2 vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=315000/7875/1 reply=315000/7875/1 tuples=2
tx speed(Bps/kbps): 80/0 rx speed(Bps/kbps): 80/0
orgin->sink: org pre->in, reply out->post dev=18->8/8->18 <——入接口为Hub_1接口 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.10.1.1:32554->10.10.2.1:8(0.0.0.0:0)
hook=post dir=reply act=noop 10.10.2.1:32554->10.10.1.1:0(0.0.0.0:0)
misc=0 policy_id=1 pol_uuid_idx=15849 auth_info=0 chk_client_info=0 vd=0
serial=0000a704 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
no_ofld_reason:  local
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IPSec解密

加密IPSec报文类型

IKE协商阶段

1. IKE协商阶段，部分IKE报文会被加密：
   - IKEv1：
     - 主模式（Main）：Phase 1第5、6个包，Phase 2全部报文。
     - 野蛮模式（Aggressive）：Phase 1第3个包，Phase 2全部报文。
   - IKEv2：
     - IKE_AUTH阶段的全部报文。
     - CREATE_CHILD_SA的全部报文。
2. 报文封装格式（默认端口）：
   - 没有NAT-T：以上报文为UDP 500封装。
   - 有NAT-T：以上报文为UDP 4500封装。
3. 如果在config system settings下修改了ike-port为非500，例如修改为5555，不论有没有NAT-T，IKE协商报文全部用UDP 5555来封装。
4. 不仅包含IKE协商报文，IPSec协商成功后或协商中发送的被加密的Information报文也属于此类型。
5. 当遇到IKE协商失败的情况时，如果IKE Debug无法判断具体的原因，可能需要解密IKE报文来进行判断。

IPSec业务阶段

1. IPSec业务阶段，所有的业务流量会被ESP封装并加密。
2. 报文封装格式：
   - 没有NAT-T：所有的加密报文为IP Protocol 50的ESP包。
   - 有NAT-T：所有的加密报文为UDP 4500封装（默认端口）的ESP包。
3. 如果在config system settings下修改了ike-port为非500，例如修改为5555：
   - 没有NAT-T，所有的加密报文为IP Protocol 50的ESP包。
   - 有NAT-T：所有的加密报文为UDP 5555封装的ESP包。
4. 当遇到IPSec隧道两端内网的PC无法互相通信时，在FortiGate上抓取明文，报文都已送入隧道接口，但不确定ESP报文是否正确发出和接收，此时可以抓取ESP并解密后判断业务流量丢失是发生在FortiGate还是外部网络。

ESP解密步骤

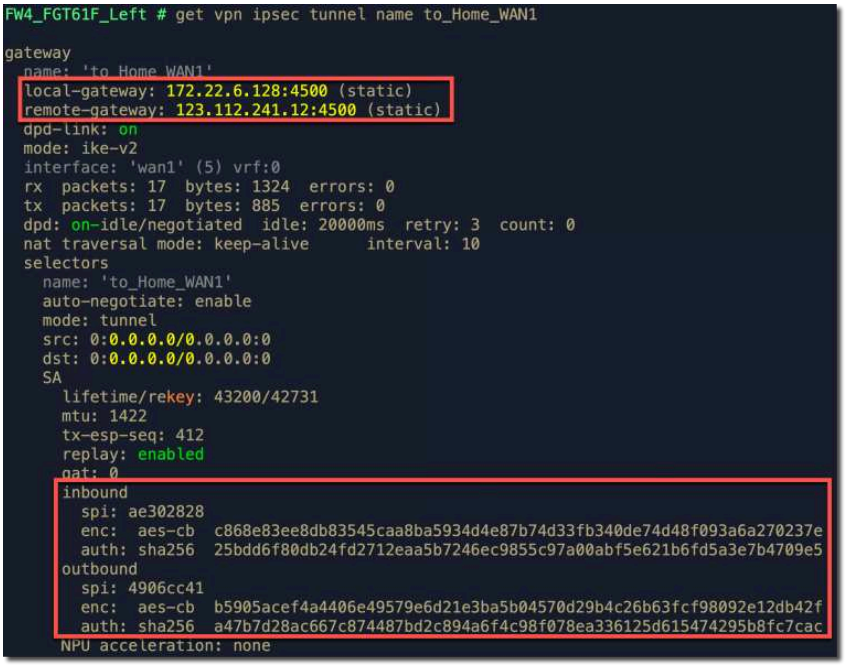
1. 关闭FortiGate IPSec一阶段配置中的npu-offload（VM虚机不需要执行此步骤），否则抓出的ESP包解密后无法看到正确的明文。

> **重要**
>
> 执行此操作后，IPSec隧道会新进行协商，且之后IPSec业务流量无法被NP加速，请在非业务窗口期执行。
>
> 或不执行此步，使用中间可抓包的设备（如交换机的端口镜像）执行抓包操作。

```bash
config vpn ipsec phase1-interface
    edit "to_Home_WAN1"
        set npu-offload disable
    next
end
```

2. 执行如下`get vpn ipsec tunnel name <Tunnel_name>`命令收集当前IPSec隧道的解密信息：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- local-gateway：本地IPSec加密点IP为172.22.6.128
- remote-gateway：对端IPSec加密点123.112.241.12
- inbound（解密方向）：
  - SPI：ae302828
  - enc：解密算法为AES-CBC，解密密钥为c868e83ee8db83545caa8ba5934d4e87b74d33fb340de74d48f093a6a270237e
  - auth：验证算法为sha256，验证密钥为25bdd6f80db24fd2712eaa5b7246ec9855c97a00abf5e621b6fd5a3e7b4709e5
- outbound（加密方向）：
  - SPI：4906cc41
  - enc：解密算法为AES-CBC，解密密钥为b5905acef4a4406e49579e6d21e3ba5b04570d29b4c26b63fcf98092e12db42f
  - auth：验证算法为sha256，验证密钥为a47b7d28ac667c874487bd2c894a6f4c98f078ea336125d615474295b8fc7cac

3. 以上密钥信息也可以通过`diagnose debug application ike -1`的输出结果中找到。

```bash
FortiGate # diagnose debug application ike -1
FortiGate # diagnose debug enable
......
ike 0:to_Home_WAN1:221:to_Home_WAN1:18115: IPsec SA dec spi ae302828 key
32:C868E83EE8DB83545CAA8BA5934D4E87B74D33FB340DE74D48F093A6A270237E auth
32:25BDD6F80DB24FD2712EAA5B7246EC9855C97A00ABF5E621B6FD5A3E7B4709E5
ike 0:to_Home_WAN1:221:to_Home_WAN1:18115: IPsec SA enc spi 4906cc41 key
32:B5905ACEF4A4406E49579E6D21E3BA5B04570D29B4C26B63FCF98092E12DB42F auth
32:A47B7D28AC667C874487BD2C894A6F4C98F078EA336125D615474295B8FC7CAC
ike 0:to_Home_WAN1:221:to_Home_WAN1:18115: added IPsec SA: SPIs=ae302828/4906cc41
ike 0:to_Home_WAN1: HA send IKE connection add 172.22.6.128→123.112.241.12
......
```

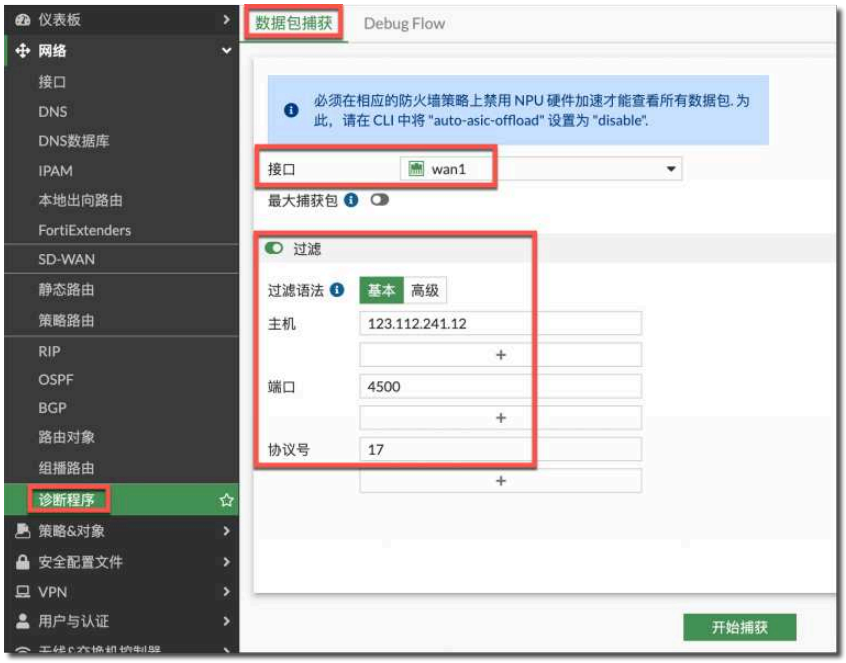
4. 在IPSec通讯接口上抓取ESP包：

- 没有NAT-T：抓取IP Protocol 50的报文。
- 有NAT-T：抓取UDP 4500的报文（默认端口，如果在config system settings下修改了ike-port，则抓取UDP对应的端口号，详见VPN技术→IPSec VPN→点到点VPN→修改IPSec协商端口↗章节）。

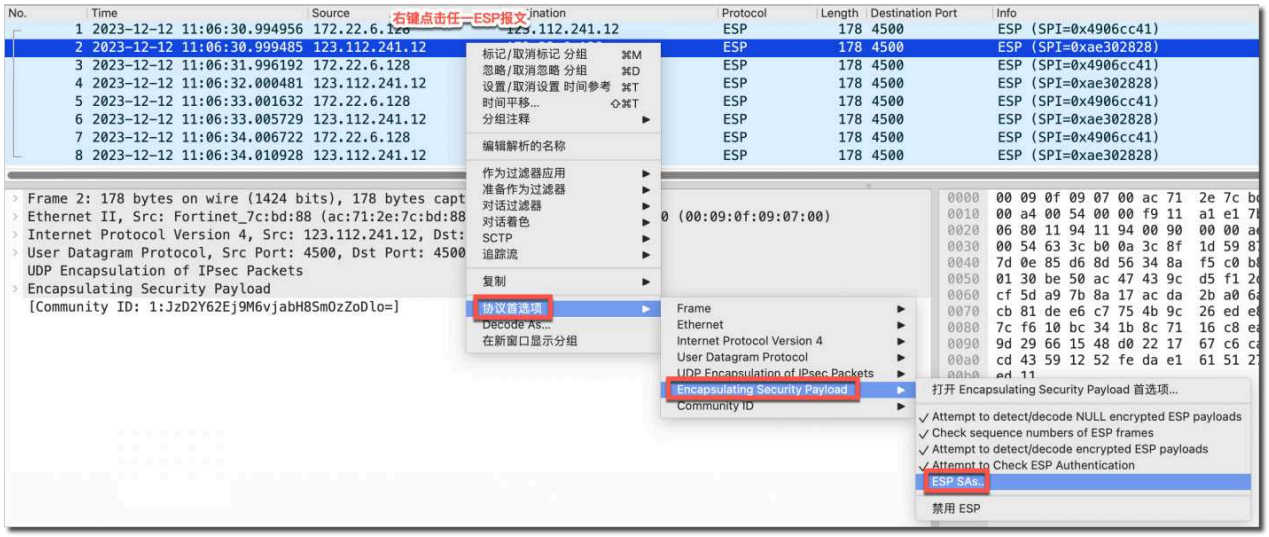
5. 这里我们以有NAT-T环境为例，在ESP报文的出接口wan1上抓取UDP 4500的ESP加密报文，如果没有NAT-T，则抓取IP Protocol 50的报文（GUI方式抓包方法详见故障排查→Sniffer工具→通过GUI界面抓包↗章节）。

> **重要**
>
> 也可以在CLI下使用sniffer抓取格式6的ESP报文，再转换为Wireshark可以打开的格式，详见如下章节：故障排查→Sniffer工具→使用wireshark打开抓包文件↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

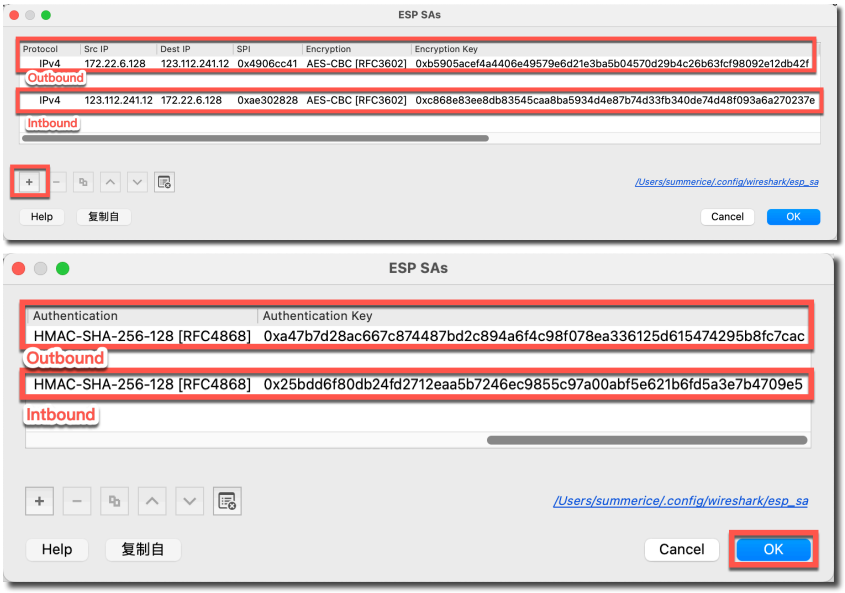


6. 执行两个IPSec站点之间的流量访问后，停止抓包后下载抓包文件，使用Wireshark打开下载的抓包文件，右键点击任意一个ESP报文，依次选择“协议首选项→Encapsulating Security Payload→ESP SAs...”。



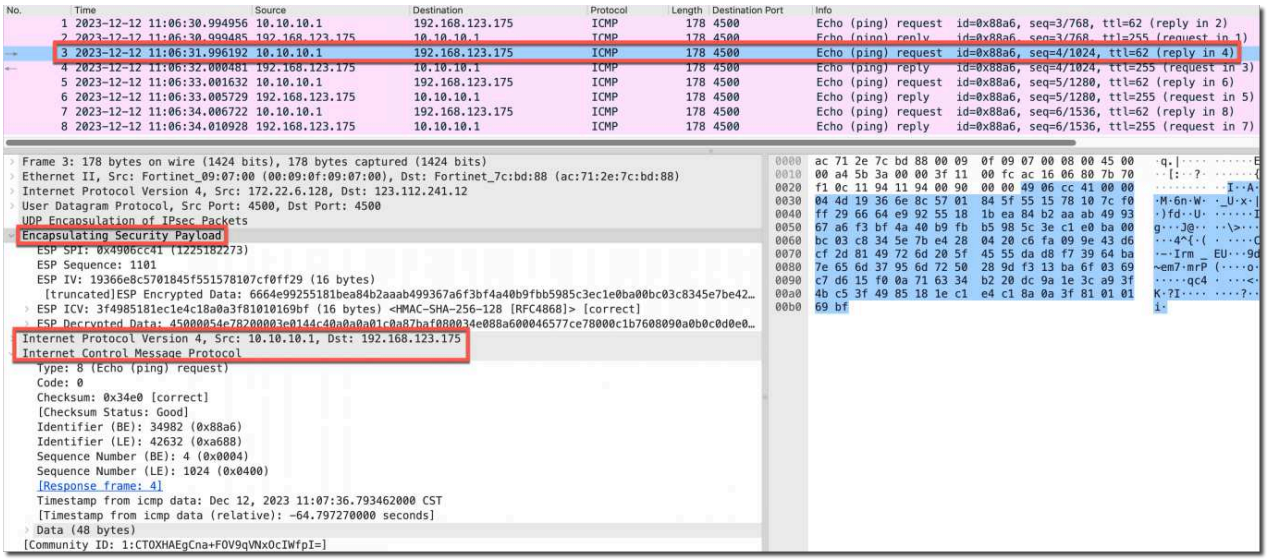
7. 点击左下角的✚，分别新建outbound方向和Inbound方向的SA，根据步骤2或3收集到的网关地址、SPI、算法及密钥信息，填入相应的配置中，填写完成后，点击OK按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 所有的SPI、加密密钥、验证密钥填入时前边都要加入字符0x，如outbound方向的SPI应填写为0x4906cc41。
- 加密算法和验证算法根据步骤2或3收集到的算法选择，这里选择为AES-CBC[RFC3602]和HMAC-SHA-256-128[RFC4868]。

8. 此时即可以看到ESP中加密的明文内容。



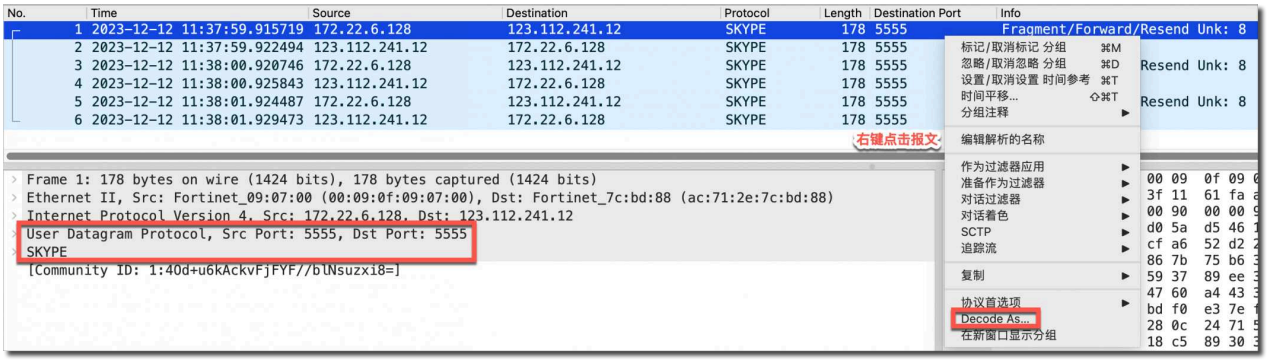
注意事项

1. 如果在 `config system settings` 下修改了ike-port，且存在NAT-T环境，则抓取ESP报文时过滤UDP端口为设置的ike-port端口号（详见VPN技术→IPSec VPN→点到点VPN→修改IPSec协商端口↗章节），如下所示，将两端FortiGate的ike-port均修改为5555。

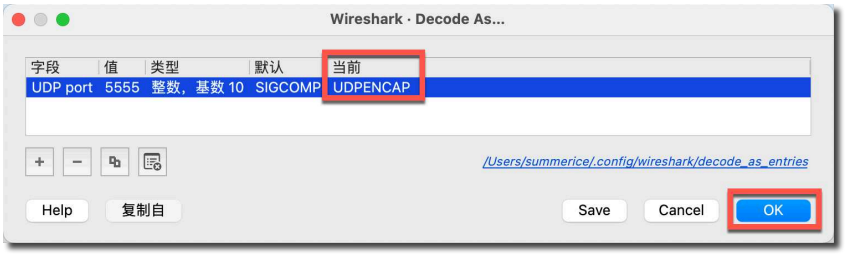
```bash
config system settings
    set ike-port 5555
end
```

2. ESP报文抓取后并使用Wireshark打开，由于ESP报文被UDP 5555封装，Wireshark无法直接解析出这是ESP报文，而是识别为其他协议。这时我们需要右键点击抓到的UDP 5555报文，选择“Decode As...”按钮。

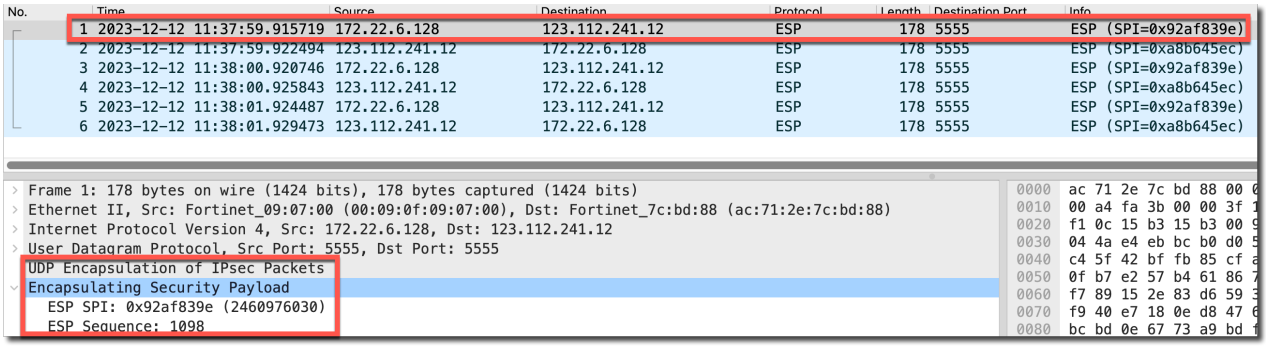
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在弹出的“Decode As...”窗口中，选择UDP 5555的当前列为“UDPENCAP”，即UDP封装的ESP。



4. 再次查看抓到的ESP包，Wireshark可以解析到ESP包头，随后继续使用本章节介绍的ESP解密方法进行解密即可。



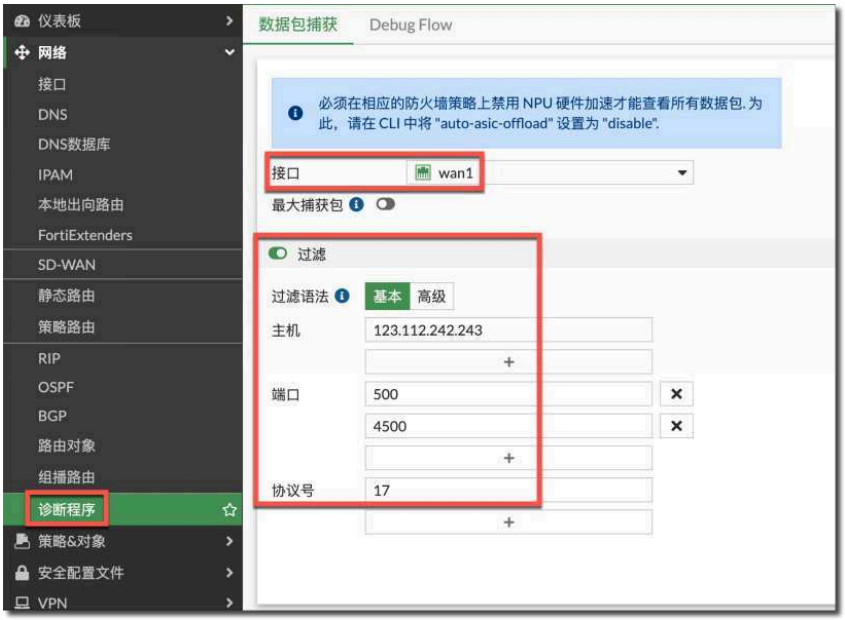
IKE解密步骤

IKEv1

1. 抓取IKE报文不需要关闭npu-offload。首先在IKE协商前开启抓包，这里我们以有NAT-T + IKEv1主模式的环境为例，抓取UDP 500或UDP 4500的数据包。如果没有NAT-T，则只需抓取UDP 500的数据包（GUI方式抓包方法详见故障排查→Sniffer工具→通过GUI界面抓包↗章节）。

> **重要**
>
> 也可以在CLI下使用sniffer抓取格式6的IKE报文，再转换为Wireshark可以打开的格式，详见如下章节：故障排查→Sniffer工具→使用wireshark打开抓包文件↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 发起IKE协商或重协商，并保存抓取的IKE协商报文（ISAKMP）。

3. 协商完成后，在FortiGate上执行 `get vpn ike gateway <tunnel_name>` 获取IKE密钥信息，需要获取2个如下信息。

```
FW4_FGT61F_Left # get vpn ike gateway to_Home_WAN1

vd: root/0
name: to_Home_WAN1
version: 1
interface: wan1 5
addr: 172.22.6.128:4500 -> 123.112.242.243:4500
created: 478s ago
peer-id: 192.168.123.175
peer-auth: no
IKE SA  created: 1/1  established: 1/1  time: 20/20/20 ms
IPsec SA  created: 1/1  established: 1/1  time: 10/10/10 ms

  id/spi: 291 7992f75f885621d0/f522761ae47783ad
  direction: initiator
  status: established 478-478s ago = 20ms
  proposal: aes-256-sha256
  key: 54e29ac67129db6d-96c7e03b20b877f2-bdb4b15288826e8e-13cb202b0bb2cccf
  lifetime/rekey: 86400/85621
  DPD sent/recv: 0000440c/00000000
```

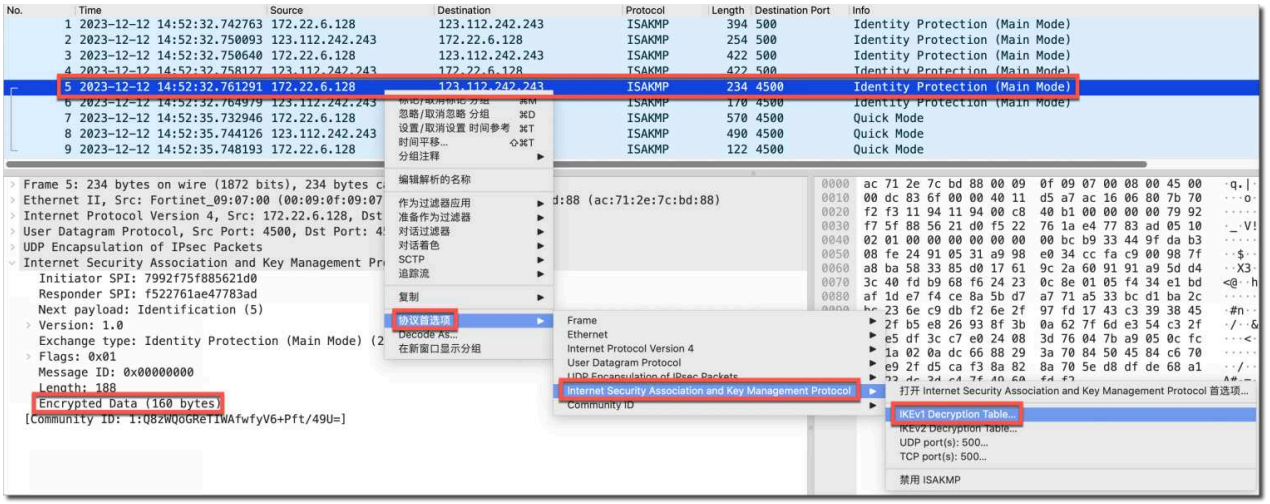
   - 发起方的SPI（Cookie）：这个值从“id/spi”项的值中“/”前边的16进制字符获取，此例中为7992f75f885621d0（发起方的Cookie永远在“/”符号之前）。
   - key：54e29ac67129db6d96c7e03b20b877f2bdb4b15288826e8e13cb202b0bb2cccf（需要将中间的“-”字符删除）。

4. 以上解密材料也可以通过 `diagnose debug application ike -1` 的协商过程输出结果中找到（如果IKE协商过程中失败，或协商成功后就中断，来不及使用步骤3的命令查看密钥信息，可以使用此方法代替）。

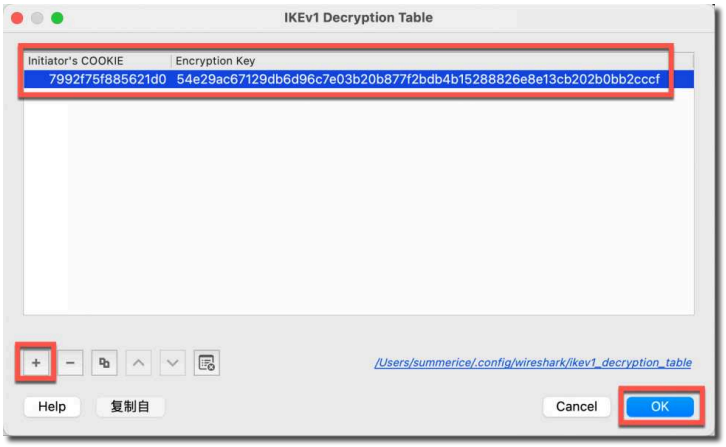
```bash
FortiGate # diagnose debug application ike -1
FortiGate # diagnose debug enable
......
ike 0:to_Home_WAN1:291: ISAKMP SA 7992f75f885621d0/f522761ae47783ad key
32:54E29AC67129DB6D96C7E03B20B877F2BDB4B15288826E8E13CB202B0BB2CCCF
......
```

5. 使用Wireshark打开步骤2中抓取的IKE协商报文（ISAKMP）。可以看到IKEv1主模式从第5个报文开始加密。右键点击任意一个ISAKMP报文，依次选择“协议首选项→Internet Security Association and Key Management Protocol→IKEv1 Decryption Table...”。

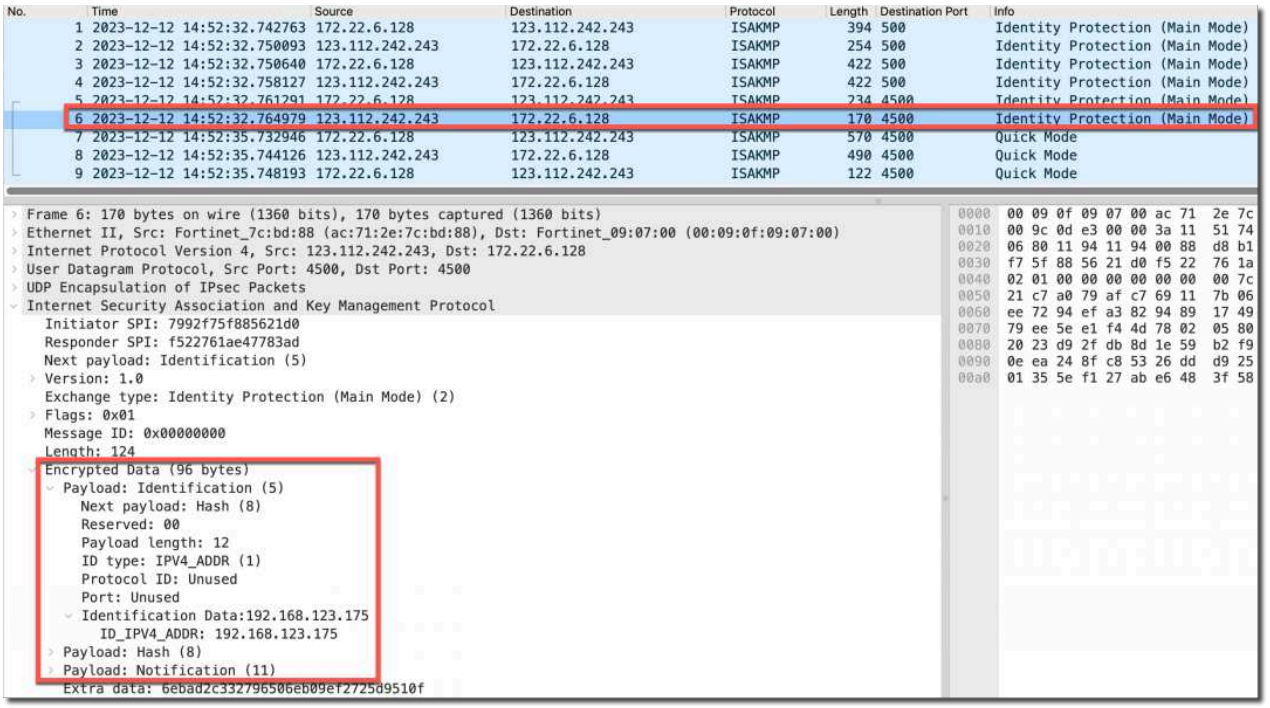
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 在弹出的“IKEv1 Decryption Table”窗口中，点击左下角的✚ 按钮，在“Initiator's COOKIE”中填写步骤3或4获取的发起方的SPI（Cookie）：7992f75f885621d0；在“Encryption Key”中填写步骤3或4获取的key 54e29ac67129db6d96c7e03b20b877f2bdb4b15288826e8e13cb202b0bb2cccf。随后点击OK按钮。



7. 此时即可以看到IKEv1协商报文中加密的明文内容。

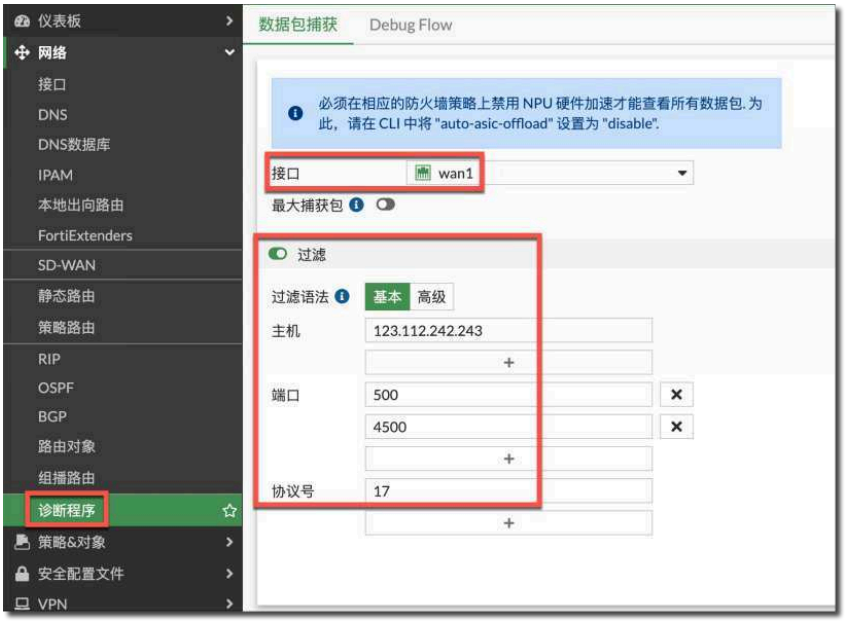


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IKEv2

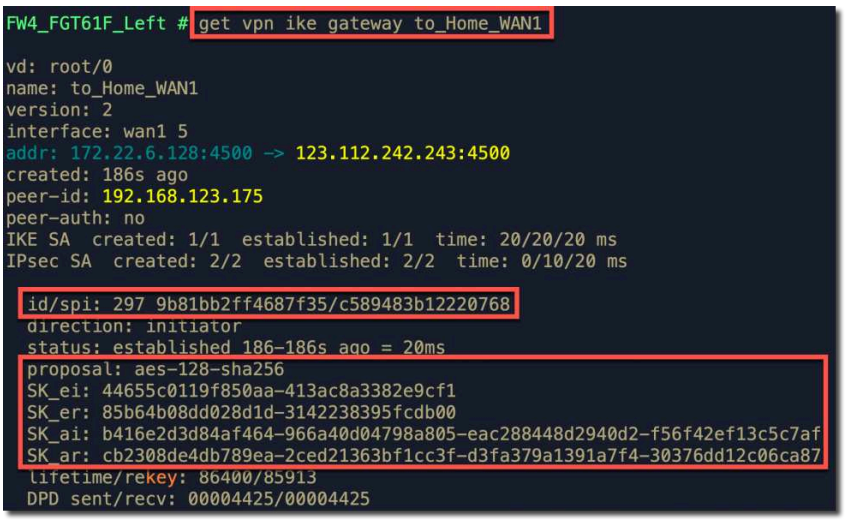
1. 抓取IKE报文不需要关闭npu-offload。首先在IKE协商前开启抓包，这里我们以有NAT-T + IKEv2的环境为例，抓取UDP 500或UDP 4500的数据包。如果没有NAT-T，则只需抓取UDP 500的数据包（GUI方式抓包方法详见故障排查→Sniffer工具→通过GUI界面抓包 ↗章节）。

> **重要**
>
> 也可以在CLI下使用sniffer抓取格式6的IKE报文，再转换为Wireshark可以打开的格式，详见如下章节：故障排查→Sniffer工具→使用wireshark打开抓包文件 ↗。



2. 发起IKE协商或重协商，并保存抓取的IKE协商报文（ISAKMP）。

3. 协商完成后，在FortiGate上执行 `get vpn ike gateway <Tunnel_name>` 获取IKE密钥信息，需要获取8个如下信息。



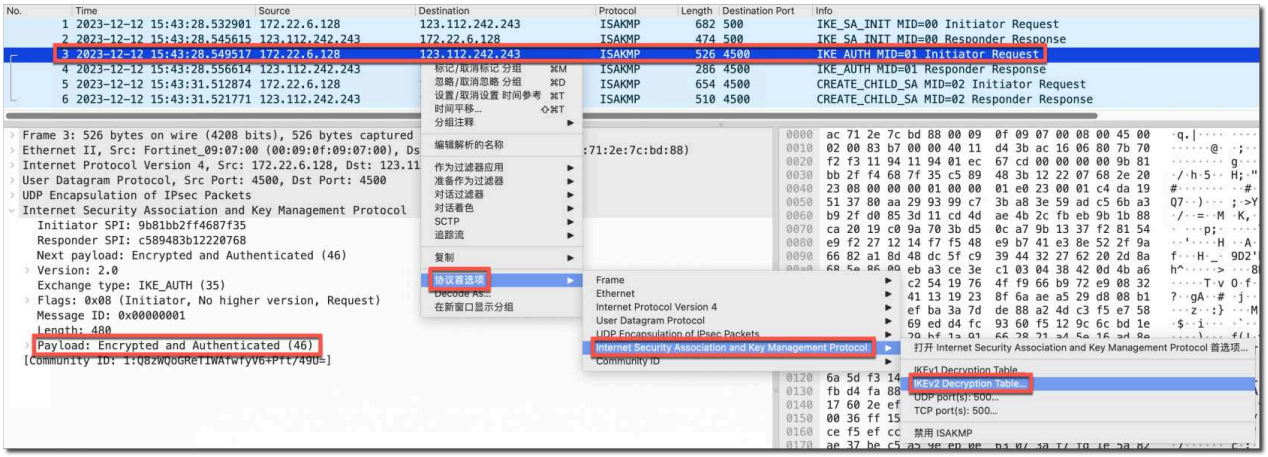
- 发起方的SPI（Cookie）：这个值从“id/spi”项的值中“/”前边的16进制字符获取，此例中为9b81bb2ff4687f35（发起方的Cookie永远在“/”符号之前）。
- 响应方的SPI（Cookie）：这个值从“id/spi”项的值中“/”后边的16进制字符获取，此例中为c589483b12220768（响应方的Cookie永远在“/”符号之后）。
- 加密算法：从“proposal”项中获取，此例为AES-128。
- 验证算法：从“proposal”项中获取，此例为SHA-256。
- SK_ei：44655c0119f850aa413ac8a3382e9cf1（需要将中间的“-”字符删除）。
- SK_er：85b64b08dd028d1d-3142238395fcdb00（需要将中间的“-”字符删除）。
- SK_ai：b416e2d3d84af464966a40d04798a805eac288448d2940d2f56f42ef13c5c7af（需要将中间的“-”字符删除）。
- SK_ar：cb2308de4db789ea2ced21363bf1cc3fd3fa379a1391a7f430376dd12c06ca87（需要将中间的“-”字符删除）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

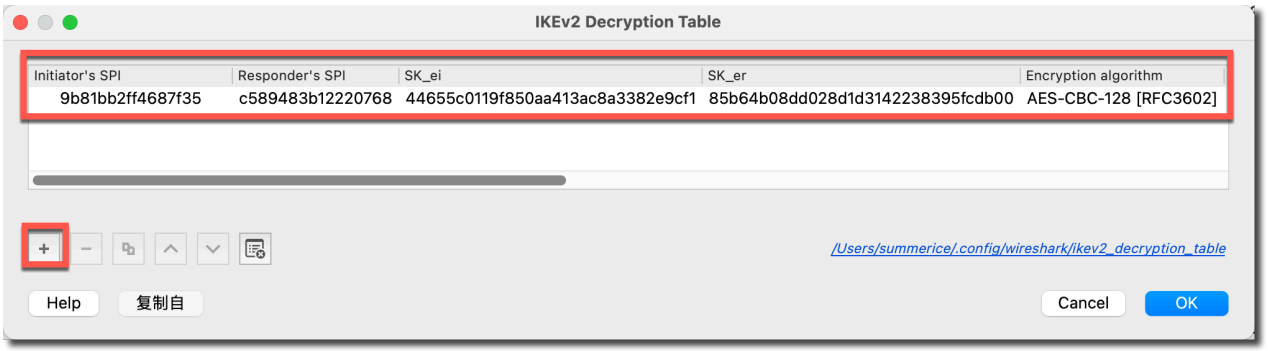
4. 以上解密材料也可以通过 `diagnose debug application ike -1` 的协商过程输出结果中找到（**如果IKE协商过程中失败，或协商成功后就中断，来不及使用步骤3的命令查看密钥信息，可以使用此方法代替**）。

```bash
FortiGate # diagnose debug application ike -1
FortiGate # diagnose debug enable
......
ike 0: comes 123.112.242.243:500→172.22.6.128:500,ifindex=5,vrf=0....
ike 0: IKEv2 exchange=SA_INIT_RESPONSE id=9b81bb2ff4687f35/c589483b12220768 len=432
......
ike 0:to_Home_WAN1:297: matched proposal id 1
ike 0:to_Home_WAN1:297: proposal id = 1:
ike 0:to_Home_WAN1:297:   protocol = IKEv2:
ike 0:to_Home_WAN1:297:      encapsulation = IKEv2/none
ike 0:to_Home_WAN1:297:         type=ENCR, val=AES_CBC (key_len = 128)
ike 0:to_Home_WAN1:297:         type=INTEGR, val=AUTH_HMAC_SHA2_256_128
ike 0:to_Home_WAN1:297:         type=PRF, val=PRF_HMAC_SHA2_256
ike 0:to_Home_WAN1:297:         type=DH_GROUP, val=MODP2048.
ike 0:to_Home_WAN1:297: lifetime=86400
......
ike 0:to_Home_WAN1:297: IKE SA 9b81bb2ff4687f35/c589483b12220768 SK_ei 16:44655C0119F850AA413AC8A3382E9CF1
ike 0:to_Home_WAN1:297: IKE SA 9b81bb2ff4687f35/c589483b12220768 SK_er 16:85B64B08DD028D1D3142238395FCDB00
ike 0:to_Home_WAN1:297: IKE SA 9b81bb2ff4687f35/c589483b12220768 SK_ai
32:B416E2D3D84AF464966A40D04798A805EAC288448D2940D2F56F42EF13C5C7AF
ike 0:to_Home_WAN1:297: IKE SA 9b81bb2ff4687f35/c589483b12220768 SK_ar
32:CB2308DE4DB789EA2CED21363BF1CC3FD3FA379A1391A7F430376DD12C06CA87
......
```

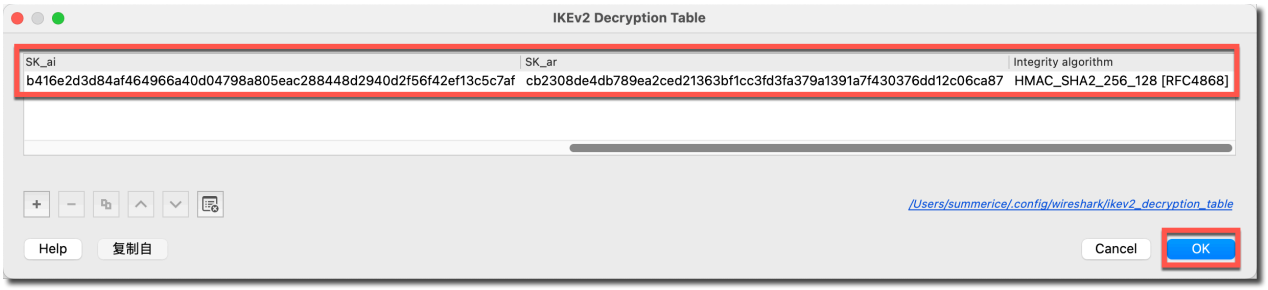
5. 使用Wireshark打开步骤2中抓取的IKE协商报文（ISAKMP）。可以看到IKEv2从IKE_AUTH Initiator Request报文开始加密。右键点击任意一个ISAKMP报文，依次选择“协议首选项→Internet Security Association and Key Management Protocol→IKEv2 Decryption Table...”。



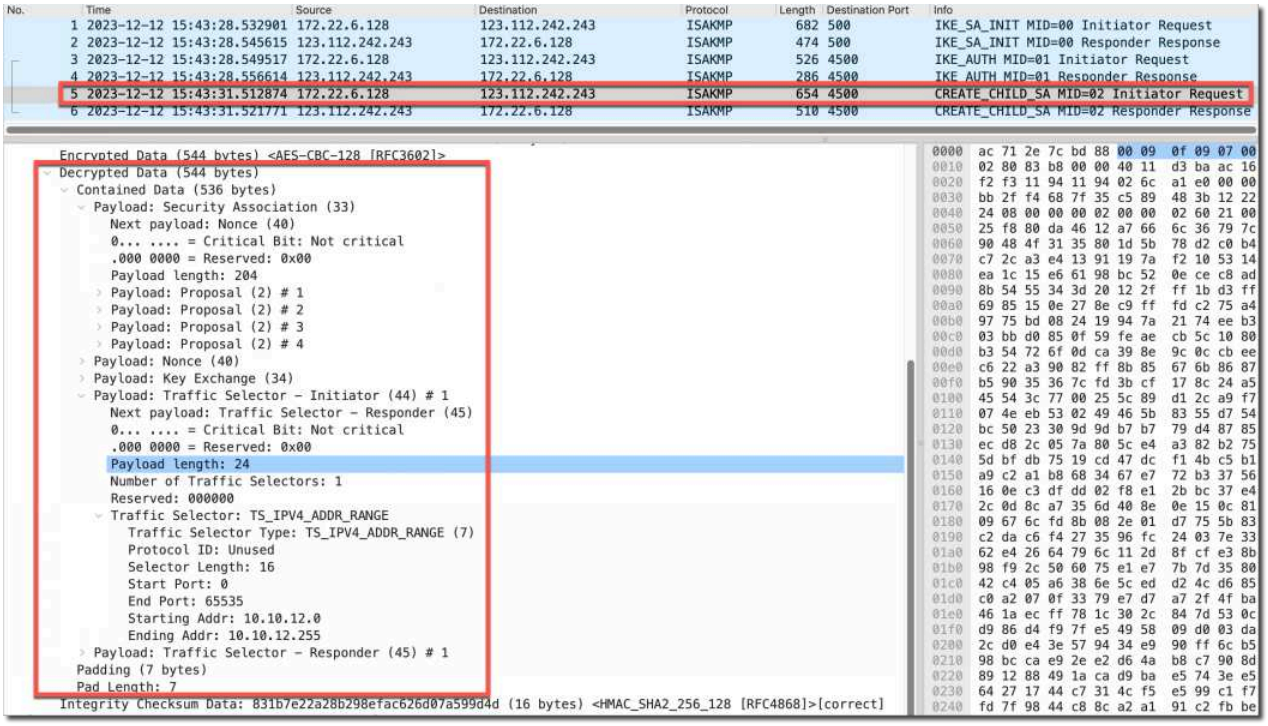
6. 在弹出的“IKEv2 Decryption Table”窗口中，点击左下角的✚ 按钮，依次填写步骤3或4获取的解密材料信息。随后点击OK按钮。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 此时即可以看到IKEv2协商报文中加密的明文内容。



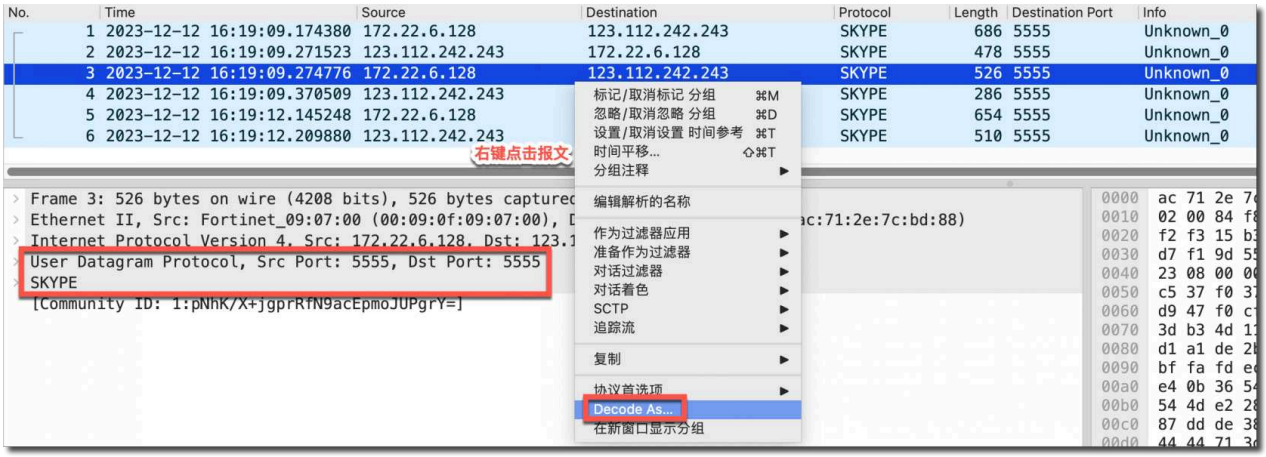
注意事项

1. 如果在`config system settings`下修改了ike-port，无论是否存在NAT-T环境，抓取IKE协商报文时要过滤UDP对应设置的ike-port端口号（详见VPN技术→IPSec VPN→点到点VPN→修改IPSec协商端口↗章节），如下所示，将两端FortiGate的ike-port均修改为5555，所有的IKE协商包和Information报文会被UDP 5555封装。

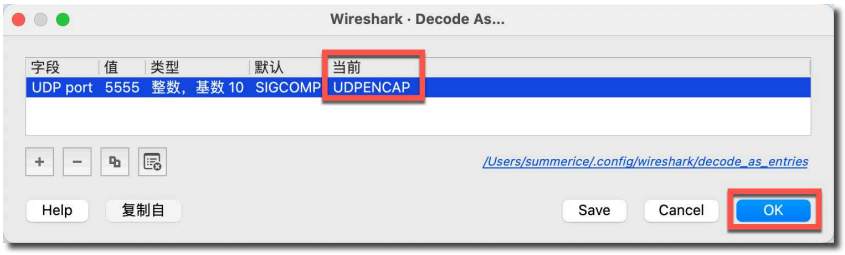
```bash
config system settings
    set ike-port 5555
end
```

2. IKE报文抓取后并使用Wireshark打开，由于IKE报文被UDP 5555封装，Wireshark无法直接解析出这是ISAKMP报文，而是识别为其他协议。这时我们需要右键点击抓到的UDP 5555报文，选择“Decode As...”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

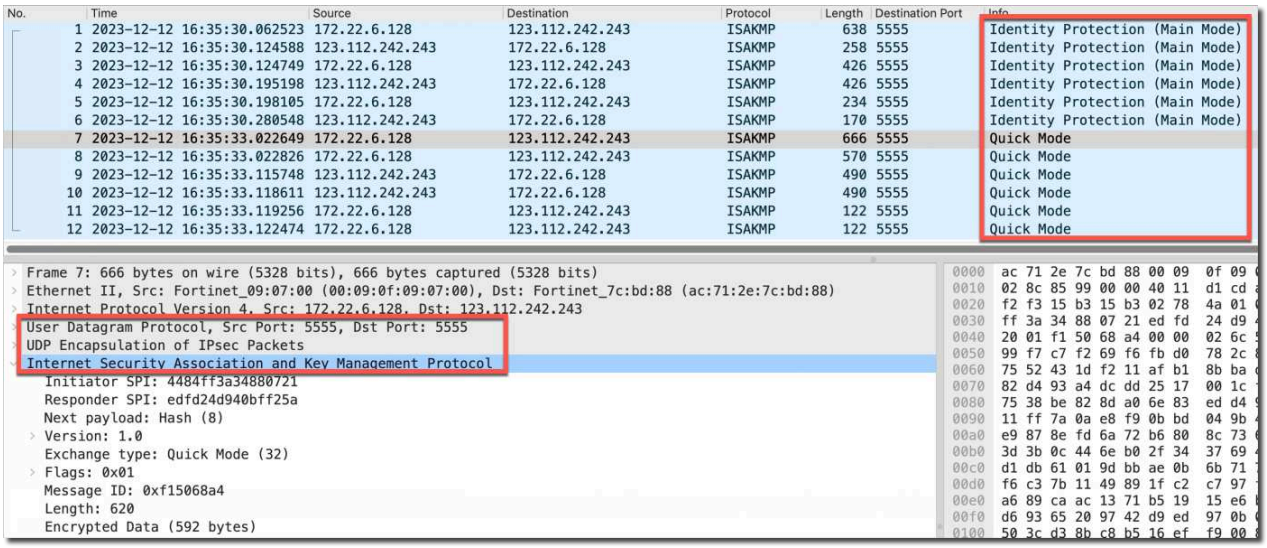


3. 在弹出的“Decode As...”窗口中，选择UDP 5555的“当前”列为“UDPENCAP”，然后点击OK按钮后（注意在修改了ike-port后，这里要选择UDPENCAP，而不是ISAKMP）。



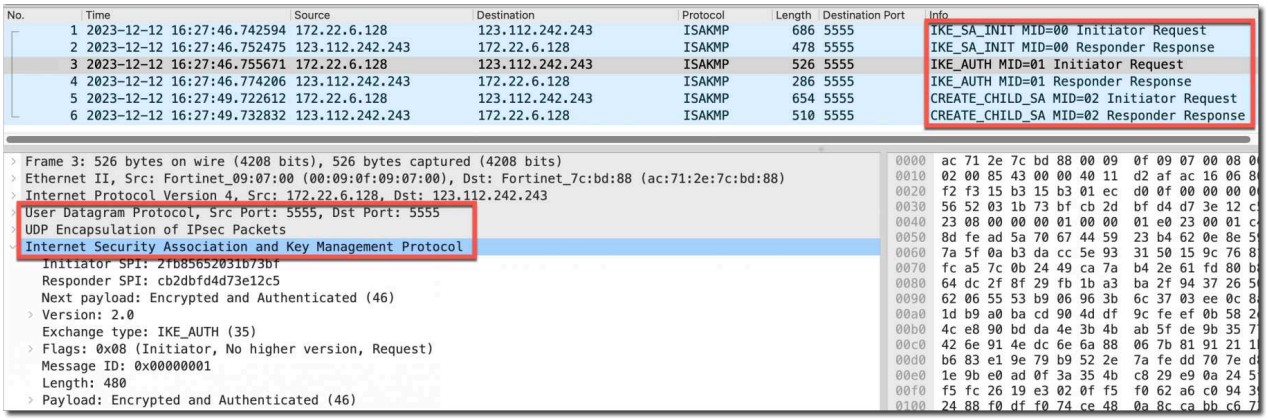
4. 可以看到Wireshark可以解析到IKEv1和IKEv2的ISAKMP协商报文。随后继续使用本章节介绍的IKE解密方法进行解密即可。

- IKEv1：



- IKEv2：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

查看预共享密钥明文

网络需求

某用户配置了认证类型为预共享密钥（PSK）的IPsec隧道，但后期忘记了预共享密钥的明文。在配置文件中，保存的预共享密钥为密文形式，用户想要找回明文格式的预共享密钥。

假设已配置的IPSec连接的预共享密钥明文为`fortinet`。

实现步骤

> **重要**
>
> 此方法只能恢复IPSec预共享密钥，其他密码无法恢复。

1. 在IPSec一阶段中查看当前IPSec配置的密文格式的预共享密钥。

```bash
FortiGate # show vpn ipsec phase1-interface IPSec_1

config vpn ipsec phase1-interface
    edit "IPSec_1"
......
        set psksecret ENC
1zFzDNIyx0t7nN3n1J5xW0YWelhqtPwrAPkjV1cozoRlvqZiP/ZLeeSDXEcdColyuB0s6601rq1gKzhnlsMTlqNKeg70ErfeBY/ITsHZzAioQtCNhe
BJwCL1I4reJQGnY8lBPAmyMkrYL+yJruzwdsUb3pQ84PYadXrZneRqLFQJGFxMku1f646JH0s9ya1TC51CgQ==
    next
end
```

2. 复制密钥内容，如下所示，包含`ENC`字段。

```bash
ENC
1zFzDNIyx0t7nN3n1J5xW0YWelhqtPwrAPkjV1cozoRlvqZiP/ZLeeSDXEcdColyuB0s6601rq1gKzhnlsMTlqNKeg70ErfeBY/ITsHZzAioQtCNhe
BJwCL1I4reJQGnY8lBPAmyMkrYL+yJruzwdsUb3pQ84PYadXrZneRqLFQJGFxMku1f646JH0s9ya1TC51CgQ==
```

3. 在CLI下创建一个测试用的SSID，将上步保存的密钥文本粘贴在`set passphrase`后，完成配置。

```bash
config wireless-controller vap
    edit TestSSID
        set passphrase ENC
1zFzDNIyx0t7nN3n1J5xW0YWelhqtPwrAPkjV1cozoRlvqZiP/ZLeeSDXEcdColyuB0s6601rq1gKzhnlsMTlqNKeg70ErfeBY/ITsHZzAioQtCNhe
BJwCL1I4reJQGnY8lBPAmyMkrYL+yJruzwdsUb3pQ84PYadXrZneRqLFQJGFxMku1f646JH0s9ya1TC51CgQ==
    next
end
```

4. 进入FortiGate的管理页面，打开“无线控制&交换机→SSIDs”页面，右键点击上步创建的SSID，点击编辑按钮查看SSID配置。



5. 在“WiFi设置→预共享密钥”中的“密码”选项中，点击右侧的眼睛按钮，查看明文信息，可以看到明文为`fortinet`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 获取到明文预共享密钥后，删除创建的测试SSID。

重要

创建SSID后会对应创建DHCP服务器和`wqt.<VDOM>`接口、`wqtn.13.TestSSI`接口，依次删除关联项后才能删除SSID。

```bash
config system dhcp server
    delete 2    //确认SSID对应的DHCP服务器ID后再删除//
end

config sys switch-interface
    delete wqtn.root
end

config system interface
    delete wqtn.13.TestSSI
end

config wireless-controller vap
    delete TestSSID
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

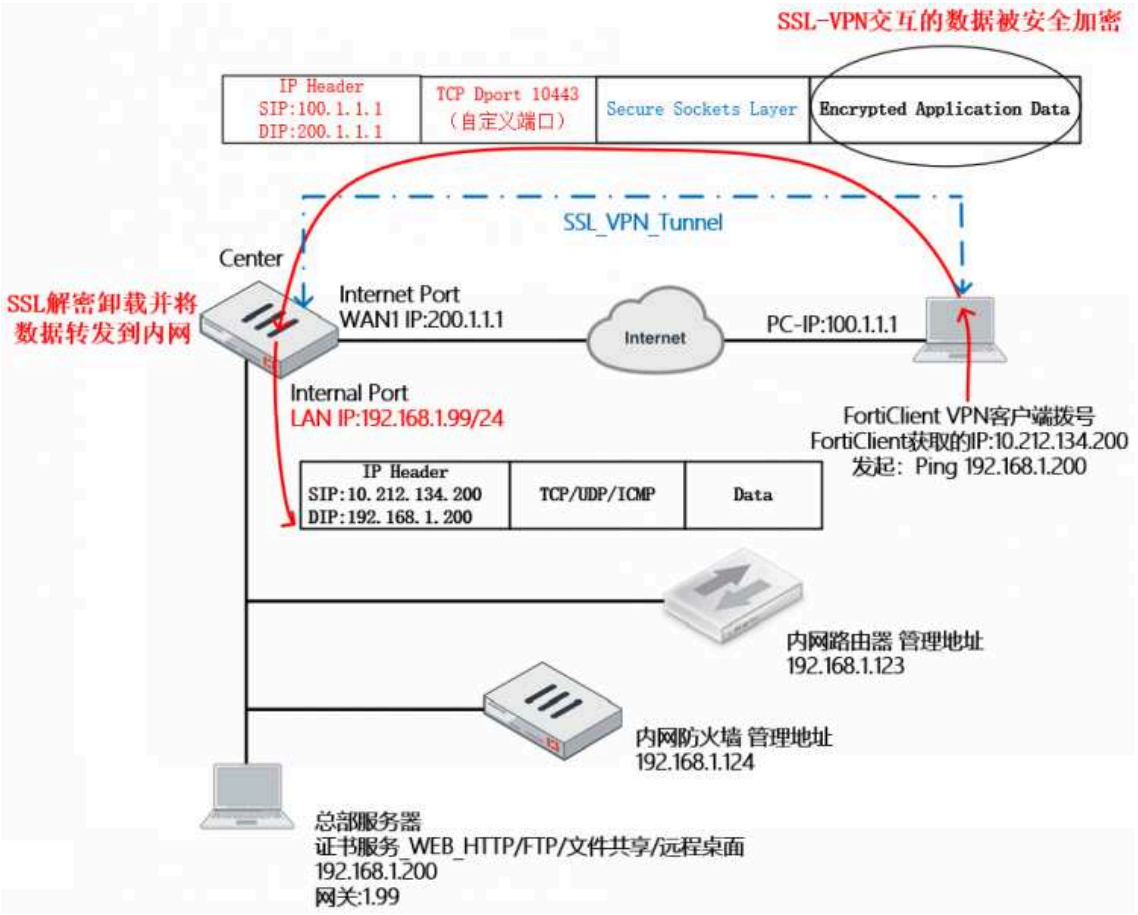
SSL VPN的两种模式

重要

由于部分用户Web服务器的网页代码不够规范，可能与SSL VPN Web代理模式不兼容，导致访问异常，强烈建议使用SSL VPN隧道模式。

SSL VPN 隧道模式

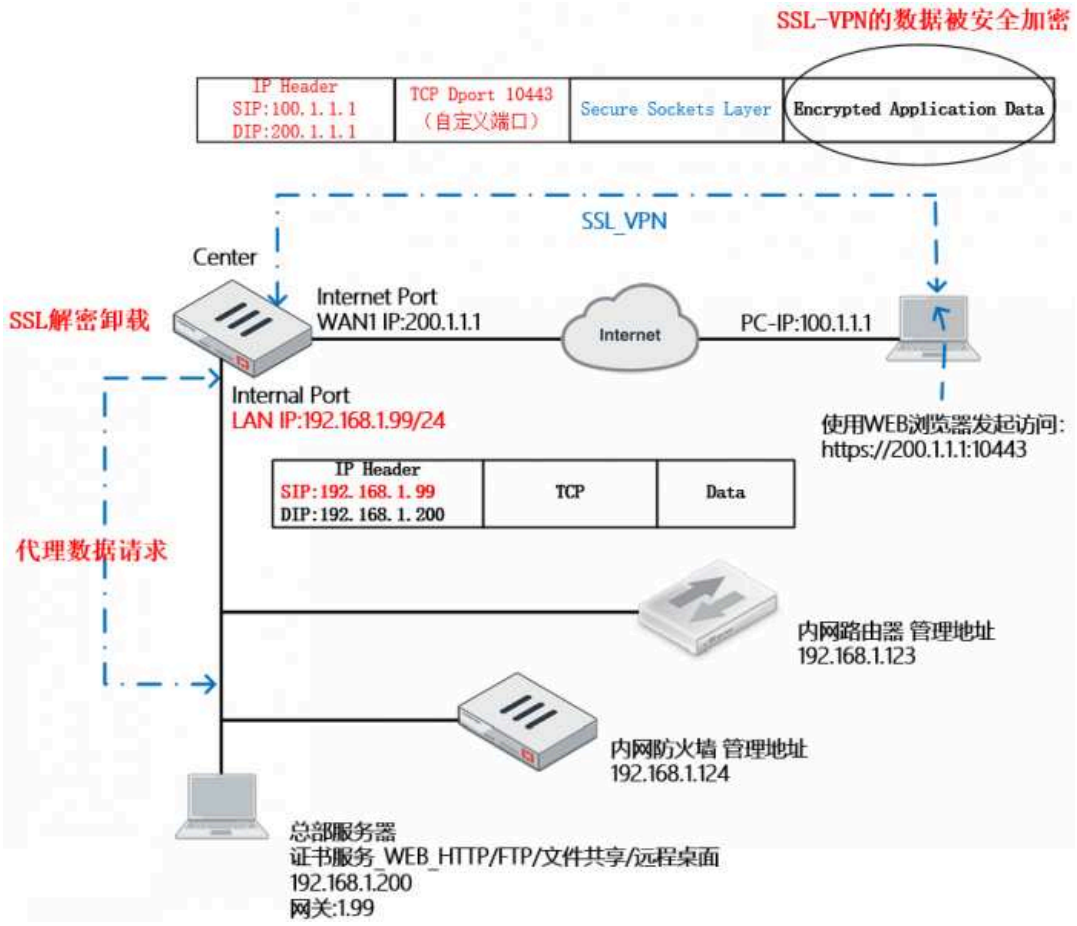
Tunnel模式，需要下载运行的客户端支持。客户端和FortiGate设备建立SSL隧道后，FortiGate为客户端分配IP，客户端通过建立的虚接口直接通过SSL隧道连接到内部网络，推荐使用。



WEB代理模式

Web代理模式，FortiGate将来自远端浏览器的页面请求转发给Web服务器，然后将服务器的响应回传给终端用户。由于有时用户Web服务器的网页代码不够规范，可能与SSLVPN代理模式不兼容，会导致访问异常。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

开启SSL VPN

GUI开启SSL VPN

从FortiOS 7.4.1和7.6.0开始，默认配置下，“VPN→SSL-VPN”相关菜单在GUI界面中被隐藏（但仍可以通过CLI命令配置SSL VPN的相关功能）。

如果需要在GUI启用SSL VPN功能的可见性，需要在CLI下执行以下命令：

```bash
config system settings
    set gui-sslvpn enable    //隧道模式//
end
config system global
    set sslvpn-web-mode enable    //Web模式//
end
```

SSL VPN移除情况

在以下版本的特定型号上完全移除了SSL VPN功能（**即使在CLI下也无法配置和使用**）。

IPSec可以实现与SSL VPN基本相同的接入功能，且支持TCP封装，推荐使用IPSec进行远程接入（请参考VPN技术→IPSec VPN→拨号VPN→基于TCP的FortiClient拨号 ↗章节。

> **重要**
>
> 以下表格中未列出的版本/型号组合仍然可以正常使用SSL VPN功能。

移除SSL VPN的版本	移除SSL VPN的型号
7.6.0	FortiGate-40F/40F-3G4G
	FortiWiFi-40F/40F-3G4G
	FortiGate-60F/61F
	FortiWiFi-60F/61F
	FortiGate-Rugged-60F/60F-3G4G
	FortiGate-80E/81E
	FortiGate-90E/91E
	FortiGate-90G/91G
7.6.3(移除Tunnel模式，仅支持Web模式)	其他所有型号
所有版本	FortiGate-30G
	FortiWiFi-30G
	FortiGate-50G/51G
	FortiGate-50G-SFP-POE/51G-SFP-POE
	FortiWiFi-50G/50G-SFP/50G-DSL
	FortiGate-70G
	FortiWiFi-70G

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSL VPN FortiClient隧道模式

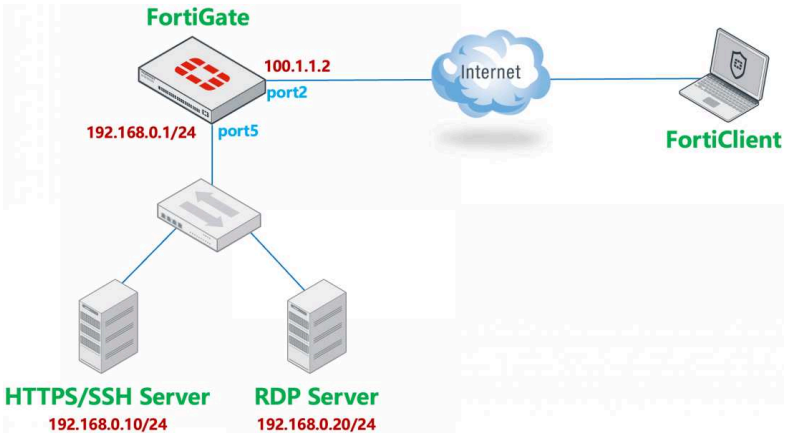
重要

由于部分用户Web服务器的网页代码不够规范，可能与SSL VPN Web代理模式不兼容，导致访问异常，强烈建议使用隧道模式，而不是Web代理模式。

网络需求

在外移动办公的工作人员需要通过SSL VPN隧道模式拨入到公司内网来对内网主机进行访问。

网络拓扑

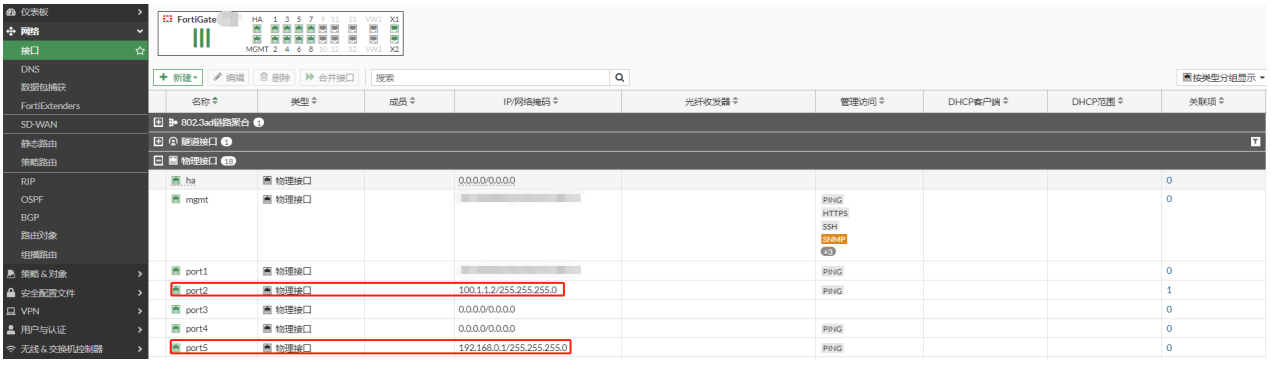


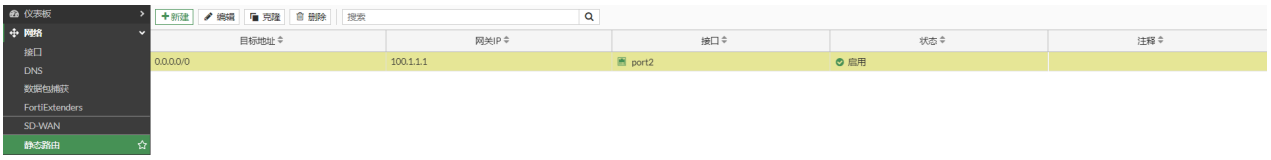
配置步骤

配置SSL VPN

1. **基本配置**

   配置接口IP和路由

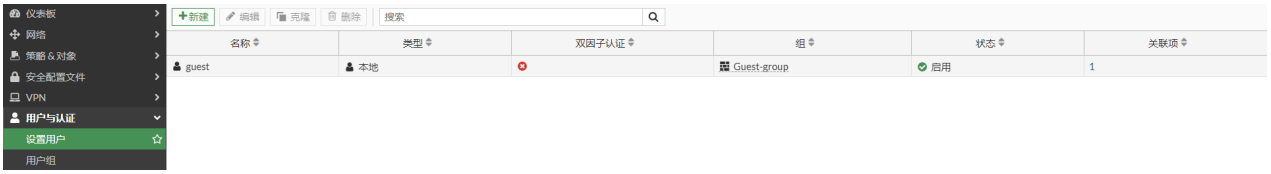




2. **创建用户**

   选择“用户与认证”-->“设置用户”，点击“新建”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



选择“本地用户”，点击“下一步”。



输入用户名和密码，点击“下一步”。

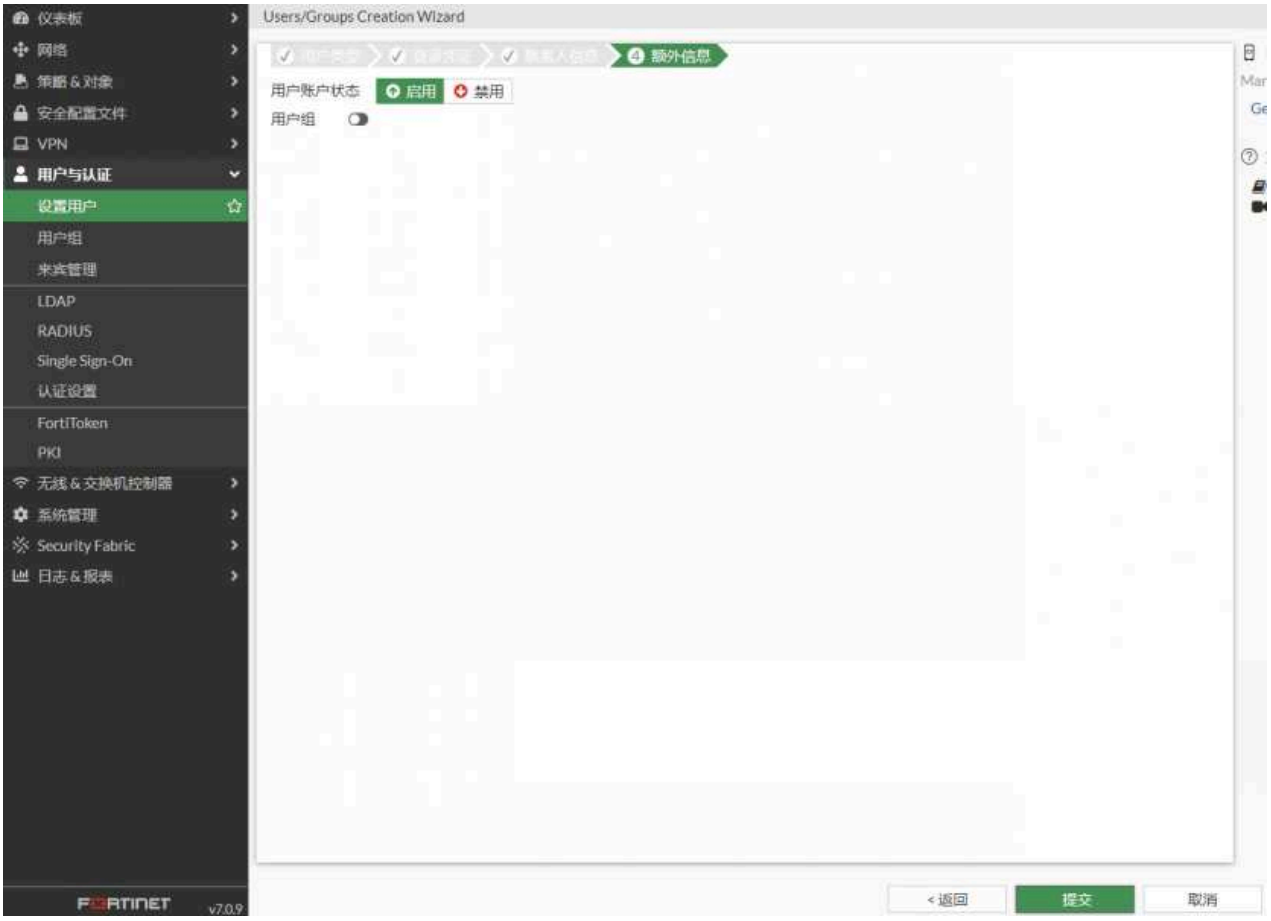


可根据需求选择启用。这里不启用，点击“下一步”。

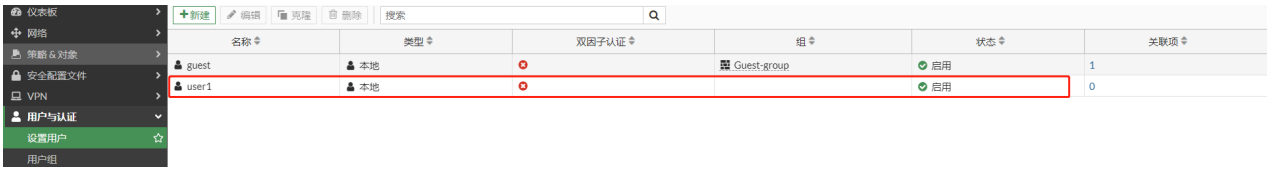


点击“提交”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

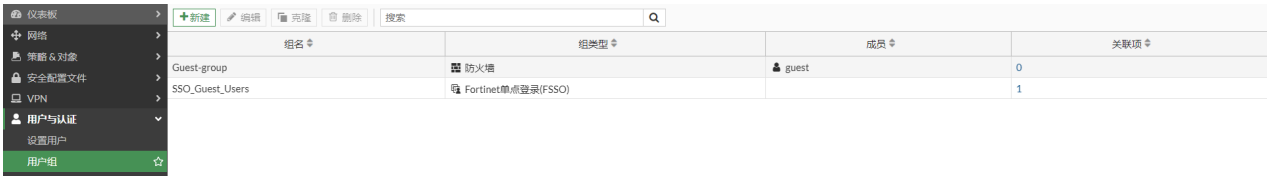


完成用户创建。

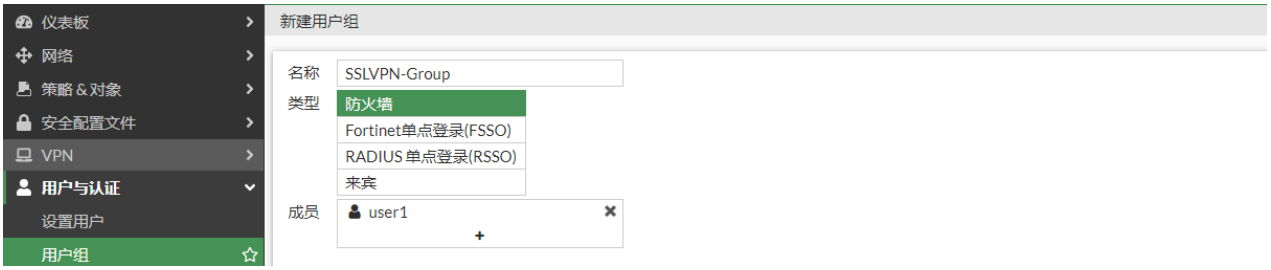


3. 创建用户组

选择“用户与认证”-->“用户组”，点击“新建”。

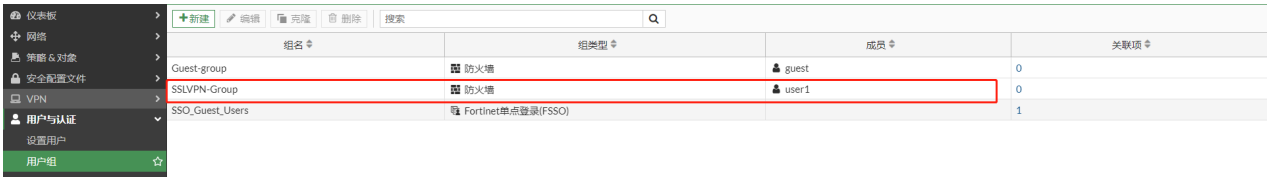


输入名称，即组名，并将用户加入用户组，点击“确认”。



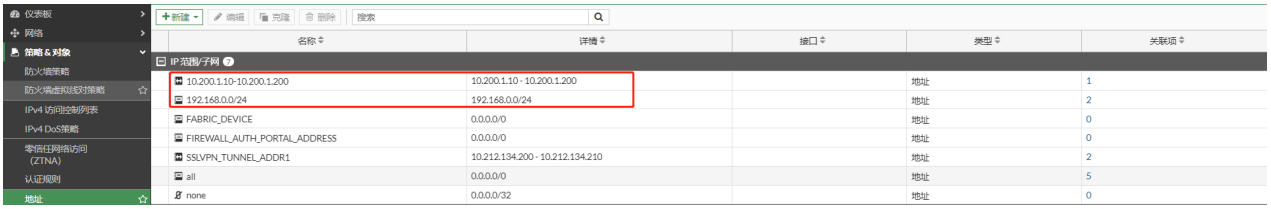
完成用户组创建。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. **配置地址对象**

10.200.1.10-10.200.1.200作为SSLVPN地址池；192.168.0.0/24作为需要访问的内网地址段。



5. **配置SSL-VPN门户**

系统默认创建3个SSLVPN门户：full-access:开启了隧道模式和web代理模式；tunnel-access只开启了隧道模式；web-access：只开启web代理模式。可以根据实际需求进行修改，也可以新建新的SSL-VPN门户。这里使用tunnel-access。



隧道分割的三个选项：

- **禁用**：所有客户端流量都将走SSLVPN隧道；
- **基于策略目标启用**：只有在SSL VPN防火墙策略中的目标地址的流量走SSLVPN；

> **重要**
>
> 在SSL VPN安全策略中配置的目标IP地址对象的相关路由将会下发到客户端的VPN路由表，不支持目标为ISDB条目。
>
> 另外，如果在下方配置了“隧道分割地址”并选择了地址对象，则会覆盖安全策略配置的目标地址作为VPN路由下发到客户端，安全策略将仅做流量控制使用。

- **基于可信目标启用**：访问除192.168.0.0/24之外的流量走SSLVPN。

允许客户端保持密码：FortiClient第一次拨号成功后，FortiClient会显示“保存密码”的选项。

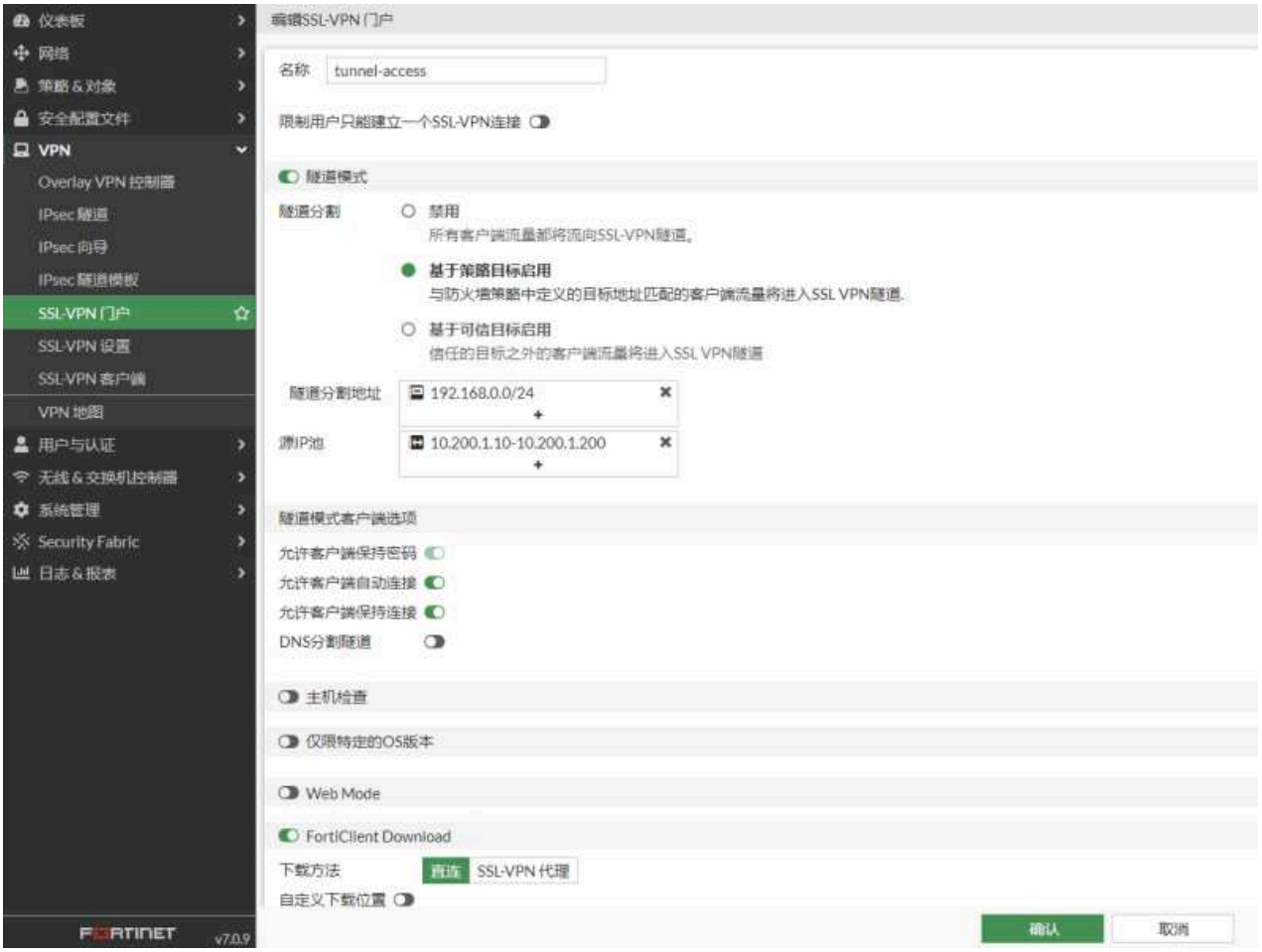
允许客户端自动连接：FortiClient第一次拨号成功后，FortiClient会显示“自动连接”的选项，该功能是运行FortiClient会拨入该SSLVPN。

允许客户端保持连接：FortiClient第一次拨号成功后，FortiClient会显示“保持连接”的选项，该功能是SSLVPN由于网络原因中断后，会自动重拨。

免费的FortiClient版本不支持自动连接和保持连接，需要完整版的FortiClient，需要购买EMS license。

源IP池：客户端SSLVPN拨号成功后获取的地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

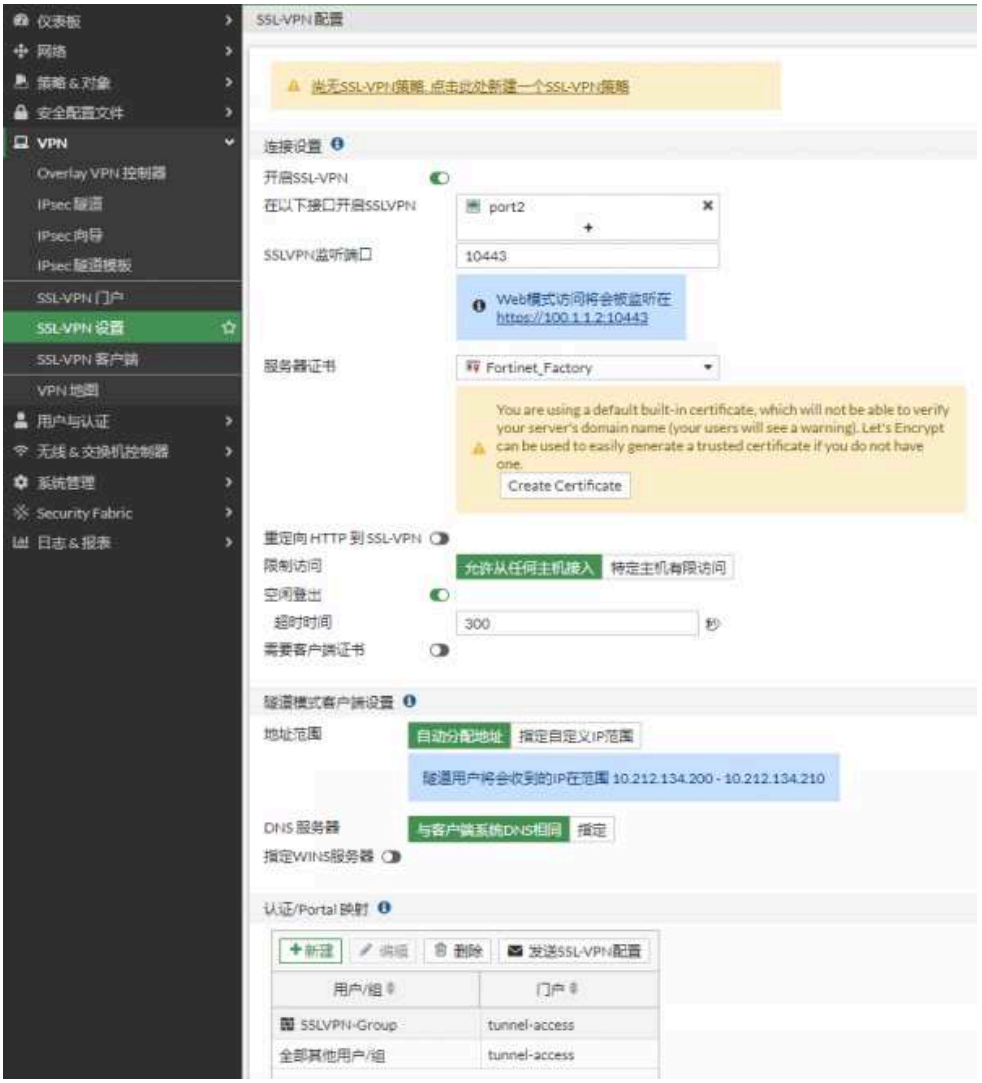


6. **配置SSLVPN**

   设置提供SSLVPN服务的接口和端口，将SSLVPN-Group用户组和tunnel-access门户关联；全部其他用户/组也要关联一个门户，用于没有配置关联的用户/用户组访问。

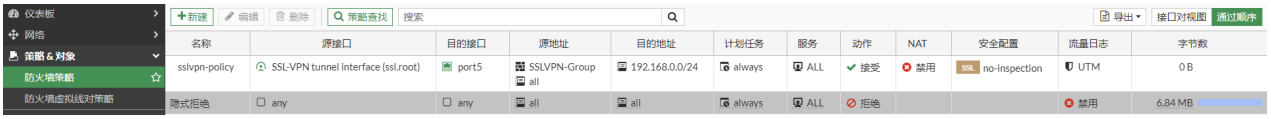
   tunnel-access门户中的 源IP池 优先于SSL-VPN设置中的 地址范围。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 创建策略

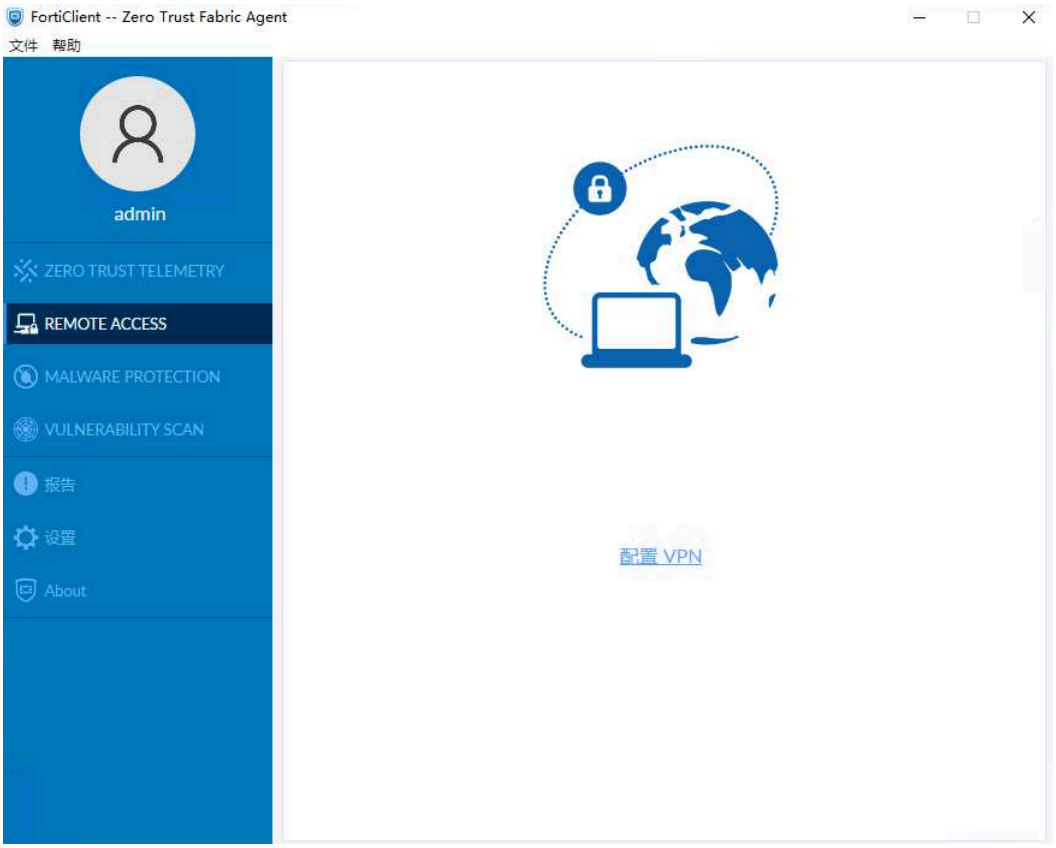
当客户端SSLVPN拨号成功后，将会使用获取的地址（10.200.1.10-10.200.1.200）访问内部主机，因此内部网络需要增加到10.200.1.0/24网段的回程路由指向FortiGate 或者 可以在策略中开启NAT，那么源地址将被转换为FortiGate接口地址，则不用考虑回程路由。



配置FortiClient

1. 选择“Remote Access”，点击“配置VPN”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

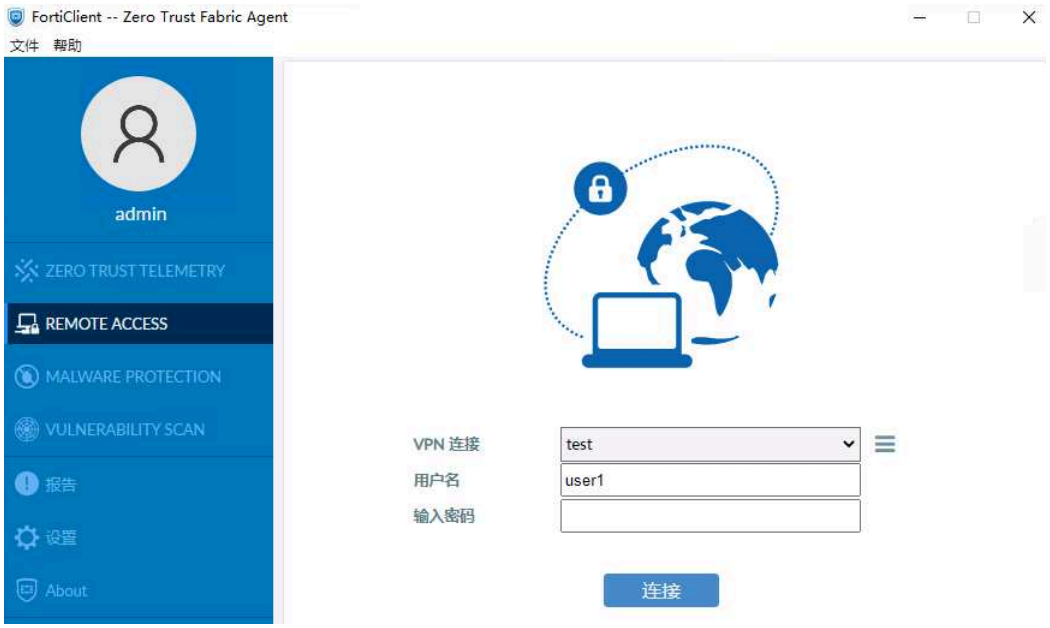


2. 选择SSL VPN，设置连接名，远程网关，SSLVPN端口以及用户名，然后点击保存。



3. 配置完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



业务测试

1. 在FortiClient中输入密码，并点击连接，在弹出的窗口中，点击“是”，信任SSLVPN证书



2. SSLVPN拨号成功，获取的地址是10.200.1.10

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看终端获取到的地址

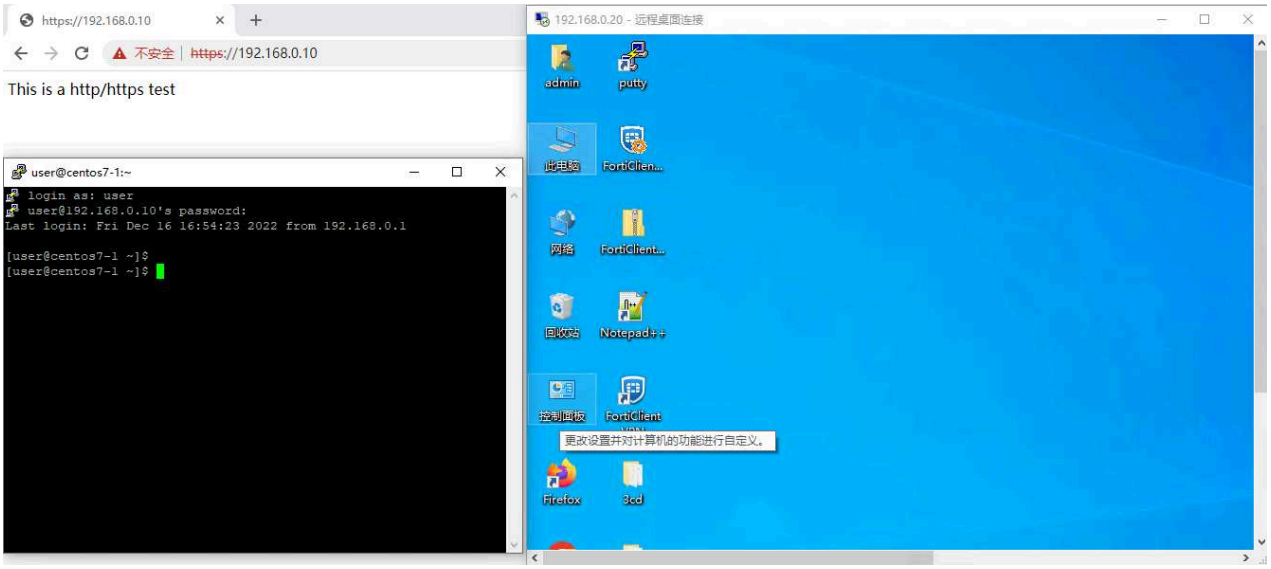
```
C:\Users\admin>ipconfig/all
以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Fortinet SSL VPN Virtual Ethernet Adapter
   物理地址. . . . . . . . . . . . . : 00-09-0F-AA-00-01
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::9124:e3aa:1ace:74d2%7(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.200.1.10(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.255
   默认网关. . . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 100665615
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-29-1C-CC-4A-00-0C-29-A2-90-E0
   DNS 服务器  . . . . . . . . . . . : 114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

查看终端获取到的路由

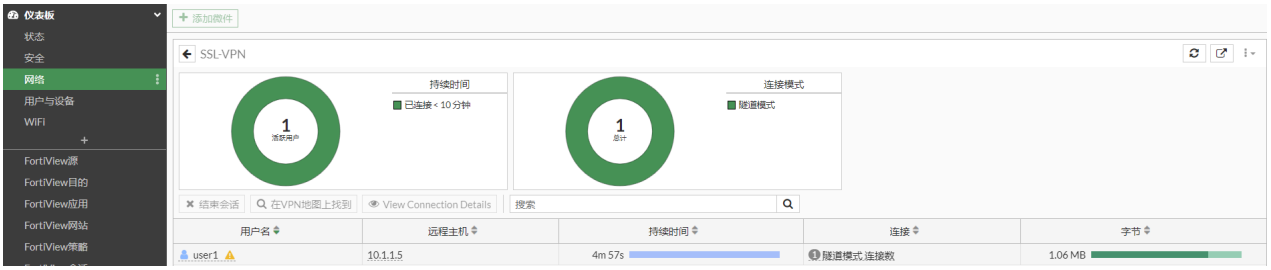
```
C:\Users\admin>route print
===========================================================================
接口列表
  6...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
  7...00 09 0f aa 00 01 ......Fortinet SSL VPN Virtual Ethernet Adapter
 10...00 0c 29 a2 90 e0 ......Intel(R) 82574L Gigabit Network Connection
  5...00 0c 29 a2 90 ea ......Intel(R) 82574L Gigabit Network Connection #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0         10.1.1.1         10.1.1.5    281
         10.1.1.0    255.255.255.0            在链路上          10.1.1.5    281
         10.1.1.5  255.255.255.255            在链路上          10.1.1.5    281
       10.1.1.255  255.255.255.255            在链路上          10.1.1.5    281
      10.200.1.10  255.255.255.255            在链路上       10.200.1.10    257
        100.1.1.2  255.255.255.255         10.1.1.1         10.1.1.5     25
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
      192.168.0.0    255.255.255.0      10.200.1.11      10.200.1.10      1
```

3. 访问内网主机HTTPS，SSH，RDP服务都正常

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. FortiGate查看SSLVPN连接




```
# get vpn ssl monitor
SSL-VPN Login Users:
 Index   User    Group   Auth Type      Timeout         Auth-Timeout    From     HTTP in/out    HTTPS in/out  Two-factor Auth
 0       user1   SSLVPN-Group   1(1)       276             28434        10.1.1.5       0/0            0/0           0

SSL-VPN sessions:
 Index   User    Group          Source IP      Duration        I/O Bytes       Tunnel/Dest IP
 0       user1   SSLVPN-Group   10.1.1.5         366           236265/838218     10.200.1.10
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSL VPN分配IP的方式

网络需求

如果在“SSL-VPN配置”（`config vpn ssl settings`）中与“SSL-VPN门户”（`config vpn ssl web portal`）中同时引用了两个不同的地址池，那么对应Portal用户的FortiClient拨号后获取的IP地址应该是“SSL-VPN配置”还是“SSL-VPN门户”引用的地址池中的呢?

SSL VPN Tunnel模式分配IP的模式有两种：

- 默认配置下，FortiClient拨号后获取的IP为“SSL-VPN门户”引用的地址池中的IP。且分配IP的方式为`first-available`，即永远使用用户对应Portal引用的地址池中可用的最小地址来分配IP。
- 如果想要使用轮询（`round-robin`）方式，当已经从地址池分配过一个IP后，即使该IP已经释放，也使用该IP后的可用IP进行分配（类似于PPPoE的IP分配方式）。使用此种方式时，IP将从“SSL-VPN配置”（`config vpn ssl settings`）的地址池中分配。

配置方法

```bash
FortiGate # config vpn ssl settings
FortiGate (settings) # set tunnel-addr-assigned-method ?
first-available    Assign the first available address from the pools.    //默认最小可用优先方式，使用config vpn ssl web portal中引用的地址池//
round-robin        Assign the available address from the pool with a round robin fashion.    //轮询方式，使用config vpn ssl settings中引用的地址池//
```

配置步骤

1. `config vpn ssl settings`配置，引用地址池为`sslvpn_pool`，用户组`VPN`对应的Portal为`full-access`，使用默认选项`first-available`作为IP分配方式（相关用户、策略配置略）。

```bash
config vpn ssl settings
    set servercert "Fortinet_Factory"
    set tunnel-ip-pools "sslvpn_pool"
    set source-interface "wan1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "web-access"
    config authentication-rule
        edit 2
            set groups "VPN"
            set portal "full-access"
        next
    end
    set tunnel-addr-assigned-method first-available    //默认配置//
end

config firewall address
    edit "sslvpn_pool"
        set type iprange
        set start-ip 3.3.3.1
        set end-ip 3.3.3.100
    next
end
```

2. `config vpn ssl web portal`配置，引用地址池为`SSLVPN_TUNNEL_ADDR1`。

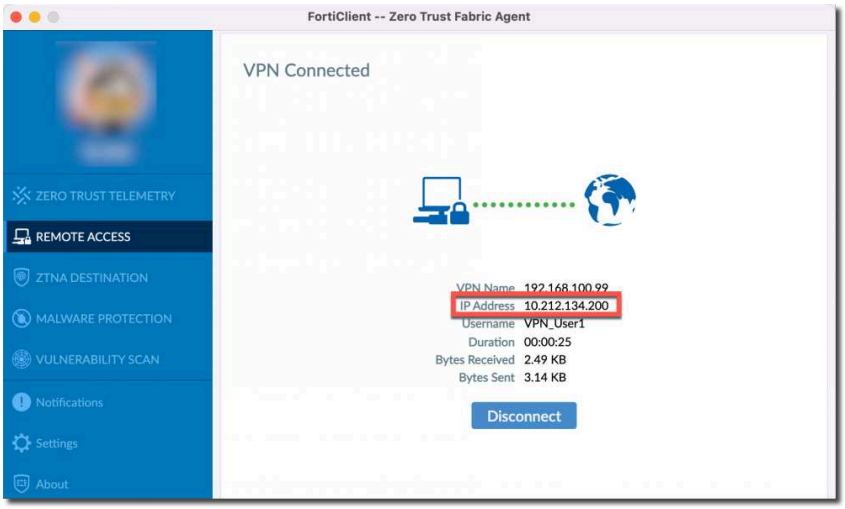
```bash
config vpn ssl web portal
    edit "full-access"
        set tunnel-mode enable
        set ip-pools "SSLVPN_TUNNEL_ADDR1"
    next
end

config firewall address
    edit "SSLVPN_TUNNEL_ADDR1"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

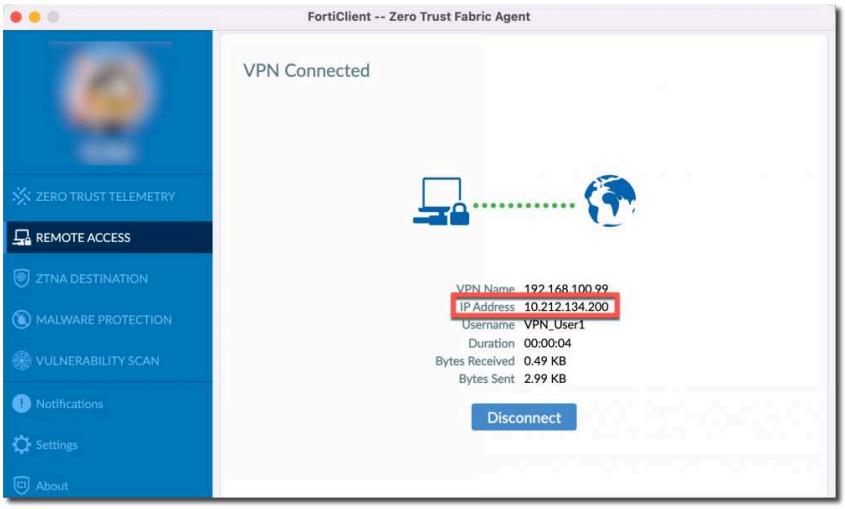
```
        set type iprange
        set start-ip 10.212.134.200
        set end-ip 10.212.134.210
    next
end
```

结果验证

1. FortiClient使用用户组VPN中的用户连接FortiGate的SSL VPN，连接成功后，获取的IP为`config vpn ssl web portal`引用的地址池`SSLVPN_TUNNEL_ADDR1`中的IP 10.212.134.200。



2. 断开FortiClient的SSL VPN连接，再次连接FortiGate的SSL VPN，会获取到地址池`SSLVPN_TUNNEL_ADDR1`最小可用的地址10.212.134.200，与步骤1中获取的地址一样（该地址释放后没有其他客户端获取）。

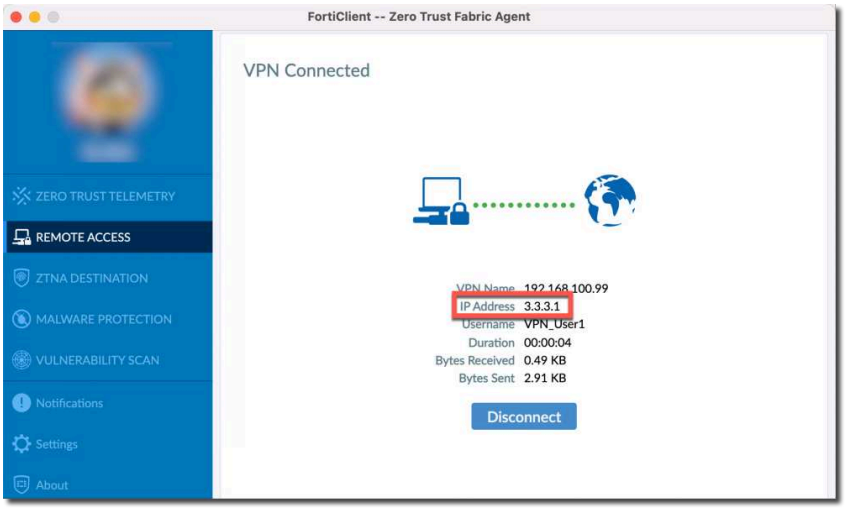


3. 在`config vpn ssl settings`中修改IP分配方式为`round-robin`。

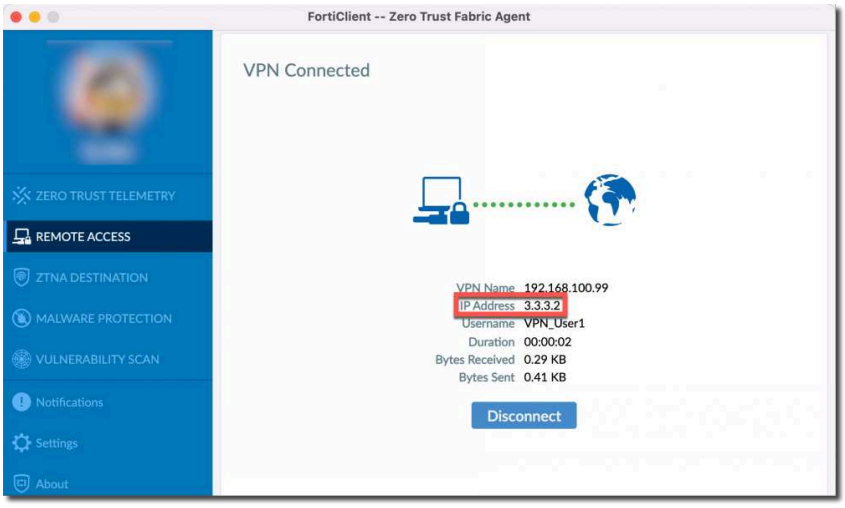
```bash
config vpn ssl settings
    set tunnel-addr-assigned-method round-robin
end
```

4. 再次使用FortiClient连接FortiGate的SSL VPN，获取的IP为`config vpn ssl settings`引用的地址池`sslvpn_pool`中的IP 3.3.3.1。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 断开FortiClient的SSL VPN连接，再次连接FortiGate的SSL VPN，会获取到地址池`sslvpn_pool`的下一个可用IP 3.3.3.2（即使上一个IP 3.3.3.1已经释放）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSL VPN WEB代理模式配置

重要

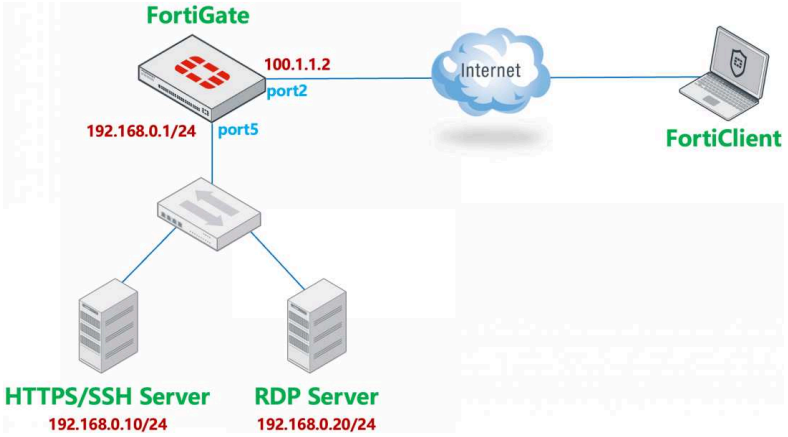
由于部分用户Web服务器的网页代码不够规范，可能与SSL VPN Web代理模式不兼容，导致访问异常，强烈建议使用SSL VPN隧道模式。

SSL VPN Web代理模式目前不支持HTML5格式。

网络需求

在外移动办公的工作人员需要通过SSL VPN WEB模式拨入到公司内网来对内网主机进行访问。

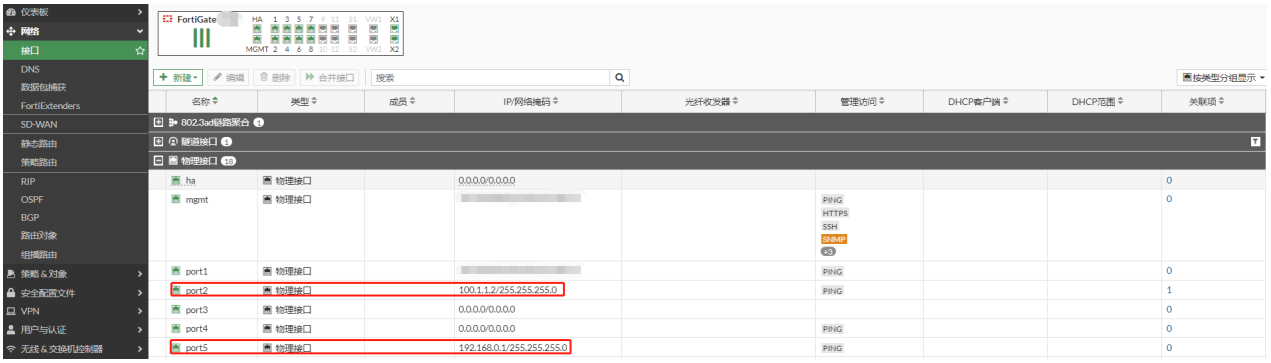
网络拓扑

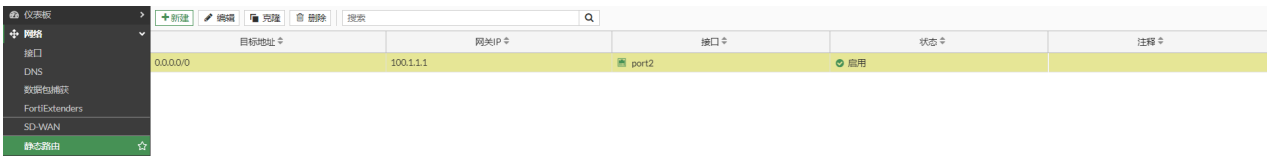


配置步骤

1. **基本配置**

   配置接口IP和路由

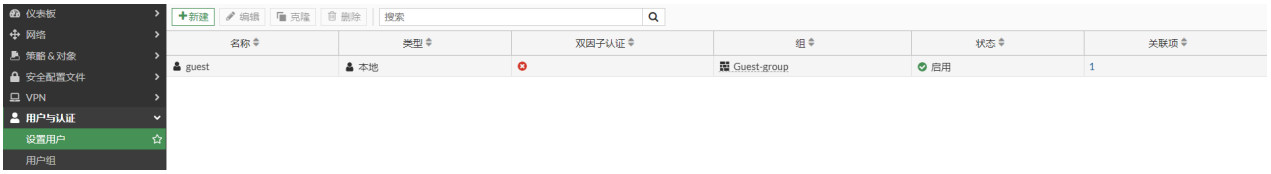




2. **创建用户**

   选择“用户与认证”-->“设置用户”，点击“新建”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



选择“本地用户”，点击“下一步”。



输入用户名和密码，点击“下一步”。

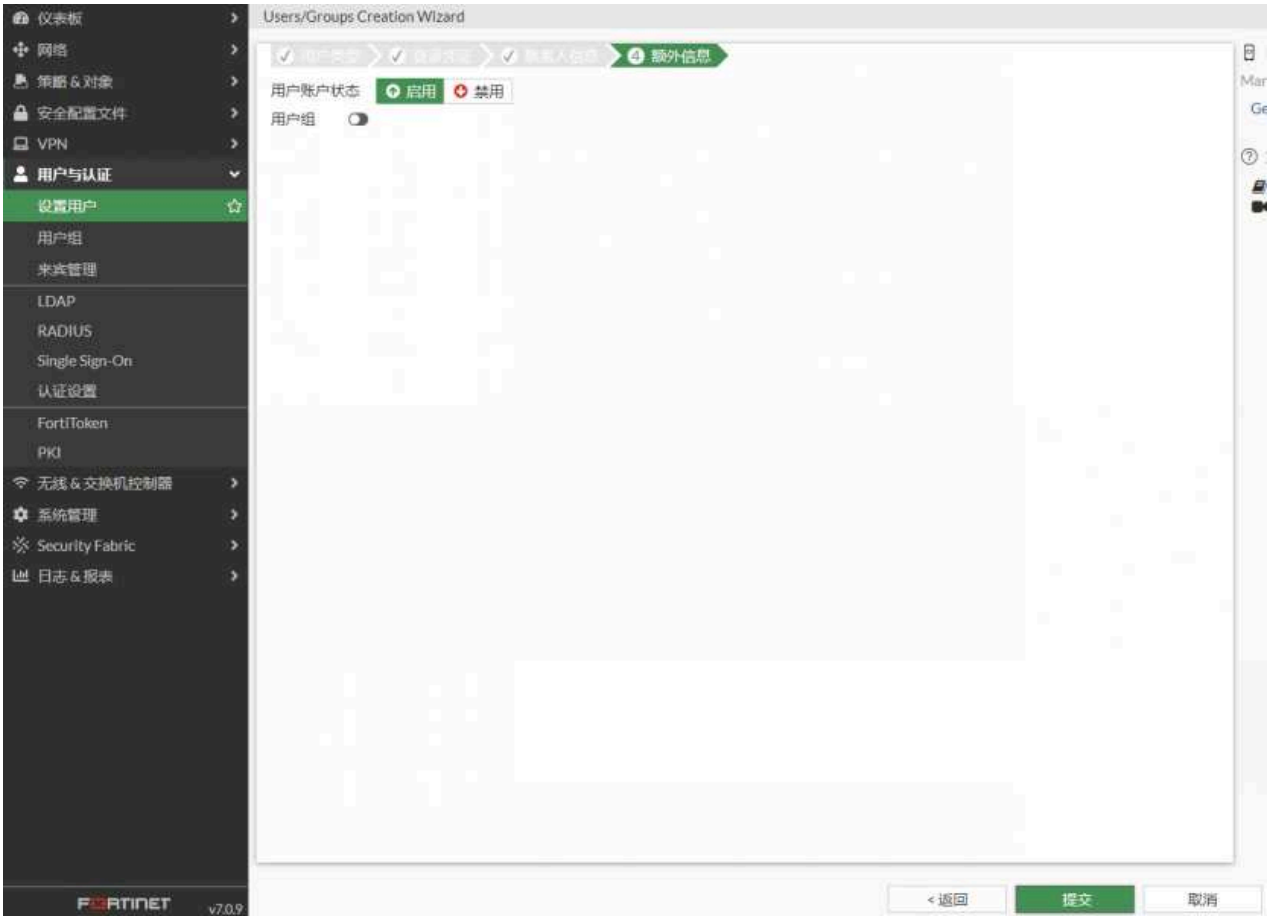


可根据需求选择启用。这里不启用，点击“下一步”。

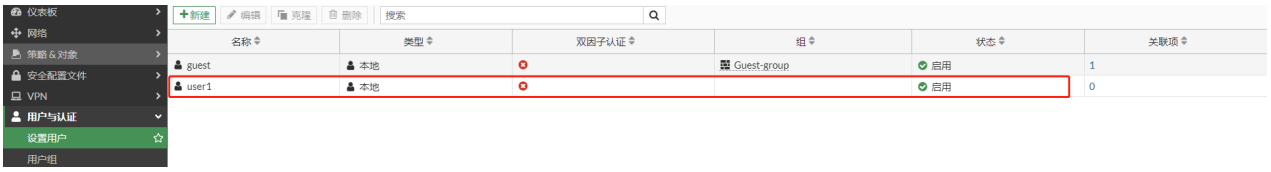


点击“提交”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

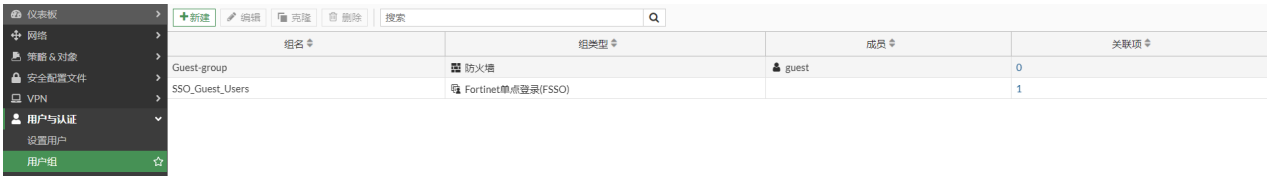


完成用户创建。

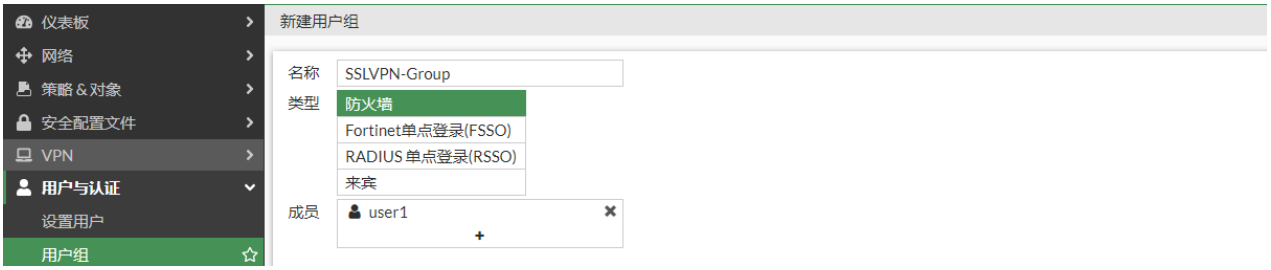


3. 创建用户组

选择“用户与认证”-->“用户组”，点击“新建”。

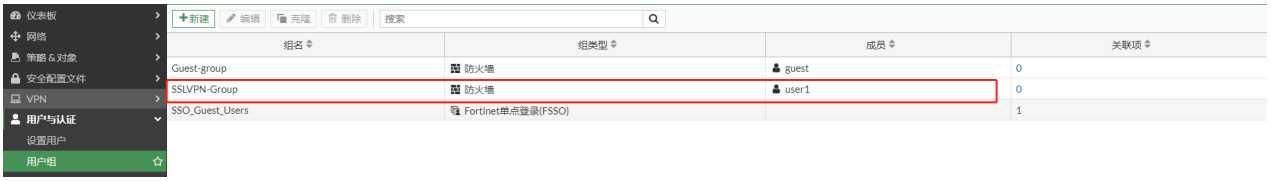


输入名称，即组名，并将用户加入用户组，点击“确认”。



完成用户组创建。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

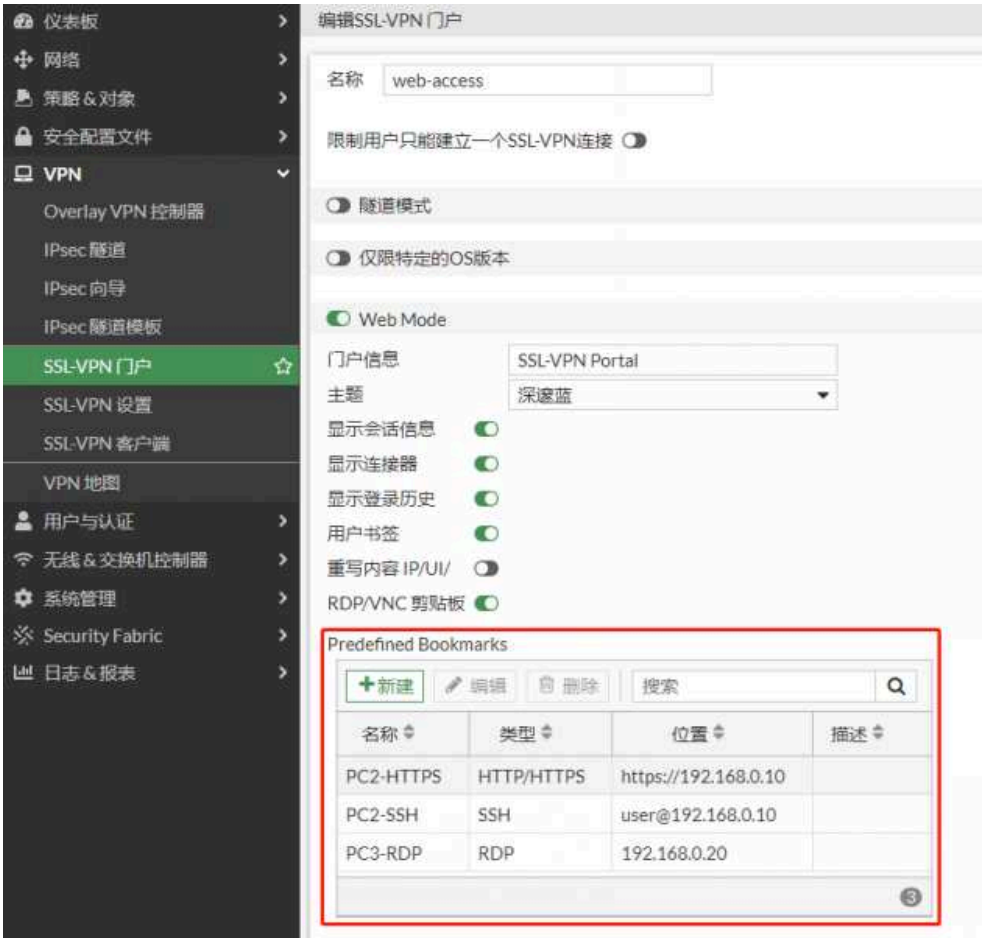


4. 配置SSL-VPN门户

系统默认创建3个SSLVPN门户：full-access:开启了隧道模式和web代理模式；tunnel-access只开启了隧道模式；web-access：只开启web代理模式。可以根据实际需求进行修改，也可以新建新的SSL-VPN门户。



这里使用web-access门户，新建HTTPS，SSH，RPD 3个资源供客户端拨号后访问。



PC2-HTTPS资源配置：

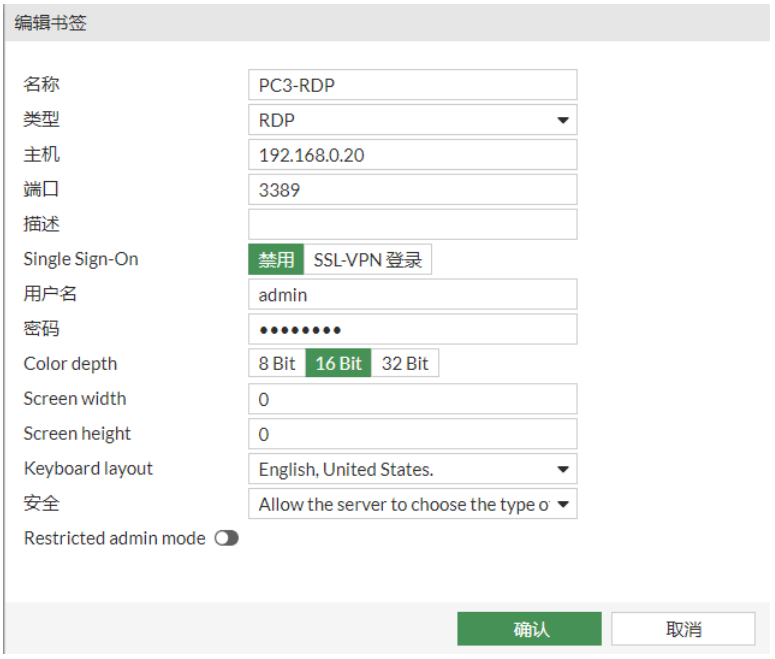
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



PC2-SSH资源配置：



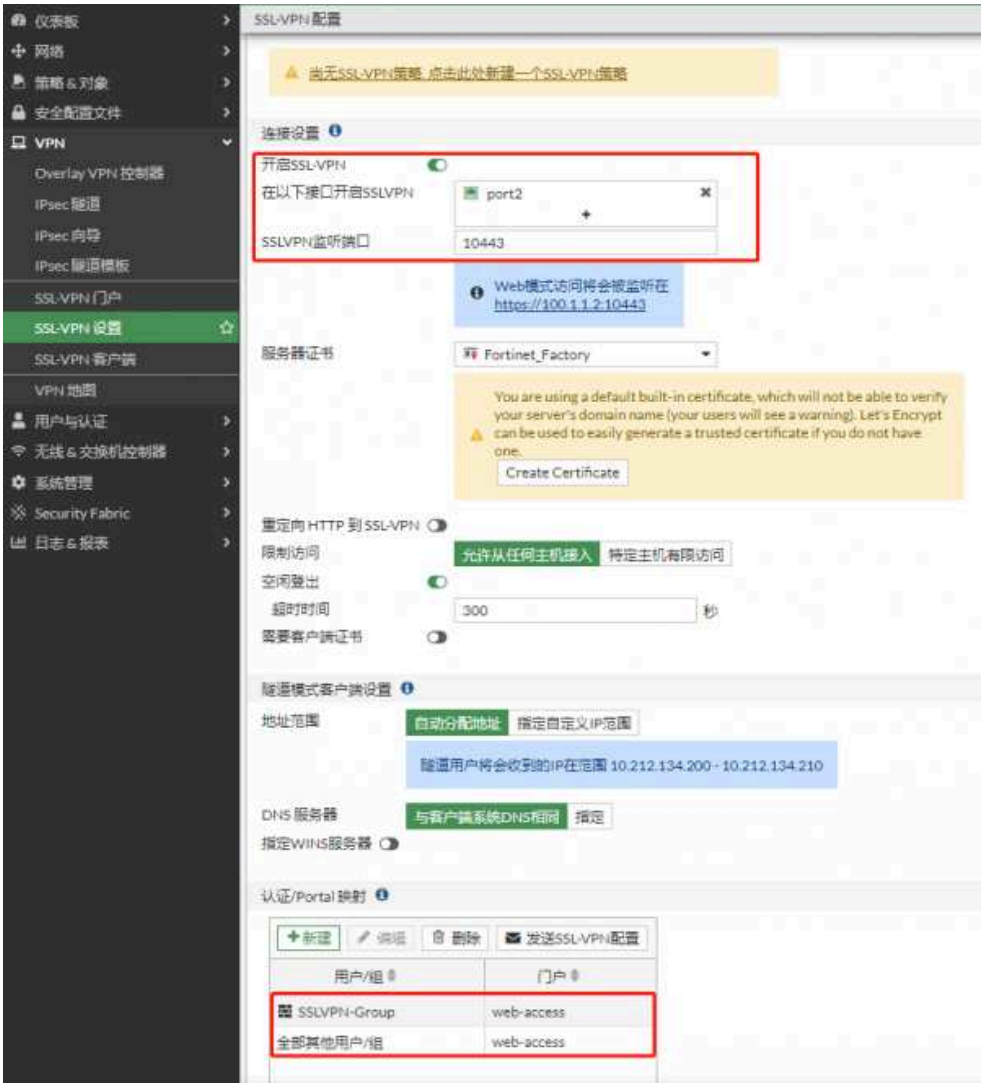
PC3-RDP资源配置：



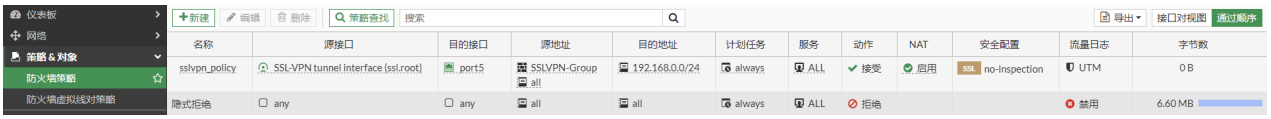
5. **配置SSLVPN**

设置提供SSLVPN服务的接口和端口，将SSLVPN-Group用户组和web-access门户关联，全部其他用户/组也要关联一个门户，用于没有配置关联的用户/用户组访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



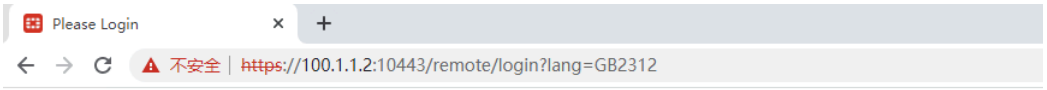
6. 创建策略



业务测试

1. PC1使用chrome访问SSLVPN，并输入用户名和密码。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



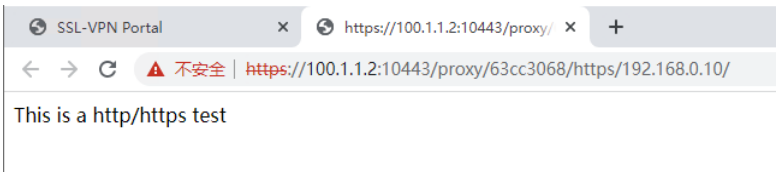


2. 登录成功后，可以看到之前创建好的3个资源。



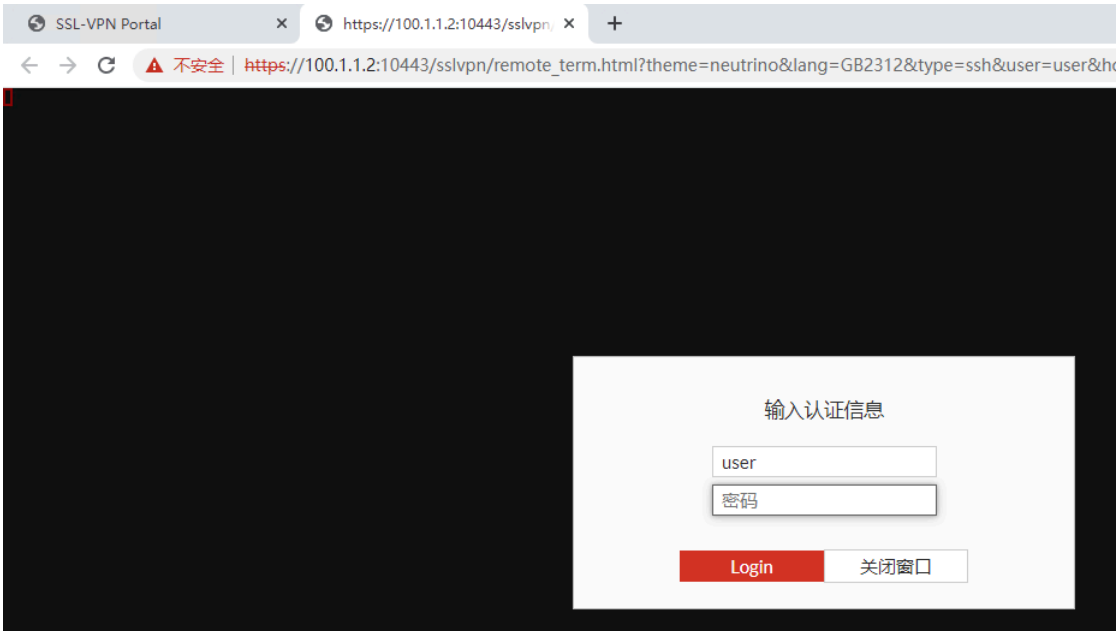
3. 业务访问

点击PC2-HTTPS，访问成功。

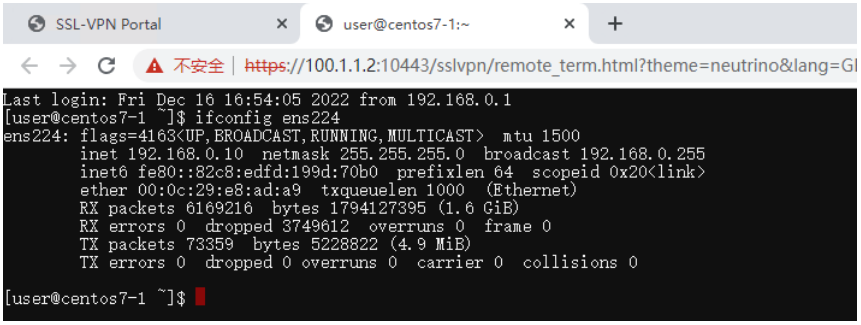


点击PC2-SSH，访问成功。

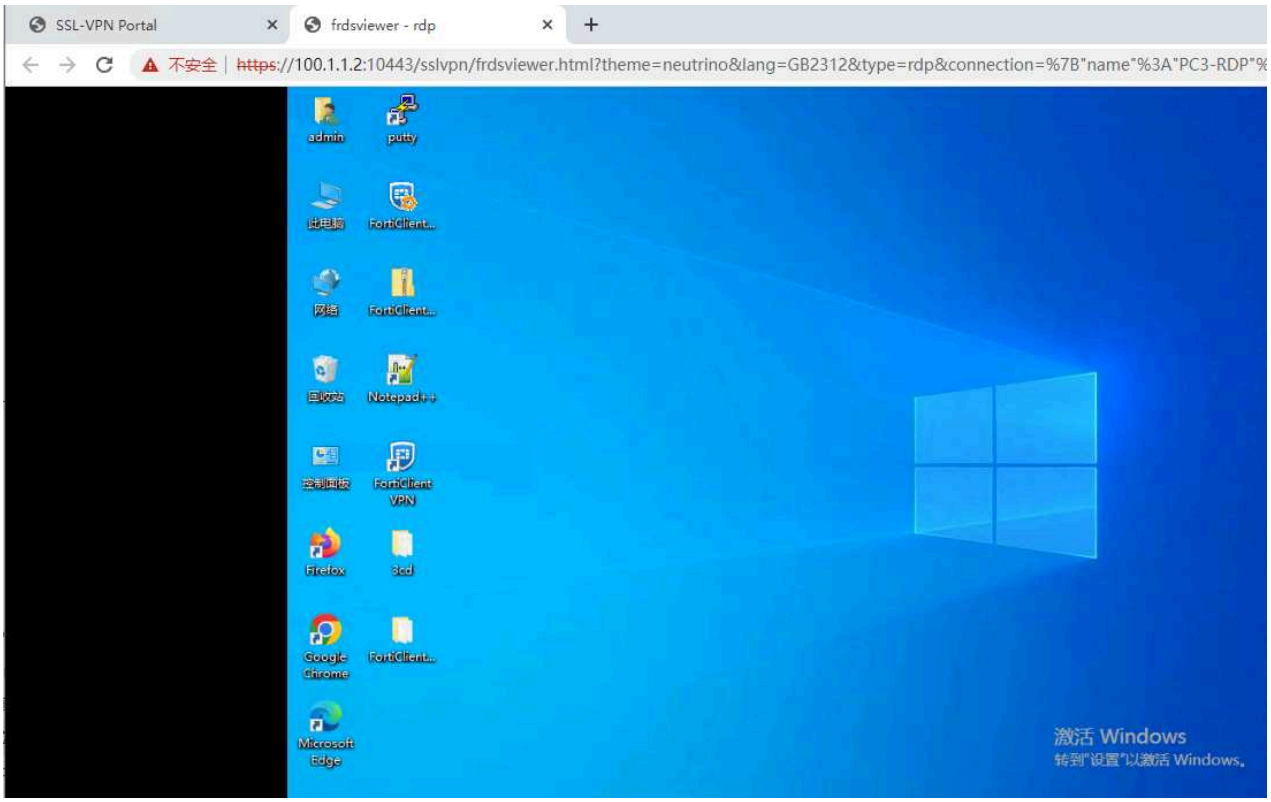
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



输入PC2 SSH的用户的密码，登录成功。

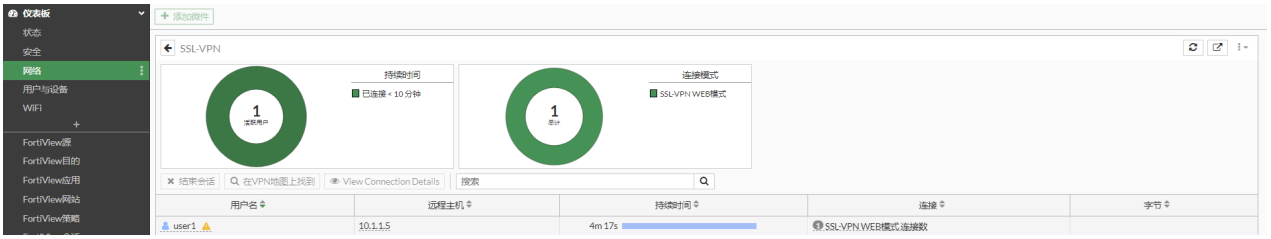


点击PC3-RDP，访问成功。



4. FortiGate查看SSLVPN用户状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
 # get vpn ssl monitor
SSL-VPN Login Users:
 Index   User    Group   Auth Type      Timeout         Auth-Timeout    From     HTTP in/out    HTTPS in/out  Two-
factor Auth
 0       user1   SSLVPN-Group   1(1)      289               28788    10.1.1.5       0/0              0/0
0

SSL-VPN sessions:
 Index   User    Group   Source IP      Duration        I/O Bytes       Tunnel/Dest IP
```

Web代理模式自定义代理IP

默认情况下，使用Web代理模式的SSL VPN时，客户端访问内部服务器，是通过FortiGate上流量的出接口IP作为代理IP访问内部服务器的，如果想要修改这个IP为其他IP地址，可以使用如下方法实现。

1. 配置IPPool，内容为自定义的代理IP地址，例如默认出接口IP为172.16.1.254作为SSL VPN Web模式的代理IP，但用户想使用172.16.1.1作为代理IP，则配置该IP为地址池的范围。

```
config firewall ippool
    edit "SSL-VPN-IP-Pool"
        set type overload
        set startip 172.16.1.1
        set endip 172.16.1.1
    next
end
```

2. 在SSL VPN的访问策略（从SSL VPN接口到内网口方向）中，开启SNAT，并引用上述地址池。

```
config firewall policy
    edit 1
        set name "SSL-VPN Web Mode"
        set srcintf "ssl.root"
        set dstintf "LAN"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set ippool enable
        set poolname "SSL-VPN-IP-Pool"
    end
```

3. 在SSL VPN配置中开启Web模式的SNAT。

```
config vpn ssl settings
    set web-mode-snat enable
end
```

4. **此步很重要：**在SSL VPN绑定的接口上，开启第二地址，并配置第二地址为上述地址池中的IP（32位）。

```
config system interface
    edit "wan1"
        set ip 172.16.1.254 255.255.255.0
        set secondary-IP enable
        set interface "port2"
        config secondaryip
            edit 1

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set ip 172.16.1.1 255.255.255.255
            next
        end
    next
end
```

5. 随后，SSL VPN客户端通过Web模式访问内网Web服务器，将通过地址池中配置的IP作为代理源IP访问。

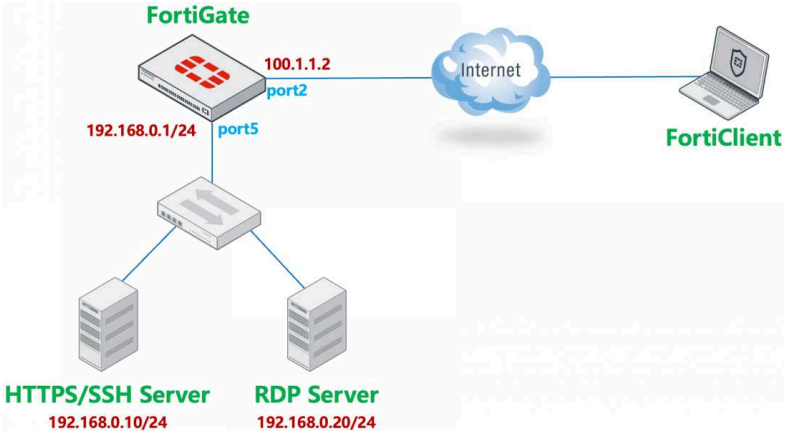
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSL VPN数字证书认证

网络需求

在外移动办公的工作人员需要通过SSL VPN 并且使用数字证书认证的方式，拨入到公司内网来对内网主机进行访问。

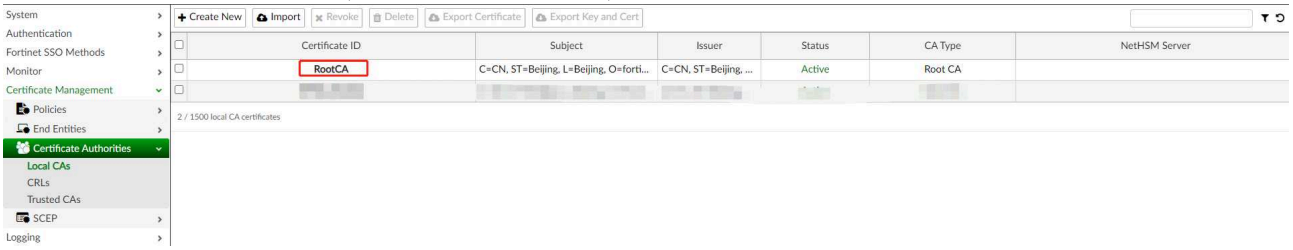
网络拓扑



配置步骤

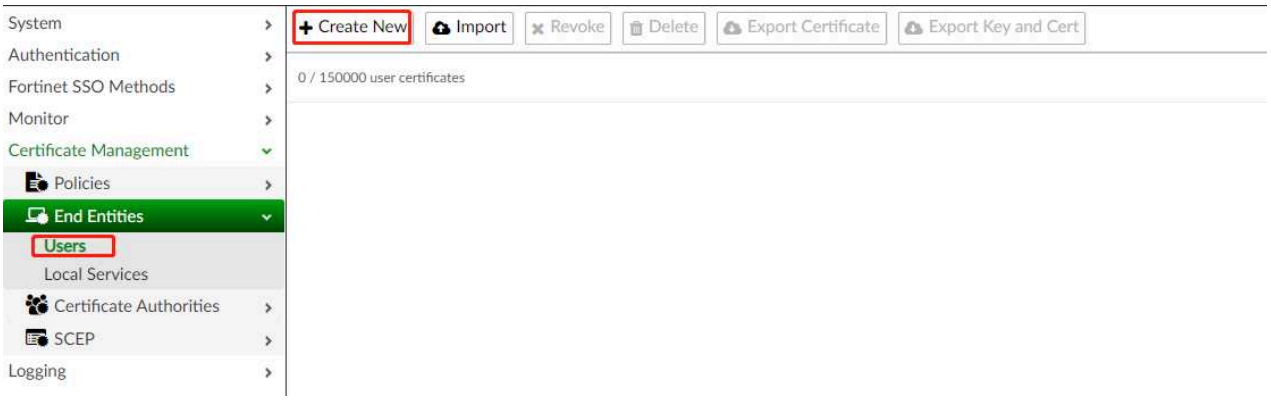
使用FortiAuthenticator为FGT-BJ和终端颁发证书

FortiAuthenticator可以做为证书服务器，RootCA是已创建好的根证书，这里使用RootCA为这两台FortiGate签发证书。（也可以使用其他证书服务器）

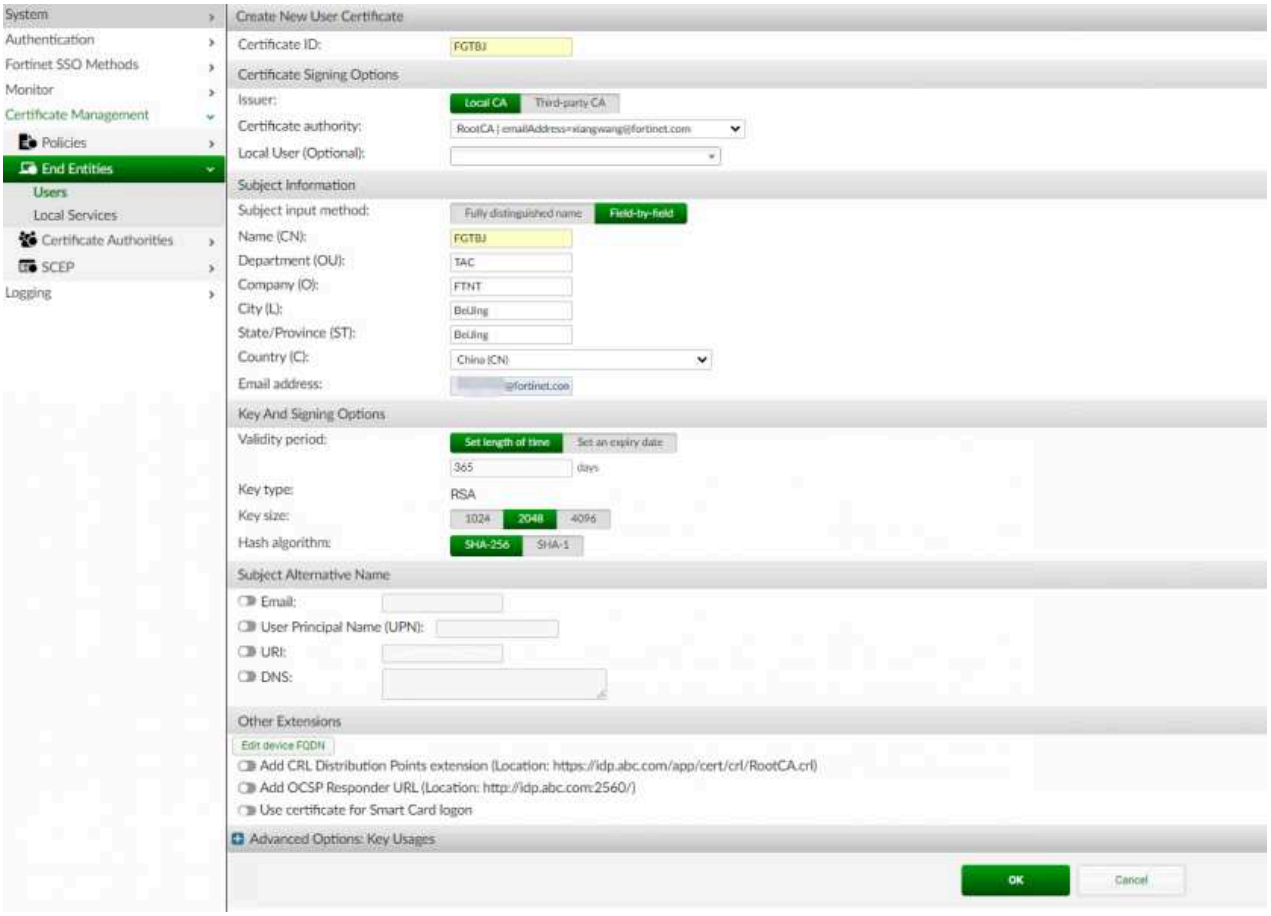


1. **为FGT-BJ颁发证书**

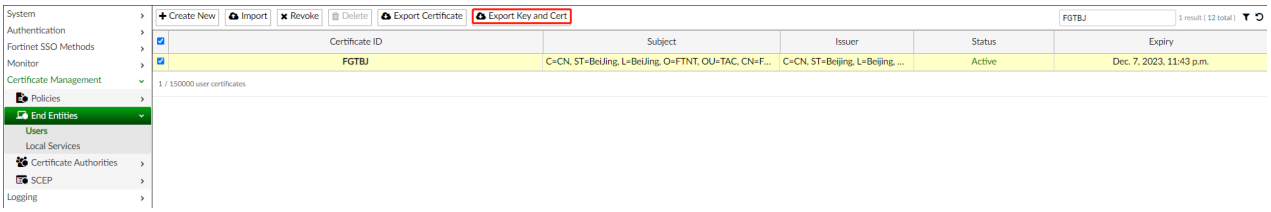
   为FGT-BJ创建证书。选择“End Entities”-->"User"，点击“Create New”，输入证书相关信息，并点击完成。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击“Export Key and Cert”导出FGTBJ证书的私钥和公钥。



输入一个密码保护私钥



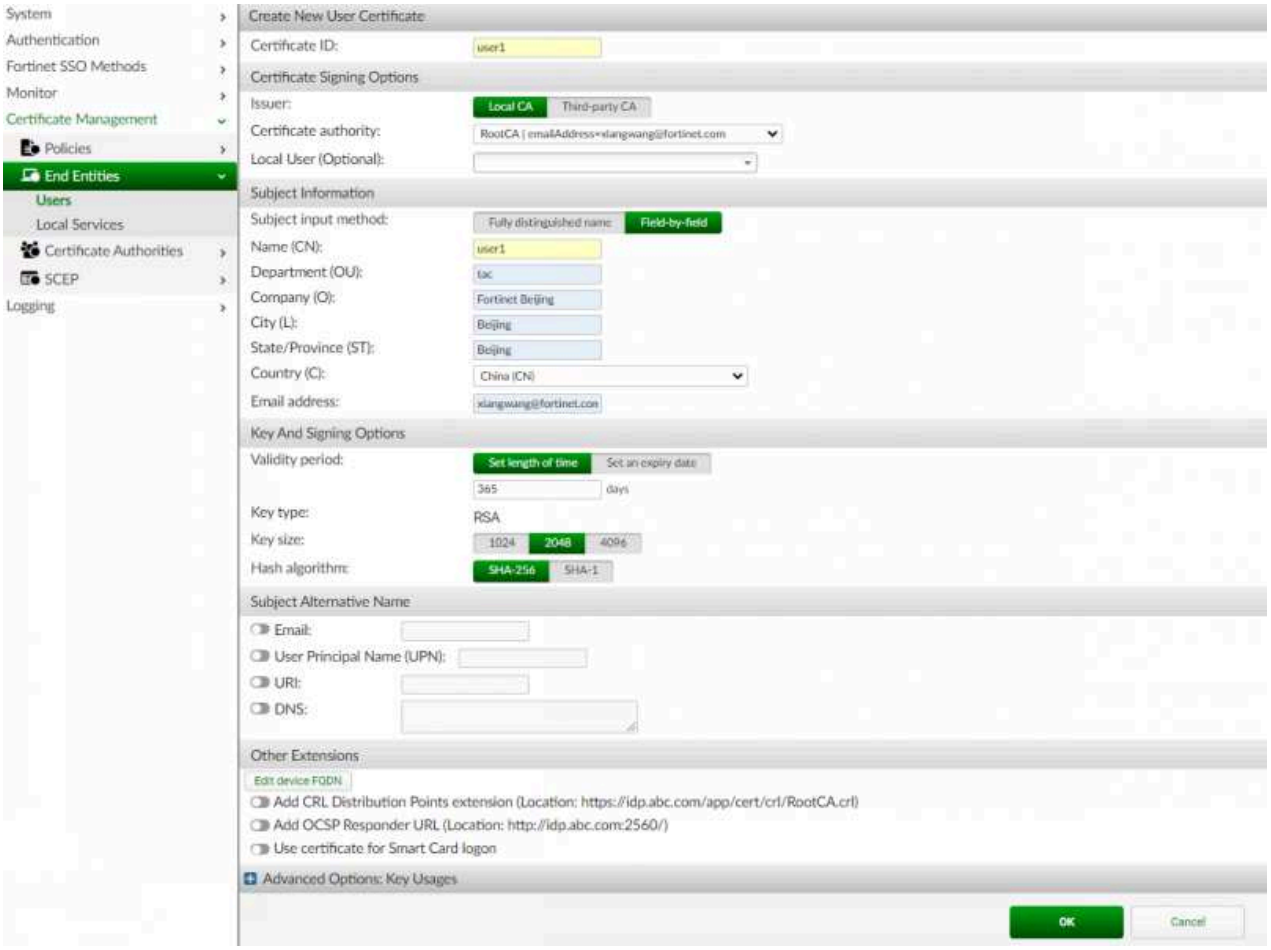
下载证书

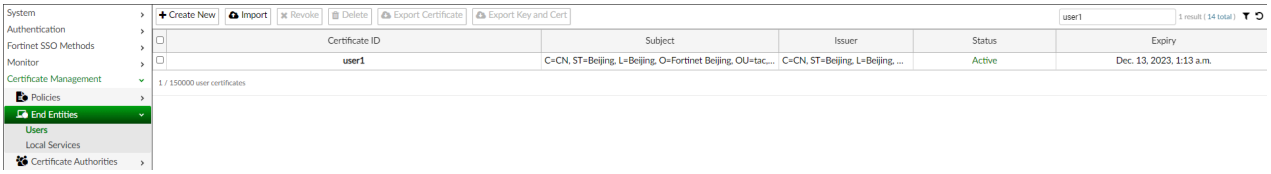
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **为终端颁发证书**

为终端颁发证书和上述步骤是一样的。





FortiGate导入证书

将根证书RootCA.crt和证书FGTBJ.p12导入到FGT_BJ。

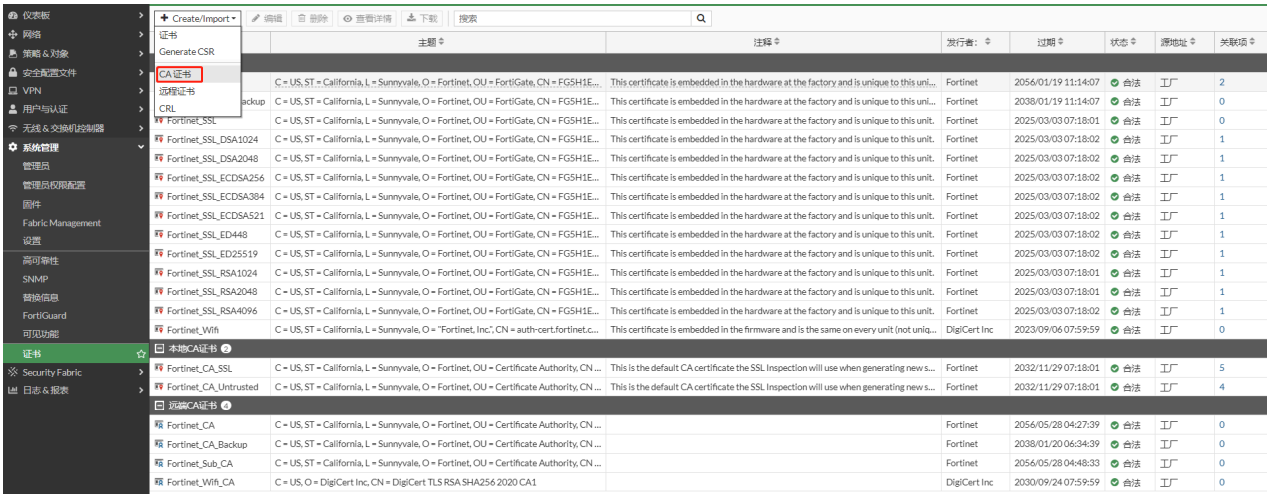
在数字证书认证中，通信双方使用CA证书进行数字证书合法性验证，双方各有自己的公钥（网络上传输）和私钥（本地存储）。发送方对报文进行Hash计算，并用自己的私钥对报文计算结果进行加密，生成数字签名。接收方使用发送方的公钥对数字签名进行解密，并对报文进行Hash计算，判断计算结果与解密后的结果是否相同。如果相同，则认证通过；否则认证失败。

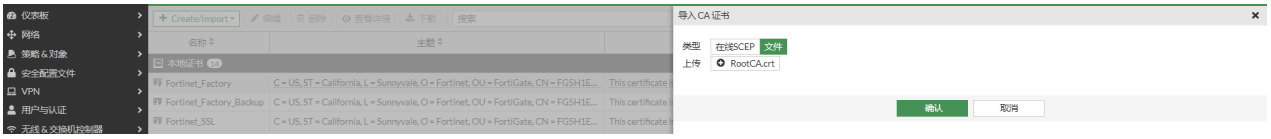
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



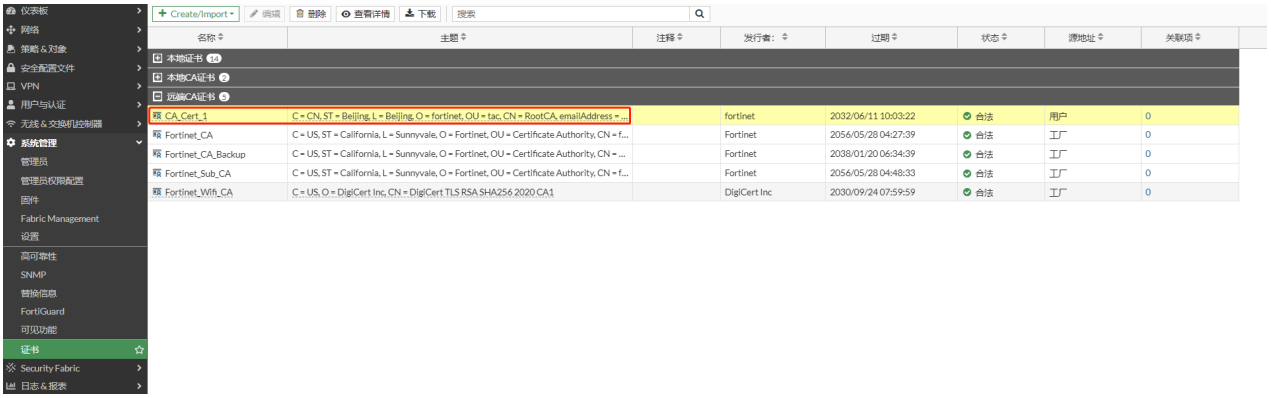
1. 导入CA证书

选择“系统管理”-->“证书”，点击“Create/Import”，选择CA证书。





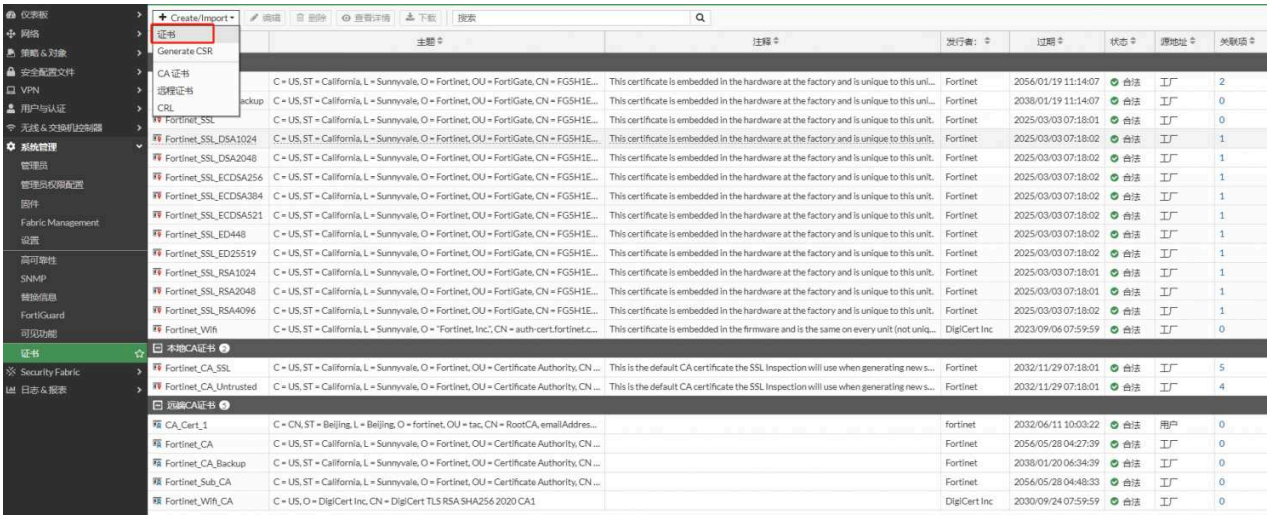
查看导入的CA证书



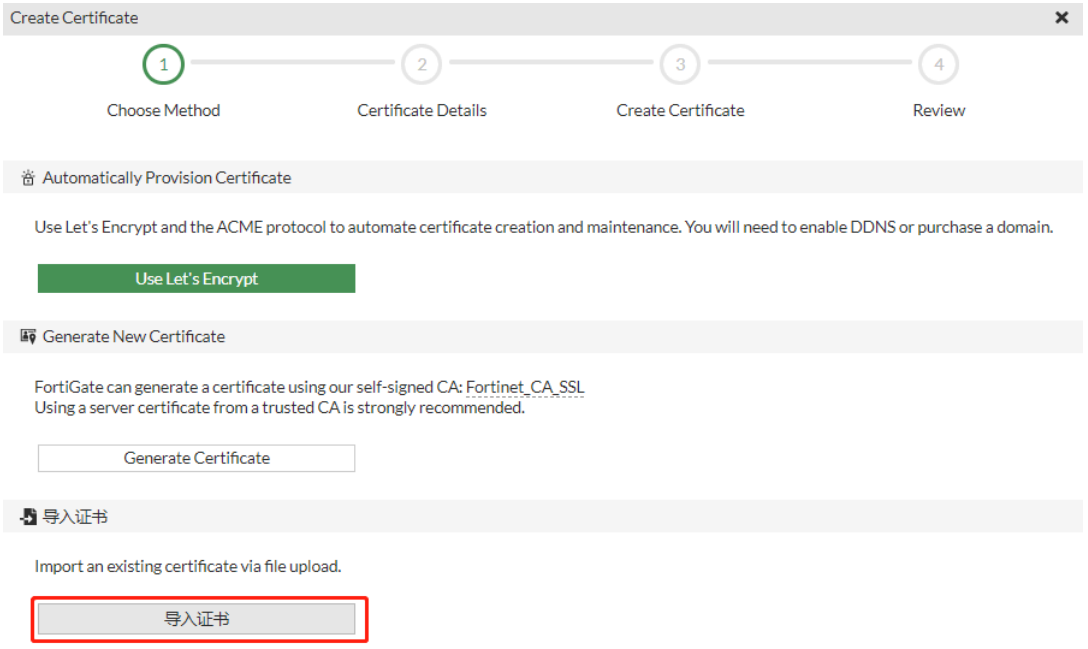
2. 导入本地证书

选择“系统管理”-->“证书”，点击“Create/Import”，选择“证书”。

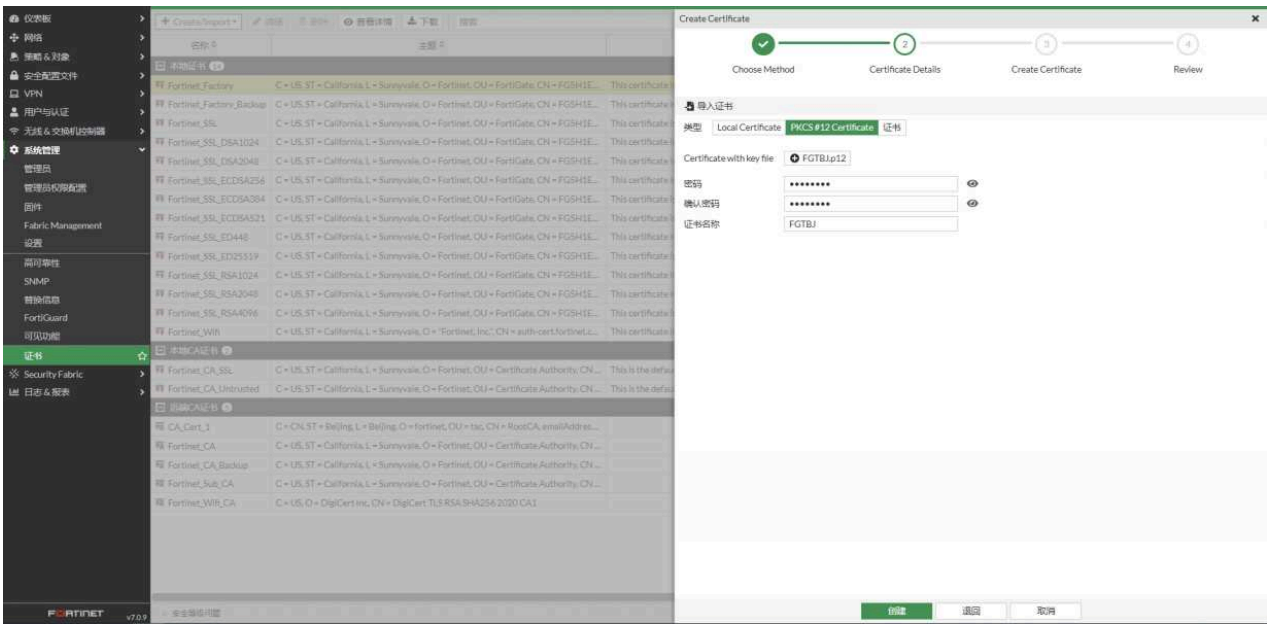
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击导入证书

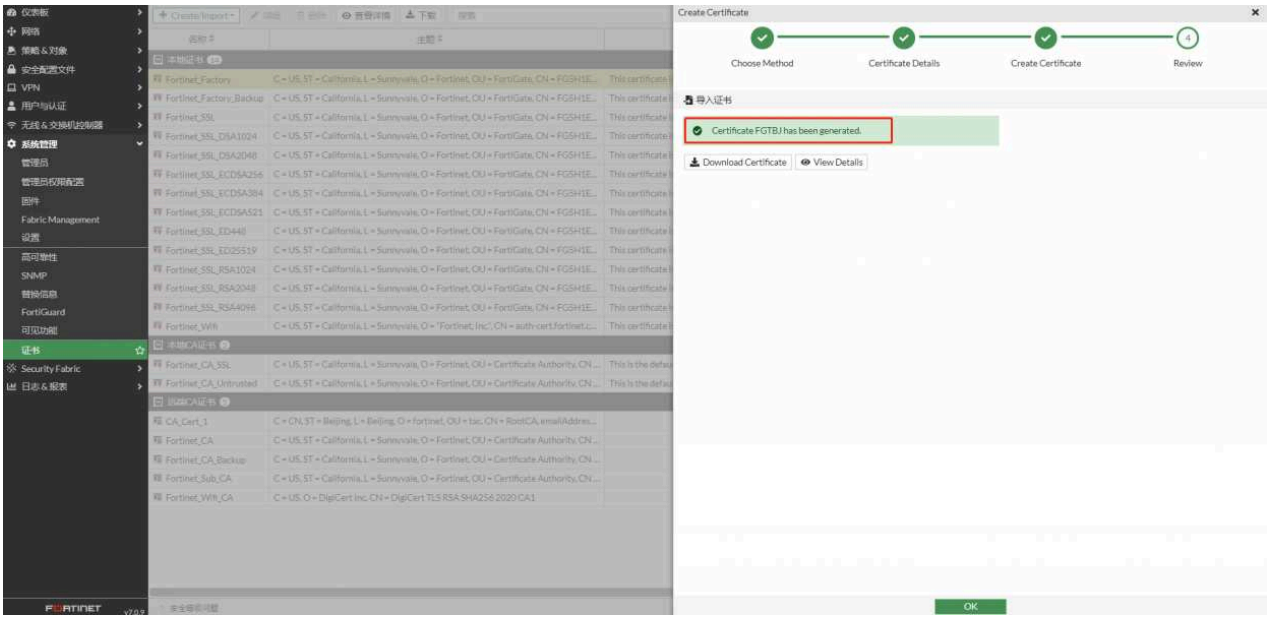


输入证书的密码，点击“创建”

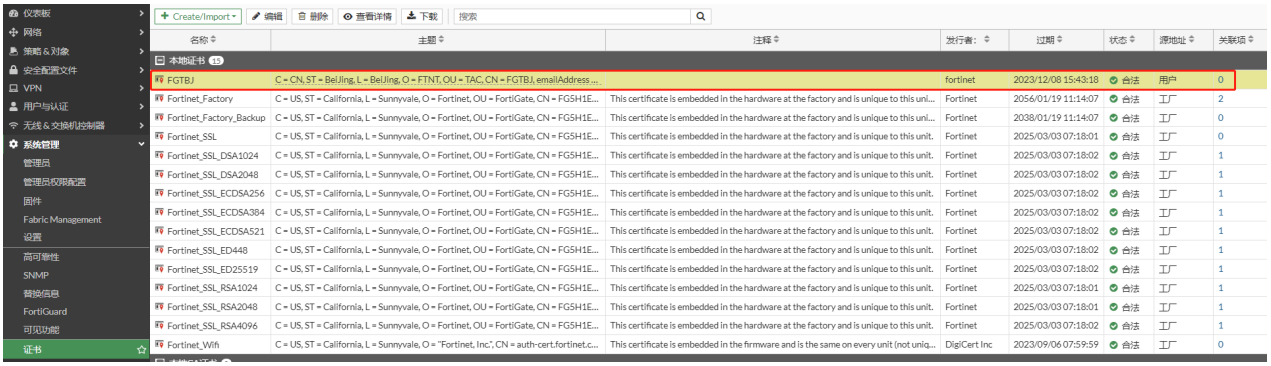


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

提示证书已成功导入



查看导入的本地证书



终端导入证书

将根证书RootCA.crt和证书user1.p12导入到终端。



1. 导入根证书RootCA.crt

双击RootCA.crt，点击“安装证书”。

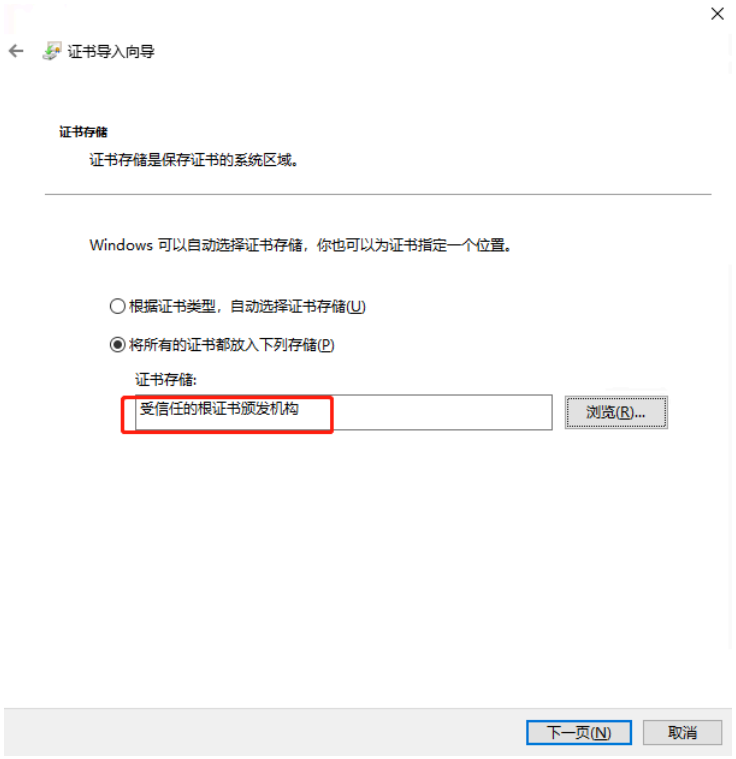
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

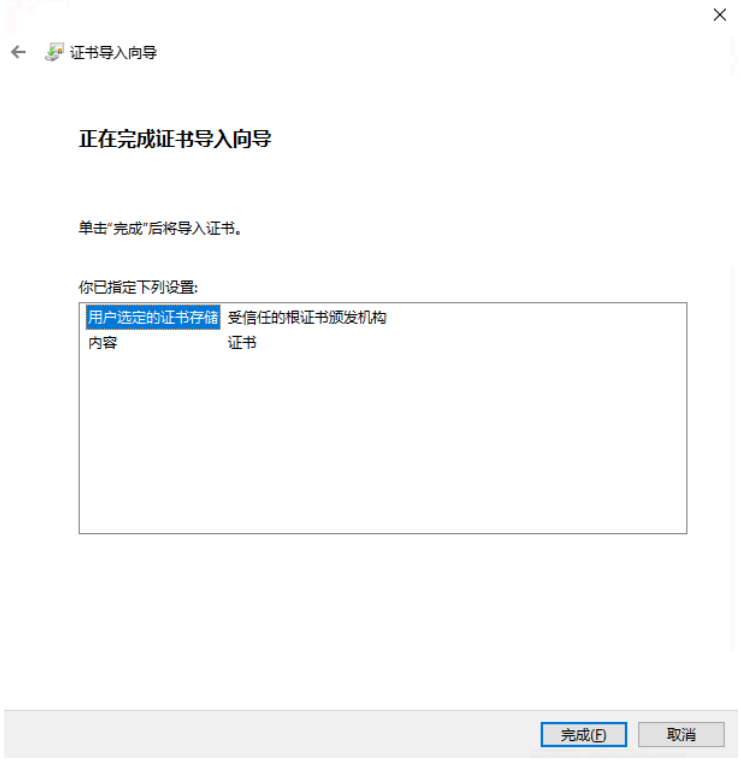




证书存入“受信任的根证书颁发机构”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

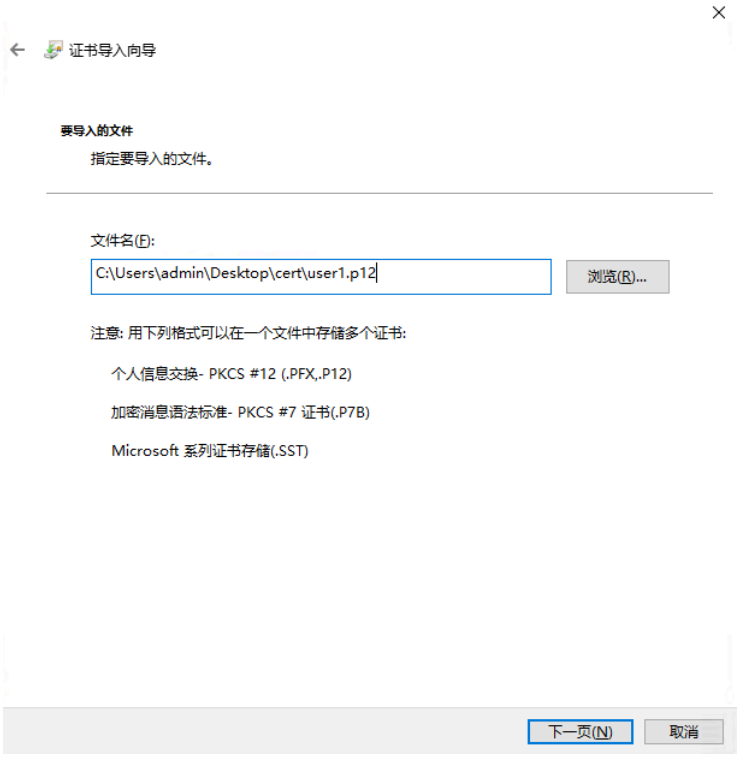




2. 导入个人证书user1.p12

   双击user1.p12，然后安装证书

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

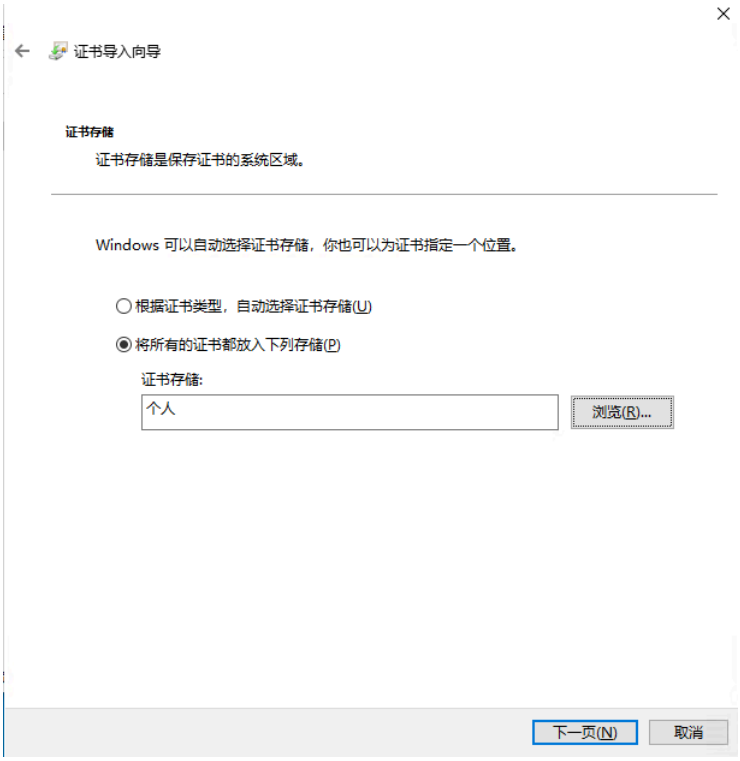


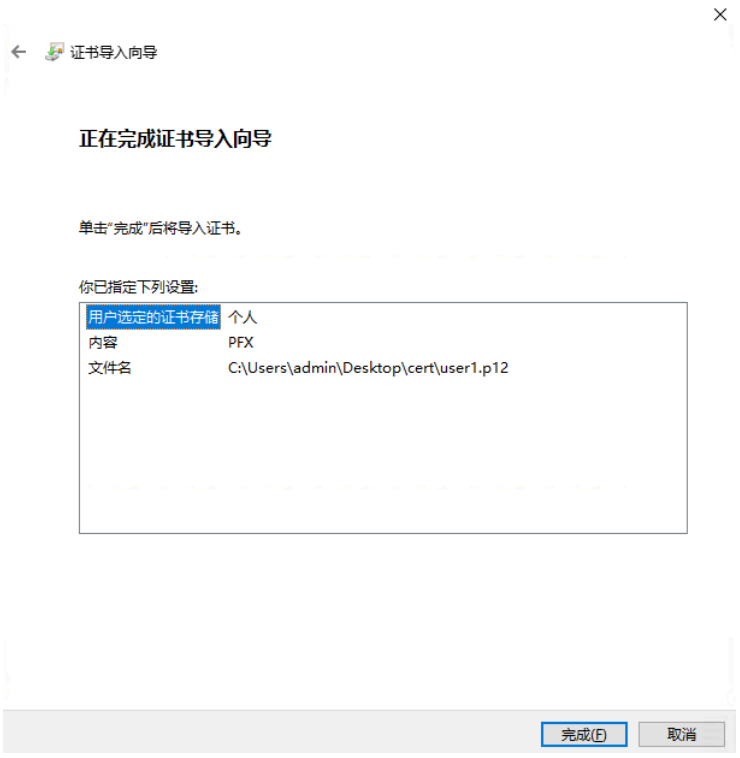
输入证书的密码



证书存入“个人”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



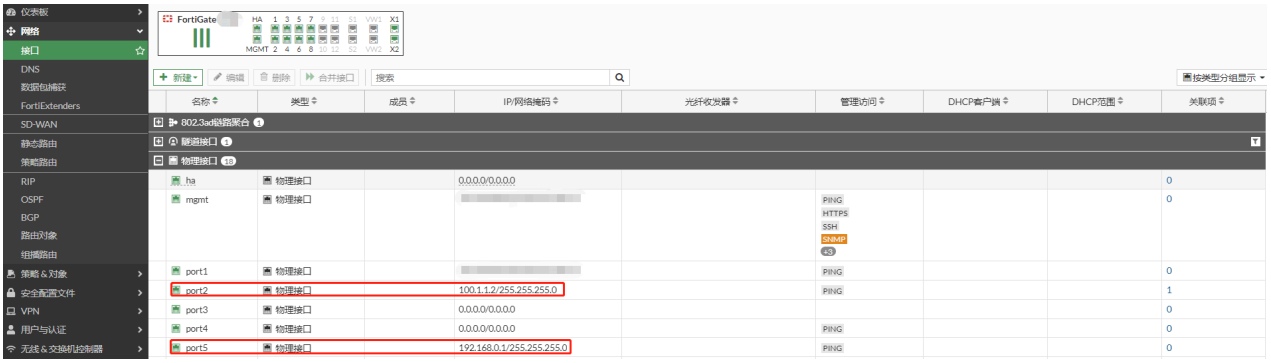


配置SSL VPN

1. **基本配置**

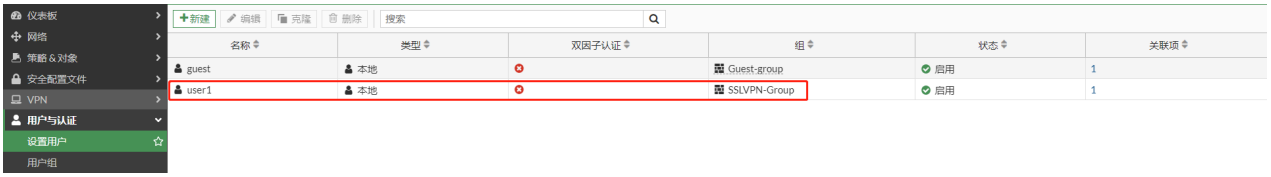
   配置接口IP和路由

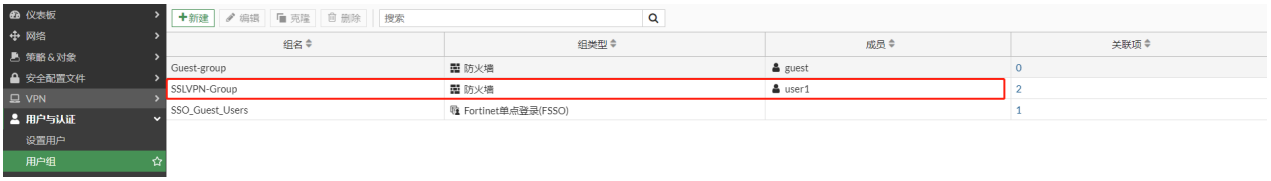
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 创建用户，并将用户加入到用户组。

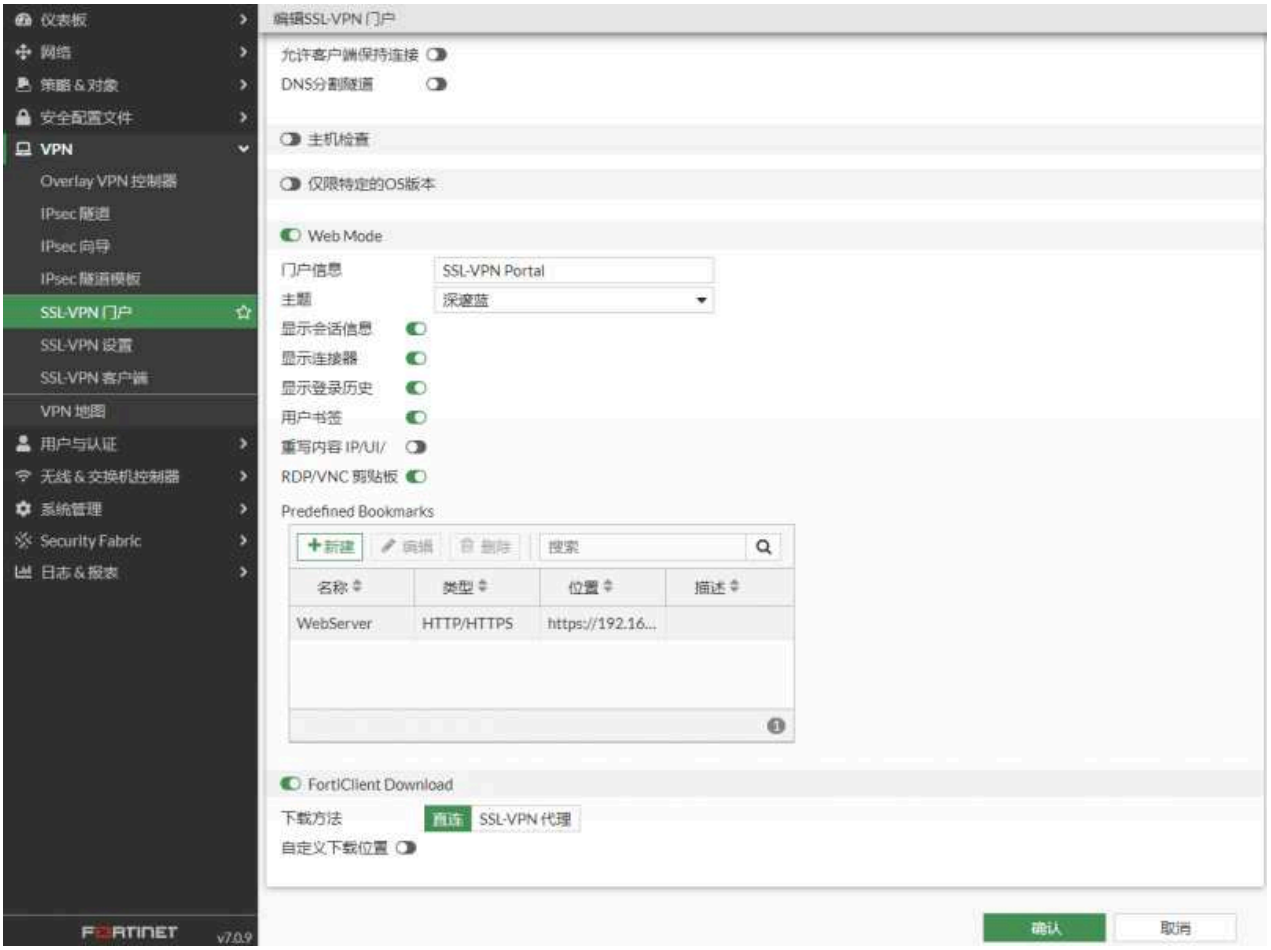




3. 配置SSL-VPN门户



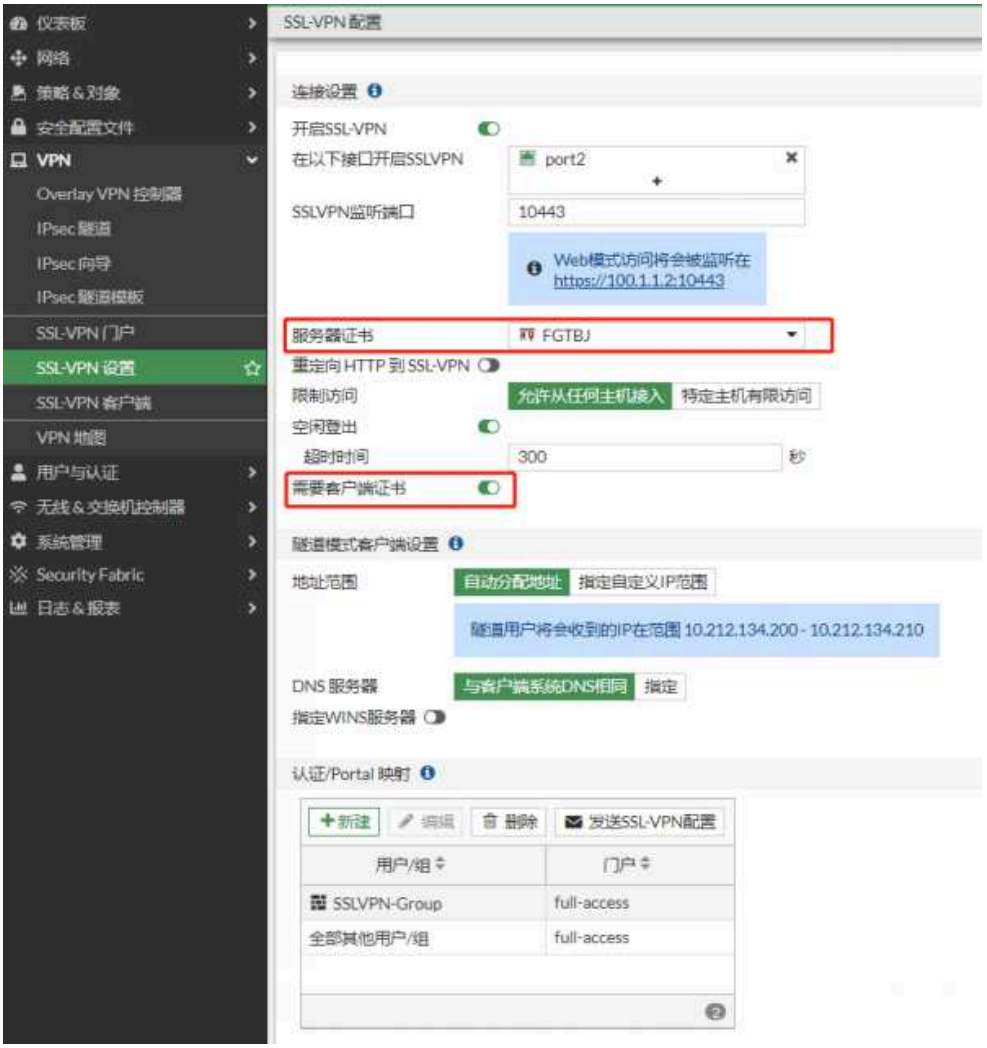
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. **配置SSLVPN**

服务器证书选择“FGTBJ”，FortiGate会使用FGTBJ证书与终端交互；勾选“需要客户端证书”，那么认证过程中FortiGate会要求客户端提供证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 创建策略

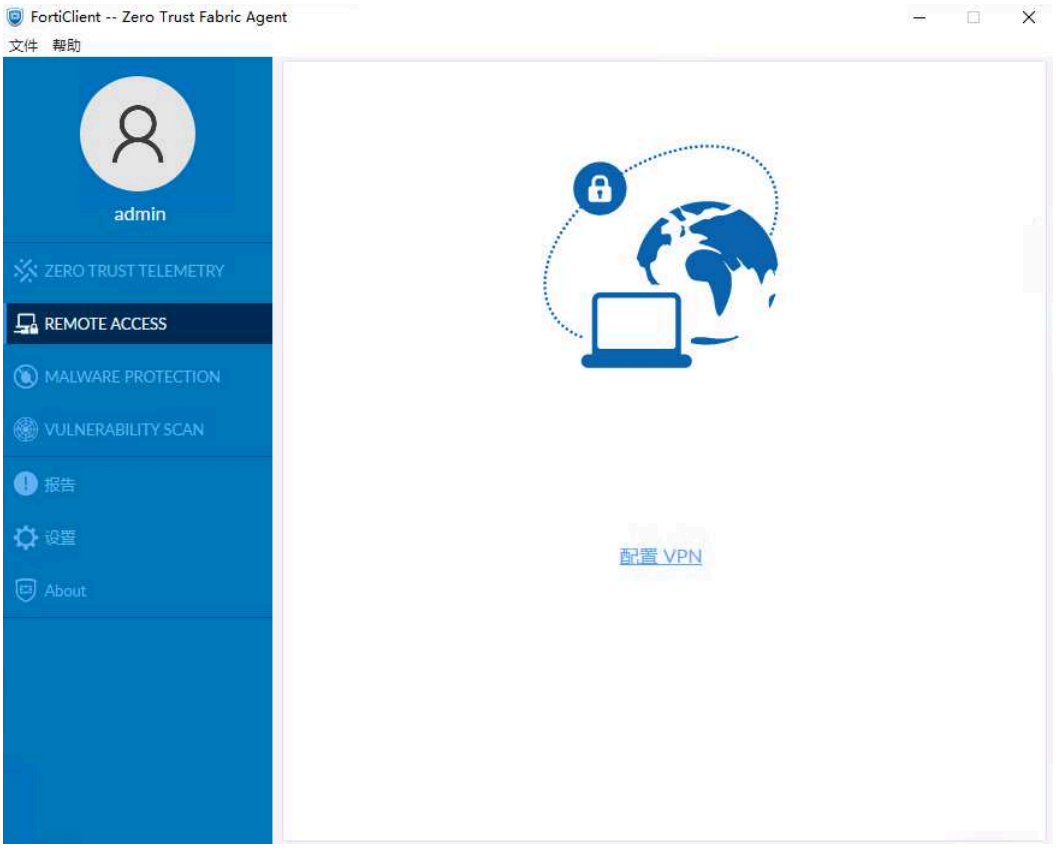
当客户端SSLVPN拨号成功后，将会使用获取的地址（10.200.1.10-10.200.1.200）访问内部主机，因此内部网络需要增加到10.200.1.0/24网段的回程路由指向FortiGate 或者 可以在策略中开启NAT，那么源地址将被转换为FortiGate接口地址，则不用考虑回程路由。



配置FortiClient

1. 选择“Remote Access”，点击“配置VPN”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

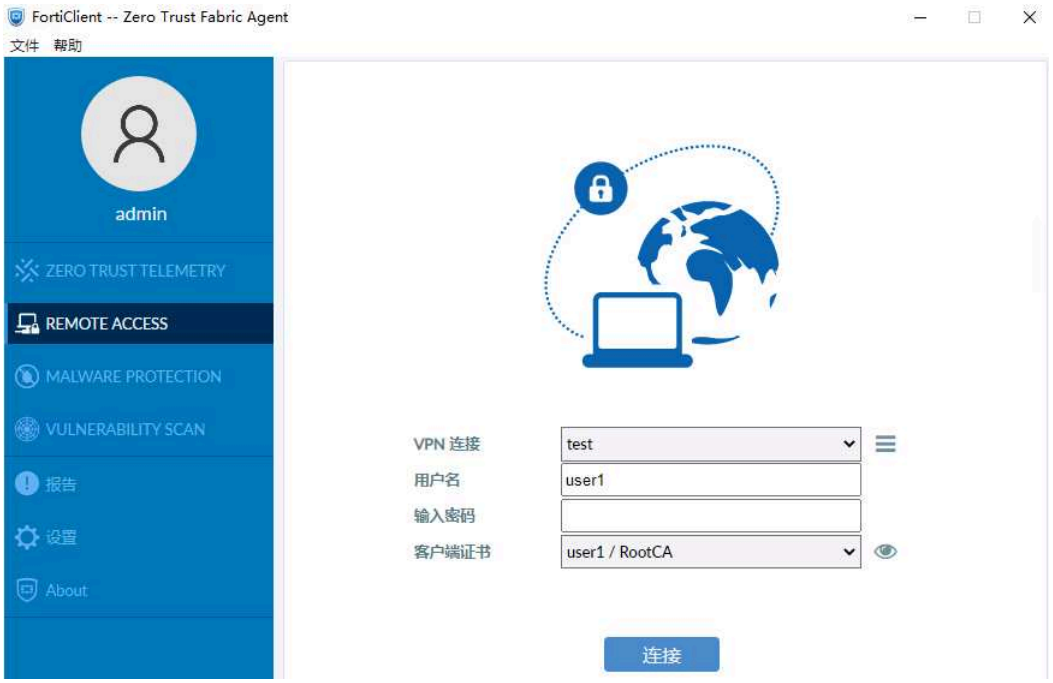


2. 选择SSL VPN，设置连接名，远程网关，SSLVPN端口，用户名以及选择终端证书，然后点击保存。



3. 配置完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



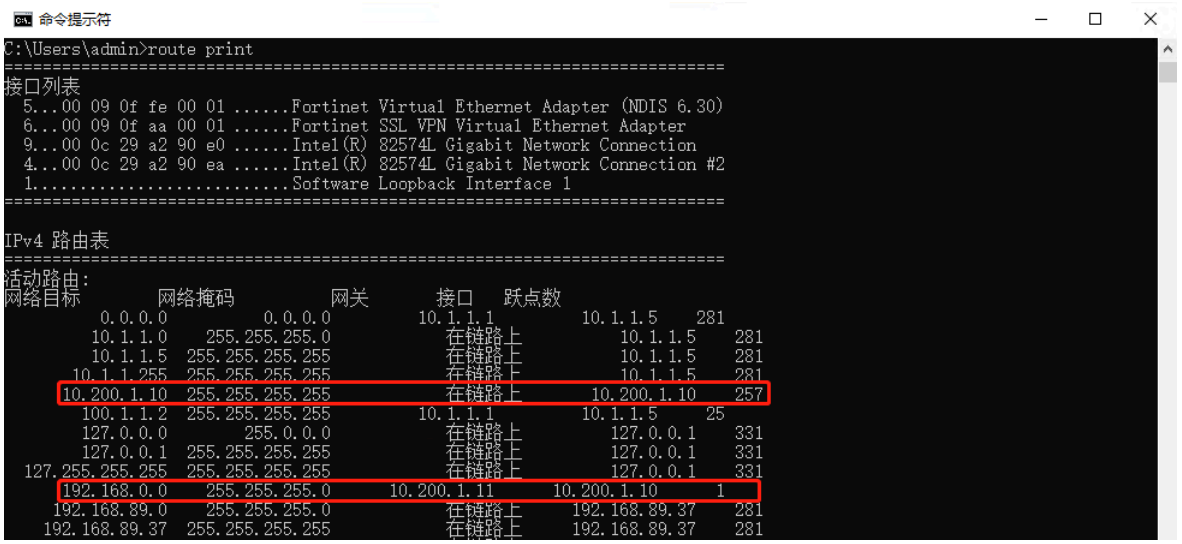
FortiClient拨号测试

1. 输入密码，点击连接。

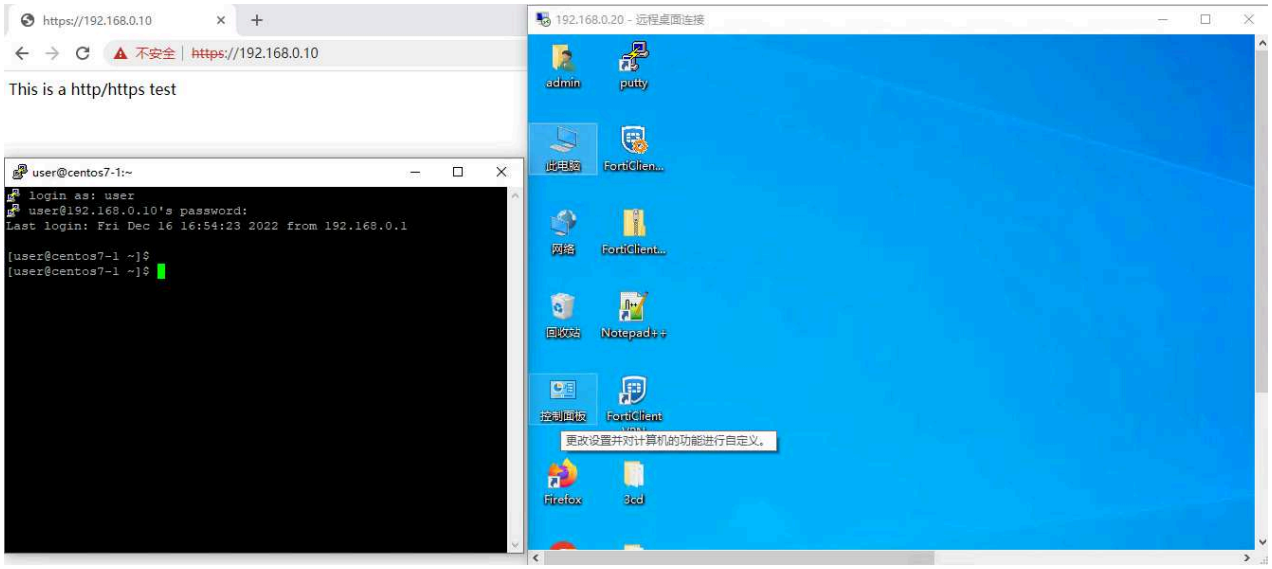


查看终端获取到的路由

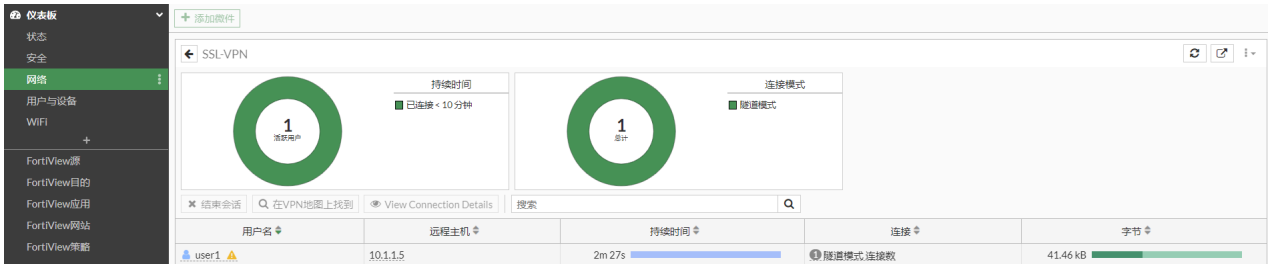
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 访问内网主机HTTPS，SSH，RDP服务都正常



3. FortiGate查看SSLVPN连接

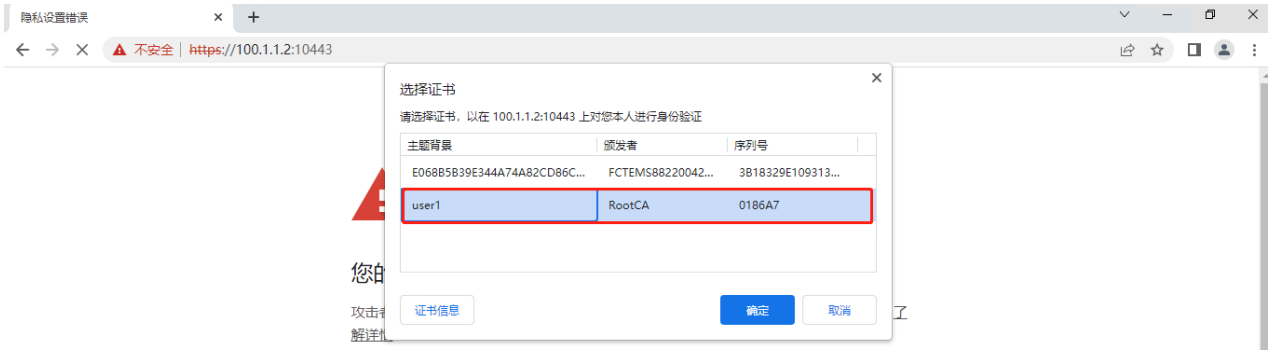



```
# get vpn ssl monitor
SSL-VPN Login Users:
 Index   User    Group   Auth Type      Timeout         Auth-Timeout    From     HTTP in/out    HTTPS in/out
Two-factor Auth
 0       user1   SSLVPN-Group   1(1)             189    28625    10.1.1.5       0/0     0/0     0

SSL-VPN sessions:
 Index   User    Group   Source IP      Duration        I/O Bytes       Tunnel/Dest IP
 0       user1   SSLVPN-Group   10.1.1.5         175     27388/14075    10.200.1.10
```

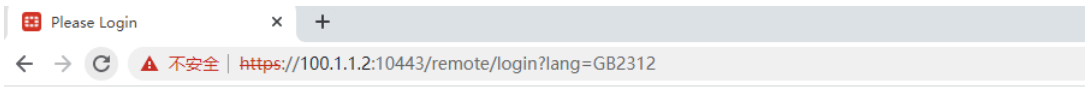
浏览器拨号测试

1. PC1使用chrome访问SSLVPN，在弹出的证书选择框中，使用user1证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 跳转到输入账号密码界面。



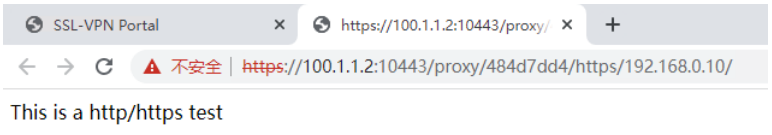


3. 登录成功。

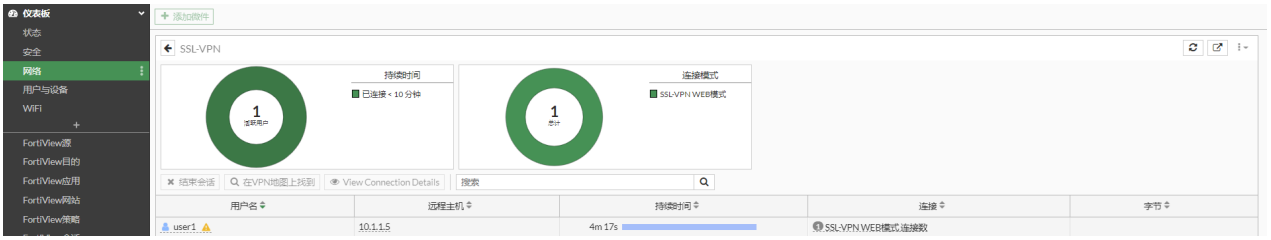


4. 访问webserver成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. FortiGate查看SSLVPN用户状态。




```
 # get vpn ssl monitor
SSL-VPN Login Users:
 Index   User    Group   Auth Type      Timeout         Auth-Timeout    From     HTTP in/out    HTTPS in/out  Two-
factor Auth
 0       user1   SSLVPN-Group   1(1)      289               28788    10.1.1.5       0/0              0/0
0

SSL-VPN sessions:
 Index   User    Group   Source IP      Duration        I/O Bytes       Tunnel/Dest IP
```

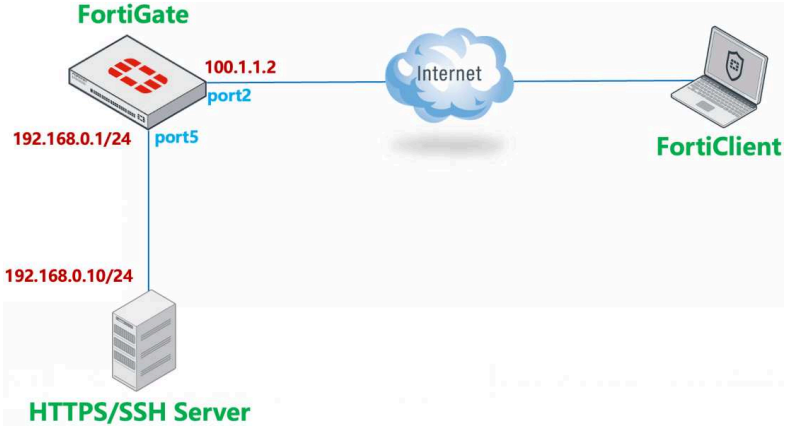

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiToken双因子认证

网络需求

在外移动办公的工作人员需要通过SSL VPN 隧道模式拨入到公司内网来对内网主机进行访问。

网络拓扑



配置步骤

FortiToken配置

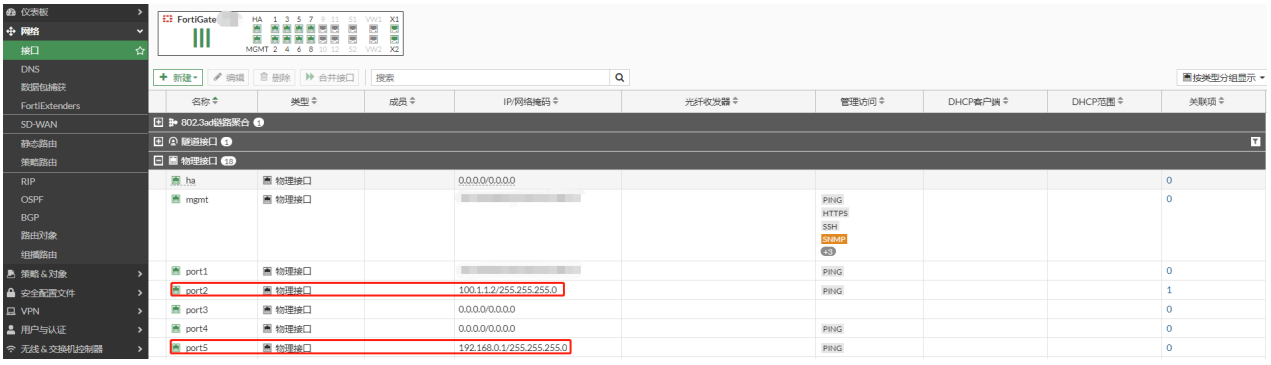
请参考如下章节：

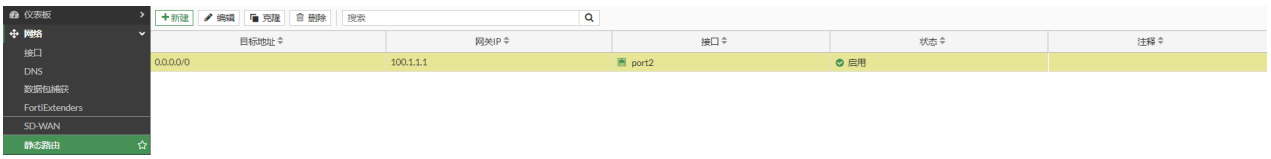
- 用户与认证→FortiToken认证→FortiToken Mobile在FortiGate上的激活
- 用户与认证→FortiToken认证→FortiToken Mobile APP软件下载与安装
- 用户与认证→FortiToken认证→FortiToken Mobile与用户进行绑定

配置SSL VPN

1. **基本配置**

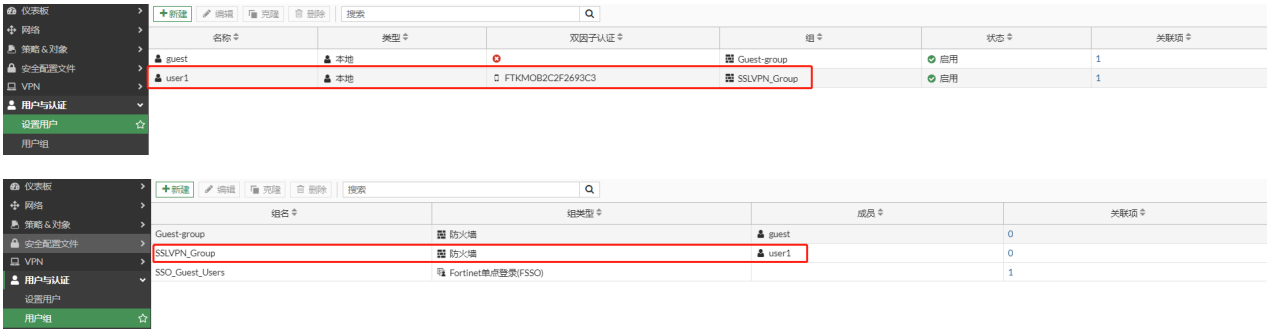
   配置接口IP和路由





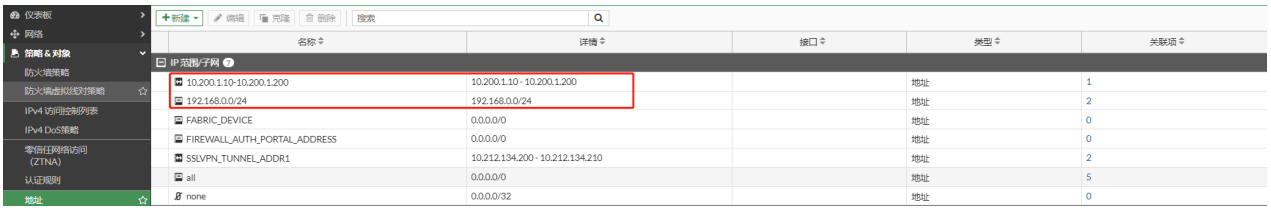
2. **创建用户，开启双因子认证，并将用户加入到用户组**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

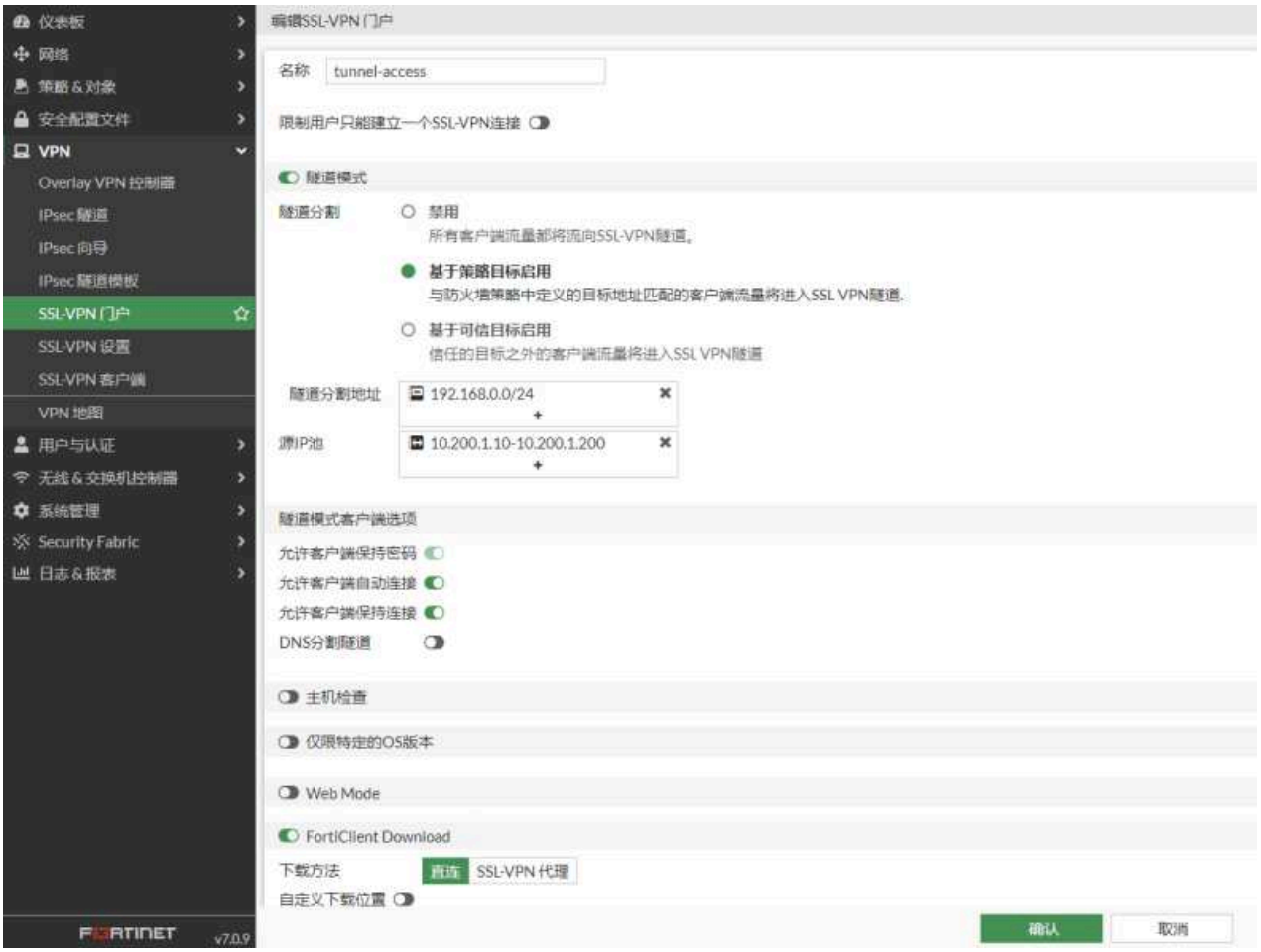


3. **配置地址对象**

10.200.1.10-10.200.1.200作为SSLVPN地址池；192.168.0.0/24作为需要访问的内网地址段。



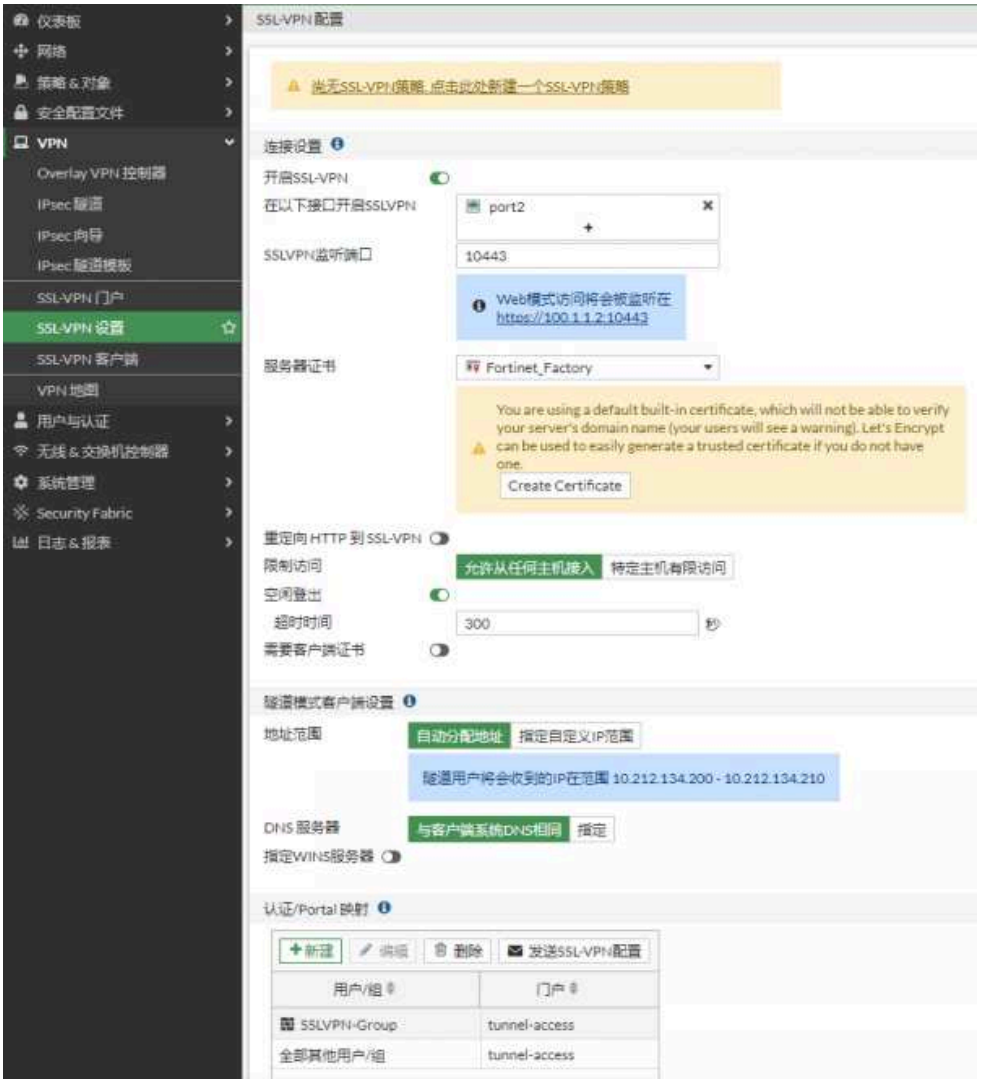
4. **配置SSL-VPN门户**



5. **配置SSLVPN**

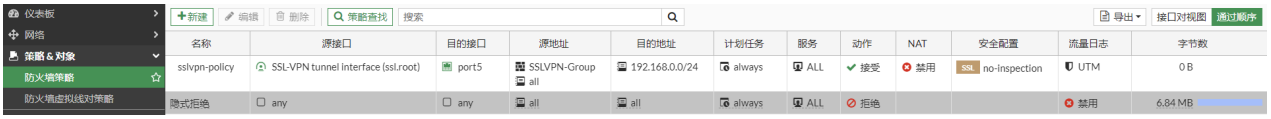
设置提供SSLVPN服务的接口和端口，将SSLVPN-Group用户组和tunnel-access门户关联；全部其他用户/组也要关联一个门户，用于没有配置关联的用户/用户组访问。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 创建策略

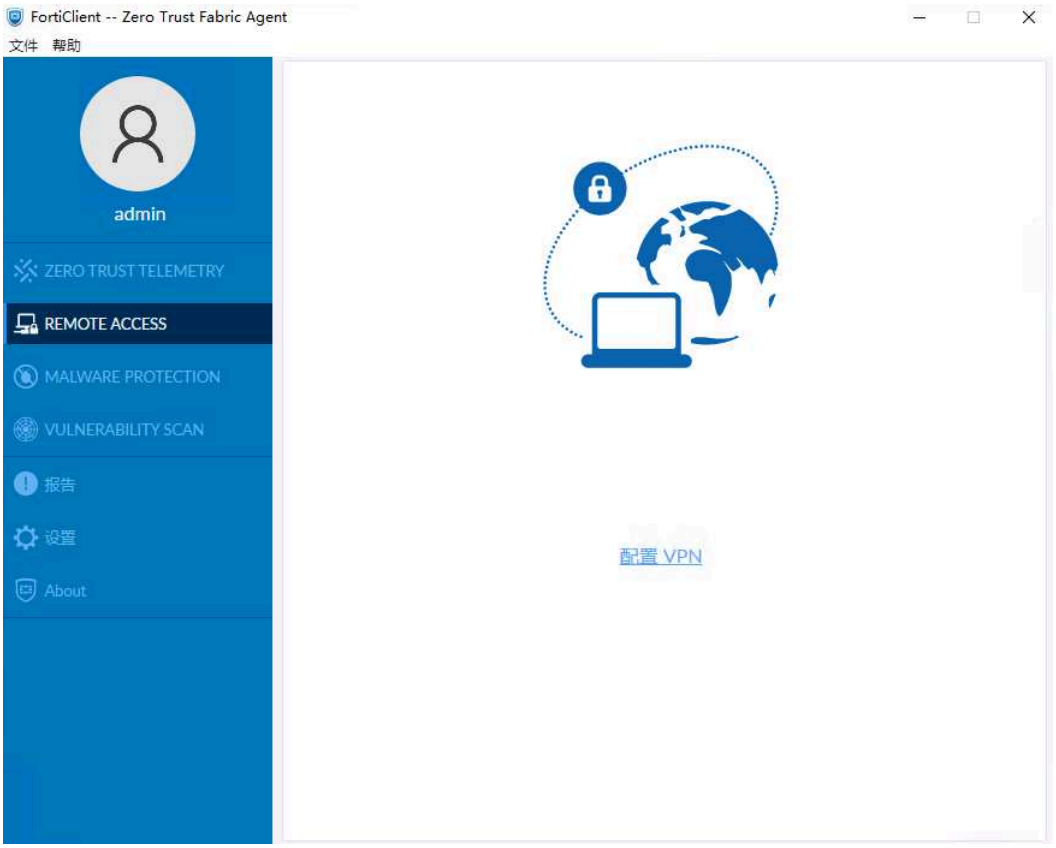
当客户端SSLVPN拨号成功后，将会使用获取的地址（10.200.1.10-10.200.1.200）访问内部主机，因此内部网络需要增加到10.200.1.0/24网段的回程路由指向FortiGate 或者 可以在策略中开启NAT，那么源地址将被转换为FortiGate接口地址，则不用考虑回程路由。



配置FortiClient

1. 选择“Remote Access”，点击“配置VPN”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

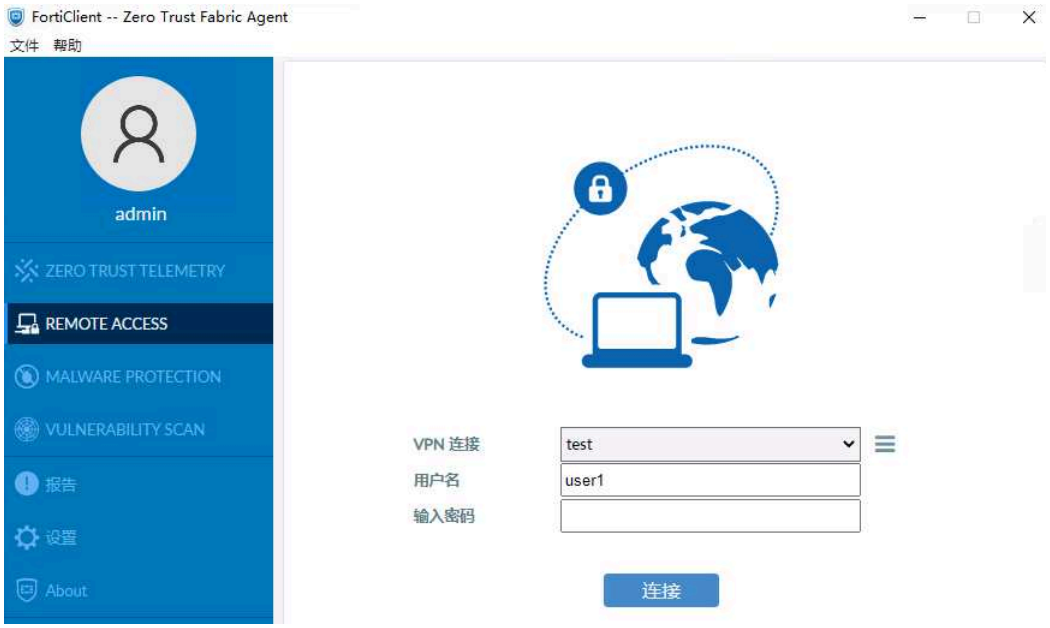


2. 选择SSL VPN，设置连接名，远程网关，SSLVPN端口以及用户名，然后点击保存。



3. 配置完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



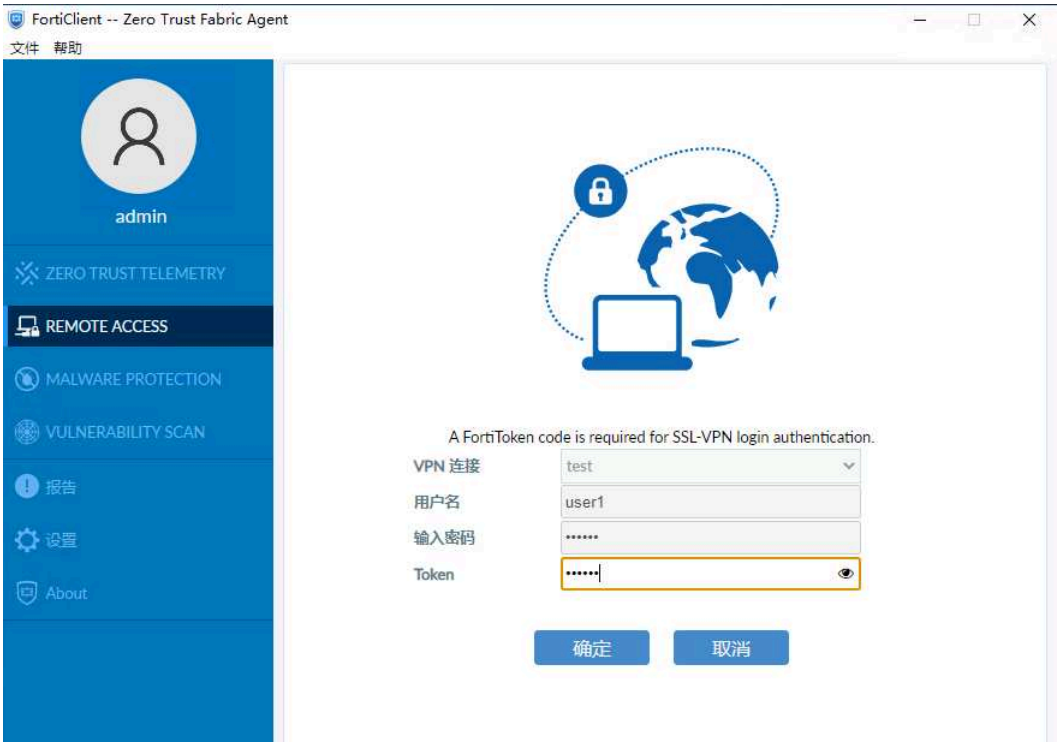
业务测试

1. 在FortiClient中输入密码，并点击连接，在弹出的窗口中，点击“是”，信任SSLVPN证书



2. 输入token码

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 连接成功



查看终端获取到的地址

```
C:\Users\admin>ipconfig/all
以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . . : Fortinet SSL VPN Virtual Ethernet Adapter
   物理地址. . . . . . . . . . . . . : 00-09-0F-AA-00-01
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::9124:e3aa:1ace:74d2%7(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.200.1.10(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.255
```

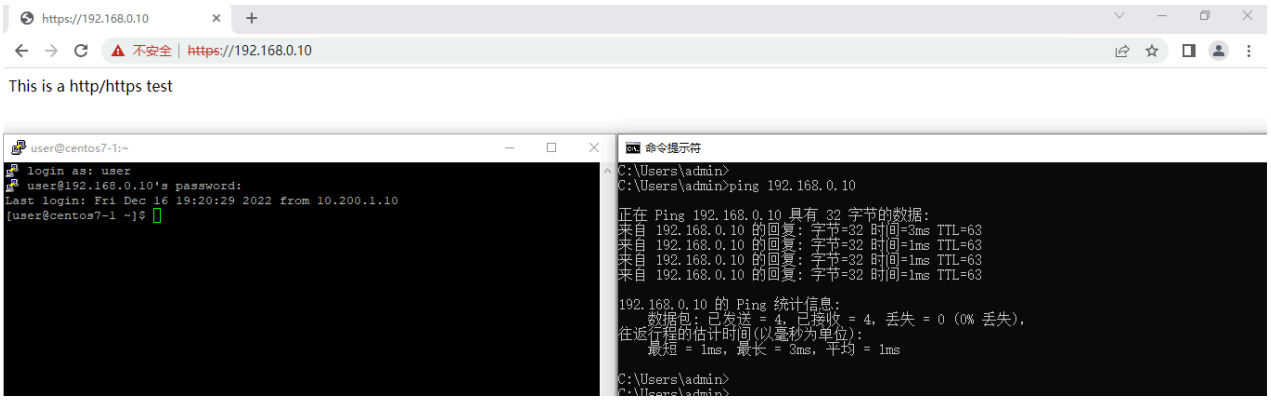

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
   默认网关. . . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 100665615
   DHCPv6 客户端 DUID  . . . . . . . . : 00-01-00-01-29-1C-CC-4A-00-0C-29-A2-90-E0
   DNS 服务器  . . . . . . . . . . . : 114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . . : 已启用
```

查看终端获取到的路由

```
C:\Users\admin>route print
===========================================================================
接口列表
  6...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
  7...00 09 0f aa 00 01 ......Fortinet SSL VPN Virtual Ethernet Adapter
 10...00 0c 29 a2 90 e0 ......Intel(R) 82574L Gigabit Network Connection
  5...00 0c 29 a2 90 ea ......Intel(R) 82574L Gigabit Network Connection #2
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0         10.1.1.1         10.1.1.5    281
         10.1.1.0    255.255.255.0            在链路上          10.1.1.5    281
         10.1.1.5  255.255.255.255            在链路上          10.1.1.5    281
       10.1.1.255  255.255.255.255            在链路上          10.1.1.5    281
     10.200.1.10  255.255.255.255            在链路上        10.200.1.10    257
       100.1.1.2  255.255.255.255         10.1.1.1         10.1.1.5     25
        127.0.0.0        255.0.0.0            在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上          127.0.0.1    331
      192.168.0.0    255.255.255.0      10.200.1.11      10.200.1.10      1
```

4. 访问内网主机PING，HTTPS，SSH服务都正常



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSL VPN源地址连接控制

简介

SSL VPN可以在功能层面对访问的客户端源地址进行限制，分为两种方式：

- 白名单：仅允许配置的IP范围访问SSL VPN服务。
- 黑名单：禁止特定的IP范围访问SSL VPN服务，其他源IP允许正常访问。

配置步骤

白名单

需求：只允许中国地区的IP访问FortiGate的SSL VPN服务。

1. 在“VPN→SSL-VPN设置”页面中，配置“限制访问”的方式为“特定主机有限访问”，点击下方的+ 按钮，在选择条目窗口中点击“新建”按钮。



2. 选择地址类型。

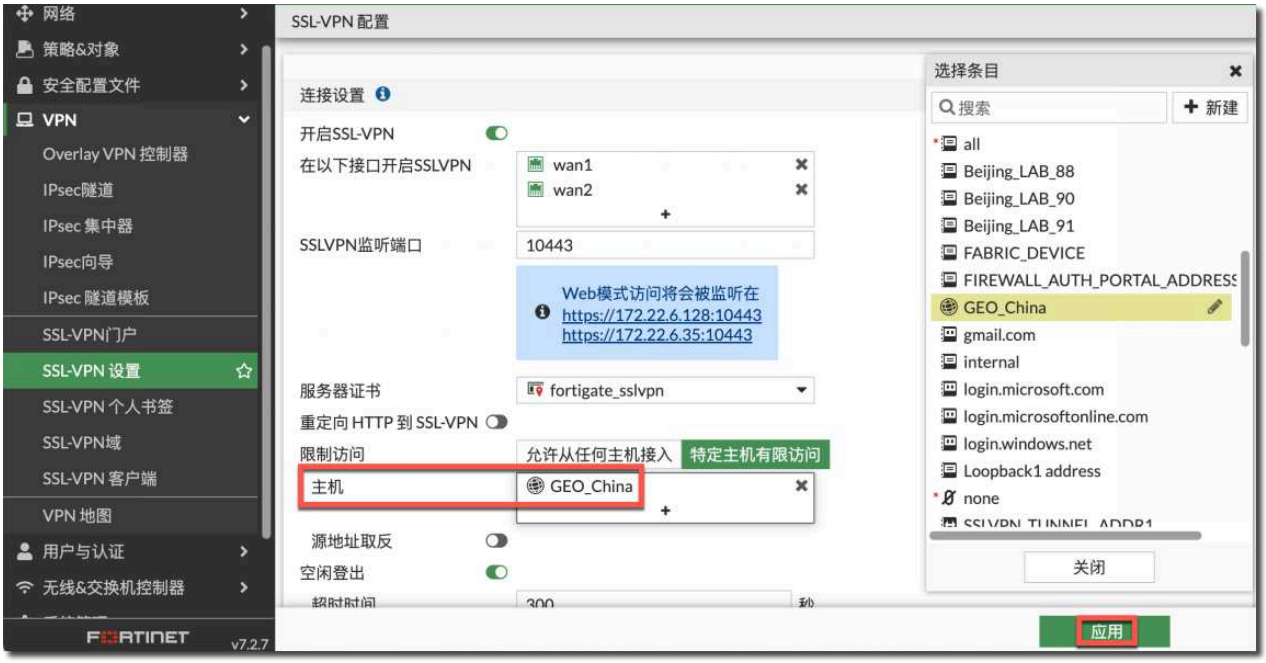


3. 配置地址名称，类型选择“地理”，国家选择China，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 选择上步创建的地理地址对象为限制访问的主机，点击页面下方的应用按钮下发配置。

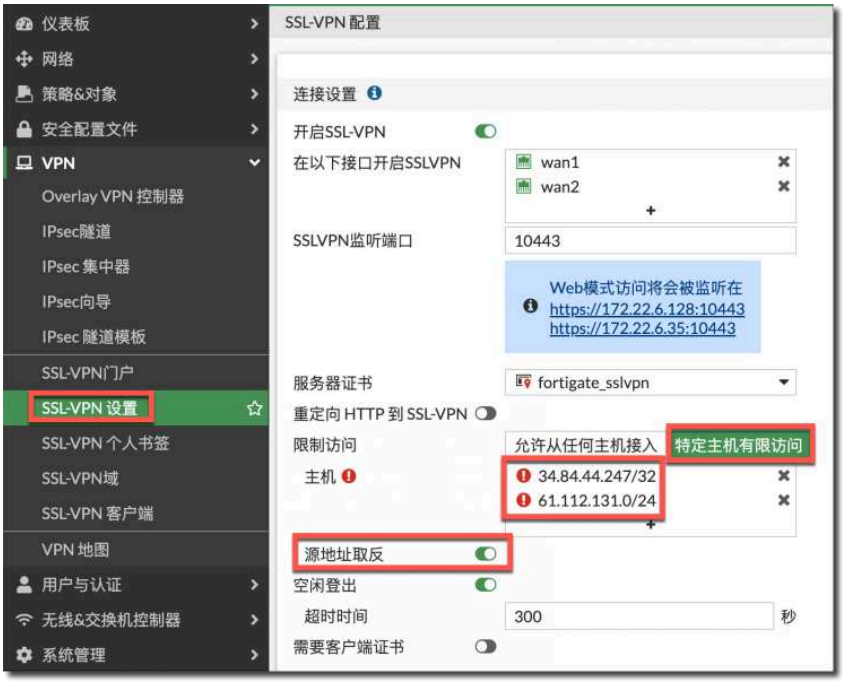



```bash
config firewall address
    edit "GEO_China"
        set type geography
        set country "CN"
    next
end

config vpn ssl settings
    set source-address "GEO_China"
end
```

黑名单

在“VPN→SSL-VPN设置”页面中，配置“限制访问”的方式为“特定主机有限访问”，开启“源地址取反”功能，并配置不允许访问的客户端网段，如下图所示，除了“34.84.44.247/32”和“61.112.131.0/24”网段不允许访问SSL VPN服务外，其他客户端可以正常访问SSL VPN服务。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config vpn ssl settings
    set source-address "34.84.44.247/32" "61.112.131.0/24"
    set source-address-negate enable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

解锁SSL VPN用户

重要

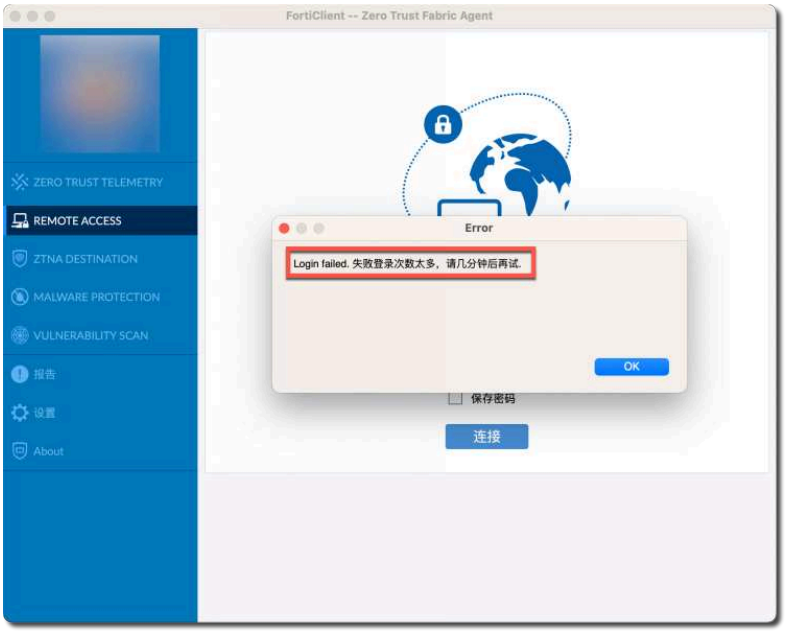
此功能在FortiOS 7.2.6及以上版本、7.4.1及以上版本、7.6.0及以上版本支持。

功能介绍

1. 默认配置下，SSL VPN用户登录失败2次后会被锁定60s。

```bash
config vpn ssl setting
    set login-attempt-limit 2
    set login-block-time 60
end
```

2. SSL VPN用户被锁定后，FortiClient登录会有如下提示。



3. FortiGate的SSL VPN Debug会有如下提示。

```bash
diagnose debug application sslvpn -1
diagnose debug enable

[15356:root:6]req: /remote/logincheck
[15356:root:6]fsv_blocklist_check:65 locked: rowid=1,host=192.168.100.177
[15356:root:6]Transfer-Encoding n/a
[15356:root:6]Content-Length 75
[15356:root:6]readPostEnter:19 Post Data length 0.
[15356:root:6]sslConnGotoNextState:318 error (last state: 1, closeOp: 0)
[15356:root:6]Destroy sconn 0x7fb0ea2800, connSize=0. (root)
[15356:root:6]SSL state:warning close notify (192.168.100.177)
```

解锁方法

1. 查看当前SSL VPN被锁定的用户列表，其中包含第一次尝试登录时间、最后一次尝试登录时间、登录失败次数、所属VDOM ID。

```bash
FortiGate # diagnose vpn ssl blocklist list
|id|addr|status|first-attempt|last-attempt|fail-count|vfid|
|1|192.168.100.177|locked|2024-12-27 15:51:07|2024-12-27 15:51:11|2|0|
Total 1 entry.
```

2. 通过FortiView页面“按认证失败排名”可以看到每个用户在特定时间范围内的尝试登录失败次数。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 通过如下CLI命令可以解锁已被锁定的SSL VPN用户。

```bash
FortiGate # diagnose vpn ssl blocklist del <all|vfid|addr>
```

- `all`：解锁所有被锁定的SSL VPN用户。
- `vfid`：解锁特定VDOM ID下被锁定的所有SSL VPN用户。
- `addr`：解锁特定IP被锁定的SSL VPN用户。

4. 通过IP地址的形式解锁SSL VPN用户，可以看到IP 192.168.100.177被锁定的用户被解锁。

```bash
FortiGate # diagnose vpn ssl blocklist del 192.168.100.177

FortiGate # diagnose vpn ssl blocklist list
|id|addr|status|first-attempt|last-attempt|fail-count|vfid|
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

DTLS

默认配置下，SSL VPN使用TCP来封装TLS，当SSL VPN封装的业务数据为TCP时，就形成了TCP-in-TCP流量。这种情况下性能可能比预期的要慢。

Datagram Transport Layer Security (DTLS) 允许SSL VPN使用TLS加密流量，并使用 UDP 作为传输层，而不是TCP。DTLS具有与SSL相同的安全性，但使用UDP而不是TCP。这可以显著提高性能，避免了在TCP-in-TCP中可能发生的重传问题。

配置步骤

FortiGate

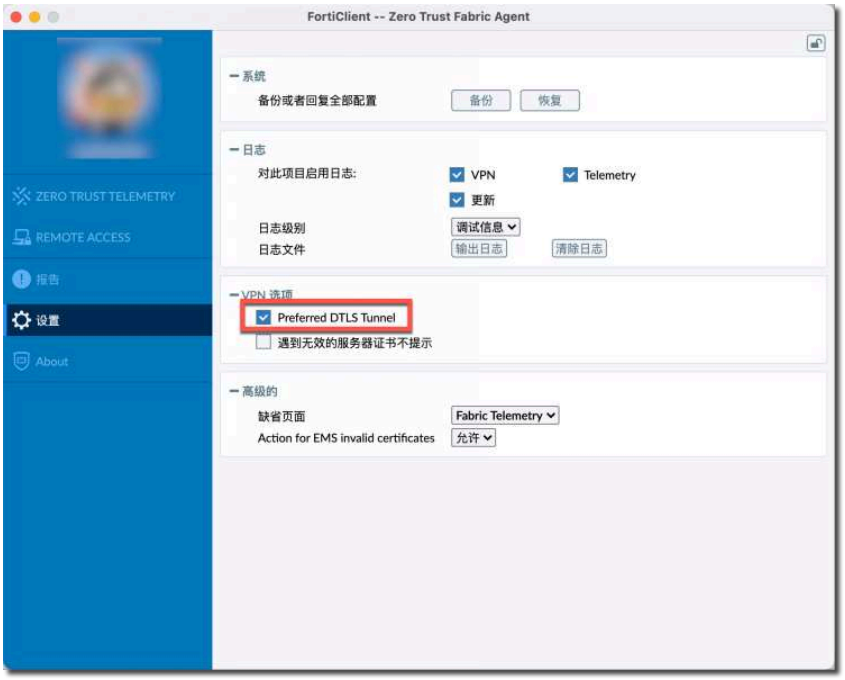
通过如下CLI开启SSL VPN的DTLS。

```
config vpn ssl settings
    set dtls-tunnel enable
end
```

FortiClient

对应的FortiClient也需要开启DTLS功能。

> **重要**
>
> 如果FortiClient连接到了EMS Server，这里的配置是无法修改的，需要管理员在EMS Server端进行修改。如果FortiClient未连接EMS Server，或使用的是FortiClient VPN only版本，需要点击FortiClient界面左下角的 图标解锁后，才可以继续配置。



- 开启“Preferred DTLS Tunnel”：FortiClient将在FortiGate上启用并成功建立隧道时使用DTLS。如果在FortiGate上未启用或隧道建立不成功，则使用TLS。DTLS隧道使用UDP而不是TCP，可以提高VPN的吞吐量。
- 关闭“Preferred DTLS Tunnel”：当禁用时，FortiClient将使用TLS，即使在FortiGate上启用了DTLS。

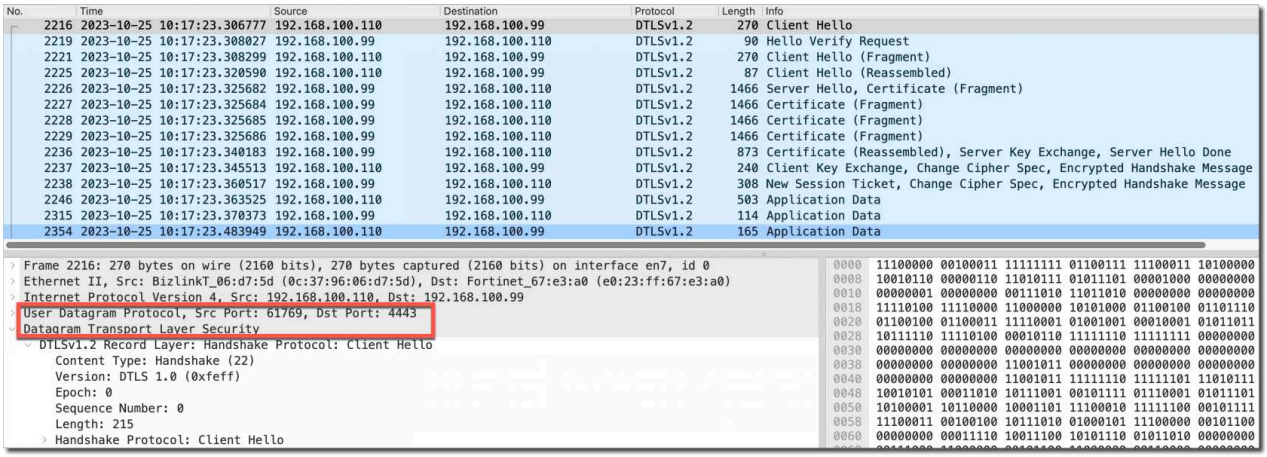
结果验证

1. FortiClient连接FortiGate的SSL VPN服务，查看FortiGate的sslvpnd进程debug信息，可以看到SSL VPN连接使用DTLS建立。

```
[321:root:5]DTLS established: DTLSv1 ECDHE-RSA-AES256-GCM-SHA384 from 192.168.100.110
```

2. 抓包查看SSL VPN协商与业务流量，可以看到SSL VPN协商与后续业务流量均使用DTLS封装。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSL VPN连接后断开

问题现象

1. FortiClient在连接SSL VPN成功后，马上断开连接。

2. FortiClient所在PC的真实公网IP为121.211.6.3。

3. 但在`diagnose debug application sslvpn -1`的debug信息中，FortiClient的公网IP却显示显示为221.211.135.16（`host[221.211.135.16]`）。

```bash
diagnose debug application sslvpn -1
diagnose debug

[12260:root:27]deconstruct_session_id:494 decode session id ok, user=[jszn], group=[sslvpn-group],authserver=
[],portal=[tunnel-access],host[221.211.135.16],realm=[],csrf_token=
[467291DF2B61CBF51DD42F8B423FFB99],idx=1,auth=1,
sid=3471a060,login=1755833636,access=1755833636,saml_logout_url=no,pip=201.218.89.162,grp_info=
[QOa1Sc],rmt_grp_info=[]
[12260:root:27]session removed s: 0×7f8b9fd000 (root)
```

4. 正常的debug信息应为`host[121.211.6.3]`：

```
[12260:root:27]deconstruct_session_id:494 decode session id ok, user=[jszn], group=[sslvpn-group],authserver=
[],portal=[tunnel-access],host[121.211.6.3],realm=[],csrf_token=[467291DF2B61CBF51DD42F8B423FFB99],idx=1,auth=1,
sid=3471a060,login=1755833636,access=1755833636,saml_logout_url=no,pip=205.218.89.162,grp_info=
[QOa1Sc],rmt_grp_info=[]
[12260:root:27]session removed s: 0×7f8b9fd000 (root)
```

5. `diagnose debug application sslvpn -1`的debug信息中，SSL VPN连接中断的原因是`source ip check failed`。

```bash
diagnose debug application sslvpn -1
diagnose debug

......
[12261:root:27]get_shm_session:1368 source ip check failed
......
```

问题原因

SSL VPN的`source ip check failed`会导致身份验证失败，并在成功连接后几秒内终止SSL VPN连接。此情况可能出现在客户端使用NAT、代理服务或负载均衡等技术，这些技术可能会在SSL VPN会话建立过程中更改客户端的实际公网IP。

解决方法

允许SSL VPN认证会话令牌中的源IP与客户端实际建立连接的源IP地址不同的情况下，仍应能成功认证。执行以下命令禁用SSL VPN连接的源IP地址验证：

```bash
config vpn ssl settings
    set auth-session-check-source-ip disable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiClient下载

本地下载

Windows (v7.2.12.1269)

完整版（需要购买EMS License）

FortiClient_windows.zip ↗

VPN Only版（免费使用，仅包含VPN功能，不提供技术支持）

FortiClientVPN_windows.exe ↗

macOS (v7.2.12.1106)

完整版（需要购买EMS License）

FortiClient_macosx.dmg ↗

VPN Only版（免费使用，仅包含VPN功能，不提供技术支持）

FortiClientVPN_macosx.dmg ↗

Android (v7.4.3-build0184)

完整版（需要购买EMS License）

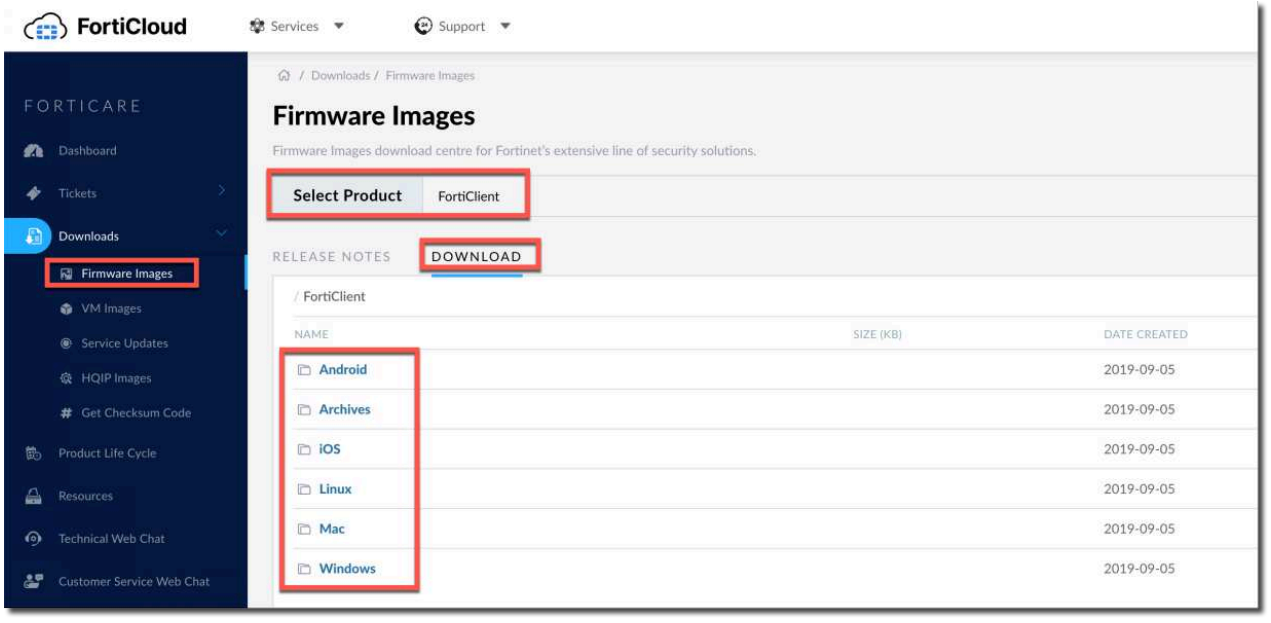
FortiClient_android ↗

VPN Only版（免费使用，仅包含VPN功能，不提供技术支持）

FortiClientVPN_android ↗

官网下载

1. 直接打开并登录https://support.fortinet.com/support/#/downloads/firmware ↗，选择产品为FortiClient，点击Download模块，选择对应系统与版本下载。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. iOS版本请参考VPN技术→FortiClient VPN→iPhone FortiClient安装及使用 ↗章节。

注意事项

1. 完整版FortiClient需要EMS License，可根据EMS序列号提供技术支持。免费的FortiClient VPN仅支持SSL VPN和IPSec VPN，且不提供技术支持服务。



2. 免费版FortiClient（FortiClient VPN Only）不支持以下VPN功能：
   - VPN自动连接、保持在线。
   - 在系统登录前登录VPN。
   - EMS集中管理。
   - 调试工具。

3. FortiClient与操作系统兼容性请参考：
   - FortiClient iOS客户端与系统兼容性：https://docs.fortinet.com/document/forticlient/7.2.99/ios-administration-guide/394867/supported-platforms ↗
   - FortiClient Android客户端与系统兼容性：https://docs.fortinet.com/document/forticlient/7.2.99/android-administration-guide/191370/product-integration-and-support ↗
   - FortiClient Windows客户端与系统兼容性：https://docs.fortinet.com/document/forticlient/7.2.99/windows-release-notes/549781/product-integration-and-support ↗
   - FortiClient macOS客户端与系统兼容性：https://docs.fortinet.com/document/forticlient/7.2.99/macos-release-notes/471180/product-integration-and-support ↗
   - FortiClient EMS与Fortinet其他产品兼容性：https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/afec3249-ed3f-11ea-96b9-00505692583a/FortiClient_ems-compatibility-matrix.pdf ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

系统兼容性列表

提示

- ❓ 表示该版本不支持 ZTNA，未填项表示 FCT 版本不支持该 OS 版本。
- ✔️ 表示该版本是 Beta 版本，支持有限的功能。
- Metro 表示 Windows Metro 应用， 需要通过 Window Store 下载：https://apps.microsoft.com/detail/9wzdncrdh6mc?hl=zh-CN&gl=CN
- 不推荐使用 7.0.0 - 7.0.7，所以此表暂未收录，详细信息请参考 Release Note：https://docs.fortinet.com/product/forticlient/7.0

OS/FCT 版本		6.4.7	6.4.8	6.4.9	6.4.10	7.0.7	7.0.8	7.0.9	7.0.10	7.0.11	7.0.12	7.0.13	7.0.14	7.2.0	7.2.1	7.2.2	7.2.3	7.2.4	7.2.5
Windows	Winows 7	✅	✅	✅	✅	❓	❓	❓						❓	❓				
	Windows 8																		
	Windows 8.1	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅						
	Windows 10	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	Windows 11	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
Windows ARM	Windows RT 8																		
	Windows RT 8.1																		
	Windows 10 ARM																		
	Windows 11 ARM																		
Windows Server	Windows Server 2003																		
	Windows Server 2008																		
	Windows Server 2008 R2	✅	✅	✅	✅	✅	✅												
	Windows Server 2012	✅	✅	✅	✅	✅	✅	✅											
	Windows Server 2012 R2	✅	✅	✅	✅	✅	✅	✅											
	Windows Server 2016	✅	✅	✅	✅	✅	✅	✅											
	Windows Server 2019	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	Windows Server 2022	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
macOS	macOS 10.14 (Mojave)	✅	✅		✅														
	macOS 10.15 (Catalina)	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅						
	macOS 11 (Big Sur)	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅			
	macOS 12 (Monterey)	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	macOS 13 (Ventura)			✅		✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	macOS 14 (Sonoma)								✅	✅	✅	✅	✅			✅	✅	✅	✅
	macOS 15 (Sequoia)											✅	✅						✅
	macOS 26 (Tahoe)																		

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Windows FortiClient安装及使用

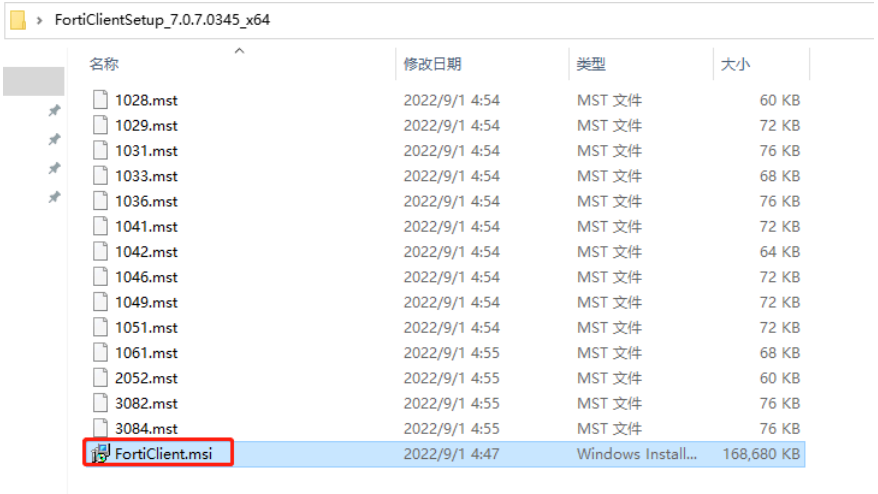
Windows FortiClient完整版安装

1. **下载FortiClient**

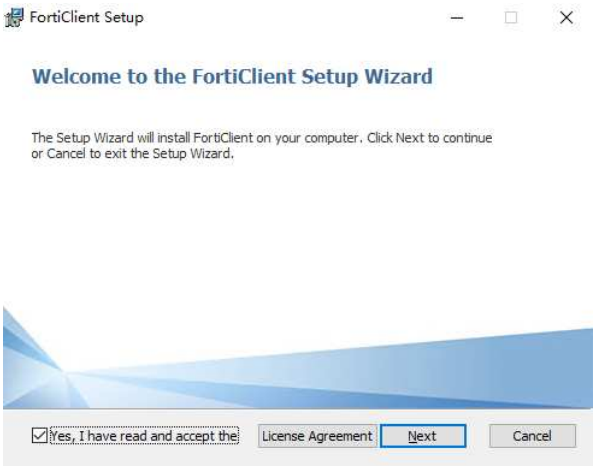
   参考：VPN技术→FortiClient VPN→FortiClient下载 ↗。

2. **安装FortiClient**

   解压FortiClient下载包，然后点击“FortiClient.msi”安装（版本号仅举例使用，请根据实际下载的版本文件执行）。

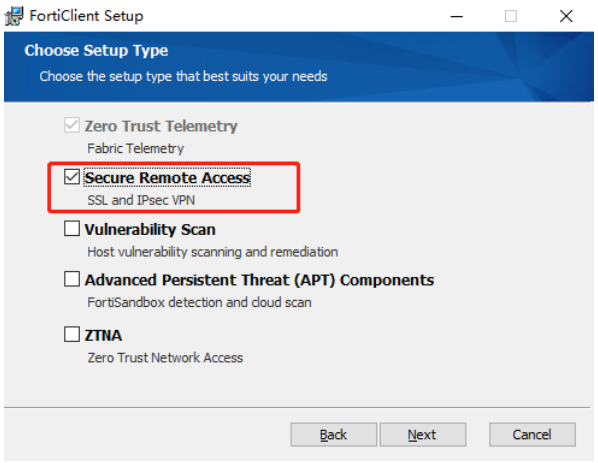


勾选“Yes,I have read an accept the ...”，点击Next。

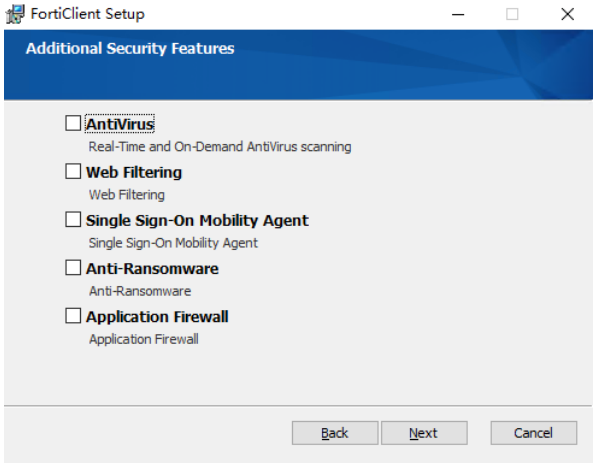


选择“Secure Remote Access”，即SSLVPN和IPSEC VPN，点击Next。

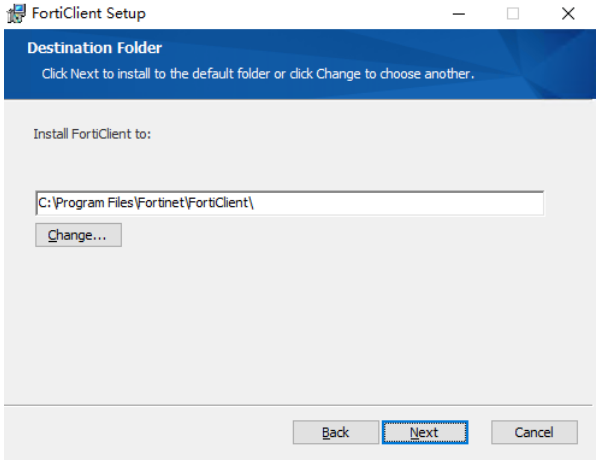
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击Next。

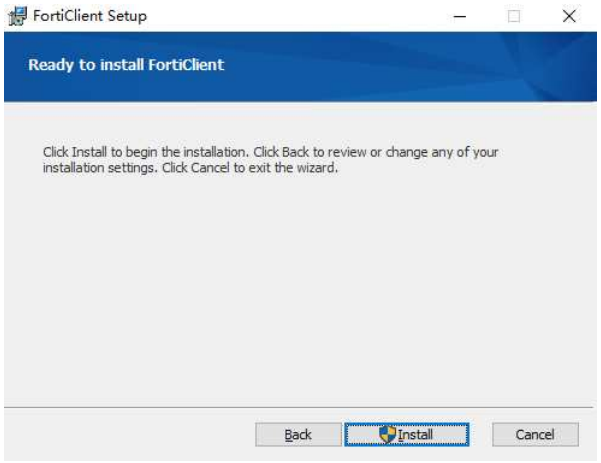


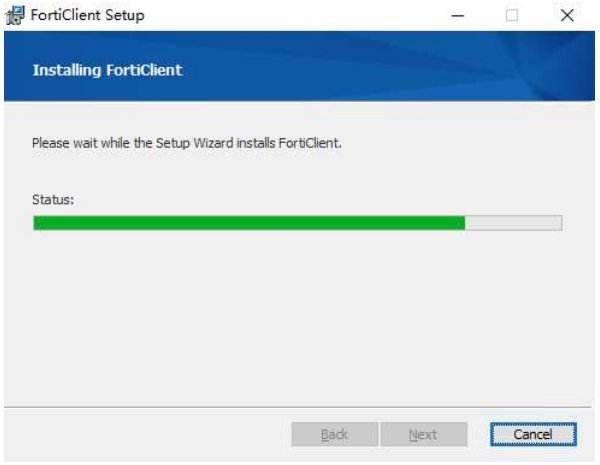
点击Next。



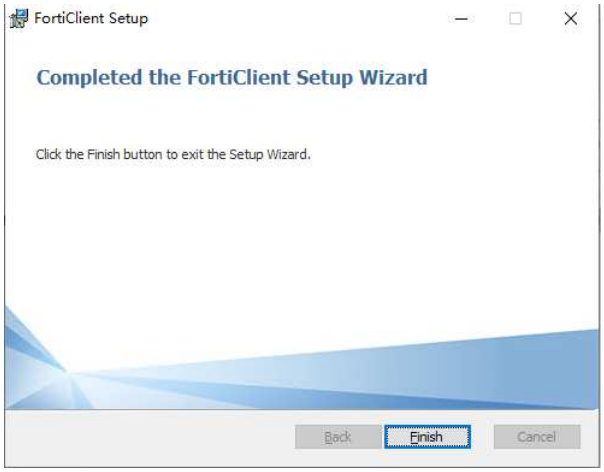
点击Install。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





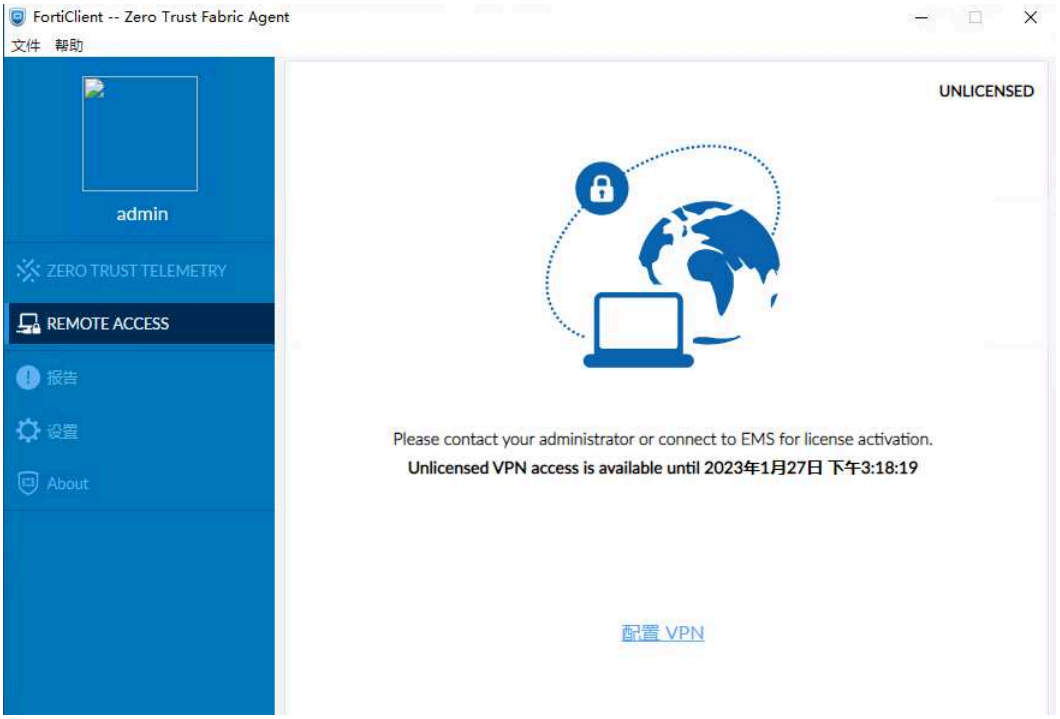
点击“Finish”，安装完成。



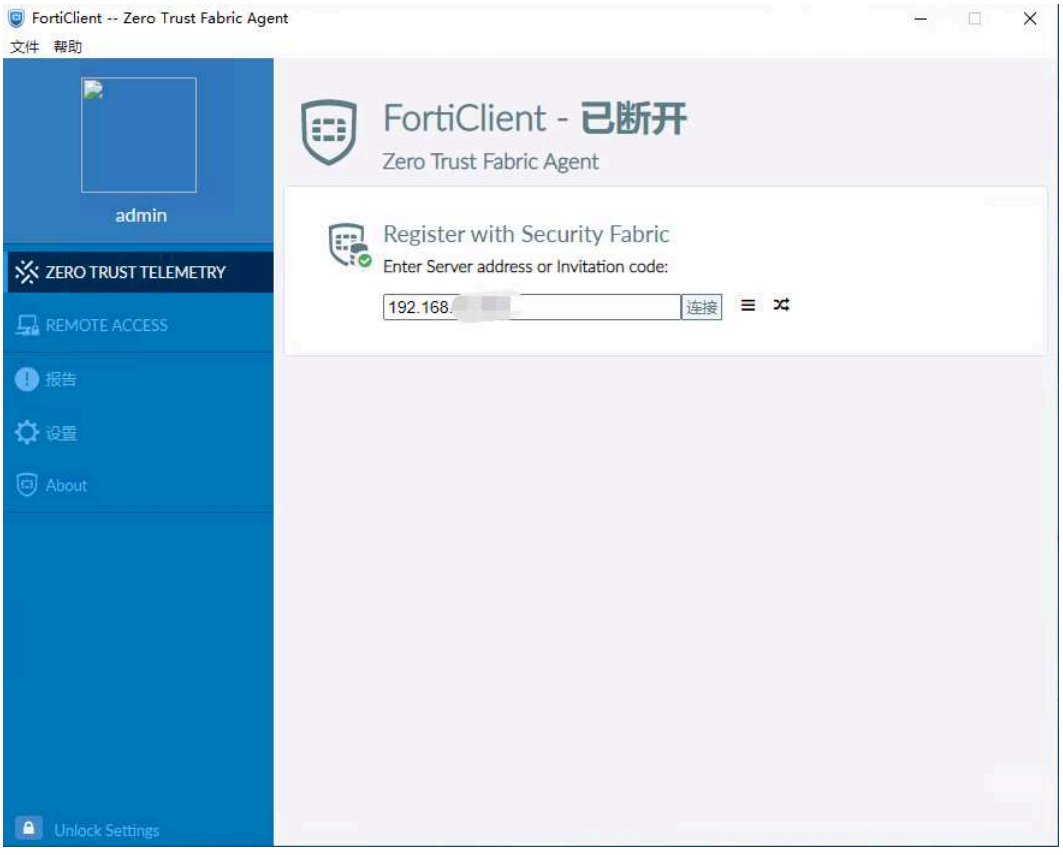
3. **连接EMS**

打开FortiClient，在没有连接EMS之前，FortiClient会显示UNLICNESED，并提示试用时间。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

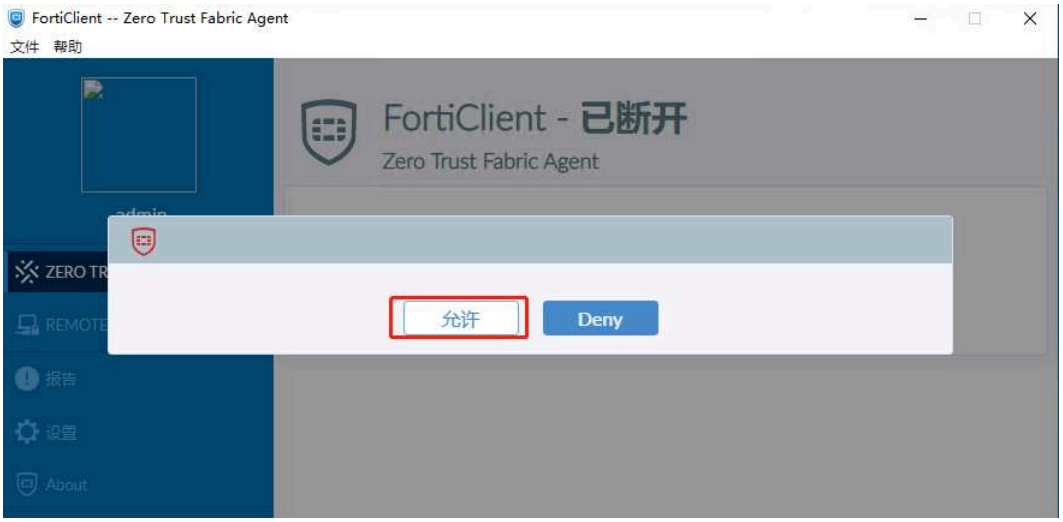


输入EMS服务器的地址或者域名。



选择”允许“

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



已连接上EMS，并且不再提示UNLICNESED。





Windows免费版FortiClient VPN安装

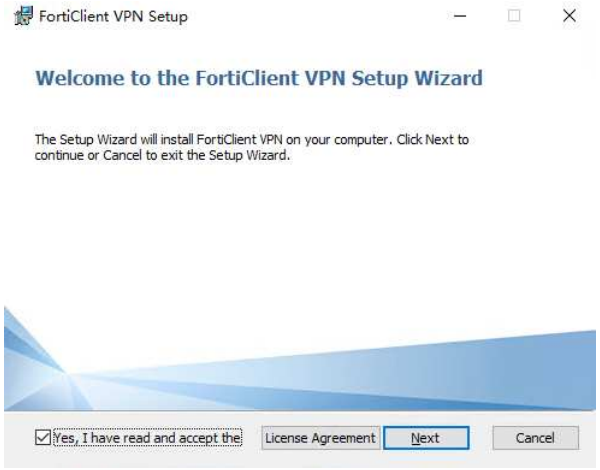
1. 下载FortiClient

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

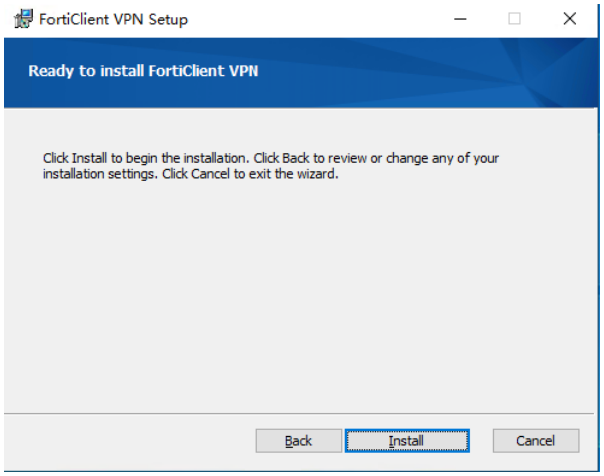
参考：VPN技术→FortiClient VPN→FortiClient下载 ↗。

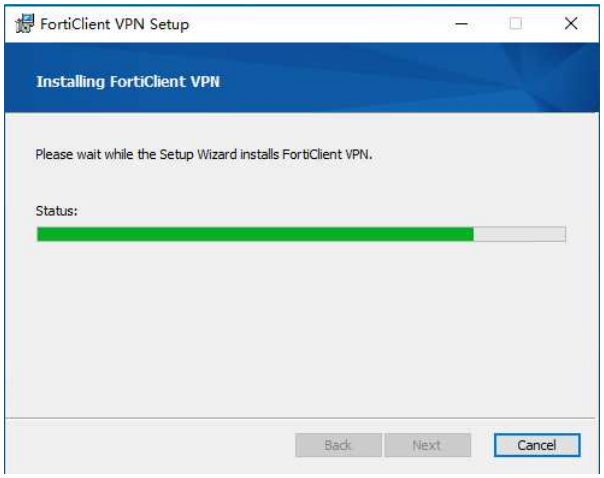
2. **安装FortiClient**

双击FortiClientVPNSetup_7.0.7.0345_x64.exe（版本号仅举例使用，请根据实际下载的版本文件执行）安装，勾选“Yes,I have read an accept the ...”，点击Next。



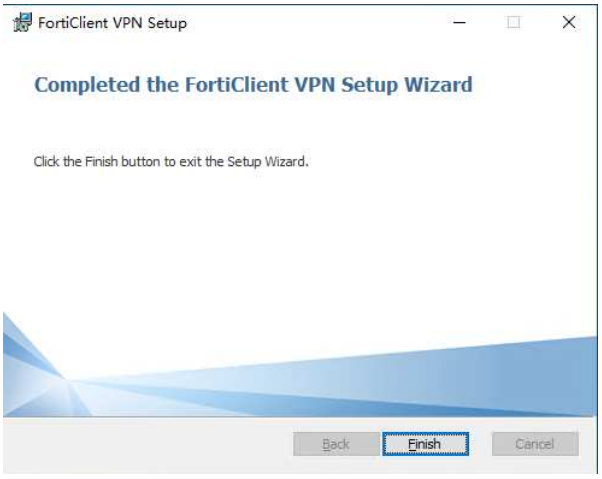
点击Install。





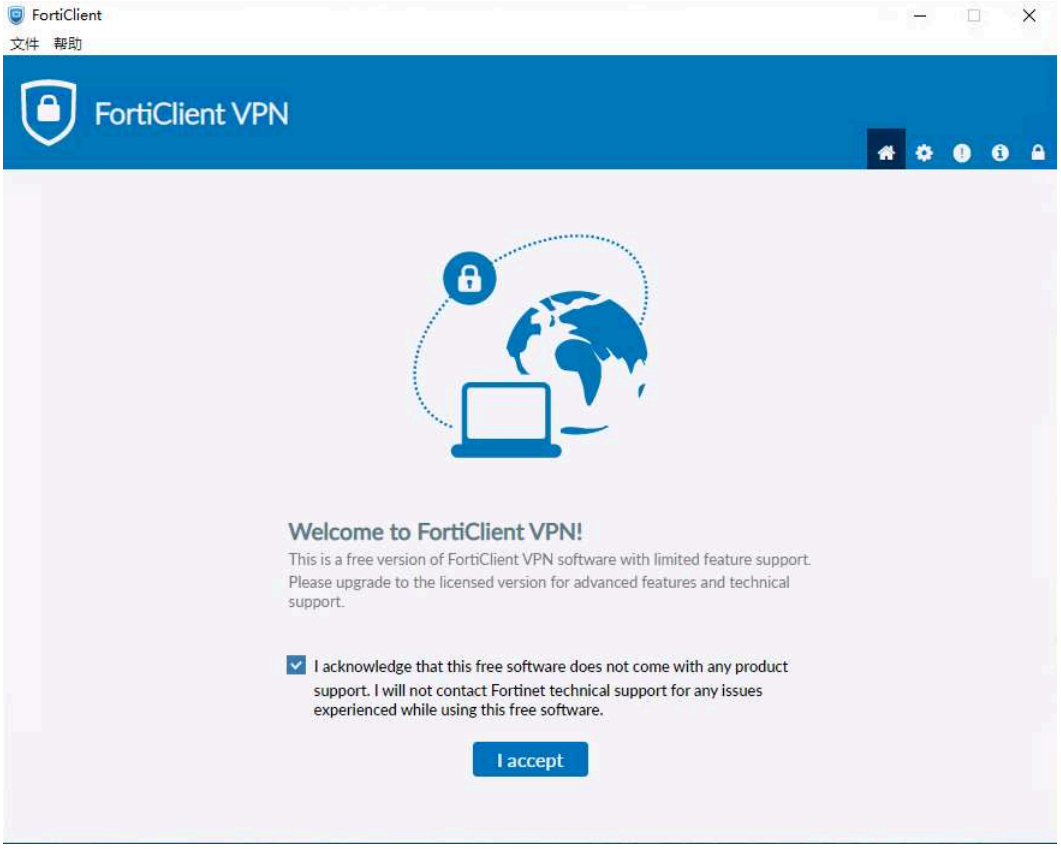
安装完成，点击“Finish”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



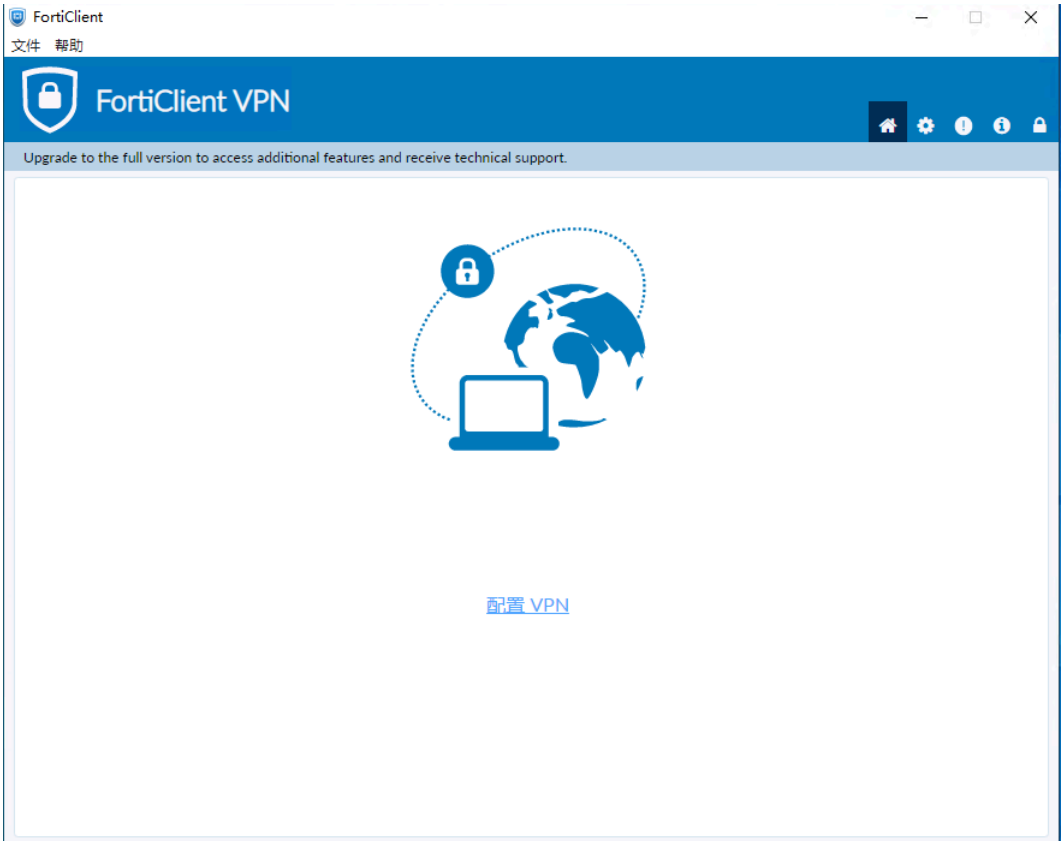
3. **打开FortiClient**

勾选“I acknowledge that this free software...”，点击I accept。免费的FortiClient是不提供技术支持服务的。



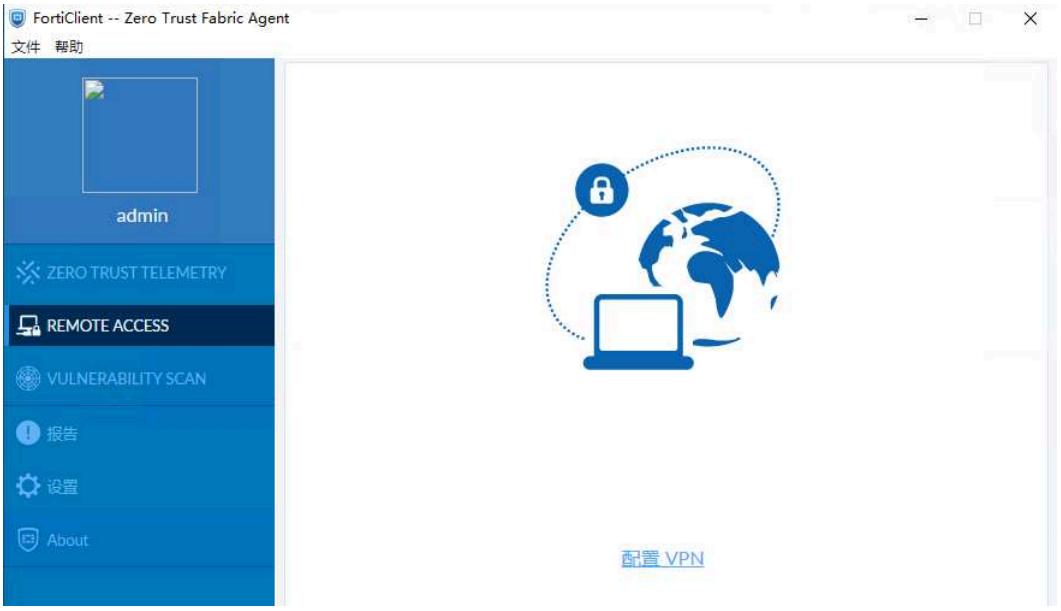
同意后显示配置界面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Windows设置SSLVPN

1. **点击“配置VPN”**



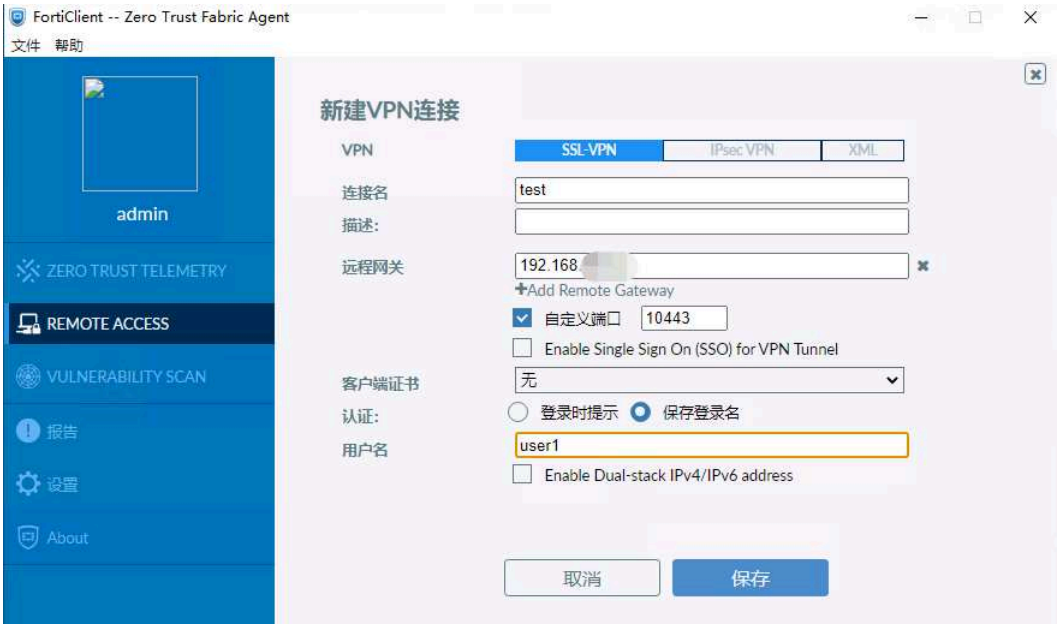
2. **设置SSLVPN连接**

   连接名：SSLVPN名称

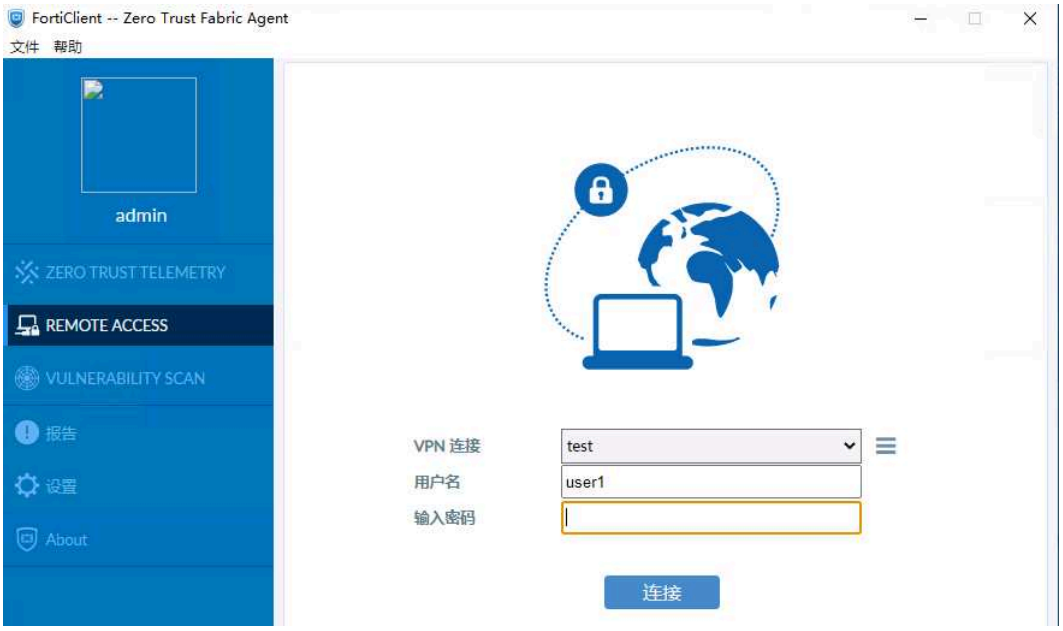
   远程网关：FortiGate开启SSLVPN服务的接口地址；

   自定义端口：SSLVPN服务的端口号；

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



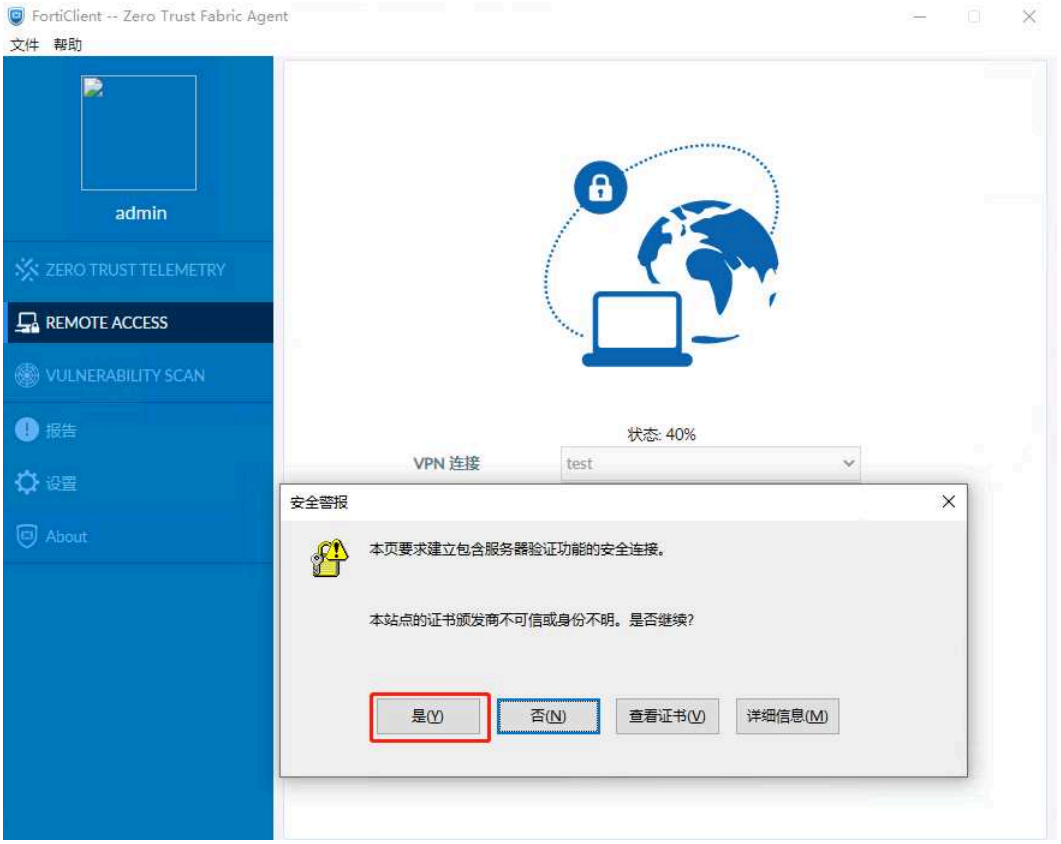
3. **配置完成**



4. **SSLVPN连接**

输入账号和密码后，点击连接，再弹出窗口选择是，接受FortiGate的证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



连接成功。



通过CLI方式安装FortiClient

1. 您可以使用CLI方式安装FortiClient，从而实现安装时的参数设置。下表总结了使用CLI时可用的安装选项。 无论您使用.exe 文件还是.msi文件和.mst 文件，这些选项都可用：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

安装参数	说明
/quiet	安装处于静默模式，不需要用户交互。
/passive	安装处于无人值守模式，仅显示进度条。
/norestart	安装完成后不重启系统。
/promptrestart	如有必要，提示您重新启动系统。
/forcerestart	安装后强制重启系统。
/uninstallfamilys	安装前卸载已安装的FortiClient。使用此选项，FortiClient安装程序会检测当前系统已安装的FortiClient并卸载FortiClient。例如，FortiClient 7.0.8安装前可以检测并卸载之前已安装的FortiClient 7.0.7。

2. 以下示例以静默模式安装FortiClient build 1131，安装后不重启系统，并在c:\temp目录中输出名为“example.log”的安装日志文件。

```
FortiClientSetup_7.0.8.1131_x64.exe /quiet /norestart /log c:\temp\example.log
```

3. 以下示例使用.msi 和.mst文件安装FortiClient，并创建一个名为“output”的日志文件。

```
msiexec.exe /i "FortiClient.msi" TRANSFORMS="FortiClient.mst" /log output.log
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

mac FortiClient安装及使用

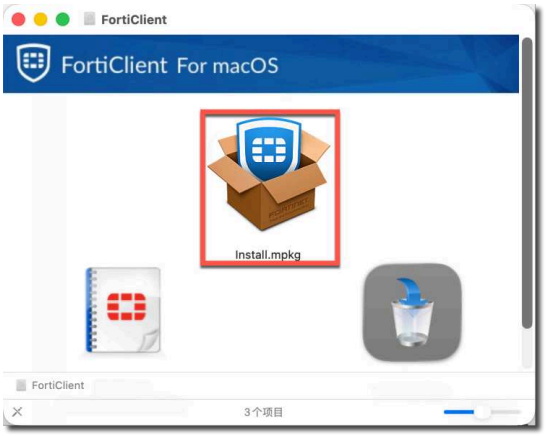
FortiClient完整版本安装

1. **下载FortiClient**

   参考：VPN技术→FortiClient VPN→FortiClient下载 ↗。

2. **安装FortiClient**

   双击FortiClientVPNSetup_7.4.3.1761_macosx.dmg（版本号仅举例使用，请根据实际下载的版本文件执行）安装，双击“Install.mpkg”。



点击“继续”。



点击继续并在弹出窗口中点击“同意”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击“继续”。

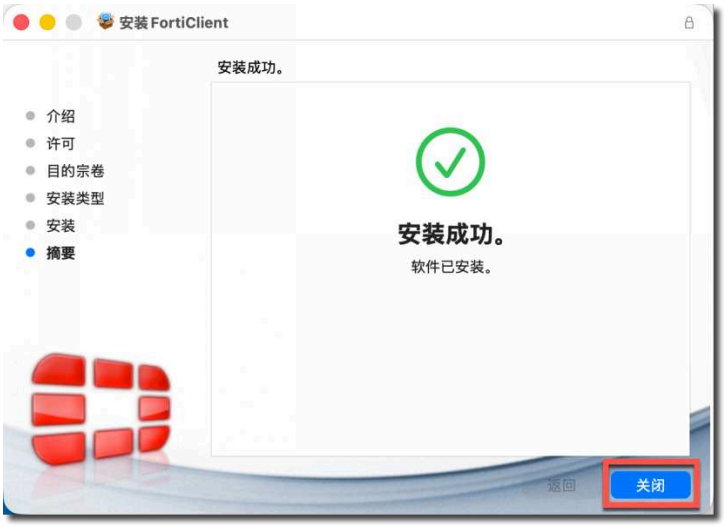


点击“安装”，在弹出窗口中输入系统用户名和密码授权安装。



安装完成后，关闭安装程序。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



在弹出的“添加VPN配置”窗口中点击允许。

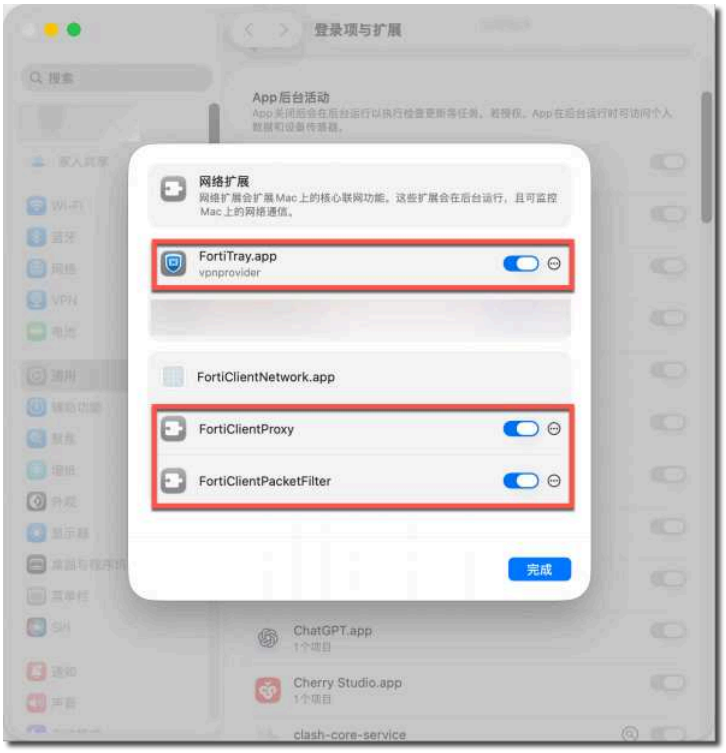


在弹出的网络扩展使用请求窗口中点击“打开系统设置”（点击其中一个即可）。



打开授权以下权限（需要系统账户验证）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

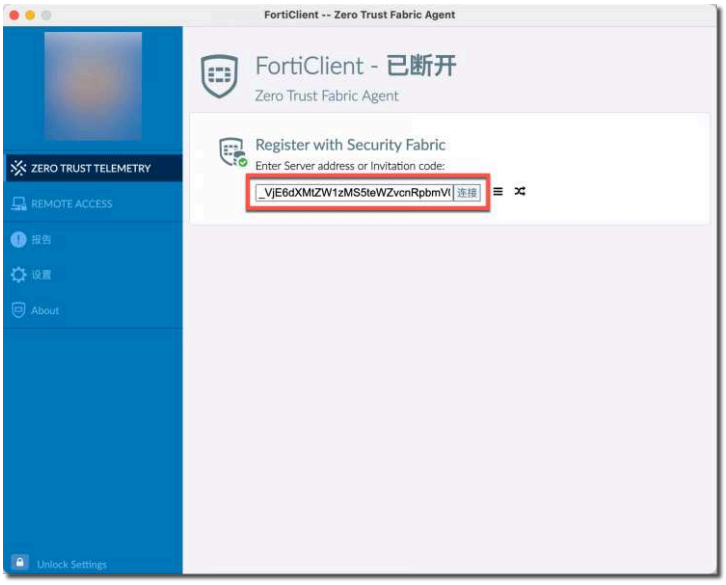


在弹出的“过滤网络内容”窗口中点击允许。



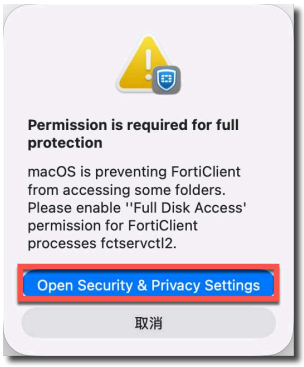
3.连接EMS

打开FortiClient输入EMS IP地址或邀请码，点击“连接”。

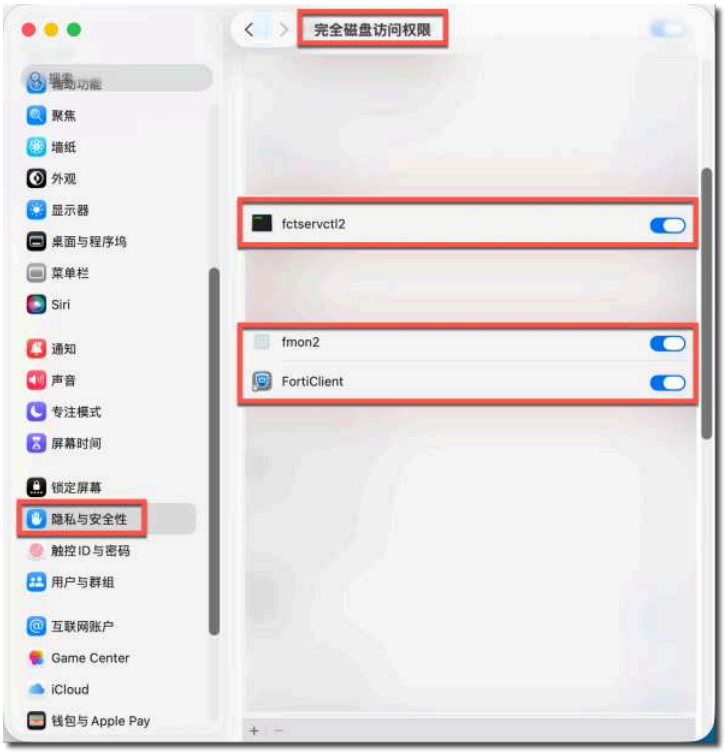


在弹出的磁盘权限窗口中点击“Open Security & Private Settings”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



在弹出的“隐私与安全性→完全磁盘访问权限”窗口中授予fctservctl2、fmon2、FortiClient的磁盘访问权限（需要系统账户验证）。

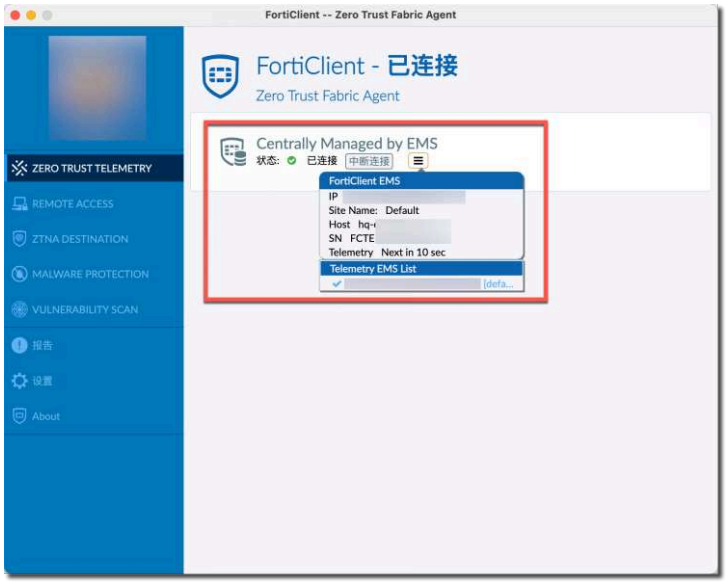


在弹出的“过滤网络内容”窗口中点击“允许”。



EMS连接成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiClient VPN Only版本安装

1. **下载FortiClient**

   参考：VPN技术→FortiClient VPN→FortiClient下载 ↗。

2. **安装FortiClient**

   双击FortiClientVPNSetup_7.4.3.1761_macosx.dmg（版本号仅举例使用，请根据实际下载的版本文件执行），双击“Install.mpkg”。



   点击“继续”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击继续并在弹出窗口中点击“同意”。



选择安装位置，并点击“继续”。

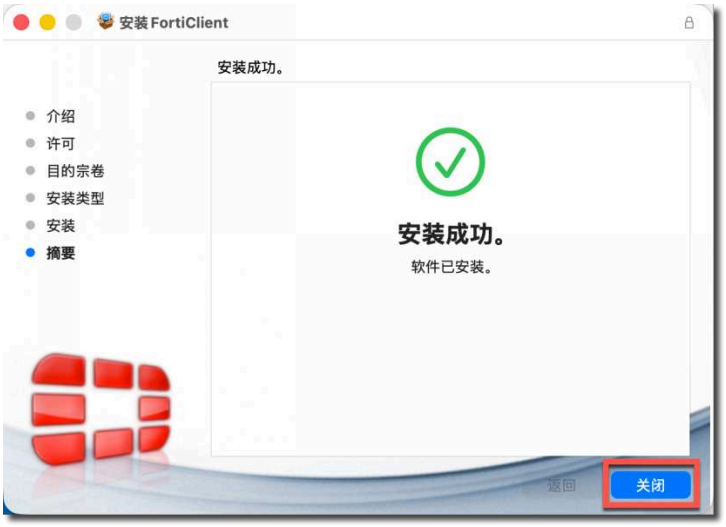


点击“安装”，在弹出窗口中输入系统用户名和密码授权安装。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



安装完成后，关闭安装程序。



在弹出的“添加VPN配置”窗口中点击允许。

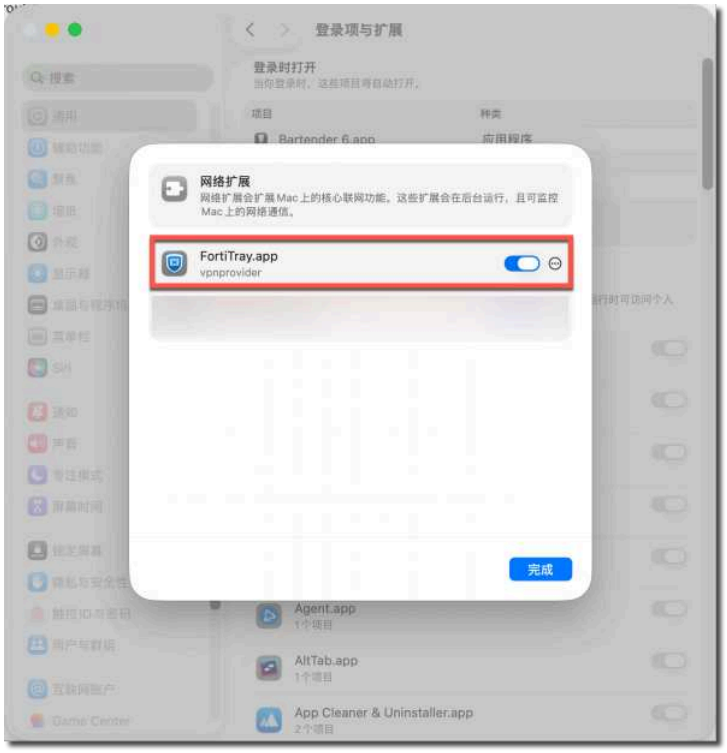


在弹出的网络扩展使用请求窗口中点击“打开系统设置”（点击其中一个即可）。

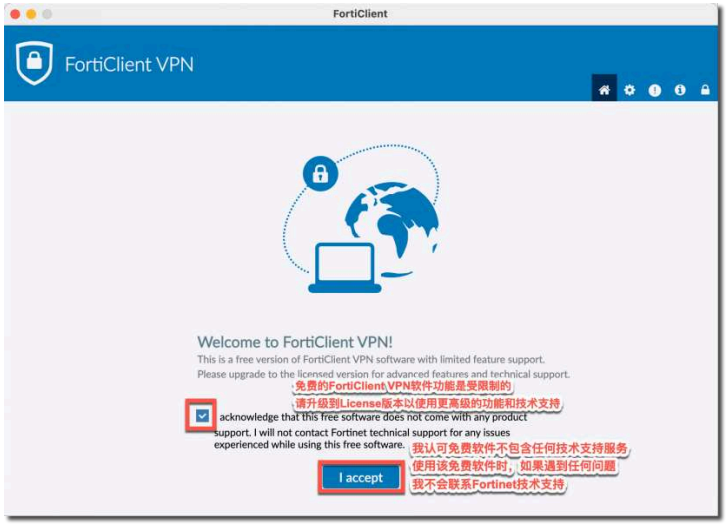


打开授权以下权限（需要系统账户验证）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

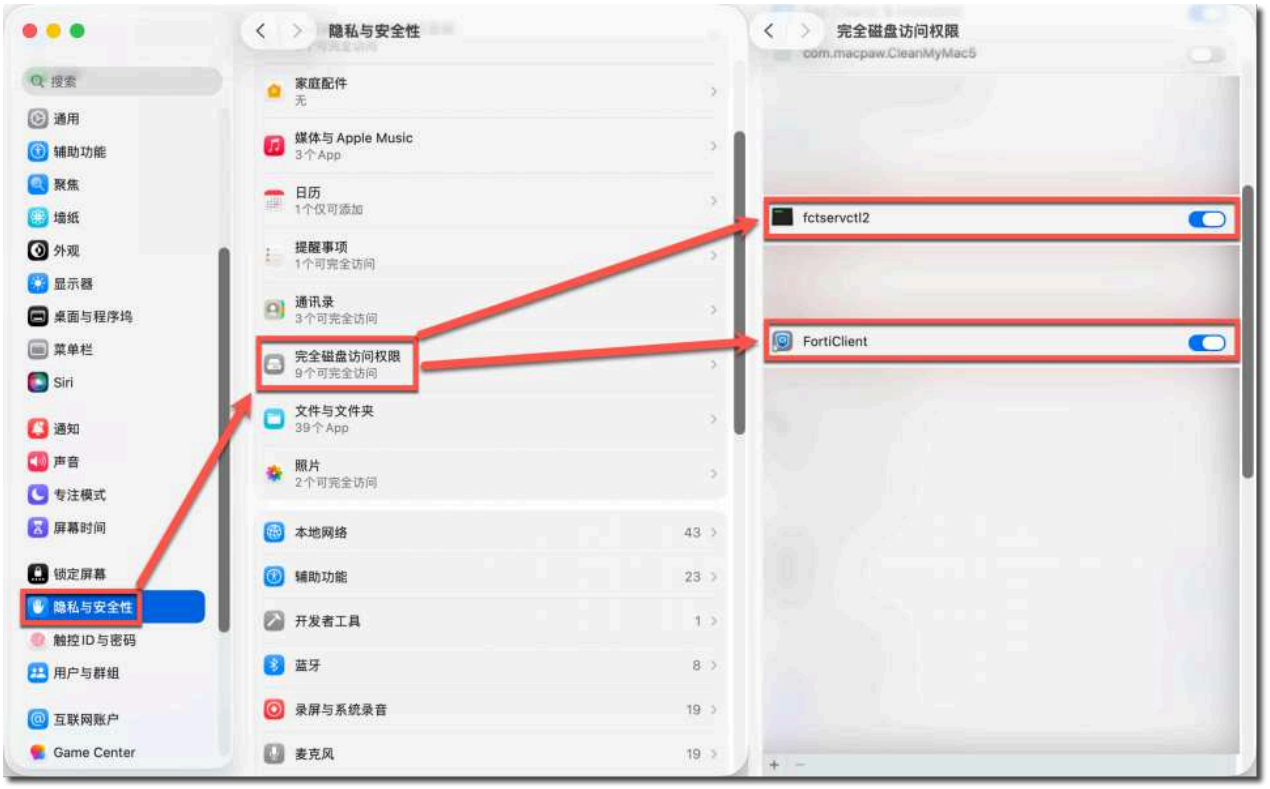


3. 打开FortiClient，勾选“I acknowledge that this free software...”，点击I accept。请注意免费的FortiClient不提供技术支持服务。



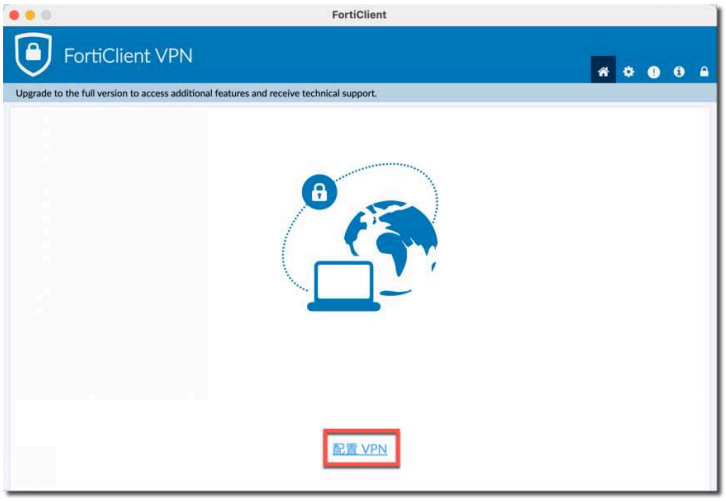
确认在“隐私与安全性→完全磁盘访问权限”窗口中授予FortiClient的磁盘访问权限（需要系统账户验证）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



设置SSLVPN

1. 点击“配置VPN”：



2. 配置SSLVPN：

   VPN：VPN类型

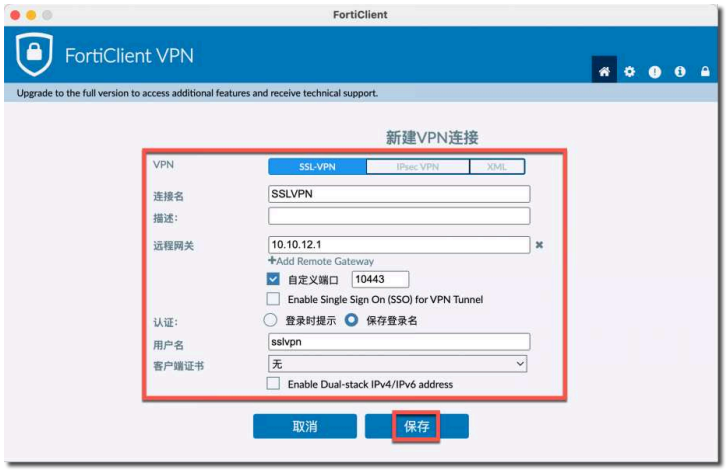
   连接名：VPN名称

   远程网关：FortiGate开启VPN服务的接口地址

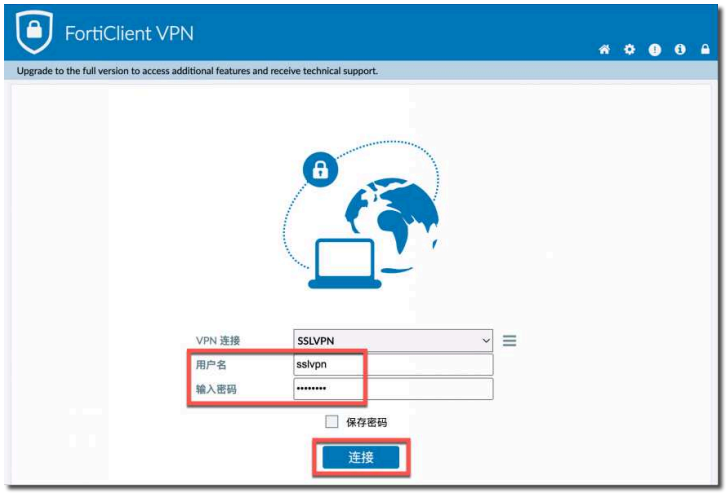
   自定义端口：SSLVPN服务的端口号

   用户名：VPN用户名称

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 配置完成后，输入用户名和密码，点击连接。



4. 如弹出如下查找本地网络设备的窗口，请点击允许。



5. 在弹出窗口中点击Continue，接受FortiGate的证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. SSLVPN连接成功。



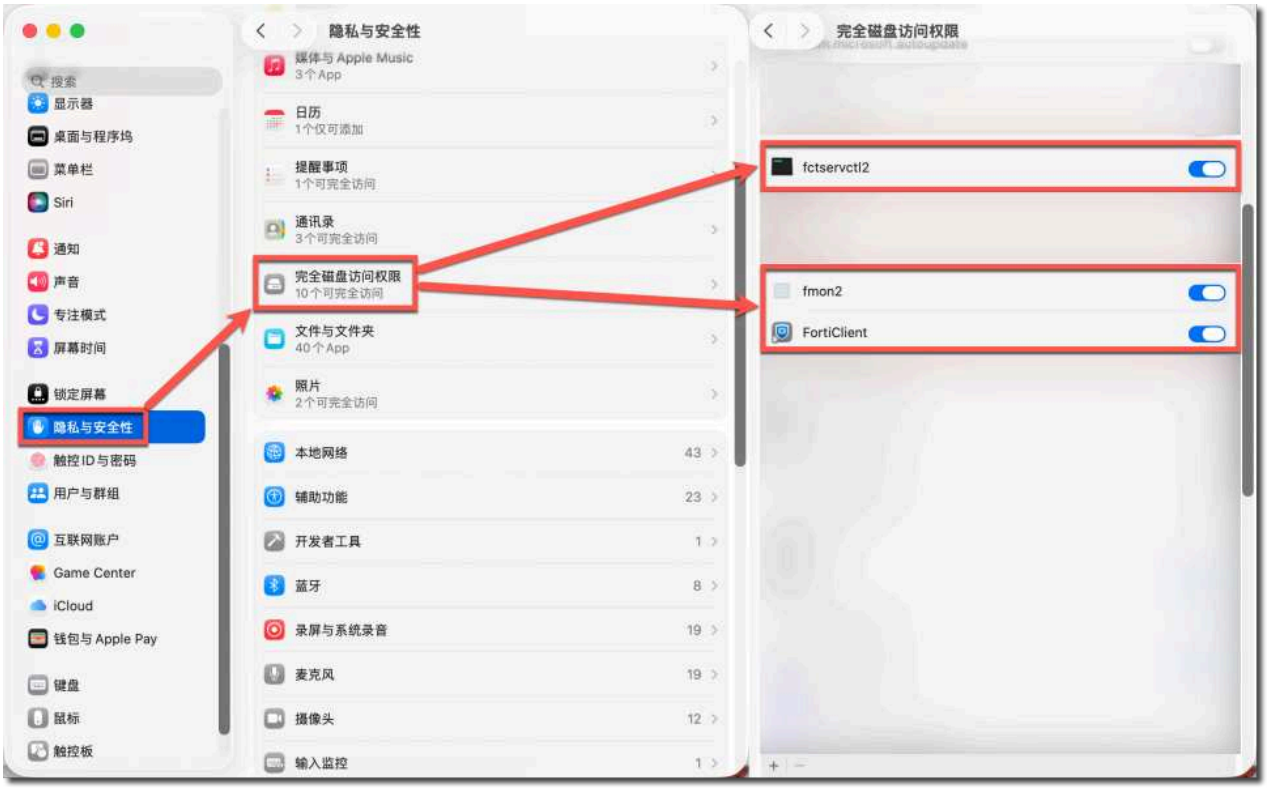
macOS权限要求

在macOS系统下，FortiClient需要允许一些系统权限才能正常使用。如果在安装过程中没有允许相关权限，可以通过如下方式允许FortiClient要求的相关权限。

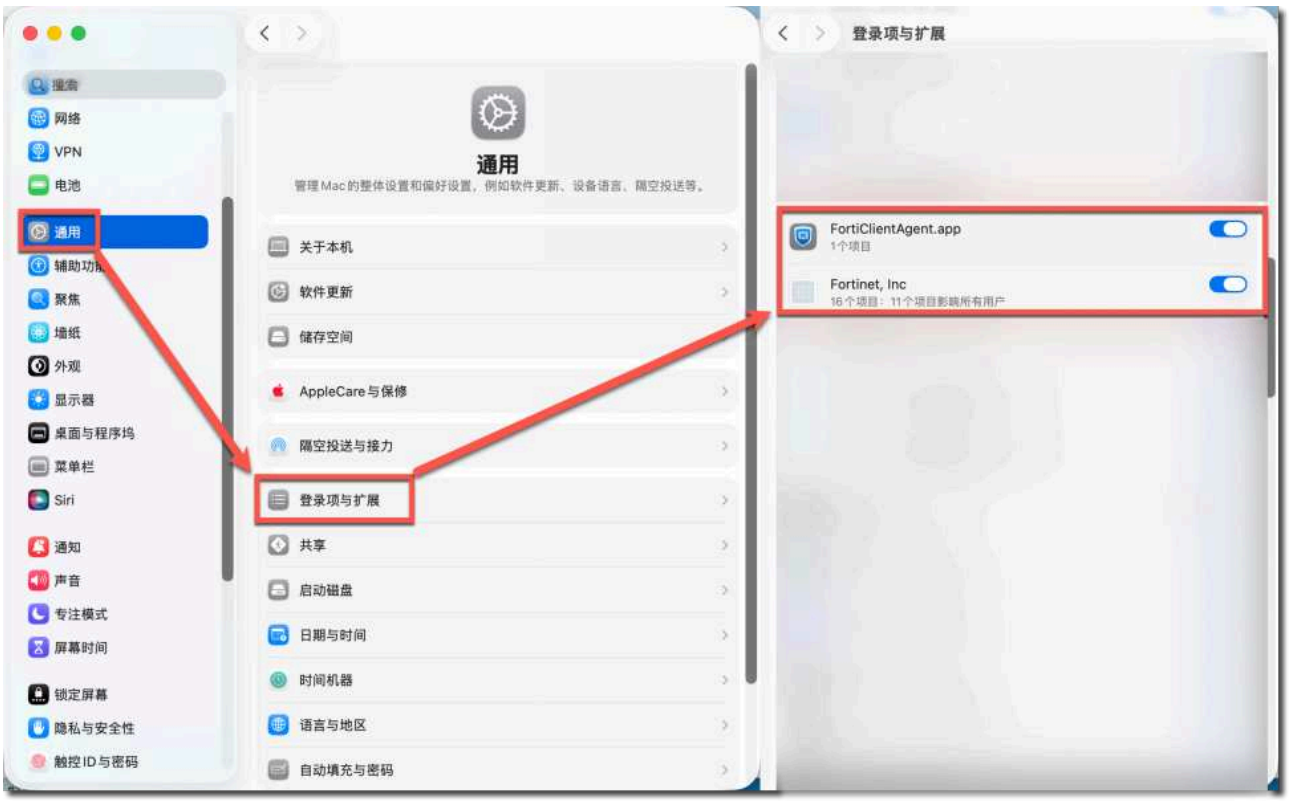
FortiClient完整版本

1. 设置→隐私与安全性→完全磁盘访问权限，开启fctservctl2、fmon2、FortiClient的权限。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 设置→通用→登录项与扩展，开启ForticlientAgent.app与Fortinet, Inc的权限。



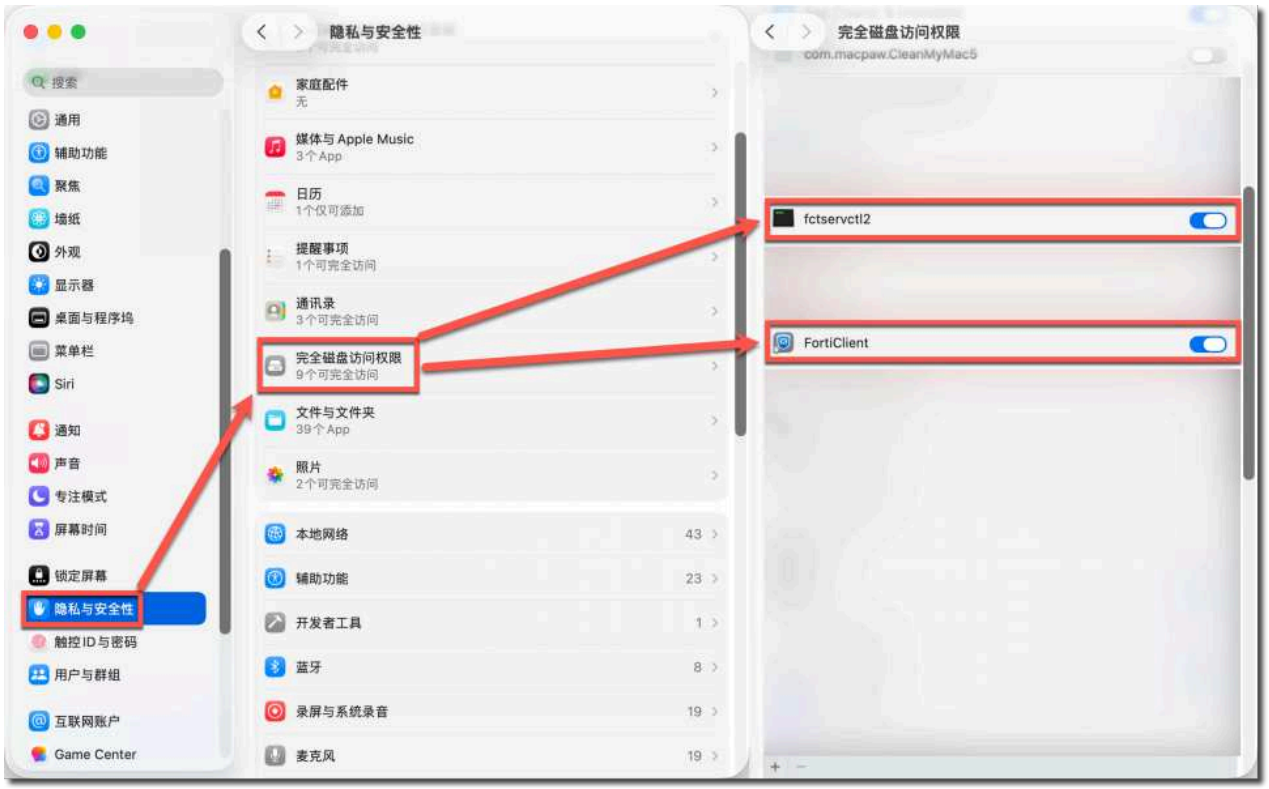
3. 设置→通用→登录项与扩展→拓展→按类别→网络扩展，开启FortiTray.app、FortiClientNetwork.app、FortiClientProxy、FortiClientPacketFilter的权限。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



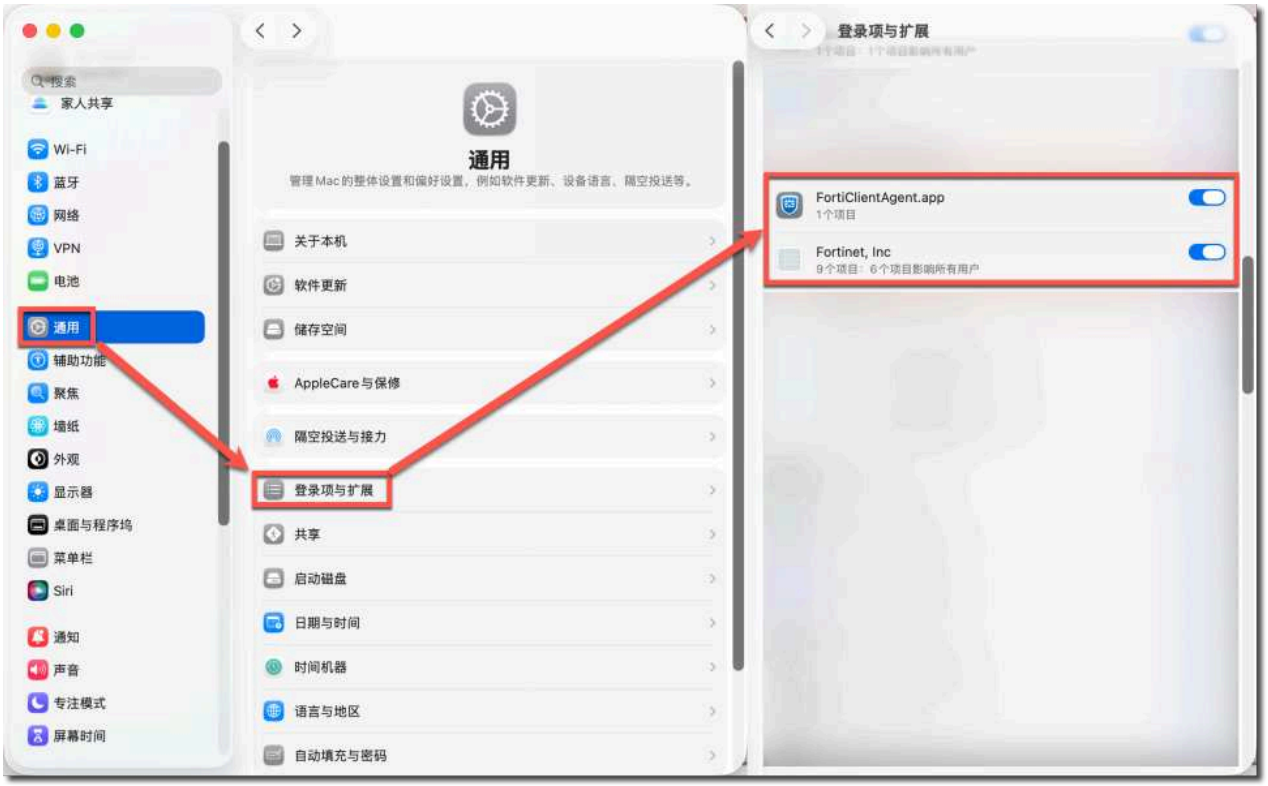
FortiClient VPN Only版本

1. 设置→隐私与安全性→完全磁盘访问权限，开启fctservctl2、FortiClient的权限。



2. 设置→通用→登录项与扩展，开启ForticlientAgent.app与Fortinet, Inc的权限。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 设置→通用→登录项与扩展→拓展→按类别→网络扩展，开启FortiTray.app的权限。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

iPhone FortiClient安装及使用

说明

FortiExplorer VPN是Fortinet公司在App Store中国区上线的SSL VPN连接客户端。它可以方便的下载到iPhone和iPad上，然后连接FortiGate SSL VPN网关，实现远程办公。

> **重要**
>
> 如果您的Apple ID属于非中国区，也可以从Apple Store直接下载FortiClient或FortiClient VPN使用。

配置文档请参考：FortiExplorer VPN使用指南v1.0 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Android FortiClient安装及使用

Android FortiClient完整版安装

1. **下载FortiClient：**

   参考：VPN技术→FortiClient VPN→FortiClient下载 ↗。

2. **安装FortiClient**

   可以通过邮件，QQ等方式将FortiClient发送给Android手机，点击安装（版本号仅举例使用，请根据实际下载的版本文件执行）。



   允许从QQ安装。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击继续安装。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



安装完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



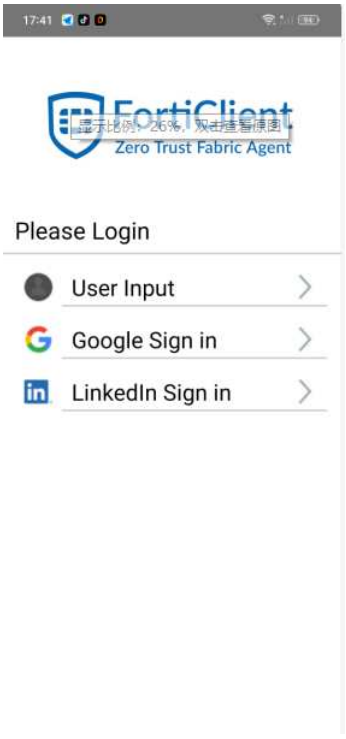
3. **连接EMS**

   打开FortiClient，允许所需的权限。

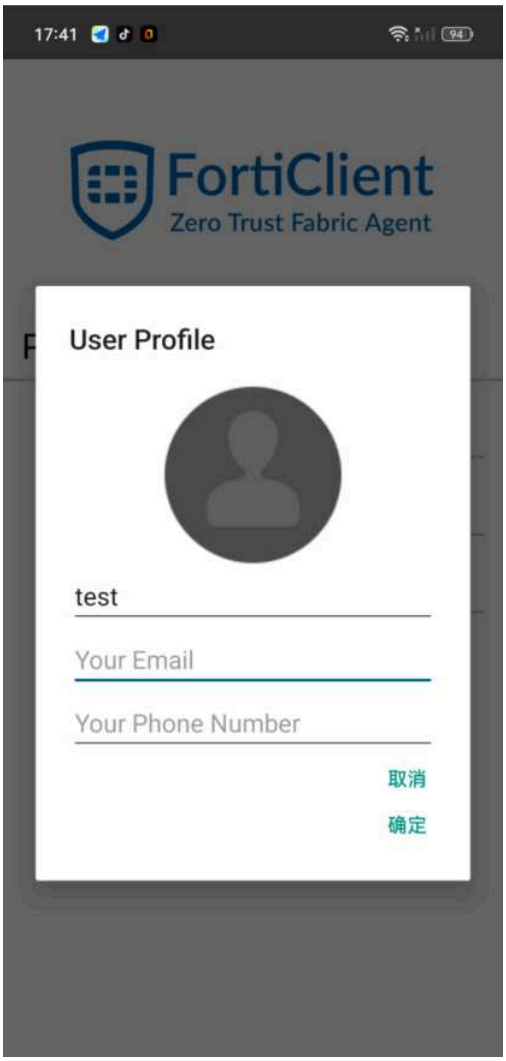
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击User Input，输入FortiClient名称。

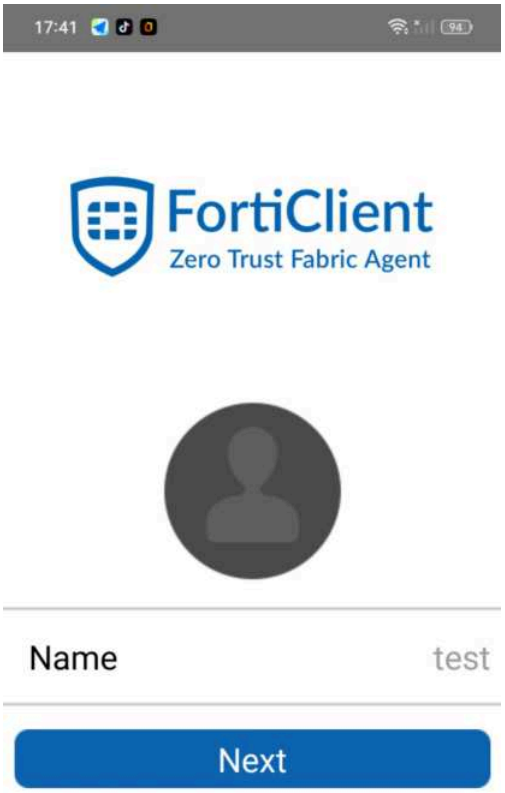


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



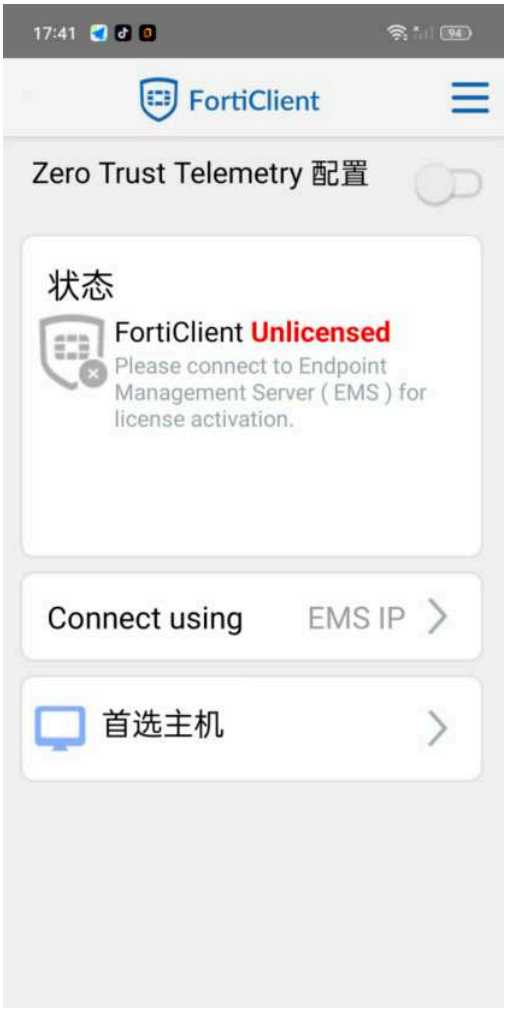
点击确定。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击“首选主机”，在“主机”中输入EMS的IP地址，端口默认是8013。



EMS已连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



免费版FortiClient VPN安装

1. **下载FortiClient**

   参考：VPN技术→FortiClient VPN→FortiClient下载 ↗。

2. 安装FortiClient

   通过邮件、QQ等方式将forticlient发送给手机，点击安装（版本号仅举例使用，请根据实际下载的版本文件执行）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



允许FortiClient从qq安装。



点击继续安装。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



安装成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



设置SSLVPN

1. **配置SSLVPN**

   输入SSLVPN名称，选择SSL VPN。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



在Servers中输入FortiGate的SSLVPN侦听的IP，端口中输入SSLVPN端口，输入用户名。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



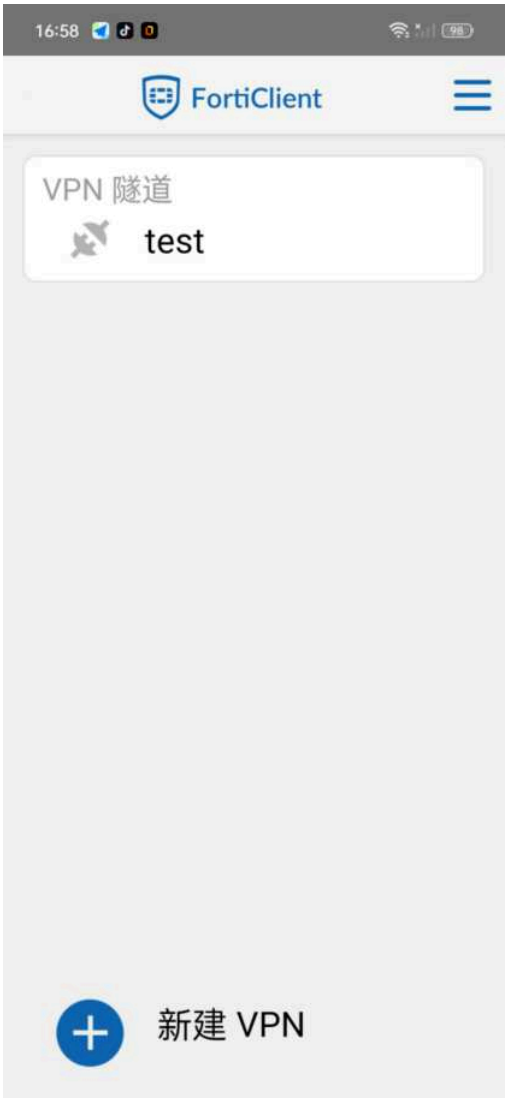
点击右上角三横杠，选择VPN，切换到VPN连接。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



配置完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **SSLVPN连接**

   选择SSLVPN名称test，点击“连接”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



证书由FortiGate自签发，选择“继续”。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

输入密码



连接成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiClient连接问题

本文介绍SSL VPN以特定百分比停止协商的常见错误原因与解决办法。

10%断开连接

这种情况下FortiClient通常会弹出“Unable to establish the VPN connection. The VPN server may be unreachable.”的提示信息，通常是由于网络连接问题引起的。

1. 请检查FortiClient到FortiGate的SSL VPN端口的网络联通性（不只是使用Ping测试，而是需要确保FortiClient和FortiGate之间TCP的SSL VPN端口是否正常连通，可以尝试使用客户端telnet SSL VPN服务器的IP和端口，或通过浏览器访问SSL VPN的HTTPS地址以确认联通性）。
2. 检查FortiClient是否配置了正确的SSL VPN IP和端口号，并启用了SSL VPN功能。



3. 检查FortiGate是否配置了服务器证书。
4. 检查FortiGate是否配置了以`ssl.<vdom_name>`为入接口的防火墙策略。
5. 检查FortiGate的VIP是否使用了SSL VPN的IP/端口。
6. 检查基于地理位置/源IP的限制设置，这些设置可能位于SSL VPN配置（参考“VPN技术→SSL VPN→SSL VPN源地址连接控制↗”章节）或local-in策略配置（参考“策略与对象→本地流量策略→ Local-in策略 ↗”章节）中。
7. 如果在FortiGate之前还有其他路由/NAT设备，请检查路由器的端口转发是否正确映射了SSL VPN的IP/端口。
8. 检查`ssl.<vdom_name>`（如ssl.root）接口是否为down状态，如果被认为关闭，请重新启用。

```bash
config system interface
    edit "ssl.root"
        set vdom "root"
        set status up
    next
end
```

9. 抓取FortiClient与FortiGate之间的SSL VPN报文

```bash
diagnose sniffer packet any ' host <source public IP address> and port <SSL VPN port> ' 4 0 l
```

   - 如果FortiGate响应了客户端请求，当TCP三次握手未完成或客户端在TCP三次握手完成后reset连接时，连接将终止，FortiClient将显示连接在10%停止。
   - 如果流量到达FortiGate，但FortiGate未做出响应，可以使用debug flow来判断是否匹配了拒绝策略，或因未匹配任何允许策略而被隐式拒绝。

```bash
diagnose debug disable
diagnose debug reset
diagnose debug flow show iprope en
diagnose debug flow show func en
diagnose debug flow filter addr <source public ip addr>
diagnose debug flow filter port <SSL VPN port>
diagnose debug flow trace start 300
diagnose debug enable
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

31%断开连接

通常FortiClient会弹出“Unable to establish the VPN connection. The VPN server may be unreachable or your identity certificate is not trusted. (-5029)”的提示信息。这是由于TLS版本协商失败导致，请检查FortiGate配置的SSL VPN TLS版本是否被FortiClient所在的PC使用。

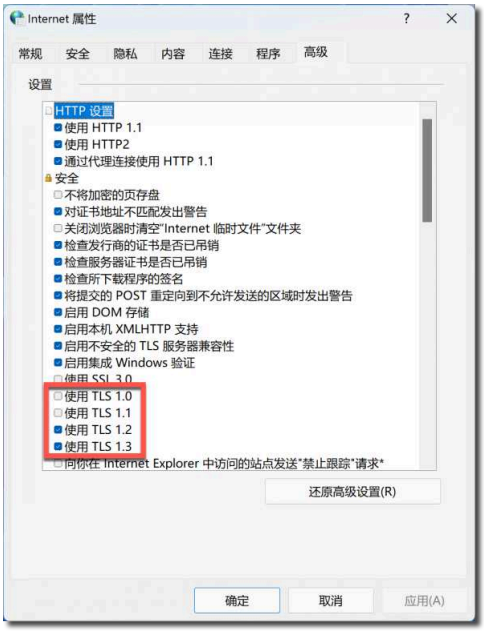
1. 检查FortiGate配置的SSL VPN TLS版本，如下所示，SSL VPN使用的TLS版本最大为1.3（ssl-max-proto-ver），最小为1.2（ssl-min-proto-ver），也就是只接受TLS 1.2 ~ 1.3的版本（如果开启了DTLS，需要参考dtls-max-proto-ver和dtls-min-proto-ver）：

```bash
FortiGate # config vpn ssl settings
FortiGate (settings) # show full-configuration | grep proto
    set ssl-max-proto-ver tls1-3
    set ssl-min-proto-ver tls1-2
    set dtls-max-proto-ver dtls1-2
    set dtls-min-proto-ver dtls1-0
```

2. 可以根据实际情况修改FortiGate的TLS设置：

```bash
FortiGate # config vpn ssl setting
FortiGate (settings) # set ssl-max-proto-ver ?
tls1-0    TLS version 1.0.
tls1-1    TLS version 1.1.
tls1-2    TLS version 1.2.
tls1-3    TLS version 1.3.

FortiGate (settings) # set ssl-min-proto-ver ?
tls1-0 TLS version 1.0.
tls1-1 TLS version 1.1.
tls1-2 TLS version 1.2.
tls1-3 TLS version 1.3.
```

3. 检查FortiClient所在PC的TLS版本设置，这里以Windows为例，打开“Internet选项”，进入高级选项卡，在“安全”部分中找到TLS版本相关选项，如下图所示，选取的TLS版本为1.2和1.3，可根据FortiGate端的配置进行修改。



40%断开连接

1. 可能是由于FortiClient在连接时弹出了是否希望继续使用非受信任的TLS/SSL证书的弹窗，但用户未选择或选择了取消（有时候这个弹窗没有弹出，需要在任务栏点开）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 与31%中断类似，FortiClient会弹出“Unable to establish the VPN connection. The VPN server may be unreachable or your identity certificate is not trusted. (-5029)”的提示信息，这由TLS版本协商失败导致。可参考31%中断的解决方法。
3. 可能是因为SSL VPN使用的服务器证书已过期。请更换服务器证书，或选择“Fortinet_Factory”证书作为Workaround。
4. 如果使用SAML认证，请确保从IDP下载了正确的证书，并将其导入到SP（FortiGate）中。
5. 如果出现“The VPN server may be unreachable. (-5)' errors”错误，可能是由于FortiClient所在PC安装的某些安全应用阻断了FortiClient与FortiGate的SSL协商，或是外部安全设备进行了阻断。

42%或43%断开连接

通常是用户权限问题（sslvpn_login_permission_denied）。

- 对于本地用户，可能是用户名/密码输入错误。
- 对于远程用户，在 `diagnose debug application sslvpn -1` 和 `diagnose debug application fnbamd -1` 调试中可能有以下错误：“find_matched_usr_grps-Failed group matching”。以下debug信息可用于验证用户是否属于正确的LDAP用户组，将用户添加到正确的组中可解决此问题。

```
diagnose debug application sslvpn -1
diagnose debug application fnbamd -1
diagnose debug enable
```

45%断开连接

1. 对于本地用户，可能是用户名/密码输入错误。
2. 对于远程认证（如LDAP）用户，可能的原因包括：FortiGate无法连接到远程服务器、远程服务器返回身份验证失败，或LDAPS的加密连接失败。举例：如果连接在45%停止并显示错误“ldap connection timeout”，可以尝试调整LDAP认证超时设置。

```bash
config system global
    set ldapconntimeout 3000
end
```

3. 远程认证也可以参考“48%断开连接”中SAML认证相关的解决方法。

48%断开连接

1. 可能是由于 `ssl.root` （ `ssl.<vdom>` ）接口被手动禁用（admin down），但在 `config vpn ssl settings` 配置中 `set status enable` ，请检查SSL VPN接口和SSL VPN功能都处于开启状态。
2. 可能是由于双因子（two-factor）认证失败导致断开，检查双因子认证的配置与Token信息输入是否正确。
3. 如果FortiClient弹出提示“Credential or SSL VPN configuration is wrong (-7200)”，在FortiClient连接过程中通过Debug信息来判断问题原因：
    - 如果Debug信息中提示 `error:0A000126:SSL routines::unexpected eof while reading` 。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
diagnose debug application sslvpn -1
diagnose debug application fnbamd -1
diagnose debug enable

[2612:root:1b]deconstruct_session_id:716 decode session id ok, user=[guest], group=[],authserver=[],portal=
[full-access],host[10.200.20.10],realm=[],csrf_token=
[D3D4129C5AB9CB25CDCE01CCF8E40],idx=0,auth=1,sid=2d772154,login=1686904099,access=1686904099,saml_logout_url=no,
pip=no,grp_info=[4xAcoJ],rmt_grp_info=[]
[2612:root:1b]rmt_web_auth_info_parser_common:557 authentication required
[2612:root:1b]rmt_web_access_check:776 access failed, uri=[/remote/logout],ret=4103,
[2612:root:1b]SSL state:fatal decode error (10.200.20.10)
[2612:root:0]ap_read,105, error=1, errno=0 ssl 0×7f3bb1bb6000 Success. error:0A000126:SSL routines::unexpected
eof while reading
//[2612:root:1b]sslvpn_read_request_common,684, ret=-1 error=-1, sconn=0×7f3bb2854800.//
[2612:root:1b]Destroy sconn 0×7f3bb2854800, connSize=0. (root)
```

- 首先确认FortiClient使用的用户名和密码完全正确。
- 也可能是由于PC的Internet选项中的安全等级设置为“高”导致，通过调整Internet选项中的安全等级为“中-高”或“中”可以修复此问题。

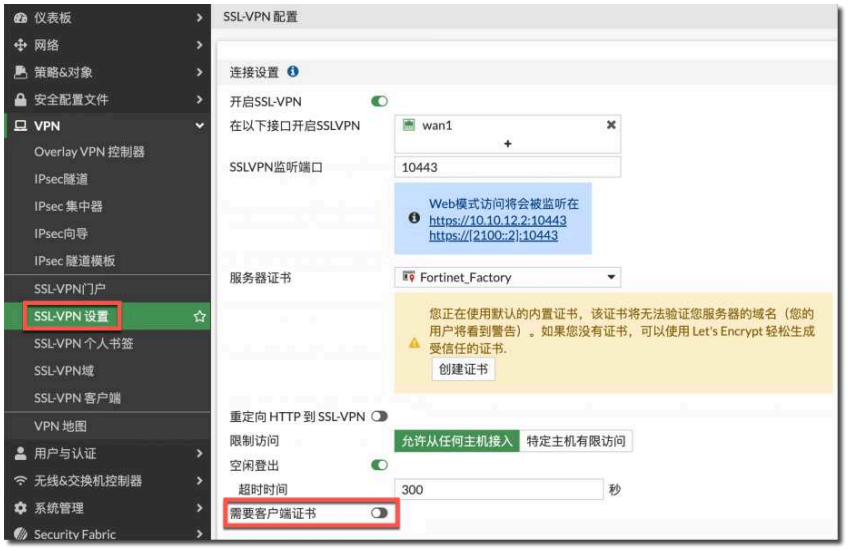


- 如果Debug信息中提示`failed [sslvpn_login_cert_checked_error]`。

```bash
diagnose debug application sslvpn -1
diagnose debug enable

2023-11-02 14:15:59 [11178:root:34]req: /remote/logincheck
2023-11-02 14:15:59 [11178:root:34]rmt_web_auth_info_parser_common:470 no session id in auth info
2023-11-02 14:15:59 [11178:root:34]rmt_web_access_check:723 access failed, uri=[/remote/logincheck],ret=4103,
2023-11-02 14:15:59 [11178:root:34]User Agent: FortiSSLVPN (Windows NT; SV1 [SV{v=02.01; f=07;}])
2023-11-02 14:15:59 [11178:root:34]rmt_logincheck_cb_handler:1189 user 'test15' has a matched local entry.
//2023-11-02 14:15:59 [11178:root:34]login_failed:384 user[test15],auth_type=32768 failed
[sslvpn_login_cert_checked_error]//
2023-11-02 14:15:59 [11178:root:0]dump_one_blocklist:84 status=1;host=15.15.15.15;fails=1;logintime=1698730139
```

- 这可能是由于误开启了FortiGate SSL VPN的“需要客户端证书”功能，而实际不需要证书认证客户端证书。需要手动关闭该功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config vpn ssl settings
    set reqclientcert disable
end
```

- 如果FortiGate使用了LDAP作为SSL VPN认证，请参考用户与认证→LDAP认证→LDAP常见错误代码↗章节排查。

4. 如果出现“Permission denied. (-455)”错误，检查用户是否包含在“SSL VPN认证/门户配置”中的用户组中。

5. 使用SAML认证时，FortiClient会弹出登录窗口，此登录窗口存在远程认证超时时间。如果在此时间内没有完成认证（例如SAML认证同时开启了双因子认证，默认的计时器时间可能不够），FortiClient将在48%时断开连接。`remoteauthtimeout`默认为5s，可通过以下CLI命令将其适当增加。

```bash
config system global
    set remoteauthtimeout 120    ←——FortiGate等待远程身份验证服务器响应的秒数，1~480s，默认5s
end
```

- 请注意`remoteauthtimeout`的设置时间并非SSL VPN在关闭连接前实际等待的时间，实际等待时间 = 10 * remoteauthtimeout + 30s。
- 如果同时开启了双因子认证，双因子认证也有一个认证超时时间`two-factor-email-expiry`。

```bash
config system global
    set two-factor-email-expiry 60    ←——FortiGate等待双因子认证的超时秒数，30~300s，默认60s
end
```

- 在SSL VPN同时使用SAML + 双因子认证时，SSL VPN在关闭连接前实际等待的时间以10 × remoteauthtimeout + 30s为准。即使`two-factor-email-expiry`更长。
- 示例：如果将`two-factor-email-expiry`设置为240s，则`remoteauthtimeout`必须大于或等于21s。 240 = 10 × remoteauthtimeout (21) + 30。
- 对于使用Azure SAML的SSL VPN身份验证，`remoteauthtimeout`时间将翻倍。例如，当设置为30s时，实际的等待时间将变为30 × 2 × 10 + 30 = 630s 。

6. 如果出现“Host check requirement error (-455)”错误。如果SSL VPN没有开启主机检查（host check），请检查防火墙是否发生了“sslvpnd”进程崩溃。

```
diagnose debug crashlog read
```

7. 检查SSL VPN是否开启了MAC地址检查，如果开启了MAC地址检查，请检查连接的FortiClient所在的PC的MAC地址是否在FortiGate配置的允许列表中。

```bash
config vpn ssl web portal
    edit <portal_name>
        set mac-addr-check enable
         config mac-addr-check-rule
             edit <rule_name>
                 set mac-addr-list <address> [address]
                 set mac-addr-mask <mask between 1-48>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            next
        end
        set mac-addr-action {allow | deny}
    next
end
```

80%断开连接

1. 检查FortiGate的SSL VPN中用于匹配用户的门户（portal，如full-aacess）是否开启了隧道模式（tunnel mode）。
2. 如果弹出提示“Unable to log on to the server. Your username or password may not be configured properly for this connection. (-14)”，检查FortiClient输入的用户名和密码是否与FortiGate上配置的一致。
3. 在FortiGate检查用户和用户组的关系，可能是用户未加入正确的用户组。
4. 检查是否配置了对应用户/用户组的防火墙策略。
5. 检查FortiGate中SSL VPN设置的“认证/门户配置（Authentication/Portal Mapping）”配置中的用户/用户组是否与防火墙策略中SSL VPN相关策略中引用的用户/用户组完全一致，如果不一致，FortiClient会出现以下提示（英文系统下会提示“Unable to log on to the server. Your username or password may not be configured properly for this connection. (-14)”）：



重要

- 如果SSL VPN设置的“认证/门户配置”选择了用户组，那么防火墙策略中也要引用用户组，不要引用该用户组中的用户成员。
- 如果SSL VPN设置的“认证/门户配置”选择了用户，那么防火墙策略中也要引用用户，不要引用该用户所属的用户组。
- 如果有多条SSL VPN相关的防火墙策略，无论策略的顺序如何，只要有策略中配置了“认证/门户配置”中不一致的用户/用户组，都可能导致这个问题的出现。
- 如果不按照上述规则配置，会出现FortiClient连接SSL VPN时，无法匹配自定义配置的“认证/门户配置（Authentication/Portal Mapping）”，而匹配到默认的Portal Mapping时：
  - 如果默认的Portal Mapping为“web-access”（只开启了Web模式的访问，没有开启Tunnel模式的访问），那么就会连接失败。
  - 即使默认的Portal Mapping选择了开启Tunnel模式的Portal，FortiClient可以成功连接SSL VPN，但也有可能匹配到非用户预期的Portal，所以还是要按照上述规则进行配置。

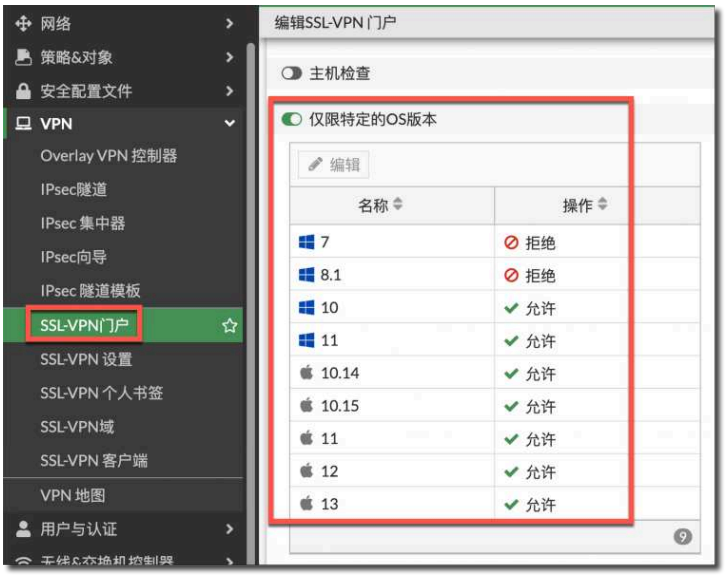


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

6. 检查用户/用户组是否匹配了正确的门户（Portal）。

7. 如果在SSL VPN设置中为用户/用户组配置了域（Realm），请检查FortiClient是否连接了正确的域（Realm）。

8. 如果FortiGate上用户/用户组所属的门户（Portal）开启了OS版本检查，请确认客户端的OS类型与版本是否满足FortiGate上配置。




```bash
config vpn ssl web portal
    edit "full-access"
        set os-check enable
        config os-check-list "windows-7"
            set action deny
        end
        config os-check-list "windows-8.1"
            set action deny
        end
        config os-check-list "windows-10"
        end
        config os-check-list "windows-11"
        end
        config os-check-list "macos-mojave-10.14"
        end
        config os-check-list "macos-catalina-10.15"
        end
        config os-check-list "macos-bigsur-11"
        end
        config os-check-list "macos-monterey-12"
        end
        config os-check-list "macos-ventura-13"
        end
    next
end
```

9. 如果FortiGate上用户/用户组所属的门户（Portal）开启了主机检查，请确认客户端的主机是否通过了AV/防火墙/MAC地址检查。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config vpn ssl web portal
    edit "full-access"
        set host-check av
        set mac-addr-check enable
        config mac-addr-check-rule
            edit "BingBai"
                set mac-addr-list 0c:37:96:06:d7:5d
            next
        end
    next
end
```

.0. FortiGate固件降级可能会导致SSL-VPN门户（portal）设置初始化，因此请尽量避免版本降级，或确认降级后portal配置是否保留。

89%断开连接

1. 在此阶段，FortiTray.exe将尝试向位于`%localappdata%\FortiClient`目录下的`fortisslvpn_xml.txt`文件写入数据。

2. 如果无法访问`%localappdata%\FortiClient`，将显示错误代码`-5052`。

3. 如果`%localappdata%\FortiClient`目录可访问，但无法修改`fortisslvpn_xml.txt`文件，会出现错误代码`-5053`。

4. 在CMD中运行如下命令可以显示为何`fortitray.exe`无法写入`fortisslvpn_xml.txt`文件。

```bash
notepad %localappdata%\FortiClient\fortisslvpn_xml.txt
```

98%断开连接

此阶段断开连接标识身份验证已完成，但无法建立隧道。这种情况下通常是由于FortiClient所在主机的OS问题导致。

1. 尝试在主机上重装FortiClient程序（先卸载现有FortiClient程序，根据提示信息重启后再重装）。
2. 检查FortiClient、FortiGate、EMS Server之间的版本兼容性。请参考“VPN技术→FortiClient VPN→系统兼容性列表↗”章节。
3. 可能由网络问题引起，例如IPv6到IPv4的连接（不支持）、高网络延迟、被阻塞的流量。

其他百分比断开连接

请参考FortiClient 维护手册↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiClient排错与卸载

FortiClient排错

FortiClient排错请参考链接：https://handbook.fortinet.com.cn/files/Forticlient_maintenance_manual.pdf ↗

FortiClient卸载

FortiClient卸载请参考链接：https://handbook.fortinet.com.cn/files/Forticlient卸载指南.pdf ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

iOS原生客户端接入IPSec（IKEv1）

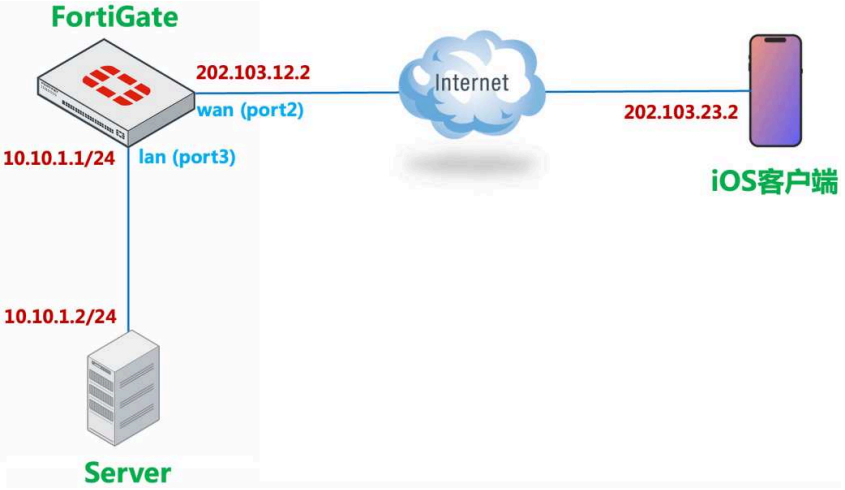
重要

本文基于iOS 16.3编写。

网络需求

通过iOS原生客户端（IKEv1）连接FortiGate的IPSec，并访问VPN内部资源。

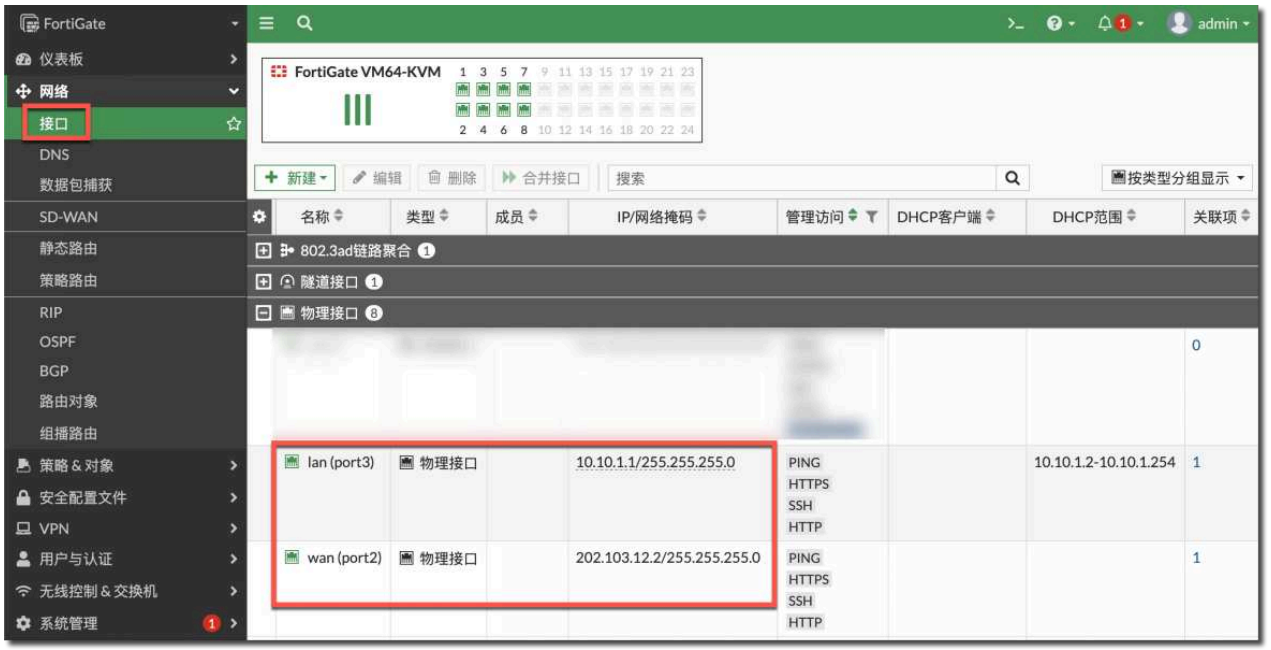
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。



2. 创建本地VPN用户和用户组，参考用户与认证→本地用户和用户组↗章节（如需使用远程认证，请参考用户与认证→LDAP认证→LDAP认证配置与排错↗或用户与认证→Radius认证→Radius认证配置与排错↗章节）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config user local
    edit "vpn_user"
        set type password
        set passwd xxxxxxxx
    next
end
```




```
config user group
    edit "VPN"
        set member "vpn_user"
    next
end
```

3. 进入FortiGate的VPN→IPSec隧道页面，点击新建按钮，新建IPSec隧道。



4. 填写VPN名称，模版选择远程拨号，远程设备选择Native，然后选择iOS Native，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 配置流入接口为wan口，填入预共享密钥，选择VPN用户组，点击下一步。



6. 配置本地接口（VPN客户端要访问的网络所属出接口），本地地址新建并选择内网的VPN网段地址对象，分配客户端地址范围（注意不要和现有网段冲突），DNS可选择系统DNS或指定DNS，默认开启隧道分割，只有本地地址中的网段会被客户端转发至VPN隧道（关闭隧道分割的话，客户端会将自身发起的所有流量转发至VPN隧道）。点击下一步。

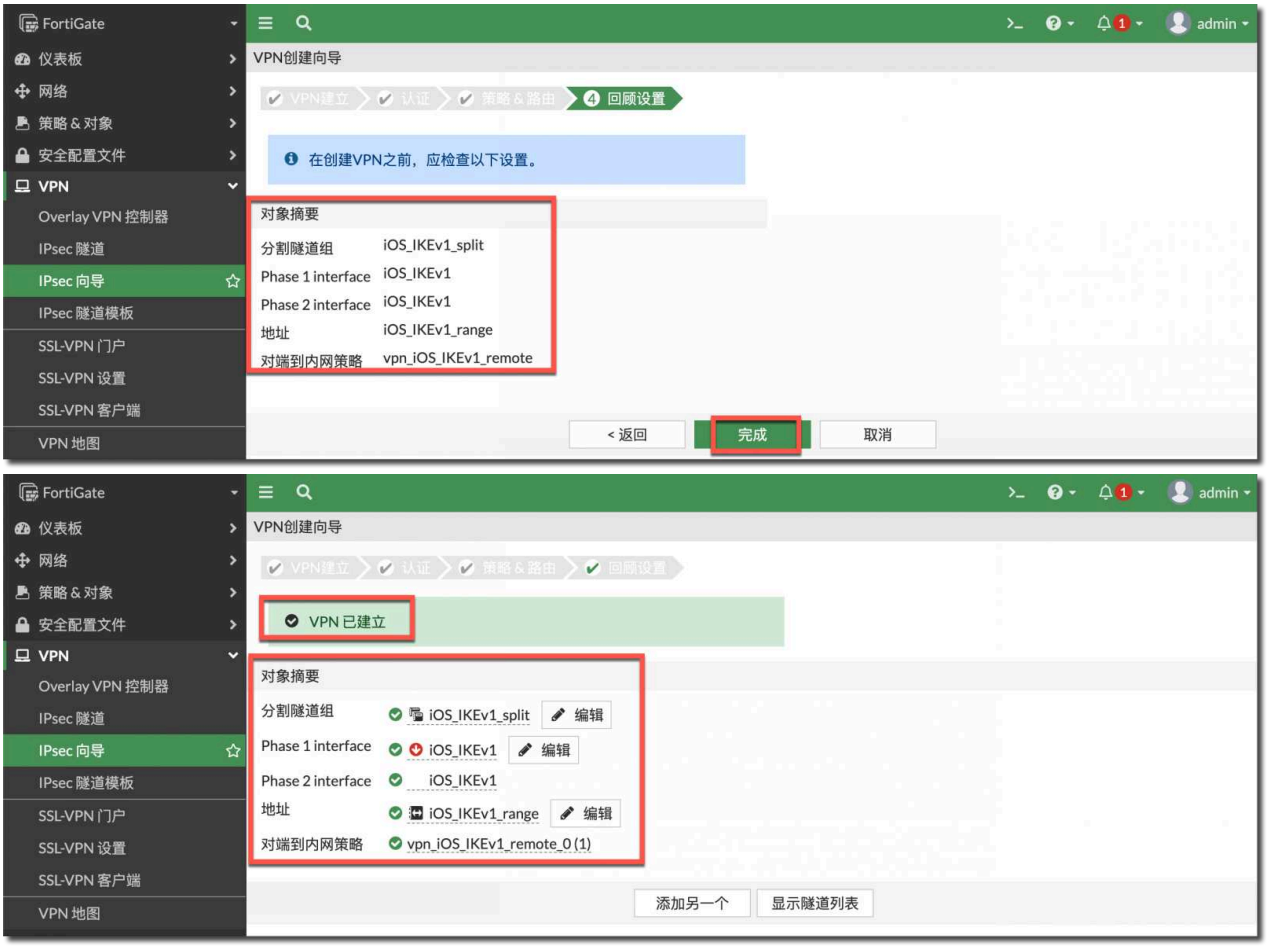


重要

如果开启了隧道分割，本地地址不要填写为0.0.0.0/0，否则会导致客户端连接失败。

7. 检查配置无误后，点击完成按钮，完成隧道建立。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 向导配置完成后，FortiGate会自动创建IPSec一阶段和二阶段、内网地址对象、客户端到内网的防火墙访问策略，对应的CLI如下：

```
第一阶段和第二阶段VPN配置：
config vpn ipsec phase1-interface
    edit "iOS_IKEv1"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256 aes256-md5 aes256-sha1
        set comments "VPN: iOS_IKEv1 (Created by VPN wizard)"
        set dhgrp 14 5 2
        set wizard-type dialup-ios
        set xauthtype auto
        set authusrgrp "VPN"
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100
        set dns-mode auto
        set ipv4-split-include "iOS_IKEv1_split"
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "iOS_IKEv1"
        set phase1name "iOS_IKEv1"
        set proposal aes256-sha256 aes256-md5 aes256-sha1
        set pfs disable
        set keepalive enable
        set comments "VPN: iOS_IKEv1 (Created by VPN wizard)"
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
地址和地址组：
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "iOS_IKEv1_range"
        set type iprange
        set comment "VPN: iOS_IKEv1 (Created by VPN wizard)"
        set start-ip 10.10.100.1
        set end-ip 10.10.100.100
    next
end

config firewall addrgrp
    edit "iOS_IKEv1_split"
        set member "LAN_10.10.1.0/24"
        set comment "VPN: iOS_IKEv1 (Created by VPN wizard)"
    next
end
```

```
允许客户端访问内网VPN资源的防火墙策略：
config firewall policy
    edit 1
        set name "vpn_iOS_IKEv1_remote_0"
        set srcintf "iOS_IKEv1"
        set dstintf "port3"
        set action accept
        set srcaddr "iOS_IKEv1_range"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
        set nat enable
        set comments "VPN: iOS_IKEv1 (Created by VPN wizard)"
    next
end
```

客户端配置

1. 打开设置→VPN，点击最下方的“添加VPN配置…”按钮。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 类型选择IPSec，填写VPN名称、服务器IP、用户名、用户密码、预共享密钥，其他不填写（如果想要使用群组名称，请在FortiGate侧配置），点击完成按钮。



3. 点击创建的VPN连接，确保该连接被选中（连接前有一个✅）。



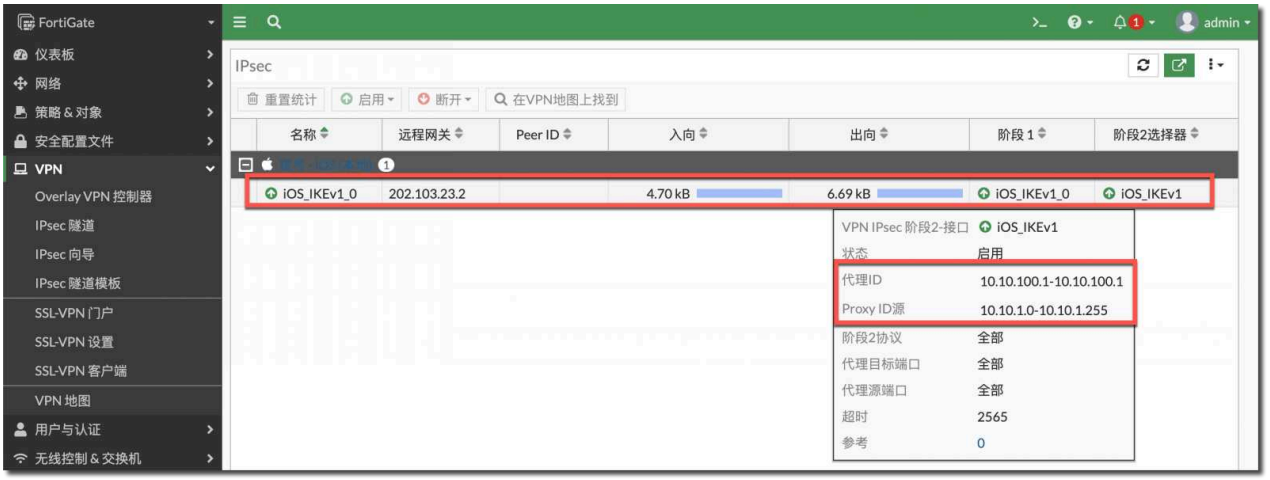
结果验证

1. 在客户端点击连接按钮，查看连接状态，点击VPN连接右侧的信息按钮，可以看到连接的具体信息，获取的IP为FortiGate配置的网段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: iOS_IKEv1_0
version: 1
interface: port2 4
addr: 202.103.12.2:4500 -> 202.103.23.2:60417
tun_id: 10.10.100.1/::10.0.0.4
remote_location: 0.0.0.0
network-id: 0
created: 1144s ago
xauth-user: vpn_user
2FA: no
assigned IPv4 address: 10.10.100.1/255.255.255.255
nat: peer
IKE SA: created 1/1  established 1/1  time 60/60/60 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms
  id/spi: 2 1ab45dd9b8ad53a1/229987eaaab4142e
  direction: responder
  status: established 1144-1144s ago = 60ms
  proposal: aes256-sha256
  key: 26d033d72c0d55fe-6652a7159cf151dd-1113c3dd29c29cf9-74dabccc059f96ac
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

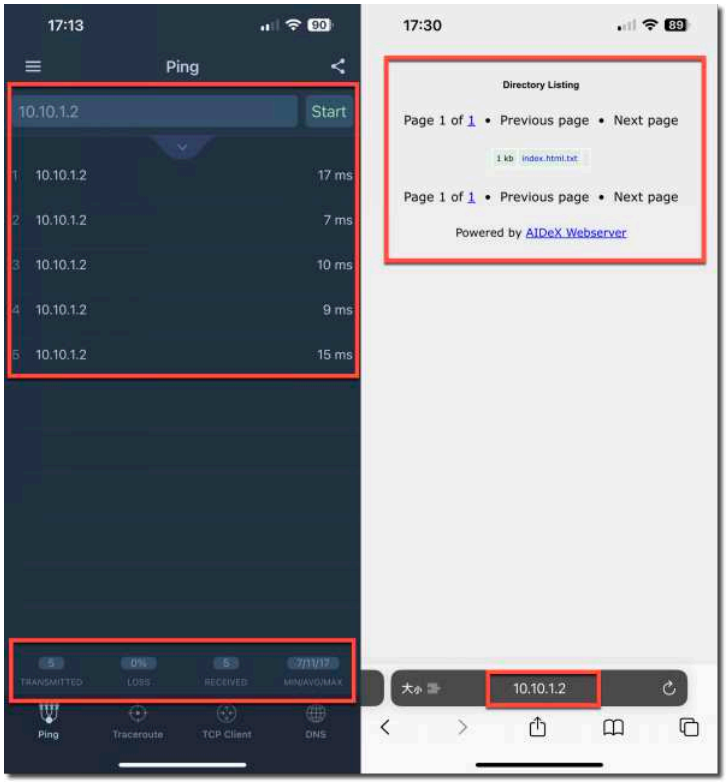
```
  lifetime/rekey: 3600/2185
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=iOS_IKEv1 ver=1 serial=1 202.103.12.2:0->0.0.0.0:0 tun_id=10.0.0.1 tun_id6=::10.0.0.1 dst_mtu=0 dpd-link=on
weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=42957570 olast=42957570 ad=/0
stat: rxp=115 txp=96 rxb=10525 txb=16656
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=iOS_IKEv1_0 ver=1 serial=4 202.103.12.2:4500->202.103.23.2:60417 tun_id=10.10.100.1 tun_id6=::10.0.0.4
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=iOS_IKEv1 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=873 olast=873 ad=/0
stat: rxp=51 txp=44 rxb=4704 txb=6692
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=silent draft=32 interval=10 remote_port=60417
proxyid=iOS_IKEv1 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:10.10.1.0-10.10.1.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20083 type=00 soft=0 mtu=1422 expire=2440/0B replaywin=2048
       seqno=2d esn=0 replaywin_lastseq=00000033 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3588/3600
  dec: spi=f3a58344 esp=aes key=32 a8ff490c9fb2e89be964d1a6993b11eedf71191e520ca99ed294c8eb4ea26301
       ah=sha256 key=32 7be5011c5d5a80768497ea9a4421bf8016797480cf6e31bd887d7367db35f30b
  enc: spi=05a9cf2e esp=aes key=32 83392937fdf5872826b529822a07a81c22e076d7bd648c8887451a2ce51b8336
       ah=sha256 key=32 a1897271122f887c59149acb755abc2959d1916a2c3340a35ef40f7172809d9b
  dec:pkts/bytes=102/9408, enc:pkts/bytes=88/16868
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=2 dec_npuid=0 enc_npuid=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

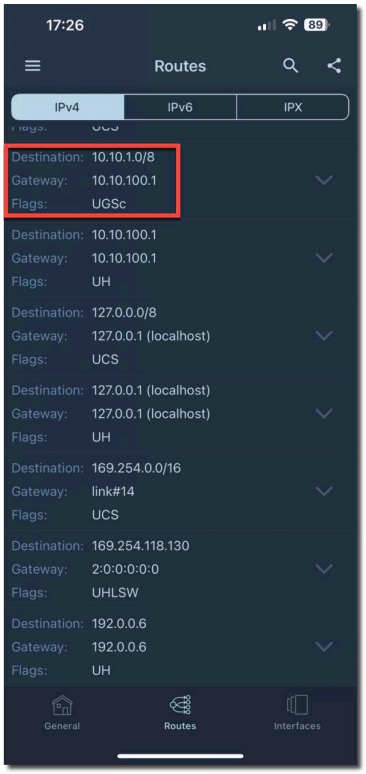
```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0->10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=25(iOS_IKEv1)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 查看客户端的路由表，可以看到隧道分割的路由。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

iOS原生客户端接入IPSec（IKEv2预共享密钥认证）

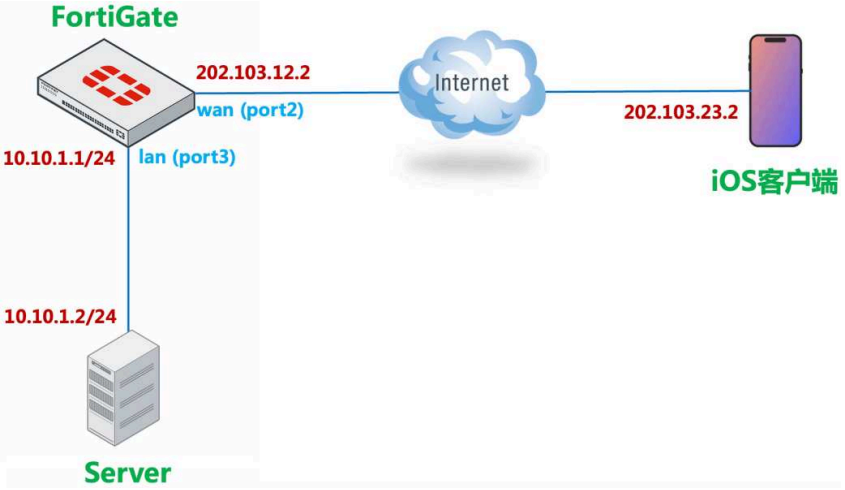
重要

本文基于iOS 16.3编写。

网络需求

通过iOS原生客户端（IKEv2预共享密钥认证）连接FortiGate的IPSec，并访问VPN内部资源。

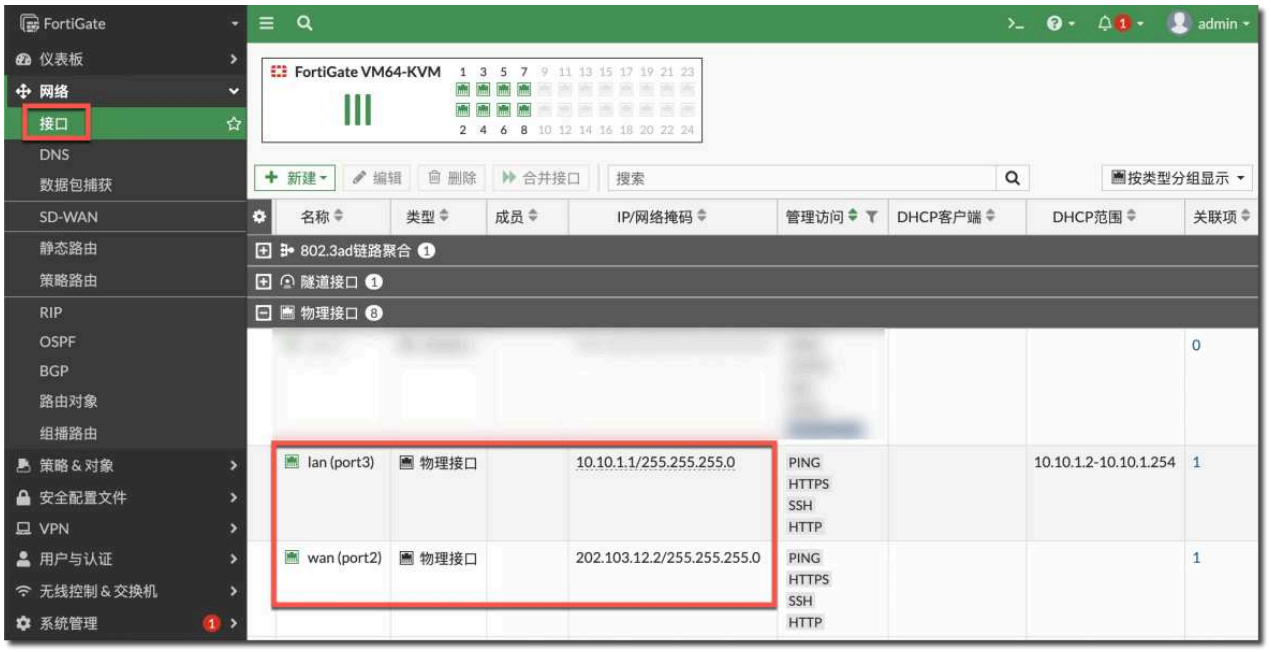
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。

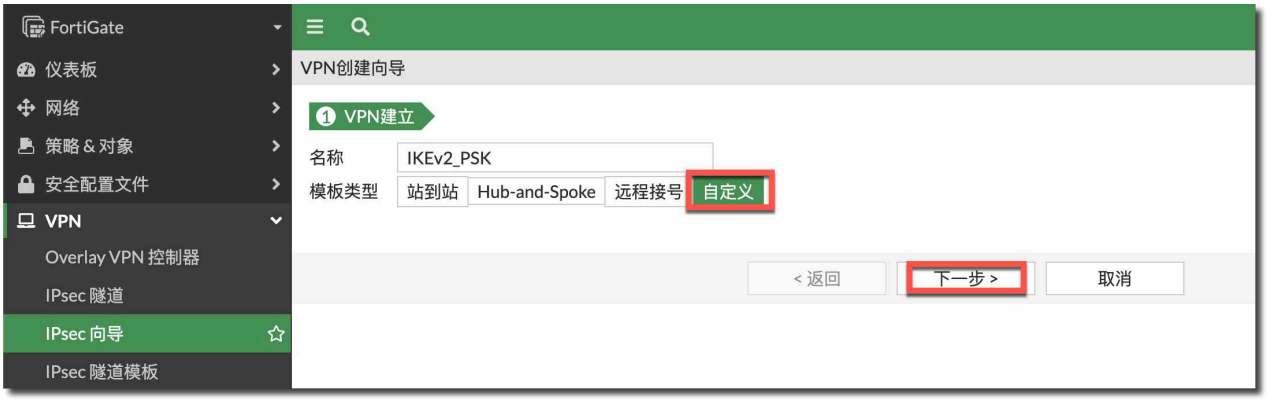


2. 进入FortiGate的VPN→IPSec隧道页面，点击新建按钮，新建IPSec隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 填写VPN名称，模版选择自定义，点击下一步。



4. 按照下图修改配置，其他配置保持默认即可，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

如果开启了隧道分割，本地地址不要填写为0.0.0.0/0，否则会导致客户端连接失败。

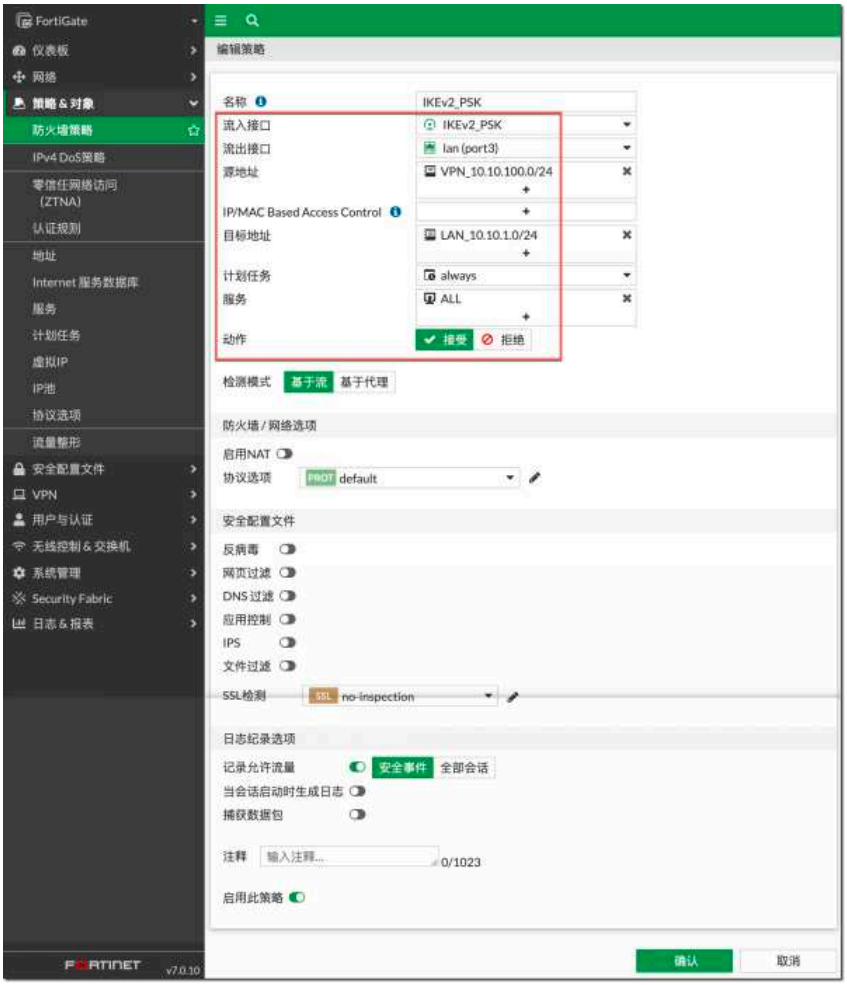
5. 对应的CLI如下：

```
第一阶段配置:
config vpn ipsec phase1-interface
    edit "IKEv2_PSK"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 10.10.1.2
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100
        set ipv4-split-include "LAN_10.10.1.0/24"
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end

第二阶段配置:
config vpn ipsec phase2-interface
    edit "IKEv2_PSK"
        set phase1name "IKEv2_PSK"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
        set pfs disable
        set keepalive enable
    next
end
```

```
地址对象:
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，允许客户端访问内网VPN资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
客户端地址对象:
config firewall address
    edit "VPN_10.10.100.0/24"
        set subnet 10.10.100.0 255.255.255.0
    next
end

防火墙策略:
config firewall policy
    edit 1
        set name "IKEv2_PSK"
        set srcintf "IKEv2_PSK"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

客户端配置

1. 打开设置→VPN，点击最下方的“添加VPN配置…”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 类型选择IKEv2，填写VPN名称、服务器IP，远程ID随意填写，用户鉴定选择“无”，关闭“使用证书”，填写预共享密钥，点击完成按钮。



3. 点击创建的VPN连接，确保该连接被选中（连接前有一个✅）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



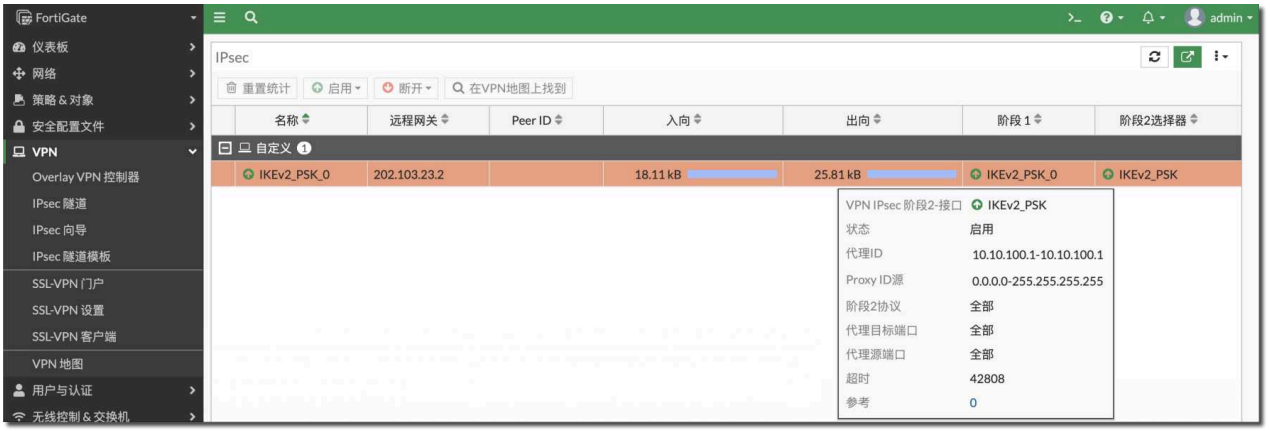
结果验证

1. 在客户端点击连接按钮，查看连接状态，点击VPN连接右侧的信息按钮，可以看到连接的具体信息，获取的IP为FortiGate配置的网段。



2. 在FortiGate侧查看连接状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
diagnose vpn ike gateway list

vd: root/0
name: IKEv2_PSK_0
version: 2
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:64916
tun_id: 10.10.100.1/::10.0.0.9
remote_location: 0.0.0.0
network-id: 0
created: 421s ago
assigned IPv4 address: 10.10.100.1/255.255.255.255
nat: peer
PPK: no
IKE SA: created 1/1  established 1/1  time 450/450/450 ms
IPsec SA: created 1/1  established 1/1  time 140/140/140 ms
  id/spi: 10 5198d872487677ea/31cdf17287e5560c
  direction: responder
  status: established 421-420s ago = 450ms
  proposal: aes256-sha256
  child: no
  SK_ei: dc94f8538f947677-a09ddef1a1bec336-c65701c8f563da84-1812eb919f080c9c
  SK_er: f845db38cae914bf-f45903f0d16af51b-756ce4808bcfedde-f28ff9ec28b3dfe0
  SK_ai: d733f1548b7a4e66-0b7bc5e25539c612-7d9b58309bf6b7ac-539bbdbf51610ccd
  SK_ar: b4b85aecdc194e94-3b04954ddb321f23-fec94182c35dc0d9-ee6c3f8edaab46f4
  PPK: no
  message-id sent/recv: 0/3
  lifetime/rekey: 86400/85709
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=IKEv2_PSK_0 ver=2 serial=f 202.103.12.2:4500→202.103.23.2:64916 tun_id=10.10.100.1 tun_id6=::10.0.0.9
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=IKEv2_PSK index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=347 txp=338 rxb=23044 txb=31852
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=64916
proxyid=IKEv2_PSK proto=0 sa=1 ref=24 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20483 type=00 soft=0 mtu=1422 expire=42739/0B replaywin=2048
       seqno=153 esn=0 replaywin_lastseq=0000015b qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43185/43200
  dec: spi=4d836866 esp=aes key=16 8ae2318c0e96f4a41b454135917178a9
       ah=sha1 key=20 87cc5f5d5de49187019ea267a812df1873b9cf6f
  enc: spi=0c26fd39 esp=aes key=16 08bfbe6a97eb166634337de47be3925f
       ah=sha1 key=20 d670dba9af5500ae408f62052c5c192c1b45feff
  dec:pkts/bytes=694/46088, enc:pkts/bytes=676/88844
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=7 dec_npuid=0 enc_npuid=0
------------------------------------------------------
```

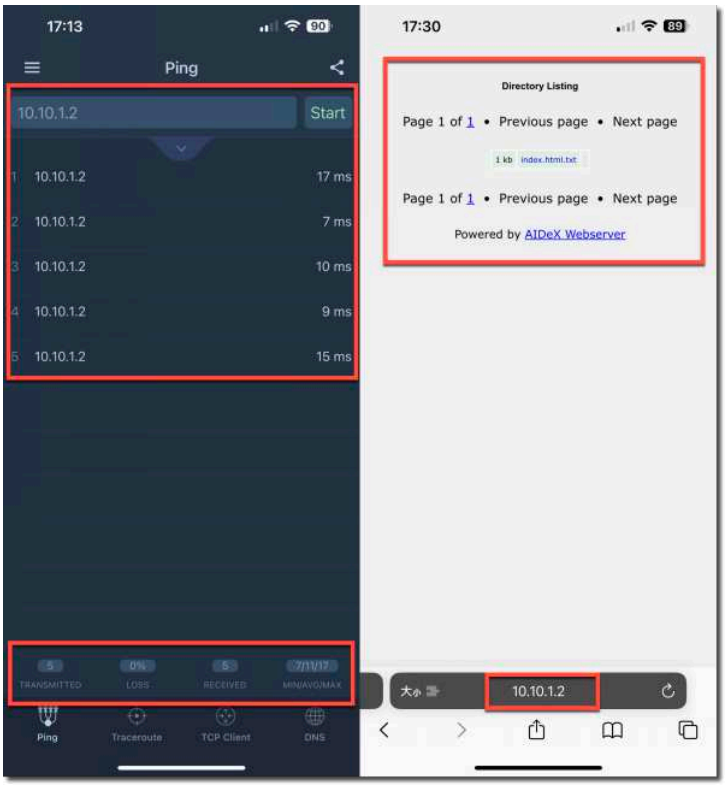

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
name=IKEv2_PSK ver=2 serial=e 202.103.12.2:0→0.0.0.0:0 tun_id=10.0.0.7 tun_id6=::10.0.0.7 dst_mtu=0 dpd-link=on
weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=43032051 olast=43032051 ad=/0
stat: rxp=347 txp=338 rxb=23044 txb=31852
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=25(IKEv2_PSK)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。



重要

实际测试iOS/macOS使用IKEv2，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

iOS原生客户端接入IPSec（IKEv2用户名/密码+预共享密钥认证）

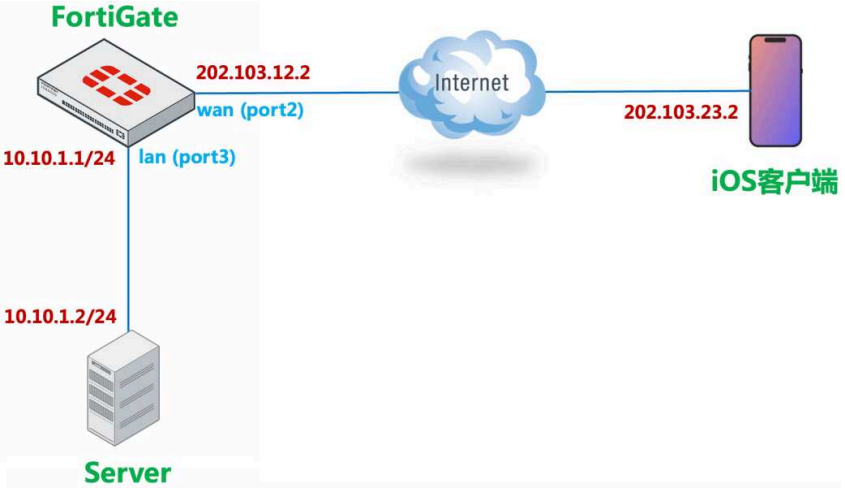
重要

本文基于iOS 16.3编写。

网络需求

通过iOS原生客户端（IKEv2用户名/密码+预共享密钥认证）连接FortiGate的IPSec，并访问VPN内部资源。

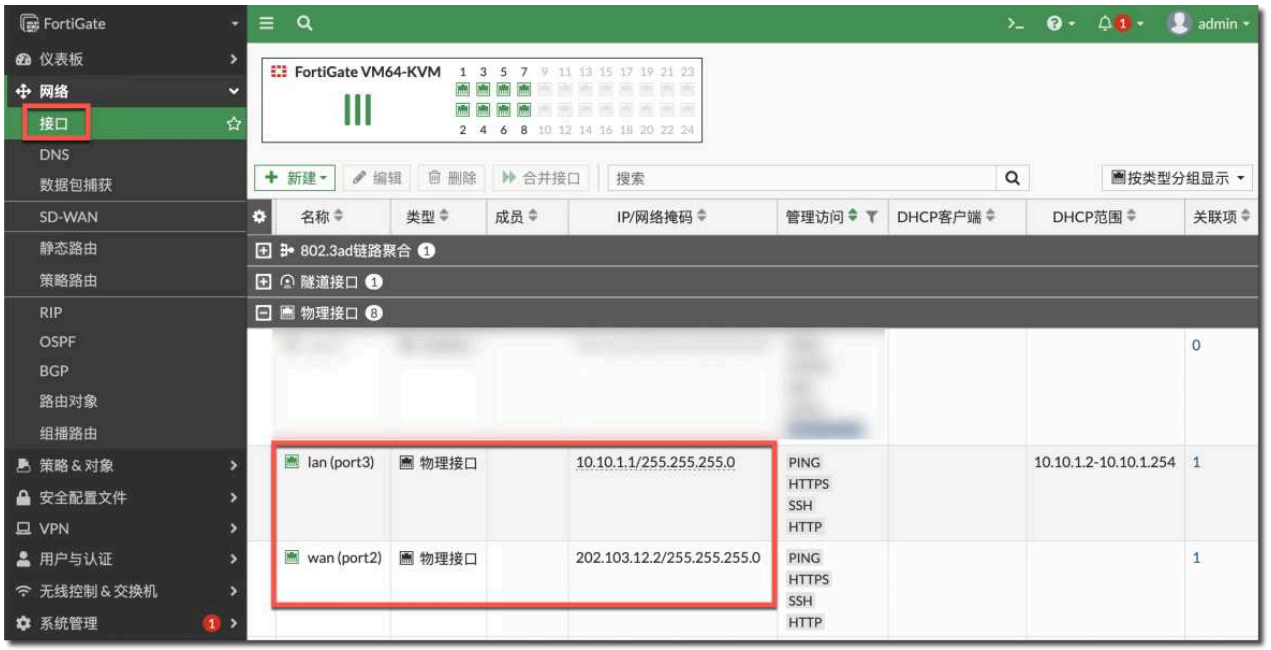
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。



2. 创建本地VPN用户和用户组，参考用户与认证→本地用户和用户组↗章节（如需使用远程认证，请参考用户与认证→LDAP认证→LDAP认证配置与排错↗或用户与认证→Radius认证→Radius认证配置与排错↗章节）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config user local
    edit "vpn_user"
        set type password
        set passwd xxxxxxxx
    next
end
```




```
config user group
    edit "VPN"
        set member "vpn_user"
    next
end
```

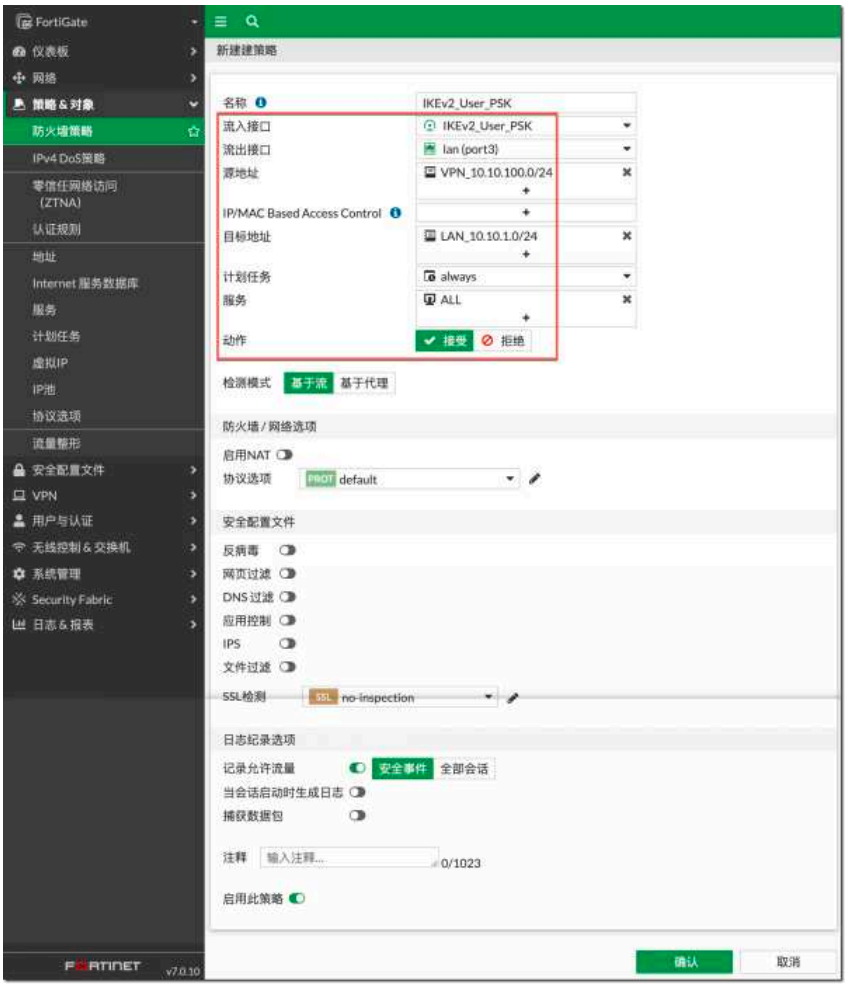
3. 该种方式的IPSec需要使用CLI方式配置，分别配置IPSec一阶段和二阶段。

```
IPSec一阶段配置:
config vpn ipsec phase1-interface
    edit "IKEv2_User_PSK"
        set type dynamic
        set interface "port2"
        set ike-version 2    //IKE协议2
        set peertype any
        set net-device disable
        set mode-cfg enable    //开启为客户端分配IP
        set ipv4-dns-server1 10.10.1.2  //为客户端分配的DNS地址
        set proposal aes256-sha256
        set negotiate-timeout 300
        set dpd on-idle
        set dhgrp 14 5 2
        set eap enable    //需要开启EAP做用户密码认证
        set eap-identity send-request    //开启EAP主动发送认证请求
        set authusrgrp "VPN"    //选择认证的用户组
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100    //客户端分配地址范围
        set ipv4-netmask 255.255.255.0
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end

IPSec二阶段配置:
config vpn ipsec phase2-interface
    edit "IKEv2_User_PSK"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set phase1name "IKEv2_User_PSK"
        set proposal aes256-sha256
        set keepalive enable
    next
end
```

4. 配置防火墙策略，允许客户端访问内网VPN资源。




```
VPN资源地址对象：
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
end

客户端地址对象：
config firewall address
    edit "VPN_10.10.100.0/24"
        set subnet 10.10.100.0 255.255.255.0
    next
end

防火墙策略：
config firewall policy
    edit 1
        set name "IKEv2_User_PSK"
        set srcintf "IKEv2_User_PSK"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

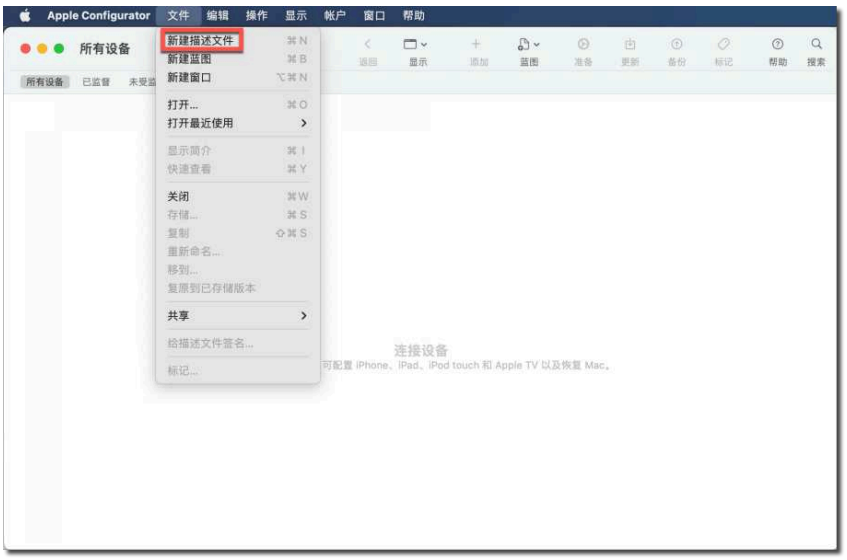
```
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

制作和安装描述文件

重要

想要使用IKEv2用户名/密码+预共享密钥方式的VPN认证，需要使用Apple Configurator工具为iOS/macOS制作描述文件，该工具可以在macOS下的App Store中下载。

1. 打开Apple Configurator，点击菜单栏的“文件→新建描述文件”（或使用快捷键Command + N）。

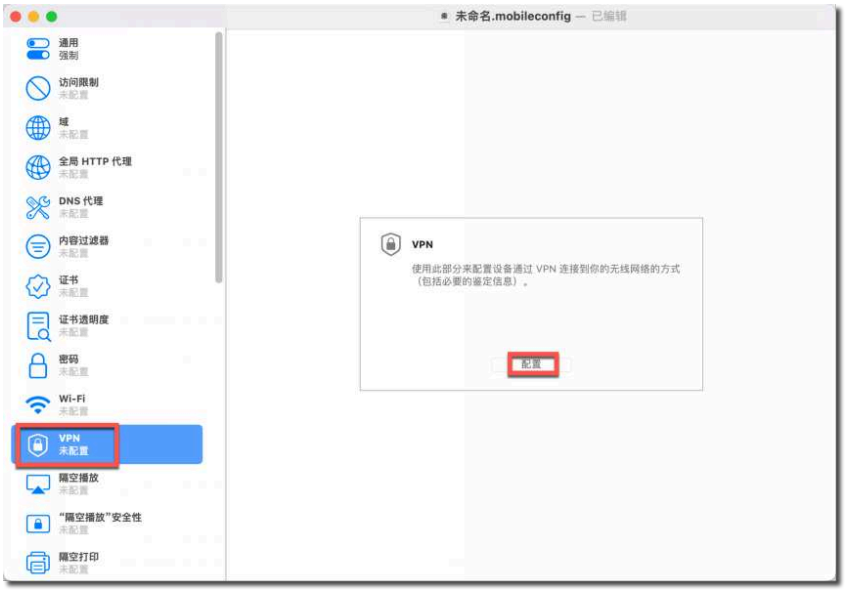


2. 在弹出的配置文件编辑器中，配置描述文件的名称。



3. 选择VPN选项卡，点击配置按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置描述文件，选择连接类型为IKEv2，填写服务器IP地址，远程标识符和局部标识符随意填写，填写预共享密钥，开启EAP，选择EAP鉴定为用户名/密码模式，其他配置保持默认即可（或根据实际需求更改）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 选择菜单栏的“文件→存储”按钮（或使用快捷键Command + S），保存该描述文件到本地。



6. 通过邮件等方式，将描述文件发送至iPhone。

7. iPhone通过邮件App收取该描述文件后，点击该描述文件，会弹出提示进入设置中查看描述文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 进入设置，点击“已下载描述文件”。



9. 选择制作的描述文件并安装（需要输入手机密码）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



10. 根据提示输入用户名和密码，点击完成按钮安装描述文件。



11. VPN列表中自动生成VPN配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



客户端配置

1. 打开设置→VPN，点击创建的VPN连接，确保该连接被选中（连接前有一个✅）。



2. 可根据实际需要修改VPN连接中的用户名或密码。

结果验证

1. 在客户端点击连接按钮，查看连接状态，点击VPN连接右侧的信息按钮，可以看到连接的具体信息，获取的IP为FortiGate配置的网段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: IKEv2_User_PSK_0
version: 2
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:64916
tun_id: 10.10.100.1/::10.0.0.17
remote_location: 0.0.0.0
network-id: 0
created: 194s ago
eap-user: vpn_user
2FA: no
peer-id: client
peer-id-auth: no
assigned IPv4 address: 10.10.100.1/255.255.255.0
nat: peer
PPK: no
IKE SA: created 1/1  established 1/1  time 90/90/90 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms
  id/spi: 13 d5ae11369c1b3d95/68eb5a2b96838488
  direction: responder
  status: established 194-194s ago = 90ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

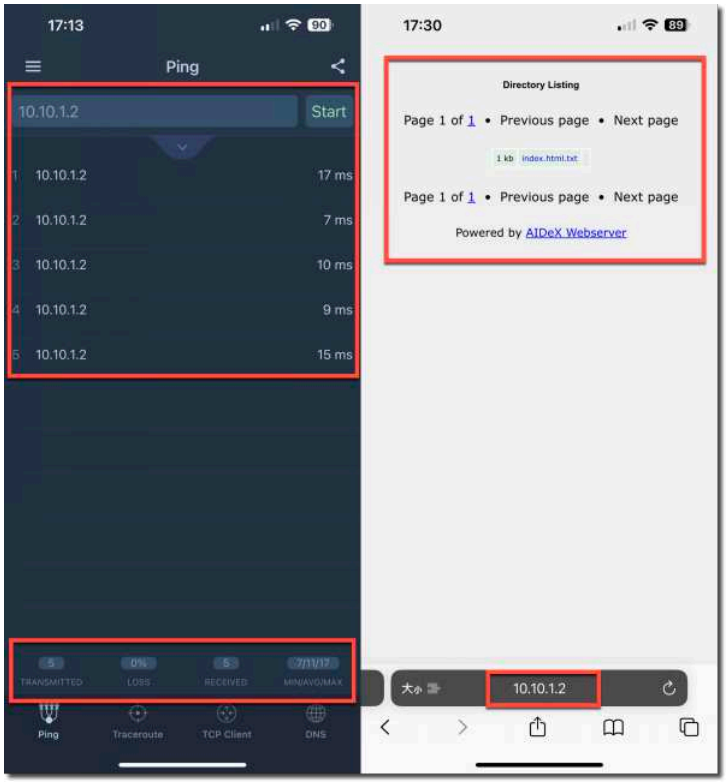
```
  proposal: aes256-sha256
  child: no
  SK_ei: 5f2946151d12c26b-0ca7ea2a894ba835-a6a5c9a24d44caa8-e11178ab9a2cd6f5
  SK_er: fe330d4fbd3f7753-77748964618e4a94-4bf4f7baeedcca70-ba645a3fc31f2265
  SK_ai: 488d6b7d9df75b01-d2c8bdc7049e552a-0c17d452a8b4ebe8-631caa5abacaa0c6
  SK_ar: 782bdd0189841d1c-fc202aa4598d009e-056e04417ae4ad9b-da9ede3c92250546
  PPK: no
  message-id sent/recv: 0/6
  lifetime/rekey: 86400/85935
  DPD sent/recv: 00000000/00000000
  peer-id: client

FortiGate # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=IKEv2_User_PSK ver=2 serial=14 202.103.12.2:0->0.0.0.0:0 tun_id=10.0.0.9 tun_id6=::10.0.0.9 dst_mtu=0 dpd-
link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=43039746 olast=43039746 ad=/0
stat: rxp=1723 txp=337 rxb=127170 txb=41184
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=IKEv2_User_PSK_0 ver=2 serial=1a 202.103.12.2:4500->202.103.23.2:64916 tun_id=10.10.100.1 tun_id6=::10.0.0.17
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=IKEv2_User_PSK index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=12 olast=12 ad=/0
stat: rxp=113 txp=38 rxb=7546 txb=3581
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=64916
proxyid=IKEv2_User_PSK proto=0 sa=1 ref=10 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20683 type=00 soft=0 mtu=1422 expire=42991/0B replaywin=2048
       seqno=27 esn=0 replaywin_lastseq=00000071 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43190/43200
  dec: spi=7b8ba378 esp=aes key=32 e2651b177effa8747d930eacb965a527f5758f5f0a6503225f2d21eac7d549fe
       ah=sha256 key=32 1f86d1b2efb0dbe0511f2c0b79257ab6b76c3f42aa9ddbafde6f8f4c7b13eb27
  enc: spi=0846436d esp=aes key=32 87d133ec91eccd6c9b10671111bd07242f9560ba62c4735c5a8dffc52ededf59
       ah=sha256 key=32 792ce83e7dce6fdfdb8df9edf286a206023b236a263fa9ab09cdd3b819064386
  dec:pkts/bytes=226/15092, enc:pkts/bytes=76/10133
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=f dec_npuid=0 enc_npuid=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0->10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=27(IKEv2_User_PSK)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

实际测试iOS/macOS使用IKEv2，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

鸿蒙（HarmonyOS）及Android12以下系统（IKEv1）

重要

本文基于鸿蒙（HarmonyOS）3.0编写，Android12以下系统配置步骤与其一致。

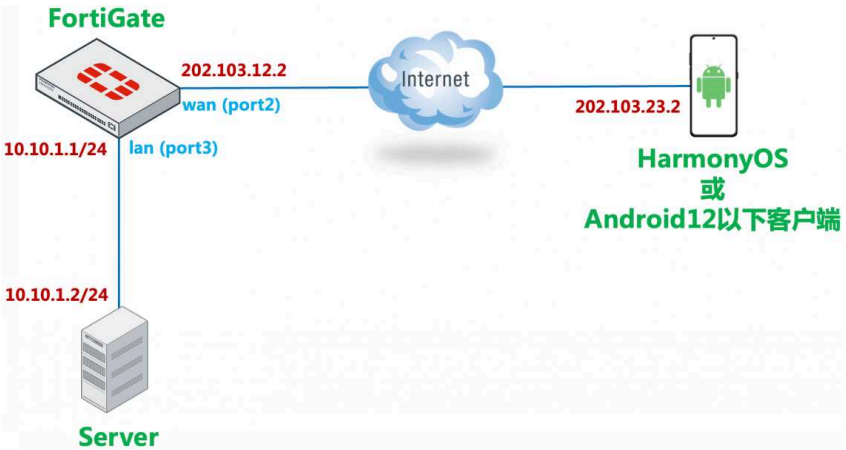
网络需求

通过鸿蒙（HarmonyOS）或Android12以下系统客户端（IKEv1）连接FortiGate的IPSec，并访问VPN内部资源。

重要

通过IKEv1用户名/密码+预共享密钥的方式认证（不涉及L2TP）。

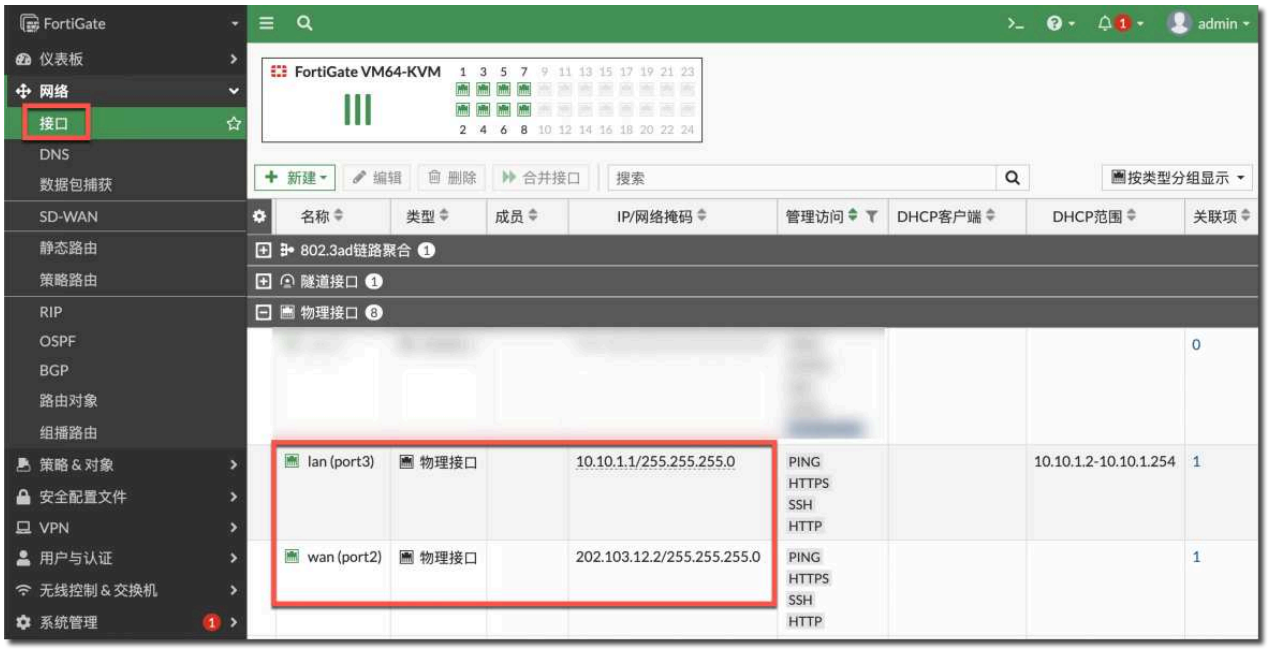
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。

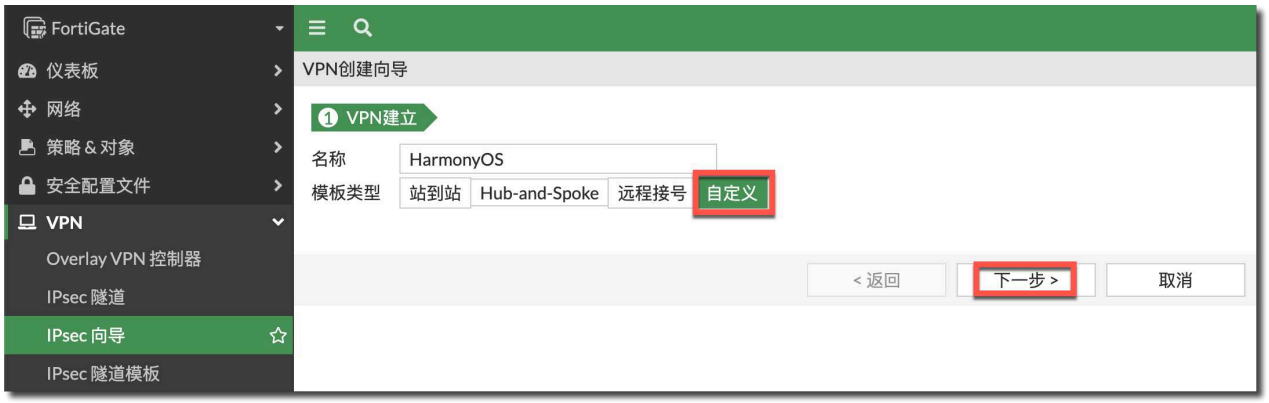


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 进入FortiGate的VPN→IPSec隧道页面，点击新建按钮，新建IPSec隧道。



3. 填写VPN名称，模版选择自定义，点击下一步。



4. 按照下图修改配置，其他配置保持默认即可，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 对应的CLI如下：

```
第一阶段配置:
config vpn ipsec phase1-interface
    edit "HarmonyOS"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 10.10.1.2
        set proposal aes256-sha256 aes128-sha1
        set dpd on-idle
        set dhgrp 14 5 2
        set xauthtype auto
        set authusrgrp "VPN"
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end

第二阶段配置:
config vpn ipsec phase2-interface
    edit "HarmonyOS"
        set phase1name "HarmonyOS"
        set proposal aes256-sha256 aes128-sha1
        set pfs disable
        set keepalive enable
    next
end
```

```
地址对象:
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，允许客户端访问内网VPN资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
客户端地址对象:
config firewall address
    edit "VPN_10.10.100.0/24"
        set subnet 10.10.100.0 255.255.255.0
    next
end

防火墙策略:
config firewall policy
    edit 1
        set name "HarmonyOS"
        set srcintf "HarmonyOS"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

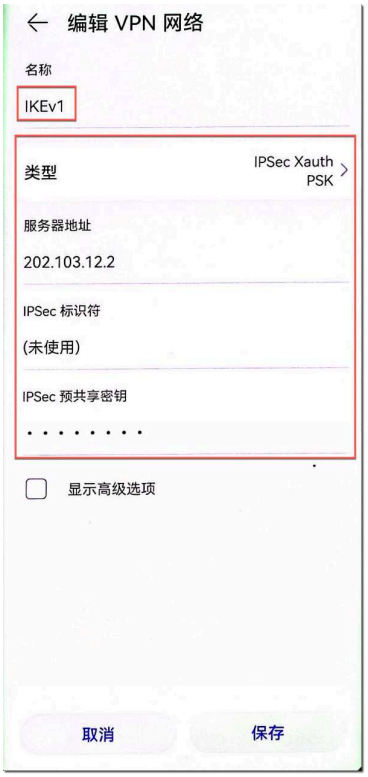
客户端配置

1. 打开设置→更多连接→VPN，点击下方的“添加VPN网络”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 类型选择IPSec Xauth PSK，填写名称、服务器地址、IPSec预共享密钥，点击保存按钮保存连接（由于华为手机在VPN连接配置界面无法截图，所以下图为拍照）。



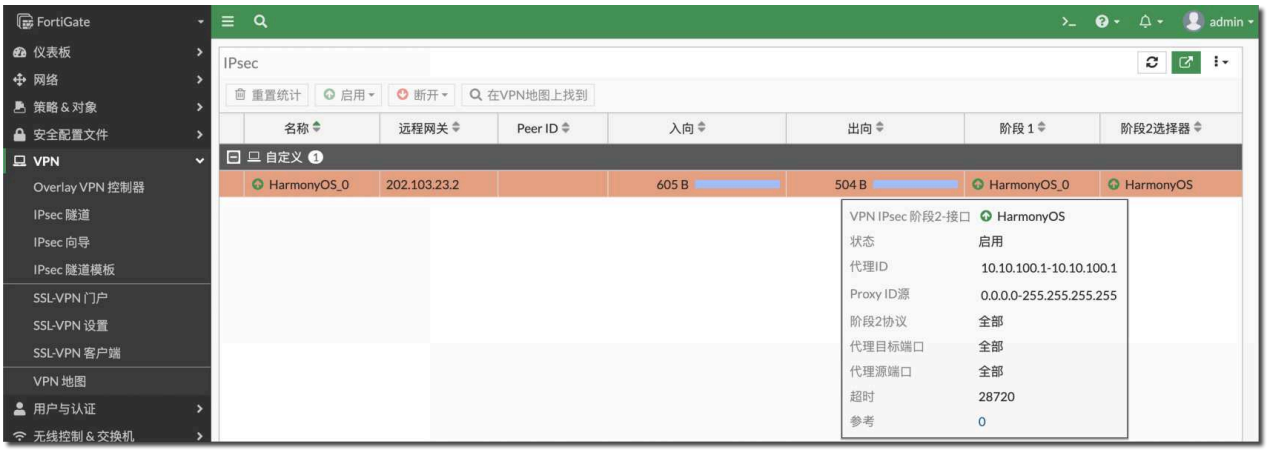
结果验证

1. 点击创建的VPN连接，输入用户名与密码，按需求勾选“保存账户信息”（由于华为手机在VPN连接配置界面无法截图，所以下图为拍照），点击连接按钮。连接成功后，点击查看连接状态，可以看到连接的具体信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: HarmonyOS_0
version: 1
interface: port2 4
addr: 202.103.12.2:4500 -> 202.103.23.2:64916
tun_id: 10.10.100.1/::10.0.0.19
remote_location: 0.0.0.0
network-id: 0
created: 26s ago
xauth-user: vpn_user
2FA: no
assigned IPv4 address: 10.10.100.1/255.255.255.255
nat: peer
IKE SA: created 1/1  established 1/1  time 240/240/240 ms
IPsec SA: created 1/1  established 1/1  time 440/440/440 ms
  id/spi: 73 39a070180abf8f20/7c90c7a59d942c95
  direction: responder
  status: established 26-26s ago = 240ms
  proposal: aes256-sha256
  key: 888ae90f86ef043e-a160f4d6b782c66d-c6d006f30ed9f5d7-923c853d34fa1e06
  lifetime/rekey: 28800/28503
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

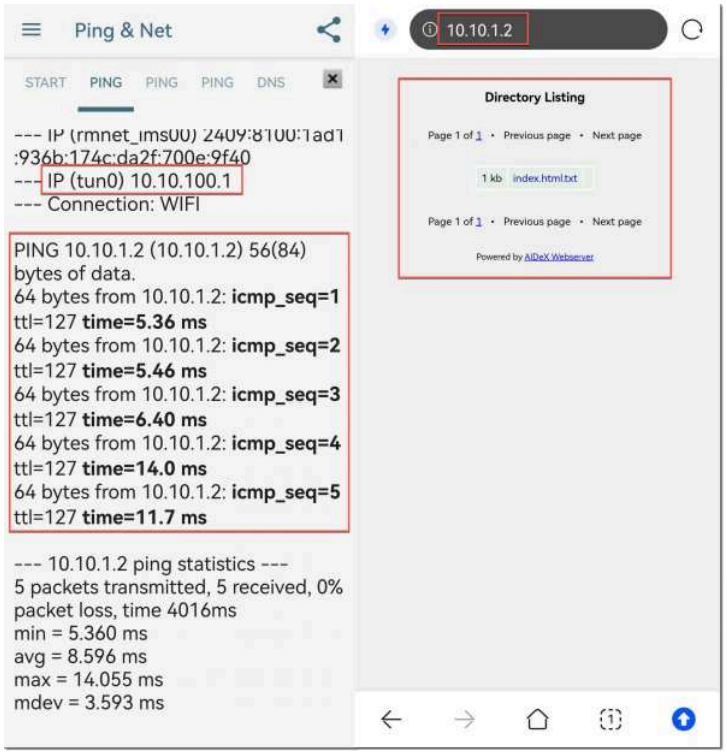
```
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=HarmonyOS_0 ver=1 serial=17 202.103.12.2:4500->202.103.23.2:64916 tun_id=10.10.100.1 tun_id6=::10.0.0.19
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=HarmonyOS index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=7 olast=7 ad=/0
stat: rxp=5 txp=3 rxb=331 txb=289
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=1
natt: mode=silent draft=32 interval=10 remote_port=64916
proxyid=HarmonyOS proto=0 sa=1 ref=5 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20083 type=00 soft=0 mtu=1422 expire=28757/0B replaywin=2048
       seqno=4 esn=0 replaywin_lastseq=00000005 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=28786/28800
  dec: spi=a06d669d esp=aes key=32 bb01635fcbcfec11f8970f8b58a23c6cadc3c12e6b506a799b8563c73501e5db
       ah=sha256 key=32 d8eb7b5dea988ea7b2d0509a6160b7f285827c4f56d6293aa77230759034518d
  enc: spi=02c359e0 esp=aes key=32 d8e3495f33ee0a4b7f851a4eaa1756f6ab16bddb6ba9d9c07b34fcc4c63d6e55
       ah=sha256 key=32 39e4c2b7c0b060c6d27a605c55821e27276b780699081975f1362a13580bd012
  dec:pkts/bytes=10/662, enc:pkts/bytes=6/813
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=11 dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=HarmonyOS ver=1 serial=13 202.103.12.2:0->0.0.0.0:0 tun_id=10.0.0.5 tun_id6=::10.0.0.5 dst_mtu=0 dpd-link=on
weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=42980186 olast=42980186 ad=/0
stat: rxp=7 txp=5 rxb=459 txb=473
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0->10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=23(HarmonyOS)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

实际测试Android使用IKEv1，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Android12或以上系统（IKEv2）

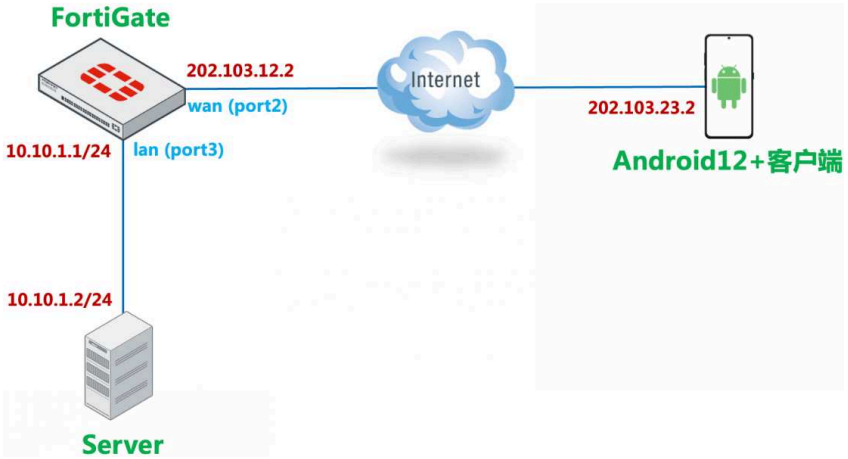
> **重要**
>
> 本文基于Sumsung One UI 5.1 (Android13)系统编写。

网络需求

通过Android12或以上系统客户端（IKEv2）连接FortiGate的IPSec，并访问VPN内部资源。

> **重要**
>
> 通过IKEv2预共享密钥的方式认证（无用户密码认证）。

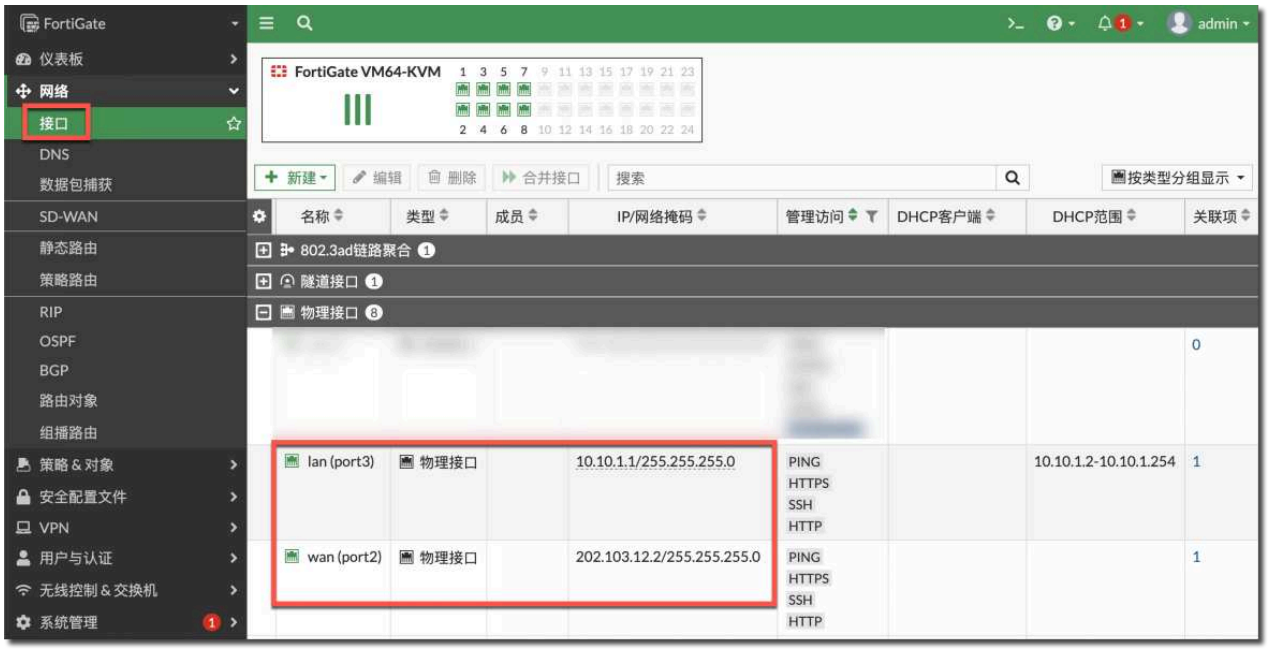
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。

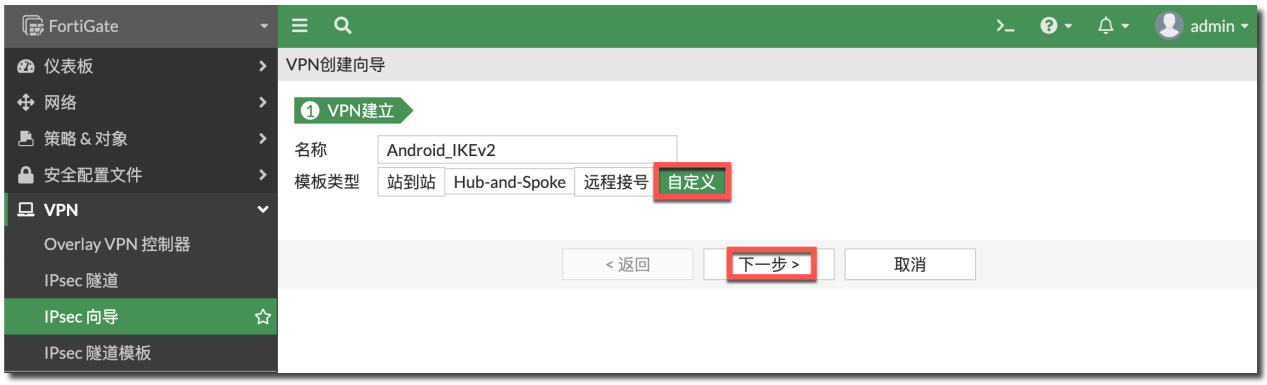


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 进入FortiGate的VPN→IPSec隧道页面，点击新建按钮，新建IPSec隧道。



3. 填写VPN名称，模版选择自定义，点击下一步。



4. 按照下图修改配置，其他配置保持默认即可，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

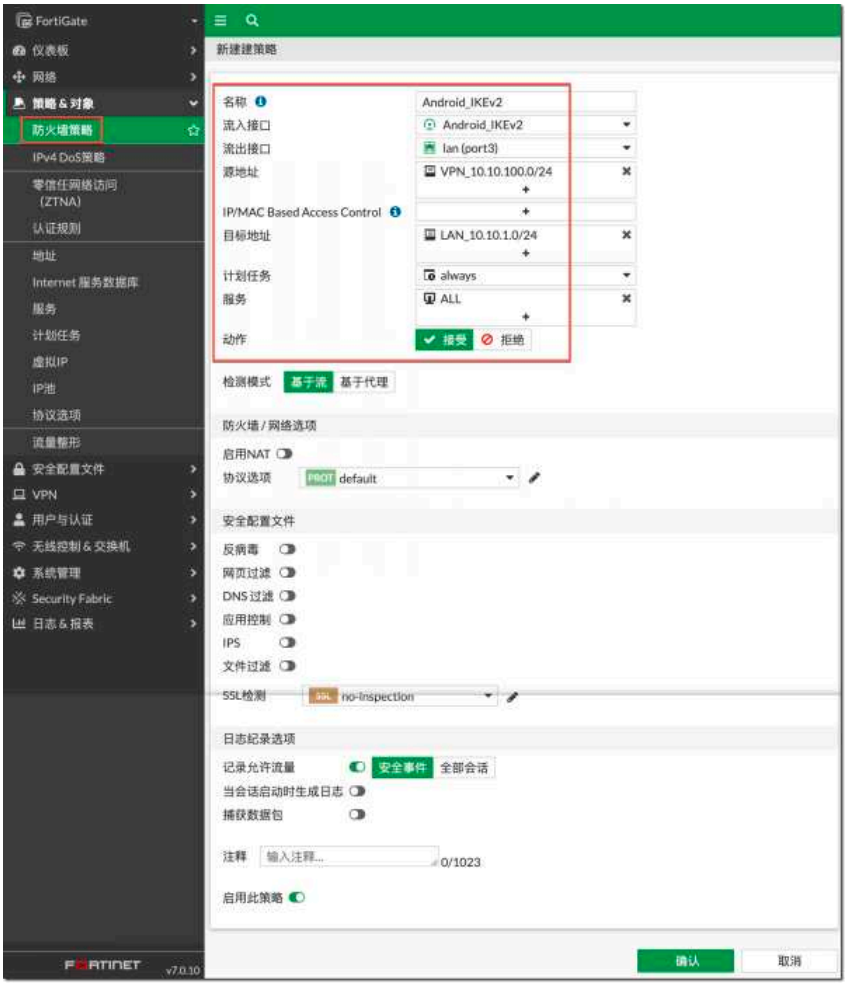


5. 对应的CLI如下：

```
第一阶段配置:
config vpn ipsec phase1-interface
    edit "Android_IKEv2"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 10.10.12.2
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-
prfsha256
        set dpd on-idle
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end

第二阶段配置:
config vpn ipsec phase2-interface
    edit "Android_IKEv2"
        set phase1name "Android_IKEv2"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
        set keepalive enable
    next
end
```

6. 配置防火墙策略，允许客户端访问内网VPN资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
内网VPN资源地址对象：
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
 next
end

客户端地址对象：
config firewall address
       edit "VPN_10.10.100.0/24"
           set subnet 10.10.100.0 255.255.255.0
       next
   end

防火墙策略：
config firewall policy
    edit 1
        set name "Android_IKEv2"
        set srcintf "Android_IKEv2"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

客户端配置

7. 打开设置→连接→更多连接设置→VPN（找不到可以使用搜索功能），点击“添加VPN配置文件”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 类型选择IKEv2/IPSec PSK，填写名称、服务器地址、IPSec预共享密钥，注意必须填写IPSec标识符（随意填写即可），点击保存按钮保存连接。



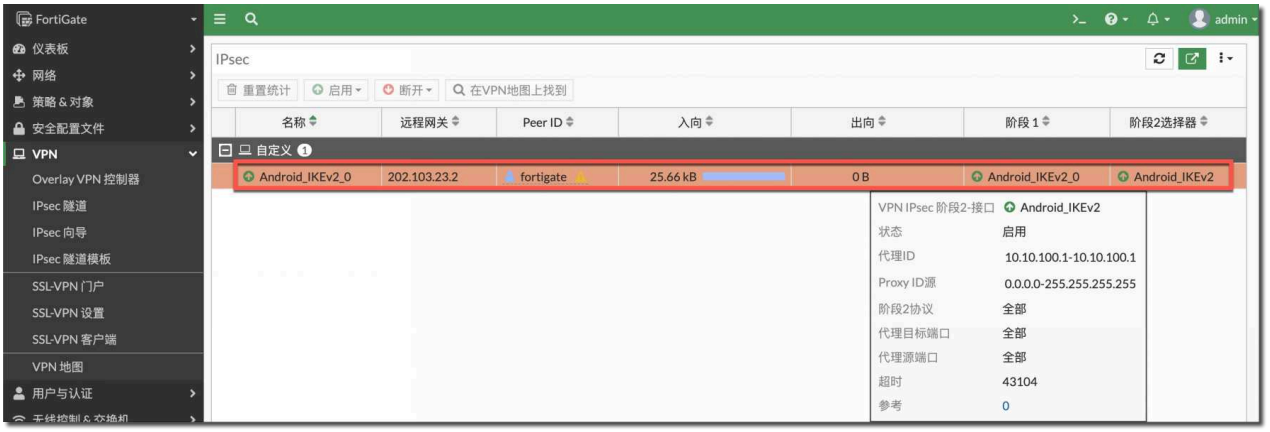
结果验证

1. 点击创建的VPN连接，点击连接按钮。连接成功后，点击查看连接状态，可以看到连接的具体信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: Android_IKEv2_0
version: 2
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:35653
tun_id: 10.10.100.1/::10.0.0.29
remote_location: 0.0.0.0
network-id: 0
created: 8s ago
peer-id: fortigate
peer-id-auth: no
assigned IPv4 address: 10.10.100.1/0.0.0.0
nat: peer
PPK: no
IKE SA: created 1/1  established 1/1  time 20/20/20 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms
  id/spi: 5 24e28229fbb0aabf/af590cf99666b224
  direction: responder
  status: established 8-8s ago = 20ms
  proposal: aes128-sha256
  child: no
  SK_ei: ebe7fafddd9a3afa-d25d578817491d46
  SK_er: d498cfd72bc78306-5d96c828c054dc49
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

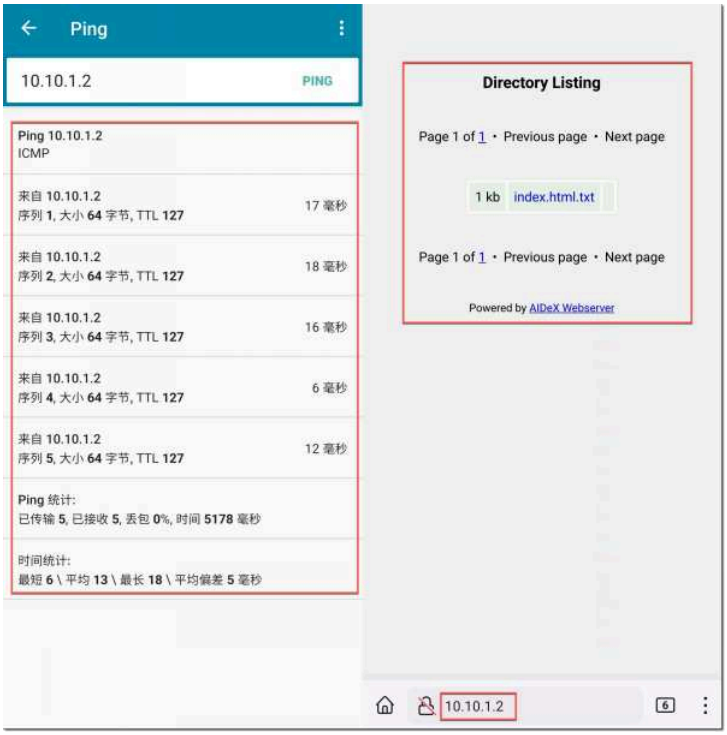
```
  SK_ai: db2fe8a3c377d068-043cb17abe4a50dc-0b6a7406d9136909-d8f071b76a03d411
  SK_ar: 0816650a93fb45f2-620c1f63caa107c3-bdf507a33957e29e-e22ec78cdf616f11
  PPK: no
  message-id sent/recv: 0/2
  lifetime/rekey: 86400/86121
  DPD sent/recv: 00000000/00000000
  peer-id: fortigate

FortiGate # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=Android_IKEv2_0 ver=2 serial=25 202.103.12.2:4500->202.103.23.2:35653 tun_id=10.10.100.1 tun_id6=::10.0.0.29
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=Android_IKEv2 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=11 ad=/0
stat: rxp=63 txp=0 rxb=3644 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=35653
proxyid=Android_IKEv2 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20683 type=00 soft=0 mtu=1422 expire=43175/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=0000003f qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43187/43200
  dec: spi=02cf6ed7 esp=aes key=16 e9a35403758eddeaa21370e37e36ea8d
       ah=sha256 key=32 54a6e676edae65bb37a0f4a6605b8fcfde743af1f229d29624abbbd4cc8bf8ec
  enc: spi=cbf93f37 esp=aes key=16 4e475164fbf9ac1be9c81497cd8ff98f
       ah=sha256 key=32 682b3b42a8f121a227f70a8952cc92110371f06f32309e5a0c7bb43a48677667
  dec:pkts/bytes=126/7288, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=1b dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=Android_IKEv2 ver=2 serial=22 202.103.12.2:0->0.0.0.0:0 tun_id=10.0.0.9 tun_id6=::10.0.0.9 dst_mtu=0 dpd-
link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=43054304 olast=43054304 ad=/0
stat: rxp=7209 txp=12 rxb=427332 txb=832
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
 ...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0->10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=27(Android_IKEv2)
 ...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

实际测试Android使用IKEv2，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

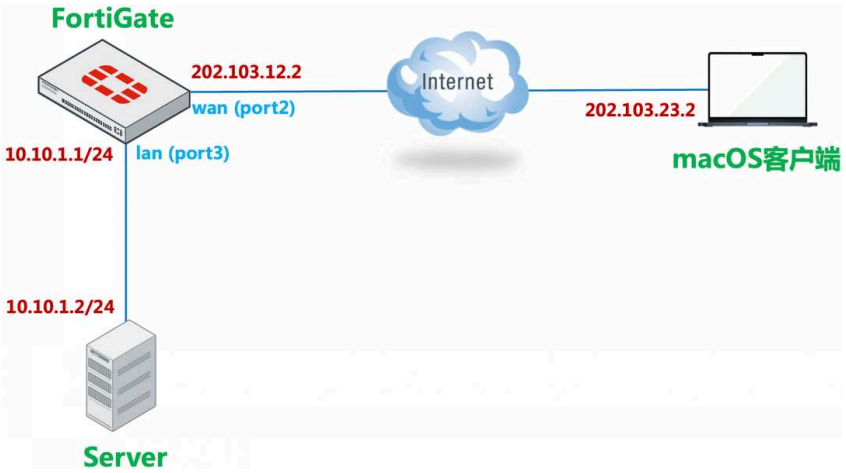
macOS原生客户端接入IPSec（IKEv1）

> **重要**
>
> 本文基于macOS 13.2编写。

网络需求

通过macOS原生客户端（IKEv1）连接FortiGate的IPSec，并访问VPN内部资源。

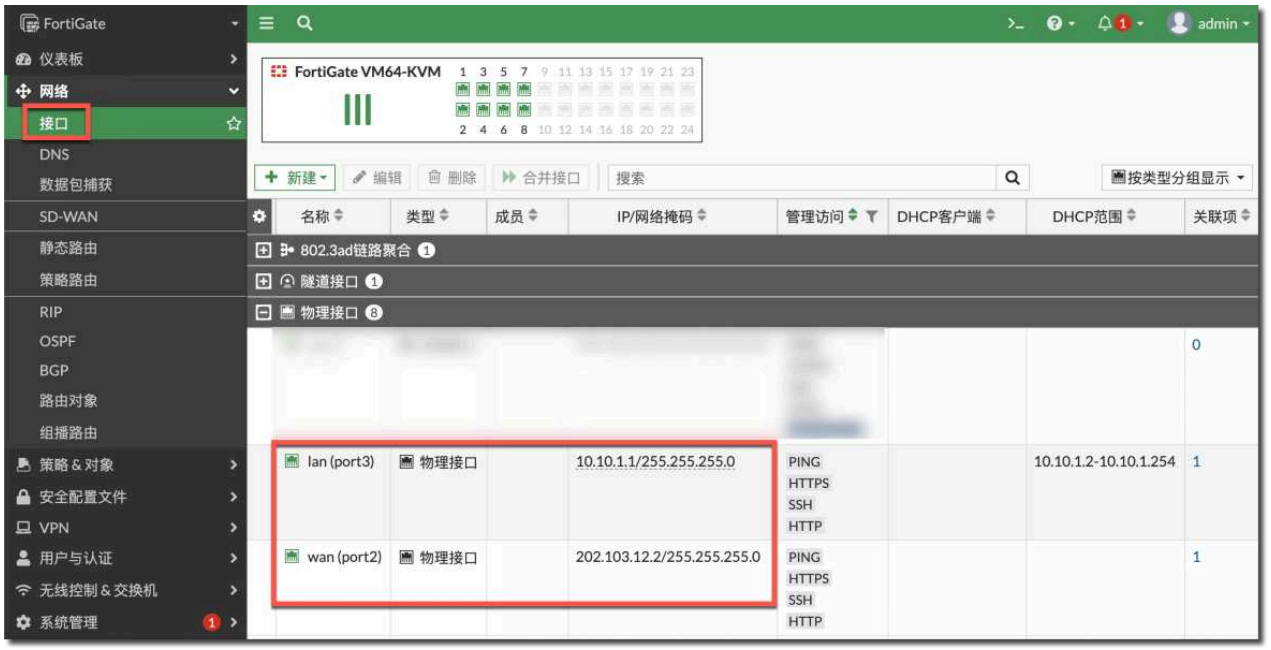
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。



2. 创建本地VPN用户和用户组，参考用户与认证→本地用户和用户组↗章节（如需使用远程认证，请参考用户与认证→LDAP认证→LDAP认证配置与排错↗或用户与认证→Radius认证→Radius认证配置与排错↗章节）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config user local
    edit "vpn_user"
        set type password
        set passwd xxxxxxxx
    next
end
```




```
config user group
    edit "VPN"
        set member "vpn_user"
    next
end
```

3. 进入FortiGate的VPN→IPSec隧道页面，点击新建按钮，新建IPSec隧道。



4. 填写VPN名称，模版选择远程拨号，远程设备选择Native，然后选择iOS Native，点击下一步。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

5. 配置流入接口为wan口，填入预共享密钥，选择VPN用户组，点击下一步。



6. 配置本地接口（VPN客户端要访问的网络所属出接口），本地地址新建并选择内网的VPN网段地址对象，分配客户端地址范围（注意不要和现有网段冲突），DNS可选择系统DNS或指定DNS，默认开启隧道分割，只有本地地址中的网段会被客户端转发至VPN隧道（关闭隧道分割的话，客户端会将自身发起的所有流量转发至VPN隧道）。点击下一步。



> **重要**
>
> 如果开启了隧道分割，本地地址不要填写为0.0.0.0/0，否则会导致客户端连接失败。

7. 检查配置无误后，点击完成按钮，完成隧道建立。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





8. 向导配置完成后，FortiGate会自动创建IPSec一阶段和二阶段、内网地址对象、客户端到内网的防火墙访问策略，对应的CLI如下：

```
第一阶段和第二阶段VPN配置：
config vpn ipsec phase1-interface
    edit "macOS_IKEv1"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes256-sha256 aes256-md5 aes256-sha1
        set comments "VPN: macOS_IKEv1 (Created by VPN wizard)"
        set dhgrp 14 5 2
        set wizard-type dialup-ios
        set xauthtype auto
        set authusrgrp "VPN"
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100
        set dns-mode auto
        set ipv4-split-include "macOS_IKEv1_split"
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "macOS_IKEv1"
        set phase1name "macOS_IKEv1"
        set proposal aes256-sha256 aes256-md5 aes256-sha1
        set pfs disable
        set keepalive enable
        set comments "VPN: macOS_IKEv1 (Created by VPN wizard)"
    next
end
```

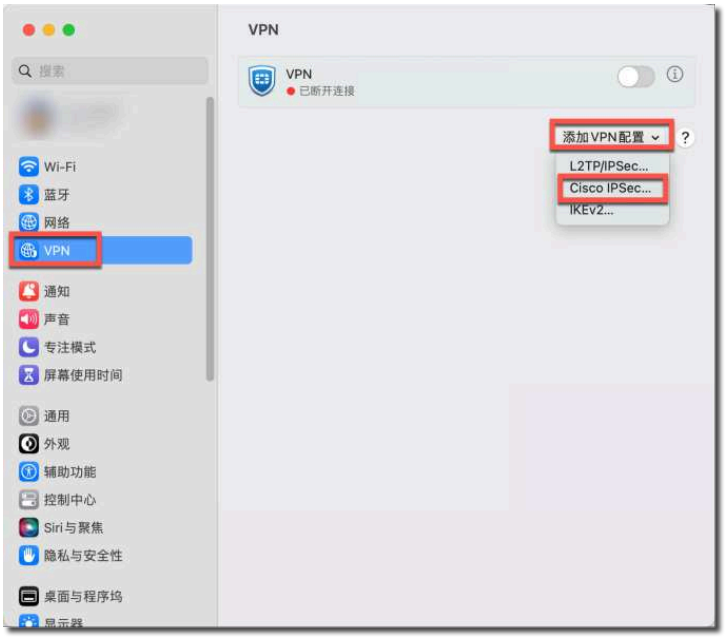

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
地址和地址组：
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
    edit "macOS_IKEv1_range"
        set type iprange
        set comment "VPN: macOS_IKEv1 (Created by VPN wizard)"
        set start-ip 10.10.100.1
        set end-ip 10.10.100.100
    next
end

config firewall addrgrp
    edit "macOS_IKEv1_split"
        set member "LAN_10.10.1.0/24"
        set comment "VPN: macOS_IKEv1 (Created by VPN wizard)"
    next
end
```

```
允许客户端访问内网VPN资源的防火墙策略：
config firewall policy
    edit 1
        set name "vpn_macOS_IKEv1_remote_0"
        set srcintf "macOS_IKEv1"
        set dstintf "port3"
        set action accept
        set srcaddr "macOS_IKEv1_range"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
        set nat enable
        set comments "VPN: macOS_IKEv1 (Created by VPN wizard)"
    next
end
```

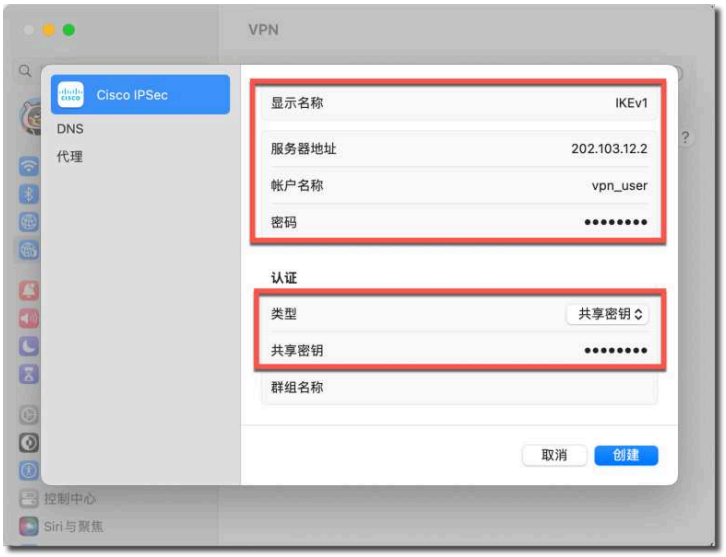
客户端配置

1. 打开系统设置→VPN，点击“添加VPN配置”，选择Cisco IPSec VPN。

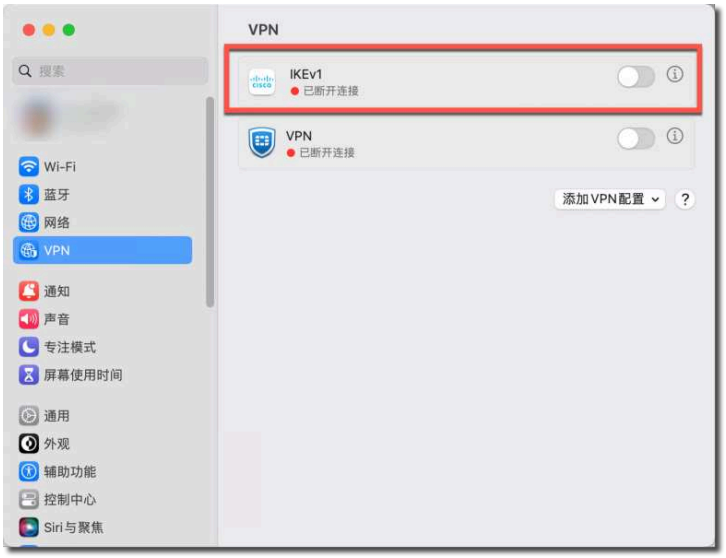


2. 填写VPN名称、服务器IP、用户名、用户密码，认证类型选择共享密钥，填写预共享密钥，其他不填写（如果想要使用群组名称，请在FortiGate侧配置），点击创建按钮建立IPSec。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



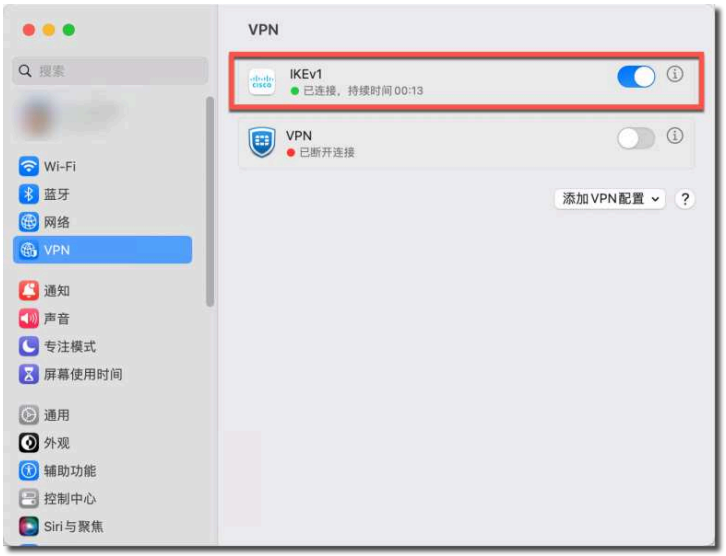
3. VPN连接配置完成。



结果验证

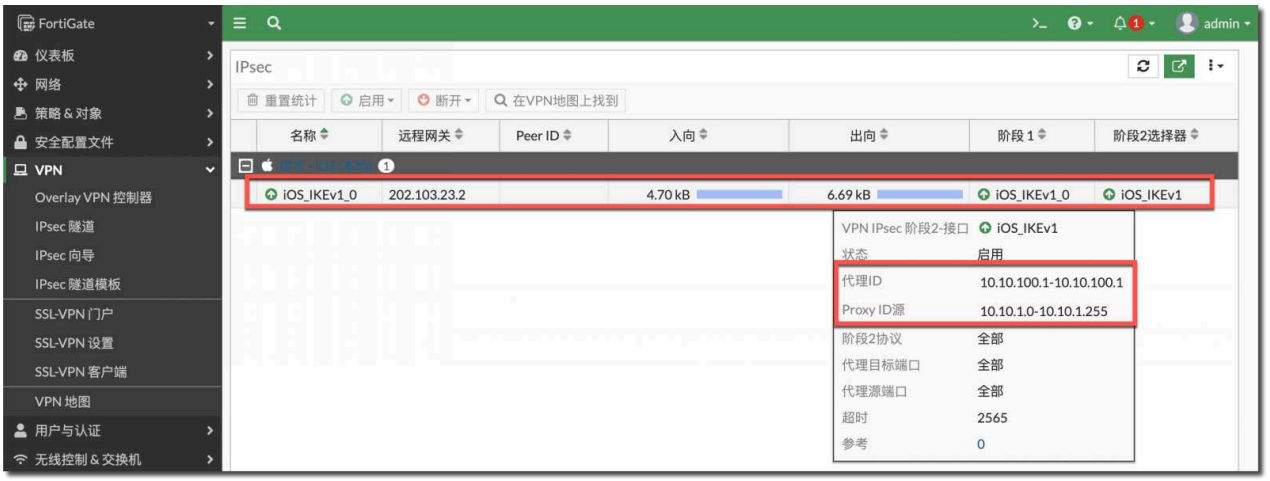
1. 在客户端点击连接按钮，查看连接状态，点击VPN连接右侧的信息按钮，可以看到连接的具体信息，获取的IP为FortiGate配置的网段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 在FortiGate侧查看IPSec连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: macOS_IKEv1_0
version: 1
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:60417
tun_id: 10.10.100.1/::10.0.0.4
remote_location: 0.0.0.0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

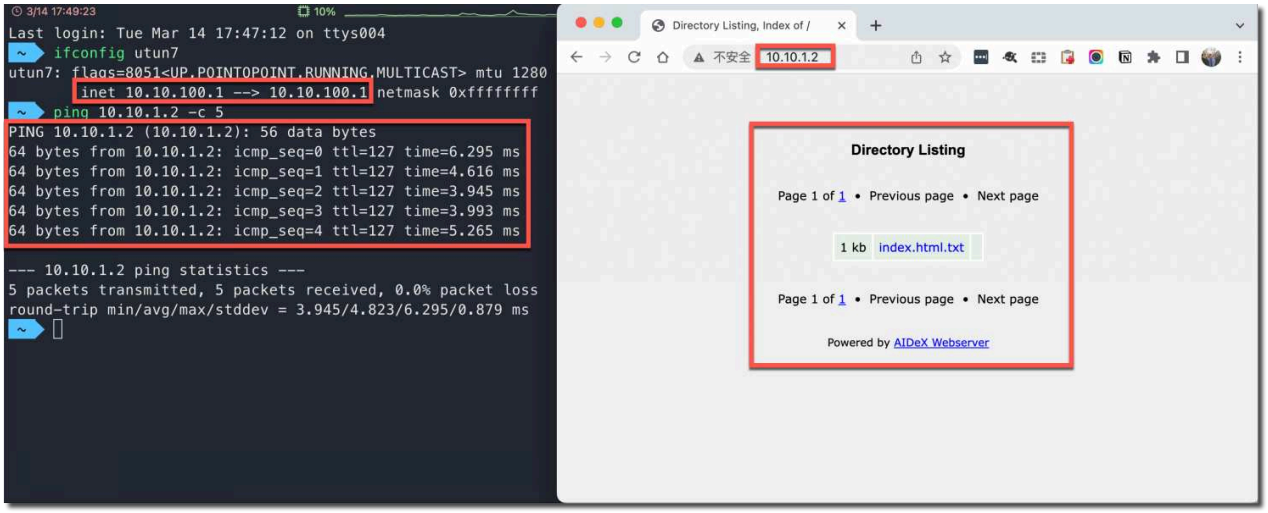
```
network-id: 0
created: 1144s ago
xauth-user: vpn_user
2FA: no
assigned IPv4 address: 10.10.100.1/255.255.255.255
nat: peer
IKE SA: created 1/1  established 1/1  time 60/60/60 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms
  id/spi: 2 1ab45dd9b8ad53a1/229987eaaab4142e
  direction: responder
  status: established 1144-1144s ago = 60ms
  proposal: aes256-sha256
  key: 26d033d72c0d55fe-6652a7159cf151dd-1113c3dd29c29cf9-74dabccc059f96ac
  lifetime/rekey: 3600/2185
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=macOS_IKEv1 ver=1 serial=1 202.103.12.2:0→0.0.0.0:0 tun_id=10.0.0.1 tun_id6=::10.0.0.1 dst_mtu=0 dpd-link=on
weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=42957570 olast=42957570 ad=/0
stat: rxp=115 txp=96 rxb=10525 txb=16656
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=macOS_IKEv1_0 ver=1 serial=4 202.103.12.2:4500→202.103.23.2:60417 tun_id=10.10.100.1 tun_id6=::10.0.0.4
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=macOS_IKEv1 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=873 olast=873 ad=/0
stat: rxp=51 txp=44 rxb=4704 txb=6692
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=silent draft=32 interval=10 remote_port=60417
proxyid=macOS_IKEv1 proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:10.10.1.0-10.10.1.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20083 type=00 soft=0 mtu=1422 expire=2440/0B replaywin=2048
       seqno=2d esn=0 replaywin_lastseq=00000033 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3588/3600
  dec: spi=f3a58344 esp=aes key=32 a8ff490c9fb2e89be964d1a6993b11eedf71191e520ca99ed294c8eb4ea26301
       ah=sha256 key=32 7be5011c5d5a80768497ea9a4421bf8016797480cf6e31bd887d7367db35f30b
  enc: spi=05a9cf2e esp=aes key=32 83392937fdf5872826b529822a07a81c22e076d7bd648c8887451a2ce51b8336
       ah=sha256 key=32 a1897271122f887c59149acb755abc2959d1916a2c3340a35ef40f7172809d9b
  dec:pkts/bytes=102/9408, enc:pkts/bytes=88/16868
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=2 dec_npuid=0 enc_npuid=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

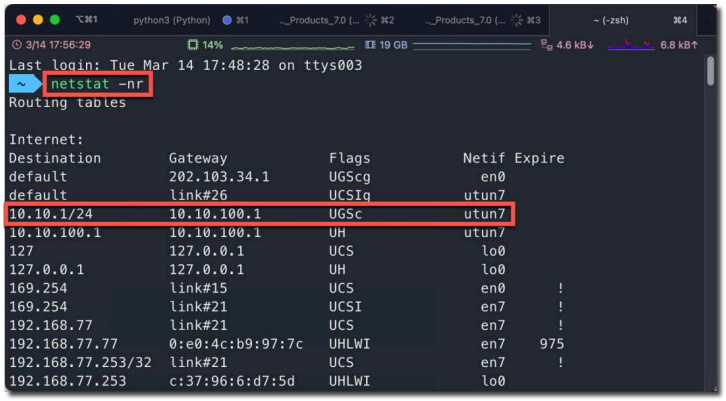
```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=25(macOS_IKEv1)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 查看客户端的路由表（netstat -nr），可以看到隧道分割的路由。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

macOS原生客户端接入IPSec（IKEv2预共享密钥认证）

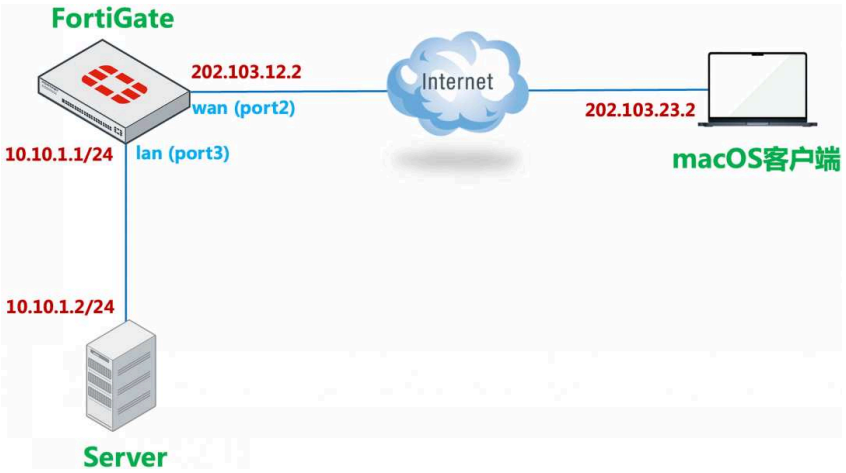
重要

本文基于macOS 13.2编写。

网络需求

通过macOS原生客户端（IKEv2预共享密钥认证）连接FortiGate的IPSec，并访问VPN内部资源。

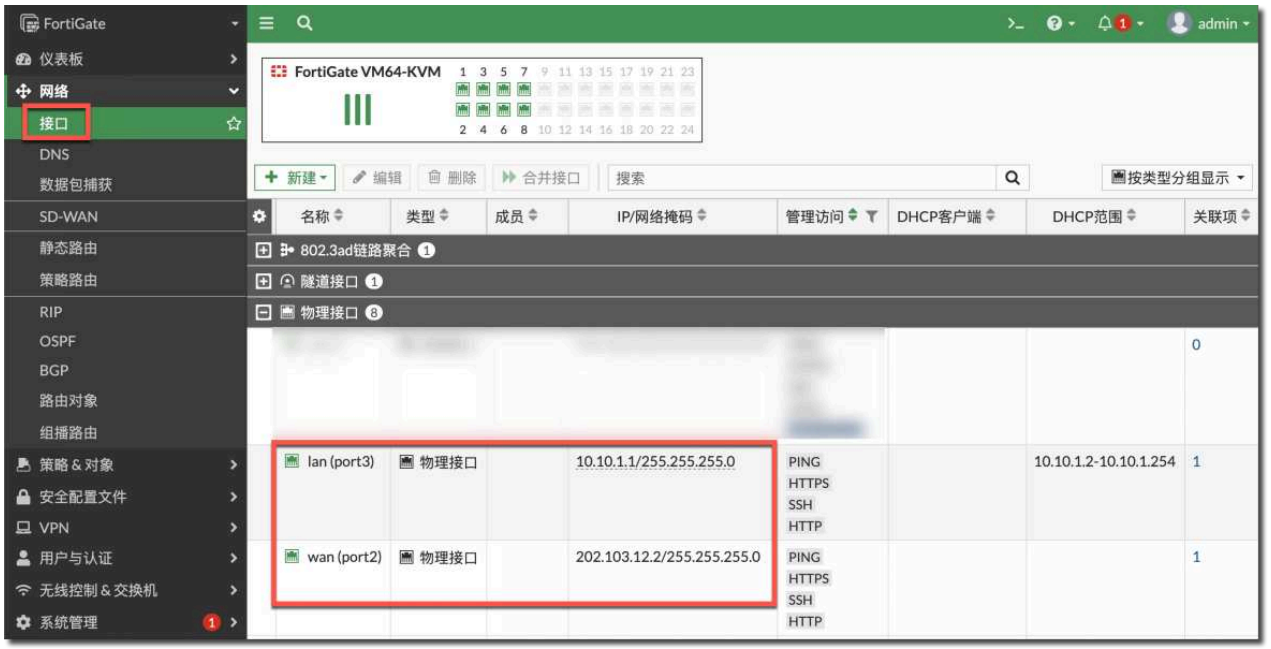
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。

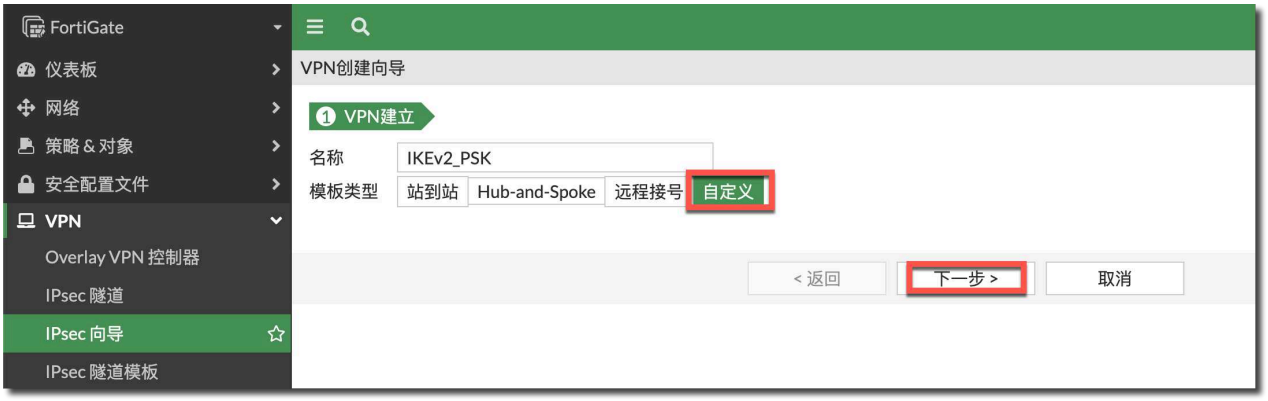


2. 进入FortiGate的VPN→IPSec隧道页面，点击新建按钮，新建IPSec隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 填写VPN名称，模版选择自定义，点击下一步。



4. 按照下图修改配置，其他配置保持默认即可，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

如果开启了隧道分割，本地地址不要填写为0.0.0.0/0，否则会导致客户端连接失败。

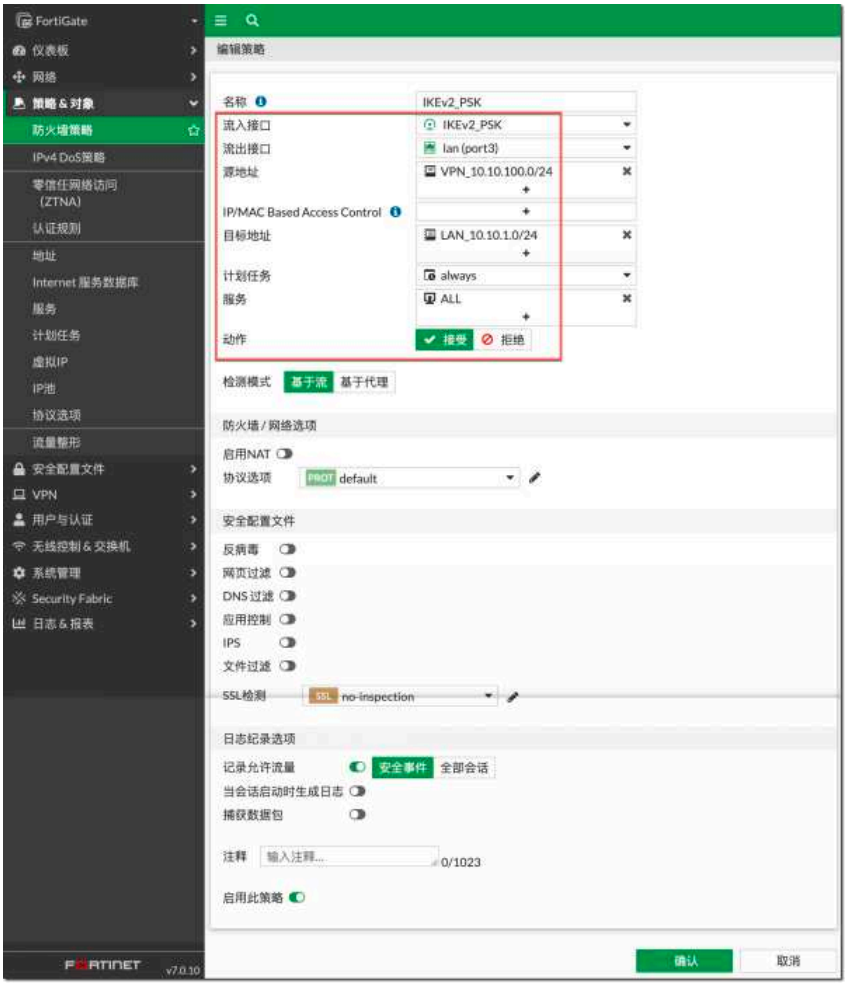
5. 对应的CLI如下：

```
第一阶段配置:
config vpn ipsec phase1-interface
    edit "IKEv2_PSK"
        set type dynamic
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device disable
        set mode-cfg enable
        set ipv4-dns-server1 10.10.1.2
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100
        set ipv4-split-include "LAN_10.10.1.0/24"
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end

第二阶段配置:
config vpn ipsec phase2-interface
    edit "IKEv2_PSK"
        set phase1name "IKEv2_PSK"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
        set pfs disable
        set keepalive enable
    next
end
```

```
地址对象:
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
end
```

6. 配置防火墙策略，允许客户端访问内网VPN资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
客户端地址对象:
config firewall address
    edit "VPN_10.10.100.0/24"
        set subnet 10.10.100.0 255.255.255.0
    next
end

防火墙策略:
config firewall policy
    edit 1
        set name "IKEv2_PSK"
        set srcintf "IKEv2_PSK"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

客户端配置

1. 打开系统设置→VPN，点击“添加VPN配置”，选择IKEv2。

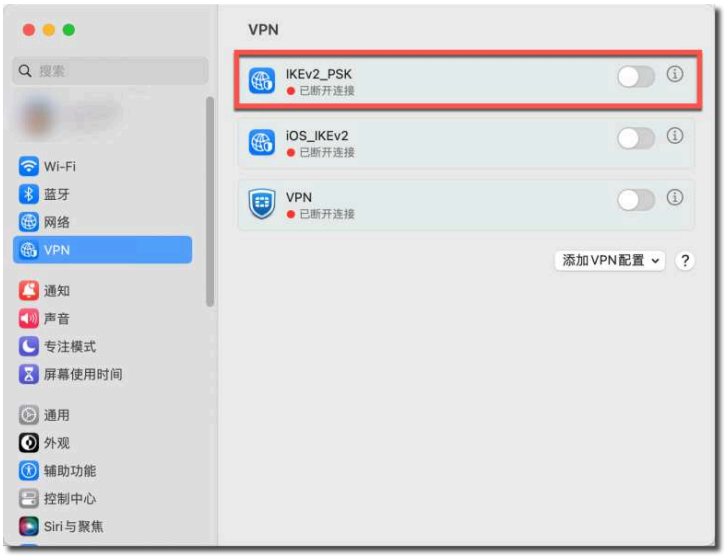
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 填写VPN名称、服务器IP，远程ID随意填写，用户认证选择“无”，机器认证选择“共享密钥”，填写预共享密钥，点击创建完成客户端VPN配置。



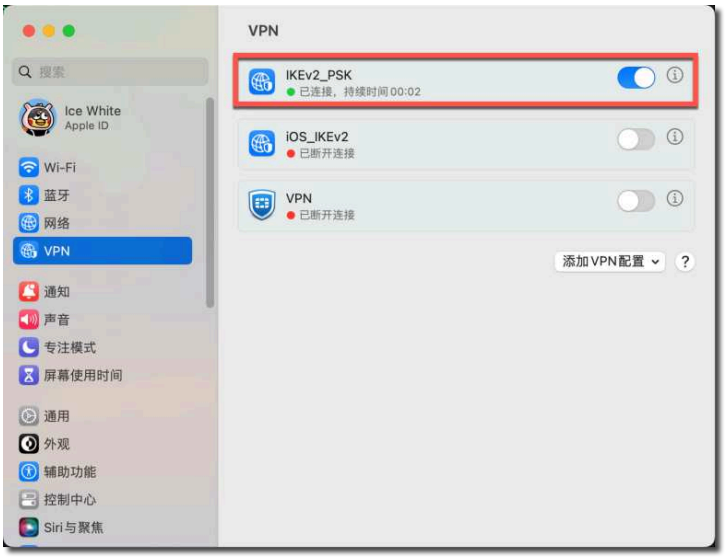
3. VPN连接配置完成。

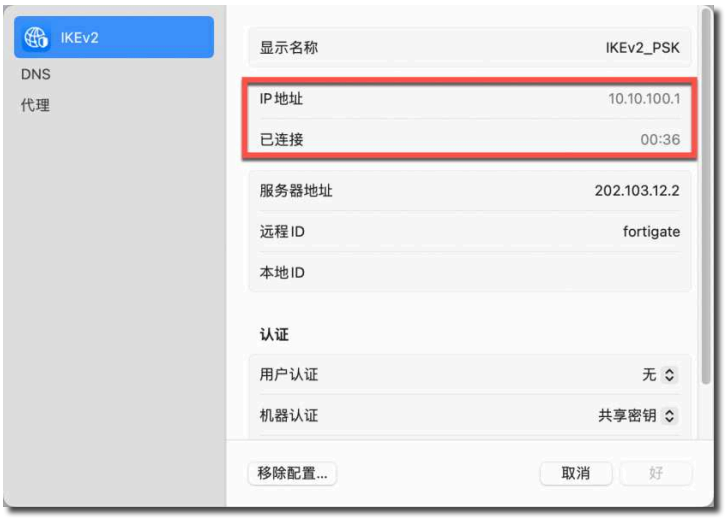


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

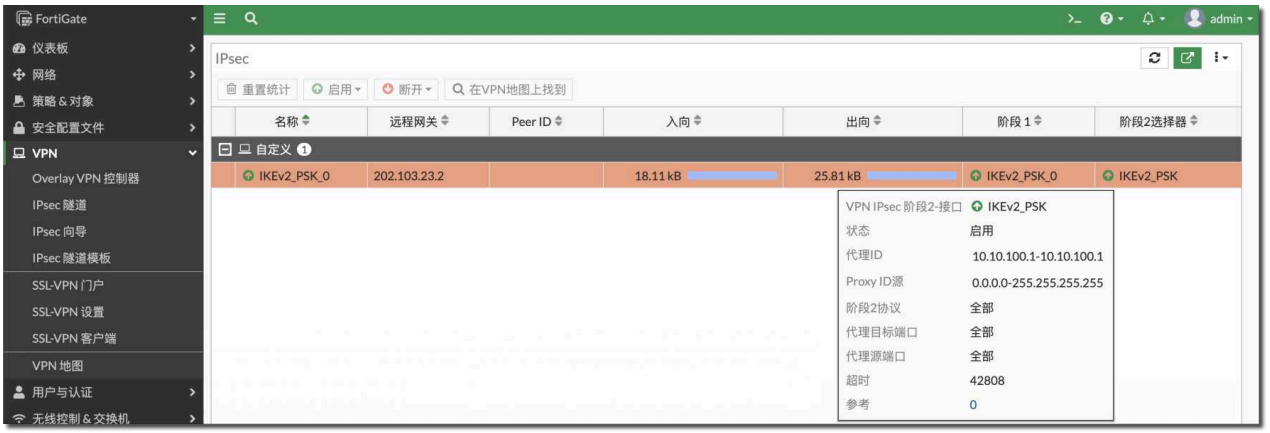
结果验证

1. 在客户端点击连接按钮，查看连接状态，点击VPN连接右侧的信息按钮，可以看到连接的具体信息，获取的IP为FortiGate配置的网段。





2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: IKEv2_PSK_0
version: 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

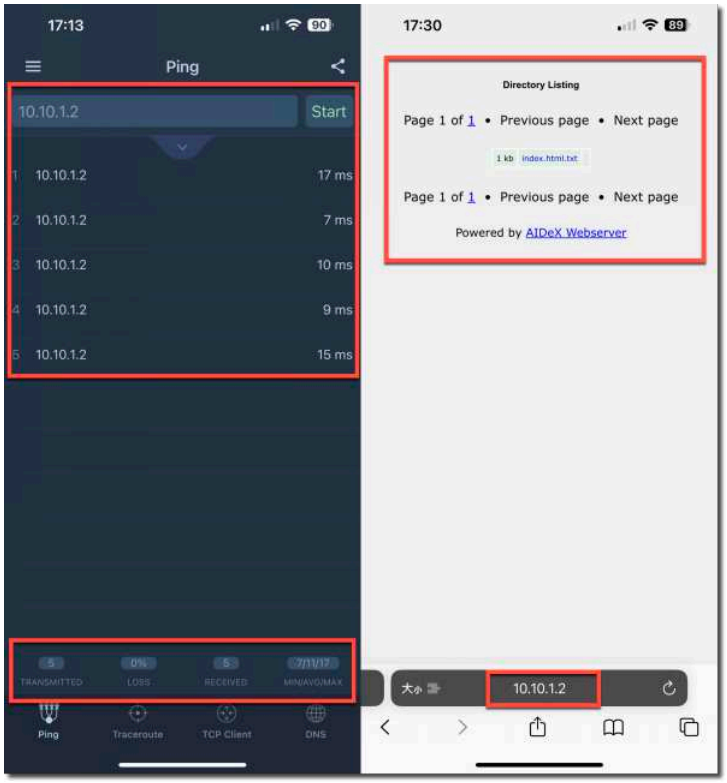
```
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:64916
tun_id: 10.10.100.1/::10.0.0.12
remote_location: 0.0.0.0
network-id: 0
created: 27s ago
assigned IPv4 address: 10.10.100.1/255.255.255.255
nat: peer
PPK: no
IKE SA: created 1/1  established 1/1  time 370/370/370 ms
IPsec SA: created 1/1  established 1/1  time 110/110/110 ms
  id/spi: 16 675a02dbbef8cc4a/096820e48922db26
  direction: responder
  status: established 27-27s ago = 370ms
  proposal: aes256-sha256
  child: no
  SK_ei: d5113c70c4d78f54-f34f30091bf79475-aa35a97d71c0a5aa-2c9859861946d414
  SK_er: 9414d48bd22ecbc1-709aa14d0de11cd6-64b0829447435a9f-3b31a85afdeeff38
  SK_ai: 36305c3ad8a415b5-bee89c242a7faf32-04dee1ec7526fd4d-d952bf68c9014731
  SK_ar: 13adcd000ee30fde-d6c84d005c113924-1c3866f0d5b8a973-224225fb19d7e865
  PPK: no
  message-id sent/recv: 0/2
  lifetime/rekey: 86400/86102
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=IKEv2_PSK_0 ver=2 serial=13 202.103.12.2:4500→202.103.23.2:64916 tun_id=10.10.100.1 tun_id6=::10.0.0.12
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=IKEv2_PSK index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=533 txp=28 rxb=48088 txb=2804
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=64916
proxyid=IKEv2_PSK proto=0 sa=1 ref=15 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20483 type=00 soft=0 mtu=1422 expire=43160/0B replaywin=2048
       seqno=1d esn=0 replaywin_lastseq=00000215 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43191/43200
  dec: spi=4d83686c esp=aes key=32 ccab803299265af9f609977a5bb055b3c66537ac6500719ba9c78d4fa04b6738
       ah=sha256 key=32 b808b44ed4d288c2a2d518f1ff6bf6380c20247cbb1ed2bd3c3ffb3779854d34
  enc: spi=093170d2 esp=aes key=32 63423c52af9b3e35dcccfd7e9d0d1ceaca390652a45506419d8a339e89a5b714
       ah=sha256 key=32 a66edb55e69ac116d48c073458319388b2b413966a273f38898e22580b93adfe
  dec:pkts/bytes=1066/96176, enc:pkts/bytes=56/7812
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=a dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=IKEv2_PSK ver=2 serial=e 202.103.12.2:0→0.0.0.0:0 tun_id=10.0.0.7 tun_id6=::10.0.0.7 dst_mtu=0 dpd-link=on
weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=43033783 olast=43033783 ad=/0
stat: rxp=3330 txp=1051 rxb=236299 txb=103007
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=25(IKEv2_PSK)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

实际测试iOS/macOS使用IKEv2，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

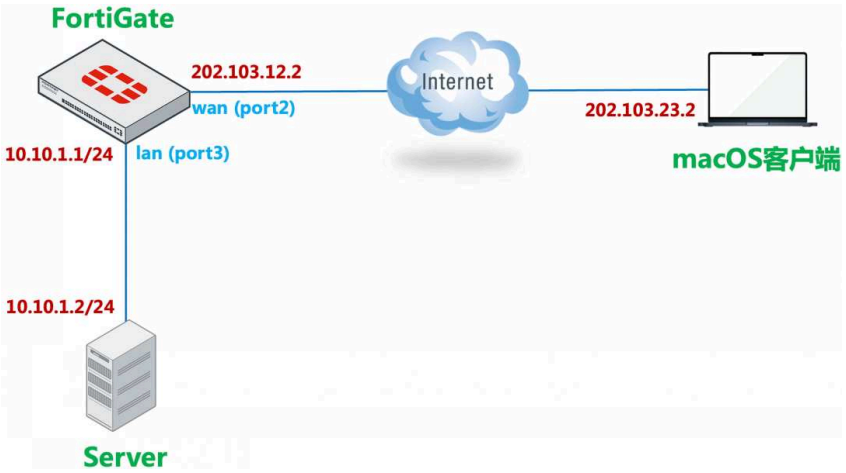
macOS原生客户端接入IPSec（用户名/密码+预共享密钥认证）

> **重要**
>
> 本文基于macOS 13.2编写。

网络需求

通过macOS原生客户端（IKEv2用户名/密码+预共享密钥认证）连接FortiGate的IPSec，并访问VPN内部资源。

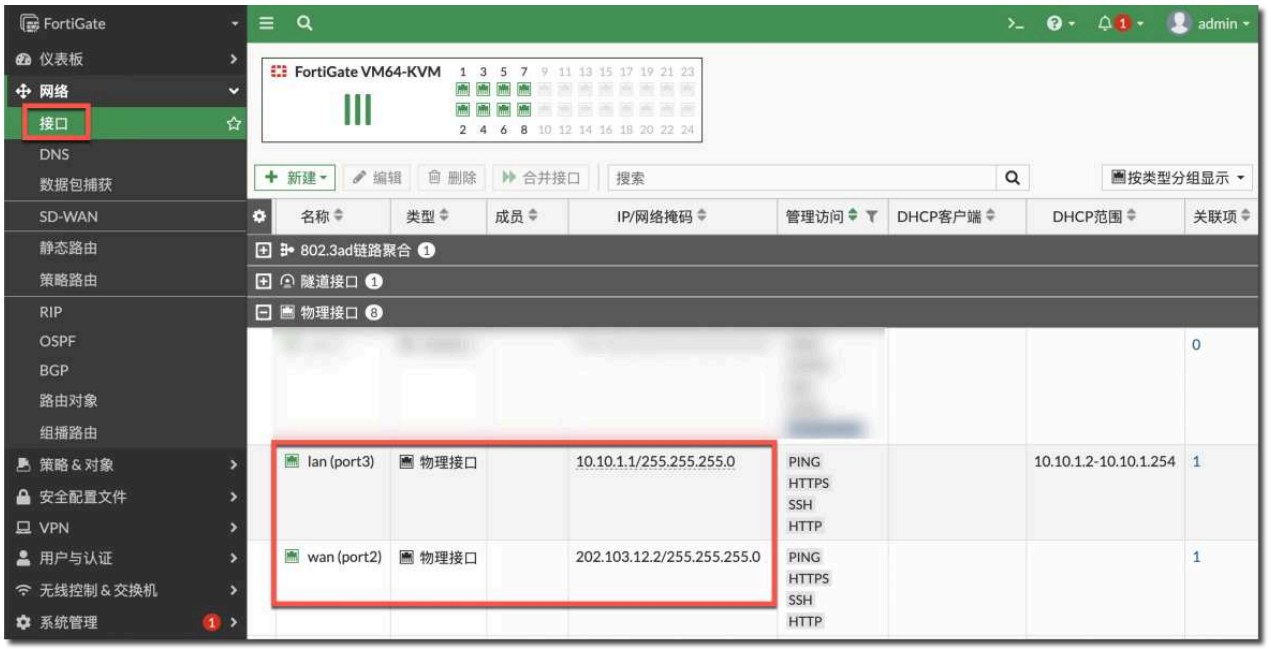
网络拓扑



配置步骤

FortiGate配置

1. 配置FortiGate的接口IP。



2. 创建本地VPN用户和用户组，参考用户与认证→本地用户和用户组↗章节（如需使用远程认证，请参考用户与认证→LDAP认证→LDAP认证配置与排错↗或用户与认证→Radius认证→Radius认证配置与排错↗章节）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
config user local
    edit "vpn_user"
        set type password
        set passwd xxxxxxxx
    next
end
```




```
config user group
    edit "VPN"
        set member "vpn_user"
    next
end
```

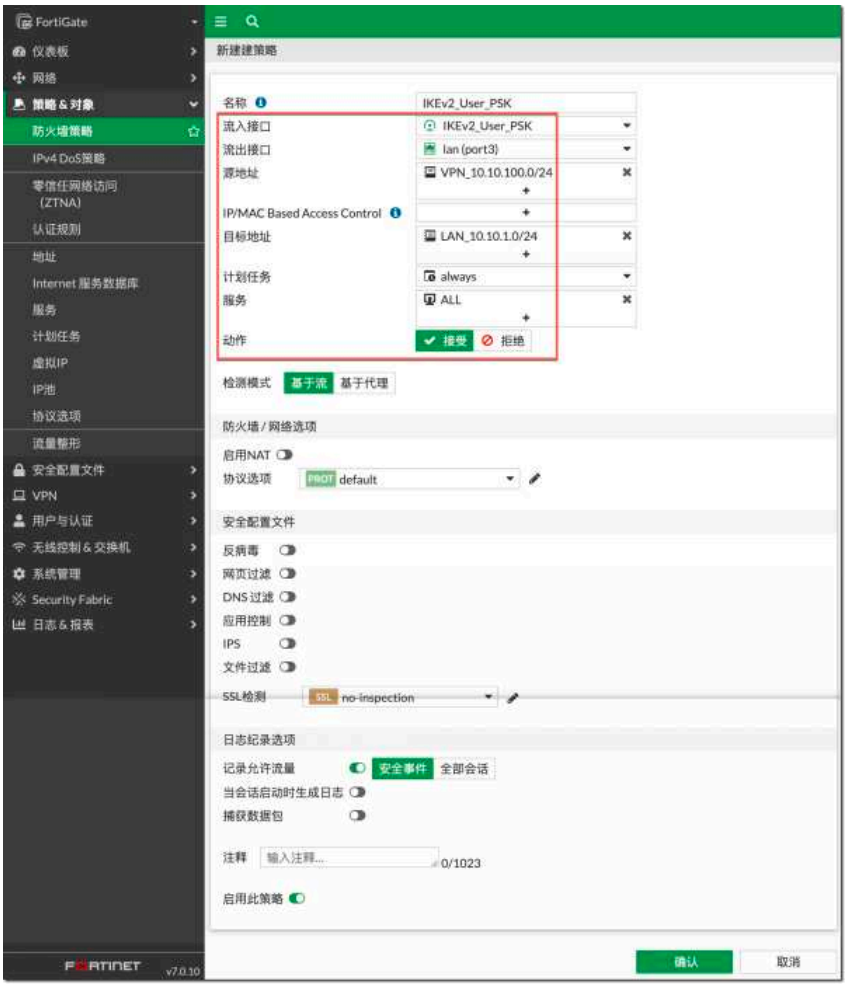
3. 该种方式的IPSec需要使用CLI方式配置，分别配置IPSec一阶段和二阶段。

```
IPSec一阶段配置:
config vpn ipsec phase1-interface
    edit "IKEv2_User_PSK"
        set type dynamic
        set interface "port2"
        set ike-version 2    //IKE协议2
        set peertype any
        set net-device disable
        set mode-cfg enable    //开启为客户端分配IP
        set ipv4-dns-server1 10.10.1.2  //为客户端分配的DNS地址
        set proposal aes256-sha256
        set negotiate-timeout 300
        set dpd on-idle
        set dhgrp 14 5 2
        set eap enable    //需要开启EAP做用户密码认证
        set eap-identity send-request    //开启EAP主动发送认证请求
        set authusrgrp "VPN"    //选择认证的用户组
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100    //客户端分配地址范围
        set ipv4-netmask 255.255.255.0
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end

IPSec二阶段配置:
config vpn ipsec phase2-interface
    edit "IKEv2_User_PSK"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set phase1name "IKEv2_User_PSK"
        set proposal aes256-sha256
        set keepalive enable
    next
end
```

4. 配置防火墙策略，允许客户端访问内网VPN资源。




```
VPN资源地址对象:
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
end

客户端地址对象:
config firewall address
    edit "VPN_10.10.100.0/24"
        set subnet 10.10.100.0 255.255.255.0
    next
end

防火墙策略:
config firewall policy
    edit 1
        set name "IKEv2_User_PSK"
        set srcintf "IKEv2_User_PSK"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

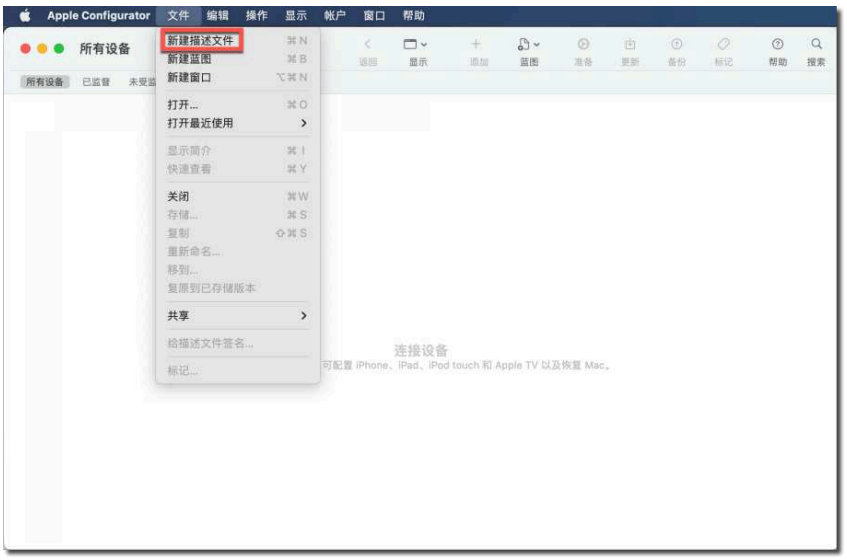
```
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

制作和安装描述文件

重要

想要使用IKEv2用户名/密码+预共享密钥方式的VPN认证，需要使用Apple Configurator工具为iOS/macOS制作描述文件，该工具可以在macOS下的App Store中下载。

1. 打开Apple Configurator，点击菜单栏的“文件→新建描述文件”（或使用快捷键Command + N）。

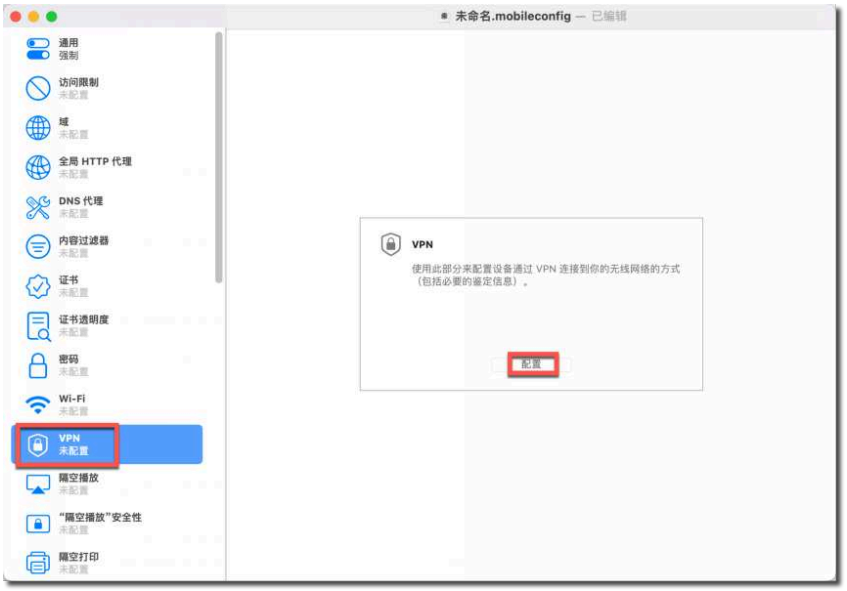


2. 在弹出的配置文件编辑器中，配置描述文件的名称。



3. 选择VPN选项卡，点击配置按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置描述文件，选择连接类型为IKEv2，填写服务器IP地址，远程标识符和局部标识符随意填写，填写预共享密钥，开启EAP，选择EAP鉴定为用户名/密码模式，其他配置保持默认即可（或根据实际需求更改）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 选择菜单栏的“文件→存储”按钮（或使用快捷键Command + S），保存该描述文件到本地。

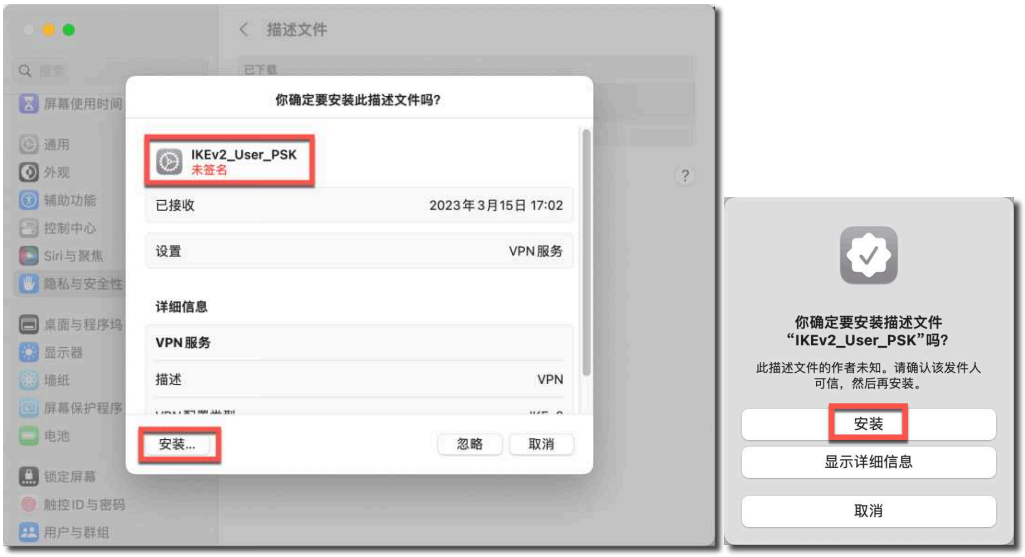


6. 将描述文件发送至客户端macOS电脑中，macOS下直接双击该描述文件安装，会弹出系统提示，在系统设置中查看该描述文件。

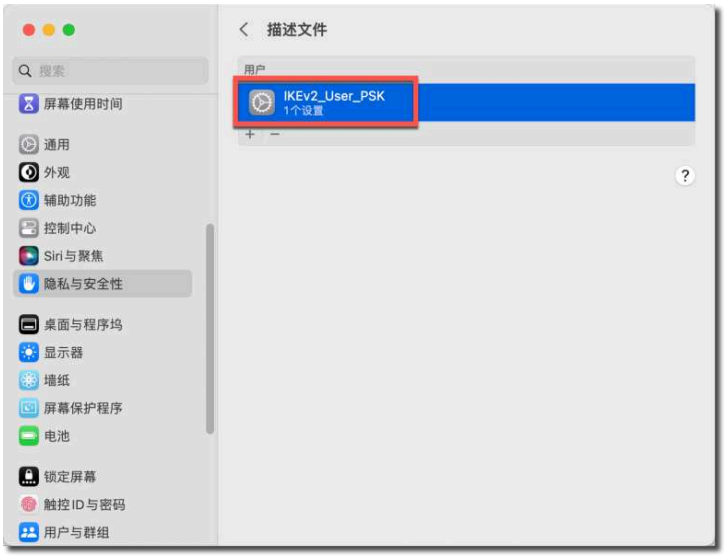
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 进入系统设置→隐私与安全→其他→描述文件，双击“已下载”中的描述文件，确认描述文件无误后，点击安装按钮，在弹出的确认框中点击“安装”（随后需要系统密码验证）。



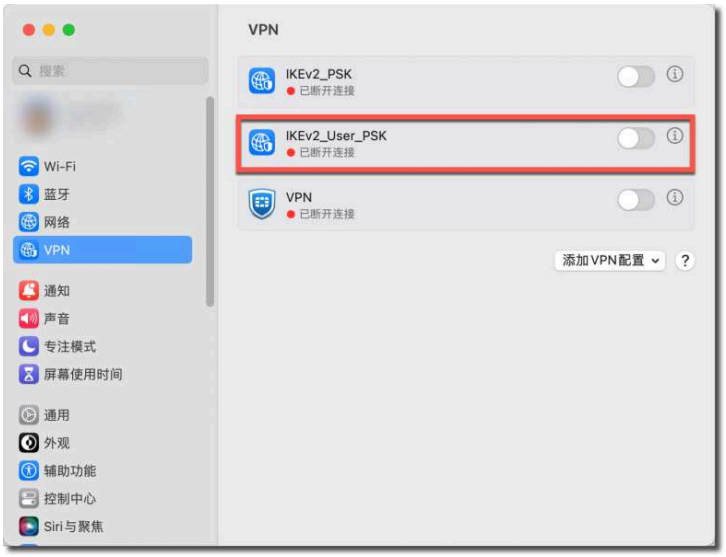
8. 描述文件安装完成。



客户端配置

1. 打开系统设置→VPN，可以看到描述文件中的VPN连接已经自动添加。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



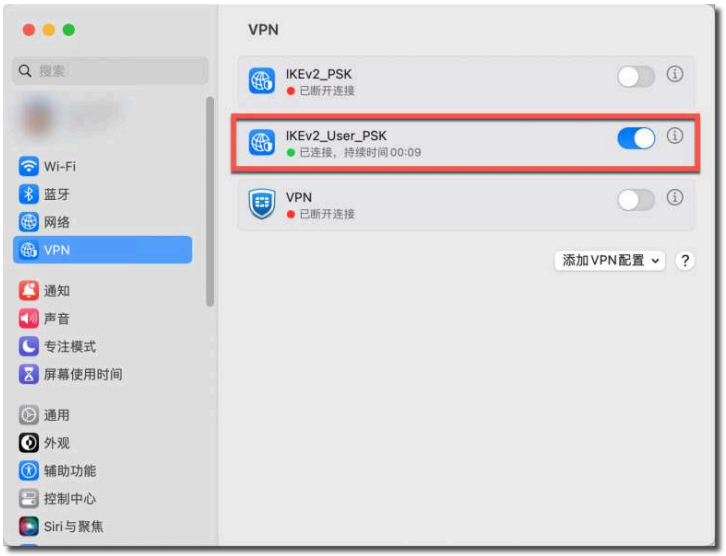
2. 编辑该VPN连接，将“用户认证”修改为“用户名”，并填写用户名和密码，点击“好”保存配置。

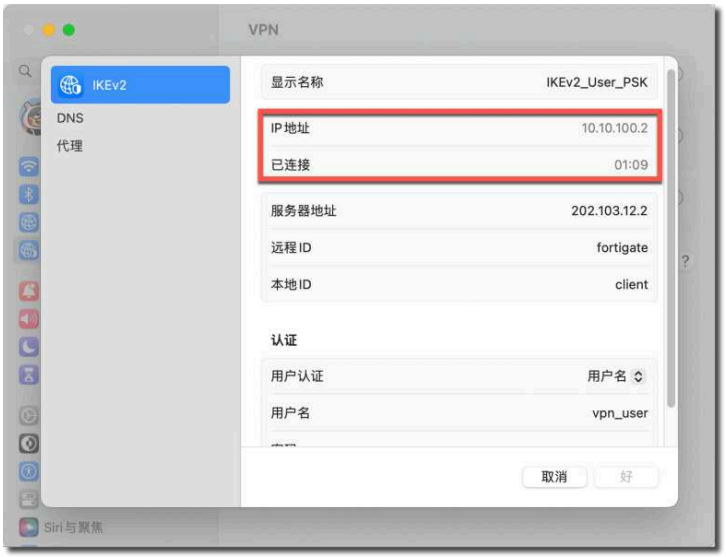


结果验证

1. 在客户端点击连接按钮，查看连接状态，点击VPN连接右侧的信息按钮，可以看到连接的具体信息，获取的IP为FortiGate配置的网段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: IKEv2_User_PSK_1
version: 2
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:60422
tun_id: 10.10.100.2/::10.0.0.18
remote_location: 0.0.0.0
network-id: 0
created: 304s ago
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

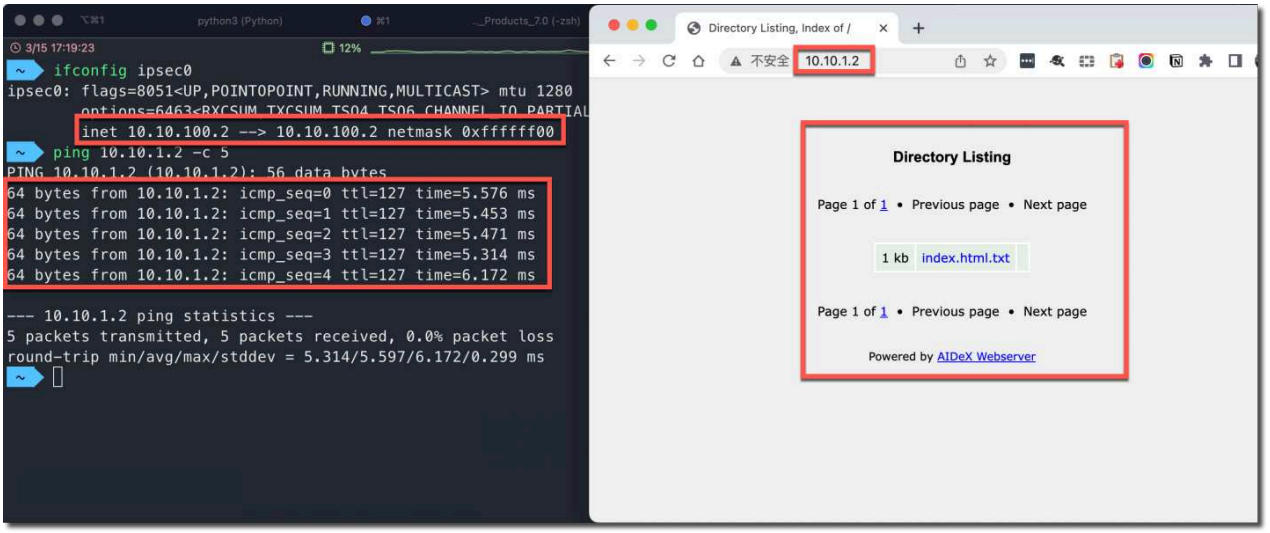
```
eap-user: vpn_user
2FA: no
peer-id: client
peer-id-auth: no
assigned IPv4 address: 10.10.100.2/255.255.255.0
nat: peer
PPK: no
IKE SA: created 1/1  established 1/1  time 80/80/80 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms
  id/spi: 15 4d29f0750955cfd8/2910aaac36020ad6
  direction: responder
  status: established 304-304s ago = 80ms
  proposal: aes256-sha256
  child: no
  SK_ei: c447820d037114b1-50c54fe2851c9be3-0a85e0a1dd660bda-44fb37b6cdfac588
  SK_er: e674721b86f9e390-bdb97e39262e21de-08c0ceeb85f8f4e9-4cd4237c6e4b45a2
  SK_ai: 49d92f240fce91f9-933fa239f76db314-21b8279f552a327f-fbdbed66fbe4a30f
  SK_ar: 68e4bee505827ac5-72af90407c973fe0-34ef0b85985cea0e-a596b75344157af4
  PPK: no
  message-id sent/recv: 0/6
  lifetime/rekey: 86400/85825
  DPD sent/recv: 00000000/00000000
  peer-id: client

FortiGate # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=IKEv2_User_PSK ver=2 serial=14 202.103.12.2:0→0.0.0.0:0 tun_id=10.0.0.9 tun_id6=::10.0.0.9 dst_mtu=0 dpd-
link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=43041062 olast=43041062 ad=/0
stat: rxp=5440 txp=1378 rxb=374506 txb=142425
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
------------------------------------------------------
name=IKEv2_User_PSK_1 ver=2 serial=1b 202.103.12.2:4500→202.103.23.2:60422 tun_id=10.10.100.2 tun_id6=::10.0.0.18
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=IKEv2_User_PSK index=1
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=2638 txp=815 rxb=176380 txb=80140
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=60422
proxyid=IKEv2_User_PSK proto=0 sa=1 ref=97 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.2-10.10.100.2:0
  SA:  ref=3 options=20683 type=00 soft=0 mtu=1422 expire=42881/0B replaywin=2048
       seqno=330 esn=0 replaywin_lastseq=00000a4e qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=7b8ba379 esp=aes key=32 7ba541f88e4abc0197580faa828f71aac8f501399ff5962c96bc5ae43c037ece
       ah=sha256 key=32 e2082800cf7dce1c6796d3080969319ec9e52b536e1ba4d4edeefc165f76ff4e
  enc: spi=011f2d7b esp=aes key=32 01b2eb5d0ad5876f35f60382599e97fe84eed38d6023fb8bb45f42893a3da0dd
       ah=sha256 key=32 30d5bed3a56098c277f1213e94bb792bffff86074edfe64dc8761bee1c0403fa
  dec:pkts/bytes=5276/352760, enc:pkts/bytes=1630/223528
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=10 dec_npuid=0 enc_npuid=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0→10.10.100.2/32 pref=0.0.0.0 gwy=10.10.100.2
dev=27(IKEv2_User_PSK)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

实际测试iOS/macOS使用IKEv2，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Windows原生客户端接入IPSec IKEv1（L2TP over IPSec）

重要

本文基于Windows 10专业版编写。

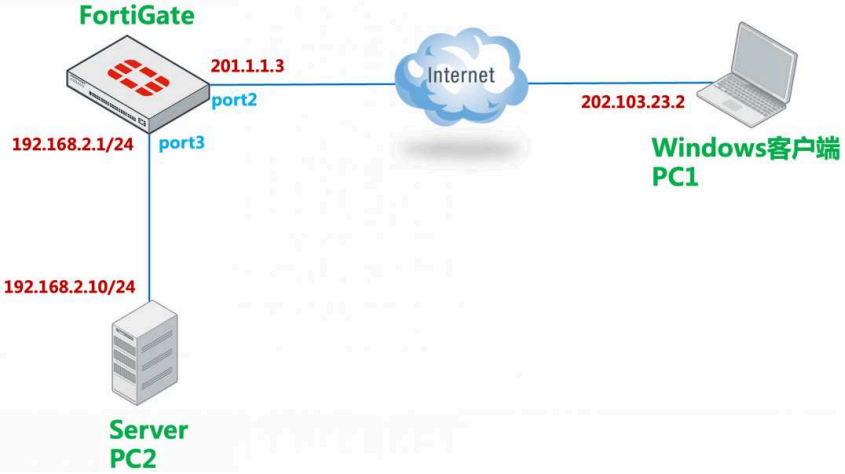
网络需求

通过Windows原生客户端（IKEv1）连接FortiGate的IPSec，并访问VPN内部资源。

重要

Windows系统使用IKEv1，必须配合L2TP使用，也就是L2TP over IPSec。

网络拓扑



配置步骤

配置FortiGate

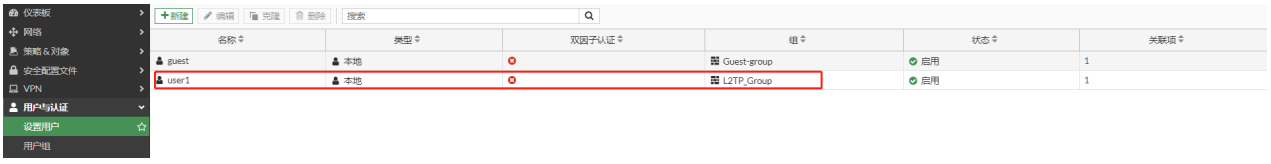
1. 基础配置



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

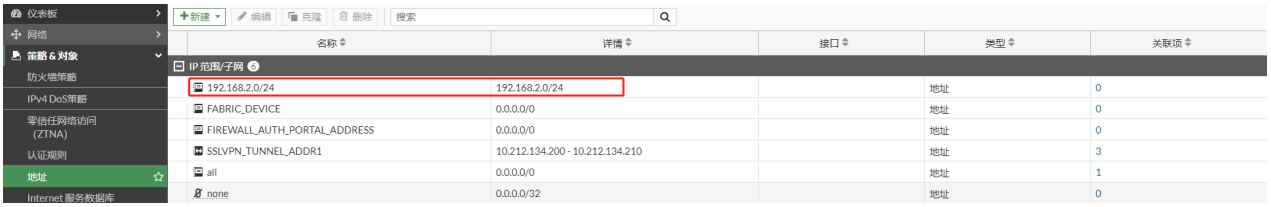


2. 创建用户并将用户加入到用户组





3. 创建地址对象



4. 配置L2TP over IPSEC VPN

选择“IPsec隧道”，点击“新建”，选择“远程拨号”-->"Native"--> “Windows Native”，然后点击下一步。



设置流入接口，预共享秘钥及用户组。



设置本地接口，地址地址以及客户端地址范围。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



VPN向导即将创建的对象。



创建完成。



查看配置

通过“VPN创建向导”可以很方便的配置VPN，但我们需要知道向导具体做了哪些配置。

1. 创建IPSEC VPN



对应的命令行

```
config vpn ipsec phase1-interface
    edit "L2TP_over_IPSEC"
        set type dynamic
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal aes256-md5 3des-sha1 aes192-sha1
        set comments "VPN: L2TP_over_IPSEC (Created by VPN wizard)"
        set dhgrp 2
        set wizard-type dialup-windows
        set psksecret ENC
DCMMcDpdFzv7KXC1lwF5xK3SdOBK0RXf8G8UhEXU+wFRq58XOOoZOcDVaKxLd/mBg1CgkwMqEEXV+IwHs1kpFOTfoGAG428fkKO8BmwlfmDerRWCu5
W8IcI6DwsDF1PllXIefGl+3H2tjySQ8gm6SeBCKD6XLFjRVlHIW+EwJiTfC1c+bPIEBq60ii9Puckspiec0g==
    next
end
config vpn ipsec phase2-interface
    edit "L2TP_over_IPSEC"
        set phase1name "L2TP_over_IPSEC"
        set proposal aes256-md5 3des-sha1 aes192-sha1
```

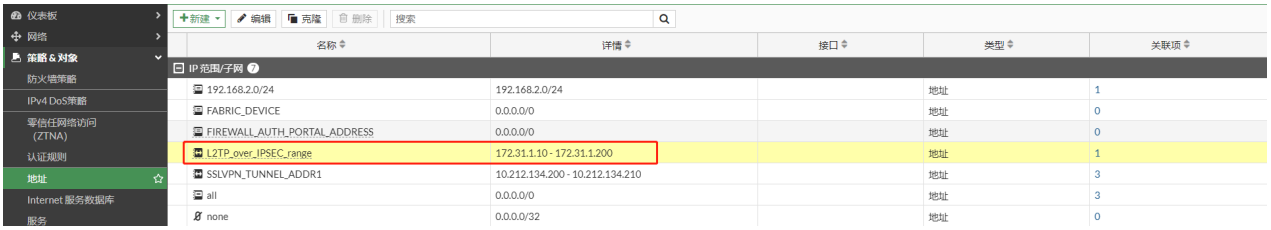

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set pfs disable
        set encapsulation transport-mode
        set l2tp enable
        set comments "VPN: L2TP_over_IPSEC (Created by VPN wizard)"
        set keylifeseconds 3600
    next
end
```

2. 创建L2TP

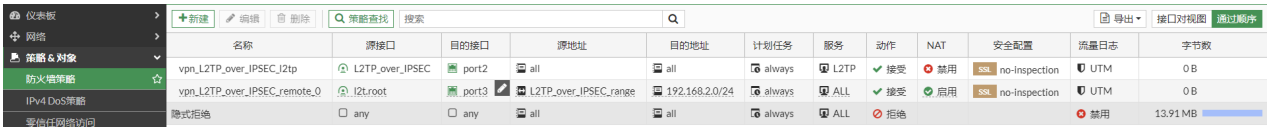
```
config vpn l2tp
    set status enable
    set eip 172.31.1.200
    set sip 172.31.1.10
    set usrgrp "L2TP_over_IPSEC_Group"
end
```

3. 创建地址对象

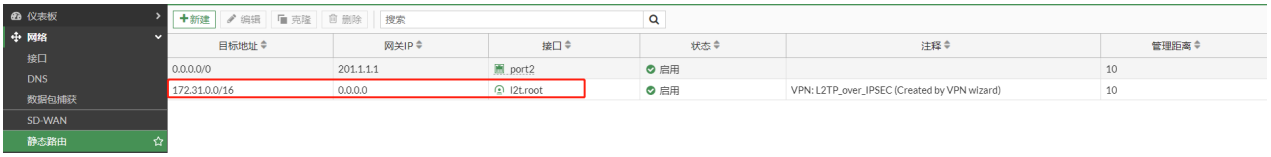


4. 创建策略

第1条是L2TP over IPSEC的策略；第2条是L2TP到内网的策略。模板没有创建到Internet的策略，如果有需求，则要单独创建。



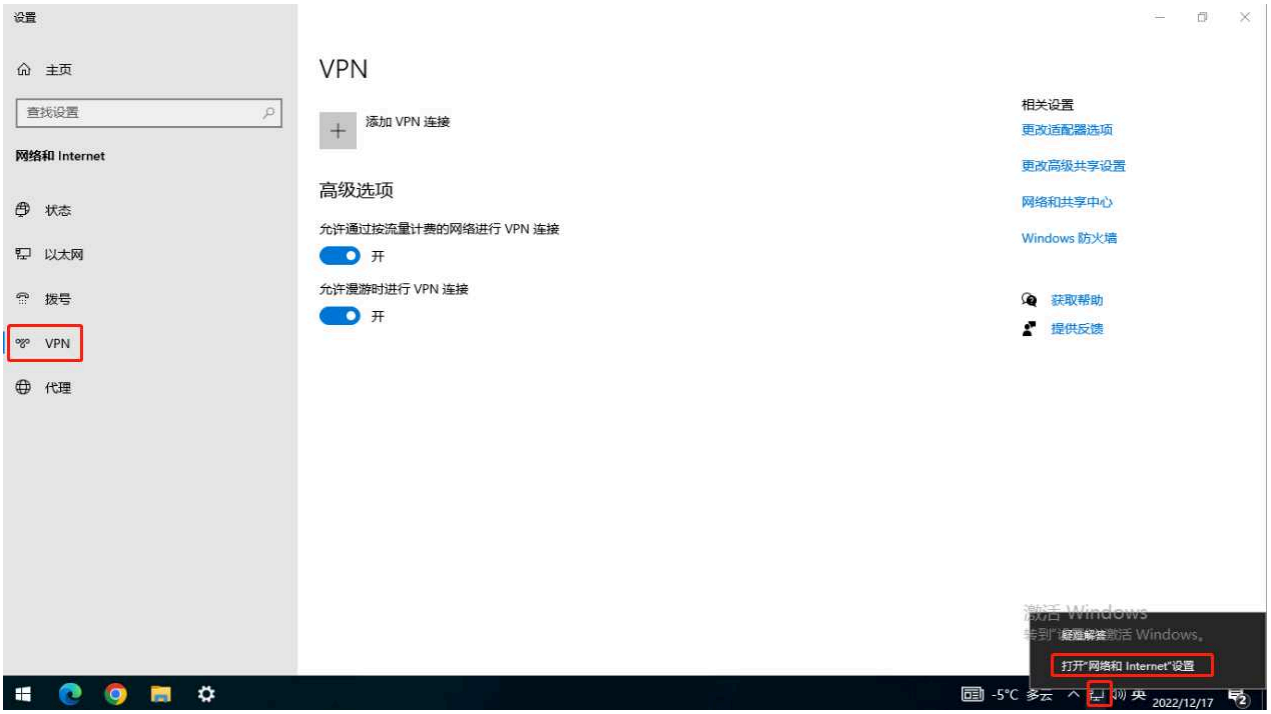
5. 创建路由



配置Windows客户端

1. 右击本地连接图标，选择“打开网络和Internet设置”，选择VPN。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 点击“添加VPN连接”，设置L2TP over IPSEC，然后点击保存。



3. L2TP over IPSEC创建完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



结果验证

1. 点击创建的“L2TP_Over_IPSEC”，点击连接



2. 连接成功

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看L2TP_Over_IPSEC获取的地址

```
C:\Users\admin>ipconfig/all
以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection #2
   物理地址. . . . . . . . . . . . . : 00-0C-29-91-0B-35
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::bc4e:191a:510a:62ba%7(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.1.1.6(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.1.1.1
   DHCPv6 IAID . . . . . . . . . . . : 402656297
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-29-1C-6E-ED-00-0C-29-91-0B-2B
   DNS 服务器  . . . . . . . . . . . : 192.168.91.208
                                       114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

PPP 适配器 L2TP_Over_IPSEC:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : L2TP_Over_IPSEC
   物理地址. . . . . . . . . . . . . :
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   IPv4 地址 . . . . . . . . . . . . : 172.31.1.11(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.255
   默认网关. . . . . . . . . . . . . : 0.0.0.0
   DNS 服务器  . . . . . . . . . . . : 114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

查看路由表

```
C:\Users\admin>route print
===========================================================================
接口列表
 10...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
  5...00 09 0f aa 00 01 ......Fortinet SSL VPN Virtual Ethernet Adapter
 13...00 0c 29 91 0b 2b ......Intel(R) 82574L Gigabit Network Connection
  7...00 0c 29 91 0b 35 ......Intel(R) 82574L Gigabit Network Connection #2
 43...........................L2TP_Over_IPSEC
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
```

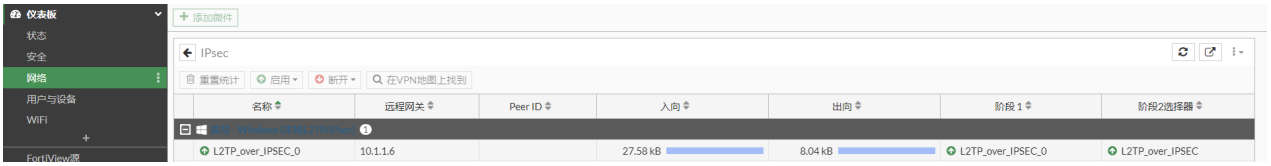

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0         10.1.1.1         10.1.1.6   4506
          0.0.0.0          0.0.0.0            在链路上       172.31.1.11     26
         10.1.1.0    255.255.255.0            在链路上          10.1.1.6   4506
         10.1.1.6  255.255.255.255            在链路上          10.1.1.6   4506
       10.1.1.255  255.255.255.255            在链路上          10.1.1.6   4506
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1   4556
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1   4556
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1   4556
      172.31.1.11  255.255.255.255            在链路上       172.31.1.11    281
        201.1.1.3  255.255.255.255         10.1.1.1         10.1.1.6   4251
```

3. 访问内部主机

```
C:\Users\admin>ping 192.168.2.10

正在 Ping 192.168.2.10 具有 32 字节的数据:
来自 192.168.2.10 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63

192.168.2.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

4. FortiGate查看L2TP over IPSEC连接




```
# diagnose vpn ike gateway list

vd: root/0
name: L2TP_over_IPSEC_0
version: 1
interface: port2 6
addr: 201.1.1.3:500 → 10.1.1.6:500
tun_id: 10.1.1.6/::10.0.0.2
remote_location: 0.0.0.0
network-id: 0
created: 667s ago
IKE SA: created 1/1  established 1/1  time 40/40/40 ms
IPsec SA: created 1/1  established 1/1  time 10/10/10 ms

  id/spi: 0 3074e3c6042e3bd7/445ef45c6bf46ef9
  direction: responder
  status: established 667-667s ago = 40ms
  proposal: 3des-sha1
  key: b894656df6d73056-3c8f6e0801b4977e-f932994583512431
  lifetime/rekey: 28800/27862
  DPD sent/recv: 00000000/00000000

# diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=L2TP_over_IPSEC ver=1 serial=8 201.1.1.3:0→0.0.0.0:0 tun_id=10.0.0.3 tun_id6=::10.0.0.3 dst_mtu=0 dpd-
link=on weight=1
bound_if=6 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0

proxyid_num=0 child_num=1 refcnt=3 ilast=44533053 olast=44533053 ad=/0
stat: rxp=403 txp=180 rxb=30057 txb=8731
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
run_tally=0
--------------------------------------------------------------
name=L2TP_over_IPSEC_0 ver=1 serial=9 201.1.1.3:0->10.1.1.6:0 tun_id=10.1.1.6 tun_id6=::10.0.0.2 dst_mtu=1500 dpd-
link=on weight=1
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/8872 options[22a8]=npu rgwy-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0

parent=L2TP_over_IPSEC index=0
proxyid_num=1 child_num=0 refcnt=6 ilast=0 olast=2 ad=/0
stat: rxp=403 txp=180 rxb=30057 txb=8731
dpd: mode=on-demand on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=L2TP_over_IPSEC proto=17 sa=1 ref=3 serial=1 transport-mode add-route
  src: 17:201.1.1.3-201.1.1.3:1701
  dst: 17:10.1.1.6-10.1.1.6:0
  SA:  ref=3 options=182 type=00 soft=0 mtu=1470 expire=2915/0B replaywin=2048
       seqno=b5 esn=0 replaywin_lastseq=00000193 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=3590/3600
  dec: spi=4b06e27a esp=3des key=24 b4765186ea5f3ac392a6009a3e9173907f2b1872715a317a
       ah=sha1 key=20 75f29e67a8a100e5d7a58b84451675d318b36ee5
  enc: spi=ba90d928 esp=3des key=24 7cbbc629743b42ac00b0ab328129364de3b157c67dfd1a39
       ah=sha1 key=20 e8fd28ceaf0d55c30643495a95af9e5b562d2443
  dec:pkts/bytes=806/60114, enc:pkts/bytes=360/23491
  npu_flag=00 npu_rgwy=10.1.1.6 npu_lgwy=201.1.1.3 npu_selid=6 dec_npuid=0 enc_npuid=0
```

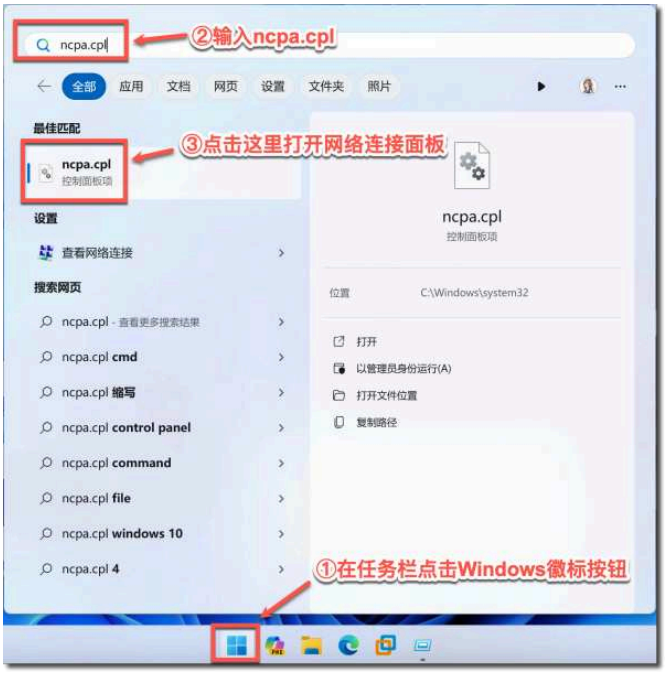
注意事项

如果FortiGate上配置的L2TP用户为LDAP认证用户，则需要确保客户端L2TP连接的认证方法为PAP。

重要

- LDAP用户身份验证支持PPTP、L2TP、IPsec VPN和防火墙身份验证，但由于点对点协议的限制，只支持PAP（Packet Authentication Protocol）。
- 由于Windows本机客户端默认使用MSCHAP或MSCHAPv2，LDAP认证场景下，您需要将其更改为PAP。

1. 在Windows系统中按照下图方式打开网络连接面板（或使用Win + R快捷键，然后运行ncpa.cpl）。



2. 在弹出的网络连接面板中，右键点击已创建的L2TP连接，然后点击属性按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在弹出的L2TP连接属性中，选择“安全”面板，然后勾选“允许使用这些协议”，勾选“未加密的密码(PAP)(H)”，取消勾选CHAP和MS-CHAP v2，然后点击确定按钮。之后即可正常连接L2TP。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Windows原生客户端接入IPSec（IKEv2）

重要

本文基于Windows 11专业版22H2编写。

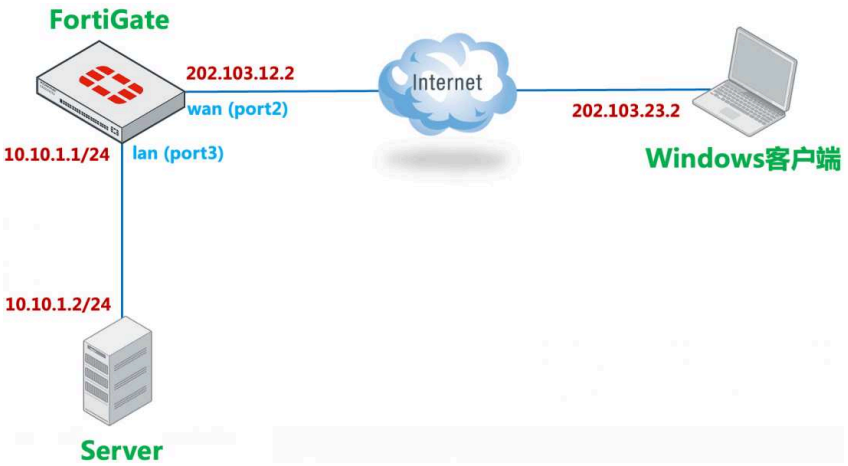
网络需求

通过Windows原生客户端（IKEv2）连接FortiGate的IPSec，并访问VPN内部资源。

重要

Windows系统使用IKEv2，必须配合证书认证（客户端验证服务器的证书，服务器不认证客户端的证书）。

网络拓扑



配置步骤

证书颁发

1. 通过证书颁发机构为FortiGate颁发证书（这里我们使用FortiAuthenticator为例）的注意事项。

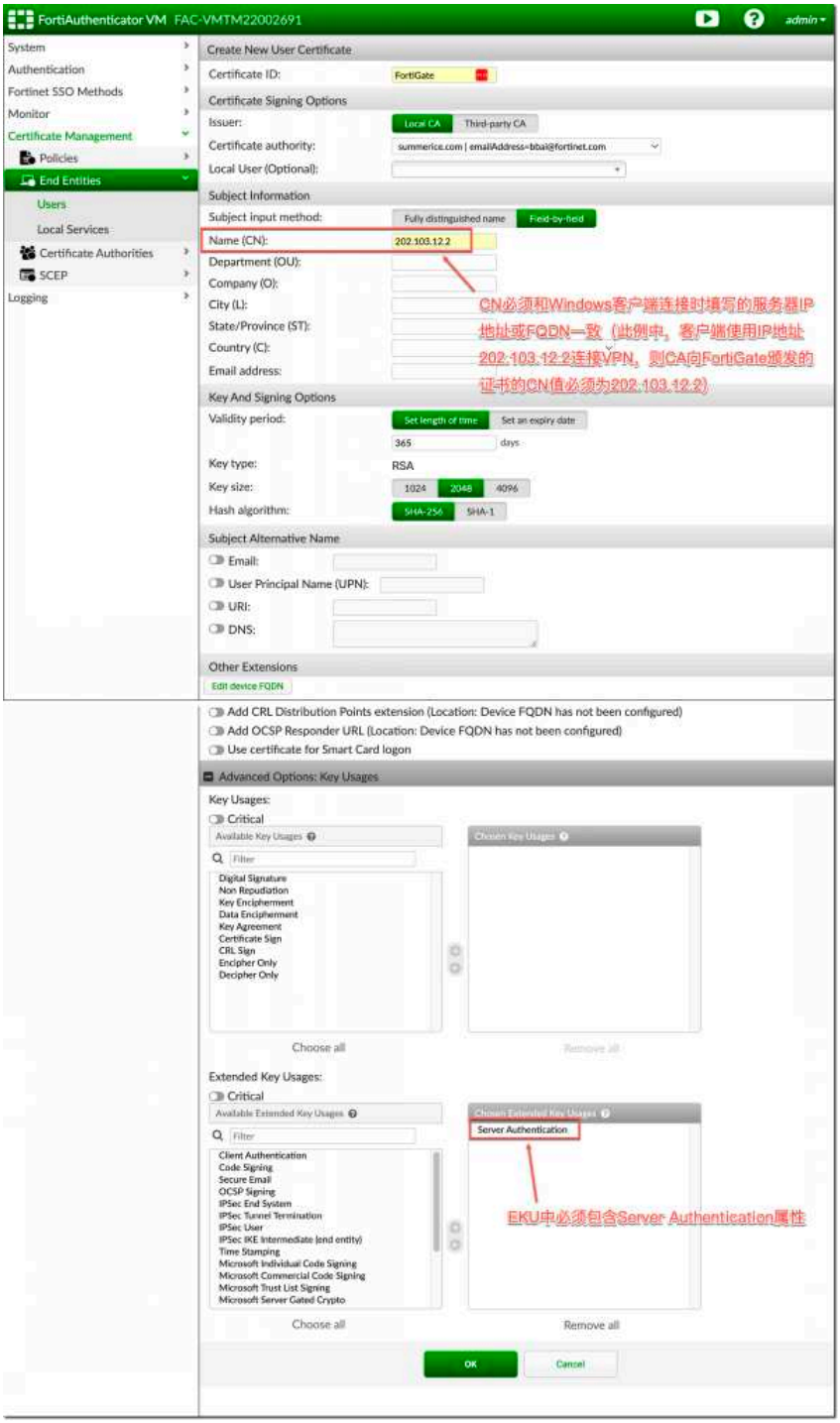
重要

Windows系统使用IKEv2，必须配合证书认证（客户端验证服务器的证书，服务器不认证客户端的证书），而且对颁发的证书有严格要求：

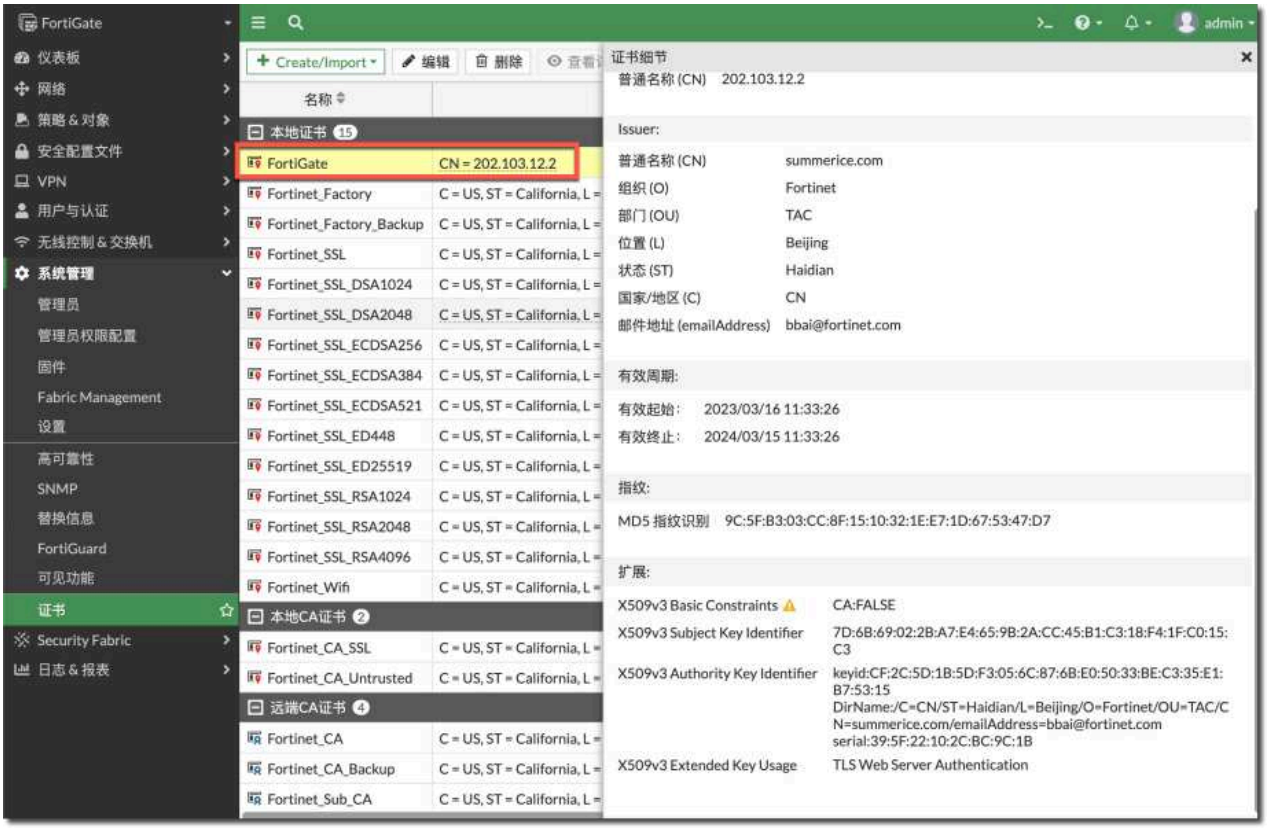
- CA向FortiGate颁发的证书的CN必须和Windows客户端连接时填写的服务器IP地址或FQDN一致（例如此例中，客户端使用IP地址202.103.12.2连接VPN，则CA向FortiGate颁发的证书的CN值必须为202.103.12.2）。
- CA向FortiGate颁发的证书的EKU（Extended Key Usages）必须包含Server Authentication属性。
- 客户端必须导入CA证书并加入受信任的根证书颁发机构。

2. 为FortiGate颁发证书，并导入FortiGate（导入过程可参考系统管理→系统设置→证书管理↗章节）。

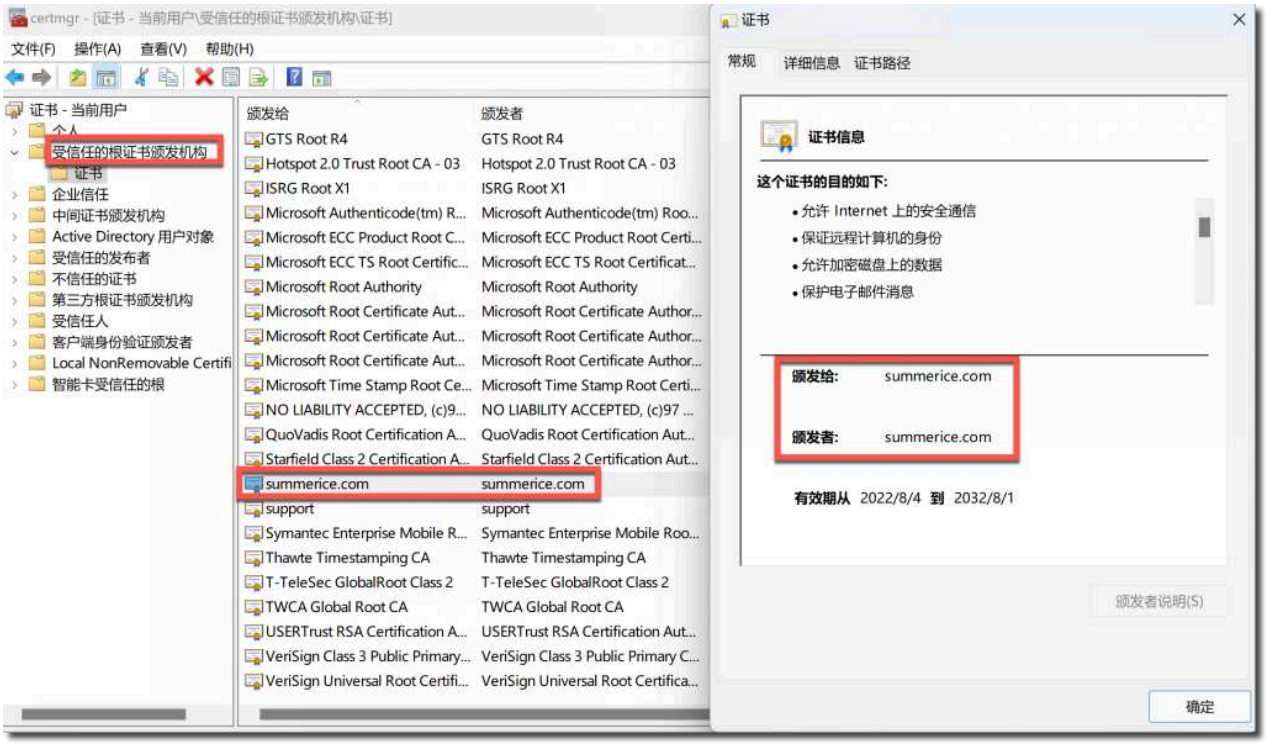
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



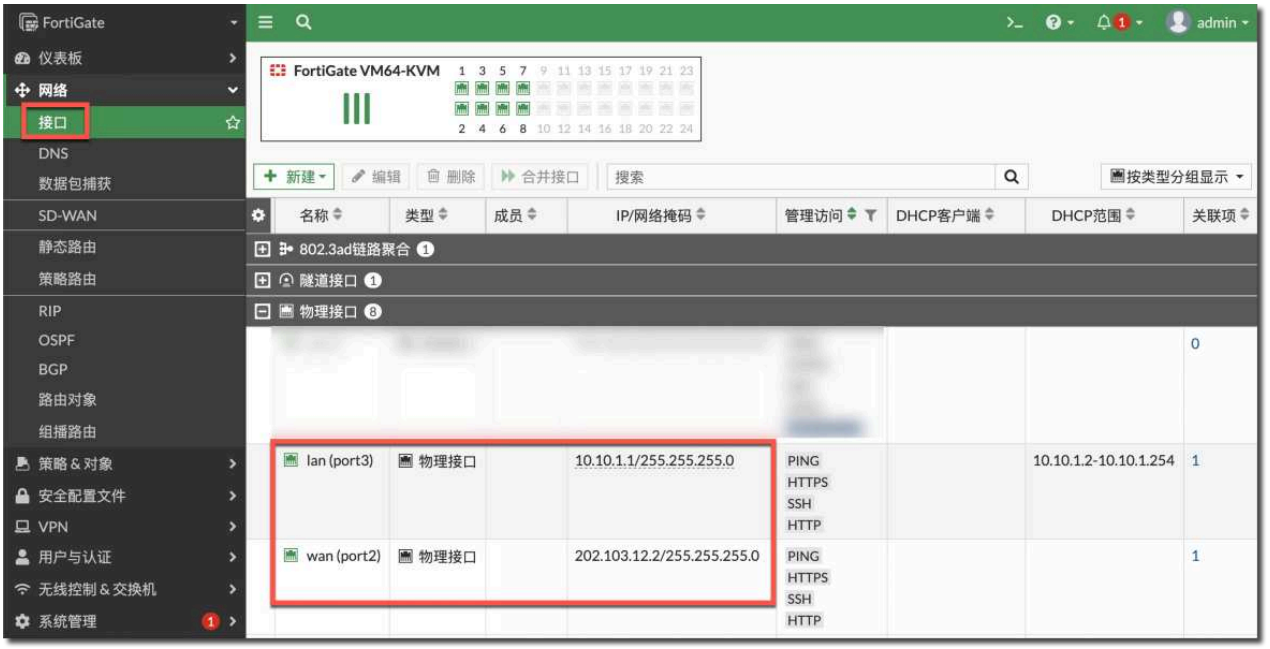
3. 下载CA证书，并导入Windows PC的受信任根证书颁发机构列表中。



FortiGate配置

1. 配置FortiGate的接口IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 创建本地VPN用户和用户组，参考用户与认证→本地用户和用户组↗章节（如需使用远程认证，请参考用户与认证→LDAP认证→LDAP认证配置与排错↗或用户与认证→Radius认证→Radius认证配置与排错↗章节）。




```
config user local
    edit "vpn_user"
        set type password
        set passwd xxxxxxxx
    next
end
```




```
config user group
    edit "VPN"
        set member "vpn_user"
    next
end
```

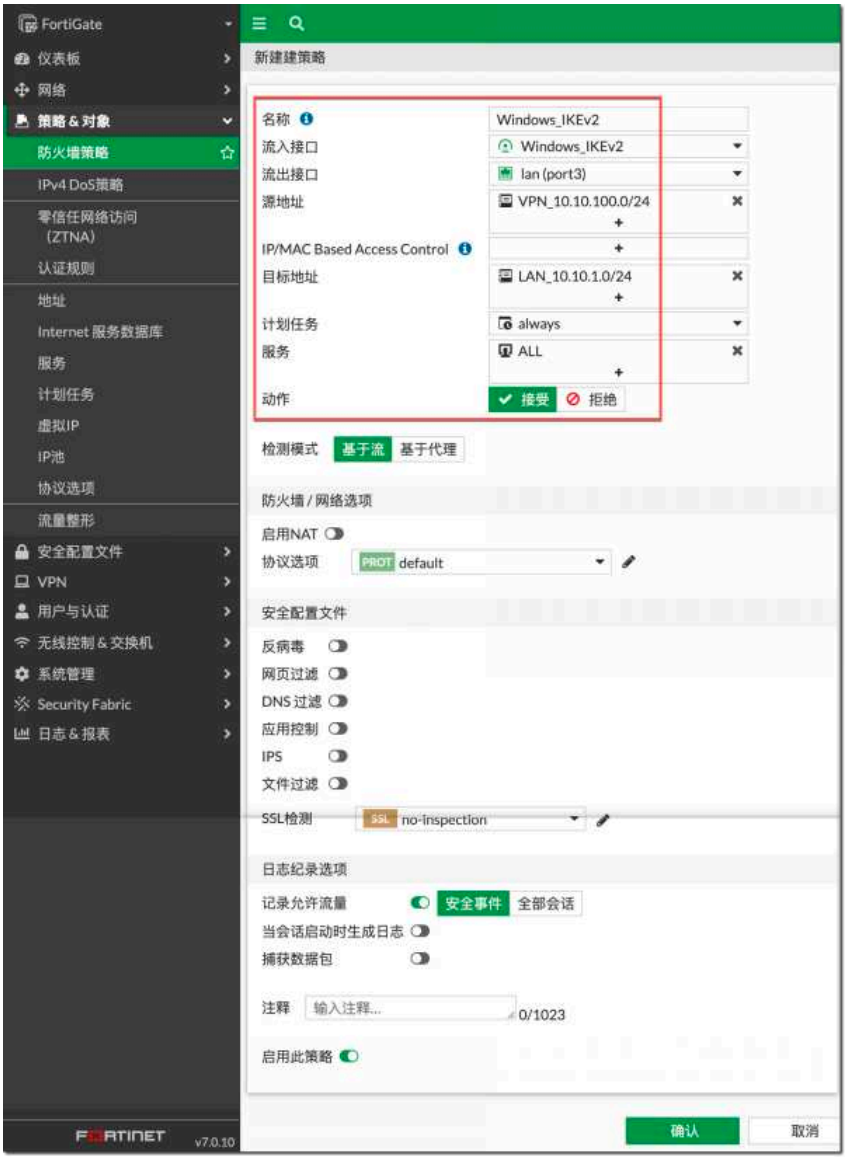
3. 该种方式的IPSec需要使用CLI方式配置，分别配置IPSec一阶段和二阶段。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
IPSec一阶段配置:
config vpn ipsec phase1-interface
    edit "Windows_IKEv2"
        set type dynamic
        set interface "port2"
        set ike-version 2    //IKE协议2
        set authmethod signature    //认证模式为证书认证
        set peertype any
        set net-device disable
        set mode-cfg enable    //开启为客户端分配IP
        set ipv4-dns-server1 10.10.1.2  //为客户端分配的DNS地址
        set proposal aes128-sha1 aes256-sha256
        set dhgrp 2
        set eap enable    //需要开启EAP做用户密码认证
        set eap-identity send-request    //开启EAP主动发送认证请求
        set authusrgrp "VPN"    //选择认证的用户组
        set certificate "FortiGate"    //选择服务器证书为导入的FortiGate证书
        set ipv4-start-ip 10.10.100.1
        set ipv4-end-ip 10.10.100.100    //客户端分配地址范围
    next
end

IPSec二阶段配置:
config vpn ipsec phase2-interface
    edit "Windows_IKEv2"
        set phase1name "Windows_IKEv2"
        set proposal aes128-sha1 aes256-sha1
        set pfs disable
        set keepalive enable
    next
end
```

4. 配置防火墙策略，允许客户端访问内网VPN资源。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
VPN资源地址对象:
config firewall address
    edit "LAN_10.10.1.0/24"
        set subnet 10.10.1.0 255.255.255.0
    next
end

客户端地址对象:
config firewall address
    edit "VPN_10.10.100.0/24"
        set subnet 10.10.100.0 255.255.255.0
    next
end

防火墙策略:
config firewall policy
    edit 1
        set name "Windows_IKEv2"
        set srcintf "Windows_IKEv2"
        set dstintf "port3"
        set action accept
        set srcaddr "VPN_10.10.100.0/24"
        set dstaddr "LAN_10.10.1.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

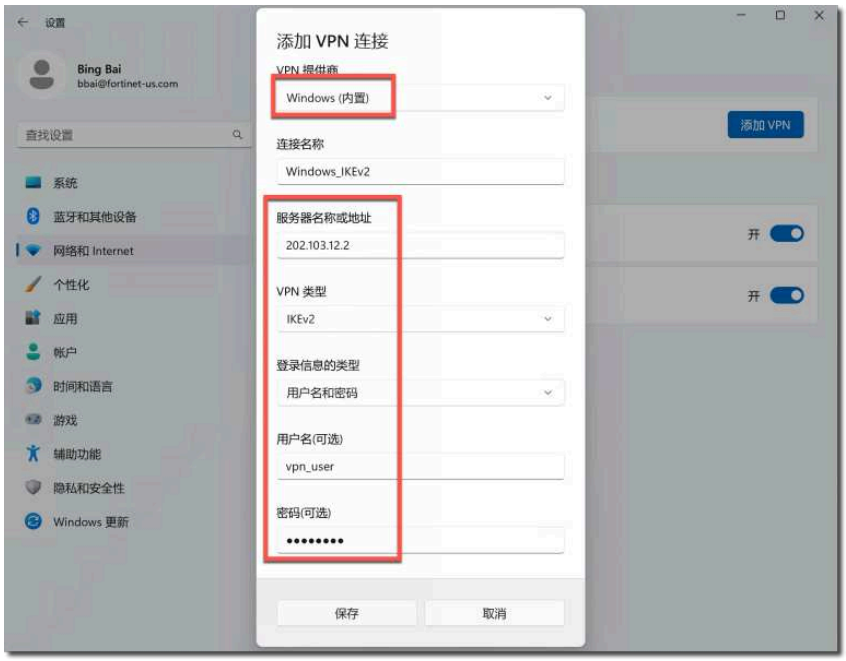

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

客户端配置

1. 打开设置→网络和Internet→VPN，点击新建按钮。



2. 配置VPN提供商为Windows，配置连接名称和服务器IP（或FQDN），“VPN类型”选择“IKEv2”，“登录信息的类型”选择“用户名和密码”，填写用户名和密码信息，点击保存按钮。



结果验证

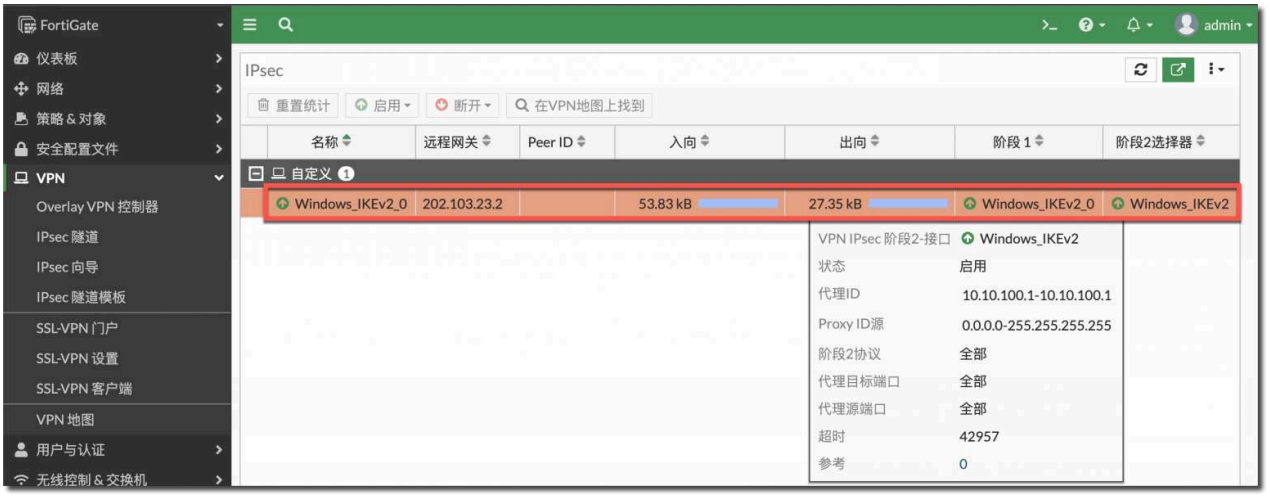
1. 在客户端VPN点击连接按钮，然后查看连接状态，可以看到VPN连接已建立。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 在FortiGate侧查看连接状态。




```
FortiGate # diagnose vpn ike gateway list

vd: root/0
name: Windows_IKEv2_0
version: 2
interface: port2 4
addr: 202.103.12.2:4500 → 202.103.23.2:64916
tun_id: 10.10.100.1/::10.0.0.15
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

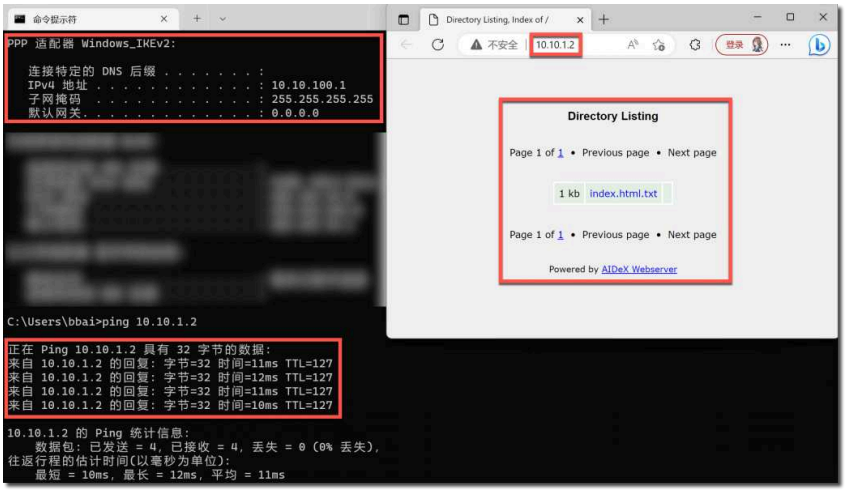
```
remote_location: 0.0.0.0
network-id: 0
created: 281s ago
eap-user: vpn_user
2FA: no
assigned IPv4 address: 10.10.100.1/0.0.0.0
nat: peer
PPK: no
IKE SA: created 1/1  established 1/1  time 50/50/50 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms
  id/spi: 28 1a1ac0eb795737c0/45eb750afe25ce3f
  direction: responder
  status: established 281-281s ago = 50ms
  proposal: aes128-sha1
  child: no
  SK_ei: d4088e142220d3f2-24c73e8bd23cc361
  SK_er: 23dad2bdacf52ae7-ea3e3f1ad62e48cd
  SK_ai: 2db36c765a403317-66950b37f90fc178-3ff9a0a4
  SK_ar: 919125e418fb94dc-d1978545c2da767a-e5f32bb9
  PPK: no
  message-id sent/recv: 0/6
  lifetime/rekey: 86400/85848
  DPD sent/recv: 00000000/00000000

FortiGate # diagnose vpn tunnel list

list all ipsec tunnel in vd 0
------------------------------------------------------
name=Windows_IKEv2_0 ver=2 serial=10 202.103.12.2:4500->202.103.23.2:64916 tun_id=10.10.100.1 tun_id6=::10.0.0.15
dst_mtu=1500 dpd-link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/9128 options[23a8]=npu rgwy-chg rport-chg frag-rfc
run_state=0 role=primary accept_traffic=1 overlay_id=0
parent=Windows_IKEv2 index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=0 olast=0 ad=/0
stat: rxp=813 txp=280 rxb=61158 txb=30402
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=silent draft=0 interval=10 remote_port=64916
proxyid=Windows_IKEv2 proto=0 sa=1 ref=74 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:10.10.100.1-10.10.100.1:0
  SA:  ref=3 options=20483 type=00 soft=0 mtu=1422 expire=42903/0B replaywin=2048
       seqno=119 esn=0 replaywin_lastseq=0000032d qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=24832a57 esp=aes key=16 7b7328d6fe3ee6230a5072fea98c57d0
       ah=sha1 key=20 1fa4bee8e25fd477e8e79ea28291695d84c4d783
  enc: spi=60f3ab06 esp=aes key=16 aaaf1aca419bf8dd8743f2c267f97b70
       ah=sha1 key=20 50b086fddc0810e3dc5f204c8889f236e18d5663
  dec:pkts/bytes=1626/122316, enc:pkts/bytes=560/81074
  npu_flag=00 npu_rgwy=202.103.23.2 npu_lgwy=202.103.12.2 npu_selid=f dec_npuid=0 enc_npuid=0
------------------------------------------------------
name=Windows_IKEv2 ver=2 serial=2 202.103.12.2:0->0.0.0.0:0 tun_id=10.0.0.2 tun_id6=::10.0.0.2 dst_mtu=0 dpd-
link=on weight=1
bound_if=4 lgwy=static/1 tun=intf mode=dialup/2 encap=none/552 options[0228]=npu frag-rfc  role=primary
accept_traffic=1 overlay_id=0
proxyid_num=0 child_num=1 refcnt=3 ilast=42973370 olast=42973370 ad=/0
stat: rxp=3292 txp=280 rxb=241855 txb=30402
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

3. 在FortiGate侧查看路由kernel表，可以看到FortiGate已经自动添加了到客户端的路由。

```
FortiGate # get router info kernel
...
tab=254 vf=0 scope=0 type=1 proto=11 prio=1 0.0.0.0/0.0.0.0/0->10.10.100.1/32 pref=0.0.0.0 gwy=10.10.100.1
dev=20(Windows_IKEv2)
...
```

4. 使用客户端访问VPN内网资源（Ping和HTTP访问）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



重要

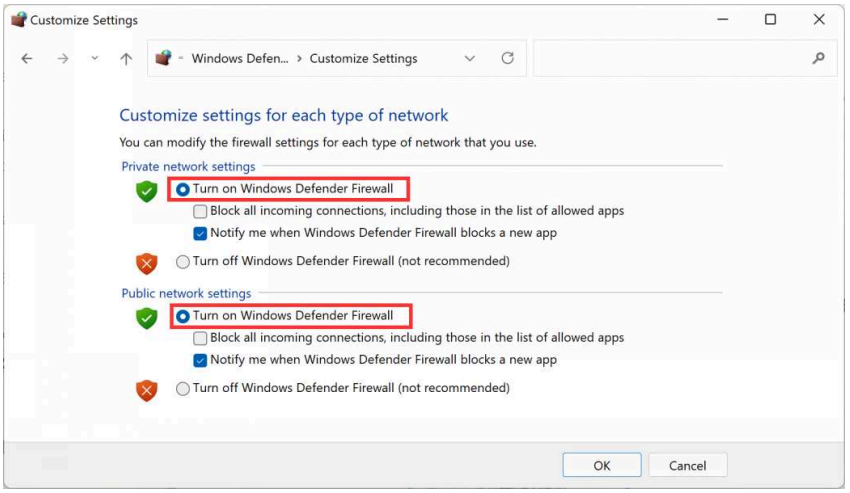
实际测试Windows使用IKEv2，无法使用隧道分割功能，VPN建立后，所有流量被送入VPN隧道。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

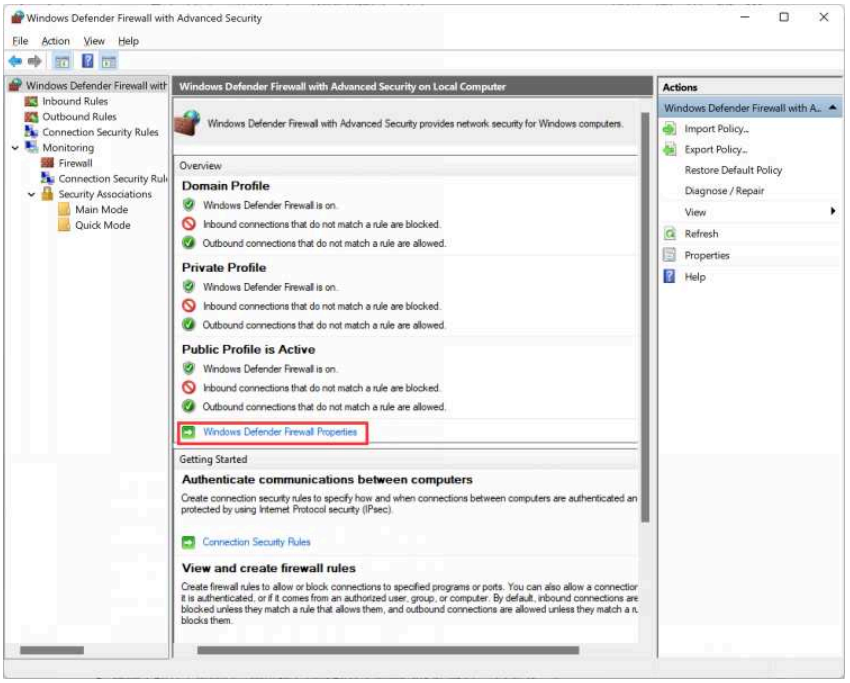
使用Windows系统防火墙与FortiGate建立IPSec VPN

Windows Firewall IPSec配置步骤

1. 在使用Windows防火墙的IPSec功能前，需要将Windows防火墙功能打开。点击键盘Win（徽标）键，输入“Windows Defender Firewall”，点击左侧的“Turn Windows Defender Firewall on or off”，将需要使用VPN的网络的防火墙功能打开。

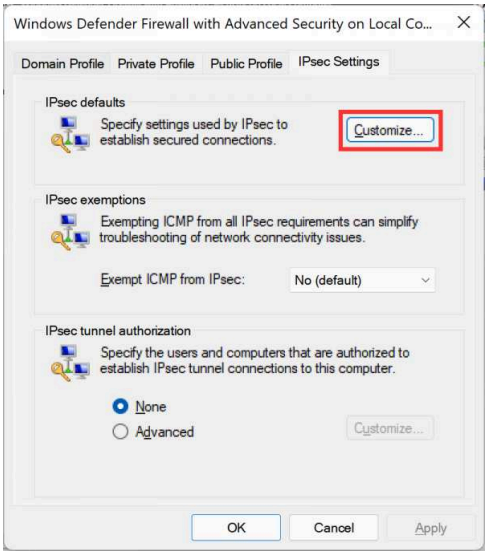


2. 配置Windows Firewall IPSec的自定义安全提议。上图中点击返回按钮，然后点击左侧的“Advanced Settings”，点击“Windows Defender Firewall Properties”。

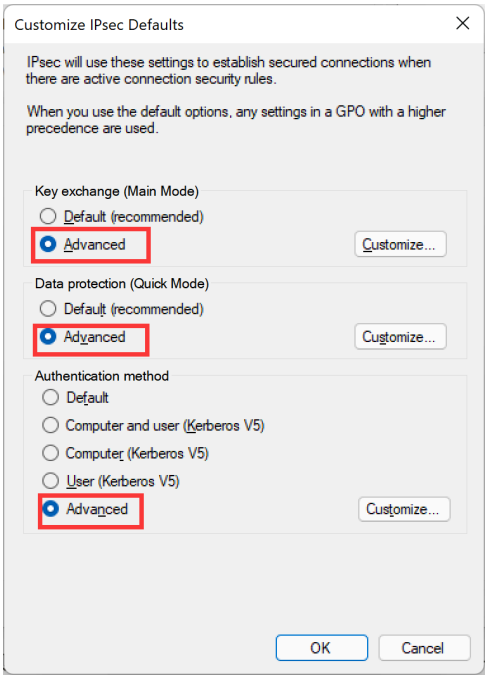


3. 在弹出的属性界面中点击“IPSec Settings”选项卡，在“IPSec defaults”中点击“Customize...”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

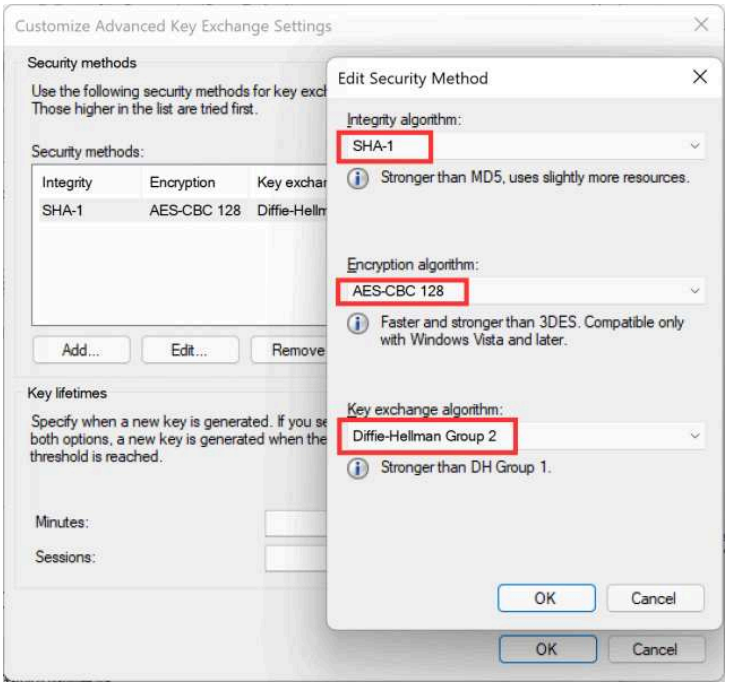


4. 配置“Key exchange (Main Mode)”、“Data protection (Quick Mode)”、“Authentication method”均为“Advanced”。

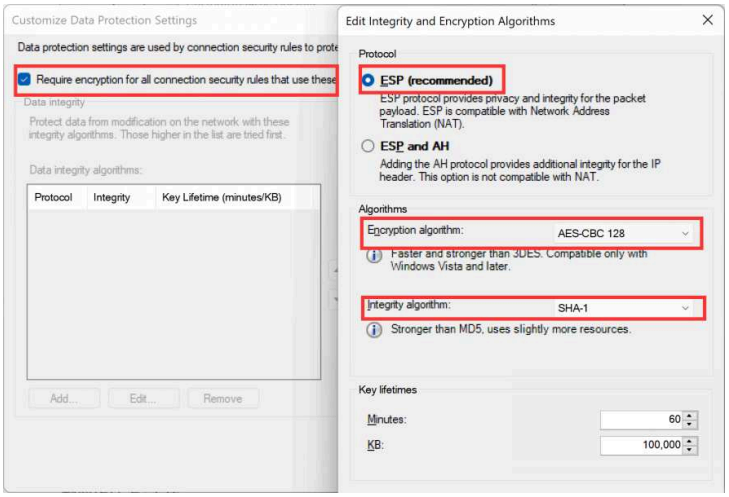


5. 配置第一阶段自定义安全提议。点击“Key exchange (Main Mode)”中的“Customize...”按钮。配置完整性算法、加密算法和DH组。

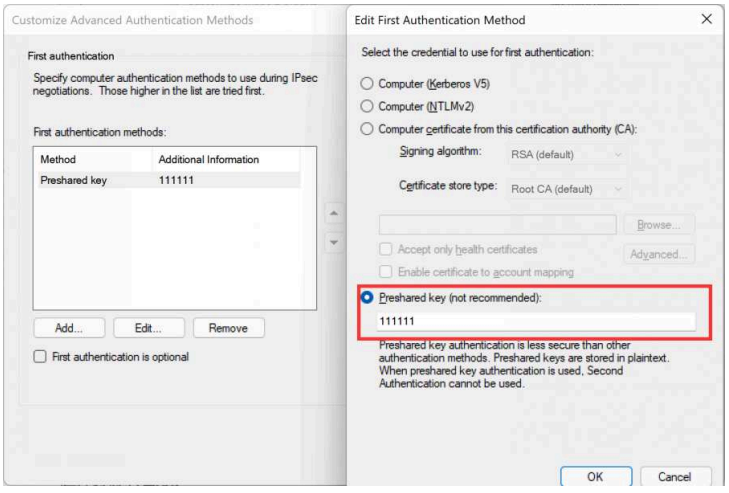
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 配置第二阶段自定义安全提议。点击“Data protection (Quick Mode)”中的“Customize...”按钮。开启“Require encryption for all connection security rules that use these settings”，配置完整性算法、加密算法。

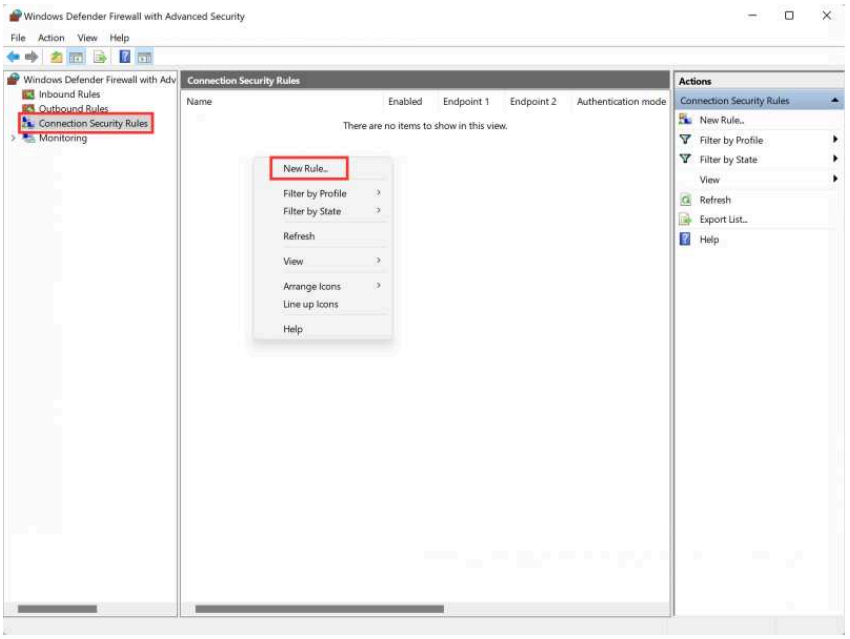


7. 配置自定义的认证方式。点击“Authentication method”中的“Customize...”按钮，按需求配置认证方法，这里以“预共享密钥”为例。

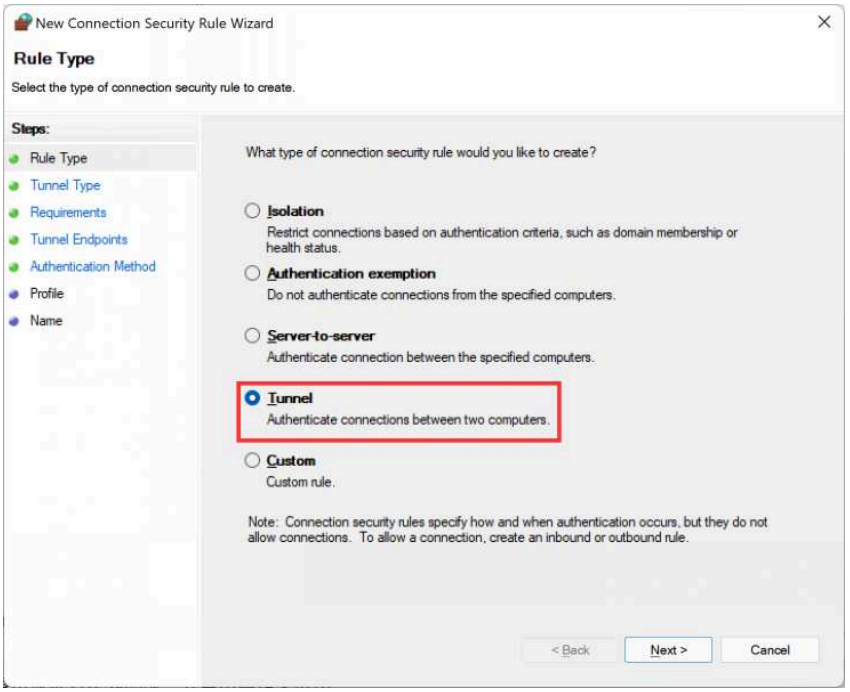


8. 在Windows高级防火墙中创建IPSec连接。进入Windows Defender Firewall with Advanced Security→Connection Security Rules，右键点击后选择“New Rules”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

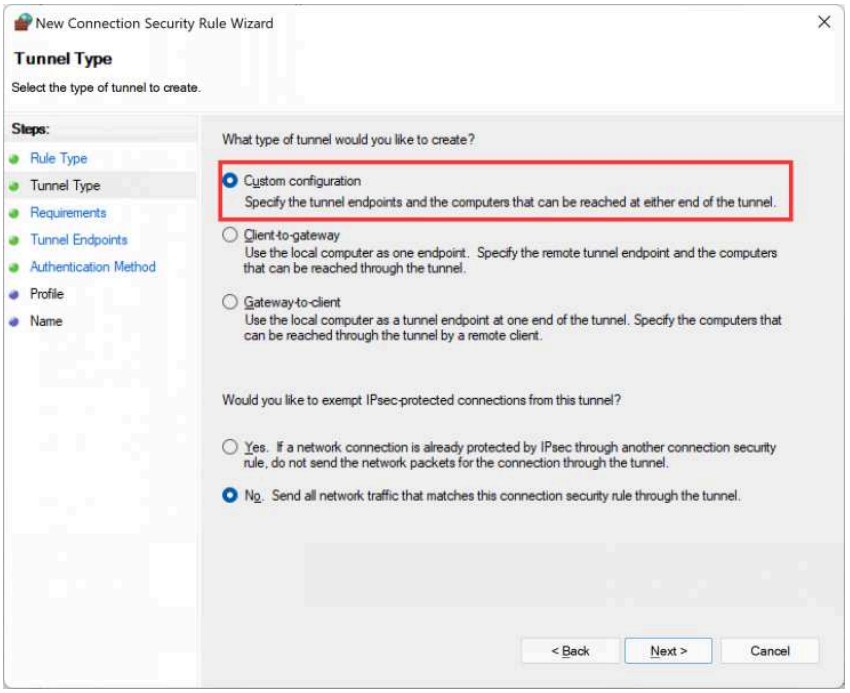


9. 在弹出的安全规则向导中选择要创建的安全规则类型为“Tunnel”，点击下一步。

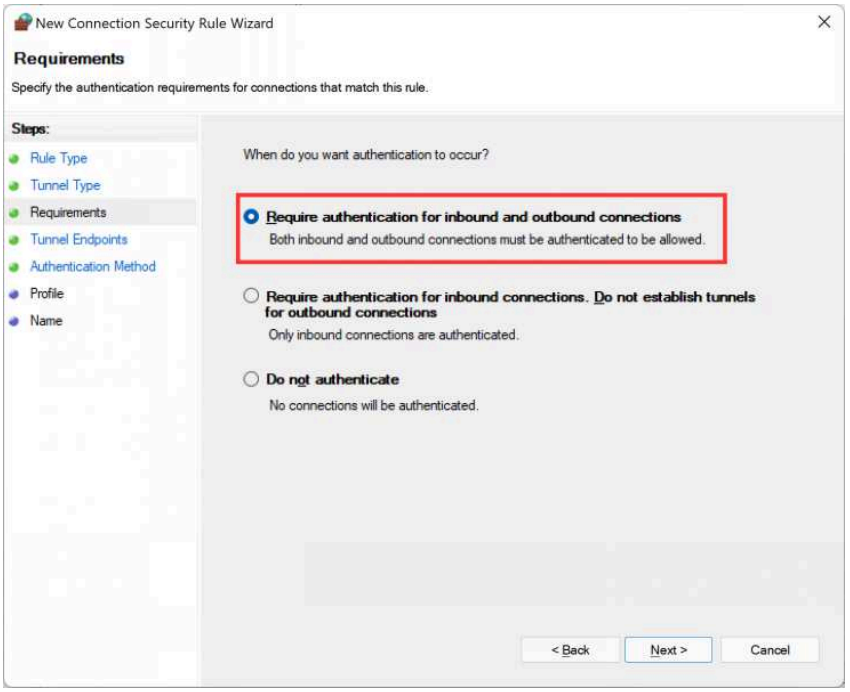


.0. 隧道类型选择“Custom configuration”，其余选项默认，点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

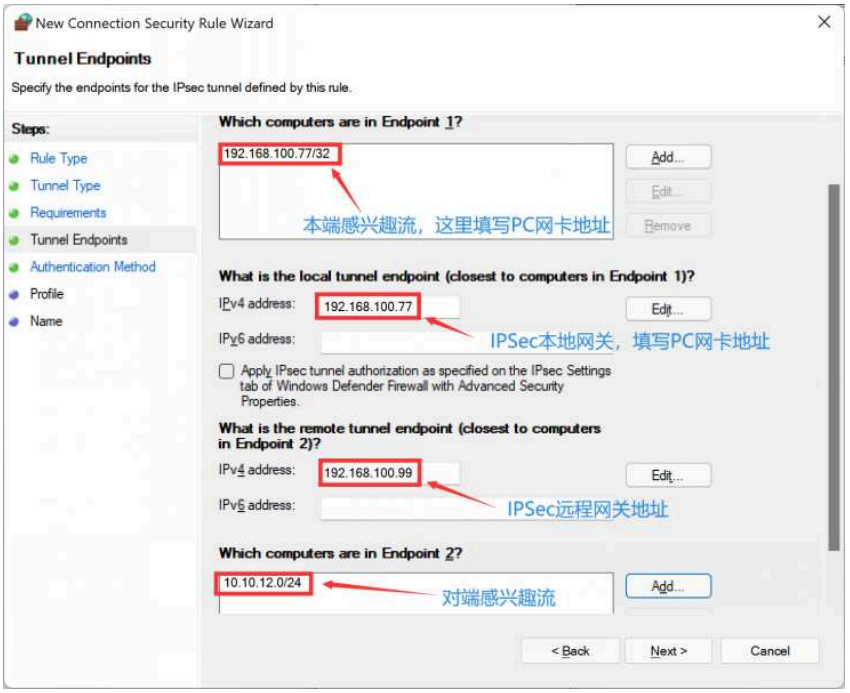


1. 身份验证时间选择“Require authentication for inbound and outbound connections”，点击下一步。

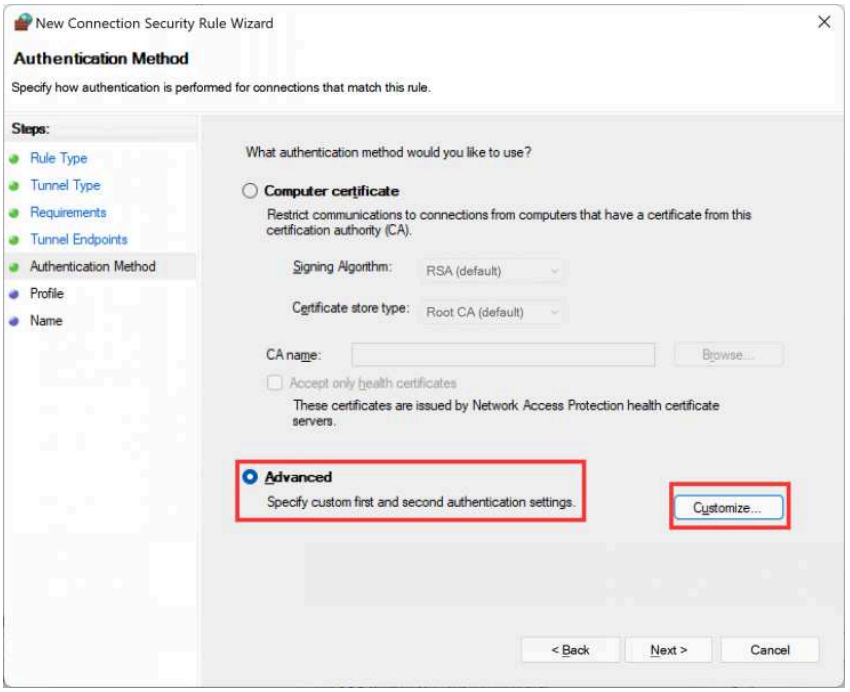


2. 配置终结点1中的计算机，这里填写Windows本端的保护网段，一般情况下为PC的通信地址；配置终结点2中的计算机，这里填写对端的保护网段，注意只有PC发起了向该保护网段的流量，协商才能被触发；配置本地隧道和远程隧道终结点，这里填写Windows本端和对端IPSec服务器的协商IP地址。注意只有PC发起了向该保护网段的流量，协商才能被触发。点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

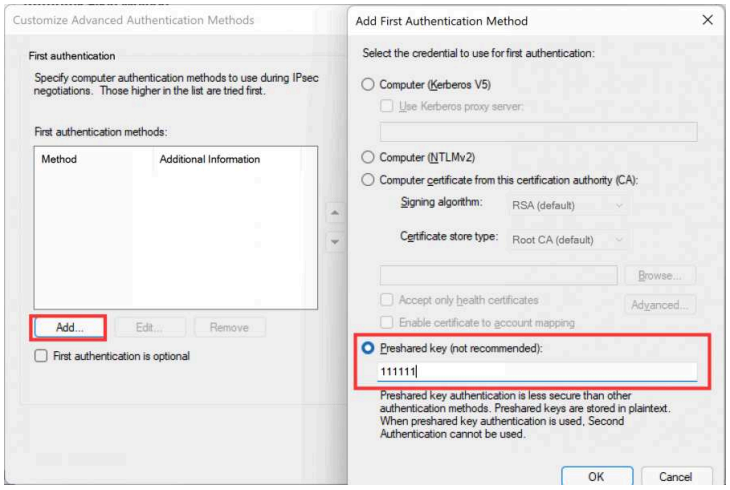


3. 选择身份认证方法为“Advanced”，并点击“Customize...”按钮。

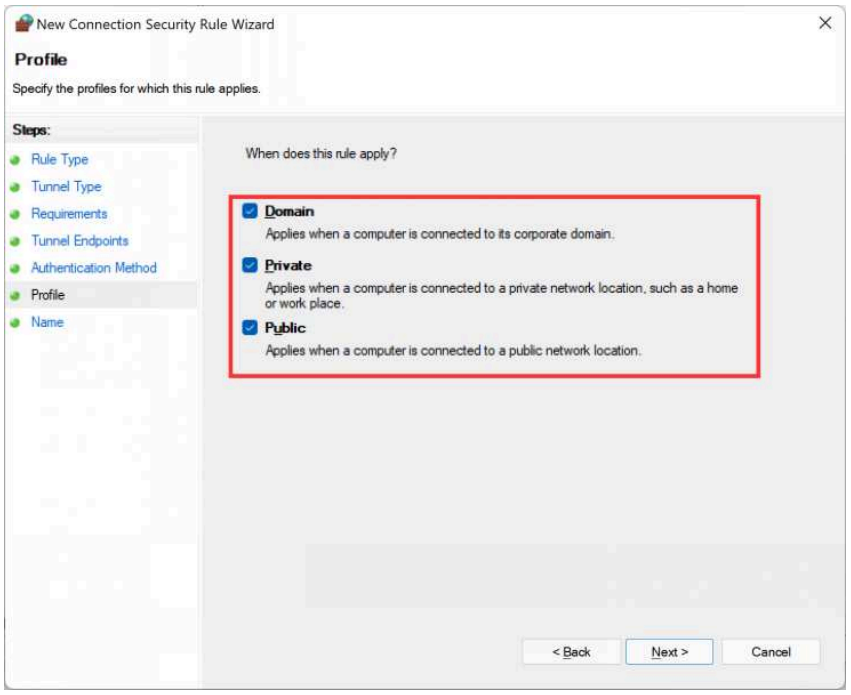


4. 按需求配置认证算法，这里以预共享密钥为例。保存后点击下一步。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

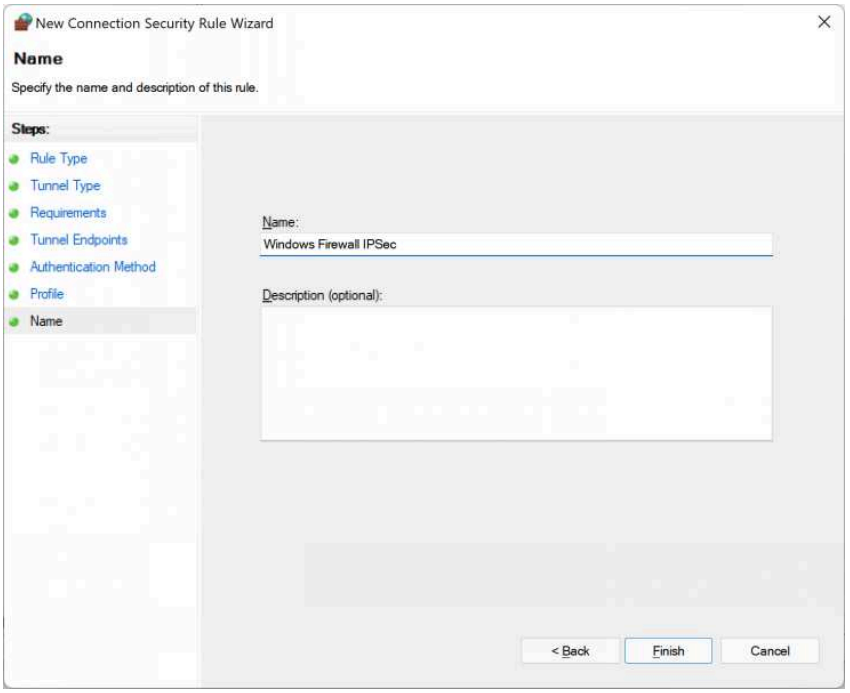


5. “When does this rule apply”选择默认即可。点击下一步。



6. 为IPSec连接配置名称，完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 补充：高级防火墙IPSec配置的特点是每条连接只用简单的配置本、对端的公网IP以及保护网段，安全提议是一个全局配置，所有连接都会受此安全提议影响。这样非常简单快速但也缺少很多灵活性，比如需要这些连接的安全提议不一致时就无法满足。其实高级防火墙是做了很多东西的。在后台的命令行，使用netsh advfirewall命令可以对高级防火墙并进行灵活配置，以下是一些简单的配置实例。

```bash
- cmd>netsh advfirewall（进入高级防火墙配置）
- netsh advfirewall consc（更改防火墙配置）
- netsh advfirewall consc [add|delete|set] rule name=连接名 new option=value（增、删、改一条连接。具体选项和可用参数可以在[add|delete|set] rule help中可以查看，内容非常详细的）
- netsh advfirewall consec>set rule name=v4_ipsec new qmsecmethods（第二阶段的安全提议，如果需要配置PFS必须先配置安全提议）=esp:md5-3des+600000min+100000kb qmpfs=dhgroup2（开启PFS，并且使用DH2，当ESP加密算法为空时开启PFS不生效）
```

FortiGate配置

IPSec配置

```bash
config vpn ipsec phase1-interface
    edit "WindowsFw"
        set type dynamic
        set interface "lan"
        set peertype any
        set net-device disable
        set proposal aes128-sha1
        set dpd on-idle
        set dhgrp 2
        set psksecret xxxxxxxx
        set dpd-retryinterval 60
    next
end
```

```bash
config vpn ipsec phase2-interface
    edit "WindowsFw"
        set phase1name "WindowsFw"
        set proposal aes128-sha1
        set pfs disable
        set src-subnet 10.10.12.0 255.255.255.0
        set dst-subnet 192.168.100.77 255.255.255.255
    next
end
```

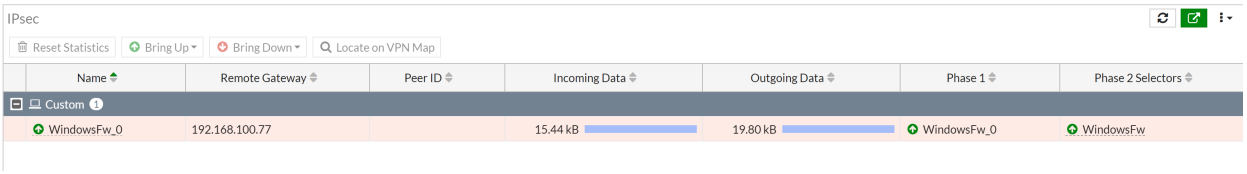

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

防火墙策略配置

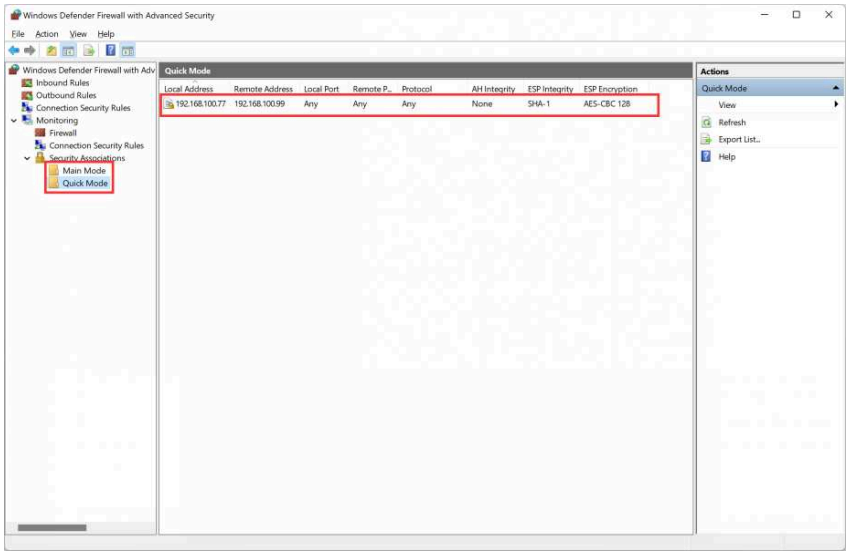
```bash
VPN资源地址对象:
config firewall address
    edit "Local_10.10.12.0/24"
        set subnet 10.10.12.0 255.255.255.0
    next
end

客户端地址对象:
config firewall address
    edit "Remote_192.168.100.77/32"
        set subnet 192.168.100.77 255.255.255.255
    next
end

config firewall policy
    edit 1
        set name "WindowsFw"
        set srcintf "WindowsFw"
        set dstintf "port3"
        set action accept
        set srcaddr "Remote_192.168.100.77/32"
        set dstaddr "Local_10.10.12.0/24"
        set schedule "always"
        set service "ALL"
    next
end
```

结果验证

1. 使用PC ping FortiGate端的感兴趣流，触发IPSec协商，查看IPSec连接建立状态：



2. Windows Firewall连接监控：



3. 客户端抓包：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

No.	Time	Source	Destination	Protocol	Length	Info
84…	1921.031377	192.168.100.77	192.168.100.99	ISAKMP	298	Identity Protection (Main Mode)
84…	1921.032873	192.168.100.99	192.168.100.77	ISAKMP	234	Identity Protection (Main Mode)
84…	1921.033321	192.168.100.77	192.168.100.99	ISAKMP	302	Identity Protection (Main Mode)
84…	1921.035152	192.168.100.99	192.168.100.77	ISAKMP	270	Identity Protection (Main Mode)
84…	1921.035496	192.168.100.77	192.168.100.99	ISAKMP	118	Identity Protection (Main Mode)
84…	1921.036783	192.168.100.99	192.168.100.77	ISAKMP	118	Identity Protection (Main Mode)
84…	1921.037072	192.168.100.77	192.168.100.99	ISAKMP	246	Quick Mode
84…	1921.039256	192.168.100.99	192.168.100.77	ISAKMP	214	Quick Mode
84…	1921.039531	192.168.100.77	192.168.100.99	ISAKMP	102	Quick Mode
84…	1921.039558	192.168.100.77	192.168.100.99	ESP	134	ESP (SPI=0x2b5bf512)
84…	1921.039573	192.168.100.77	192.168.100.99	ESP	134	ESP (SPI=0x2b5bf512)
84…	1921.041155	192.168.100.99	192.168.100.77	ESP	134	ESP (SPI=0x440a2fac)
84…	1921.041242	192.168.100.77	192.168.100.99	ESP	118	ESP (SPI=0x2b5bf512)
84…	1921.041251	192.168.100.99	192.168.100.77	ESP	134	ESP (SPI=0x440a2fac)
84…	1921.041283	192.168.100.77	192.168.100.99	ESP	118	ESP (SPI=0x2b5bf512)
84…	1921.041409	192.168.100.77	192.168.100.99	ESP	630	ESP (SPI=0x2b5bf512)
84…	1921.041505	192.168.100.77	192.168.100.99	ESP	630	ESP (SPI=0x2b5bf512)

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

L2TP VPN

L2TP VPN简介

L2TP（Layer 2 Tunneling Protocol） VPN是一种用于承载PPP报文的隧道技术，基于UDP，端口1701。该技术主要应用在远程办公场景中为出差员工远程访问企业内网资源提供接入服务。

> **重要**
>
> 针对FortiGate，L2TP相比较SSL VPN/IPSec VPN，更推荐用户使用SSL VPN/IPSec VPN，一方面是安全性更高（数据加密），另一方面是性能上SSL VPN/IPSec VPN比L2TP强得多（SSL VPN/IPSec VPN可以被NP芯片加速，而L2TP只能由CPU处理）。而且IPSec VPN也支持各种系统原生客户端接入。

L2TP数据报文

L2TP数据报文分为两种：控制报文和数据报文；

控制报文：控制消息用于隧道和会话连接的建立、维护以及传输控制；位于隧道和会话建立过程中。控制消息的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制；主要的控制消息包括控制报文、会话报文等。




```
No.  Time    Source       Destination  Protocol  Length  Source Port  Destinationo Port  Info
  7  0.001…  10.1.1.5     201.1.1.3    L2TP          90         1701              1701  Control Message - ICCN (tunnel id=1, session id=1)

> Frame 7: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{0FB48074-675E-4FD5-8D41-A0C4ACC8F9F7}, id 0
> Ethernet II, Src: VMware_a2:90:ea (00:0c:29:a2:90:ea), Dst: VMware_2e:3f:cf (00:0c:29:2e:3f:cf)
> Internet Protocol Version 4, Src: 10.1.1.5, Dst: 201.1.1.3
> User Datagram Protocol, Src Port: 1701, Dst Port: 1701
v Layer 2 Tunneling Protocol
  > Packet Type: Control Message Tunnel Id=1 Session Id=1
    Length: 48
    Tunnel ID: 1
    Session ID: 1
    Ns: 3
    Nr: 2
  > Control Message AVP
  > Connect Speed AVP
  > Framing Type AVP
  > Proxy Authen Type AVP
```

数据报文：用于承载用户的PPP连接数据报文，并在隧道上进行传输。数据消息的传输是不可靠传输，若数据报文丢失，不予重传。不支持对数据消息的流量控制和拥塞控制。




```
No.  Time    Source        Destination   Protocol  Length  Source Port  Destinationo Port  Info
196  4.799…  172.31.1.11   192.168.2.10  ICMP         111         1701              1701  Echo (ping) request  id=0x0001, seq=69/17664, ttl=128

> Frame 196: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF_{0FB48074-675E-4FD5-8D41-A0C4ACC8F9F7}, id 0
> Ethernet II, Src: VMware_a2:90:ea (00:0c:29:a2:90:ea), Dst: VMware_2e:3f:cf (00:0c:29:2e:3f:cf)
> Internet Protocol Version 4, Src: 10.1.1.5, Dst: 201.1.1.3
v User Datagram Protocol, Src Port: 1701, Dst Port: 1701
    Source Port: 1701
    Destination Port: 1701
    Length: 77
    Checksum: 0xbbb6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (69 bytes)
v Layer 2 Tunneling Protocol
  > Packet Type: Data    Message Tunnel Id=1 Session Id=1
    Length: 69
    Tunnel ID: 1
    Session ID: 1
v Point-to-Point Protocol
    Protocol: Internet Protocol version 4 (0x0021)
> Internet Protocol Version 4, Src: 172.31.1.11, Dst: 192.168.2.10
> Internet Control Message Protocol
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

L2TP协议交互过程

1. 建立L2TP隧道

   SCCRQ（Start-Control-Connection-Request）：终端向FortiGate发起控制连接请求；

   SCCRP（Start-Control-Connection-Reply）：FortiGate接受了终端的连接请求，隧道的建立过程可以继续；

   SCCCN（Start-Control-Connection-Connected）：对SCCRP的回应，完成隧道的建立。

2. 建立L2TP会话

   ICRQ（Incoming-Call-Request）：终端请求在已经建立的隧道中建立会话；

   ICRP（Incoming-Call-Reply）：FortiGate回应ICRQ，表示ICRQ成功，也会在ICRP中标识L2TP会话必要的参数；

   ICCN（Incoming-Call-Connected）：回应ICRP，L2TP会话建立完成。

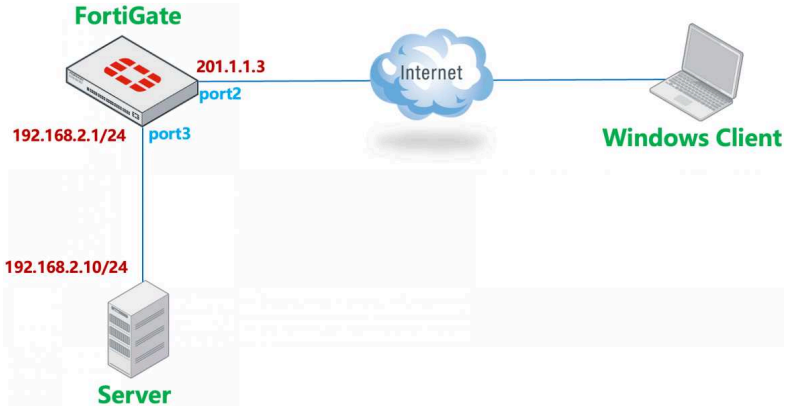
3. 对用户认证，认证通过，建立PPP连接

No.	Time	Source	Destination	Protocol	Length	Source Port	Destinationo Port	Info
1	0.000…	10.1.1.5	201.1.1.3	L2TP	150	1701	1701	Control Message - SCCRQ (tunnel id=0, session id=0)
2	0.000…	201.1.1.3	10.1.1.5	L2TP	121	1701	1701	Control Message - SCCRP (tunnel id=8, session id=0)
3	0.000…	10.1.1.5	201.1.1.3	L2TP	62	1701	1701	Control Message - SCCCN (tunnel id=1, session id=0)
4	0.000…	10.1.1.5	201.1.1.3	L2TP	90	1701	1701	Control Message - ICRQ (tunnel id=1, session id=0)
5	0.000…	201.1.1.3	10.1.1.5	L2TP	60	1701	1701	Control Message - ZLB (tunnel id=8, session id=0)
6	0.001…	201.1.1.3	10.1.1.5	L2TP	70	1701	1701	Control Message - ICRP (tunnel id=8, session id=1)
7	0.001…	10.1.1.5	201.1.1.3	L2TP	90	1701	1701	Control Message - ICCN (tunnel id=1, session id=1)
8	0.001…	201.1.1.3	10.1.1.5	L2TP	60	1701	1701	Control Message - ZLB (tunnel id=8, session id=1)
9	0.025…	10.1.1.5	201.1.1.3	PPP LCP	75	1701	1701	Configuration Request
10	0.026…	201.1.1.3	10.1.1.5	PPP LCP	81	1701	1701	Configuration Request
11	0.026…	201.1.1.3	10.1.1.5	PPP LCP	60	1701	1701	Configuration Reject
12	0.026…	10.1.1.5	201.1.1.3	PPP LCP	83	1701	1701	Configuration Ack
13	0.026…	10.1.1.5	201.1.1.3	PPP LCP	72	1701	1701	Configuration Request
14	0.026…	201.1.1.3	10.1.1.5	PPP LCP	70	1701	1701	Configuration Ack
15	0.026…	201.1.1.3	10.1.1.5	PPP LCP	60	1701	1701	Echo Request
16	0.026…	201.1.1.3	10.1.1.5	PPP CHAP	89	1701	1701	Challenge (NAME='FGVM08[redacted]', VALUE=0xc749f167d96cb0f3e4ee9486389fb3ee)
17	0.027…	10.1.1.5	201.1.1.3	PPP LCP	70	1701	1701	Identification
18	0.027…	10.1.1.5	201.1.1.3	PPP LCP	83	1701	1701	Identification
19	0.027…	10.1.1.5	201.1.1.3	PPP LCP	76	1701	1701	Identification
20	0.027…	201.1.1.3	10.1.1.5	PPP LCP	74	1701	1701	Code Reject
21	0.027…	201.1.1.3	10.1.1.5	PPP LCP	87	1701	1701	Code Reject
22	0.027…	201.1.1.3	10.1.1.5	PPP LCP	80	1701	1701	Code Reject
23	0.028…	10.1.1.5	201.1.1.3	PPP LCP	60	1701	1701	Echo Reply
24	0.028…	10.1.1.5	201.1.1.3	PPP CHAP	111	1701	1701	Response (NAME='user1', VALUE=0xbf896f17a3dde3d72967a5a5ce1161da00000000000000000b8108a806e593f9977b2ee4d…)
25	0.029…	201.1.1.3	10.1.1.5	PPP CHAP	98	1701	1701	Success (MESSAGE='S=F5DE5686706850292F4C41C76EABCA14DF7D71C6')

网络需求

在外移动办公的工作人员需要通过L2TP VPN 隧道模式拨入到公司内网来对内网主机进行访问。

网络拓扑

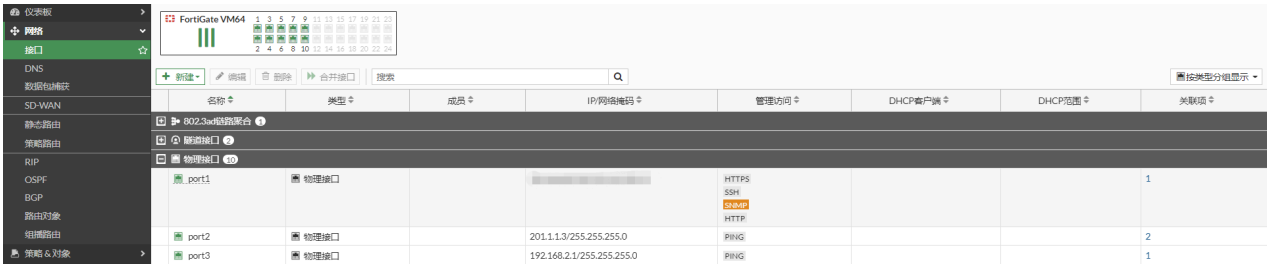


配置步骤

配置FortiGate L2TP VPN

1. 基础配置

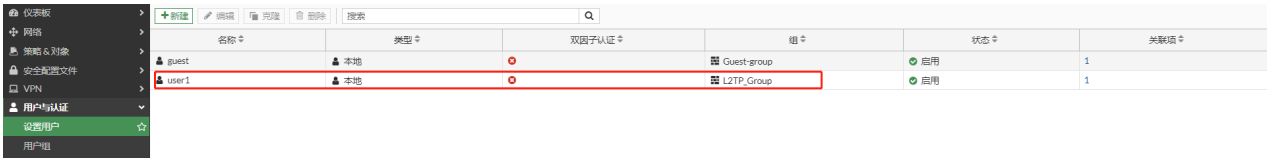
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

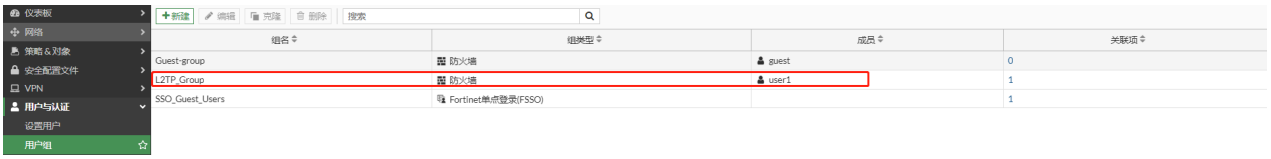






2. 创建用户并将用户加入到用户组

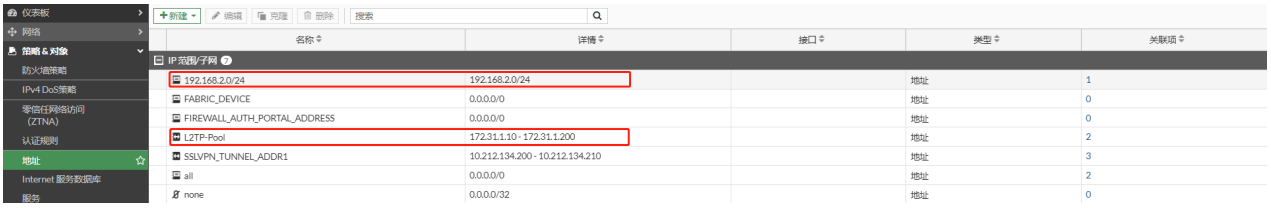




3. 配置L2TP VPN

```
config vpn l2tp
    set status enable
    set eip 172.31.1.200
    set sip 172.31.1.10
    set usrgrp "L2TP_Group"
end
```

4. 配置地址对象



5. 配置防火墙策略

FortiGate会自动创建L2TP的接口l2t.root。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



第1条策略用于客户端L2TP VPN拨号后访问内网；第2条策略用于客户端L2TP VPN拨号后上网。

当客户端L2TP VPN拨号成功后，将会使用获取的地址（172.31.1.10-172.31.1.200）访问内部主机，因此内部网络需要增加到172.31.1.0/24网段的回程路由指向FortiGate 或者 可以在策略中开启NAT，那么源地址将被转换为FortiGate接口地址，则不用考虑回程路由。



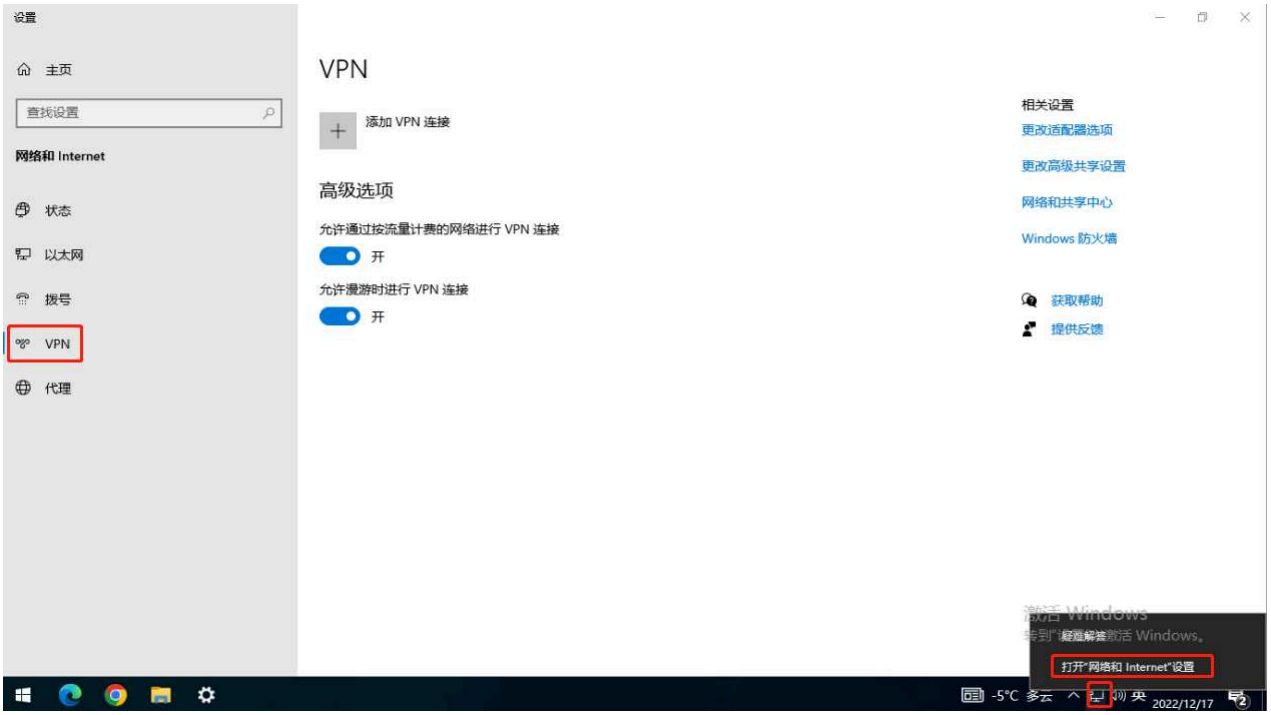
6. **配置路由**

将L2TP地址池的地址段指向l2t.root接口。

```
config router static
    edit 0
        set dst 172.31.1.0 255.255.255.0
        set device "l2t.root"
    next
end
```

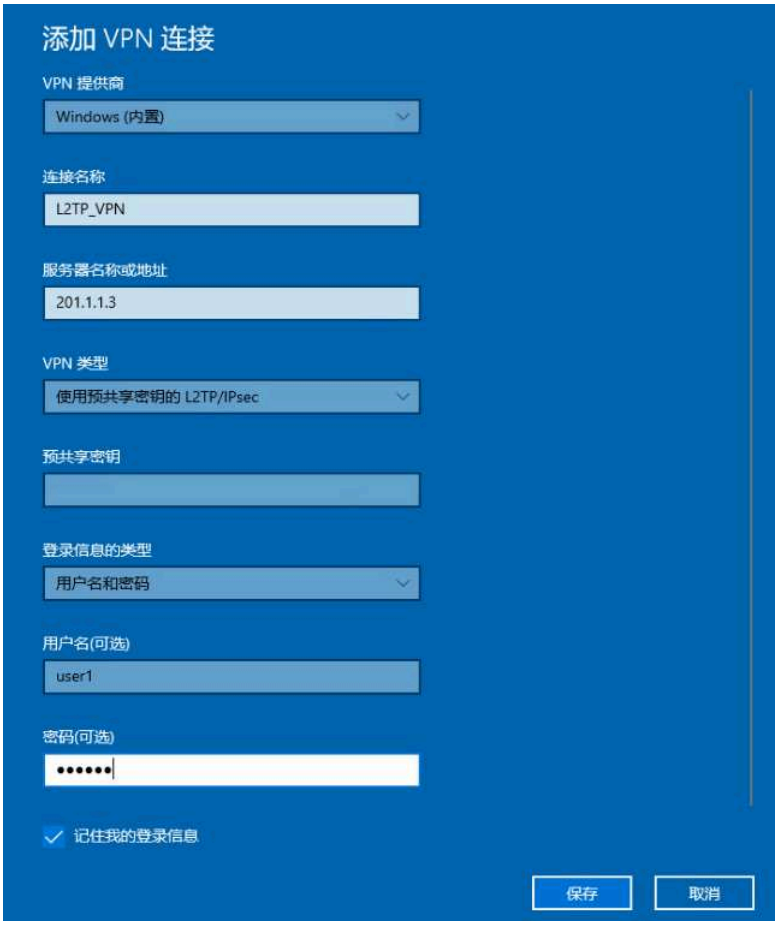
配置终端L2TP VPN

1. 右击本地连接图标，选择“打开网络和Internet设置”，选择VPN。



2. 点击“添加VPN连接”，设置L2TP，然后点击保存。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. L2TP VPN创建完整。



4. 修改注册表

Windows系统默认使用L2TP over IPSec的拨号方式，因此首先会发起IKE的协商，并不是纯L2TP的协商，需要修改电脑的注册表，让电脑发起纯L2TP的协商，而非IKE的协商。

> **重要**
>
> 修改注册表后需要重启计算机才能生效。

修改方法：

- 打开注册表编辑器，找到注册表路径 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters` 下的 `ProhibitIpSec` 选项（若没有则在 `Parameters` 目录下创建DWORD(32位)值 `ProhibitIpSec` 即可）的值修改为1。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 也可以通过如下CMD命令执行（需要管理员权限）。

```bash
reg add "HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters" /v prohibiteIPsec /t REG_DWORD /d 1 /f
```

L2TP VPN拨号测试

1. 点击创建的“L2TP_VPN”，点击“连接”。



2. 连接成功。



查看L2TP_VPN获取的地址

```
C:\Users\admin>ipconfig/all
以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection #2
   物理地址. . . . . . . . . . . . . : 00-0C-29-A2-90-EA
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::65c4:a7eb:1876:83ac%5(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.1.1.5(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.1.1.1
   DHCPv6 IAID . . . . . . . . . . . : 402656297
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-29-1C-CC-4A-00-0C-29-A2-90-E0
   DNS 服务器  . . . . . . . . . . . : 114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

PPP 适配器 L2TP_VPN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : L2TP_VPN
   物理地址. . . . . . . . . . . . . :
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   IPv4 地址 . . . . . . . . . . . . : 172.31.1.12(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.255
   默认网关. . . . . . . . . . . . . : 0.0.0.0
   DNS 服务器  . . . . . . . . . . . : 114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

查看终端路由表。

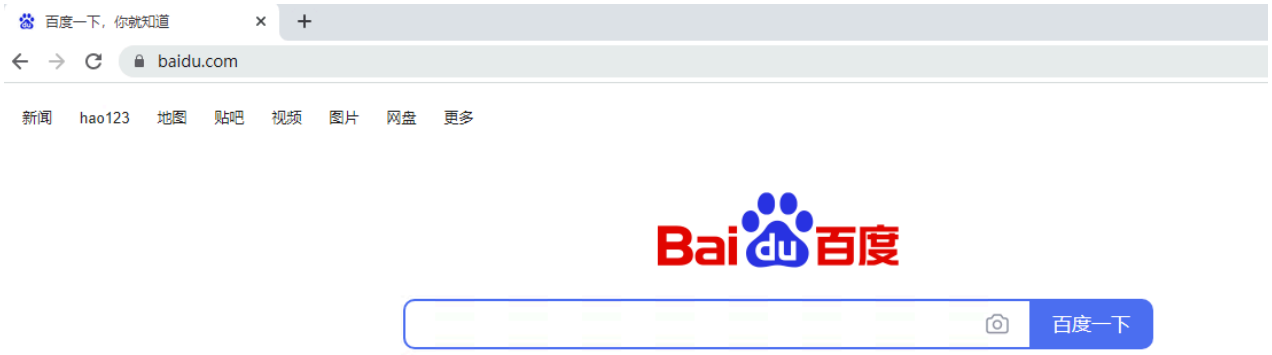
```
C:\Users\admin>route print
===========================================================================
接口列表
  6...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
 10...00 0c 29 a2 90 e0 ......Intel(R) 82574L Gigabit Network Connection
  5...00 0c 29 a2 90 ea ......Intel(R) 82574L Gigabit Network Connection #2
 46...........................L2TP_VPN
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0         10.1.1.1         10.1.1.5   4506
          0.0.0.0          0.0.0.0            在链路上       172.31.1.12     26
         10.1.1.0    255.255.255.0            在链路上          10.1.1.5   4506
         10.1.1.5  255.255.255.255            在链路上          10.1.1.5   4506
       10.1.1.255  255.255.255.255            在链路上          10.1.1.5   4506
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1   4556
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1   4556
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1   4556
      172.31.1.12  255.255.255.255            在链路上       172.31.1.12    281
```

3. 访问内部主机。

```
C:\Users\admin>ping 192.168.2.10

正在 Ping 192.168.2.10 具有 32 字节的数据:
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63

192.168.2.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

访问Internet

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



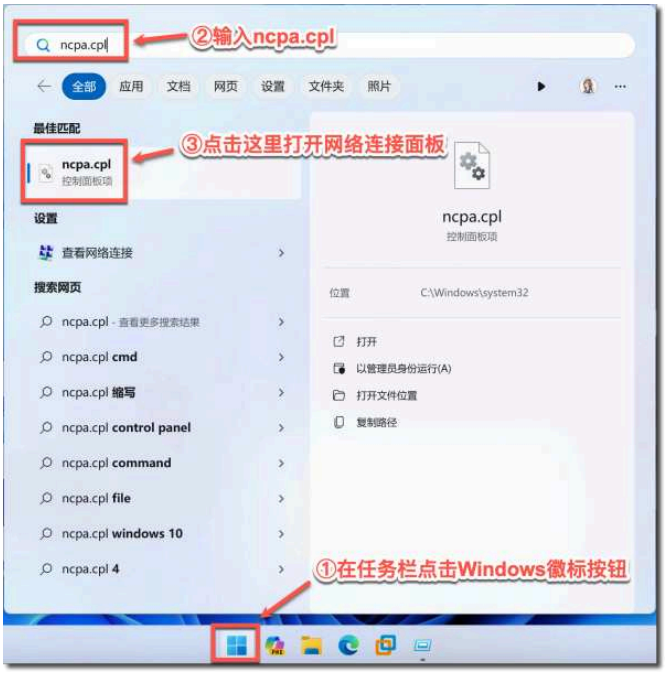
注意事项

如果FortiGate上配置的L2TP用户为LDAP认证用户，则需要确保客户端L2TP连接的认证方法为PAP。

重要

- LDAP用户身份验证支持PPTP、L2TP、IPsec VPN和防火墙身份验证，但由于点对点协议的限制，只支持PAP（Packet Authentication Protocol）。
- 由于Windows本机客户端默认使用MSCHAP或MSCHAPv2，LDAP认证场景下，您需要将其更改为PAP。

1. 在Windows系统中按照下图方式打开网络连接面板。



2. 在弹出的网络连接面板中，右键点击已创建的L2TP连接，然后点击属性按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在弹出的L2TP连接属性中，选择“安全”面板，然后勾选“允许使用这些协议”，勾选“未加密的密码(PAP)(H)”，取消勾选CHAP和MS-CHAP v2，然后点击确定按钮。之后即可正常连接L2TP。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

PPTP VPN

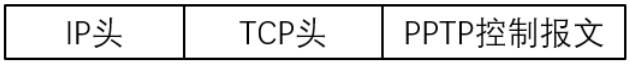
PPTP VPN简介

PPTP（Point to Point Tunneling Protocol），即点对点隧道协议，默认端口号：TCP 1723。该协议是在PPP协议的基础上开发的一种新的增强型安全协议，可以通过密码验证协议（PAP）、可扩展认证协议（EAP）等方法增强安全性，远程用户可以通过PPTP VPN拨号访问公司内网资源。

PPTP数据报文

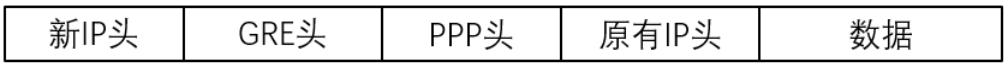
PPTP数据报文分为两种：

控制报文：用于创建、维护、终止PPTP连接；




```
No.  Time    Source       Destination  Protocol  Length  Source Port  Destinationo Port  Info
  9  0.009…  10.1.1.5     201.1.1.3    PPTP          78        53956               1723  Set-Link-Info

Frame 9: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{0FB48074-675E-4FD5-8D41-A0C4ACC8F9F7}, id 0
Ethernet II, Src: VMware_a2:90:ea (00:0c:29:a2:90:ea), Dst: VMware_2e:3f:cf (00:0c:29:2e:3f:cf)
Internet Protocol Version 4, Src: 10.1.1.5, Dst: 201.1.1.3
Transmission Control Protocol, Src Port: 53956, Dst Port: 1723, Seq: 2729513262, Ack: 3409293323, Len: 24
Point-to-Point Tunnelling Protocol
    Length: 24
    Message type: Control Message (1)
    Magic Cookie: 0x1a2b3c4d (correct)
    Control Message Type: Set-Link-Info (15)
    Reserved: 0000
    Peer Call ID: 48890
    Reserved: 0000
    Send ACCM: 0xffffffff
    Receive ACCM: 0xffffffff
```

数据报文：用来传送PPP数据包，PPP数据包封装在GRE里进行传送。




```
No.  Time    Source       Destination  Protocol  Length  Source Port  Destinationo Port  Info
 73  2.226…  10.1.1.5     201.1.1.3    PPP Comp      91                                 Compressed data

Frame 73: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{0FB48074-675E-4FD5-8D41-A0C4ACC8F9F7}, id 0
Ethernet II, Src: VMware_a2:90:ea (00:0c:29:a2:90:ea), Dst: VMware_2e:3f:cf (00:0c:29:2e:3f:cf)
Internet Protocol Version 4, Src: 10.1.1.5, Dst: 201.1.1.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 77
    Identification: 0x2f02 (12034)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: Generic Routing Encapsulation (47)
    Header Checksum: 0x3676 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.1.1.5
    Destination Address: 201.1.1.3
Generic Routing Encapsulation (PPP)
  > Flags and Version: 0x3001
    Protocol Type: PPP (0x880b)
    Payload Length: 45
    Call ID: 48890
    Sequence Number: 23
Point-to-Point Protocol
    Protocol: Compressed datagram (0x00fd)
PPP Compressed Datagram
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

PPTP协议交互过程

1. 建立TCP三次握手；

2. 建立PPTP控制层连接：

   Start Control Connection Request：Client发起控制链接请求，用于初始化PPTP Client 和Server之间的Tunnel,开始Tunnel的建立过程；

   Start Control Connection Reply：Server控制链接响应，表示接受了对端的连接请求；

   Outgoing Call Request：创建隧道，选择一个调用ID用于标识客户端到服务器发送数据的PPTP隧道；

   Outgoing Call Reply：隧道创建成功应答，选择一个调用ID用于标识从服务器到客户端发送数据的PPTP隧道；

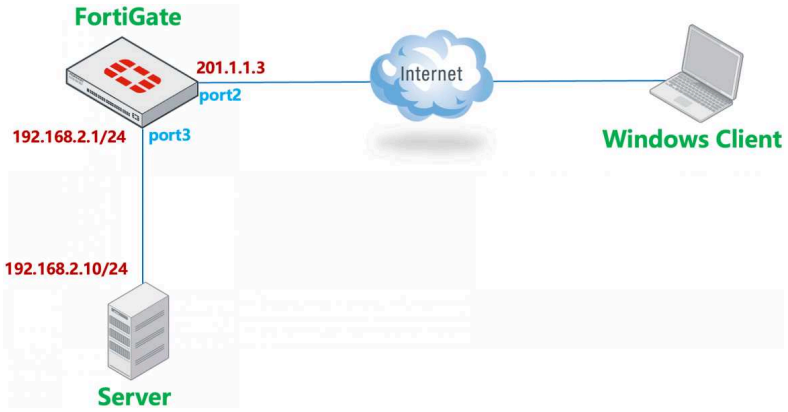
   Set-Link-Info：指定PPP协商选项。

No.	Time	Source	Destination	Protocol	Length	Source Port	Destinationo Port	Info
1	0.000…	10.1.1.5	201.1.1.3	TCP	66	53956	1723	53956 → 1723 [SYN] Seq=2729512937 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000…	201.1.1.3	10.1.1.5	TCP	66	1723	53956	1723 → 53956 [SYN, ACK] Seq=3409293134 Ack=2729512938 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=16384
3	0.000…	10.1.1.5	201.1.1.3	TCP	54	53956	1723	53956 → 1723 [ACK] Seq=2729512938 Ack=3409293135 Win=2102272 Len=0
4	0.001…	10.1.1.5	201.1.1.3	PPTP	210	53956	1723	Start-Control-Connection-Request
5	0.002…	201.1.1.3	10.1.1.5	TCP	60	1723	53956	1723 → 53956 [ACK] Seq=3409293135 Ack=2729513094 Win=180224 Len=0
6	0.002…	201.1.1.3	10.1.1.5	PPTP	210	1723	53956	Start-Control-Connection-Reply
7	0.002…	10.1.1.5	201.1.1.3	PPTP	222	53956	1723	Outgoing-Call-Request
8	0.003…	201.1.1.3	10.1.1.5	PPTP	86	1723	53956	Outgoing-Call-Reply
9	0.009…	10.1.1.5	201.1.1.3	PPTP	78	53956	1723	Set-Link-Info
10	0.012…	10.1.1.5	201.1.1.3	PPP LCP	71			Configuration Request
11	0.017…	201.1.1.3	10.1.1.5	PPP LCP	75			Configuration Request
12	0.017…	10.1.1.5	201.1.1.3	PPP LCP	79			Configuration Ack
13	0.017…	201.1.1.3	10.1.1.5	GRE	60			Encapsulated PPP
14	0.047…	201.1.1.3	10.1.1.5	TCP	60	1723	53956	1723 → 53956 [ACK] Seq=3409293323 Ack=2729513286 Win=180224 Len=0
15	2.009…	10.1.1.5	201.1.1.3	PPP LCP	71			Configuration Request
16	2.009…	201.1.1.3	10.1.1.5	GRE	60			Encapsulated PPP

网络需求

在外移动办公的工作人员需要通过PPTP VPN 隧道模式拨入到公司内网来对内网主机进行访问。

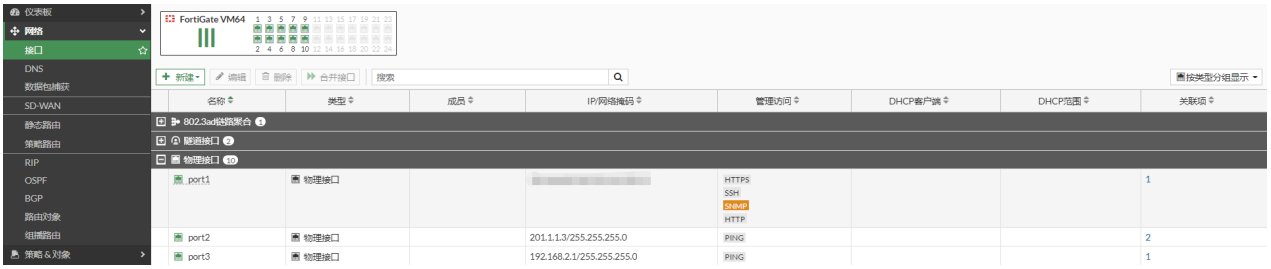
网络拓扑



配置步骤

配置FortiGate PPTP VPN

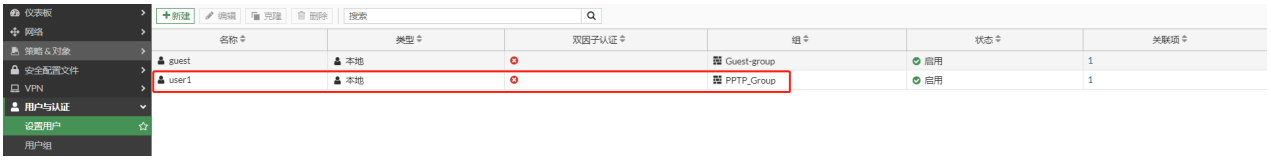
1. **基础配置**

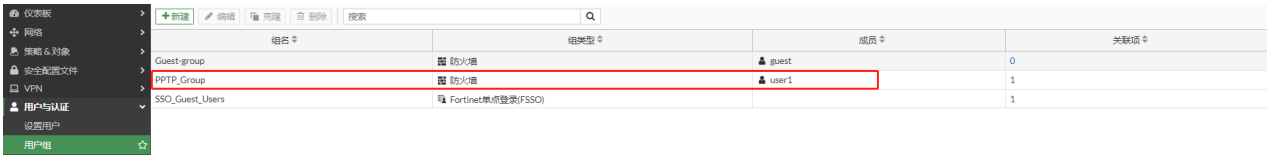


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 创建用户并将用户加入到用户组





3. 配置PPTP VPN

```
config vpn pptp
    set status enable
    set eip 172.31.1.200
    set sip 172.31.1.10
    set usrgrp "PPTP_Group"
end
```

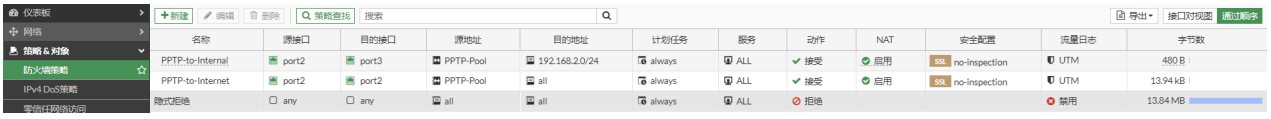
4. 配置地址对象



5. 配置防火墙策略

第1条策略用于客户端PPTP VPN拨号后访问内网；第2条策略用于客户端PPTP VPN拨号后上网。

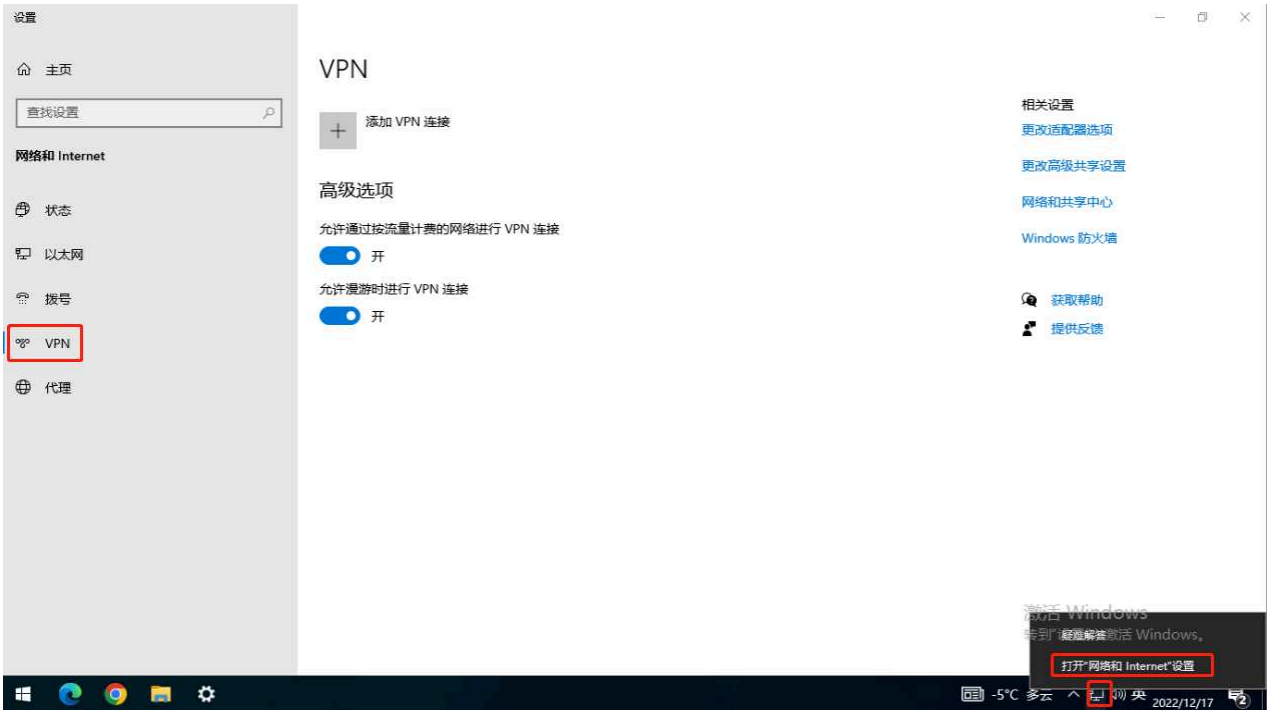
当客户端PPTP VPN拨号成功后，将会使用获取的地址（172.31.1.10-172.31.1.200）访问内部主机，因此内部网络需要增加到172.31.1.0/24网段的回程路由指向FortiGate 或者 可以在策略中开启NAT，那么源地址将被转换为FortiGate接口地址，则不用考虑回程路由。



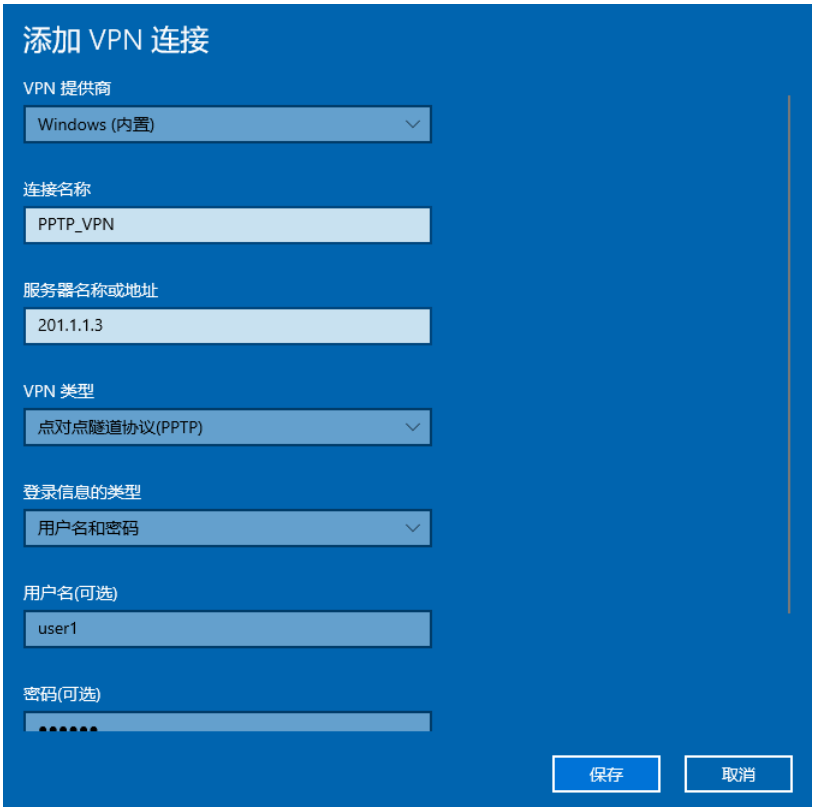
配置终端PPTP VPN

1. 右击本地连接图标，选择“打开网络和Internet设置”，选择VPN。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 点击“添加VPN连接”，设置PPTP，然后点击保存。



3. PPTP VPN创建完成。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



PPTP VPN拨号测试

1. 点击创建的“PPTP_VPN”，点击“连接”。



2. 连接成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看PPTP VPN获取的地址，可以看到FortiGate无法推送DNS给PPTP客户端，如果PPTP客户端需要使用DNS，则需要手动编辑客户端的PPTP连接

```
C:\Users\admin>ipconfig/all
以太网适配器 Ethernet1:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection #2
   物理地址. . . . . . . . . . . . . : 00-0C-29-A2-90-EA
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::65c4:a7eb:1876:83ac%5(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.1.1.5(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.1.1.1
   DHCPv6 IAID . . . . . . . . . . . : 402656297
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-29-1C-CC-4A-00-0C-29-A2-90-E0
   DNS 服务器  . . . . . . . . . . . : 114.114.114.114
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

PPP 适配器 PPTP_VPN:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : PPTP_VPN
   物理地址. . . . . . . . . . . . . :
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   IPv4 地址 . . . . . . . . . . . . : 172.31.1.11(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.255
   默认网关. . . . . . . . . . . . . : 0.0.0.0
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

查看终端路由表。

```
C:\Users\admin>route print
===========================================================================
接口列表
  6...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
 10...00 0c 29 a2 90 e0 ......Intel(R) 82574L Gigabit Network Connection
  5...00 0c 29 a2 90 ea ......Intel(R) 82574L Gigabit Network Connection #2
 46...........................PPTP
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0         10.1.1.1         10.1.1.5   4506
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
          0.0.0.0          0.0.0.0            在链路上       172.31.1.11     26
         10.1.1.0    255.255.255.0            在链路上         10.1.1.5   4506
         10.1.1.5  255.255.255.255            在链路上         10.1.1.5   4506
       10.1.1.255  255.255.255.255            在链路上         10.1.1.5   4506
        127.0.0.0        255.0.0.0            在链路上        127.0.0.1   4556
        127.0.0.1  255.255.255.255            在链路上        127.0.0.1   4556
  127.255.255.255  255.255.255.255            在链路上        127.0.0.1   4556
      172.31.1.11  255.255.255.255            在链路上       172.31.1.11    281
```

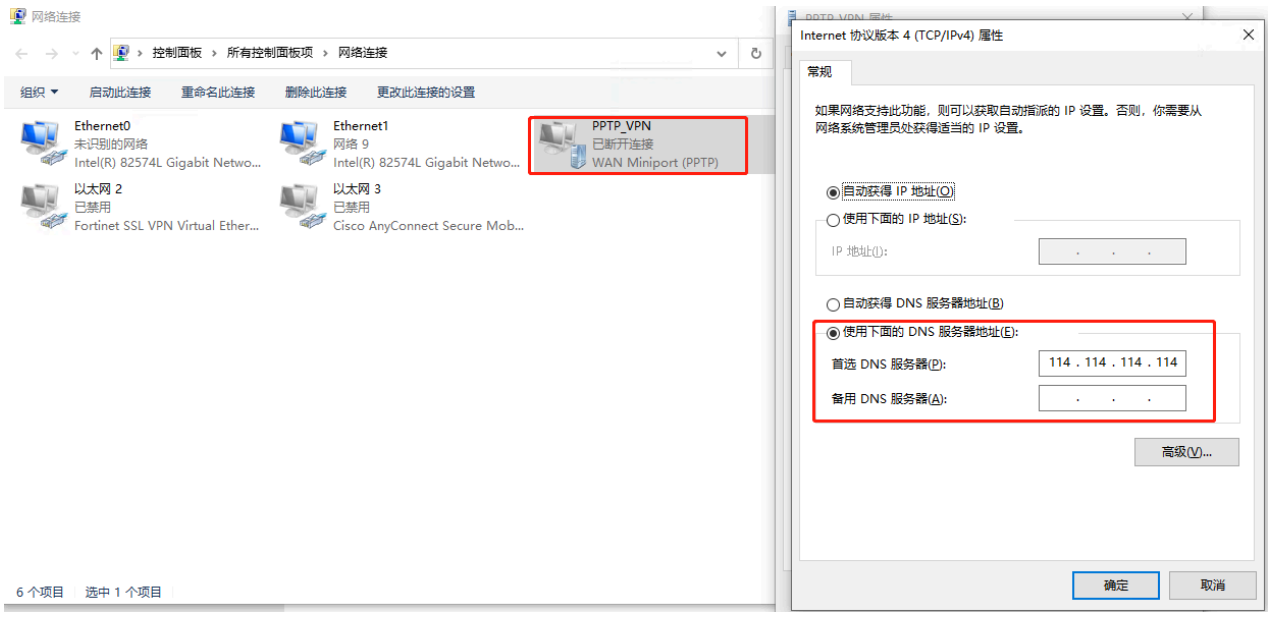
3. 访问内部主机。

```
C:\Users\admin>ping 192.168.2.10

正在 Ping 192.168.2.10 具有 32 字节的数据:
来自 192.168.2.10 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.10 的回复: 字节=32 时间=1ms TTL=63

192.168.2.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

4. 访问Internet

```
C:\Users\admin>ping 114.114.114.114

正在 Ping 114.114.114.114 具有 32 字节的数据:
来自 114.114.114.114 的回复: 字节=32 时间=23ms TTL=82
来自 114.114.114.114 的回复: 字节=32 时间=21ms TTL=71
来自 114.114.114.114 的回复: 字节=32 时间=21ms TTL=89
来自 114.114.114.114 的回复: 字节=32 时间=20ms TTL=75

114.114.114.114 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 20ms, 最长 = 23ms, 平均 = 21ms
```

5. 如果需要通过PPTP访问域名，则需要手动设置PPTP的DNS。先中断PPTP连接，手动设置DNS，然后再次拨号。



6. 访问 `www.baidu.com` 正常。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

GRE

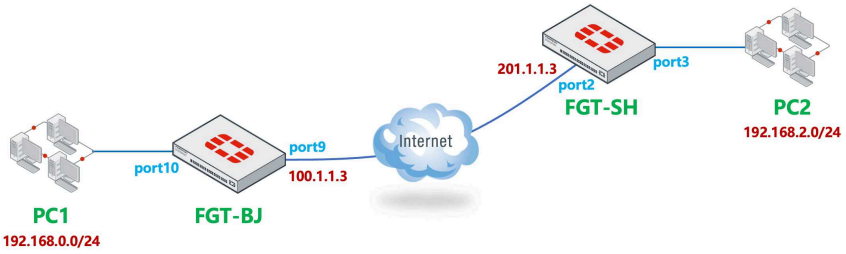
GRE简介

GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如IPv4，IPv6，IPX）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议中传输。

网络需求

通过GRE将2个局域网连接起来，实现192.168.0.0/24与192.168.2.0/24两个网段的通信。

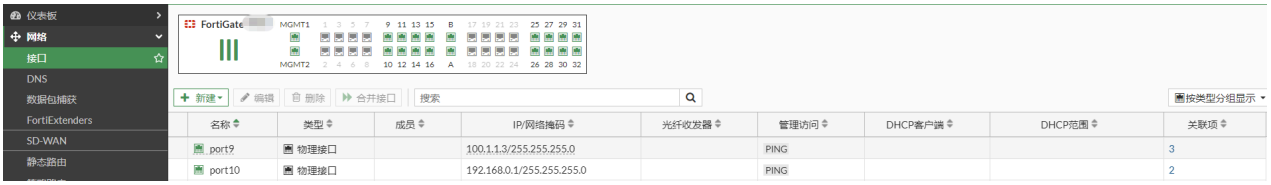
网络拓扑



配置步骤

FGT-BJ GRE配置

1. 基础配置

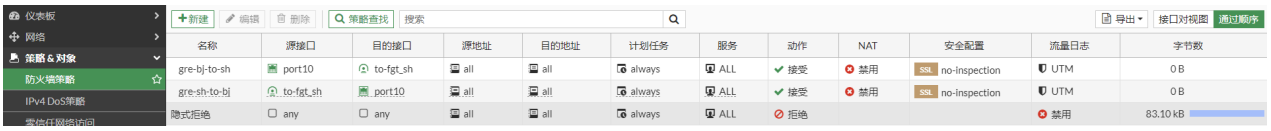




2. 配置GRE

```
config system gre-tunnel
    edit "to-fgt_sh"
        set interface "port9"
        set remote-gw 201.1.1.3
        set local-gw 100.1.1.3
    next
end
```

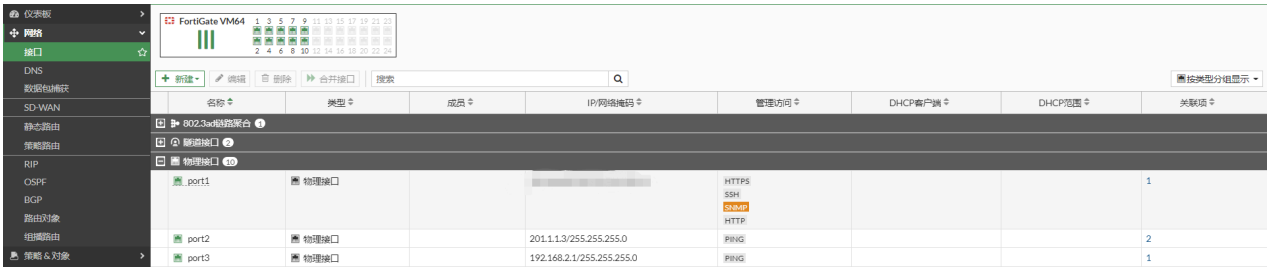
3. 配置策略



FGT-SH GRE配置

1. 基础配置

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





2. 配置GRE

```
config system gre-tunnel
    edit "to-fgt_bj"
        set interface "port2"
        set remote-gw 100.1.1.3
        set local-gw 201.1.1.3
    next
end
```

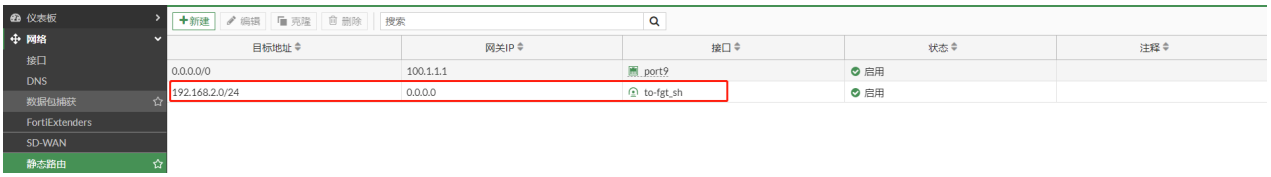
3. 配置策略



路由及业务测试

静态路由互通

1. FGT-BJ 配置静态路由



2. FGT-SH配置静态路由



3. 业务测试

从FGT-BJ内网能ping通FGT-SH的内网

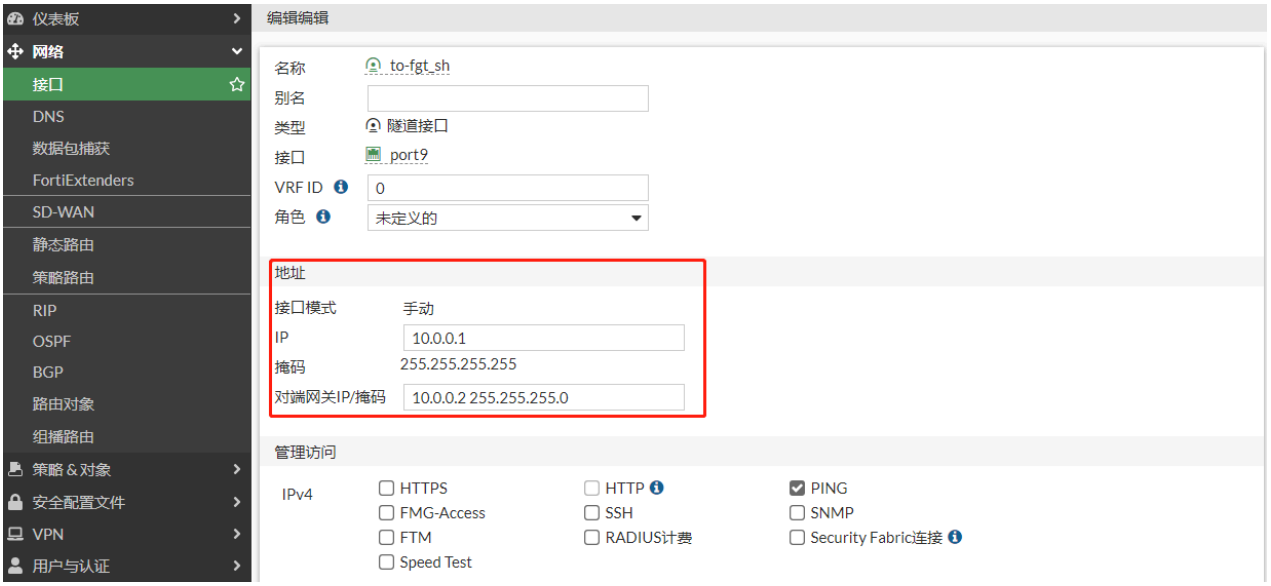
```
PC1# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6225014  bytes 1799326210 (1.6 GiB)
        RX errors 0  dropped 3749612  overruns 0  frame 0
        TX packets 75758  bytes 5398290 (5.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC1# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
64 bytes from 192.168.2.10: icmp_seq=1 ttl=62 time=1.15 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=62 time=0.931 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=0.994 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=0.673 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.673/0.938/1.155/0.174 ms
```

动态路由互通

1. FGT-BJ 配置GRE隧道接口IP

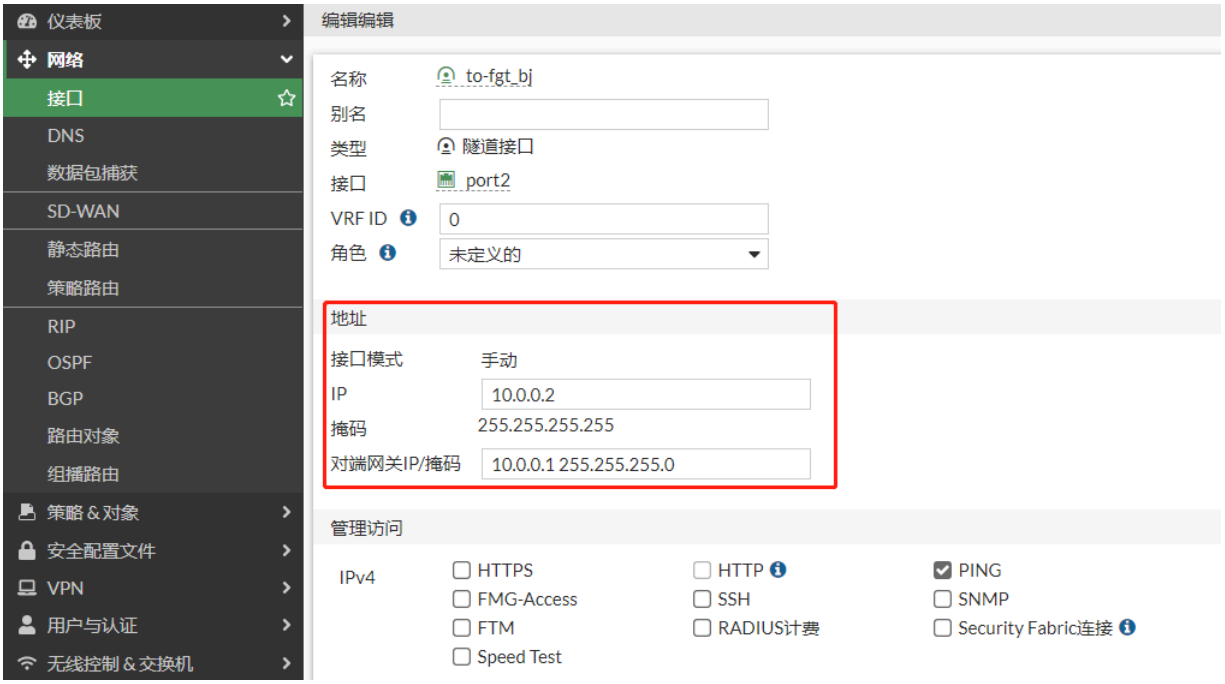


查看路由表

```
# get router info routing-table  all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port9, [1/0]
C       10.0.0.0/24 is directly connected, to-fgt_sh
C       10.0.0.1/32 is directly connected, to-fgt_sh
C       100.1.1.0/24 is directly connected, port9
C       192.168.0.0/24 is directly connected, port10
```

2. FGT-SH配置GRE隧道接口IP

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看路由表

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 201.1.1.1, port2, [1/0]
C       10.0.0.0/24 is directly connected, to-fgt_bj
C       10.0.0.2/32 is directly connected, to-fgt_bj
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected
```

3. GRE接口连通性测试

```
从FGT-BJ的GRE接口地址 ping FGT-SH的GRE接口地址
# execute ping-options source 10.0.0.1
# execute ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=255 time=0.5 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=255 time=0.5 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=255 time=0.4 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=255 time=0.1 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.4/0.5 ms
```

4. 配置动态路由

BGP互通

1. 配置BGP

FGT-BJ配置BGP

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config router bgp
    set as 65001
    set router-id 100.1.1.3
    config neighbor
        edit "10.0.0.2"
            set next-hop-self enable
            set soft-reconfiguration enable
            set interface "to-fgt_sh"
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 192.168.0.0 255.255.255.0
        next
    end
end
```

FGT-SH配置BGP

```
config router bgp
    set as 65001
    set router-id 201.1.1.3
    config neighbor
        edit "10.0.0.1"
            set next-hop-self enable
            set soft-reconfiguration enable
            set remote-as 65001
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```

2. 查看BGP邻居和路由

FGT-BJ查看BGP邻居和路由

```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.0.0.2, remote AS 65001, local AS 65001, internal link
  BGP version 4, remote router ID 201.1.1.3
  BGP state = Established, up for 04:22:48
  Last read 00:00:13, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 302 messages, 0 notifications, 0 in queue
  Sent 302 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Inbound soft reconfiguration allowed
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes, 1 prefixes in rib
  1 announced prefixes
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes, 0 prefixes in rib
  0 announced prefixes
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
 Connections established 1; dropped 0
Local host: 10.0.0.1, Local port: 179
Foreign host: 10.0.0.2, Foreign port: 14233
Egress interface: 55
Nexthop: 10.0.0.1
Nexthop interface: to-fgt_sh
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

# get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port9, [1/0]
C       10.0.0.0/24 is directly connected, to-fgt_sh
C       10.0.0.1/32 is directly connected, to-fgt_sh
C       100.1.1.0/24 is directly connected, port9
C       192.168.0.0/24 is directly connected, port10
B       192.168.2.0/24 [200/0] via 10.0.0.2 (recursive is directly connected, to-fgt_sh), 04:22:34
```

FGT-SH查看BGP邻居和路由

```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.0.0.1, remote AS 65001, local AS 65001, internal link
  BGP version 4, remote router ID 100.1.1.3
  BGP state = Established, up for 04:24:18
  Last read 00:00:30, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 303 messages, 0 notifications, 0 in queue
  Sent 304 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 8, neighbor version 7
  Index 1, Offset 0, Mask 0x2
  Inbound soft reconfiguration allowed
  NEXT_HOP is always this router
  Community attribute sent to this neighbor (both)
  1 accepted prefixes, 1 prefixes in rib
  1 announced prefixes
 For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes, 0 prefixes in rib
  0 announced prefixes
 Connections established 1; dropped 0
Local host: 10.0.0.2, Local port: 14233
Foreign host: 10.0.0.1, Foreign port: 179
Egress interface: 34
Nexthop: 10.0.0.2
Nexthop interface: to-fgt_bj
Nexthop global: ::
Nexthop local: ::
BGP connection: non shared network

FGVM08TM22000410 # get router info routing-table  all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 201.1.1.1, port2, [1/0]
C       10.0.0.0/24 is directly connected, to-fgt_bj
C       10.0.0.2/32 is directly connected, to-fgt_bj
B       192.168.0.0/24 [200/0] via 10.0.0.1 (recursive is directly connected, to-fgt_bj), 04:23:24
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected, port2
```

3. 业务测试

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

从FGT-BJ内网能ping通FGT-SH的内网

```
PC1# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6225014  bytes 1799326210 (1.6 GiB)
        RX errors 0  dropped 3749612  overruns 0  frame 0
        TX packets 75758  bytes 5398290 (5.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC1# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=62 time=1.15 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=62 time=0.931 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=0.994 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=0.673 ms

--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.673/0.938/1.155/0.174 ms
```

OSPF互通

1. 配置OSPF

FGT-BJ配置OSPF

```
config router ospf
    set router-id 100.1.1.3
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 10.0.0.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.0.0 255.255.255.0
        next
    end
end
```

FGT-SH配置OSPF

```
config router ospf
    set router-id 201.1.1.3
    config area
        edit 0.0.0.0
        next
    end
    config network
        edit 1
            set prefix 10.0.0.0 255.255.255.0
        next
        edit 2
            set prefix 192.168.2.0 255.255.255.0
        next
    end
en
```

2. 查看OSPF邻居和路由

FGT-BJ查看OSPF邻居和路由

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
201.1.1.3         1   Full/ -         00:00:33    10.0.0.2        to-fgt_sh

# get router info routing-table  all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 100.1.1.1, port9, [1/0]
C       10.0.0.0/24 is directly connected, to-fgt_sh
C       10.0.0.1/32 is directly connected, to-fgt_sh
C       100.1.1.0/24 is directly connected, port9
C       192.168.0.0/24 is directly connected, port10
O       192.168.2.0/24 [110/101] via 10.0.0.2, to-fgt_sh, 00:01:12
```

FGT-SH查看OSPF邻居和路由

```
# get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
100.1.1.3         1   Full/ -         00:00:34    10.0.0.1        to-fgt_bj

# get router info routing-table all
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 201.1.1.1, port2, [1/0]
C       10.0.0.0/24 is directly connected, to-fgt_bj
C       10.0.0.2/32 is directly connected, to-fgt_bj
O       192.168.0.0/24 [110/101] via 10.0.0.1, to-fgt_bj, 00:01:43
C       192.168.2.0/24 is directly connected, port3
C       201.1.1.0/24 is directly connected, port2
```

3. **业务测试**

从FGT-BJ内网能ping通FGT-SH的内网

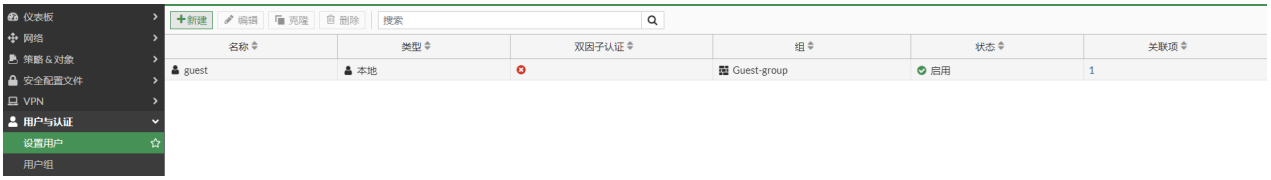
```
PC1# ifconfig ens224
ens224: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.10  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::82c8:edfd:199d:70b0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:ad:a9  txqueuelen 1000  (Ethernet)
        RX packets 6225014  bytes 1799326210 (1.6 GiB)
        RX errors 0  dropped 3749612  overruns 0  frame 0
        TX packets 75758  bytes 5398290 (5.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

PC1# ping 192.168.2.10 -c 4
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 bytes from 192.168.2.10: icmp_seq=1 ttl=62 time=1.15 ms
64 bytes from 192.168.2.10: icmp_seq=2 ttl=62 time=0.931 ms
64 bytes from 192.168.2.10: icmp_seq=3 ttl=62 time=0.994 ms
64 bytes from 192.168.2.10: icmp_seq=4 ttl=62 time=0.673 ms
--- 192.168.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.673/0.938/1.155/0.174 ms
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

本地用户和用户组

创建本地用户

1. 选择“用户与认证”-->“设置用户”，点击“新建”



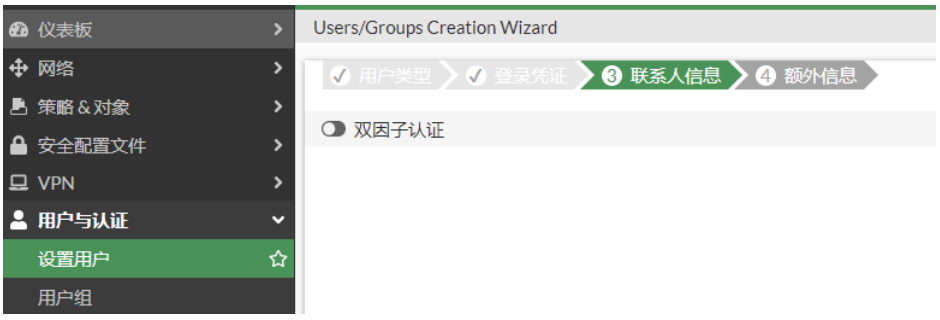
2. 选择“本地用户”，点击“下一步”



3. 输入用户名和密码，点击“下一步”



4. 如果本地用户需要绑定FortiGate本地的Fortitoken，则勾选“双因子认证”。这里不需要，直接点击“下一步”

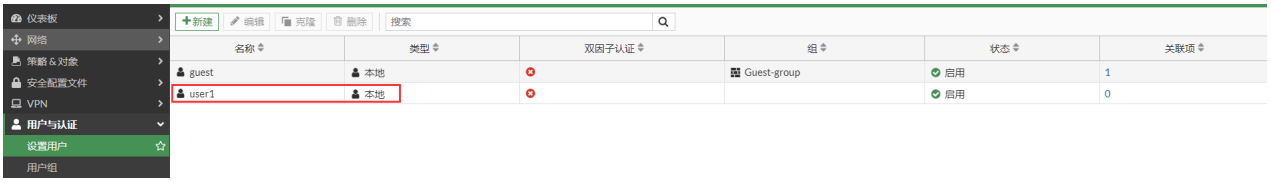


5. 如果需要现在为本地用户指定一个用户组，可以勾选“用户组”来指定，也可以等创建完用户后，在用户组菜单中添加。这里不勾选，直接点击“提交”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

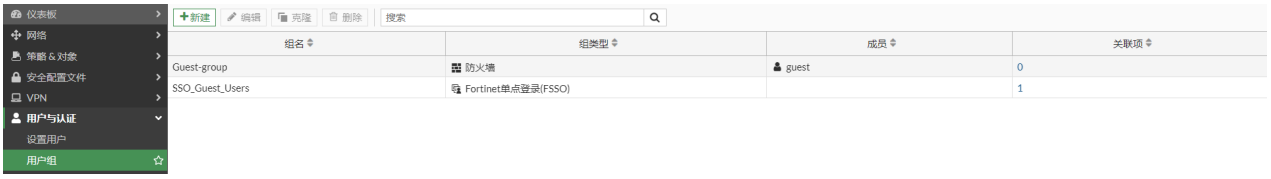


6. 配置完成

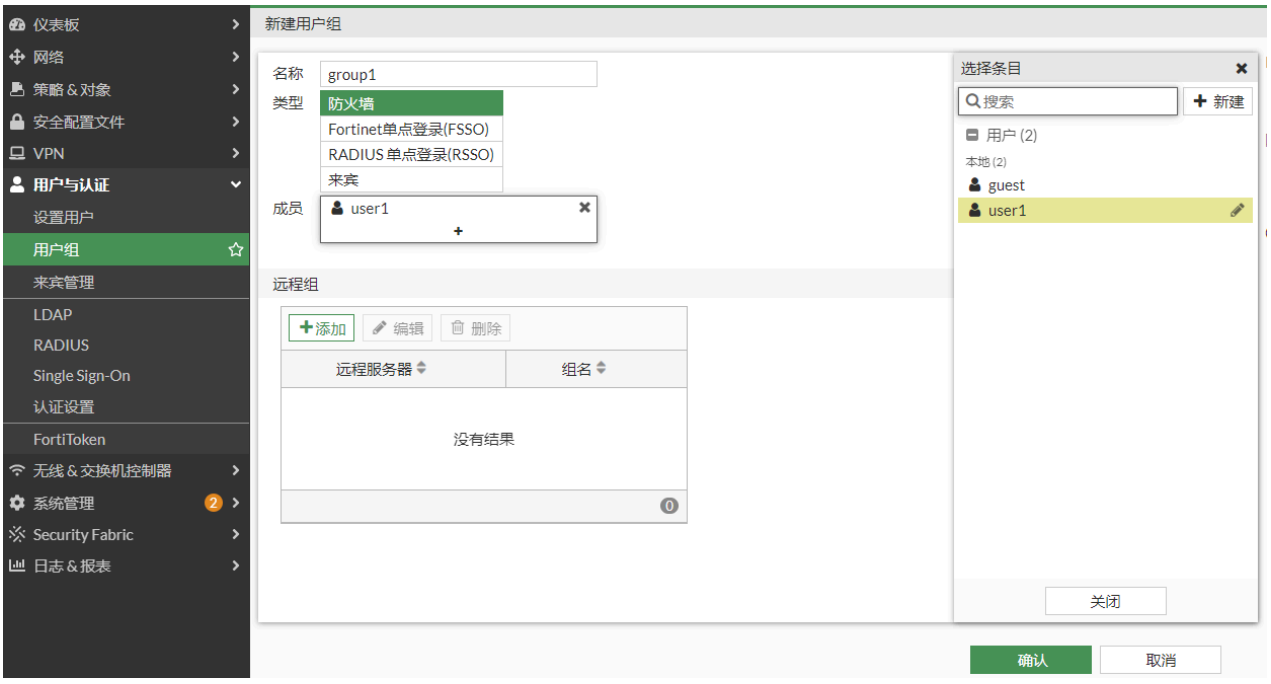


创建本地用户组

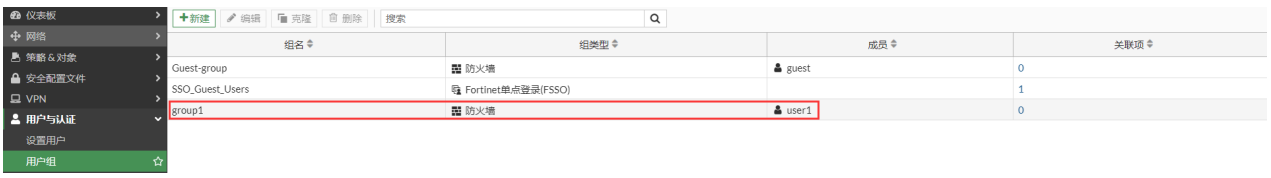
1. 选择“用户与认证”-->“用户组”，点击“新建”



2. 输入用户组名称，在“成员”中选择已创建好的用户，如user1，可以添加多个用户，点击“确认”



3. 配置完成



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

LDAP认证原理

LDAP简介

LDAP（Light Directory Access Protocol），轻量级目录访问协议，是一个为查询、浏览和搜索而优化的专业分布式数据库，它成树状结构组织数据。目录服务是由目录数据库和一套访问协议组成的系统。

LDAP组织结构

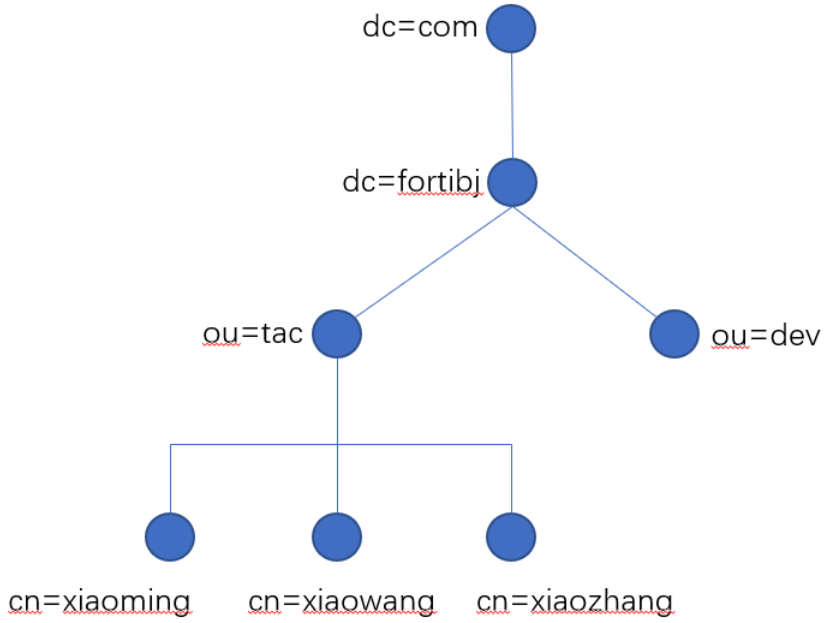
在LDAP中目录是按树形结构组织，而DN（Distinguished Name）唯一可区别的名称，记录了一条记录的位置。DN有三个主要属性，分别是DC（Domain Component）、OU（Organizational Unit）与CN（Common Name）。

DC：域控制器，类似于文件系统目录；

OU：组织单元，类似部门；

CN：区分身份的属性，类似名称。

如下图所示，dn是从树的叶子节点逐层向根节点推导出的一条唯一路径，表明了这个数据结构中的唯一一条记录。一个完整的dn：cn=xiaoming,ou=tac,dc=fortibj,dc=com，查询得到一条完整的记录，然后再取出所需属性(Attribute)的值。

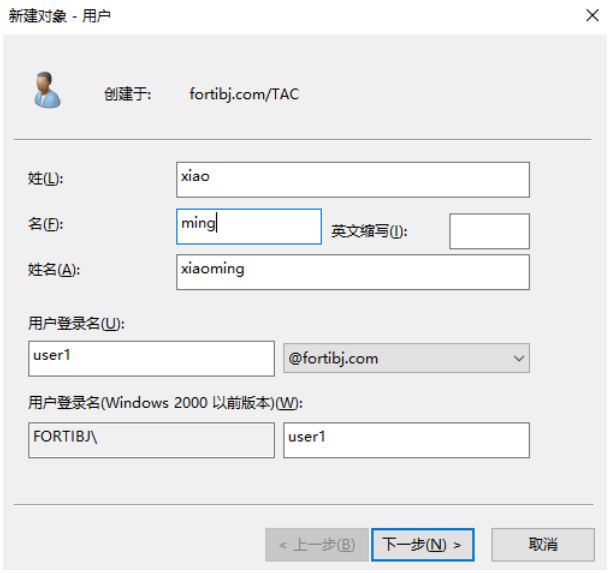


Windows AD域中几个属性

1. **CN和sAMAccountName**

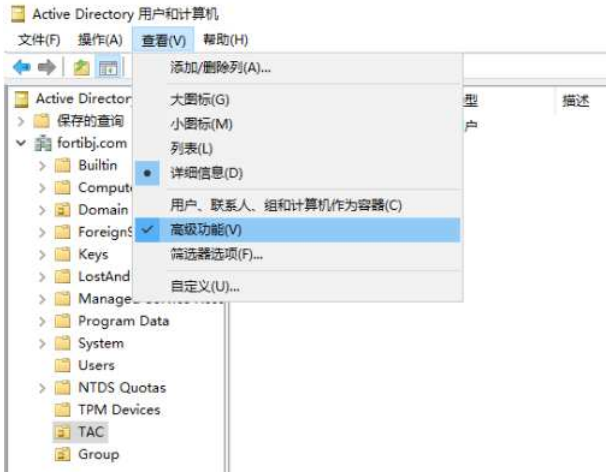
   Windows AD域中创建用户时，输入信息如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

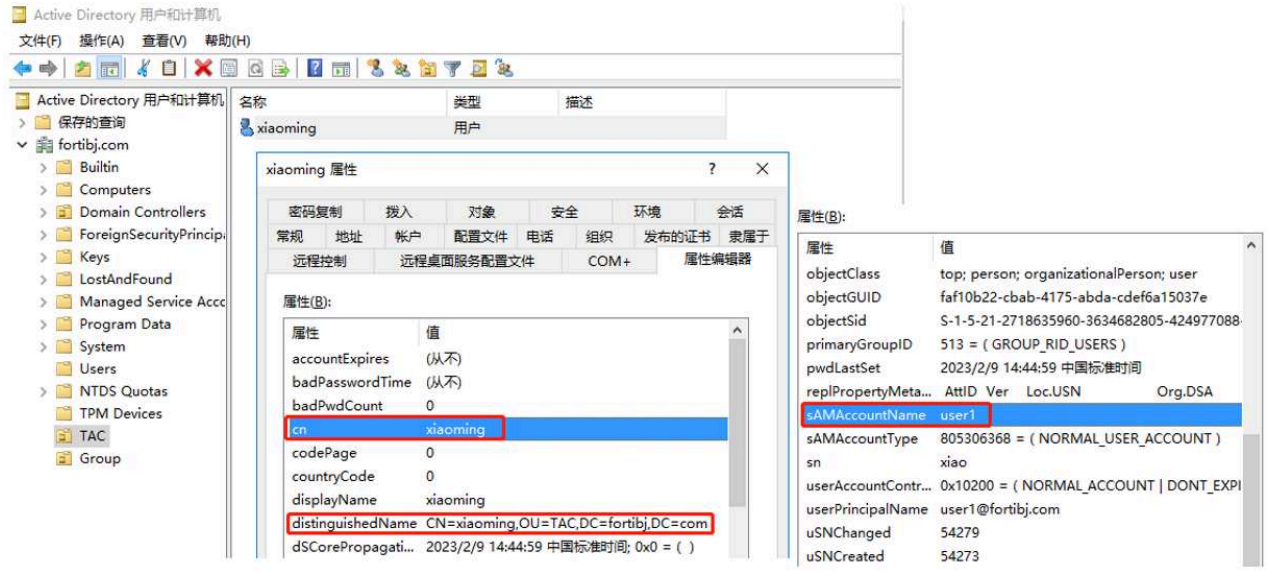


cn表示姓名（full user name），即xiaoming，sAMAccountName表示用户登录名（login user name），即user1。

在windows Active Directory用户和计算机中，点击”查看“，选择”高级功能“，然后可以查看更多的用户属性。



通过用户属性查询到用户xiaoming的CN是xiaoming，sAMAccountName是user1，dn是CN=xiaoming,OU=TAC,DC=fortibj,DC=com



windows CLI查询DN

- **根据full name查询**

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
C:\Users\Administrator>dsquery user -name xiaoming
"CN=xiaoming,OU=TAC,DC=fortibj,DC=com"
```

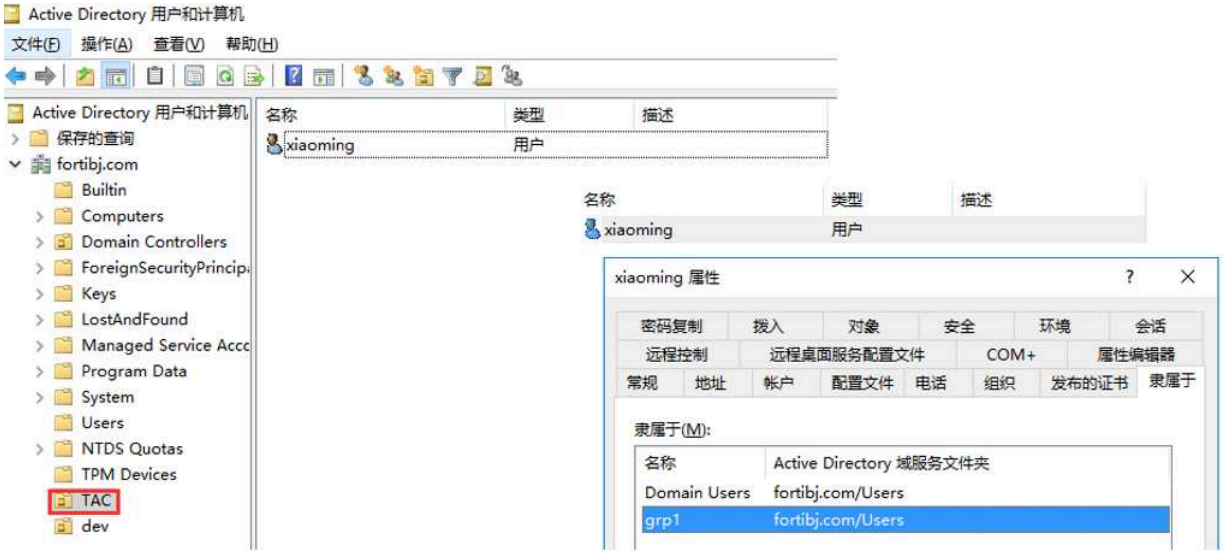
- **根据login name查询**

```
C:\Users\Administrator>dsquery user -samid user1
"CN=xiaoming,OU=TAC,DC=fortibj,DC=com"
```

2. **OU和Group**

OU是组织单元，Group是用户组，两者不一样。

从下图可以看出用户xiaoming在组织单元OU TAC下，属于用户组Domain Users和grp1。



LDAP交互过程

1. **LDAP交互过程**



2. **报文交互过程分析**

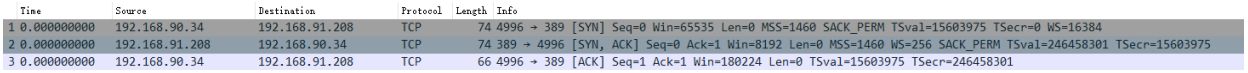
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate执行如下命令验证用户名和密码，获取用户组属性。

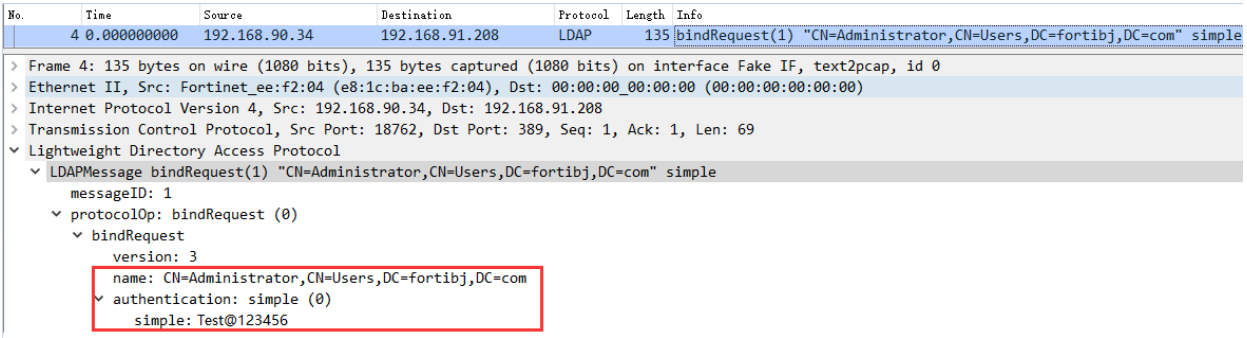
```
# diagnose test authserver ldap LDAP208 user1 Pass@123456
authenticate 'user1' against 'LDAP208' succeeded!
Group membership(s) - CN=grp1,CN=Users,DC=fortibj,DC=com
                      CN=Domain Users,CN=Users,DC=fortibj,DC=com
```

报文交互过程如下：

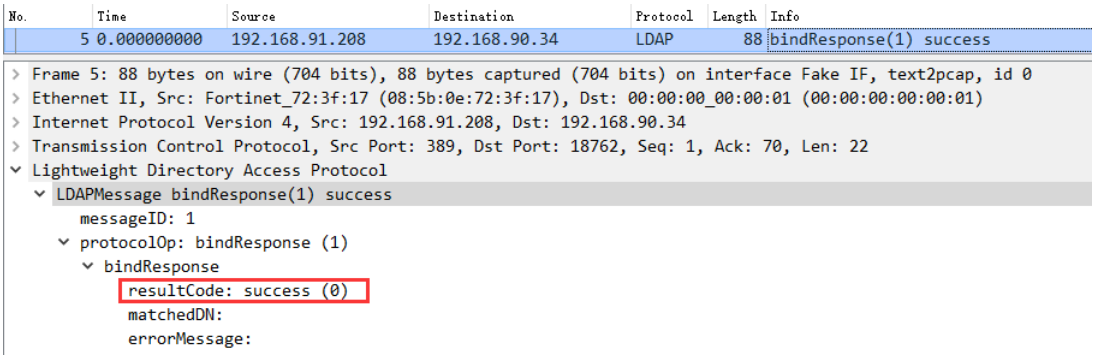
- 建立TCP连接



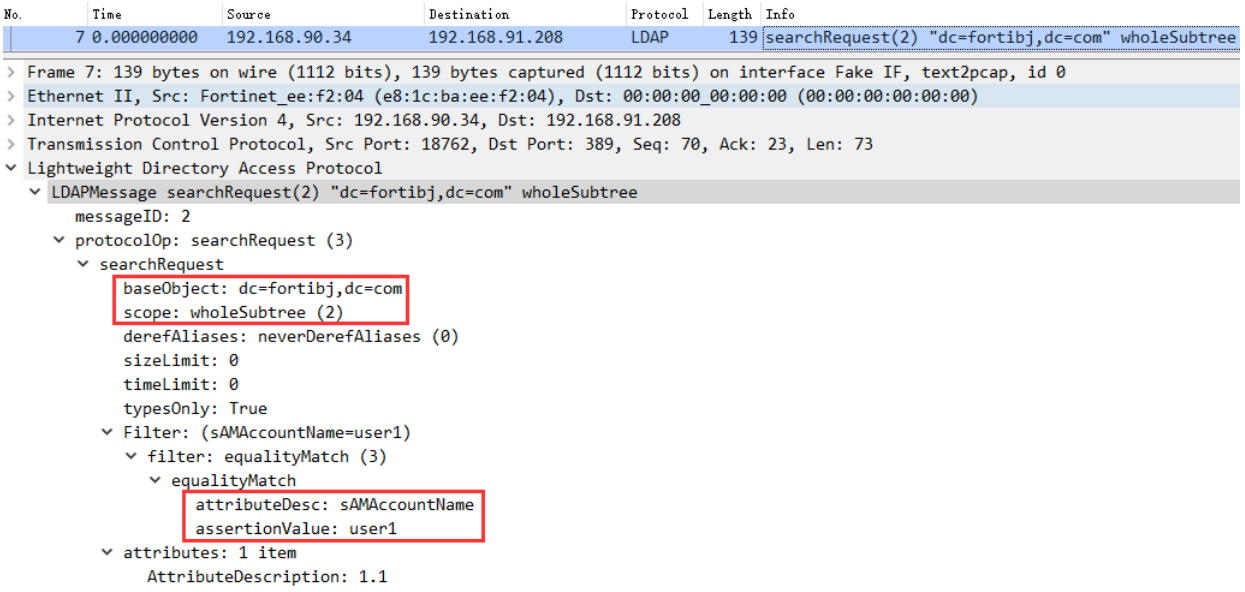
- FortiGate以管理员DN和密码为参数向LDAP服务器发送管理员绑定请求报文（Bind Request）获得查询权限



- LDAP服务器进行绑定请求报文的处理。如果绑定成功，则向FortiGate发送绑定成功的回应报文

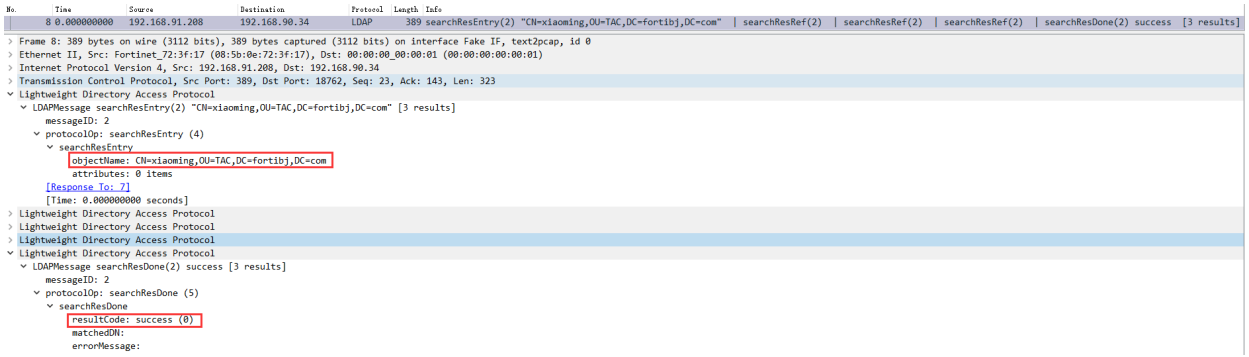


- FortiGate以输入的用户名为参数，向LDAP服务器发送用户DN查询请求报文（Search Request）

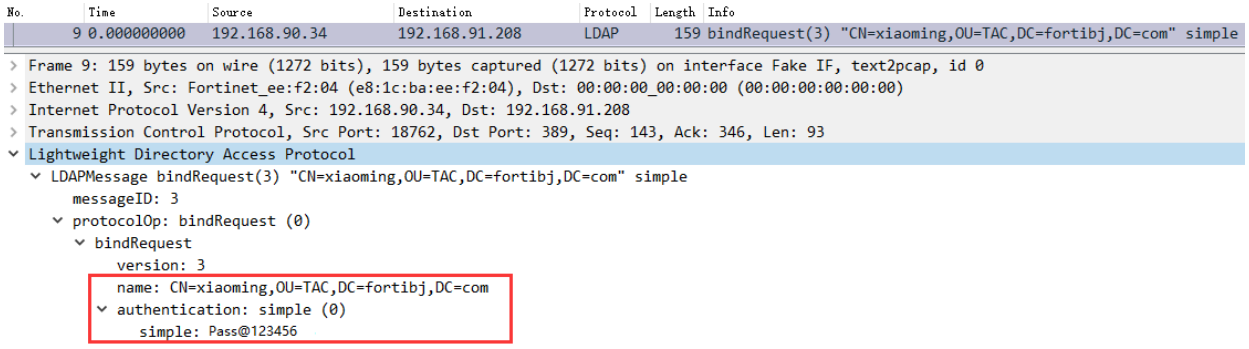


- LDAP服务器收到查询请求报文后，对用户DN进行查找。如果查询成功，则向FortiGate发送查询成功的回应报文，返回用户的DN

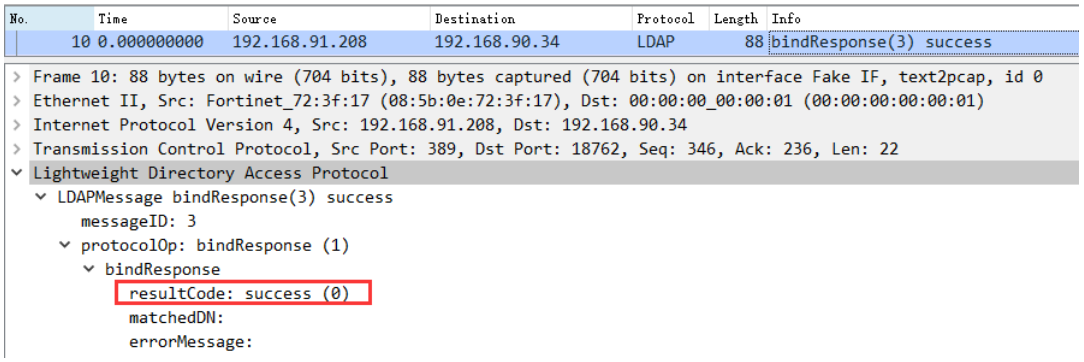
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- FortiGate以查询得到的用户DN和用户输入的密码为参数，向LDAP服务器发送用户DN绑定请求报文（Bind Request），检查用户密码是否正确



- LDAP服务器进行绑定请求报文的处理，如果绑定成功，则向FortiGate发送绑定成功的回应报文；如果绑定失败，则向FortiGate发送绑定失败的回应报文



- 如果绑定成功，FortiGate向LDAP服务器发送用户属性查询请求报文（Search Request），获取用户所属的用户组

  memberof：用户所属的组的DN。

  primaryGroupID：指定用户的主组的相对标识符(RID)。默认情况下是Domain Users组的RID，用户是其主组的成员，Domain User没有列在用户的memberOf属性中。因此需要单独查询主组的DN。

  objectSid：指定安全主体对象的安全标识符(SID)。SID是用于标识安全主体对象的唯一值。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
No.  Time          Source          Destination     Protocol  Length  Info
  11 0.000000000   192.168.90.34   192.168.91.208  LDAP         178  searchRequest(4) "CN=xiaoming,OU=TAC,DC=fortibj,DC=com" baseObject

> Frame 11: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Fortinet_ee:f2:04 (e8:1c:ba:ee:f2:04), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.90.34, Dst: 192.168.91.208
> Transmission Control Protocol, Src Port: 18762, Dst Port: 389, Seq: 236, Ack: 368, Len: 112
v Lightweight Directory Access Protocol
  v LDAPMessage searchRequest(4) "CN=xiaoming,OU=TAC,DC=fortibj,DC=com" baseObject
      messageID: 4
    v protocolOp: searchRequest (3)
      v searchRequest
          baseObject: CN=xiaoming,OU=TAC,DC=fortibj,DC=com
          scope: baseObject (0)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
        v Filter: (objectclass=*)
          v filter: present (7)
              present: objectclass
        v attributes: 3 items
            AttributeDescription: memberOf
            AttributeDescription: primaryGroupID
            AttributeDescription: objectSid
```

- LDAP服务器对查询请求报文进行处理，返回用户所在的用户组

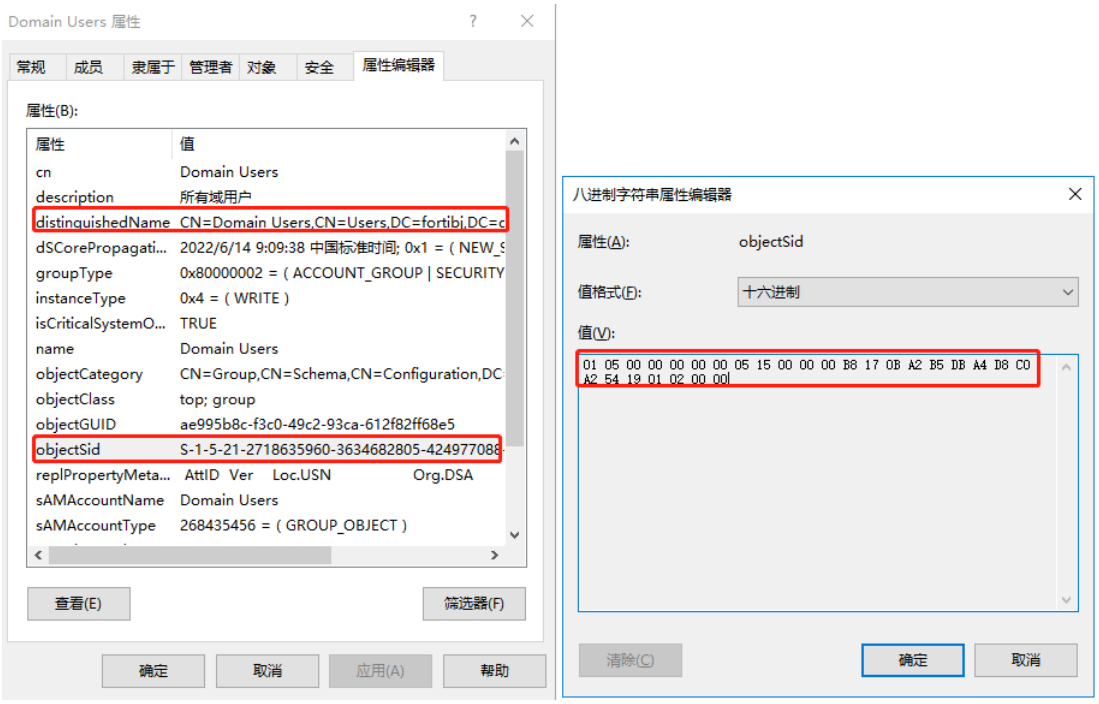
```
No.  Time          Source          Destination     Protocol  Length  Info
  12 0.000000000   192.168.91.208  192.168.90.34   LDAP         291  searchResEntry(4) "CN=xiaoming,OU=TAC,DC=fortibj,DC=com"  | searchResDone(4) success  [3 results]

> Frame 12: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Fortinet_72:3f:17 (08:5b:0e:72:3f:17), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 192.168.91.208, Dst: 192.168.90.34
> Transmission Control Protocol, Src Port: 389, Dst Port: 18762, Seq: 368, Ack: 348, Len: 225
v Lightweight Directory Access Protocol
  v LDAPMessage searchResEntry(4) "CN=xiaoming,OU=TAC,DC=fortibj,DC=com" [3 results]
      messageID: 4
    v protocolOp: searchResEntry (4)
      v searchResEntry
          objectName: CN=xiaoming,OU=TAC,DC=fortibj,DC=com
        v attributes: 3 items
          v PartialAttributeList item memberOf
              type: memberOf
            v vals: 1 item
                AttributeValue: CN=grp1,CN=Users,DC=fortibj,DC=com
          v PartialAttributeList item primaryGroupID
              type: primaryGroupID
            v vals: 1 item
                AttributeValue: 513
          v PartialAttributeList item objectSid
              type: objectSid
            v vals: 1 item
              v SID: S-1-5-21-2718635960-3634682805-424977088-2104  (Domain SID-Domain RID)
                  Revision: 1
                  Num Auth: 5
                  Authority: 5
                  Subauthorities: 21-2718635960-3634682805-424977088-2104
                  RID: 2104  (Domain RID)
      [Response To: 11]
      [Time: 0.000000000 seconds]
v Lightweight Directory Access Protocol
  v LDAPMessage searchResDone(4) success [3 results]
      messageID: 4
    v protocolOp: searchResDone (5)
      v searchResDone
          resultCode: success (0)
          matchedDN:
          errorMessage:
```

- FortiGate向LDAP服务器发送用户属性查询请求报文（Search Request），获取用户所在的主组

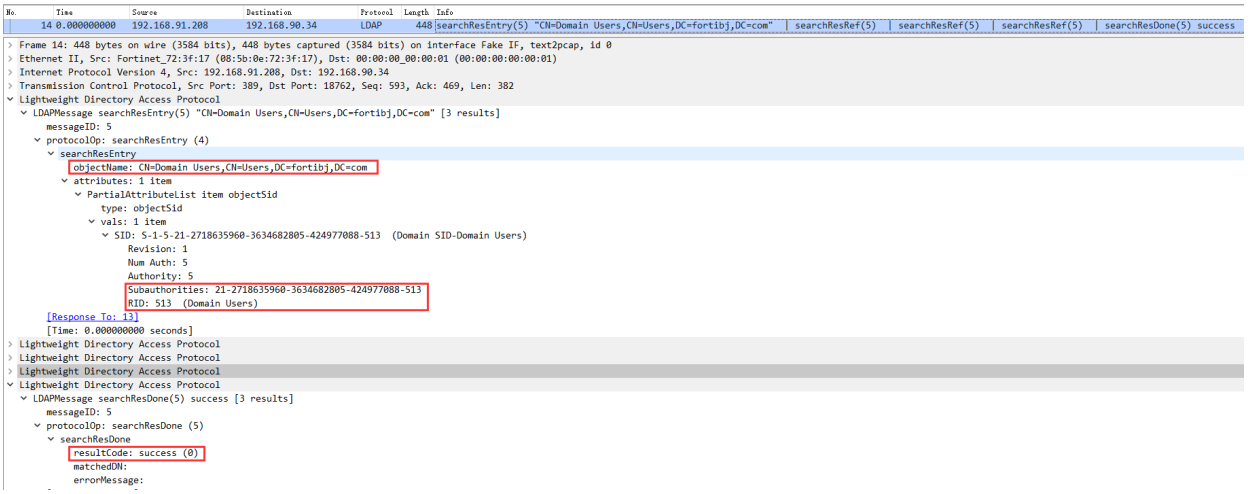
```
No.  Time          Source          Destination     Protocol  Length  Info
  13 0.000000000   192.168.90.34   192.168.91.208  LDAP         187  searchRequest(5) "dc=fortibj,dc=com" wholeSubtree

> Frame 13: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Fortinet_ee:f2:04 (e8:1c:ba:ee:f2:04), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.90.34, Dst: 192.168.91.208
> Transmission Control Protocol, Src Port: 18762, Dst Port: 389, Seq: 348, Ack: 593, Len: 121
v Lightweight Directory Access Protocol
  v LDAPMessage searchRequest(5) "dc=fortibj,dc=com" wholeSubtree
      messageID: 5
    v protocolOp: searchRequest (3)
      v searchRequest
          baseObject: dc=fortibj,dc=com
          scope: wholeSubtree (2)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
        v Filter: (&(objectclass=group)(objectSid=01:05:00:00:00:00:00:05:15:00:00:00:b8:17:0b:a2:b5:db:a4:d8:c0:a2:54:19:…))
          v filter: and (0)
            v and: (&(objectclass=group)(objectSid=01:05:00:00:00:00:00:05:15:00:00:00:b8:17:0b:a2:b5:db:a4:d8:c0:a2:54:19:…))
              v and: 2 items
                v Filter: (objectclass=group)
                  v and item: equalityMatch (3)
                    v equalityMatch
                        attributeDesc: objectclass
                        assertionValue: group
                v Filter: (objectSid=01:05:00:00:00:00:00:05:15:00:00:00:b8:17:0b:a2:b5:db:a4:d8:c0:a2:54:19:…)
                  v and item: equalityMatch (3)
                    v equalityMatch
                        attributeDesc: objectSid
                        assertionValue: 01:05:00:00:00:00:00:05:15:00:00:00:b8:17:0b:a2:b5:db:a4:d8:c0:a2:54:19:…
        v attributes: 1 item
            AttributeDescription: objectSid

0000  00 00 00 00 00 00 e8 1c  ba ee f2 04 08 00 45 00   ........ ......E·
0010  00 ad 25 15 00 00 40 06  1d f3 c0 a8 5a 22 c0 a8   ··%···@· ····Z"··
0020  5b d0 49 4a 01 85 92 0d  7b 26 66 83 9a 91 80 18   [·IJ···· {&f·····
0030  00 0b e6 55 00 00 01 01  08 0a 00 8a d7 ac 0a d0   ···U···· ········
0040  16 f0 30 77 02 01 05 63  72 04 11 64 63 3d 66 6f   ··0w···c r··dc=fo
0050  72 74 69 62 6a 2c 64 63  3d 63 6f 6d 0a 01 02 0a   rtibj,dc =com····
0060  01 00 02 01 00 02 01 00  01 01 00 a0 41 a3 14 04   ........ ····A···
0070  0b 6f 62 6a 65 63 74 63  6c 61 73 73 04 05 67 72   ·objectc lass··gr
0080  6f 75 70 a3 29 04 09 6f  62 6a 65 63 74 53 69 64   oup·)··o bjectSid
0090  04 1c 01 05 00 00 00 00  00 05 15 00 00 00 b8 17   ········ ········
00a0  0b a2 b5 db a4 d8 c0 a2  54 19 01 02 00 00 30 0b   ········ T·····0·
00b0  04 09 6f 62 6a 65 63 74  53 69 64                 ··object Sid
```

LDAP服务器中Domain User objectSid的值与上图assertionValue的值一致。

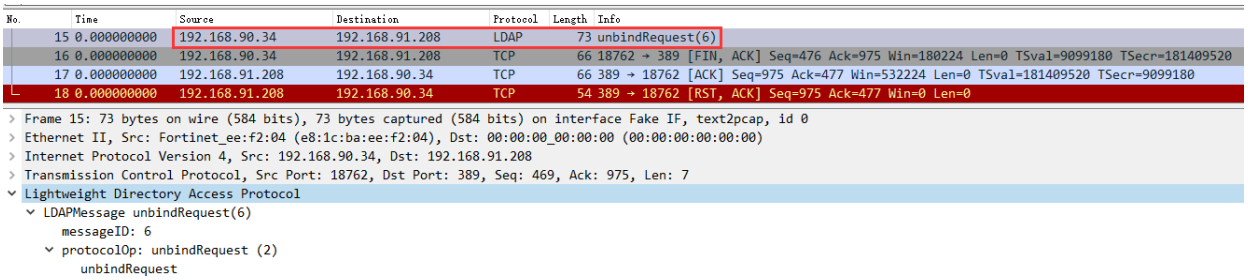
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- LDAP服务器对查询请求报文进行处理，返回用户所在主组的DN



- FortiGate解除绑定



常见的标准的LDAP响应码

1. 常见的标准的LDAP响应码

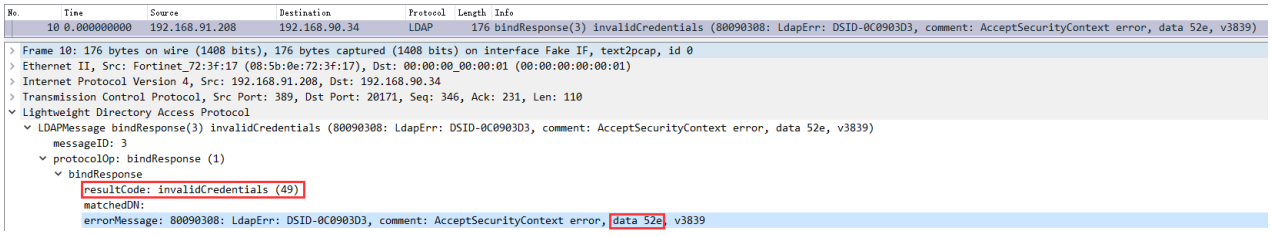
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

LDAP Result Code	Description
0	SUCCESS
2	PROTOCOL ERROR
7	AUTH METHOD NOT SUPPORTED
16	NO SUCH ATTRIBUTE
21	INVALID SYNTAX
32	NO SUCH OBJECT
34	INVALID DN SYNTAX
49	INVALID CREDENTIALS/ ACCOUNT DISABLED
50	LDAP INSUFFICIENT ACCESS

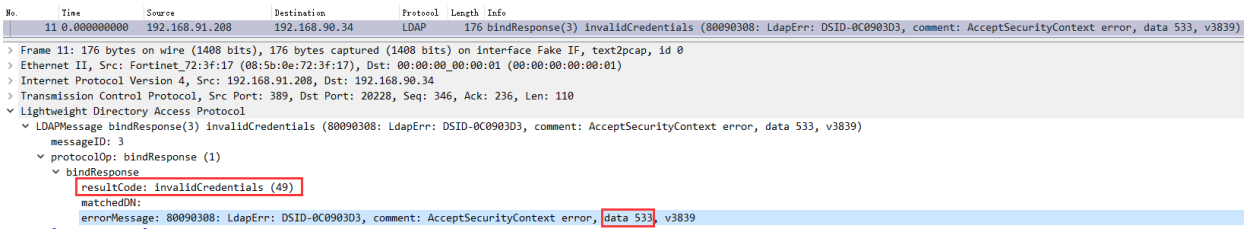
LDAP Error Message Data	Description
0x525	user not found
0x52e	invalid credentials
0x530	not permitted to logon at this time
0x531	not permitted to logon from this workstation
0x532	password expired
0x533	account disabled
0x701	account expired
0x773	user must reset password
0x775	account locked out

2. 错误码抓包举例

- 密码错误

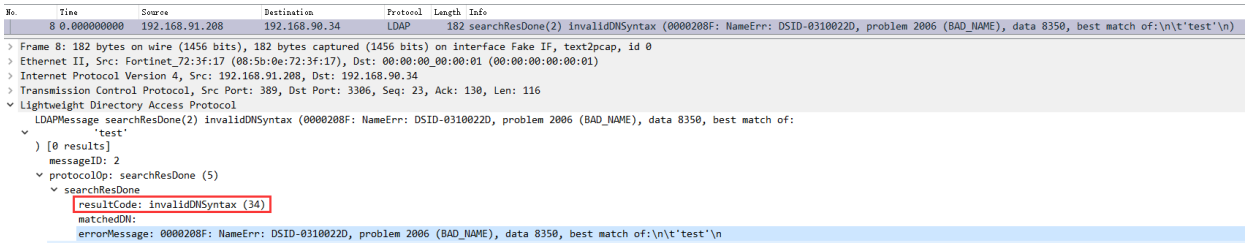


- 账号禁用



- DN语法错误

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

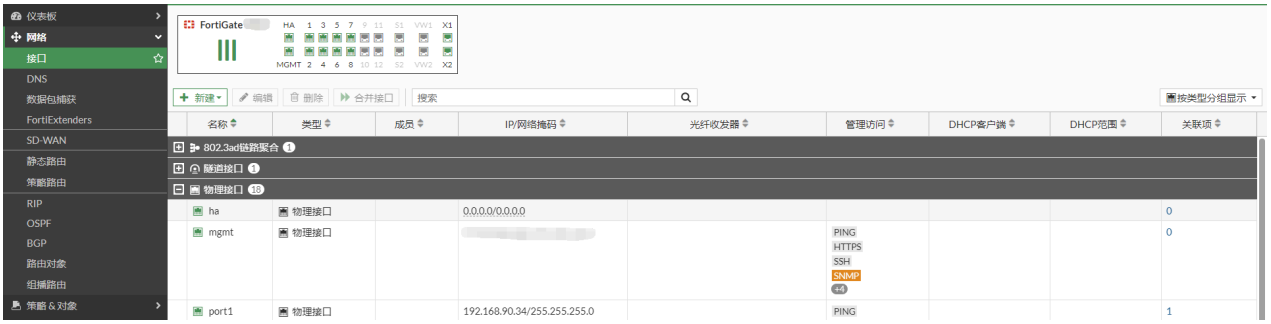


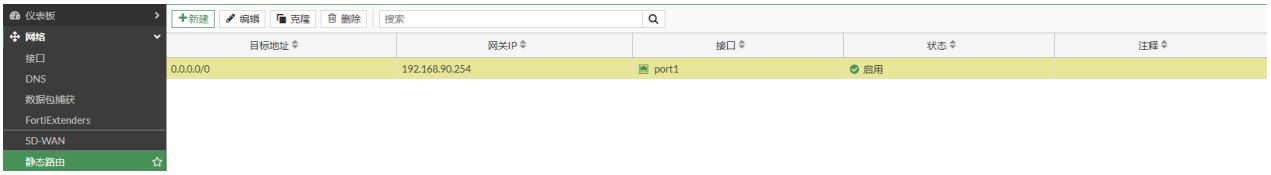
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

LDAP认证配置与排错

配置LDAP认证

1. **配置接口地址和路由**





ping测试FortiGate与LDAP服务器之间的连通性。测试环境使用Windows AD作为LDAP服务器，地址是192.168.91.208。

```
# execute ping 192.168.91.208
PING 192.168.91.208 (192.168.91.208): 56 data bytes
64 bytes from 192.168.91.208: icmp_seq=0 ttl=127 time=0.3 ms
64 bytes from 192.168.91.208: icmp_seq=1 ttl=127 time=0.2 ms
64 bytes from 192.168.91.208: icmp_seq=2 ttl=127 time=0.2 ms
64 bytes from 192.168.91.208: icmp_seq=3 ttl=127 time=0.2 ms
64 bytes from 192.168.91.208: icmp_seq=4 ttl=127 time=0.2 ms

--- 192.168.91.208 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.3 ms
```

2. **配置LDAP**

选择”用户与认证“-->LDAP，点击”新建“。



配置参数：

名称：输入一个名称，不冲突即可；

服务器IP/名称：LDAP服务器的IP地址；

服务器端口：LDAP通信端口，默认TCP 389；

Common Name标识符：FortiGate用于识别连接用户的LDAP中对象的属性字段。Windows AD域使用sAMAccountName，OpenLDAP使用uid。这里使用Windows AD域；

Distinguished Name：用于在LDAP服务器上查找用户帐户条目，反映了查找的CN标识符之上的LDAP的层次结构； 输入dc=fortibj,dc=com指定包含所有对象的域根； 输入ou=tac,dc=fortibj,dc=com查询指定组织单元下的用户；

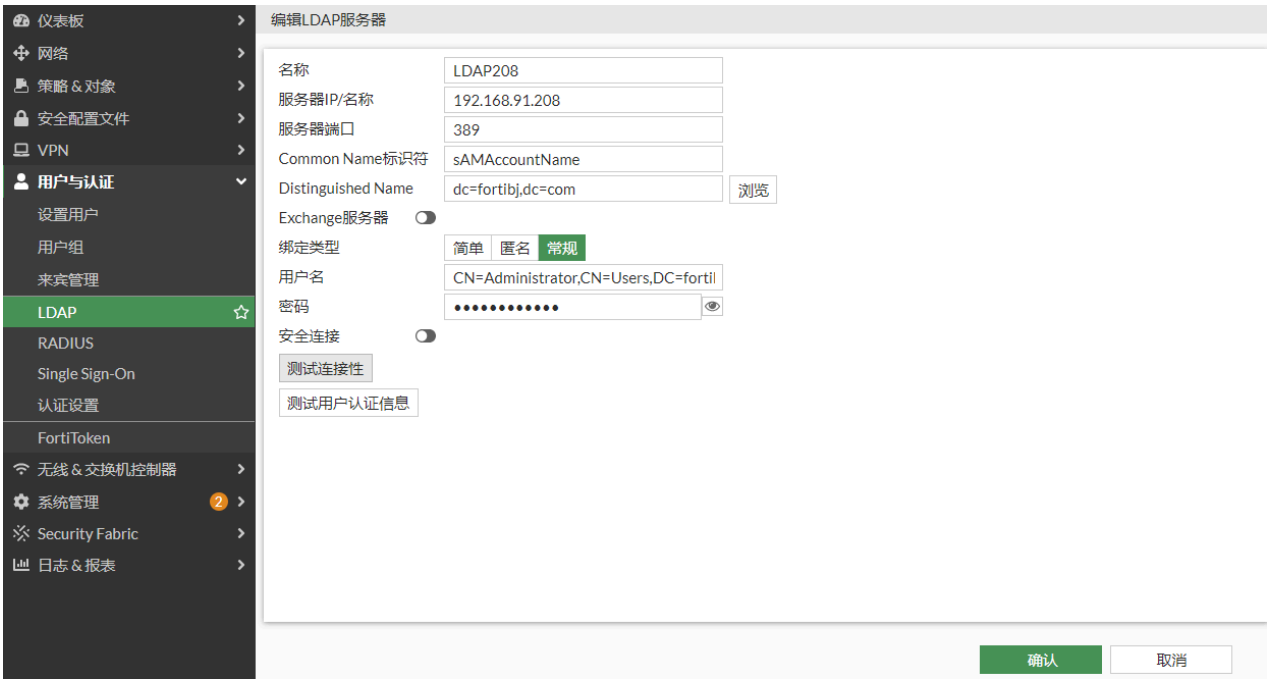
绑定类型：选择常规，使用提供的用户名和密码进行绑定，并从DN开始搜索并递归遍历子树；

用户名：用户名支持的格式：格式1：CN=Administrator,CN=Users,DC=fortibj,DC=com；格式2：Administrator@fortibj.com。

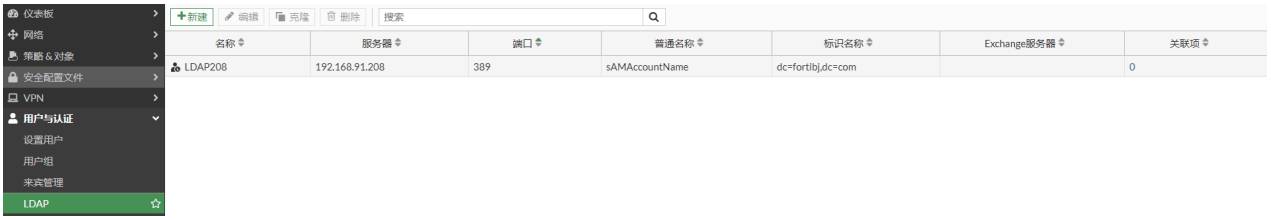
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
C:\Users\Administrator>dsquery user -name administrator
"CN=Administrator,CN=Users,DC=fortibj,DC=com"
```

密码：用户的密码；



点击”确定“，配置完成。



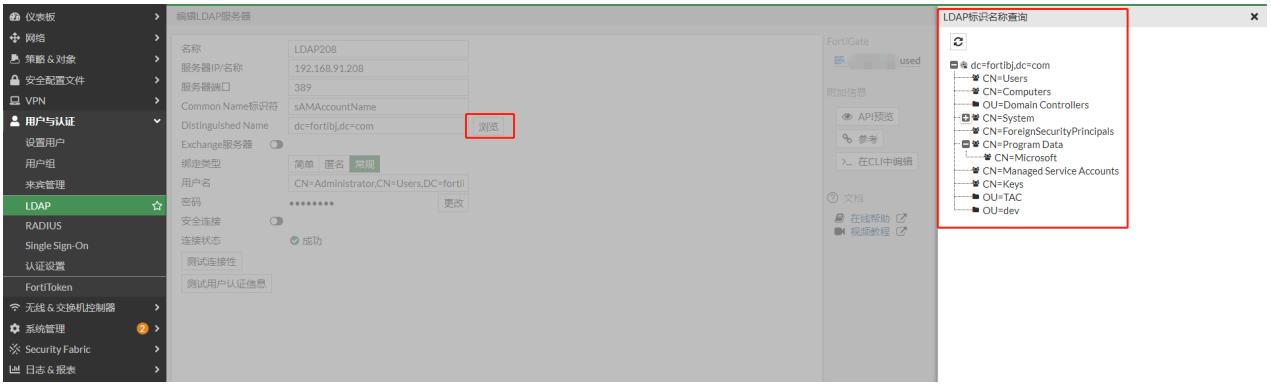
对应的命令行如下：

```
config user ldap
    edit "LDAP208"
        set server "192.168.91.208"
        set cnid "sAMAccountName"
        set dn "dc=fortibj,dc=com"
        set type regular
        set username "CN=Administrator,CN=Users,DC=fortibj,DC=com"
        set password xxxxxxxx
    next
end
```

3. 查看LDAP目录结构

当LDAP配置正确时，可以点击”浏览“，查看LDAP目录结构。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



LDAP服务器测试

1. **FortiGate与LDAP服务器之间连通性测试**

   GUI编辑LDAP服务器的配置界面，点击”测试连接性“。

   CLI语法测试连通性：

```
# diagnose test authserver ldap-direct
[IP] [port number]
```

   CLI语法测试用户和密码是否正确：

```
# diagnose test authserver ldap
<server_name> <username> <password>
```

   - 如果连接状态是”成功“，则FortiGate与LDAP服务器之间通信正常。

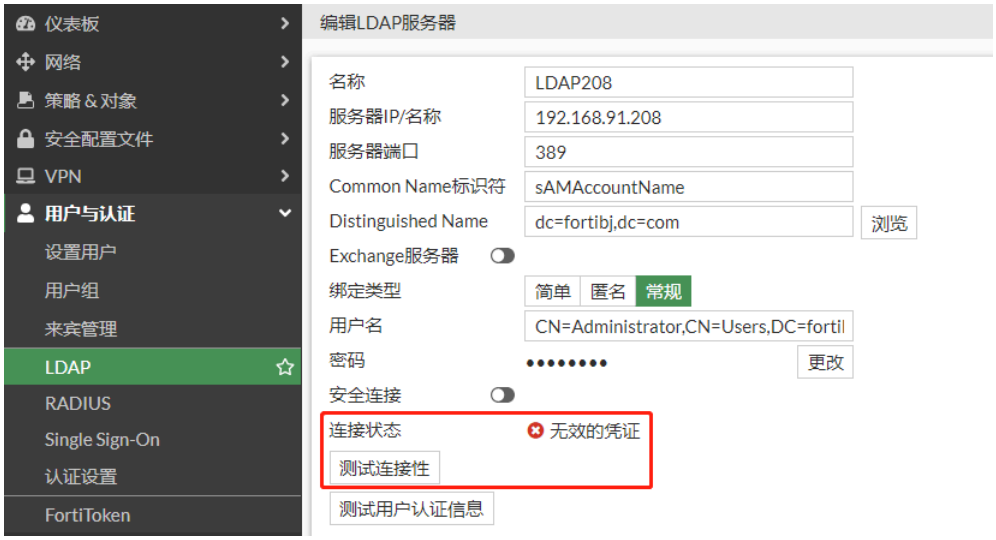


   对应CLI的测试结果：

```
# diagnose test authserver ldap-direct 192.168.91.208 389
LDAP server '192.168.91.208' status is OK
```

   - 如果连接状态是”无效的凭证“，则说明LDAP服务器的账号或者密码不正确。

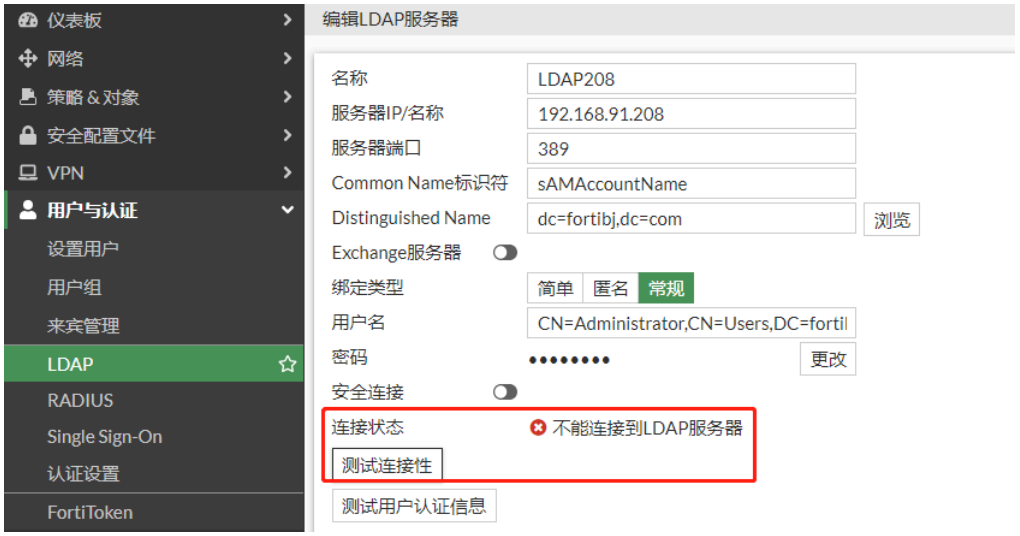
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的命令行：

```
# diagnose test authserver ldap LDAP208 administrator Test@123456
authenticate 'administrator' against 'LDAP208' succeeded!
Group membership(s) - CN=Group Policy Creator Owners,CN=Users,DC=fortibj,DC=com
                      CN=Domain Admins,CN=Users,DC=fortibj,DC=com
                      CN=Enterprise Admins,CN=Users,DC=fortibj,DC=com
                      CN=Schema Admins,CN=Users,DC=fortibj,DC=com
                      CN=Remote Desktop Users,CN=Builtin,DC=fortibj,DC=com
                      CN=Administrators,CN=Builtin,DC=fortibj,DC=com
                      CN=Domain Users,CN=Users,DC=fortibj,DC=com
```

- 如果连接状态是”不能连接到LDAP服务器“，则说明到LDAP服务器不可达。



对应CLI的测试结果：

```
# diagnose test authserver ldap-direct 192.168.91.208 389
LDAP server '192.168.91.208' status is Server unreachable
```

2. **测试LDAP服务器中的用户及密码**

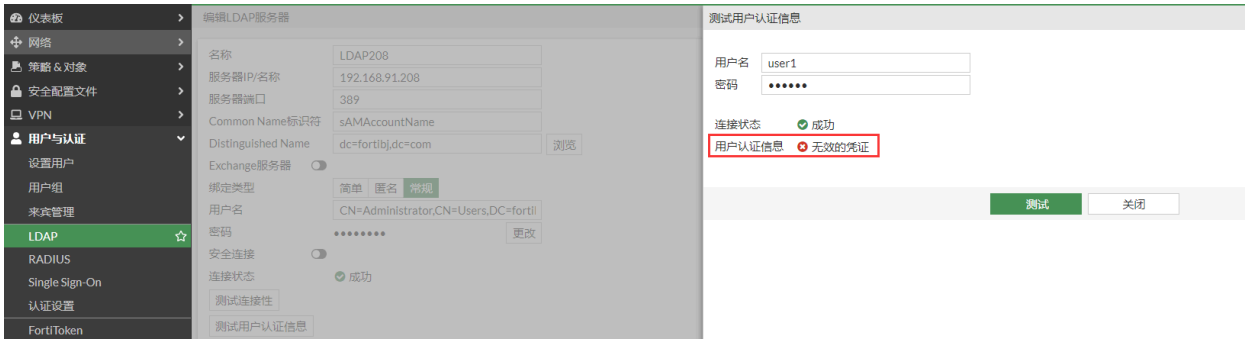
GUI编辑Radius服务器的配置界面，点击”测试用户认证信息“。

CLI的语法：

```
# diagnose test authserver ldap
<server_name> <username> <password>
```

- 用户名或者密码不正确

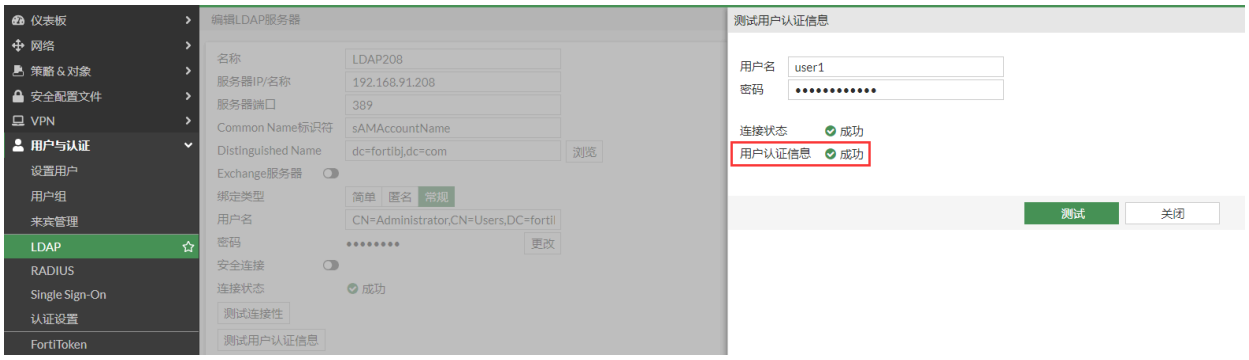
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的CLI测试结果如下：

```
# diagnose test authserver ldap LDAP208 user1 123456
authenticate 'user1' against 'LDAP208' failed!
```

- 用户名和密码正确



对应的CLI测试结果如下，CLI显示了用户user1所在的用户组信息。

```
# diagnose test authserver ldap LDAP208 user1 Pass@123456
authenticate 'user1' against 'LDAP208' succeeded!
Group membership(s) - CN=grp1,CN=Users,DC=fortibj,DC=com
                      CN=Domain Users,CN=Users,DC=fortibj,DC=com
```

其他LDAP配置参数

1. 修改LDAP端口

```
config user ldap
    edit LDAP208
        set port xx
    next
end
```

2. 指定原IP地址

```
config user ldap
    edit LDAP208
        set source-ip x.x.x.x
    next
end
```

创建ldap用户

1. 选择“用户与认证”-->“设置用户”，点击新建

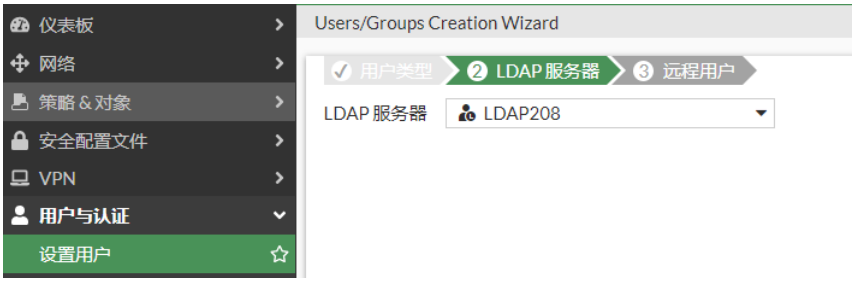
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



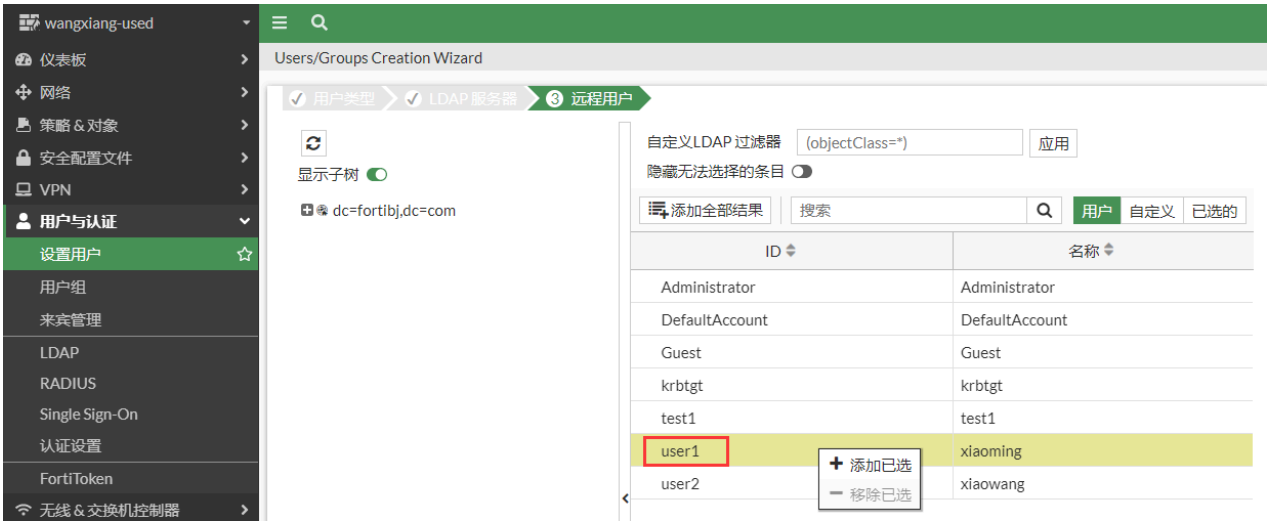
2. 选择LDAP用户，点击“下一步”



3. 选择配置好的LDAP服务器，点击“下一步”

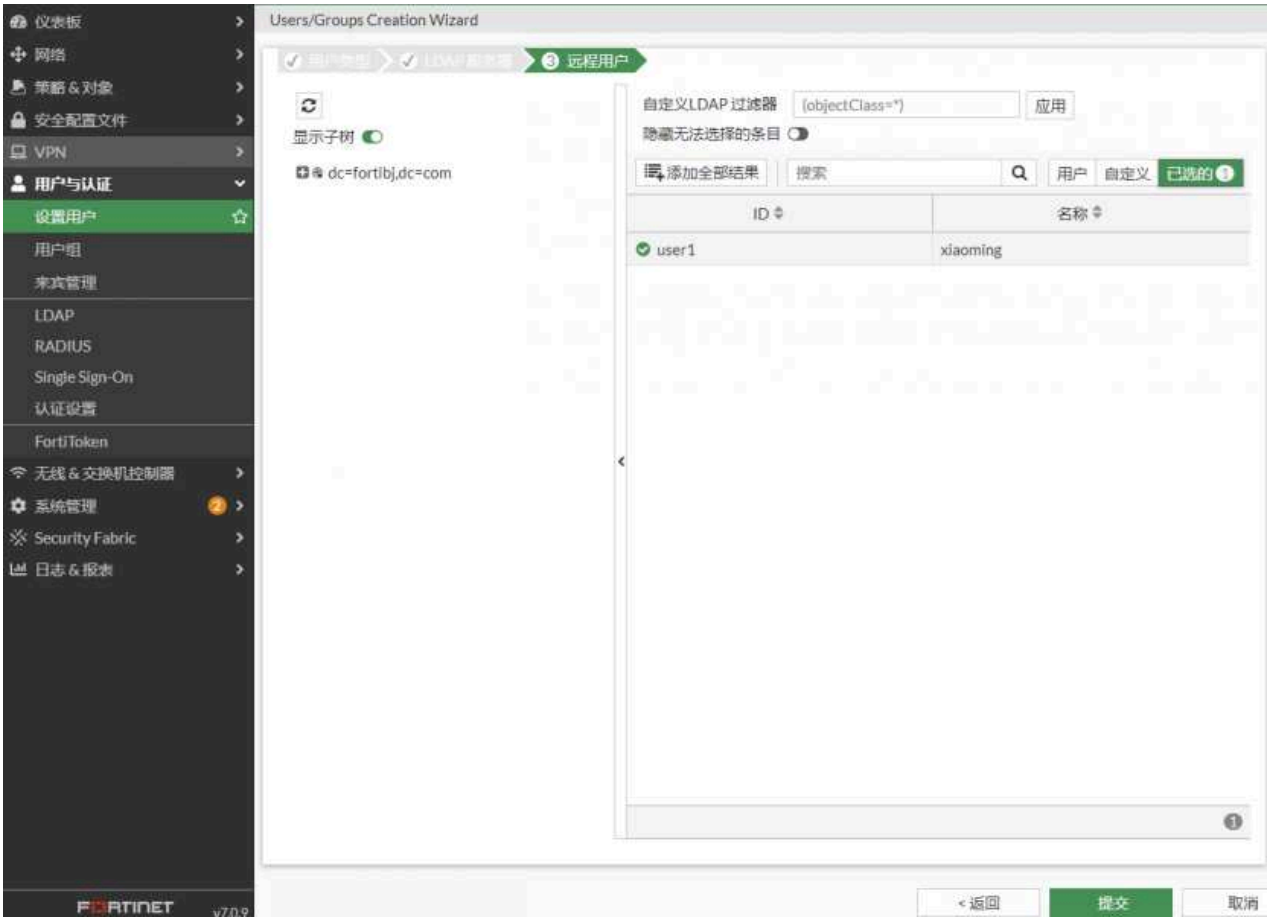


4. 这里添加user1，右击user1，点击“添加已选”

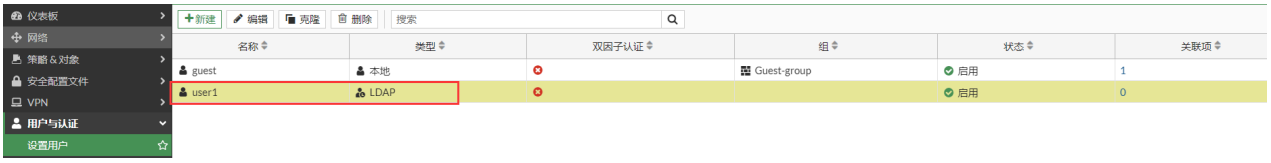


点击“已选的”，查看选中的用户，确认无误后，点击“提交”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

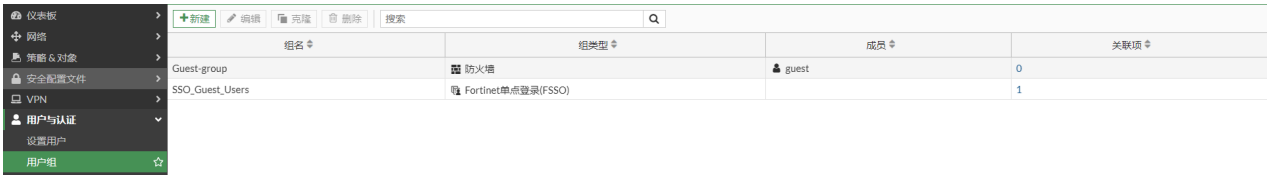


5. 完成LDAP用户创建



创建ldap用户组

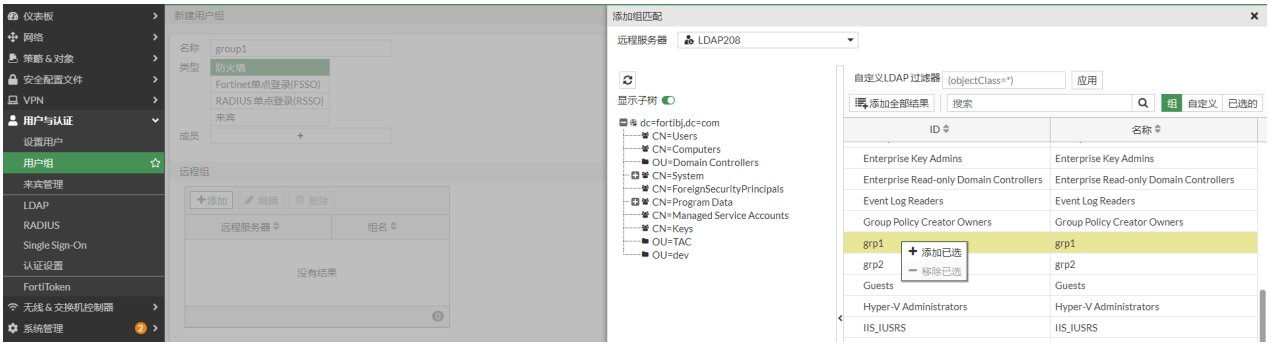
1. 选择“用户与认证”-->“用户组”，点击“新建”



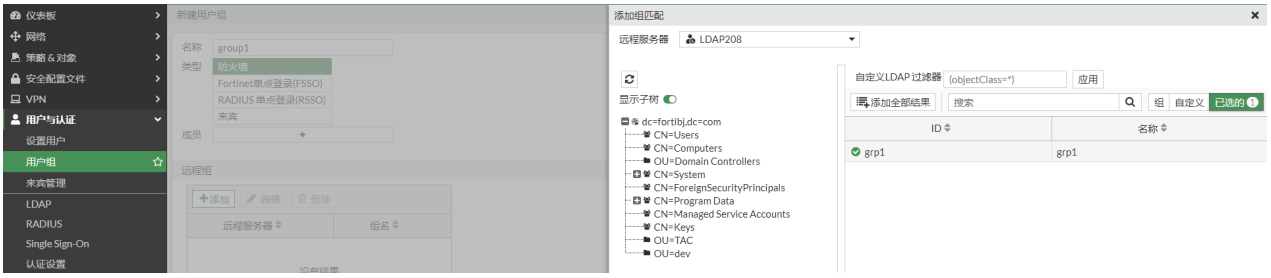
2. 配置LDAP

设置FortiGate用户组名称 group1，在远程组中，点击“添加”，选择配置好的远程服务器，会自动显示出目录树，找到需要添加的用户组，这里选择grp1，右击“添加已选”，**那么group1匹配远端LDAP用户组grp1中的用户**。可以添加多个用户组，如再增加grp2，那么group1匹配远端LDAP用户组grp1和grp2中的用户。

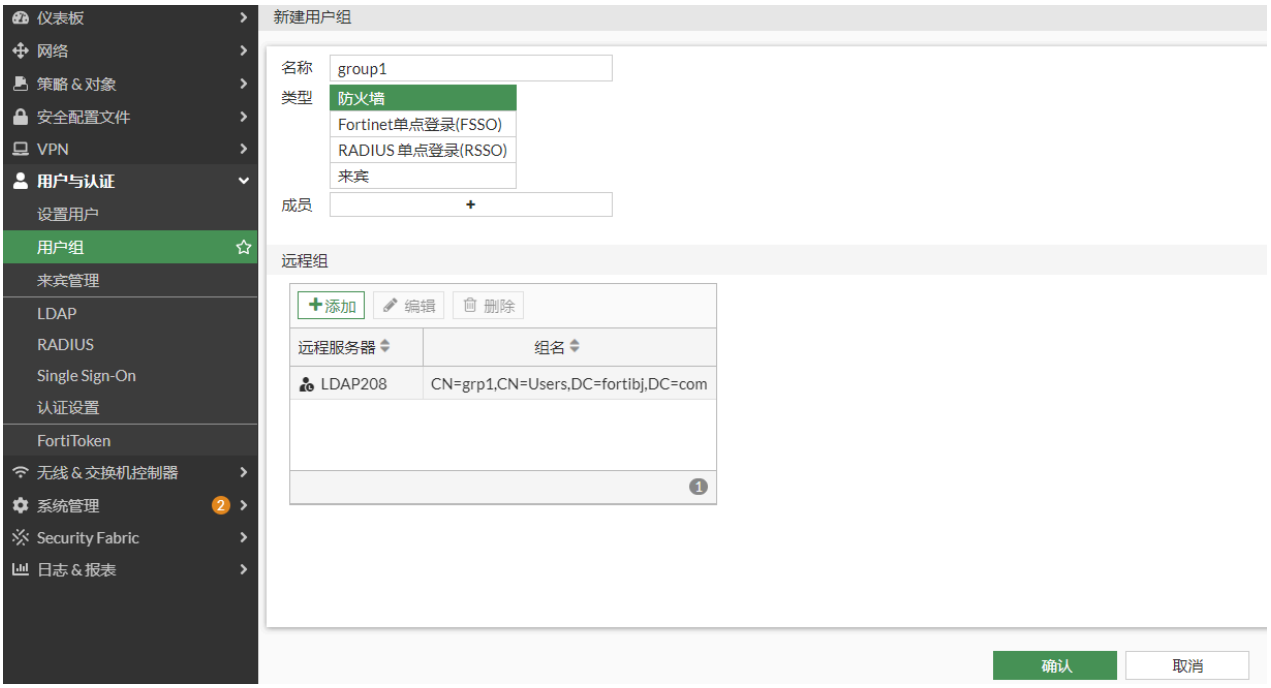
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



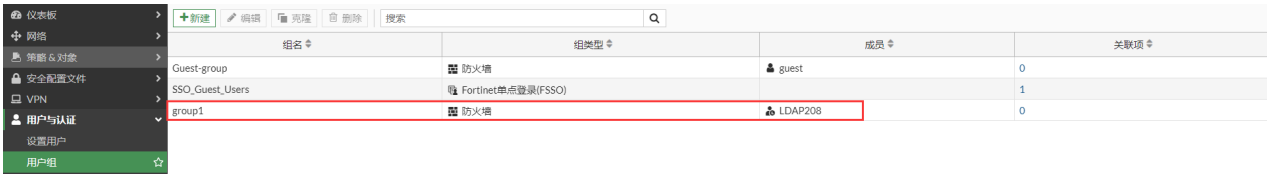
点击“已选的”，查看选中的用户组，确认无误后，点击“确认”。



3. 点击确认



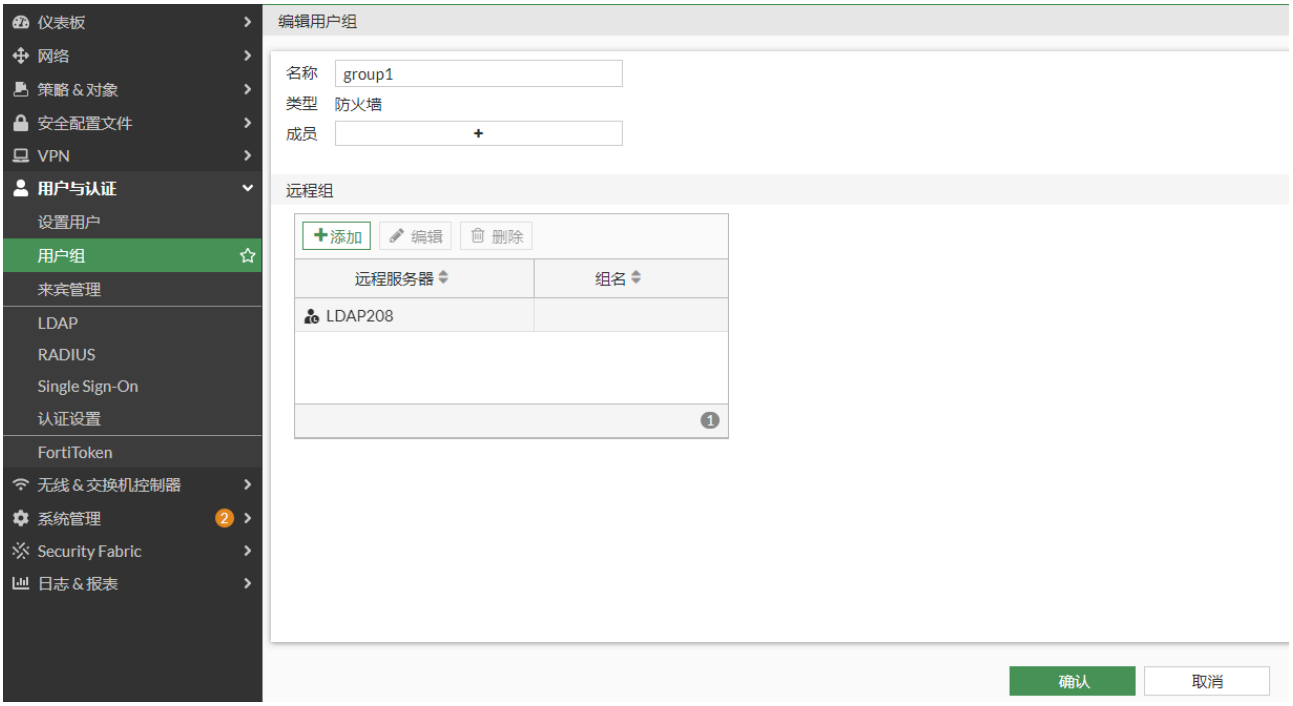
4. 配置完成



重要

如果在group1用不选择任何用户组，那么group1匹配LDAP服务器配置的DN目录下的所有用户。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



LDAP认证debug

认证成功

1. 准备查询的用户名user1和base DN。

```
# diagnose debug application fnbamd -1
# diagnose debug  enable

[1906] handle_req-Rcvd auth req 730526726 for user1 in LDAP208 opt=0000001b prot=0
[466] __compose_group_list_from_req-Group 'LDAP208', type 1
[616] fnbamd_pop3_start-user1
[989] __fnbamd_cfg_get_ldap_list_by_server-
[995] __fnbamd_cfg_get_ldap_list_by_server-Loaded LDAP server 'LDAP208'
[1150] fnbamd_cfg_get_ldap_list-Total ldap servers to try: 1

[1717] fnbamd_ldap_init-search filter is: sAMAccountName=user1
[1727] fnbamd_ldap_init-search base is: dc=fortibj,dc=com

[1149] __fnbamd_ldap_dns_cb-Resolved LDAP208:192.168.91.208 to 192.168.91.208, cur stack size:1
[924] __fnbamd_ldap_get_next_addr-
[1154] __fnbamd_ldap_dns_cb-Connection starts LDAP208:192.168.91.208, addr 192.168.91.208
[879] __fnbamd_ldap_start_conn-Still connecting 192.168.91.208.
[633] create_auth_session-Total 1 server(s) to try
[1107] __ldap_connect-tcps_connect(192.168.91.208) is established.
```

2. LDAP管理员账号绑定。

```
[985] __ldap_rxtx-state 3(Admin Binding)
[363] __ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=fortibj,DC=com'
[1083] fnbamd_ldap_send-sending 69 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 1

[985] __ldap_rxtx-state 4(Admin Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
response-ret=0    //绑定成功
[1023] fnbamd_ldap_parse_response-ret=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 查询user1的DN。

```
[1052] __ldap_rxtx-Change state to 'DN search'
[985] __ldap_rxtx-state 11(DN search)
[750] fnbamd_ldap_build_dn_search_req-base:'dc=fortibj,dc=com' filter:sAMAccountName=user1
[1083] fnbamd_ldap_send-sending 73 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 2

[985] __ldap_rxtx-state 12(DN search resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 51
[1306] fnbamd_ldap_recv-Response len: 53, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
```

4. 查询成功，获得user1的DN是 xiaoming,OU=TAC,DC=fortibj,DC=com。

```
response-ret=0    //查询成功，获得user1的DN是 xiaoming,OU=TAC,DC=fortibj,DC=com
[1023] fnbamd_ldap_parse_response-ret=0
[1225] __fnbamd_ldap_dn_entry-Get DN 'CN=xiaoming,OU=TAC,DC=fortibj,DC=com'

[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 78
[1306] fnbamd_ldap_recv-Response len: 80, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 78
[1306] fnbamd_ldap_recv-Response len: 80, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 62
[1306] fnbamd_ldap_recv-Response len: 64, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
[1023] fnbamd_ldap_parse_response-ret=0
```

5. 用户user1绑定请求成功。

```
[1052] __ldap_rxtx-Change state to 'User Binding'
[985] __ldap_rxtx-state 5(User Binding)
[596] fnbamd_ldap_build_userbind_req-Trying DN 'CN=xiaoming,OU=TAC,DC=fortibj,DC=com'
[363] __ldap_build_bind_req-Binding to 'CN=xiaoming,OU=TAC,DC=fortibj,DC=com'
[1083] fnbamd_ldap_send-sending 93 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 3

[985] __ldap_rxtx-state 6(User Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind

response-ret=0 //绑定成功
[1023] fnbamd_ldap_parse_response-ret=0
```

6. memberOf属性查询。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[1052] __ldap_rxtx-Change state to 'Attr query'
[985] __ldap_rxtx-state 7(Attr query)
[649] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[661] fnbamd_ldap_build_attr_search_req-base:'CN=xiaoming,OU=TAC,DC=fortibj,DC=com' filter:cn=*
[1083] fnbamd_ldap_send-sending 112 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 4

[985] __ldap_rxtx-state 8(Attr query resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 195
[1306] fnbamd_ldap_recv-Response len: 197, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:4, type:search-entry
```

7. 查询成功，获得user1的用户组CN=grp1,CN=Users,DC=fortibj,DC=com。

```
[1023] fnbamd_ldap_parse_response-ret=0
[556] __get_member_of_groups-Get the memberOf groups.
[522] __retrieve_group_values-Get the memberOf groups.
[532] __retrieve_group_values- attr='memberOf', found 1 values
[542] __retrieve_group_values-val[0]='CN=grp1,CN=Users,DC=fortibj,DC=com'

[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:4, type:search-result
[1023] fnbamd_ldap_parse_response-ret=0
[1305] __fnbamd_ldap_attr_next-Entering CHKPRIMARYGRP state
```

8. Primary group属性查询。

```
[1052] __ldap_rxtx-Change state to 'Primary group query'
[985] __ldap_rxtx-state 13(Primary group query)
[685] fnbamd_ldap_build_primary_grp_search_req-starting primary group check ...
[689] fnbamd_ldap_build_primary_grp_search_req-number of sub auths 5
[707] fnbamd_ldap_build_primary_grp_search_req-base:'dc=fortibj,dc=com' filter:(&(objectclass=group)
(objectSid=\01\05\00\00\00\00\00\05\15\00\00\00\b8\17\0b\a2\b5\db\a4\d8\c0\a2\54\19\01\02\00\00))
[1083] fnbamd_ldap_send-sending 121 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 5

[985] __ldap_rxtx-state 14(Primary group query resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 110
[1306] fnbamd_ldap_recv-Response len: 112, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-entry
```

9. 获得Primary group是CN=Domain Users,CN=Users,DC=fortibj,DC=com。

```
[1023] fnbamd_ldap_parse_response-ret=0
[472] __get_one_group-group: CN=Domain Users,CN=Users,DC=fortibj,DC=com

[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 78
[1306] fnbamd_ldap_recv-Response len: 80, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 78
[1306] fnbamd_ldap_recv-Response len: 80, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 62
[1306] fnbamd_ldap_recv-Response len: 64, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-reference
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-result
[1023] fnbamd_ldap_parse_response-ret=0
[1433] __fnbamd_ldap_primary_grp_next-Auth accepted
```

10. 查询完成。

```
[1052] __ldap_rxtx-Change state to 'Done'
[985] __ldap_rxtx-state 23(Done)
[1083] fnbamd_ldap_send-sending 7 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 6
[785] __ldap_done-svr 'LDAP208'
[755] __ldap_destroy-
[724] __ldap_stop-Conn with 192.168.91.208 destroyed.
```

11. 查询的结果。

```
[2678] fnbamd_ldap_result-Result for ldap svr 192.168.91.208(LDAP208) is SUCCESS
[401] ldap_copy_grp_list-copied CN=grp1,CN=Users,DC=fortibj,DC=com
[401] ldap_copy_grp_list-copied CN=Domain Users,CN=Users,DC=fortibj,DC=com

[2693] fnbamd_ldap_result-Skipping group matching
[216] fnbamd_comm_send_result-Sending result 0 (nid 0) for req 730526726, len=2227
[789] destroy_auth_session-delete session 730526726
[755] __ldap_destroy-
[1764] fnbamd_ldap_auth_ctx_free-Freeing 'LDAP208' ctx
```

认证失败

1. 准备查询的用户名user1和base DN。

```
# diagnose debug application fnbamd -1
# diagnose debug  enable

[1906] handle_req-Rcvd auth req 730526741 for user1 in LDAP208 opt=0000001b prot=0
[466] __compose_group_list_from_req-Group 'LDAP208', type 1
[616] fnbamd_pop3_start-user1
[989] __fnbamd_cfg_get_ldap_list_by_server-
[995] __fnbamd_cfg_get_ldap_list_by_server-Loaded LDAP server 'LDAP208'
[1150] fnbamd_cfg_get_ldap_list-Total ldap servers to try: 1

[1717] fnbamd_ldap_init-search filter is: sAMAccountName=user1
[1727] fnbamd_ldap_init-search base is: dc=fortibj,dc=com

[1149] __fnbamd_ldap_dns_cb-Resolved LDAP208:192.168.91.208 to 192.168.91.208, cur stack size:1
[924] __fnbamd_ldap_get_next_addr-
[1154] __fnbamd_ldap_dns_cb-Connection starts LDAP208:192.168.91.208, addr 192.168.91.208
[879] __fnbamd_ldap_start_conn-Still connecting 192.168.91.208.
[633] create_auth_session-Total 1 server(s) to try
[1107] __ldap_connect-tcps_connect(192.168.91.208) is established.
```

2. LDAP管理员账号绑定成功。

```
[985] __ldap_rxtx-state 3(Admin Binding)
[363] __ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=fortibj,DC=com'
[1083] fnbamd_ldap_send-sending 69 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 1

[985] __ldap_rxtx-state 4(Admin Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind

response-ret=0    //绑定成功
[1023] fnbamd_ldap_parse_response-ret=0
```

3. 查询user1的DN。

```
[1052] __ldap_rxtx-Change state to 'DN search'
[985] __ldap_rxtx-state 11(DN search)
[750] fnbamd_ldap_build_dn_search_req-base:'dc=fortibj,dc=com' filter:sAMAccountName=user1
[1083] fnbamd_ldap_send-sending 73 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 2

[985] __ldap_rxtx-state 12(DN search resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 51
[1306] fnbamd_ldap_recv-Response len: 53, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
```

4. 查询成功，获得user1的DN是 xiaoming,OU=TAC,DC=fortibj,DC=com。

```
response-ret=0    //查询成功，获得user1的DN是 xiaoming,OU=TAC,DC=fortibj,DC=com
[1023] fnbamd_ldap_parse_response-ret=0
[1225] __fnbamd_ldap_dn_entry-Get DN 'CN=xiaoming,OU=TAC,DC=fortibj,DC=com'

[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 78
[1306] fnbamd_ldap_recv-Response len: 80, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 78
[1306] fnbamd_ldap_recv-Response len: 80, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 62
[1306] fnbamd_ldap_recv-Response len: 64, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-reference
[1023] fnbamd_ldap_parse_response-ret=0
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
[1306] fnbamd_ldap_recv-Response len: 16, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
[1023] fnbamd_ldap_parse_response-ret=0
```

5. 用户user1绑定请求。

```
[1052] __ldap_rxtx-Change state to 'User Binding'
[985] __ldap_rxtx-state 5(User Binding)
[596] fnbamd_ldap_build_userbind_req-Trying DN 'CN=xiaoming,OU=TAC,DC=fortibj,DC=com'
[363] __ldap_build_bind_req-Binding to 'CN=xiaoming,OU=TAC,DC=fortibj,DC=com'
[1083] fnbamd_ldap_send-sending 88 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 3

[985] __ldap_rxtx-state 6(User Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 102
[1306] fnbamd_ldap_recv-Response len: 104, svr: 192.168.91.208
[987] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
```

6. 绑定失败，响应码49，响应消息52e，即密码不对。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[1009] fnbamd_ldap_parse_response-Error 49(80090308: LdapErr: DSID-0C0903D3, comment: AcceptSecurityContext error,
data 52e, v3839)
[1023] fnbamd_ldap_parse_response-ret=49

[262] fnbamd_ldap_more_dn_left-idx:0, total:1
[1052] __ldap_rxtx-Change state to 'Done'
[985] __ldap_rxtx-state 23(Done)
[1083] fnbamd_ldap_send-sending 7 bytes to 192.168.91.208
[1096] fnbamd_ldap_send-Request is sent. ID 4
[785] __ldap_done-svr 'LDAP208'
[755] __ldap_destroy-
[724] __ldap_stop-Conn with 192.168.91.208 destroyed.
[216] fnbamd_comm_send_result-Sending result 1 (nid 0) for req 730526741, len=2148
[789] destroy_auth_session-delete session 730526741
[755] __ldap_destroy-
[1764] fnbamd_ldap_auth_ctx_free-Freeing 'LDAP208' ctx
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

LDAP常见错误代码

LDAP错误代码位置

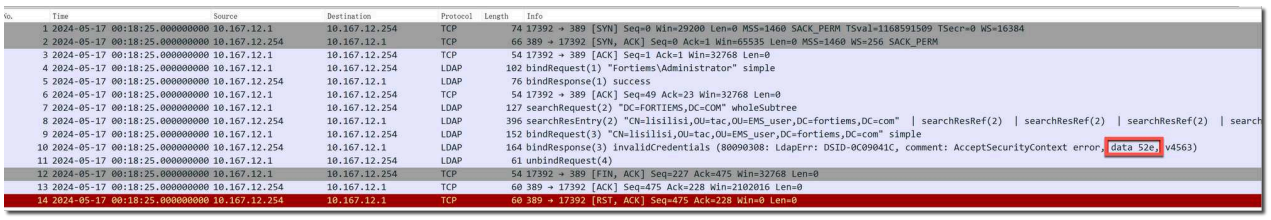
当通过FortiGate的LDAP认证失败时（例如显式代理认证、SSLVPN认证、ZTNA认证），可以通过在FortiGate上执行`diagnose debug application fnbamd -1`或通过抓取LDAP认证报文来排查错误原因。

`fnbamd`的Debug信息或LDAP认证结果报文中会包含的LDAP服务器返回的错误代码，从错误代码代表的含义，可以快速定位到LDAP认证失败的原因。

- 如下所示的`fnbamd`的Debug信息，`[778] fnbamd_ldap_parse_response-Error 49(80090308: LdapErr: DSID-0C090446, comment: AcceptSecurityContext error, data 52e, v4563)`中的`data 52e`即为错误代码”。

```bash
FortiGate # diagnose debug application fnbamd -1
FortiGate # diagnose debug enable

[584] fnbamd_ldap_build_dn_search_req-base:'DC=fortinet,dc=com' filter:sAMAccountName=xxxxx
[1100] __fnbamd_ldap_dn_entry-Get DN 'CN=XXX,CN=XXX,DC=XXX,DC=com'
[90] ldap_dn_list_add-added CN=XXX,CN=XXX,DC=XXX,DC=com
[52] ldap_dn_list_del_all-Del CN=XXX,CN=XXX,DC=XXX,DC=com
[2821] fnbamd_ldap_result-Result for ldap svr XXX.XXX.XXX.XXX is SUCCESS
[1552] fnbamd_ldap_init-search filter is: sAMAccountName=XXX
[1561] fnbamd_ldap_init-search base is: DC=XXX,dc=com
[584] fnbamd_ldap_build_dn_search_req-base:'DC=XXX,dc=com' filter:sAMAccountName=XXX
[1100] __fnbamd_ldap_dn_entry-Get DN 'CN=XXX,OU=XXX,OU=XXX,OU=XXX,DC=XXX,DC=com'
[90] ldap_dn_list_add-added CN=XXX,OU=XXX,OU=XXX,OU=XXX,OU=XXX,DC=XXX,DC=com
[429] fnbamd_ldap_build_userbind_req-Trying DN ' CN=XXX,OU=XXX,OU=XXX,OU=XXX,OU=XXX,DC=XXX,DC=com '
[196] __ldap_build_bind_req-Binding to ' CN=XXX,OU=XXX,OU=XXX,OU=XXX,OU=XXX,DC=XXX,DC=com'
[852] fnbamd_ldap_send-sending 123 bytes to XXX.XXX.XXX.XXX
[864] fnbamd_ldap_send-Request is sent. ID 3
[815] __ldap_rxtx-state 6(User Bind resp)
[895] __fnbamd_ldap_read-Read 8
[895] __fnbamd_ldap_read-Read 102
[1075] fnbamd_ldap_recv-Response len: 104, svr: XXX.XXX.XXX.XXX
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[778] fnbamd_ldap_parse_response-Error 49(80090308: LdapErr: DSID-0C090446, comment: AcceptSecurityContext error,
data 52e, v4563)
//这里的“data 52e”，即为错误代码//
[791] fnbamd_ldap_parse_response-ret=49
[882] __ldap_rxtx-Change state to 'User Binding'
[815] __ldap_rxtx-state 5(User Binding)
[425] fnbamd_ldap_build_userbind_req-No more DN left
[737] __ldap_error-
[726] __ldap_stop-svr 'ad_server'
[52] ldap_dn_list_del_all-Del CN=XXX,OU=XXX,OU=XXX,OU=XXX,OU=XXX,DC=XXX,DC=com
[182] fnbamd_comm_send_result-Sending result 1 (error 0, nid 0) for req 1824141631
[653] destroy_auth_session-delete session 1824141631
```

- 使用`diagnose sniffer packet any 'tcp and port 389' 6 0 l`（或GUI抓包）抓取LDAP报文，也可以看到类似的错误代码信息。



LDAP错误代码含义

- `525 - User not found`：当提供的用户名无效时，将返回此错误，表明LDAP目录中不存在指定的用户。
- `52e - Invalid credentials`：表示提供了有效的用户名，但提供的密码或凭据不正确。此错误通常会阻止显示其他错误，因为没有有效凭据身份验证无法继续。
- `530 - Not permitted to logon at this time`：当在限制登录期间提供有效用户名和密码时，将返回此错误。可能存在基于时间的访问限制。
- `531 - Not permitted to logon from this workstation`：当提供有效的用户名和密码时，将返回该错误，但用户被限制使用尝试登录的工作站。基于工作站的访问限制生效。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- `532 - Password expired`：当提供了有效的用户名并且提供的密码正确但已过期时，会出现此错误。用户需要更改他们的密码。
- `533 - Account disabled`：当提供了有效的用户名和密码，但用户的帐户已被禁用时返回。由于帐户的禁用状态，身份验证被阻止。
- `701 - Account expired`：当提供了有效的用户名和密码，但用户的帐户已过期，无法成功进行身份验证时，将返回此错误。
- `773 - User must reset password`：如果提供了有效的用户名和密码，此错误表示用户需要在首次登录前或管理员重置密码后立即重置密码。
- `775 - Account locked out`：当提供了有效的用户名，但用户的帐户由于登录尝试失败次数过多而被锁定时，将返回此错误。请务必注意，即使提供的密码有效，也会返回此错误。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

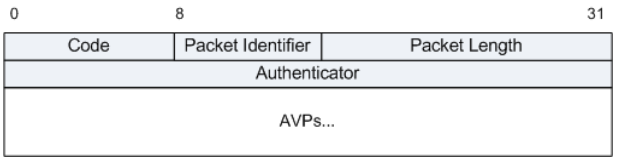
Radius认证原理

Radius简介

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证）是一种广泛支持的客户机-服务器协议，提供集中的身份验证、授权和计费功能。RADIUS服务器使用UDP报文与网络中的RADIUS客户端通信，在允许用户访问网络之前对用户进行认证，授权适当的用户访问资源，并对所使用的资源进行说明。

Radius报文格式及交互过程

1. **Radius报文格式**



Code：表示Radius报文的类型：

- Code = 1: Access-Request，认证请求报文；
- Code = 2: Access-Accept，认证成功报文；
- Code = 3: Access-Reject，认证拒绝报文；
- Code = 4: Accounting-Request，计费请求报文；
- Code = 5: Accounting-Response，计费响应报文；
- Code = 11: Access-Challenge，认证挑战报文；
- Code = 255: Reserved，保留；

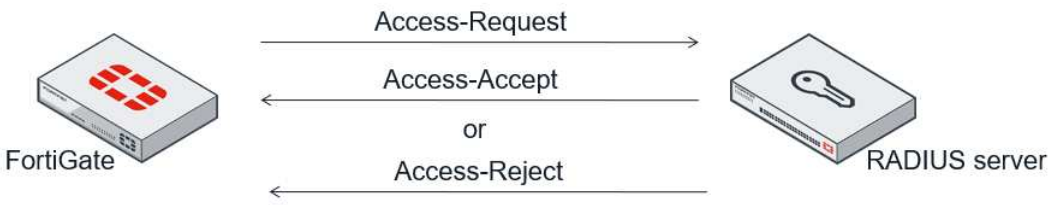
Packet Identifier：用于匹配请求和回应报文。

Packet Length：Radius报文长度；

Authenticator：用于认证来自服务端的响应，也用于用户密码的加密处理；

AVPs：属性字段，用于RADIUS服务器和RADIUS客户端之间的信息交换，Fortinet RADIUS属性的供应商ID是12356。

2. **Radius报文交互过程**



- FortiGate向RADIUS服务器发送包含用户名和密码信息的认证请求报文。
- RADIUS服务器对用户身份的合法性进行检验：

  如果用户身份合法，RADIUS服务器向FortiGate返回认证接受报文。

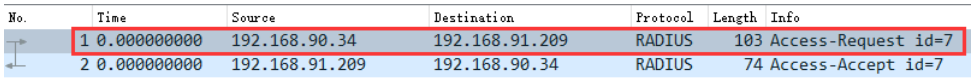
  如果用户身份不合法，RADIUS服务器向RADIUS客户端返回认证拒绝报文。

PAP和CHAP认证

1. **PAP认证**

在认证请求报文Access-Request报文中，PAP将用户和加密后的密码传递给Radius服务器。

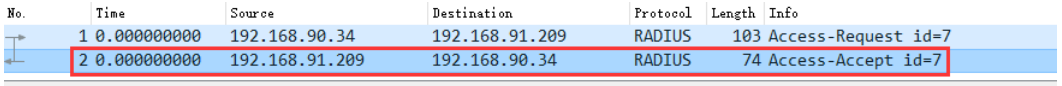
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.90.34	192.168.91.209	RADIUS	103	Access-Request id=7
2	0.000000000	192.168.91.209	192.168.90.34	RADIUS	74	Access-Accept id=7

```
> Frame 1: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface Fake IF, text2pc
> Ethernet II, Src: Fortinet_ee:f2:04 (e8:1c:ba:ee:f2:04), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00
> Internet Protocol Version 4, Src: 192.168.90.34, Dst: 192.168.91.209
> User Datagram Protocol, Src Port: 1716, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x7 (7)
    Length: 61
    Authenticator: 6aae17d4b66d029697aab86fd4ab6ed2
    [The response to this request is in frame 2]
  v Attribute Value Pairs
    v AVP: t=NAS-Identifier(32) l=16 val=wangxiang-used
        Type: 32
        Length: 16
        NAS-Identifier: wangxiang-used
    v AVP: t=User-Name(1) l=7 val=user1
        Type: 1
        Length: 7
        User-Name: user1
    v AVP: t=User-Password(2) l=18 val=Encrypted
        Type: 2
        Length: 18
        User-Password (encrypted): 50527af24b2f150fd2a0157eb59c6c5e
```

Radius服务器将解密后的密码，与用户的密码进行比较，如果一致， 则认为密码正确。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.90.34	192.168.91.209	RADIUS	103	Access-Request id=7
2	0.000000000	192.168.91.209	192.168.90.34	RADIUS	74	Access-Accept id=7

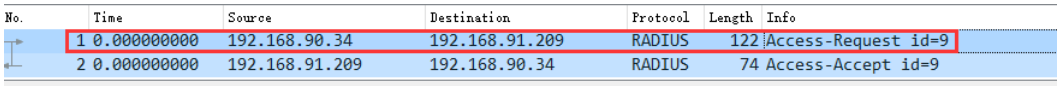
```
> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Fortinet_72:3f:17 (08:5b:0e:72:3f:17), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 192.168.91.209, Dst: 192.168.90.34
> User Datagram Protocol, Src Port: 1812, Dst Port: 1716
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7 (7)
    Length: 32
    Authenticator: f59759669f7cb64a4bda4e2eef863af4
    [This is a response to a request in frame 1]
    [Time from request: 0.000000000 seconds]
  v Attribute Value Pairs
    v AVP: t=Vendor-Specific(26) l=12 vnd=Fortinet, Inc.(12356)
        Type: 26
        Length: 12
        Vendor ID: Fortinet, Inc. (12356)
      v VSA: t=Fortinet-Group-Name(1) l=6 val=grp1
          Type: 1
          Length: 6
          Fortinet-Group-Name: grp1
```

2. **CHAP认证**

> **重要**
>
> CHAP认证传递的是一个HASH值，不是密码，因此这要求用户的密码保存在Radius服务器本地。如果Radius服务器用户的密码不在本地，如FortiGate----Radius服务器----LDAP服务器，像这样的部署方式，用户的密码保存在LDAP服务器中，Radius服务器无法获取LDAP服务器中用户的密码，因此认证将失败。

在认证请求报文Access-Request报文中，CHAP认证并不会直接在认证过程传递用户密码， 而是传递 chapID + 密码 + challenge的MD5值。

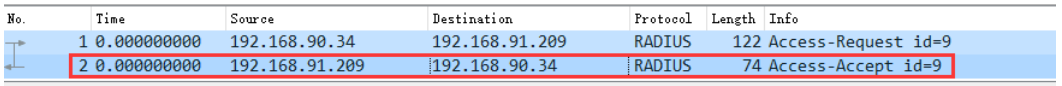
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.90.34	192.168.91.209	RADIUS	122	Access-Request id=9
2	0.000000000	192.168.91.209	192.168.90.34	RADIUS	74	Access-Accept id=9

```
> Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Fortinet_ee:f2:04 (e8:1c:ba:ee:f2:04), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.90.34, Dst: 192.168.91.209
> User Datagram Protocol, Src Port: 12269, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x9 (9)
    Length: 80
    Authenticator: 541baba7049951ac53476ecb1f2f9918
    [The response to this request is in frame 2]
  v Attribute Value Pairs
    v AVP: t=NAS-Identifier(32) l=16 val=wangxiang-used
        Type: 32
        Length: 16
        NAS-Identifier: wangxiang-used
    v AVP: t=User-Name(1) l=7 val=user1
        Type: 1
        Length: 7
        User-Name: user1
    v AVP: t=CHAP-Password(3) l=19 val=c537f2e59792a37b600318a39c7896ce2f
        Type: 3
        Length: 19
      v CHAP-Password: c537f2e59792a37b600318a39c7896ce2f
          CHAP Ident: 0xc5
          CHAP String: 37f2e59792a37b600318a39c7896ce2f
    v AVP: t=CHAP-Challenge(60) l=18 val=000933e8af645c56ab1437032c0fd2f6
        Type: 60
        Length: 18
        CHAP-Challenge: 000933e8af645c56ab1437032c0fd2f6
```

Radius服务器通过用户名找到对应的密码，计算chapID + 密码 + challenge的MD5值， 并判断是否与 chap-password一致（从第2个字节开始比较），如果一致， 则认为密码正确。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.90.34	192.168.91.209	RADIUS	122	Access-Request id=9
2	0.000000000	192.168.91.209	192.168.90.34	RADIUS	74	Access-Accept id=9

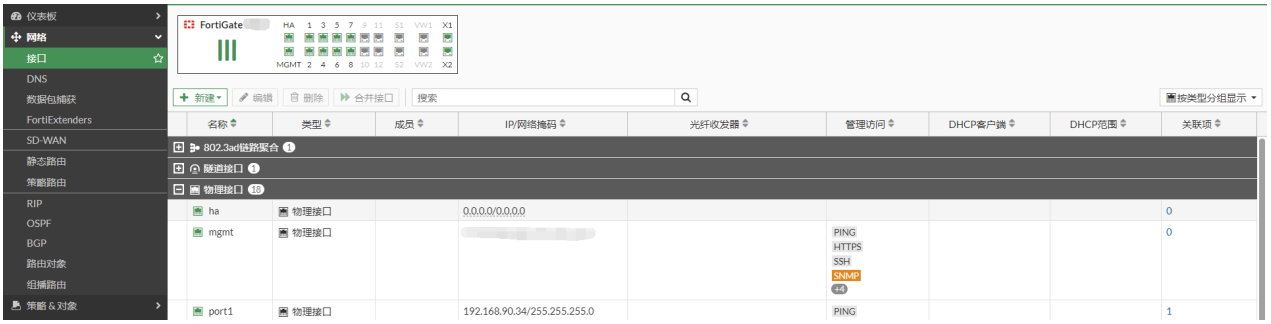
```
> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface Fake IF, text2pcap, id 0
> Ethernet II, Src: Fortinet_72:3f:17 (08:5b:0e:72:3f:17), Dst: 00:00:00_00:00:01 (00:00:00:00:00:01)
> Internet Protocol Version 4, Src: 192.168.91.209, Dst: 192.168.90.34
> User Datagram Protocol, Src Port: 1812, Dst Port: 12269
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x9 (9)
    Length: 32
    Authenticator: 3b5c7adf49f224b267faf26472664e15
    [This is a response to a request in frame 1]
    [Time from request: 0.000000000 seconds]
  v Attribute Value Pairs
    v AVP: t=Vendor-Specific(26) l=12 vnd=Fortinet, Inc.(12356)
        Type: 26
        Length: 12
        Vendor ID: Fortinet, Inc. (12356)
      v VSA: t=Fortinet-Group-Name(1) l=6 val=grp1
          Type: 1
          Length: 6
          Fortinet-Group-Name: grp1
```

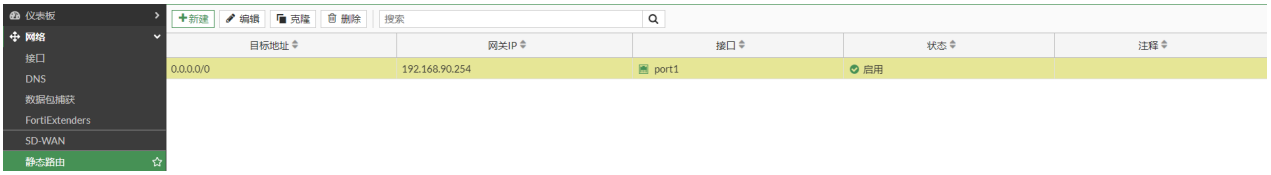

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Radius认证配置与排错

配置Radius认证

1. **配置接口地址及路由**





ping测试FortiGate与Radius Server之间的连通性。测试环境使用FortiAuthenticator作为Radius服务器，地址是192.168.91.209。

```
# execute ping 192.168.91.209
PING 192.168.91.209 (192.168.91.209): 56 data bytes
64 bytes from 192.168.91.209: icmp_seq=0 ttl=63 time=0.3 ms
64 bytes from 192.168.91.209: icmp_seq=1 ttl=63 time=0.2 ms
64 bytes from 192.168.91.209: icmp_seq=2 ttl=63 time=0.1 ms
64 bytes from 192.168.91.209: icmp_seq=3 ttl=63 time=0.1 ms
64 bytes from 192.168.91.209: icmp_seq=4 ttl=63 time=0.2 ms

--- 192.168.91.209 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
```

2. **配置Radius服务器**

选择”用户与认证“-->”RADIUS“，点击”新建“。



配置参数：

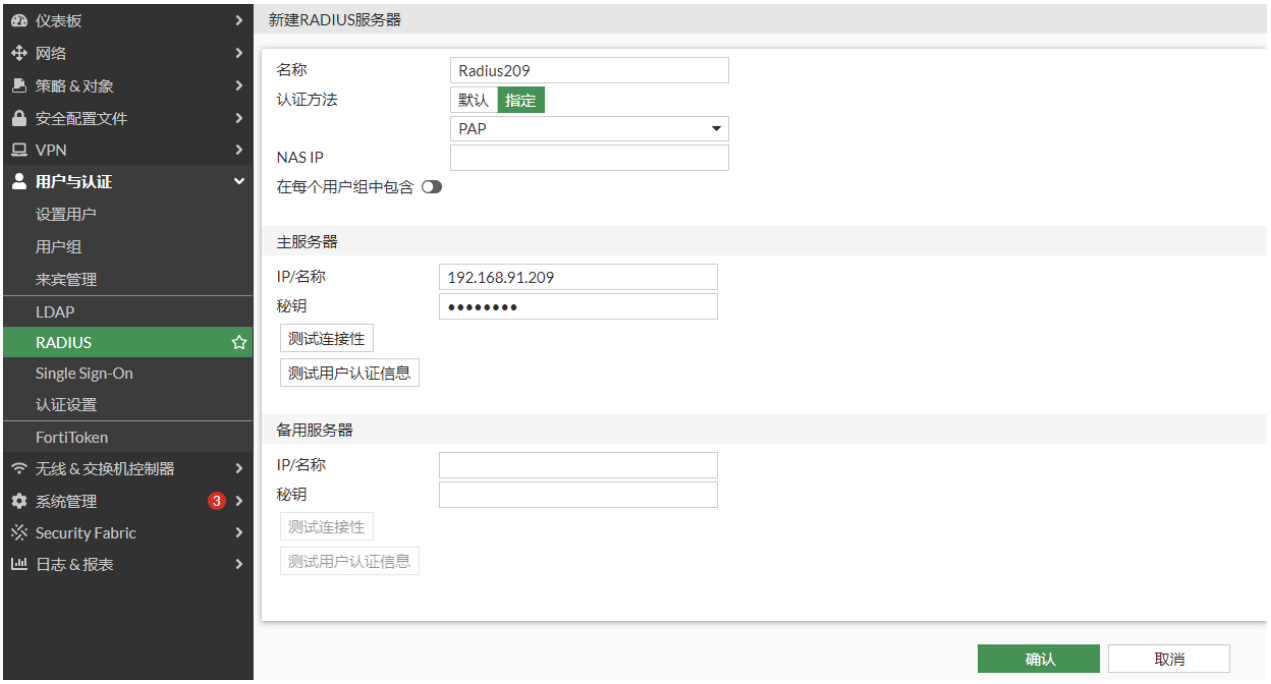
名称：输入一个名称，不冲突即可；

认证方法：FortiGate支持CHAP，MS-CHAP，MS-CHAP，PAP认证方法。如果认证方法是默认，则FortiGate会使用PAP、MSCHAP_v2和CHAP三种方式向Radius服务器发送请求，Radius服务器的日志中往往会报一些错误，因此**请指定一种认证方法**，这里使用PAP；

IP/名称：在主服务器输入Radius服务器的IP地址；

密钥：FortiGate和Radius服务器之间的共享密钥，这里设置为fortinet。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



点击”确认“，配置完成。



对应的命令行如下：

```
config user radius
    edit "Radius209"
        set server "192.168.91.209"
        set secret ENC
fJ6Xhg0wVEZyp8qAJfiuNSJLqyNVrWsRwQ1zELqWc7GnyBso4IrSelJJR4DBKmXQ/ex9cFWq3nJfoWEbWjRy1nrwUMl5HJGPiHO+c8MXXy6IAUE38e
c4Y/x5VnRPZpEgPPiVIuCXZfbpnjcR1t5RdO8lgTTRkhiNqBFvrZtyxsucpqRYSH7eyTN0ih5nJigvUn8oAg==
        set auth-type pap
    next
end
```

Radius服务器测试

1. **FortiGate与Radius服务器之间连通性测试**

   GUI编辑Radius服务器的配置界面，点击”测试连接性“。

   CLI的语法：

```
#diagnose test authserver radius-direct
<server_name or IP> <port number (0 default port)> <secret> <pap | chap | mschap | mschap2> <user> <password>
```

   - 如果连接状态是”成功“，则FortiGate与Radius服务器之间通信正常。

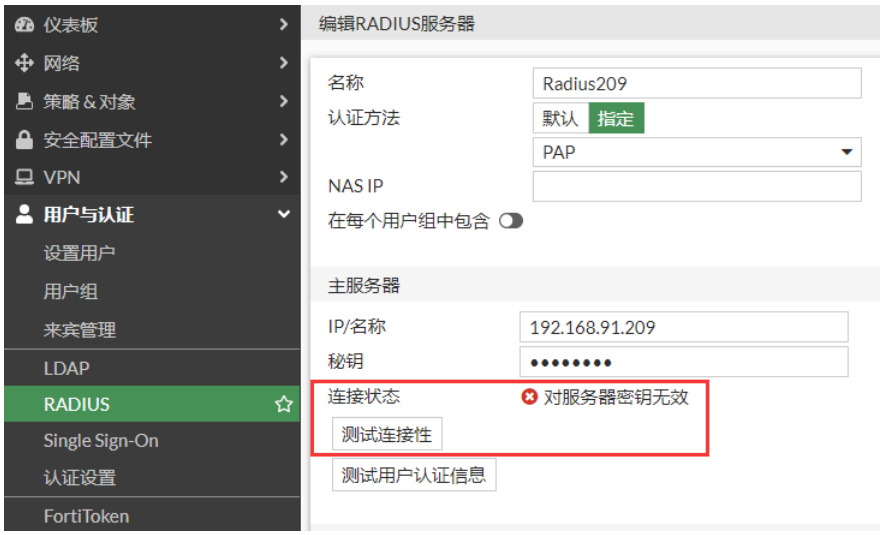
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的CLI测试结果如下：

```
# diagnose test authserver radius-direct 192.168.91.209 1812 fortinet pap user1 12345678
RADIUS server '192.168.91.209' status is OK
Access-Accept
AVP: l=12 t=Vendor-Specific(26) v=Fortinet(12356)
  VSA: l=6 t=Fortinet-Group-Name(1)
  Value: 'grp1'
```

- 如果连接状态是“对服务器密钥无效”，则FortiGate与Radius服务器之间的密钥不一致。



对应的CLI测试结果如下：

```
# diagnose test authserver radius-direct 192.168.91.209 1812 fortinet pap user1 12345678
RADIUS server '192.168.91.209' status is Secret invalid
```

- 如果连接状态是“不能连接 RADIUS 服务器”，则Radius服务器的地址或者端口不正确，或者Radius服务器没有授权FortiGate作为客户端。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的CLI测试结果如下：

```
# diagnose test authserver radius-direct 192.168.91.209 1812 fortinet pap user1 12345678
RADIUS server '192.168.91.209' status is Server unreachable
```

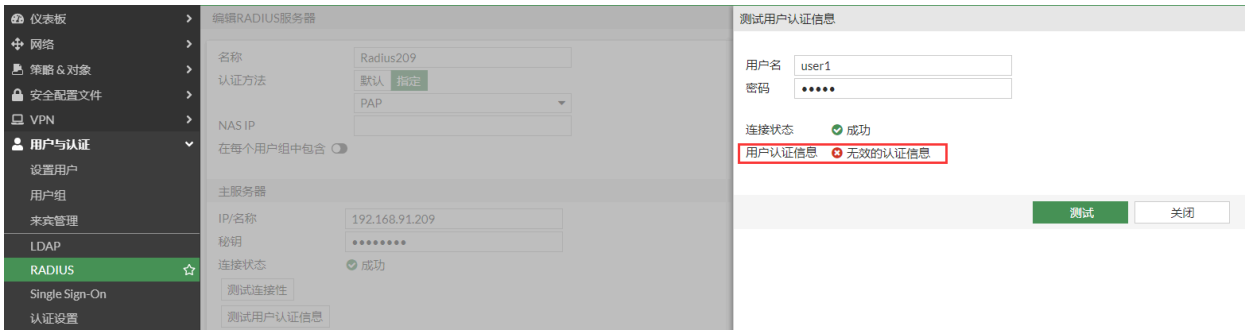
2. 测试Radius服务器中的用户及密码

GUI编辑Radius服务器的配置界面，点击”测试用户认证信息“。

CLI的语法：

```
# diagnose test authserver radius
<server_name> <chap | pap | mschap | mschap2> <username> <password>
```

- 用户名或者密码不正确



对应的CLI测试结果如下：

```
# diagnose test authserver radius Radius209 pap user1 test123
authenticate 'user1' against 'pap' failed, assigned_rad_session_id=730523922 session_timeout=0 secs
idle_timeout=0 secs!
```

- 用户名和密码正确

可以看到Radius服务器返回的状态是成功，以及用户属于，如user1属于用户组grp1。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的CLI测试结果如下：

```
# diagnose test authserver radius Radius209 pap user1 12345678
authenticate 'user1' against 'pap' succeeded, server=primary assigned_rad_session_id=730523923 session_timeout=0
secs idle_timeout=0 secs!
Group membership(s) - grp1
```

其他Radius配置参数

1. 修改Radius端口

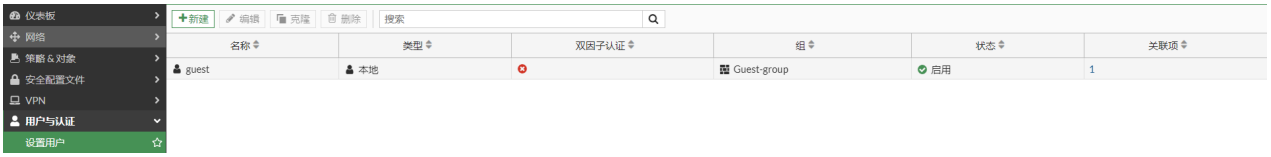
```
config user radius
    edit Radius209
        set radius-port xxx
    next
end
```

2. 指定原IP地址

```
config user radius
    edit Radius209
        set source-ip x.x.x.x
    next
end
```

创建radius用户

1. 选择“用户与认证”-->“设置用户”，点击“新建”



2. 选择"远程RADIUS用户"，点击“下一步”



3. 输入“用户名”和“RADIUS服务器”，点击“下一步”

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



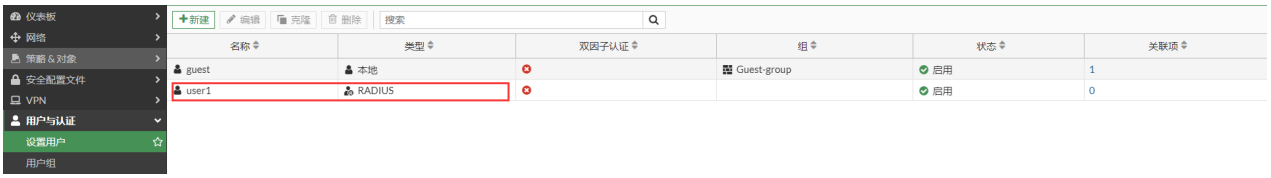
4. 如果Radius用户需要绑定FortiGate本地的Fortitoken，则勾选“双因子认证”。这里不需要，直接点击“下一步”



5. 如果需要现在为Radius用户指定一个用户组，可以勾选“用户组”来指定，也可以等创建完用户后，在用户组菜单中添加。这里不勾选，直接点击“提交”



6. 创建完成



创建radius用户组

1. 选择“用户与认证”-->"用户组"，点击"新建"

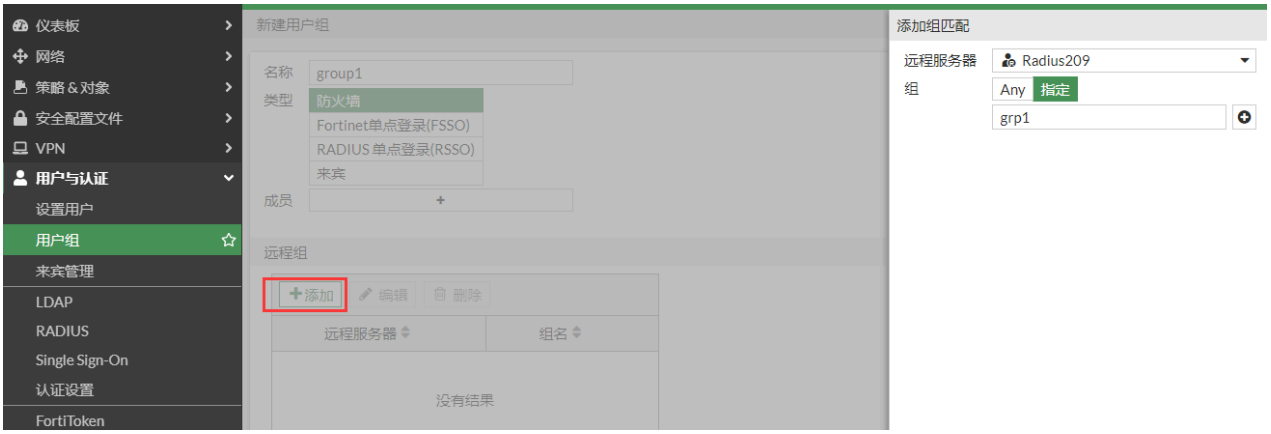


2. 配置参数

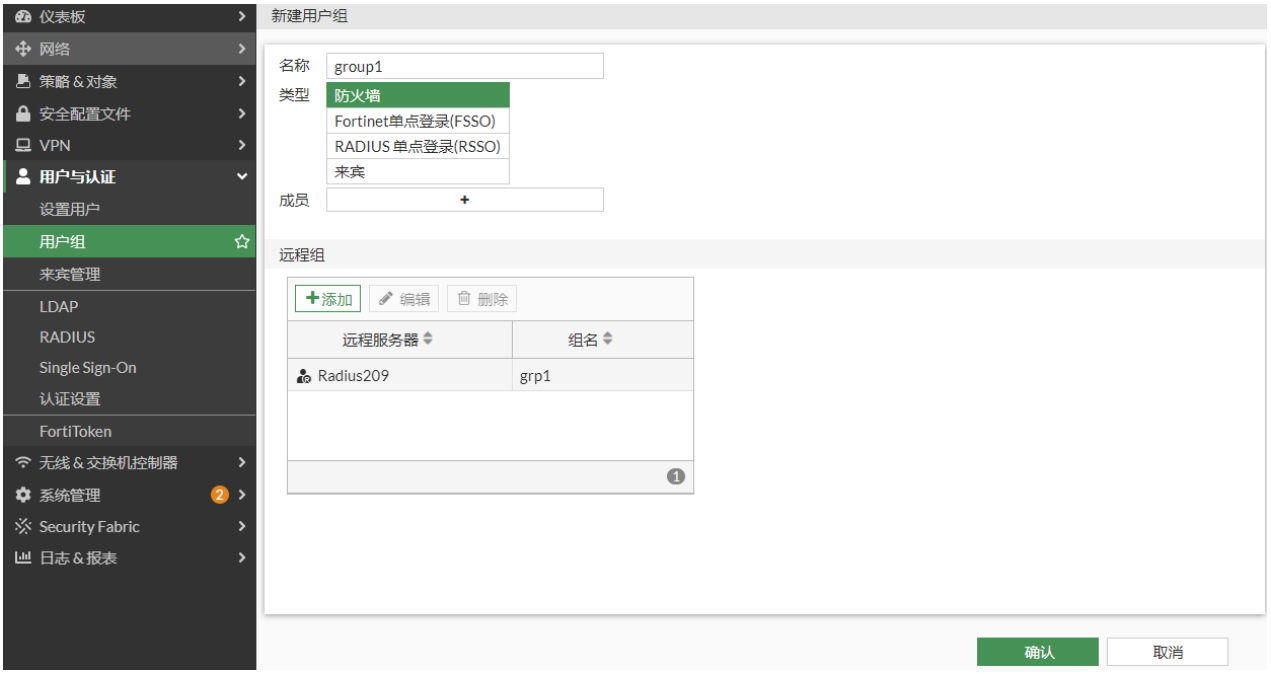
输入用户组名称group1，在远程组下，点击“添加”，在”远程服务器“中选择已配置的Radius服务器。

指定Radius的用户组，这里使用grp1，表示group1匹配Radius用户组grp1下的用户，可以添加多个组；如果组选择“Any”，表示匹配Radius服务器下的所用用户。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



选择完成后，点击“确认”。



3. 配置完成



Radius认证Debug

1. 认证成功

```
[1906] handle_req-Rcvd auth req 730524052 for user1 in Radius209 opt=0000001d prot=0
[466] __compose_group_list_from_req-Group 'Radius209', type 1
[616] fnbamd_pop3_start-user1
[518] __fnbamd_cfg_get_radius_list_by_server-Loading RADIUS server 'Radius209'
[342] fnbamd_create_radius_socket-Opened radius socket 12
[342] fnbamd_create_radius_socket-Opened radius socket 13
[1394] fnbamd_radius_auth_send-Compose RADIUS request
[1351] fnbamd_rad_dns_cb-192.168.91.209→192.168.91.209

认证请求，radius服务器是192.168.91.209，用户名user1，认证方法是PAP
[1323] __fnbamd_rad_send-Sent radius req to server 'Radius209': fd=12, IP=192.168.91.209(192.168.91.209:1812)
code=1 id=6 len=101 user="user1" using PAP
[319] radius_server_auth-Timer of rad 'Radius209' is added
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
[633] create_auth_session-Total 1 server(s) to try
[1360] fnbamd_auth_handle_radius_result-Timer of rad 'Radius209' is deleted

认证响应，响应code 2，认证成功，返回的用户属性
[1802] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[320] extract_success_vsas-FORTINET attr, type 1, val grp1
[1385] fnbamd_auth_handle_radius_result⟶Result for radius svr 'Radius209' 192.168.91.209(1) is 0
[266] find_matched_usr_grps-Skipped group matching
[216] fnbamd_comm_send_result-Sending result 0 (nid 0) for req 730524052, len=2154
[789] destroy_auth_session-delete session 730524052
```

2. 认证失败

```
[1906] handle_req-Rcvd auth req 730524053 for user1 in Radius209 opt=0000001d prot=0
[466] __compose_group_list_from_req-Group 'Radius209', type 1
[616] fnbamd_pop3_start-user1
[518] __fnbamd_cfg_get_radius_list_by_server-Loading RADIUS server 'Radius209'
[342] fnbamd_create_radius_socket-Opened radius socket 12
[342] fnbamd_create_radius_socket-Opened radius socket 13
[1394] fnbamd_radius_auth_send-Compose RADIUS request
[1351] fnbamd_rad_dns_cb-192.168.91.209→192.168.91.209

认证请求，radius服务器是192.168.91.209，用户名user1，认证方法是PAP
[1323] __fnbamd_rad_send-Sent radius req to server 'Radius209': fd=12, IP=192.168.91.209(192.168.91.209:1812)
code=1 id=7 len=101 user="user1" using PAP
[319] radius_server_auth-Timer of rad 'Radius209' is added
[633] create_auth_session-Total 1 server(s) to try
[1360] fnbamd_auth_handle_radius_result-Timer of rad 'Radius209' is deleted

认证响应，响应code 3，认证拒绝
[1802] fnbamd_radius_auth_validate_pkt-RADIUS resp code 3
[1385] fnbamd_auth_handle_radius_result⟶Result for radius svr 'Radius209' 192.168.91.209(1) is 1
[216] fnbamd_comm_send_result-Sending result 1 (nid 0) for req 730524053, len=3172
[789] destroy_auth_session-delete session 730524053
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiToken Mobile在FortiGate上的激活

FortiToken Mobile 是FortiToken的手机软件安装版，是一种非常环保且方便的FortiToken实现方式，只需要在手机上安装一个APP即可实现FortiToken双因子的功能。默认每一台防火墙都有2个免费提供的FortiToken Mobile许可，自带且完全免费。

免费token激活

重要

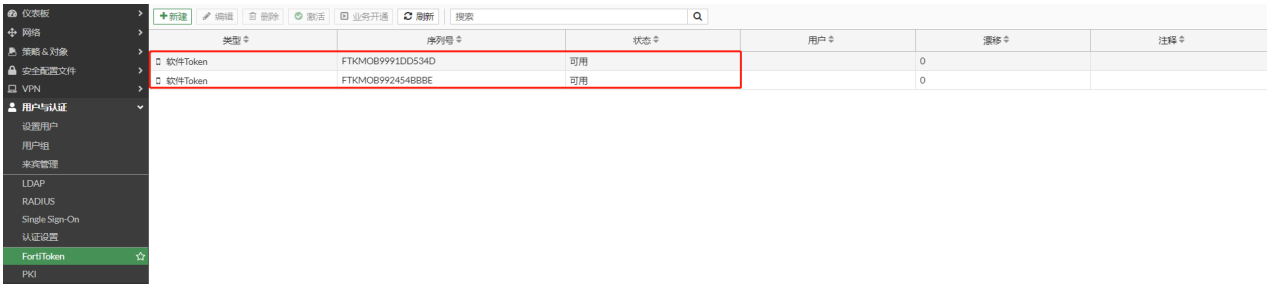
免费token常见问题请参考：免费FortiToken Mobile在FortiGate绑定时遇到的问题及处理方法 ↗。

1. 保证FortiGate能够上网

2. 选择“用户与认证”-->”FortiToken“，点击“导入免费试用令牌”



即可生成两个免费的token。



FortiToken许可激活

1. 购买FortiToken后会收到一个PDF激活文件

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 保证FortiGate能够上网

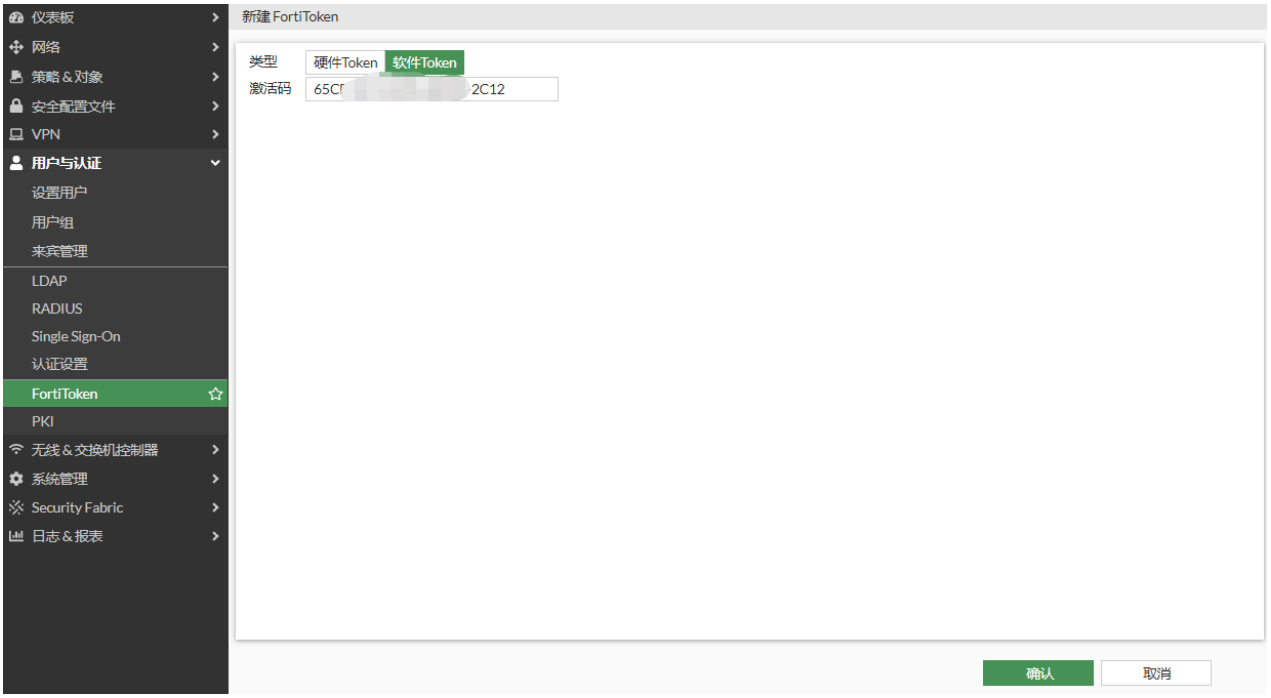
3. 激活FortiToken

选择“用户与认证”-->”FortiToken“，点击“新建”

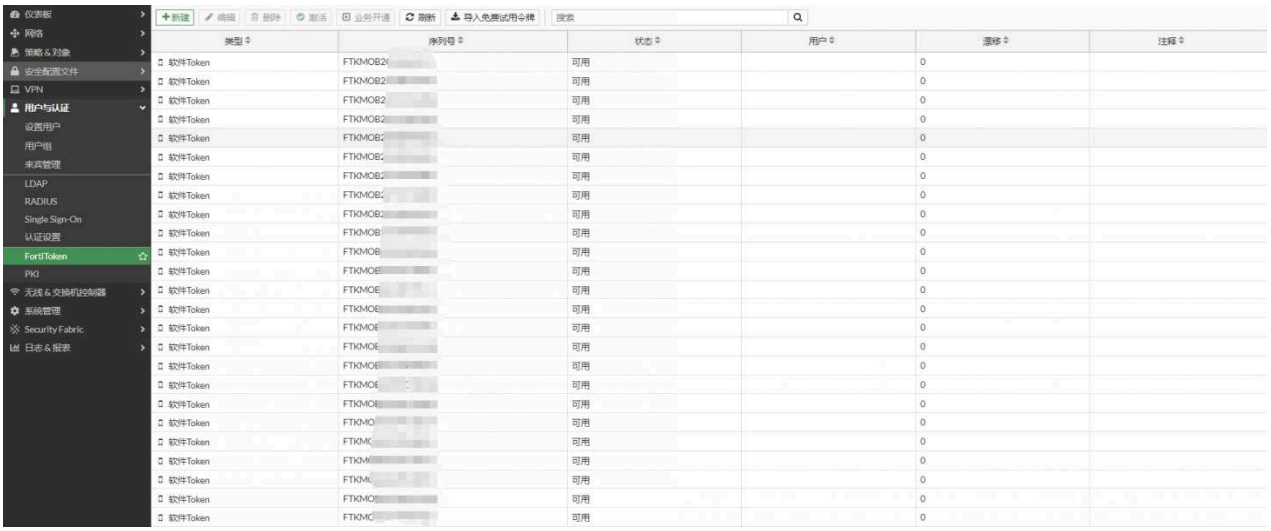


点击“软件Token”，输入PDF文件的中的Activation Code，点击确认。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiToken导入成功。



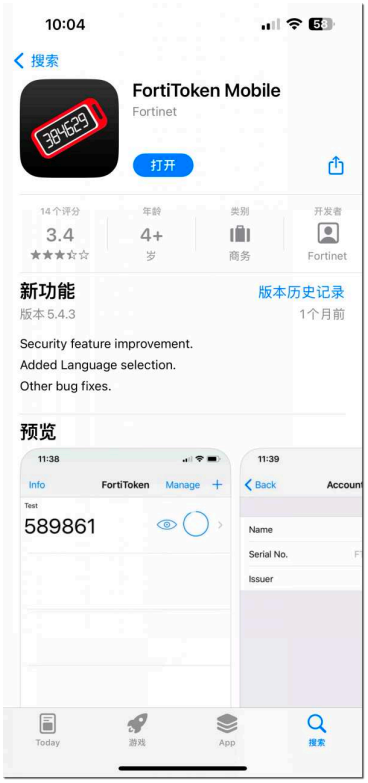
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiToken Mobile APP软件下载与安装

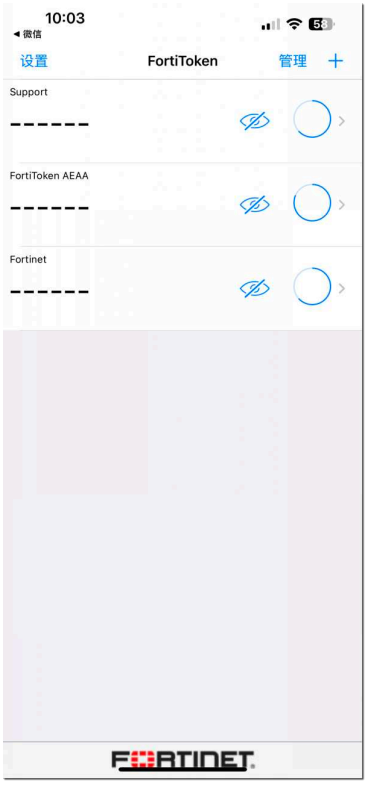
FortiToken Mobile APP 可以安装并运行在iOS系统、安卓系统手机上。

1. iPhone安装

   iPhone直接在Apple App Store搜索“FortiToken Mobile”。



   安装完后，显示如下（图中的包含了已添加过的两个token）：



2. Android手机下载

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

安装包下载：FortiTokenAndroid.apk ↗。

Android用户也可在Google Play store搜索“FortiToken Mobile”下载安装。

也可以通过发邮件给support_cn@fortinet.com来咨询获取Android安装包。



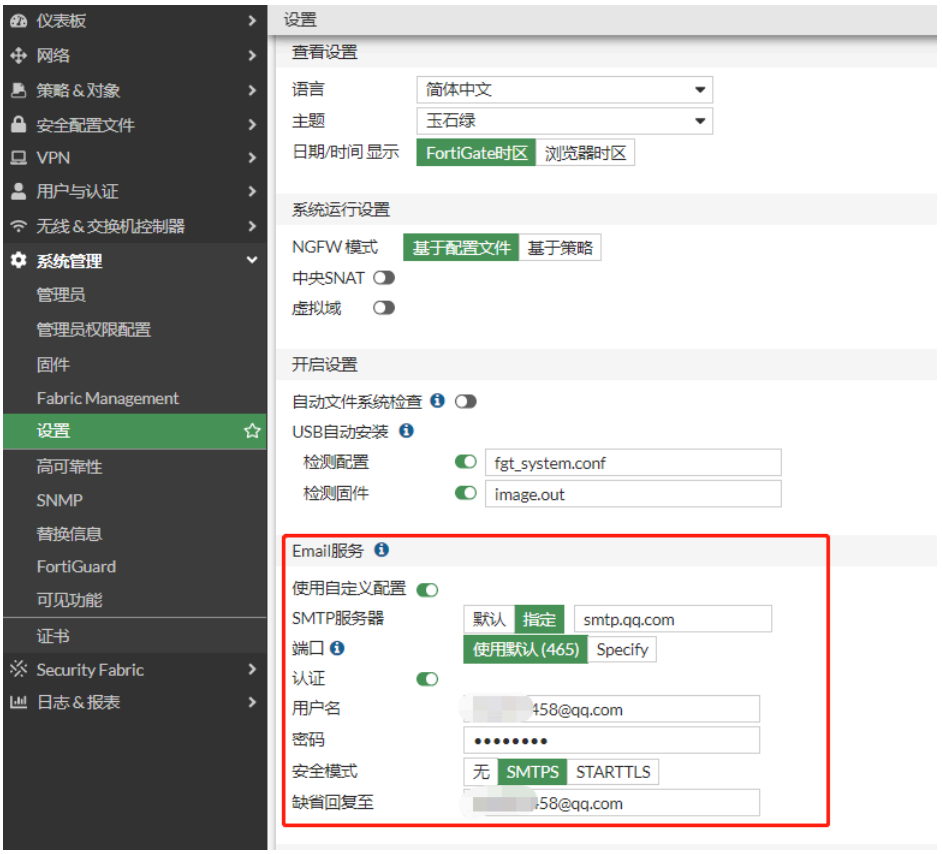
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiToken Mobile与用户进行绑定

FortiGate使用邮件发送FortiToken的二维码图片，这样用户直接使用手机APP扫描二维码即可绑定FortiToken Mobile。

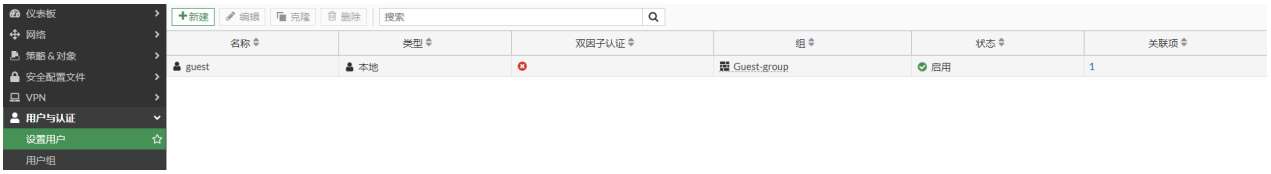
邮箱设置

这里使用QQ邮件发邮件。更多Email服务设置请参考系统管理→系统设置→Email服务 ↗章节。



绑定FortiToken

1. 选择“用户与认证”-->“设置用户”，点击“新建”。



2. 选择“本地用户”，点击“下一步”。

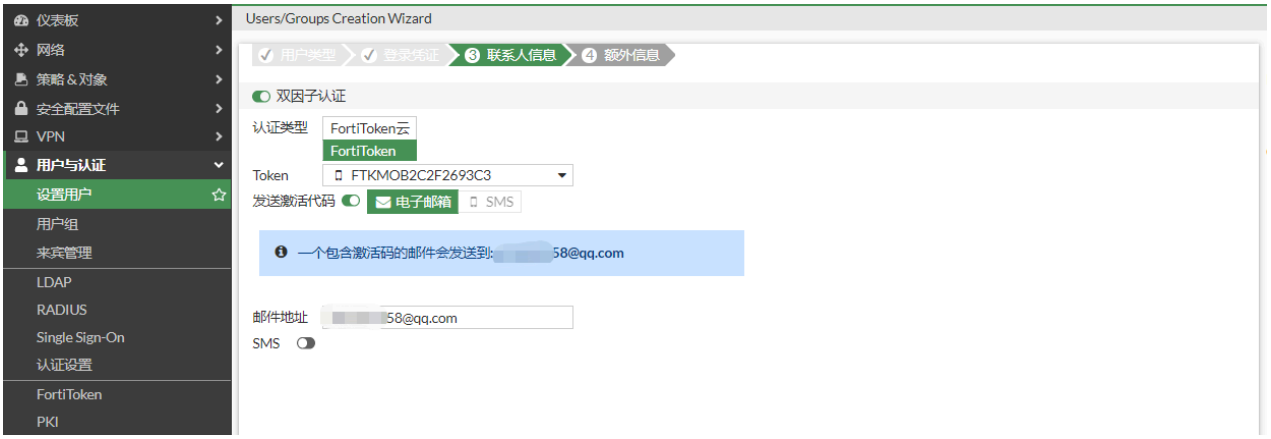


3. 输入用户名和密码，点击“下一步”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



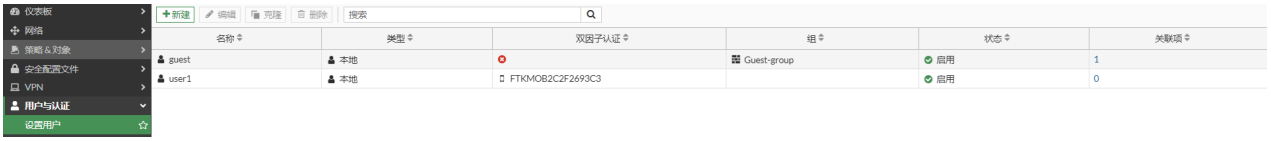
4. 启用双因子认证，选择一个token并填写用户邮箱，点击“下一步”。



5. 点击提交。

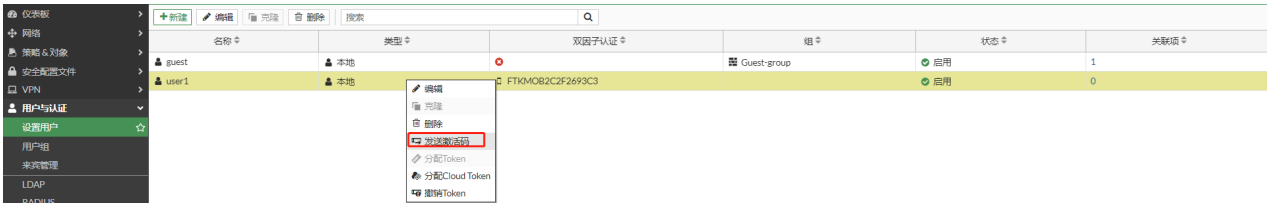


6. 完成用户创建。



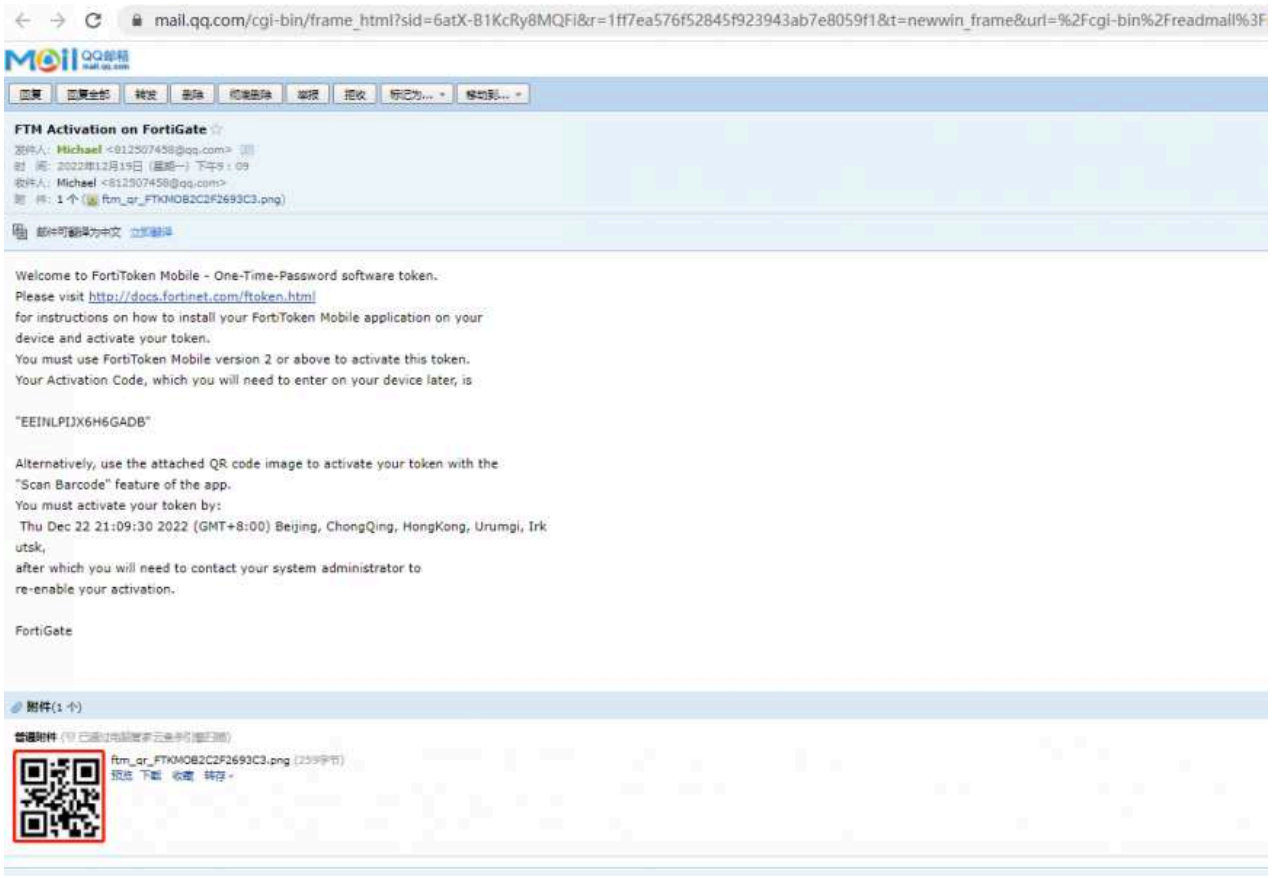
发送token到用户邮箱

1. 用户创建完成后会自动发送一封带有二维码的邮件给用户邮箱。如果没有收到，也可以右击该用户，选择“发送激活码”。



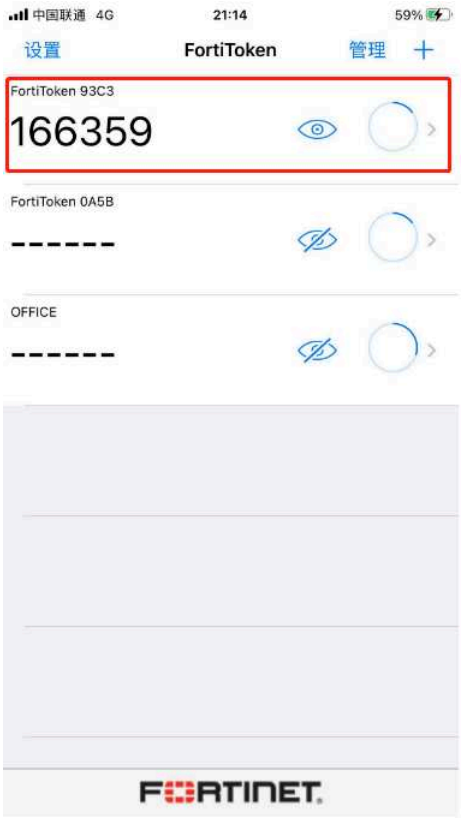
2. 邮件中的二维码如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiToken APP扫描二维码

使用FortiToken扫描二维码即可拿到该Token。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

1. 每个令牌只能在一台 FortiGate 设备上使用。
2. 每个令牌只能绑定一个用户。
3. 可以将令牌从用户上解除绑定，每次绑定用户均需要再次激活。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

免费FortiToken Mobile在FortiGate绑定时遇到的问题及处理方法

请参考链接：免费FortiToken Mobile在FortiGate绑定时遇到的问题及处理方法 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FSSO认证

重要

感谢东区SE提供的文档支持！

请参考链接：FortiGate FSSO部署手册 ↗。

关于FSSO账户权限的更多信息，可参考：https://community.fortinet.com/t5/FortiGate/Technical-Tip-Restricting-a-Fortinet-Single-Sign-On-Agent/ta-p/198065 ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

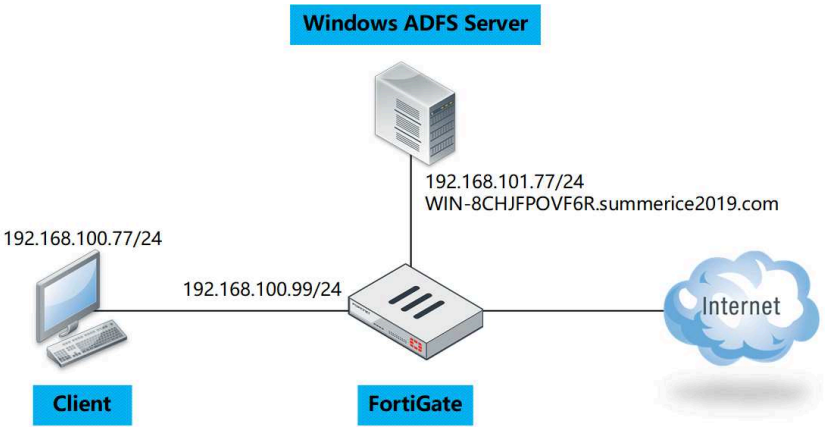
防火墙用户与SSL VPN SAML认证（Windows ADFS）

网络需求

ADFS（Active Directory Federation Service），Active Directory 联合身份验证服务是一项需要单独安装在 AD 服务器上的功能。其主要目的是为AD用户提供单一登录（SSO）访问权限。

ADFS可以配合FortiGate实现SAML认证，本文详细介绍了FortiGate代理策略认证与Windows Server 2019 ADFS配合做SAML认证的配置，本例中Fortigate作为SAML SP（Service Provider），ADFS作为SAML IDP（Identity Provider）。

网络拓扑



1. FortiGate作为SP，Windows Server安装ADFS服务后作为IDP。
2. FortiGate和Client将DNS服务器地址配置为Windows Server的IP。

配置步骤

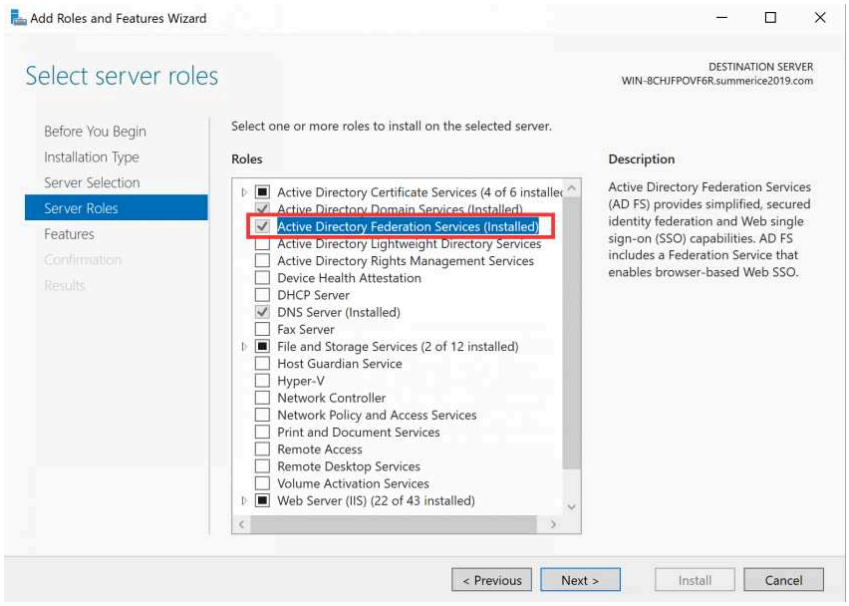
防火墙策略用户SAML认证

Windows Server端配置

1. 在Windows Server中安装AD域控，加入或新建AD域。

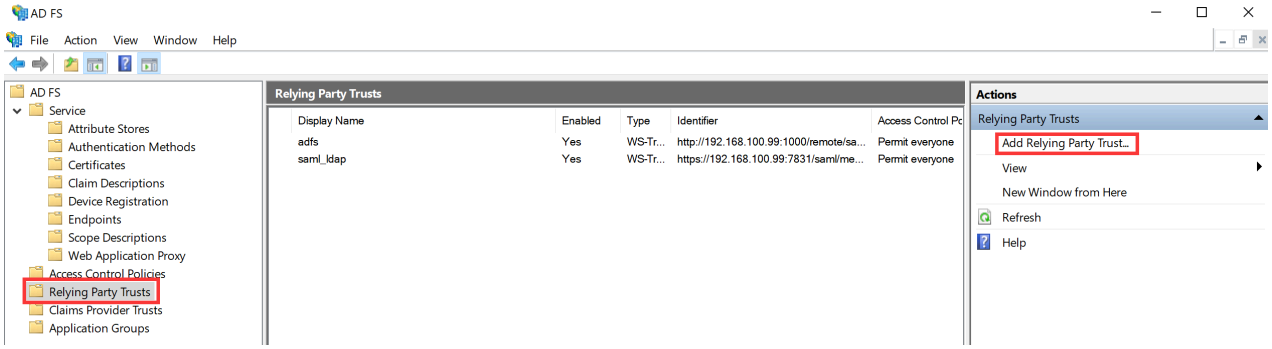
2. 在服务器配置中，安装Windows ADFS服务。

3. Client为AD用户。

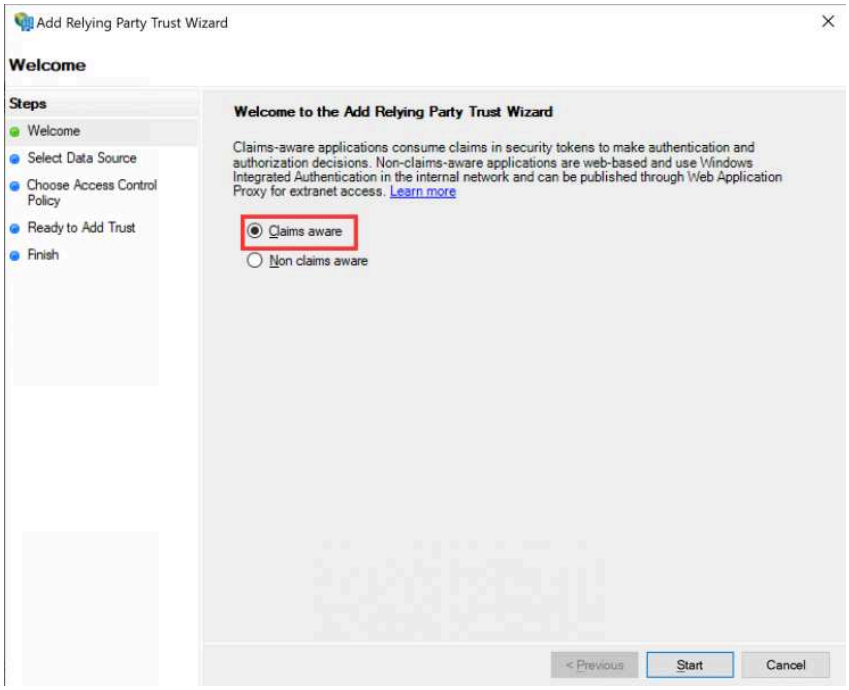


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

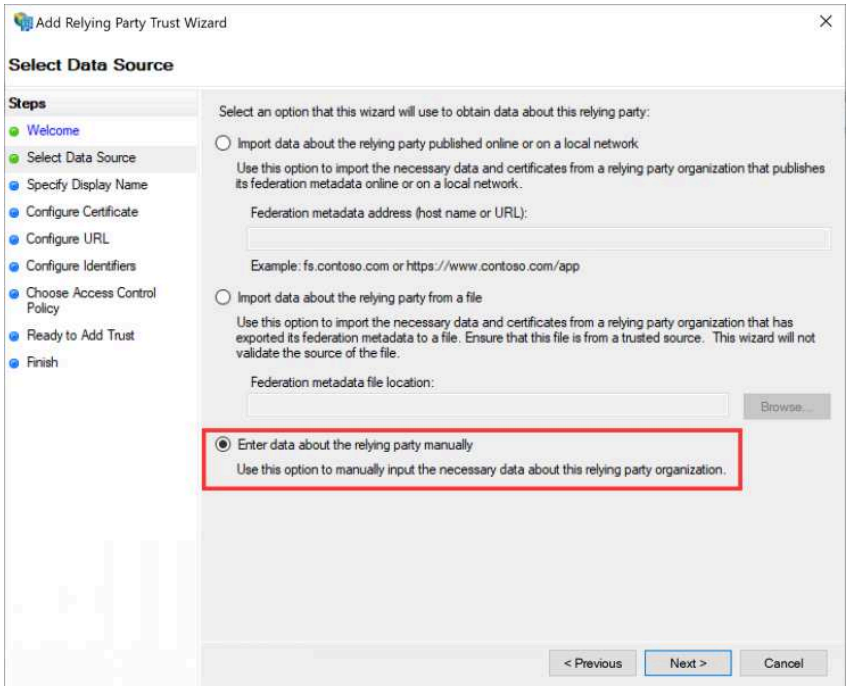
4. 安装完成后，通过Server Manager -> Tools -> AD FS Management打开ADFS管理器，并点击Relying Party Trust，点击右侧的Add Relying Party Trust按钮添加信任方。



5. 弹出向导界面，这里选择感知方式，由于配合的是外部的FortiGate，需要选择Claims aware，点击Start。

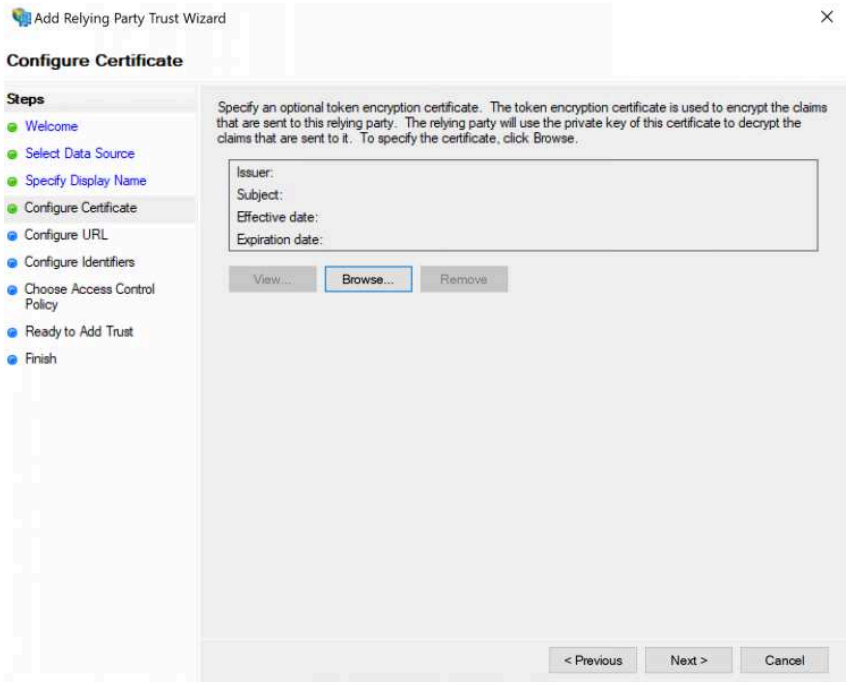


6. 数据源选择手动输入，点击Next。

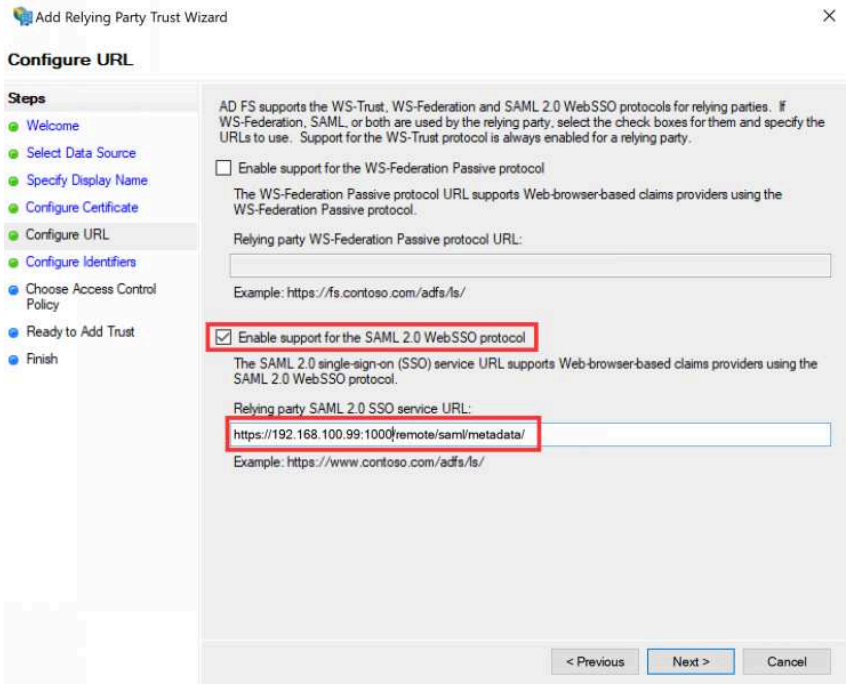


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

7. 直接点击Next。

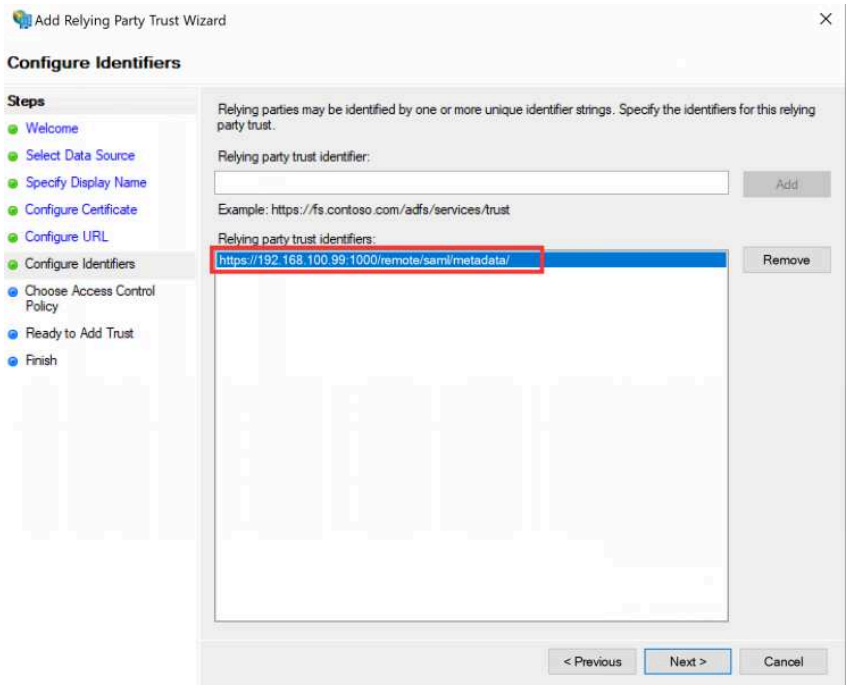


8. 选择SAML认证，并填写信赖方的metadata地址（FortiGate内网口的认证地址和端口号）。

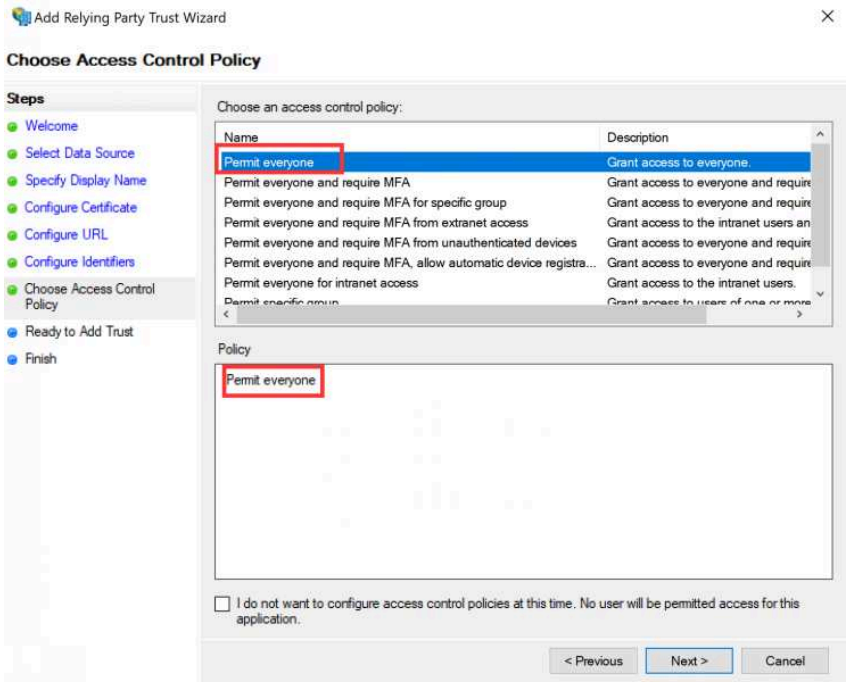


9. 配置信赖方identifier URL，这里填写和上步相同的URL，并点击Add。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

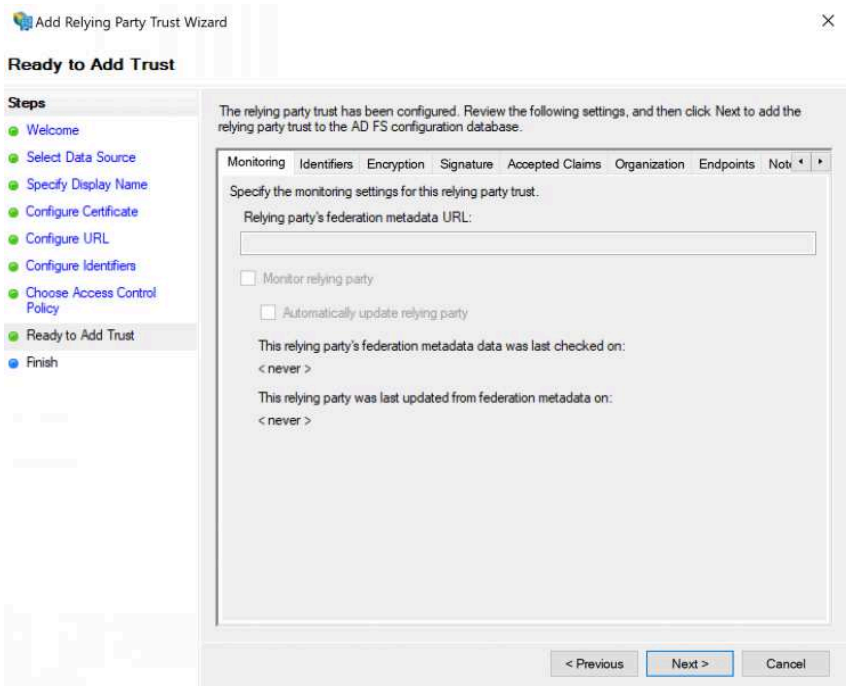


0. 访问控制策略选择允许所有人访问。

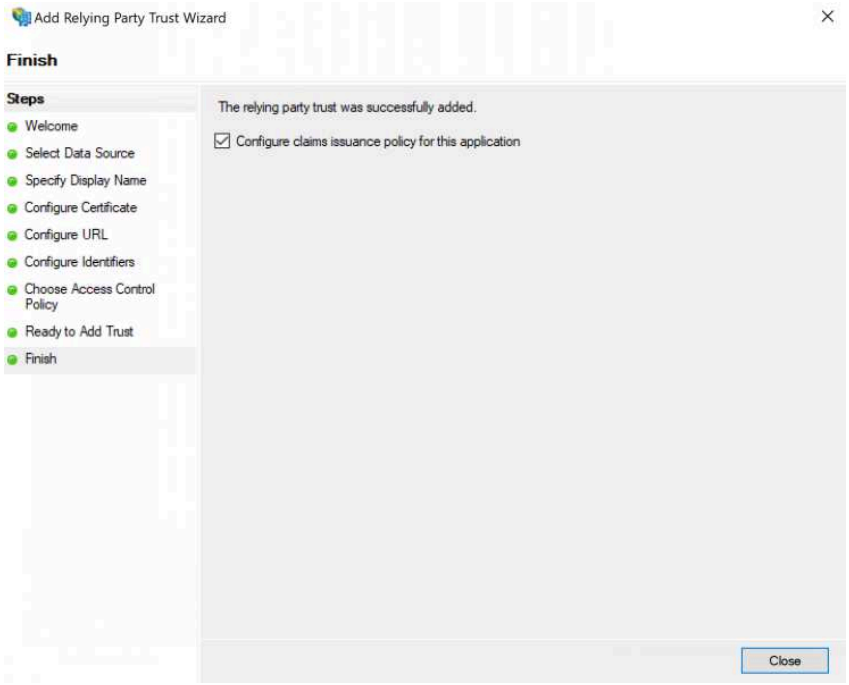


1. 检查配置无误，点击Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

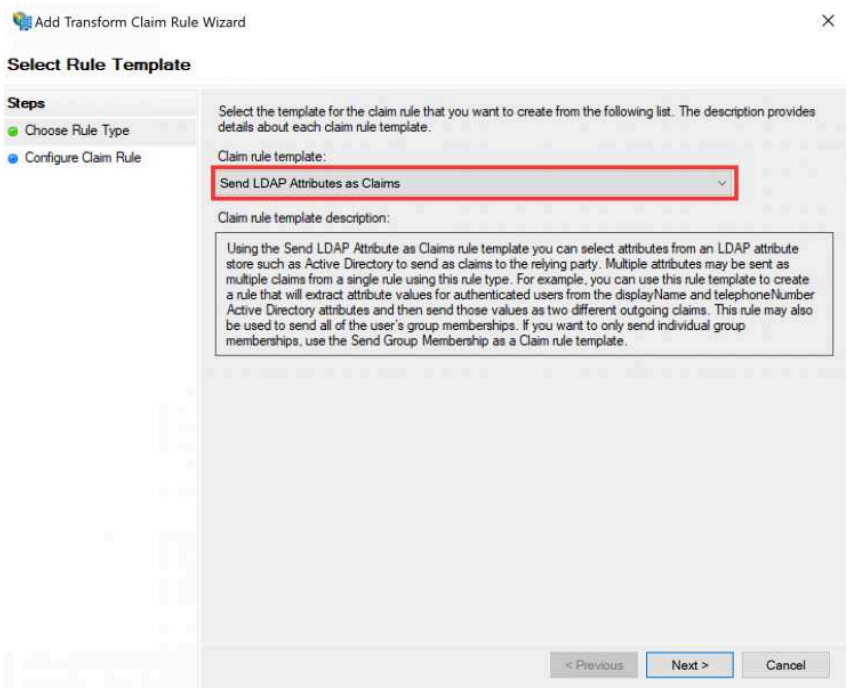


2. 点击Configure claims issuance policy for this application，点击Close。

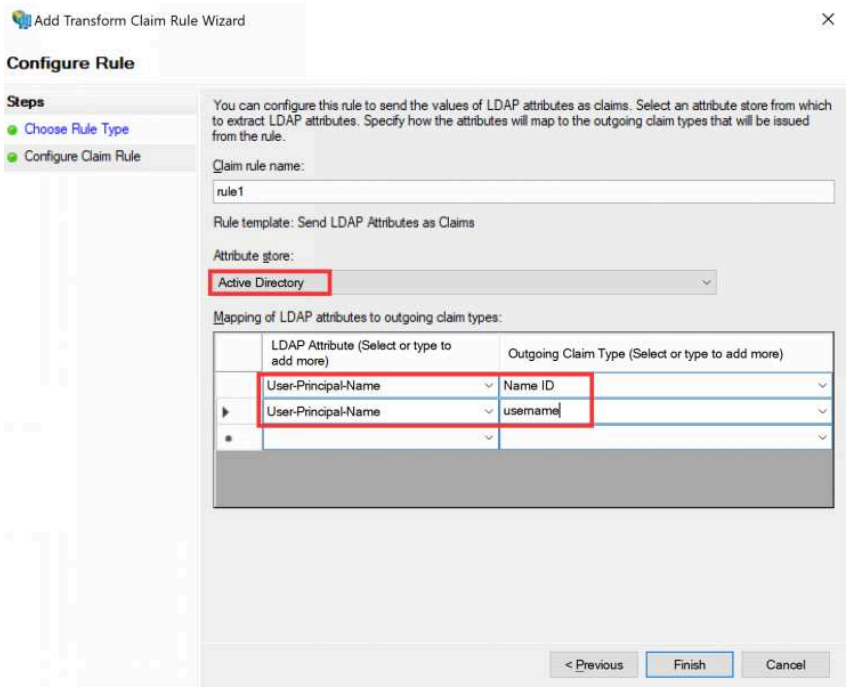


3. 在弹出的Claim规则中，选择模版为Send LDAP Attributes as Claims。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

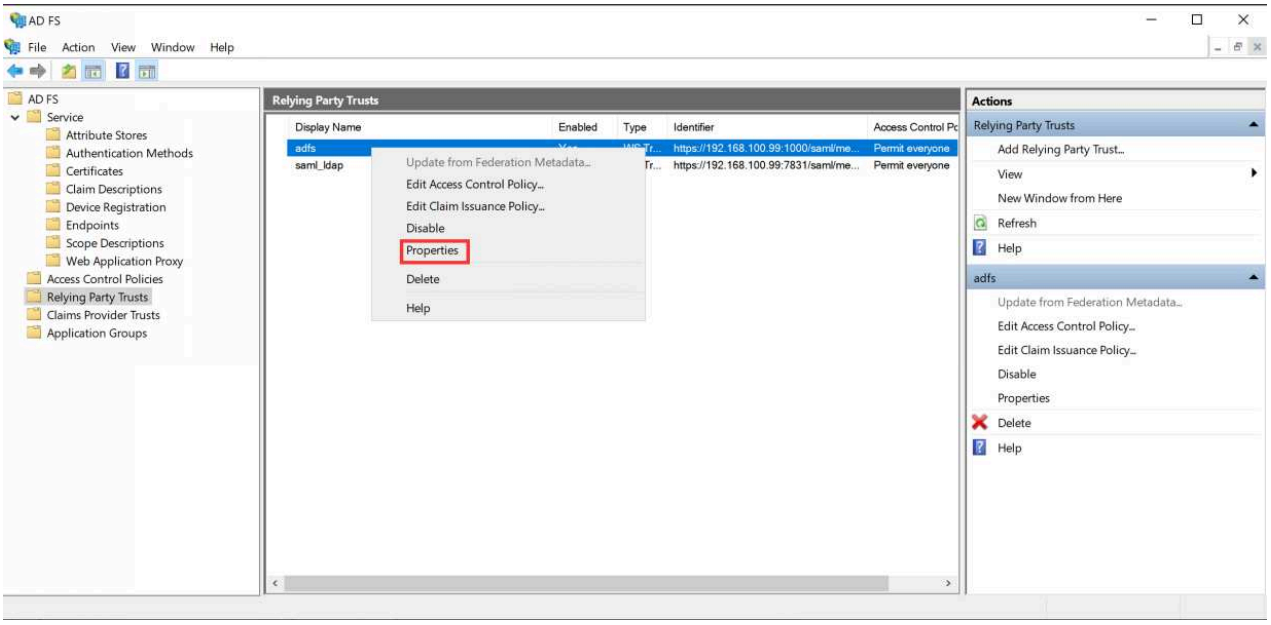


4. 配置Claim规则，Attribute store选择Active Dictionary，如下图配置映射关系，点击Finish。

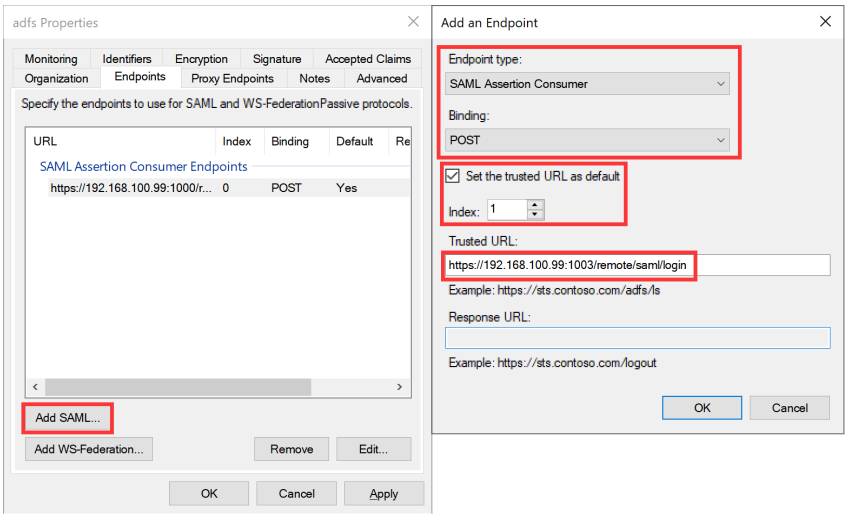


5. 右键单击已创建的Relying Party Trust，点击Properties。

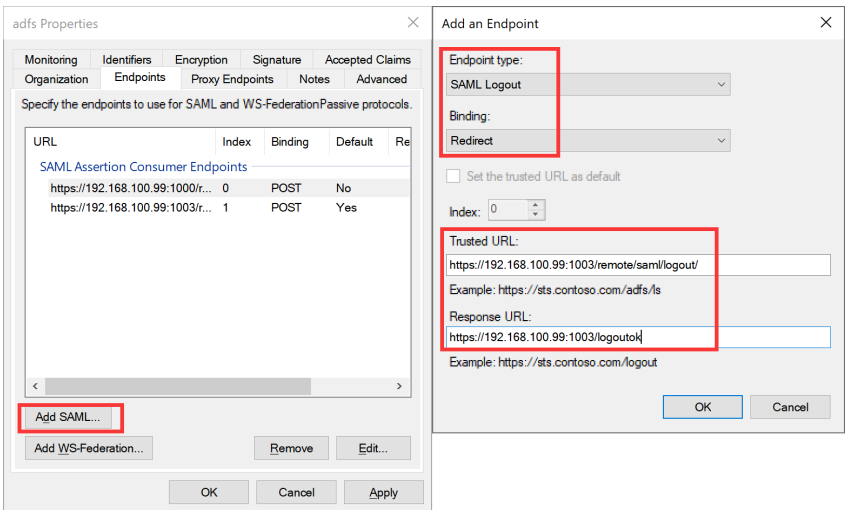
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 选择Endpoints选项卡，点击Add SAML按钮，Endpoint type选择SAML Assertion Consumer，Binding选择POST，Index修改为1，Trusted URL填写FortiGate内网口的SAML登陆URL。

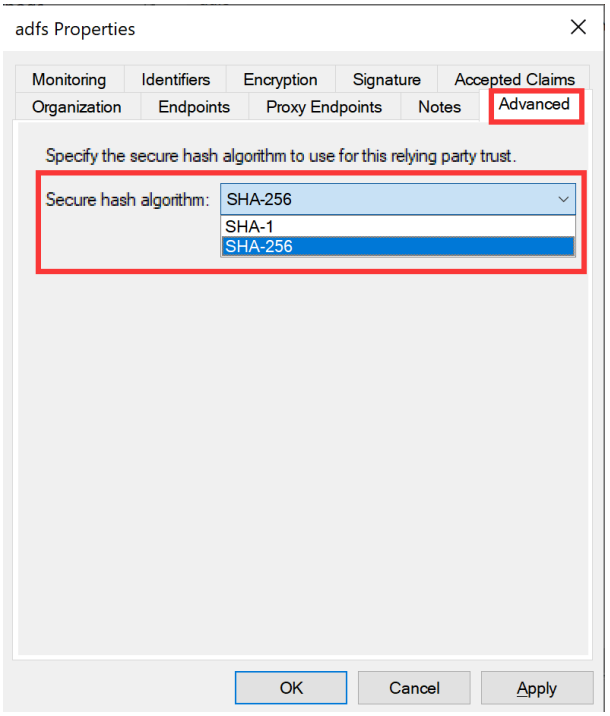


7. 再次新建一个SAML，Endpoint type选择SAML logout，Binding选择Redirect，Trusted URL填写FortiGate内网口的SAML登出URL，Response URL填写FortiGate的登出成功页面。

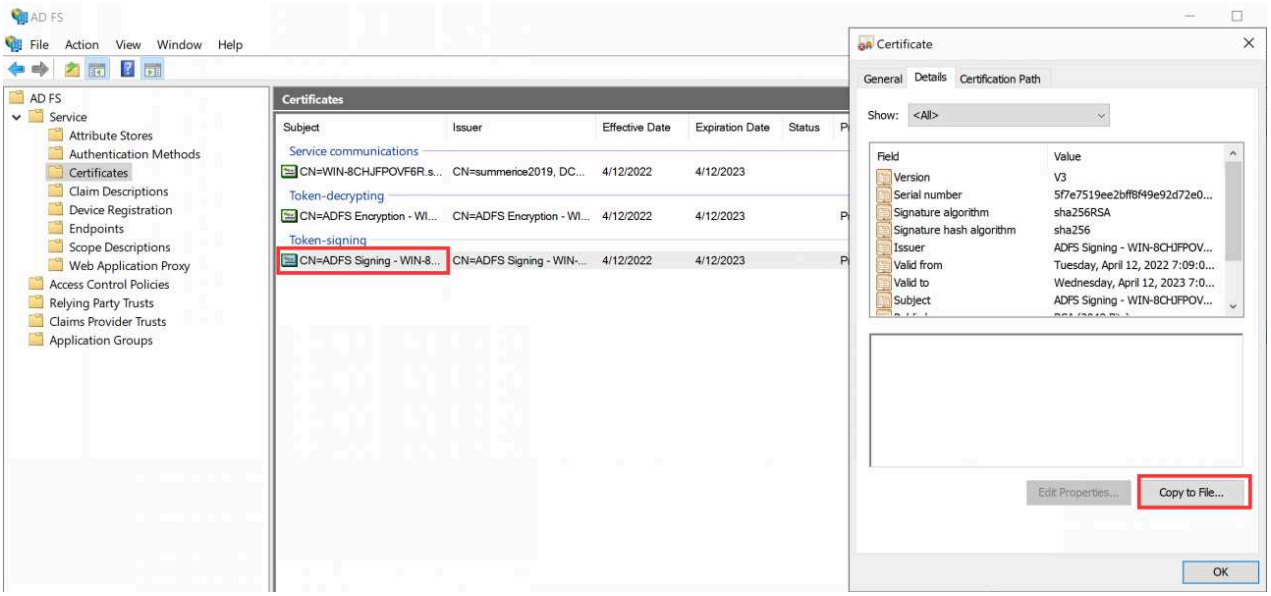


8. Advance选项卡可以配置hash算法，默认为SHA256。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



9. 进入ADFS服务器管理器的Service→Certificates界面，选择Token-signing下的证书，导出该证书。



10. 将该证书导入FortiGate的Remote Certificate中。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



1. 访问URL：`https://<ADFS Domain name>/FederationMetadata/2007-06/FederationMetadata.xml`，例如实验这台Windows Server的URL为`https://win-8chjfpovf6r.summerice2019.com/FederationMetadata/2007-06/FederationMetadata.xml`，下载的XML文件中可以看到IDP相关信息，并记录。
   - Metadata URL（`http://WIN-8CHJFPOVF6R.summerice2019.com/adfs/services/trust`）：



   - Login URL（`https://win-8chjfpovf6r.summerice2019.com/adfs/ls/`），Logout URL为`https://win-8chjfpovf6r.summerice2019.com/adfs/oauth2/logout`：



FortiGate端配置

1. 在FortiGate上配置SAML用户，配置SP和IDP信息，注意这里填写的SP信息要和ADFS中配置的Endpoints信息一致，IDP信息从XML文件中记录的得来，证书选择导入的ADFS的Remote Certificate，算法选择sha256。

```bash
config user saml
    edit "adfs_saml_user"
        set entity-id "https://192.168.100.99:1000/remote/saml/metadata"
        set single-sign-on-url "https://192.168.100.99:1003/remote/saml/login"
        set single-logout-url "https://192.168.100.99:1003/remote/saml/logout"
        set idp-entity-id "http://WIN-8CHJFPOVF6R.summerice2019.com/adfs/services/trust"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set idp-single-sign-on-url "https://WIN-8CHJFPOVF6R.summerice2019.com/adfs/ls/"
        set idp-single-logout-url "https://win-8chjfpovf6r.summerice2019.com/adfs/oauth2/logout"
        set idp-cert "REMOTE_Cert_1"
        set user-name "username"
        set digest-method sha256
    next
end

```

2. 创建用户组，将SAML用户加入用户组。

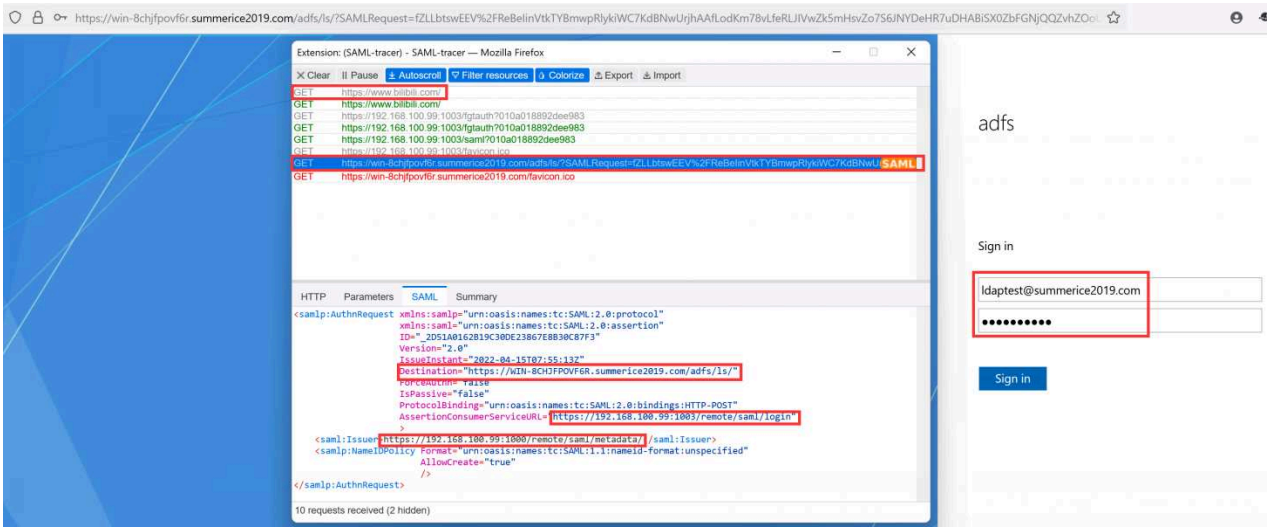
```bash
config user group
    edit "adfs_saml_group"
        set member "adfs_saml_user"
    next
end
```

3. 在FortiGate的防火墙策略中引用该用户组。

```bash
config firewall policy
    edit 1
        set srcintf "lan" "port20"
        set dstintf "port18" "port20"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        **set groups "adfs_saml_group"**
    next
end
```

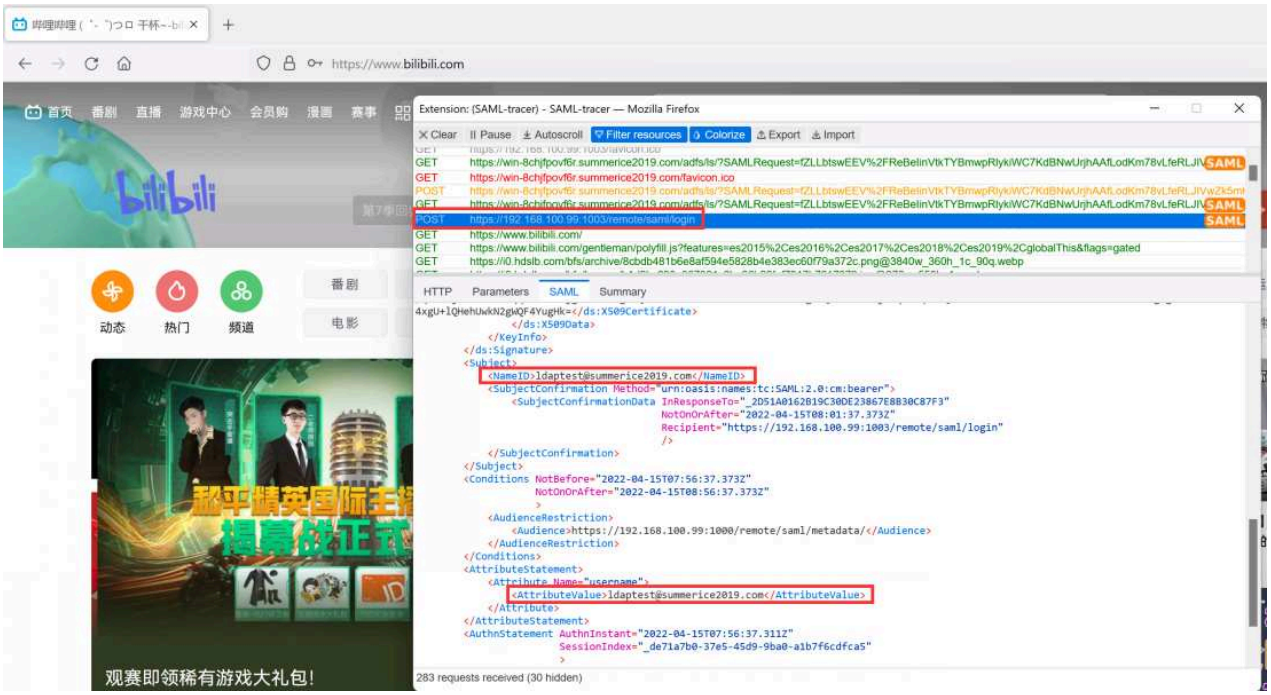
验证配置

1. Client访问www.bilibili.com ↗ ，重定向到IDP弹出ADFS登录页面，使用SAML tracer可以看到SAML SP和IDP的具体URL。



2. 输入帐号和密码，可以看到向SP URL POST了账户信息，登陆成功，正常弹出网页。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```
FortiGate-101F # diagnose firewall auth list

192.168.100.77, ldaptest@summerice2019.com
        src_mac: 0c:37:96:06:d7:5d
        type: fw, id: 0, duration: 146, idled: 0
        expire: 300, allow-idle: 300
        server: adfs_saml_user
        packets: in 72 out 172, bytes: in 3771 out 12163
        group_id: 2
        group_name: adfs_saml_group

----- 1 listed, 0 filtered ------
```

SSL VPN用户认证

Windows Server端配置

参考以上IDP、SP URL的端口号配置为SSL VPN端口号。

FortiGate端配置

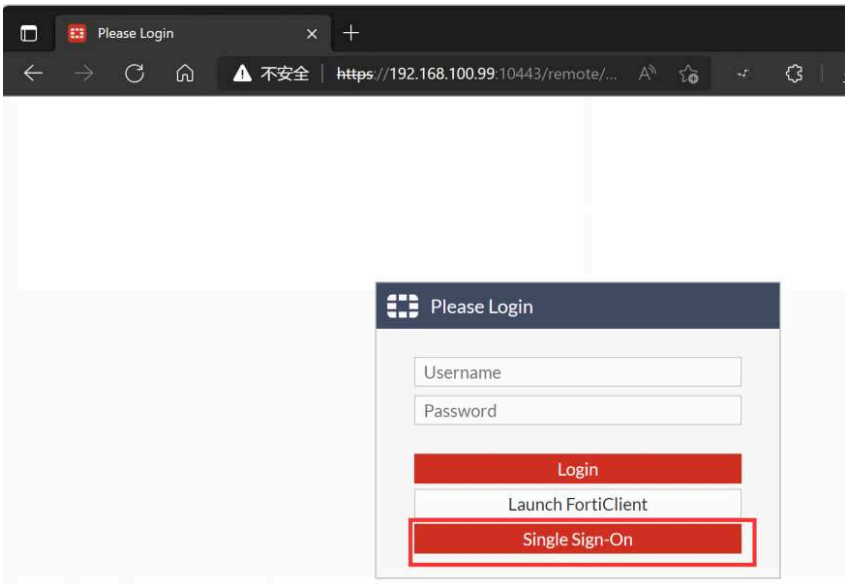
参考以上IDP、SP URL的端口号改为SSL VPN端口，并使用SSL VPN引用该用户组即可。

```bash
config user saml
    edit "adfs_saml_user"
        set entity-id "https://192.168.100.99:10443/remote/saml/metadata/"
        set single-sign-on-url "https://192.168.100.99:10443/remote/saml/login"
        set single-logout-url "https://192.168.100.99:10443/remote/saml/logout/"
        set idp-entity-id "http://WIN-8CHJFPOVF6R.summerice2019.com/adfs/services/trust"
        set idp-single-sign-on-url "https://WIN-8CHJFPOVF6R.summerice2019.com/adfs/ls/"
        set idp-single-logout-url "https://win-8chjfpovf6r.summerice2019.com/adfs/oauth2/logout"
        set idp-cert "REMOTE_Cert_1"
        set user-name "username"
        set digest-method sha256
    next
end
```

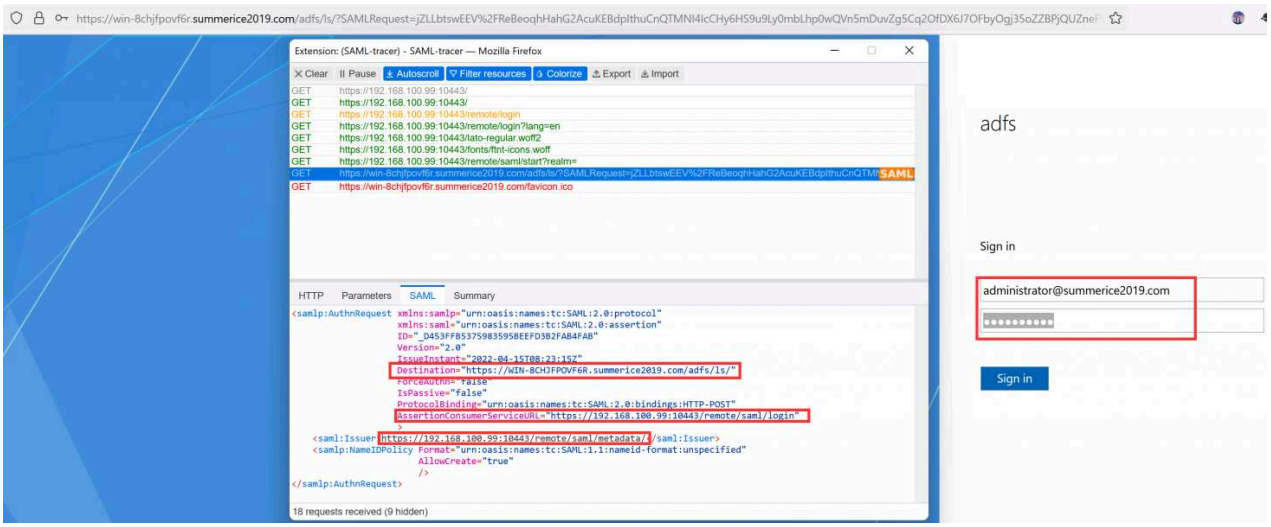
验证配置

1. 打开SSL VPN Web登陆界面，点击Single Sign-On。

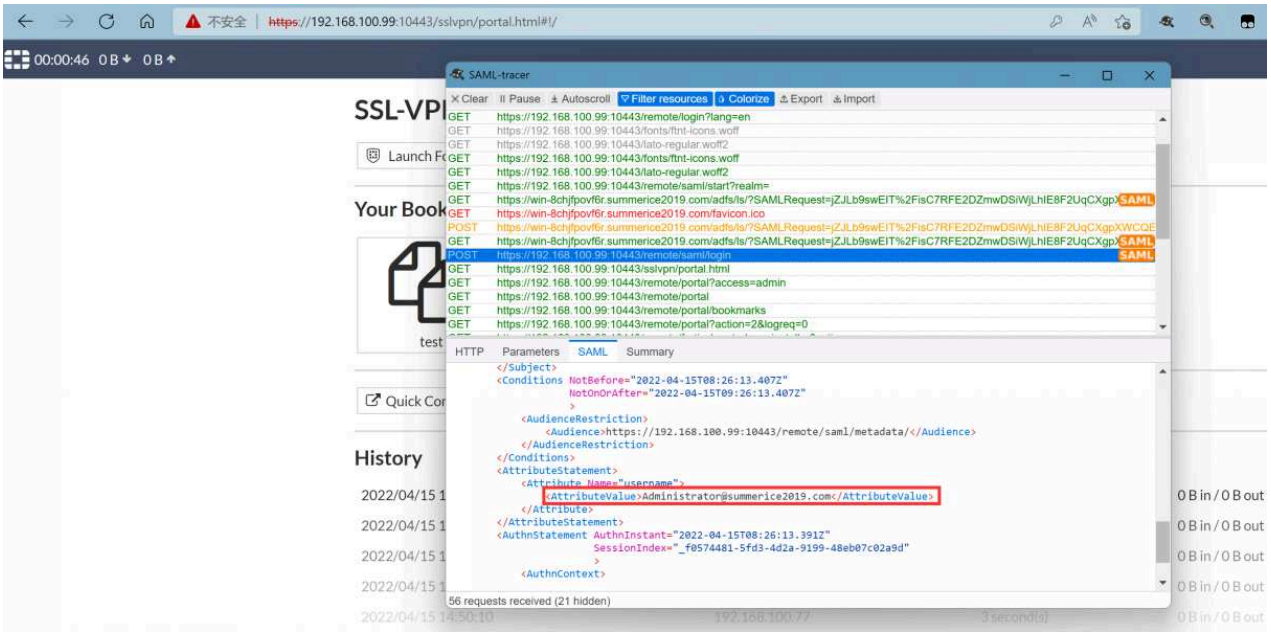
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 重定向到IDP弹出ADFS登录页面，使用SAML tracer可以看到SAML SP和IDP的具体URL。

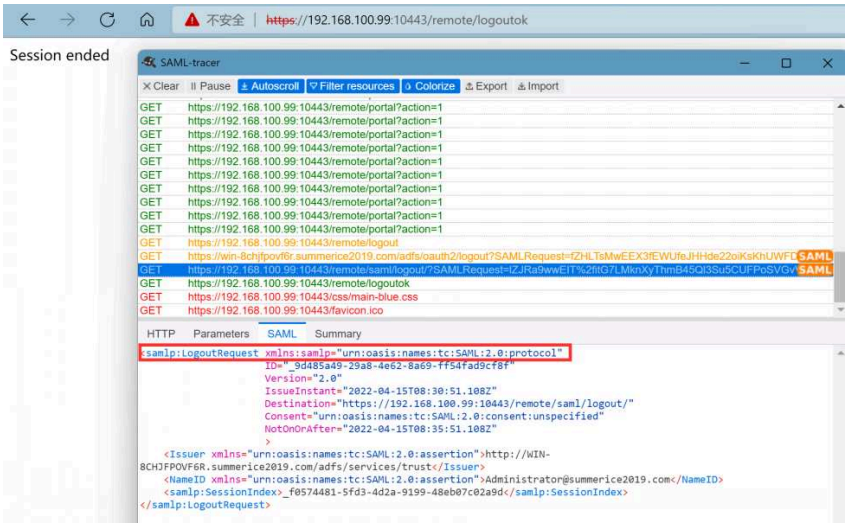


3. 输入帐号和密码，可以看到向SP URL POST了账户信息，登陆成功，正常弹出SSL VPN资源页面。

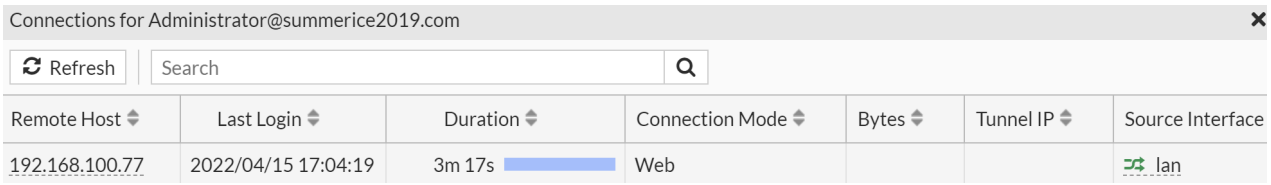


4. 登出SSL VPN，可以看到IDP登出成功，且正常弹出logoutok页面。

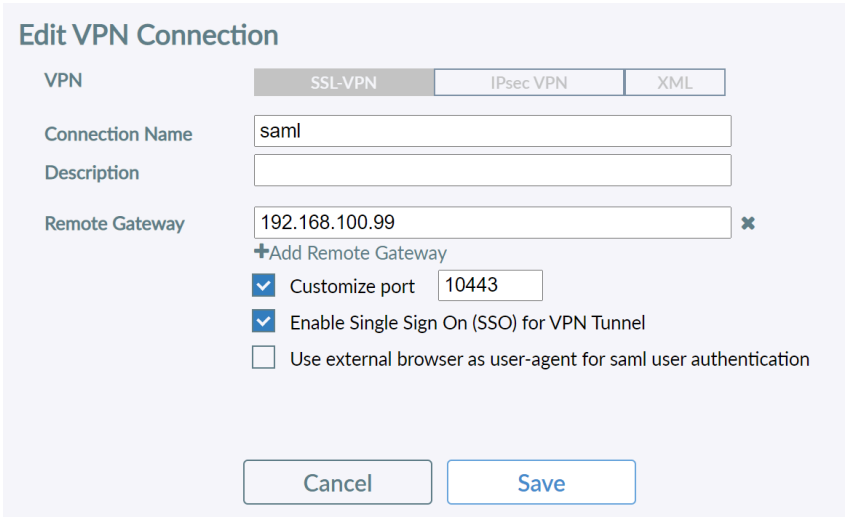
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 在FortiGate查看登陆用户。

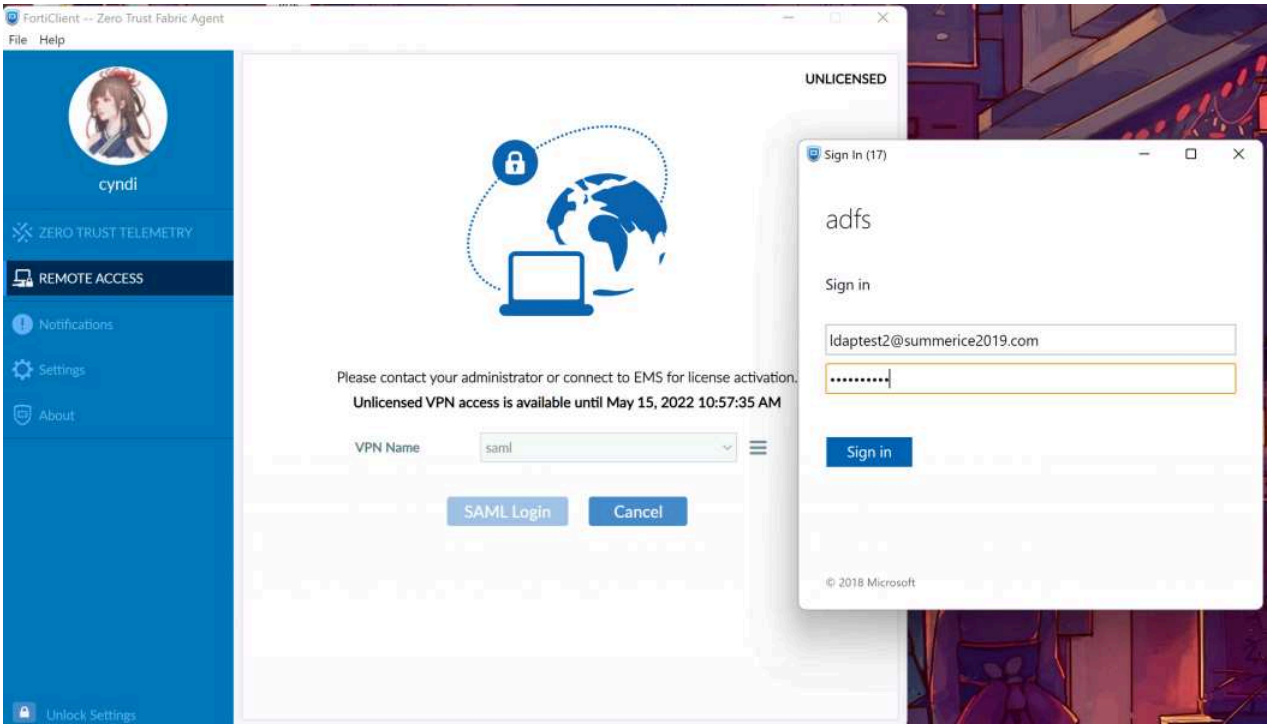


6. 使用FortiClient进行SSL VPN SAML认证。

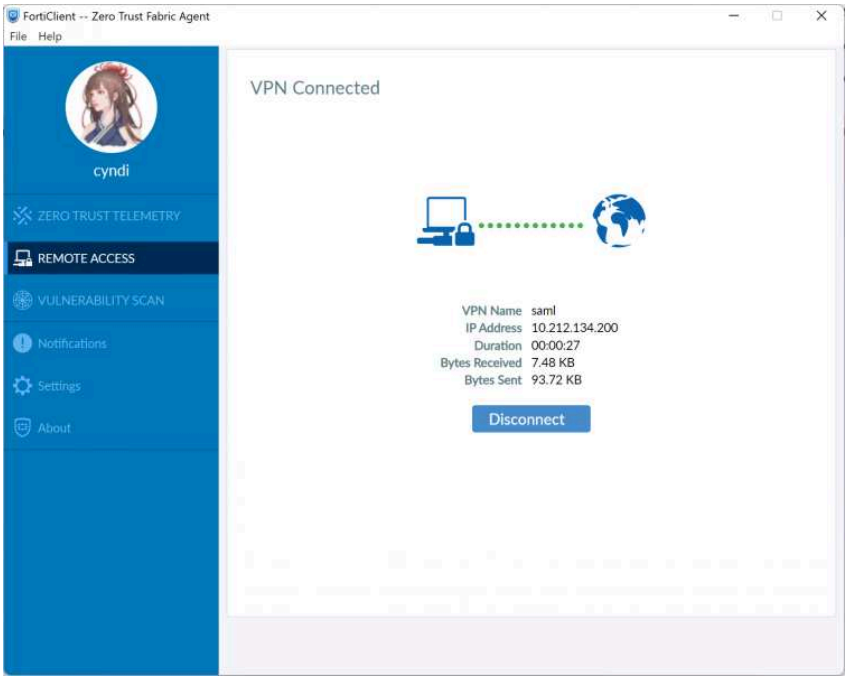


7. 弹出ADFS认证页，输入帐号密码。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 登陆成功。



9. 在防火墙上查看登陆用户。

```
FortiGate-101F # diagnose firewall auth list

10.212.134.200, ldaptest2@summerice2019.com
        type: fw, id: 0, duration: 82, idled: 0
        expire: 28797, allow-idle: 28797
        flag(80): sslvpn
        server: adfs_saml_user
        packets: in 10898 out 14201, bytes: in 2628530 out 13760383
        group_id: 2
        group_name: adfs_saml_group
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

1. 确保SAML IDP服务器的系统时间和客户端的时间一致，否则会认证失败，通过diagnose debug application samld -1可以看到该错误信息。

```
__samld_sp_login_resp [859]: Clock skew tolerance: 21

__samld_sp_login_resp [866]: Clock skew issue.
```

bash

重要

7.0.4 GA开始支持配置Clock skew tolerance超时时间：

```
config user saml
    edit <>
        set clock-tolerance <in seconds>      ( 0-300, 15 by default)
    next
end
```

2. 如果客户端访问IDP需要穿过防火墙，需要在认证策略前配置一条去往IDP服务器的策略，并开启captive-portal-exempt。

```
config firewall policy
    edit 2
        set srcintf "lan"
        set dstintf "port18"
        set action accept
        set srcaddr "all"
        set dstaddr "192.168.101.77/32"
        set schedule "always"
        set service "ALL"
        **set captive-portal-exempt enable**
    next
```

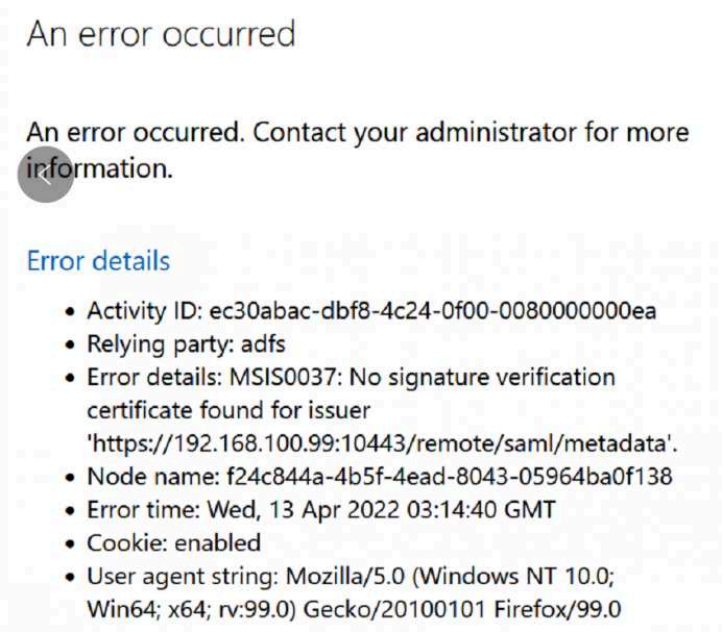
bash

3. 该错误表示FortiGate上的SP、IDP URL与ADFS中Endpoints中配置的URL不一致，需要检查配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 该错误表示客户端未安装ADFS所属AD域的CA证书。



5. 如果SAML弹出的登陆界面超时时间过短，来不及输入密码就过期了，可以通过以下命令修改超时时间。

```bash
config system global
    set remoteauthtimeout 60    //Number of seconds that the FortiGate waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. (1-300 sec, default = 5).
end
```

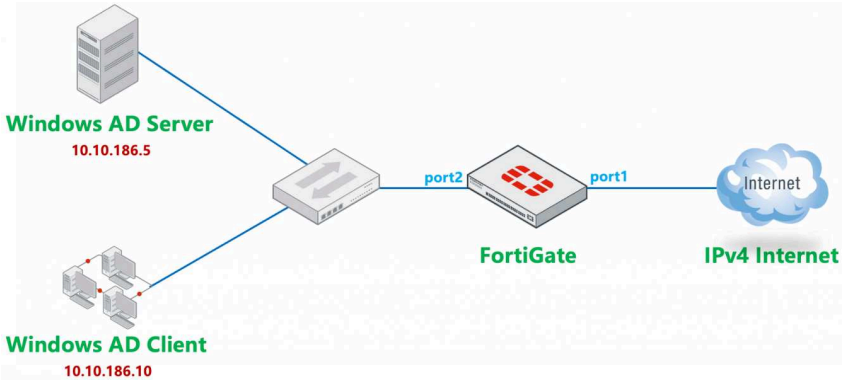

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

显式代理SAML认证（Windows ADFS）

网络需求

在防火墙上启用显示代理，并且配置基于AD FS的SAML SSO进行用户验证。

网络拓扑



1. FortiGate的LAN口port2连接Windows AD服务器和Windows AD电脑。
2. FortiGate的WAN口port1连接Internet。
3. port2上启用explicit proxy和captive portal，验证通过SAML SSO完成。SAML SSO由Windows AD服务器上的AD FS提供。
4. Windows AD电脑上设置FortiGate的port2作为上网的代理服务器。
5. 完成配置后，Windows AD服务器作为SAML IdP（提供验证服务），FortiGate作为SAML SP（发起验证请求）。

配置步骤

Windows服务器配置

1. 在本示例中，Windows AD服务器的OS是Windows 2019, version 1809。FortiGate是VM 7.0.12，SAML SSO 验证服务由Windows AD服务器上的AD FS (Active Directory Federation Service) 提供。
2. Windows AD服务器和FortiGate的时间需要在同一时区，时间差默认不能超过15秒。建议都使用NTP。可以在FortiGate上修改时间差的容忍值 ↗。

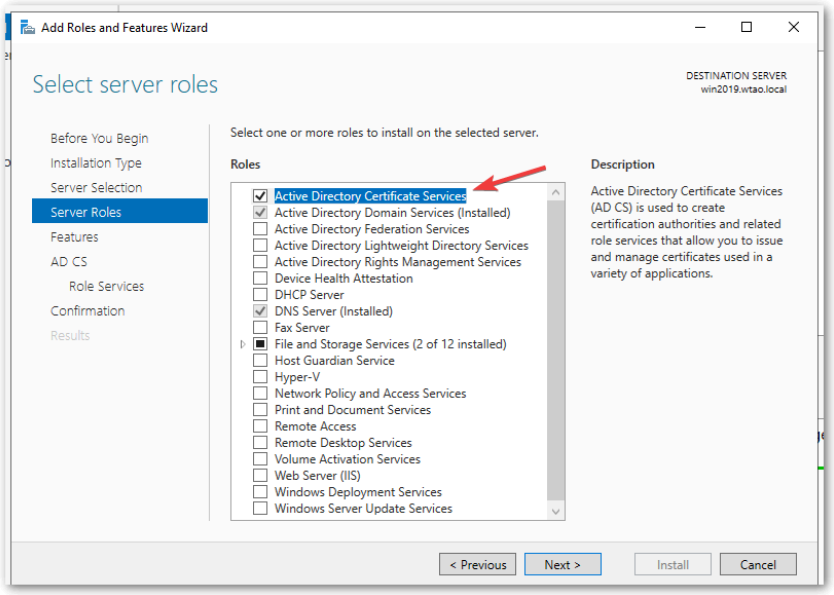
安装LDAP服务

1. LDAP服务由Active Direcotry Domain Service，或者Active Directory Lightweight Directory Services提供。
2. 在本示例中，Windows服务器10.10.186.5已经安装了Active Direcotry Domain Service。

安装AD Certificate Services证书服务

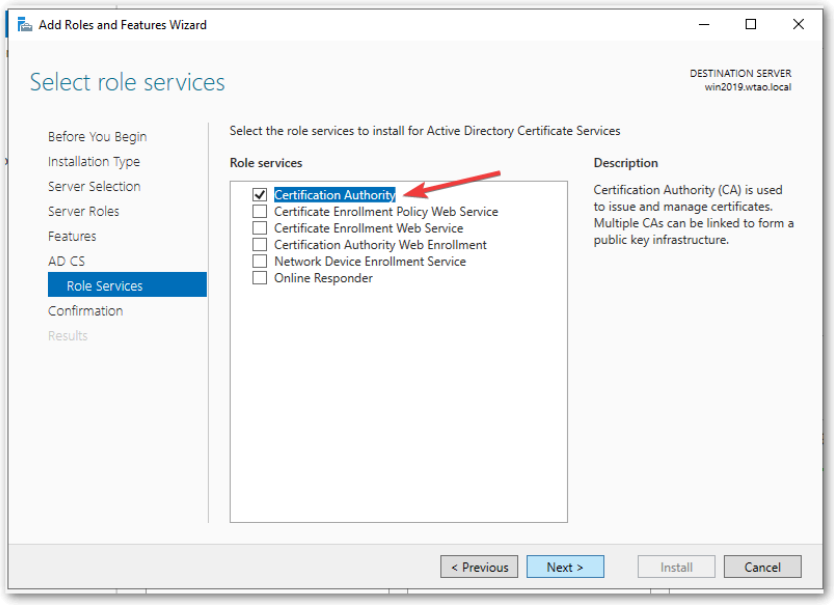
1. AD FS服务需要用到SSL证书，如果没有证书，可以在Windows Server上安装AD DC，然后在AD DC上为AD FS服务新建证书。
2. 如果你已经有供AD FS服务使用SSL证书，或者已经安装了AD DC，可以跳过这一步。
3. 你也可以使用openssl或者其他工具为AD FS服务生成证书，然后将证书导入AD FS，将CA导入Windows AD服务器。
4. 在Server Manager中安装”Active Directory Certificate Services”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. Features: 直接Next。

6. Role Services: Certification Authority。



7. 使用默认配置，完成安装。

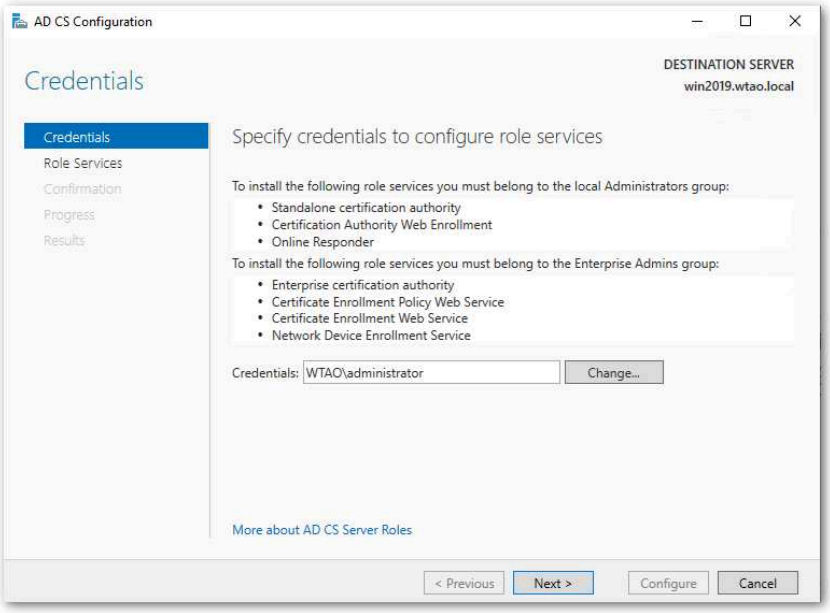
配置AD 证书服务

> **重要**
>
> 如果你已经有供AD FS服务使用SSL证书，可以跳过这一步。

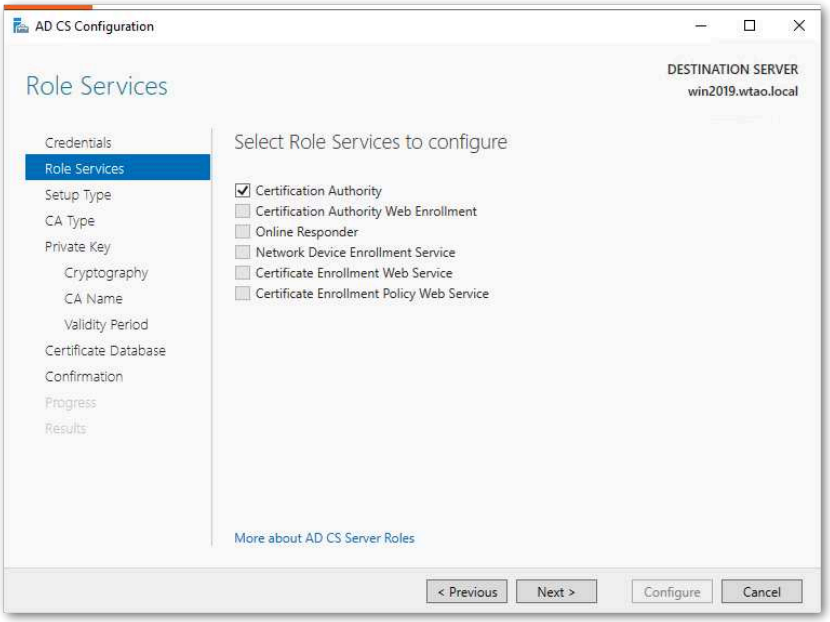
1. 打开AD CS configuration。

2. Credentials: 默认。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

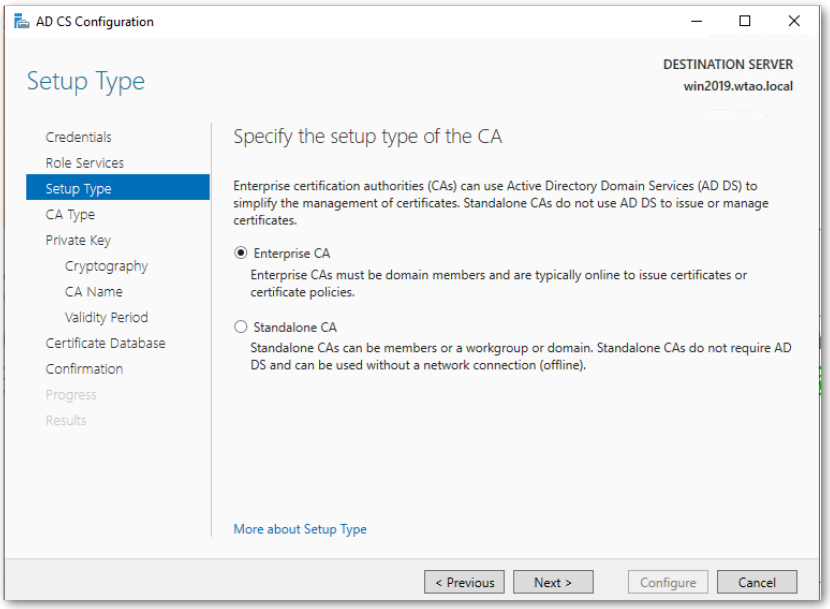


3. Role Serivces 选择Certificateion Authority。

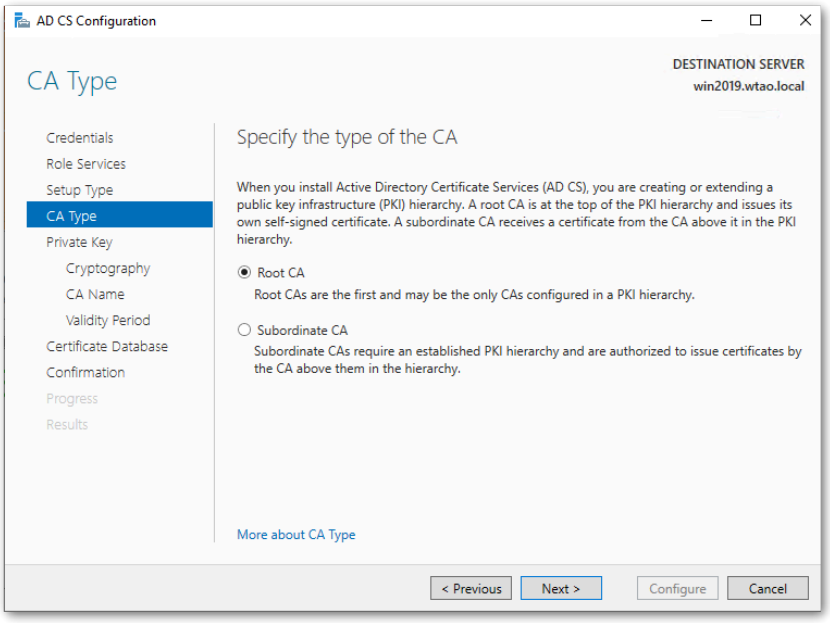


4. Setup Type 选择Enternprise CA。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

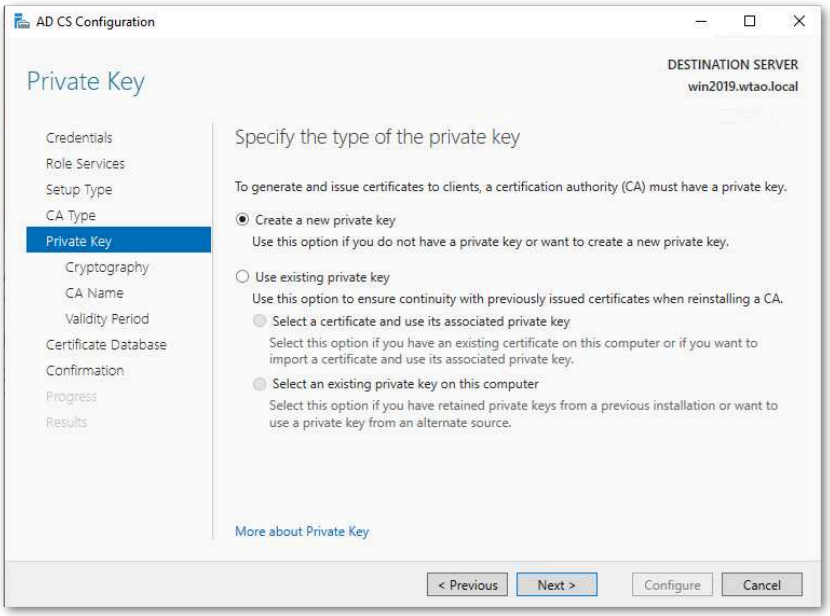


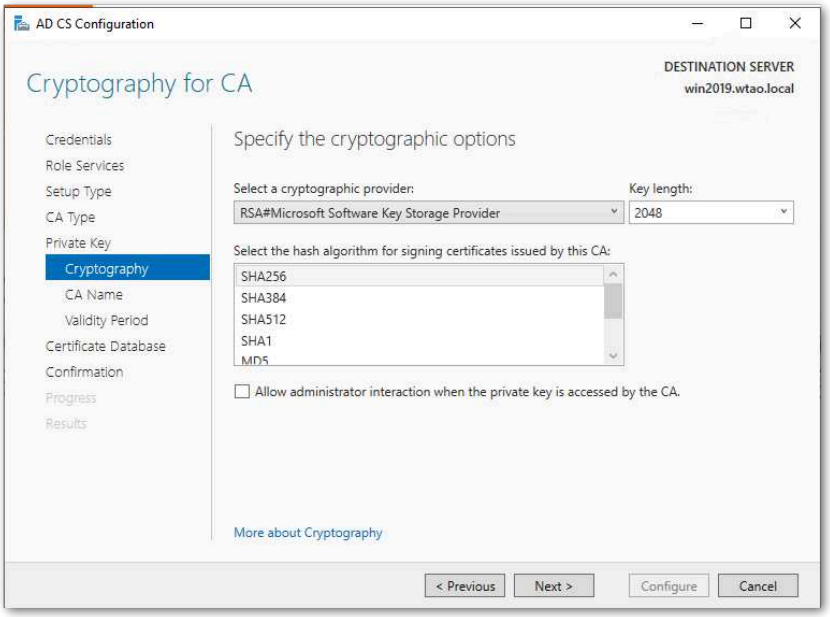
5. CA Type 选择 Root CA。

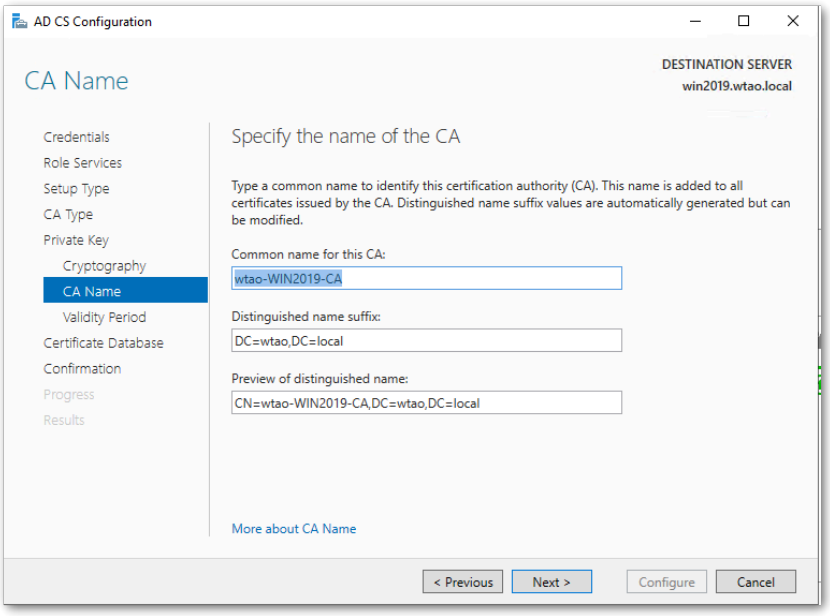


6. 使用默认配置，完成AD CS的配置。

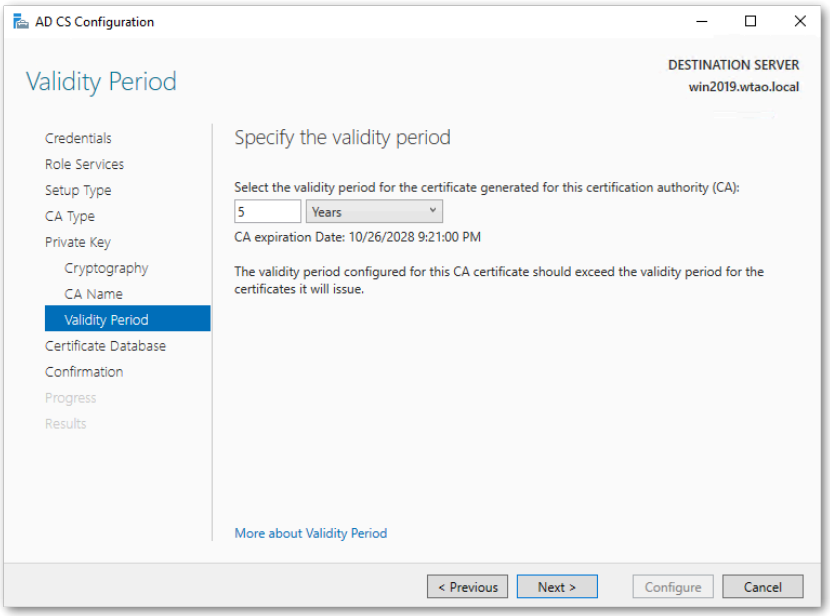
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

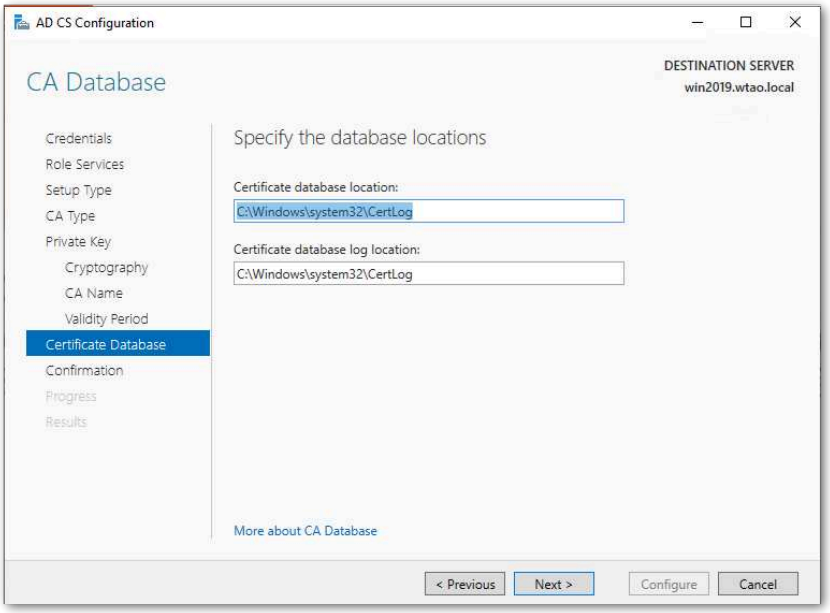


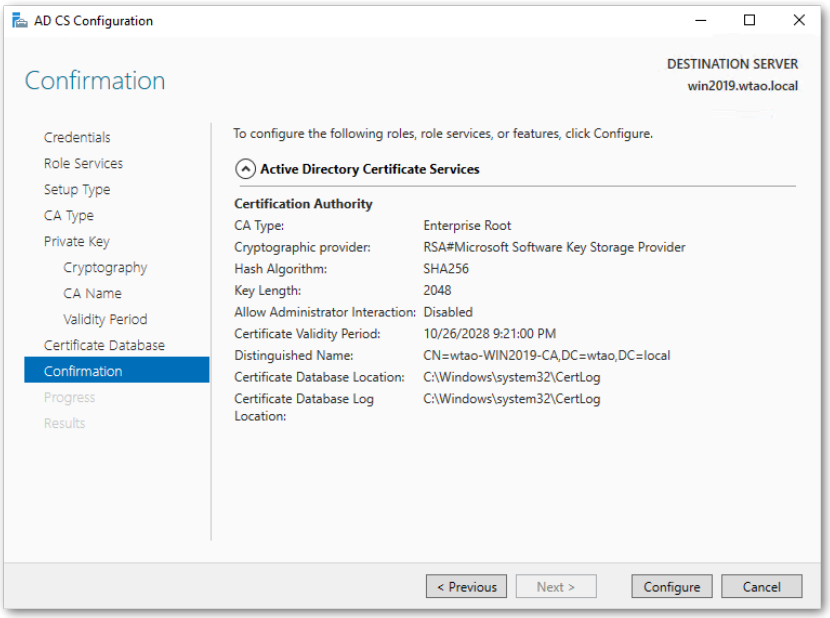




Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







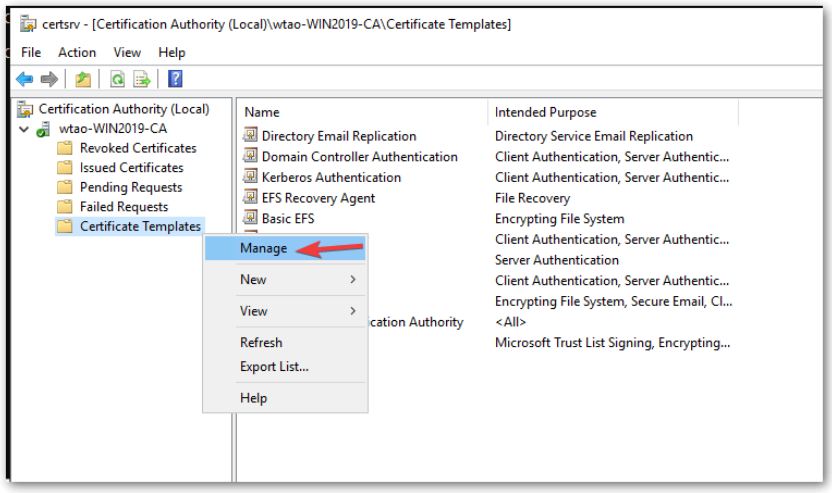
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

在AD证书服务中创建证书模板

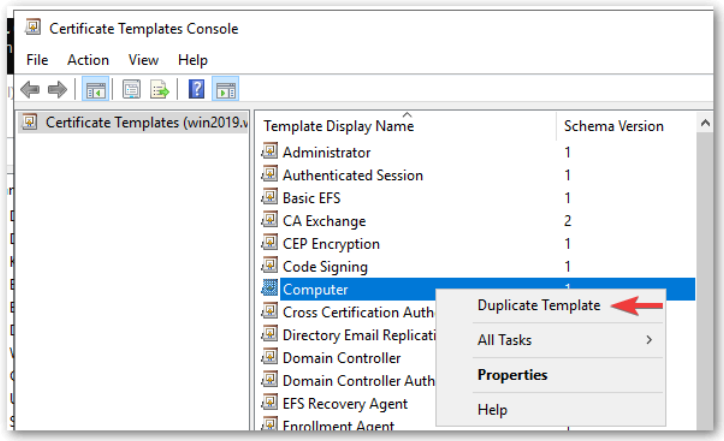
> **重要**
>
> 如果你已经有供AD FS服务使用SSL证书，可以跳过这一步。

1. 在Windows CMD中运行certsrv.msc。

2. 右键点击Certificate Templates，点击Manage。

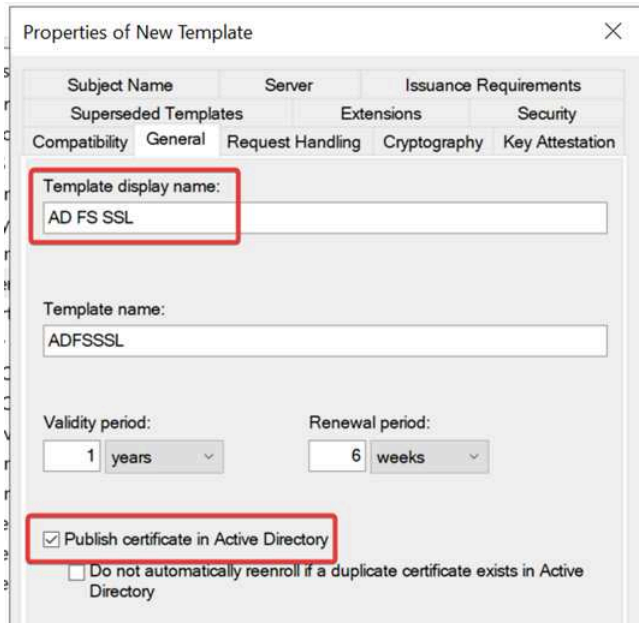


3. 右键点击Computer，点击Duplicate Template。

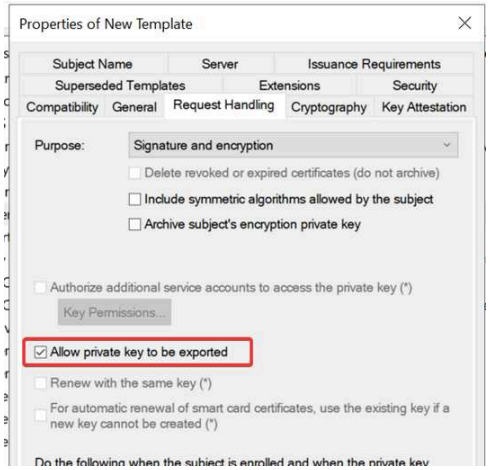


4. 在General标签页，给模板取名，并且选中”Publish certificate in Active Directory”。

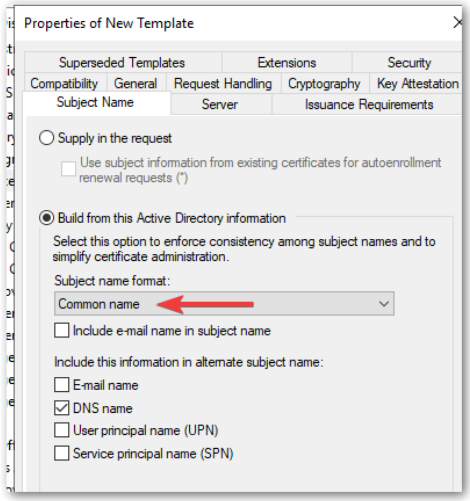
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 在Request Handling标签页，选中”Allow private key to be exported”。

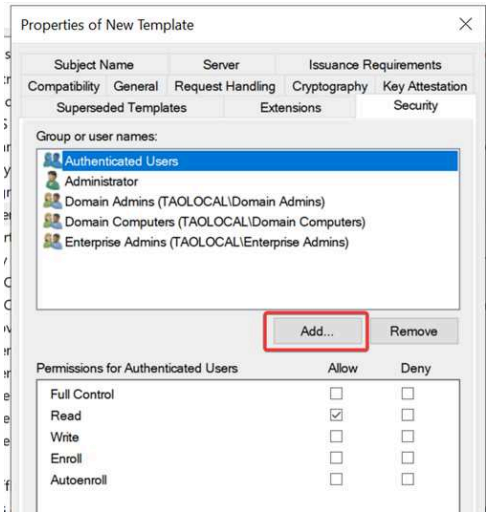


6. 在Subject Name标签页，设置Subject name format: Common name。

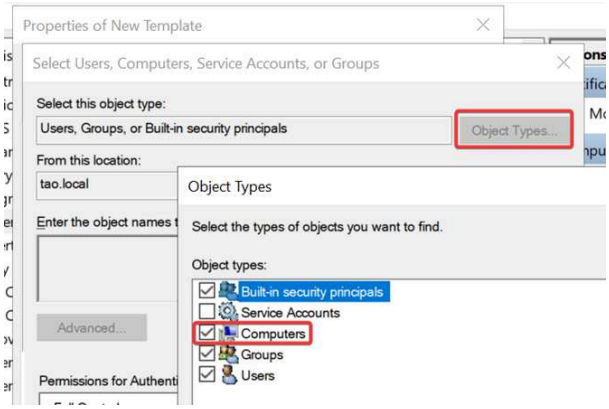


7. 在Security标签页，点击Add…。

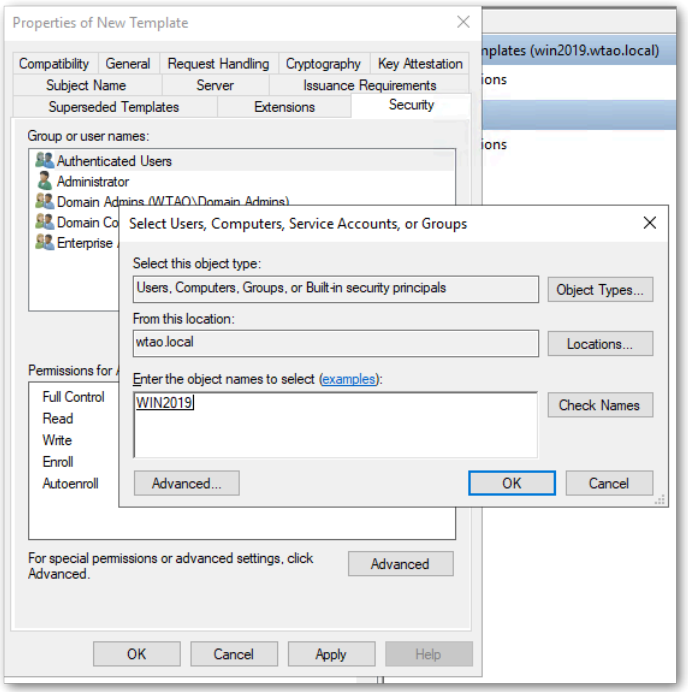
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 修改Select this object type: Computers。

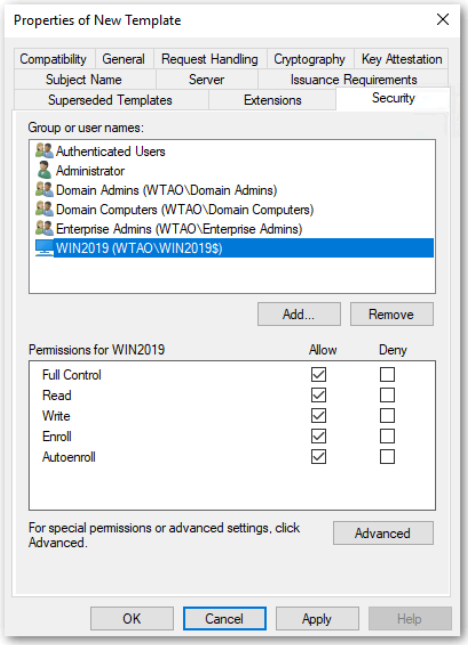


9. Enter the ojbect names to select中找到AD证书服务器。



.0. 赋予AD证书服务器Full Control。

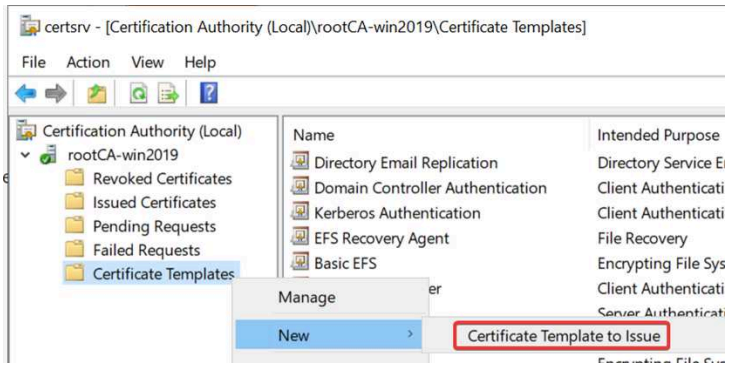
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



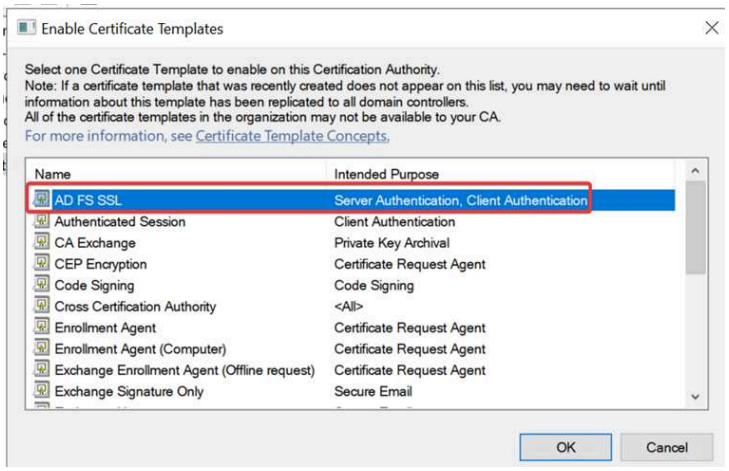
1. 点击OK完成证书模板配置。

2. 回到certsrv.msc。

3. 右键点击Certificate Templates，点击New > Certificate Template to Issue。

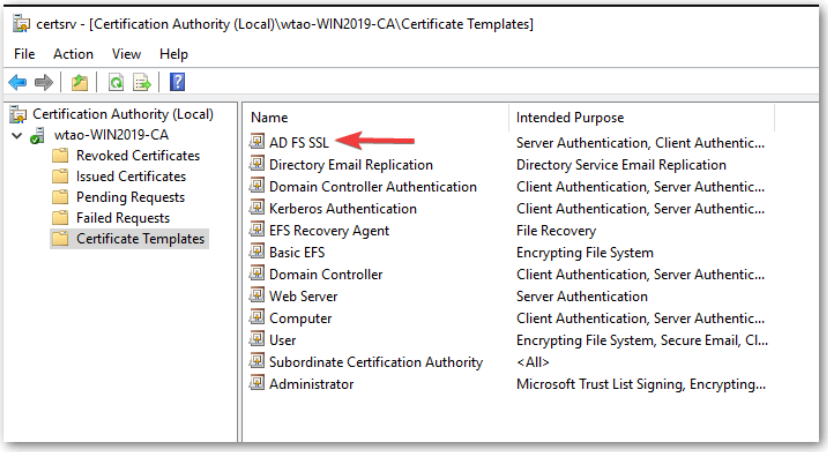


4. 选中刚才创建的证书模板。点击OK。



5. 在列表中可以看到发布的证书模板。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

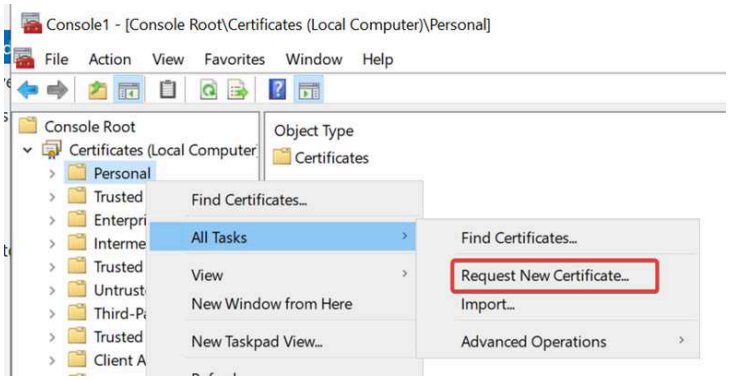


为AD FS创建证书

> **重要**
>
> 如果你已经有供AD FS服务使用SSL证书，可以跳过这一步。

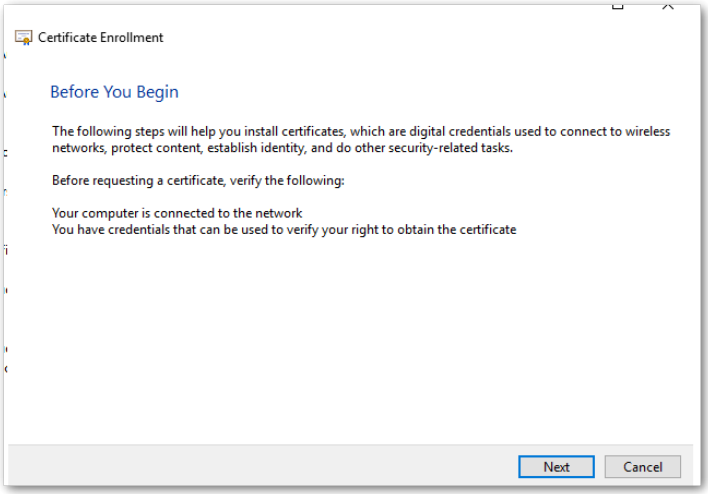
1. 在Windows CMD中运行certlm.msc。

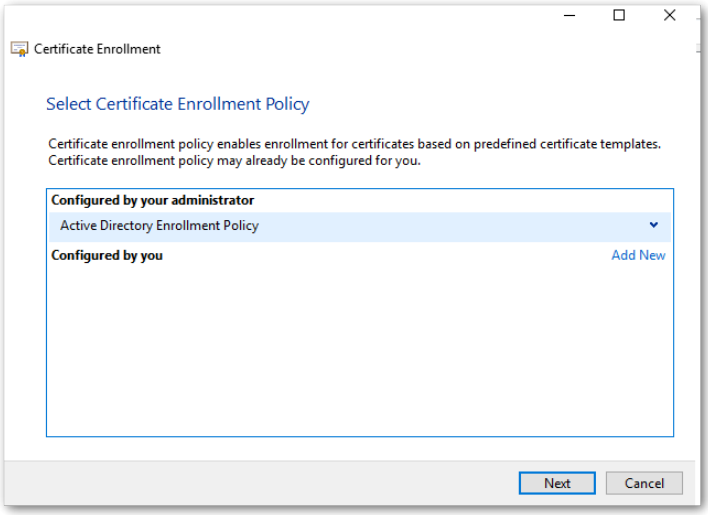
2. 右键点击Personal， 点击All Taks > Request New Certificate…



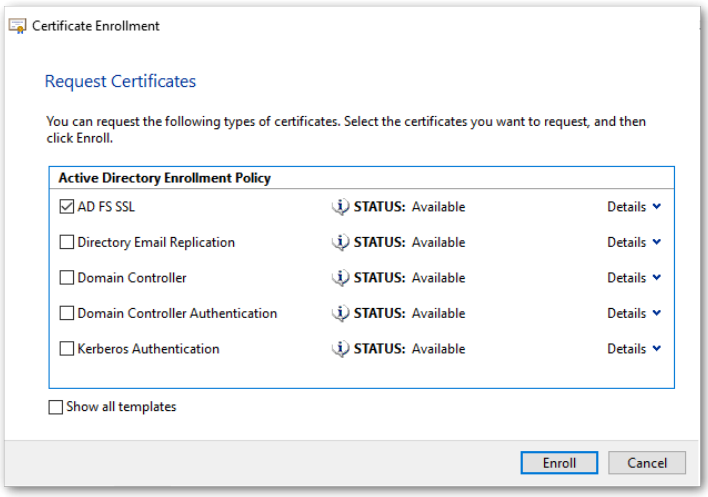
3. 点击Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



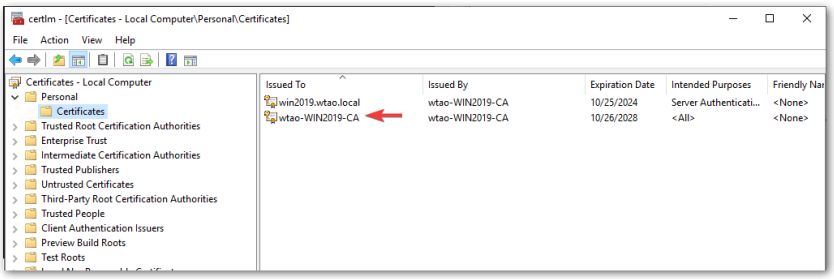


4. 选中刚才创建的证书模板，点击Enroll。



5. 可以在Personal > Certificate中看到新创建的证书，这个证书将会提供给AD FS使用。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

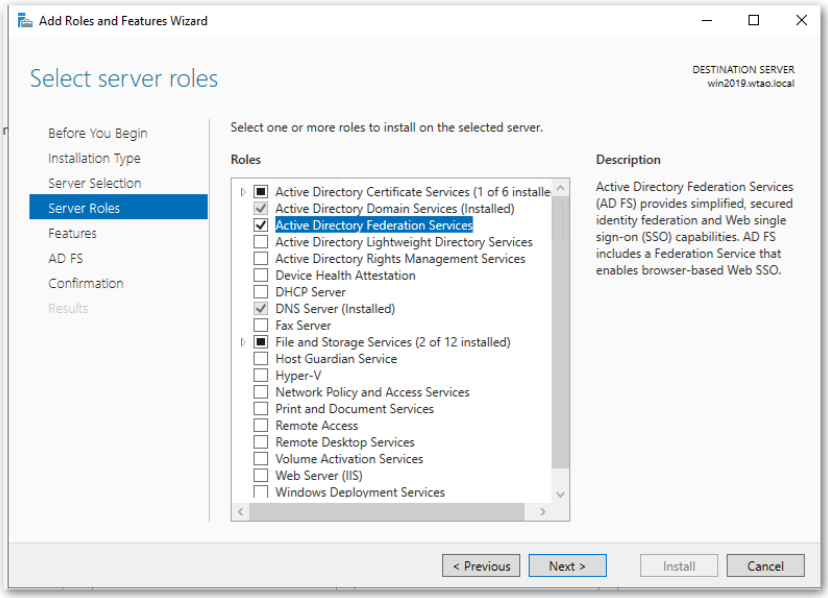


6. 这是生成的证书，供参考：AD FS SSL.cer ↗。

安装AD FS

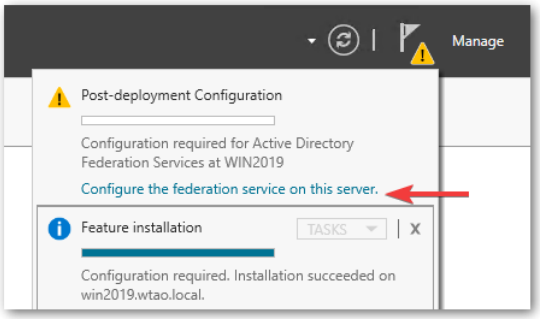
> **重要**
>
> 如果你已经安装了AD FS，可以跳过这一步。

在Server Manager中安装Active Direcotry Federation Services。选择默认配置，完成安装。



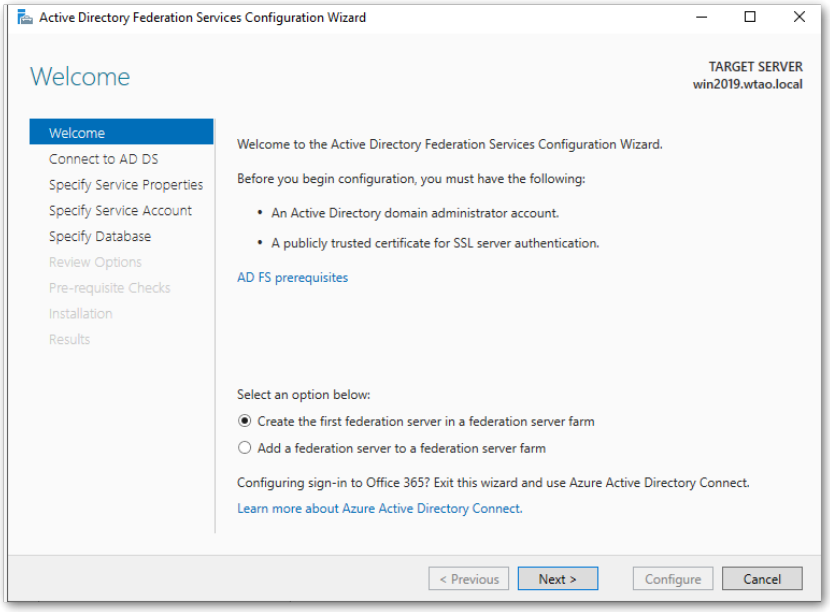
初始化AD FS

1. 在Server Manger点击Configure the federation service on this server，初始化AD FS。

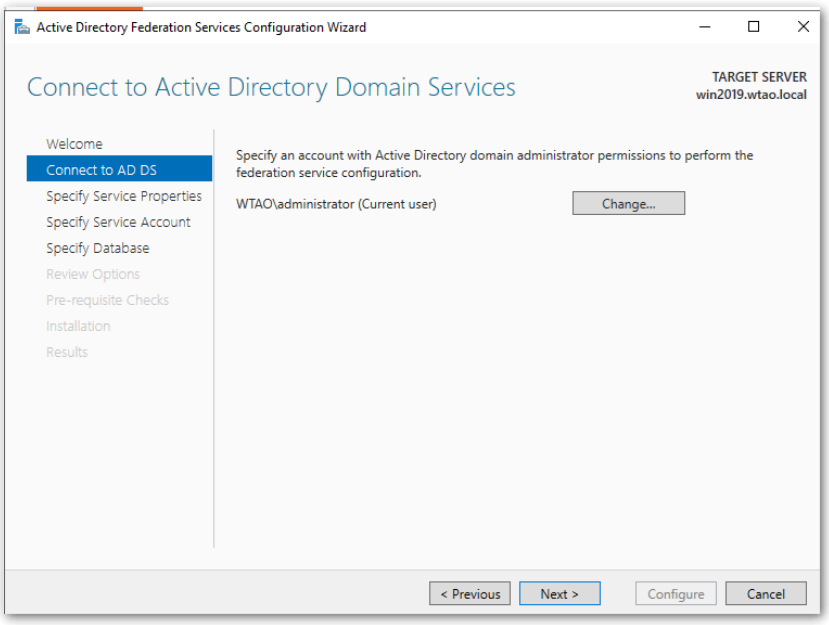


2. Welcome，保持默认。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

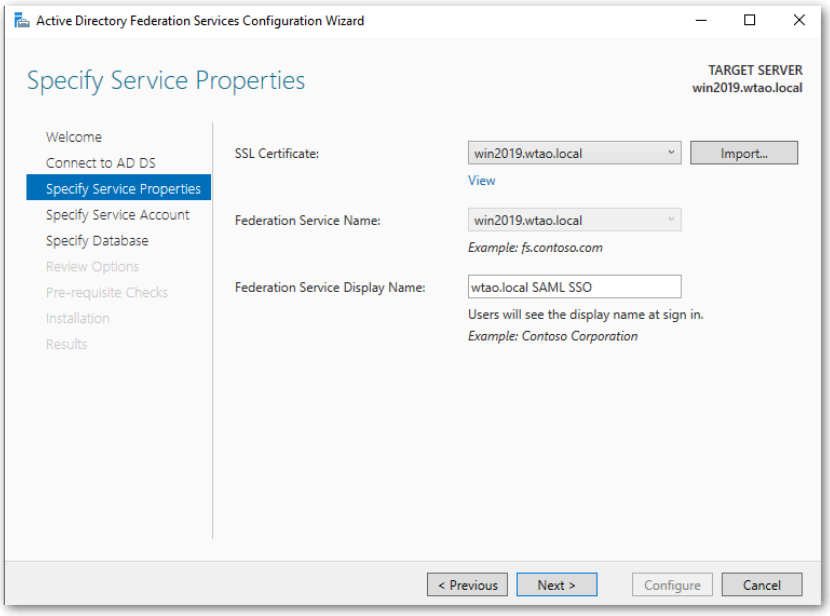


3. Connect to AD DS，保持默认。

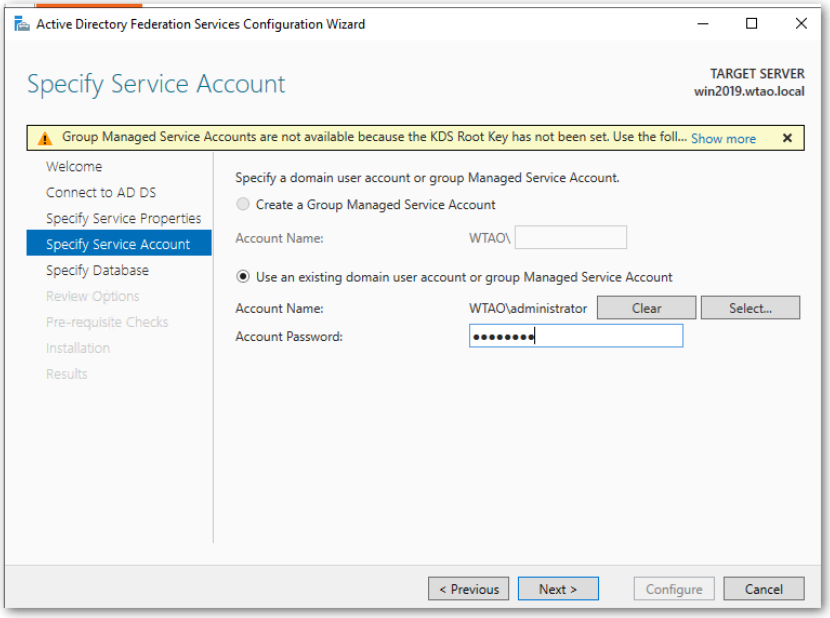


4. Specify Service Properties：SSL Certificate: 选择刚才生成的证书；Federation Service Display Name：可按需输入。这些字符将出现在SSO 登陆页面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

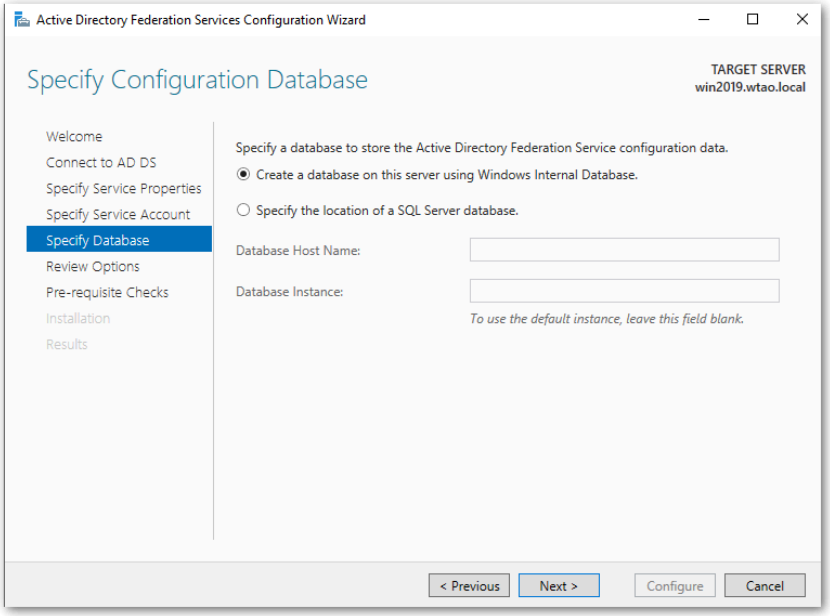


5. Specify Service Account，可以使用普通的AD user账号，也可以是AD admin账号。



6. Specify Database，创建一个数据库即可。然后Next，完成配置。

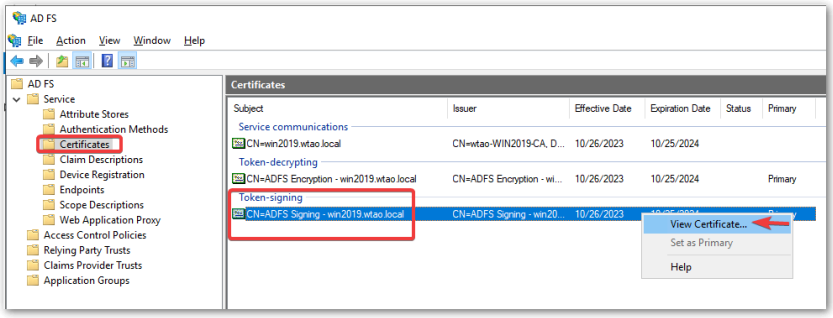
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



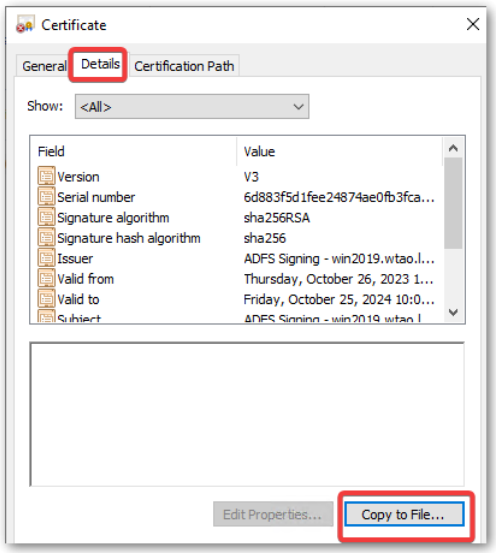
配置FortiGate作为SAML SP

导入AD FS的证书

1. 进入Windows AD FS Management，点击Service > Certificates，右键点击Token-signing的证书，点击View Certificate…



2. 在Details标签页，点击Copy to File…

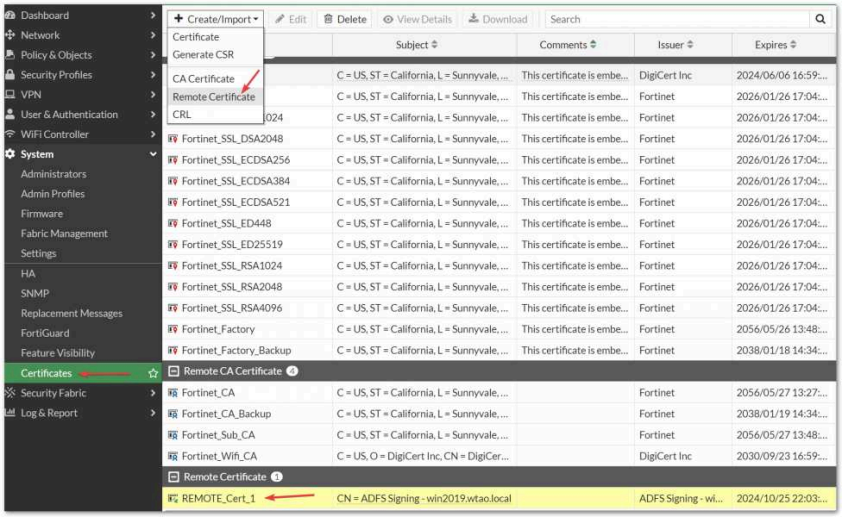


3. 以Base-64的格式保存。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 然后将证书以Remote Certificate的方式导入到防火墙。



配置user saml，输入SP 和 IdP URL

1. 现在我们可以在user saml中配置SP和IdP的 URL。

```bash
config user saml
    edit "saml_user"
        set cert "Fortinet_CA_SSL"
        set entity-id "https://fgt.wtao.local:7831/XX/YY/ZZ/saml/metadata/"
        set single-sign-on-url "https://fgt.wtao.local:7831/XX/YY/ZZ/saml/login/"
        set single-logout-url "https://fgt.wtao.local:7831/XX/YY/ZZ/saml/logout/"
        set idp-entity-id "http://win2019.wtao.local/adfs/services/trust"
        set idp-single-sign-on-url "https://win2019.wtao.local/adfs/ls/"
        set idp-single-logout-url "https://win2019.wtao.local/adfs/ls/"
        set idp-cert "REMOTE_Cert_1"
        set digest-method sha1
        set adfs-claim enable
        set user-claim-type name
        set group-claim-type group
    next
end
```

2. 配置解释：

- entity-id, single-sign-on-url, single-logout-url中写的是FortiGate的SP URL，这是由需要用到SAML SSO的服务预定义的。例如：
  - explicit proxy需要SAML SSO时，这3项是：

```jsx
# 10.10.186.1是电脑访问的，位于防火墙上的提供explicit proxy的接口IP地址。
# 它也可以是FQDN - 用户电脑、防火墙(SP)和AD FS(IdP)需要能够解析到相同的IP地址。
# 7831是固定端口
set entity-id "https://10.10.186.1:7831/XX/YY/ZZ/saml/metadata/"
set single-sign-on-url "https://10.10.186.1:7831/XX/YY/ZZ/saml/login/"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
set single-logout-url "https://10.10.186.1:7831//XX/YY/ZZ/saml/logout/"
```

- captive portal需要SAML SSO时，这3项是

```jsx
# 10.10.186.1是防火墙上进行captive portal验证的接口IP地址，1003是固定端口。
set entity-id "https://10.10.186.1:1003/remote/saml/metadata/"
set single-sign-on-url "https://10.10.186.1:1003/remote/saml/login/"
set single-logout-url "https://10.10.186.1:1003/remote/saml/logout/"
```

- SSL VPN需要SAML SSO时，这3项是

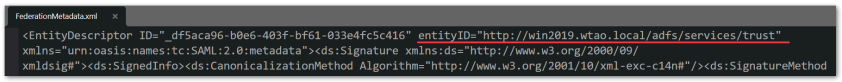
```jsx
# sslvpn.mycompany.com 是用户访问的SSL VPN地址，10443是SSL VPN服务端口
set entity-id "https://sslvpn.mycompany.com:10443/remote/saml/metadata/"
set single-sign-on-url "https://sslvpn.mycompany.com:10443/remote/saml/login/"
set single-logout-url "https://sslvpn.mycompany.com:10443/remote/saml/logout/"
```

- idp-entity-id, idp-single-sign-on-url, idp-single-logout-url写的是AD FS提供IdP服务的URL，这3个URL在AD FS安装后是固定的。所有使用AD FS的SP都是用相同的这3个URL。

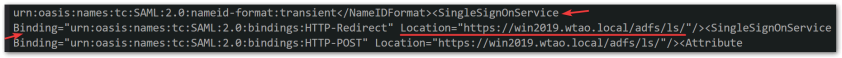
> **重要**
>
> 防火墙和用户电脑都必须能够解析AD FS的主机名。

```bash
set idp-entity-id "http://win2019.wtao.local/adfs/services/trust"
set idp-single-sign-on-url "https://win2019.wtao.local/adfs/ls/"
set idp-single-logout-url "https://win2019.wtao.local/adfs/ls/"
```

- 他们可以在AD FS的metadata file中找到（参考文档FortiGate SSL VPN Authentication with AD FS ↗），AD FS的metadata file可以在 https://win2019.wtao.local/FederationMetadata/2007-06/FederationMetadata.xml ↗ 打开。
  - *idp-entity-id*: 搜索'entityID'。



  - *idp-single-sign-on-url*: 搜索'SingleSignOnService'，找到'Binding'属性旁边的'Location'属性。



  - *idp-single-logout-url*: 搜索'SingleLogoutService'，找到'Binding'属性旁边的'Location'属性。



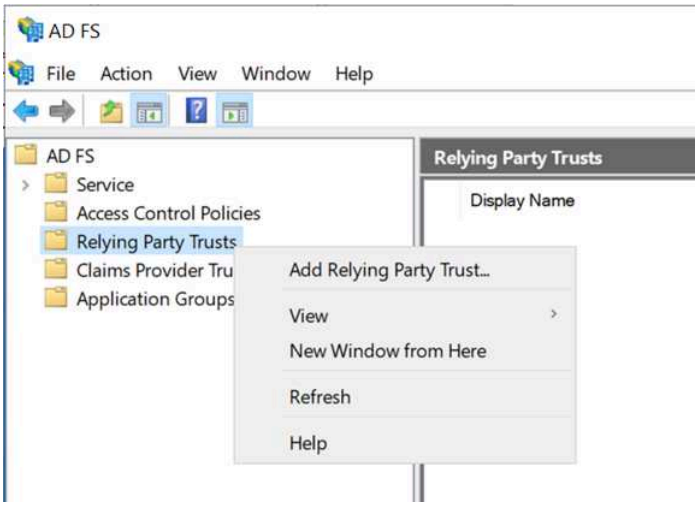
配置AD FS作为SAML IdP

AD FS上的Relying Party Trust定义了AD FS为哪个SP提供服务，当我们把防火墙配置成为SAML SP后，需要把那3个 SP URL写入到AD FS的Relying Party Trust。

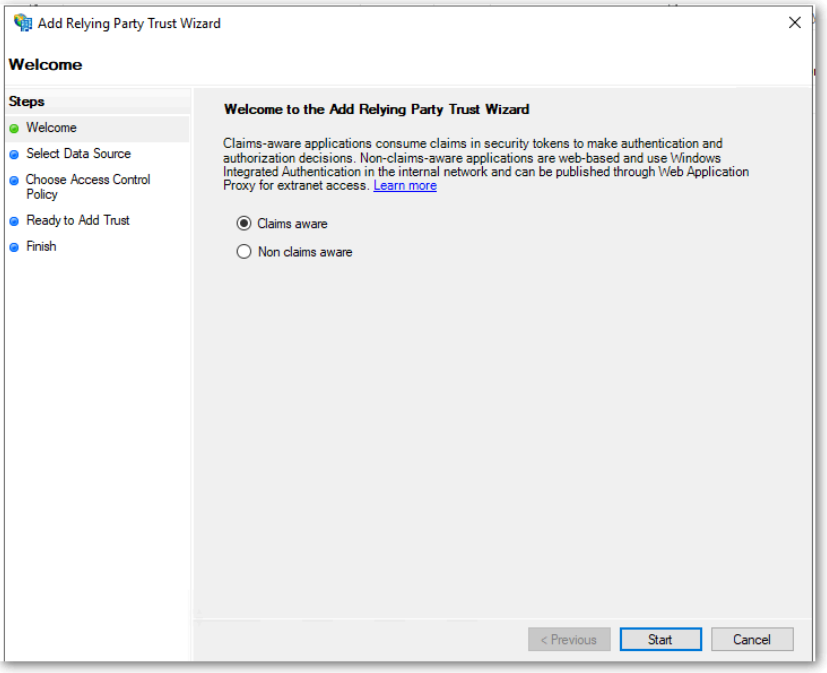
添加Relying Party Trust

1. 进入AD FS Management。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

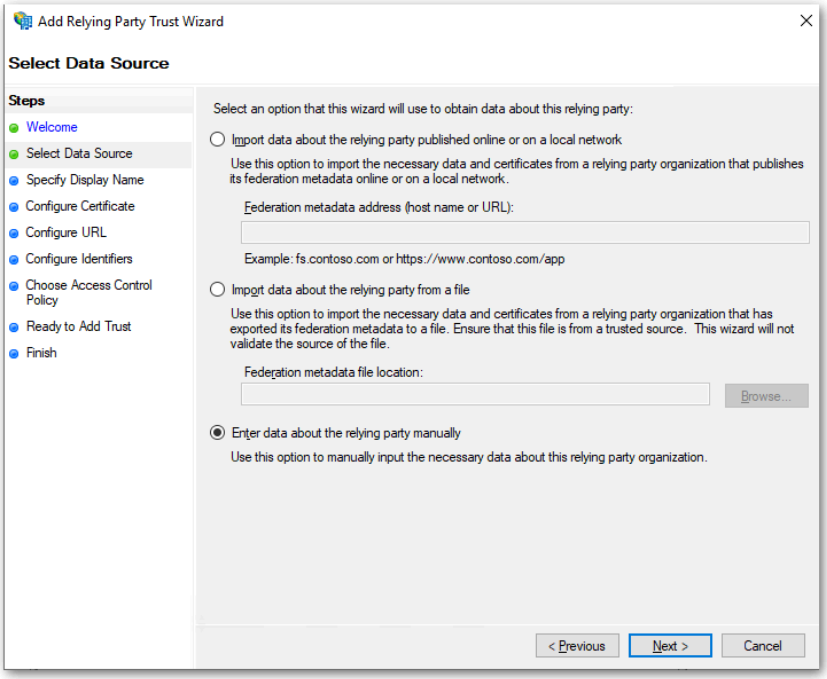


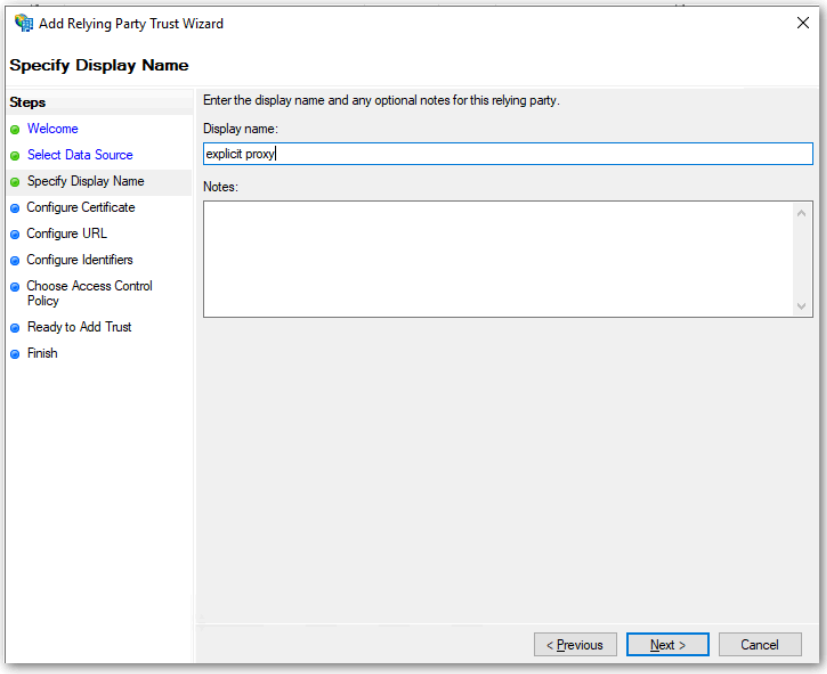
2. select 'Claims Aware' and click 'Start' 。



3. 选择 “Enter data about the relying party manually”。

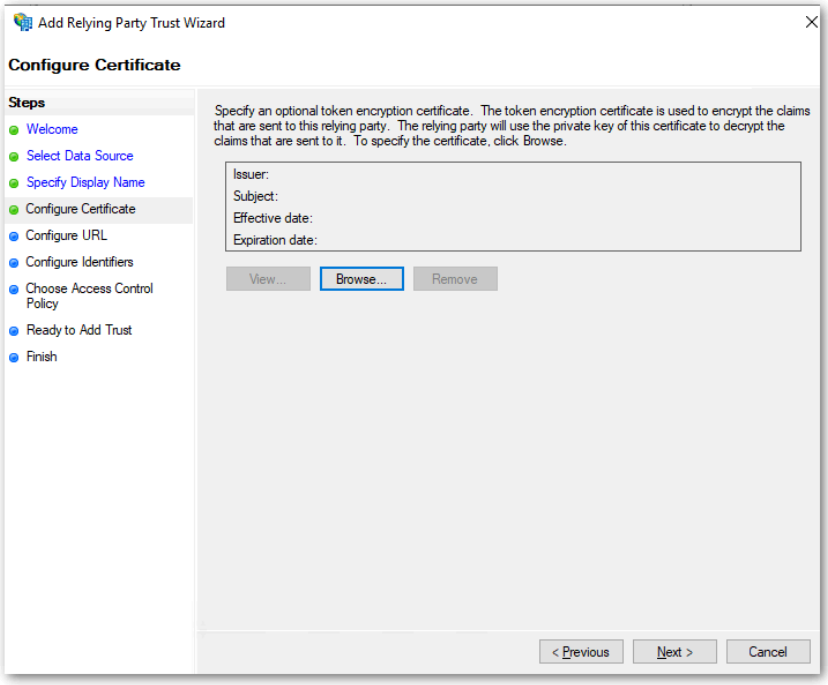
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



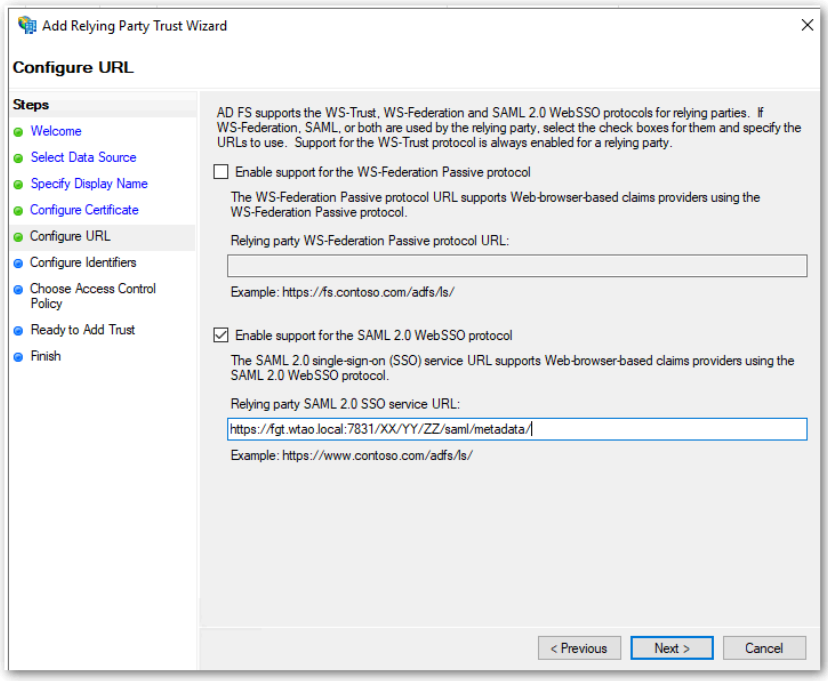


4. 保持默认，Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

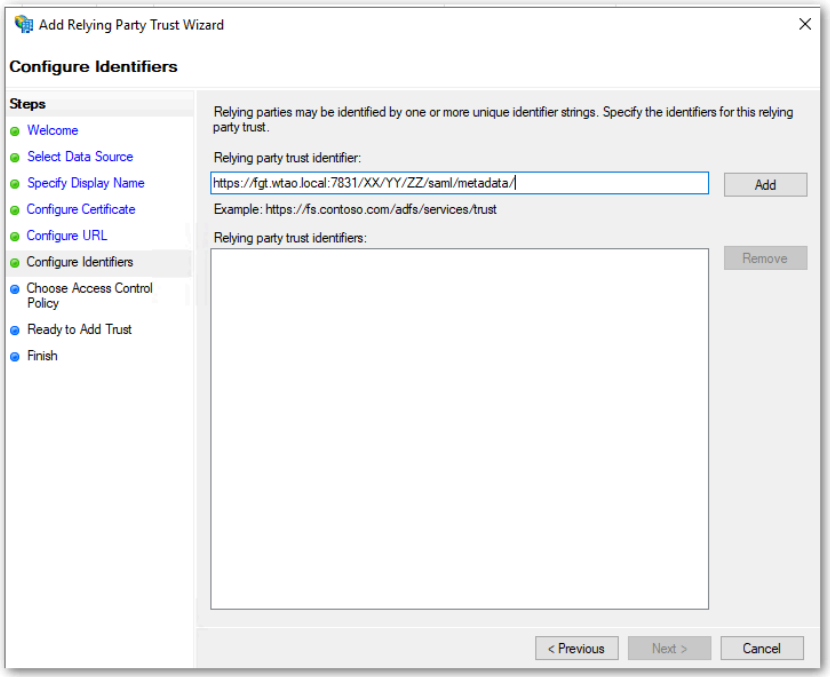


5. Configure URL, 选择”Enable support for the SAML 2.0 WebSSO protocol”，输入防火墙上user saml中的entity-id, `https://fgt.wtao.local:7831/XX/YY/ZZ/saml/metadata/`。

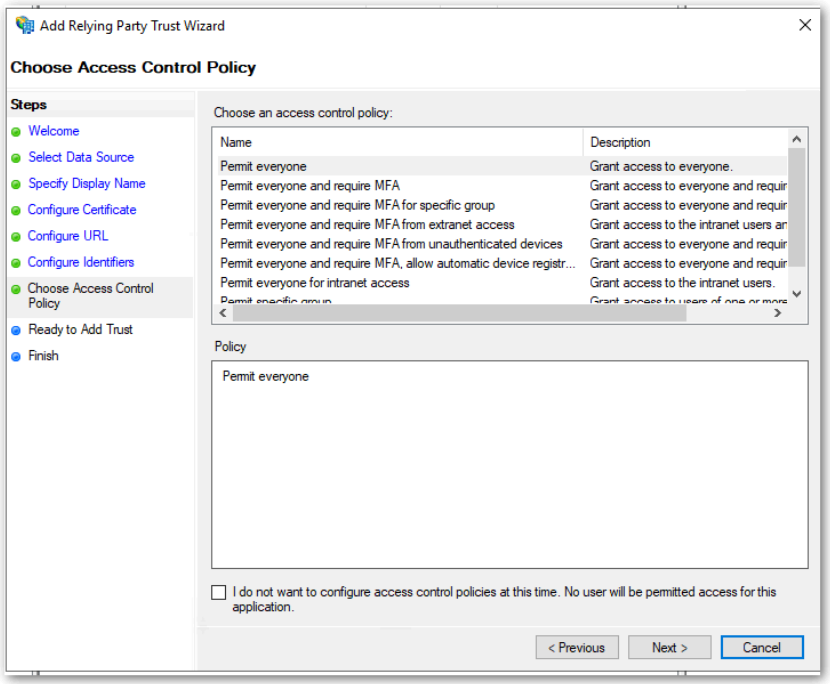


6. Configure Identifiers中，还是输入防火墙上user saml中的entity-id：`https://fgt.wtao.local:7831/XX/YY/ZZ/saml/metadata/`，点击Add，再点击Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

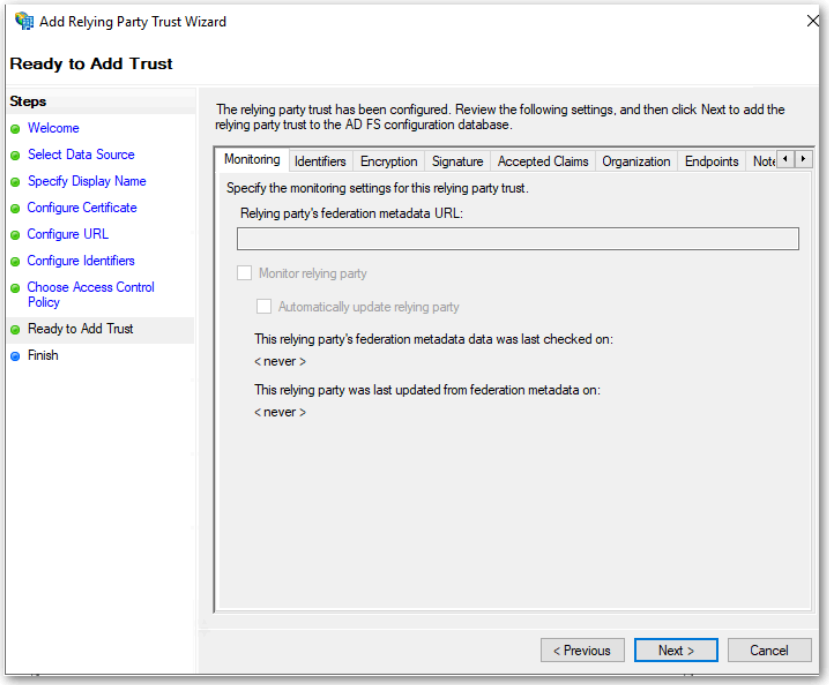


7. Choose Access Control Policy选择 Permit everyone。

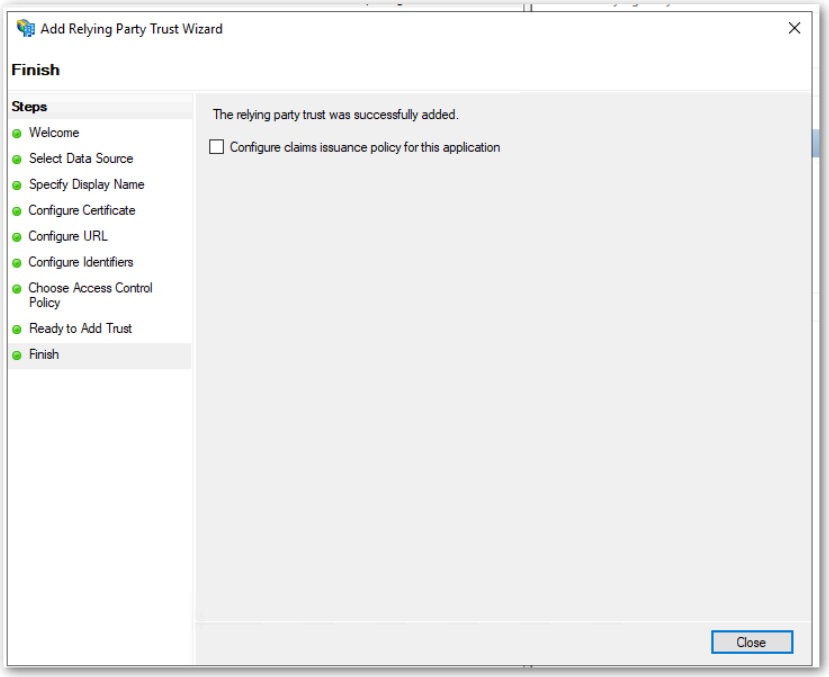


8. Ready to Add Trust，先不填写，Next。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



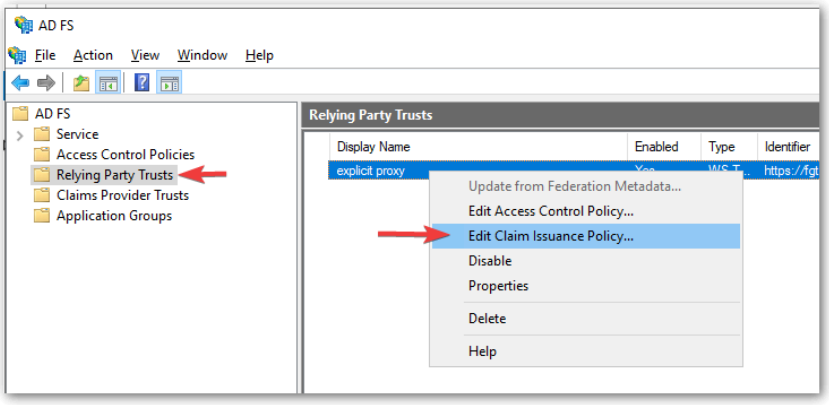
9. 取消“Configure claims issuance policy for this application”，点击Close。



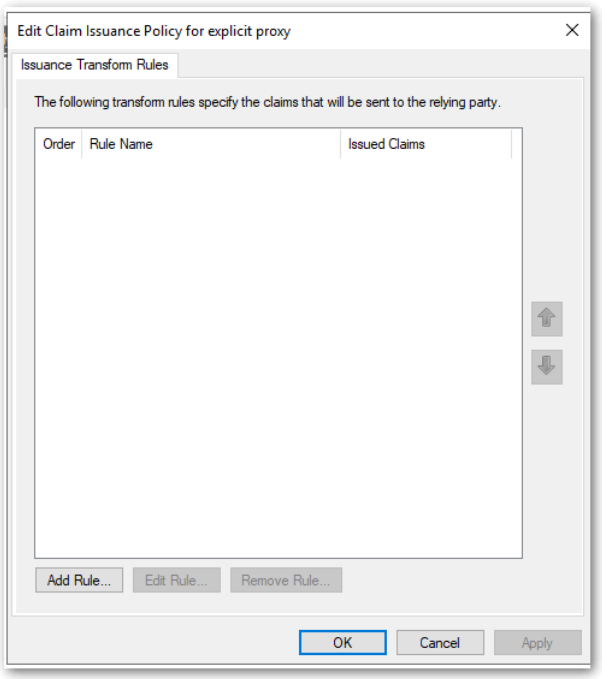
配置Relying Party Trust > Claim Issuance Policy

1. 在Relying Party Trust，右键点击刚才创建的relying party trust，点击“Edit Claim Issuance Policy”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

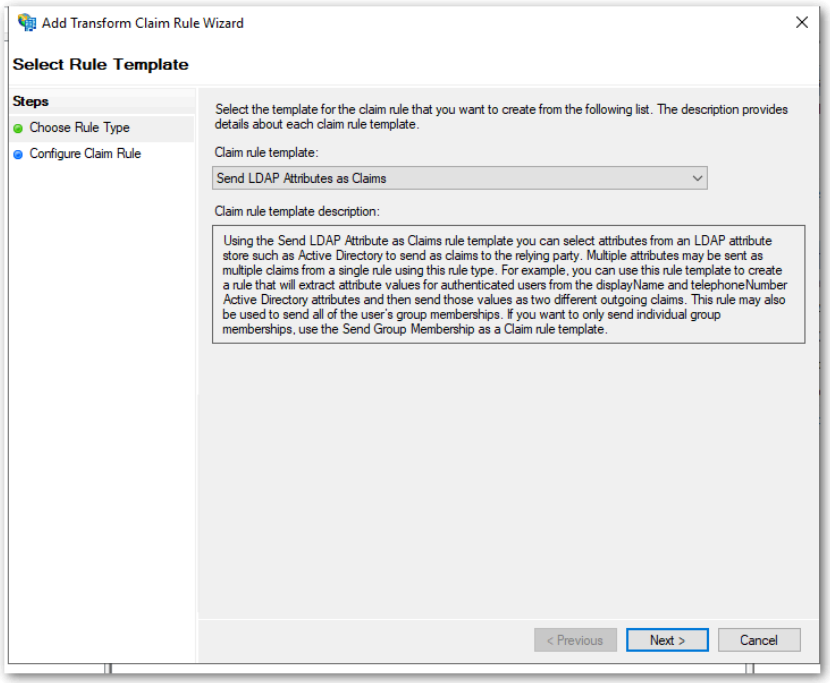


2. click on 'Add Rule'。

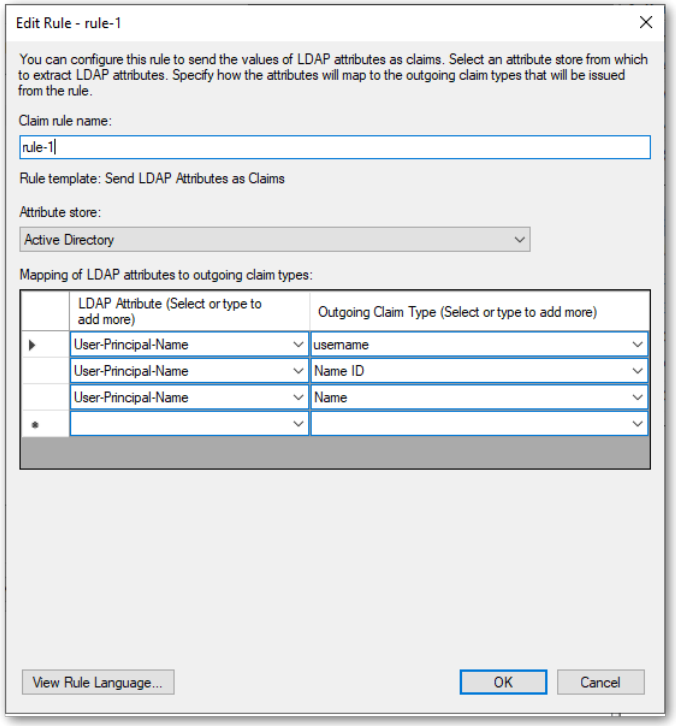


3. Claim rule template: Send LDAP Attributes as Claims。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. Configure Claim Rule：



- Claim rule name: 按需取名。
- Attribute store: Active Directory。
- Mapping of LDAP attributes to outgoing claim types:
  - User-Principal-Name: username (手动输入)
  - User-Principal-Name: Name ID （有预选项）
  - User-Principal-Name: Name（有预选项）

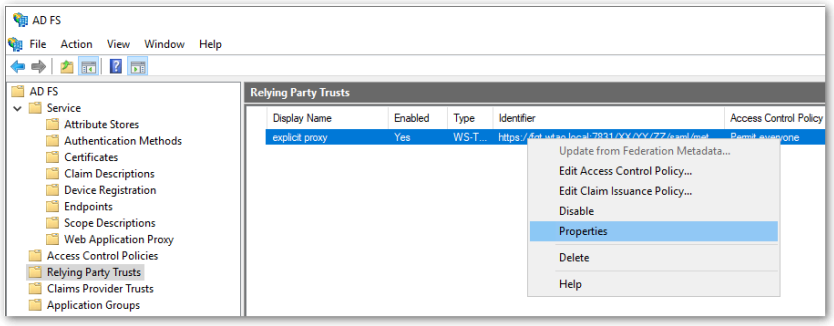
5. 点击Finish保存。

配置Relying Party Trust > SP URL

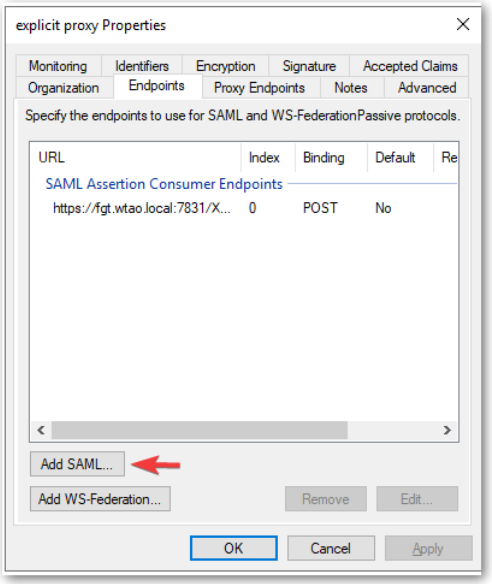
1. 在Relying Party Trust中将防火墙的SP URL输入。

2. 在Relying Party Trust，右键点击刚才创建的relying party trust，点击”Properties”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

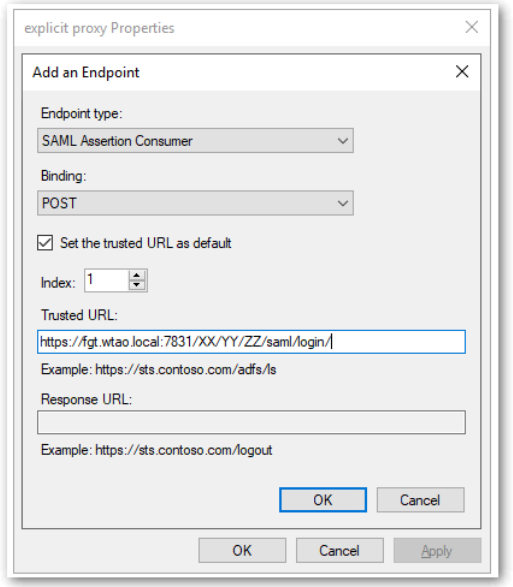


3. Endpoint标签页, 点击Add SAML…



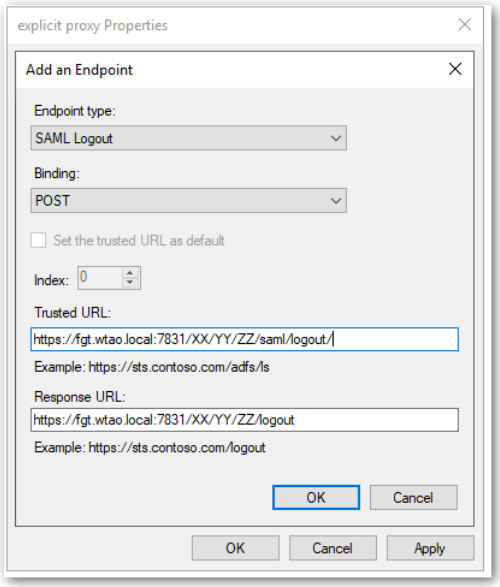
- Endpoint type: SAML Assertion Consumer
- Binding: POST
- Set the trusted URL as default: 选中
- Index: 1
- Trusted URL: 输入防火墙上user saml中的single-sign-on-url, https://fgt.wtao.local:7831/XX/YY/ZZ/saml/login/ ↗

4. 点击OK。



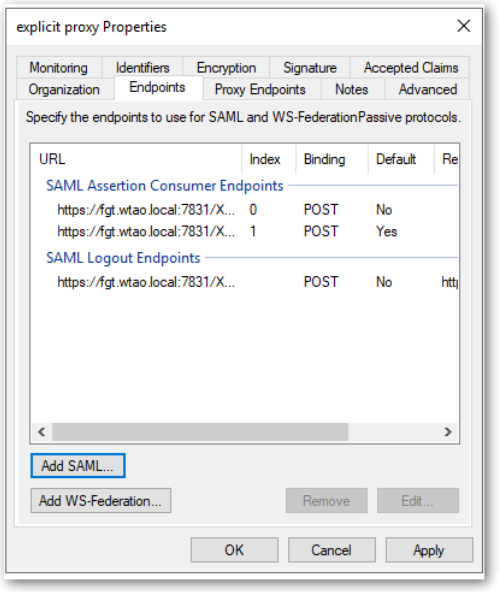
5. 再次点击Add SAML…

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



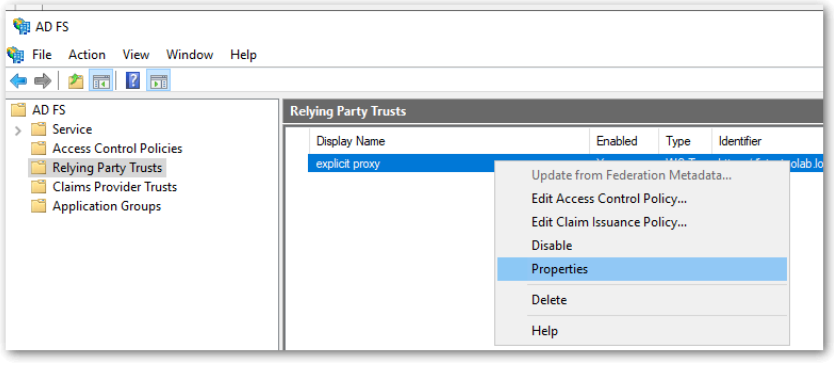
- Endpoint type: SAML Logout
- Binding: POST
- Trusted URL: 输入防火墙上user saml中的single-logout-url, https://fgt.wtao.local:7831/XX/YY/ZZ/saml/logout/
- Response URL: 如果防火墙说明文档中没有提供，可以尝试填写 https://fgt.wtao.local:7831/XX/YY/ZZ/logout

6. 点击OK，这是完成配置的Endpoitns标签页。点击OK。



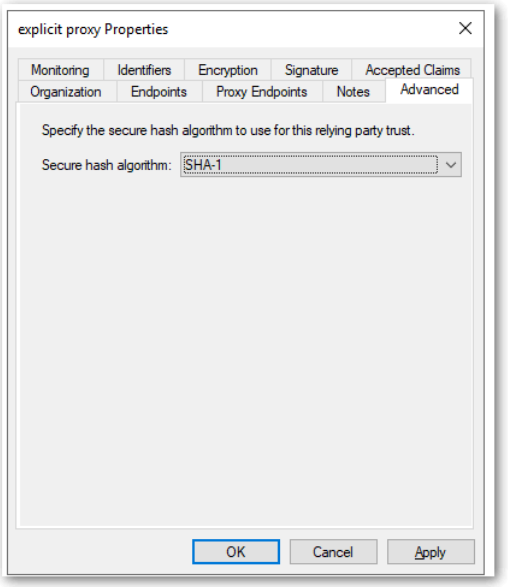
配置Relying Party Trust >SHA和防火墙证书

1. 在Relying Party Trust，右键点击刚才创建的relying party trust，点击”Properties”。



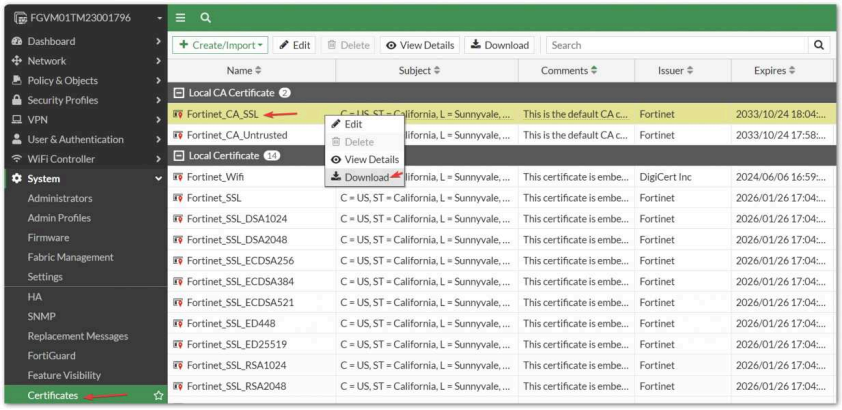
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 在Advanced标签页，将Secure hash algorithm设置为SHA-1，**和防火墙上的user saml > “set digest-method sha1” 保持一致。**

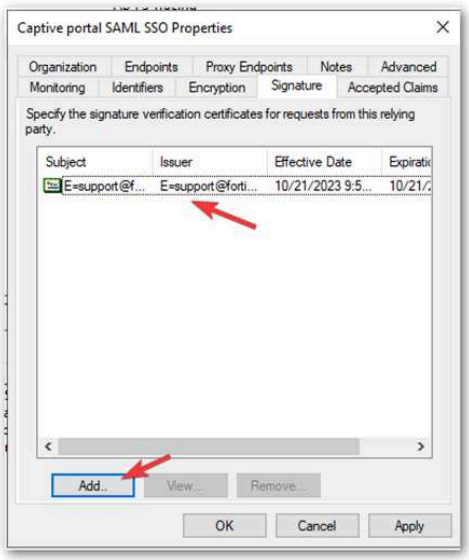


3. explicit proxy使用AD FS 作为SAML SSO时，**AD FS会验证防火墙SP URL的证书**，因此需要将防火墙上的Forinet_CA_SSL导入AD FS。

4. 在防火墙上下载Forinet_CA_SSL。



5. 在Signature标签页，导入Forinet_CA_SSL。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置FortiGate启用explicit proxy和captive portal

1. 启用explicity proxy和captive portal。在内网口port2上启用explicit-web-proxy和proxy-captive-portal。

```bash
# Enable the web proxy:
config system settings
  set gui-explicit-proxy enable
end

config web-proxy explicit
    set status enable
    set http-incoming-port 8080
    set unknown-http-version best-effort
end

# Enable the proxy captive portal:
config system interface
    edit "port2"
        set explicit-web-proxy enable
        set proxy-captive-portal enable
    next
end
```

2. 配置LDAP服务器和LDAP用户组。

```bash
# Configure the LDAP server
config user ldap
    edit "ldap-10.10.186.5"
        set server "10.10.186.5"
        set cnid "userPrincipalName"
        set dn "dc=wtao,dc=local"
        set type regular
        set username "cn=administrator,cn=users,dc=wtao,dc=local"
        set password password_of_the_user
        set group-search-base "cn=users,dc=wtao,dc=local"
    next
end

config user group
    edit "ldap-group-saml"
        set member "ldap-10.10.186.5"
    next
end
```

3. 配置authentication scheme, rule和setting。

```bash
config authentication scheme
    edit "auth_scheme_saml"
        set method saml
        set saml-server "saml_user"
        set user-database "ldap-10.10.186.5"
    next
end

config authentication rule
    edit "auth_rule_saml"
        set srcaddr "all"
        set active-auth-method "auth_scheme_saml"
    next
end

config firewall address
    edit "fgt.wtao.local"
      set type fqdn
      set fqdn "fgt.wtao.local"
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config authentication setting
    set active-auth-scheme "auth_scheme_saml"
    set captive-portal "fgt.wtao.local"
end
```

4. 配置proxy-policy。proxy-policy #2，访问Windows AD FS服务器时，不需要用户名；proxy-policy #1，访问外网时，需要用户名，触发SAML SSO验证。

```bash
config firewall address
    edit "win2019.wtao.local_IP"
        set type iprange
        set start-ip 10.10.186.5
        set end-ip 10.10.186.5
    next
end
config firewall proxy-policy
    edit 2
        set name "bypass"
        set proxy explicit-web
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "win2019.wtao.local_IP"
        set service "webproxy"
        set action accept
        set schedule "always"
        set logtraffic all
        set ssl-ssh-profile "certificate-inspection"
        set comment "no user identity is required for traffic to AD FS"
    next
    edit 1
        set name "proxy"
        set proxy explicit-web
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set schedule "always"
        set logtraffic all
        set groups "ldap-group-saml"
        set ssl-ssh-profile "certificate-inspection"
    next
end
```

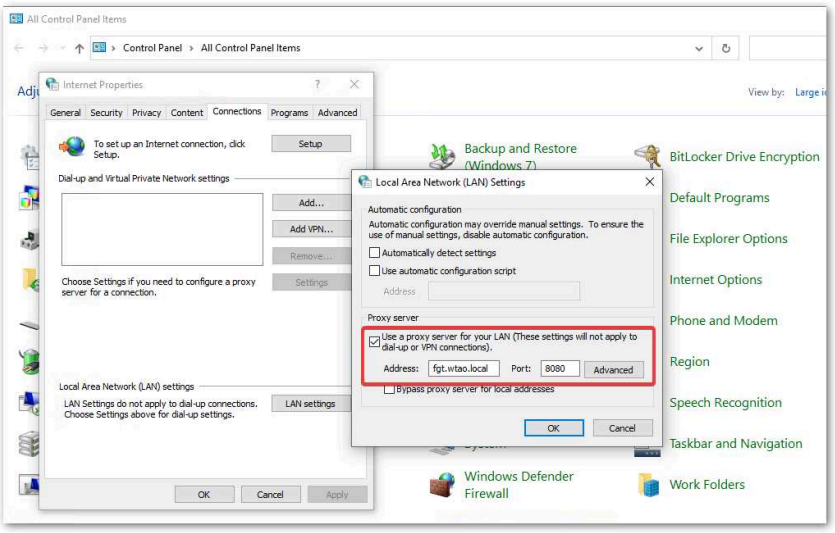
5. 配置防火墙策略。firewall policy#1，访问外网时，需要用户名。

```bash
config firewall policy
    edit 1
        set name "LANtoWAN"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set nat enable
        set groups "ldap-group-saml"
    next
end
```

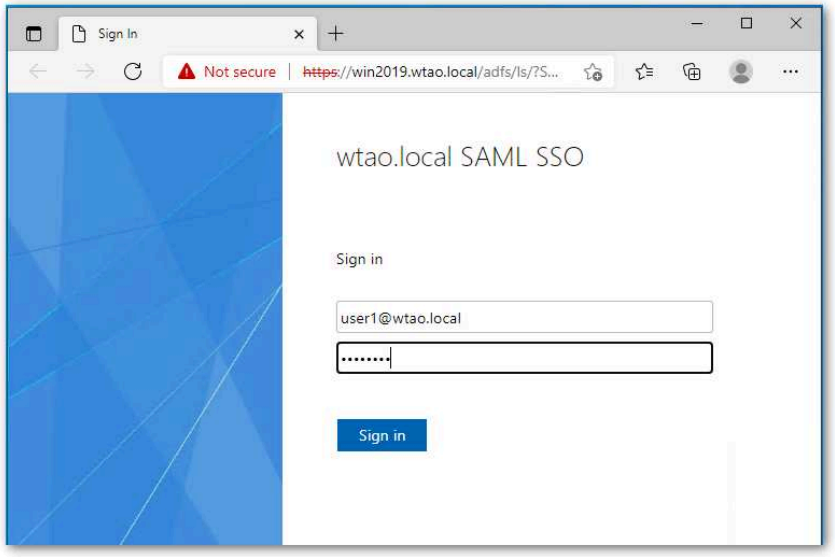
电脑上设置使用防火墙作为上网代理

1. 在Windows AD电脑上设置使用FortiGate的LAN port2作为上网代理服务器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

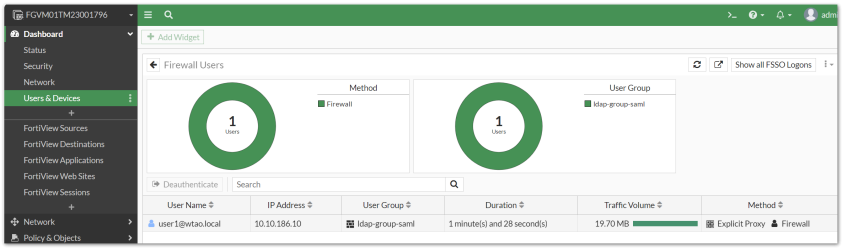


2. 当Windows AD电脑访问公网网站时，会被重定向到AD FS SAML登陆页面。登陆页面的标题文字是在”1.7 初始化AD FS”中设置的。用户名的格式是UPN (User Principal Name)。



结果验证

1. GUI > Dashboard > Users & Devices > Firewall Users显示登陆的用户。



2. diag wad user list 会显示用户详情。

```bash
FGVM01TM23001796 # diag wad user list

ID: 2, VDOM: root, IPv4: 10.10.186.10
  user name    : user1@wtao.local
  worker       : 0
  duration     : 70
  auth_type    : IP
  auth_method  : SAML
  pol_id       : 1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    g_id        : 2
    user_based  : 0
    expire      : no
    LAN:
      bytes_in=319243 bytes_out=17951352
    WAN:
      bytes_in=17925608 bytes_out=277637

  FGVM01TM23001796 #
```

故障排查

下面的错误表明在步骤“配置Relying Party Trust > Claim Issuance Policy”时，缺少User-Principal-Name: Name 的映射。加上后，问题可以解决。

```bash
Authentication failed.
user.saml.saml_user.user-name='http://schemas.xmlsoap.org/ws/2005/05/identity/claims/**name**' was NOT FOUND in the
SAML Assertion Response.
Please check with the Administrator.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

认证相关参数设置

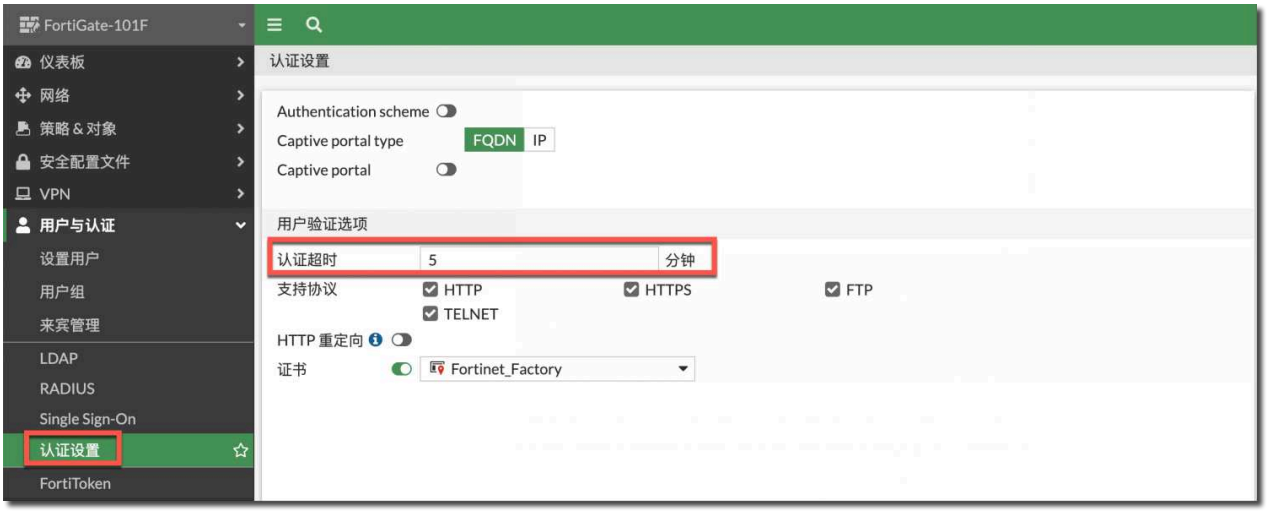
远程认证超时时间

FortiGate远程认证（如Radius、LDAP）超时的时间指的是与服务器认证过程的超时时间，认证过程的时间超过这个配置的值，FortiGate就认为认证超时。默认是5s，为了避免Radius、LDAP等远程服务器响应的数据大或者网络延时的影响，通常需要将远端超时时间调大。

```bash
config system global
    set remoteauthtimeout 120  <1-300s>
end
```

防火墙用户认证超时时间

1. 用户认证超时时间规定了经过防火墙身份验证的连接在空闲多久后需要必须重新进行身份验证。默认值为5分钟。您可以使用1到1440（24 小时）之间的数字。




```bash
config user setting
    set auth-timeout ?
        auth-timeout    Enter an integer value from <1> to <1440> (default = <5>).
end
```

2. 防火墙用户认证超时时间支持以下三种方式：

```bash
config user setting
    set auth-timeout-type ?
          idle-timeout    Idle timeout.
          hard-timeout    Hard timeout.
          new-session     New session timeout.
```

- idle-timeout（默认配置）：如果FortiGate在配置的空闲时间内未收到该用户的流量，则清除用户在线状态。
- hard-timeout：不管用户是否有流量，都会在设定的超时时间后清除用户的在线状态。
- new-session：在配置的auth-timeout计时器后，将提示用户对新会话进行身份验证，已经存在的旧会话不用被重新认证。

SSL VPN超时时间

SSL VPN空闲超时时间

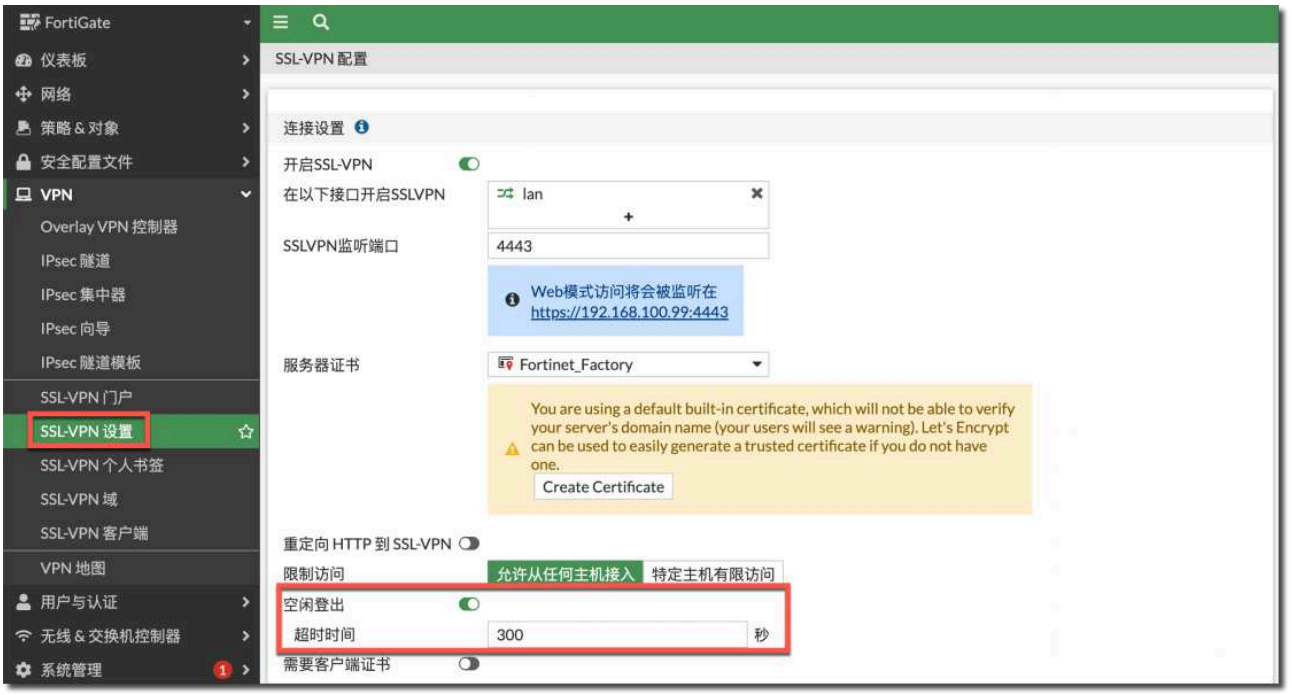
您可以设置SSL VPN用户空闲超时来控制SSL VPN用户在登录后空闲多久后需要再次认证，最大时间为259200秒（3天），默认为300秒。如果FortiGate在配置的SSL VPN空闲时间内未收到该SSL VPN用户的流量，则清除SSL VPN用户在线状态。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

SSL VPN空闲超时计时期间内，有任何的流量进入SSL VPN隧道，空闲超时都会重置。

有时候即使客户端系统没有任何的人为操作，也可能产生一些系统流量进入SSL VPN隧道，导致空闲超时重置。具体请参考：
https://community.fortinet.com/t5/FortiClient/Technical-Tip-SSL-VPN-Idle-timeout-not-working/ta-p/194568




```bash
config vpn ssl settings
    set idle-timeout ?
        idle-timeout    Enter an integer value from <0> to <259200> (default = <300>).
```

SSL VPN强制重认证超时时间

SSL VPN用户在登录后，强制重新认证的超时时间（即使客户端没有变为空闲状态）。可以将值设置为1-259200（默认为28800s，8小时），设置为0表示不会超时。

```bash
config vpn ssl settings
    set auth-timeout ?
        auth-timeout    Enter an integer value from <0> to <259200> (default = <28800>).
```

SSL VPN登录失败超时时间

```bash
config vpn ssl settings
    set login-attempt-limit ?
        <login_attempt_limit_integer>    The login-attempt-limit range is 0-10, 0 for no limit
    set login-block-time ?
        <login_block_time_integer>    The login-block-time range is 0-86400(seconds)
    set login-timeout ?
        login-timeout    Enter an integer value from <10> to <180> (default = <30>).
end
```

- login-attempt-limit：设置用户在账户失败锁定之前可以尝试的失败次数。请注意，此值是包容性的（默认值为 2，用户将在第2次登录尝试失败后被锁定），当设置为0时，永远不会因为登陆失败而锁定用户。
- login-block-time：设置用户在登录失败锁定后被锁定的时间量（以秒为单位，默认为60s），设置为0时表示不锁定（相当于login-attempt-limit设置为0的效果）。
- login-timeout：设置多次失败的登录被认为连续的时间窗口，默认为30s。例如，如果进行了一次失败登录尝试，然后在第20秒进行第2次失败的登录尝试，这两次将被视为连续的，因为它们在登录超时窗口内（即两次尝试之间的时间少于 30 秒），随后会触发FortiGate的用户锁定动作。但是，如果第二次尝试是在31秒后进行的，则不会被FortiGate视为连续尝试，也不会发生锁定。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

防火墙认证不绑定MAC地址

默认用户通过防火墙认证后，FortiGate会记录客户端的MAC地址，并将客户端认证信息与MAC地址绑定，当客户端MAC地址变化后，会导致认证失败，如果想关闭防火墙认证绑定MAC地址的功能（例如认证时的源MAC与认证成功后实际流量的源MAC不一致的场景），可以通过如下CLI实现（默认为开启状态）：

```bash
config user setting
    set auth-src-mac disable
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

认证与策略顺序的关系

网络需求

1. 源地址为192.168.100.77/32、192.168.100.78/32的PC需要经过防火墙认证才能访问Internet。
2. 其他源IP不需要防火墙认证就可以直接访问Internet。

配置步骤

1. 在FortiGate上配置防火墙认证的用户与用户组。

```bash
config user local
    edit "user1"
        set type password
        set passwd xxxxxx
    next
    edit "user2"
        set type password
        set passwd xxxxxx
    next
end

config user group
    edit "Auth_Users"
        set member "user1" "user2"
    next
end
```

2. 创建第1条上网策略，源IP为192.168.100.77/32、192.168.100.78/32，用户选择用户组`Auth_Users`，目标为all，开启SNAT。



3. 在步骤2的策略下创建第2条上网策略，源IP为192.168.100.0/24，不选择用户，目标为all，开启SNAT。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



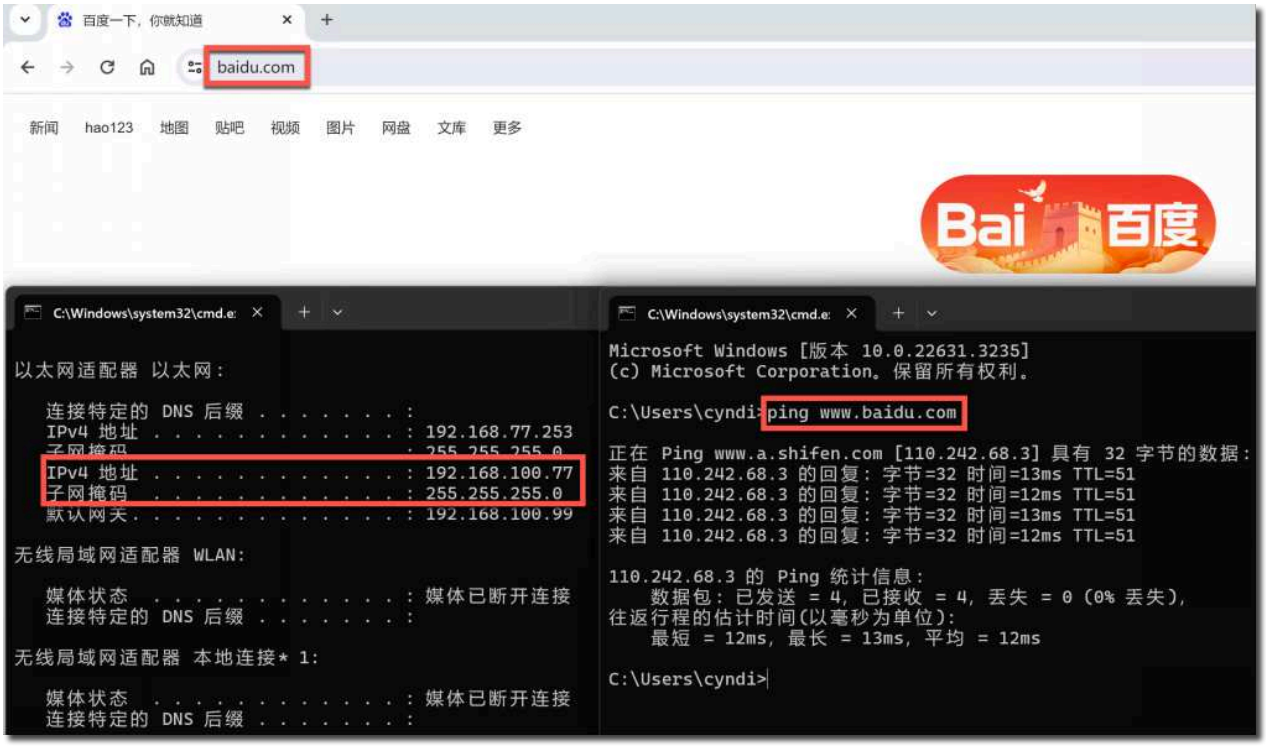



```bash
config firewall policy
    edit 17
        set srcintf "internal5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "192.168.100.77/32" "192.168.100.78/32"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set groups "Auth_Users"
    next
    edit 1
        set srcintf "internal5"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "192.168.100.0/24"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

结果验证

1. 192.168.100.77/32、192.168.100.78/32与192.168.100.0/24的其他PC都不需要防火墙认证，可以直接访问Internet，这显然与用户的需求是不一致的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 对应会话显示匹配的策略为ID 1（配置的第2条其他网段的上网策略），没有认证标记。

```bash
session info: proto=6 proto_state=01 duration=2 expire=3597 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu synced f00    //未包含auth标记//
statistic(bytes/packets/allow_err): org=92/2/1 reply=52/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=12->5/5->12 gwy=172.22.6.1/10.10.12.2
hook=post dir=org act=snat 192.168.100.77:18489->110.242.68.4:443(172.22.6.128:40598)
hook=pre dir=reply act=dnat 110.242.68.4:443->172.22.6.128:40598(192.168.100.77:18489)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=e0:23:ff:67:e3:9c
misc=0 policy_id=1 //匹配策略ID 17// pol_uuid_idx=636 auth_info=0 chk_client_info=0 vd=0
serial=013c33e2 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=3 sdwan_service_id=1
rpdb_link_id=ff000001 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/71, ipid=71/64, vlan=0x0000/0x0000
vlifid=71/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=1/3
```

解决办法

1. 默认配置下，**未认证的流量**经过FortiGate时，允许匹配开启认证的策略（ID 17）后的防火墙策略，由于开启认证的策略（ID 17）后的策略（ID 1）为整个网段的上网策略，且未开启认证，所以需要认证的流量就可以匹配策略ID 1直接访问Internet。

2. 默认情况，该特性配置如下，`auth-on-demand` 的模式为 `implicitly`。

```bash
FortiGate # config user setting
FortiGate (setting) # set auth-on-demand ?
always        Always trigger firewall authentication on demand.
implicitly    Implicitly trigger firewall authentication on demand.
```

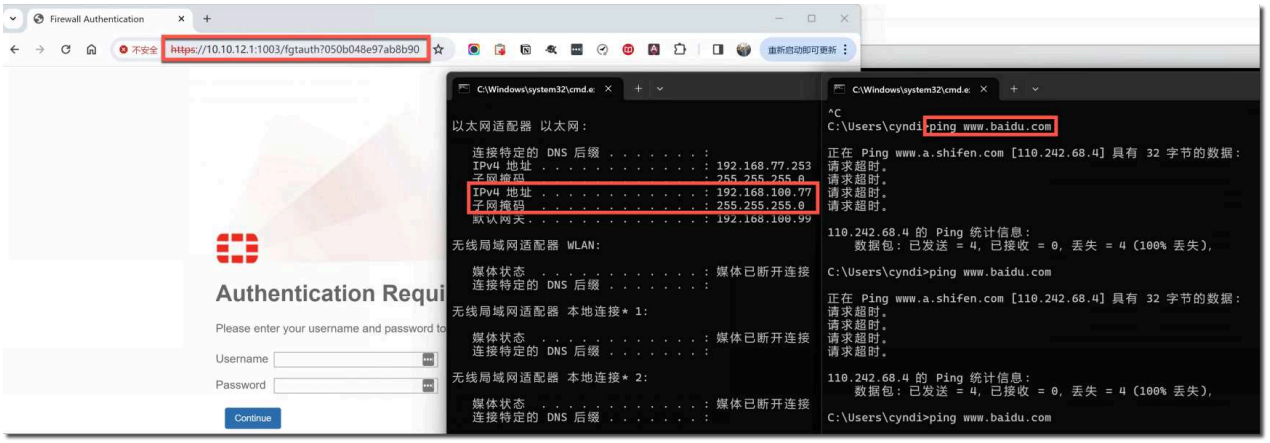
- `always`：按照策略配置的顺序来触发防火墙身份验证，如果**未认证流量**已经匹配上认证策略，则**未认证流量**不会匹配认证策略后的其他策略（需要强制认证，认证通过后，**已认证流量**可以匹配认证策略后的其他策略），如果**未认证流量**没有匹配上开启认证的策略，则会按照顺序继续匹配认证策略后的其他策略。
- `implicitly`：默认配置。隐式触发防火墙身份验证，**未认证的流量**也可以匹配认证策略下的其他策略，如果认证策略后有其他可以匹配的策略，则没有经过认证也可以匹配其他策略放通。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 想要实现此用户的需求，需要将`auth-on-demand`的模式修改为`always`，表示按照策略配置的顺序来触发防火墙身份验证：

```
config user setting
    set auth-on-demand always
end
```

4. 再次使用192.168.100.77/32访问Internet，弹出了认证页面。

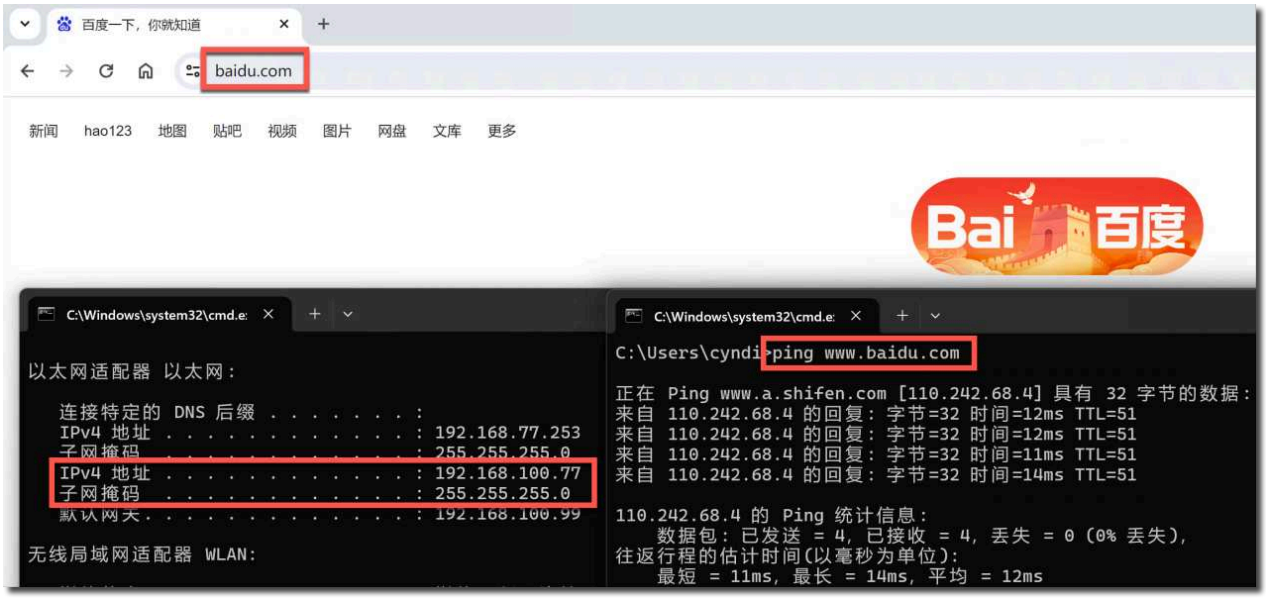


5. 查看会话需要认证的流量匹配了策略ID 17，也就是配置的第1条认证策略，会话中有`auth`标记。

```bash
session info: proto=6 proto_state=05 duration=0 expire=0 timeout=3600 flags=00000004 socktype=4 sockport=10100
av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=redir log local may_dirty auth npu synced f00    //包含auth标记//
statistic(bytes/packets/allow_err): org=0/0/0 reply=6945/9/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=12->5/5->12 gwy=172.22.6.1/0.0.0.0
hook=pre dir=org act=noop 192.168.100.77:19011->110.242.68.4:443(0.0.0.0:0)
hook=post dir=reply act=noop 110.242.68.4:443->192.168.100.77:19011(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=e0:23:ff:67:e3:9c
misc=0 policy_id=17 //匹配策略ID 17// pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=0
serial=013d220f tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=3 sdwan_service_id=1
rpdb_link_id=ff000001 ngfwid=n/a
npu_state=0x4000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  redir-to-av auth    //提示重定向到认证模块//
```

6. 认证成功后，192.168.100.77/32可以正常访问Internet。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 会话状态的auth标记变为authed，匹配的策略ID仍为认证策略17。

```bash
session info: proto=6 proto_state=01 duration=3 expire=3596 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=user1 state=log may_dirty npu authed synced f00 acct-ext    //包含authed标记//
statistic(bytes/packets/allow_err): org=92/2/1 reply=52/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=12->5/5->12 gwy=172.22.6.1/10.10.12.2
hook=post dir=org act=snat 192.168.100.77:19231->110.242.68.4:443(172.22.6.128:19231)
hook=pre dir=reply act=dnat 110.242.68.4:443->172.22.6.128:19231(192.168.100.77:19231)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=e0:23:ff:67:e3:9c
misc=0 policy_id=17 //匹配策略ID 17// pol_uuid_idx=643 auth_info=3 chk_client_info=0 vd=0
serial=013d776b tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=3 sdwan_service_id=1
rpdb_link_id=ff000001 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=64/71, ipid=71/64, vlan=0x0000/0x0000
vlifid=71/64, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Web认证弹出2个页面

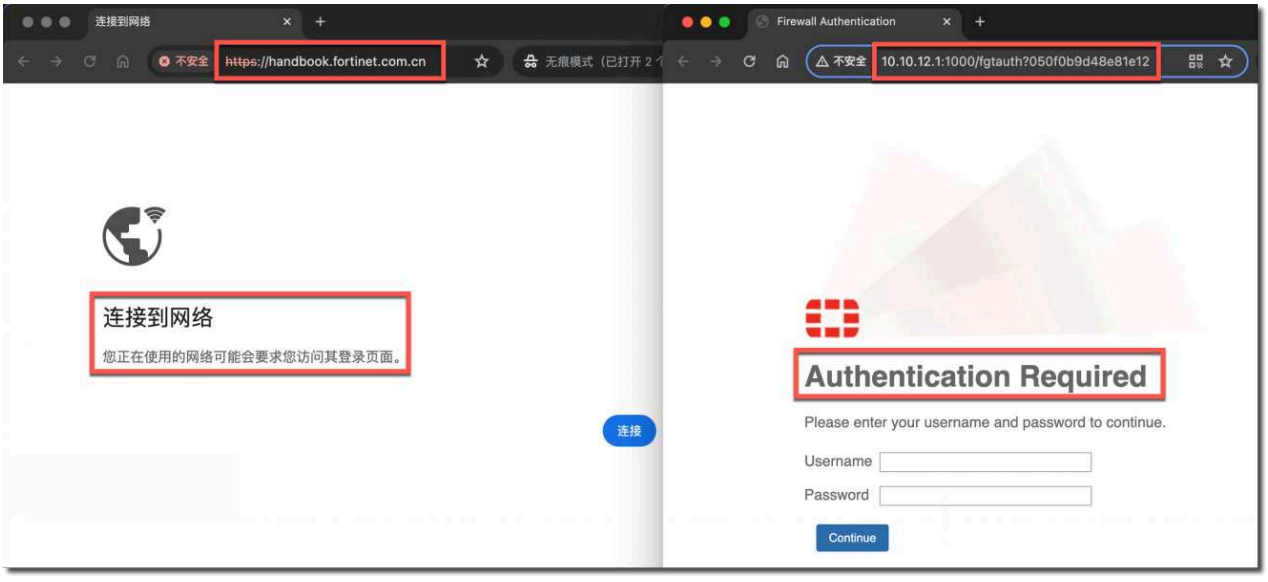
问题现象

1. 用户配置了防火墙Web认证，用户与用户组配置如下，认证相关配置（`config user setting`）均为默认配置，使用上网的防火墙策略引用用户组。

```bash
config user local
    edit "user1"
        set type password
        set passwd xxxxxx
    next
end

config user group
    edit "Auth_Users"
        set member "user1"
    next
end

config user setting
end

config firewall policy
    edit 1
        set name "LAN_to_Internet"
        set srcintf "internal5"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
        set groups "Auth_Users"
    next
end
```

2. 内网PC使用浏览器（以Chrome为例）以HTTPS的URL格式访问Internet网站（例如`https://handbook.fortinet.com.cn`）时，会弹出2个页面，1个页面提示“连接到网络”，另一个为防火墙认证页面（理论上只应弹出认证页面）。

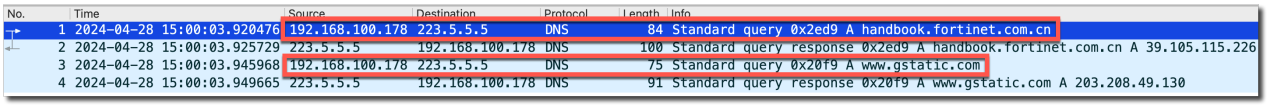
> **重要**
>
> 由于浏览器可能有历史记录的原因，即使输入的是`handbook.fortinet.com.cn`，浏览器也可能会自动替换为`https://handbook.fortinet.com.cn`。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

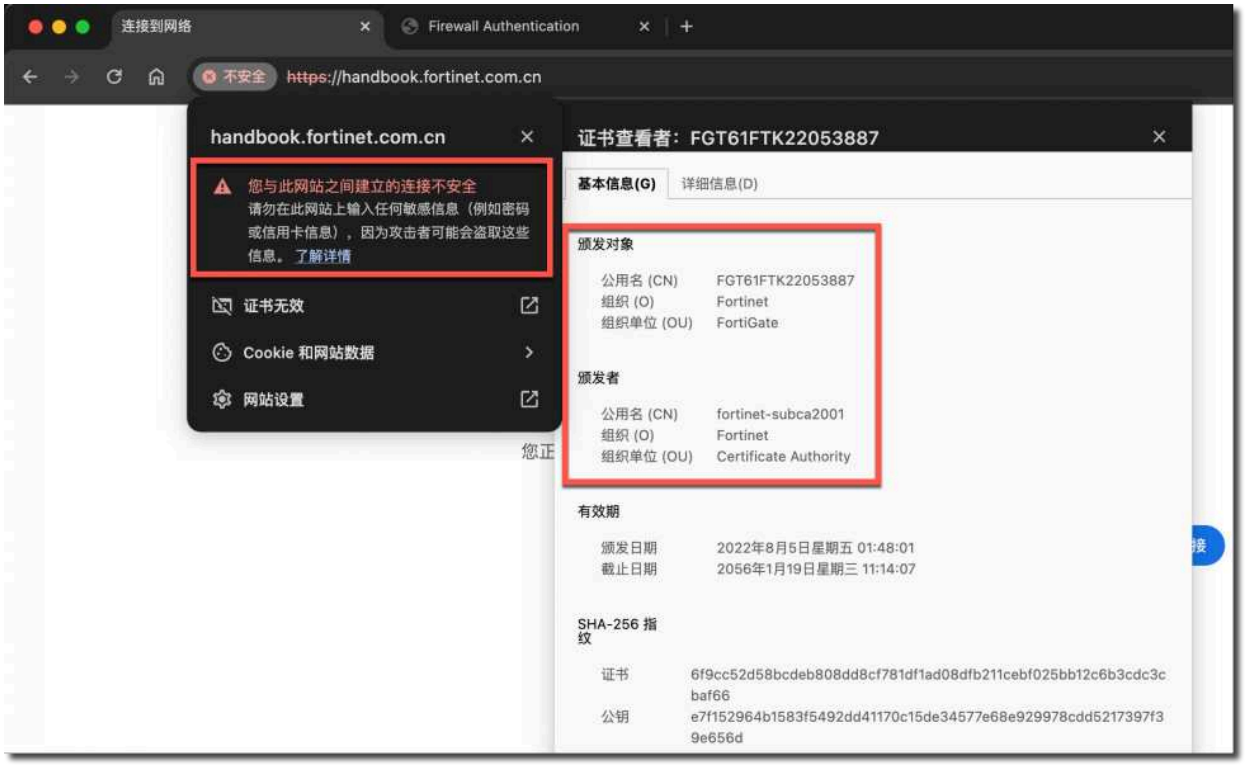
问题原因

1. 通过抓包发现，PC浏览器（Chrome）每次访问 `https://handbook.fortinet.com.cn`，不只会请求访问的域名 `handbook.fortinet.com.cn` 的IP地址，同时会请求 `www.gstatic.com` 的IP地址（抓包文件请参考：auth_dns.pcapng）。

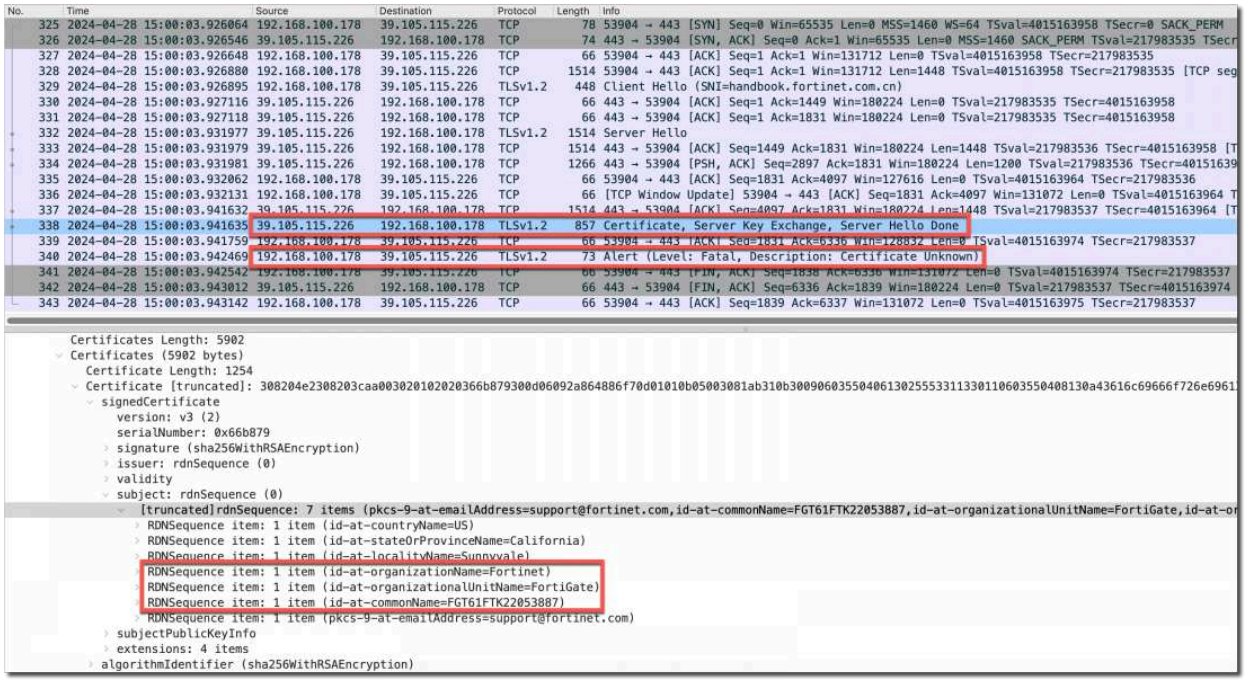


No.	Time	Source	Destination	Protocol	Length	Info
1	2024-04-28 15:00:03.920476	192.168.100.178	223.5.5.5	DNS	84	Standard query 0x2ed9 A handbook.fortinet.com.cn
2	2024-04-28 15:00:03.925729	223.5.5.5	192.168.100.178	DNS	100	Standard query response 0x2ed9 A handbook.fortinet.com.cn A 39.105.115.226
3	2024-04-28 15:00:03.945968	192.168.100.178	223.5.5.5	DNS	75	Standard query 0x20f9 A www.gstatic.com
4	2024-04-28 15:00:03.949665	223.5.5.5	192.168.100.178	DNS	91	Standard query response 0x20f9 A www.gstatic.com A 203.208.49.130

2. 此后PC浏览器会分发起2个HTTP请求：
   - 访问 `https://handbook.fortinet.com.cn`，由于FortiGate开启了防火墙认证，FortiGate会拦截PC的对该网站的访问，并使用相同的HTTPS返回自签名的证书，默认情况下该证书不受PC信任，浏览器向服务器返回了“Certificate Unknown”的告警信息（抓包文件请参考：auth_to_handbook.pcapng））。

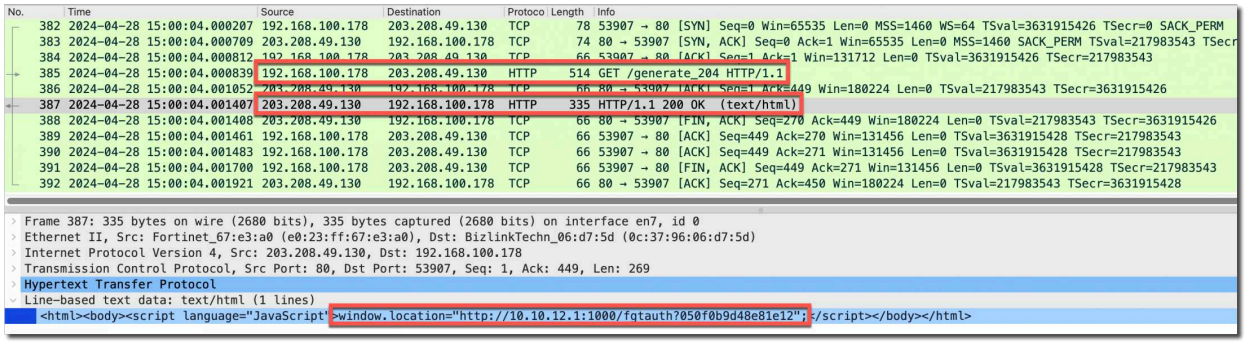


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

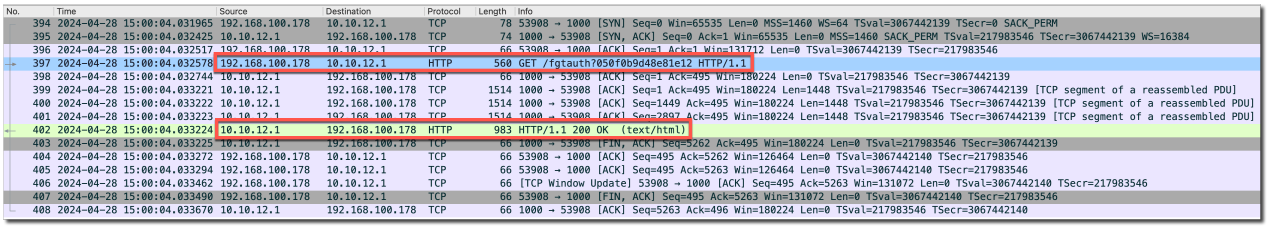


- 访问 `http://www.gstatic.com/generate_204`，由于FortiGate开启了防火墙认证，FortiGate会拦截PC的对 `/generate_204` 网页的访问请求，并使用HTTP协议返回HTTP 200 OK，其中携带需要重定向的认证页面（通过JS脚本的方式进行重定向，此例中重定向的URL为 `http://10.10.12.1:1000/fgtauth?050f0b9d48e81e12`，抓包文件请参考：auth_to_gstatic.pcapng ↗）。

> **重要**
>
> Chrome浏览器在访问网页时会同时使用 `http://www.gstatic.com/generate_204` 来确认浏览器是否可以访问Internet。



3. PC浏览器使用返回的HTTP 200 OK中的重定向地址 `http://10.10.12.1:1000/fgtauth?050f0b9d48e81e12` 打开FortiGate的认证页面（抓包文件请参考：auth_to_authserver.pcapng ↗）。



4. 所以PC需要认证时，访问网页会打开2个页面。

解决方法

1. 在用户认证配置中，使用FortiGate的自签名CA证书 `Fortinet_CA_SSL`（默认没有指定证书，总是使用HTTP Portal进行认证），强制使用HTTPS Portal进行认证。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

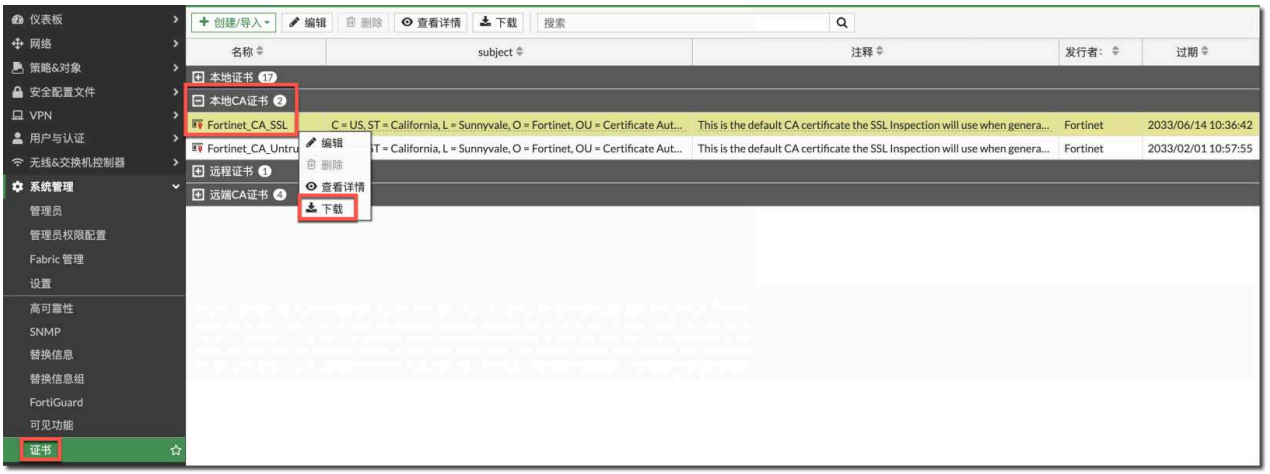
也可以使用其他证书颁发机构（如用户自建CA）颁发的Sub CA，需携带私钥导入FortiGate（导入步骤请参考系统管理→系统设置→证书管理↗的“本地CA证书”部分）。

```bash
config user setting
    set auth-ca-cert "Fortinet_CA_SSL"
end
```

2. （可选）使用IP或域名作为认证的Portal（使用域名时，DNS需要能够解析该域名）。此步可以不配置，默认使用需要认证的流量的入接口IP地址作为Portal页面的IP。

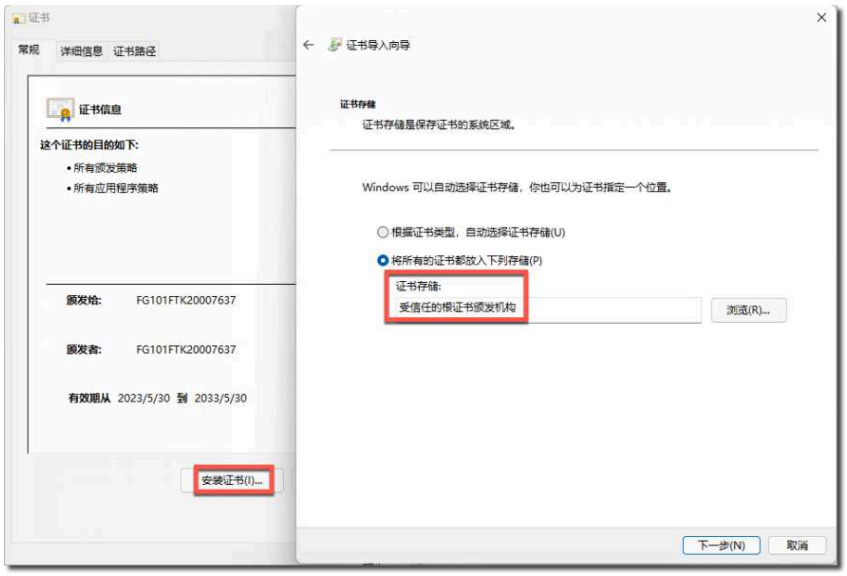
```bash
config firewall auth-portal
    set portal-addr "fgt.portal.com"
end
```

3. 从FortiGate管理页面的“系统管理→证书”页面中的“本地CA证书”中，右键点击并下载`Fortinet_CA_SSL`证书。



4. 在PC上信任该CA证书（具体证书信任步骤请参考系统管理→管理方式→消除Web证书告警↗的“导入和信任CA证书部分”）。

   - Windows：将CA证书导入PC的“受信任的根证书颁发机构中”。

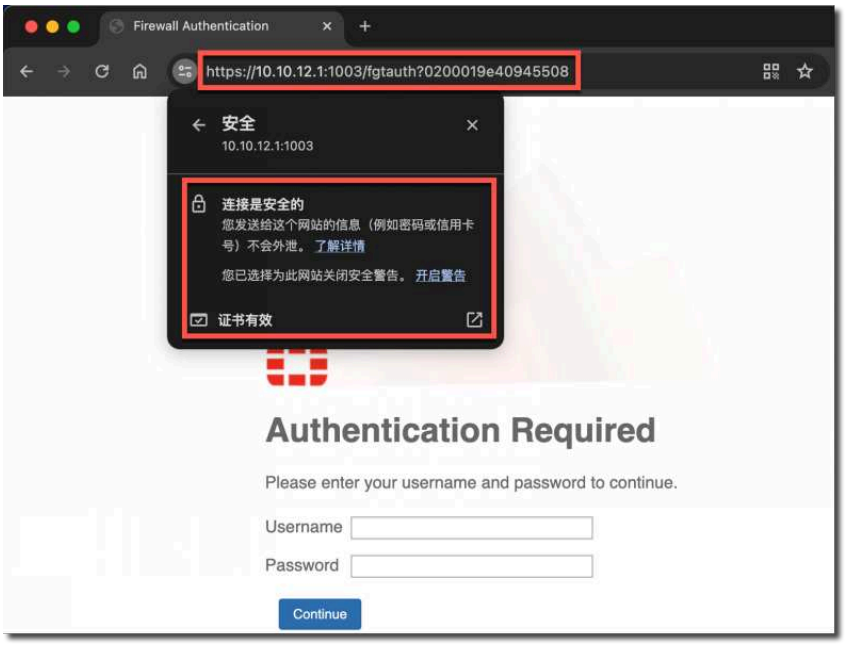


   - MacOS：在“钥匙串访问”中信任该证书。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 再次使用PC访问 `https://handbook.fortinet.com.cn` ，只会弹出1个HTTPS认证页面，且不会提示网站不安全。



6. 查看该认证页面证书内容，可以看到是由CA证书Fortinet_CA_SSL签发的证书，CN为需要认证流量的入接口地址（如果第2步中配置了Portal域名，则这里的CN为对应域名）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

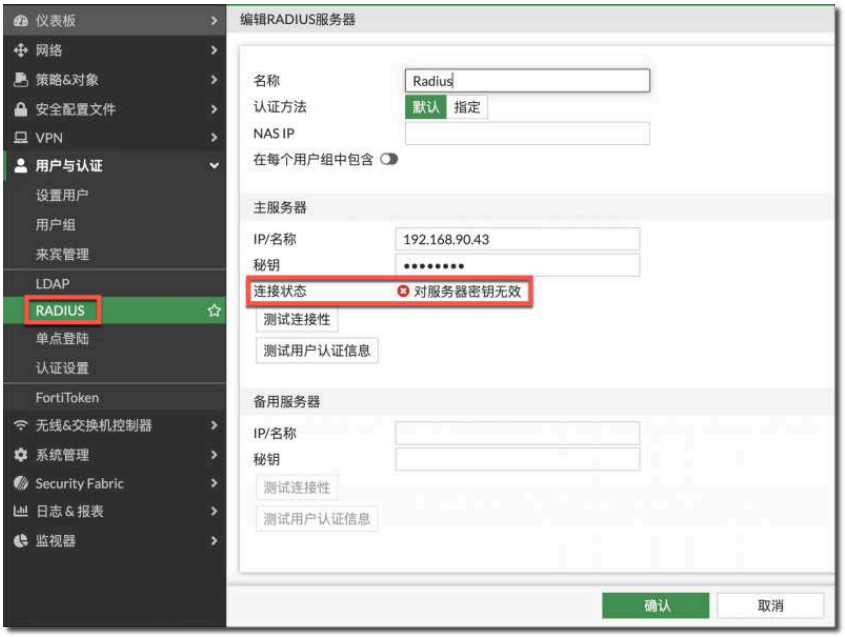


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

升级版本后Radius连接失败

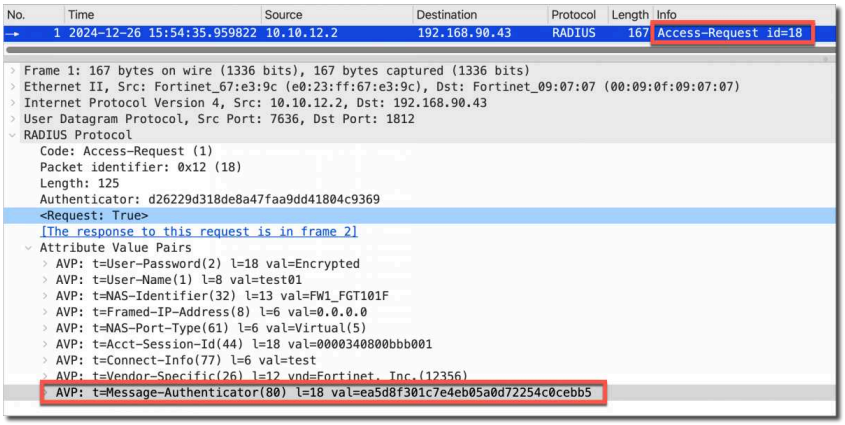
问题现象

在升级到FortiOS 7.2.10、7.4.5之后，FortiGate已配置的Radius服务器无法正常连接，显示“对服务器密钥无效”，升级前是可以正常连接的。



问题原因

为了避免Radius协议漏洞CVE-2024-3596造成的影响，在FortiOS 7.2.10和7.4.5的版本中，FortiGate强制验证Radius Message-Authenticator属性。即FortiGate作为Radius Client发送的Radius Access Request报文里面会携带Radius Message-Authenticator属性，FortiGate要求Radius Server在返回给防火墙的Radius报文中也必须要携带Radius Message-Authenticator属性，如果Radius Server不携带该属性，则FortiGate拒绝其响应。



解决方法

1. 升级Radius服务器到已经修复漏洞CVE-2024-3596的版本，例如Windows Server系统在KB5040268补丁中增加了对Radius Message-Authenticator属性的支持。

2. 在之后的7.2.11或7.4.6的版本中，有选项可以关闭强制验证Radius Message-Authenticator属性（默认开启）。

```bash
config user radius
    edit xxx
        set require-message-authenticator disable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 如果方法1和方法2都不可行，可以暂时降级到7.2.9或7.4.5版本。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

AWS部署FortiGate

请参考AWS部署FortiGate ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

AWS同AZ部署FortiGate HA

请参考AWS同AZ部署FortiGate HA ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

AWS跨AZ部署FortiGate HA

请参考AWS跨AZ部署FortiGate HA ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

AWS扩充硬盘容量

网络需求

某用户在AWS上部署的FortiGate VM，原有硬盘容量分配了30GB用于日志记录，随着日志存储量的增加，现在需要将硬盘容量扩充到200GB用于日志记录。




```bash
FortiGate_AWS # exe disk list
Disk Virtual-Disk    ref: 255  30.0GiB    type: SSD [NVME] dev: /dev/nvme1n1
  partition ref:   1  29.4GiB,  29.4GiB free  mounted: Y  label: LOGUSEDX8C26DB0A dev: /dev/nvme1n1p1 start: 2048
```

```bash
FortiGate_AWS # show system storage
config system storage
    edit "Virtual-Disk"
        set status enable
        set media-status enable
        set order 1
        set partition "LOGUSEDX8C26DB0A"
        set device "/dev/nvme1n1p1"
        set size 30108
        set usage log
    next
end
```

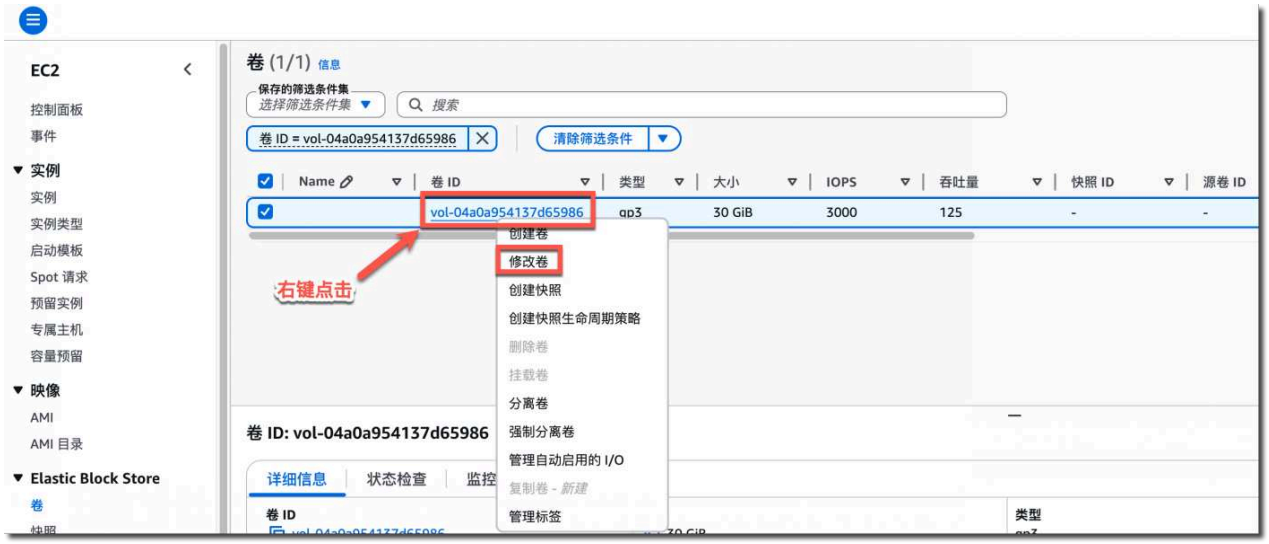
扩充步骤

1. 无需停止AWS VM实例，点击该实例下的存储选项，点击30GB的存储卷ID。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

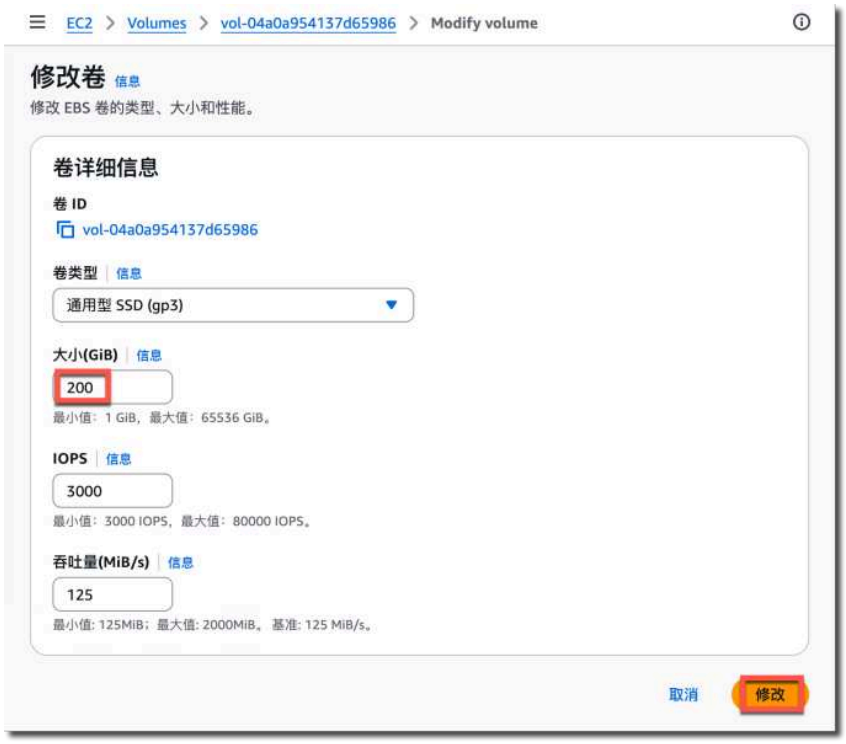


2. 在卷页面右键点击该卷ID，并选择“修改卷”。



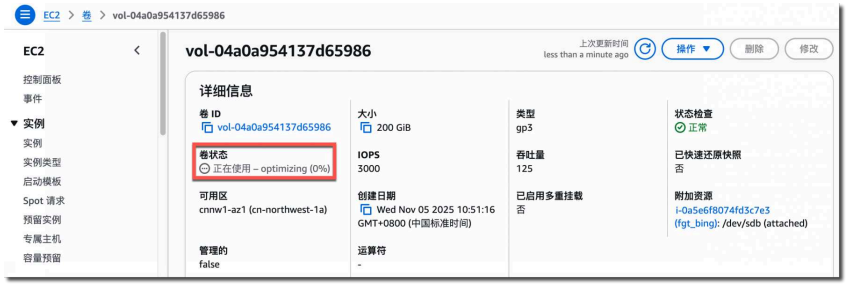
3. 将大小修改为200GB，然后点击“修改”按钮，之后该实例的硬盘会被扩展到200GB。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





4. 硬盘扩展需要一定时间，期间卷状态状态为“optimizing”。



5. 等待硬盘扩展完成（卷状态变为“正在使用”）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 在FortiGate的CLI查看硬盘状态，硬盘容量已经变为200GB，但日志分区仍然为30GB。

```bash
FortiGate_AWS # exe disk list
Disk Virtual-Disk    ref: 255 200.0GiB    type: SSD [NVME] dev: /dev/nvme1n1
  partition ref:   2  29.4GiB,  29.4GiB free  mounted: Y  label: LOGUSEDX8C26DB0A dev: /dev/nvme1n1p1 start: 2048

FortiGate_AWS # show system storage
config system storage
    edit "Virtual-Disk"
        set status enable
        set media-status enable
        set order 1
        set partition "LOGUSEDX8C26DB0A"
        set device "/dev/nvme1n1p1"
        set size 30108
        set usage log
    next
end
```

7. 需要在FortiGate上执行格式化整个硬盘的操作，参考“exe disk list”执行结果中的分区ref数字。输入y后确认，设备会重启并执行格式化操作。

重要

- 注意这里执行格式化的分区数字为整个硬盘的ref数字（Disk Virtual-Disk ref，此例中为255），而不是日志分区的ref数字（partition ref，此例中为1）
- 您需要根据您的FortiGate VM中执行“exe disk list”结果中的硬盘ref数字来决定“execute disk format”命令后的数字。如您的硬盘ref数字（Disk Virtual-Disk ref）为251，则执行“execute disk format 251”。

```bash
FortiGate_AWS # exe disk list
Disk Virtual-Disk    ref: 255 200.0GiB    type: SSD [NVME] dev: /dev/nvme1n1
  partition ref:   2  29.4GiB,  29.4GiB free  mounted: Y  label: LOGUSEDX8C26DB0A dev: /dev/nvme1n1p1 start: 2048

FortiGate_AWS # execute disk format 255
format requested for:  device=/dev/nvme1n1 255/(no storage);
Formatting this storage will erase all data on it, including
  logs, quarantine files;
  certificate revocation lists (CRLs);
This action requires the unit to reboot.
Do you want to continue? (y/n)y
```

8. 设备重启完成后，再次查看硬盘与日志分区状态，日志分区已经扩容到200GB。

```bash
FortiGate_AWS # exe disk list
Disk Virtual-Disk    ref: 255 200.0GiB    type: SSD [NVME] dev: /dev/nvme1n1
  partition ref:   1 195.9GiB, 195.8GiB free  mounted: Y  label: LOGUSEDX8C26DB0A dev: /dev/nvme1n1p1 start: 2048

FortiGate_AWS # show system storage
config system storage
    edit "Virtual-Disk"
        set status enable
        set media-status enable
        set order 1
        set partition "LOGUSEDX8C26DB0A"
        set device "/dev/nvme1n1p1"
        set size 200561
        set usage log
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

注意事项

1. FortiGate VM只支持一块硬盘作为日志记录盘，如果是通过新增更大硬盘的方式扩充日志记录盘容量，新增的硬盘卷将无法用于日志记录，建议通过直接扩充现有硬盘卷的容量来扩充日志分区大小。
2. 格式化操作时必须使用“execute disk format XXX”命令，使用“exe formatlogdisk”是无效的。
3. 阿里云、Azure上的FortiGate VM也可以参考此方法进行日志分区扩容。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

阿里云部署FortiGate

请参考阿里云部署FortiGate↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

阿里云同AZ部署FortiGate HA

请参考阿里云同AZ部署FortiGate HA ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

阿里云跨AZ部署FortiGate HA

请参考阿里云跨AZ部署FortiGate HA ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Azure部署FortiGate

请参考Azure部署FortiGate ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

结合Azure负载均衡器部署FortiGate HA

请参考结合Azure负载均衡器部署FortiGate HA ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

阿里云更换License后无法增加CPU

问题现象

1. 某用户将运行在云上的FortiGate HA两台虚机的License由评估License更换为正式License，如FortiGate-VM04替换为FortiGate-VM04-S。

2. 更换后，备机VM的CPU变为1个。

```bash
FGT-VM64-KVM-1502 # get system status
......
Serial-Number: FGVMSLTM23007738
License Status: Valid
VM Resources: 1 CPU/1 allowed, 7735 MB RAM
......

FGT-VM64-KVM-1502 # diagnose debug vm-print-license
SerialNumber: FGVMSLTM23007738
CreateDate: Thu Dec 21 03:23:20 2023
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: SL (18)
CPU: 1 (subscription:0)
MEM: 2147483647
VDOM license:
  permanent: 1
  subscription: 0

FGT-VM64-KVM-1502 # diagnose hardware sysinfo vm full
UUID:     95790208a255482da2b95a817a2ffdd3
valid:    1
status:   1
code:     200
warn:     0
copy:     0
received: 4294939474
warning:  4294939474
recv:     202312260754
dup:
```

3. 无法通过`exe cpu add`添加CPU。

```bash
FGT-VM64-KVM-1502 # exe cpu add 3
CPU number exceeds license limit.
Command fail. Return code -61
```

解决办法

1. 将FortiGate HA主备切换后，在新主机（原备机）执行`execute update-now`手动触发更新，之后可以正常添加CPU Core。

```bash
FGT-VM64-KVM-1502 # exe update-now
......
FGT-VM64-KVM-1502 # exe cpu add 3
Active CPU number: 4
Total CPU number: 4

FGT-VM64-KVM-1502 # exe cpu show
Active CPU number: 4
Total CPU number: 4
```

2. 查看该VM相关参数均显示为新License的CPU信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FGT-VM64-KVM-1502 # get system status
......
Serial-Number: FGVMSLTM23007738
License Status: Valid
VM Resources: 4 CPU/4 allowed, 7735 MB RAM
......

FGT-VM64-KVM-1502 # diagnose debug vm-print-license
SerialNumber: FGVMSLTM23007738
CreateDate: Thu Dec 21 03:23:20 2023
License expires: Wed Feb 21 08:00:00 2024
Key: yes
Cert: yes
Key2: yes
Cert2: yes
Model: SL (18)
CPU: 4 (subscription:4)
MEM: 2147483647
VDOM license:
  permanent: 1
  subscription: 0

FGT-VM64-KVM-1502 # diagnose hardware sysinfo vm full
UUID:     95790208a255482da2b95a817a2ffdd3
valid:    1
status:   1
code:     200
warn:     0
copy:     0
received: 4294939353
warning:  4294986323
recv:     202312260824
dup:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

SSH使用账号/密码登录

云上部署完成的FortiGate，默认会使用实例创建过程中配置的密钥对来登录SSH，无法通过账户/密码的方式登录SSH。

如果要使用账户/密码的方式登录SSH，需要在FortiGate中执行以下CLI命令：

```
config system global
    set admin-ssh-password enable
end
```

随后即可以通过账户/密码的方式登录云上部署的FortiGate。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

工作流

自动化简介

自动化（Automation）功能能够根据特定的触发条件自动执行相应的动作，可以让客户更快的发现设备发生的事件，以及更快地处理事件。它可以监控来自Security Fabric中任何成员的事件，然后设置对应的执行动作。

自动化设置可以在Security Fabric成员中同步，或只用于Security Fabric中的一个单独FortiGate。当FortiGate加入了Security Fabric，自动化只能在Security Fabric的Root FortiGate上创建。

当然，如果一台FortiGate未加入Security Fabric，也可以使用自动化功能。

FortiGate上的每个自动化配置包含3个部分：

- 触发器（Trigger）：用于触发自动化流程的条件，可以是某个系统事件日志、UTM日志、计划时间等。系统会内置一些常用的Trigger。
- 动作（Action）：触发器触发后执行的动作，可以是执行CLI脚本、发送邮件、重启设备等。系统会内置一些常用的Action。
- 串联器（Stitch）：将触发器（Trigger）和动作（Action）关联起来，在Stitch中，一个Stitch可以包含1个Trigger和多个Action，可以单独设置每个Action和Trigger的执行延迟时间。系统会内置一些常用的Stitch。Stitch有两种执行Action的模式：
  - 顺序：如果有多个动作（Action），触发器（Trigger）触发后，按照动作（Action）的顺序依次执行。
  - 并行：如果有多个动作（Action），触发器（Trigger）触发后，同时执行所有动作（Action）。

工作流（Workflow）就是每个自动化配置的统称。

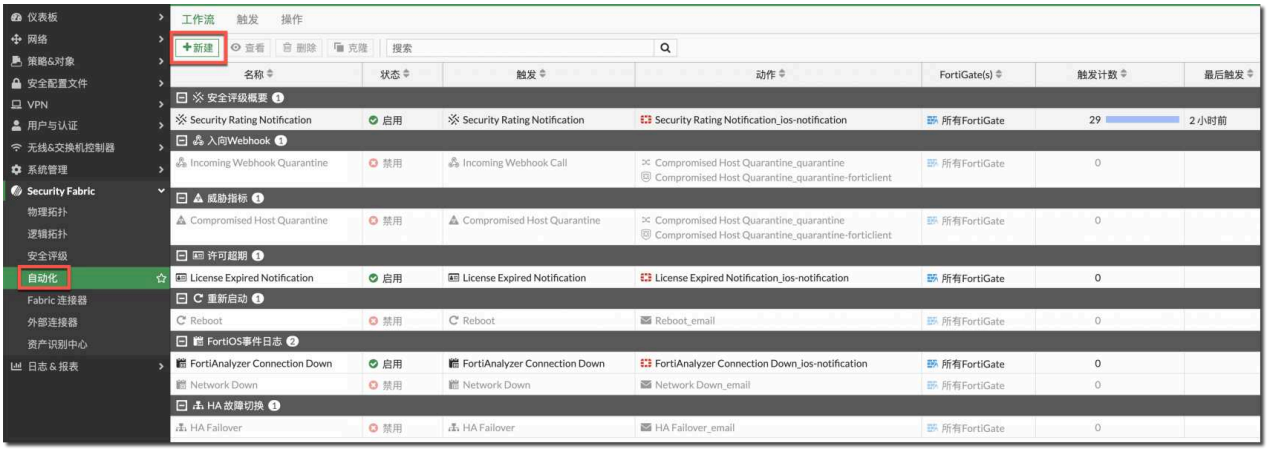
单动作配置示例

网络需求

当IPSec由于DPD超时中断，等待5s后，向管理员的邮箱发送通知邮件。

配置步骤

1. 首先配置告警邮件发送的配置（参考日志→邮件告警 ↗章节，也可使用默认配置）。
2. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击新建按钮，新建一个工作流（此页也有一些内置的工作流，可根据需求自行使用或禁用）。



3. 配置工作流的名称，点击“添加触发器”按钮，在右侧的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 操作执行-顺序：如果有多个动作（Action），触发器（Trigger）触发后，按照动作（Action）的顺序依次执行。
- 操作执行-并行：如果有多个动作（Action），触发器（Trigger）触发后，同时执行所有动作（Action）。

4. 在右侧弹出的窗口中，找到“其他条件”分类，点击“FortiOS事件日志”选项。



5. 配置触发器（Trigger）的名称，事件选择“IPSec DPD failed”（可根据需求在字段过滤中配置日志中要求包含的字段），点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system automation-trigger
    edit "DPD_Failure"
        set event-type event-log
        set logid 37136
    next
end
```

6. 在选择条目中选择上步创建的触发器（Trigger），点击应用按钮。

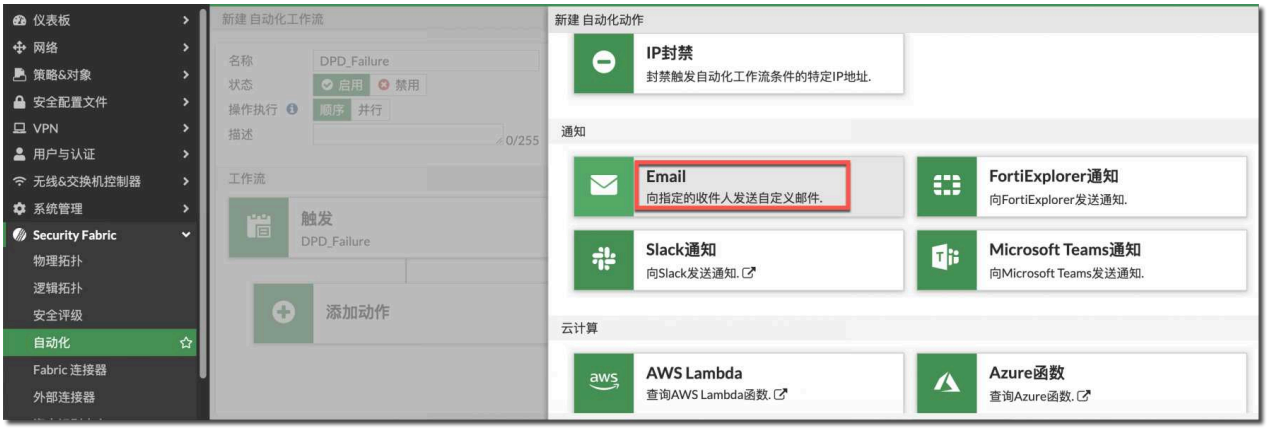


7. 点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 在右侧弹出的窗口中，找到“通知”分类，点击“Email”选项。



9. 配置动作（Action）的名称，以及邮件通知的收件人，邮件内容为DPD失败的日志内容，点击确认下发配置。



- 最小间隔：如果Trigger频繁触发了，Action执行的最小间隔。
- 源：指定邮件通知的发件人，默认为DoNotReply@notification.fortinet.net。
- 目的：配置邮箱的收件人，可以配置多个收件人。
- Body：邮件内容。
- 更换信息：可以更换为自定义内容和格式。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system automation-action
    edit "Email_DPD_Failure"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "DPD_Failure_Notice"
    next
end
```

10. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

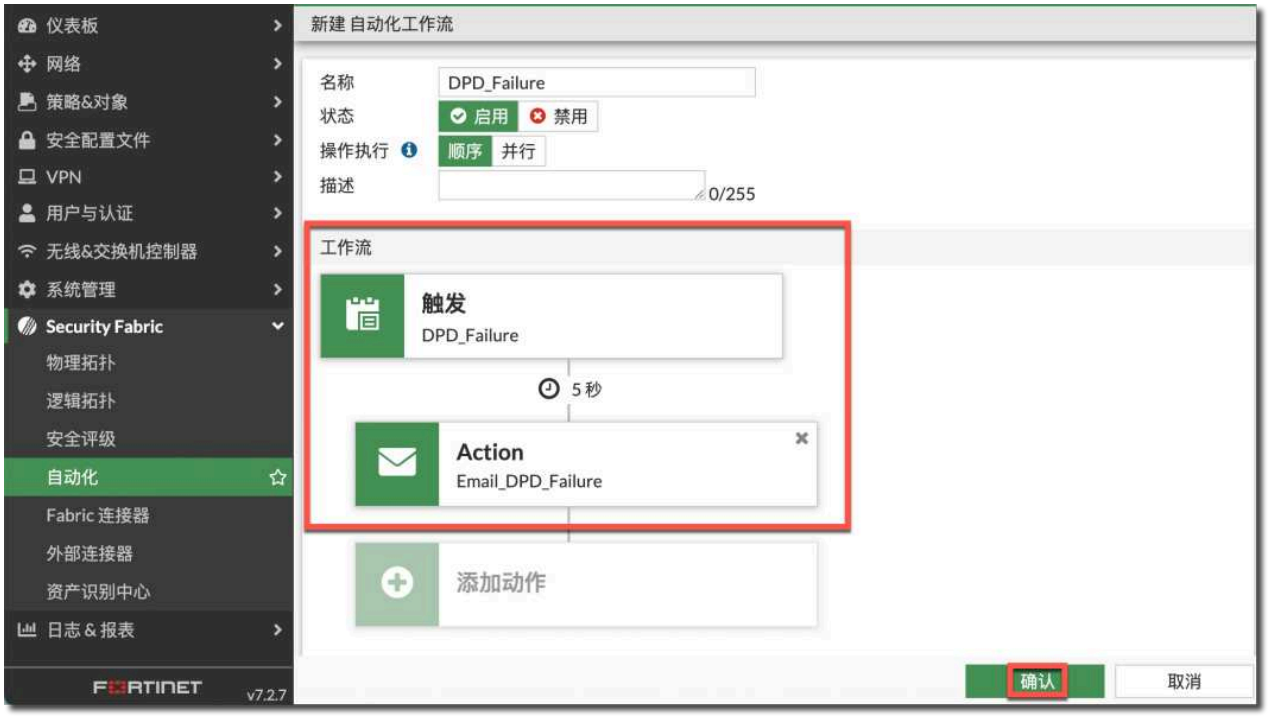


11. 可以点击“Add delay”添加触发器（Trigger）触发后执行动作（Action）间的延迟，这里以5s为例。



12. 检查无误后，点击确认下发配置。

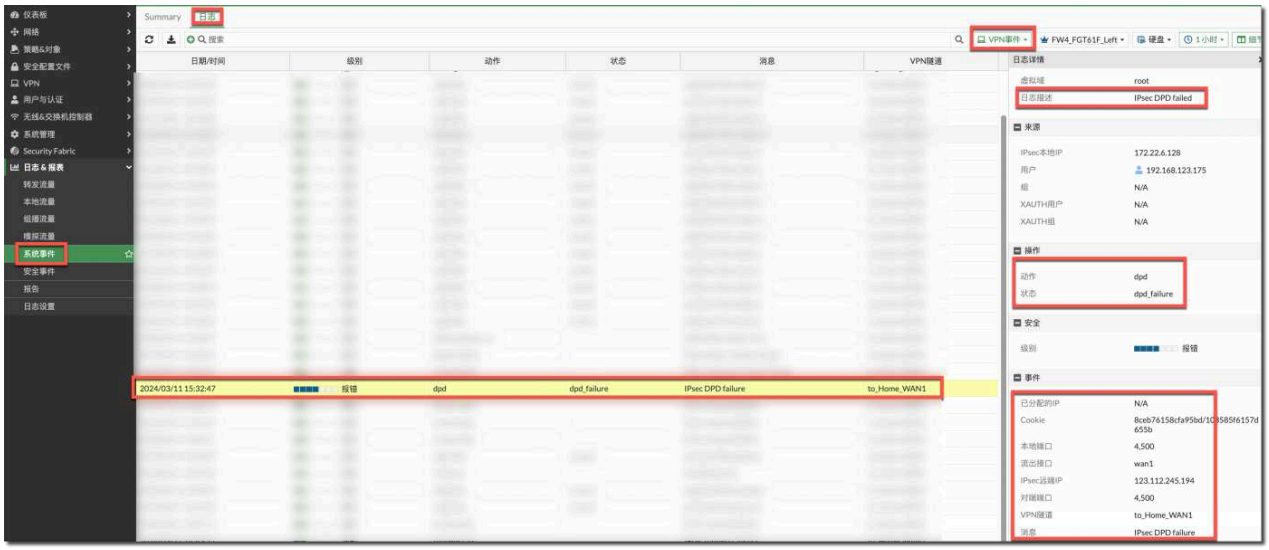
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system automation-stitch
    edit "DPD_Failure"
        set trigger "DPD_Failure"
        config actions
            edit 1
                set action "Email_DPD_Failure"
                set delay 5
                set required enable
            next
        end
    next
end
```

配置验证

1. 触发FortiGate上的DPD超时日志。

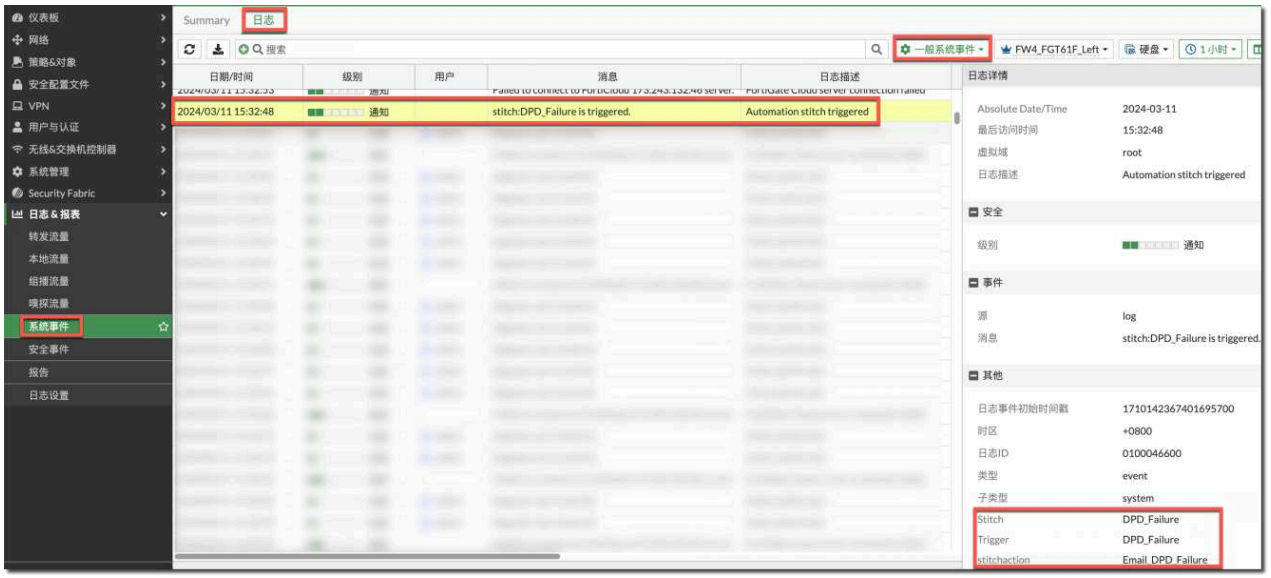



```bash
date=2024-03-11 time=15:32:47 eventtime=1710142366681265100 tz="+0800" logid="0101037136" type="event"
subtype="vpn" level="error" vd="root" logdesc="IPsec DPD failed" msg="IPsec DPD failure" action="dpd"
remip=123.112.245.194 locip=172.22.6.128 remport=4500 locport=4500 outintf="wan1"
cookies="8ceb76158cfa95bd/108585f6157d655b" user="192.168.123.175" group="N/A" useralt="N/A" xauthuser="N/A"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
xauthgroup="N/A" assignip=N/A vpntunnel="to_Home_WAN1" status="dpd_failure" advpnsc=0
```

2. 5s后，触发自动化程序，相关自动化日志如下。




```bash
date=2024-03-11 time=15:32:48 eventtime=1710142367401695780 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="DPD_Failure"
trigger="DPD_Failure"
```

3. 收件人邮箱收到了告警邮件，邮件内容为DPD Failed的日志内容，发件人为默认的DoNotReply@notification.fortinet.net。



4. 对应的自动化触发Debug信息。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable
......
__action_email_hdl()-181: email action (Email_DPD_Failure) is called.
from:
to:bbai@fortinet.com;
subject:DPD_Failure_Notice
......
```

5. 发送邮件的Debug信息如下。

```bash
FortiGate # diagnose debug application alertmail -1
FortiGate # diagnose debug enable

Arrived msg(type 9, 415 bytes):bbai@fortinet.com;
DPD_Failure_Notice
date=2024-03-11 time=16:11:15 devid="FGT61FTK22063594" devname="FortiGate" eventtime=1710144674391662240
tz="+0800" logid="0100032014" type="event" subtype="system" level="warning" vd="root" logdesc="Support license
expiring" ui="automation" action="test" msg="Automation Stitch Test: FortiCare license will expire in 1 day(s)"
stitch="License Expired Notification"

mail_info:
       from:notification.fortinet.net  user:DoNotReply@notification.fortinet.net
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
mail_info:
        reverse path:DoNotReply@notification.fortinet.net
        user name:DoNotReply
to[0]:bbai@fortinet.com
⟸_init_mail_info
create session
resolve notification.fortinet.net to 1 IP
⟹ send mail
connecting to 208.91.114.151 port 465
send mail 0×9988160 session 0×99863c0
session_io_event: creating ssl structure for session 0×99863c0
create_ssl: 0×7f9ff88000
sessionn 0×99863c0, SSL connected
session: 0×99863c0, rsp_state: greeting, code: 220
session: 0×99863c0, rsp_state: ehlo, code: 250
session: 0×99863c0, rsp_state: mail, code: 250
session: 0×99863c0, rsp_state: rcpt, code: 250
session: 0×99863c0, rsp_state: data, code: 354
⟸ send: date=2024-03-11 time=16:11:15 devid="FGT61FTK22063594" devname="FortiGate" eventtime=1710144674391662240
tz="+0800" logid="0100032014" type="event" subtype="system" level="warning" vd="root" logdesc="Support license
expiring" ui="automation" action="test" msg="Automation Stitch Test: FortiCare license will expire in 1 day(s)"
stitch="License Expired Notification"

session: 0×99863c0, rsp_state: data2, code: 250
session: 0×99863c0, rsp_state: quit, code: 221
session finined
_session_on_destroy
⟸ send mail success, m = 0×9988160 s = 0×99863c0
```

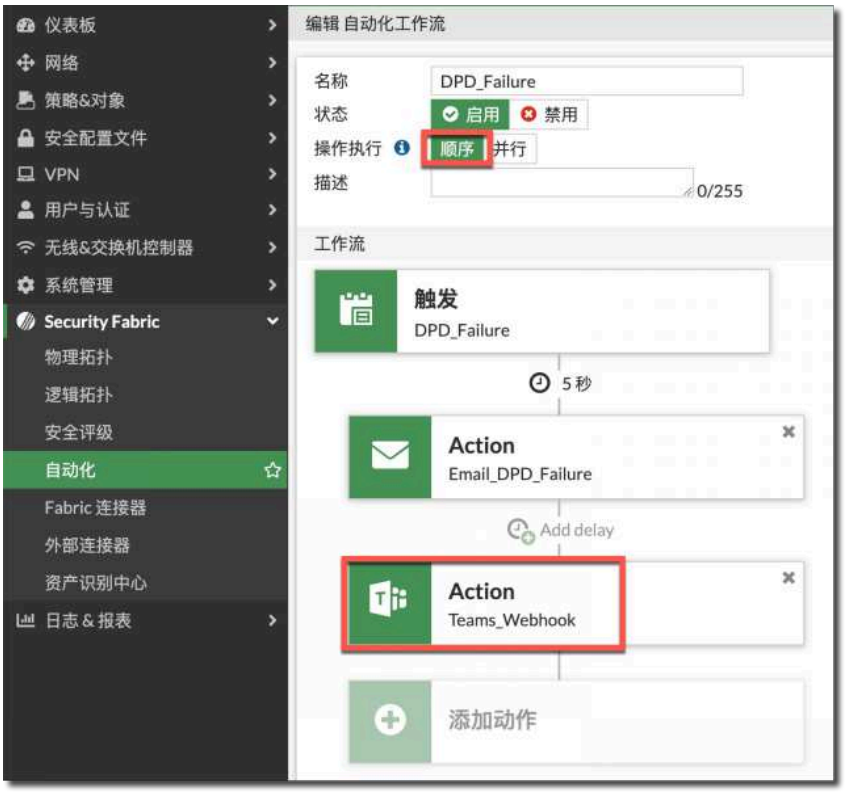
多动作顺序执行示例

网络需求

当IPSec由于DPD超时中断时，等待5s后向管理员的邮箱发送通知邮件，邮件发送成功后，再通过Webhook向Teams发送消息。

配置步骤

1. 在以上配置的基础上，使该自动化工作流以顺序模式执行多个动作。新建一个动作（Action），这里以Teams Webhook为例。

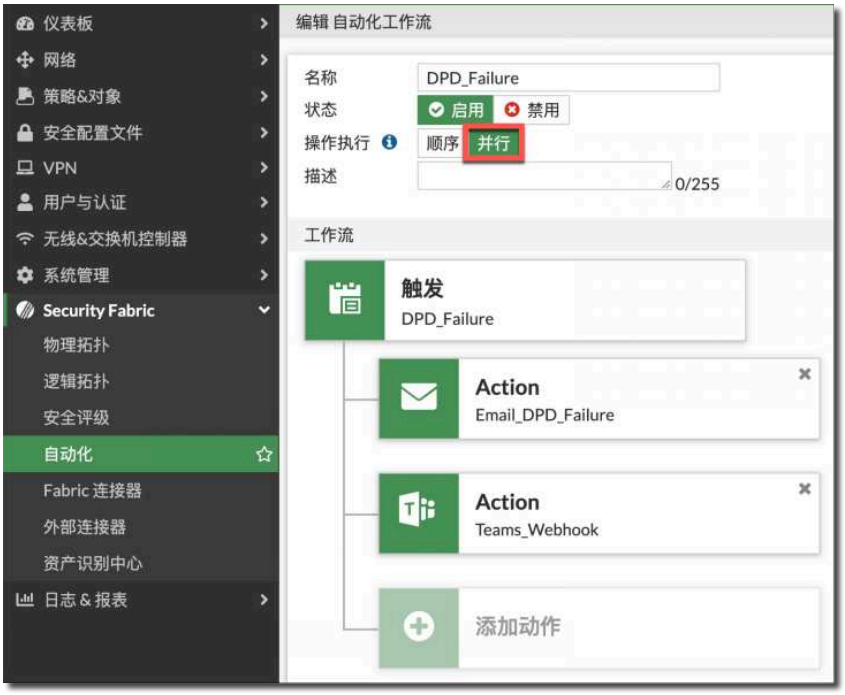


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置下发后，查看自动化工作流对应的CLI配置，可以看到action部分多了`set required enable`字段，该字段表示必须前一个Action执行完毕后，才会执行本Action，这也就实现了“顺序”的效果。

```bash
config system automation-stitch
    edit "DPD_Failure"
        set trigger "DPD_Failure"
        config actions
            edit 1
                set action "Email_DPD_Failure"
                set delay 5
                set required enable
            next
            edit 2
                set action "Teams_Webhook"
                set required enable
            next
        end
    next
end
```

3. 将该自动化工作流改为并行模式，查看CLI配置，可以看到`set required enable`配置消失。只要触发器被触发，所有的动作会立即执行。

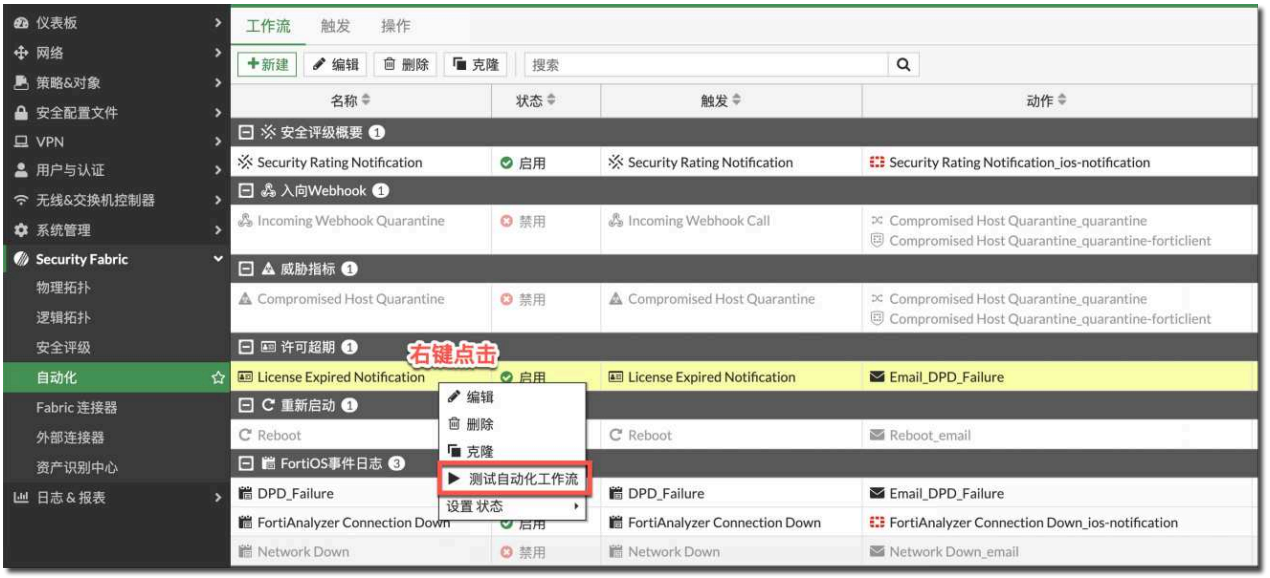



```bash
config system automation-stitch
    edit "DPD_Failure"
        set trigger "DPD_Failure"
        config actions
            edit 1
                set action "Email_DPD_Failure"
            next
            edit 2
                set action "Teams_Webhook"
            next
        end
    next
end
```

手动测试自动化

1. 部分自动化程序可以手动触发，作为配置完成后的测试手段。如下所示，在工作流页面中，右键点击某个自动化工作流，点击“测试自动化工作流程”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



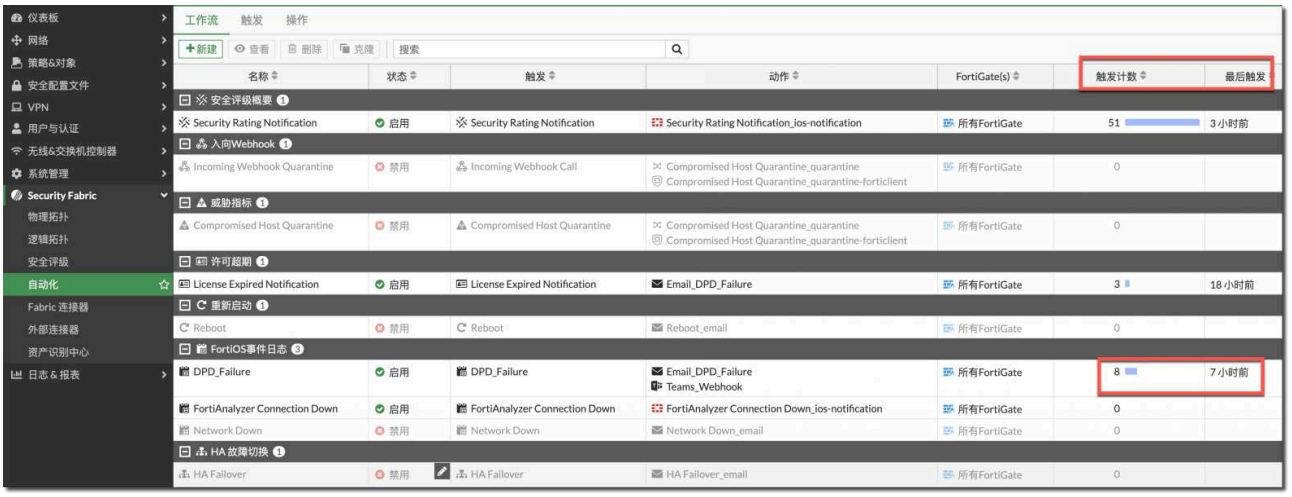
2. 此动作可以不需要配置的触发器真实触发，而直接触发执行动作。通过CLI `diagnose automation test <Stitch_name>` 也可以执行该动作。

```bash
FortiGate # diagnose automation test "License Expired Notification"
automation test is done. stitch:License Expired Notification
```

查看自动化状态信息

GUI

在工作流页面可以直接查看每个工作流的触发次数和最后触发时间。



CLI

1. 通过 `diagnose test application autod 2` 可以看到所有的自动化工作流的配置与匹配计数。

```bash
FortiGate # diagnose test application autod 2
csf: disabled   root: no        sync connection: connecting
version:0 sync time:
total stitches activated: 4

stitch: DPD_Failure
        destinations: all
        trigger: DPD_Failure
                type:logid
                        logids:
                                0: 37136
        local hit: 6 relayed to: 0 relayed from: 0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        actions:
                Email_DPD_Failure type:email interval:0
                        delay:5 required:yes
                        subject: DPD_Failure_Notice
                        body: %%log%%
                        sender:
                        mailto:bbai@fortinet.com;
......
```

2. 查看自动化工作流的触发次数、最后触发时间、被自动化引用的日志ID等统计。

```bash
FortiGate # diagnose test application autod 3
alert mail log count: 0

stitch: DPD_Failure

        local hit: 7 relayed to: 0 relayed from: 0
        last trigger:Mon Mar 11 16:00:45 2024
        last relay:
        actions:
                Email_DPD_Failure:
                        done: 6 relayed to: 0 relayed from: 0
                        last trigger:Mon Mar 11 16:00:45 2024
                        last relay:

                          ......

logid to stitch mapping:
id:20101  local hit: 0 relayed hits: 0
        License Expired Notification

id:20102  local hit: 0 relayed hits: 0
        License Expired Notification

id:20103  local hit: 0 relayed hits: 0
        License Expired Notification

id:20104  local hit: 0 relayed hits: 0
        License Expired Notification

id:22902  local hit: 0 relayed hits: 0
        FortiAnalyzer Connection Down

id:32014  local hit: 2 relayed hits: 0
        License Expired Notification

id:32045  local hit: 0 relayed hits: 0
        License Expired Notification

id:32049  local hit: 0 relayed hits: 0
        License Expired Notification

id:37136  local hit: 7 relayed hits: 0
        DPD_Failure

id:52000  local hit: 47 relayed hits: 0
        Security Rating Notification

log category to stitch mapping:
```

3. 查看正在运行的自动化工作流状态，以及已运行的自动化工作流的执行统计。

```bash
FortiGate # diagnose test application autod 5

runned stitches: total:56 done:55 drop:0

running stitches: 1

1. stitch:DPD_Failure id:55 running time:Mon Mar 11 16:00:45 2024

        log relayed:0 sn:FGT61FTK22063594 logid:37136 log(531):date=2024-03-11 time=16:00:45
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
devid="FGT61FTK22063594" devname="FortiGate" eventtime=1710144045841282220 tz="+0800" logid="0101037136"
type="event" subtype="vpn" level="error" vd="root" logdesc="IPsec DPD failed" msg="IPsec DPD failure" action="dpd"
remip=123.112.245.97 locip=172.22.6.128 remport=4500 locport=4500 outintf="wan1"
cookies="aa470ef86bf5705d/9d33378890990748" user="192.168.123.175" group="N/A" useralt="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=N/A vpntunnel="to_Home_WAN1" status="dpd_failure" advpnsc=0

        1. action:Email_DPD_Failure status:ready id:0 running time:Mon Mar 11 16:09:05 2024
 delay:500 required:1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

系统事件日志触发器

简介

FortiGate可以配置系统事件日志作为自动化的触发器（Trigger），在发生特定系统事件日志ID时触发。配置时可以选择多个系统事件日志ID，还可以自定义日志字段筛选器。

> **重要**
>
> 每个自动化工作流最多可以配置16个系统事件日志ID作为触发器（Trigger）。

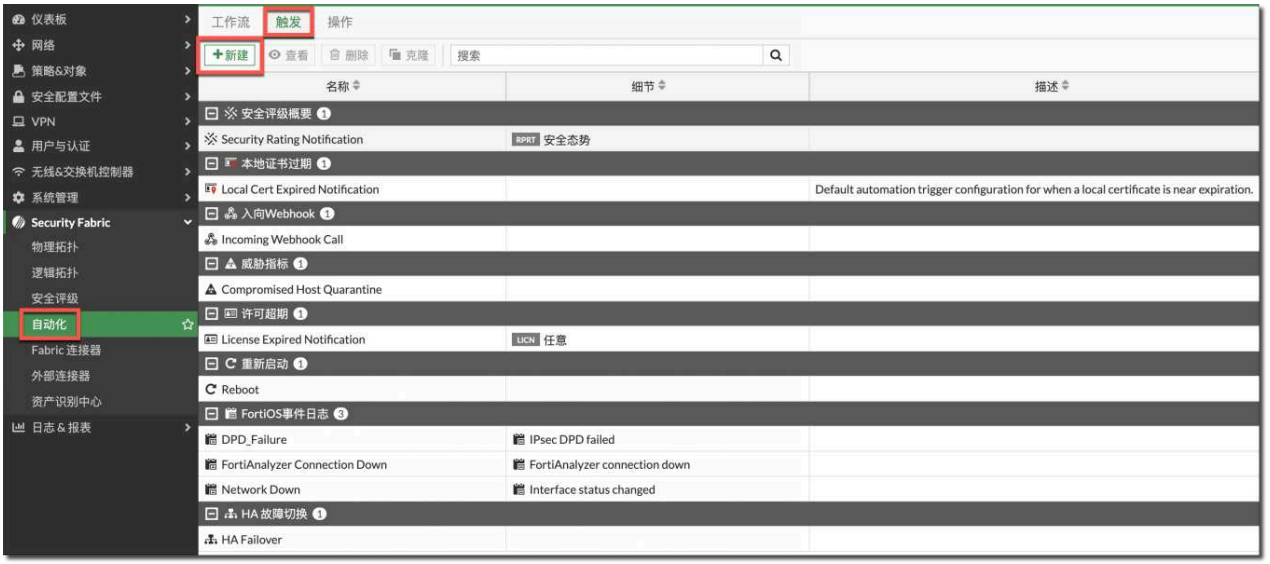
系统事件日志触发器可以从“Security Fabric→自动化→触发”页面进行配置。也可以在“日志和报告→系统事件→日志”页面上右键点击某个日志进行快速配置。

网络需求

用户想使用管理员名称为 `fgt-user1`，且登录IP为192.168.100.77的管理员登录、登出日志作为触发器。

在Security Fabric中创建

1. 进入FortiGate的“Security Fabric→自动化→触发”页面，点击新建按钮。



2. 在“其他条件”分类中选择“FortiOS事件日志”。



3. 在“事件”中选择“Admin login successful”（Log ID 32001）和“Admin logout successful”（Log ID 32003）两个日志类型。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

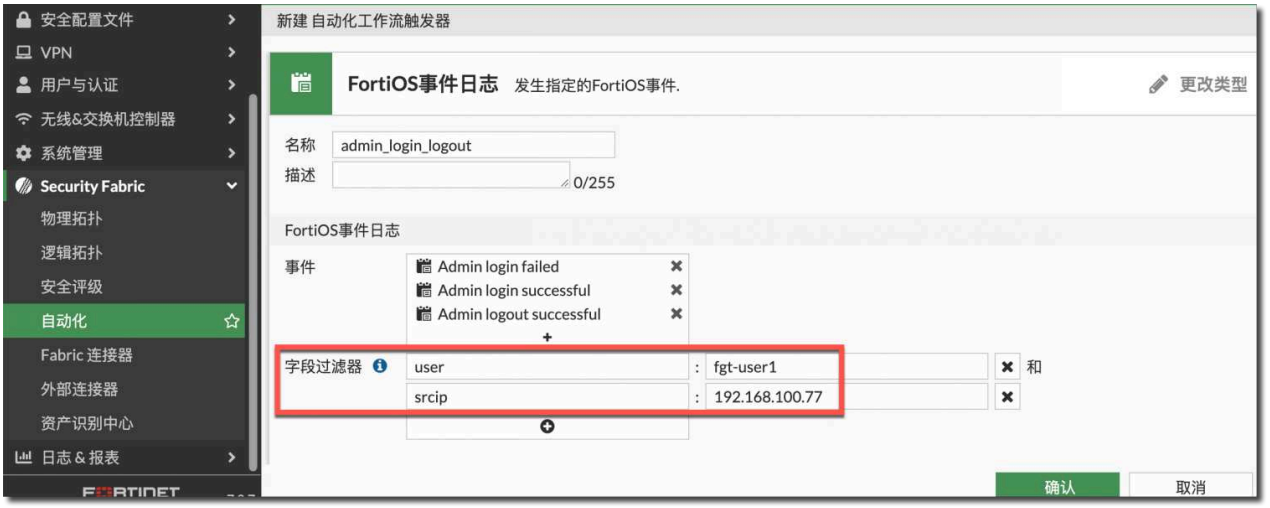


4. 在字段过滤器中，指定第一个日志字段`user`的值为`fgt-user1`，指定第二个日志字段`srcip`的值为`192.168.100.77`，点击确认下发配置。

重要

日志字段可以从相关日志文本中获取，根据需求进行配置。

```bash
date=2024-03-11 time=17:03:18 eventtime=1710147798720951460 tz="+0800" logid="0100032003" type="event" subtype="system" level="information" vd="root" logdesc="Admin logout successful" sn="1710147790" user="fgt-user1" ui="https(192.168.100.77)" method="https" srcip=192.168.100.77 dstip=10.10.12.1 action="logout" status="success" duration=8 state="Config-Changed" reason="exit" msg="Administrator fgt-user logged out from https(192.168.100.77)"
```




```bash
config system automation-trigger
    edit "admin_login_logout"
        set event-type event-log
        set logid 32002 32001 32003
        config fields
            edit 1
                set name "user"
                set value "fgt-user1"
            next
            edit 2
                set name "srcip"
                set value "192.168.100.77"
            next
        end
    next
end
```

5. 参考Security Fabric→自动化→工作流↗章节继续配置对应的Action和Stitch。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

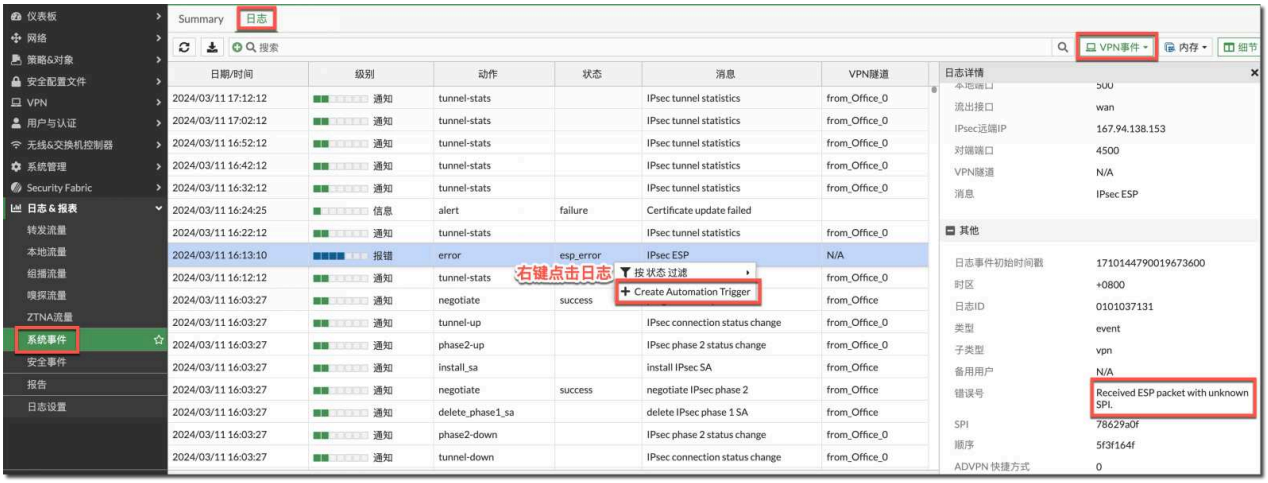
在日志中快捷创建

重要

该功能在7.4.0及更新版本支持。

需求：用户在浏览VPN事件日志时，发现有 `Received ESP packet with unknown SPI.` 的错误日志，直接通过正在浏览的该日志创建自动化的触发器。

1. 进入“日志&报表→系统事件→日志”页面，找到需要创建自动化触发器的日志，右键点击该日志，并选择“Create Automation Trigger”按钮。



2. 在弹出的新建“自动化工作流触发器”窗口中，配置触发器的名称，可自定义字段过滤器，点击确认即可下发该触发器。




```bash
config system automation-trigger
    edit "ESP_unknown_SPI"
        set event-type event-log
        set logid 37131
    next
end
```

3. 参考Security Fabric→自动化→工作流 ↗章节继续配置对应的Action和Stitch。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

UTM日志触发器

重要

该功能在7.2.0及以上版本支持。

简介

FortiGate可以配置UTM日志作为自动化的触发器（Trigger），在发生特定UTM日志ID时触发。配置时可以选择多个UTM日志ID，还可以自定义日志字段筛选器。UTM日志触发器可以从“Security Fabric→自动化→触发”页面进行配置。

重要

每个自动化工作流最多可以配置16个UTM日志ID作为触发器（Trigger）。

UTM日志触发器支持以下安全事件日志，且可以指定基于VDOM的安全事件日志：

- 异常日志（Anomaly）
- 入侵防御日志（IPS）
- SSH日志
- 反病毒日志（AV）
- 流量阻断日志（Traffic violations，被防火墙策略阻断的流量日志）
- Web过滤（Web Filter）

CLI配置方法

```bash
config system automation-trigger
    edit "Anomaly Logs"
        set trigger-type event-based
        set event-type anomaly-logs
        set vdom <name>
    next
    edit "IPS Logs"
        set trigger-type event-based
        set event-type ips-logs
        set vdom <name>
    next
    edit "SSH Logs"
        set trigger-type event-based
        set event-type ssh-logs
        set vdom <name>
    next
    edit "Traffic Violation"
        set trigger-type event-based
        set event-type traffic-violation
        set vdom <name>
    next
    edit "Virus Logs"
        set trigger-type event-based
        set event-type virus-logs
        set vdom <name>
    next
    edit "Webfilter Violation"
        set trigger-type event-based
        set event-type webfilter-violation
        set vdom <name>
    next
end
```

网络需求

FortiGate的VDOM2在遭受DoS攻击后，自动发送邮件到指定邮箱。

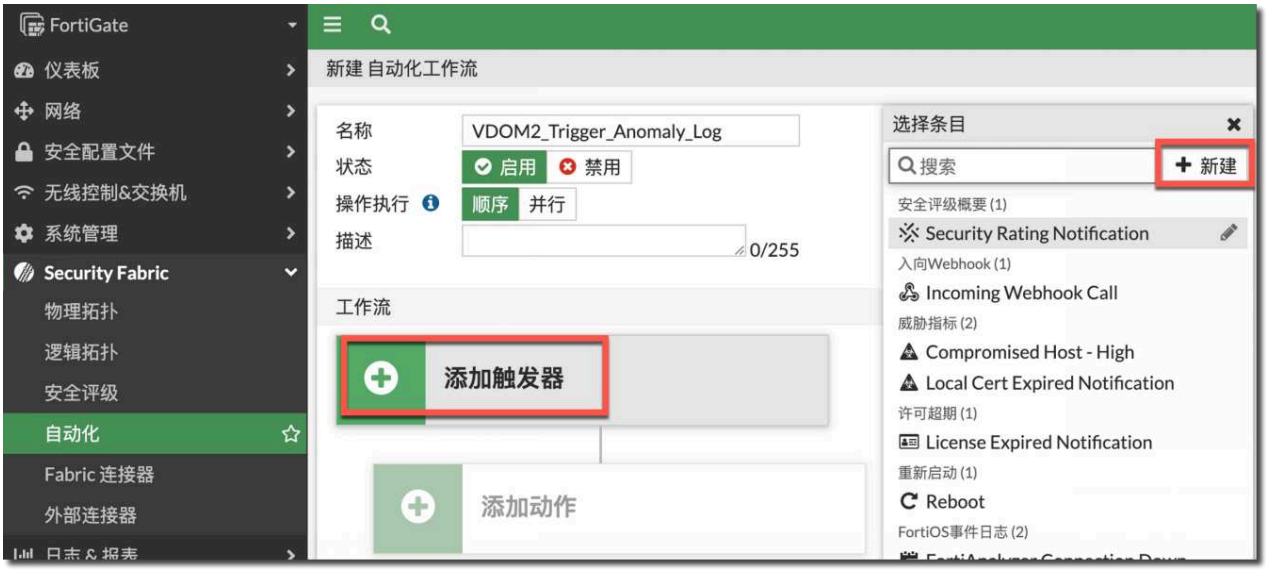
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置举例

1. 进入FortiGate全局VDOM的Security Fabric→自动化页面，新建自动化工作流。



2. 点击添加触发器按钮，在弹出的条目中选择新建。



3. 在弹出的日志类型列表中，选择Event Log分类的异常日志。



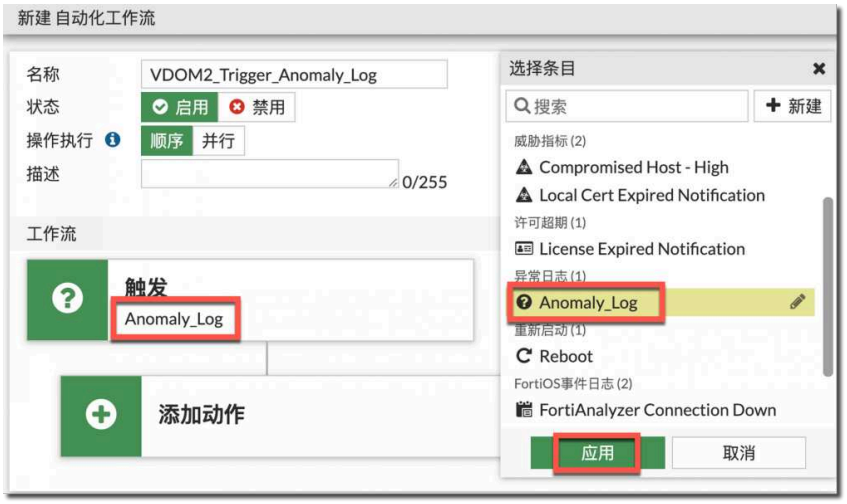
4. 配置触发器名称，并配置VDOM作为触发条件，这里以VDOM2为例，也可以选择多个VDOM，下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system global
config system automation-trigger
    edit "Anomaly_Log"
        set event-type anomaly-logs
        set vdom "VDOM2"
    next
end
```

5. 选择上步创建的触发器作为触发条件，也可以创建并选择多个触发器。

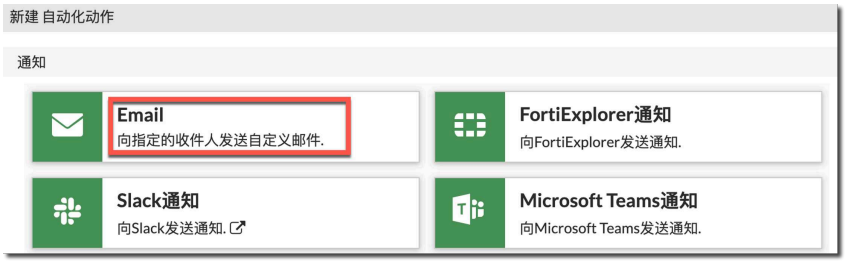


6. 点击添加动作按钮，并在弹出的条目窗口中点击新建按钮。

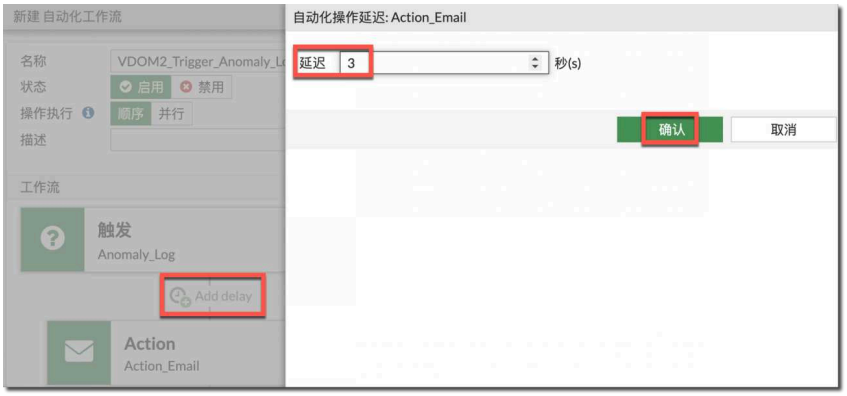


7. 在通知分类中选择Email类型的动作。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 添加触发器与动作之间的延迟为3s，点击确认下发工作流配置。




```bash
config system global
config system automation-action
    edit "Action_Email"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-from "DoNotReply@notification.fortinet.net"
        set email-subject "CSF stitch alert"
        set replacement-message enable
    next
end
```




```bash
config system global
config system automation-stitch
    edit "VDOM2_Trigger_Anomaly_Log"
        set trigger "Anomaly_Log"
        config actions
            edit 1
                set action "Action_Email"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set delay 3
                set required enable
            next
        end
    next
end
```

配置验证

1. 在FortiGate的VDOM2中配置DoS策略，并开启异常日志记录，从终端对FortiGate的VDOM2接口port2发起DoS攻击，在日志&报表→安全事件中的异常分类中，可以看到产生了UDP Flood日志。



2. 3s后收件人邮箱收到了CSF自动化发送的邮件，邮件内容为异常日志的文本。



3. 查看autod进程的debug信息，可以看到Email动作被触发。

```bash
FortiGate (global) # diagnose debug application autod -1
FortiGate (global) # diagnose debug enable
......
__action_email_hdl()-181: email action (Action_Email) is called.
from:DoNotReply@notification.fortinet.net
to:bbai@fortinet.com;
subject:CSF stitch alert
......
```

4. 查看该自动化流程的的配置和触发统计。

```bash
FortiGate (global) # diagnose test application autod 2
csf: disabled   root: no        sync connection: connecting
version:0 sync time:
total stitches activated: 4
stitch: VDOM2_Trigger_Anomaly_Log
        destinations: all
        trigger: Anomaly_Log
                type:anomaly logs
                field ids:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                        (id:6)vd=VDOM2
        local hit: 6 relayed to: 0 relayed from: 0
        actions:
                Action_Email type:email interval:0
                        delay:3 required:yes
                        subject: CSF stitch alert
                        body: %%log%%
                        sender: DoNotReply@notification.fortinet.net
                        mailto:bbai@fortinet.com;
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

证书过期触发器

简介

证书过期触发器（Certificate expiration trigger）可以在本地证书即将过期时触发自动化流程。可配置证书到期前（自定义天数0~100，默认14天）触发。

> **重要**
>
> 只针对本地证书分类中的证书（如用户证书或带私钥的Sub CA）生效。

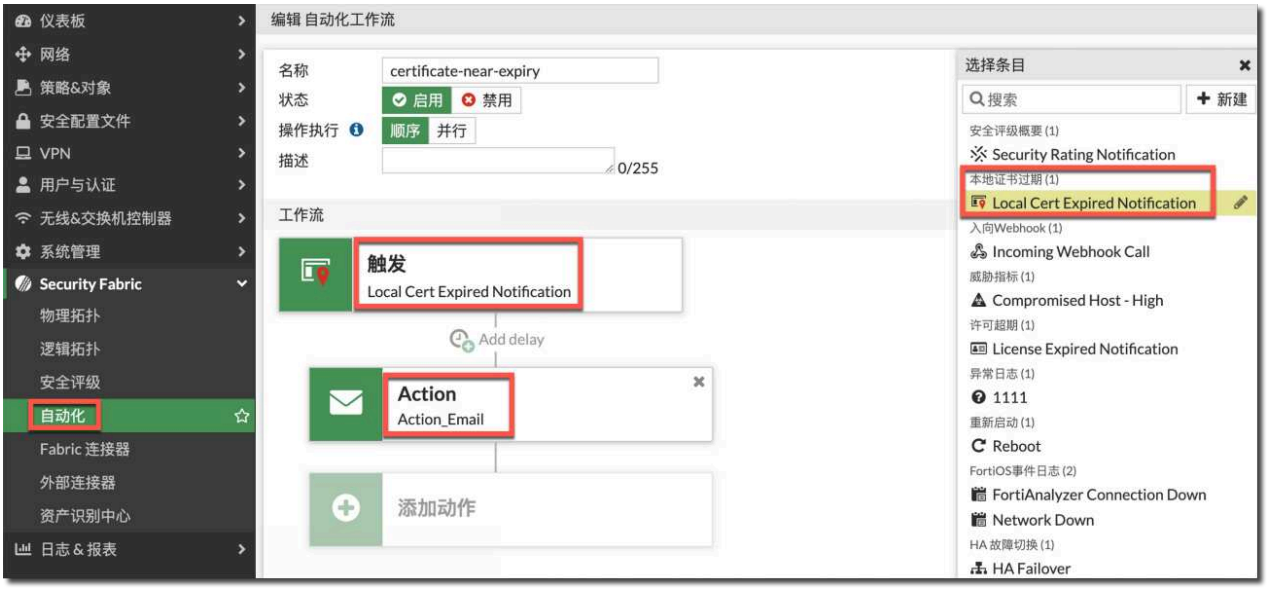
```bash
config vpn certificate setting
    set cert-expire-warning <integer>    //设置本地证书到期前触发告警的天数，范围0～100天，默认14天//
end
```

网络需求

当设备的本地证书的到期时间前1天，触发自动化流程，将本地证书即将过期的系统事件日志发送至指定邮箱。

配置步骤

1. 在Security Fabric→自动化中新建自动化工作流，触发条件选择预置的Local Certain Expired Notification（也可以手动创建该触发器），动作选择发送邮件至指定邮箱。




```bash
config system automation-trigger
    edit "Local Cert Expired Notification"
        set event-type local-cert-near-expiry
    next
end

config system automation-action
    edit "Action_Email"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-from "DoNotReply@notification.fortinet.net"
        set email-subject "CSF stitch alert"
        set replacement-message enable
    next
end

config system automation-stitch
    edit "certificate-near-expiry"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set trigger "Local Cert Expired Notification"
        config actions
            edit 1
                set action "Action_Email"
                set required enable
            next
        end
    next
end
```

2. 配置证书过期提醒为过期前1天。

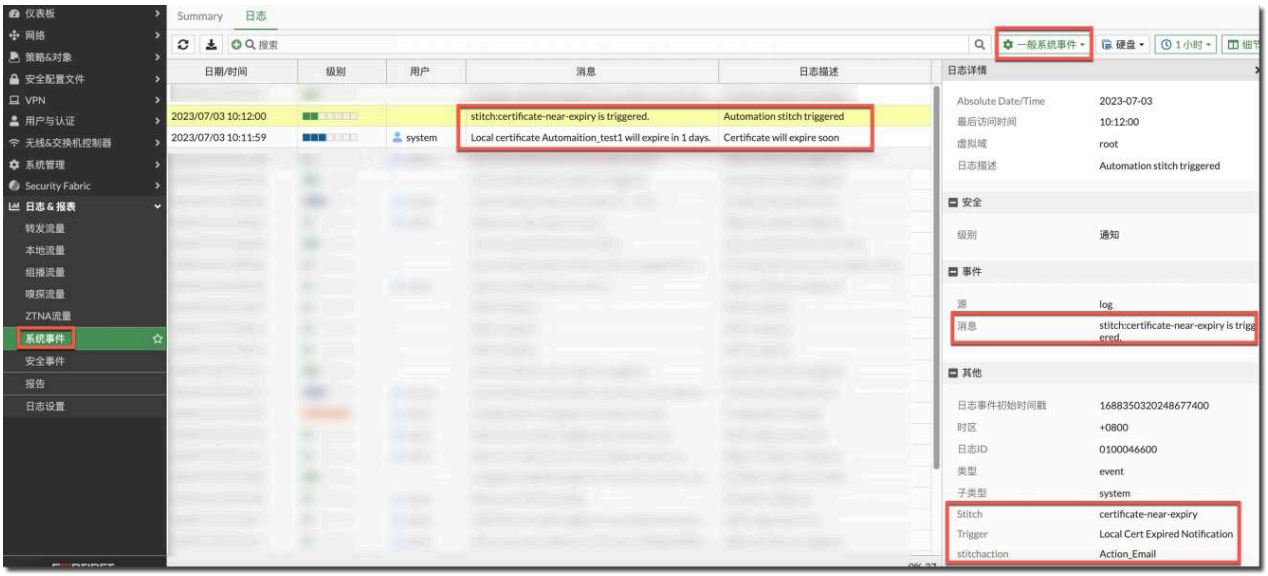
```bash
config vpn certificate setting
    set cert-expire-warning 1
end
```

3. 在FortiGate查看即将过期的用户证书、SubCA证书、CA证书（剩余有效期2天）。



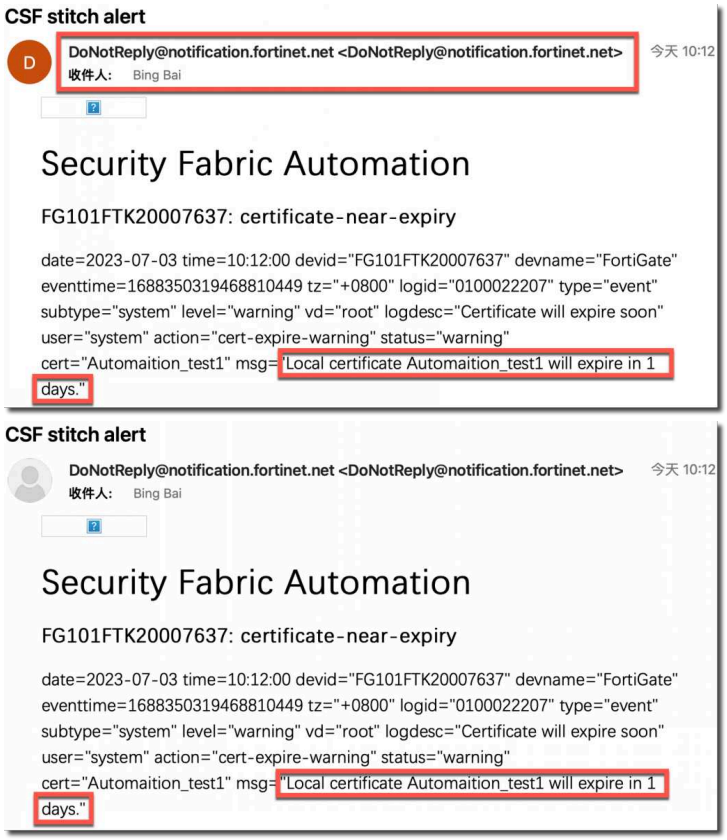
结果验证

1. 证书即将过期的触发日志如下，可以看到证书的过期倒数时间＜2天后，就会产生证书即将过期的日志，并触发配置的自动化流程。



2. 收到的邮件内容如下，只有本地证书（用户证书、Sub CA）可以触发该自动化，CA证书不会触发。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



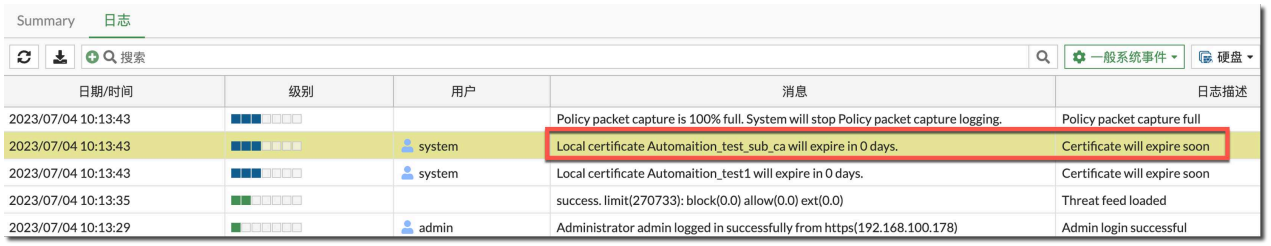
3. 查看autod进程的debug信息，可以看到Email动作被触发。

```bash
FortiGate (global) # diagnose debug application autod -1
__action_email_hdl()-181: email action (Action_Email) is called.
from:DoNotReply@notification.fortinet.net
to:bbai@fortinet.com;
subject:CSF stitch alert
```

4. 查看该自动化流程的的配置和触发统计（使用2可以看统计和配置）。

```bash
FortiGate (global) # diagnose test application autod 3
stitch: certificate-near-expiry

        local hit: 3 relayed to: 0 relayed from: 0
        last trigger:Mon Jul  3 10:12:00 2023
        last relay:
        actions:
                Action_Email:
                        done: 3 relayed to: 0 relayed from: 0
                        last trigger:Mon Jul  3 10:12:00 2023
                        last relay:
log category to stitch mapping:
id:22207 local hit: 3 relayed hits: 0
        certificate-near-expiry
```

5. 当证书的剩余时间小于1天时，产生的证书即将过期日志中，剩余时间为0天。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

计划时间触发器

计划时间触发器（Schedule trigger）可以按照计划时间来触发自动化流程，支持的计划类型如下：

- 每小时（hourly）：指定在每小时的特定分钟循环触发。
- 每天（daily）：指定在每天的特定小时和分钟循环触发。
- 每周（weekly）：指定在每周的特定某天的小时和分钟循环触发。
- 每月（monthly）：指定在每月的特定某天的小时和分钟循环触发。
- 单次（once）：指定在特定的年/月/日/小时/分钟触发一次。

```bash
config system automation-trigger
    edit <name>
        set trigger-type scheduled
        set trigger-frequency {hourly | daily | weekly | monthly | once}
        set trigger-hour <inetger>
        set trigger-minute <integer>
        set trigger-weekday {sunday | monday | tuesday | wednesday | thursday | friday | saturday}
        set trigger-day <integer>
        set trigger-datetime <YYYY-MM-DD HH:MM:SS>
    next
end
```

网络需求

在每天的凌晨3点备份FortiGate的配置文件到FTP服务器，备份的配置文件名称中要包含备份的日期。

配置步骤

1. 进入FortiGate的“Security Fabric→自动化→触发器”页面，点击“新建”按钮。



2. 在弹出的页面的“其他条件”分类中点击“计划任务”。



3. 配置触发器名称，计划任务频率选择“每天”，小时填写“3”，分钟保持默认“0”（24小时表示法），点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.






```bash
config system automation-trigger
    edit "Daily_3am"
        set trigger-type scheduled
        set trigger-hour 3
    next
end
```

4. 进入FortiGate的“Security Fabric→自动化→操作”页面，点击“新建”按钮。



5. 在弹出的页面的“通用”分类中点击“CLI脚本”。



6. 配置动作名称，脚本中填写备份配置到FTP服务器的CLI命令，点击确认下发配置。

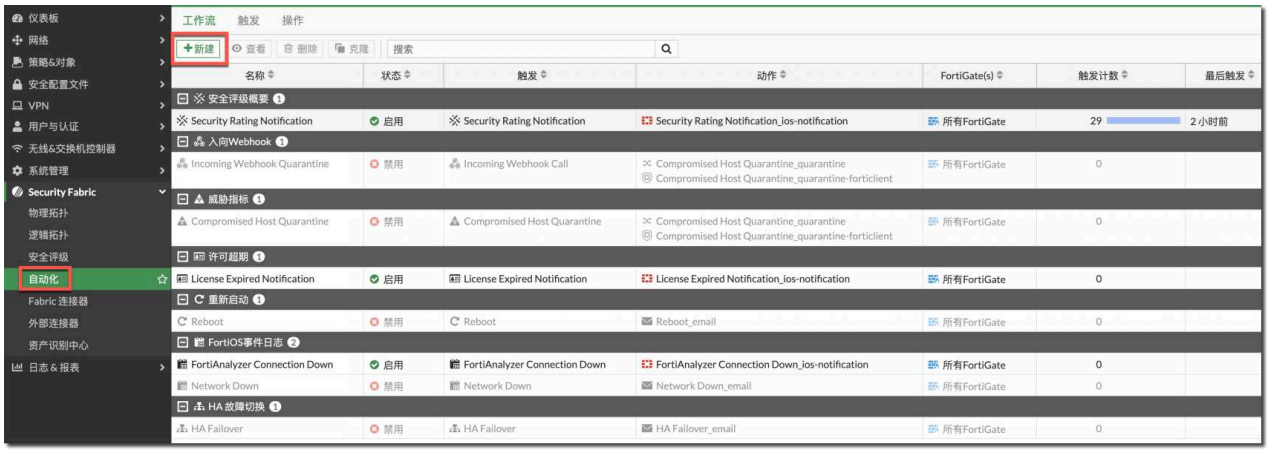
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system automation-action
    edit "Backup_config_to_FTP"
        set action-type cli-script
        set script "exe backup config ftp AutoBackup_%%date%%.conf 192.168.100.110 backup 111111"
        set accprofile "super_admin"
    next
end
```

- `AutoBackup_%%date%%.conf` 表示备份到FTP服务器的配置文件名称，其中 `%%date%%` 是一个变量，表示备份时的日期。
- `192.168.100.110` 为FTP服务器的IP，如果FTP服务器使用的是非21端口，则需要在IP后添加加 `:<port>` ，如 `192.168.100.110:2121` 。
- `backup` ： FTP用户名。
- `111111` ： FTP用户密码。

7. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击“新建”按钮。



8. 配置工作流（Stitch的）名称，在触发中选择步骤3创建的触发器，在Action中选择步骤6创建的动作，点击“确认”下发配置。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system automation-stitch
    edit "Auto_backup"
        set trigger "Daily_3am"
        config actions
            edit 1
                set action "Backup_config_to_FTP"
                set required enable
            next
        end
    next
end
```

结果验证

1. 等待自动化流程被触发，检查FortiGate自动备份并上传到FTP服务器上的配置文件，可以看到文件名字与自动化Action中配置的CLI脚本的格式一致，包含备份日期。



2. 查看FortiGate的自动化触发日志，可以看到该自动化流程在凌晨3点被触发并完成执行对应动作。

```bash
date=2024-03-13 time=03:00:17 eventtime=1710316517425603720 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="Auto_backup"
trigger="Daily_3am" stitchaction="Backup_config_to_FTP" from="scheduled" msg="stitch:Auto_backup is triggered."

date=2024-03-13 time=03:00:22 eventtime=1710316522252196480 tz="+0800" logid="0100032549" type="event"
subtype="system" level="information" vd="root" logdesc="Autoscript stop automatically" msg="script autod.10
stopped automatically"
date=2024-03-13 time=15:55:22 eventtime=1710316522239782720 tz="+0800" logid="0100032142" type="event"
subtype="system" level="notice" vd="root" logdesc="System configuration backed up" ui="auto-script"
action="backup" msg="User  backed up the configuration from auto-script"
```

3. 查看自动化触发的Debug信息，可以看到整个触发和执行备份配置文件到FTP的全部过程。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable

__action_cli_script_open()-186: cli script action:Backup_config_to_FTP is called. svc ctx:0×a1cabf0
accprof:super_admin script:
exe backup config ftp AutoBackup_%%date%%.conf 192.168.100.110 backup 111111

pid:283-__handle_msg()-414: Subscriber:4 received package. pubid:2 pkgid:65017 pkg_index:0
pid:283-__handle_pkg_logs()-356: Subscriber:4 processing package size:1198 logs:1 pickup:1
auto_event_pub_handle_log()-331: publish 46600 to subscr-node
pid:283-__subscr_close_cur_pkg()-140: close package size:1198 logs:1
__cli_script_close()-121: cli script:
autod.10
 output:
########## script name: autod.10 ##########

========== #1, 2024-03-13 15:55:17 ==========
FW1_FGT101F $  exe backup config ftp AutoBackup_2024-03-13.conf 192.168.100.110 backup 111111
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Connect to ftp server 192.168.100.110 ...
Please wait...
Send config file to ftp server OK.

__action_cli_script_close()-213: cli script action is done. script:
exe backup config ftp AutoBackup_%%date%%.conf 192.168.100.110 backup 111111
output:
########## script name: autod.10 ##########

========== #1, 2024-03-13 15:55:17 ==========
FW1_FGT101F $  exe backup config ftp AutoBackup_2024-03-13.conf 192.168.100.110 backup 111111

Connect to ftp server 192.168.100.110 ...
Please wait...
Send config file to ftp server OK.
```

4. 查看该自动化流程的状态统计信息。

```bash
FortiGate # diagnose test application autod 3
alert mail log count: 0

stitch: Auto_backup (scheduled)

        local hit: 1 relayed to: 0 relayed from: 0
        last trigger:Wed Mar 13 15:55:17 2024
        last relay:
        next scheduled trigger:Thu Mar 14 15:55:00 2024
        actions:
                Backup_config_to_FTP:
                        done: 1 relayed to: 0 relayed from: 0
                        last trigger:Wed Mar 13 03:00:17 2024
                        last relay:

logid to stitch mapping:
id:0 (scheduled stitches) local hit: 1 relayed hits: 0
        Auto_backup

log category to stitch mapping:
```

5. 附备份配置文件的CLI命令格式。

```bash
FTP:
execute backup config ftp <backup_filename> <ftp_server>[<:ftp_port>] [<user_name>] [<password>]
[<backup_password>]

TFTP:
execute backup config tftp <backup_filename> <tftp_servers> [<backup_password>]

SFTP:
execute backup config sftp <backup_filename> <sftp_server>[<:sftp_port>] <user> <password> [<backup_password>]
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

内存/CPU达到阈值时收集信息

简介

当FortiGate CPU利用率达到阈值或设备内存占用过高进入保护模式时，客户有可能为了快速恢复业务而重启设备，重启完成后，可以收集到的故障信息较少，难以定位。

自动化功能可以在FortiGate CPU利用率达到阈值或内存进入保护模式时，触发相关的CLI命令（CLI script action）来收集故障时的设备状态信息，以方便技术人员进行问题定位。

> **重要**
>
> CLI类型的动作（Action）可以收集的信息输出结果最大支持192000个字符，超过192000个字符的内容会被截断。

CLI script action配置

```bash
config system automation-action
    edit <name>
        set action-type cli-script
        set output-size <integer>
        set timeout <integer>
    next
end
```

- `output-size <integer>`：最大输出大小。单位为megabytes，范围1 ~ 1024，默认为10。
- `timeout <integer>`：执行CLI的超时时间，超过这个时间CLI未执行完成，则结束action。单位为秒，范围0 ~ 300，默认为0，表示持续等待CLI执行完成。

内存保护模式

网络需求

当FortiGate进入内存保护模式后，触发CLI动作收集设备当前的运行信息，并将信息发送至指定邮箱。

配置步骤

1. 内存保护模式阈值配置。

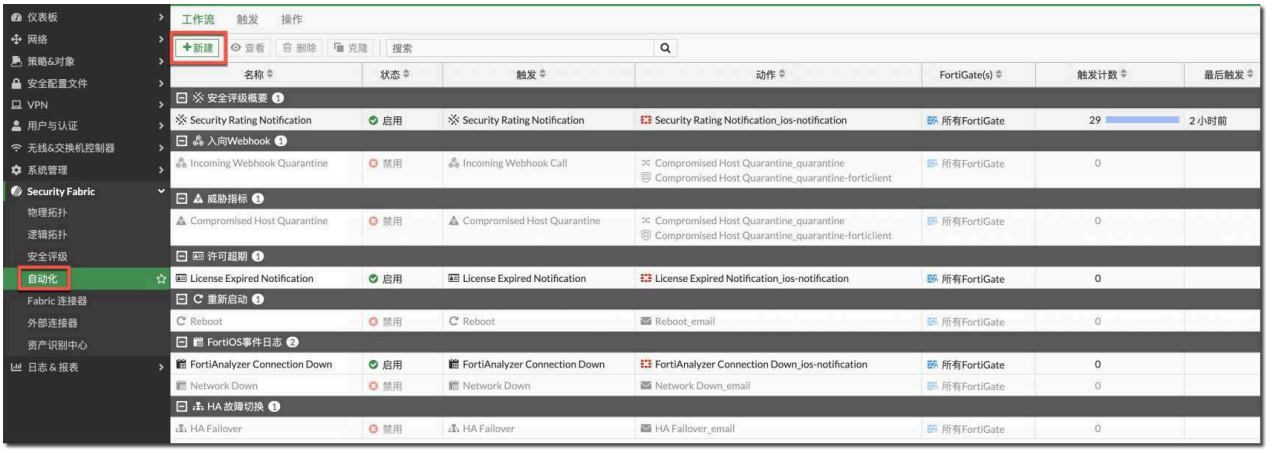
```bash
config system global
    set memory-use-threshold-extreme <percent>
    set memory-use-threshold-green <percent>
    set memory-use-threshold-red <percent>
end
```

   - `memory-use-threshold-red`：进入内存保护模式的阈值，默认为88%。
   - `memory-use-threshold-extreme`：内存保护的extreme模式，新建会话会被丢弃，默认为95%。
   - `memory-use-threshold-green`：退出内存保护模式的低阈值，默认为82%。

2. 首先配置告警邮件发送的配置（参考日志→邮件告警↗章节，也可使用默认配置）。

3. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击新建按钮，新建一个工作流。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置工作流的名称，点击“添加触发器”按钮，在右侧的“选择条目”中点击“新建”按钮。

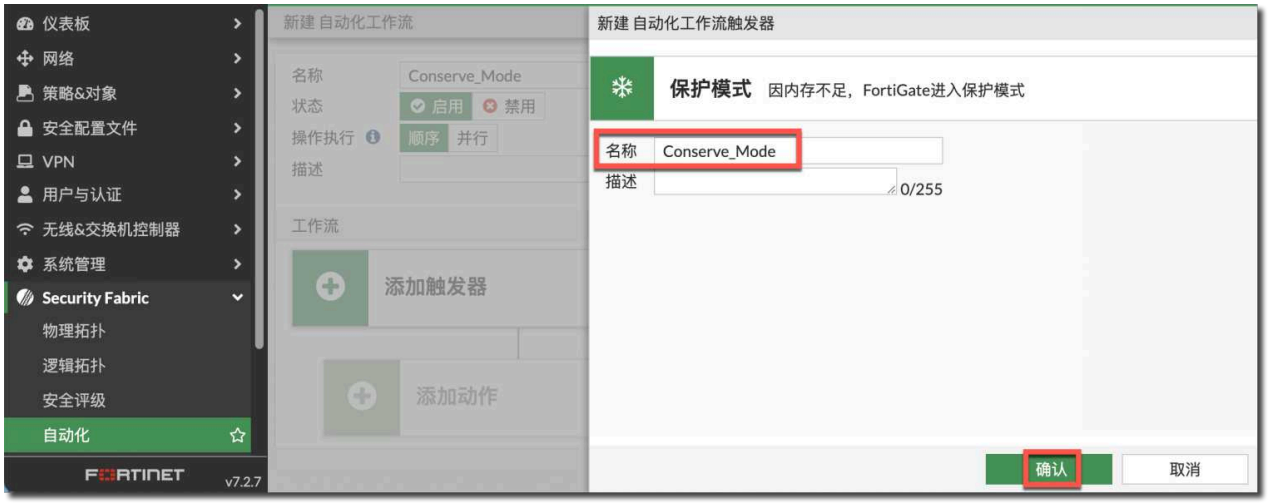


5. 在右侧弹出的窗口中，找到“系统”分类，点击“保护模式”选项。



6. 配置触发器（Trigger）的名称，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system automation-trigger
    edit "Conserve_Mode"
        set event-type low-memory
    next
end
```

7. 在选择条目中选择上步创建的触发器（Trigger），点击应用按钮。



8. 点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

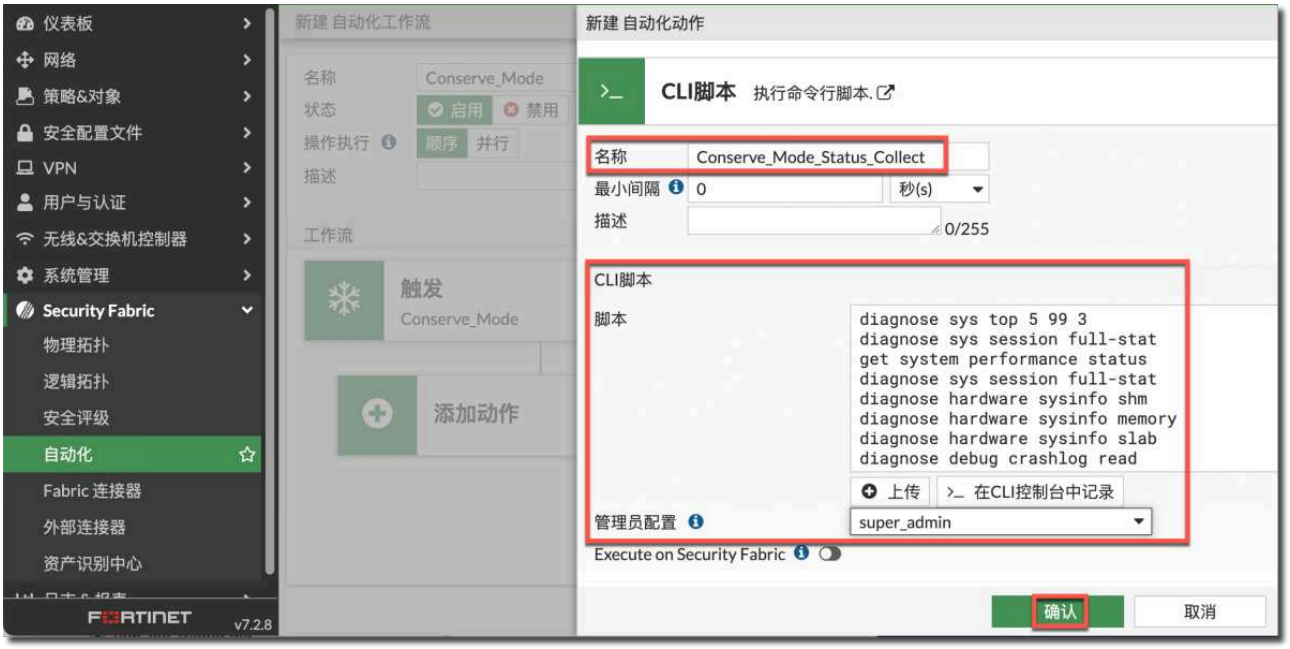


9. 在右侧弹出的窗口中，找到“通用”分类，点击“CLI脚本”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



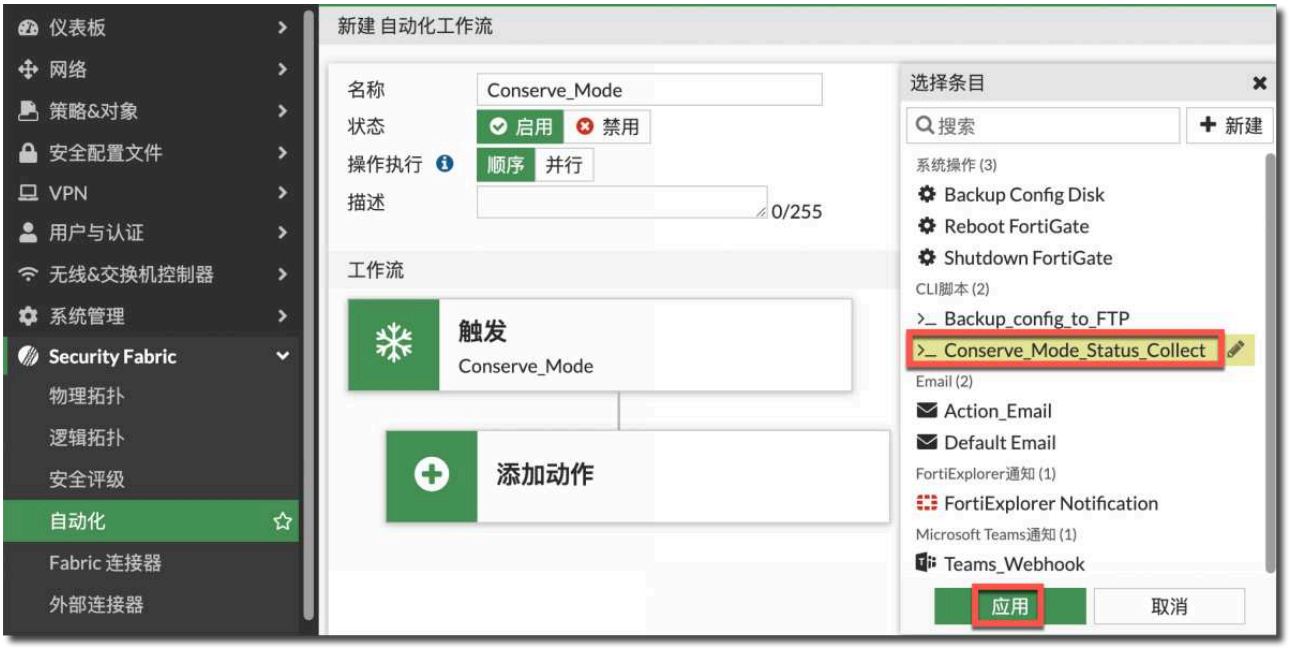
.0. 配置动作（Action）的名称，配置CLI脚本内容为FortiGate进入内存保护模式后收集信息需要执行的CLI命令，点击确认下发配置。



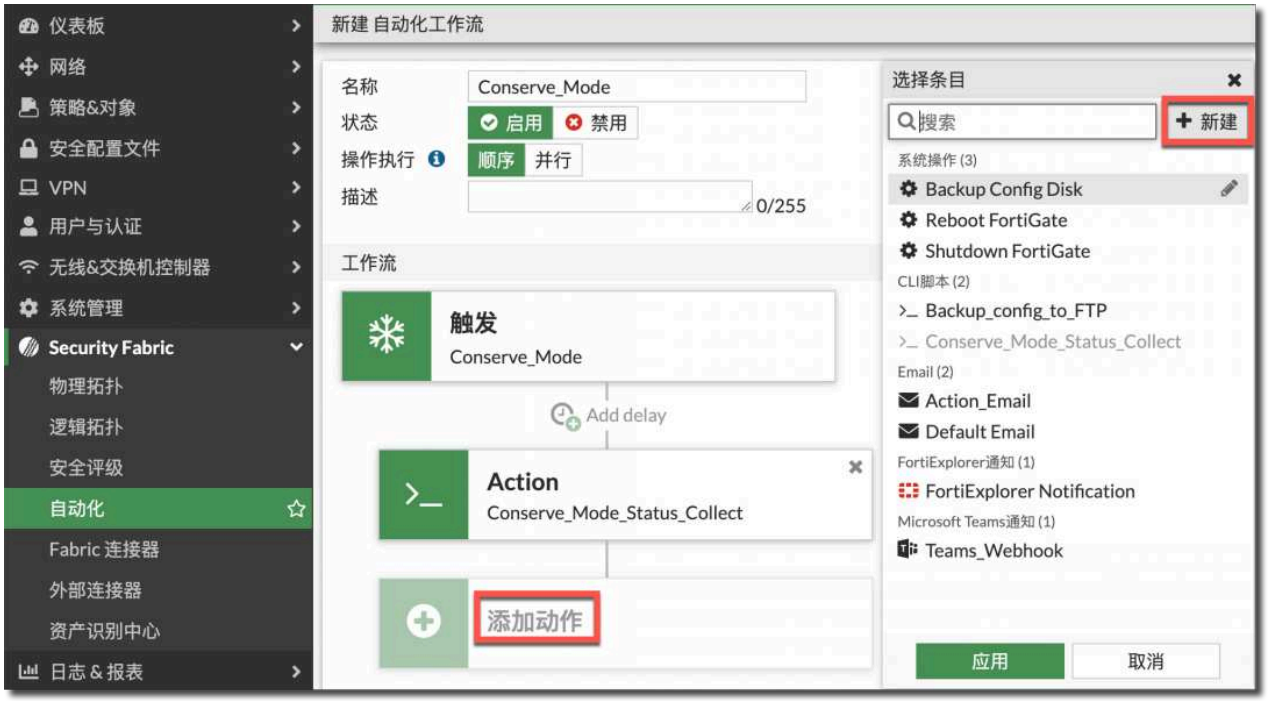

```bash
config system automation-action
    edit "Conserve_Mode_Status_Collect"
        set action-type cli-script
        set script "diagnose sys top 5 99 3
diagnose sys session full-stat
get system performance status
diagnose sys session full-stat
diagnose hardware sysinfo shm
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose debug crashlog read"
        set accprofile "super_admin"
    next
end
```

.1. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

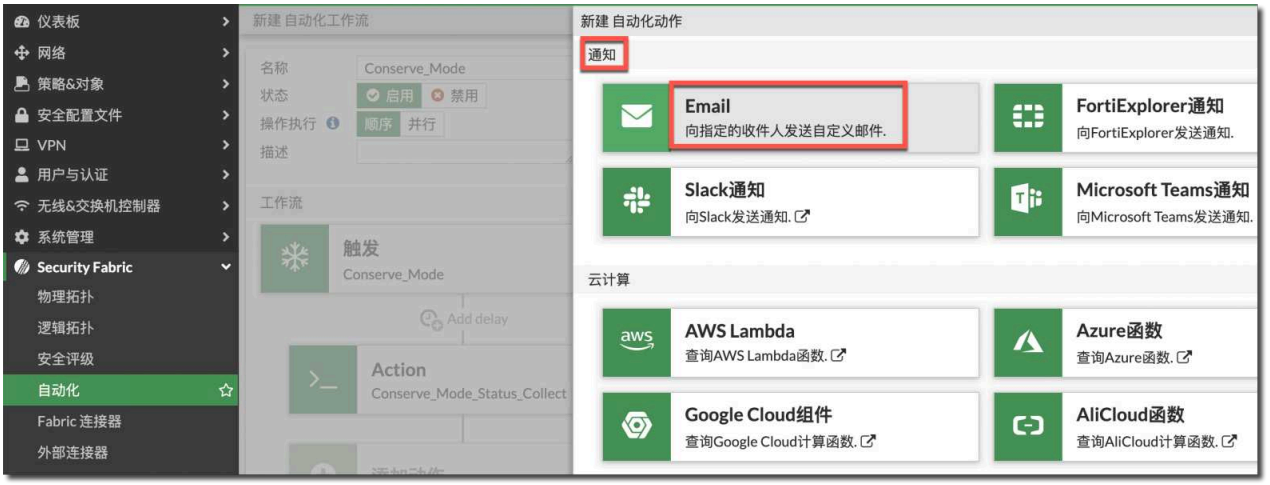


2. 再次点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

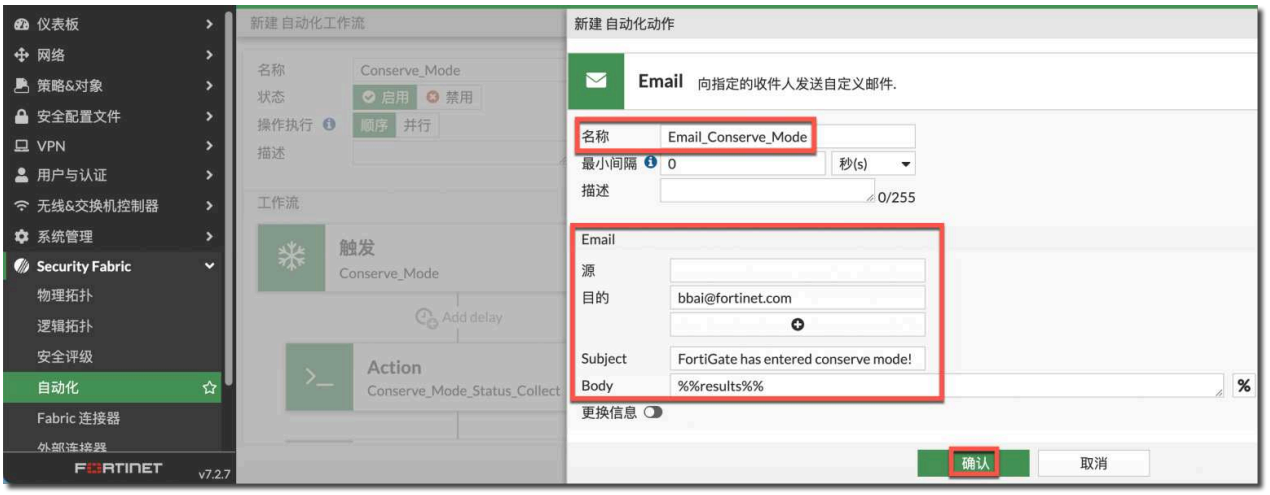


3. 在右侧弹出的窗口中，找到“通知”分类，点击“Email”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 配置动作（Action）的名称，以及邮件通知的收件人、邮件标题，邮件内容填写 `%%results%%` ，这是一个变量，表示使用前序动作CLI命令执行的结果作为邮件正文，点击确认下发配置。

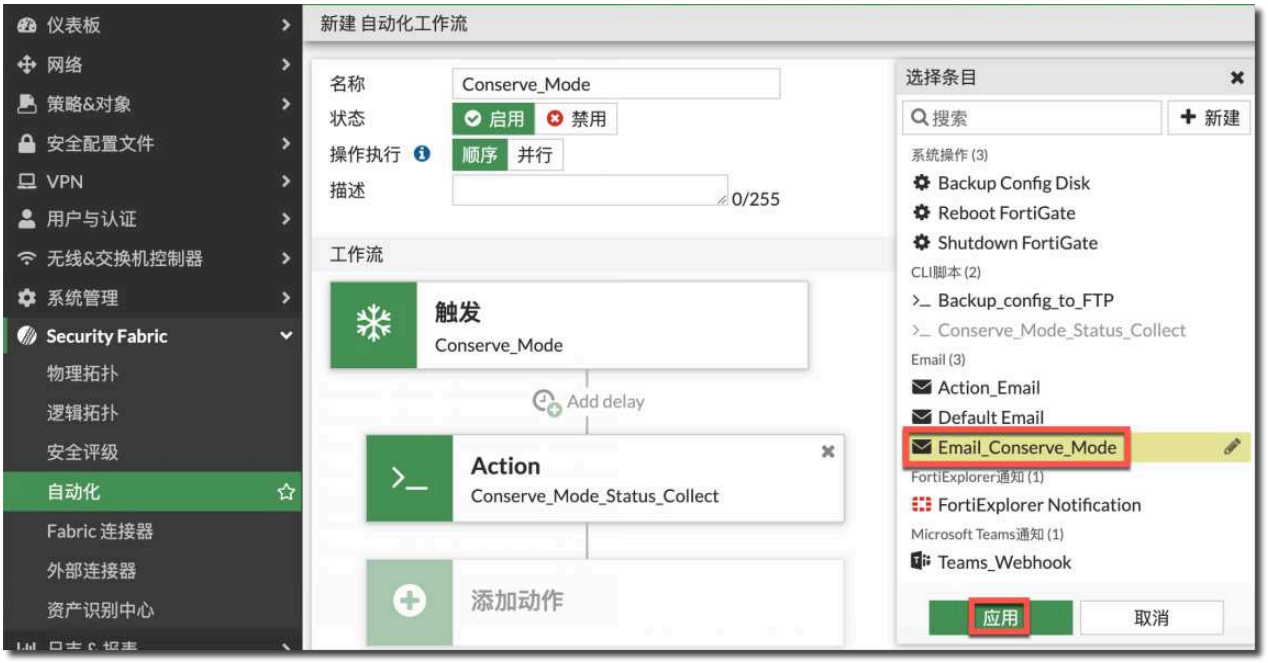


- 最小间隔：如果Trigger频繁触发了，Action执行的最小间隔。
- 源：指定邮件通知的发件人，默认为DoNotReply@notification.fortinet.net。
- 目的：配置邮箱的收件人，可以配置多个收件人。
- Body：邮件内容。
- 更换信息：可以更换为自定义内容和格式。

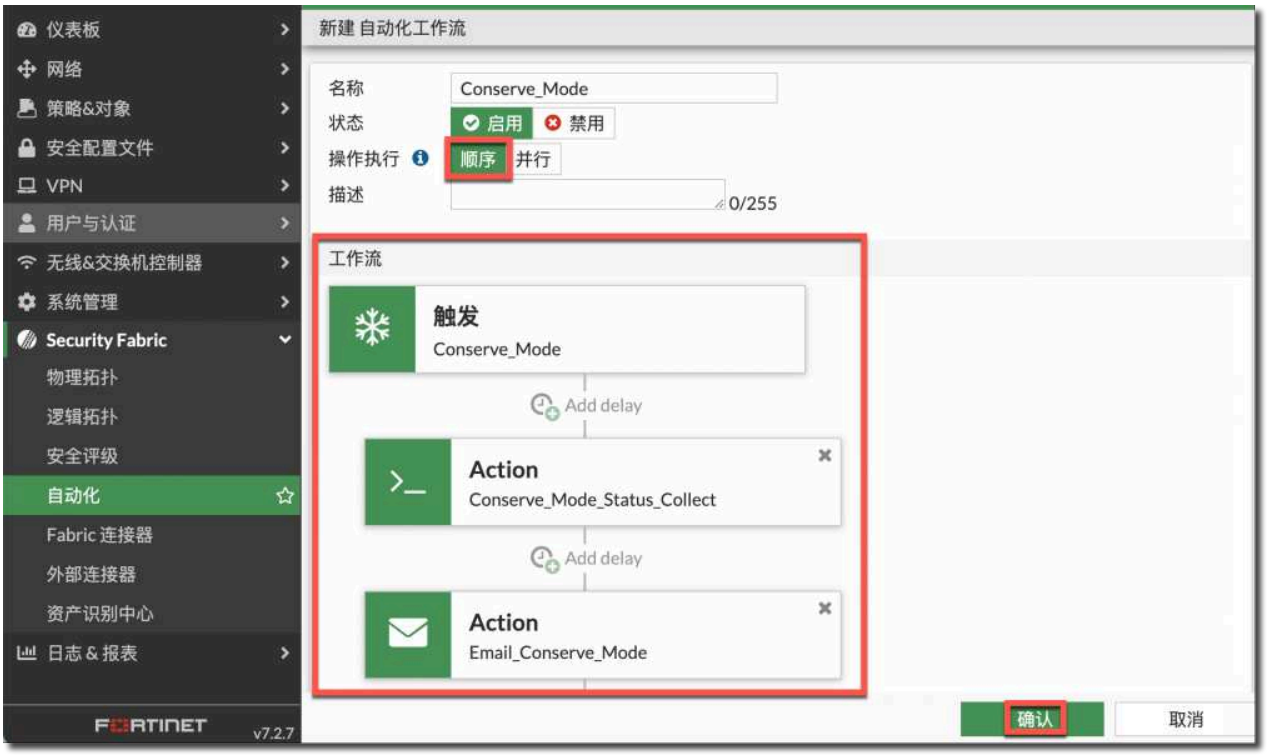
```bash
config system automation-action
    edit "Email_Conserve_Mode"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "FortiGate has entered conserve mode!"
        set message "%%results%%"
    next
end
```

5. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 检查无误后，点击确认下发配置。



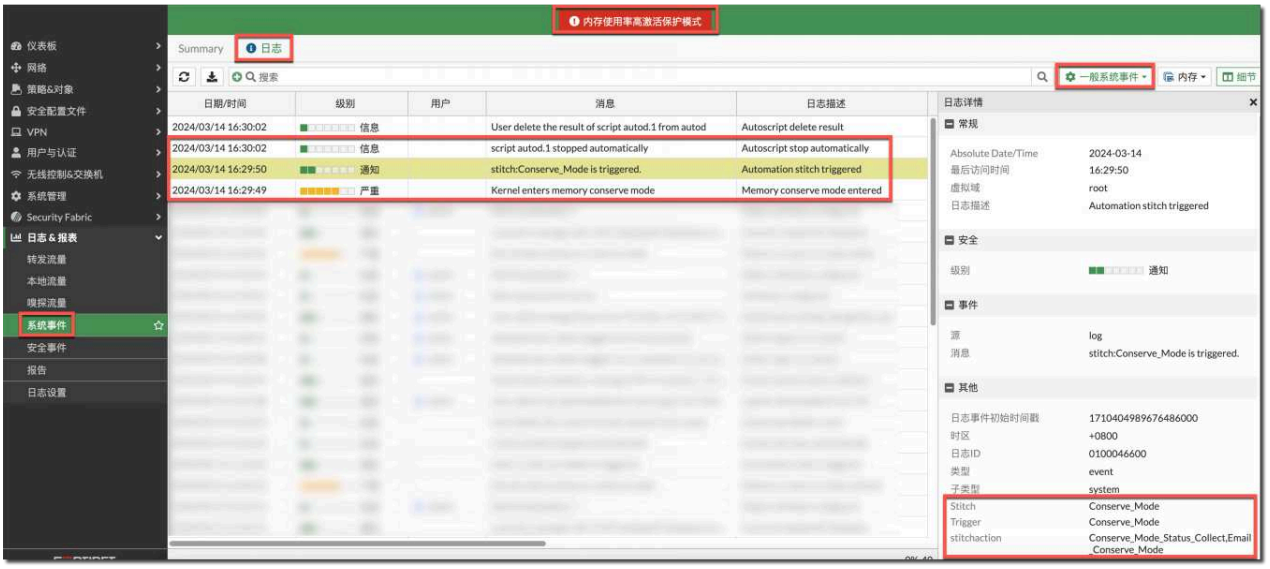

```bash
config system automation-stitch
    edit "Conserve_Mode"
        set trigger "Conserve_Mode"
        config actions
            edit 1
                set action "Conserve_Mode_Status_Collect"
                set required enable
            next
            edit 2
                set action "Email_Conserve_Mode"
                set required enable
            next
        end
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

配置验证

1. 触发FortiGate进入内存保护模式（Conserve Mode）。

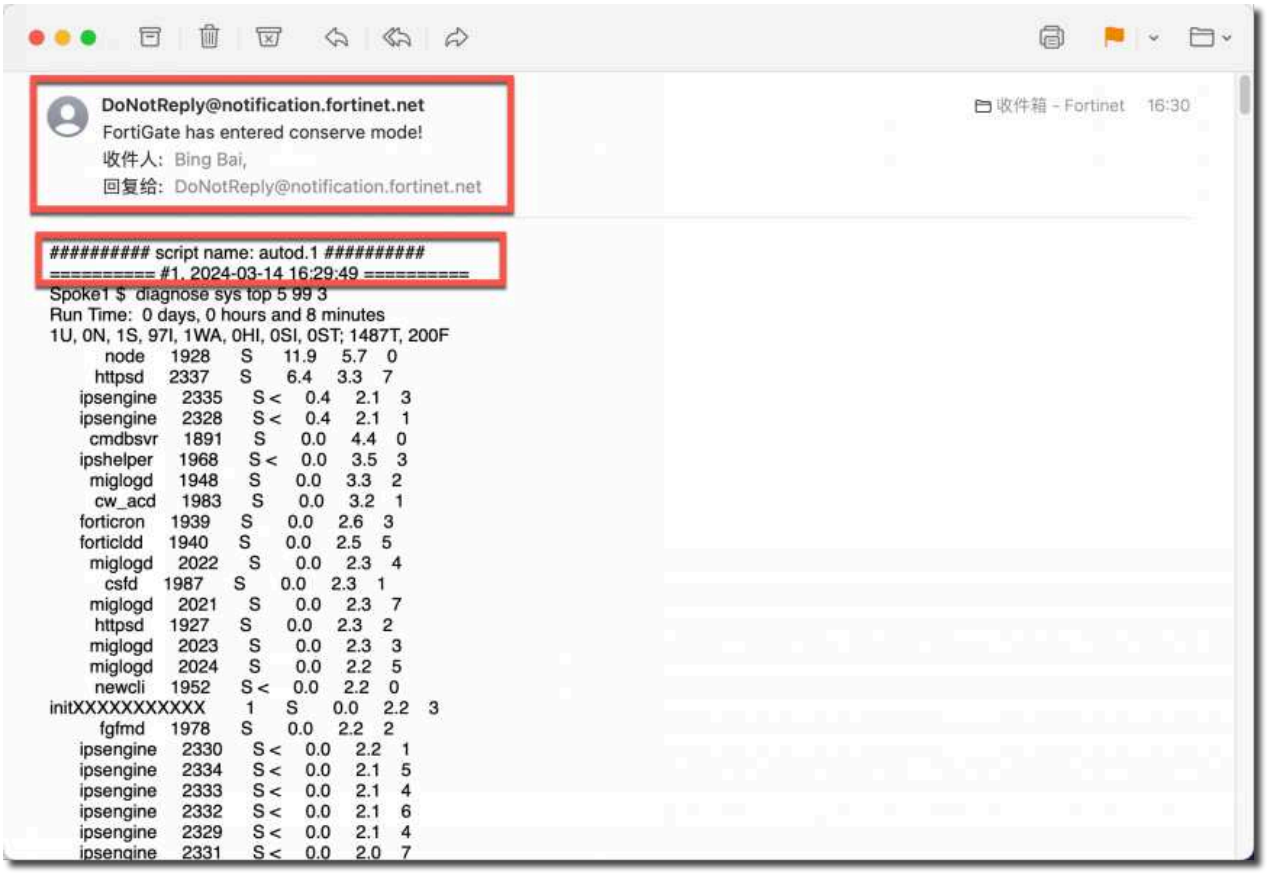
2. 触发自动化程序，相关自动化日志如下。




```bash
date=2024-03-14 time=16:29:50 eventtime=1710404989676485934 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="Conserve_Mode"
trigger="Conserve_Mode" stitchaction="Conserve_Mode_Status_Collect,Email_Conserve_Mode" from="log"
msg="stitch:Conserve_Mode is triggered."

date=2024-03-14 time=16:29:49 eventtime=1710404989471003340 tz="+0800" logid="0100022011" type="event"
subtype="system" level="critical" vd="root" logdesc="Memory conserve mode entered" service="kernel" conserve="on"
total=1487 MB used=1118 MB red="1115 MB" green="1040 MB" msg="Kernel enters memory conserve mode"
```

3. 收件人邮箱收到了告警邮件，邮件内容为通过CLI动作收集到的设备状态信息，发件人为默认的DoNotReply@notification.fortinet.net。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 对应的自动化触发Debug信息。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable

__action_cli_script_open()-186: cli script action:Conserve_Mode_Status_Collect is called. svc ctx:0×fc044a0
accprof:super_admin script:
diagnose sys top 5 99 3
diagnose sys session full-stat
get system performance status
diagnose sys session full-stat
diagnose hardware sysinfo shm
diagnose hardware sysinfo memory
diagnose debug crashlog read

__cli_script_close()-121: cli script:
autod.2
 output:
########## script name: autod.2 ##########

========== #1, 2024-03-14 16:35:13 ==========
Spoke1 $  diagnose sys top 5 99 3
Run Time:  0 days, 0 hours and 13 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 1487T, 217F
          autod     1988      S       1.0     1.7    5
      ipshelper     1968      S <     0.5     3.4    7
      forticron     1939      S       0.5     2.6    7
      ipsengine     2441      S <     0.5     2.2    0
      ipsengine     2439      S <     0.5     2.1    4

......

__action_cli_script_close()-213: cli script action is done. script:
diagnose sys top 5 99 3
diagnose sys session full-stat
get system performance status
diagnose sys session full-stat
diagnose hardware sysinfo shm
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
diagnose hardware sysinfo memory
diagnose debug crashlog read
output:
########## script name: autod.2 ##########

========== #1, 2024-03-14 16:35:13 ==========
Spoke1 $  diagnose sys top 5 99 3
Run Time:  0 days, 0 hours and 13 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 1487T, 217F
           autod     1988      S       1.0     1.7    5
       ipshelper     1968      S <     0.5     3.4    7
       forticron     1939      S       0.5     2.6    7
       ipsengine     2441      S <     0.5     2.2    0
       ipsengine     2439      S <     0.5     2.1    4

......

pid:1988-__handle_msg()-414: Subscriber:4 received package. pubid:2 pkgid:73 pkg_index:0
pid:1988-__handle_pkg_logs()-356: Subscriber:4 processing package size:516 logs:1 pickup:1
auto_event_pub_handle_log()-331: publish 32550 to subscr-node
pid:1988-__subscr_close_cur_pkg()-140: close package size:516 logs:1
__action_email_hdl()-181: email action (Email_Conserve_Mode) is called.
from:
to:bbai@fortinet.com;
subject:FortiGate has entered conserve mode!
```

5. 发送邮件的Debug信息如下。

```bash
FortiGate # diagnose debug application alertmail -1
FortiGate # diagnose debug enable

Arrived msg(type 9, 46668 bytes):bbai@fortinet.com;

FortiGate has entered conserve mode!
########## script name: autod.3 ##########
========== #1, 2024-03-14 16:35:13 ==========
Spoke1 $  diagnose sys top 5 99 3
Run Time:  0 days, 0 hours and 13 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 1487T, 217F
           autod     1988      S       1.0     1.7    5
       ipshelper     1968      S <     0.5     3.4    7
       forticron     1939      S       0.5     2.6    7
       ipsengine     2441      S <     0.5     2.2    0
       ipsengine     2439      S <     0.5     2.1    4

......

    mail_info:
        from:notification.fortinet.net  user:DoNotReply@notification.fortinet.net
mail_info:
        reverse path:DoNotReply@notification.fortinet.net
        user name:DoNotReply
to[0]:bbai@fortinet.com
⟸_init_mail_info
create session
resolve notification.fortinet.net to 1 IP
⟹ send mail
connecting to 208.91.114.151 port 465
send mail 0×fb2cbb0 session 0×fb315e0
session_io_event: creating ssl structure for session 0×fb315e0
create_ssl_ctx
create_ssl: 0×7f99cedbd000
sessionn 0×fb315e0, SSL connected
session: 0×fb315e0, rsp_state: greeting, code: 220
session: 0×fb315e0, rsp_state: ehlo, code: 250
session: 0×fb315e0, rsp_state: mail, code: 250
session: 0×fb315e0, rsp_state: rcpt, code: 250
session: 0×fb315e0, rsp_state: data, code: 354
⟹ send: ########## script name: autod.3 ##########
========== #1, 2024-03-14 16:35:13 ==========
Spoke1 $  diagnose sys top 5 99 3
Run Time:  0 days, 0 hours and 13 minutes
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 1487T, 217F
           autod     1988      S       1.0     1.7    5
       ipshelper     1968      S <     0.5     3.4    7
       forticron     1939      S       0.5     2.6    7
       ipsengine     2441      S <     0.5     2.2    0
       ipsengine     2439      S <     0.5     2.1    4

......

1session: 0×fb315e0, rsp_state: data2, code: 250
session: 0×fb315e0, rsp_state: quit, code: 221
session finined
_session_on_destroy
⟸ send mail success, m = 0×fb2cbb0 s = 0×fb315e0
```

平均CPU使用率高

网络需求

当FortiGate的CPU多个核心的平均利用率达到设定的阈值后，触发CLI动作收集设备当前的运行信息，并将信息发送至指定邮箱。

配置步骤

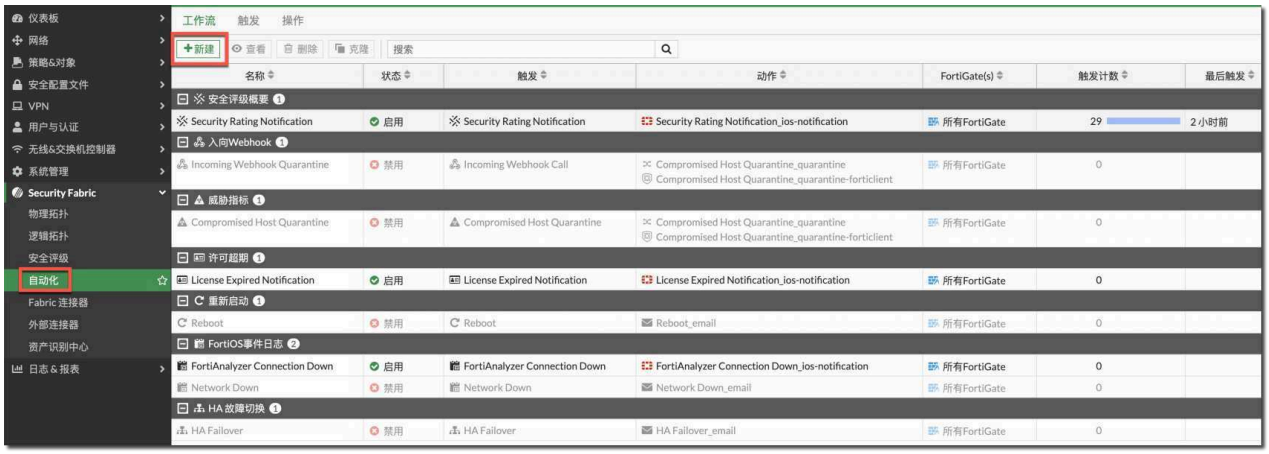
1. CPU阈值配置。

```bash
config system global
    set cpu-use-threshold 85
end
```

   - `cpu-use-threshold`：CPU所有核心的平均利用率阈值，默认为90%。

2. 首先配置告警邮件发送的配置（参考日志→邮件告警↗章节，也可使用默认配置）。

3. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击新建按钮，新建一个工作流。



4. 配置工作流的名称，点击“添加触发器”按钮，在右侧的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 在右侧弹出的窗口中，找到“系统”分类，点击“高CPU使用率”选项。



6. 配置触发器（Trigger）的名称，点击确认下发配置。




```bash
config system automation-trigger
    edit "CPU_High"
        set event-type high-cpu
    next
end
```

7. 在选择条目中选择上步创建的触发器（Trigger），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



8. 点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

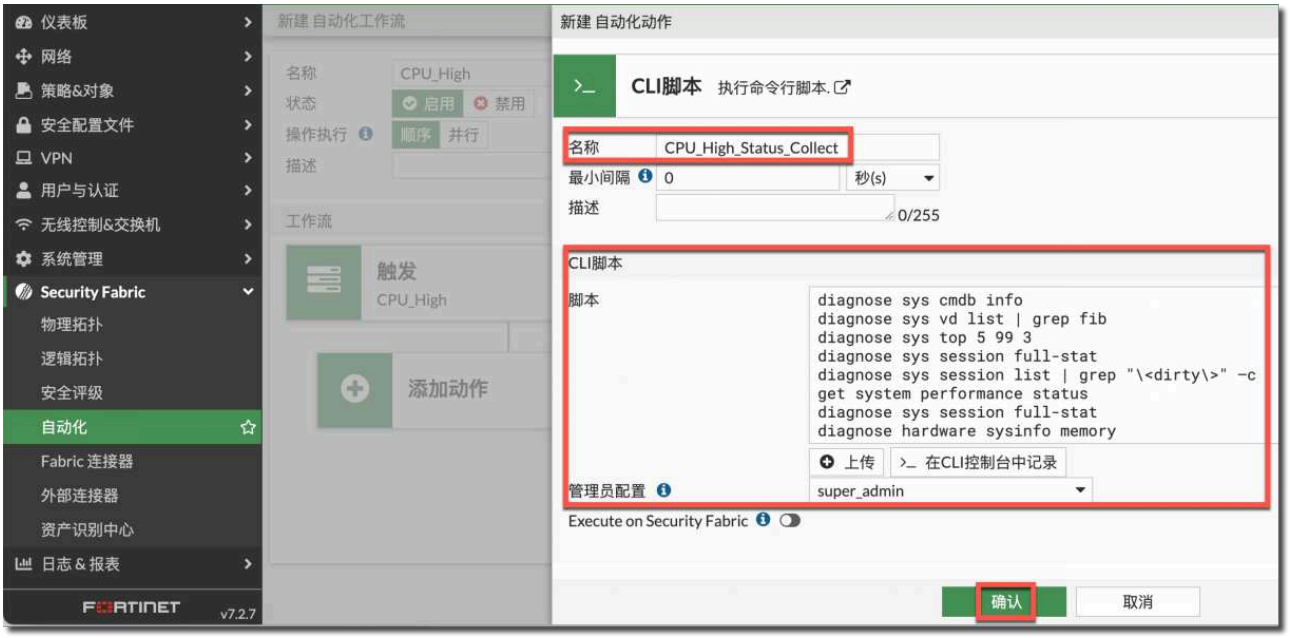


9. 在右侧弹出的窗口中，找到“通用”分类，点击“CLI脚本”选项。



.0. 配置动作（Action）的名称，配置CLI脚本内容为FortiGated的CPU利用率达到阈值后收集信息需要执行的CLI命令，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



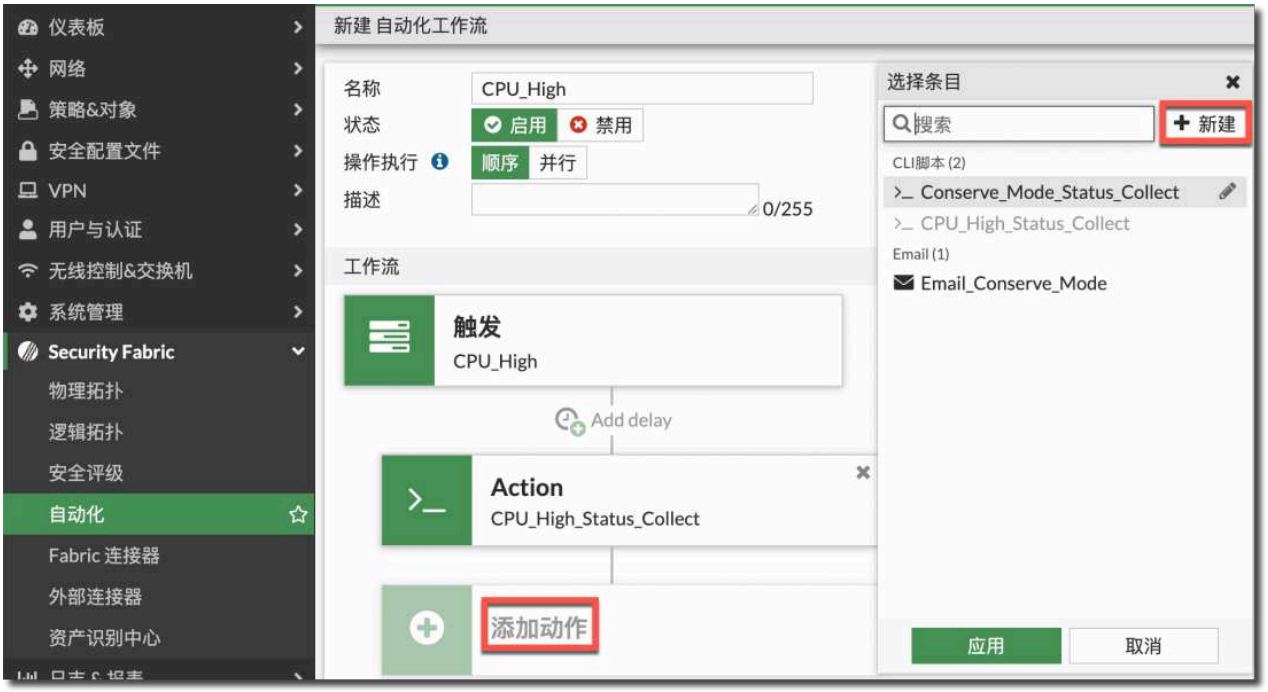

```bash
config system automation-action
    edit "CPU_High_Status_Collect"
        set action-type cli-script
        set script "diagnose sys cmdb info
diagnose sys vd list | grep fib
diagnose sys top 5 99 3
diagnose sys session full-stat
diagnose sys session list | grep \"\\<dirty\\>\" -c
get system performance status
diagnose sys session full-stat
diagnose hardware sysinfo memory"
        set accprofile "super_admin"
    next
end
```

1. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

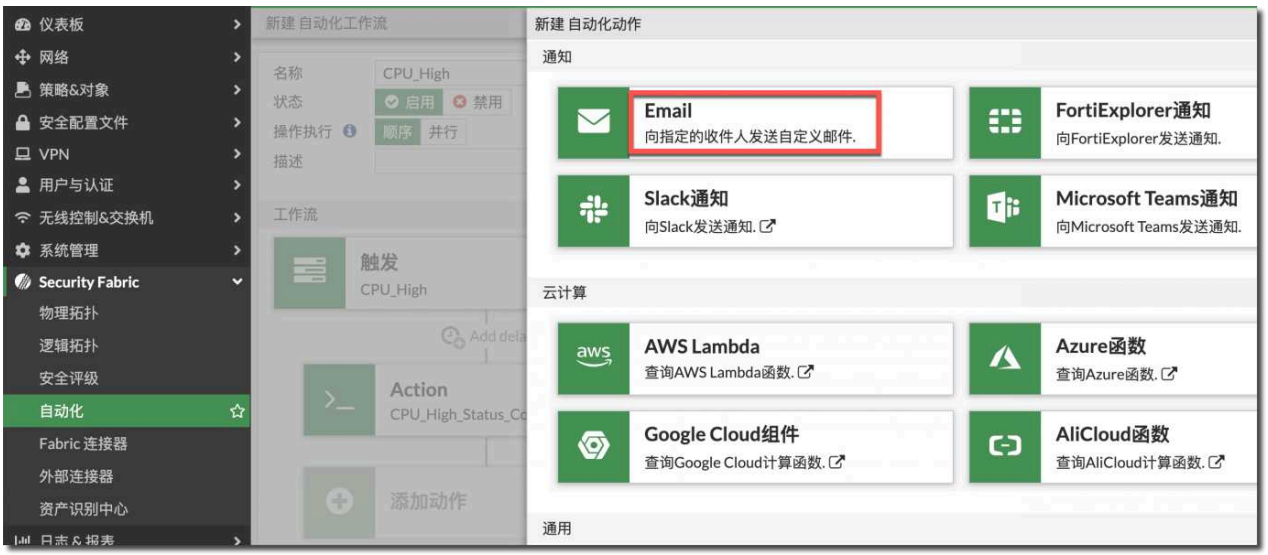


2. 再次点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

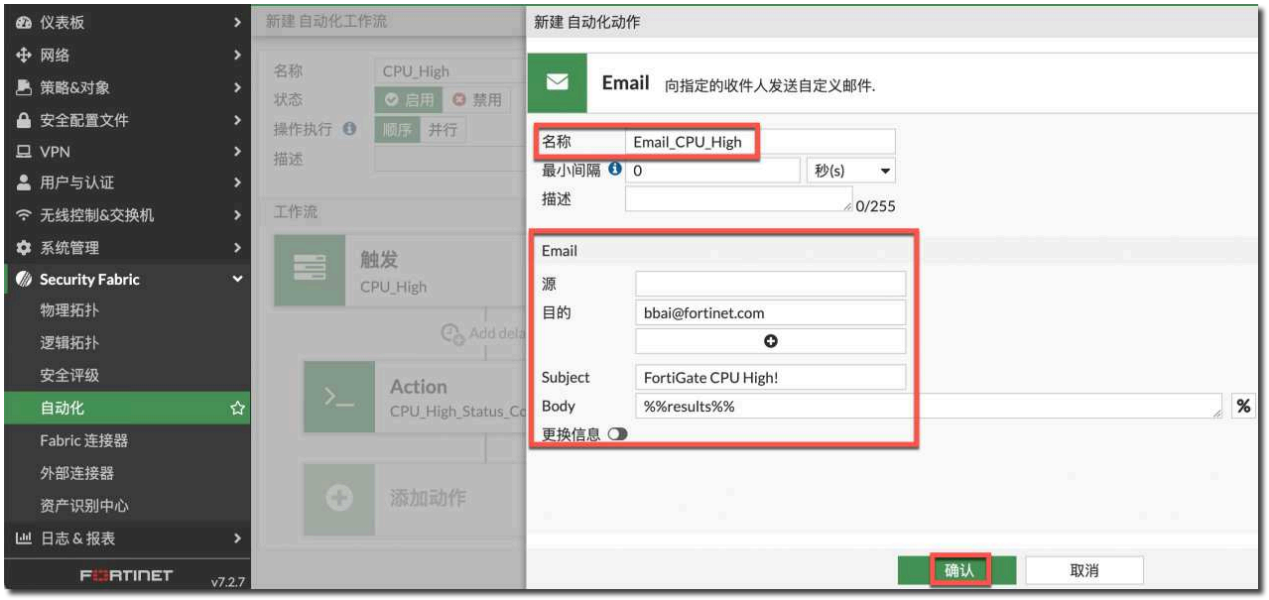


3. 在右侧弹出的窗口中，找到“通知”分类，点击“Email”选项。



4. 配置动作（Action）的名称，以及邮件通知的收件人、邮件标题，邮件内容填写 `%%results%%` ，这是一个变量，表示使用前序动作CLI命令执行的结果作为邮件正文，点击确认下发配置。

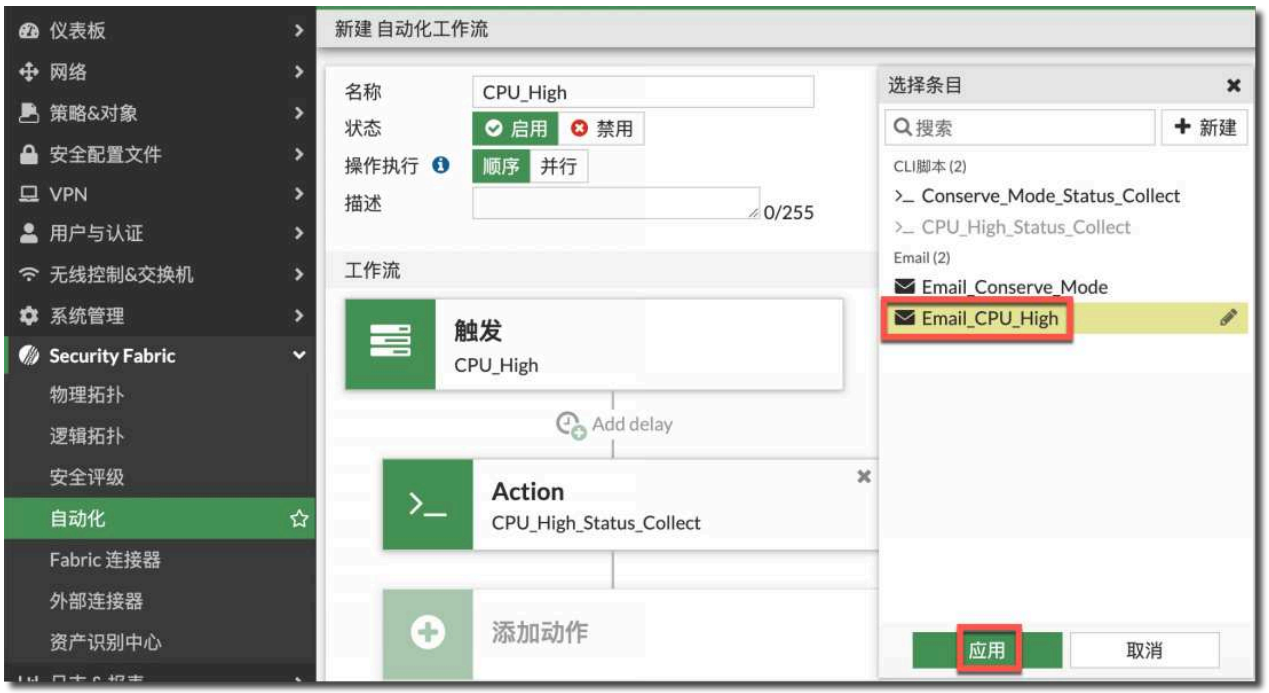
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 最小间隔：如果Trigger频繁触发了，Action执行的最小间隔。
- 源：指定邮件通知的发件人，默认为DoNotReply@notification.fortinet.net。
- 目的：配置邮箱的收件人，可以配置多个收件人。
- Body：邮件内容。
- 更换信息：可以更换为自定义内容和格式。

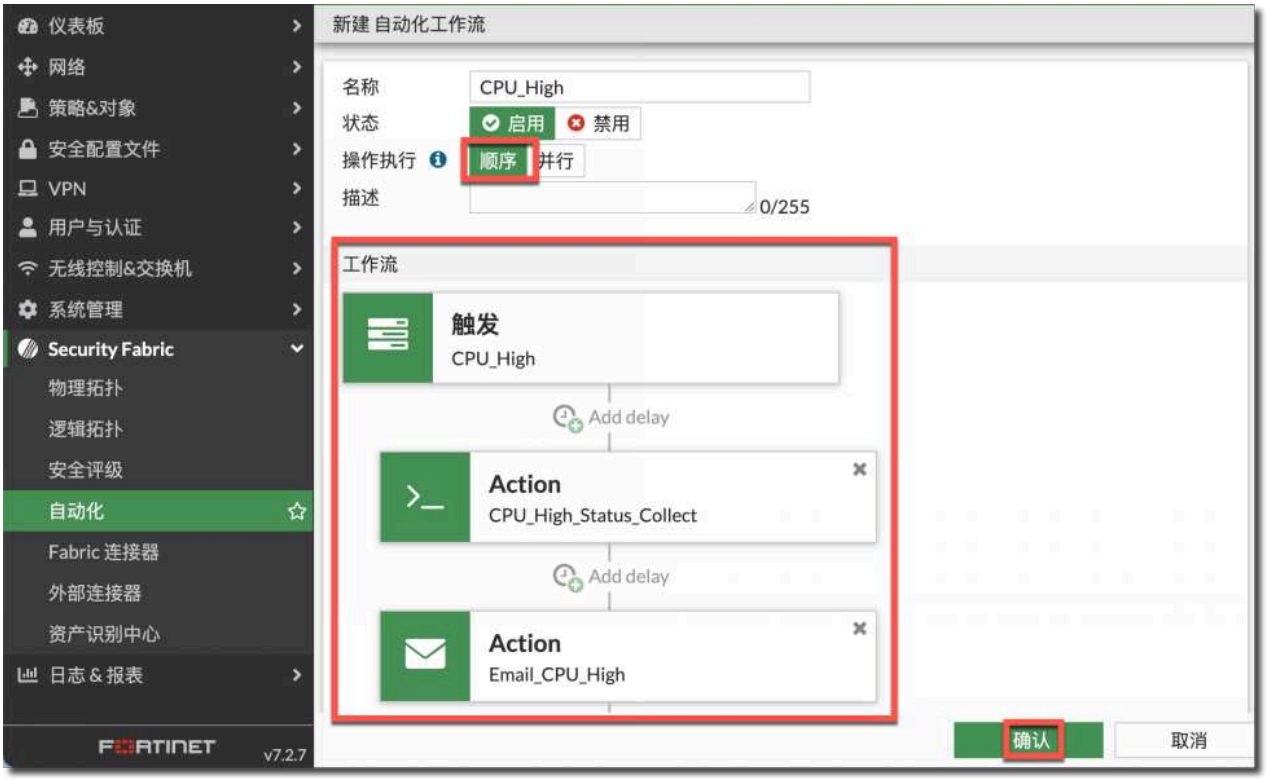
```bash
config system automation-action
    edit "Email_CPU_High"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "FortiGate CPU High!"
        set message "%%results%%"
    next
end
```

5. 在选择条目中选择上步创建的动作（Action），点击应用按钮。



6. 检查无误后，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



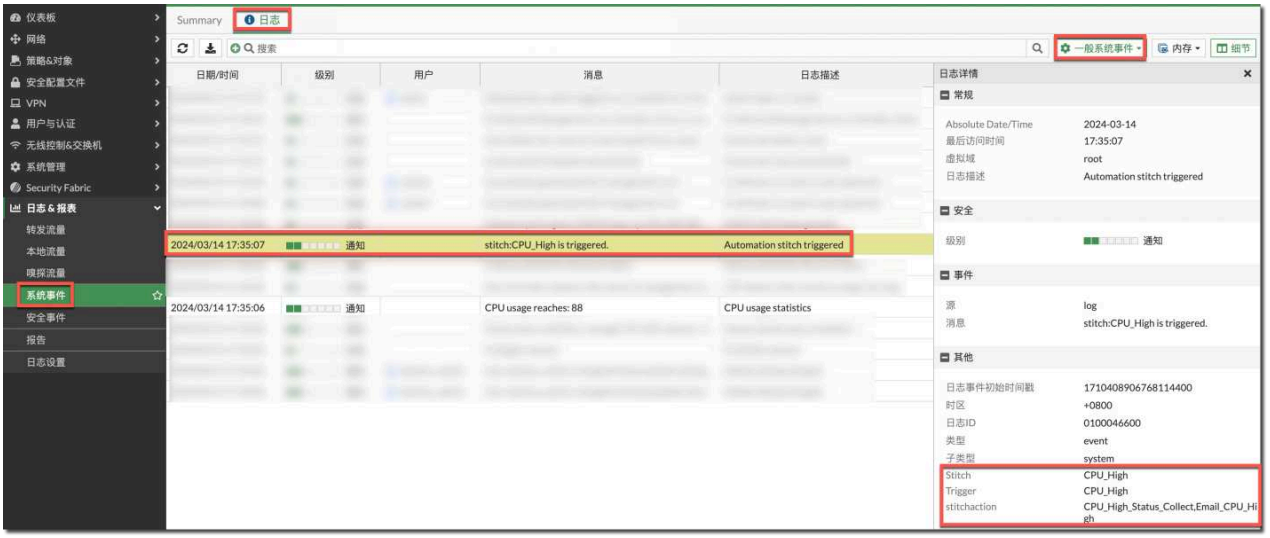

```bash
config system automation-stitch
    edit "CPU_High"
        set trigger "CPU_High"
        config actions
            edit 1
                set action "CPU_High_Status_Collect"
                set required enable
            next
            edit 2
                set action "Email_CPU_High"
                set required enable
            next
        end
    next
end
```

配置验证

1. 触发FortiGate的CPU利用率达到设定的阈值（此例中的FortiGate CPU高阈值设置为85%）。

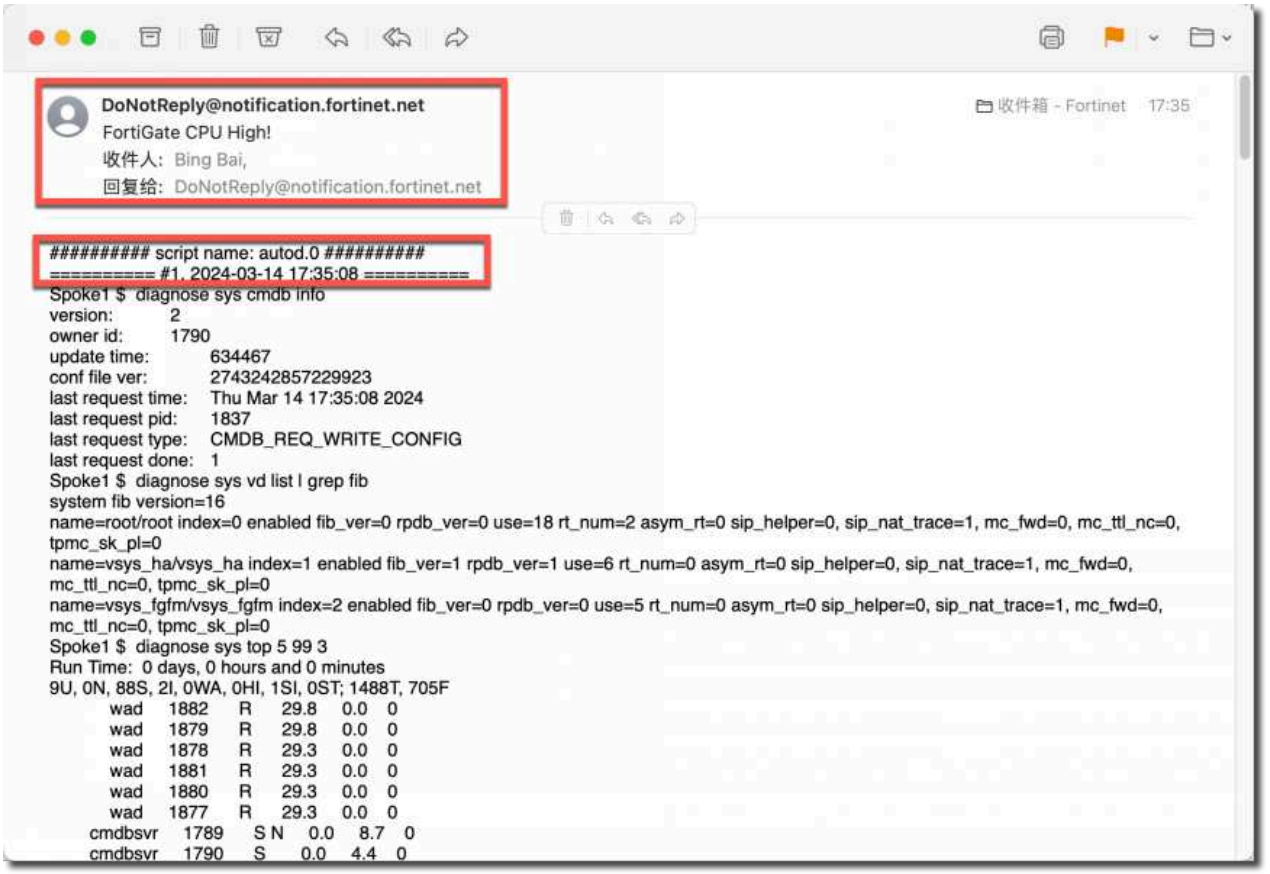
2. 触发自动化程序，相关自动化日志如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
date=2024-03-14 time=17:35:07 eventtime=1710408906768114390 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="CPU_High"
trigger="CPU_High" stitchaction="CPU_High_Status_Collect,Email_CPU_High" from="log" msg="stitch:CPU_High is
triggered."

date=2024-03-14 time=17:35:06 eventtime=1710408897701912754 tz="+0800" logid="0100040705" type="event"
subtype="system" level="notice" vd="root" logdesc="CPU usage statistics" action="cpu-usage" cpu=88 msg="CPU usage
reaches: 88"
```

3. 收件人邮箱收到了告警邮件，邮件内容为通过CLI动作收集到的设备状态信息，发件人为默认的DoNotReply@notification.fortinet.net。



4. 查看自动化触发Debug信息（略，参考内存保护模式自动化的Debug信息）。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable
```

5. 查看发送邮件的Debug信息（略，参考内存保护模式自动化动作的邮件告警Debug信息）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # diagnose debug application alertmail -1
FortiGate # diagnose debug enable
```

单核CPU使用率高

> **重要**
>
> 该功能在7.2.4及以上版本支持。

网络需求

很多情况下，FortiGate的某个CPU持续高也会影响到正常运行，这种情况下是无法触发上个章节中平均CPU高触发器的，此章节可以实现单个CPU核利用率超过配置的阈值时，触发CLI动作收集设备当前的运行信息，并将信息发送至指定邮箱。

配置步骤

1. 首先配置告警邮件发送的配置（参考日志→邮件告警 ↗章节，也可使用默认配置）。

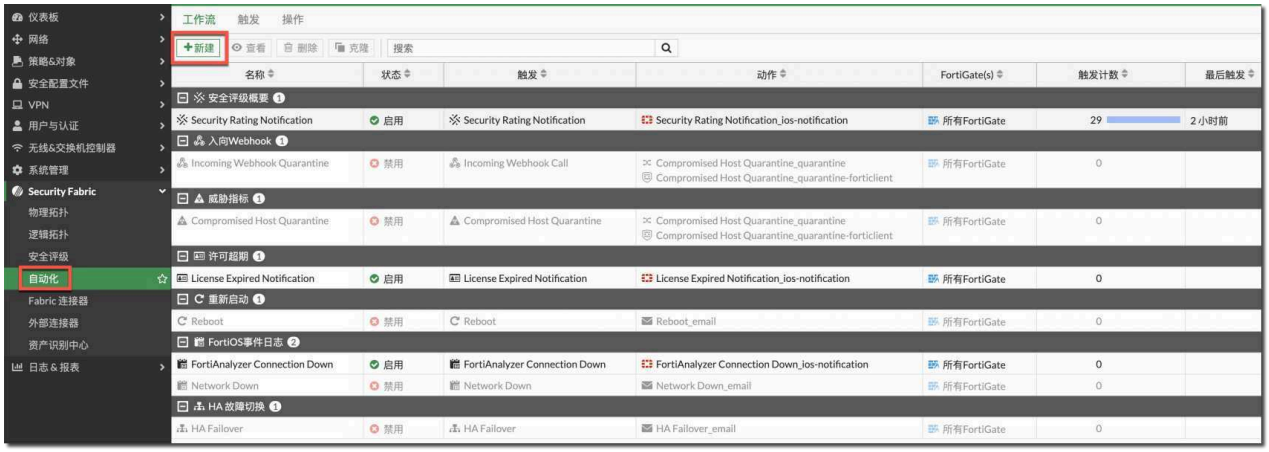
2. 在FortiGate的CLI中开启日志记录单核CPU高的功能，开启后，`cpu-use-threshold`也会对单个CPU核心生效。

```bash
config system global
    set log-single-cpu-high enable
    set cpu-use-threshold 85
end
```

3. 产生的日志示例如下，Log ID为40707。

```bash
date=2024-03-15 time=14:08:23 eventtime=1710482896991349328 tz="+0800" logid="0100040707" type="event" subtype="system" level="notice" vd="root" logdesc="CPU single core usage statistics" action="cpu-single-core-usage" core=1 cpu=97 msg="CPU core 1 usage reaches: 97"
```

4. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击新建按钮，新建一个工作流。



5. 配置工作流的名称，点击“添加触发器”按钮，在右侧的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 在右侧弹出的窗口中，找到“其他条件”分类，点击“FortiOS事件日志”选项。



7. 配置触发器（Trigger）的名称，FortiOS事件日志中选择“CPU single core usage statistics”，点击确认下发配置。




```bash
config system automation-trigger
    edit "Single_CPU_High"
        set event-type event-log
        set logid 40707
    next
end
```

8. 在选择条目中选择上步创建的触发器（Trigger），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



9. 点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。



0. 在右侧弹出的窗口中，找到“通用”分类，点击“CLI脚本”选项。



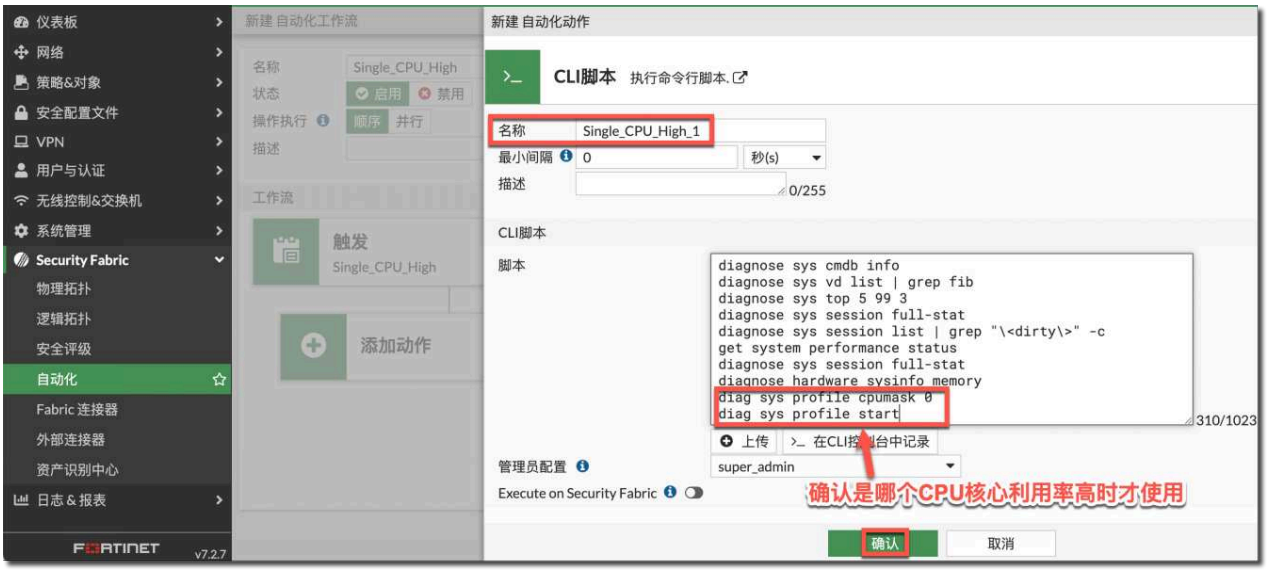
1. 配置动作（Action）的名称，配置CLI脚本内容为FortiGated的CPU利用率达到阈值后收集信息需要执行的CLI命令，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

如果已经确定是哪个CPU核心持续高，但出现该单核高的时间不确定，可以在上个章节收集的CLI命令后加入如下命令来查看该CPU代码级别的Debug信息（由于前2条命令和后2条命令中间需要1分钟的收集间隔，需要2个Action来完成所有的信息收集）：

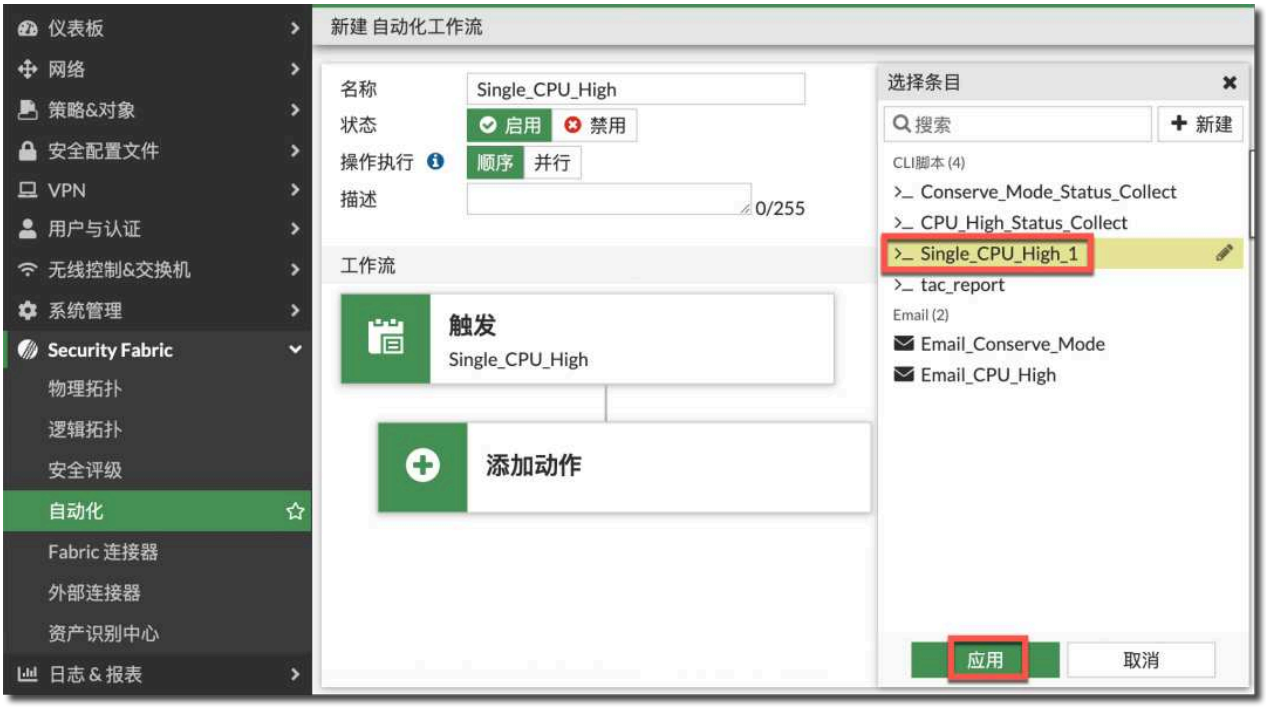
```bash
diag sys profile cpumask 0      //抓取特定的CPU核心，这里以CPU核心0为例//
diag sys profile start          //开启profile程序，等待1分钟，再执行后续命令//
diag sys profile stop
diag sys profile show order
```



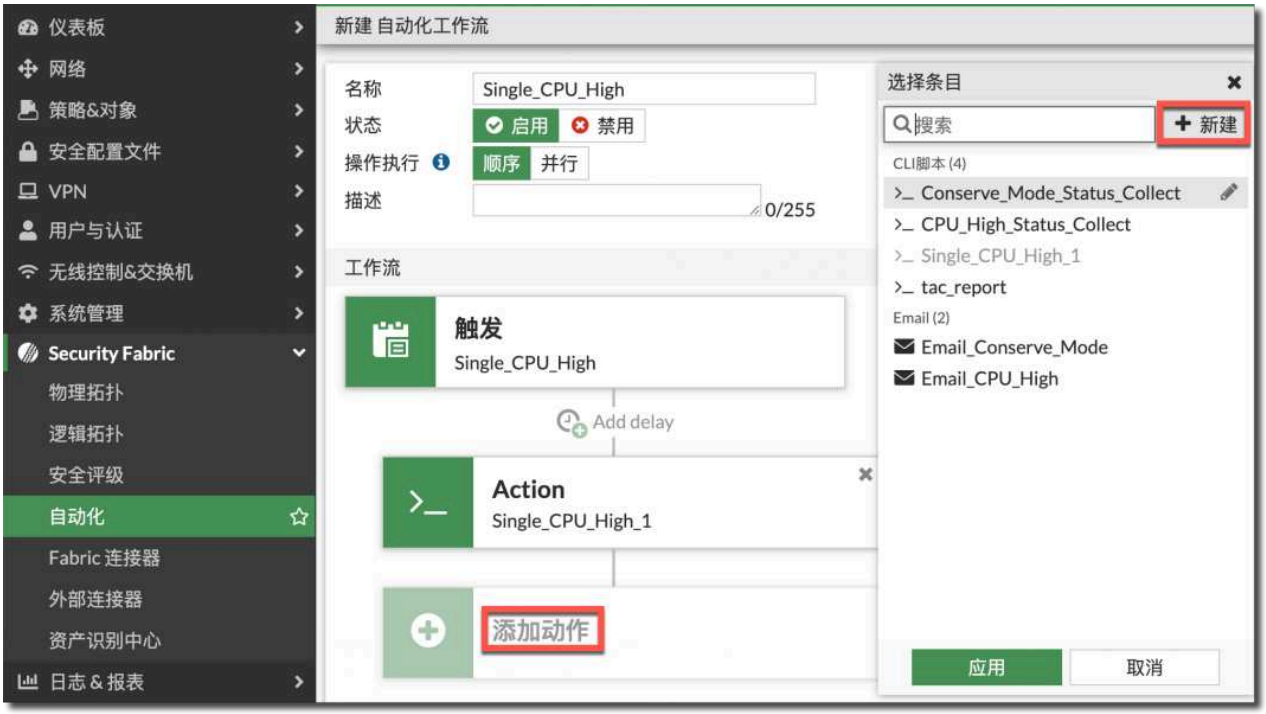

```bash
config system automation-action
    edit "CPU_High_Status_Collect"
        set action-type cli-script
        set script "diagnose sys cmdb info
diagnose sys vd list | grep fib
diagnose sys top 5 99 3
diagnose sys session full-stat
diagnose sys session list | grep "\<dirty\>" -c
get system performance status
diagnose sys session full-stat
diagnose hardware sysinfo memory"
————以下CLI在确认哪个CPU核心高的情况下可用（CLI脚本不包含此行）————
diag sys profile cpumask 0      //抓取特定的CPU核心，这里以CPU核心0为例//
diag sys profile start          //开启profile程序，等待1分钟，再执行后续命令//
————以上CLI在确认哪个CPU核心高的情况下可用（CLI脚本不包含此行）————
        set accprofile "super_admin"
    next
end
```

2. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 再次点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

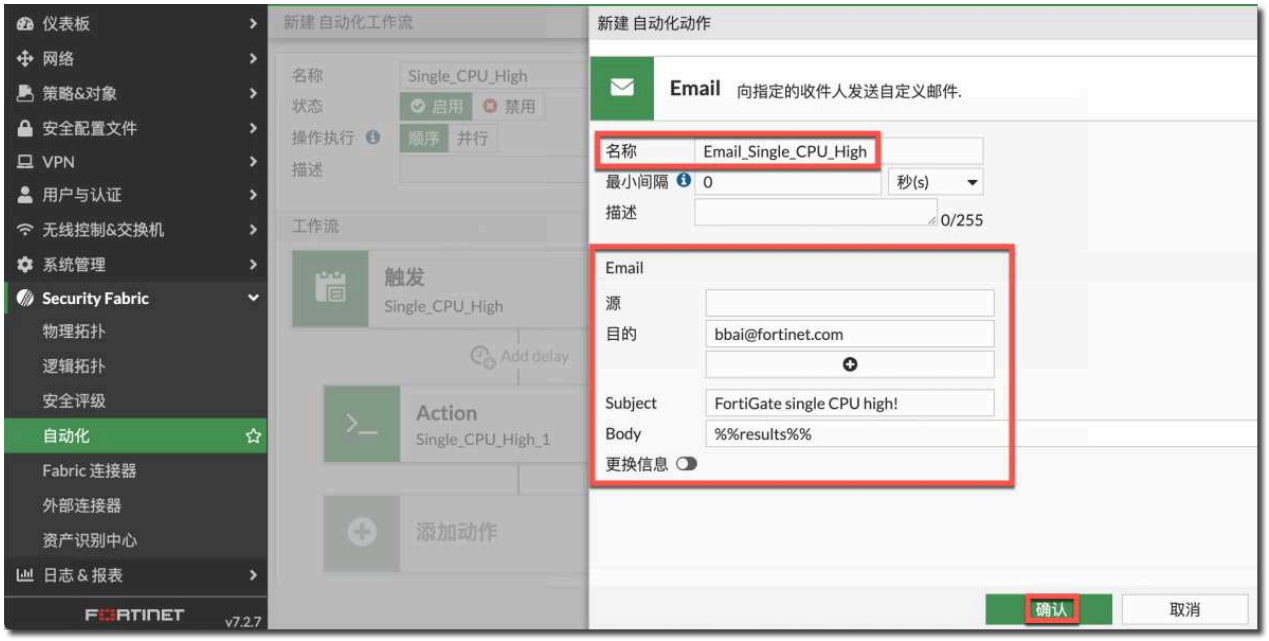


4. 在右侧弹出的窗口中，找到“通知”分类，点击“Email”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 配置动作（Action）的名称，以及邮件通知的收件人、邮件标题，邮件内容填写 `%%results%%` ，这是一个变量，表示使用前序动作CLI命令执行的结果作为邮件正文，点击确认下发配置，发送第一个CLI Action执行的输出结果。



- 最小间隔：如果Trigger频繁触发了，Action执行的最小间隔。
- 源：指定邮件通知的发件人，默认为DoNotReply@notification.fortinet.net。
- 目的：配置邮箱的收件人，可以配置多个收件人。
- Body：邮件内容。
- 更换信息：可以更换为自定义内容和格式。

```bash
config system automation-action
    edit "Email_Single_CPU_High"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "FortiGate single CPU high!"
        set message "%%results%%"
    next
end
```

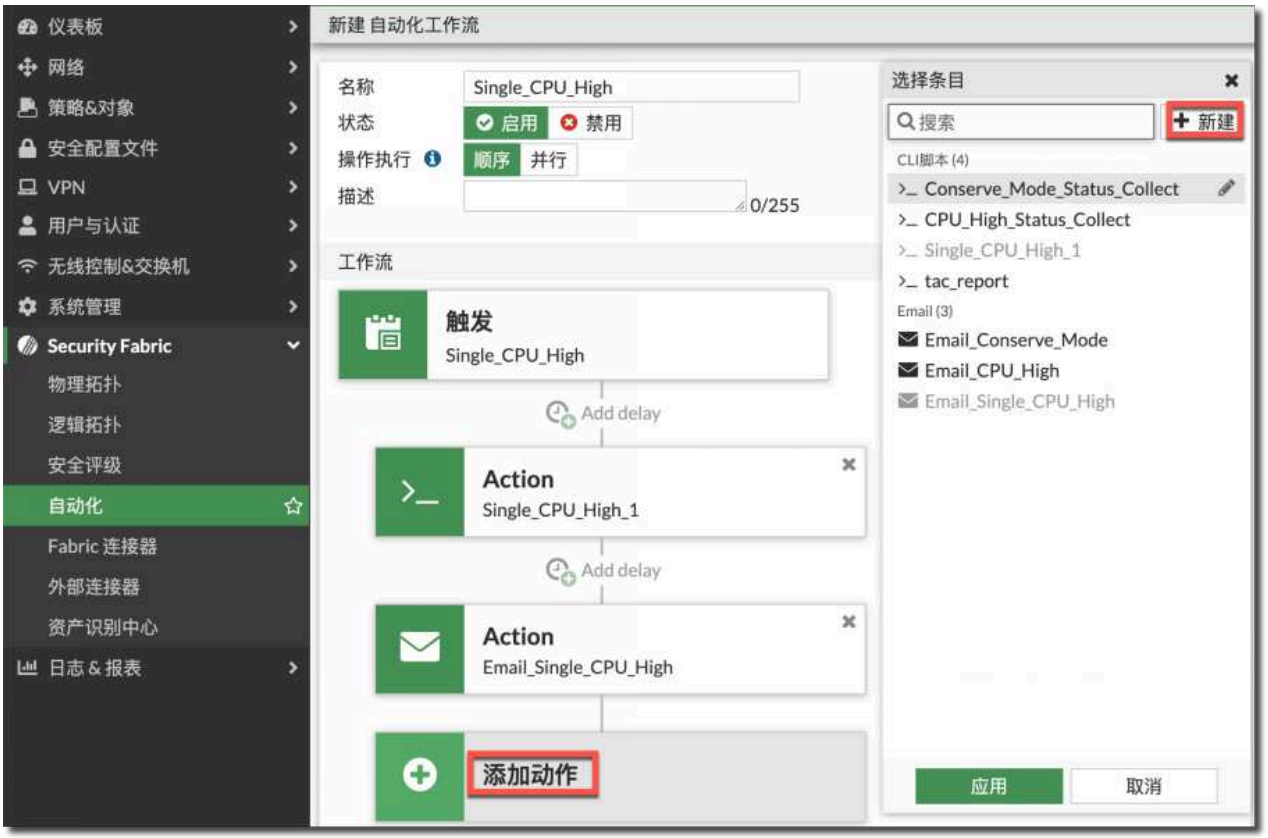
6. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. 再次点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

> **重要**
>
> 参考步骤11，在确认是哪个CPU核心高，但高的时间随机的情况下，才执行此步，否则跳过17 ~ 25步。

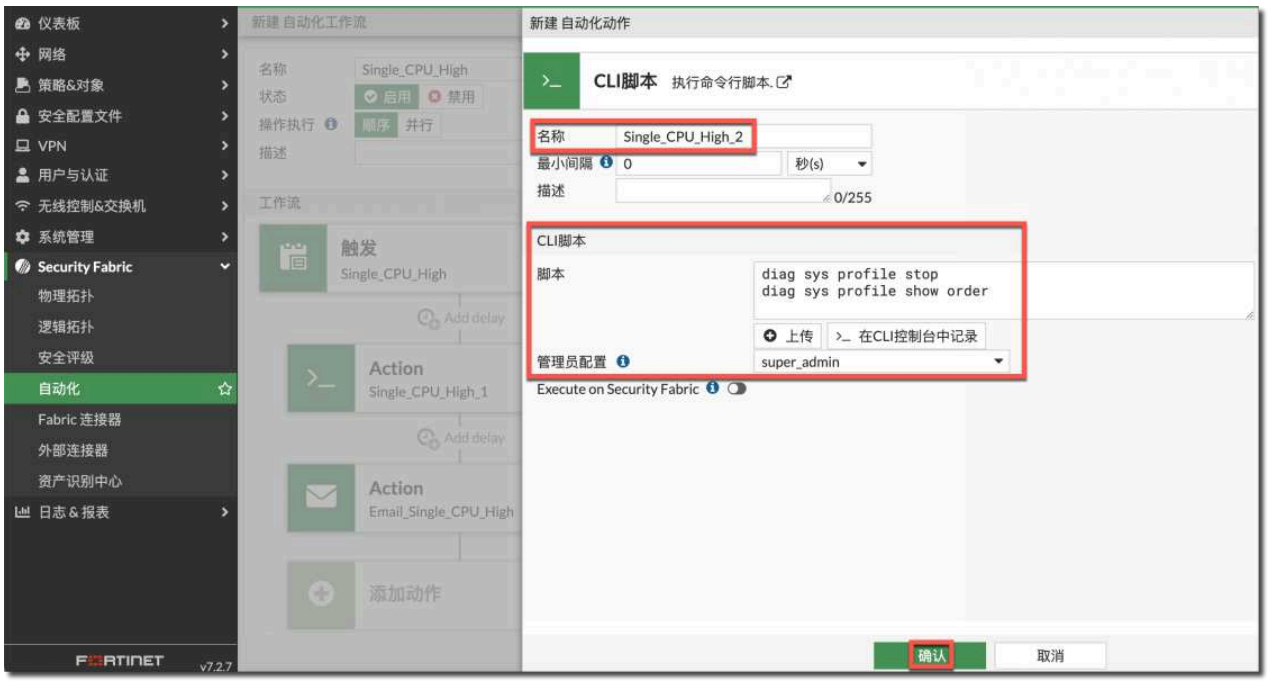


8. 在右侧弹出的窗口中，找到“通用”分类，点击“CLI脚本”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



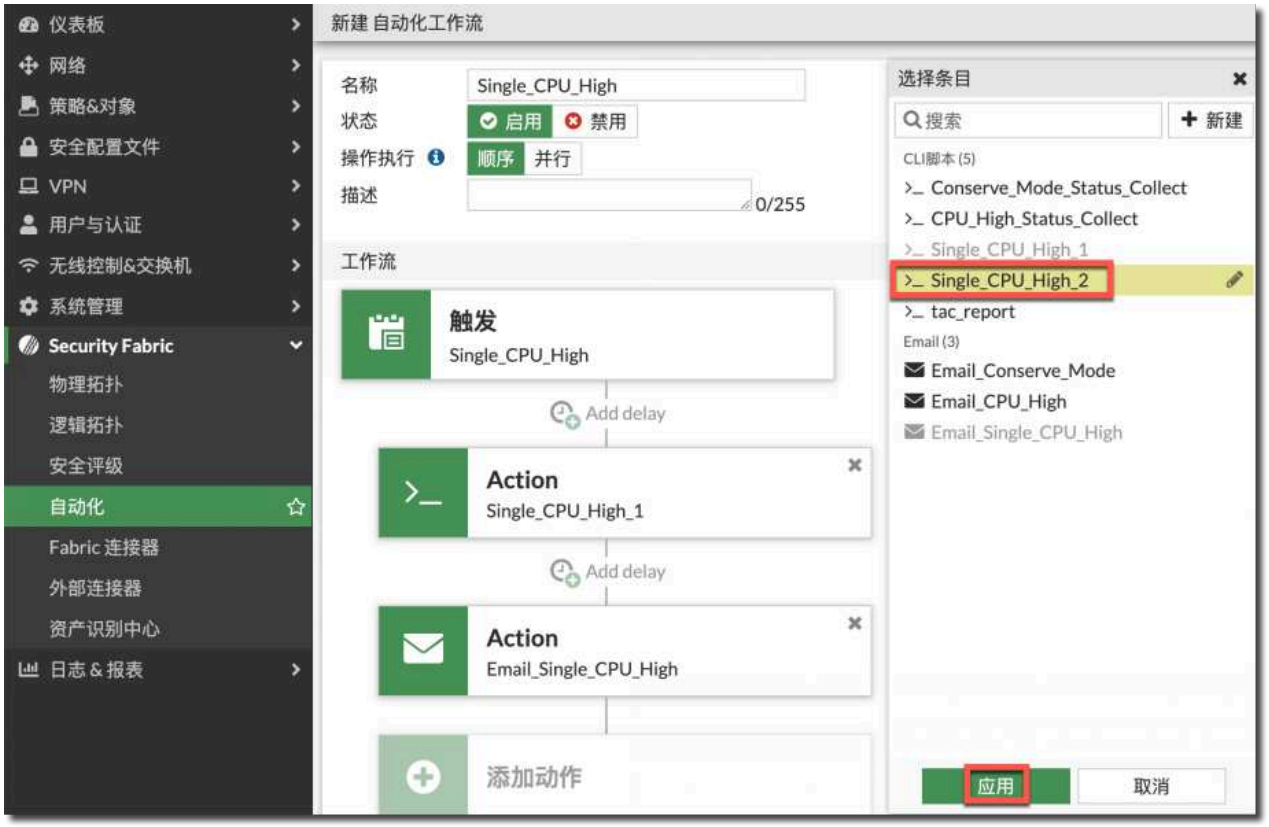
9. 配置动作（Action）的名称，配置CLI脚本内容为结束CPU profile信息收集并打印统计结果，点击确认下发配置。



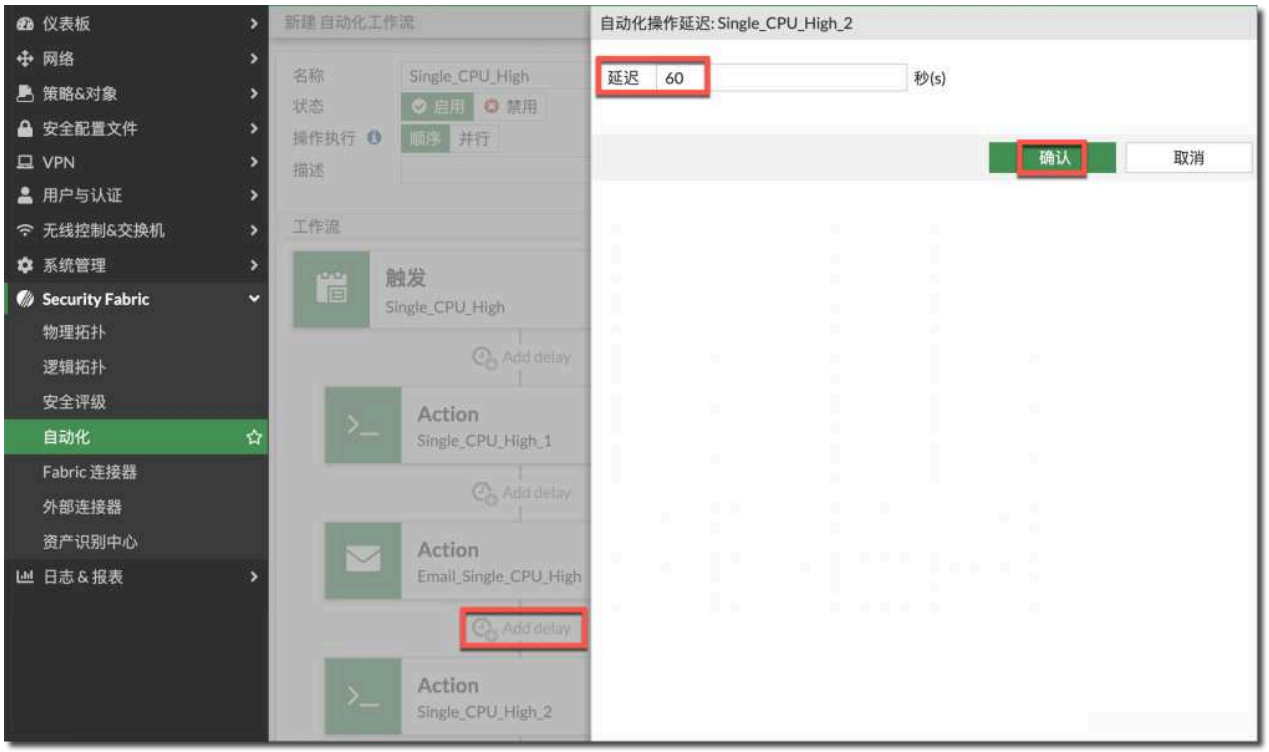

```bash
config system automation-action
    edit "Single_CPU_High_2"
        set action-type cli-script
        set script "diag sys profile stop
diag sys profile show order"
        set accprofile "super_admin"
    next
end
```

10. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

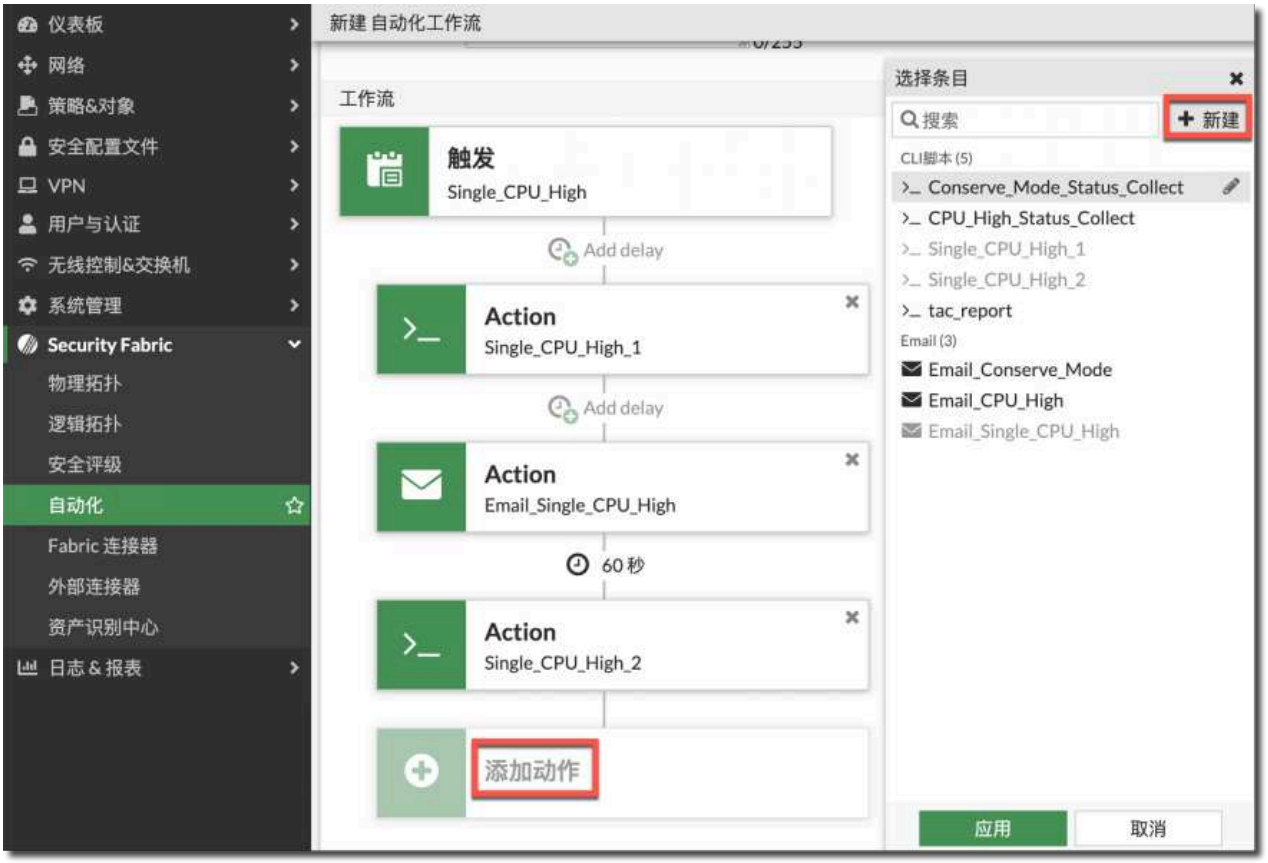


1. 在第2个Action和第3个Action之间点击“Add delay”，添加延迟为60秒，点击确认按钮下发配置。

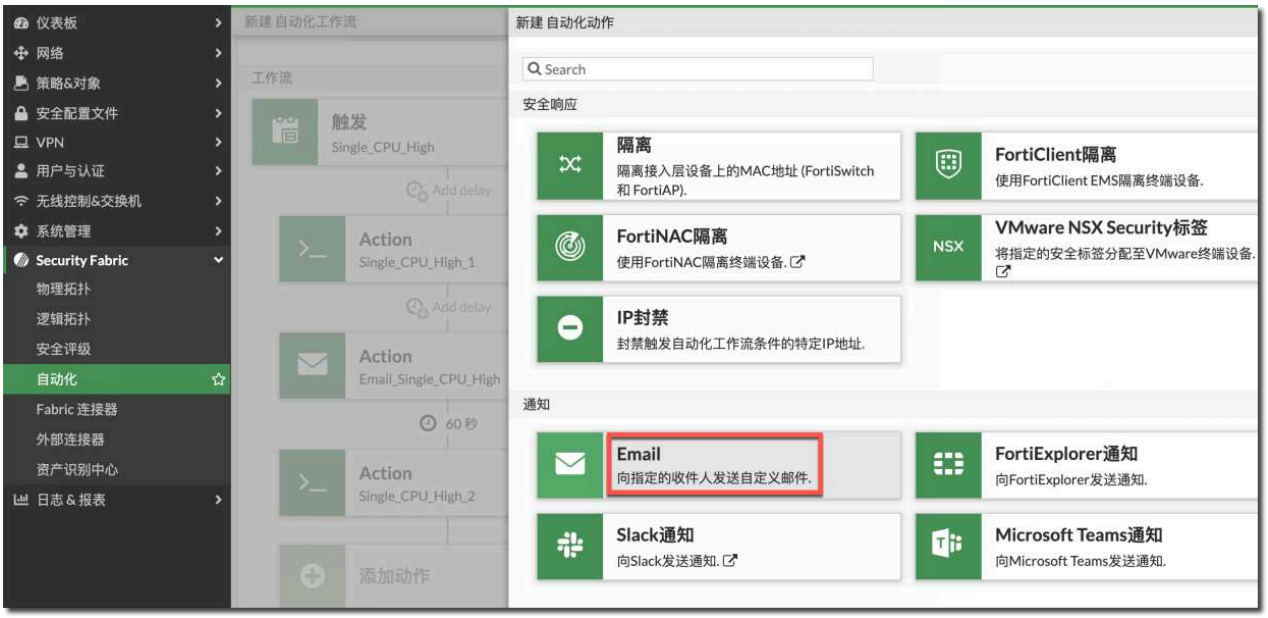


2. 再次点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

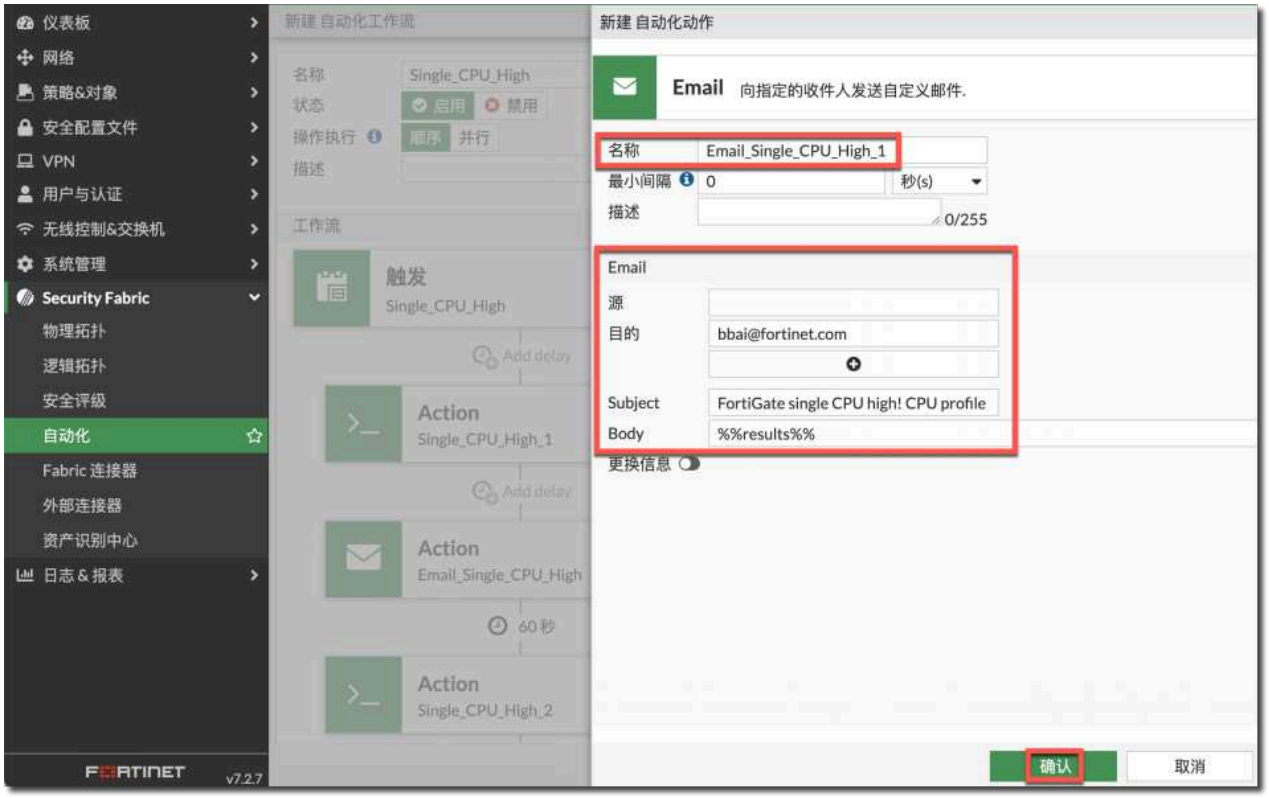


3. 在右侧弹出的窗口中，找到“通知”分类，点击“Email”选项。



4. 配置动作（Action）的名称，以及邮件通知的收件人、邮件标题，邮件内容填写 `%%results%%` ，这是一个变量，表示使用前序动作CLI命令执行的结果作为邮件正文，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

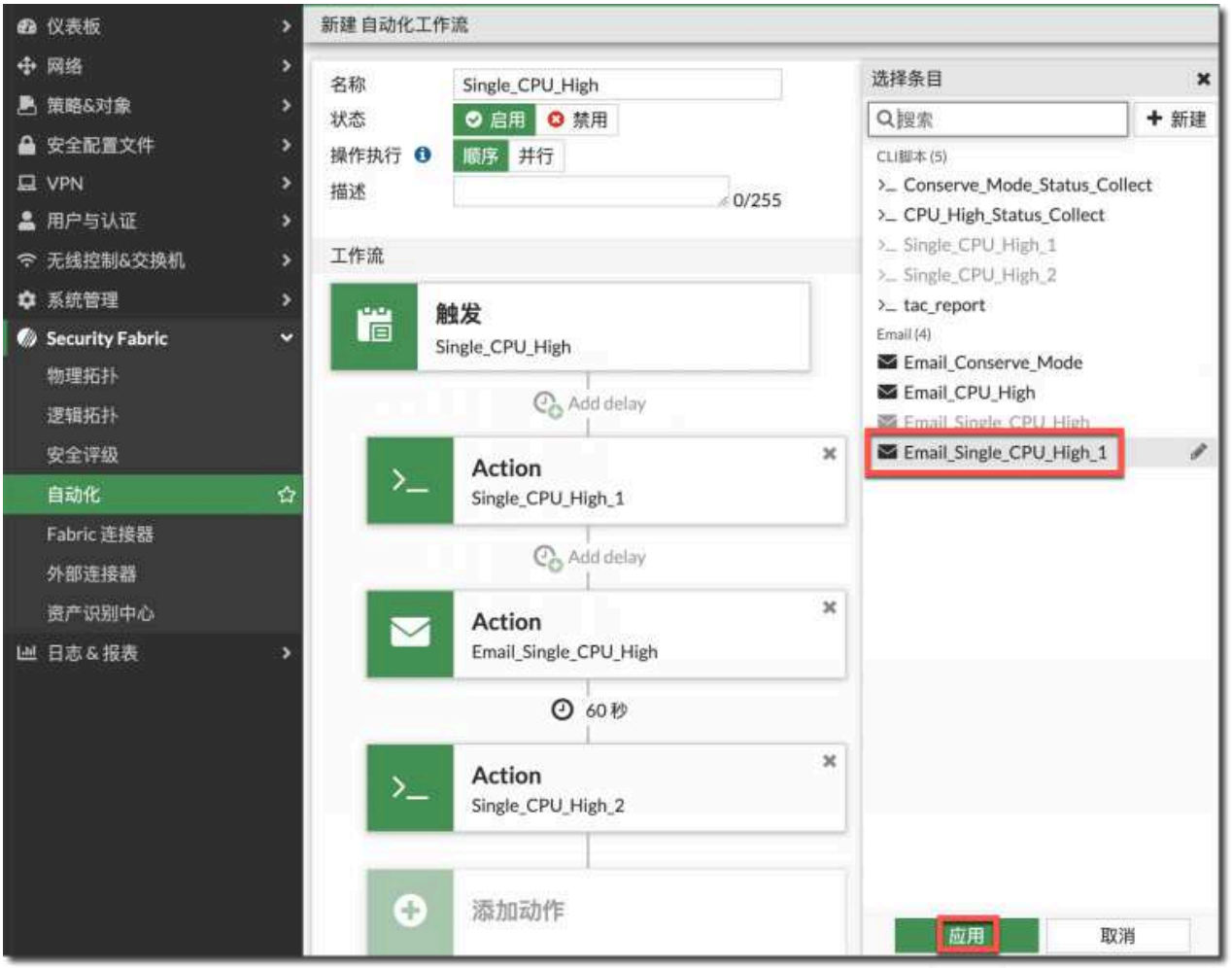


- 最小间隔：如果Trigger频繁触发了，Action执行的最小间隔。
- 源：指定邮件通知的发件人，默认为DoNotReply@notification.fortinet.net。
- 目的：配置邮箱的收件人，可以配置多个收件人。
- Body：邮件内容。
- 更换信息：可以更换为自定义内容和格式。

```bash
config system automation-action
    edit "Email_Single_CPU_High"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "FortiGate single CPU high!"
        set message "%%results%%"
    next
end
```

5. 在选择条目中选择上步创建的动作（Action），点击应用按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

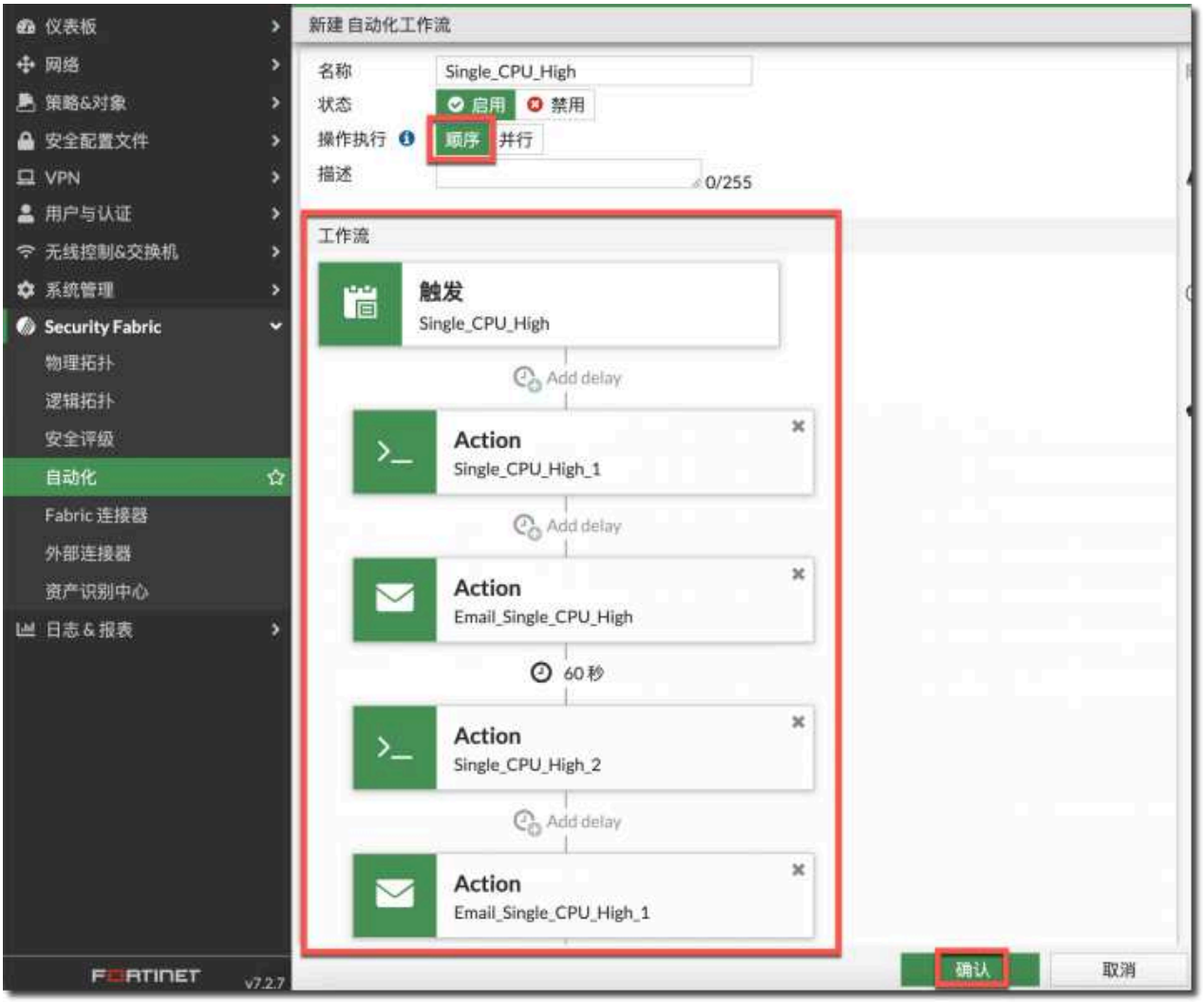


6. 检查无误后，点击确认下发配置。

重要

参考步骤11，在确认是哪个CPU核心高，但高的时间随机的情况下，才配置第3和第4个Action。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



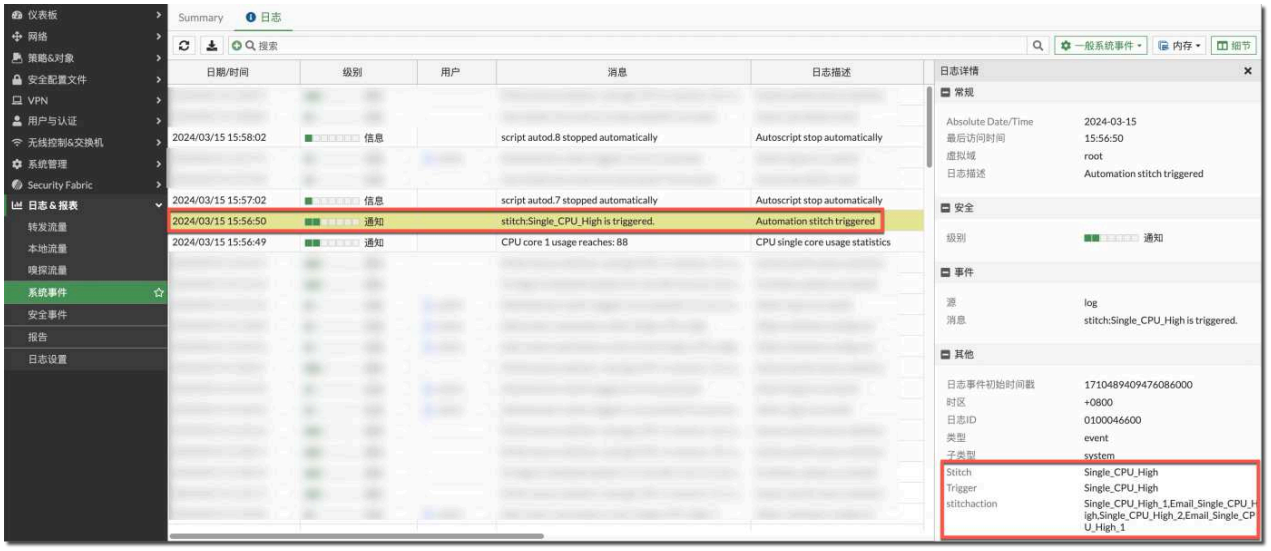

```bash
config system automation-stitch
    edit "Single_CPU_High"
        set trigger "Single_CPU_High"
        config actions
            edit 1
                set action "Single_CPU_High_1"
                set required enable
            next
            edit 2
                set action "Email_Single_CPU_High"
                set required enable
            next
            edit 3
                set action "Single_CPU_High_2"
                set delay 60
                set required enable
            next
            edit 4
                set action "Email_Single_CPU_High_1"
                set required enable
            next
        end
    next
end
```

配置验证

1. 触发FortiGate的CPU核心0利用率达到设定的阈值（此例中的FortiGate CPU高阈值设置为85%）。

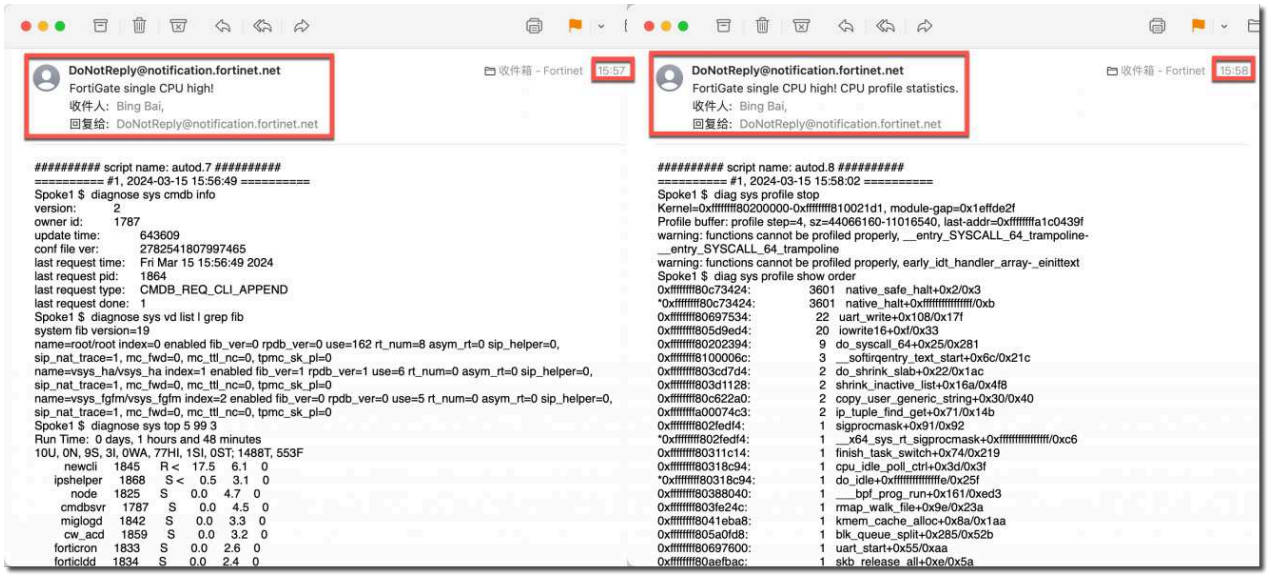
2. 触发自动化程序，相关自动化日志如下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
date=2024-03-15 time=15:56:50 eventtime=1710489409476085970 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="Single_CPU_High"
trigger="Single_CPU_High"
stitchaction="Single_CPU_High_1,Email_Single_CPU_High,Single_CPU_High_2,Email_Single_CPU_High_1" from="log"
msg="stitch:Single_CPU_High is triggered."

date=2024-03-15 time=15:56:49 eventtime=1710489408805031532 tz="+0800" logid="0100040707" type="event"
subtype="system" level="notice" vd="root" logdesc="CPU single core usage statistics" action="cpu-single-core-
usage" core=1 cpu=88 msg="CPU core 1 usage reaches: 88"
```

3. 收件人邮箱收到了2封告警邮件，第1封为除CPU profile统计信息外的收集信息，第2封为CPU profile的统计信息，发件人为默认的DoNotReply@notification.fortinet.net。



4. 查看自动化触发Debug信息（略，参考内存保护模式自动化的Debug信息）。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable
```

5. 查看发送邮件的Debug信息（略，参考内存保护模式自动化动作的邮件告警Debug信息）。

```bash
FortiGate # diagnose debug application alertmail -1
FortiGate # diagnose debug enable
```

注意事项

如果FortiGate的内存保护模式已经进入了Extreme状态，可能无法完成相关CLI命令的信息收集。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Email动作

简介

本章节介绍Email动作的两个特性：

- 邮件内容可以指定为前序CLI动作执行的输出结果，或前序事件日志触发器中对应的日志内容。在此基础上，也可以指定日志中的特定字段，或是过滤符合某些条件的日志。
- 自定义邮件的格式。

自定义邮件内容

网络需求

用户想要在FortiGate的管理员登录或等出时，通过邮件通知登录和登出的系统事件日志信息，但只想得到系统事件日志中的源IP、目的IP、和登录/登出信息，过滤掉其他的日志内容。

配置步骤

1. 进入FortiGate的“Security Fabric→自动化→触发器”页面，点击“新建”按钮。

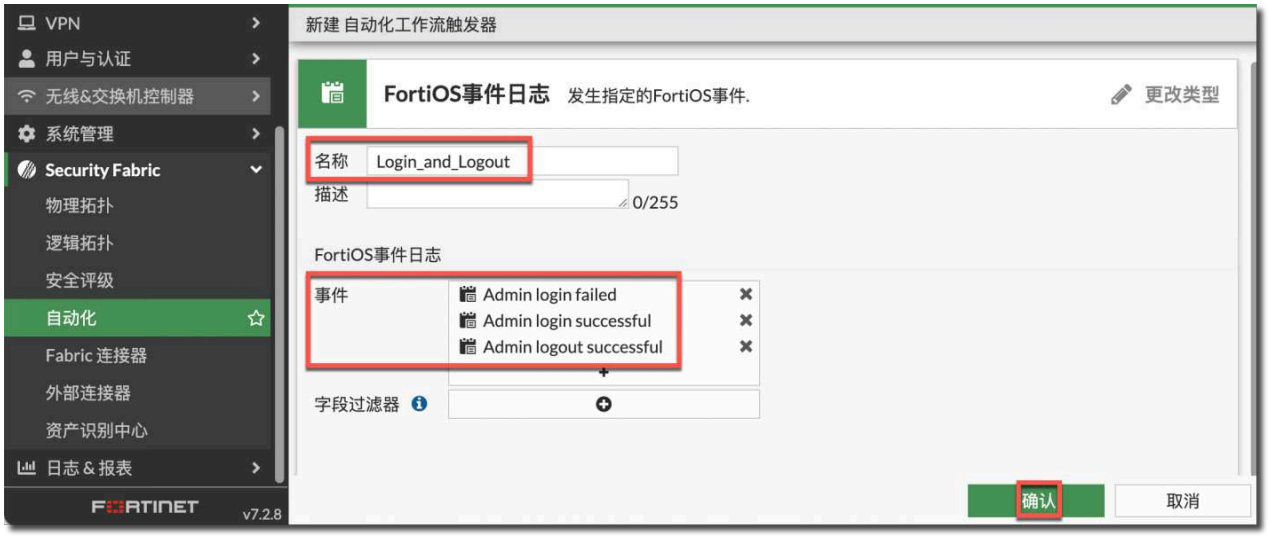


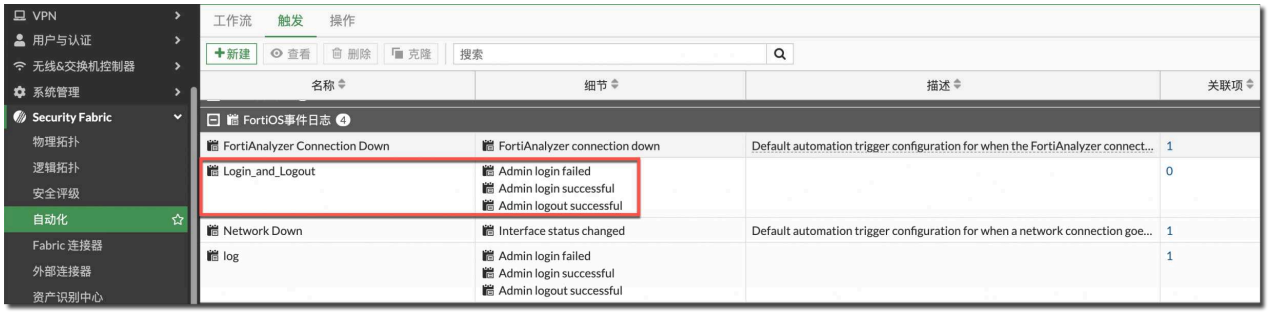
2. 在弹出的页面的“其他条件”分类中点击“FortiOS事件日志”。



3. 配置触发器名称，事件选择管理员登录成功、失败、以及登出三种类型，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





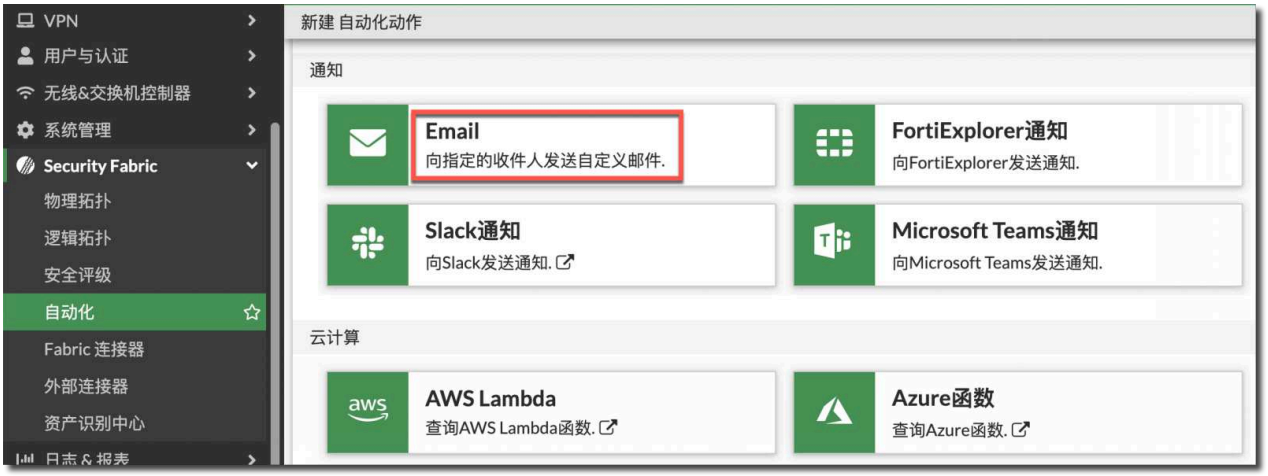

```bash
config system automation-trigger
    edit "Login_and_Logout"
        set event-type event-log
        set logid 32002 32001 32003
    next
end
```

4. 进入FortiGate的“Security Fabric→自动化→操作”页面，点击“新建”按钮。



5. 在弹出的页面的“通知”分类中点击“Email”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 配置动作名称，Email的目的，以及邮件标题，在“Body”配置中，默认配置为`%%log%%`，也就是前序日志触发器的完整日志内容，这里我们可以点击“Body”右侧的“%”按钮，会弹出一些其他的变量示例。



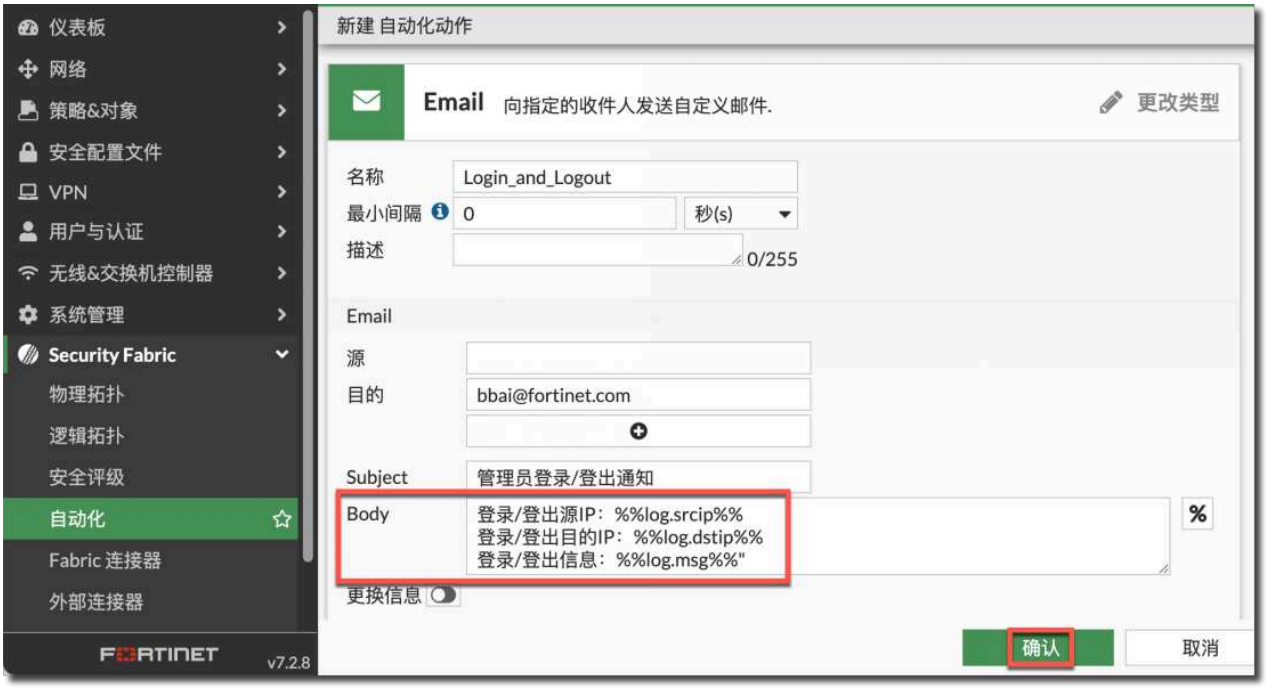

```bash
config system automation-action
    edit "Backup_config_to_FTP"
        set action-type cli-script
        set script "exe backup config ftp AutoBackup_%%date%%.conf 192.168.100.110 backup 111111"
        set accprofile "super_admin"
    next
end
```

- 最小间隔：如果Trigger频繁触发了，Action执行的最小间隔。
- 源：指定邮件通知的发件人，默认为DoNotReply@notification.fortinet.net。
- 目的：配置邮箱的收件人，可以配置多个收件人。
- Body：邮件内容。
- 更换信息：可以更换为自定义内容和格式。

7. 按照上步的变量示例，来自定义发送邮件的内容，点击“确认”按钮下发配置。

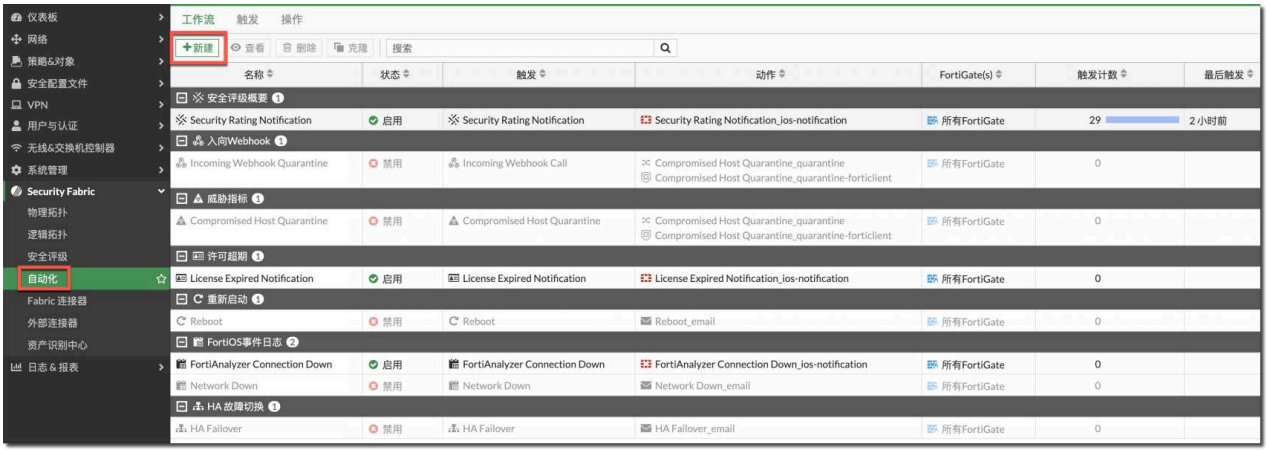
> **重要**
>
> 内容包括三个日志字段的信息：登录/登出源IP：`%%log.srcip%%`（表示从日志中的`srcip`字段取值）、登录/登出目的IP：`%%log.dstip%%`（表示从日志中的`dstip`字段取值）、登录/登出信息：`%%log.msg%%"`（表示从日志中的`msg`字段取值）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



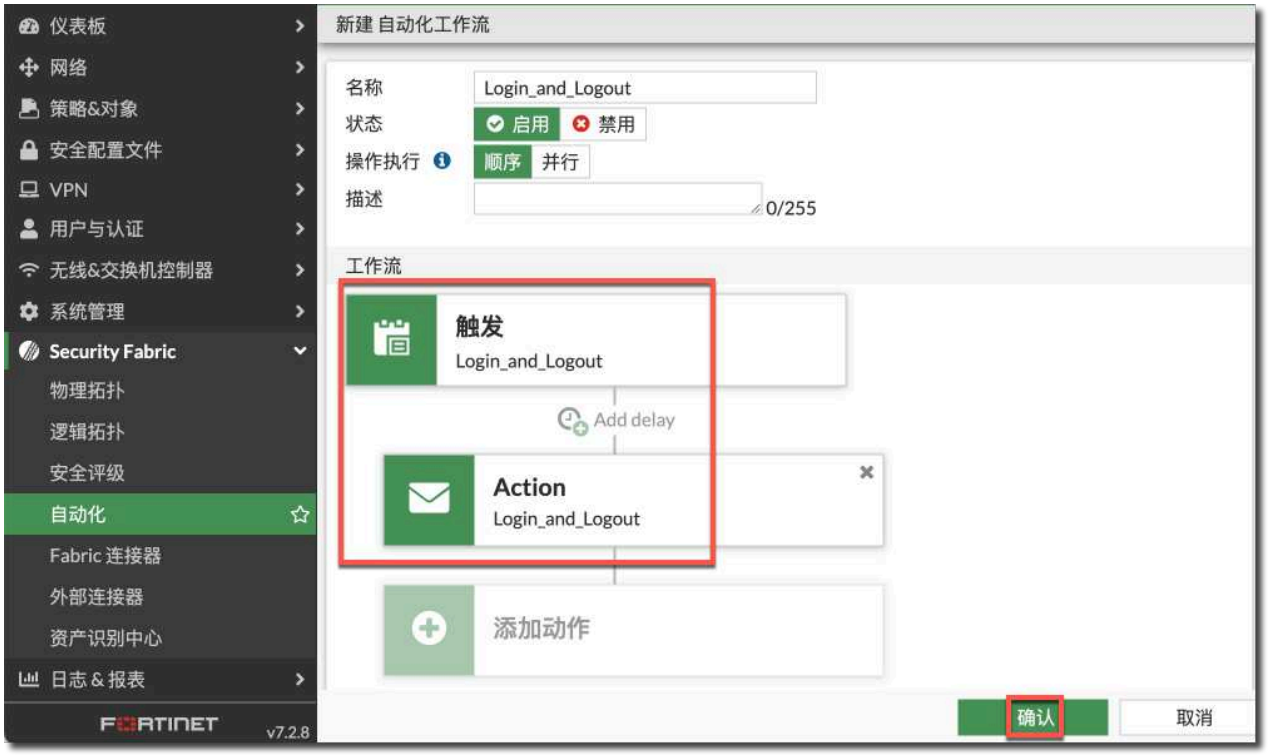

```bash
config system automation-action
    edit "Login_and_Logout"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "管理员登录/登出通知"
        set message "登录/登出源IP：%%log.srcip%%
登录/登出目的IP：%%log.dstip%%
登录/登出信息：%%log.msg%%\""
    next
end
```

8. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击“新建”按钮。



9. 配置工作流（Stitch的）名称，在触发中选择步骤3创建的触发器，在Action中选择步骤7创建的动作，点击“确认”下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system automation-stitch
    edit "Login_and_Logout"
        set trigger "Login_and_Logout"
        config actions
            edit 1
                set action "Login_and_Logout"
                set required enable
            next
        end
    next
end
```

配置验证

1. 触发FortiGate上的登录或登出日志，如下所示一次管理员登录失败的日志。

```bash
date=2024-03-20 time=17:56:17 eventtime=1710928577859214379 tz="+0800" logid="0100032002" type="event"
subtype="system" level="alert" vd="root" logdesc="Admin login failed" sn="0" user="administrator"
ui="https(192.168.100.178)" method="https" srcip=192.168.100.178 dstip=192.168.100.99 action="login"
status="failed" reason="passwd_invalid" msg="Administrator administrator login failed from https(192.168.100.178)
because of invalid password"
```

2. 触发自动化程序，相关自动化日志如下。

```bash
date=2024-03-20 time=17:56:18 eventtime=1710928577859816539 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="Login_and_Logout"
trigger="Login_and_Logout" stitchaction="Login_and_Logout" from="log" msg="stitch:Login_and_Logout is triggered."
```

3. 收件人邮箱收到了告警邮件，邮件内容为自定义的日志字段内容，发件人为默认的DoNotReply@notification.fortinet.net。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. 对应的自动化触发Debug信息。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable
......
__action_email_hdl()-181: email action (Login_and_Logout) is called.
from:
to:bbai@fortinet.com;
subject:管理员登录/登出通知
......
```

5. 发送邮件的Debug信息如下。

```bash
FortiGate # diagnose debug application alertmail -1
FortiGate # diagnose debug enable

Arrived msg(type 9, 251 bytes):bbai@fortinet.com;

管理员登录/登出通知
登录/登出源IP：192.168.100.178
登录/登出目的IP：192.168.100.99
登录/登出信息：Administrator administrator login failed from https(192.168.100.178) because of invalid password"

mail_info:
        from:notification.fortinet.net  user:DoNotReply@notification.fortinet.net
mail_info:
        reverse path:DoNotReply@notification.fortinet.net
        user name:DoNotReply
to[0]:bbai@fortinet.com
⟸_init_mail_info
create session
resolve notification.fortinet.net to 1 IP
⟹ send mail
connecting to 208.91.114.151 port 465
send mail 0×a1b6d80 session 0×a1bc7e0
session_io_event: creating ssl structure for session 0×a1bc7e0
create_ssl: 0×7fa5d8a000
sessionn 0×a1bc7e0, SSL connected
session: 0×a1bc7e0, rsp_state: greeting, code: 220
session: 0×a1bc7e0, rsp_state: ehlo, code: 250
session: 0×a1bc7e0, rsp_state: mail, code: 250
session: 0×a1bc7e0, rsp_state: rcpt, code: 250
session: 0×a1bc7e0, rsp_state: data, code: 354
⟹ send: 登录/登出源IP：192.168.100.178
登录/登出目的IP：192.168.100.99
登录/登出信息：Administrator administrator login failed from https(192.168.100.178) because of invalid password"

session: 0×a1bc7e0, rsp_state: data2, code: 250
session: 0×a1bc7e0, rsp_state: quit, code: 221
session finined
_session_on_destroy
⟸ send mail success, m = 0×a1b6d80 s = 0×a1bc7e0
```

##自定义邮件格式

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

网络需求

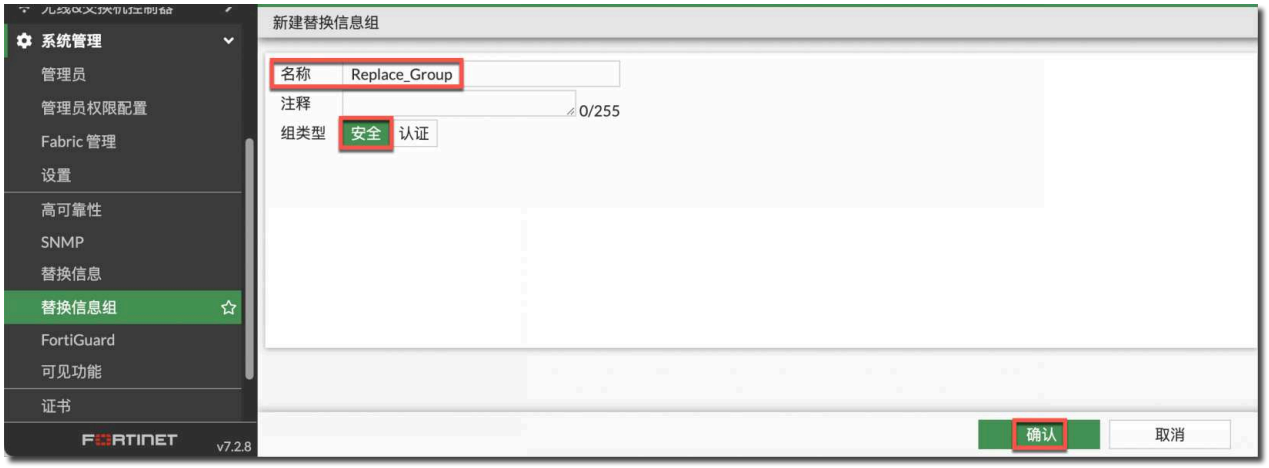
在上个章节的需求基础上，修改发送邮件的样式，添加一个告警图片。

配置步骤

1. 进入FortiGate的“系统管理→替换信息组”页面，点击“新建”按钮。



2. 配置替换信息组名称，“组类型”选择“安全”，点击“确认”按钮下发配置。



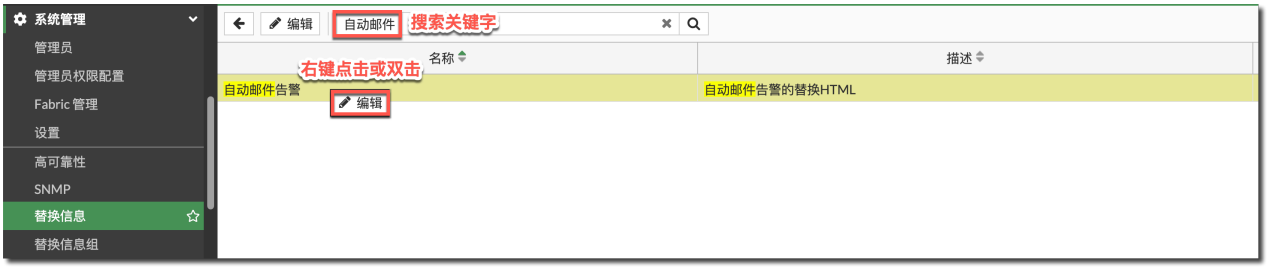
3. 右键点击新建的替换信息组，点击“编辑”按钮（或双击编辑）。



4. 搜索关键字“自动邮件”，找到“自动邮件告警”条目，右键或双击编辑该条目。

> **重要**
>
> 替换信息组中也包含其他功能模块页面的替换信息，当用户需要替换多个功能模块的页面信息时，可以使用此功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 在HTML编辑页面，将想要添加的告警图片URL添加到`message-container`部分，如下图所示（`<img src="https://www.fortinet.com/content/dam/fortinet/images/icons/benefits/icon-wireless-fortinet-ips.svg" alt="Fortinet Logo"/>`），左侧的预览可以正常显示该图片，点击“备份配置”按钮保存配置。



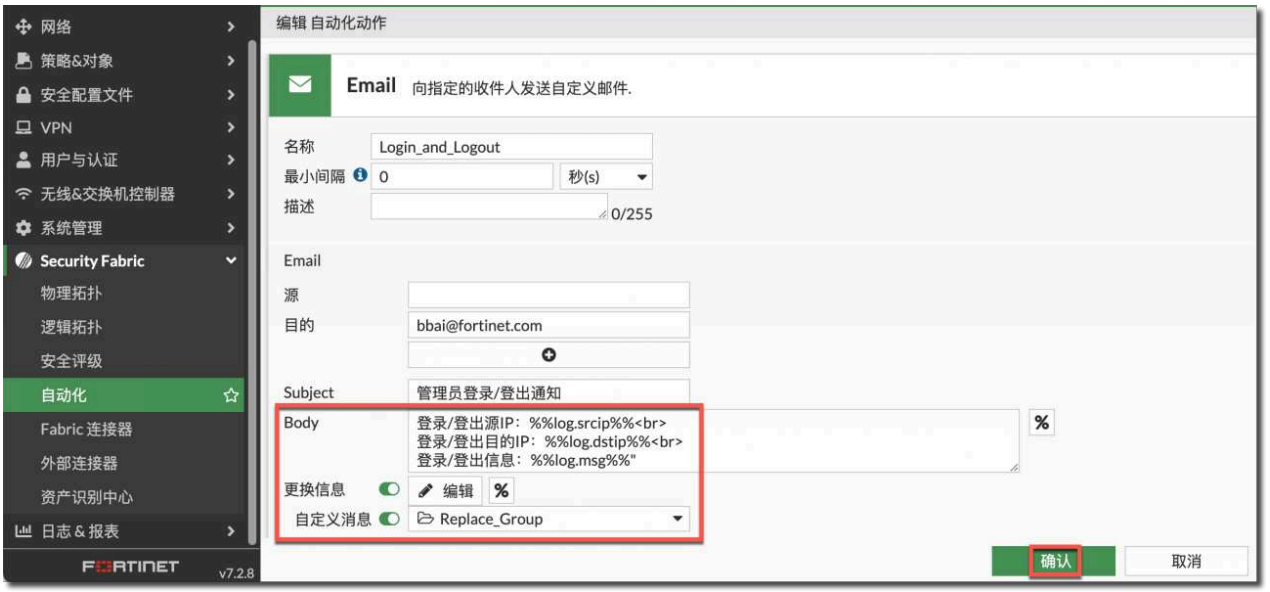

```bash
config system replacemsg-group
    edit "Replace_Group"
        set comment ''
        set group-type utm
        config automation
            edit "automation-email"
                set buffer "<!DOCTYPE html>
<html lang=\"en\">
 <head>
 <meta charset=\"UTF-8\">
 <meta http-equiv=\"X-UA-Compatible\" content=\"IE=8; IE=EDGE\">
 <meta name=\"viewport\" content=\"width=device-width, initial-scale=1\">
 <link href=\"https://fonts.googleapis.com/css?family=Roboto&display=swap\" rel=\"stylesheet\">
 <style>
 body {
 height: 100%;
 font-family: Roboto, Helvetica, Arial, sans-serif;
 margin: 0;
 display: flex;
 align-items: center;
 justify-content: center;
 }
 .message-container{
 margin: 0 auto;
 max-width: 580px;
 }
 .email-body {
 line-height: 1.5em;
 }
 </style>
 </head>
 <body>
 <div class=\"message-container\">
 <img src=\"https://www.fortinet.com/content/dam/fortinet/images/icons/benefits/icon-wireless-fortinet-ips.svg\"
alt=\"Fortinet Logo\"/>
 <h1>
 Security Fabric Automation
 </h1>
 <h3>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
 %%AUTOMATION_FGT_SERIAL%%: %%AUTOMATION_STITCH_NAME%%
 </h3>
 <div class=\"email-body\">
 %%AUTOMATION_EMAIL_BODY%%
 </div>
 </div>
 </body>
</html>
"
                set header http
                set format html
            next
        end
    next
end
```

6. 进入FortiGate的“Security Fabric→自动化→操作”页面，编辑上个章节创建的动作“Login_and_Logout”。开启“更换信息”选项，然后开启“自定义消息”选项，并选择上步创建的替换信息组。注意由于调用了替换信息组（HTML格式），所以需要在“Body”中每行加入HTML换行符 `<br>`。点击“确认”按钮下发配置。

> **重要**
>
> 如果仅需要替换此邮件动作的格式，则不需要步骤1~5创建替换信息组，只在此页面开启“更换信息”选项并点击编辑按钮编辑HTML格式即可。

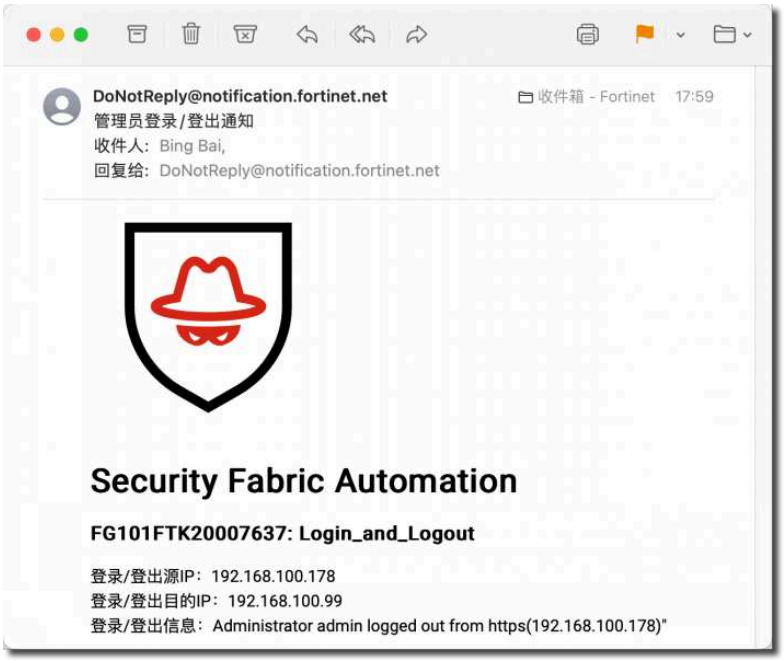



```bash
config system automation-action
    edit "Login_and_Logout"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "管理员登录/登出通知"
        set message "登录/登出源IP：%%log.srcip%%<br>
登录/登出目的IP：%%log.dstip%%<br>
登录/登出信息：%%log.msg%%\""
        set replacement-message enable
        set replacemsg-group "Replace_Group"
    next
end
```

配置验证

触发FortiGate上的登录或登出日志，查看收件人收到的邮件格式按照替换信息组中的配置的样式显示。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Teams Webhook

简介

Microsoft Teams通知动作可以通过Webhook将自动化执行的结果信息发送到指定的Teams频道。

需要FortiGate可以访问Internet。

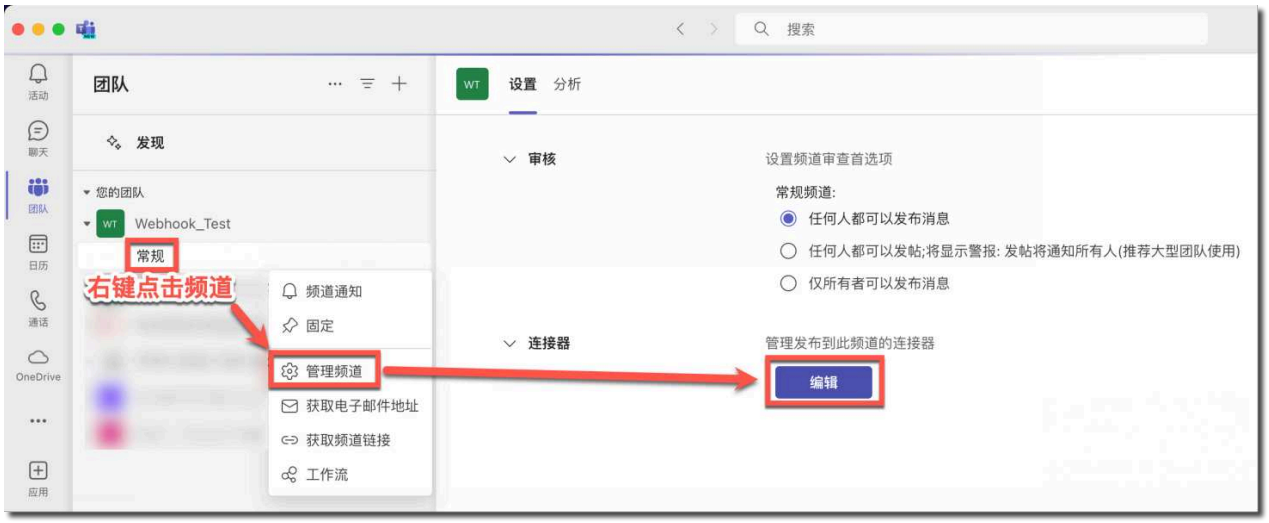
网络需求

当FortiGate的配置发生变更时，向Teams对应频道发送通知消息。

配置步骤

获取Teams Webhook链接

1. 打开Teams，进入团队页面，右键点击需要接收消息的频道，选择“管理频道”，在“连接器”中点击“编辑”按钮。

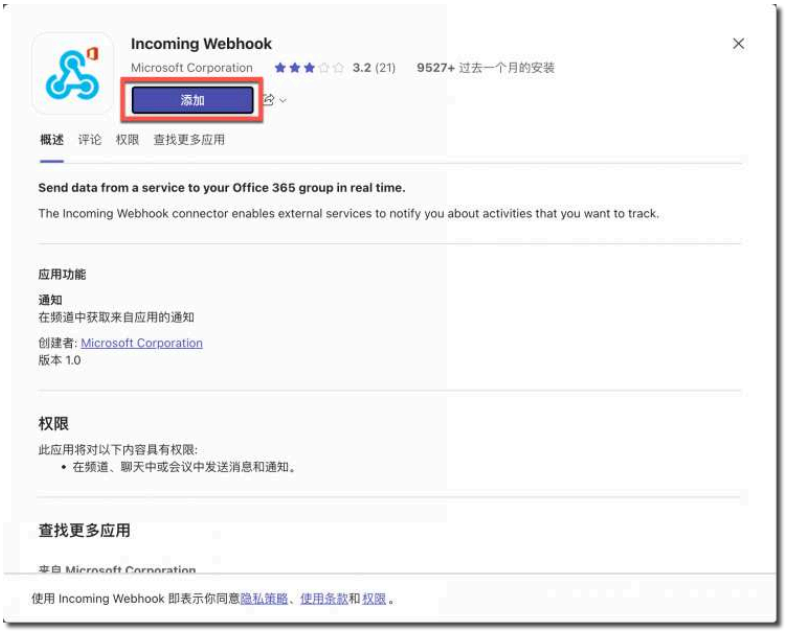


2. 在弹出的连接器列表中选择“Incoming Webhook”，点击该连接器右侧的“添加”按钮。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 在弹出的连接器详情页面中，继续点击“添加”按钮。

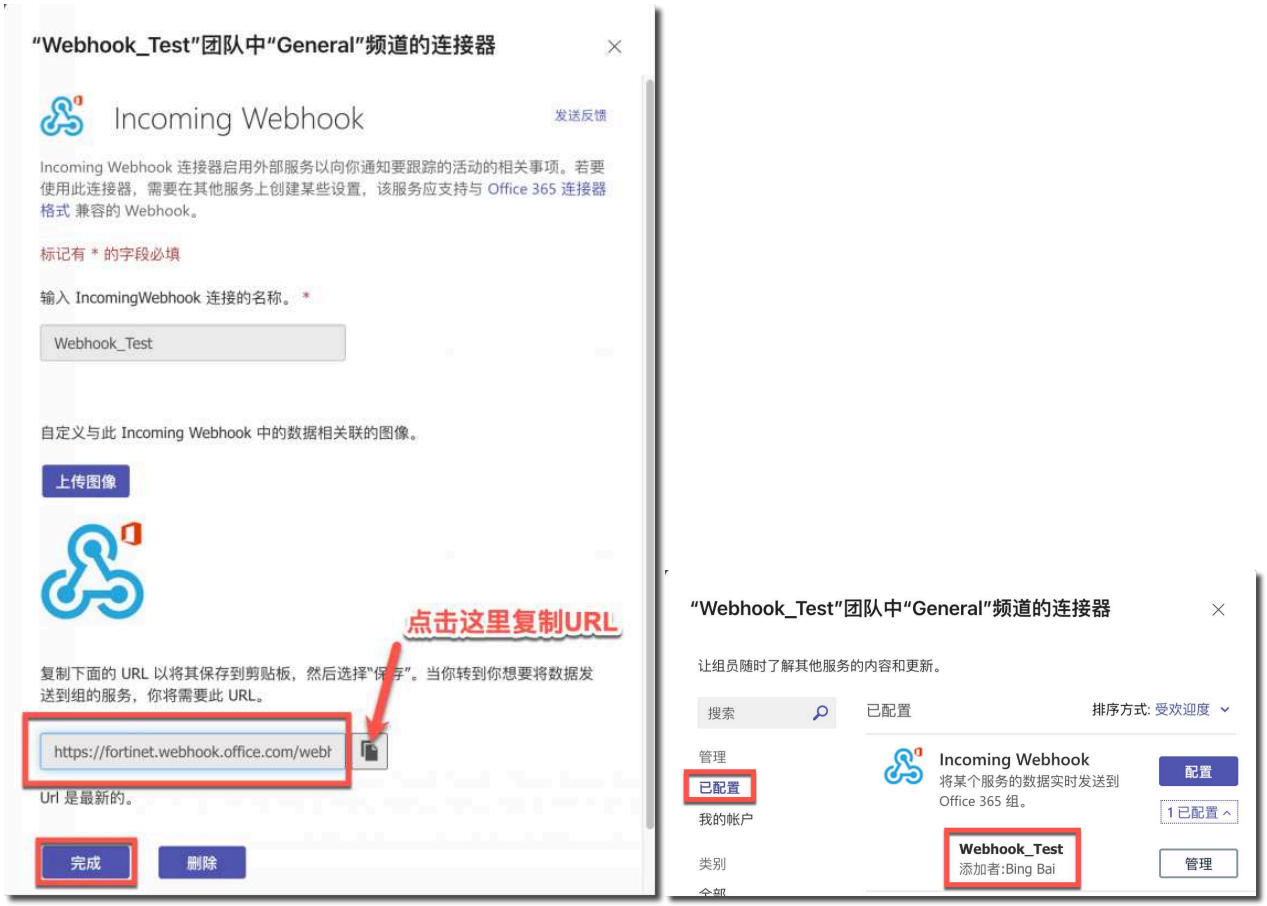


4. 随后会自动弹出连接器配置界面，配置连接器名称，可自行选择性上传发送消息时显示的图标，点击“创建”按钮。



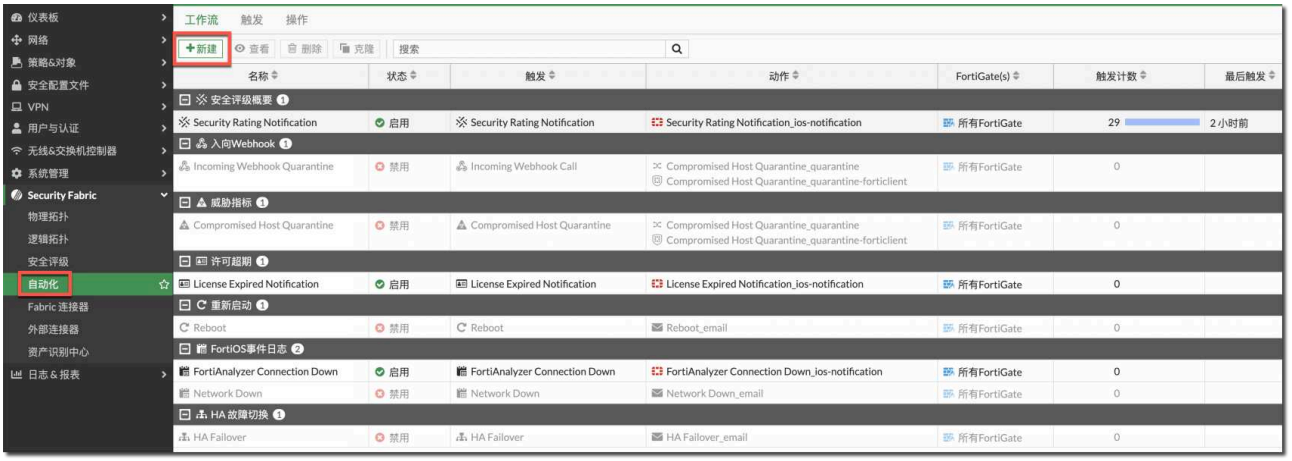
5. 复制生成的Webhook URL并妥善保存，点击“完成”按钮，完成“Incoming Webhook”连接器的配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiGate自动化配置

1. 进入FortiGate的“Security Fabric→自动化→工作流”页面，点击“新建”按钮。



2. 配置工作流的名称，点击“添加触发器”按钮，在右侧的“选择条目”中点击“新建”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 在右侧弹出的窗口中，找到“系统”分类，点击“配置改变”选项。



4. 配置触发器（Trigger）的名称，点击确认下发配置。




```bash
config system automation-trigger
    edit "Config_change"
        set event-type config-change
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

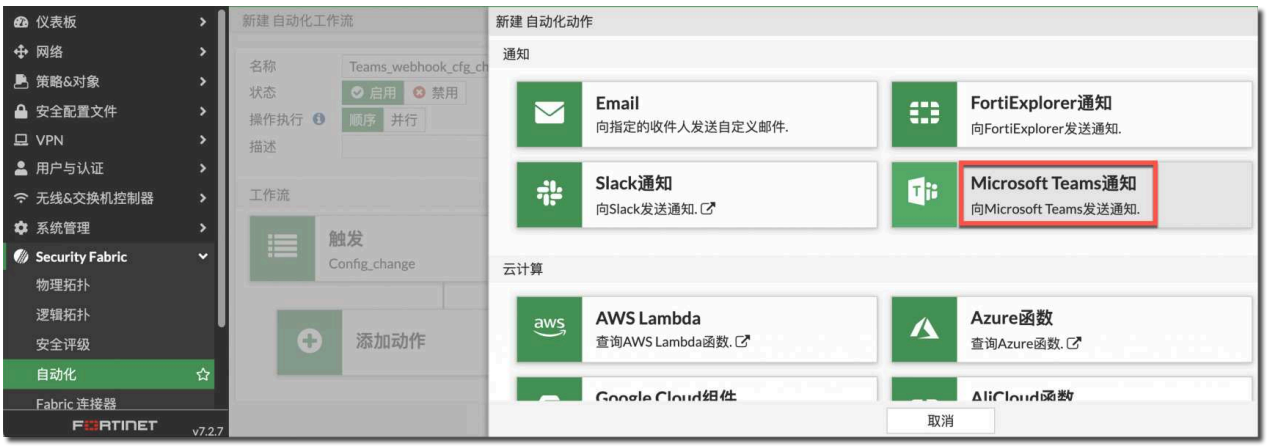
5. 在选择条目中选择上步创建的触发器（Trigger），点击应用按钮。



6. 点击“添加动作”按钮，在右侧弹出的“选择条目”中点击“新建”按钮。

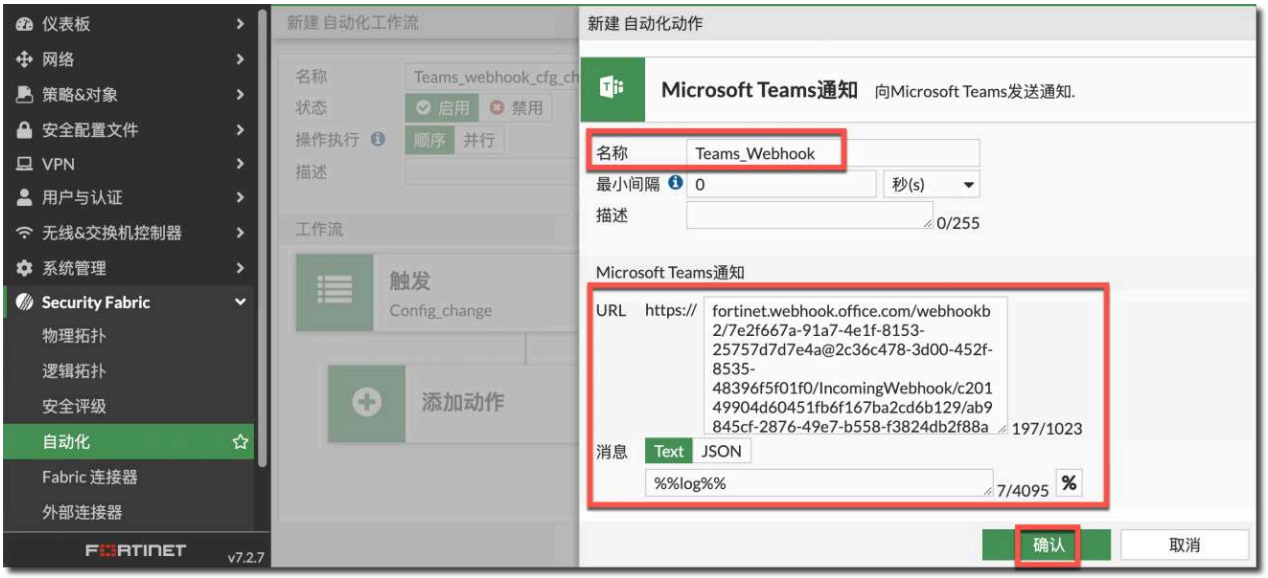


7. 在右侧弹出的窗口中，找到“通知”分类，点击“Microsoft Teams通知”选项。



8. 配置动作（Action）的名称，将从Teams连接器中复制出的Webhook URL粘贴进“URL”选项（不包含`https`字段），消息格式这里以“Text”为例，消息内容为配置变更的日志信息，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



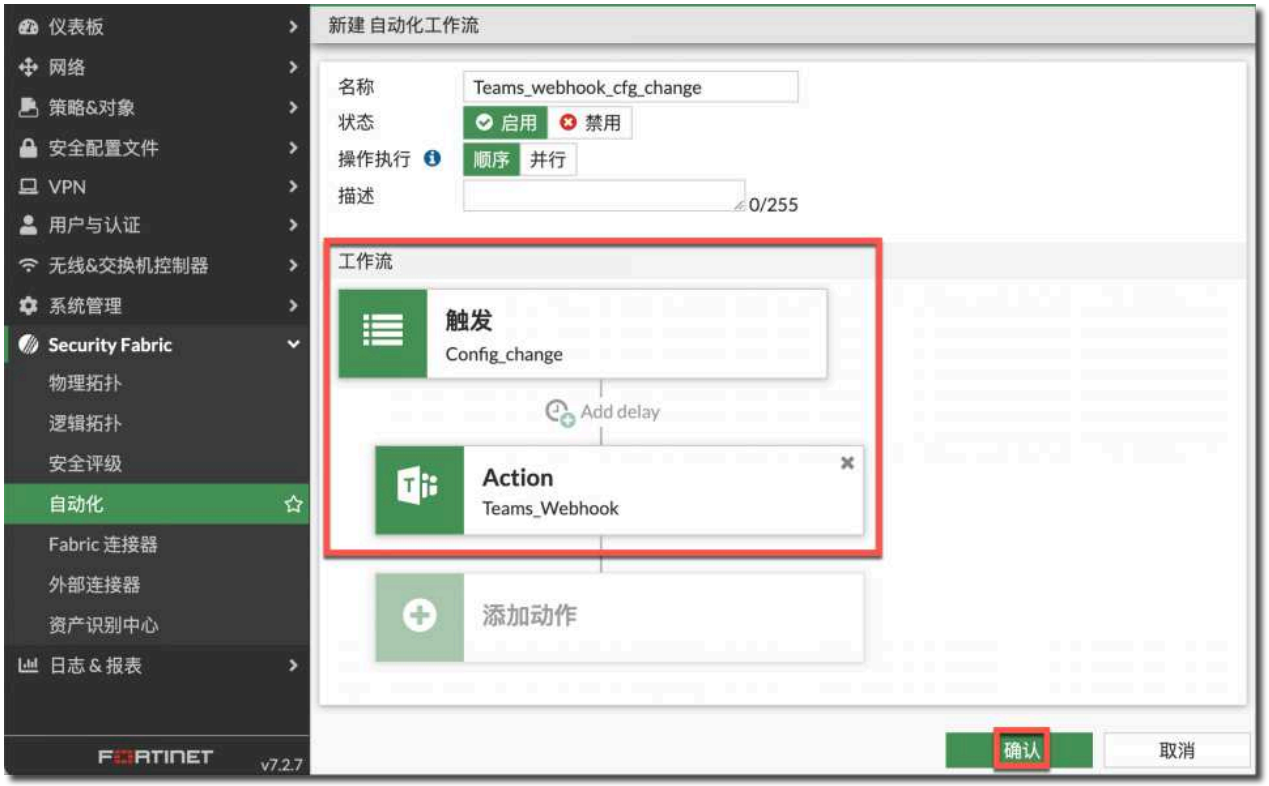
9. 在选择条目中选择上步创建的动作（Action），点击应用按钮。




```bash
config system automation-action
    edit "Teams_Webhook"
        set action-type microsoft-teams-notification
        set uri "fortinet.webhook.office.com/webhookb2/7e2f667a-91a7-4e1f-8153-25757d7d7e4a@2c36c478-3d00-452f-8535-48396f5f01f0/IncomingWebhook/c20149904d60451fb6f167ba2cd6b129/ab9845cf-2876-49e7-b558-f3824db2f88a"
    next
end
```

10. 检查无误后，点击确认下发配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



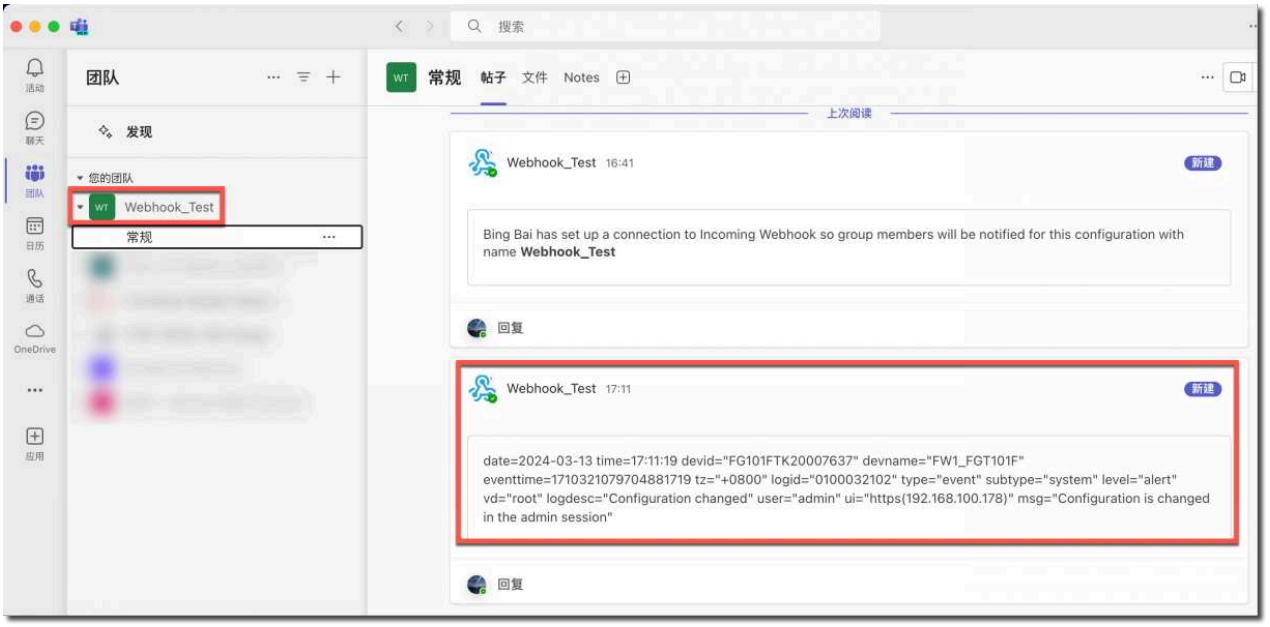

```bash
config system automation-stitch
    edit "Teams_webhook_cfg_change"
        set trigger "Config_change"
        config actions
            edit 1
                set action "Teams_Webhook"
                set required enable
            next
        end
    next
end
```

配置验证

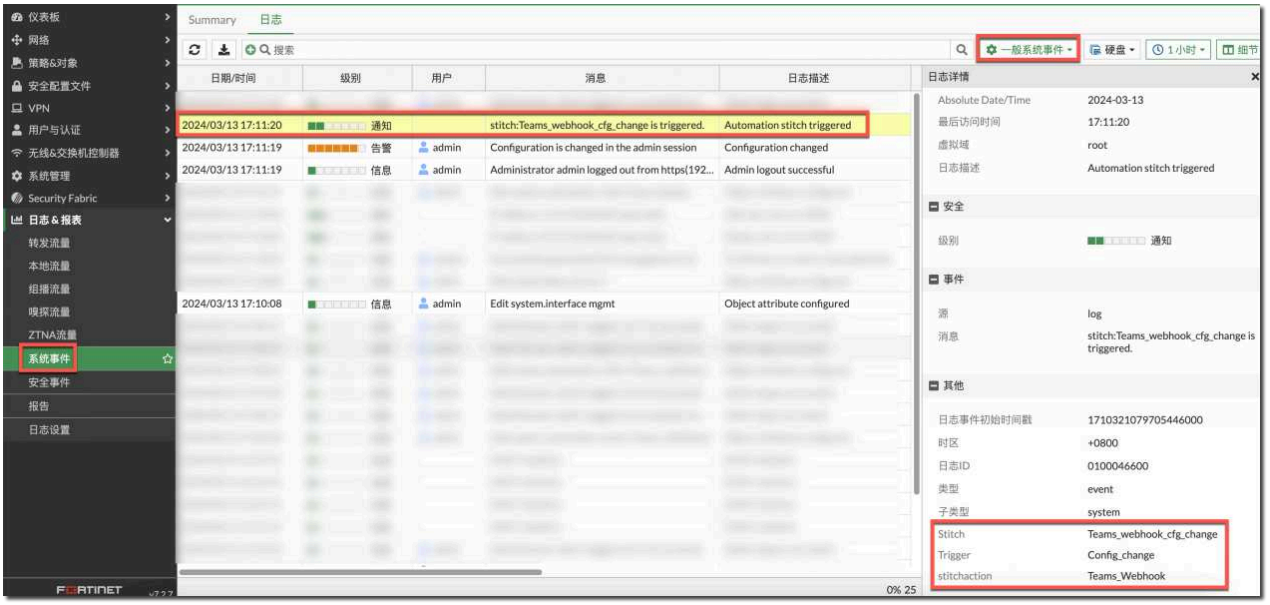
1. 修改FortiGate的配置并退出登录管理员账户。

2. 在Teams的对应频道中可以看到FortiGate通过Webhook自动发送了配置变更的消息，消息内容为修改配置产生的系统事件日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 查看自动化触发的系统事件日志。




```bash
date=2024-03-13 time=17:11:20 eventtime=1710321079705445859 tz="+0800" logid="0100046600" type="event" subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="Teams_webhook_cfg_change" trigger="Config_change" stitchaction="Teams_Webhook" from="log" msg="stitch:Teams_webhook_cfg_change is triggered."
```

4. 查看自动化触发的Debug信息。

```bash
FortiGate # diagnose debug application autod -1
FortiGate # diagnose debug enable

auto_generate_generic_curl_request()-441: Generating generic automation CURL request for action (Teams_Webhook).
auto_generate_generic_curl_request()-493: Generic automation CURL request POST data for action (Teams_Webhook):
{ "text": "date=2024-03-13 time=17:11:19 devid=\"FG101FTK20007637\" devname=\"FW1_FGT101F\"
eventtime=1710321079704881719 tz=\"+0800\" logid=\"0100032102\" type=\"event\" subtype=\"system\" level=\"alert\"
vd=\"root\" logdesc=\"Configuration changed\" user=\"admin\" ui=\"https(192.168.100.178)\" msg=\"Configuration is
changed in the admin session\"" }

auto_generate_generic_curl_request()-548: Generic automation CURL request Host header: fortinet.webhook.office.com
auto_generate_generic_curl_request()-551: Adding 0 user defined headers
pid:283-__handle_msg()-414: Subscriber:4 received package. pubid:2 pkgid:65509 pkg_index:127
pid:283-__handle_pkg_logs()-356: Subscriber:4 processing package size:1215 logs:1 pickup:1
auto_event_pub_handle_log()-331: publish 46600 to subscr-node
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
pid:283-__subscr_close_cur_pkg()-140: close package size:1215 logs:1
auto_generic_curl_request_close()-632: Generic CURL request response body from
Teams_Webhook(https://fortinet.webhook.office.com/webhookb2/7e2f667a-91a7-4e1f-8153-25757d7d7e4a@2c36c478-3d00-
452f-8535-48396f5f01f0/IncomingWebhook/c20149904d60451fb6f167ba2cd6b129/ab9845cf-2876-49e7-b558-f3824db2f88a):
1
```

5. 查看该自动化工作流的状态统计信息。

```bash
FortiGate # diagnose test application autod 3
alert mail log count: 0

stitch: Teams_webhook_cfg_change

        local hit: 1 relayed to: 0 relayed from: 0
        last trigger:Wed Mar 13 17:11:19 2024
        last relay:
        actions:
                Teams_Webhook:
                        done: 1 relayed to: 0 relayed from: 0
                        last trigger:Wed Mar 13 17:11:19 2024
                        last relay:

logid to stitch mapping:
id:32099  local hit: 0 relayed hits: 0
        Teams_webhook_cfg_change

id:32102  local hit: 1 relayed hits: 0
        Teams_webhook_cfg_change

log category to stitch mapping:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

系统动作

简介

系统动作针对FortiGate包含备份配置（到Flash）、重新启动和关机。

即使FortiGate处于内存保护模式，系统动作也能完成，自动化流程会自动绕过CLI命令确认提示（手动在CLI脚本执行这些操作时需要确认执行）。

CLI配置

3种系统动作的配置已经内置在FortiGate默认配置中。

```bash
config system automation-action
    edit "Backup Config Disk"
        set action-type system-actions
        set system-action backup-config
    next
    edit "Reboot FortiGate"
        set action-type system-actions
        set system-action reboot
    next
    edit "Shutdown FortiGate"
        set action-type system-actions
        set system-action shutdown
    next
end
```

网络需求

当FortiGate进入内存保护模式时，自动备份配置文件到Flash，随后重启设备。

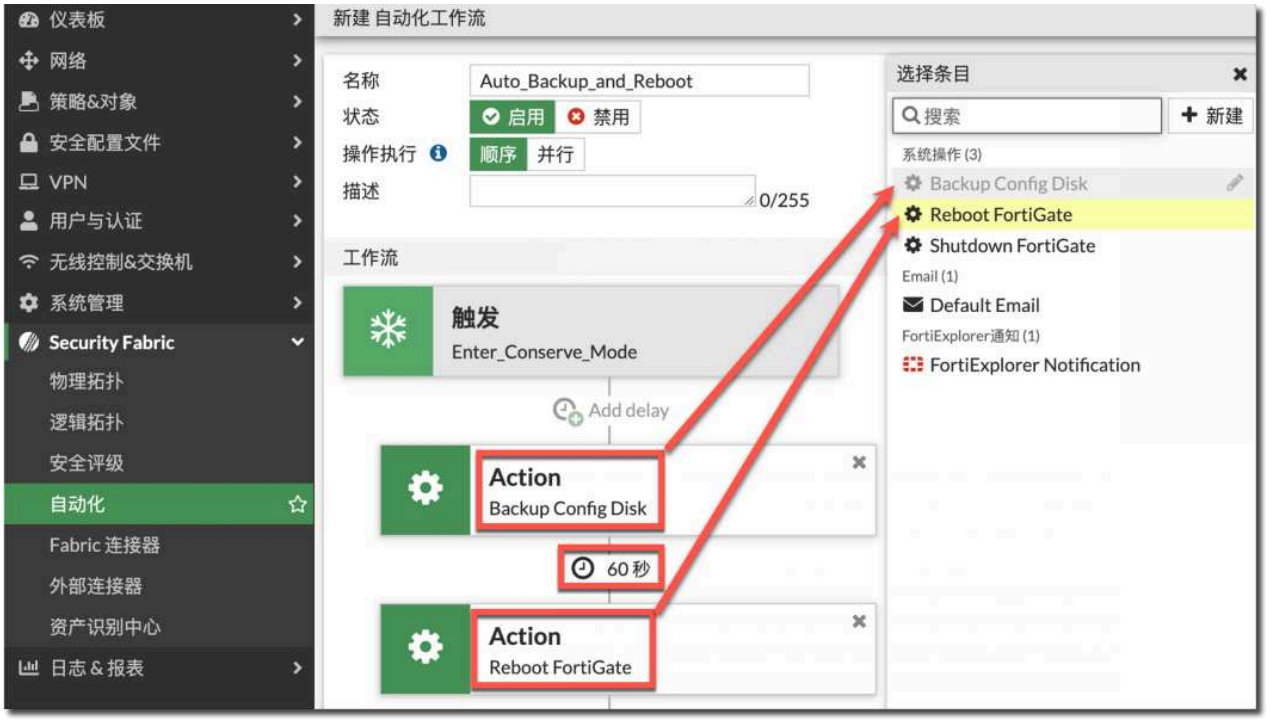
配置步骤

1. 配置设备进入保护模式后自动备份配置并重启。在Security Fabric→自动化中新建自动化工作流，触发条件新建并选择系统分类中的保护模式。



2. 添加第一个动作为预置的Backup Config Disk，第二个动作为Reboot FortiGate，中间添加60s的间隔，然后下发该工作流配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 相关CLI如下，配置了Reboot动作的最小间隔为300s，防止频繁重启。

```bash
config system automation-trigger
    edit "Enter_Conserve_Mode"
        set event-type low-memory
    next
end

config system automation-action
    edit "Reboot FortiGate"
        set action-type system-actions
        set system-action reboot
        set minimum-interval 300
    next
    edit "Backup Config Disk"
        set action-type system-actions
        set system-action backup-config
    next
end

config system automation-stitch
    edit "Auto_Backup_and_Reboot"
        set trigger "Enter_Conserve_Mode"
        config actions
            edit 1
                set action "Backup Config Disk"
                set required enable
            next
            edit 2
                set action "Reboot FortiGate"
                set delay 60
                set required enable
            next
        end
    next
end
```

配置验证

1. 触发FortiGate进入内存保护模式。

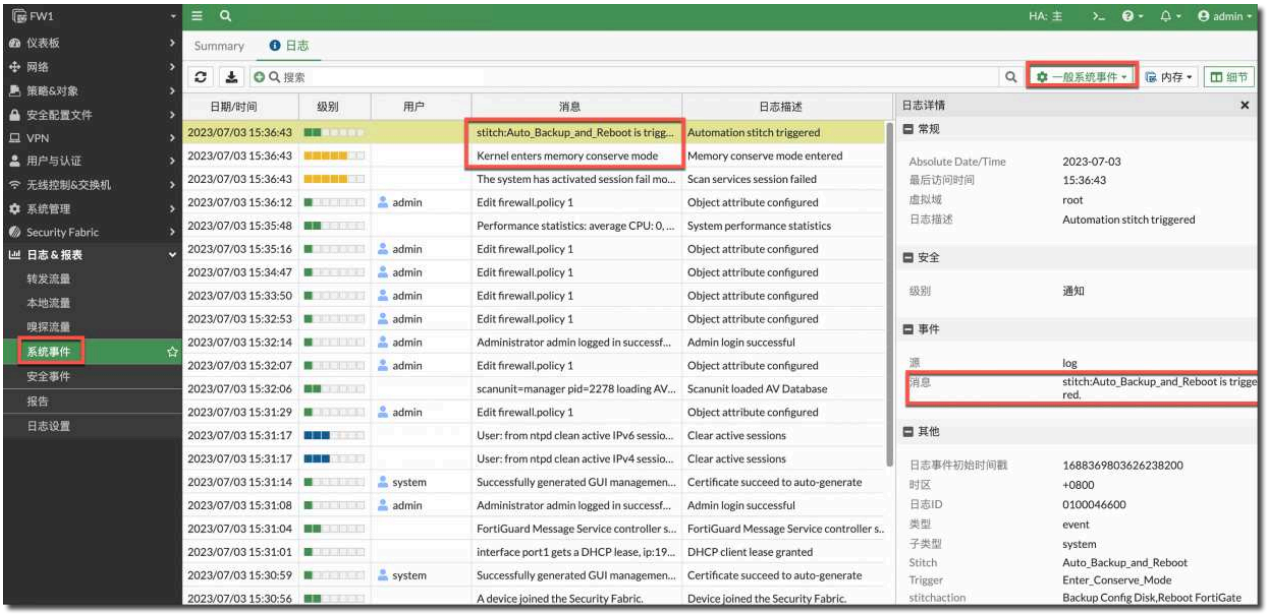
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # diagnose hardware sysinfo conserve
memory conserve mode:                          on
total RAM:                                   1465 MB
memory used:                                 1293 MB   88% of total RAM
memory freeable:                              150 MB   10% of total RAM
memory used + freeable threshold extreme:    1392 MB   95% of total RAM
memory used threshold red:                   1289 MB   88% of total RAM
memory used threshold green:                 1201 MB   82% of total RAM
```

2. 查看autod进程的debug信息，可以看到FortiGate进入保护模式后，触发了配置的Trigger，自动执行配置备份到Flash Disk，60s后重启设备。

```bash
FortiGate # diagnose debug application autod -1
......
__dump_action_msg()-26: System will backup config, msg: Autod backup config by stitch: Auto_Backup_and_Reboot
......
__dump_action_msg()-26: System will reboot, msg: Autod reboot by stitch: Auto_Backup_and_Reboot
```

3. 查看自动化触发的系统日志。



4. 查看自动备份的配置文件。

```bash
FortiGate # execute revision list config
Last Firmware Version: V0.0.0-build000-REL0

ID  TIME                ADMIN           FIRMWARE VERSION          COMMENT
6   2023-07-03 15:36:44 daemon_admin    V7.2.5-build1517-REL0     Autod backup config by stitch:
Auto_Backup_and_Reboot
```

5. 查看该自动化流程的的配置和触发统计（使用2可以看统计和配置）。

```bash
FortiGate # diagnose test application autod 3
stitch: Auto_Backup_and_Reboot
        local hit: 3 relayed to: 0 relayed from: 0
        last trigger:Mon Jul  3 15:58:03 2023
        last relay:
        actions:
                Backup Config Disk:
                        done: 3 relayed to: 0 relayed from: 0
                        last trigger:Mon Jul  3 15:57:03 2023
                        last relay:
                Reboot FortiGate:
                        done: 3 relayed to: 0 relayed from: 0
                        last trigger:Mon Jul  3 15:57:03 2023
                        last relay:
```

6. 在HA环境下，自动化中备份配置的动作是不会同步的，只有触发了自动化的那台设备会备份配置到Flash Disk。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate1 # execute revision list config
Last Firmware Version: V0.0.0-build000-REL0
ID  TIME                  ADMIN             FIRMWARE VERSION          COMMENT
6   2023-07-03 15:36:44   daemon_admin      V7.2.5-build1517-REL0     Autod backup config by stitch:
Auto_Backup_and_Reboot

FortiGate2 # execute revision list config
Last Firmware Version: V0.0.0-build000-REL0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

自动抓包

网络需求

某客户遇到HA中的成员FortiGate由于HA心跳包丢失而成为双主状态，影响到正常业务。但出现该问题后一段时间会自动恢复，且出现的时间随机。

需要在出现此问题时在两台FortiGate的心跳接口抓取HA心跳报文，以进一步定位问题，但由于该问题出现的时间不固定，不好掌握抓包的时机。

通过自动化功能，可以实现在FortiGate HA心跳包丢失时，自动抓取心跳接口的报文，并发送至指定邮箱。

配置步骤

自动化触发器

配置自动化触发器为事件日志类型，事件日志类型为“Heartbeat packet lost”，logid为37910。

```bash
config system automation-trigger
    edit "HA_HB_Lost"
        set event-type event-log
        set logid 37910
    next
end
```

自动化动作

1. 配置第1个自动化动作，在HA心跳接口抓取HA心跳报文，该报文为二层报文，ether protocol默认为0x8890，抓取个数为100个。为了防止频繁触发抓包进程导致的内存占用问题，配置最小触发间隔为120s。

```bash
config system automation-action
    edit "Sniffer_HA_HB_Start"
        set action-type cli-script
        set minimum-interval 120
        set script "diagnose sniffer packet port8 \'ether proto 0×8890\' 6 100 l"
        set accprofile "super_admin"
    next
end
```

2. 配置第2个自动化动作，将抓包结果发送到指定邮箱。

```bash
config system automation-action
    edit "Email_HA_HB_Lost_Sniffer_Result"
        set action-type email
        set email-to "bbai@fortinet.com"
        set email-subject "HA_HB_Lost_Sniffer_Result"
        set message "%%results%%"
    next
end
```

自动化工作流

配置自动化工作流，触发器引用已创建的“Heartbeat packet lost”类型的事件日志触发器，触发器触发后，动作为开始在HA心跳接口抓包，并发送抓包结果。

```bash
config system automation-stitch
    edit "HA_HB_Lost_Sniffer"
        set trigger "HA_HB_Lost"
        config actions
            edit 1
                set action "Sniffer_HA_HB_Start"
                set required enable
            next
            edit 2
                set action "Email_HA_HB_Lost_Sniffer_Result"

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
                set required enable
            next
        end
    next
end
```

- 触发器引用已创建的“Heartbeat packet lost”类型的事件日志触发器。
- 第1个动作引用开始抓取HA心跳报文的动作，抓取到100个包后会自动停止。
- 第2个动作引用发送邮件的动作，发送抓包结果。
- 第3个动作引用停止抓包的动作。

配置验证

1. 触发HA中两台FortiGate的心跳报文检测超时，并产生“Heartbeat packet lost”的HA系统事件日志。

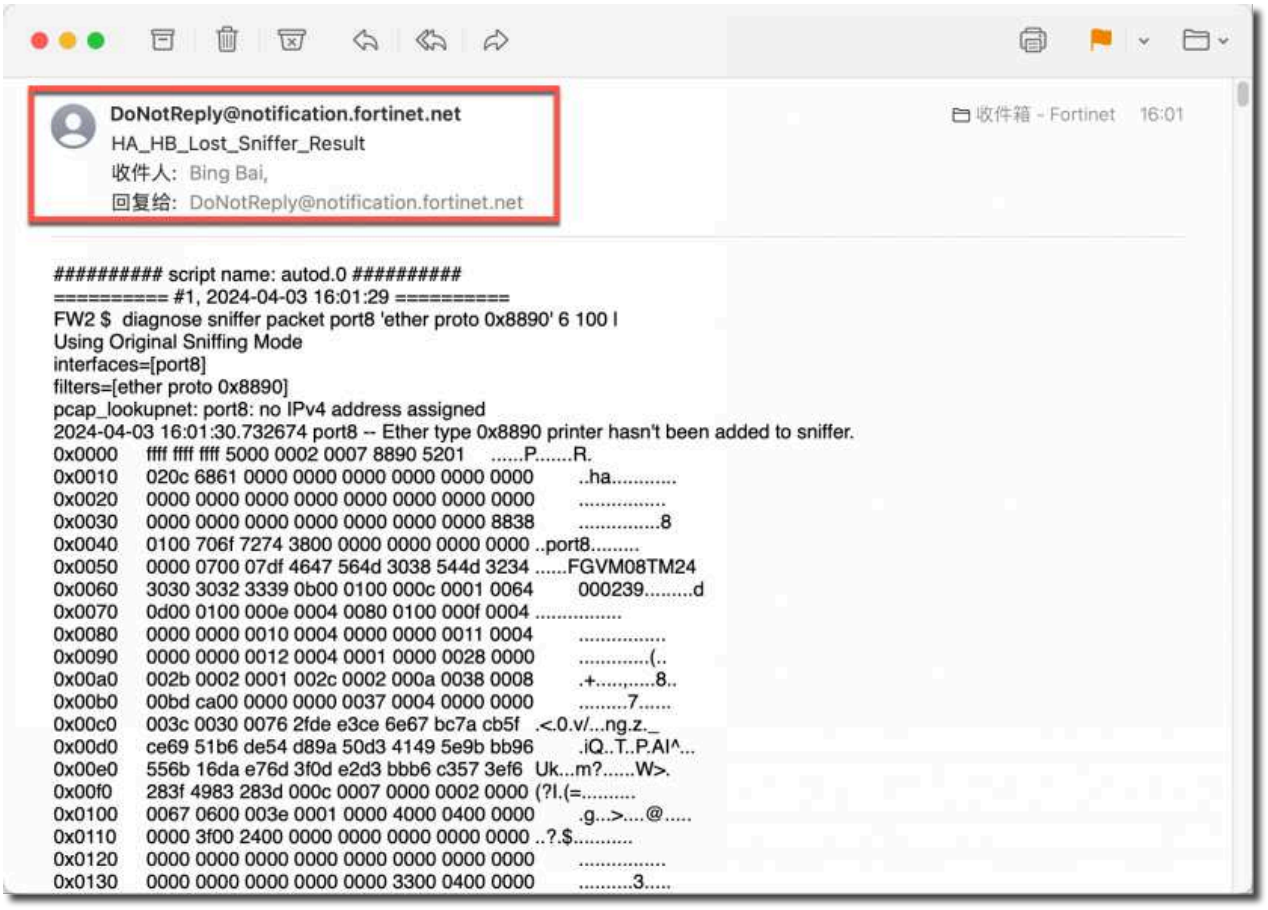
```bash
date=2024-04-02 time=17:02:22 eventtime=1712048543265466260 tz="+0800" logid="0108037910" type="event"
subtype="ha" level="critical" vd="root" logdesc="Heartbeat packet lost" msg="Heartbeat packet lost"
ha_role="primary" devintfname="dmz"
```

2. 随后触发了自动化流程。

```bash
date=2024-04-02 time=17:02:22 eventtime=1712048543265705880 tz="+0800" logid="0100046600" type="event"
subtype="system" level="notice" vd="root" logdesc="Automation stitch triggered" stitch="HA_HB_Lost_Sniffer"
trigger="HA_HB_Lost" stitchaction="Sniffer_HA_HB_Start,Sniffer_HA_HB_Stop,Email_HA_HB_Lost_Sniffer_Result"
from="log" msg="stitch:HA_HB_Lost_Sniffer is triggered."
```

3. 配置的收件邮箱收到了包含抓包结果的邮件。

> **重要**
>
> 当HA心跳接口只有一对时，HA发生心跳丢失会造成HA成员成为双主状态，此时HA的2个成员设备由于都触发了“Heartbeat packet lost”类型的事件日志，均会执行自动化流程，并发送抓包结果邮件到指定邮箱。



4. FortiGate上的autod进程对应的自动化执行Debug信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FW1 # diagnose debug application autod -1
FW1 # diagnose debug enable

pid:2044-__handle_pkg_logs()-356: Subscriber:4 processing package size:459 logs:1 pickup:1
pid:2044-__subscr_close_cur_pkg()-140: close package size:459 logs:1
__action_cli_script_open()-186: cli script action:Sniffer_HA_HB_Start is called. svc ctx:0×1072dd90
accprof:super_admin script:
diagnose sniffer packet port8 'ether proto 0×8890' 6 100 l

......

__cli_script_close()-121: cli script:
autod.0
 output:
########## script name: autod.0 ##########

========== #1, 2024-04-03 16:01:29 ==========
FW1 $  diagnose sniffer packet port8 'ether proto 0×8890' 6 100 l
Using Original Sniffing Mode
interfaces=[port8]
filters=[ether proto 0×8890]
pcap_lookupnet: port8: no IPv4 address assigned
2024-04-03 16:01:30.743701 port8 -- Ether type 0×8890 printer hasn't been added to sniffer.
0×0000   ffff ffff ffff 5000 0001 0007 8890 5201        ......P.......R.

......

__action_email_hdl()-181: email action (Email_HA_HB_Lost_Sniffer_Result) is called.
from:
to:bbai@fortinet.com;
subject:HA_HB_Lost_Sniffer_Result
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

威胁情报源

简介

威胁源列表是一个动态列表，其中可以包含域名、IPv4/IPv6地址、地址范围及子网、MAC地址等。FortiGate可将其用作防火墙策略、代理策略、Local-in策略、ZTNA规则中的源地址或目标地址，DNS Filter分类、Web Filter分类等功能中。

威胁源列表有以下几种类型：

- **FortiGuard分类**：可以在WebFilter中的远程分类中使用。
- **IP地址**：IPv4/IPv6地址、地址范围及子网。可将其用作防火墙策略、代理策略、Local-in策略、ZTNA规则中的源地址或目标地址。
- **域名**：可将其作为DNS过滤配置文件中"远程类别"组下的一个类别，用于阻止或监控匹配该类别的域名。
- **MAC地址**：可以包含MAC地址、MAC地址范围及MAC OUI。可将其作为防火墙策略、代理策略及ZTNA规则的源。对于透明模式策略或虚拟线对（VWP）策略，MAC地址威胁源可作为源地址或目标地址使用。
- **恶意软件哈希**：FortiGate获取该列表后，当在AV启用"使用外部恶意软件阻止列表"功能后，可以选择将其应用于AV的文件哈希检查。该功能不需要开启“防病毒扫描”（av-scan）功能。

威胁源列表有两种更新方式：

- **外部订阅**
  - 该文件需要以文本文件格式（txt）存储于外部服务器（HTTP/HTTPS），FortiGate会从外部服务器定期更新该列表。
- 如果FortiGate与外部服务器失去连接，威胁源列表将继续运行。但威胁源列表将不会更新（添加/删除条目），直到与外部服务器重新建立连接。
- **API推送（FortiOS 7.2.1开始支持）**
  - 通过Push API的方式更新威胁源列表。
  - 威胁源列表存放在FortiGate本地，而不是HTTP/HTTPS服务器上。
  - Push API的方法分为三种：add（添加）、remove（删除）、snapshot（覆盖原有全部条目为推送的条目）。

资源格式要求

文件格式

- 外部资源需要使用纯文本格式，其中每个条目独占一行。文件内可通过`#`号添加注释，例如：`# 这是注释内容`。
- 外部资源更新周期可设置为1 ~ 43200 min。
- 外部威胁源不进行重复条目验证。
- 若外部威胁源内的条目数量超过限制，将显示警告，超出阈值的额外条目将不会被加载。

FortiGuard分类

- 可以使用通配符，例如：`*.domain.com`。
- 支持IDN和UTF编码的URL。
- URL可为IPv4或IPv6地址。IPv6 URL必须采用`[ ]`格式，如`[2100::2]`。
- 示例txt文本：

```bash
# 以下为示例内容
www.fortinet.com
*.fortinet.com
münchen.de
202.103.1.1
[2001:0db8::eade:27ff:fe04:9a01]
```

IP地址

- IP地址可为单个地址、子网地址或地址范围。例如：`192.168.1.1`、`192.168.10.0/24`、`192.168.100.1-192.168.100.254`。
- 地址可为IPv4或IPv6格式。
- 示例txt文本：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
# 以下为示例内容
192.168.2.100
172.200.1.4/32
172.16.1.0/24
172.16.8.1-172.16.8.100
2001:db8::eade:27ff:fe04:9a00/120
2001:0db8::eade:27ff:fe04:aa01-2001:0db8::eade:27ff:fe04:ab01
```

域名

- 域名列表支持通配符，例如：`*.test.com`。
- 支持IDN格式。
- 示例txt文本：

```bash
# 以下为示例内容
*.test.com
www.fortinet.com
handbook.fortinet.com.cn
münchen.de
新华网.cn
```

- DNS Filter引用示例：

```bash
config system external-resource
    edit "fqdn"
        set type domain
        set category 193
        set resource "https://handbook.fortinet.com.cn/fqdn.txt"
    next
end

config dnsfilter profile
    edit "default"
        set external-ip-blocklist "fqdn"
    next
end
```

MAC地址

- MAC地址可以是单个地址、MAC OUI或地址范围。如：`01:01:01:01:01:01`、`8c:aa:b5`、`01:01:01:01:01:01-01:01:02:50:20:ff`。
- MAC地址中的十六进制数字必须用`:`分隔。
- 示例txt文本：

```bash
# 以下为示例内容
01:01:01:01:01:01
8c:aa:b5
01:01:01:01:01:01-01:01:02:50:20:ff
```

- 防火墙策略引用示例：

```bash
config system external-resource
    edit "mac"
        set type mac-address
        set resource "https://handbook.fortinet.com.cn/mac.txt"
    next
end

config firewall policy
    edit 2
        set srcintf "lan"
        set dstintf "wan1"
        set action deny
        set srcaddr "mac"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

恶意软件哈希

- 恶意软件哈希列表需遵循严格格式方为有效。每个哈希签名条目必须独占一行。有效签名格式如下：

```bash
# 加上hash算法的描述，以空格隔开
aa67243f746e5d76f68ec809355ec234  md5

# 加上hash算法的描述，以空格隔开
a57983cb39e25ab80d7d3dc05695dd0ee0e49766  sha1

# 加上hash算法的描述，以空格隔开
ae9bc0b4c5639d977d720e4271da06b50f7c60d1e2070e9c75cc59ab30e49379 sha256

# 无效条目
7688499dc71b932feb126347289c0b8a_md5_sample2
7614e98badca10b5e2d08f8664c519b7a906fbd5180ea5d04a82fce9796a4b87sha256_sample3
```

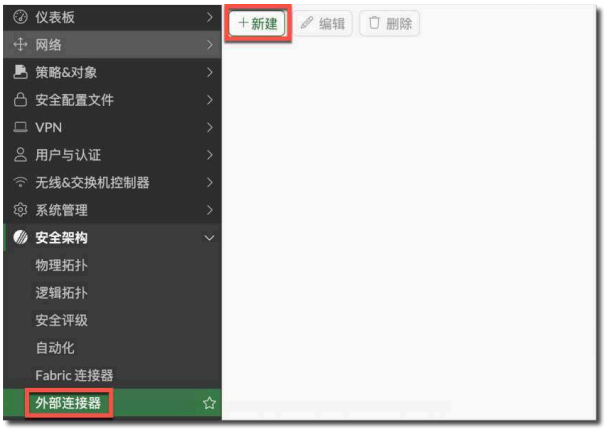
- AV配置文件引用示例：

```bash
config system external-resource
    edit "av"
        set type malware
        set resource "https://handbook.fortinet.com.cn/av.txt"
    next
end

config antivirus profile
    edit "default"
        set external-blocklist "av"
    next
end
```

配置步骤

外部订阅

1. 这里以IP地址威胁源为例。进入FortiGate的“安全架构→外部连接器”页面，点击“新建”按钮。



2. 选择“外部源”中的“IP地址”选项。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



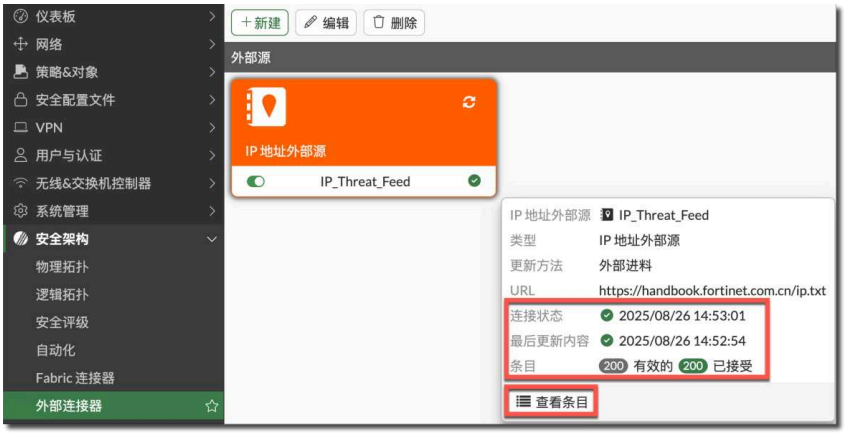
3. 配置IP威胁源列表的名称，更新方法选择“外部进料”，外部资源URL填写HTTP/HTTPS服务器上的txt文本文件链接，按需开启“HTTP认证”与“客户端认证书认证”，刷新率使用默认的5min。

> **重要**
>
> - 示例中提供的URL仅用于演示目的，并不代表一个维护良好的IP地址列表。建议您使用一个信誉良好的外部IP地址列表URL，且该列表应定期更新。
> - 为了提高连接的安全性，建议使用HTTPS链接，并按需开启“HTTP认证”与“客户端认证书认证”。



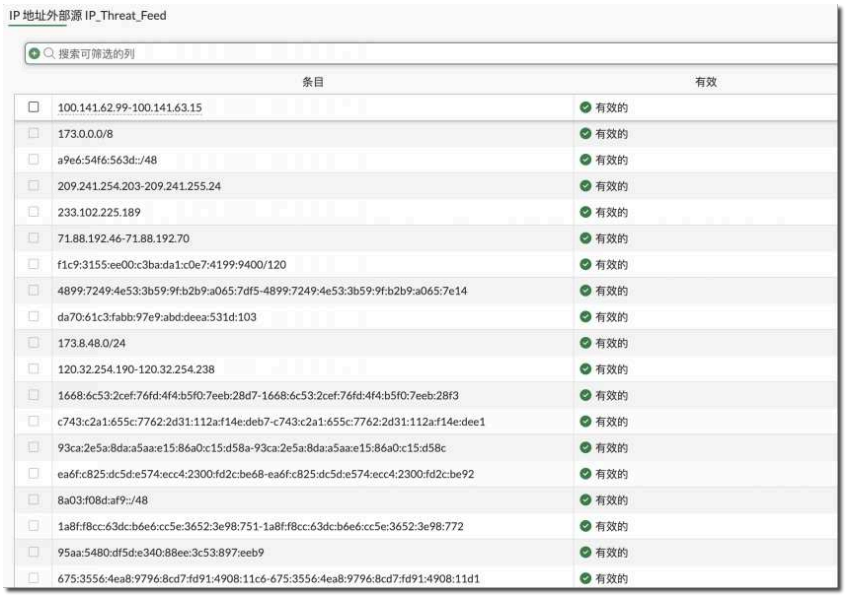

```bash
config system external-resource
    edit "IP_Threat_Feed"
        set type address
        set resource "https://handbook.fortinet.com.cn/ip.txt"
    next
end
```

4. 鼠标悬浮至该IP威胁源列表上，可以看到该外部源的连接状态（绿色√表示与外部服务器正常连接，红色×表示与外部服务器通信中断）、最后更新时间和当前的条目数，点击右上角的刷新按钮可以立刻请求更新。



5. 点击查看条目按钮，可以看到FortiGate从外部服务器上获取到的IP地址列表，有效状态表示该IP格式是否符合FortiGate要求。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 如果是无法识别的IP格式，则会显示红色×，如下所示恶意软件哈希外部源获取到的格式为IP地址，就会显示无效标记。



7. 创建防火墙策略，在目标地址中引用该IP威胁源列表对象，动作选择“拒绝”。

重要

由于示例里的IP威胁源列表中同时包含IPv4和IPv6地址，针对防火墙策略配置：

- 源要同时引用IPv4地址对象和IPv6地址对象。
- 目的地址要同时引用IPv4威胁源和IPv6威胁源，FortiGate获取到“IP威胁源列表”后，会自动将其中的IPv4和IPv6地址分别放在两个地址对象中。
- 当然，也可以将此防火墙策略拆分成2条，一条IPv4的，一条IPv6的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config firewall policy
    edit 2
        set name "Deny_Threat_IP"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "192.168.100.0/24"
        set dstaddr "IP_Threat_Feed"
        set srcaddr6 "all"
        set dstaddr6 "IP_Threat_Feed"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

8. 内网客户端穿过FortiGate访问IP威胁源列表中的IP地址，访问失败，FortiGate产生了拦截的防火墙日志。

```bash
date=2025-08-26 time=15:28:29 eventtime=1756193309197961159 tz="+0800" logid="0000000013" type="traffic"
subtype="forward" level="notice" vd="root" srcip=192.168.100.177 srcport=53915 srcintf="lan" srcintfrole="lan"
dstip=17.57.145.25 dstport=5223 dstintf="wan1" dstintfrole="wan" dstthreatfeed="IP_Threat_Feed"
srccountry="Reserved" dstcountry="United States" sessionid=392389 proto=6 action="deny" policyid=2
policytype="policy" poluuid="f18e907a-824b-51f0-8704-409b8dba5152" policyname="Deny_Threat_IP" service="tcp/5223"
trandisp="noop" appcat="unscanned" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 crscore=30 craction=131072
crlevel="high" srcserver=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

9. 在Local-in策略中调用IP威胁源列表。

```bash
config firewall local-in-policy
    edit 1
        set intf "port1"
        set srcaddr "IP_Threat_Feed"
        set dstaddr "all"
        set action deny
        set service "ALL"
        set schedule "always"
    next
end
```

10. 在DNS过滤器中调用IP威胁源列表，可以阻止客户端以DNS的方式访问威胁源中的IP。

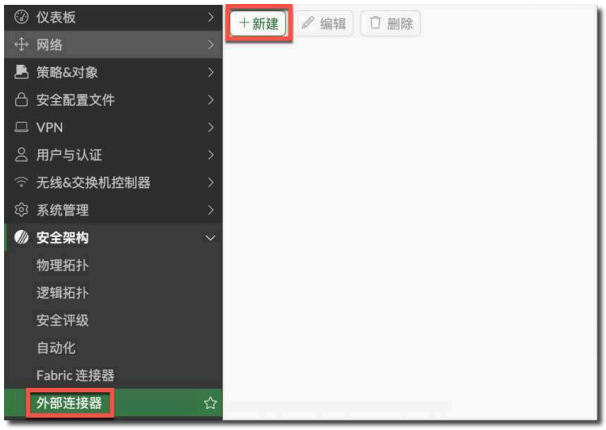
```bash
config dnsfilter profile
    edit "dns_profile"
        set external-ip-blocklist "IP_Threat_Feed"
    next
end

date=2025-08-26 time=15:06:50 eventtime=1675724810452621179 tz="-0800" logid="1501054400" type="utm" subtype="dns"
eventtype="dns-response" level="warning" vd="root" policyid=0 sessionid=555999 srcip=192.168.100.178 srcport=35113
srccountry="Reserved" srcintf="lan" srcintfrole="undefined" dstip=17.57.145.25 dstport=53 dstcountry="Reserved"
dstintf="root" dstintfrole="undefined" proto=17 profile="dns_profile" xid=25532 qname="www.fortinet.com" qtype="A"
qtypeval=1 qclass="IN" ipaddr="2.2.2.2" msg="Domain was blocked because it is in the domain-filter list"
action="redirect" domainfilteridx=0 domainfilterlist="IP_Threat_Feed"
```

API推送

> **重要**
>
> 该功能在FortiOS 7.2.1及更高版本支持。

1. 这里以FortiGuard威胁源为例。创建API用户，赋予super_admin权限，并生成API key。配置方法请参考：系统管理→管理员配置→API用户↗章节。

2. 进入FortiGate的“安全架构→外部连接器”页面，点击“新建”按钮。

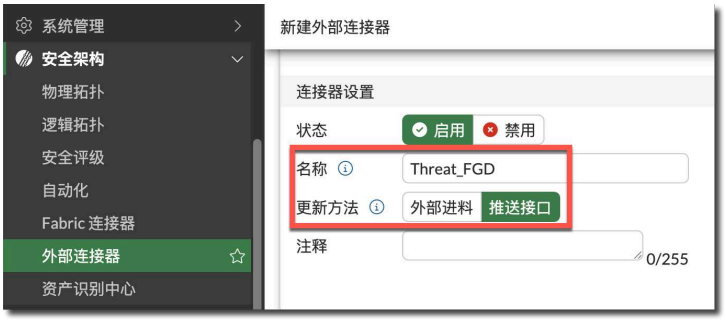


3. 选择“外部源”中的“FortiGuard分类”选项。



4. 配置FortiGuard分类威胁源的名称，更新方法选择“推送接口”，点击确认按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.




```bash
config system external-resource
    edit "Threat_FGD"
        set update-method push
        set category 192
    next
end
```

5. 随后会弹出API示例窗口，在此窗口中，可以根据输入的API密钥、条目（可以多个，以，隔开）、推送命令（添加、删除、快照），来即时生成对应的cURL请求样本，生成后，点击右侧的复制按钮可以复制cURL。注意是否需要修改IP为设备接受API推送的接口IP，这里以添加2个域名为例。



6. 客户端执行该cURL，结果显示执行成功（如果报403错误，可能是API用户权限不够）。

```bash
# curl -k -X POST -H 'Authorization: Bearer q6G9mhwppNjNns40xN5qp45pzmxHHG' --data '{ "commands": [{ "name": "Threat_FGD", "command": "add", "entries": [ "www.summerice.com", "www.abc.com" ] } ]}' "https://192.168.100.99/api/v2/monitor/system/external-resource/dynamic"

{"http_method":"POST","results":[{"name":"Threat_FGD","command":"add","status":"success"}],"vdom":"root","path":"system","name":"external-resource","action":"dynamic","status":"success","serial":"FG101FTK20007637","version":"v7.6.4","build":3596}%
```

7. GUI查看该威胁源的条目数为2。



8. 点击查看条目按钮，可以看到两个域名被成功添加。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



9. 失败的API更新，可以返回错误原因，如下错误原因为更新方法填写错误。

```bash
# curl -k -X POST -H 'Authorization: Bearer q6G9mhwppNjNns40xN5qp45pzmxHHG' --data '{ "commands": [{ "name": "Threat_FGD", "command": "update", "entries": [ "www.summerice.com", "www.abc.com" ] } ]}' "https://192.168.100.99/api/v2/monitor/system/external-resource/dynamic"

{"http_method":"POST","results":[{"name":"Threat_FGD","command":"update","error":"Invalid command.","status":"error"}],"vdom":"root","path":"system","name":"external-resource","action":"dynamic","status":"success","serial":"FG101FTK20007637","version":"v7.6.4","build":3596}%
```

10. 在WebFilter配置文件中的远程分类中，将上述创建的FortiGuard威胁源的动作配置为“屏蔽”。



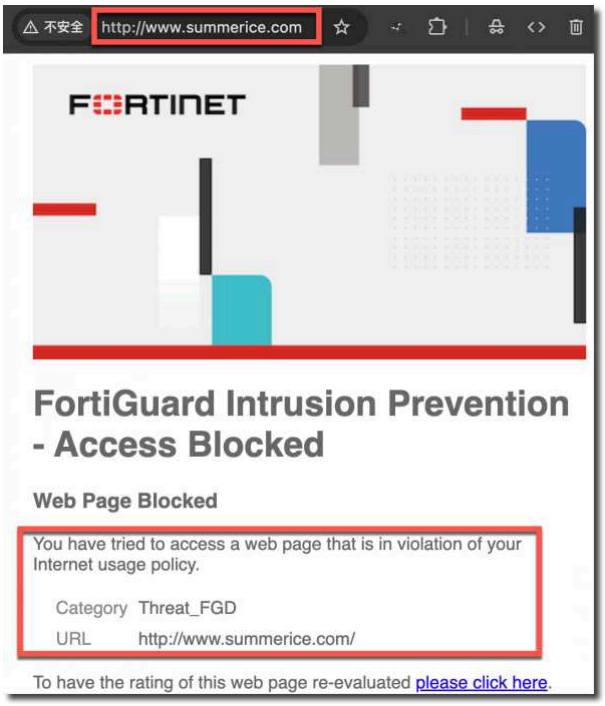

```bash
config webfilter profile
    edit "Treat_FGD"
        config ftgd-wf
            config filters
                edit 35
                    set category 192
                    set action block
                next
            end
        end
    next
end
```

11. 在上网的防火墙策略中调用该WebFilter配置文件。

```bash
config firewall policy
    edit 1
        set name "to_Internet"
        set srcintf "lan"
        set dstintf "wan1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set webfilter-profile "Treat_FGD"
        set logtraffic all
        set nat enable
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 客户端浏览器通过FortiGate访问FortiGuard威胁源中的域名，可以正常拦截威胁源中的网址。



3. cURL中也可以在commands字段中包含多个威胁源，执行不同的动作，如下所示，分别对多个威胁源连接器进行更新，以`,`隔开。

```bash
# curl -k -X POST -H 'Authorization: Bearer q6G9mhwppNjNns40xN5qp45pzmxHHG' --data '{ "commands": [{ "name": "Threat_FGD", "command": "add", "entries": [ "www.summerice.com", "www.abc.com" ]} ,
{"name":"ip","command":"delete","entries":["10.10.10.3/32","10.10.10.4/32"]},
{"name":"domain","command":"snapshot","entries":["www.baidu.com","www.sina.com.cn"]}]}'
"https://192.168.100.99/api/v2/monitor/system/external-resource/dynamic"
```

CLI相关

- 查看威胁源已获取并保存在FortiGate上的列表内容。

```bash
FortiGate # diagnose sys external-resource list IP_Threat_Feed
Dump external resource address table 'IP_Threat_Feed':
167.3.182.140
225.60.62.231/24
31.158.227.180-31.158.228.166
52.231.72.77/24
152.39.145.129/8
......

FortiGate # diagnose sys external-resource list Threat_FGD
Dump external resource category 'Threat_FGD':
www.abc.com
www.summerice.com
```

- 查看外部威胁源列表的统计信息。

```bash
FortiGate # diagnose sys external-resource stats
name: IP_Threat_Feed; uuid_idx: 662; type: address table; update_method: feed; total lines: 200; valid lines: 200;
error lines: 0; used: yes; buildable: 200; total in count file: 200; ranges: 151;
name: Threat_FGD; uuid_idx: 667; type: category; update_method: push; total lines: 2; valid lines: 2; error lines:
0; used: yes; buildable: 2; total in count file: 2;
```

- 通过FortiGate的CLI对Push API类型的威胁源进行更新（add、remove、snapshot）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
diagnose sys external-resource {push-add | push-remove | push-snapshot} <feed_name> <entry>

FortiGate # diagnose sys external-resource push-remove Threat_FGD www.abc.com
Command result: { "name": "Threat_FGD", "command": "remove", "status": "success" }

FortiGate # diagnose sys external-resource list Threat_FGD
Dump external resource category 'Threat_FGD':
www.summerice.com
```

- 通过FortiGate的CLI对威胁源进行更新（使用json command格式，可以对多个威胁源执行不同的动作）。

```bash
FortiGate # diagnose sys external-resource push-api-json-commands '{"commands":
[{"name":"ip","command":"add","entries":["10.10.10.1","10.10.10.2"]},
{"name":"Threat_FGD","command":"snapshot","entries":["www.fortinet.com","www.sina.com.cn"]}]}'

Returned json:
[
  {
    "name":"ip",
    "command":"add",
    "status":"success"
  },
  {
    "name":"Threat_FGD",
    "command":"snapshot",
    "status":"success"
  }
]

FortiGate # diagnose sys external-resource list ip
Dump external resource address table 'ip':
10.10.10.2/32
10.10.10.1
10.10.10.2
10.10.10.1/32

FortiGate # diagnose sys external-resource list Threat_FGD
Dump external resource category 'Threat_FGD':
www.fortinet.com
www.sina.com.cn
```

配置规格

外部资源文件的最大容量和条目数量受设备型号限制。

- 外部资源个数的配置规格可以使用`print tablesize`查看`system.external-resource`部分，如下所示，此FortiGate的全局限制为512个，每个虚拟域VDOM的限制为256个。

```bash
FortiGate # print tablesize
...
system.external-resource: 0 256 512 0
...
```

- 每种外部威胁源文件中的最大条目数及每种型号的文件大小限制如下（入门型号、中端型号、入门型号的具体型号可以参考：系统管理→固件与配置管理→固件版本管理→固件下载↗章节）：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

外部威胁源类型	入门型号	中端型号	高端型号
FortiGuard分类	150 000	300 000	2 000 000
IP地址	300 000	1 000 000	5 000 000
域名	1 000 000	3 000 000	5 000 000
MAC地址	1 000 000	1 000 000	1 000 000
文件大小限制（MB）	128	64	32

ext-resource-session-check

外部威胁源对象（如IP、域名、Web分类等）的内容发生变化后，相关会话的dirty状态变化会根据`ext-resource-session-check`配置决定。

> **重要**
>
> 会话dirty的机制请参考：策略与对象→会话dirty机制 ↗章节。

```bash
config system settings
    set fqdn-session-check { enable | disable }
end
```

- `disable`（默认）：现有会话不会被标记为`dirty`，而是被标记为`persistent`，原有匹配该会话的流量也不会被重新评估（直至该会话老化），仅检查新创建的流量。
- `enable`：现有相关会话被标记为`dirty`，无论是匹配原有会话的流量还是新创建的流量，重新评估为新会话。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

日志存储方式

防火墙上的日志存储主要有4种方式：**1.硬盘；2.内存；3.FortiAnalyzer；4.第三方syslog服务器**

硬盘记录日志

1. 格式化硬盘

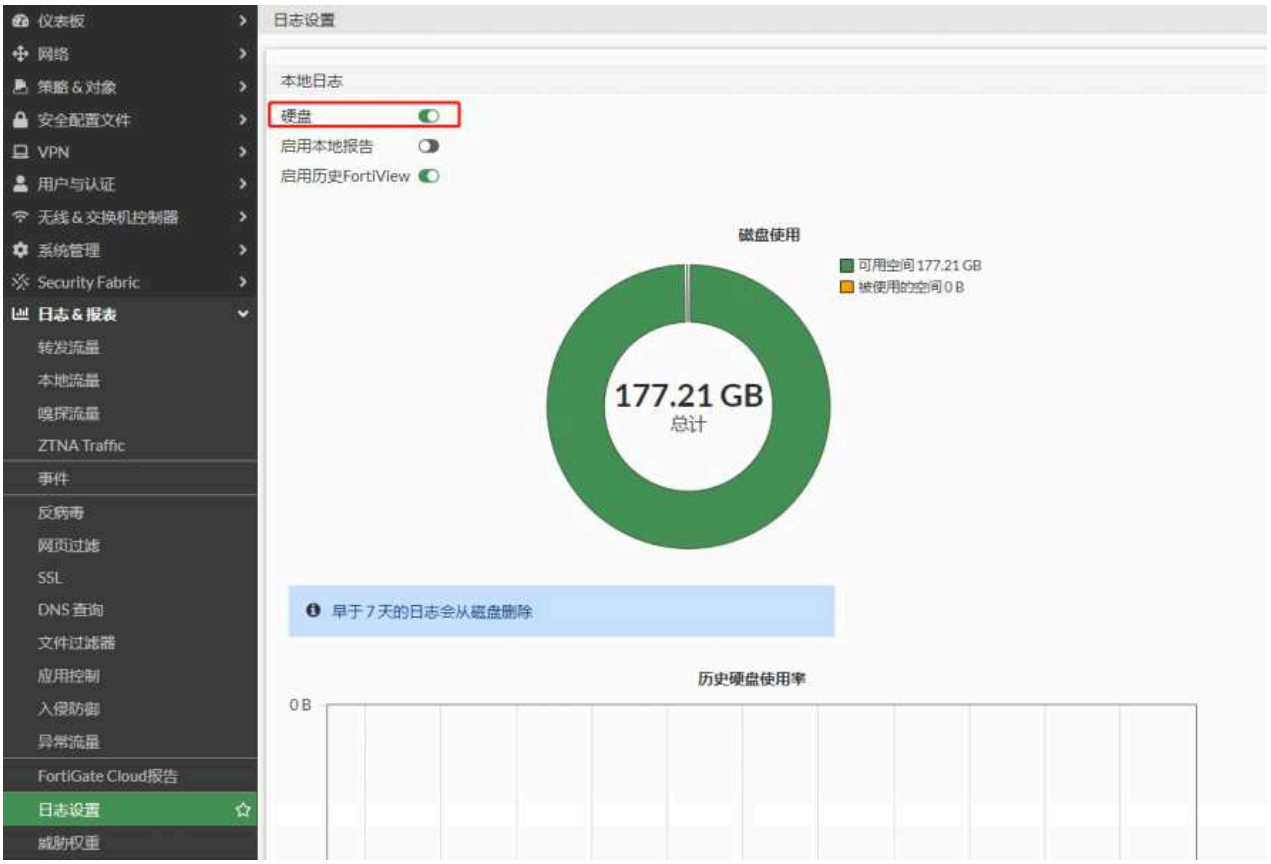
在设备部署前，请先格式化硬盘，以免后续使用硬盘记录日志时产生异常情况，格式化硬盘会重启设备，硬盘中的数据将清空。设备的版本，配置文件是保存在flash中的，不会被影响。

不是所有的FortiGate设备都有硬盘，如FortiGate 500E，FortiGate600F不带硬盘，FortiGate 501E，FortiGate601F带硬盘，没有硬盘则没有execute formatlogdisk命令。

```
FGT # execute formatlogdisk
Log disk is /dev/sda1.
Formatting this storage will erase all data on it, including
  logs, quarantine files;
and require the unit to reboot.
Do you want to continue? (y/n)
```

2. 开启硬盘日志

选择“日志设备”，在本地日志，在”本地日志“中打开”硬盘“选项即可。



3. 不建议使用硬盘记录流量日志

由于流量日志非常大，所以记录于硬盘将带来设备性能损耗，减少硬盘寿命，以及从大量的流量日志中进行查询也非常消耗CPU资源。建议将流量日志发送到FortiAnalyzer或者syslog服务器。

```
过滤硬盘记录流量日志的配置如下：
config log disk filter
    config free-style
        edit 1
            set category traffic

```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set filter "type traffic"
            set filter-type exclude
        next
    end
end
```

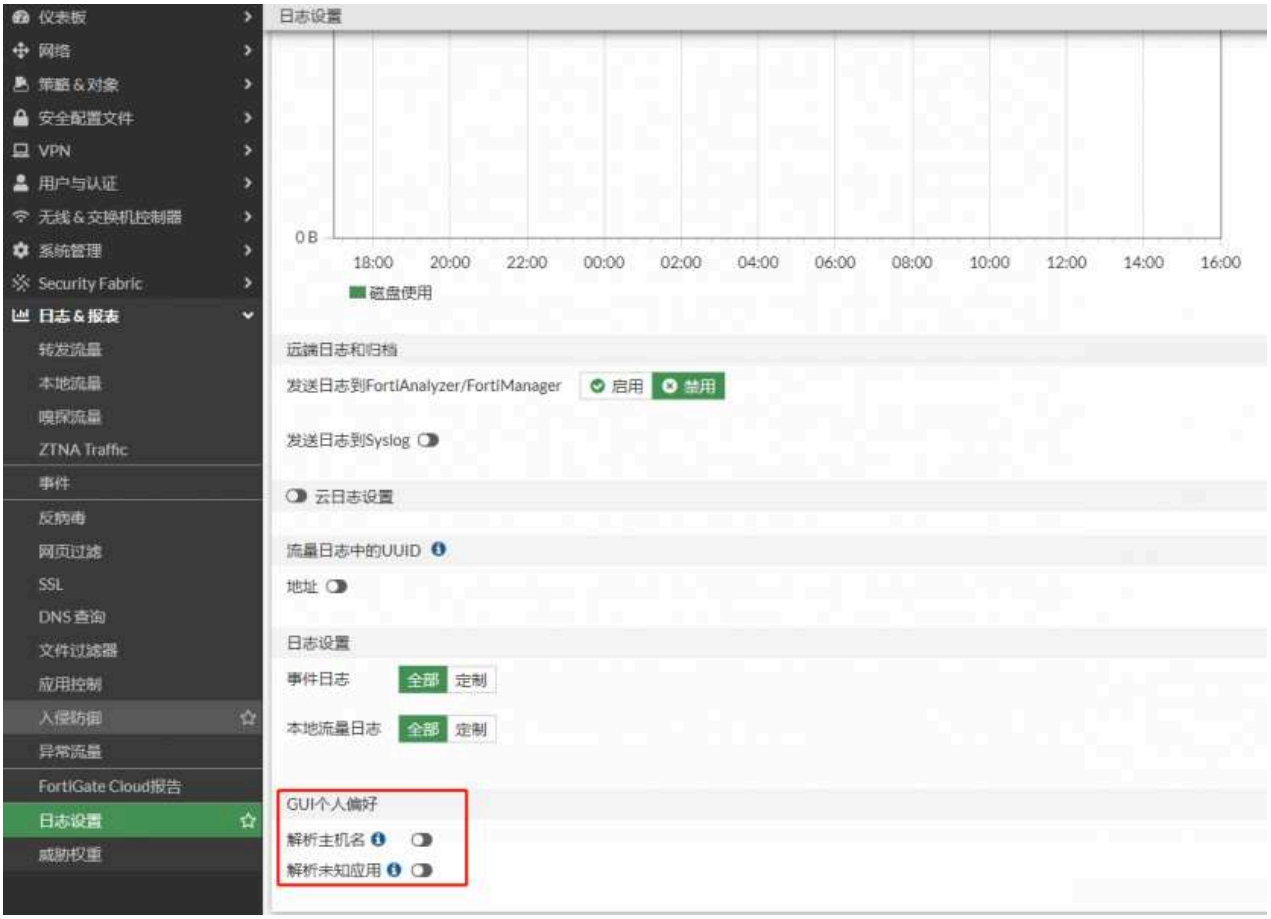
4. 设置硬盘记录日志的参数

默认硬盘日志保存的时间为7天，可以根据需求进行修改。当硬盘满时，会覆盖最早的日志。

```
config log disk setting
    set maximum-log-age 7
    set diskfull overwrite
end
```

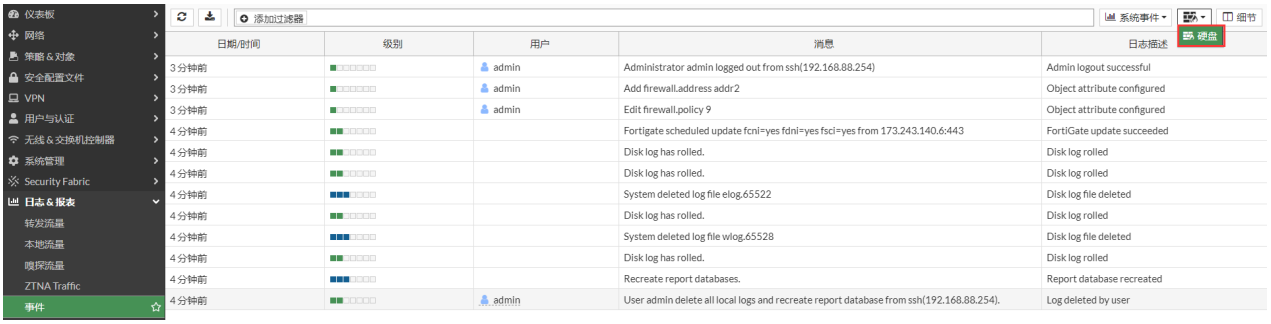
建议取消勾选“解析主机名”和“解析未知应用”两个选项，影响日志观察。

解析主机名：使用反向DNS解析；**解析未知应用**：使用Internet服务数据库解析



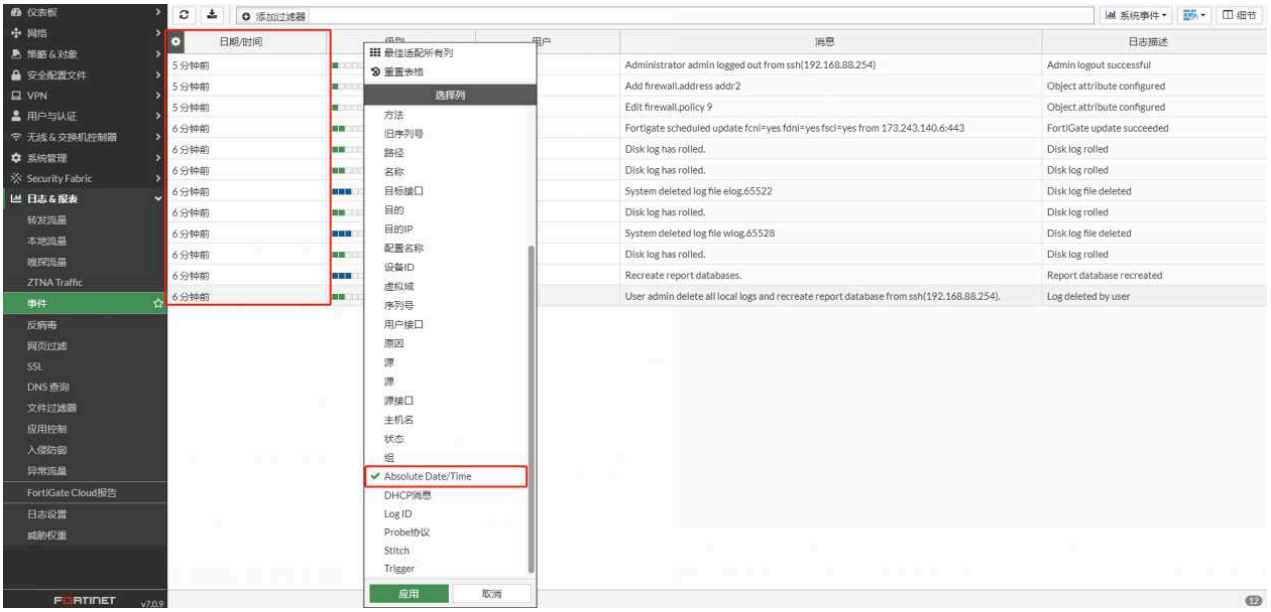
5. 查看硬盘日志

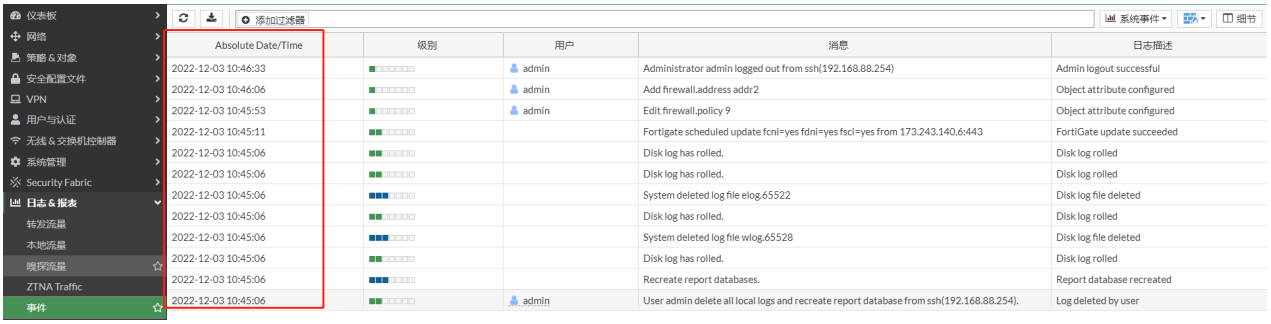
在GUI界面右上角选择“硬盘”，就可以查看到硬盘的对应的日志，也可以通过“添加过滤器”来过滤日志。



上图日志的第一栏显示了日志产生的相对时间，但排错往往需要查看日志的绝对时间。通过右击日志的标题栏，选择“Absolute Date/Time”，去掉原有的“时间/日期”列，就可以看到日志的绝对时间了，而且列是可以拖动的。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





内存记录日志

重要

在FortiGate中不建议使用内存记录日志，建议将日志发送到FortiAnalyzer或者syslog服务器。通常是为了排除任何特定问题或在本地监视日志而临时开启，稍后再禁用它。重启后内存日志会丢失。

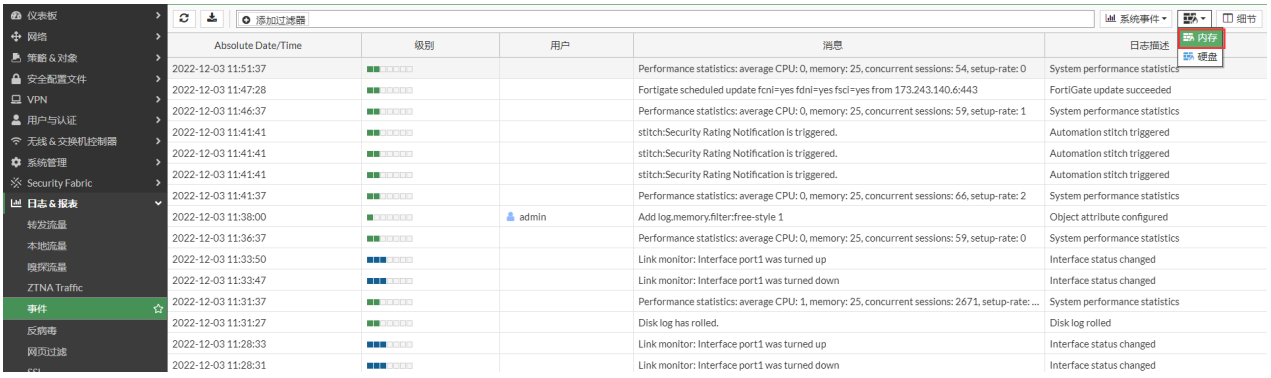
1. 开启内存记录日志

通过在config log memory setting中开启内存记录日志。

```
config log memory setting
    set status enable
end
```

2. 查看内存日志

在GUI界面右上角选择“内存”，查看内存日志。



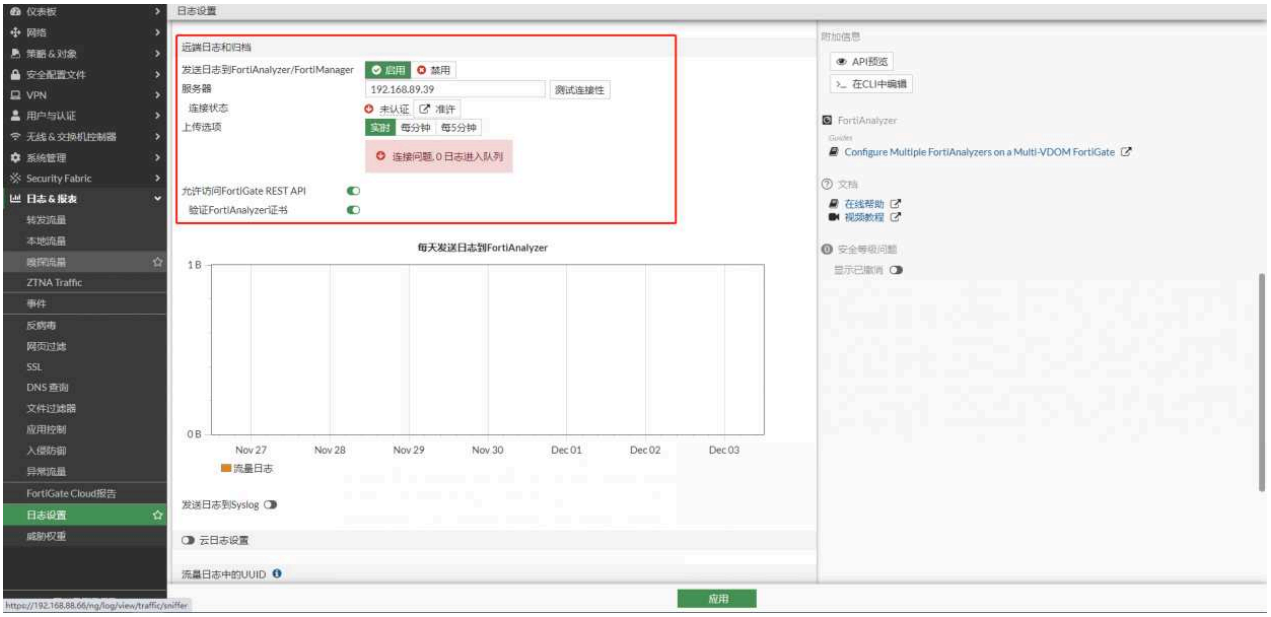
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiAnalyzer记录日志

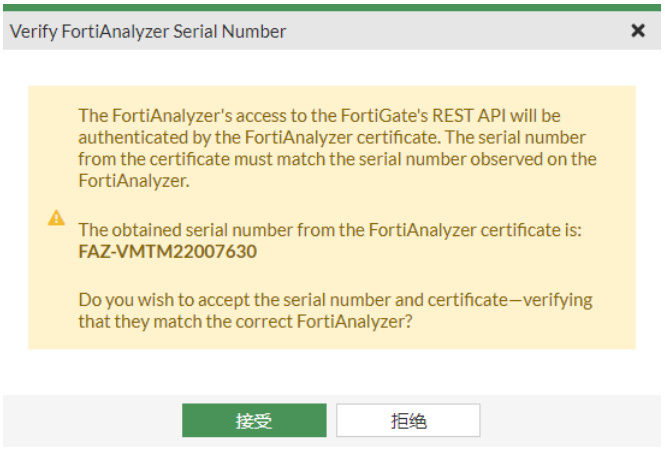
FortiAnalyzer是专门用来做为Fortinet设备的网路安全日志记录、分析、统计和产生报表的产品。FortiGate和FortiAnalyzer之间使用OFTP协议交互，端口是TCP 514。FortiAnalyzer的固件版本应该等于或高于运行在FortiGate上的版本，如FortiAnalyzer的版本如果是7.0，FortiGate的版本可以是7.0或者6.4。

1. **开启FortiAnalyzer记录日志**

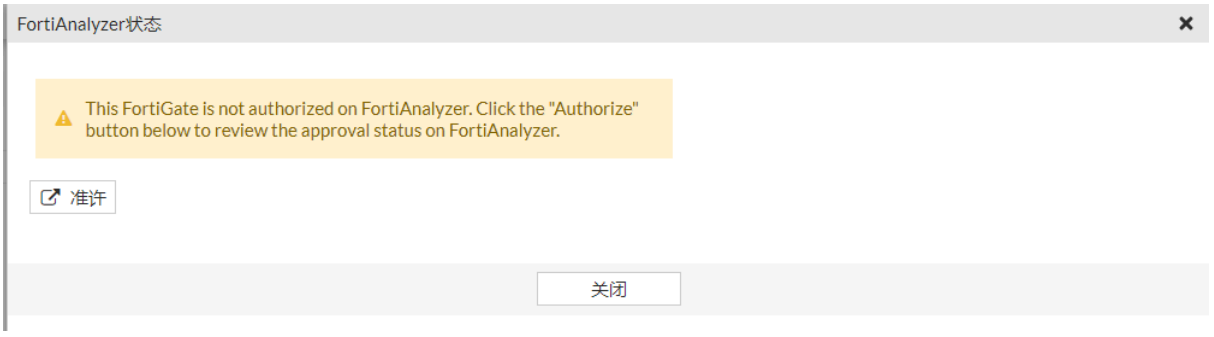
   在“日志设置”中，启用”发送日志到FortiAnalyzer/FortiManager“，“服务器”填写FortiAnalyzer的IP地址，”上传选项“选择 “实时”，然后点击“应用”。



   弹出”Verify FortiAnalyzer Serial Number“，点击“接受”。

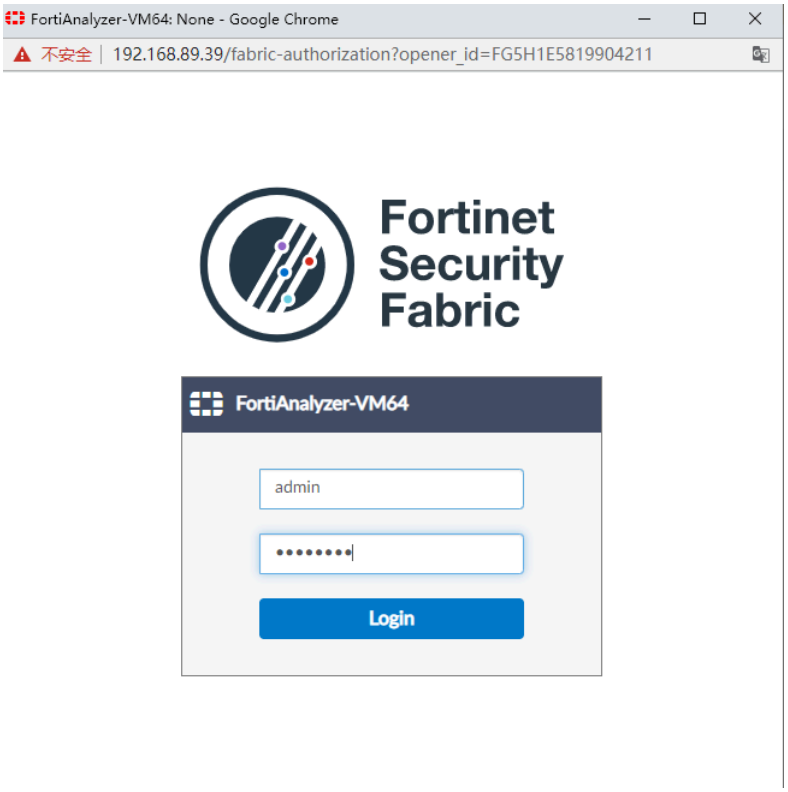


   点击“准许”。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

弹出FortiAnalyzer登录窗口，输入FortiAnalyzer账号密码登录。

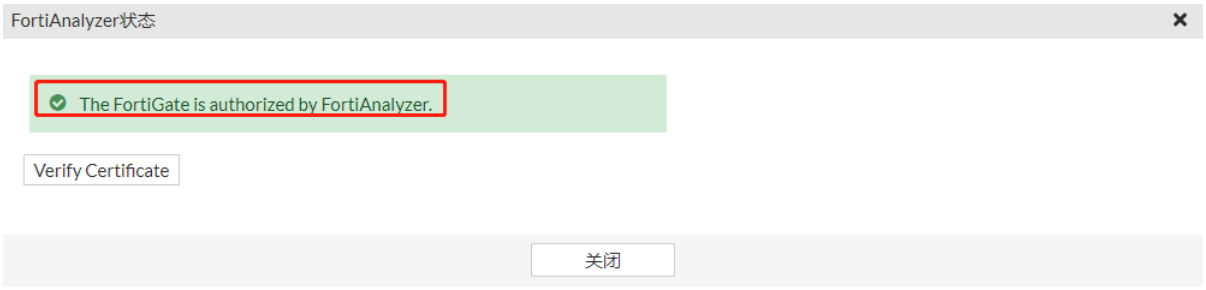


登录成功后，点击“Approve”准许FortiGate注册到FortiAnalyzer，并点击“OK”。



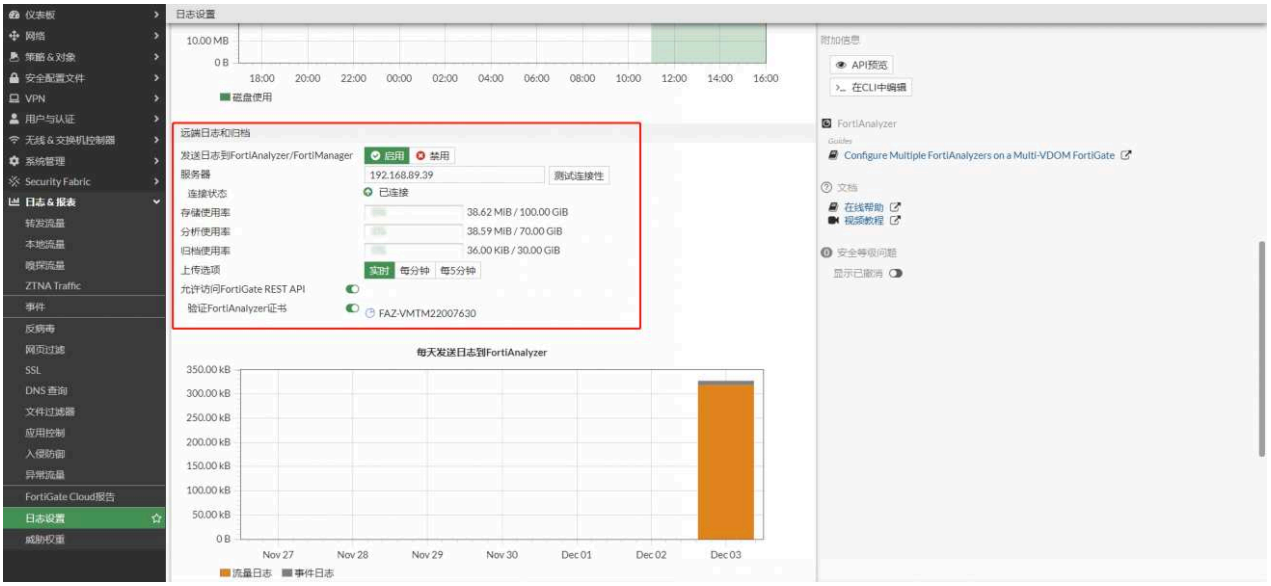
FortiGate已成功被FortiAnalyzer授权成功。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **查看连接状态**

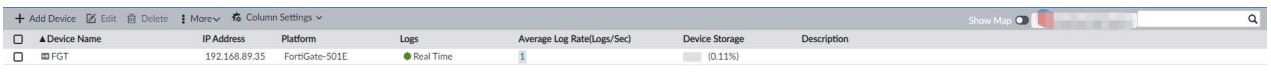
分别从FortiGate和FortiAnalyzer上查看两者的状态。FortiGate连接状态如下，可以通过“测试连接性”进行测试。



FortiGate CLI通过execute log fortianalyzer test-connectivity测试连接状态。

```
# execute log fortianalyzer test-connectivity
FortiAnalyzer Host Name: FAZVM64
FortiAnalyzer Adom Name: root
FortiGate Device ID: FG5H1E5819904211
Registration: registered
Connection: allow
Adom Disk Space (Used/Allocated): 41997274B/107374182400B
Analytics Usage (Used/Allocated): 41960410B/75161927680B
Analytics Usage (Data Policy Days Actual/Configured): 60/60 Days
Archive Usage (Used/Allocated): 36864B/32212254720B
Archive Usage (Data Policy Days Actual/Configured): 0/365 Days
Log: Tx & Rx (33 logs received since 16:19:54 12/03/22)
IPS Packet Log: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx

Certificate of Fortianalyzer valid and serial number is:FAZ-VMTM22007630
```

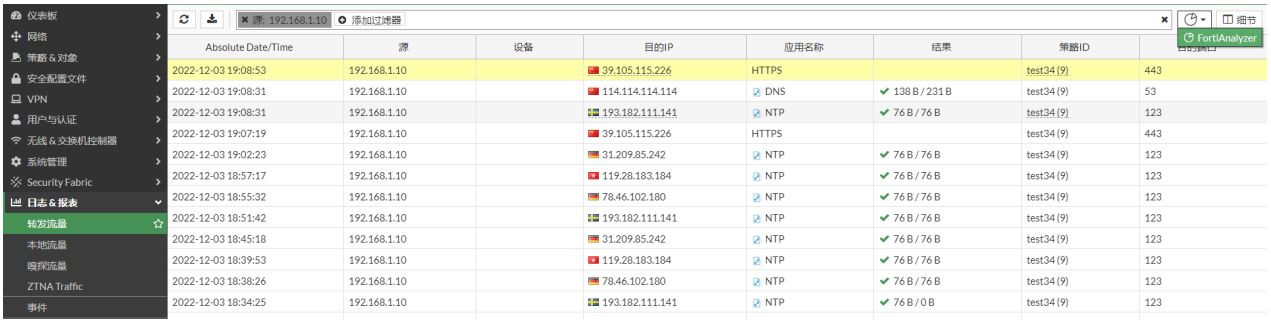
FortiAnalyzer查看该FortiGate连接如下：



3. **在FortiGate上查看FortiAnalyzer的日志**

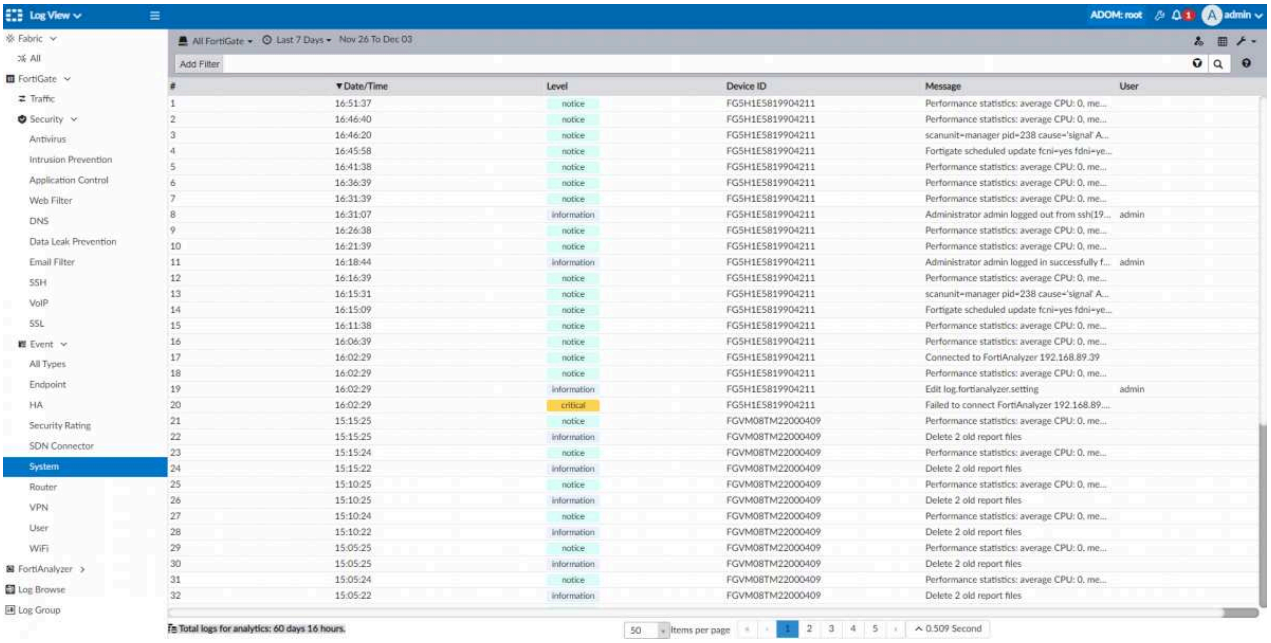
在GUI界面右上角选择“FortiAnalyzer”，查看FortiAnalyzer记录的此FortiGate的日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



4. **在FortiAnalyzer上查看日志**

登录FortiAnalyzer，在Log View界面可以查看到FortiGate产生的系统日志，流量日志，UTM日志等。



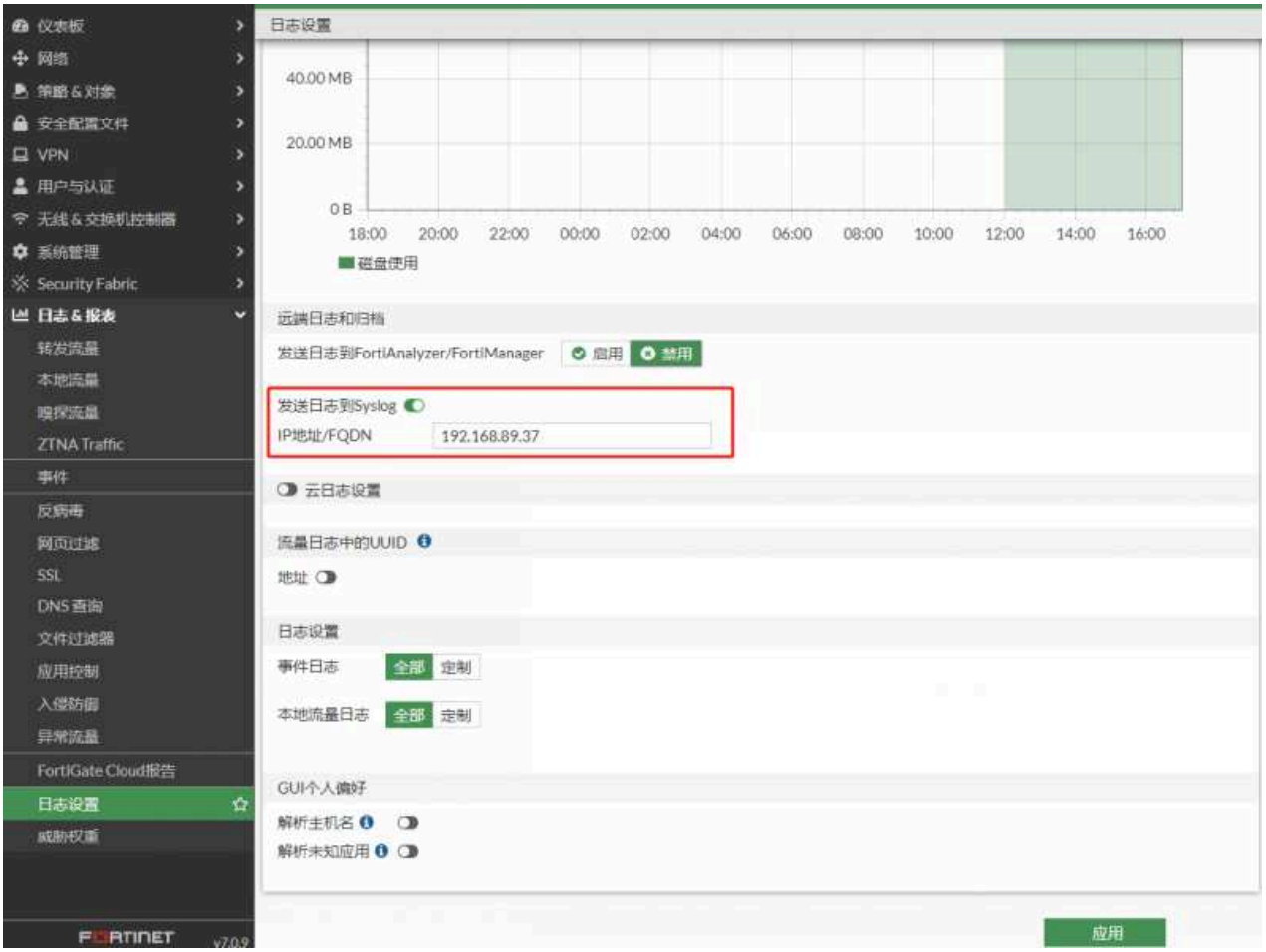
Syslog记录日志

Syslog 也称为系统日志协议，是一种标准协议，用于将事件消息或系统日志发送到特定服务器，即 Syslog 服务器。 Syslog 主要用于从各种机器收集不同的设备日志，并将它们存储在一个中央位置以进行监控和查看。Syslog协议使用UDP 514端口。

1. **开启syslog记录日志**

开启“发送日志到Syslog"，IP地址是syslog服务器的IP地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



对应的命令行如下：

```
config log syslogd setting
    set status enable
    set server "192.168.89.37"
    set port 514           //syslog默认使用UDP 514端口传输数据，可以根据需求修改
end
```

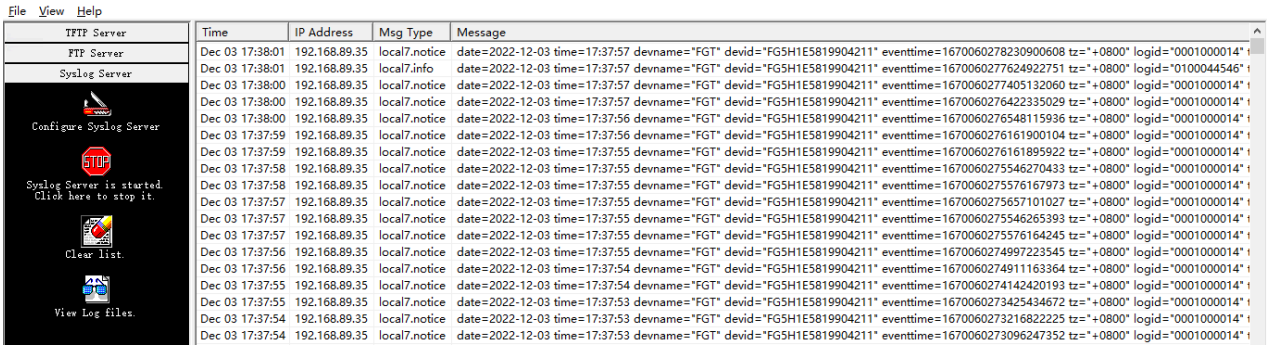
如果有多个syslog服务器，可以通过命令行设置多个。

```
config log syslogd (敲? 号)
syslogd     Configure first syslog device.
syslogd2    Configure second syslog device.
syslogd3    Configure third syslog device.
syslogd4    Configure fourth syslog device.

如设置第2个日志服务器:
config log syslogd2 setting
    set status enable
    set server "192.168.89.38"
end
```

2. **在syslog服务器上查看日志**

如下使用简易的syslog测试软件3CD查看收到的日志。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

日志类型

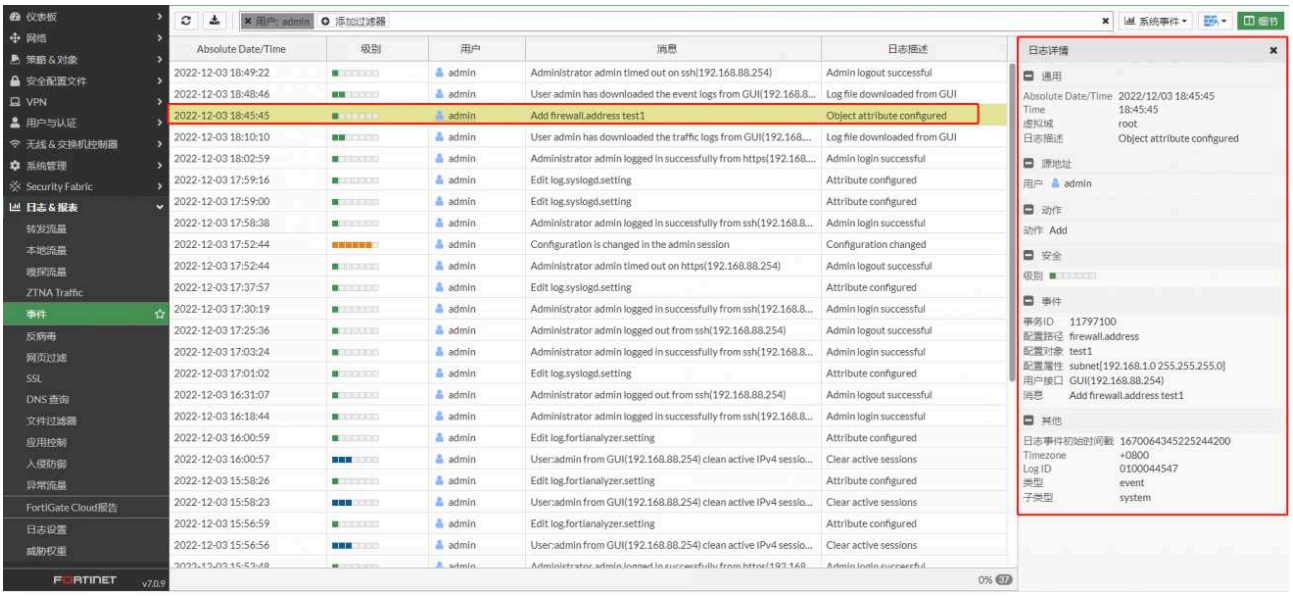
每个日志条目都包含一个Type(类型)字段，该字段表示其日志类型。主要有三种类型：Event（事件日志），Traffic（流量日志），UTM（安全日志）。

事件日志

事件日志用于记录系统和管理事件，如用户的操作日志，进程的活动日志等。根据事件日志 目的原因 的不同又分为很多Subtype（子类），如：System，Router，VPN，SD-WAN，User，Endpoint control，High Availability等，可以在GUI界面根据子菜单查看对应的事件。



如管理员admin的添加地址对象的操作日志



该日志对应的文本

```
date=2022-12-03 time=18:45:45 eventtime=1670064345225244185 tz="+0800" logid="0100044547" type="event"
subtype="system" level="information" vd="root" logdesc="Object attribute configured" user="admin"
ui="GUI(192.168.88.254)" action="Add" cfgtid=11797100 cfgpath="firewall.address" cfgobj="test1"
cfgattr="subnet[192.168.1.0 255.255.255.0]" msg="Add firewall.address test1"
```

流量日志

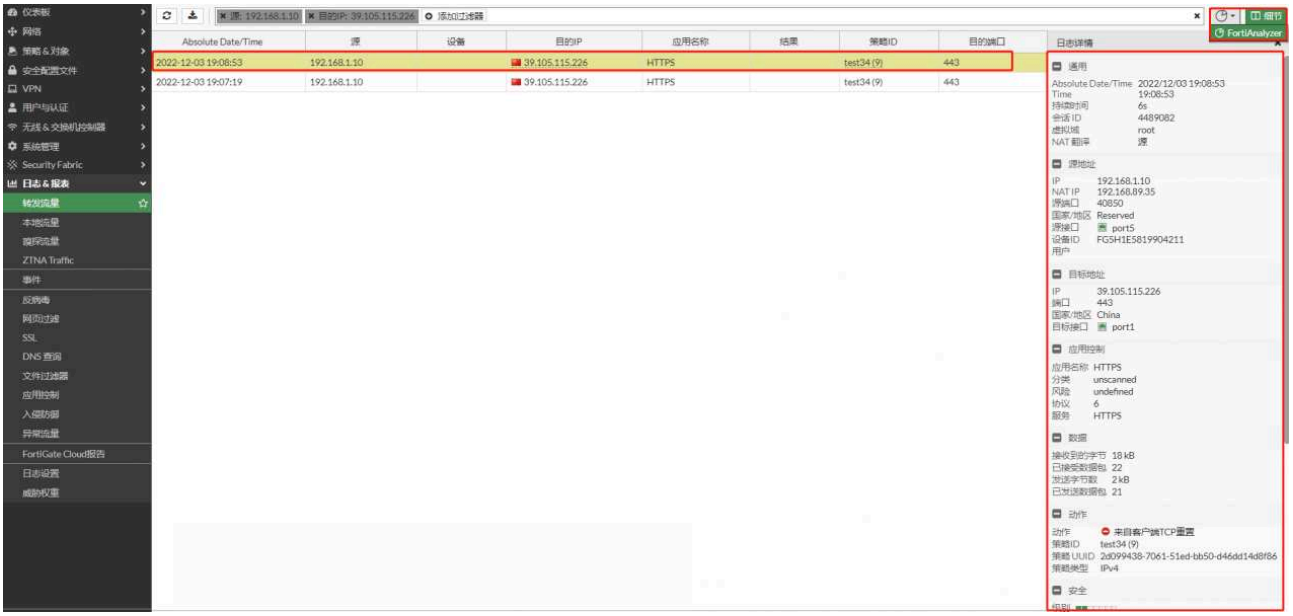
流量日志用于记录流量信息，如终端访问HTTPS站点。根据流量日志 目的原因 的不同又分为很多Subtype（子类），如：Forward，Local，Sniffer等。建议将流量日志发送到FortiAnalyzer或者syslog服务器。

在策略中，”记录允许流量“选择”全部会话“，这样FortiGate才会记录流量日志。“全部会话”包含了“安全事件”。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



流量日志可以在GUI界面通过对应的菜单查看，这里FortiGate GUI的”转发流量“通过FortiAnalyzer读取。



该日志对应的文本

```
date=2022-12-03 time=19:08:53 id=7172877726888493056 itime="2022-12-03 19:08:58" euid=3 epid=1030 dsteuid=3
dstepid=101 logflag=1 logver=700090444 type="traffic" subtype="forward" level="notice" action="client-rst"
policyid=9 sessionid=4489082 srcip=192.168.1.10 dstip=39.105.115.226 transip=192.168.89.35 srcport=40850 dstport=443
transport=40850 trandisp="snat" duration=6 proto=6 sentbyte=2101 rcvdbyte=18304 sentpkt=21 rcvdpkt=22
logid=0000000013 service="HTTPS" app="HTTPS" appcat="unscanned" srcintfrole="undefined" dstintfrole="undefined"
```

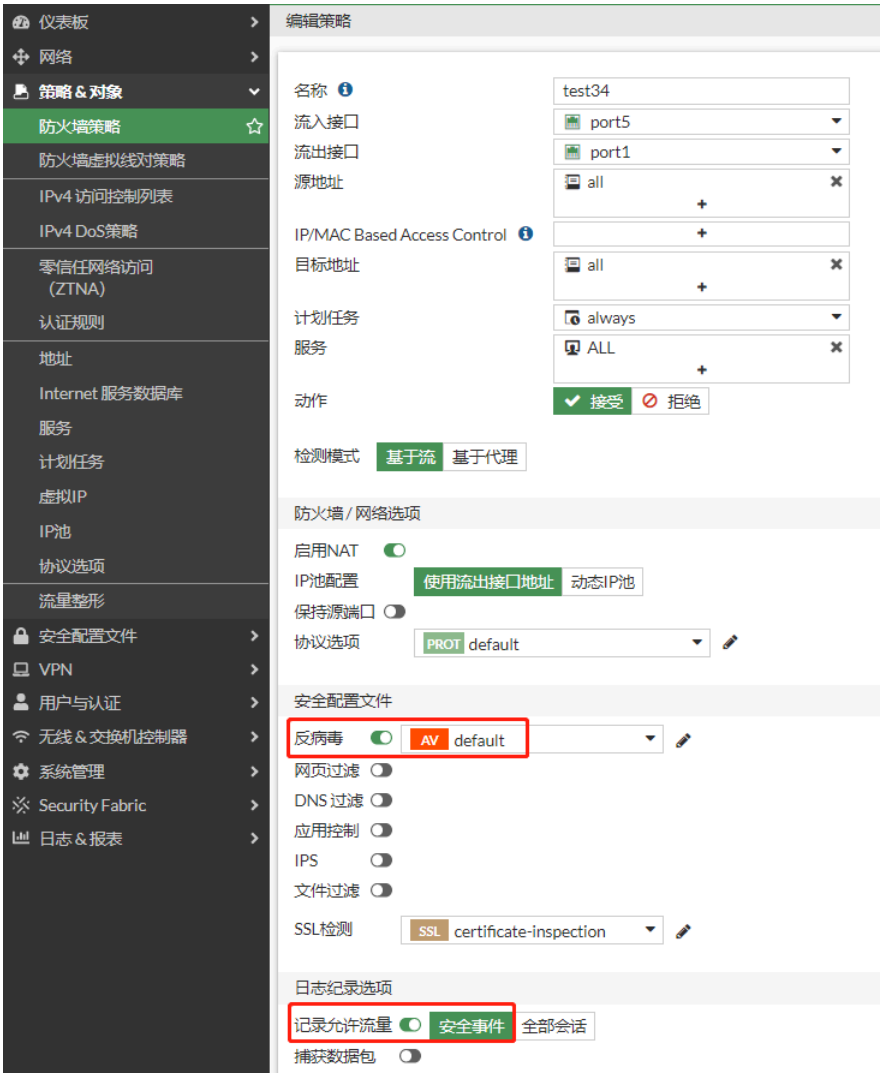

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
policytype="policy" eventtime=1670065734672429913 poluuid="2d099438-7061-51ed-bb50-d46dd14d8f86"
srccountry="Reserved" dstcountry="China" srcintf="port5" dstintf="port1" policyname="test34" tz="+0800"
devid="FG5H1E5819904211" vd="root" dtime="2022-12-03 19:08:53" itime_t=1670065738 devname="FGT"
```

UTM日志

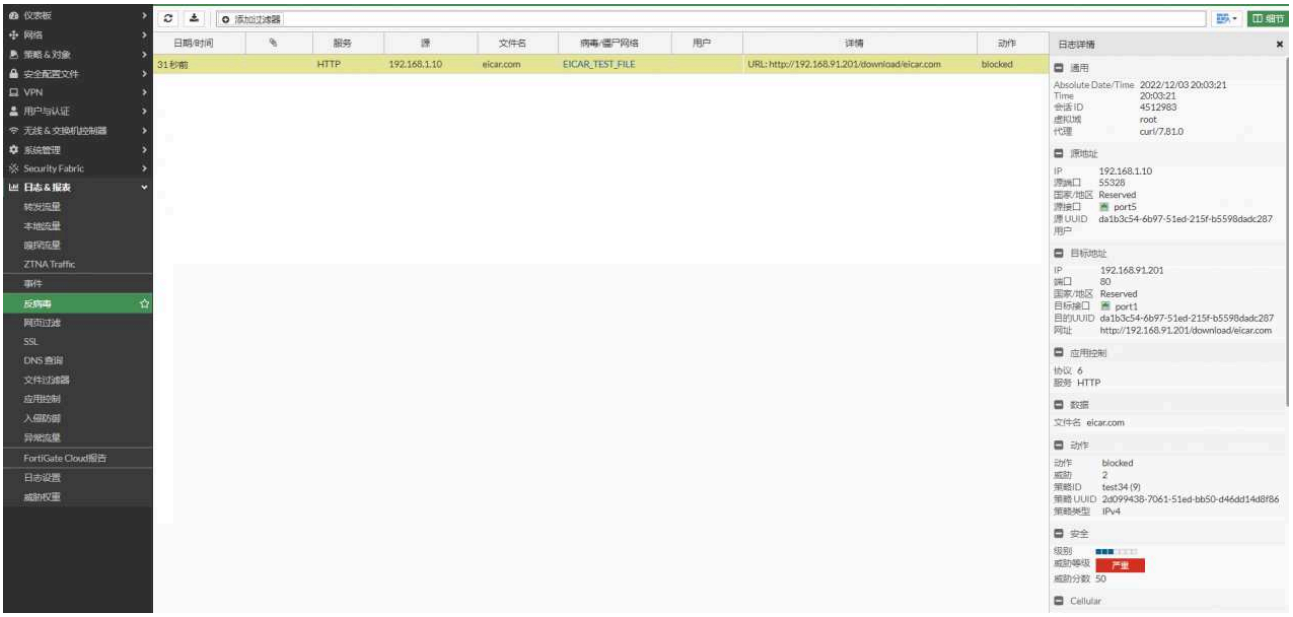
UTM日志用于记录UTM事件，如IPS拦截的流量。根据UTM日志 目的原因 的不同又分为很多Subtype（子类），如：Virus，Web Filter，IPS，App-CTRL等。

在策略中，根据需求开启所需的UTM功能，这里开启AV功能。UTM日志默认是开启的，即“记录允许流量”中的“安全事件”。



反病毒日志可以在GUI界面通过对应的菜单查看。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



该日志对应的文本

```
date=2022-12-03 time=20:03:21 eventtime=1670069001604241098 tz="+0800" logid="0211008192" type="utm" subtype="virus"
eventtype="infected" level="warning" vd="root" policyid=9 poluuid="2d099438-7061-51ed-bb50-d46dd14d8f86"
policytype="policy" msg="File is infected." action="blocked" service="HTTP" sessionid=4512983 srcip=192.168.1.10
dstip=192.168.91.201 srcport=55328 dstport=80 srccountry="Reserved" dstcountry="Reserved" srcintf="port5"
srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" srcuuid="da1b3c54-6b97-51ed-215f-b5598dadc287"
dstuuid="da1b3c54-6b97-51ed-215f-b5598dadc287" proto=6 direction="incoming" filename="eicar.com"
quarskip="Quarantine-disabled" virus="EICAR_TEST_FILE" viruscat="Virus" dtype="av-engine"
ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172 url="http://192.168.91.201/download/eicar.com"
profile="default" agent="curl/7.81.0"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f" analyticssubmit="false" crscore=50
craction=2 crlevel="critical"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

删除日志

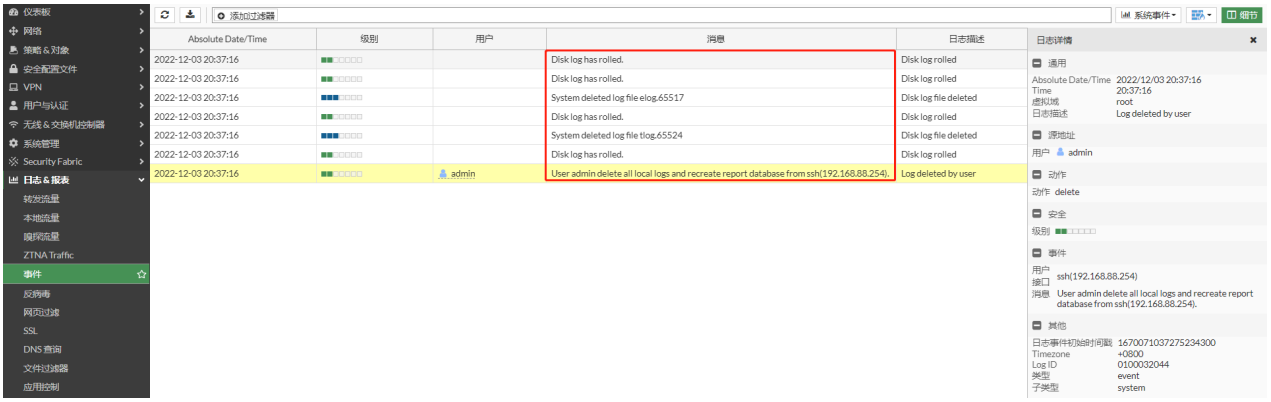
FortiGate可以对记录在本地的日志（硬盘和内存）进行删除。

1. **删除所有的本地日志**

   执行execute log delete-all删除所有日志

```
# execute log delete-all
This will delete all local logs and recreate report database.
Do you want to continue? (y/n)y
```

   删除日志后，删除日志动作本身也会产生日志



2. **指定删除某个类型的日志**

   选择日志的存储类型

```
# execute log filter device
Available devices:
 0: memory
 1: disk
 2: fortianalyzer
 3: fortianalyzer-cloud
 4: forticloud
```

   选择日志的类型

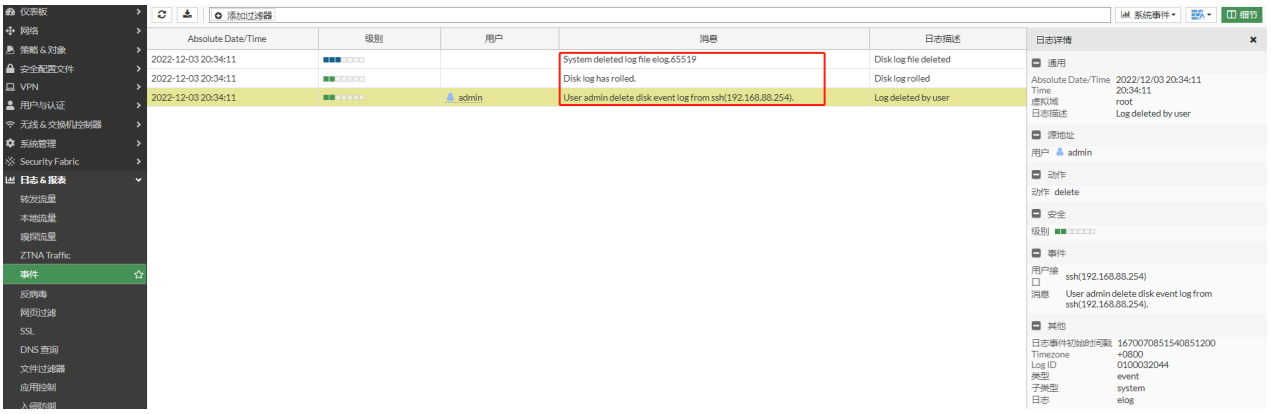
```
# execute log  filter category
Available categories:
 0: traffic
 1: event
 2: utm-virus
 3: utm-webfilter
 4: utm-ips
 5: utm-emailfilter
 7: utm-anomaly
 8: utm-voip
 9: utm-dlp
10: utm-app-ctrl
12: utm-waf
15: utm-dns
16: utm-ssh
17: utm-ssl
19: utm-file-filter
20: utm-icap
22: utm-sctp-filter
```

   删除日志

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
这里删除硬盘的日志事件日志

# execute log filter device 1
# execute log filter category 1
# execute log delete
This will delete disk event log
Do you want to continue? (y/n)y
```

删除日志后，删除动作本身也会产生日志



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

自定义日志过滤器

功能需求

1. 默认情况下，在log filter中配置日志过滤器时（FortiOS 7.0及以上版本），只能指定某个分类的日志的开启和关闭；对于记录的日志级别，只能指定≥一个级别的日志的记录（例如日志级别设置为warning，则会记录warning、error、critical、alert、emergency级别的所有日志）。

```bash
FortiGate # config log disk filter

FortiGate (filter) # set ?
severity             Log to disk every message above and including this severity level.
forward-traffic      Enable/disable forward traffic logging.
local-traffic        Enable/disable local in or out traffic logging.
multicast-traffic    Enable/disable multicast traffic logging.
sniffer-traffic      Enable/disable sniffer traffic logging.
ztna-traffic         Enable/disable ztna traffic logging.
anomaly              Enable/disable anomaly logging.
voip                 Enable/disable VoIP logging.
dlp-archive          Enable/disable DLP archive logging.

FortiGate (filter) # set severity ?
emergency       Emergency level.
alert           Alert level.
critical        Critical level.
error           Error level.
warning         Warning level.
notification    Notification level.
information     Information level.
debug           Debug level.
```

2. 有些情况下，用户想要自定义本地或syslog日志的类型或级别。

   - **举例1：只需要记录或发送流量日志中包含源地址为192.168.100.77或192.168.100.177，同时，协议为TCP的日志。**
   - **举例2：只需要记录或发送事件日志中级别为alert或information，同时用户为test的日志。**

3. 这种情况下通过简单的log filter是无法实现的。

解决方案

通过配置free-style类型的log filter，允许用户为每个日志记录设备配置个性化的日志类型/级别组合。筛选器可以包括日志类别和特定日志字段，可以创建为包含（include）关系和排除（exclude）关系，该方式需要通过CLI配置，配置方法如下，可配置多个free-style ID，多个free-style ID过滤的日志均会被记录/发送。

```bash
config log disk filter
    config free-style
        edit <id>
            set category <option>
            set filter <string>
            set filter-type {include | exclude}
        next
    end
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

选项	说明
`category <option>`	日志类型： `traffic` , `event` , `virus` , `webfilter` , `attack` , `spam` , `anomaly` , `voip` , `dlp` , `app-ctrl` , `waf` , `dns` , `ssh` , `ssl` , `file-filter` , `icap` , `ztna`
`filter <string>`	过滤关键字，可填写多个关键字，通过“or” 或“and”字符指定多个关键字之间的关系，举例： set filter "((srcip 192.168.100.77) and (dstip 8.8.8.8)) or (srcip 192.168.100.177)"，表示过滤源目IP字段为192.168.100.177和8.8.8.8，或源地址为192.168.100.177的日志。
filter-type {include exclude}	过滤器类型： include表示包含，exclude表示排除

配置举例

我们使用功能需求中的举例1和举例2来进行配置。

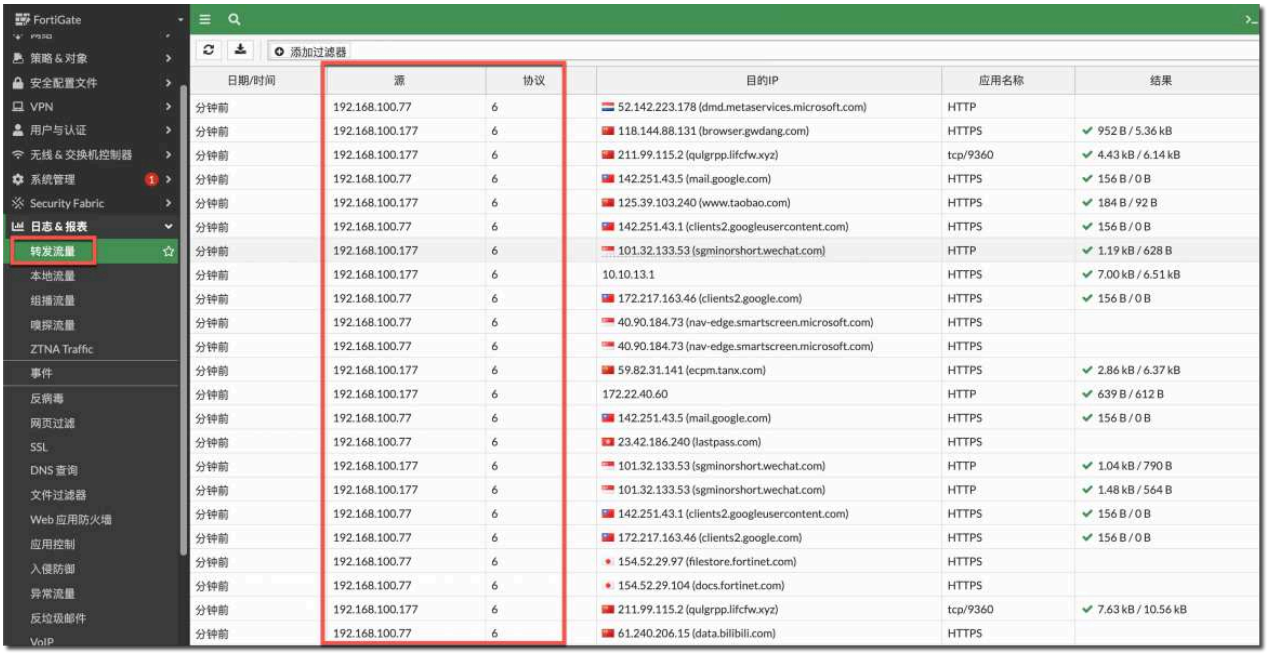
举例1

只需要记录流量日志中包含源地址为192.168.100.77或192.168.100.177，同时，协议为TCP的日志。

1. 在FortiGate的CLI下配置free-style类型的过滤器，需要注意的是，freestyle过滤的日志类型和级别，需要在filter中开启（同理可以配置syslog和FortiAnalyzer日志的过滤器）。

```bash
config log disk filter
    set forward-traffic enable    //首先需要确认流量日志的总开关是开的//
    set set severity information    //freestyle日志记录的流量日志的级别为information，所以filter中的日志级别至少要设置为information//
    config free-style
        edit 1
            set category traffic
            set filter "((srcip 192.168.100.77) or (srcip 192.168.100.177)) and  proto 6"
            set filter-type include
        next
    end
end
```

2. 进入FortiGate的“日志&报表→转发流量”页面，查看相关日志，可以看到只有源地址为192.168.100.77或192.168.100.177，同时，协议为TCP的流量日志被记录。



3. 使用CLI设置该freestyle过滤器，以及过滤器的dump。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # execute log filter free-style  "((srcip 192.168.100.77) or (srcip 192.168.100.177)) and (proto 6)"
FortiGate # execute log display
...

FortiGate # execute log filter dump
category: traffic
device: disk
start-line: 11
view-lines: 10
max-checklines: 0
HA member:
log search mode: on-demand
pre-fetch-pages: 2
Filter: ((srcip 192.168.100.77) or (srcip 192.168.100.177)) and (proto 6)
Oftp search string:  (and  (or proto==6)  (or  (or srcip==192.168.100.177)  (or srcip==192.168.100.77)))
```

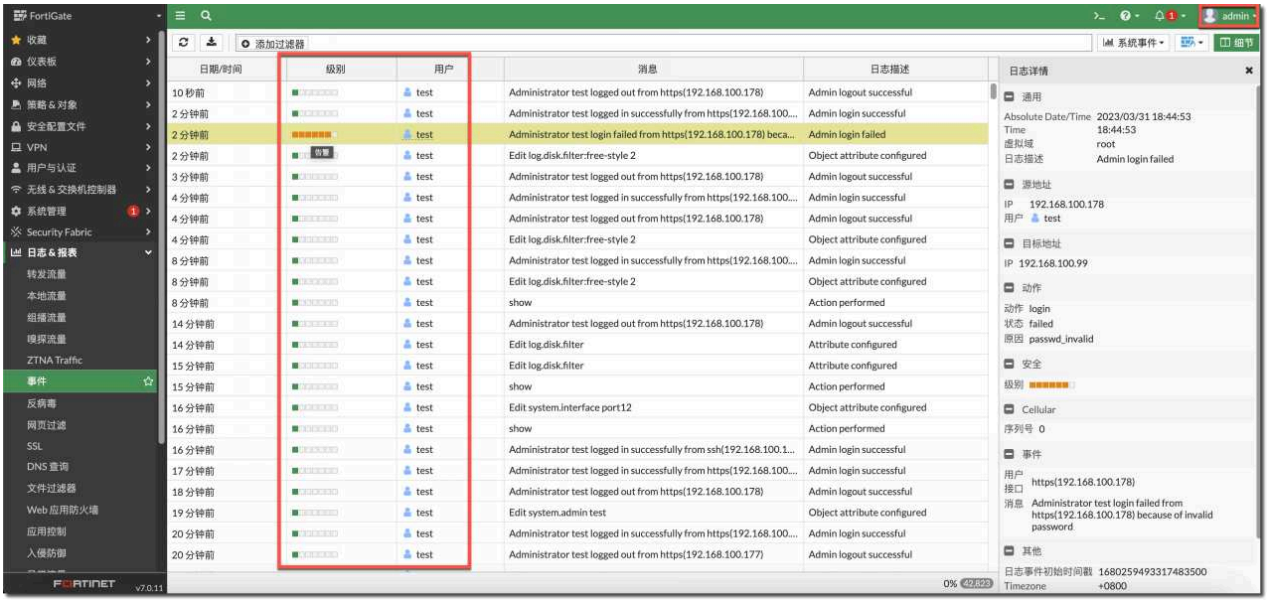
举例2

只需要记录或发送事件日志中级别为alert或information，同时用户为test的日志。

1. 在FortiGate的CLI下配置free-style类型的过滤器，需要注意的是，freestyle过滤的日志类型和级别，需要在filter中开启（同理可以配置syslog和FortiAnalyzer日志的过滤器）。

```bash
config log disk filter
    set set severity information    //freestyle日志记录的事件日志的级别为warning或information，所以filter中的日志级别至少要设置为information//
    config free-style
        edit 1
            set category traffic
            set filter  "((level alert) or (level information)) and (user test)"
            set filter-type include
        next
    end
end
```

2. 使用admin账户登录FortiGate，进入“日志&报表→事件→系统事件”页面，查看相关日志，可以看到事件日志中只有级别为alert或information，同时用户为test的日志。



3. 使用CLI设置该freestyle过滤器，以及过滤器的dump。

```bash
FortiGate # execute log filter free-style "((level alert) or (level information)) and (user test)"
FortiGate # execute log display
...

FortiGate # execute log filter dump
category: traffic
device: disk
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
start-line: 1
view-lines: 10
max-checklines: 0
HA member:
log search mode: on-demand
pre-fetch-pages: 2
Filter: ((level alert) or (level information)) and (user test)
Oftp search string:  (and  (or user=="test" not-exact)  (or  (or level=="information" not-exact)  (or
level=="alert" not-exact)))
```

举例3

Syslog发送的日志中排除本地流量日志、流量日志、应用控制日志和Web过滤日志，剩余其他类型日志正常发送。

在FortiGate的CLI `config log syslogd filter` 下配置关闭 `local-traffic` 发送。配置free-style类型的过滤器（同理可以配置Disk和FortiAnalyzer日志的过滤器）。

> **重要**
>
> `set filter "(logid *)"` 可以表示该分类下的所有日志。

bash
```
config log syslogd filter
    set local-traffic disable
    config free-style
        edit 3
            set category traffic
            set filter "(logid *)"
            set filter-type exclude
        next
        edit 4
            set category app-ctrl
            set filter "(logid *)"
            set filter-type exclude
        next
        edit 5
            set category webfilter
            set filter "(logid *)"
            set filter-type exclude
        next
    end
end
```

注意事项

1. 在6.4版本中freestyle的log filter配置方式与7.0有所不同，6.4版本中自定义filter中多个条件的关系为或（or）。如果6.4版本配置了自定义的log filter后，再升级到7.0版本后，或（or）的关系配置会被转换为与（and）的关系，请在升级后自行手动更改（将and改为or）。

bash
```
6.4版本:
config log disk filter
    set severity information
    set filter "event-level(warning) logid(44547)"    //6.4版本中filter中的多个条件关系为或（or）//
    set filter-type include
end

7.0版本:
config log disk filter
    config free-style
        edit 1
            set category event
            set filter "((level warning error critical alert emergency) and (logid 44547))"    //升级到7.0后，配置被
转换为与（and）的关系//
        next
    end
end
```

2. 多个free-style ID之间为与（and）的关系，多个free-style ID过滤的日志均会被记录/发送。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

CLI审计日志

功能介绍

默认配置下，FortiGate的系统事件日志不会记录在CLI下的相关操作（除了execute命令）。

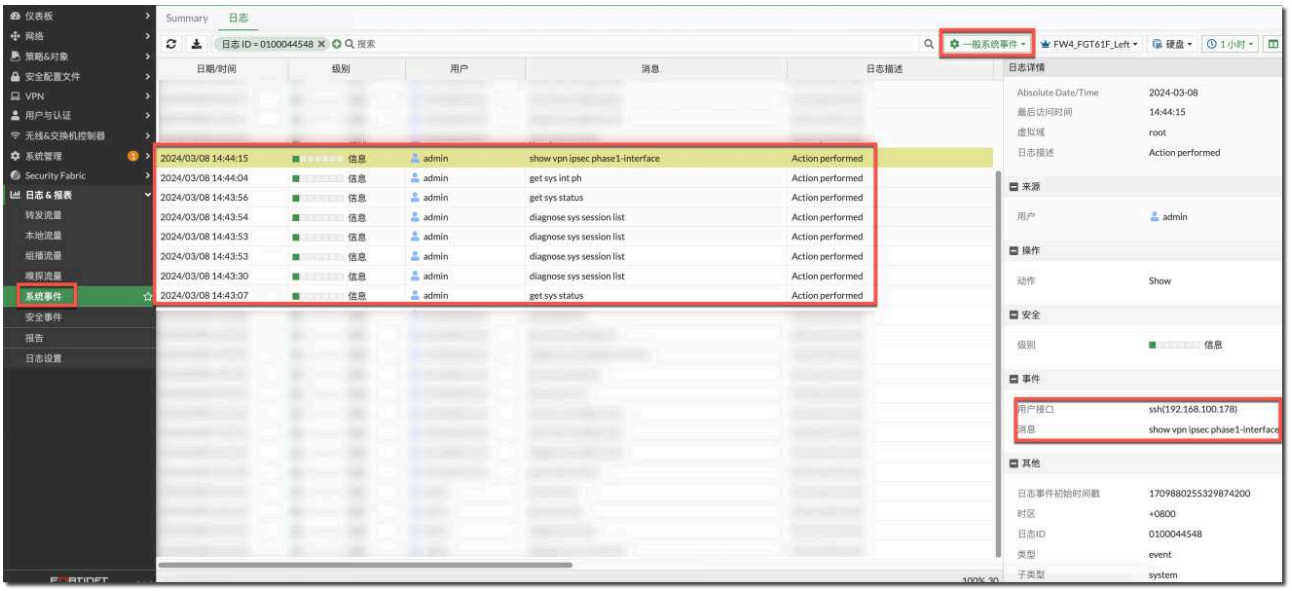
如果想要记录CLI下的相关操作日志，可以通过如下命令开启记录。

```bash
config system global
    set cli-audit-log enable
end
```

开启此功能后，FortiGate会记录在CLI下所有以`show`、`get`、`diagnose`开头执行成功的命令。

日志示例

Log ID为`0100044548`，级别为`Information`，日志类别为“一般系统事件”。




```bash
date=2024-03-08 time=14:44:15 eventtime=1709880255329874080 tz="+0800" logid="0100044548" type="event"
subtype="system" level="information" vd="root" logdesc="Action performed" user="admin" ui="ssh(192.168.100.178)"
action="Show" msg="show vpn ipsec phase1-interface"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

日志显示地区/主机名

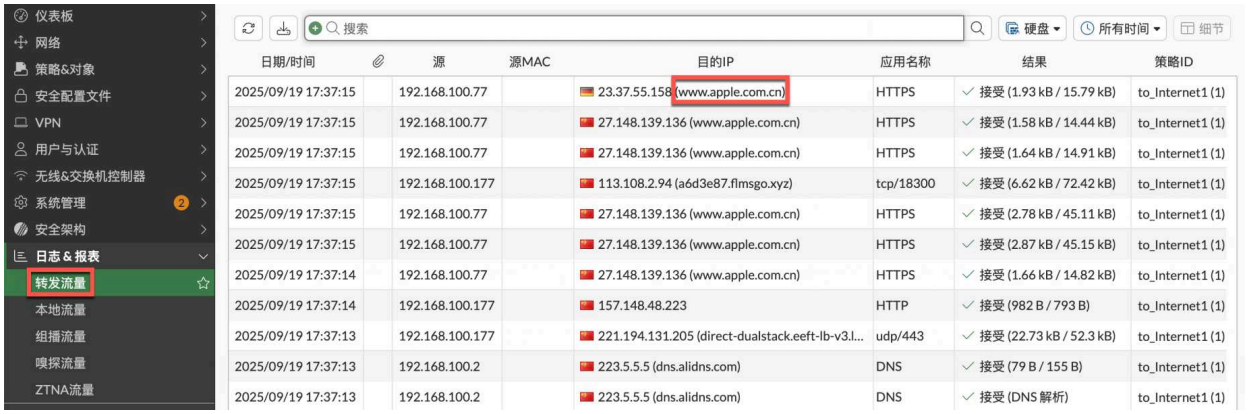
本文介绍了“network-visibility”功能，在流量日志中显示源/目的IP对应的国家/地区、对应国家/地区的图标，以及目标IP对应的主机名，可通过如下CLI开启或关闭。

```bash
config system network-visibility
    set destination-visibility enable
    set source-location enable
    set destination-hostname-visibility enable
    set destination-location enable
end
```

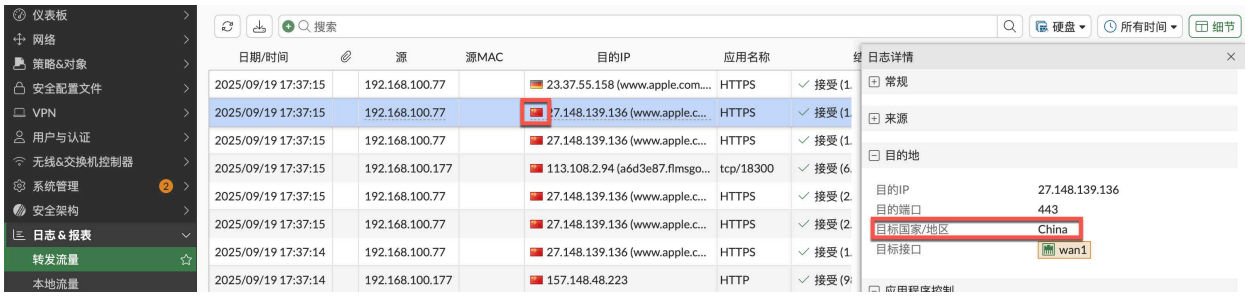
- `destination-visibility`：在转发流量日志中显示目标国家/地区，默认开启。
  - `destination-hostname-visibility`：需要先开启`destination-visibility`。在流量日志中的目标IP中嵌入对应的主机名。主机名将与IP地址一同显示在转发流量日志的“目的IP”字段中。默认开启。

    重要

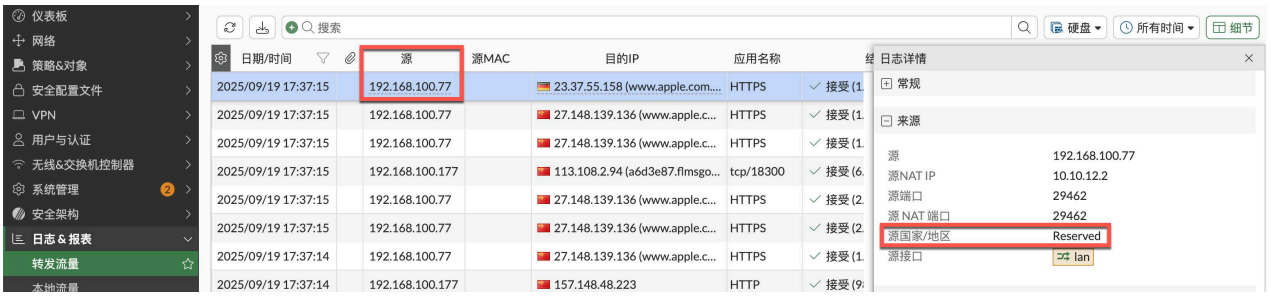
    该功能通过FortiGate进行DNS反查实现，所以需要FortiGate可以正常连接Internet。



  - `destination-location`：需要先开启`destination-visibility`。在转发流量日志中显示目标国家/地区字段及目标国家“标识”。默认开启。



- `source-location`：在转发流量日志中显示“源国家/地区”（对于内部IP源将显示“Reserved”标记）。默认开启。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

硬盘与Flash闪存

本文档主要介绍FortiGate硬盘与Flash闪存相关调试方法。

请参考：FortiGate硬盘与Flash闪存 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

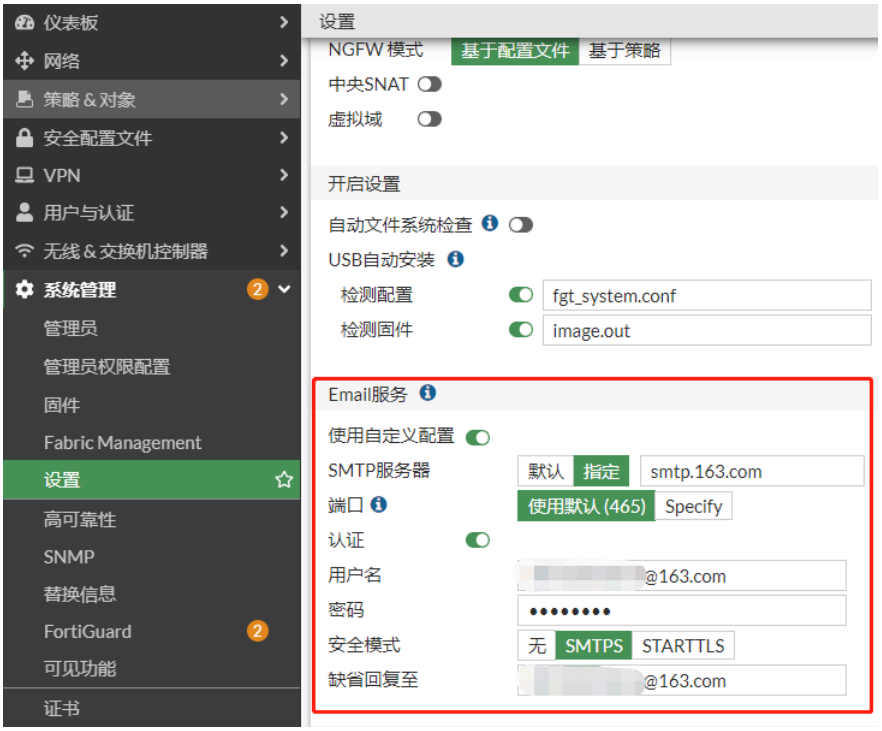
邮件告警

邮件告警用于通知管理员有关FortiGate设备上的事件，从而快速处理问题。

邮件告警配置

1. 配置Email服务

这里使用163邮件发邮件。更多Email服务设置请参考系统管理→系统设置→Email服务↗章节。



2. 配置邮件告警

配置发件人和收件人。

```
config alertemail setting
    set username "186xxxxxxxx@163.com"
    #username和email服务中的用户名一致，即邮箱账号；如果使用ForitGate默认的邮件服务，则username配置为
DoNotReply@notification.fortinet.net
    set mailto1 "test1@qq.com"
end
```

可以配置多个收件人。

```
config alertemail setting
    set mailto2 "test2@qq.com"
    set mailto3 "test3@qq.com"
end
```

3. 配置邮件告警的内容

FortiGate可以基于日志类别发送邮件告警，也可以基于日志安全级别发送邮件告警。

1. 基于日志的类别

```
config alertemail setting
    set username "186xxxxxxxx@163.com"
    set mailto1 "test1@qq.com"
    #过滤模式为 类别
    set filter-mode category


```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
    #根据需求选择需要发送的日志类别，如这里发送IPS和AV日志，set ? 查看支持的类别
    set IPS-logs enable
    set antivirus-logs enable
end
```

2. **基于安全级别**

```
config alertemail setting
    set username "186xxxxxxxx@163.com"
    set mailto1 "test1@qq.com"
    #过滤模式为 安全级别
    set filter-mode threshold
    #critical及以上级别的日志发送日志告警
    set severity critical
end

日志的级别从高到底为：
emergency       Emergency level.
alert           Alert level.
critical        Critical level.
error           Error level.
warning         Warning level.
notification    Notification level.
information     Information level.
debug           Debug level.
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

产品知识

1. **FortiGate系列全新下一代防火墙硬件架构是什么样子的?**

   答：FortiGate采用多核CPU+ASIC芯片的一种处理架构，芯片分为两种、一种是NP芯片、一种是CP芯片，NP芯片是处理网络层以及传输层的一些数据转发、可以达到线速转发。一旦防火墙建立会话之后，在后续的匹配同一个会话的数据包都会有NP芯片直接处理转发。还有一种是CP芯片，CP芯片主要是用于处理应用层内容加速的，比如ips、防病毒、应用过滤等需要应用层检测的都会由CPU送到CP芯片进行加速处理。正式因为有了NP芯片和CP芯片的处理架构，所以FortiGate具有非常高的性能。

2. **哪些型号带交换口？是否可以转换成路由口？如何转换?**

   FortiGate60E、FortiGate100E、FortiGate100F等低端型号设备带交换口，均可以转换为路由口， 转换方式如下（以FortiGate60E举例）:

   > **重要**
   >
   > 执行操作前，确保internal或lan口没有被防火墙策略、dhcp、路由等引用。

   ```
   config system virtual-switch
        edit internal
              config port
                   delete internal1
                   delete internal2
         end
   end
   ```

3. **FortiGate60E、FortiGate100E、FortiGate100F设备面板的小孔是否可以用来恢复出厂**

   答：设备面板的小孔可以用来恢复出厂。防火墙系统正常启动后（可以ping通或登录管理页面）30S内，长按10S左右，系统将自动重启，届时将恢复为出厂设置；

4. **combo光电复用口默认什么优先，如何切换?**

   答：combo口没有光电优先之分，插什么口，什么口都可以用，不需要切换。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

防火墙部署

1. **防火墙支持几种模式**

   答：防火墙支持nat（路由模式）、透明模式两种模式，不支持混合模式。

2. **透明模式和nat(路由模式)有什么区别**

   答：透明模式不支持路由功能、不支持接口模式ipsec vpn、不支持sslvpn、l2tp、pptp、gre功能，仅仅为二层转发。

3. **如何实现混合模式场景需求**

   答：如果需要实现混合模式的场景需求，需要采用VDOM方式来实现，把防火划分成两个虚拟域，一个虚拟域做透明模式，另外一个虚拟域做路由模式。

4. **什么是VDOM（虚拟域）模式**

   答：虚拟域(VDOM)，可以理解为虚拟防火墙，是一种将一个FortiGate设备分为两个或两个以上虚拟设备的技术，它能起到多个独立设备的作用。VDOM可提供单独防火墙策略。在NAT/路由模式下，它可完全分开配置，从而为各连通网络或组织提供路由或VPN服务，同时VDOM之间也可以互访。设备的系统资源可以手动分配给不同的VDOM。一般常用于需要完成独立分割的多个网络，比如云环境；当存在多个区域，即有透明模式又有路由模式的混合环境，由于FortiGate只支持透明模式和NAT/路由模式，所以这种环境必须用VDOM功能来解决。

5. **防火墙是否支持旁路部署模式?**

   答：支持旁路部署模式，接口开启sniffer模式，做数据分析之用，使用场景较少，可以用于ips测试回访攻击包使用**。**

6. **wan口可以单做内网口使用吗?**

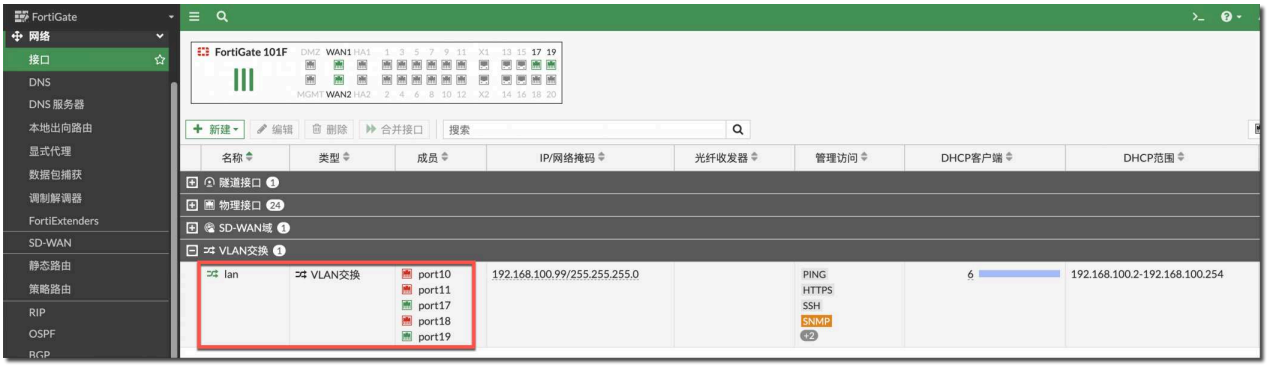
   答：wan口可以做内网口使用，接口的名称只是一个代号，不具有特殊特性。可以按照自己习惯以及现场环境灵活使用。

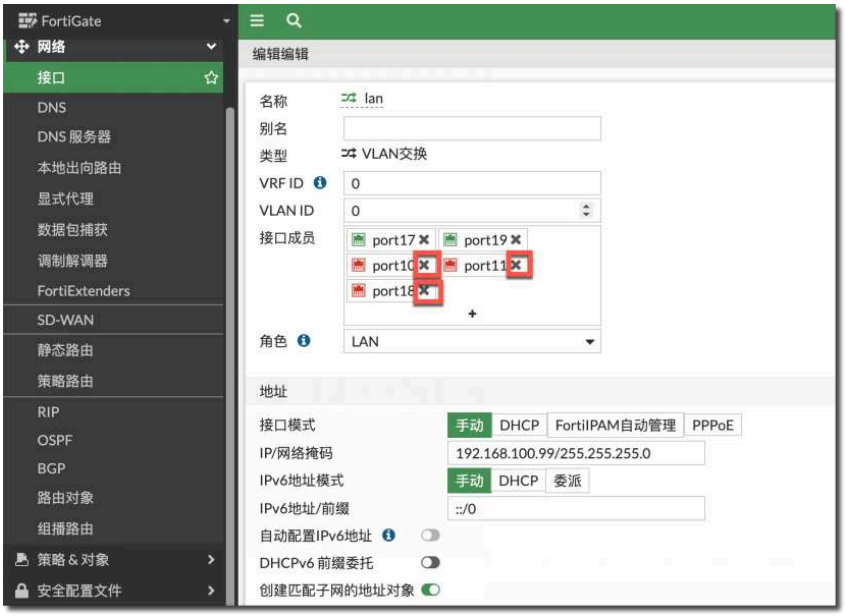
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

功能配置

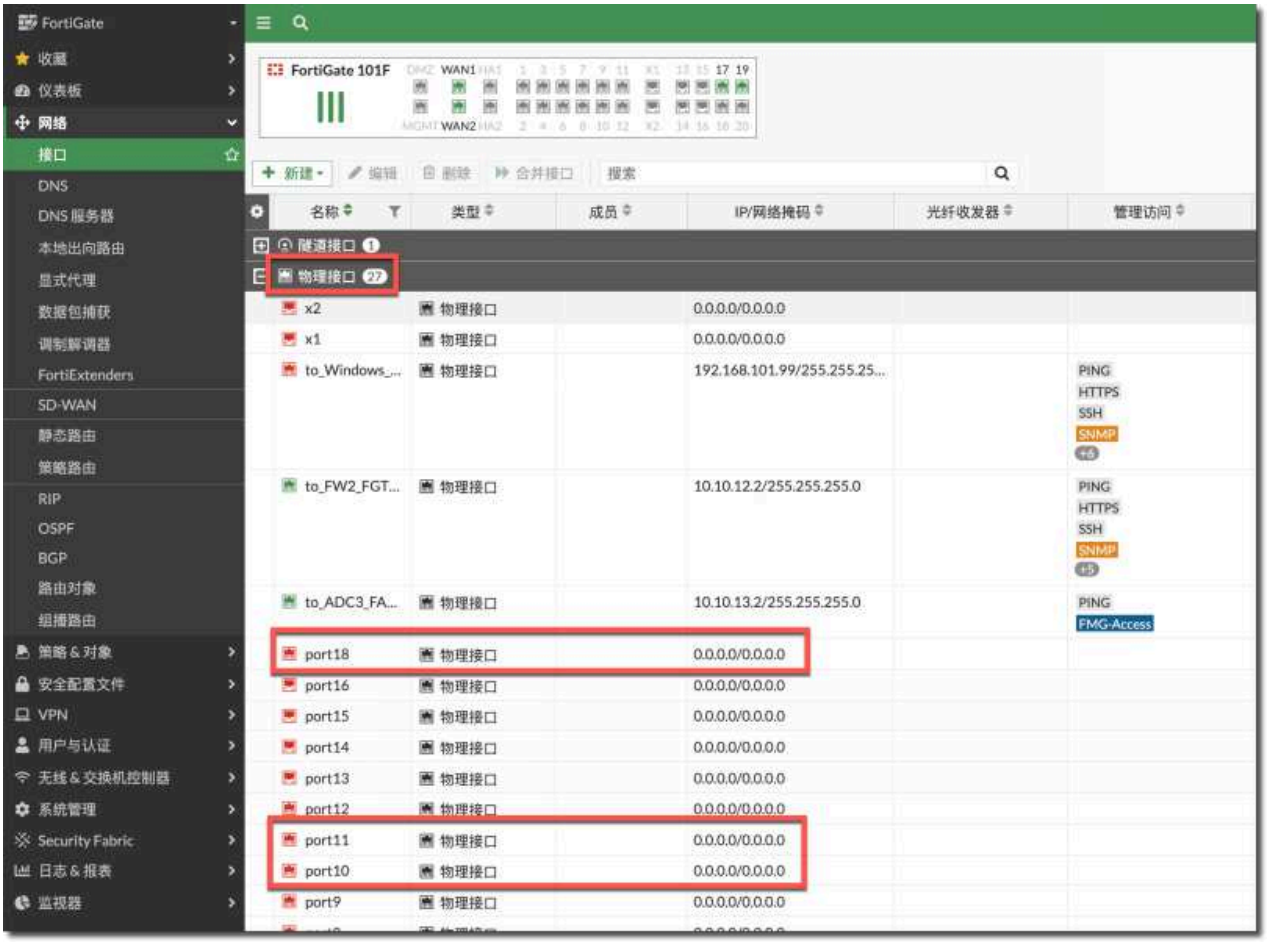
1. **为什么我的防火墙有些接口在“网络→接口”页面无法显示，命令行无法编辑，无法单独配置IP地址。**

   答：部分型号的FortiGate（如FortiGate 101F、60F、80F）内置有一个Hardware Switch（VLAN Switch）接口，默认情况下在配置文件中该接口被命名为lan或internal，这是一个交换接口，默认配置下，与该Hardware Switch（VLAN Switch）内部相连的接口均会被加入该接口（二层接口，类似于交换机的Access接口）。如果想单独配置某个Hardware Switch（VLAN Switch）的成员接口，需要将该接口从Hardware Switch（VLAN Switch）接口中移除，移除后，成员接口会变为独立的三层接口，可以独立配置IP等信息。





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. **如何实现源NAT，防火墙策略中启用NAT、ip地址池、和中央NAT分别是什么意思?**

答：源NAT：即源地址转换，源NAT在防火墙策略中实现，通过开启NAT、引用ip地址池、和引用中央NAT来实现源地址转换。

策略中启用NAT：代表源地址转换为此策略出接口的ip地址。

ip地址池：如果选择了ip地址池，代表源地址转换为ip地址池中的ip地址，或者也可以直接定义源地址对应关系，不受策略限制。

中央NAT：中央NAT是一个单独的地址转换表，防火墙策略选择了中央NAT后，会根据策略的源地址去到中央NAT查找匹配相应的转换关系。

3. **什么是虚拟ip?**

答：虚拟ip即vip，虚拟ip是用来做目的地址转换使用，实现目的映射的对应关系的策略，需要引用到防火墙策略中才能生效，需要注意，虚拟ip的映射关系会影响到源地址转换，也就是，防火墙会优先匹配虚拟ip的映射关系，再匹配防火墙策略中选择的源地址转换方式。

4. **如何实现目的NAT?**

答：目的NAT即目的转换，目的转换在防火墙策略中实现，通过事先新建一个vip，然后在防火墙策略中的目的选择vip即可实现目的地址映射。

5. **如何实现双向NAT?**

答：如果要实现双向地址转换，在防火墙策略的目的选择相应的vip，然后在策略中启用NAT或者引用ip地址池，或者直接使用中央NAT。

6. **接口和区的有什么关系**

答：区域可以包含多个接口，可以理解为接口组，接口一旦划入到区中，就不能单独做策略，在防火墙策略中只能找到相应的区，而无法选择所划入区的接口了，所以区通常较少使用。

7. **内网用户需要通过公网映射地址访问内部服务器，需要什么特殊配置?**

答：请参考策略与对象→虚拟IP映射→内网主机通过公网IP访问VIP ↗章节。

8. **HA主备模式系统升级是否会中断业务，如何操作?**

答：主备防火墙升级系统不会中断，只要按照正常的方式升级即可，通过管理主墙，上传版本文件后，主墙把版本文件同步给备墙，备墙先升级，备墙升级完后，主墙开始升级，升级过程中会切换到备墙工作，整个过程透明，无需其他额外操作，通单台升级操作一样。

9. **sslvpn支持几种模式？是否支持sslvpn的site-to-site模式?**

答： a. 支持代理模式：代理模式只支持B/S架构的http、https应用代理

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

b. 支持客户端模式：即隧道模式，无应用限制。

c. 不支持插件方式

d. 不支持site-to-site模式

10. 移动终端vpn支持情况?

答：IPSEC vpn支持ios和android，ios和android均采用系统自带的客户端

SSLVPN支持支持ios和android，FortiExplore VPN支持ios，FortiClient支持Android。

11. 防火墙支持stp功能吗?

答：低端型号如FortiGate 60E，FortiGate 100E，FortiGate 100F的硬交换接口支持。

12. 防火墙是否支持 802.1x ?

答：低端型号如FortiGate 60E，FortiGate 100E，FortiGate 100F的硬交换接口支持。

13. 防火墙支持链路聚合 802.3ad 功能吗?

答：支持

14. 防火墙聚合口成员可以从聚合口中分离吗？需要注意什么?

可以从聚合口中取出，但需要注意：成员接口从聚合口中取出后，务必重启一次防火墙，否则可能会出现网络通信问题，此为硬件限制，目前无解。所以建议在部署前就规划好聚合口的成员，避免后期频繁修改聚合口成员配置。

15. 转换或接口提示被占用，如何查找接口被哪些模块被调用

关联项就是接口被引用的次数，如点击"7"可以查看具体被哪些模块引用。



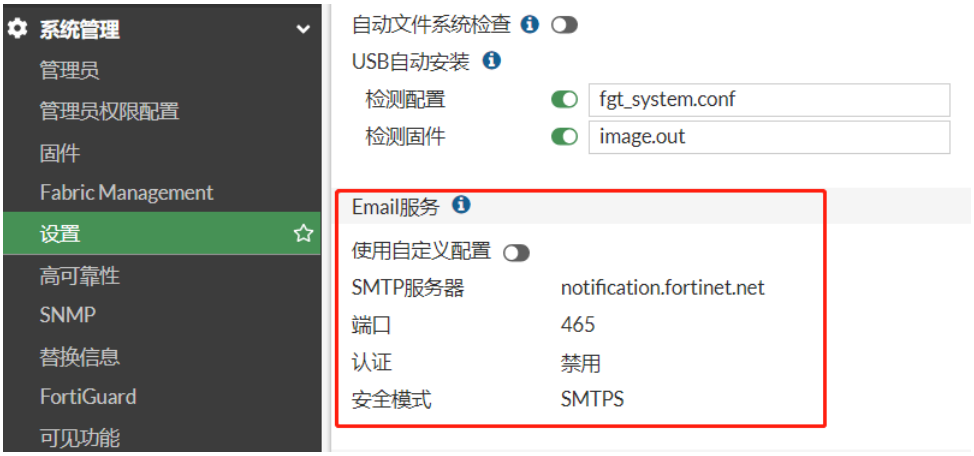


16. 防火墙通过默认的notification.fortinet.net:465邮件服务器，邮件方式发送FortiToken（双因子认证）、告警或日志到特定邮箱时，为什么收件邮箱经常收不到，或被识别为了垃圾邮件?

答：出现该情况时，请在系统→设置→Email Service中配置“缺省回复至”，定义username，域名保证为notification.fortinet.net ↗，就不会被其他email server认为是垃圾邮件。

在FortiGate版本7.0.11，7.2.4及后续的版本中，默认的notification.fortinet.net:465邮件服务器 将取消 “缺省回复至” 选项，将该选项强制为DoNotReply@notification.fortinet.net

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



7. **配置了FQDN形式的地址对象并使用静态/策略路由引用，但实际效果不稳定，客户端访问配置的FQDN时，仍然从其他线路出去了。**

   答：FQDN地址对象中获取的IP地址有两种方式：1、设备使用自身配置的DNS解析到的结果；2、穿过防火墙的DNS流量被设备记录。（具体原理可以参考附件：https://handbook.fortinet.com.cn/files/fqdn.pdf ↗ ）

   在FQDN地址对象的CLI配置下：

   1）如果配置的cache-ttl>DNS服务器返回的TTL，认为该FQDN下面配置的cache-ttl时间优先。

   2）如果cache-ttl < DNS服务器返回的TTL，则DNS服务器返回的TTL优先。

   3）如果没有没配置cache-ttl（默认为0），以DNS服务器返回的TTL为准。

   当TTL变为0时，防火墙会删除该FQDN下的相关地址记录。

   解决办法：在CLI下，编辑FQDN形式的地址对象，将cache-ttl修改为86400。

```
config firewall address
  edit "www.baidu.com"
    set type fqdn
    set allow-routing enable
    set fqdn "www.baidu.com"
    set cache-ttl 86400
  next
end
```

8. **Flow模式和Proxy模式的区别。**

   答：

   Flow模式：

   当防火墙策略的检测方式设置为Flow时，经过该策略的流量不会被FortiGate进行缓冲。与代理模式不同的是，通过策略的内容负载将被逐包检查，最后一个包由FortiGate保存，直到扫描返回结果。如果检测到异常流量，则向接收端发送一个重置包，终止连接，并阻止有效负载成功发送。

   基于Flow检测能够实时识别和阻断安全威胁。所有适用的基于流的安全模块在一次通过中同时应用，使用DFA（Direct Filter Approach）模式匹配来识别可能的攻击或威胁。模式匹配由CP8或CP9处理器卸载和加速。

   基于流程的检查通常比基于代理的检查需要更少的处理资源，并且不改变报文，除非发现威胁并阻断报文。

   Proxy模式：

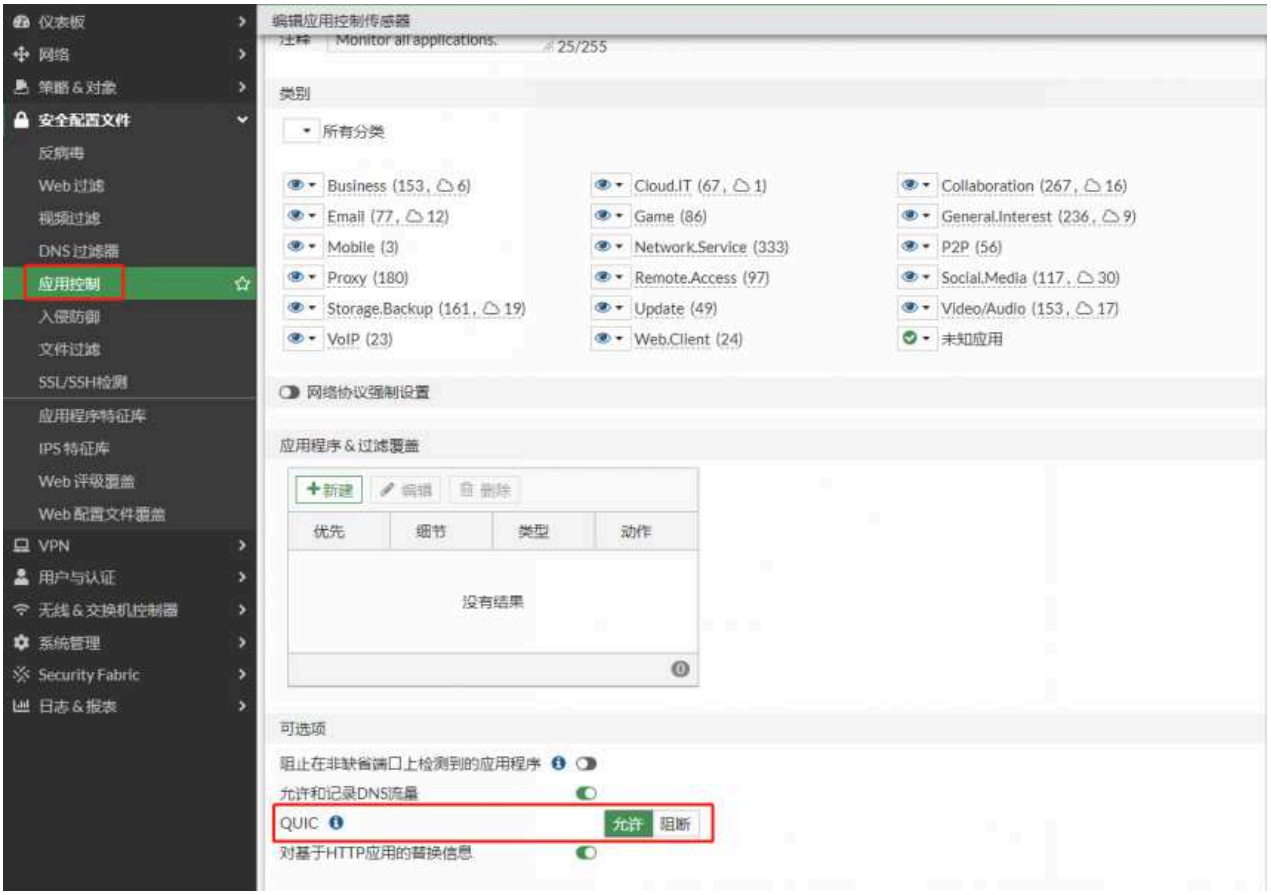
   当防火墙策略的检测方式设置为Proxy时，通过该策略的流量会被FortiGate进行缓冲检测。这意味着FortiGate将保存文件、电子邮件消息或网页的信息包，直到整个有效负载被检查是否违反(病毒、垃圾邮件或恶意web链接)。在FortiOS完成检查之后，如果流量是干净的，负载要么被发送到目的地，如果流量有异常，则被丢弃并用替换消息替换。

   代理模式提供了最彻底的流量检查，但是它的彻底的牺牲了性能，使得它的吞吐量比流模式策略慢。

9. **在策略中调用“应用控制”的安全配置文件后，发现微信发图片很慢，或一些手机App无法正常访问。**

   答：微信、支付宝等一些手机App在使用时会用到QUIC协议。默认情况下，应用控制安全配置文件不允许QUIC业务通过，此时微信在发图片时，首先会考虑使用QUIC协议，当QUIC协议被防火墙阻断后，微信再使用HTTPS协议进行发送，导致出现发图片慢的情况。通过在安全配置文件→应用控制中，将QUIC的动作配置为允许，可以解决此问题。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



0. **License无法验证，或特征库无法更新。**

答：FortiGate与FortiGuard服务器通信问题造成。FortiGate默认使用anycast方式连接FortiGuard，在国内使用时这种方式可能会出现网络通讯故障，建议FortiGate使用如下CLI命令关闭anycast方式连接FortiGuard，使用单播方式连接FortiGuard。

```bash
config system fortiguard
    set fortiguard-anycast disable
    set protocol udp
    set port 8888
end

exe update-now
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

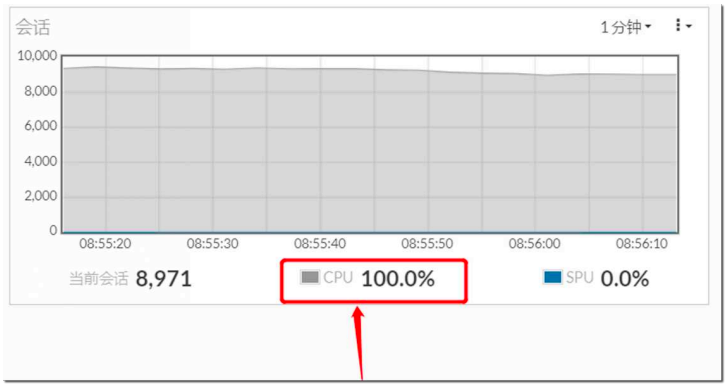
流量无法被NP加速

问题现象

1. 拓扑信息：

   LAN network----LAG (PG_SNAT_LAN, "port9" "port10") [**FortiGate**] WAN (port5/port6)----Internet

2. 在FortiGate 200E/201E、2000E、2500E设备上，出现大部分或所有会话均由CPU处理，没有被硬件加速。



3. 以FortiGate 201E为例，查看会话，可以看到大部分会话中的接口信息是从内网聚合口PG_SNAT_LAN（成员为port9和port10）与port5/port6之间的流量。

```bash
diagnose sys session list | grep dev=
dev=43→24/24→43
dev=43→23/23→43
dev=23→34/34→23
...

diagnose ip address list
...
IP=10.179.1.62→10.179.1.62/255.255.255.252 index=43 devname=PG_SNAT_LAN
IP=123.157.210.114→123.157.210.114/255.255.255.248 index=23 devname=port5
IP=39.174.163.216→39.174.163.216/255.255.255.128 index=24 devname=port6
...
```

4. 会话信息显示无法加速的原因为`non-npu-intf`。

```bash
session info: proto=6 proto_state=01 duration=4505 expire=3587 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=40MB
class_id=0 shaping_policy_id=2 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty per_ip
statistic(bytes/packets/allow_err): org=442701/2567/1 reply=624811/3382/1 tuples=2
tx speed(Bps/kbps): 155/1 rx speed(Bps/kbps): 188/1
orgin→sink: org pre→post, reply pre→post dev=43→24/24→43 gwy=39.174.163.254/10.179.1.61
hook=post dir=org act=snat 10.179.16.15:61926→120.232.31.208:8080(39.174.163.216:61926)
hook=pre dir=reply act=dnat 120.232.31.208:8080→39.174.163.216:61926(10.179.16.15:61926)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=54:c6:ff:a0:18:c1
misc=0 policy_id=3 pol_uuid_idx=1050 auth_info=0 chk_client_info=0 vd=1
serial=424a822d tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=80000000 ngfwid=n/a
npu_state=0x040000
//no_ofld_reason:  non-npu-intf//
```

5. 关于`non-npu-intf`或其他无法被NP加速的原因，可以参考Fortinet官方文档↗。其中提到`non-npu-intf`的可能原因：

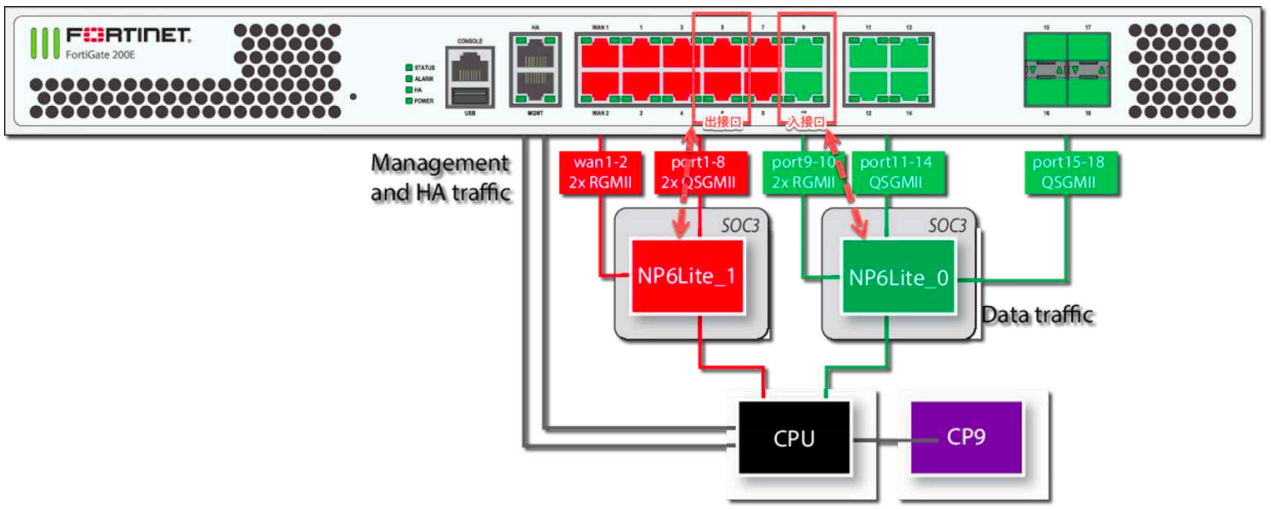
   - 会话的入接口或出接口不是NP加速接口。
   - 会话的入接口或出接口是软交换（Software Switch）接口的成员。（此例中不符合）
   - 禁用了config system npu下的fastpath。（此例中不符合）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

问题原因

1. 在此例中，流量从port9/port10进入，从port5/port6流出，不满足201E的硬件加速条件，因为port9/port10与port5/port6属于不同的NP芯片，且接口间的硬件结构没有内置交换模块，所以是无法被NP加速的。

2. 参考FortiGate 201E的硬件加速架构 ↗：



   - 只有当流量在连接到同一个NP6Lite的接口上转发时，才能被NP加速。
   - NP6Lite连接的接口如下：
     - NP6Lite_0连接到6个1GE RJ-45接口（port9 ~ 14）和4个1GE SFP接口（port15 ~ port18）。
     - NP6Lite_1连接到10个1GE RJ45 接口（wan1、wan2、port1 ~ port8）。

解决方法

- 选择流量的入接口为port9 ~ port18，出接口为port9 ~ port18。
- 或选择流量的入接口为wan1/wan2、port1 ~ port8，出接口为wan1/wan2、port1 ~ port8。
- 参考：点击链接查看FortiGate 2000E ↗与2500E ↗的硬件加速架构。

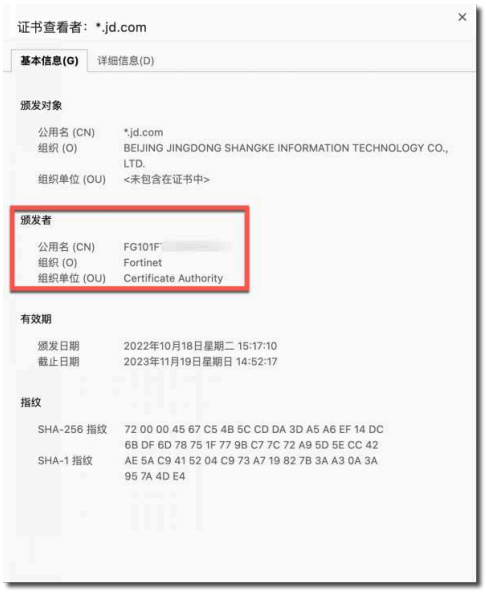
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

阻断/认证页面无法点击继续

问题描述

1. 当用户访问的网页被WebFilter功能阻断（或开启了防火墙用户认证）时，会在浏览器中弹出WebFilter阻断（或用户登录）页面，由于默认情况下FortiGate阻断页面使用的是FortiGate的自带证书（未被客户端信任的CA颁发的证书），会导致浏览器提示网页不安全（以Chrome为例）。

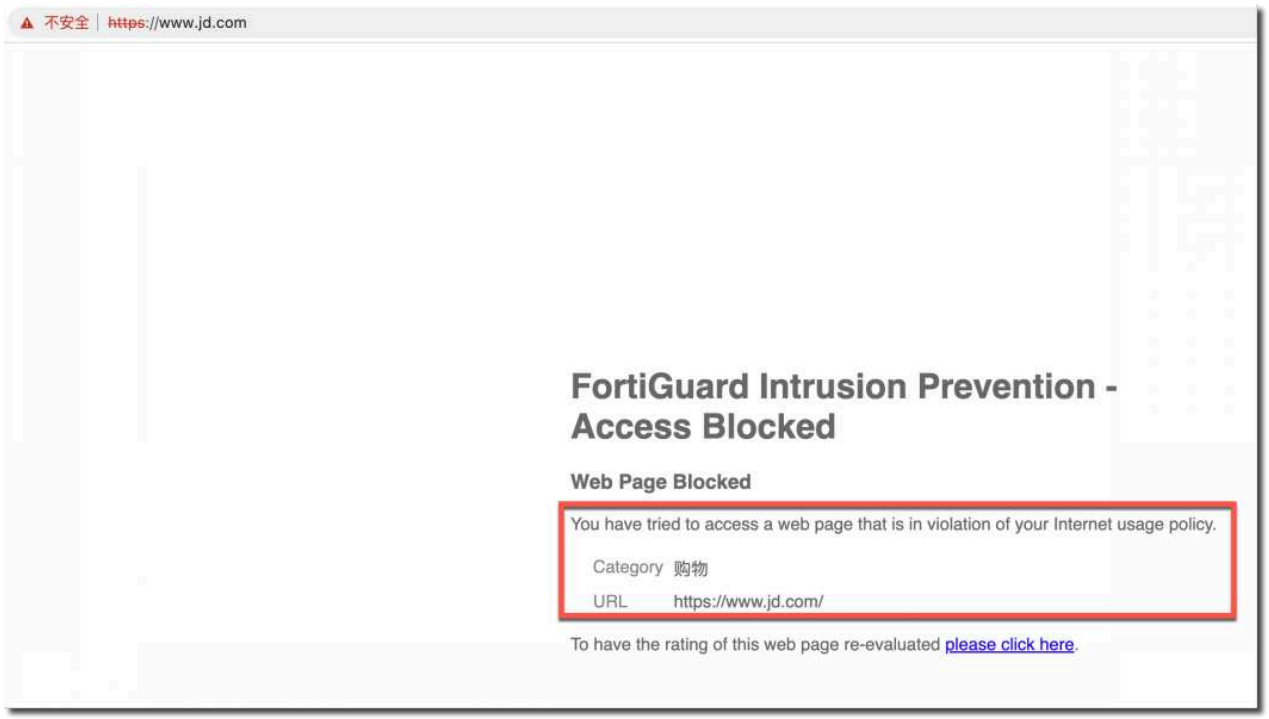




2. 该提示信息有时可以跳过，从而显示出FortiGate的阻断（或用户登录）页面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





3. 但有时会出现没有点击继续的按钮，导致无法继续显示UTM阻断页面（或用户登录页面），即使使用键入“thisisunsafe”的方法也无法继续。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



问题原因

这是由于访问的网站开启了HSTS功能。

HSTS介绍

HTTP严格传输安全（HTTP Strict Transport Security）是一套由互联网工程任务组发布的互联网安全策略机制。网站可以选择使用HSTS策略，来让浏览器强制使用HTTPS与网站进行通信，以减少会话劫持风险。

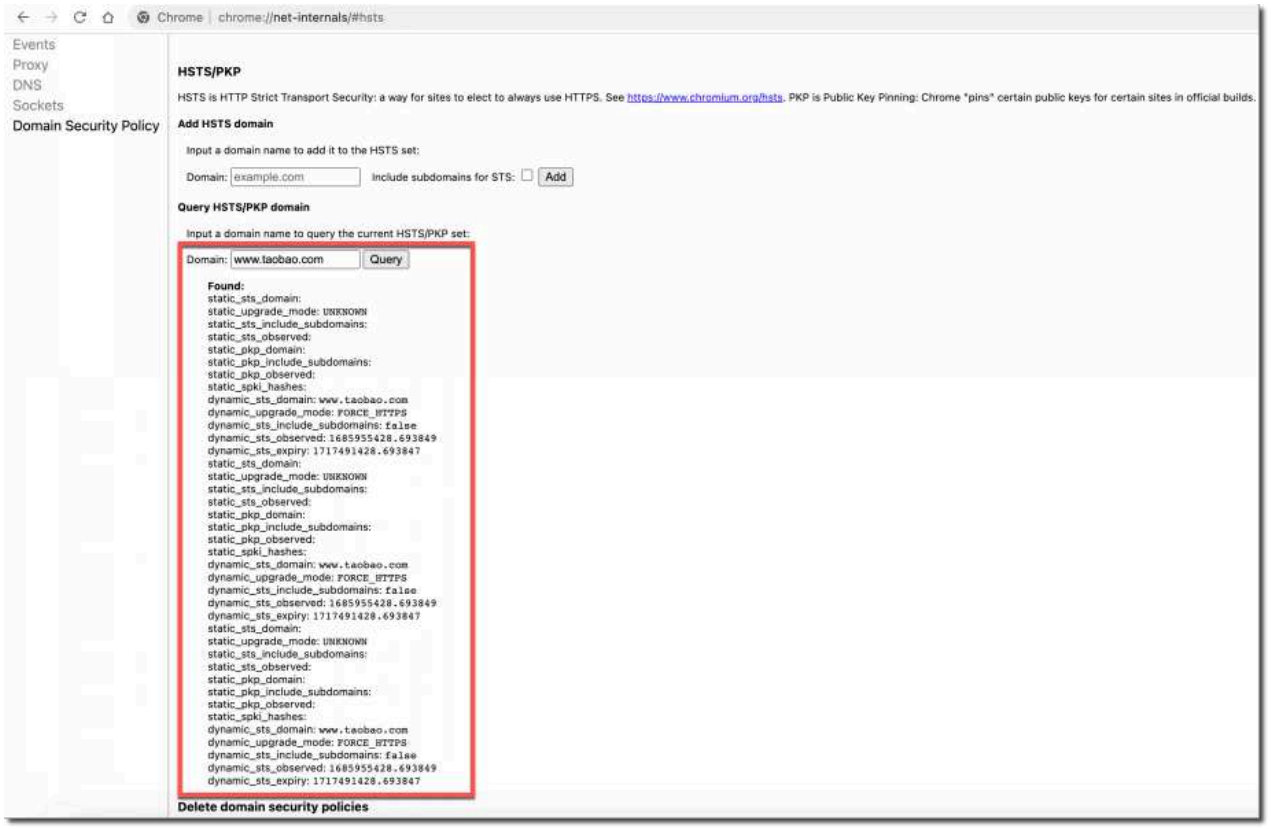
用户首次访问某网站是不受HSTS保护的。这是因为首次访问时，浏览器还未收到网站的HSTS，所以仍有可能通过明文HTTP来访问。

另外，如果中间人使用自己的自签名证书来替换网站证书，浏览器会给出警告（FortiGate的UTM阻断页面或登录页面就是此种情况），但是许多用户会忽略警告。HSTS为了解决了这一问题，一旦服务器发送了HSTS字段（HSTS信息被储存在浏览器中），在HSTS老化时间到期前，将不再允许用户忽略警告。这就导致了浏览器除了第1次访问开启HSTS的网站可以点击继续按钮显示出阻断页面（或登录页面），后续再访问此网站时，没有继续按钮显示。

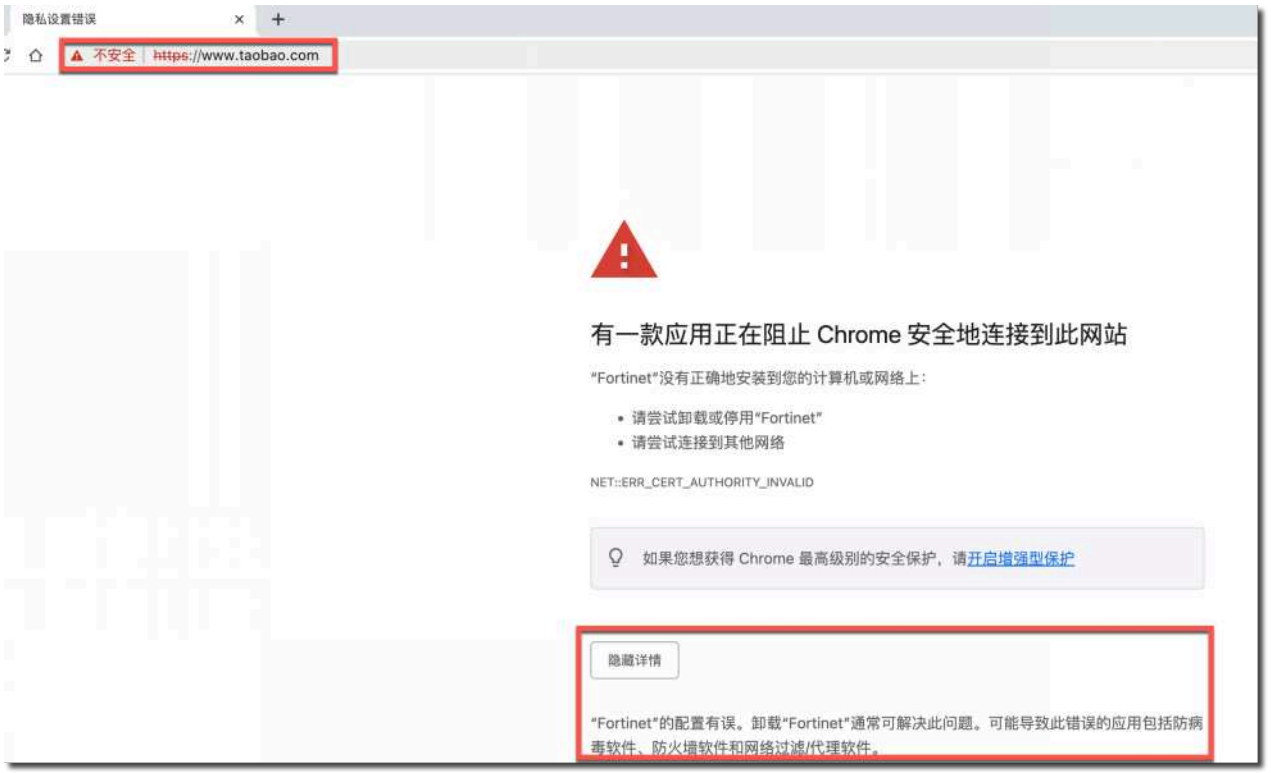
浏览器中的HSTS信息查询

1. 我们可以在Chrome里的chrome://net-internals/#hsts（Edge为edge://net-internals/#hsts）页面下查询网站的HSTS信息是否被储存在了浏览器中，如下举例，www.taobao.com 网站开启了HSTS，并在某次成功访问的时候被加入了Chrome的HSTS列表，目前还未过期。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



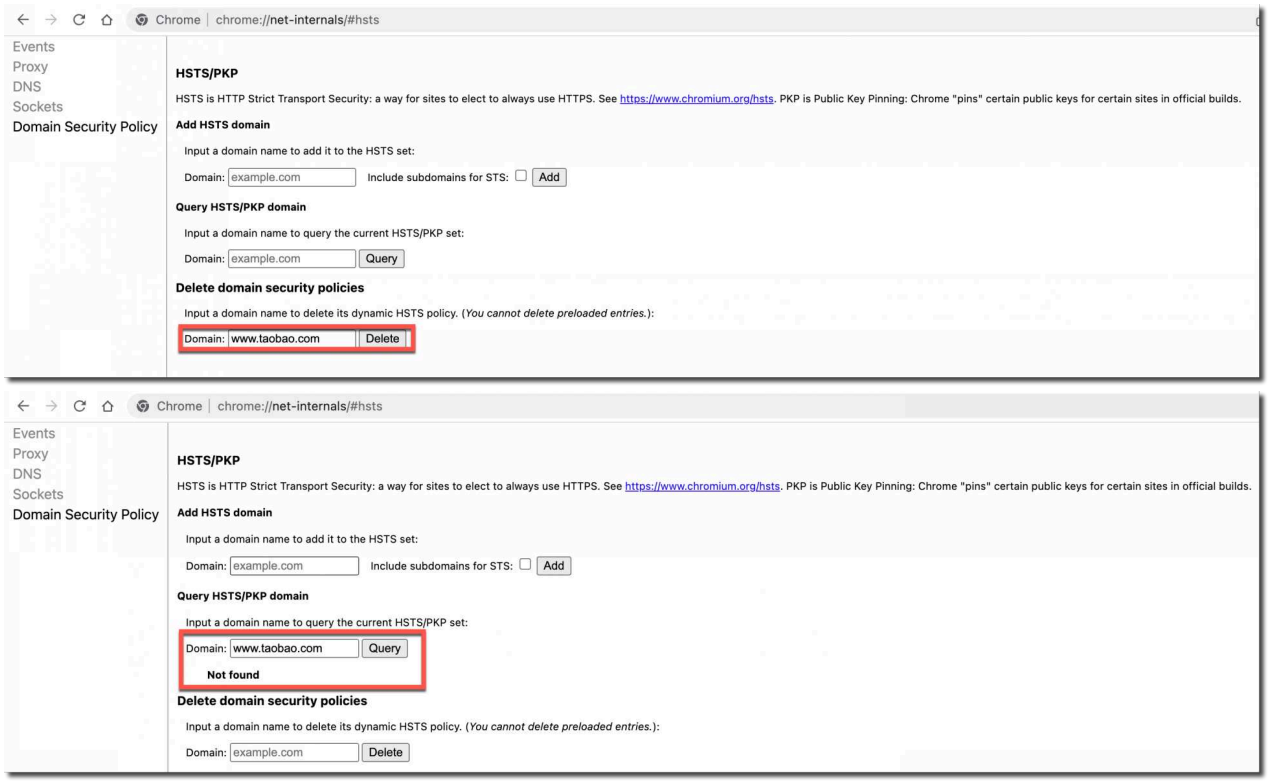
2. FortiGate开启WebFilter并阻断该网站后，客户端访问该网站时会出现警告页面无法点击继续按钮的情况。



删除浏览器中的HSTS信息

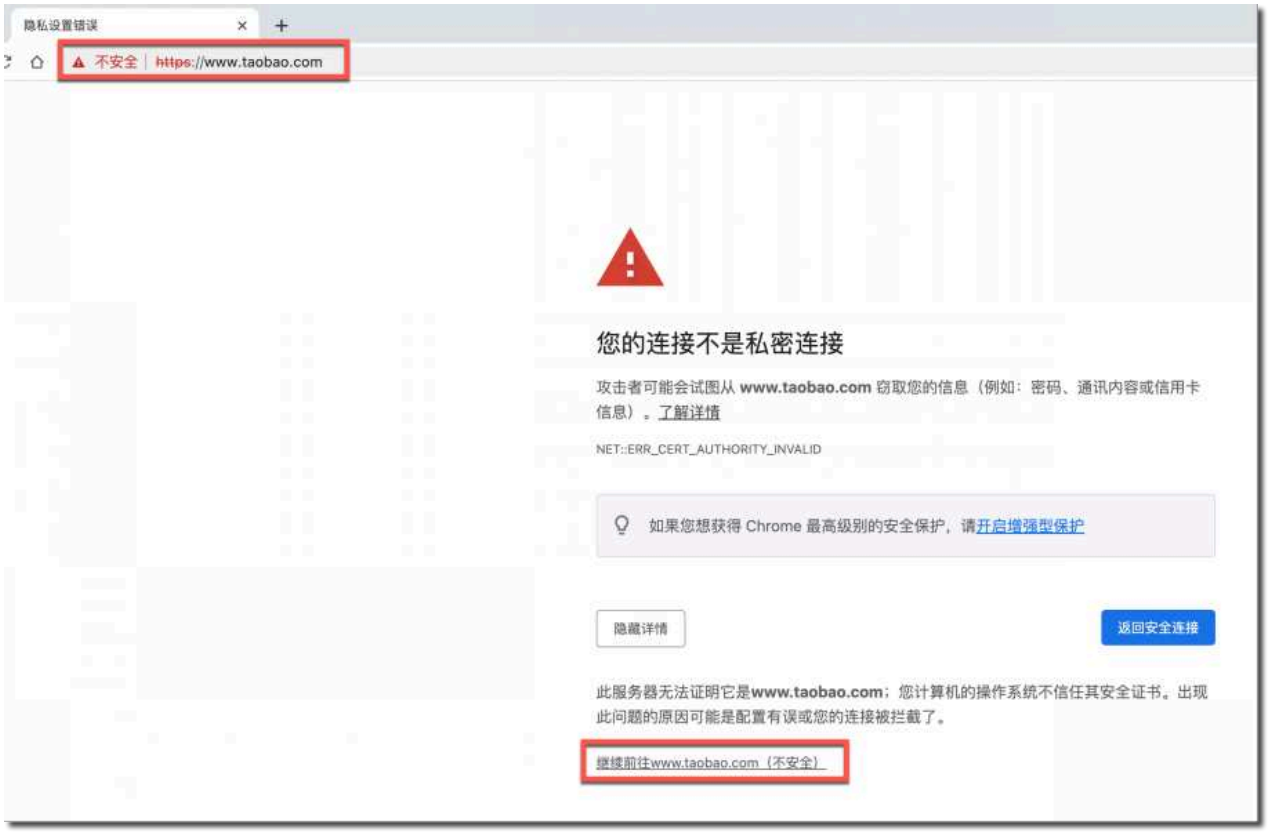
1. 在Chrome里的chrome://net-internals/#hsts（Edge为edge://net-internals/#hsts）页面下删除网站的HSTS信息，删除后，无法再查询到该网站的HSTS信息。

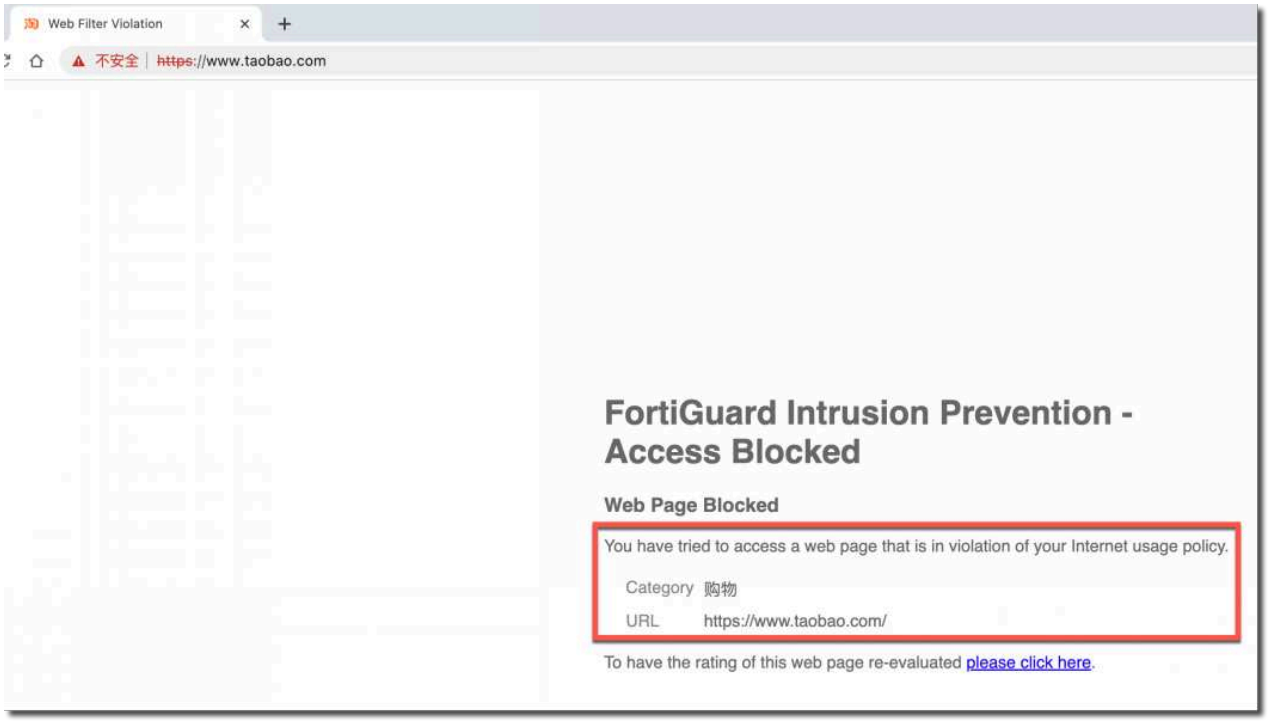
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



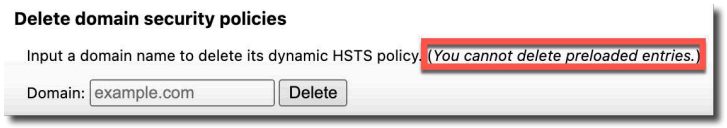
2. 客户端再次访问该网站时，警告页面可以点击继续按钮，并显示出FortiGate的阻断页面。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





3. 请注意，有一些知名网站的HSTS信息被预置在了浏览器中，如www.google.com ↗ 、www.gmail.com ↗ 、www.facebook.com ↗ 等，这些HSTS信息是无法被删除的。

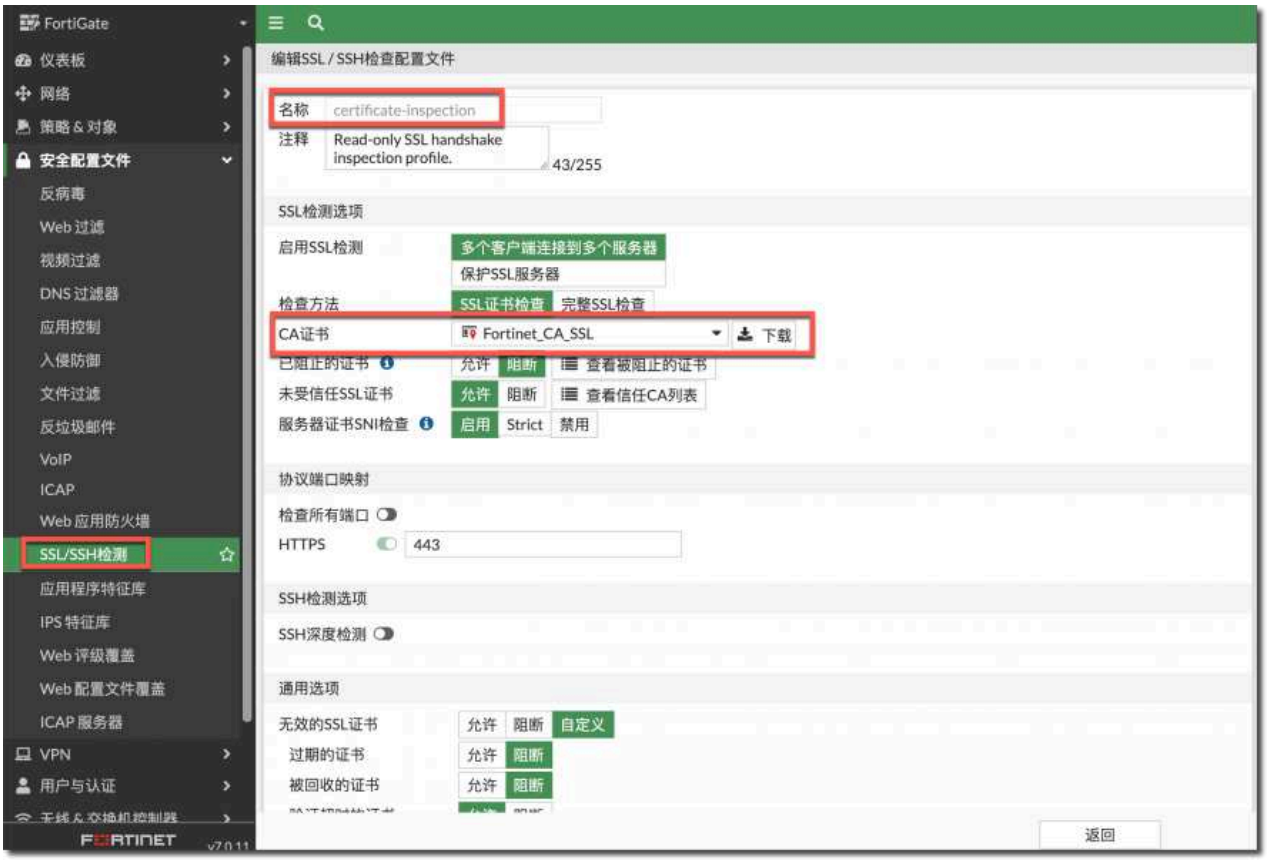


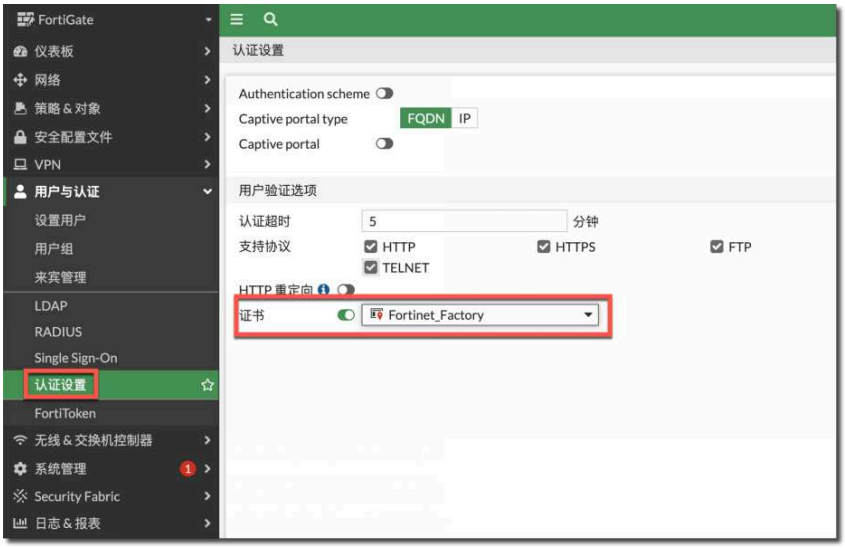
4. Firefox需要通过删除对应网站的缓存信息来删除HSTS信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

解决方法

1. 下载FortiGate用于UTM阻断页面（或用户认证页面，用户认证的证书需要到“系统管理→证书”页面下载）使用的CA证书，如下图所示，WebFilter功能所属的安全策略使用的SSL检查配置文件为默认的“certificate-inspection”，编辑该SSL检查配置文件后，下载CA证书。



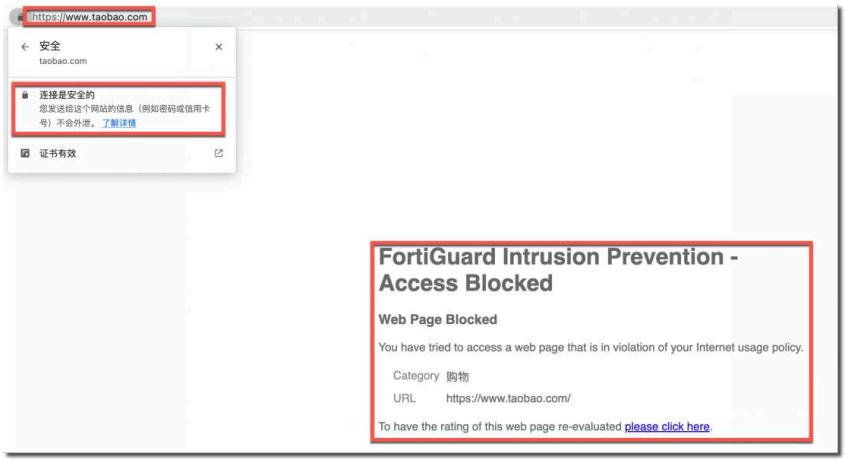


2. 将FortiGate使用的CA证书加入设备或者浏览器的信任列表（Chrome/Edge依赖系统的证书信任列表，而Firefox有自己的信任列表，需要在浏览器设置中添加）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 客户端再次访问该网站时，会直接显示出FortiGate的阻断页面（或登录页面），不会弹出证书告警页面。



4. 因为浏览器在访问网站时，检查HSTS的时候会优先查找自己本地证书的信任关系（Firefox有自己的信任列表，需要在浏览器设置中添加），只要证书被设备或者浏览器本身信任，那么就不会被阻止，同样的事情，就算网站没有开启HSTS，因为对FortiGate证书信任了后，也不会弹出对应的证书错误提示页面，从而直接访问到UTM阻断页面（或用户登录页面）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate Cloud无法登录

问题描述

1. 某用户环境使用SD-WAN部署，SD-WAN成员中包含IPSec隧道（无法访问Internet）和ISP线路（可以访问Internet），本机默认路由指向SD-WAN接口（默认路由在IPSec接口和ISP线路上负载），FortiGuard配置中指定FortiGuard流量的出接口为wan1。

```bash
Spoke1 # get router info routing-table all

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 172.22.6.1, wan2, [1/0]
                  [10/0] via 172.22.6.1, wan1, [1/0]
```

```bash
config system fortiguard
    set interface-select-method specify
    set interface "wan1"
end
```

2. FortiGuard更新正常，但登录FortiGate Cloud时提示错误，无法登录。





问题原因

FortiGate Cloud登录、记录日志流量的源IP、线路选择方式在config log fortiguard setting下配置，而不是在“config system fortiguard”下。默认配置如下，接口选择方式为自动，参考路由表决定出接口和源IP，可能选择IPSec接口发送，导致FortiGate Cloud无法登录或发送日志到FortiCloud。

```bash
config log fortiguard setting
    set status enable
    set source-ip 0.0.0.0
    set interface-select-method auto
end
```

解决方法

在config log fortiguard setting下指定FortiCloud流量的接口为ISP线路接口。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config log fortiguard setting
    set interface-select-method specify
    set interface "wan1"
end
```

结果验证

FortiGate Cloud可以正常登录，且可以正常发送日志到FortiCloud。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

获取接口对应的公网IP

1. 当FortiGate的WAN接口（配置私网IP）位于Internet设备（针对FortiGate的WAN接口做SNAT）后时，可以通过如下CLI命令获取WAN接口对应的公网IP。

> **重要**
>
> 该CLI命令需要FortiGate可以正常解析并访问 `https://api.ipify.org` 。

```
diagnose sys waninfo ipify
```

2. 如下所示：

```bash
FortiGate # diagnose sys waninfo ipify
Try to get my public IP through https://api.ipify.org with src_ip=0.0.0.0 device=unspecified vfid=0(root) ...

Public/WAN IP: 60.247.121.226
Location:
        Latitude: 39.904202
        Longitude: 116.407402
        Accuracy radius: Unknown
        Time zone: Asia/Shanghai
City: Beijing
Subdivisions:
        0: Beijing
Country: China
Postal: Unknown
        Code: Unknown
Continent: Asia
Registered country: Unknown
ISP: Unknown
```

3. 如果存在多个WAN接口连接，需要获取特定WAN接口对应的公网IP，请使用如下CLI命令，指定要获取对应公网IP的接口，或使用接口私网IP作为源IP去获取对应的公网IP。

```bash
diagnose sys waninfo ipify <interface_name> | <source_IP_address>
```

4. 如下所示：

```bash
FortiGate # diagnose sys waninfo ipify wan
Try to get my public IP through https://api.ipify.org with src_ip=0.0.0.0 device=wan vfid=0(root) ...

Public/WAN IP: 45.62.167.221
Location:
        Latitude: 22.278320
        Longitude: 114.174690
        Accuracy radius: Unknown
        Time zone: Asia/Hong_Kong
City: Hong Kong
Subdivisions:
        0: Hong Kong
Country/Zone: Hong Kong
Postal: Unknown
        Code: Unknown
Continent: Asia
Registered country: Unknown
ISP: Unknown
```

```bash
FortiGate # diagnose sys waninfo ipify 192.168.123.175
Try to get my public IP through https://api.ipify.org with src_ip=192.168.123.175 device=unspecified vfid=0(root)
...

Public/WAN IP: 123.112.242.161
Location:
        Latitude: 39.904202
        Longitude: 116.407402
        Accuracy radius: Unknown
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
        Time zone: Asia/Shanghai
City: Beijing
Subdivisions:
        0: Beijing
Country: China
Postal: Unknown
        Code: Unknown
Continent: Asia
Registered country: Unknown
ISP: Unknown
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

常用排错命令

请参考CLI troubleshooting cheat sheet ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

查找对象引用

网络需求

在删除一些配置对象前，通常需要先解除该对象的引用关系，如果对象被其他配置被引用，那么通常无法删除它们或将它们分配给某些新的配置，例如：

- 在GUI下将接口internal1添加到一个新的Hardware/Software交换接口时，新的交换接口成员列表中可能不显示该接口。从CLI执行此操作时也会因“Object is in use”错误而中断，这是因为该接口已被一些其他配置引用。例如配置了静态IP地址、配置了DHCP服务器、设置了静态路由等，这些都与该接口相关联。
- 尝试删除一个未使用的地址对象，但无法执行此操作。这是因为该地址对象可能被防火墙策略、地址组等配置引用。

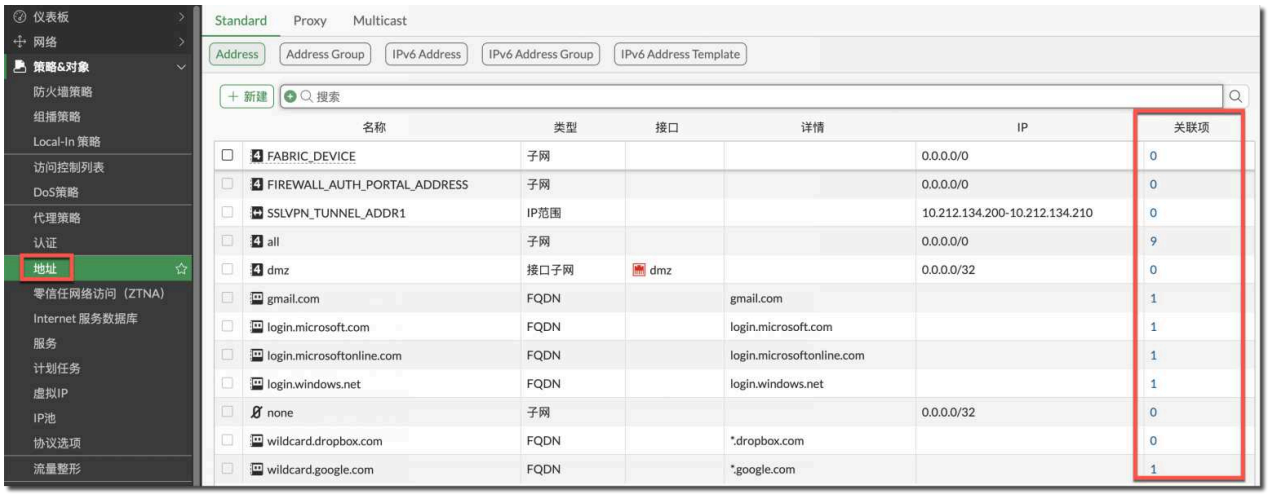
本文主要介绍如何快速找到并解除这些引用关系。

GUI

方法1

1. 在某个功能配置页面的列表上方，可以看到“关联项”列。





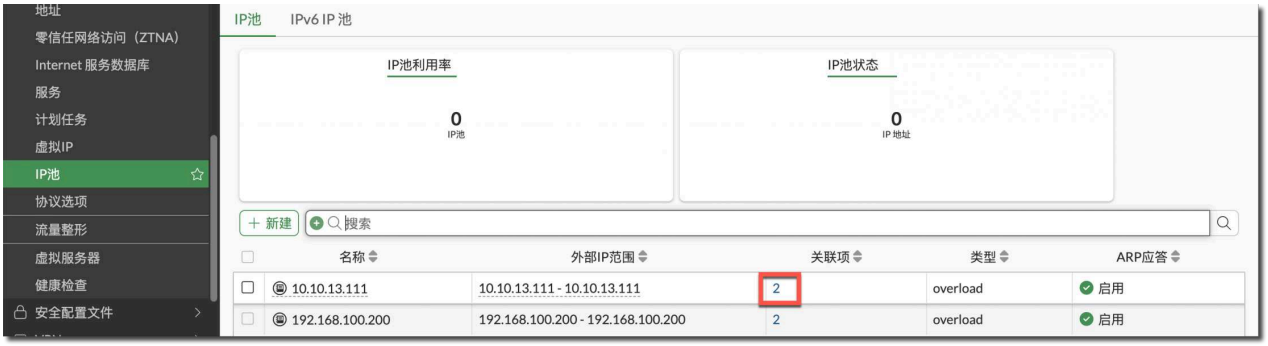
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 如果“关联项”列不可见，点击左侧的齿轮按钮（或右键单机标题列），然后选中“关联项”。



3. 点击“关联项”下的数字。



4. 弹出“使用率”页面，可以看到该对象当前被哪些配置引用，在该页面可以直接修改/删除引用该对象的配置，如下所示，点击查询一个IP池的关联项，有2条防火墙策略引用了这个IP池。



- 编辑：选中某个配置并点击编辑按钮，可以在当前页面编辑引用该对象（防火墙策略）的配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 删除：直接删除引用该对象的配置。
- 条目：跳转到选中的配置所在页面。



- 查看属性：查看对象被引用的配置的简要信息。



方法2

编辑某个配置对象，页面右侧点击“关联项”按钮，也可以弹出“使用率”页面。



CLI

主要方法

FortiOS的CLI采用树状语法定义配置对象的位置，例如防火墙地址对象的路径为`Firewall/Address/<name>`，进入该配置的CLI语法为`config firewall address <name>`。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

通过如下命令可以查找对象的配置关联项。

```bash
diagnose sys cmdb refcnt show <path.object.mkey>
```

`<path.object.mkey>`是对象存储位置、对象类别、对象数据库主键的组合。如下所示，该命令显示`config system interface`下名称为“wan2”的接口的所有配置引用，接口“wan2”已被firewall sniffer、ACME以及SD-WAN member配置引用。

```bash
FortiGate # diag sys cmdb refcnt show system.interface.name wan2

entry used by child table members:seq-num '2' of complex system.sdwan:members.interface
entry used by table firewall.sniffer:id '1'
entry used by child table interface:interface-name 'wan2' of complex system.acme:interface.interface-name
```

定位对象的mkey

上述命令要求使用`<path.object.mkey>`格式指定需要查找关联项的对象。虽然可以很容易找到path和object的字段（例如，地址对象的`path.object`为`firewall.address`），但要确定该对象使用的具体mkey字段需要用到如下方法（mkey并不总是`name`）。

方法1-使用tree命令

1. 如下所示的SD-WAN成员配置，该SD-WAN区域的成员序号1为wan1。

```bash
config system sdwan
    config members
        edit 1    ←——SD-WAN成员序号
            set interface "wan1"
            set zone "virtual-wan-link"
        next
    end
end
```

2. 使用tree命令查看，SD-WAN功能的配置路径为`system.sdwan`，对象为`members`，而mkey为`seq-num`（被`*`标记的为mkey），而不是接口名称（SD-WAN成员在配置中是通过其成员ID编号而非接口名称进行引用的）。

```bash
FortiGate # tree system sdwan members
-- [members] --*seq-num (0,512)    ←——“*”标记表示该对象的mkey
├─ interface (15)
├─ zone (35)
├─ gateway
......
```

3. 已经知道了SD-WAN成员的mkey`seq-num`在配置（`config system sdwan`→`config members`）中为“1”，使用`diagnose sys cmdb refcnt show system.sdwan.members.seq-num 1`命令就可以查找所有引用SD-WAN成员#1的配置，如下所示，该SD-WAN成员被一个SD-WAN健康检查引用（`health-check.members.seq-num`）：

```bash
FortiGate # diagnose sys cmdb refcnt show system.sdwan.members.seq-num 1
entry used in complex system.sdwan:health-check.members.seq-num child table health-check:name '223.5.5.5'  entry
members:seq-num '1' (From VDOM: 'root')

config system sdwan
    config health-check
        edit "223.5.5.5"
            set server "223.5.5.5"
            set members 1    ←——引用关系
        next
    end
end
```

重要

`<path.object.mkey>`之间的分隔符可以使用`.`或`:`。如下所有分隔方式均可正常使用：

```bash
diagnose sys cmdb refcnt show system.interface.name wan1
diagnose sys cmdb refcnt show system.interface:name wan1
diagnose sys cmdb refcnt show system:interface:name wan1
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

方法2-使用get命令

`get` 命令可以仅列出对象的mkey，如下所示，防火墙地址对象的mkey为 `name` 。

```bash
get firewall address
== [ all ]
name: all    ←——mkey为“name”
== [ SSLVPN_TUNNEL_ADDR1 ]
name: SSLVPN_TUNNEL_ADDR1
== [ 10.10.1.4 ]
name: 10.10.1.4
......
```

举例

1. 查找防火墙地址对象“all”的关联配置。如下所示，地址对象“all”正在被多个防火墙策略中的源地址引用。

```bash
FortiGate # diagnose sys cmdb refcnt show firewall.address:name all

entry used by child table source-address:name 'all' of complex vpn.ssl.settings:source-address.name
entry used by child table dst:name 'all' of table service:id '1' of complex system.sdwan:service.dst.name
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '10'
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '25'
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '20'
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '2'
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '23'
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '13'
entry used by child table srcaddr:name 'all' of table firewall.policy:policyid '12'
```

2. 查找对象所有可能关联的所有配置（并非实际被引用），将mkey留空即可：

```bash
FortiGate # diagnose sys cmdb refcnt show firewall.address:name

may used by table firewall.addrgrp.member.name
may used by table vpn.ssl.web.portal.widget.ip-pools.name
may used by table vpn.ssl.web.portal.widget.split-tunneling-routing-address.name
may used by table vpn.ssl.settings.tunnel-ip-pools.name
may used by table vpn.ipsec.phase2.src-name
may used by table vpn.ipsec.phase2.dst-name
may used by table vpn.ipsec.phase1-interface.ipv4-split-include
may used by table vpn.ipsec.phase2-interface.src-name
may used by table vpn.ipsec.phase2-interface.dst-name
may used by table firewall.policy.srcaddr.name
may used by table firewall.policy.dstaddr.name
may used by table firewall.interface-policy.srcaddr.name
may used by table firewall.interface-policy.dstaddr.name
may used by table firewall.sniff-interface-policy.srcaddr.name
may used by table firewall.sniff-interface-policy.dstaddr.name
```

3. 其他举例：

```bash
diagnose sys cmdb refcnt show system.interface.name <interface name>
diagnose sys cmdb refcnt show firewall.address:name <address name>
diagnose sys cmdb refcnt show firewall.profile: <profile name>
diagnose sys cmdb refcnt show firewall.service.group:name <servicegroup name>
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

会话管理

CLI方式

使用`diagnose sys session`命令可以过滤、查看和删除会话。

过滤条件

1. 查看和删除某特定会话时，都需要先设置filter。

```bash
diagnose sys session filter ?    //键入?查看会话支持的过滤条件，如源IP，目的IP，目的端口等//
vd                Index of virtual domain. -1 matches all.
vd-name           Name of virtual domain. -1 or "any" matches all.
sintf             Source interface.
dintf             Destination interface.
src               Source IP address.
nsrc              NAT'd source ip address
dst               Destination IP address.
proto             Protocol number.
sport             Source port.
nport             NAT'd source port
dport             Destination port.
policy            Policy ID.
expire            expire
duration          duration
proto-state       Protocol state.
session-state1    Session state1.
session-state2    Session state2.
ext-src           Add a source address to the extended match list.
ext-dst           Add a destination address to the extended match list.
ext-src-negate    Add a source address to the negated extended match list.
ext-dst-negate    Add a destination address to the negated extended match list.
clear             Clear session filter.
negate            Inverse filter.
```

2. 查看当前的过滤条件。

```bash
diagnose sys session filter    //直接键入回车查看当前的过滤条件//
session filter:
        vd: any
        sintf: any
        dintf: any
        proto: any
        proto-state: any
        source ip: any
        NAT'd source ip: any
        dest ip: any
        source port: any
        NAT'd source port: any
        dest port: any
        policy id: any
        expire: any
        duration: any
        state1: any
        state2: any
```

查看会话

1. 查看某特定会话时，需要先设置filter。如果不设置过滤条件，则diagnose sys session list 将列出FortiGate当前所有的会话。

```bash
diagnose sys session filter proto 1
diagnose sys session filter src 192.168.1.10
```

2. 查看设置的过滤条件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
diagnose sys session filter
session filter:
        vd: any
        sintf: any
        dintf: any
        proto: 1-1
        proto-state: any
        source ip: 192.168.1.10-192.168.1.10
        NAT'd source ip: any
        dest ip: any
        source port: any
        NAT'd source port: any
        dest port: any
        policy id: any
        expire: any
        duration: any
        state1: any
```

3. 查看过滤后的会话。

```bash
diagnose sys session list
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=13->14/14->13 gwy=192.168.2.10/192.168.1.10
hook=pre dir=org act=noop 192.168.1.10:13898->192.168.2.10:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.10:13898->192.168.1.10:0(0.0.0.0:0)
misc=0 policy_id=8 pol_uuid_idx=520 auth_info=0 chk_client_info=0 vd=0
serial=00091df7 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=158/156, ipid=156/158, vlan=0x0000/0x0000
vlifid=156/158, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=5/4
total session 1    //过滤的会话，总共有1条//
```

删除会话

1. 删除某特定会话时，需要先设置filter。如果不设置过滤条件，则diagnose sys session clear 将清空FortiGate当前所有的会话，可能会引起断网。

```bash
diagnose sys session filter proto 1
diagnose sys session filter src 192.168.1.10
```

2. 查看设置的过滤条件。

```bash
diagnose sys session filter
session filter:
        vd: any
        sintf: any
        dintf: any
        proto: 1-1
        proto-state: any
        source ip: 192.168.1.10-192.168.1.10
        NAT'd source ip: any
        dest ip: any
        source port: any
        NAT'd source port: any
        dest port: any
        policy id: any
        expire: any
        duration: any
        state1: any
```

3. 查看过滤后的会话是否是需要删除的会话。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
FortiGate # diagnose sys session list
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=13->14/14->13 gwy=192.168.2.10/192.168.1.10
hook=pre dir=org act=noop 192.168.1.10:13898->192.168.2.10:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.10:13898->192.168.1.10:0(0.0.0.0:0)
misc=0 policy_id=8 pol_uuid_idx=520 auth_info=0 chk_client_info=0 vd=0
serial=00091df7 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=158/156, ipid=156/158, vlan=0x0000/0x0000
vlifid=156/158, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=5/4
total session 1
```

4. 确认无误后，再执行删除会话的命令。

```bash
FortiGate # diagnose sys session clear
```

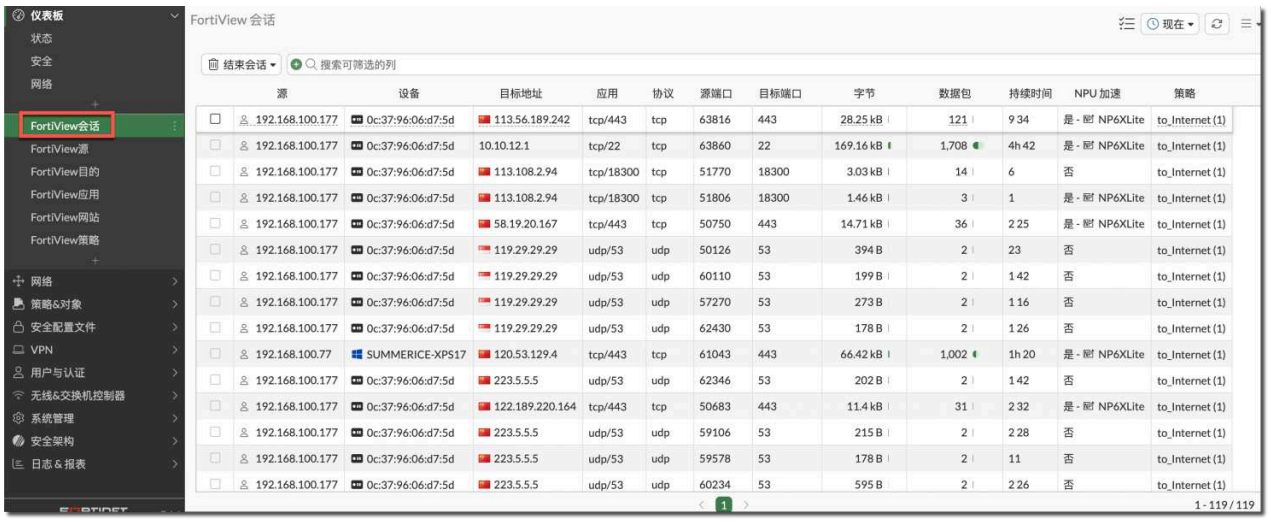
GUI方式

重要

该功能在FortiOS 7.4.0及以上版本支持。

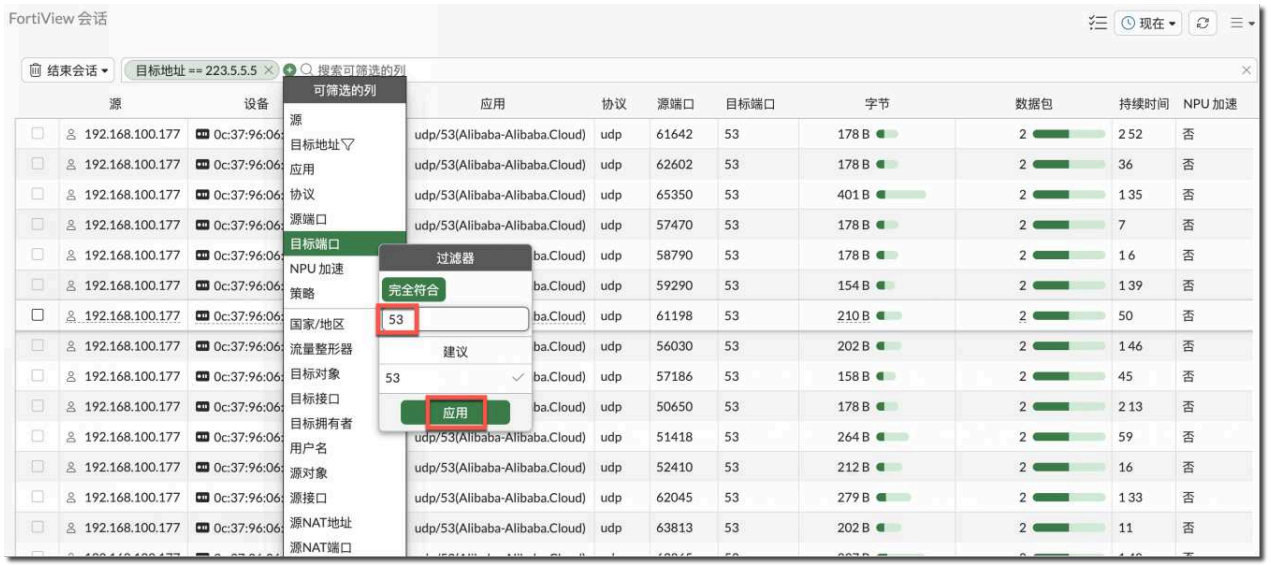
过滤条件

1. 登录设备的管理页面，进入仪表盘→FortiView会话页面，可以看到当前设备所有活动的会话信息。



2. 在页面上方的搜索框中点击“+”按钮，可以根据不同的会话参数配置过滤条件，可以设置多个过滤条件，点击应用按钮，可以过滤出对应的会话列表。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



查看会话

部分列会被隐藏，右键点击任意列标题，可以配置显示/隐藏的会话参数列。



删除会话

删除过滤结果中的会话

1. 删除过滤结果中的会话，配置筛选条件后查询会话信息（如下所示过滤所有的ICMP协议会话），然后点击页面左上角的“结束会话→仅筛选”按钮（不会删除本地会话）。



2. 弹出确认提示，点击OK按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

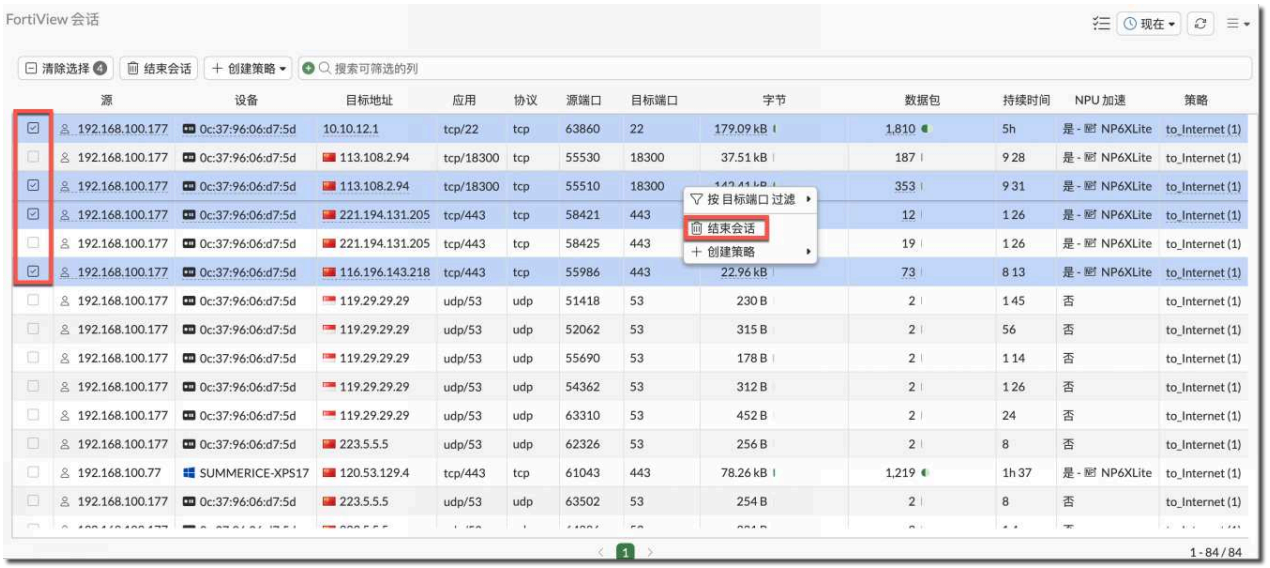


3. 会话删除成功，查看系统日志，显示管理员删除会话的记录，日志中会显示删除会话时所用的过滤器（`filter:vd:0;sintf:not 0;dintf:not 0;proto:1-1;policy id:not 4294967295-4294967295;state1:not (100 mask:102);)`，包含IPv4和IPv6会话。

```bash
date=2025-08-29 time=16:34:19 eventtime=1756456458243468840 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv6 sessions ( filter:vd:0;sintf:not
0;dintf:not 0;proto:1-1;policy id:not 4294967295-4294967295;state1:not (100 mask:102);)"

date=2025-08-29 time=16:34:19 eventtime=1756456458231928019 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv4 sessions ( filter:vd:0;sintf:not
0;dintf:not 0;proto:1-1;policy id:not 4294967295-4294967295;state1:not (100 mask:102);)"
```

删除手工选中的会话

1. 会话左侧手工选中4条会话（或使用Ctrl/Shift + 鼠标点击选中），右键点击会话，并选择“结束会话”，只会删除手工选中的这4个会话（不会删除本地会话）。



2. 弹出确认提示，点击OK按钮。



3. 会话删除成功，查看系统日志，显示管理员删除会话的记录，日志中会显示这4个会话对应的过滤器。

```bash
date=2025-08-29 time=16:44:38 eventtime=1756457078331716159 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv4 sessions ( filter:vd:0;proto:6-6;source
ip:192.168.100.177-192.168.100.177;dest ip:116.196.143.218-116.196.143.218;source port:55986-55986;dest port:443-
443;)"

date=2025-08-29 time=16:44:38 eventtime=1756457078281143959 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv4 sessions ( filter:vd:0;proto:6-6;source
ip:192.168.100.177-192.168.100.177;dest ip:221.194.131.205-221.194.131.205;source port:58421-58421;dest port:443-
443;)"
```

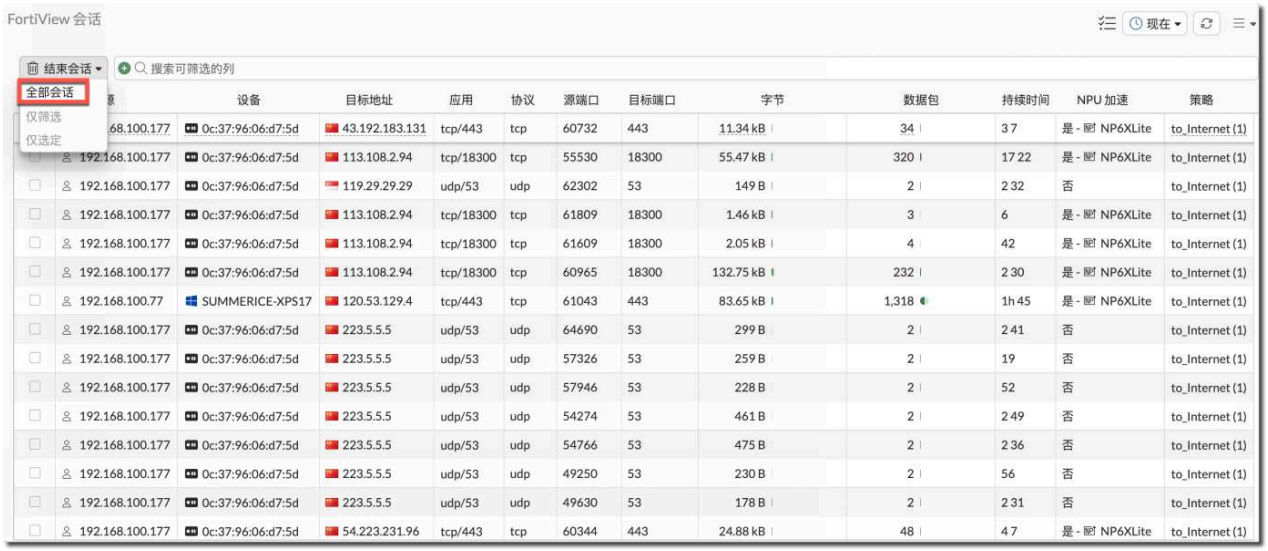

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
date=2025-08-29 time=16:44:38 eventtime=1756457078230556839 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv4 sessions ( filter:vd:0;proto:6-6;source
ip:192.168.100.177-192.168.100.177;dest ip:113.108.2.94-113.108.2.94;source port:55510-55510;dest port:18300-
18300;)"

date=2025-08-29 time=16:44:38 eventtime=1756457078179695119 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv4 sessions ( filter:vd:0;proto:6-6;source
ip:192.168.100.177-192.168.100.177;dest ip:10.10.12.1-10.10.12.1;source port:63860-63860;dest port:22-22;)"
```

删除全部会话

> **重要**
>
> 通过GUI删除全部会话，全部会话也包含本地会话，例如BGP路由会话和管理会话等，请谨慎操作。

1. 删除整机转发流量的全部IPv4/IPv6会话，点击页面左上角的“结束会话→全部会话”按钮。



2. 弹出确认提示，注意全部会话也包含本地会话，例如BGP路由会话和管理会话等，请谨慎操作，点击OK按钮。



3. 会话删除成功，查看系统日志，显示管理员删除会话的记录，日志中显示全部会话的过滤器为`filter:vd:0`。

```bash
date=2025-08-29 time=16:51:29 eventtime=1756457488487037179 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv6 sessions ( filter:vd:0;)"

date=2025-08-29 time=16:51:29 eventtime=1756457488475491179 tz="+0800" logid="0100036883" type="event"
subtype="system" level="warning" vd="root" logdesc="Clear active sessions" user="admin" ui="GUI(192.168.100.177)"
method="https" msg="User:admin from GUI(192.168.100.177) clean active IPv4 sessions ( filter:vd:0;)"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

会话参数分析

```bash
FortiGate # diagnose sys session list
session info: proto=6 proto_state=01 duration=2 expire=3597 timeout=3600 flags=00000000 socktype=0 sockport=0
av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=13->14/14->13 gwy=192.168.2.10/192.168.1.10
hook=pre dir=org act=noop 192.168.1.10:44610->192.168.2.10:22(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.2.10:22->192.168.1.10:44610(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 pol_uuid_idx=520 auth_info=0 chk_client_info=0 vd=0
serial=000c48ed tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0x4000c00 ofld-O ofld-R
npu info: flag=0x81/0x81, offload=8/8, ips_offload=0/0, epid=158/156, ipid=156/158, vlan=0x0000/0x0000
vlifid=156/158, vtag_in=0x0000/0x0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=5/5
```

- `proto`：协议号，ICMP:1，TCP:6，UDP:17。更多请参考：https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml ↗ 。
- `proto_state`：会话状态，跟协议相关。
  - ICMP：ICMP没有状态，一直显示proto_state=00。
  - UDP：UDP是没状态状态的协议。
    - proto_state=00：表示没有收到reply方向的udp报文。
    - proto_state=01：表示收到reply方向的udp报文
  - TCP：TCP是有状态的协议，proto_state=xy。
    - x与服务器的状态相关，当没有开启UTM或者Proxy时，x一直为0。
    - y与客户端的状态相关联，当FortiGate收到syn时，y的值为2；收到syn/ack时，y的值为3；收到ack时，即完成三次握手，y的值为1。

State	Value
NONE	0
ESTABLISHED	1
SYN_SENT	2
SYN & SYN/ACK	3
FIN_WAIT	4
TIME_WAIT	5
CLOSE	6
CLOSE_WAIT	7
LAST_ACK	8
LISTEN	9

- `duration`：会话存在的时间。
- `expire`：从会话经过最后一个包开始，从timeout时间开始倒计时。
- `timeout`：会话在当前状态下的超时时间（TCP会话各状态超时时间，非特殊情况不要修改，请参考策略与对象→配置Session TTL ↗章节）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- `origin-shaper`：会话发起方流量匹配的traffic shaper策略。
- `reply-shaper`：会话反向流量匹配的traffic shaper策略。
- `per_ip_shaper`：会话匹配的per-ip策略。
- `tunnel`：隧道的名称。
- `state`：会话表示状态。

会话状态	状态说明
may-dirty	Session details allowed to be altered
dirty	Session has been altered (requires may-dirty)
npu	Session goes through an acceleration ship
npd	Session is denied for hardware acceleration
npr	Session is eligible for hardware acceleration (more info with npu info: offload=x/y)
rem	Session is allowed to be reset in case of memory shortage
eph	Session is ephemeral
oe	Session is part of Ipsec tunnel (from the originator)
re	Session is part of Ipsec tunnel (from the responder)
local	Session is attached to local fortigate ip stack
br	Session is bridged (vdom is in transparent mode)
redir	Session is redirected to an internal FGT proxy
wccp	Session is intercepted by wccp process
nlb	Session is from a load-balanced vip
log	Session is being logged
os	Session is shaped on the origin direction
rs	Session is shaped on the reply direction
ndr	Session is inspected by IPS signature
nds	Session is inspected by IPS anomaly
auth	Session is subject to authentication
block	Session was re-evaluated to block
ext	(deprecated) Session is handled by a session helper
app_ntf	Session matched a policy entry that contains "set block-notification enable"
F00	After enable traffic log in policy, session will have this flag

- `dev`：FortiGate接口索引index，可以通过diagnose netlink interface list查看，如下所示。dev=13->14/14->13表示数据流发起方从port5到port6，数据流的响应方从port6到port5。

```bash
FortiGate# diagnose netlink interface list | grep 13
if=port5 family=00 type=1 index=13 mtu=1500 link=0 master=0
# diagnose netlink interface list | grep 14
if=port6 family=00 type=1 index=14 mtu=1500 link=0 master=0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- `dir=org act=noop 192.168.1.10:44610→192.168.2.10:22(0.0.0.0:0)`：发起方：源IP→目的IP，没有做SNAT或DNAT。
- `dir=reply act=noop 192.168.2.10:22→192.168.1.10:44610(0.0.0.0:0)`：响应方：源IP→目的IP，与发起方相反，没有做SNAT或DNAT。
- `policy_id`：匹配的策略ID。
- `vd`：vdom的索引index，root vdom的索引是0，通过diagnose sys vd list查看。

```bash
FortiGate # diagnose sys vd list

list virtual firewall info:
name=root/root index=0 enabled fib_ver=136 rpdb_ver=0 use=172 rt_num=35 asym_rt=0 sip_helper=0, sip_nat_trace=1,
mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
```

- `serial`：会话ID。
- `app`：应用ID。
- `url_cat`：URL类别。
- `offload original direction/reply direction`：0：会话没有卸载到NP；8：会话卸载到NP6；9：会话卸载到NP7。
  - offload=8/8：表示发起方向和反向流量都卸载到NP6了。
  - offload=9/9：表示发起方向和反向流量都卸载到NP7了。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

会话统计命令

通过`diagnose sys session full-stat`命令，可以查看FortiGate整机会话的统计信息。

如下所示`diagnose sys session full-stat`命令的输出结果。

```bash
FortiGate # diagnose sys session full-stat

session table:           table_size=524288 max_depth=1 used=252
misc info:       session_count=127 setup_rate=0 exp_count=0 reflect_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/239104 removeable=0 extreme_low_mem=0
        npu_session_count=55
        nturbo_session_count=21
delete=0, flush=16, dev_down=64/174
session walkers: active=0, vf-397, dev-64, saddr-0, npu-0, wildcard-0
TCP sessions:
         58 in ESTABLISHED state
         2 in SYN_SENT state
         5 in CLOSE state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00103420
ips_recv=002aff57
policy_deny=000e0704
av_recv=01a29d3a
fqdn_count=0000000a
fqdn6_count=00000000
```

- `ephemeral`：当前处于ephemeral（临时）状态的会话数量。ephemeral会话指处于建立阶段的TCP会话，或仅接收单向数据包且未双向通信的UDP会话。
  - 由于FortiGate需要分配内存来管理会话，此类半连接会话是常见的DoS攻击形式。
  - 为避免此类攻击，FortiGate将处于这些状态的会话归类为ephemeral会话，并根据设备型号设定同时存在的会话数量上限，以防止内存耗尽。其核心目的是提供一种DoS防护。
- `memory_tension_drop`：因系统内存不足而删除的会话数量，将删除最旧的会话，TCP本地会话不会被删除。
- `removeable`：当可用内存不足以支持创建新会话时，统计现有防火墙会话中可供删除的候选会话数量。
- `npu_session_count`：当前被NP芯片加速转发的会话数量。
- `nturbo_session_count`：当前被nturbo加速的会话数量。
- `flush`：统计因用户操作或某些功能删除的会话数量，例如：
  - 管理员使用GUI删除特定会话。
  - 被IPS规则阻断的会话。
  - 当SIP ALG会话因通话结束而被删除时，若该通话通过UDP建立，SIP ALG将删除对应的会话，以避免该会话被意外重复用于其他SIP呼叫。
- `dev_down`：统计当IPSec接口被管理性关闭时，删除的相关IPSec接口会话。
- `cont`：统计被发送到IPS并由IPS检测后继续放通的报文数量。计数结果以十六进制形式显示。
- `ips_recv`：统计发往IPS处理的报文数量。若设备支持nTurbo且该功能已启用，则通过nTurbo传递至IPS的数据包不计入此统计。计数结果以十六进制形式显示。
- `av_recv`：统计发往AV处理的数据包数量。统计结果以十六进制形式显示。
- `fqdn_count`：统计内核中当前存在，且与`config firewall address`、`config firewall address6`和`config firewall service`中配置对应的FQDN条目数量。计数结果以十六进制形式显示。
- `error1`：统计接收到的数据包加密状态与其所属会话不匹配。例如：
  - 当会话要求解密数据包时，该数据包仍为明文（例如在欺骗攻击）。
  - 数据包已正确解密，但会话未关联任何IPsec隧道。
- `error2`：统计在数据包出站时，所选接口与关联会话中的出接口不匹配的次数。
- `error3`：ALG 的expectation会话用于在防火墙上建立针孔（如FTP协议），并始终关联至生成该expectation的父会话。系统为每个父会话设定了可同时关联的expectation上限；一旦达到该上限，error3计数器递增一次。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

sniffer工具介绍

FortiGate具备完善的sniffer功能，可以基于指定接口或所有接口附带过滤条件进行抓包。

Sniffer命令

```bash
diagnose sniffer packet <interface> <filter> <verbose> <count> <tsformat> <frame size>
```

- `<interface>`：可以指定一个具体的interface名字，比如“port1”或所有接口“any”。
- `<filter>`：非常强大的过滤功能，可以过滤出想要过滤的流，过滤条件需要引号括起来`'<filter>'`或者`"<filter>"`，与tcpdump语法基本相同。

```bash
[[src|dst] host {<host1_ipv4>}]
[and|or] [[src|dst] host <host2_ipv4>}]
[and|or] [[arp|ip|gre|esp|udp|tcp] port <port1_int>]
[and|or] [[arp|ip|gre|esp|udp|tcp] port <port2_int>]
```

  - 过滤单个IP（该IP可以是源，也可以是目的）：`'host 1.1.1.1'`
  - 过滤源IP和目的IP：`'host 1.1.1.1 and host 2.2.2.2'`
  - 过滤目的IP和协议端口：`'dst 2.2.2.2 and tcp port 80'`
  - 过滤源IP和协议：`'src 1.1.1.1 and icmp'`
- `<verbose>`：不同级别的不同内容展示，按需定义sniffer级别。
  - `1`：print header of packets（只输出报文头部内容）
  - `2`：print header and data from ip of packets（输出从ip头部开始，包含数据内容）
  - `3`：print header and data from ethernet of packets（输出从ethernet头部开始，包含数据内容）
  - `4`：print header of packets with interface name（只输出报文头部和进出接口，使用最多）
  - `5`：print header and data from ip of packets with interface name（输出从IP头部开始，包含数据内容和进出接口）
  - `6`：print header and data from ethernet of packets (if available) with intf name（从ethernet头部开始，包含数据内容和进出接口，使用较多）
- `<count>`：抓包个数，到达指定个数后停止sniffer，如100表示抓100个包，填写为0表示不限制抓包的数量。
- `<tsformat>`：时间戳格式。
  - `a`：UTC绝对时间，格式为yyyy-mm-dd hh:mm:ss.ms
  - `l`：本地时间，yyyy-mm-dd hh:mm:ss.ms
  - 不填写：开始抓包后的相对时间，ss.ms
- `<frame size>`：设置截断前帧的大小，默认是接口MTU。

Sniffer示例

- 在port1上抓取源或目的IP为172.16.1.100的包，只输出报文头部内容。

```bash
diagnose sniffer packet port1 "host 172.16.1.100" 1
```

- 在所有接口上抓取源或目的IP为172.16.1.100的ICMP报文，输出报文头部和进出接口。

```bash
diagnose sniffer packet any "host 172.16.1.100 and icmp" 4
```

- 在所有接口上抓取源或目的IP为172.16.1.100的TCP报文，输出报文头部和进出接口。

```bash
diagnose sniffer packet any "host 172.16.1.100 and tcp" 4
```

- 在所有接口上抓取源或目的IP为172.16.1.100的UDP报文，输出报文头部和进出接口。

```bash
diagnose sniffer packet any "host 172.16.1.100 and udp" 4
```

- 在所有接口上抓取源或目的IP为172.16.1.100，端口号为443的TCP报文，输出报文头部和进出接口。

```bash
diagnose sniffer packet any "host 172.16.1.100 and tcp port 443" 4
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 在所有接口上抓取源或目的IP为172.16.1.100且TCP端口≠22的报文， 输出报文头部和进出接口。

```
diagnose sniffer packet any "host 172.16.1.100 and !tcp port 22" 4
```
bash

- 在所有接口上抓取源或目的IP为172.16.1.100且TCP/UDP端口为10000的报文， 输出报文头部和进出接口。

```
diagnose sniffer packet any "host 172.16.1.100 and port 10000" 4
```
bash

- 在所有接口上抓取源或目的IP为114.114.119.119且协议为ICMP的报文，携带0表示不限制抓包个数，携带a表示携带抓包的时间戳，时间戳的格式为抓包开始后的相对时间。

```
diagnose sniffer packet any "host 114.114.119.119 and icmp" 4 0 a
```
bash

- 在所有接口上抓取目的IP为114.114.119.119且协议为ICMP的报文，携带0表示不限制抓包个数，携带l表示携带抓包的时间戳，时间戳格式为绝对时间，与设备上的时间一致。

```
diagnose sniffer packet any "dst 114.114.119.119 and icmp" 4 0 l
```
bash

- 在port1接口上抓取源IP为10.1.1.1，源或目的端口号为80，并携带VLAN Tag 10的报文。

```
diagnose sniffer packet port1 'vlan 10 and src 10.1.1.1 and port 80' 4
```
bash

- 在port1上抓取VLAN tag为3001且IP host为192.168.1.1的VLAN trunk报文，或VLAN tag为3002且IP host为192.168.2.1的VLAN trunk报文。

```
diagnose sniffer packet port1 "vlan and ((ether[14:2] == 3001 and host 192.168.1.1) or (ether[14:2] == 3002 and host 192.168.2.1))" 4 0 l
```
bash

- 在所有接口上抓取（源或目的IP为172.16.1.100）或（源或目的IP为172.16.1.101且端口号为1701）的报文。

```
diagnose sniffer packet any "host 172.16.1.100 or (host 172.16.1.101 and port 1701)" 4
```
bash

- 在internal接口上抓取SYN置位的TCP报文。

```
diagnose sniffer packet internal "tcp[13]&2≠0 and port 23" 4
```
bash

- 在internal接口上抓取SYN-ACK置位的TCP报文。

```
diagnose sniffer packet internal "tcp[13] = 18" 4
```
bash

- 在internal接口上抓取RST置位的TCP报文。

```
diagnose sniffer packet internal "tcp[13]&4≠0" 4
```
bash

- 在wan1接口上抓取PPPoE协商报文（其中0x8863发现阶段，0x8864为会话阶段）。

```
diagnose sniffer packet wan1 "ether proto 0×8863 or ether proto 0×8864" 4
```
bash

- 在internal接口上抓取源或目IP属于网段为4.2.2.0/24的所有报文。

```
diagnose sniffer packet internal "net 4.2.2.0/24" 4
```
bash

- 在internal接口上抓取源MAC地址为00:09:0f:89的报文。

```
diagnose sniffer packet internal "(ether[6:4]=0×00090f89) and (ether[10:2]=0×10ea)" 4
```
bash

- 在所有接口上抓取IP TTL为1的报文。

```
diagnose sniffer packet any "ip[8:1] = 0×01" 4
```
bash

- 在internal接口上抓取特定Payload的报文。

```
Payload:
0×0040   8f48 8a0c 7468 6973 2069 7320 7069 6e67    .H..this.is.ping

Filter:
diagnose sniffer packet internal "ether[0×44:4]=0×74686973" 4
```
bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 在所有接口上抓取大于1500 Bytes（除去二层头部长度）的报文。

```
diagnose sniffer packet any "ip[2:2] > 1500" 4
```
bash

- 抓取三层组播报文。

```
diagnose sniffer packet port1 'ip multicast' 6 0 l
```
bash

- 抓取二层组播报文。

```
diagnose sniffer packet port1 'ether multicast' 6 0 l
```
bash

- 抓取三层广播报文。

```
diagnose sniffer packet port1 'ip broadcast' 6 0 l
```
bash

- 抓取二层广播报文。

```
diagnose sniffer packet port1 'ether broadcast' 6 0 l
```
bash

- 抓取二层和三层组播。

```
diagnose sniffer packet port1 'multicast' 6 0 l
```
bash

Sniffer过程分析

ICMP

1. ICMP的请求报文是echo request，响应报文是echo reply，in表示FortiGate收到一个报文，out表示FortiGate发出一个报文。在FortiGate上抓取ICMP报文。

```
FortiGate # diagnose sniffer packet any 'host 192.168.2.10 and icmp' 4
interfaces=[any]
filters=[host 192.168.2.10 and icmp]
```
bash

2. FortiGate从port5收到192.168.1.10发送给192.168.2.10 ping的请求报文echo request。

```
7.074724 port5 in 192.168.1.10 → 192.168.2.10: icmp: echo request
```
bash

3. FortiGate将192.168.1.10发送给192.168.2.10 ping的请求报文echo request从port6转发出去了。

```
7.074748 port6 out 192.168.1.10 → 192.168.2.10: icmp: echo request
```
bash

4. FortiGate从port6收到192.168.2.10发送给192.168.1.10 ping的响应报文echo reply。

```
7.075033 port6 in 192.168.2.10 → 192.168.1.10: icmp: echo reply
```
bash

5. FortiGate将192.168.2.10发送给192.168.1.10 ping的响应报文echo reply从port5转发出去了。

```
7.075042 port5 out 192.168.2.10 → 192.168.1.10: icmp: echo reply
```
bash

6. 从上面的抓包来看，FortiGate成功转发了192.168.1.10和192.168.2.10之间ping的请求和响应报文。

TCP

1. TCP报文交互之前都需要完成3次握手，in表示FortiGate收到一个报文，out表示FortiGate发出一个报文。在FortiGate上抓取TCP报文。

```
FortiGate # diagnose sniffer packet any 'host 192.168.2.10 and port 22' 4
interfaces=[any]
filters=[host 192.168.2.10 and port 22]
```
bash

2. FortiGate从port5收到 192.168.1.10发送给192.168.2.10 的syn报文。

```
12.009383 port5 in 192.168.1.10.46028 → 192.168.2.10.22: syn 486804292
```
bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. FortiGate将192.168.1.10发送给192.168.2.10 的syn报文从port6转发出去了。

```bash
12.009752 port6 out 192.168.1.10.46028 → 192.168.2.10.22: syn 486804292
```

4. FortiGate从port6收到 192.168.2.10发送给192.168.1.10 的 syn ack报文。

```bash
12.009957 port6 in 192.168.2.10.22 → 192.168.1.10.46028: syn 1279904517 ack 486804293
```

5. FortiGate将192.168.2.10发送给192.168.1.10 的syn ack报文从port5转发出去了。

```bash
12.010120 port5 out 192.168.2.10.22 → 192.168.1.10.46028: syn 1279904517 ack 486804293
```

6. FortiGate从port5收到 192.168.1.10发送给192.168.2.10 的ack报文。

```bash
12.010233 port5 in 192.168.1.10.46028 → 192.168.2.10.22: ack 1279904518
```

7. FortiGate将192.168.1.10发送给192.168.2.10 的ack报文从port6转发出去了。

```bash
12.010245 port6 out 192.168.1.10.46028 → 192.168.2.10.22: ack 1279904518
```

8. 从上面的抓包来看，FortiGate成功转发了192.168.1.10和192.168.2.10之间tcp三次握手的报文。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Sniffer过滤条件的合理使用

过滤条件使用总结

Sniffer应该抓取一条流的五元组不变的那个参数，且过滤的条件越精确抓取的报文越准确。

- 在没有NAT场景下，源目IP及目的端口都不会变化，则过滤条件可以设置为 `host <src IP> and host <dst IP> and <dst port>`。
- 在源NAT场景下，源IP会做NAT转换，因此目的IP和目的端口是不会变化的，则过滤条件可以设置为 `host <dst IP> and <dst port>`。
- 在目的NAT场景下，目的IP会做NAT转换，因此源IP和目的端口是不会变化的，则过滤条件可以设置为 `host <src ip> and <dst port>`。
- 在目的端口NAT场景下，目的IP和端口都会做NAT转换，因此源IP是不会变化，则过滤条件可以设置为 `host <src IP>`。
- 在源NAT和目的NAT都存在的场景下，源IP和目的IP都会发生变化，则只能通过 `or` 参数分别抓取NAT前和NAT后的报文，过滤条件可以设置为 `(<源NAT前的源IP> and <目的NAT前的目的IP> and <目的NAT前目的端口>) or (<源NAT后的源IP> and <目的NAT后的目的IP> and <目的NAT后的目的端口>)`。

Sniffer过滤条件使用举例

> **重要**
>
> Ping、ESP、GRE是没有端口的，直接使用icmp、esp、gre协议过滤即可。

普通三层转发，没有NAT场景

1. 普通三层转发，没有NAT的情况下，抓 `host <src IP> and host <dst IP> and <dst port>` 可以抓到完整的数据流。

2. 拓扑：PC1(172.16.1.100)-----(port9：172.16.1.1)FGT(port10:202.106.1.1)-----PC2(202.106.1.100)。

3. 抓包结果如下。

```bash
FGT # diagnose sniffer packet  any "host 172.16.1.100 and host 202.106.1.100 and icmp" 4
interfaces=[any]
filters=[host 172.16.1.100 and icmp]
3.583522 port9 in 172.16.1.100 → 202.106.1.100: icmp: echo request
3.583541 port10 out 172.16.1.100 → 202.106.1.100: icmp: echo request
3.583808 port10 in 202.106.1.100 → 172.16.1.100: icmp: echo reply
3.583818 port9 out 202.106.1.100 → 172.16.1.100: icmp: echo reply
```

普通三层转发，有源NAT场景

1. 普通三层转发，有源NAT的情况下，抓 `host <dst IP> and <dst port>` 可以抓到完整的数据流。

2. 拓扑：PC1(172.16.1.100)-----(port9：172.16.1.1)FGT(port10:202.106.1.1)-----PC2(202.106.1.100)。

3. 抓包结果如下。

```bash
FGT # diagnose sniffer packet  any “host 172.16.1.100 and icmp” 4
//抓源IP and icmp协议，是抓不全的//
interfaces=[any]
filters=[host 172.16.1.100 and icmp]
2.821403 port9 in 172.16.1.100 → 202.106.1.100: icmp: echo request
2.821707 port9 out 202.106.1.100 → 172.16.1.100: icmp: echo reply    //只能在port9看到数据包in/out，port10的看不到//

FGT # diagnose sniffer packet  any "host 202.106.1.100 and icmp" 4
//需要抓目的IP and icmp协议//
interfaces=[any]filters=[host 202.106.1.100 and icmp]
4.624647 port9 in 172.16.1.100 → 202.106.1.100: icmp: echo request
4.625032 port10 out 202.106.1.1 → 202.106.1.100: icmp: echo request
4.625235 port10 in 202.106.1.100 → 202.106.1.1: icmp: echo reply
4.625243 port9 out 202.106.1.100 → 172.16.1.100: icmp: echo reply
```

普通三层转发，有目的NAT（一对一NAT）场景

1. 普通三层转发，有目的NAT的情况下，抓 `host <src ip> and <dst port>` 可以抓到完整的数据流。

2. 拓扑：PC1(172.16.1.100)-----(port9：172.16.1.1)FGT(port10:202.106.1.1)-----PC2(202.106.1.100)。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 访问VIP（DNAT），流量从外网侧发起，抓包结果如下。

```bash
FGT # diagnose sniffer packet any “host 202.106.1.10” 4
//抓目的IP and icmp协议，是抓不全的//
interfaces=[any]
filters=[host 202.106.1.10]
3.809005 port10 in 202.106.1.100 → 202.106.1.10: icmp: echo request
3.809294 port10 out 202.106.1.10 → 202.106.1.100: icmp: echo reply    //只能在port10看到数据包in/out，port9的看不到//

FGT # diagnose sniffer packet any “host 202.106.1.100” 4
//需要抓源IP and icmp协议//
interfaces=[any]
filters=[host 202.106.1.100]
3.523666 port10 in 202.106.1.100 → 202.106.1.10: icmp: echo request
3.523687 port9 out 202.106.1.100 → 172.16.1.100: icmp: echo request
3.523937 port9 in 172.16.1.100 → 202.106.1.100: icmp: echo reply
3.523943 port10 out 202.106.1.10 → 202.106.1.100: icmp: echo reply
```

普通三层转发，有双向NAT(源NAT+目的NAT）场景

1. 普通三层转发，有双NAT的情况下，抓`(<源NAT前的源IP> and <目的NAT前的目的IP> and <目的NAT前目的端口>) or (<源NAT后的源IP> and <目的NAT后的目的IP> and <目的NAT后的目的端口>)`可以抓到完整的数据流。

2. 拓扑：PC1(172.16.1.100)-----(port9：172.16.1.1)FGT(port10:202.106.1.1)-----PC2(202.106.1.100)。

3. 访问VIP，流量从外网侧发起 ，同时在内网接口侧开启了SNAT，抓包结果如下。

```bash
FGT # diagnose sniffer packet any "host 202.106.1.100 and icmp" 4
//只抓源IP是抓不全的//
interfaces=[any]
filters=[host 202.106.1.100 and icmp]
0.416187 port10 in 202.106.1.100 → 202.106.1.10: icmp: echo request
0.416576 port10 out 202.106.1.10 → 202.106.1.100: icmp: echo reply

FGT # diagnose sniffer packet any "host 172.16.1.100 and icmp" 4
//只目的IP也是抓不全的//
interfaces=[any]
filters=[host 172.16.1.100 and icmp]
1.417838 port9 out 172.16.1.1 → 172.16.1.100: icmp: echo request
1.418326 port9 in 172.16.1.100 → 172.16.1.1: icmp: echo reply

FGT # diagnose sniffer packet any "host 202.106.1.100 or host 172.16.1.1 and icmp" 4
//使用or组合，变化前源目的ip和变化后源目的IP可抓全//
interfaces=[any]
filters=[host 202.106.1.100 or host 172.16.1.1 or icmp]
0.419407 port10 in 202.106.1.100 → 202.106.1.10: icmp: echo request
0.419436 port9 out 172.16.1.1 → 172.16.1.100: icmp: echo request
0.419781 port9 in 172.16.1.100 → 172.16.1.1: icmp: echo reply
0.419794 port10 out 202.106.1.10 → 202.106.1.100: icmp: echo reply
```

抓取PPPoE报文

1. PPPoE Discovery阶段（协商）的的ethernet类型为`0x8863`，PPPoE Session阶段（数据）的ethernet类型为`0x8864`。

```bash
diagnose sniffer packet <PPPoe Interface> 'ether proto 0x8863 or ether proto 0x8864' 6 0 l
```

2. 也可以使用`pppoed`和`pppoes`参数来作为过滤条件。

```bash
diagnose sniffer packet any 'pppoed or pppoes' 6 0 l
```

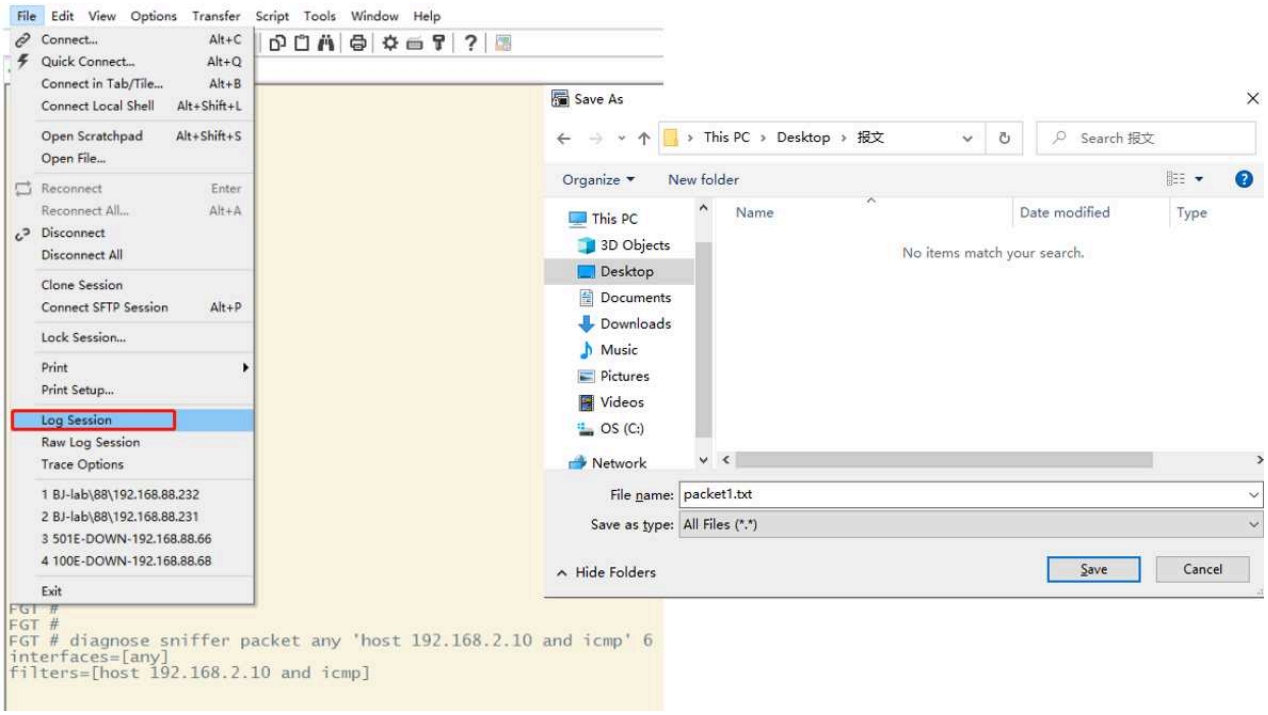

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

使用Wireshark打开抓包文件

通过抓包转换工具ConvertPcap（点击此处下载ConvertPcap ↗），我们可以将使用Sniffer格式6抓到的报文转换为Wireshark可以打开的文件格式。

> **重要**
>
> 除了使用ConvertPcap工具，还可以使用sniftran工具，该工具可以在Wireshark中显示报文的出接口和入接口。请参考“故障排查→Sniffer工具→Wireshark显示抓包接口和方向 ↗”章节。

1. 通过 `diagnose sniffer packet any "xxxx" 6` 抓取报文内容，保存为txt文本格式。



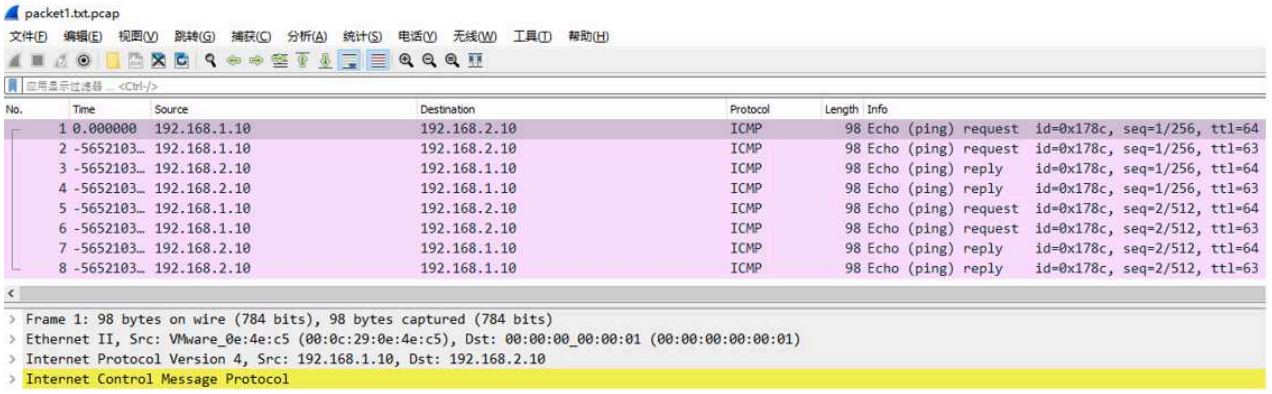
2. 安装“ConvertPcap.exe”，然后右击txt文本格式的报文，选择Convert to PACP完成数据格式的转换。

3. 安装完成后，右键点击要转换格式的抓包txt文件，点击Convert to PCAP，即可在当前目录自动生成转换后的Wireshark可打开的抓包文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.







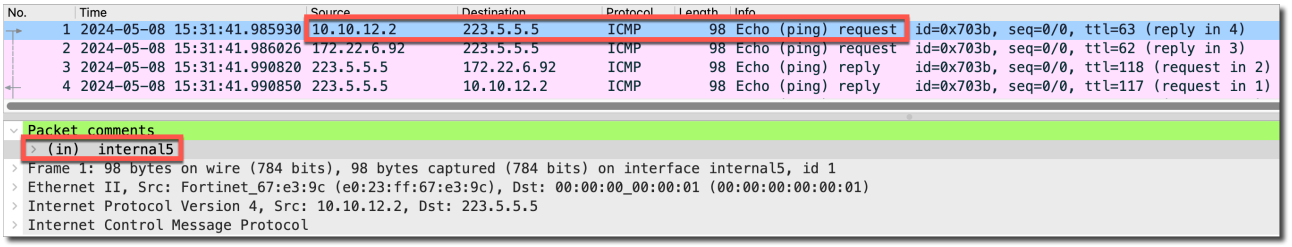
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

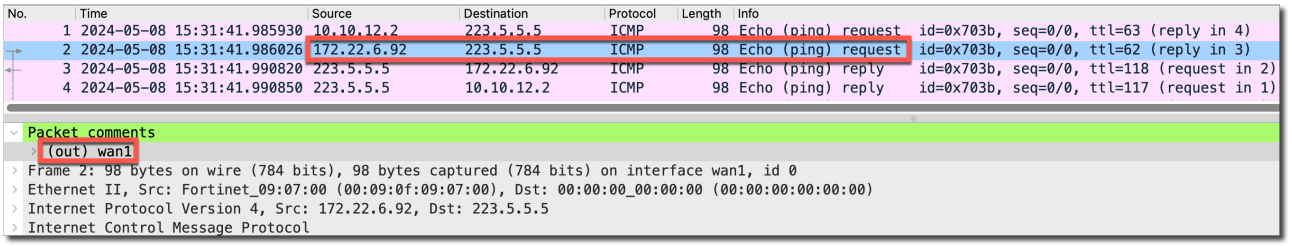
Wireshark显示抓包接口和方向

工具介绍

在“故障排查→Sniffer工具→使用Wireshark打开抓包文件”章节中，使用抓包转换工具ConvertPcap可以将Sniffer格式6抓到的文本转换为Wireshark可以打开的文件格式，但转换后的Wireshark格式中没有报文的接口与方向（in/out）信息。

如果需要同时将Sniffer格式6抓到的文本中的接口与方向（in/out）信息同步到转换后的Wireshark文件中，可以使用SnifTran工具，转换后的抓包文件如下所示，可以显示每个报文的接口与方向（in/out）信息。





SnifTran工具下载

本地下载

点击下载：sniftran-master.zip

GitHub下载

https://github.com/ondrejholecek/sniftran

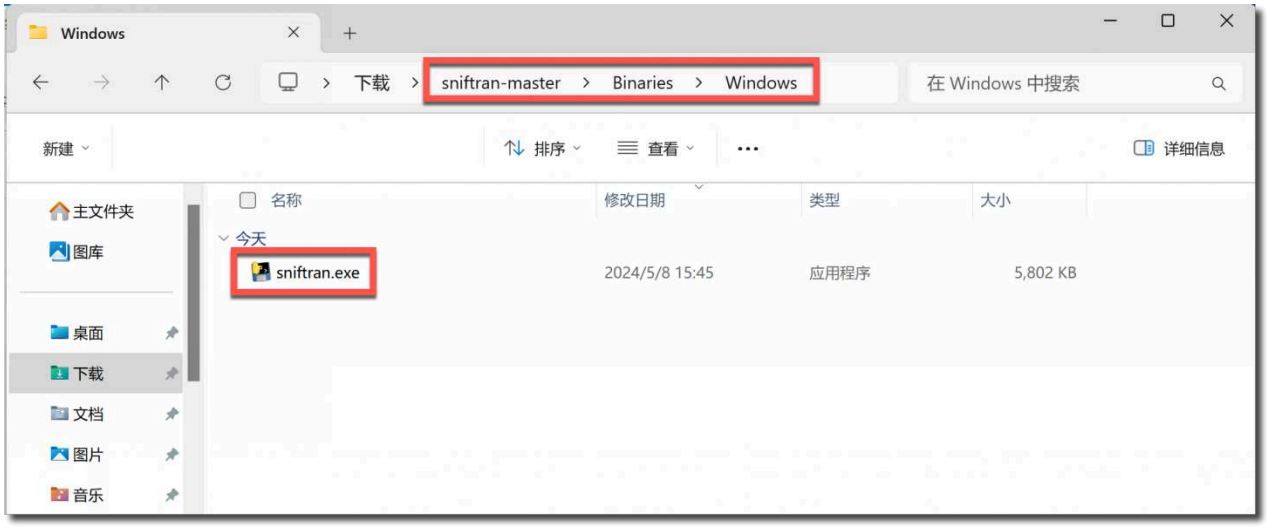
使用方法

提前准备好使用Sniffer格式6抓到的文本文件。

Windows

1. 下载 `sniftran-master.zip` 文件并解压，在 `sniftran-master/Binaries/Windows` 文件夹中，将 `sniftran.exe` 文件复制到一个特定目录下。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 这里将 `sniftran.exe` 文件复制到了 `D:\sniftran\` 目录下。

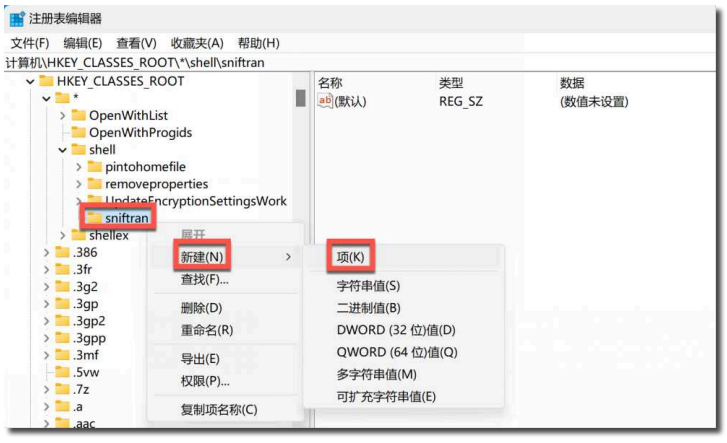
3. 使用win + R键打开运行窗口，输入regedit，然后点击“确定”按钮，打开注册表。



4. 找到 `计算机\HKEY_CLASSES_ROOT\*\shell` 路径，右键 `shell` 文件夹，点击“新建(N)”→“项(K)”。

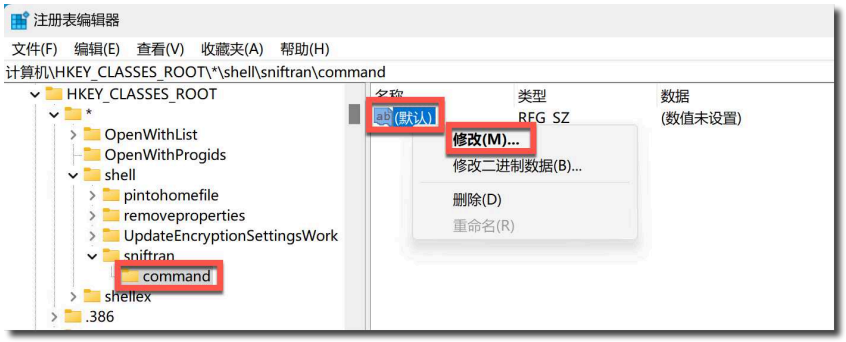


5. 为新的“项”命名 `sniftran` （或其他名称）。右键新创建的 `sniftran` 文件夹，点击“新建(N)”→“项(K)”。



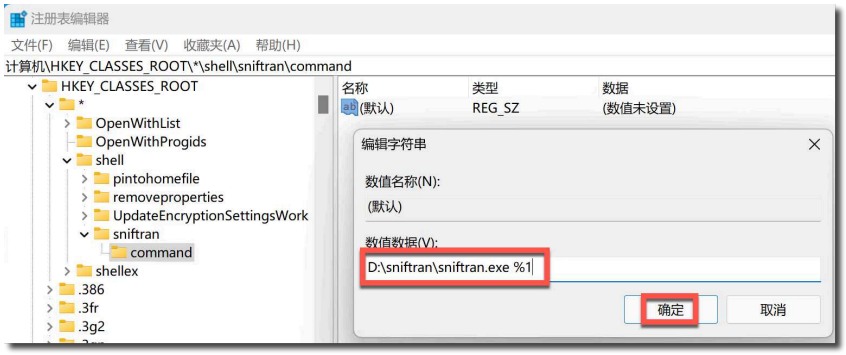
6. 为新的“项”命名 `command` ，选中 `command` 文件夹，在右侧窗口中右键点击“默认”条目，点击“修改(M)...”按钮。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

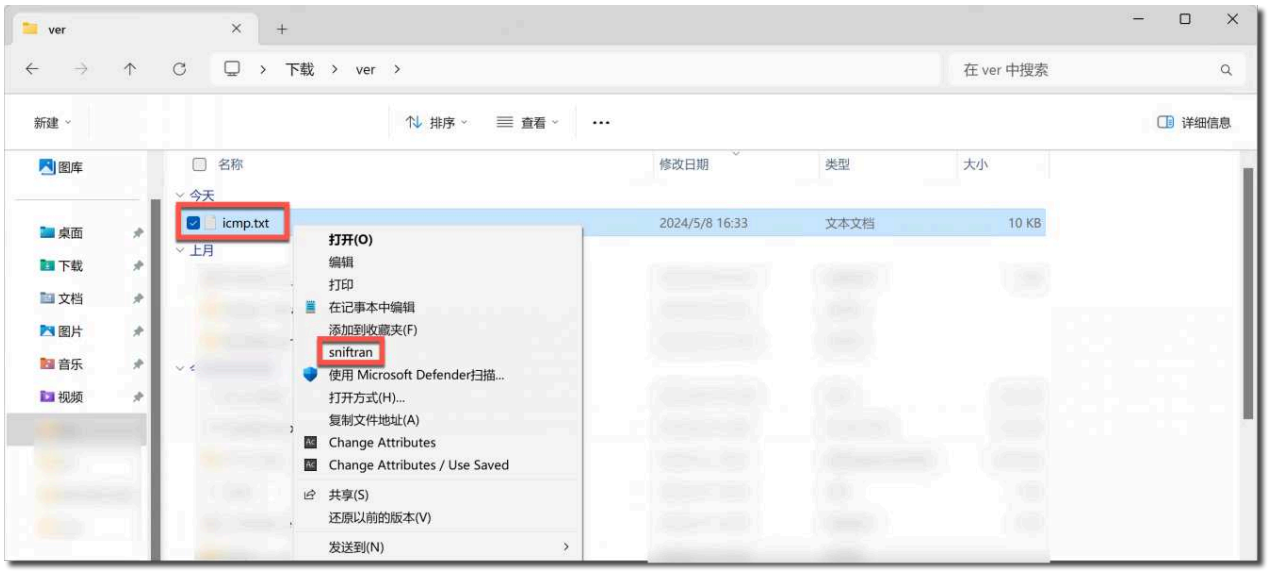


7. 在“编辑字符串”窗口中的“数值数据(V)”中填入`D:\sniftran\sniftran.exe %1`，然后点击“确定”按钮。

> **重要**
>
> `D:\sniftran\sniftran.exe`是sniftran.exe文件所在的路径，请根据您自己文件的路径修改。

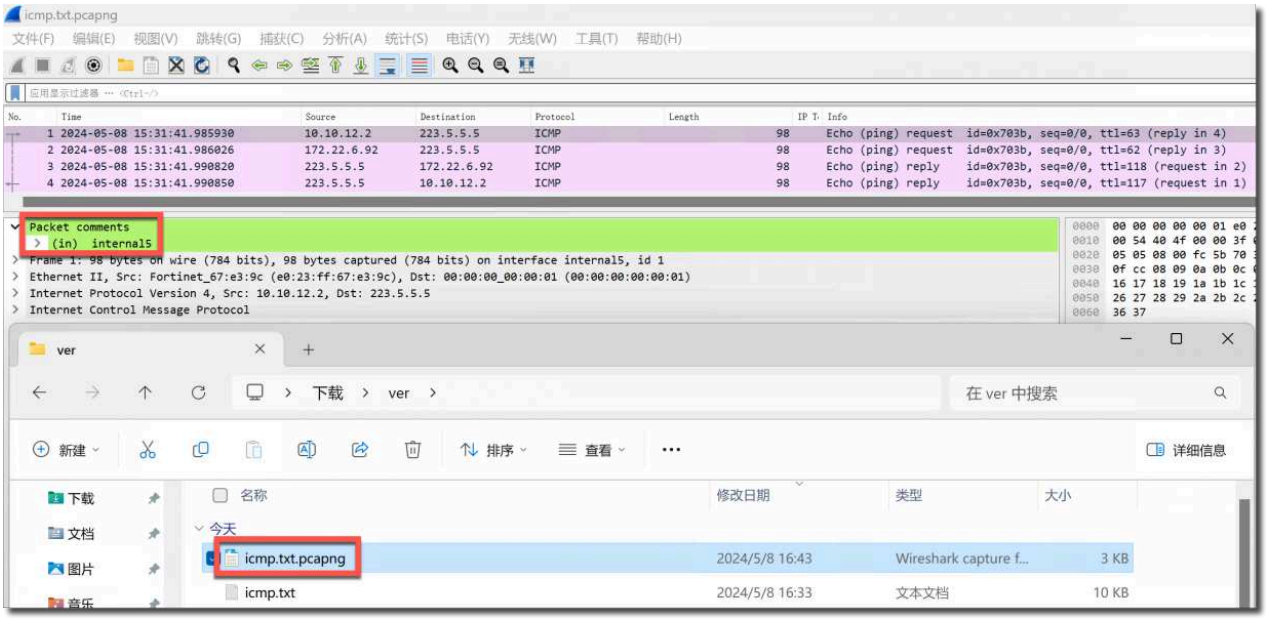


8. 右键点击需要转换格式的抓包文本文件，点击`sniftran`按钮（Windows 11需要先点击“显示更多选项”）。



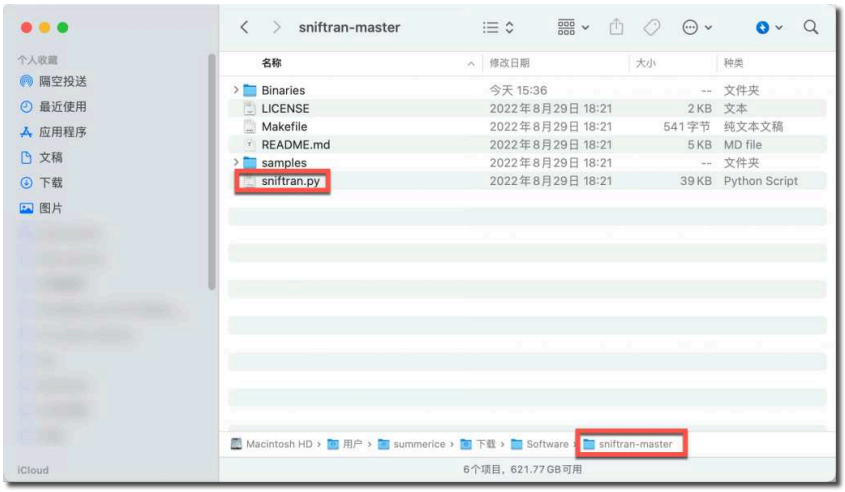
9. 随后会在当前目录下生成转换后的抓包文件，使用Wireshark打开后，可以显示每个报文的接口与方向（in/out）信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



macOS

1. 由于macOS预装了Python，可以直接使用SnifTran工具中的`sniftran.py`脚本执行转换。下载sniftran-master.zip文件并解压，在`sniftran-master`文件夹中，将`sniftran.py`文件复制到一个特定目录下。



2. 这里将`sniftran.py`文件复制到了`/Users/summerice/Tools`目录下。

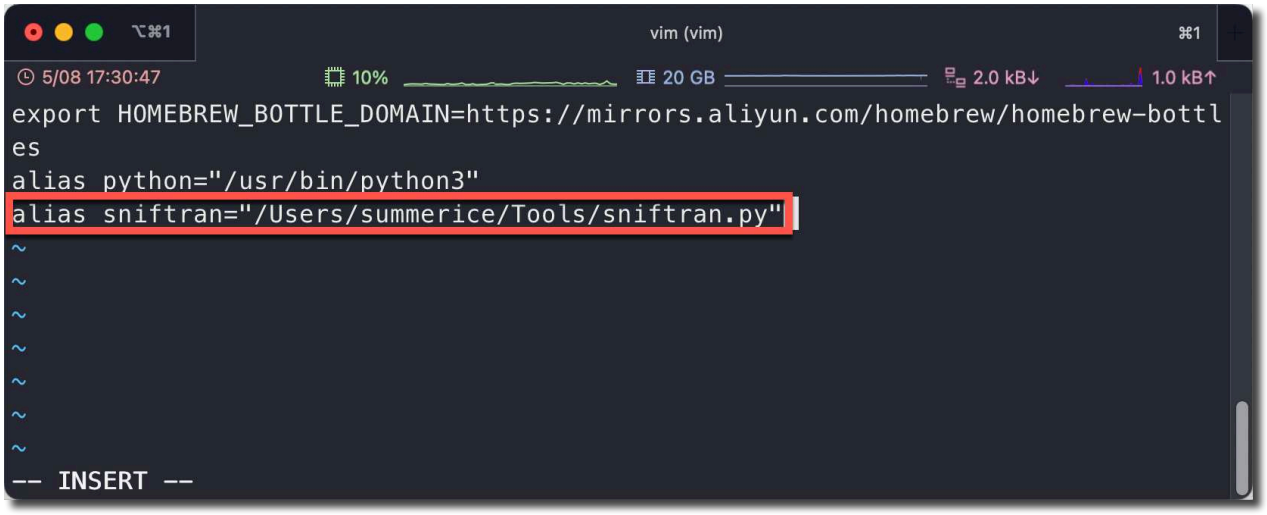
3. 将`sniftran.py`文件加入系统变量，在终端中编辑`~/.bash_profile`文件。

> **重要**
>
> 如果系统终端使用的是zsh，请编辑`~/.zshrc`文件。

```bash
vim ~/.bash_profile
```

4. 添加一行`alias sniftran="/Users/summerice/Tools/sniftran.py"`，其中`sniftran`为系统变量名称，可以自行定义，`"/Users/summerice/Tools/sniftran.py"`为`sniftran.py`文件所在路径，随后保存该文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

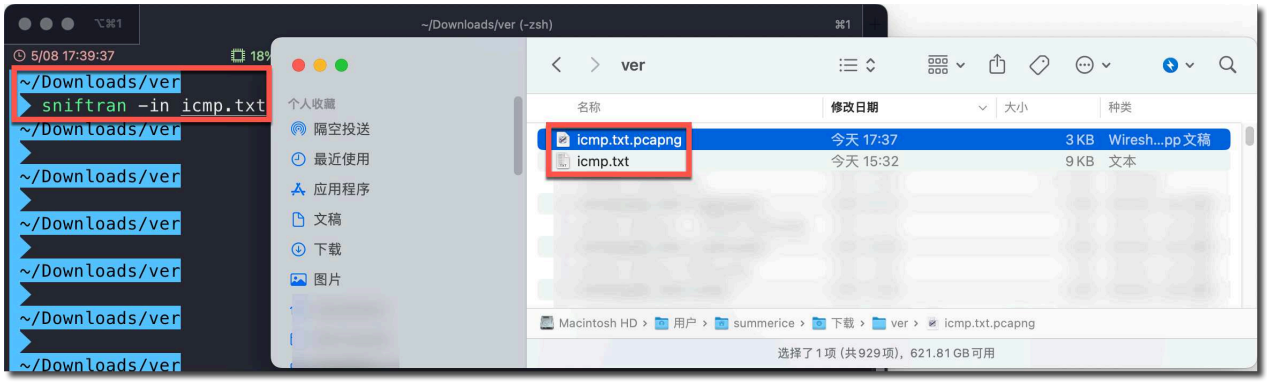


5. 使用`source`命令应用系统变量的修改。

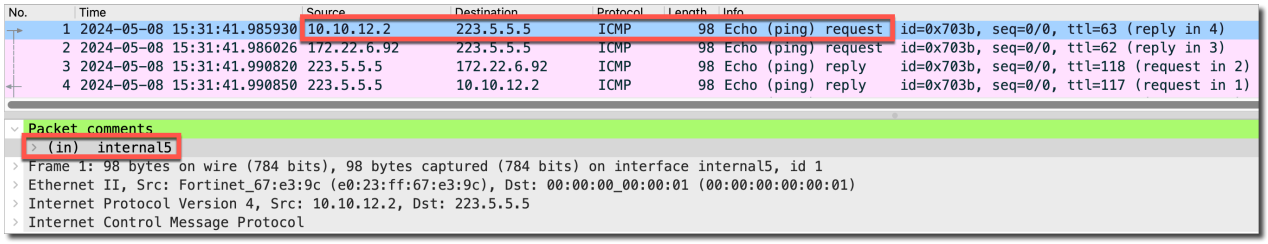
```bash
source ~/.bash_profile
```

> **重要**
>
> 如果系统终端使用的是zsh，请使用`source ~/.zshrc`文件。

6. 在终端中进入需要转换格式的抓包文本文件所在目录，使用命令`sniftran -in <file_name>`将文本转换为Wireshark可以打开的抓包文件。



7. 随后会在当前目录下生成转换后的抓包文件，使用Wireshark打开后，可以显示每个报文的接口与方向（in/out）信息。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

通过GUI界面抓包

功能介绍

除了通过在CLI下捕获数据包，FortiGate也支持在GUI界面捕获数据包，捕获的数据包下载后可以直接用Wireshark打开（PCAP格式），方便不熟悉Sniffer工具的用户使用。

使用方法

重要

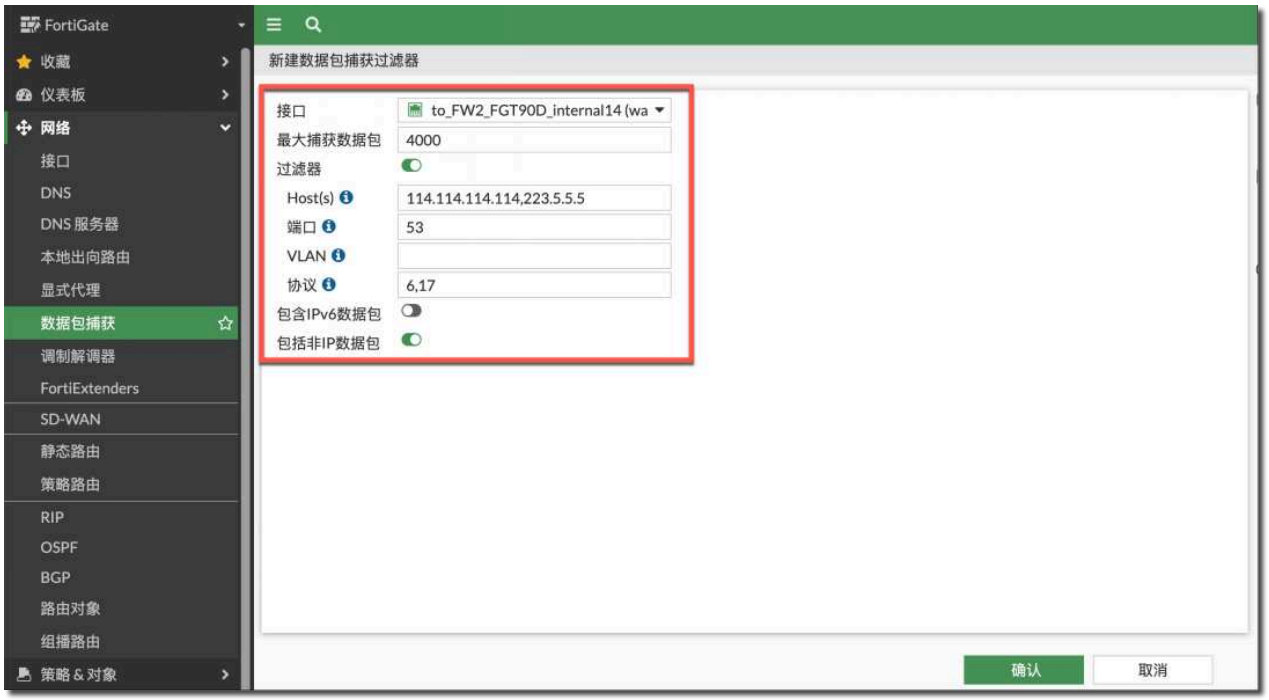
抓包之前，必须在抓取流量对应的防火墙策略上禁用NPU硬件加速才能查看所有数据包，请在CLI中将对应防火墙策略中的“auto-asic-offload”设置为“disable”。详情参考：故障排查→Sniffer、Debug Flow与NP加速的矛盾 ↗。

FortiOS 7.0

1. 进入“网络→数据包捕获”页面，点击“新建”按钮。



2. 设置捕获数据包的条件，并点击确认下发配置。



- 接口：指定抓取数据包的接口，无法指定any，如果接口开启了SNAT，抓取到的为SNAT后的数据包。
- 最大捕获数据包：每个数据包捕获可以抓取的最大数据包个数，达到该数字后，抓包自动停止（不同型号之间的最大捕获数量可能不同）。
- Host：抓取数据包过滤的源或目的IP地址/网段，可以填写多个IP地址/网段（网段的格式为192.168.1.0/24），中间用英文逗号（,）隔开，它们之间是或的关系。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 端口：过滤抓取数据包的端口号，可填写多个，中间用英文逗号（,）隔开，它们之间是或的关系。
- VLAN：如果要过滤抓取的数据包的VLAN ID，可以配置此选项，可填写多个，中间用英文逗号（,）隔开，它们之间是或的关系。
- 协议：过滤抓取数据包的协议号，可填写多个，中间用英文逗号（,）隔开，它们之间是或的关系。
- 包含IPv6数据包：默认只抓取IPv4数据包，需要抓取IPv6时，开启此选项。
- 包括非IP数据包：默认只抓取包含IP头的数据包，如果想抓取不含IP头的数据包（如ARP报文），开启此选项。

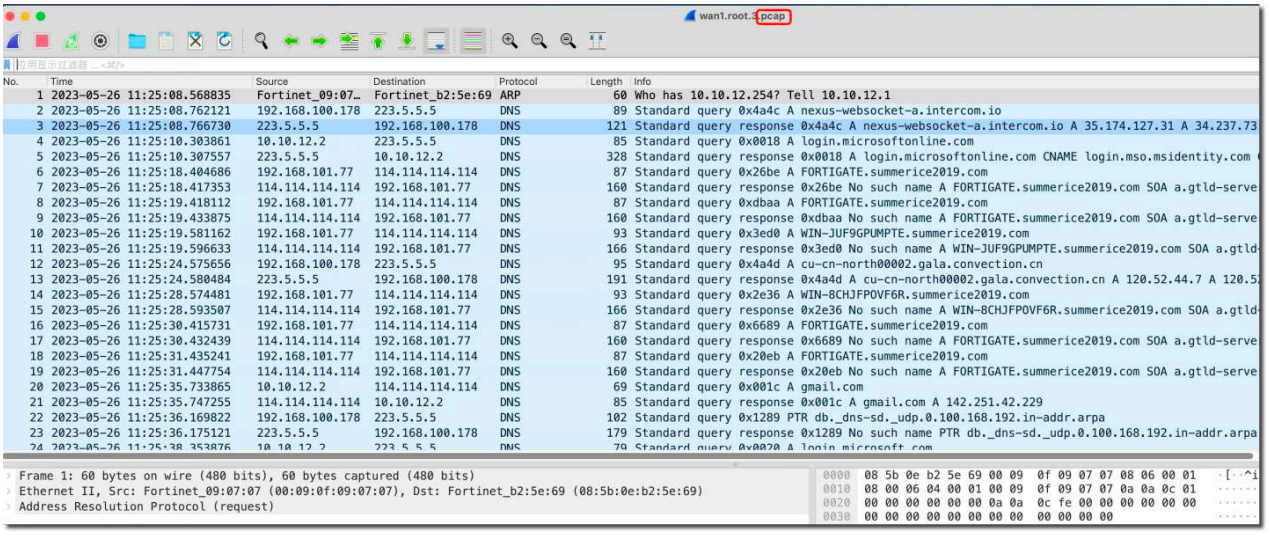
3. 右键点击创建的抓包进程，点击“开始”按钮，开启抓包，页面会显示抓包运行状态与已捕获的数据包个数。



4. 抓包完成后，右键点击该抓包进程，可以选择停止抓包，也可以不停止抓包，直接下载当前已捕获的数据包。

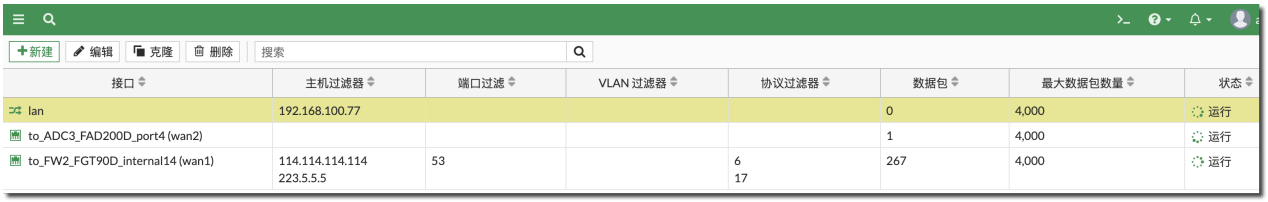


5. 下载的数据包为PCAP格式，可以直接用Wireshark打开并分析。



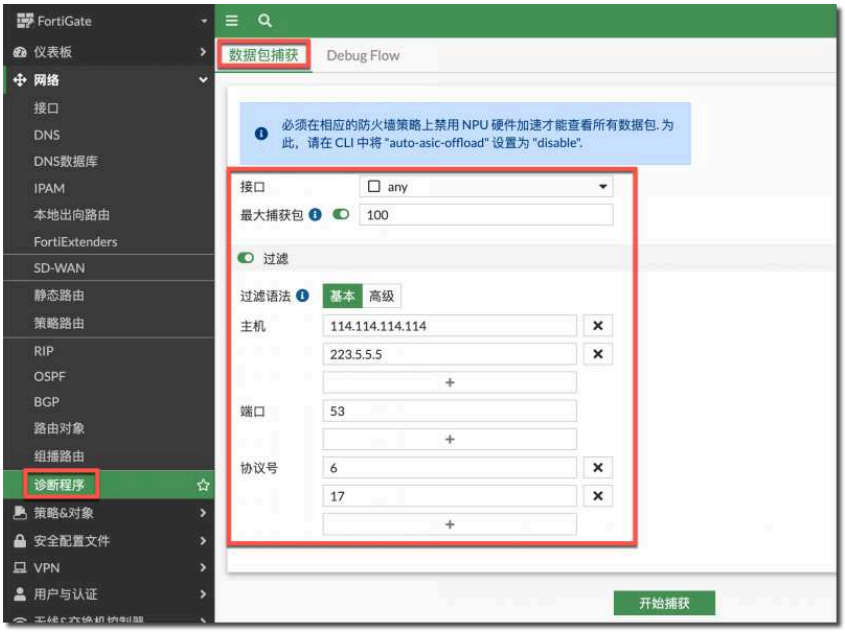
6. 同时可以创建多个抓包进程在后台抓取报文，离开此页面或登出设备不会中断抓包进程。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



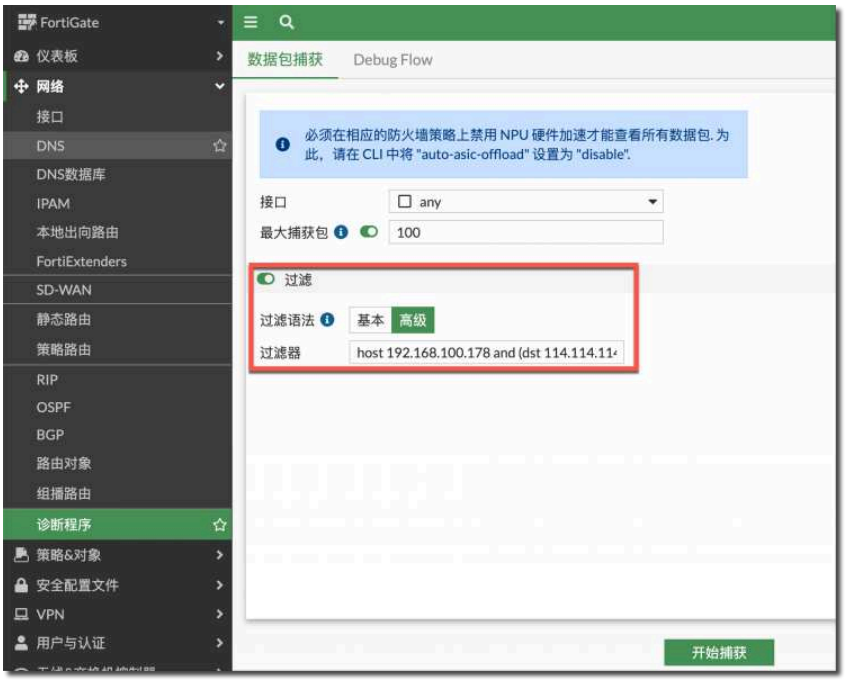
FortiOS 7.2

1. 进入“网络→诊断程序→数据包捕获”页面，配置捕获数据包的过滤条件，过滤语法选择基本时，可以过滤如下条件。



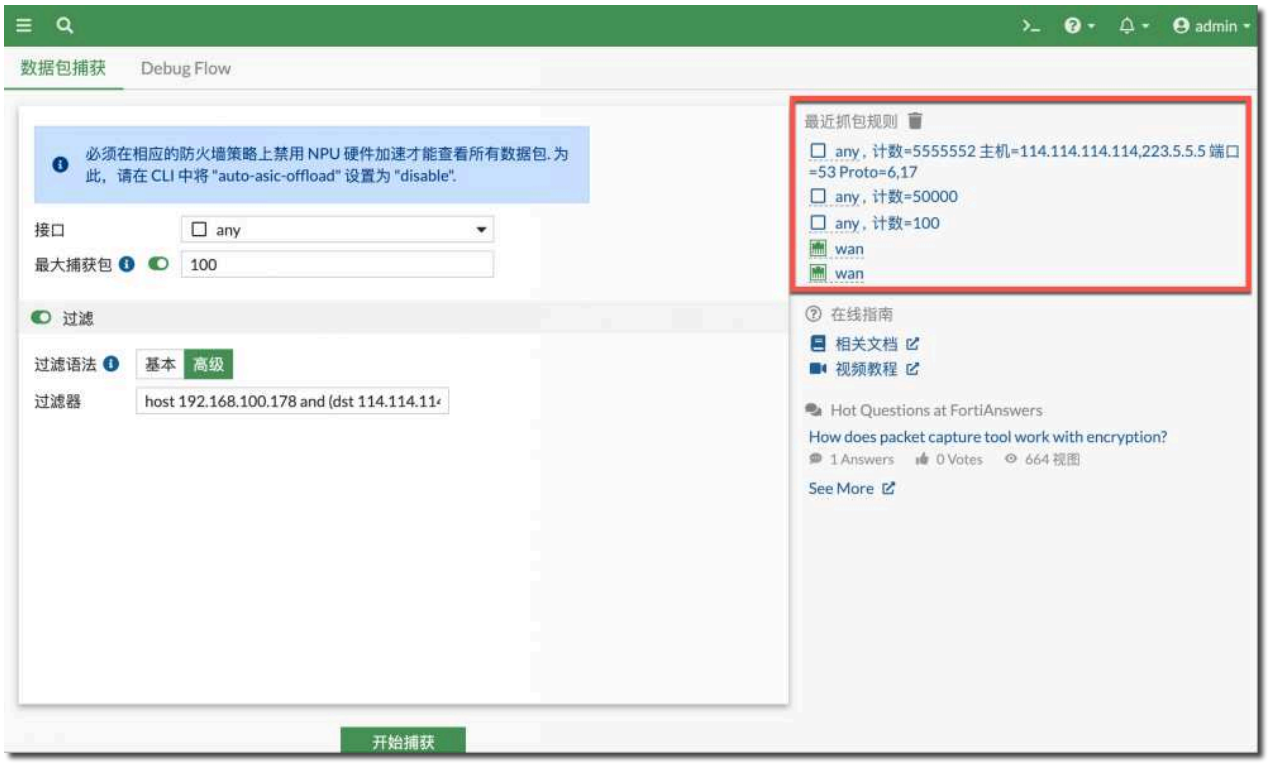
- 接口：指定抓取数据包的接口，可以指定any，如果接口开启了SNAT，抓取到的为SNAT后的数据包。
- 最大捕获数据包：每个数据包捕获可以抓取的最大数据包个数，达到该数字后，抓包自动停止，如果不指定最大捕获数量，默认在抓取50000个数据包后停止。
- Host：抓取数据包过滤的源或目的IP地址/网段，可以填写多个IP地址/网段（网段的格式为192.168.1.0/24），它们之间是或的关系。
- 端口：过滤抓取数据包的端口号，可填写多个，它们之间是或的关系。
- 协议号：过滤抓取数据包的协议号，可填写多个，它们之间是或的关系。

2. 过滤语法选择高级时，可以使用CLI下Sniffer命令中的过滤条件语法作为过滤条件（参考故障排查→Sniffer工具→Sniffer工具介绍↗），例如“*host 192.168.100.178 and (dst 114.114.114.114 or dst 223.5.5.5)* ”。

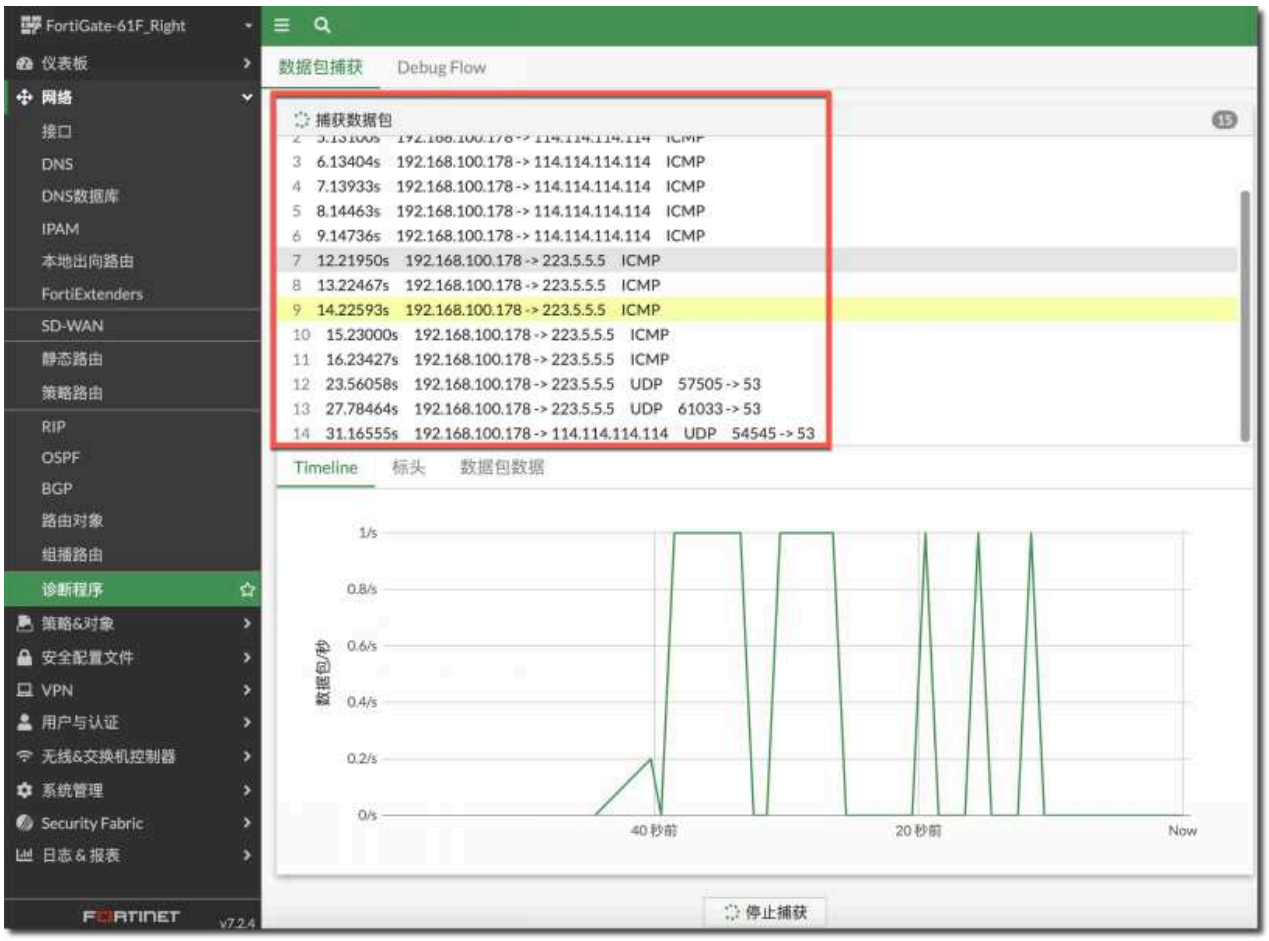


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

3. 页面右侧可以选择最近使用过的抓包规则。

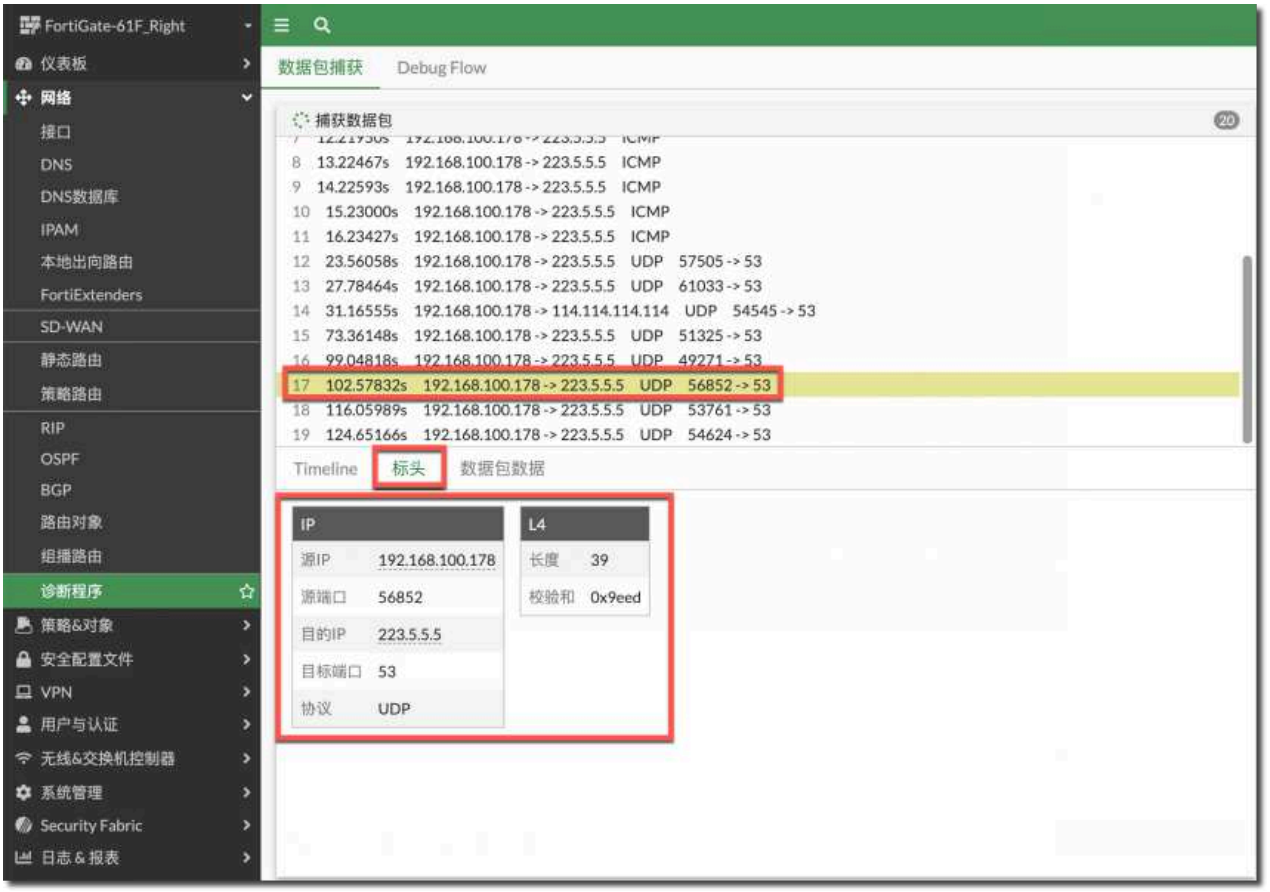


4. 点击“开始捕获”按钮开启抓包，可以看到数据包捕获的基本信息，以及对应的捕获速率。

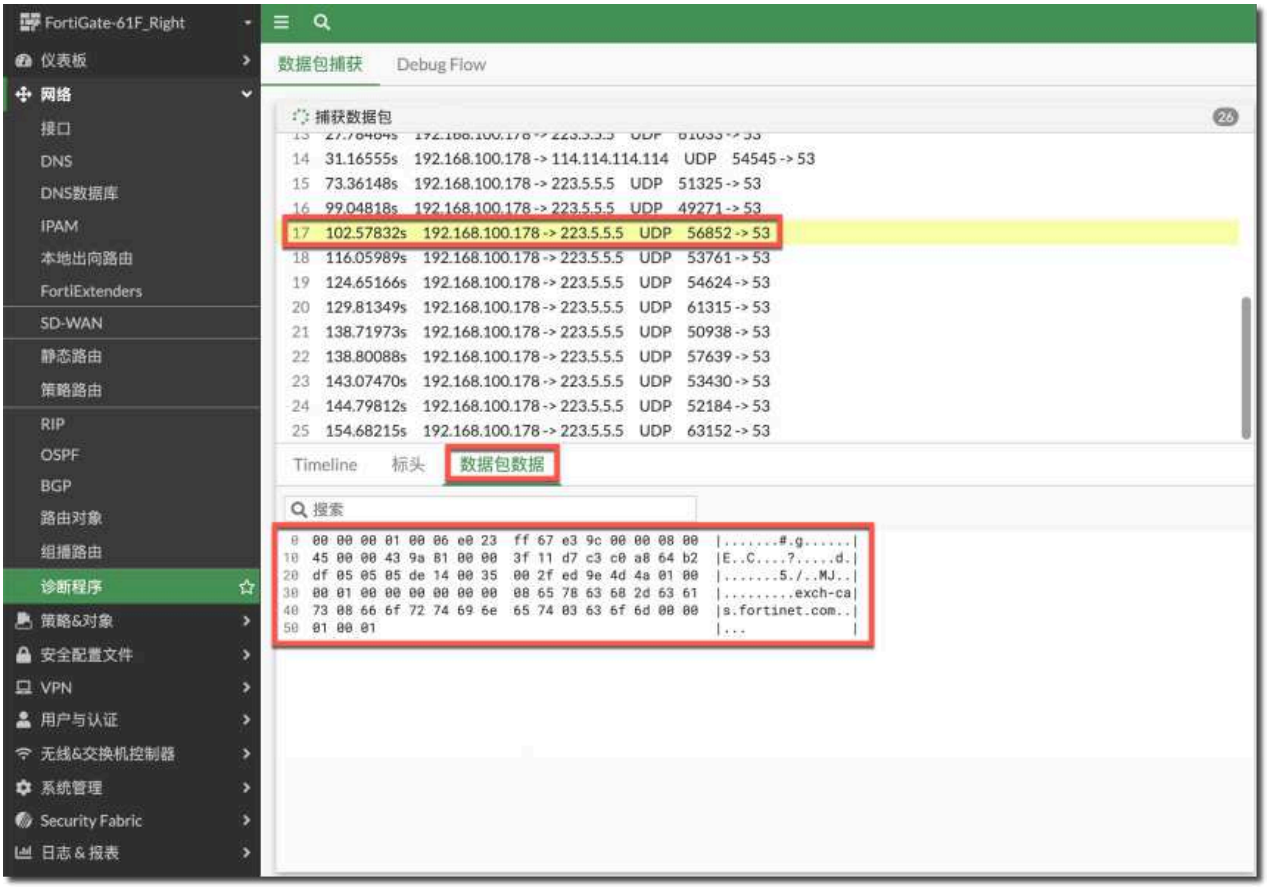


5. 选择某个数据包，点击“标头”，可以看到数据包的Header信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

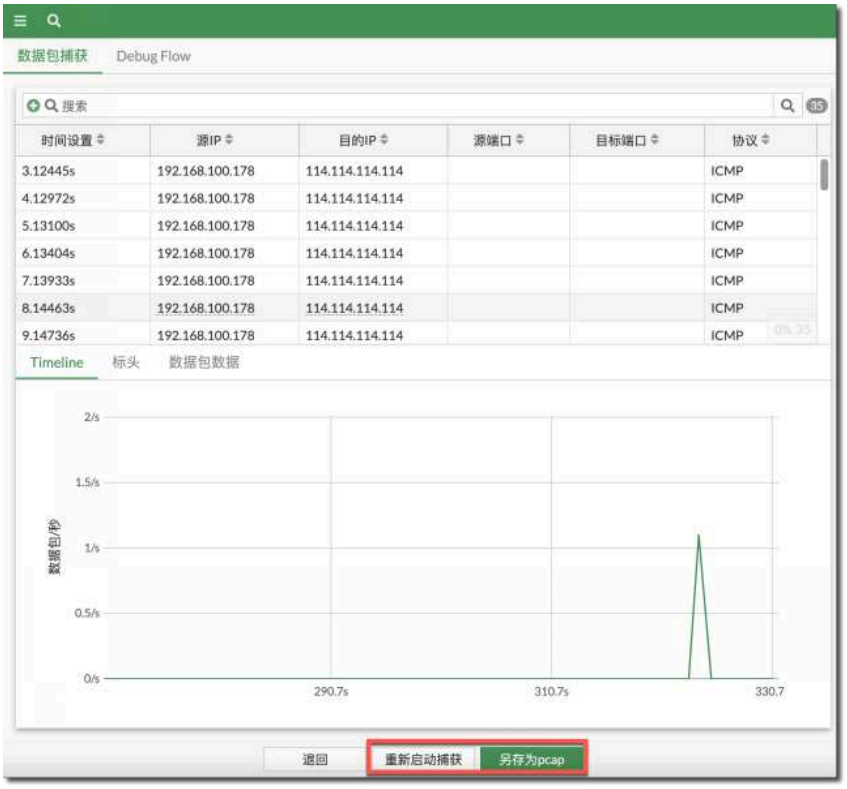


6. 选择某个数据包，点击“数据包数据”，可以看到数据包的具体Data内容。



7. 抓包自动停止或手动点击“停止捕获”，可选择重新启动捕获，或将已捕获的数据包另存为PCAP格式以供使用Wireshark进一步分析，退出后，已捕获的数据包不会存储在FortiGate上。

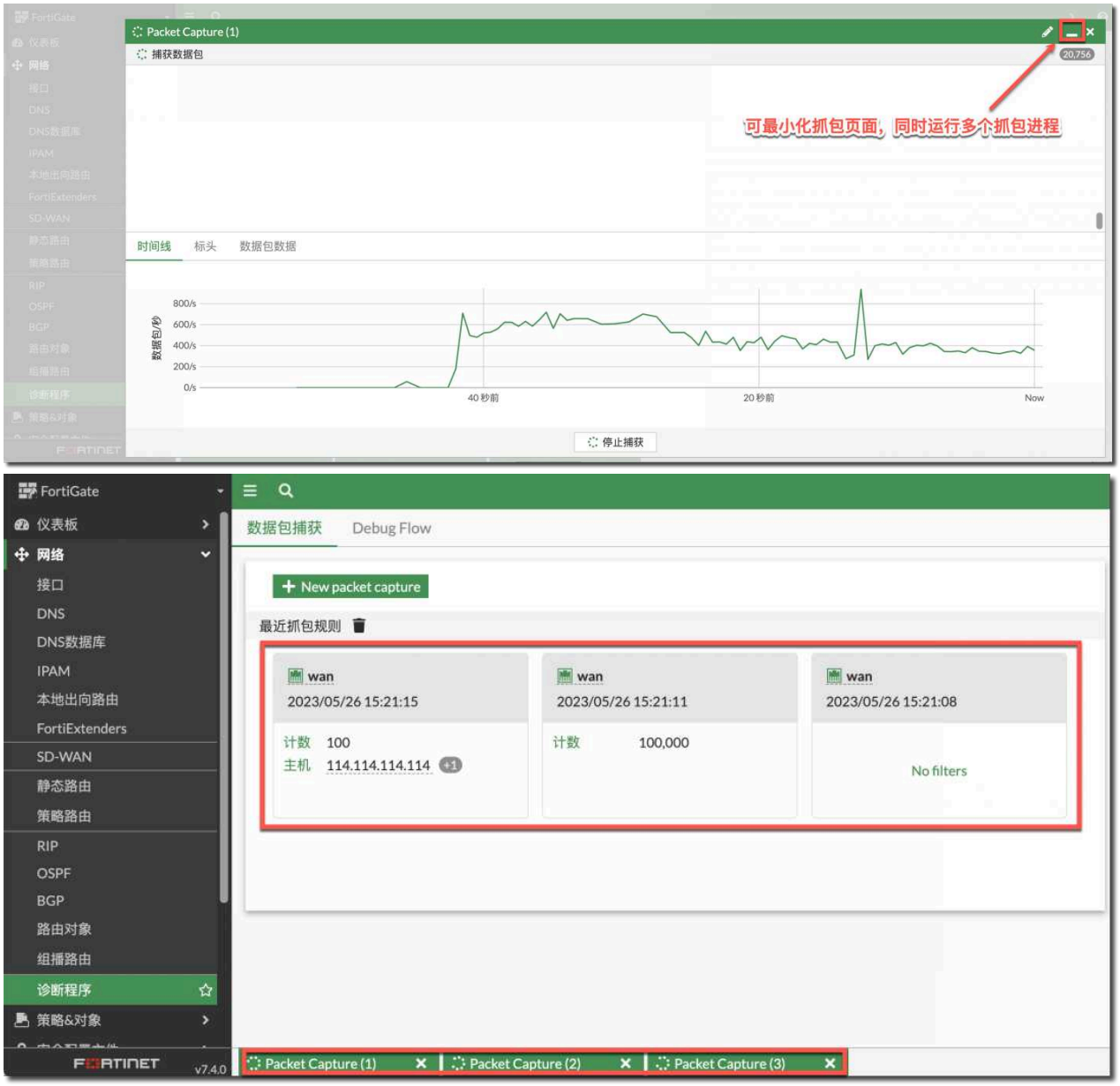
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



FortiOS 7.4

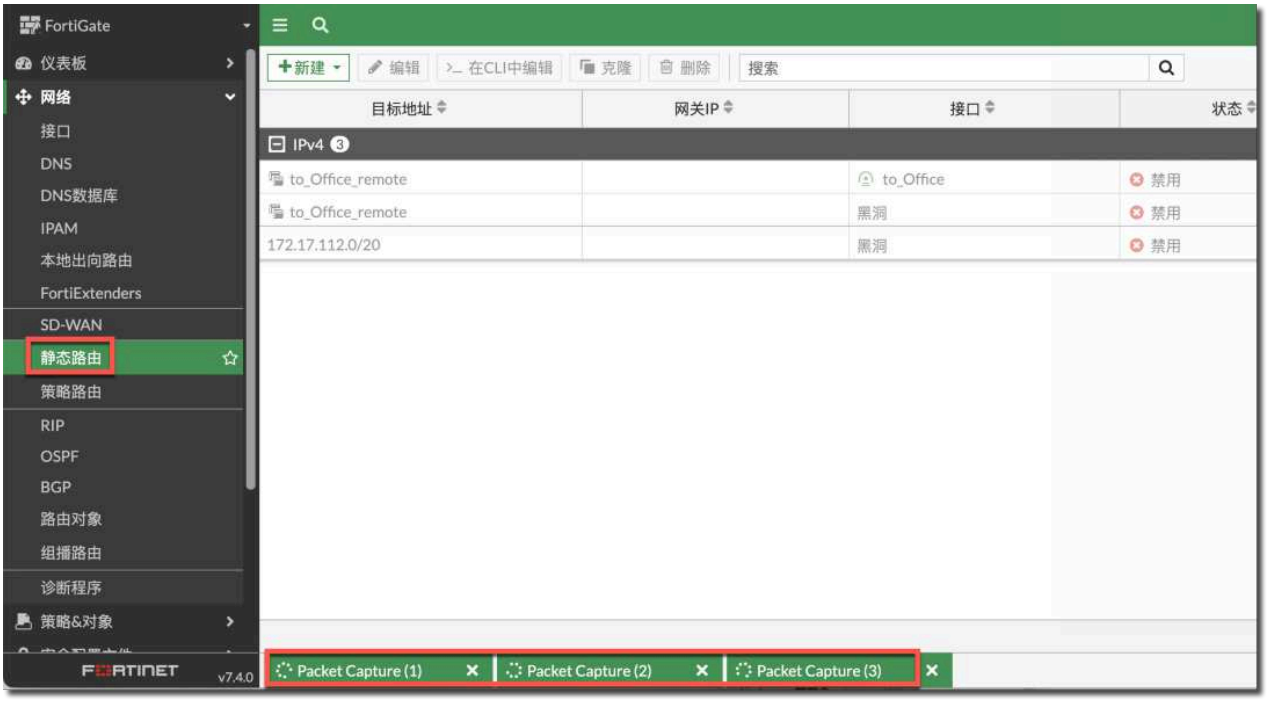
1. FortiOS 7.4 GUI的抓包方法与FortiOS 7.2一致，相比较FortiOS 7.2，FortiOS 7.4可以同时进行多个抓包进程，且可以将多个抓包进程最小化到页面下方。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

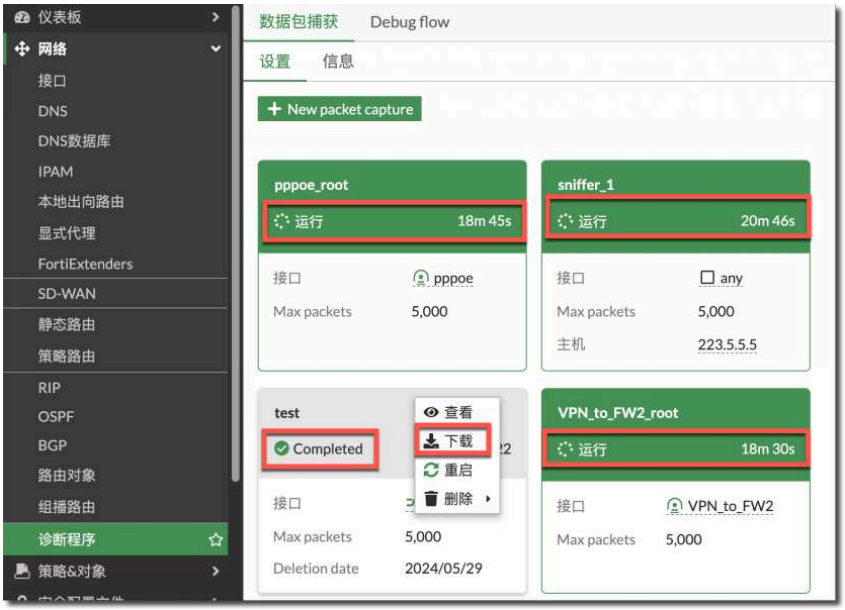


2. 离开“诊断程序”页面后，抓包进程仍然可以继续运行。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

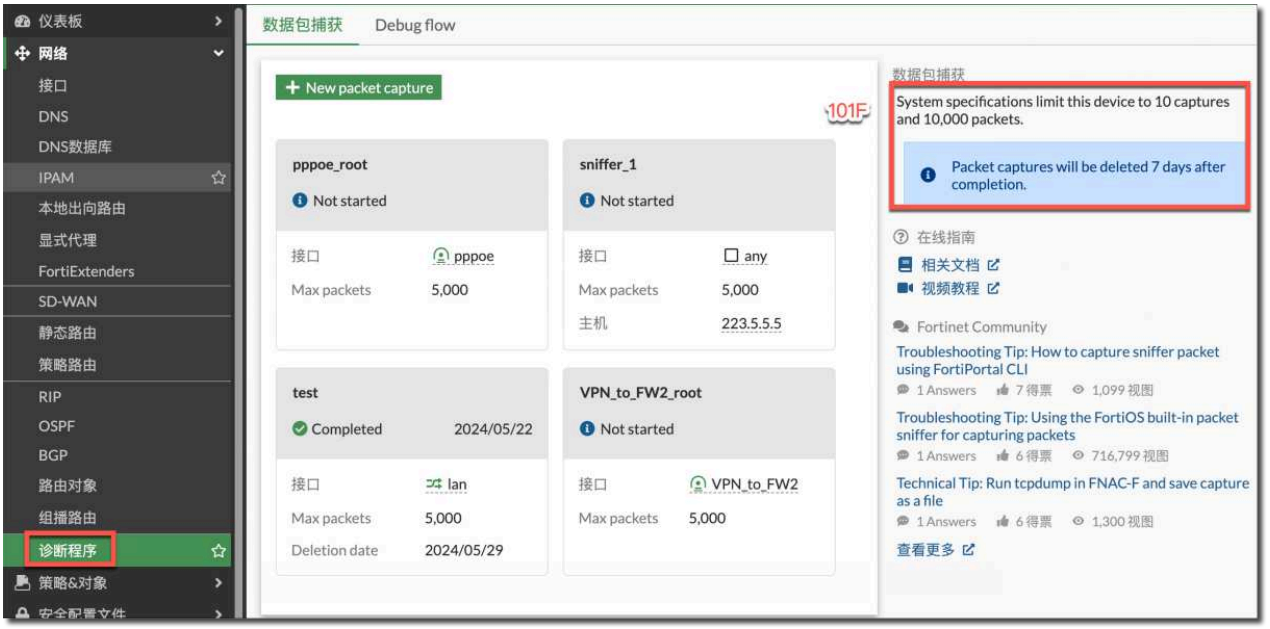


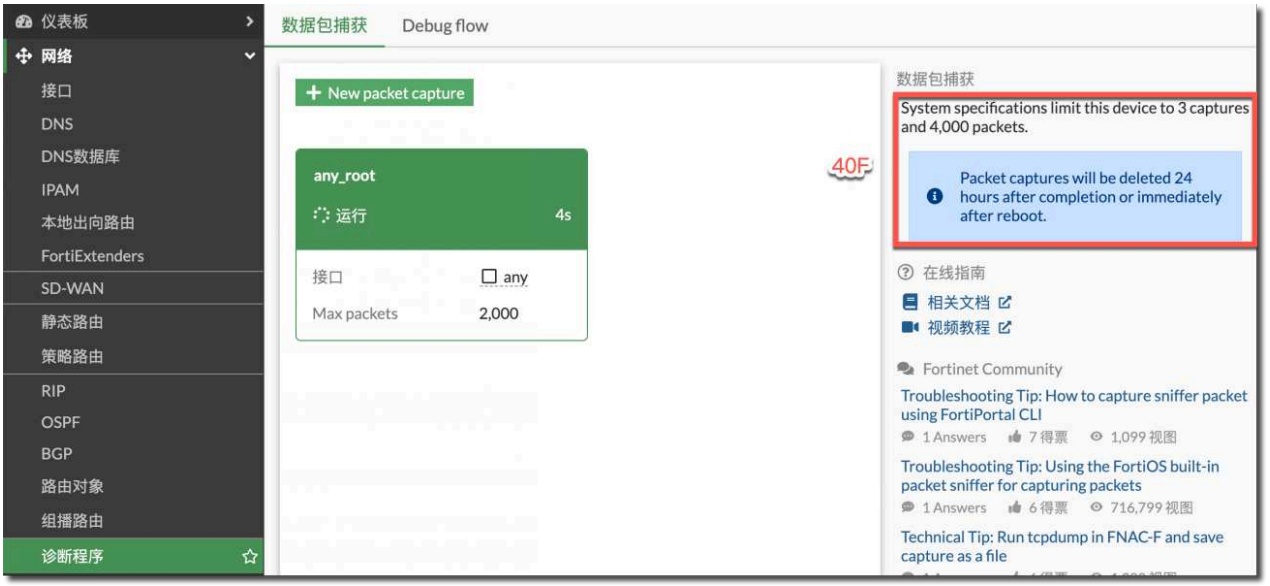
3. 退出登录或刷新页面后，页面下方的抓包窗口会消失，但回到“网络→诊断程序”页面后，抓包进程仍在进行中，已保存的抓包文件不会消失。



4. 重启设备后，带硬盘的设备（如101F）可以保留已结束的抓包文件，不带硬盘的设备（如60F）会删除已结束的抓包文件。不同型号FortiGate具体抓包规格和抓包文件最大保存天数可以参考“网络→诊断程序”页面右侧的提示信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

NP7芯片抓包

功能简介

当使用NP7平台芯片的设备（如400F、600F、1000F、1801F等）时，可以在数据流已经被NP7加速的情况下直接抓包，而不像NP6那样必须关闭流量匹配策略的NP加速后在CPU抓包。另外，也可以在NP7芯片上将过滤出的流量镜像到指定设备接口上。

```bash
diagnose npu sniffer {start | stop | filter}
```

过滤条件

必须指定过滤条件后才可以开启抓包，使用`diagnose npu sniffer filter`可以定义NP7抓包的过滤条件，可以过滤的选项如下：

- `selector`：用于保存过滤条件，最多可以创建4个selector（0 ~ 3，默认为0）。每个selector可以保存一套过滤条件。使用`diagnose npu sniffer filter selector <0 ~ 3>`可以切换到对应的selector进行设置，用于当一个selector无法表示出全部的过滤条件时使用。多个selector下的过滤条件为或（or）的关系，同时生效。
- `intf <interface-name>` ：过滤抓包接口，可以抓取除IPsec VPN隧道接口以外的任何接口上的流量。
- `dir {0 | 1 | 2}`：过滤数据包在接口上的方向。0表示入向数据包，1表示出向数据包，2表示双向数据包（默认为2）。
- `ethtype <type>`： 如果抓取二层数据包，过滤数据包二层ethertype值。
- `protocol <number>`：过滤抓包的IP协议号，范围为0 ~ 255。只能抓取到NP7处理器可以卸载的协议报文。
- `srcip <ipv4-ip-address>/<ipv4-mask>` ：过滤抓包的IPv4源地址/掩码。
- `dstip <ipv4-ip-address>/<ipv4-mask>`：过滤抓包的IPv4目的地址/掩码。
- `ip <ipv4-ip-address>/ 与<ipv4-mask>`：过滤抓包的IPv4源或目的地址/掩码。
- `srcip6 <ipv6-ip-address>/<ipv6-mask>`：过滤抓包的IPv6源地址/掩码。
- `dstip6 <ipv6-ip-address>/<ipv6-mask>`：过滤抓包的IPv6目的地址/掩码。
- `ip <ipv6-ip-address>/ 与<ipv6-mask>`：过滤抓包的IPv6源或目的地址/掩码。
- `sport <port-number>`：过滤抓包的4层源端口。
- `dport <port-number>`：过滤抓包的4层目的端口。
- `port <port-number>`：过滤抓包的4层源或目的端口。
- `outgoing_intf <interface>`：如果需要将抓取的报文镜像到设备的指定接口，在这里设置镜像的目标接口。
- `outgoing_vlan <vlan-id>`：如果镜像的目标接口需要封装VLAN tag传输，在这里设置镜像的目标接口的VLAN ID。
- `clear`：清空所有selector的过滤条件。

开启/关闭NP7抓包

配置好过滤条件后，使用`diagnose npu sniffer {start | stop}`在NP7上开始或停止抓包，然后使用`diagnose sniffer packet npudbg`显示抓取的数据包。

> **重要**
>
> 可根据需求抓取4还是6格式的报文，并指定抓包数量与时间显示方式，如下所示，这里的参数与普通sniffer是一样的。

```bash
diagnose npu sniffer {start | stop}
diagnose sniffer packet npudbg '' 4 0 l
```

NP7抓包示例

单一selector

```bash
diagnose npu sniffer filter
diagnose npu sniffer filter intf port23
diagnose npu sniffer filter dir 1
diagnose npu sniffer filter protocol 6
diagnose npu sniffer start
diagnose sniffer packet npudbg '' 4 0 l
```

- 首先清除所有的抓包过滤器。
- 过滤接口为port23。
- 过滤流量方向为出方向。
- 过滤协议为TCP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

- 开启抓包。
- 在CLI下显示抓到的数据包。

多个selector

```bash
diagnose npu sniffer filter selector 0
diagnose npu sniffer filter intf port1
diagnose npu sniffer filter protocol 6
diagnose npu sniffer filter dir 2
diagnose npu sniffer filter selector 1
diagnose npu sniffer filter intf port2
diagnose npu sniffer filter protocol 17
diagnose npu sniffer filter dir 1
diagnose npu sniffer start
diagnose sniffer packet npudbg '' 4 0 l
```

- 第1个selector 0：抓取port1上的双向TCP数据包。
- 第2个selector 1：抓取port2上的出向UDP数据包。
- 在CLI下显示经过这两个selector过滤后抓到的数据包。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Debug Flow介绍

Debug Flow 通常用于定位调试穿过或访问FortiGate数据流的处理过程，对于定位问题有很大的帮助。

命令解析

```bash
diagnose debug flow filter addr x.x.x.x          //过滤某个IP//
diagnose debug flow show function-name enable    //显示功能模块名称//
diagnose debug console timestamp enable          //显示时间戳//
diagnose debug flow trace start 10               //开启debug flow trace并显示10条debug信息//
diagnose debug enable                            //开启debug命令//
diagnose debug flow trace stop                   //关闭debug flow trace//
diagnose debug flow filter clear                 //清除过滤条件//
diagnose debug disable                           //关闭debug命令//
diagnose debug reset                             //重置所有的debug命令//
```

过滤条件

```bash
diagnose debug flow filter ?    //键入?查看Debug Flow支持的过滤条件，如IP，端口，协议等//
clear      Clear filter.
vd         Index of virtual domain.
vd-name    Name of virtual domain.
proto      Protocol number.
addr       IP address.
saddr      Source IP address.
daddr      Destination IP address.
port       port
sport      Source port.
dport      Destination port.
negate     Inverse filter.

diagnose debug flow filter    //直接键入回车查看当前的过滤条件//
        vf: any
        proto: any
        Host addr: any
        Host saddr: any
        Host daddr: any
        port: any
        sport: any
        dport: any

diagnose debug flow filter clear    //清除filter过滤条件//
```

Debug Flow配置

1. 拓扑：PC1(192.168.1.10)-----(port5：192.168.1.1)FGT(port1:192.168.89.35)-----Internet。

2. 策略配置。

```bash
config firewall policy
    edit 9
        set srcintf "port5"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

3. 设置Debug Flow，并使用PC1 ping 114.114.114.114。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
diagnose debug flow filter addr 114.114.114.114
diagnose debug flow filter proto 1
diagnose debug flow show function-name enable
diagnose debug console timestamp enable
diagnose debug flow trace start 10
diagnose debug enable
```

Debug Flow输出

1. 第1个数据包：Ping的请求报文echo reqeust。

```bash
2022-11-30 17:22:54 id=20085 trace_id=26 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
192.168.1.10:2280→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2280, seq=1."
//received a packet表示FortiGate从port5收到一个192.168.1.10到114.114.114.114的echo request报文//

2022-11-30 17:22:54 id=20085 trace_id=26 func=init_ip_session_common line=6024 msg="allocate a new session-
000e1480, tun_id=0.0.0.0"
//创建会话，会话id是000e1480//

2022-11-30 17:22:54 id=20085 trace_id=26 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000
gw-192.168.89.254 via port1"
//查找路由，该报文需要从port1转发出去//

2022-11-30 17:22:54 id=20085 trace_id=26 func=get_new_addr line=1221 msg="find SNAT: IP-192.168.89.35(from
IPPOOL), port-62696"
//需要执行源NAT//

2022-11-30 17:22:54 id=20085 trace_id=26 func=fw_forward_handler line=881 msg="Allowed by Policy-9: SNAT"
//报文匹配id是9的策略//

2022-11-30 17:22:54 id=20085 trace_id=26 func=__ip_session_run_tuple line=3471 msg="SNAT 192.168.1.10-
>192.168.89.35:62696"
//将数据包的源地址192.168.1.10转换为192.168.89.35并发出//
```

2. 第2个数据包：ping的响应报文 echo reply。

```bash
2022-11-30 17:22:54 id=20085 trace_id=27 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
114.114.114.114:62696→192.168.89.35:0) tun_id=0.0.0.0 from port1. type=0, code=0, id=62696, seq=1."
//received a packet表示FortiGate从port1收到一个114.114.114.114到的192.168.89.35 echo reply报文//

2022-11-30 17:22:54 id=20085 trace_id=27 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
000e1480, reply direction"
//匹配已创建的会话id-000e1480//

2022-11-30 17:22:54 id=20085 trace_id=27 func=__ip_session_run_tuple line=3484 msg="DNAT 192.168.89.35:0-
>192.168.1.10:2280"
//反向报文需要进行目的NAT转换，将192.168.89.35转换为PC1的真实IP 192.168.1.10//

2022-11-30 17:22:54 id=20085 trace_id=27 func=vf_ip_route_input_common line=2605 msg="find a route: flag=00000000
gw-192.168.1.10 via port5"
//查找路由，该报文需要从port5转发出去//

2022-11-30 17:22:54 id=20085 trace_id=27 func=npu_handle_session44 line=1183 msg="Trying to offloading session
from port1 to port5, skb.npu_flag=00000000 ses.state=00010200 ses.npu_state=0×04000000"
2022-11-30 17:22:54 id=20085 trace_id=27 func=fw_forward_dirty_handler line=410 msg="state=00010200,
state2=00000000, npu_state=04000000"
```

3. 第3个数据包：ping的请求报文 echo request直接匹配会话转发。

```
2022-11-30 17:22:55 id=20085 trace_id=28 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
192.168.1.10:2280→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2280, seq=2."
2022-11-30 17:22:55 id=20085 trace_id=28 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
000e1480, original direction"
2022-11-30 17:22:55 id=20085 trace_id=28 func=npu_handle_session44 line=1183 msg="Trying to offloading session
from port5 to port1, skb.npu_flag=00000400 ses.state=00010200 ses.npu_state=0×04000000"
2022-11-30 17:22:55 id=20085 trace_id=28 func=ip_session_install_npu_session line=346 msg="npu session
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
installation succeeded"
2022-11-30 17:22:55 id=20085 trace_id=28 func=fw_forward_dirty_handler line=410 msg="state=00010200,
state2=00000000, npu_state=04000400"
2022-11-30 17:22:55 id=20085 trace_id=28 func=__ip_session_run_tuple line=3471 msg="SNAT 192.168.1.10-
>192.168.89.35:62696"
```

4. 第4个数据包：ping的影响报文echo reply直接匹配会话转发。

```
2022-11-30 17:22:55 id=20085 trace_id=29 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
114.114.114.114:62696→192.168.89.35:0) tun_id=0.0.0.0 from port1. type=0, code=0, id=62696, seq=2."
2022-11-30 17:22:55 id=20085 trace_id=29 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
000e1480, reply direction"
2022-11-30 17:22:55 id=20085 trace_id=29 func=__ip_session_run_tuple line=3484 msg="DNAT 192.168.89.35:0-
>192.168.1.10:2280"
2022-11-30 17:22:55 id=20085 trace_id=29 func=npu_handle_session44 line=1183 msg="Trying to offloading session
from port1 to port5, skb.npu_flag=00000400 ses.state=00010200 ses.npu_state=0×04000400"
2022-11-30 17:22:55 id=20085 trace_id=29 func=ip_session_install_npu_session line=346 msg="npu session
installation succeeded"
2022-11-30 17:22:55 id=20085 trace_id=29 func=fw_forward_dirty_handler line=410 msg="state=00010200,
state2=00000000, npu_state=04000c00"
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Debug Flow排错举例

Denied by forward policy check (policy 0)

从Debug Flow输出发现192.168.1.10 ping 114.114.114.114 匹配了策略0（隐式丢包策略），即该数据包没有匹配的策略。

```bash
2022-11-30 18:16:43 id=20085 trace_id=30 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1, 192.168.1.10:2328→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2328, seq=1."
2022-11-30 18:16:43 id=20085 trace_id=30 func=init_ip_session_common line=6024 msg="allocate a new session-000e4d3d, tun_id=0.0.0.0"
2022-11-30 18:16:43 id=20085 trace_id=30 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-192.168.89.254 via port1"
2022-11-30 18:16:43 id=20085 trace_id=30 func=fw_forward_handler line=719 msg="Denied by forward policy check (policy 0)"
```

Denied by forward policy check (policy XX)

1. 从Debug Flow输出发现192.168.1.10 ping 114.114.114.114被policy 9丢弃。

```bash
2022-11-30 18:22:05 id=20085 trace_id=37 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1, 192.168.1.10:2335→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2335, seq=1."
2022-11-30 18:22:05 id=20085 trace_id=37 func=init_ip_session_common line=6024 msg="allocate a new session-000e5327, tun_id=0.0.0.0"
2022-11-30 18:22:05 id=20085 trace_id=37 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw-192.168.89.254 via port1"
2022-11-30 18:22:05 id=20085 trace_id=37 func=fw_forward_handler line=719 msg="Denied by forward policy check (policy 9)"
```

2. policy id 为9的策略如下。

```bash
config firewall policy
    edit 9
        set srcintf "port5"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic disable
        set action deny
    next
end
```

reverse path check fail, drop

1. 拓扑：PC1(192.168.5.10)-----(192.168.5.1)Router(192.168.1.2)-----(port5:192.168.1.1)FortiGate(port1:192.168.89.35)----Internet

2. FortiGate路由配置。

```bash
config router static
    edit 1
        set dst 0.0.0.0/0
        set gateway 192.168.89.254
        set device "port1"
    next
end
```

3. 从Debug Flow输出发现192.168.5.10 ping 114.114.114.114被反向路径检查丢弃，数据包是从port5接口收到的，FortiGate会检查port5接口是否有到源地址192.168.5.10的路由，如果没有，则将丢弃该报文。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
2022-11-30 19:02:32 id=20085 trace_id=38 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1, 192.168.5.10:2471→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2471, seq=1."
2022-11-30 19:02:32 id=20085 trace_id=38 func=init_ip_session_common line=6024 msg="allocate a new session-000e7d86, tun_id=0.0.0.0"
2022-11-30 19:02:32 id=20085 trace_id=38 func=ip_route_input_slow line=2267 msg="reverse path check fail, drop"
2022-11-30 19:02:32 id=20085 trace_id=38 func=ip_session_handle_no_dst line=6110 msg="trace"
```
bash

4. 解决方法：增加到192.168.5.0/24的路由。

```
config router static
    edit 2
        set dst 192.168.5.0/24
        set gateway 192.168.1.2
        set device "port5"
    next
end
```
bash

iprope_in_check() check failed on policy 0, drop

原因1

1. 访问一个防火墙上未开放的端口（包括自身管理端口/VIP端口等），如下port5接口只允许ping。

```
config system interface
    edit "port5"
        set ip 192.168.1.1 255.255.255.0
        set allowaccess ping
    next
end
```
bash

2. 从Debug Flow发现192.168.1.10访问FortiGate port5接口192.168.1.1的22端口被拒绝，因为port5没有允许SSH访问。

```
2022-11-30 19:27:23 id=20085 trace_id=52 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=6, 192.168.1.10:53814→192.168.1.1:22) tun_id=0.0.0.0 from port5. flag [S], seq 2134956194, ack 0, win 29200"
2022-11-30 19:27:23 id=20085 trace_id=52 func=init_ip_session_common line=6024 msg="allocate a new session-000eb1ae, tun_id=0.0.0.0"
2022-11-30 19:27:23 id=20085 trace_id=52 func=vf_ip_route_input_common line=2605 msg="find a route: flag=84000000 gw-192.168.1.1 via root"
2022-11-30 19:27:23 id=20085 trace_id=52 func=fw_local_in_handler line=500 msg="iprope_in_check() check failed on policy 0, drop"
```
bash

原因2

1. 访问FGT本机流量，接口下已经开启了此服务，但是配置了管理员可信任主机，可信任主机不包括发起访问的源IP，如下port5接口允许ping，ssh，同时配置管理主机为192.168.88.0/24网段。

```
config system interface
    edit "port5"
        set ip 192.168.1.1 255.255.255.0
        set allowaccess ping ssh
    next
end
config system admin
    edit "admin"
        set trusthost1 192.168.88.0 255.255.255.0
    next
end
```
bash

2. 从Debug Flow发现192.168.1.10访问FortiGate port5接口192.168.1.1的22端口被拒绝，因为FortiGate设置了信任主机，只允许192.168.88.0/24段的地址访问。

```
2022-11-30 19:35:13 id=20085 trace_id=58 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=6, 192.168.1.10:53818→192.168.1.1:22) tun_id=0.0.0.0 from port5. flag [S], seq 419563927, ack 0, win 29200"
2022-11-30 19:35:13 id=20085 trace_id=58 func=init_ip_session_common line=6024 msg="allocate a new session-000ec1a6, tun_id=0.0.0.0"
2022-11-30 19:35:13 id=20085 trace_id=58 func=vf_ip_route_input_common line=2605 msg="find a route: flag=84000000
```
bash

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
gw-192.168.1.1 via root"
2022-11-30 19:35:13 id=20085 trace_id=52 func=fw_local_in_handler line=500 msg="iprope_in_check() check failed on
policy 0, drop"
```

原因3

1. 访问FGT本机流量，接口下已经开启了此服务，如下所示。

```bash
config system interface
    edit "port1"
        set ip 192.168.89.35 255.255.255.0
        set allowaccess ping ssh
    next
end
```

2. 但访问流量是从另外的一个接口发起的，而另外一个接口到本接口没有配置相应的防火墙策略。

3. 从Debug Flow发现192.168.1.10访问FortiGate port1接口192.168.89.32的22端口被拒绝，因为数据包是从port5接口来的，因此被拒绝。

```bash
2022-11-30 19:42:32 id=20085 trace_id=72 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=6,
192.168.1.10:54384→192.168.89.35:22) tun_id=0.0.0.0 from port5. flag [S], seq 2800378420, ack 0, win 29200"
2022-11-30 19:42:32 id=20085 trace_id=72 func=init_ip_session_common line=6024 msg="allocate a new session-
000ed260, tun_id=0.0.0.0"
2022-11-30 19:42:32 id=20085 trace_id=72 func=vf_ip_route_input_common line=2605 msg="find a route: flag=84000000
gw-192.168.89.35 via root"
2022-11-30 19:42:32 id=20085 trace_id=72 func=fw_local_in_handler line=500 msg="iprope_in_check() check failed on
policy 0, drop"
```

4. 解决方法：增加port5到port1接口的策略。

```bash
config firewall policy
    edit 0
        set srcintf "port5"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "192.168.89.35/32"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

通过GUI进行Debug Flow

功能介绍

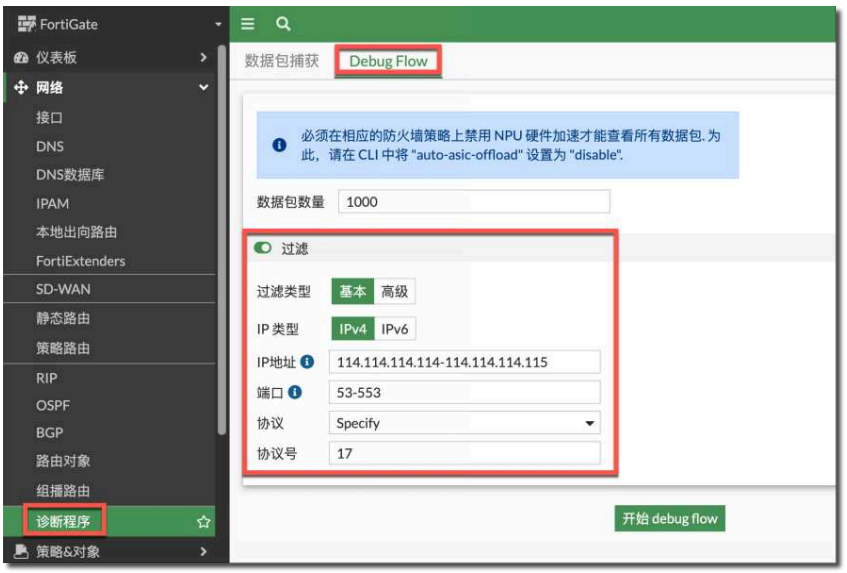
除了通过在CLI下进行Debug Flow，FortiGate也支持在GUI界面进行Debug Flow，方便不熟悉Debug Flow工具的用户使用。

> **重要**
>
> 本功能在FortiOS 7.2和7.4版本支持。

使用方法

> **重要**
>
> 进行Debug Flow之前，必须在抓取流量对应的防火墙策略上禁用NPU硬件加速才能查看所有数据包的处理流程，请在CLI中将对应防火墙策略中的“auto-asic-offload”设置为“disable”。
>
> 详情参考：故障排查→Sniffer、Debug Flow与NP加速的矛盾 ↗。

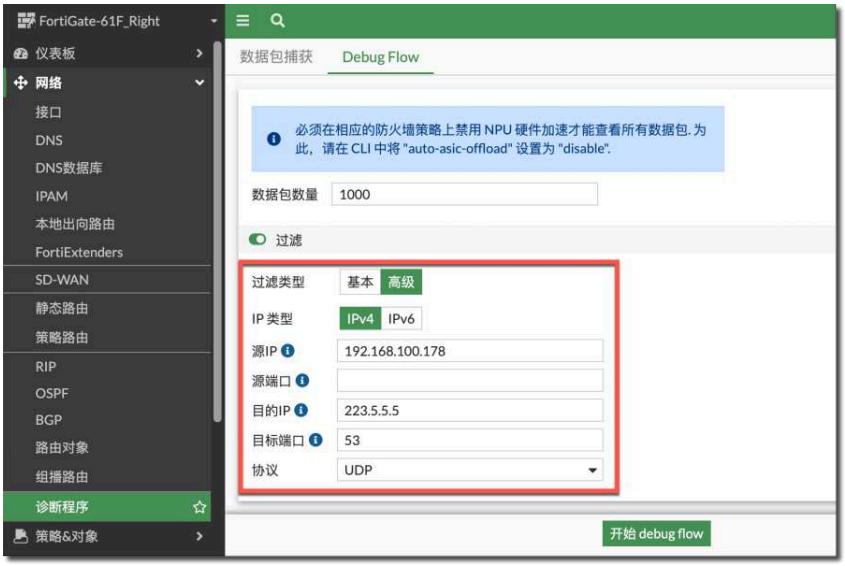
1. 进入“网络→诊断程序→Debug Flow”页面，配置Debug Flow的过滤条件，过滤语法选择基本时，可以过滤如下条件。



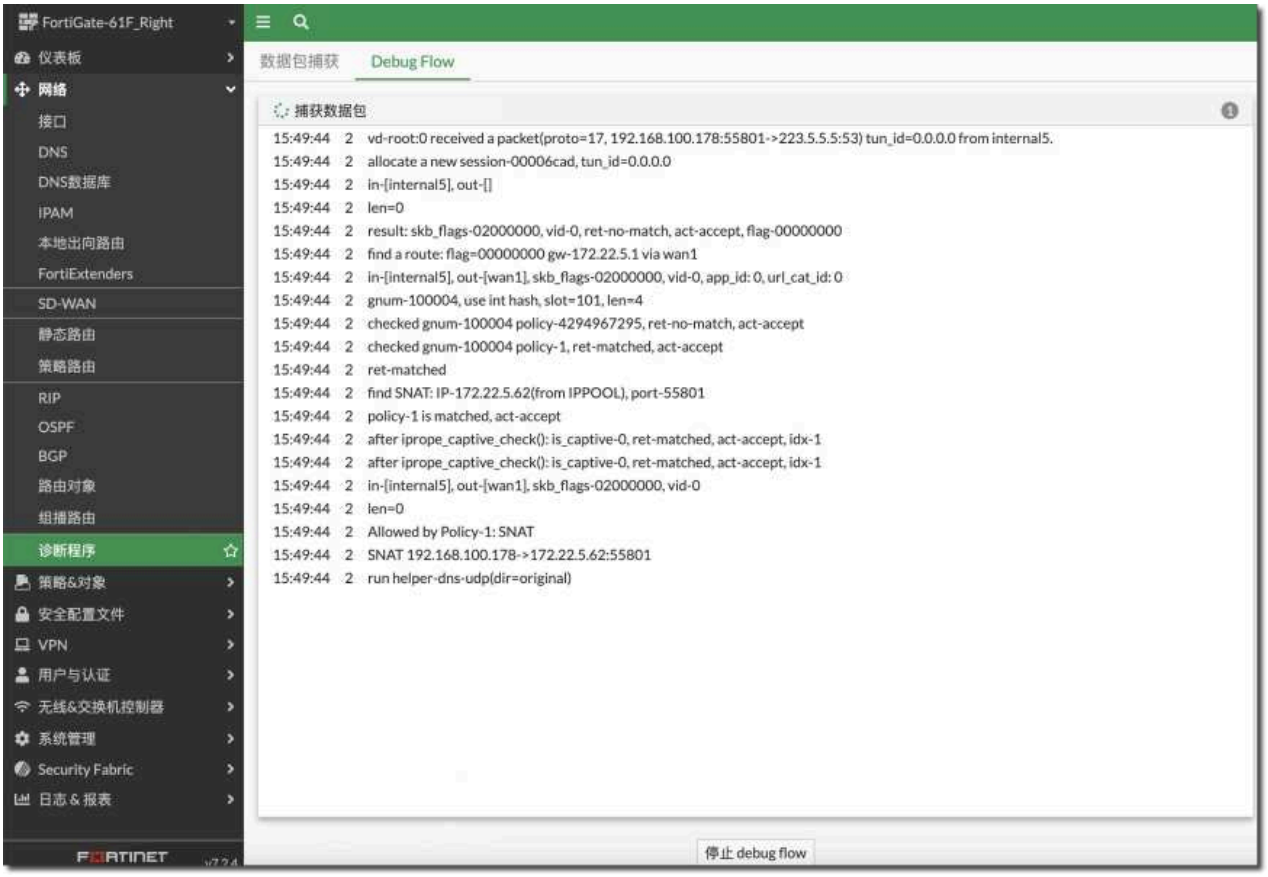
- 数据包数量：Debug Flow可以捕获的最大数据包数量。
- IP类型：过滤IP版本类型。
- IP地址：Debug Flow过滤的IP地址，可以是源IP，也可以是目的IP。格式可以写单个地址，也可以写一个IP范围，中间用“-”标识。
- 端口：过滤Debug Flow的端口号，格式可以写单个端口，也可以写一个端口范围，中间用“-”标识。。
- 协议：过滤Debug Flow的协议，可选择Any、Specify（手工配置过滤的协议号）、TCP、UDP、SCTP、ICMP。

2. 过滤语法选择高级时，可以指定如下过滤条件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

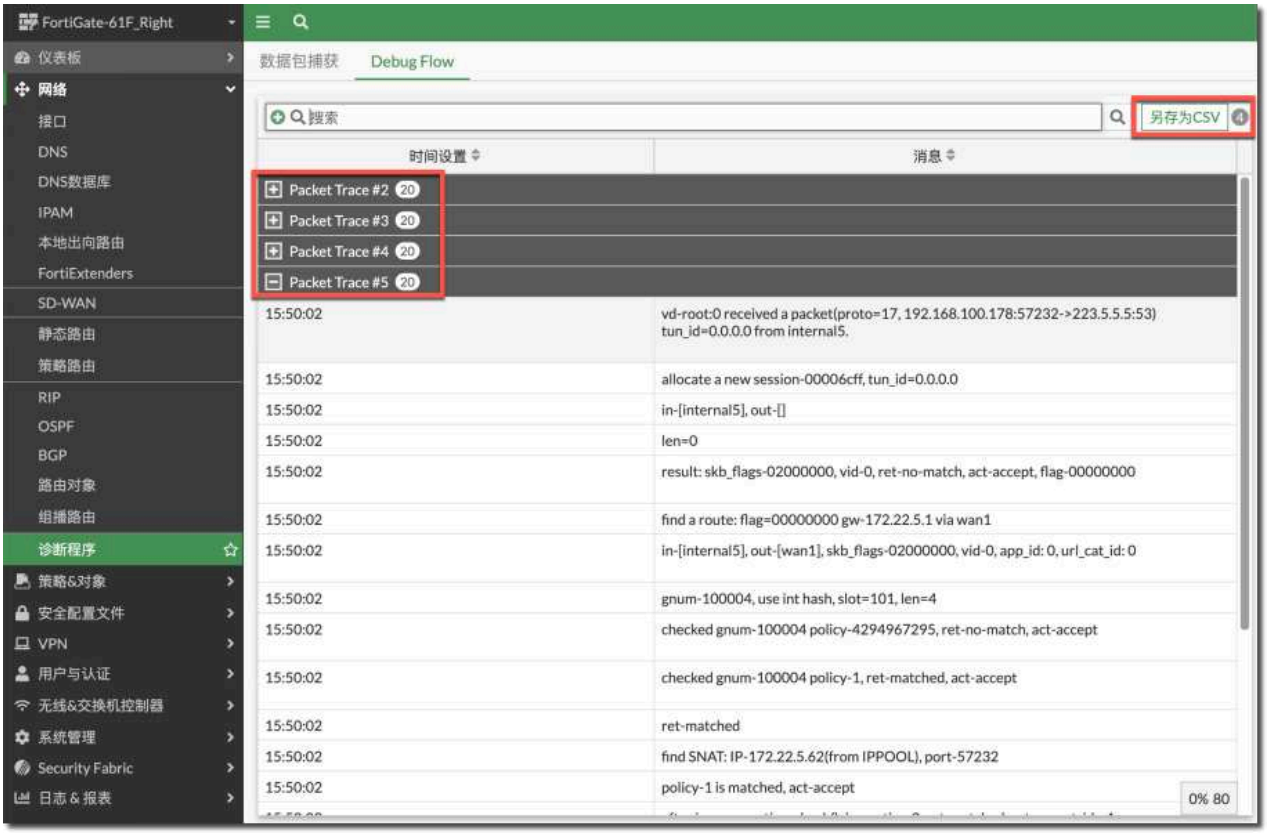


3. 点击“开始Debug Flow”按钮开启数据流分析。



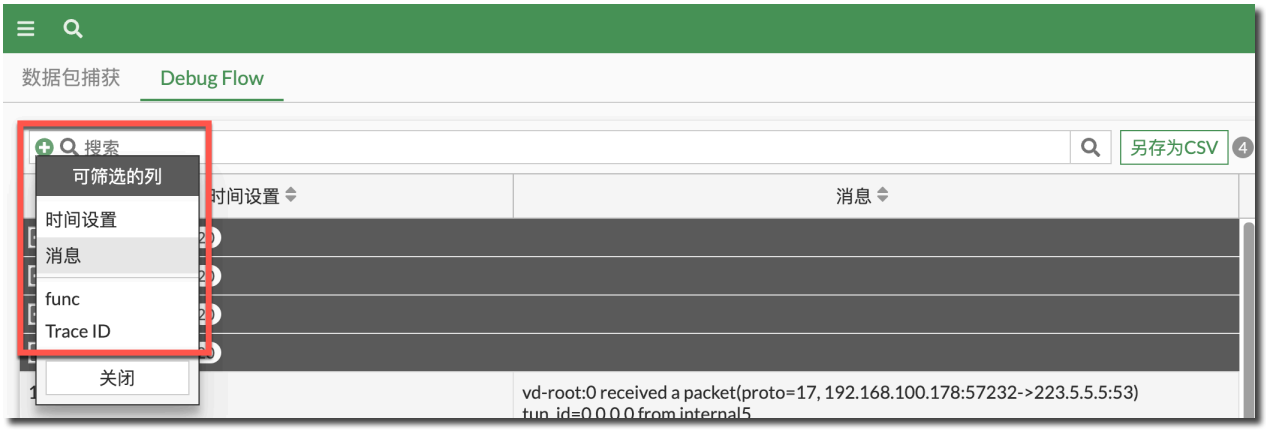
4. 点击“停止Debug Flow”按钮，FortiGate会将每个数据流合并打哦一个Trace中，可以在该结果中进行关键字搜索，也可点击“另存为CSV”下载Debug Flow的文本信息。

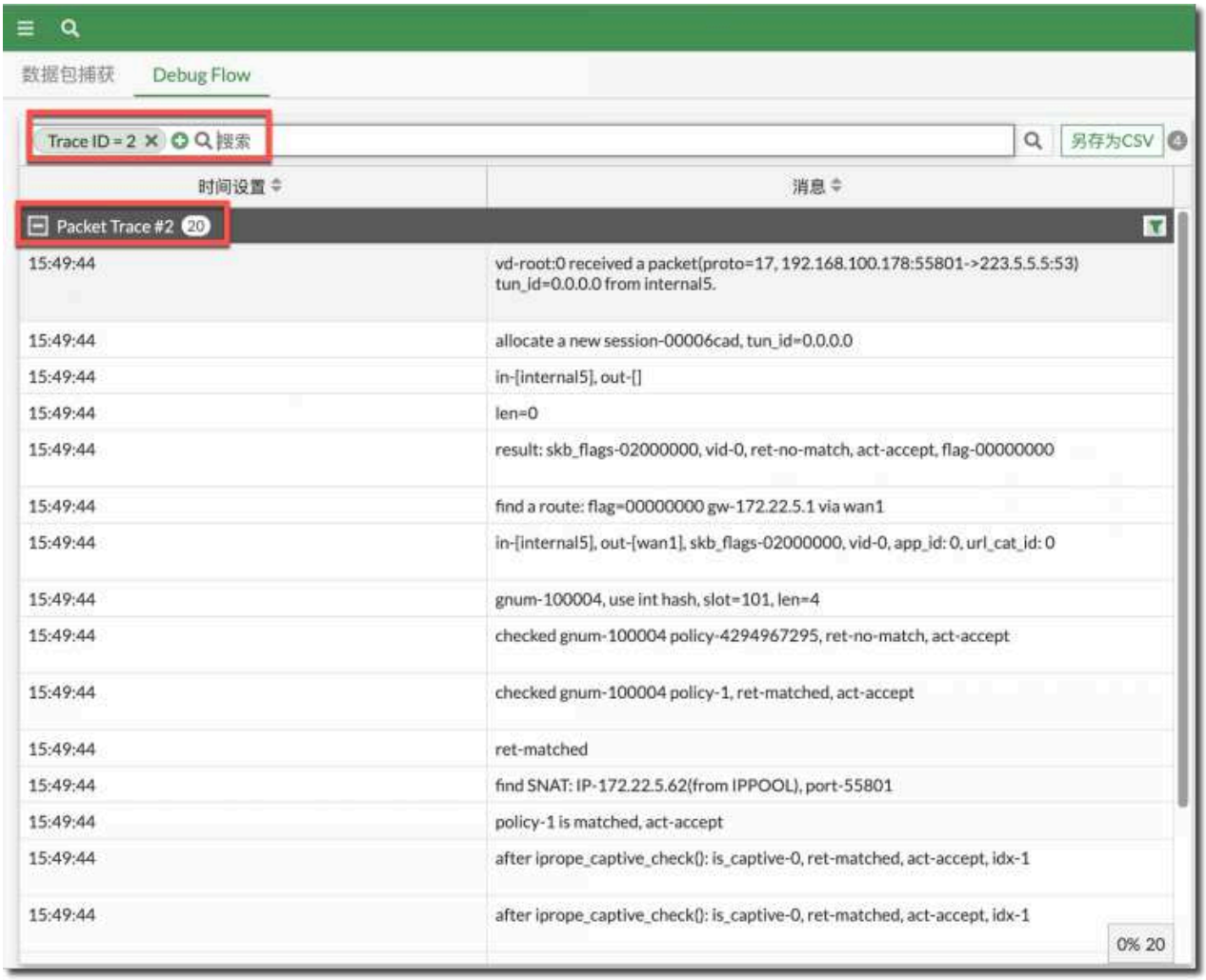
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



5. 搜索时可以使用如下条件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Sniffer/Debug Flow/NP加速的矛盾

问题现象

sniffer或debug flow抓不到包或抓不全。这是由于数据被NP加速后，数据直接由NP转发，不经过CPU处理，因此sniffer、debug flow将抓不到相应的数据包。

只有被CPU处理的数据才能被sniffer工具完整抓获，通常是新建数据流才可以抓到包，比如：ICMP的第一个/第二个包、TCP三次握手和四次拆链的包、UDP的第一个/第二个包。

网络拓扑

PC1(192.168.1.10)-----(port5：192.168.1.1)FGT(port1:192.168.89.35)-----Internet

原因分析

1. 设置Debug Flow：

```bash
diagnose debug flow filter addr 114.114.114.114
diagnose debug flow filter proto 1
diagnose debug flow show function-name enable
diagnose debug console timestamp enable
diagnose debug flow trace start 10
diagnose debug enable
```

2. 使用PC1（192.168.1.10）ping 114.114.114.114。

3. 第1个数据包：ping请求echo request。

```bash
2022-11-30 19:54:07 id=20085 trace_id=87 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
192.168.1.10:2589→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2589, seq=1."
2022-11-30 19:54:07 id=20085 trace_id=87 func=init_ip_session_common line=6024 msg="allocate a new session-
000ee70c, tun_id=0.0.0.0"
2022-11-30 19:54:07 id=20085 trace_id=87 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000
gw-192.168.89.254 via port1"
2022-11-30 19:54:07 id=20085 trace_id=87 func=get_new_addr line=1221 msg="find SNAT: IP-192.168.89.35(from
IPPOOL), port-63005"
2022-11-30 19:54:07 id=20085 trace_id=87 func=fw_forward_handler line=881 msg="Allowed by Policy-9: SNAT"
2022-11-30 19:54:07 id=20085 trace_id=87 func=__ip_session_run_tuple line=3471 msg="SNAT 192.168.1.10-
>192.168.89.35:63005"
```

4. 第2个数据包：ping响应echo reply。

```bash
2022-11-30 19:54:07 id=20085 trace_id=88 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
114.114.114.114:63005→192.168.89.35:0) tun_id=0.0.0.0 from port1. type=0, code=0, id=63005, seq=1."
2022-11-30 19:54:07 id=20085 trace_id=88 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
000ee70c, reply direction"
2022-11-30 19:54:07 id=20085 trace_id=88 func=__ip_session_run_tuple line=3484 msg="DNAT 192.168.89.35:0-
>192.168.1.10:2589"
2022-11-30 19:54:07 id=20085 trace_id=88 func=vf_ip_route_input_common line=2605 msg="find a route: flag=00000000
gw-192.168.1.10 via port5"
2022-11-30 19:54:07 id=20085 trace_id=88 func=npu_handle_session44 line=1183 msg="Trying to offloading session
from port1 to port5, skb.npu_flag=00000000 ses.state=00010204 ses.npu_state=0x04000000"
2022-11-30 19:54:07 id=20085 trace_id=88 func=fw_forward_dirty_handler line=410 msg="state=00010204,
state2=00000001, npu_state=04000000"
```

5. 第3个数据包：ping请求echo request，数据包发起方向推送到NP加速（`npu session installation succeeded`）：

```bash
2022-11-30 19:54:08 id=20085 trace_id=89 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
192.168.1.10:2589→114.114.114.114:2048) tun_id=0.0.0.0 from port5. type=8, code=0, id=2589, seq=2."
2022-11-30 19:54:08 id=20085 trace_id=89 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
000ee70c, original direction"
2022-11-30 19:54:08 id=20085 trace_id=89 func=npu_handle_session44 line=1183 msg="Trying to offloading session
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
from port5 to port1, skb.npu_flag=00000400 ses.state=00010204 ses.npu_state=0×04000000"
2022-11-30 19:54:08 id=20085 trace_id=89 func=ip_session_install_npu_session line=346 msg="npu session
installation succeeded"
2022-11-30 19:54:08 id=20085 trace_id=89 func=fw_forward_dirty_handler line=410 msg="state=00010204,
state2=00000001, npu_state=04000400"
```

6. 第4个数据包：ping响应echo reply，数据包的响应方向推送到NP加速（`npu session installation succeeded`）：

```bash
2022-11-30 19:54:08 id=20085 trace_id=89 func=__ip_session_run_tuple line=3471 msg="SNAT 192.168.1.10-
>192.168.89.35:63005"
2022-11-30 19:54:08 id=20085 trace_id=90 func=print_pkt_detail line=5845 msg="vd-root:0 received a packet(proto=1,
114.114.114.114:63005→192.168.89.35:0) tun_id=0.0.0.0 from port1. type=0, code=0, id=63005, seq=2."
2022-11-30 19:54:08 id=20085 trace_id=90 func=resolve_ip_tuple_fast line=5931 msg="Find an existing session, id-
000ee70c, reply direction"
2022-11-30 19:54:08 id=20085 trace_id=90 func=__ip_session_run_tuple line=3484 msg="DNAT 192.168.89.35:0-
>192.168.1.10:2589"
2022-11-30 19:54:08 id=20085 trace_id=90 func=npu_handle_session44 line=1183 msg="Trying to offloading session
from port1 to port5, skb.npu_flag=00000400 ses.state=00010204 ses.npu_state=0×04000400"
2022-11-30 19:54:08 id=20085 trace_id=90 func=ip_session_install_npu_session line=346 msg="npu session
installation succeeded"
2022-11-30 19:54:08 id=20085 trace_id=90 func=fw_forward_dirty_handler line=410 msg="state=00010204,
state2=00000001, npu_state=04000c00"
```

7. 对应的sniffer抓包如下。

```bash
FGT # diagnose sniffer packet any 'host 114.114.114.114 and icmp' 4
interfaces=[any]
filters=[host 114.114.114.114 and icmp]
2.544370 port5 in 192.168.1.10 → 114.114.114.114: icmp: echo request
2.544394 port1 out 192.168.89.35 → 114.114.114.114: icmp: echo request

2.564639 port1 in 114.114.114.114 → 192.168.89.35: icmp: echo reply
2.564941 port5 out 114.114.114.114 → 192.168.1.10: icmp: echo reply

3.546345 port5 in 192.168.1.10 → 114.114.114.114: icmp: echo request
3.546356 port1 out 192.168.89.35 → 114.114.114.114: icmp: echo request

3.566460 port1 in 114.114.114.114 → 192.168.89.35: icmp: echo reply
3.566467 port5 out 114.114.114.114 → 192.168.1.10: icmp: echo reply
```

8. 后续的ping报文直接通过NP芯片转发，因此sniffer和debug flow都没有输出。此时查看session list，`offload=8/8`表示数据包双向卸载到NP6（NP7的双向加速状态为`9/9`），即由NP芯片转发。

```bash
FGT # diagnose sys session list

session info: proto=1 proto_state=00 duration=9 expire=51 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty npu f00
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin→sink: org pre→post, reply pre→post dev=13→9/9→13 gwy=192.168.89.254/192.168.1.10
hook=post dir=org act=snat 192.168.1.10:2589→114.114.114.114:8(192.168.89.35:63005)
hook=pre dir=reply act=dnat 114.114.114.114:63005→192.168.89.35:0(192.168.1.10:2589)
misc=0 policy_id=9 pol_uuid_idx=521 auth_info=0 chk_client_info=0 vd=0
serial=000ee70c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=0×4000c00 ofld-O ofld-R
npu info: flag=0×81/0×81, offload=8/8, ips_offload=0/0, epid=148/156, ipid=156/148, vlan=0×0000/0×0000
vlifid=156/148, vtag_in=0×0000/0×0000 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=0/3
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

解决方法

NP6

方法1

1. 对于需要抓包的流量新建一条临时策略关闭NP加速或在对应策略（找到流量对应的策略及策略ID）里临时关掉NP加速，这样数据的处理会全部走CPU处理，可以抓取到完整的数据包。

```bash
config firewall policy
    edit 27                     //注意此处27是策略ID号，不是策略顺序号//
        set auto-asic-offload disable    //在策略中临时关闭NP加速,Sniffer完毕可再enable此命令//
    next
end
```

2. 对于已经建立起来的会话（数据已经走NP处理了），可以先过滤出来并清除掉，然后再抓包。

```bash
diagnose sys session filter dst 202.106.1.100
diagnose sys session filter proto 1
diagnose sys session list               //通过session list可以找到对应的策略ID，还可以看到NP加速的标志位//
diagnose sys session clear              //清空该会话//
```

3. 最后再开启抓包命令，这样就可以抓到完全的数据流了。

```bash
diagnose sniffer packet any "host 202.106.1.100 and icmp" 4
```

方法2

不关闭NP情况下的组合抓包脚本，但是只能抓到一次性的加速前的数据包，加速后的包将无法显示出来。

```bash
diagnose sys session filter proto 1
diagnose sys session filter dst 114.114.114.114
diagnose sys session clear    //先将需要抓包的数据流对应的会话清除//

diagnose sniffer packet any "host 114.114.114.114 and icmp" 4 0 l    //再通过抓包命令抓取，可以抓取NP加速前的报文//
```

NP7

NP7芯片支持在不关闭NP加速的情况下抓取NP7已加速的报文，请参考章故障排查→Sniffer工具→NP7芯片抓包↗章节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

简介

FortiGate 防火墙从网络层到应用层对网络流量进行全面的安全检查，检查流程由FortiGate的安全策略控制，而具体的处理路径取决于设备的硬件结构以及启用的安全检测模式：

- **硬件配置**：是否配备NP6/NP7等网络处理器，以及CP8/CP9/CP10等内容处理器。
- **检测模式**：基于流检查或基于代理检查。检查模式基于安全策略，可针对每个安全策略单独配置检查模式，灵活性大幅提升。

本章节主要介绍数据包在运行 FortiOS6.4及更高版本的FortiGate中“入站→处理→出站”的完整流程。

FortiGate的三类安全检查

FortiGate执行的主要安全检测类型：

- **基于内核的状态检查（Stateful Inspection）**：是一种由防火墙内核实现的安全机制，它不仅检查单个数据包的内容，还会跟踪整个连接的状态信息，这是FortiGate基于会话状态工作的基本原理。
  - 当一个连接（如TCP或UDP通信）开始时，防火墙会在内核中建立一条会话状态表项，记录此会话的关键信息。
  - 当后续的报文经过防火墙时，内核会首先查找会话状态表。
    - 如果报文属于一个已建立的合法会话，则直接根据会话状态快速放行（或执行相应动作）。
    - 如果是一个新的会话请求，或半连接报文（如未匹配任何会话的TCP ACK报文），则需要按照安全策略、包头字段、协议行为等进一步检查，决定是否允许建立新连接。
- **流基于检查（Flow-based Inspection）**：通过对数据流内容取样（snapshot），并进行模式匹配（pattern matching），实时识别潜在的安全威胁。
- **基于代理检查（Proxy-based Inspection）**：通过重构经过FortiGate的数据内容，对完整会话内容进行深度安全分析。

安全功能与检查类型关系表

安全功能	内核（状态检查）	基于流检查	基于代理检查
防火墙（Firewall）	是		
IPsec VPN	是		
流量整形（Traffic Shaping）	是		
用户认证（User Authentication）	是		
管理流量（Management Traffic）	是		
SSL VPN	是		
IPS（入侵防御系统）		是	
僵尸网络检查（Botnet Checking）		是	
防病毒（AntiVirus）		是	是
应用控制（Application Control）		是	
Web过滤（Web Filtering）		是	是
DLP（数据泄露防护）		是	是
邮件过滤（反垃圾邮件）		是	是
VoIP检查（VoIP Inspection）			是
ICAP			是

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

检查方法特性对比

特性	状态检查（Stateful）	基于流检查（Flow）	基于代理检查（Proxy）
每会话检查单位	每个数据包	特定数据包，单遍并行	完整内容，顺序执行
内存、CPU需求	低	中	高
威胁防护级别	良好（Good）	更好（Better）	最佳（Best）
认证支持	是	-	-
IPsec/SSL VPN支持	是	-	-
防病毒防护	-	是	是
Web过滤	-	是	是
DLP支持	-	是	是
应用控制支持	-	是	-
IPS支持	-	是	-
流量延迟	轻微（Minor）	无（No）	较小（Small）
重构完整内容	-	否（No）	是（Yes）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Parallel Path Processing

Parallel Path Processing（PPP，并行路径处理）通过防火墙策略配置从一组并行处理选项中，为数据包选择最优处理路径。大部分FortiOS功能通过防火墙策略触发，而策略中启用的功能直接决定数据包的处理逻辑。

PPP的作用

- **差异化防护高风险流量**：对HTTP、邮件等可能包含安全威胁的流量，可通过策略施加UTM/NGFW处理，并借助CP8/CP9/CP10处理器卸载加速。支持从基础IPS攻击防护（检测网络层攻击）到高级威胁管理（ATM）、应用控制、防病毒、DLP（数据泄露防护）的全维度防护。
- **优化无风险流量性能**：对低安全威胁的流量（如内部办公系统通信），可创建专用策略绕过UTM/NGFW检查。配备NP处理器的FortiGate可将此类流量卸载到NP，释放CPU资源用于高风险流量处理，实现“安全不降级、性能不损耗”。

加速技术

- **NTurbo**：部分FortiGate型号支持NTurbo，可将基于流UTM/NGFW的会话卸载到NP处理器。
- **IPSA**：基于流的会话通过IPSA技术，将模式匹配任务卸载到CP内容处理器，进一步降低CPU负载。

数据包的处理流程

穿越FortiGate的数据包会经历以下流程（并非所有数据包都需经过全部流程），具体取决于数据包类型和FortiGate软硬件配置。

入站流程（Ingress）

- 入站数据包流（Ingress Packet Flow）
  - 网络接口（Network Interface）
  - TCP/IP栈（TCP/IP Stack）
  - DoS策略（DoS Policy）
  - IP完整性头部检查（IP Integrity Header Checking）
  - IPsec VPN解密（IPsec VPN Decryption）
- 准入控制（Admission Control）
  - 隔离（Quarantine）
  - 终端遥测（FortiTelemetry）
  - 用户认证（User Authentication）
- 内核相关（Kernel）
  - 目的NAT（Destination NAT，DNAT）
  - 路由（含SD-WAN）
  - 状态检查/策略查找/会话管理（Stateful Inspection/Policy Lookup/Session Management）
  - Session Helper
  - 用户认证（User Authentication）
  - 设备识别（Device Identification）
  - SSL VPN
  - 本地管理流量（Local Management Traffic）
- UTM/NGFW相关
  - 基于流检查（Flow-based Inspection）
    - NTurbo
    - IPSA
  - 僵尸网络检查（Botnet Check）
  - 基于代理检查（Proxy-based Inspection）
  - 显式Web代理（Explicit Web Proxy）
- 内核相关（Kernel）
  - 转发（Forwarding）
  - 源NAT（Source NAT，SNAT）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

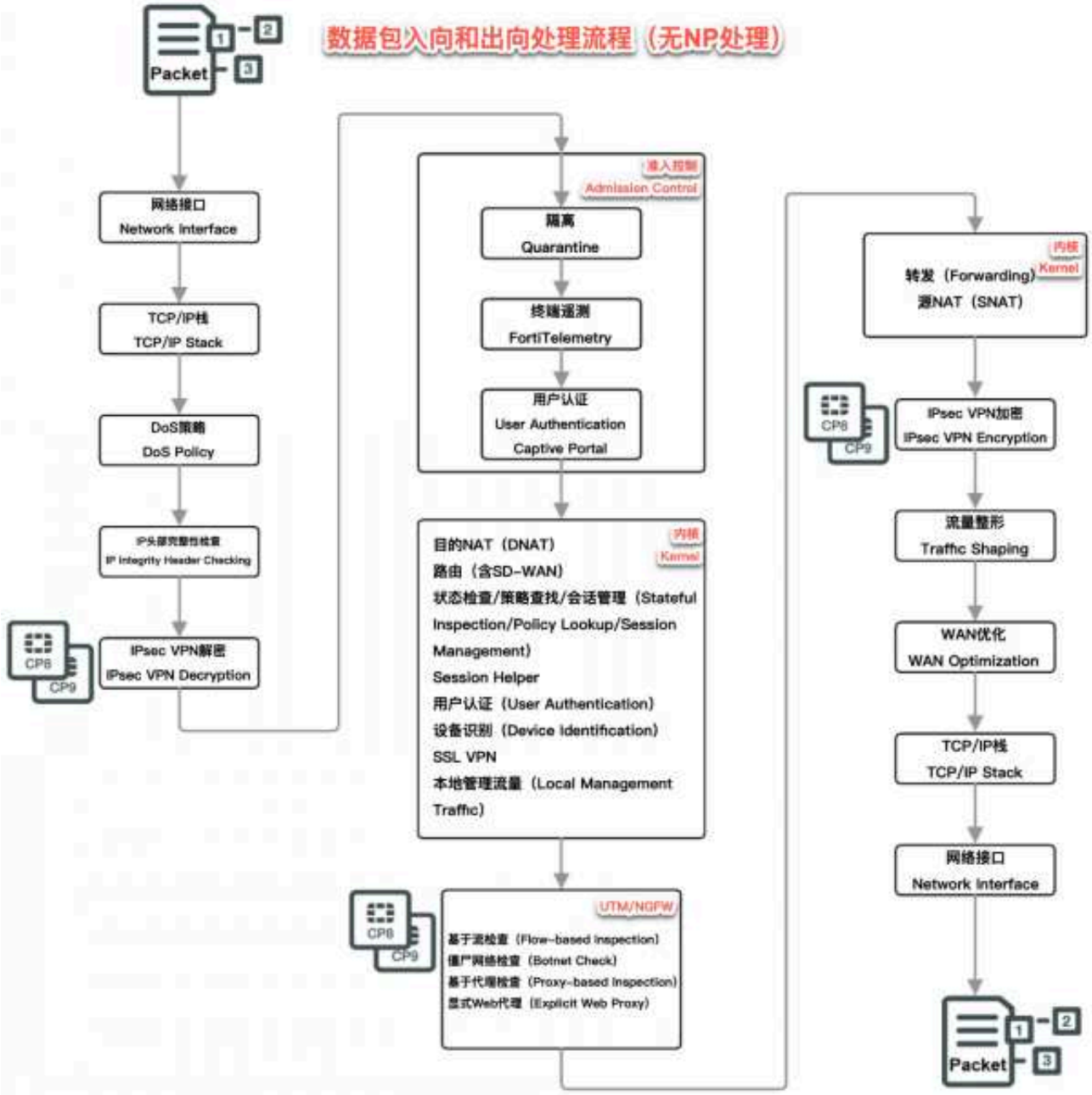
出站流程（Egress）

- IPsec VPN加密（IPsec VPN Encryption）
- 流量整形（Traffic Shaping）
- WAN优化（WAN Optimization）
- TCP/IP栈（TCP/IP Stack）
- 网络接口（Network Interface）

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

无NP处理的数据包流程

本节描述无NP处理的FortiGate中，数据包从入站到出站的完整处理步骤。



入站流程（Ingress）

所有被FortiGate接收的数据包均需通过网络接口，并由TCP/IP协议栈进行处理。若已配置DoS策略，数据包还必须通过这些策略以及自动IP头部完整性检查。

DoS策略检查

在报文进入FortIGate的早期阶段，DoS模块会检测流量是否异常，以判断是否属于拒绝服务攻击（DoS attack）。

- 检查范围：仅跟踪可能用于DoS攻击的数据包（如TCP SYN包），验证其是否符合预设参数。
- 处理逻辑：疑似攻击数据包直接阻断，合法数据包进入下一环节。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

IP完整性头部检查

此步骤主要验证 TCP、UDP、ICMP、SCTP、GRE 等协议头部长度是否合法。

- 支持协议：TCP、UDP、ICMP、SCTP、GRE。
- 处理逻辑：头部长度正确则进入下一步，错误则直接丢弃。

IPsec VPN解密

若入站数据包匹配已配置的IPsec隧道：

- IPsec引擎尝试用正确密钥解密。
- 解密成功：解密后数据包进入下一环节。
- 解密失败/非IPsec流量：直接进入下一环节（不处理）。

> **重要**
>
> IPsec解密可由CP处理器卸载加速。

准入控制

执行三层准入校验，确保流量来源合法：

1. 隔离检查：阻断源/目的地址在“隔离（quarantine）列表”中的数据包。
2. FortiTelemetry（可选）：要求设备安装FortiClient才能通过。
3. 强制门户认证（可选）：对入站流量触发Captive Portal认证。

内核处理

数据包通过入站检查后，由FortiOS内核执行核心转发与控制逻辑。

DNAT

内核查询NAT表，判断是否需要修改入站流量的目的IP地址。

- 典型场景：将互联网流量导向内网服务器（如Web服务器），隐藏内网真实地址。
- 关键顺序：DNAT必须在“路由”前执行，确保FortiGate能正确路由修改后的地址。
- 路由验证：同步检查目的地址是否存在有效路由。

路由（含SD-WAN）

通过路由表确定数据包的出接口，并区分“本地流量”（目的地为FortiGate自身）和“转发流量”（目的地为其他网络）：

- 策略匹配依据：源接口（入站时已知）+ 目的接口（路由确定）。
- SD-WAN特殊逻辑：
  1. SD-WAN 首先利用应用识别模块（Application Control）对新会话的首包进行L4的ISDB匹配。
  2. 匹配成功：按SD-WAN规则路由整个会话。
  3. 匹配失败：应用“隐式SD-WAN规则”，并通过七层应用控制继续识别。
  4. 识别成功：在ISDB缓存中添加四层匹配记录，优化后续匹配效率。

状态检查/策略查找/会话管理

针对会话的第一个数据包执行策略匹配与会话管理，是防火墙的核心逻辑。

- 会话边界识别：通过TCP SYN/FIN标志判断会话开始/结束。
- 合法性校验：检查源/目的IP、端口、协议，以及载荷/序列号的完整性。
- 会话表优化：第一个数据包匹配策略后，将会话信息存入“会话表”，后续数据包直接查询会话表（比每次都查询策略高效）。
- 会话生命周期：处理完最后一个数据包后删除会话，或触发“空闲超时”后删除。

> **重要**
>
> 更多状态检查细节可查阅维基百科“状态防火墙”词条：https://en.wikipedia.org/wiki/Stateful_firewall ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Session Helper

部分协议（如SIP、FTP）需分析数据包载荷才能正常转发，FortiOS通过Session Helper解析这些协议的载荷信息，并动态调整防火墙规则。

- 支持的Session Helper：PPTP、H323、RAS、TNS、TFTP、RTSP、FTP、MMS、PMAP、SIP、DNS-UDP、RSH、DCERPC、MGCP等。
- 典型场景：SIP协议通过TCP控制包建立通话，会话助手提取载荷中的语音端口信息，允许语音数据包通过。

用户认证

当防火墙策略匹配成功且该策略包含用户认证要求时，系统会启动认证流程（基于IP地址）。

设备识别

对流量进行设备特征分析，以识别来源设备类型（例如 PC、手机、IoT 终端等）。

SSL VPN

SSL VPN流量通过目的端口识别，解密后路由到SSL VPN接口，再通过策略转发（SSL加解密由CP加速）。

本地管理流量

- 终止接口：多VDOM模式终止于管理接口，透明模式终止于管理IP。
- 流量范围：管理员访问（GUI/CLI）、FortiManager集中管理、FortiGuard通信等。
- 访问控制：由local-in策略定义（参考策略与对象→本地流量策略→ Local-in策略↗章节），不参与后续状态检查。

UTM/NGFW处理

若匹配的安全策略包含“安全配置文件”，数据包需进入UTM/NGFW处理，处理方式取决于策略的检测模式。

基于流检查（单遍架构）

通过单遍DFA（直接过滤法）模式匹配实时阻断威胁，无代理参与。

- 处理流程：先通过解码器识别协议，再执行单遍模式匹配（IPS、应用控制等并行），最后检查僵尸网络地址。
- 支持功能：IPS、应用控制、Web过滤、DLP、僵尸网络检查、防病毒。
- 加速方式：模式匹配由CP卸载。

基于代理检查（混合模式）

结合基于流与基于代理检查，深度处理高风险流量。

- 第一步：IPS引擎执行单遍基于流检查（IPS、应用控制、僵尸网络检查）。
- 第二步：代理重构内容，按顺序执行检查（VoIP检查→DLP→反垃圾邮件→Web过滤→防病毒→ICAP）。
- 支持功能：除基于流功能外，额外支持VoIP深度检查、ICAP等。

显式Web代理检查

逻辑与基于代理检查类似，仅针对HTTP/HTTPS流量，通过指定端口（默认8080）监听。

CP（内容处理器）

大部分FortiGate配备SPU（安全处理单元）内容处理器（CP），加速资源密集型安全任务（由主CPU分配任务）。不同型号CP能力不同，新型号以CP9/CP10为主。CP的核心能力如下：

- 基于流检查加速：优化IPS/应用控制模式吞吐量。
- VPN优化：高性能IPsec/SSL/TLS处理，支持DES/3DES/AES等加密算法。
- 哈希与HMAC：支持MD5/SHA系列哈希，符合FIPS标准。
- 密钥加速：IKE/RSA密钥交换加速，含真随机数生成器。
- 其他：DLP指纹支持、TTTD内容分块。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

出站流程（Egress）

数据包完成内核与UTM/NGFW处理后，通过以下步骤离开FortiGate。

源NAT（SNAT）

查询NAT表，修改出站流量的源IP（如内网访问互联网时隐藏真实地址）。

IPsec VPN加密

若需进入IPsec隧道，执行加密封装（由CP加速）。

流量整形

按配置调整流量速率，保障关键业务带宽。

WAN优化

执行压缩、缓存等优化，提升WAN链路效率。

TCP/IP栈处理

完成协议封装。

出接口

数据包通过出接口离开。

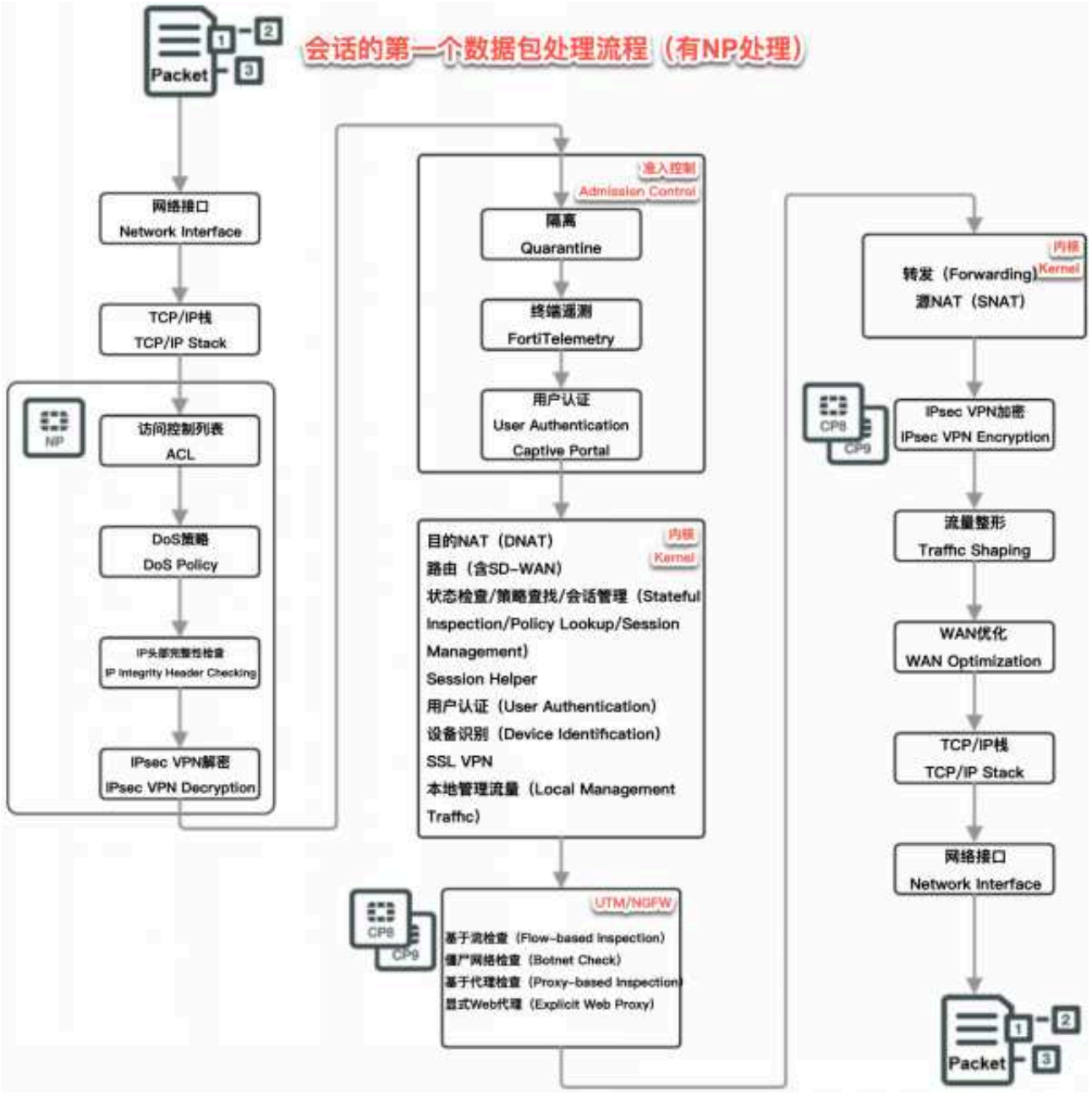
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

被NP加速的流量

NP会话

第一个数据包流程

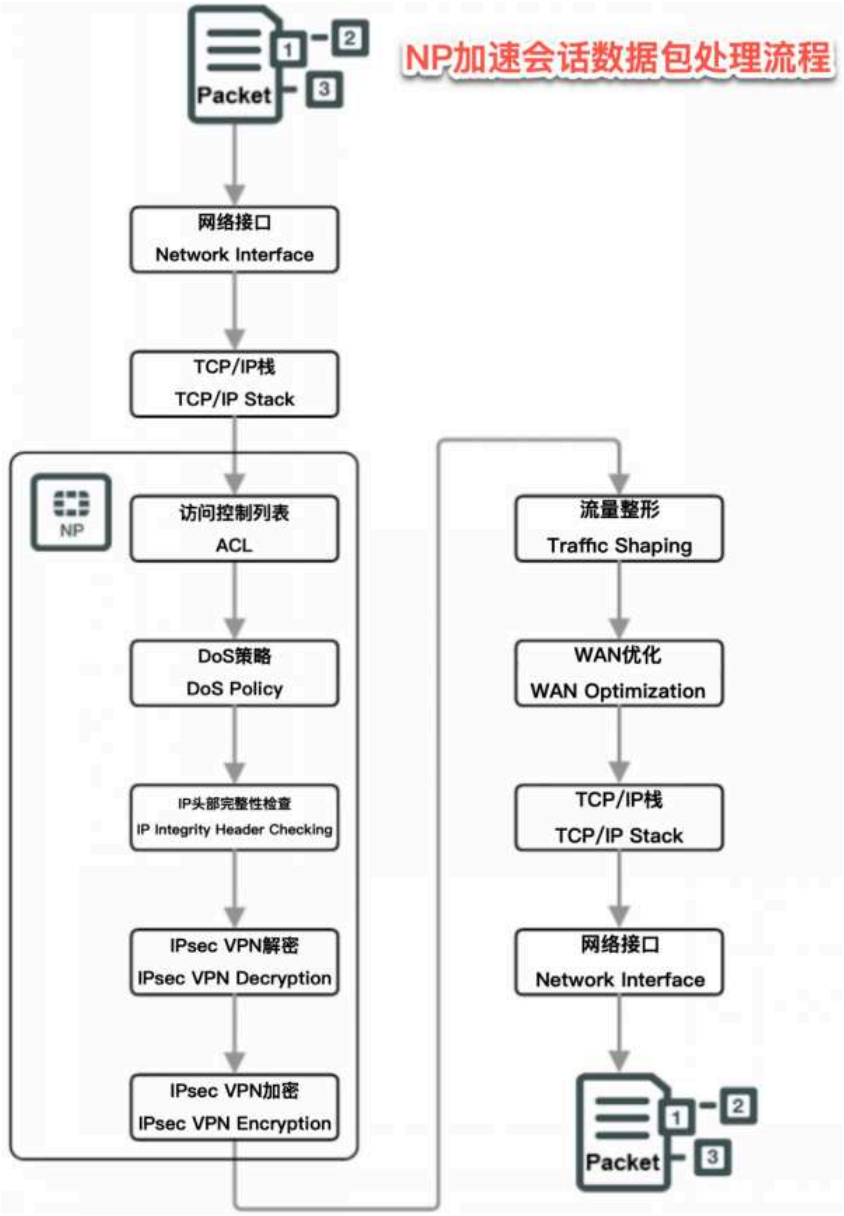
配备NP处理器的FortiGate，新会话的第一个数据包会判断是否可卸载（无基于代理UTM/NGFW时大多可卸载），其处理流程与“无NP加速设备”基本一致。后续数据包则进入简化的卸载流程。



已加速会话数据包流程

新会话第一个数据包处理完成后，后续数据包跳过路由、UTM/NGFW、内核，直接由NP转发，安全检查也由NP加速。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 入站：网络接口→TCP/IP栈→NP6执行DoS检查/IP完整性检查/ACL检查。
- 处理：（若需）IPsec VPN加密→流量整形→WAN优化。
- 出站：TCP/IP栈→出口接口。

访问控制列表（ACL）

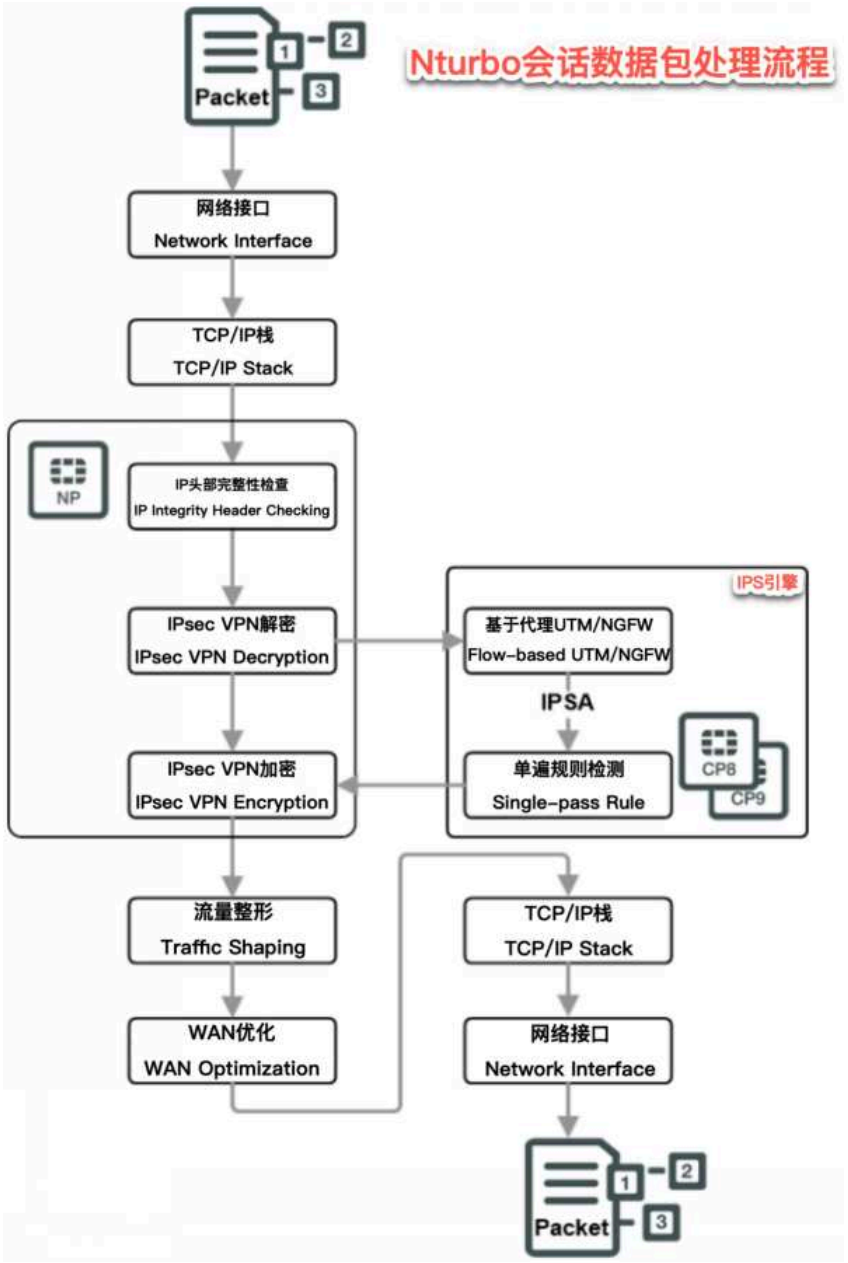
ACL是NP的功能之一，在物理接口层（CPU分析前）丢弃不合规IPv4/IPv6数据包，仅适用于NP接口。

- 优势：检查早、由NP执行，不占用CPU资源。
- 作用：在数据包到达CPU前阻断威胁，提升设备安全性。

NTurbo的数据包流程

支持NTurbo的FortiGate，可将基于流检测的UTM/NGFW会话卸载到NP，进一步提升处理效率。在已卸载的基于流的UTM/NGFW会话中，首个数据包处理完成后，后续数据包将跳过路由和内核处理器。基于流的UTM/NGFW操作仍由CPU处理，同时将IPSA卸载模式匹配任务转发至CP处理器。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



- 入站：网络接口→TCP/IP栈→NP6执行IP完整性检查。
- 处理：IPS引擎通过IPSA卸载模式匹配→（若需）IPsec VPN加密→流量整形→WAN优化。
- 出站：TCP/IP栈→出口接口。
- 威胁处理：检测到威胁则阻断会话，否则由NP转发。
- NTurbo兼容性限制：启用以下功能时，基于流UTM/NGFW会话无法通过NTurbo卸载。
- DoS策略。
- Session Helper。
- 大部分隧道类型（如GRE）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

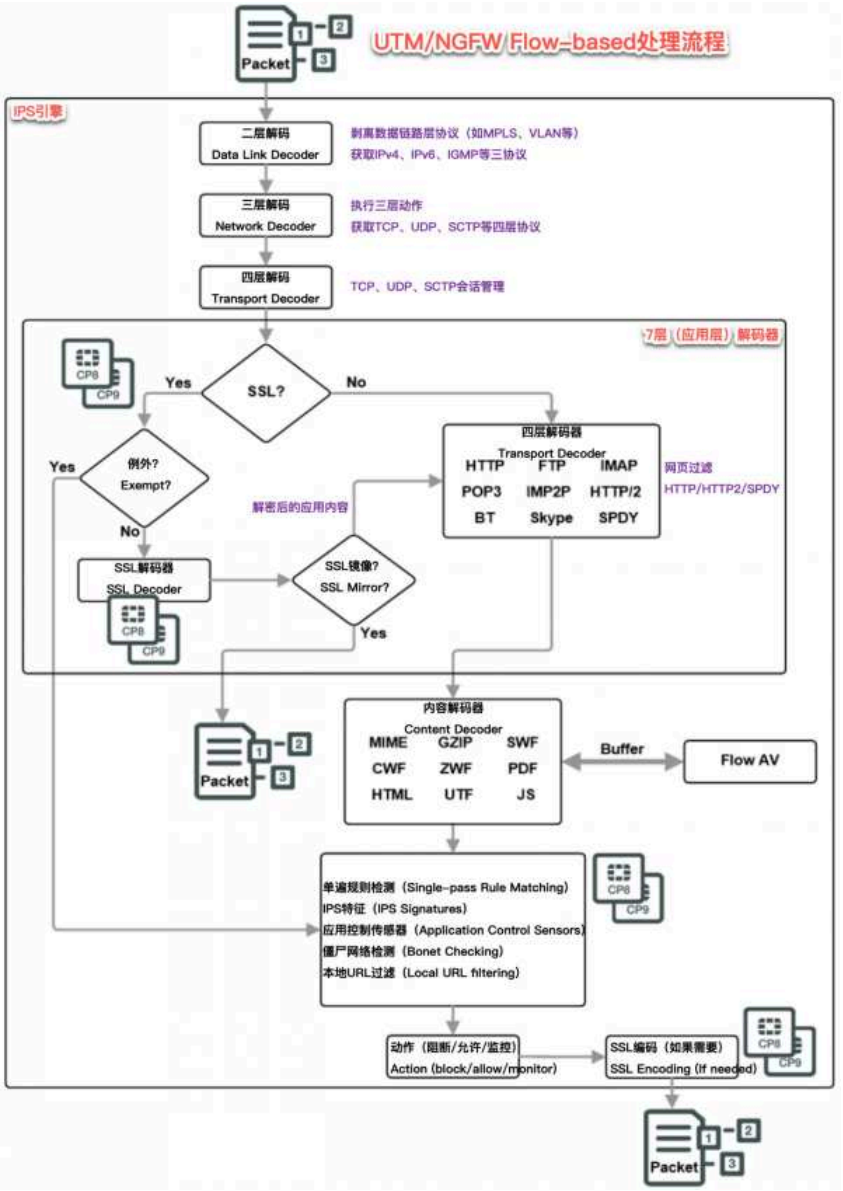
基于流的检测

基于流的UTM/NGFW检测采用单次扫描架构，通过直接过滤方法（DFA）模式匹配实时识别潜在攻击或威胁，并即时拦截安全威胁。

若防火墙策略配置为基于流检测，则根据接受会话的防火墙策略中选定的选项，基于流检测可应用入侵防御系统（IPS）、应用控制、网页过滤、数据防泄漏（DLP）、僵尸网络检测及防病毒功能。基于流检测完全由IPS引擎完成，不涉及代理操作。

```bash
config firewall policy
    edit 1
        set inspection-mode flow    //默认配置//
    next
end
```

处理流程



协议解码与SSL处理

在应用基于流的检测之前，IPS引擎会通过一系列解码器，根据数据包协议及策略设置确定应启用的安全模块。此外，若配置了SSL深度检测功能，IPS引擎还会对SSL数据包进行解密。SSL解密操作由CP处理器卸载并加速处理。

如果您配置了SSL镜像功能，IPS引擎会复制解密后的应用程序内容，将其封装在TCP数据包中（包含IP和以太网头），并发送至配置的镜像接口，二层目标地址为广播地址（FF:FF:FF:FF:FF:FF），源地址为全零地址。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

单遍安全检查

所有适用安全模块并行执行，模式匹配由CP加速。

- 并行检查：IPS、应用控制、本地URL过滤、僵尸网络检查、DLP。
- 防病毒：协议解码时缓存文件，同步执行病毒扫描。

总结

- 优点：资源占用低、不修改数据包（除阻断外）。
- 缺点：支持功能少于基于代理（如无客户端舒适、部分替换消息）。

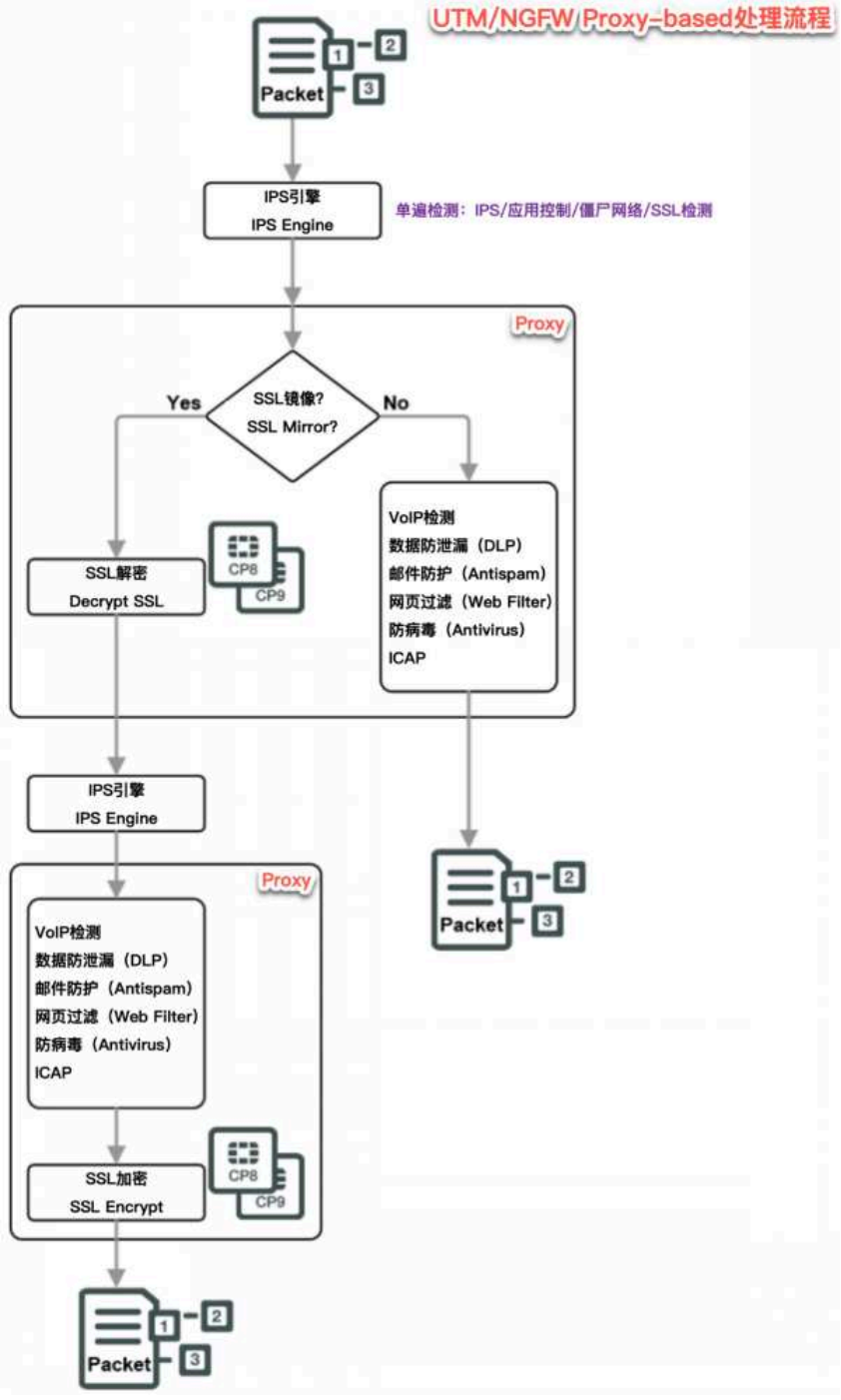
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于代理的检测

若防火墙策略配置为基于代理的检测，则会同时进行基于流和基于代理的混合检测。数据包首先经过IPS引擎处理，该引擎采用与基于流的UTM/NGFW数据包流相同的步骤：通过基于流的检测执行单次通过式入侵防御、僵尸网络检测以及应用控制。

```bash
config firewall policy
    edit 1
        set inspection-mode proxy
    next
end
```

处理流程



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

基于流检查

流量首次进入后，与基于流的检查一致，执行单遍IPS、应用控制、僵尸网络检查，SSL解密由CP加速。

代理的深度处理

代理重构内容，按以下固定顺序检查：

- VoIP检查：识别威胁并打开“针孔”允许合法语音流量。
- DLP：防止敏感数据泄露。
- 反垃圾邮件：过滤垃圾邮件。
- Web过滤：拦截不合规网页。
- 防病毒：扫描病毒。
- ICAP：转发HTTP/HTTPS流量到ICAP服务器，作为“中间人”传递请求/响应。

SSL加密与转发

- 若为SSL流量：解密检查后重新加密（CP8/CP9加速）；
- 转发逻辑：无威胁则转发，有威胁则阻断并替换为“替换消息”（如果配置了替换消息）。

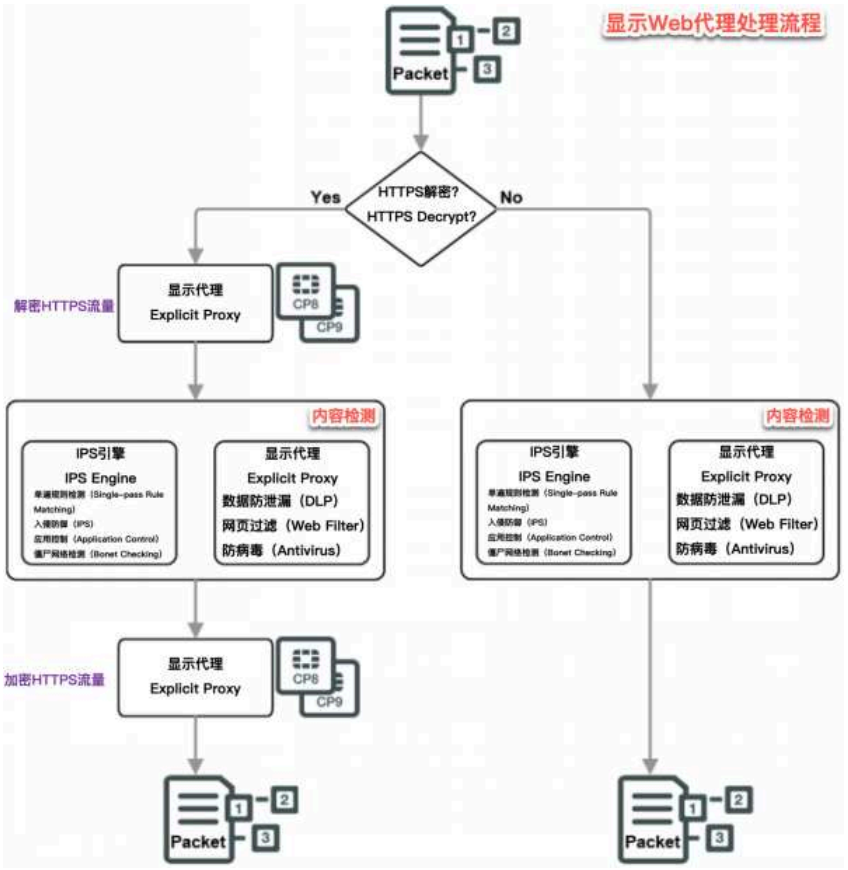
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

显式Web代理

启用显式Web代理后，FortiGate通过指定端口（默认8080）监听HTTP/HTTPS会话，采用“并行检查”模式处理流量。

- 全局/VDOM级别启用显式Web代理。
- 配置接口监听代理端口（默认8080）。
- 创建显式Web代理策略定义匹配范围。

处理流程



HTTP流量处理

- 并行检查：HTTP流量同时发送到IPS引擎（IPS/僵尸网络/应用控制）和代理（DLP/Web过滤/防病毒）。
- 转发逻辑：无威胁则转发，检测到威胁则阻断。

HTTPS流量处理

- 代理解密HTTPS流量（CP加速）。
- 并行检查（与HTTP一致）。
- 无威胁则重新加密（CP）并转发，有威胁则阻断。

源地址处理

数据包离开出口接口前，代理修改源地址：

- 普通模式：改为出口接口IP。
- 透明模式：改为透明模式管理IP。
- 可选配置：保留原始客户端IP。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

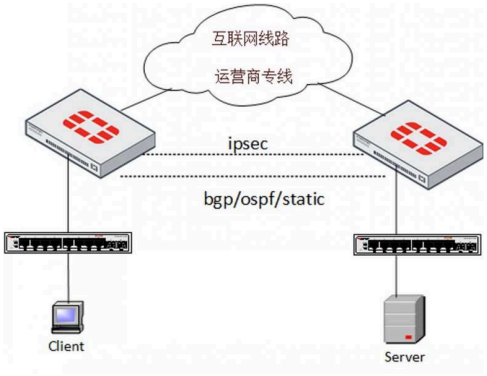
FortiGate之间测速

功能介绍

从FortiOS 7.0起，FortiGate可以作为iPerf服务器（之前只能做客户端）。

当遇到两台FortiGate之间的连接速度过低（如VPN隧道的带宽无法达到运营商带宽），可以在两台FortiGate之间进行iPerf测速，以便验证两台FortiGate之间的线路带宽。

网络拓扑



1. 客户反馈VPN Tunnel/专线互联场景下，C/S上传下载速度达不到预期值（运营商承诺的值）。
2. 某些情况下，当怀疑是营运商的问题时，可以开启防火墙的iPerf Server功能，直接在两台防火墙上跨运营商线路进行打流测试。

配置步骤

iPerf Server配置

1. 全局下开启speedtest-server，iPerf Server运行在TCP 5201，此端口无法修改，只支持TCP：

```
config system global
   set speedtest-server enable
end
```

2. 在FortiGate的WAN接口下开启允许seed-test：

```
config system interface
  edit "port1"
     append allowaccess speed-test
end
```

iPerf Client配置

1. 配置iPerf Client，server-intf和client-intf均选择WAN接口，端口配置为5201，协议配置为0（TCP）：

```
Client # diagnose traffictest server-intf port1
server-intf:    port1
Client # diagnose traffictest client-intf port1
client-intf:    port1
Client # diagnose traffictest port 5201
port:   5201
Client # diagnose traffictest proto 0
proto:  TCP

Client # diagnose traffictest show
server-intf:    port1
client-intf:    port1
port:   5201
proto:  TCP
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

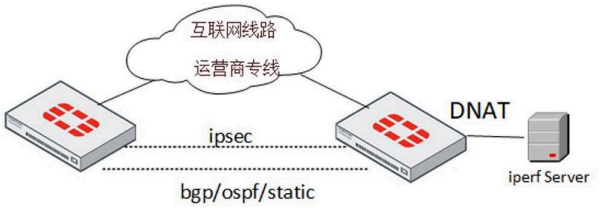
2. Client FortiGate使用traffictest工具向Server FortiGate打流（相关参数参考iPerf命令）：

```
Client # diagnose traffictest run -c 192.168.91.97 -t 120 -b 10M
```

```
Connecting to host 192.168.91.97, port 5201
[ 11] local 192.168.91.98 port 20157 connected to 192.168.91.97 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[ 11]   0.00-1.00   sec  1.24 MBytes  10.4 Mbits/sec    0   72.1 KBytes
[ 11]   1.00-2.00   sec  1.17 MBytes  9.79 Mbits/sec    0   90.5 KBytes
[ 11]   2.00-3.00   sec  1.21 MBytes  10.1 Mbits/sec    0    123 KBytes
```

注意事项

1. FortiGate作为iPerf服务器时有以下局限性：
   - Server不能修改端口
   - Server不支持UDP流量
   - Server不支持多会话并发流量
2. 某些运营商会限制客户端每条会话的速率，此时在FortiGate之间iPerf测试就无法准确的测出两台FortiGate之间运营商的实际带宽。
3. 这种情况下需要改变测试拓扑，将iPerf服务器更换为内网的真实iPerf Server，FortiGate使用DNAT映射内网的iPerf Server，可以接受多会话iPerf测速：




```
Client # diagnose traffictest run -c 192.168.91.92 -P 5
```

```
Connecting to host 192.168.91.92, port 5201
[ 11] local 192.168.91.98 port 13276 connected to 192.168.91.92 port 5201
[ 13] local 192.168.91.98 port 20172 connected to 192.168.91.92 port 5201
[ 15] local 192.168.91.98 port 24766 connected to 192.168.91.92 port 5201
[ 17] local 192.168.91.98 port 6267 connected to 192.168.91.92 port 5201
[ 19] local 192.168.91.98 port 17611 connected to 192.168.91.92 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[ 11]   0.00-1.00   sec  1.05 MBytes  8.80 Mbits/sec    0   1.43 KBytes
[ 13]   0.00-1.00   sec   843 KBytes  6.90 Mbits/sec    0   1.43 KBytes
[ 15]   0.00-1.00   sec  1.37 MBytes  11.5 Mbits/sec    0   1.43 KBytes
[ 17]   0.00-1.00   sec  5.58 MBytes  46.8 Mbits/sec    0   1.43 KBytes
[ 19]   0.00-1.00   sec  1.09 MBytes  9.15 Mbits/sec    0   1.43 KBytes
[SUM]   0.00-1.00   sec  9.92 MBytes  83.2 Mbits/sec    0
- - - - - - - - - - - - - - - - - - - - - - - - -
[ 11]   1.00-2.00   sec  1.48 MBytes  12.4 Mbits/sec    0   1.43 KBytes
[ 13]   1.00-2.00   sec   901 KBytes  7.38 Mbits/sec    0   1.43 KBytes
[ 15]   1.00-2.00   sec  1.29 MBytes  10.8 Mbits/sec    0   1.43 KBytes
[ 17]   1.00-2.00   sec  1.70 MBytes  14.2 Mbits/sec    0   1.43 KBytes
[ 19]   1.00-2.00   sec  1.19 MBytes  9.98 Mbits/sec    0   2.85 KBytes
[SUM]   1.00-2.00   sec  6.53 MBytes  54.8 Mbits/sec    0
- - - - - - - - - - - - - - - - - - - - - - - - -
[ 11]   2.00-3.00   sec  1.00 MBytes  8.40 Mbits/sec    0   2.85 KBytes
[ 13]   2.00-3.00   sec  1.45 MBytes  12.2 Mbits/sec    0   1.43 KBytes
[ 15]   2.00-3.00   sec  1.24 MBytes  10.4 Mbits/sec    0   2.85 KBytes
[ 17]   2.00-3.00   sec   649 KBytes  5.31 Mbits/sec    0   1.43 KBytes
[ 19]   2.00-3.00   sec  1.02 MBytes  8.60 Mbits/sec    0   1.43 KBytes
[SUM]   2.00-3.00   sec  5.35 MBytes  44.9 Mbits/sec    0
- - - - - - - - - - - - - - - - - - - - - - - - -
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

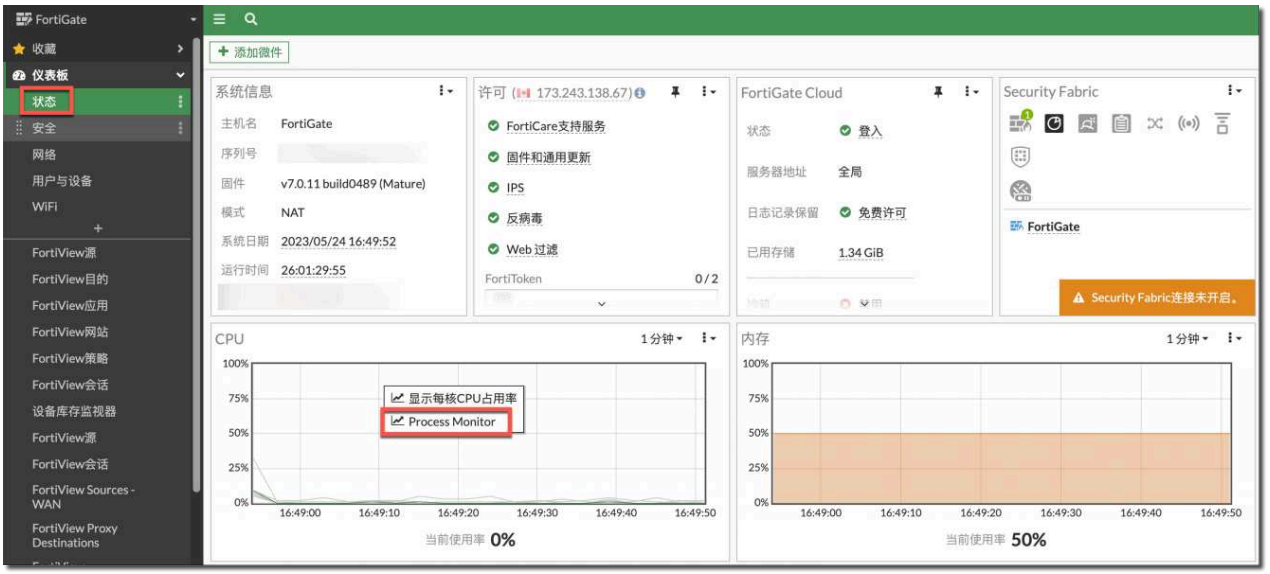
进程监控与管理

功能介绍

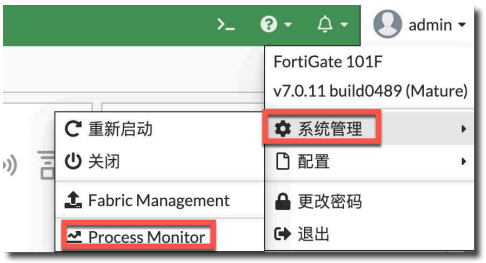
FortiOS 7.0版本后，在GUI上可以监控和管理设备运行的进程。

打开方式

1. 在仪表盘→状态的CPU监控微件中，左键单击图表任意位置，然后选择Process Monitor。



2. 在管理页面右上角点击admin→系统管理→Process Monitor。



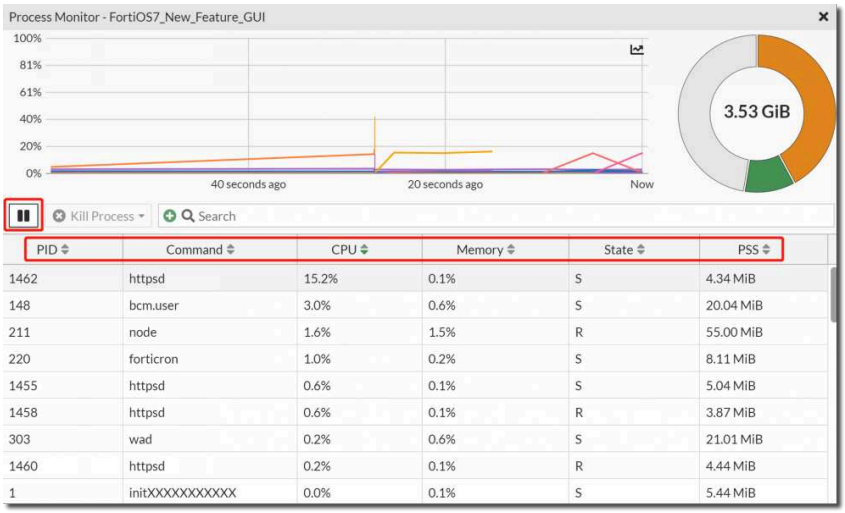
进程查看

1. 可以查看进程PID、进程名称、CPU占用比例、内存占用比例、状态、内存占用，并根据某个进程属性排序。

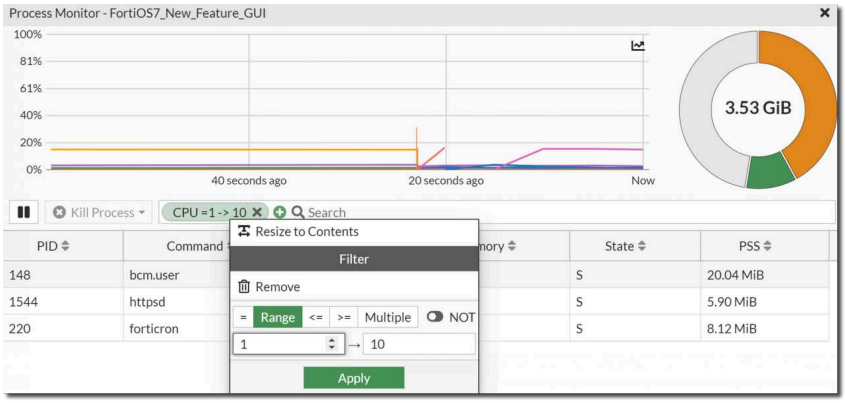
2. 图表可显示最近60s的监控信息。

3. 左侧的暂停按钮可以暂停/继续监控。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

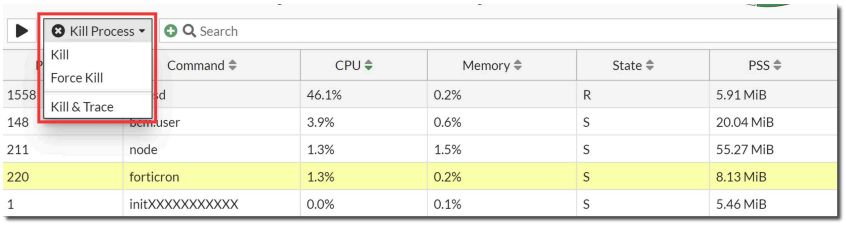


4. 根据过滤条件过滤进程，如PID、命令、CPU利用率范围、Memory利用率范围、状态、PSS范围。



进程管理

选中某个进程，右键进程或点击左上角的Kill Process按钮，可以选择三种Kill方式。

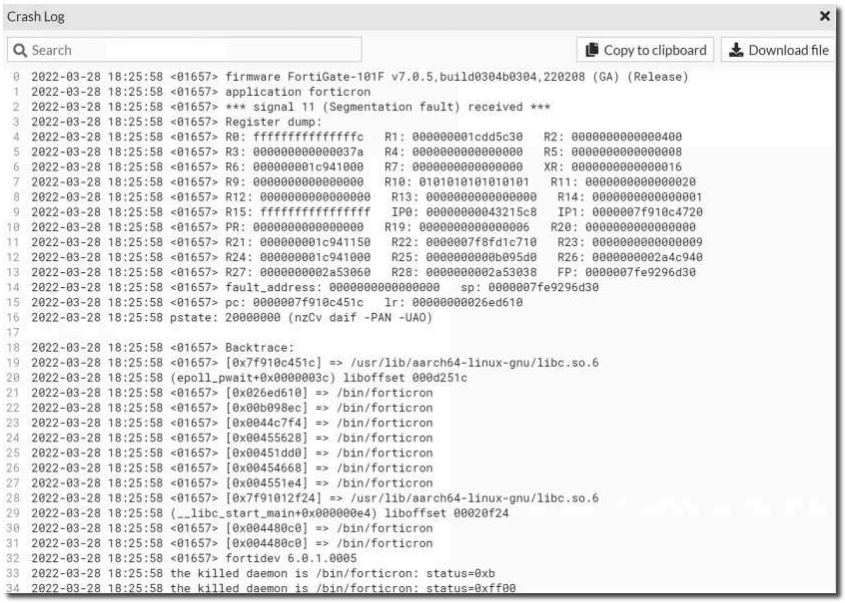


- Kill（相当于CLI下的diagnose sys kill PID_Number）。
- Force Kill（相当于CLI下的diagnose sys kill 9 PID_Number）。



- Kill & Trace（相当于CLI下的diagnose sys kill 11 PID_Number），弹出Crashlog页面，可下载、复制、搜索。当某个进程出现异常时，可以使用此方式重启进程，并将产生的Crash log发送至TAC团队进行分析。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Kernel CPU高的定位方法

在某些场景下，客户设备会遇到CPU持续高占用的情况，通过FortiGate自带的CPU Profiling程序，可以收集到CPU高时的代码级别的Debug信息。

通常来说，CPU可以在Kernel/System Space和User Space内工作，Kernel Space用于运行操作系统的可执行文件，以下方法仅适用于Kernel Space下CPU使用率高的情况，不适用于某个用户进程（如IPS engine/WAD）CPU占用高的情况。如下所示，获取的CPU状态信息中，System或softirg占用较高，即为Kernel Space CPU使用率高（而不是使用diagnose sys top中看到的用户进程占用CPU高）。

```
FortiGate # get system performance status

CPU states: 0% user 99% system 0% nice 1% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 99% system 0% nice 1% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 98% system 0% nice 2% idle 0% iowait 0% irq 0% softirq

FortiGate # get system performance status
CPU36 states: 0% user 0% system 0% nice 0% idle 0% iowait 0% irq 100% softirq
CPU37 states: 0% user 0% system 0% nice 0% idle 0% iowait 0% irq 100% softirq
CPU38 states: 0% user 0% system 0% nice 0% idle 0% iowait 0% irq 100% softirq
CPU39 states: 0% user 0% system 0% nice 0% idle 0% iowait 0% irq 100% softirq
```

定位方法

1. 在Kernel Space下CPU使用率持续高的情况下，使用如下命令收集信息。

```
diag sys profile cpumask 15    //抓取特定的CPU核心，这里以15为例
diag sys profile start    //开启profile程序，等待1分钟左右，再执行后续命令
diag sys profile stop
diag sys profile show order
diag sys profile show detail
diag sys profile sysmap
```

2. 以上操作执行完成后，使用如下命令输出CPU profile的结果。

```
FortiGate # diag sys profile show order

0×ffffffffa007990f: 2322 fqdn_ip_check+0×4f/0×a0
0×ffffffffa0078537: 547 oal_ioctl+0×a57/0×1070
0×ffffffff803ac8ec: 100 __write_lock_failed+0×c/0×20
0×ffffffffa00323bb: 57 __iprope_check_one_policy+0×32b/0×21c0
0×ffffffffa002bd4b: 38 timer_function+0×ffb/0×2e70
0×ffffffffa009c287: 37 __iprope_tree_check+0×1f7/0×3e0
```

3. 以上结果表明CPU在收集期间正在执行的函数，这些函数有两种类型，一种为标准的Linux函数，其意义何以在Linux标准中找到，另一种为Fortinet私有的函数。常见代表的意义如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

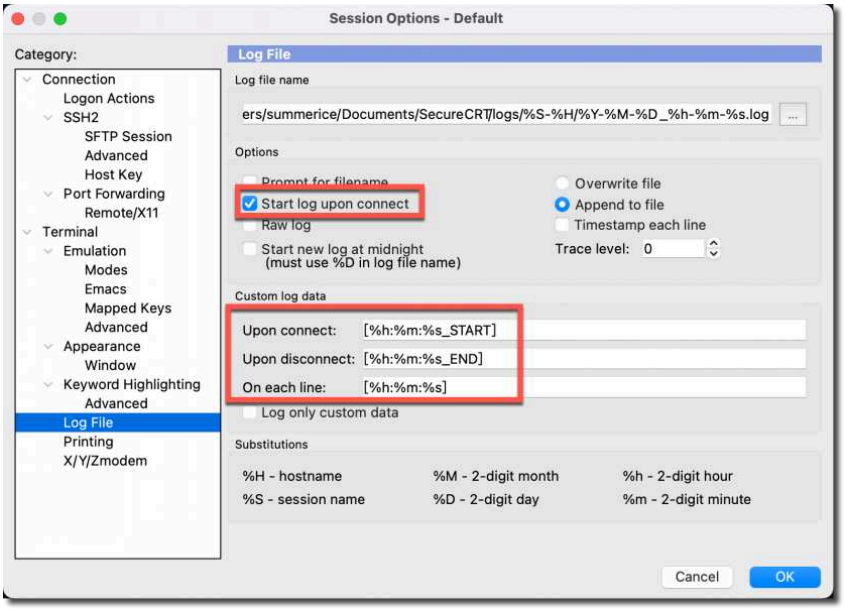
函数名称	含义	排查方法
poll_idle	CPU没有在做任何操作	忽略
inet_hash_connect inet_check_established	用于打开Socket连接	通常在显式代理中出现，可能是FortiGate无法在出接口上打开更多的端口导致，解决方法是在显示代理的出接口上设置更多的端口或IP（config web-proxy explicit）
inet_frag_find ip_defrag	分片	执行分片相关的调试命令（如sniffer、diagnose snmp ip frags），检查用户网络的MTU设置
is_csf_valid	ISDB	与ISDB进程或SD-WAN有关，检查调用大量ISDB条目的相关配置
read_ses_rate	SNMP	检查是否有大批量查询FortiGate SNMP OID的流量
__local_bh_enable_ip		
rb_next fqdn_check	FQDN	检查是否存在大量引用FQDN的策略
strncasecmp	FTP	与FTP Session Helper会话有关
queue_work_on process_one_work	Internal loop inside linux kernel	
__write_lock_failed	通用Linux函数，表示进程正在等待进程锁释放	
sal_no_sleep	FIB转发表项变化	检查是否有大规模的路由变化（BGP/OSPF/IPsec tunnel up/down）
__posix_lock_file	配置变更/更新特征库	本地配置变更，或FortiGate正在更新特征库
fqdn_ip_check oal_ioctl __write_lock_failed	被拒绝的流量	DDoS攻击、或大量数据包被FortiGate阻断
ip_session_mark_one_dirty ip6_session_mark_one_dirty	会话正在dirty	使用命令“diag sys cmdb info”检查配置变化情况，收集fcnacd进程的Debug信息，也可能有FortiClient终端注册情况导致的Session Dirty
release_pages pagevec_lru_move_fn	与WAD向IPS发送数据有关	与UTM深度包检测有关
do_gettimeoffset_tsc	IPS检测相关	
unix_find_other.constprop	配置变更	与移动安全策略顺序有关，使用“fnsysctl cat /proc/net/unix”收集信息
add_ip_mcast_session	与组播流量转发有关	
STAT_IVS_COPY_CNT	该计数器用于交换模块的Flood复制	与NP丢包无关

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

终端日志记录

对常用的终端工具，建议开启自动生成SSH会话日志的功能，对于任何通过ssh/telnet进行的CLI操作都能保留记录，方便日后追溯，文本化记录也有利于我们协同问题排查。

下图为SecureCRT默认会话的日志文件自动化生成配置示例（建议开启时间戳自动记录功能，以便后期方便追溯）。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

信息收集

基本信息

版本/序列号

```bash
get system status
```

HA状态

主备状态/优先级

```
diagnose sys ha status
```

同步状态

```
get system ha status
```

硬件相关

电源状态

```
diagnose hardware deviceinfo psu
```

风扇状态、CPU温度信息

```
exe sensor list
```

Flash/硬盘状态

```
diagnose hardware deviceinfo disk
diagnose sys flash list
exe disk list
```

Flash Disk状态检查

```
diagnose hardware smartctl /dev/sda -a
diagnose hardware smartctl /dev/sdb -a
diagnose hardware smartctl /dev/sdc -a
```

接口相关

网络接口状态

```
get system interface
```

接口丢包统计

```
diagnose hardware deviceinfo nic port1（接口名称）
```

光口收发光情况

```
get sys interface transceiver
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

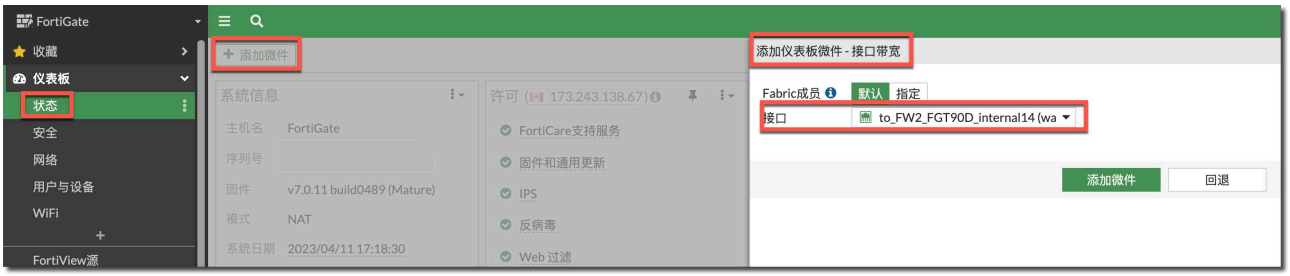
聚合口状态

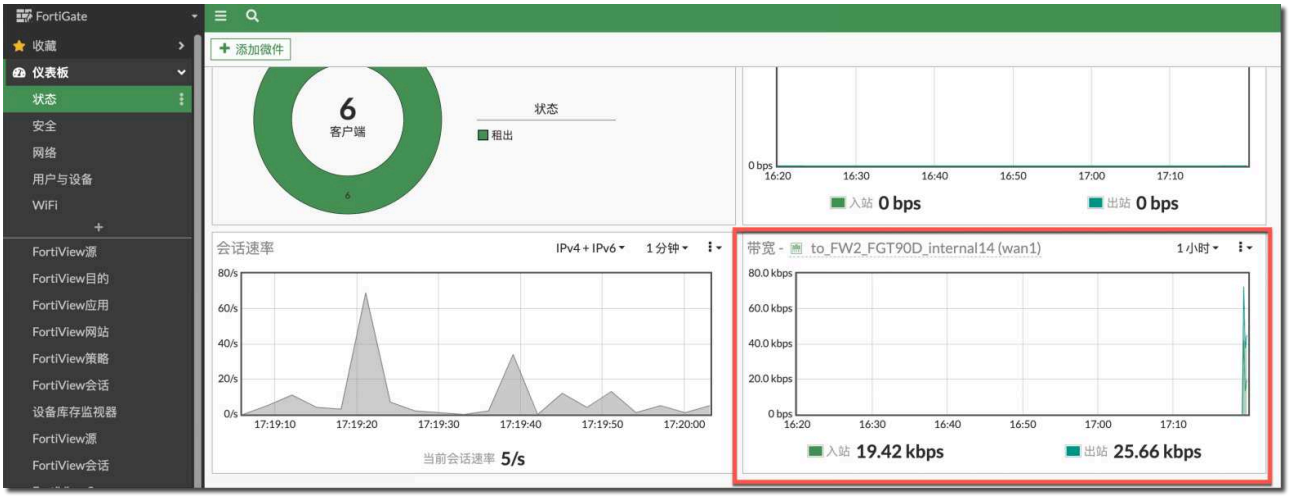
```
diagnose netlink aggregate list
```

VLAN状态

```
diagnose sys vlan list
```

接口带宽利用率





ARP表

```
get system arp
```

性能相关

CPU/内存/吞吐量

```
get system performance status
```

用户进程TOP

```
diagnose sys top 5 20
（键入shift+P以CPU占用排序，键入shift+M以内存占用排序）
```

追踪某个CPU的处理模块

> **重要**
>
> 适用于某个CPU高时的信息收集。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
diagnose sys profile cpumask x      //x为CPU编号
diagnose sys profile start
diagnose sys profile stop           //运行完start后，等一会儿再stop
diagnose sys profile show order     //一定要先运行stop再show orfer
```

内存占用

```bash
diagnose hard sysinfo memory
MemTotal: 1911036 kB            ← Total Memory of the hardware.
MemFree: 911804 kB              ← Total free memory of the hardware.
Buffers: 47244 kB               ← Buffer size for temporary memory.
Cached: 393348 kB               ← Cached = Active + Inactive.
SwapCached: 0 kB                ← Cache for memory pages.
Active: 573964 kB               ← Memory used in a particular process.
Inactive: 76000 kB              ← Pages which were not accessed recently.
Active(anon): 463264 kB         ← Anonymous memory.
Inactive(anon): 24252 kB        ← Anonymous memory.
Active(file): 110700 kB         ← Buffer/cache memory which is in active use. This memory is in recent use and is
not used by any other process.
Inactive(file): 51748 kB        ← Buffer/cache memory which is free. This memory is not in use and can be used by
any other process.
Unevictable: 0 kB               ← Pages can't be swapped out for multiple reasons.
Mlocked: 0 kB                   ← Pages locked to memory, Mlocked pages are also Unevictable.
SwapTotal: 0 kB                 ← Total Swap space in memory.
SwapFree: 0 kB                  ← Free Swap space in memory.
Dirty: 20 kB                    ← Memory in wait to get written back to the disk.
Writeback: 0 kB                 ← Memory which is currently written on the disk.
AnonPages: 209384 kB            ← Non file back pages mapped into user space.
Mapped: 78796 kB                ← Mapped files like, libraries.
Shmem: 278144 kB                ← Shared memory.
Slab: 89648 kB                  ← Kernel cache.
SReclaimable: 8292 kB           ← Part of slab/memory which can be claimed.
SUnreclaim: 81356 kB            ← Part of slab/memory which can not be claimed.
KernelStack: 1360 kB            ← Non-reclaimable kernel memory.
PageTables: 16720 kB            ← Amount of memory dedicated to the lowest level of the page.
NFS_Unstable: 0 kB              ← Memory not promised to the storage.
Bounce: 0 kB                    ← Memory used for bounce buffers.
WritebackTmp: 0 kB              ← Memory used for temporary purpose for writeback buffers.
CommitLimit: 955516 kB          ← Amount of memory available to be allocated.
Committed_AS: 7521252 kB        ← Sum of all the memory available to be allocated.
VmallocTotal: 663552 kB         ← Total size of Vmalloc memory area.
VmallocUsed: 152496 kB          ← Total size of Vmalloc memory area in used.
VmallocChunk: 349128 kB         ← Total size of free Vmalloc memory area.
```

内存Slab占用

```
diagnose hardware sys slab
......
active_objs        ← Number of objects that are currently in use.
num_objs           ← Total number of allocated objects that are in use or not in use.
objsize            ← Size of objects in this slab (in bytes).
objperslab         ← Number of objects stored in each slab.
pagesperslab       ← Number of pages allocated for each slab.

FortiGate # diagnose hardware sys slab
slabinfo - version: 2.1
# name            <active_objs> <num_objs> <objsize> <objperslab> <pagesperslab> : tunables <limit> <batchcount>
<sharedfactor> : slabdata <active_slabs> <num_slabs> <sharedavail>
packet_de_duplication6      0      0    192   20    1 : tunables  252  126    8 : slabdata      0      0      0
packet_de_duplication       0      0    128   30    1 : tunables  252  126    8 : slabdata      0      0      0
ip6_nat_record          0      0    128   30    1 : tunables  252  126    8 : slabdata      0      0      0
tcp6_session            0      0   1536    5    2 : tunables   60   30    8 : slabdata      0      0      0
ip6_session             0      3   1344    3    1 : tunables   60   30    8 : slabdata      0      1      0
ip_nat_record           0      0     64   59    1 : tunables  252  126    8 : slabdata      0      0      0
sctp_session            0      0   1536    5    2 : tunables   60   30    8 : slabdata      0      0      0
tcp_session            48    110   1536    5    2 : tunables   60   30    8 : slabdata     22     22      0
ip_session             70    105   1344    3    1 : tunables   60   30    8 : slabdata     35     35      0
fib6_nodes             20     59     64   59    1 : tunables  252  126    8 : slabdata      1      1      0
ip6_dst_cache          95    190    384   10    1 : tunables  124   62    8 : slabdata     19     19      0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
ndisc_cache            5     36    320   12    1 : tunables  124   62    8 : slabdata      3      3      0
ip6_mrt_cache          0      0    128   30    1 : tunables  252  126    8 : slabdata      0      0      0
RAWv6                 13     16   1024    4    1 : tunables  124   62    8 : slabdata      4      4      0
UDPLITEv6              0      0   1024    4    1 : tunables  124   62    8 : slabdata      0      0      0
UDPv6                 17     36   1024    4    1 : tunables  124   62    8 : slabdata      9      9      0
tw_sock_TCPv6          0      0    320   12    1 : tunables  124   62    8 : slabdata      0      0      0
request_sock_TCPv6     0      0    192   20    1 : tunables  252  126    8 : slabdata      0      0      0
TCPv6                 70     72   1856    2    1 : tunables   60   30    8 : slabdata     36     36      0
uhci_urb_priv          0      0     56   67    1 : tunables  252  126    8 : slabdata      0      0      0
scsi_sense_cache       1     30    128   30    1 : tunables  252  126    8 : slabdata      1      1      0
scsi_cmd_cache         1     15    256   15    1 : tunables  252  126    8 : slabdata      1      1      0
sd_ext_cdb             2    112     32  112    1 : tunables  252  126    8 : slabdata      1      1      0
cfq_io_context       133    210    128   30    1 : tunables  252  126    8 : slabdata      7      7      0
cfq_queue            133    204    232   17    1 : tunables  252  126    8 : slabdata     12     12      0
bsg_cmd                0      0    312   12    1 : tunables  124   62    8 : slabdata      0      0      0
mqueue_inode_cache     1      9    832    9    2 : tunables  124   62    8 : slabdata      1      1      0
fat_inode_cache        0      0    640    6    1 : tunables  124   62    8 : slabdata      0      0      0
fat_cache              0      0     32  112    1 : tunables  252  126    8 : slabdata      0      0      0
journal_handle         8    144     24  144    1 : tunables  252  126    8 : slabdata      1      1      0
journal_head          19    136    112   34    1 : tunables  252  126    8 : slabdata      4      4      0
revoke_table           6    202     16  202    1 : tunables  252  126    8 : slabdata      1      1      0
revoke_record          0      0     32  112    1 : tunables  252  126    8 : slabdata      0      0      0
ext2_inode_cache       0      0    720    5    1 : tunables  124   62    8 : slabdata      0      0      0
ext2_xattr             0      0     88   44    1 : tunables  252  126    8 : slabdata      0      0      0
ext3_inode_cache    9188   9395    712    5    1 : tunables  124   62    8 : slabdata   1879   1879      0
kioctx                 0      0    384   10    1 : tunables  124   62    8 : slabdata      0      0      0
kiocb                  0      0    256   15    1 : tunables  252  126    8 : slabdata      0      0      0
dio                    0      0    640    6    1 : tunables  124   62    8 : slabdata      0      0      0
fasync_cache         413    693     48   77    1 : tunables  252  126    8 : slabdata      9      9      0
posix_timers_cache     0      0    144   27    1 : tunables  252  126    8 : slabdata      0      0      0
uid_cache              4     60    128   30    1 : tunables  252  126    8 : slabdata      2      2      0
UNIX                 729    765    832    9    2 : tunables  124   62    8 : slabdata     85     85      0
ip_mrt_cache           0      0  20608    1    8 : tunables    8    4    0 : slabdata      0      0      0
UDP-Lite               0      0    832    9    2 : tunables  124   62    8 : slabdata      0      0      0
tcp_bind_bucket       98    336     32  112    1 : tunables  252  126    8 : slabdata      3      3      0
inet_peer_cache       57    120    192   20    1 : tunables  252  126    8 : slabdata      6      6      0
ip_fib_trie           51    134     56   67    1 : tunables  252  126    8 : slabdata      2      2      0
ip_fib_alias          58    154     48   77    1 : tunables  252  126    8 : slabdata      2      2      0
ip_dst_cache          85    285    256   15    1 : tunables  252  126    8 : slabdata     19     19      0
vf                     4      4   6784    1    2 : tunables    8    4    0 : slabdata      4      4      0
arp_cache              9     24    320   12    1 : tunables  124   62    8 : slabdata      2      2      0
PING                   0      0    832    9    2 : tunables  124   62    8 : slabdata      0      0      0
RAW                   21     36    832    9    2 : tunables  124   62    8 : slabdata      4      4      0
UDP                  100    108    832    9    2 : tunables  124   62    8 : slabdata     12     12      0
tw_sock_TCP            6     24    320   12    1 : tunables  124   62    8 : slabdata      2      2      0
request_sock_TCP       0      0    128   30    1 : tunables  252  126    8 : slabdata      0      0      0
TCP                   96    108   1664    4    2 : tunables   60   30    8 : slabdata     27     27      0
eventpoll_pwq       1139   1378     72   53    1 : tunables  252  126    8 : slabdata     26     26      0
eventpoll_epi       1117   1290    128   30    1 : tunables  252  126    8 : slabdata     43     43      0
sgpool-128             2      2   4096    1    1 : tunables   60   30    8 : slabdata      2      2      0
sgpool-64              2      2   2048    2    1 : tunables   60   30    8 : slabdata      1      1      0
sgpool-32              2      4   1024    4    1 : tunables  124   62    8 : slabdata      1      1      0
sgpool-16              2      8    512    8    1 : tunables  124   62    8 : slabdata      1      1      0
sgpool-8               2     15    256   15    1 : tunables  252  126    8 : slabdata      1      1      0
scsi_data_buffer       0      0     24  144    1 : tunables  252  126    8 : slabdata      0      0      0
blkdev_queue          27     28   1664    4    2 : tunables   60   30    8 : slabdata      7      7      0
blkdev_requests       12     22    344   11    1 : tunables  124   62    8 : slabdata      2      2      0
blkdev_ioc           101    236     64   59    1 : tunables  252  126    8 : slabdata      4      4      0
bio-0                  2     20    192   20    1 : tunables  252  126    8 : slabdata      1      1      0
biovec-256             2      2   4096    1    1 : tunables   60   30    8 : slabdata      2      2      0
biovec-128             0      0   2048    2    1 : tunables   60   30    8 : slabdata      0      0      0
biovec-64              0      0   1024    4    1 : tunables  124   62    8 : slabdata      0      0      0
biovec-16              0      0    256   15    1 : tunables  252  126    8 : slabdata      0      0      0
sock_inode_cache    1280   1309    576    7    1 : tunables  124   62    8 : slabdata    187    187      0
skbuff_head_cache   2390   3213    832    9    2 : tunables  124   62    8 : slabdata    357    357      0
file_lock_cache      336    336    184   21    1 : tunables  252  126    8 : slabdata     16     16      0
shmem_inode_cache   2794   3094    592   13    2 : tunables  124   62    8 : slabdata    238    238      0
task_delay_info      274    340    112   34    1 : tunables  252  126    8 : slabdata     10     10      0
taskstats              1     12    328   12    1 : tunables  124   62    8 : slabdata      1      1      0
proc_inode_cache    2548   2556    592    6    1 : tunables  124   62    8 : slabdata    426    426    232
sigqueue              26     72    160   24    1 : tunables  252  126    8 : slabdata      3      3      0
bdev_cache            17     20    768    5    1 : tunables  124   62    8 : slabdata      4      4      0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
sysfs_dir_cache    10098  10098    144   27    1 : tunables  252  126    8 : slabdata    374    374      0
mnt_cache             48     60    256   15    1 : tunables  252  126    8 : slabdata      4      4      0
filp               11892  13635    256   15    1 : tunables  252  126    8 : slabdata    909    909      0
inode_cache         3559   3577    528    7    1 : tunables  124   62    8 : slabdata    511    511      0
dentry             55582  56260    192   20    1 : tunables  252  126    8 : slabdata   2813   2813    236
names_cache           43     43   4096    1    1 : tunables   60   30    8 : slabdata     43     43      0
iint_cache           111    128    120   32    1 : tunables  252  126    8 : slabdata      4      4      0
buffer_head        24590  24605    104   37    1 : tunables  252  126    8 : slabdata    665    665      0
nsproxy                2     77     48   77    1 : tunables  252  126    8 : slabdata      1      1      0
vm_area_struct     42696  43470    168   23    1 : tunables  252  126    8 : slabdata   1890   1890    252
mm_struct            149    180    768    5    1 : tunables  124   62    8 : slabdata     36     36      0
fs_cache             156    354     64   59    1 : tunables  252  126    8 : slabdata      6      6      0
files_cache          156    176    704   11    2 : tunables  124   62    8 : slabdata     16     16      0
signal_cache         223    224   1024    4    1 : tunables  124   62    8 : slabdata     56     56      0
sighand_cache        223    225   2112    3    2 : tunables   60   30    8 : slabdata     75     75      0
task_struct          273    273   2368    3    2 : tunables   60   30    8 : slabdata     91     91      0
cred_jar             283    570    128   30    1 : tunables  252  126    8 : slabdata     19     19      0
anon_vma_chain     31924  34188     48   77    1 : tunables  252  126    8 : slabdata    444    444    252
anon_vma           15085  16579     64   59    1 : tunables  252  126    8 : slabdata    281    281      0
pid                  269    330    128   30    1 : tunables  252  126    8 : slabdata     11     11      0
radix_tree_node     4302   4788    560    7    1 : tunables  124   62    8 : slabdata    684    684      0
idr_layer_cache      215    219   2112    3    2 : tunables   60   30    8 : slabdata     73     73      0
size-4194304(DMA)      0      0 4194304    1 1024 : tunables    1    1    0 : slabdata      0      0      0
size-4194304           0      0 4194304    1 1024 : tunables    1    1    0 : slabdata      0      0      0
size-2097152(DMA)      1      1 2097152    1  512 : tunables    1    1    0 : slabdata      1      1      0
size-2097152           0      0 2097152    1  512 : tunables    1    1    0 : slabdata      0      0      0
size-1048576(DMA)      4      4 1048576    1  256 : tunables    1    1    0 : slabdata      4      4      0
size-1048576          69     69 1048576    1  256 : tunables    1    1    0 : slabdata     69     69      0
size-524288(DMA)       0      0 524288    1  128 : tunables    1    1    0 : slabdata      0      0      0
size-524288            0      0 524288    1  128 : tunables    1    1    0 : slabdata      0      0      0
size-262144(DMA)       0      0 262144    1   64 : tunables    1    1    0 : slabdata      0      0      0
size-262144            4      4 262144    1   64 : tunables    1    1    0 : slabdata      4      4      0
size-131072(DMA)       0      0 131072    1   32 : tunables    8    4    0 : slabdata      0      0      0
size-131072            3      3 131072    1   32 : tunables    8    4    0 : slabdata      3      3      0
size-65536(DMA)        0      0  65536    1   16 : tunables    8    4    0 : slabdata      0      0      0
size-65536             6      6  65536    1   16 : tunables    8    4    0 : slabdata      6      6      0
size-32768(DMA)        0      0  32768    1    8 : tunables    8    4    0 : slabdata      0      0      0
size-32768            38     38  32768    1    8 : tunables    8    4    0 : slabdata     38     38      0
size-16384(DMA)        0      0  16384    1    4 : tunables    8    4    0 : slabdata      0      0      0
size-16384            24     24  16384    1    4 : tunables    8    4    0 : slabdata     24     24      0
size-8192(DMA)         0      0   8192    1    2 : tunables    8    4    0 : slabdata      0      0      0
size-8192            109    109   8192    1    2 : tunables    8    4    0 : slabdata    109    109      0
size-4096(DMA)         0      0   4096    1    1 : tunables   60   30    8 : slabdata      0      0      0
size-4096           2498   2500   4096    1    1 : tunables   60   30    8 : slabdata   2498   2500      0
size-2048(DMA)         0      0   2048    2    1 : tunables   60   30    8 : slabdata      0      0      0
size-2048            796    798   2048    2    1 : tunables   60   30    8 : slabdata    399    399      0
size-1024(DMA)         1      4   1024    4    1 : tunables  124   62    8 : slabdata      1      1      0
size-1024           1267   1328   1024    4    1 : tunables  124   62    8 : slabdata    332    332      0
size-512(DMA)          0      0    512    8    1 : tunables  124   62    8 : slabdata      0      0      0
size-512            1399   1416    512    8    1 : tunables  124   62    8 : slabdata    177    177      0
size-256(DMA)          0      0    256   15    1 : tunables  252  126    8 : slabdata      0      0      0
size-256             256    285    256   15    1 : tunables  252  126    8 : slabdata     19     19      0
size-192(DMA)          0      0    192   20    1 : tunables  252  126    8 : slabdata      0      0      0
size-192           11992  12340    192   20    1 : tunables  252  126    8 : slabdata    617    617    188
size-128(DMA)          0      0    128   30    1 : tunables  252  126    8 : slabdata      0      0      0
size-64(DMA)           0      0     64   59    1 : tunables  252  126    8 : slabdata      0      0      0
size-64           897962 905591     64   59    1 : tunables  252  126    8 : slabdata  15349  15349      0
size-32(DMA)           0      0     64   59    1 : tunables  252  126    8 : slabdata      0      0      0
size-128            3926   7350    128   30    1 : tunables  252  126    8 : slabdata    245    245      0
size-32             7544   8024     64   59    1 : tunables  252  126    8 : slabdata    136    136      0
kmem_cache           143    160    192   20    1 : tunables  252  126    8 : slabdata      8      8      0
```

会话相关

会话统计

```
diagnose sys session full-stat
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

路由相关

路由表查看

当前路由表

```
get router info routing-table all
```

路由database

```
get router info routing-table database
```

OSPF

OSPF状态

```
get router info ospf status
```

OSPF邻居

```
get router info ospf neighbor
```

BGP

BGP状态

```
get router info bgp summary
```

BGP邻居

```
get router info bgp neighbors
```

BGP路由

```
get router info bgp network
```

BGP邻居收到/通告的路由

```bash
get router info bgp neighbors x.x.x.x received-routes
get router info bgp neighbors x.x.x.x advertised-routes
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate Support Tool

功能描述

FortiGate Support Tool是一个浏览器插件，它能够在FortiGate的图形用户界面上执行后台调试，以收集各种运行信息或错误信息。当您遇到FortiGate GUI相关的问题时，如页面无法正常显示，页面打开速度慢等，可以尝试使用该插件收集相关信息，并发送至Fortinet TAC团队进行分析。

该插件需要FortiOS为6.2.2 GA或更高版本才能正常工作，目前支持Chrome/Edge浏览器。

获取插件

- 通过Chrome商店 ↗下载。
- 离线安装包 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

重要

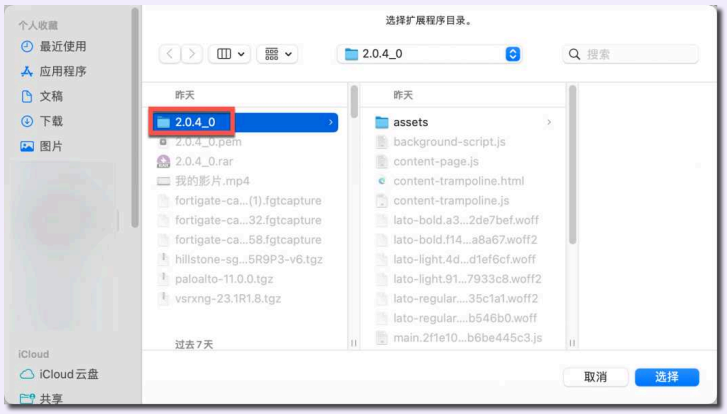
插件离线安装包的安装方法：

1. 解压离线安装包。

2. 进入Chrome的插件管理，开启“开发者模式”，点击“加载已解压的扩展程序”。



3. 选择已解压的离线安装包文件夹。



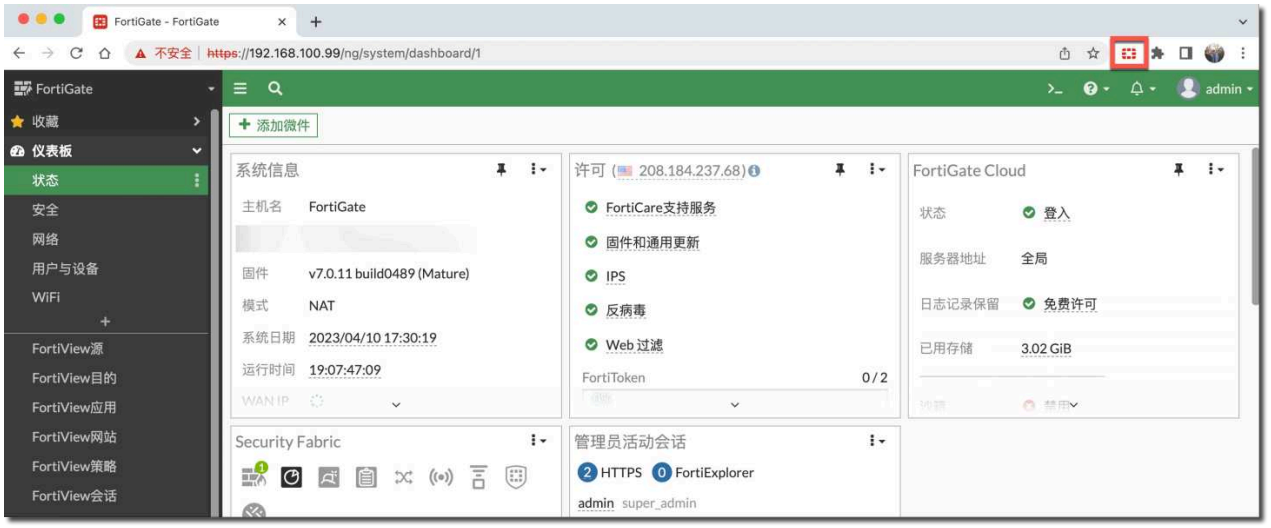
4. 安装成功。



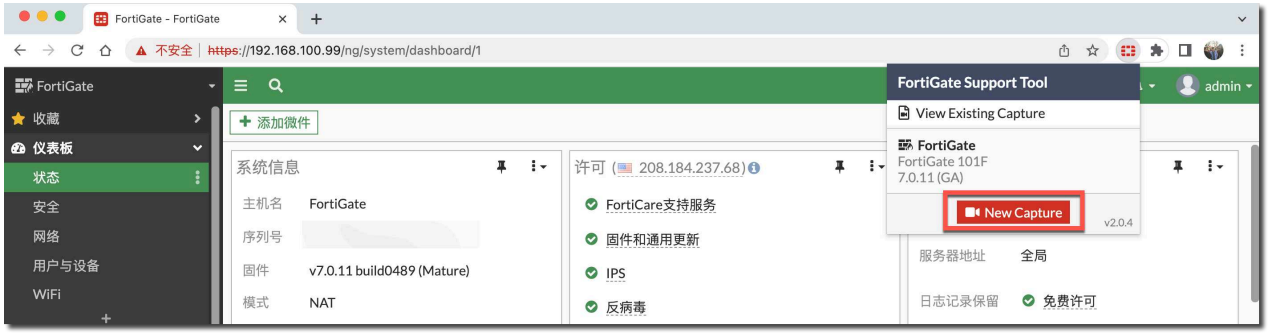
使用方法

1. 在非FortiGate管理页面浏览期间，扩展程序的图标颜色显示为灰色。 当进入FortiGate的GUI时（登录成功），可以看到该扩展程序图标变红。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



2. 点击该插件图标，并点击“New Capture”按钮，开始捕获和收集信息。



3. 可选择收集GUI或System种类。



- GUI：全面的捕获，包括视频操作记录、浏览器日志和用户选择的后端守护程序日志。最长时间限制为10分钟。
- System：轻量级捕获用户选择的后端守护程序日志，无需记录视频或浏览器活动。最长时间限制为120分钟。

4. 这里以GUI为例，选择“Deamon Logging”（收集的守护进程日志，一般默认即可），点击“Start Capture”。

5. 开启插件的捕获后，在GUI操作重现您的问题现象，重现完成后，停止捕获（点击页面右上角的停止图标），将自动从浏览器下载收集信息文件。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.





6. 最后，创建Ticket并将该文件提供给FortiGate TAC团队以供进一步分析。

7. 附操作过程演示视频：

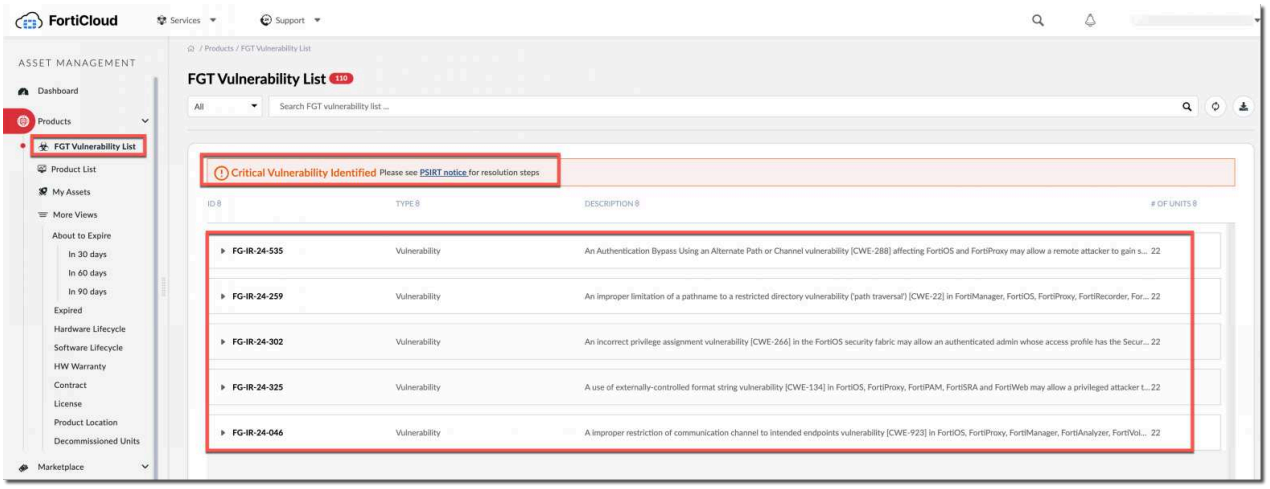


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

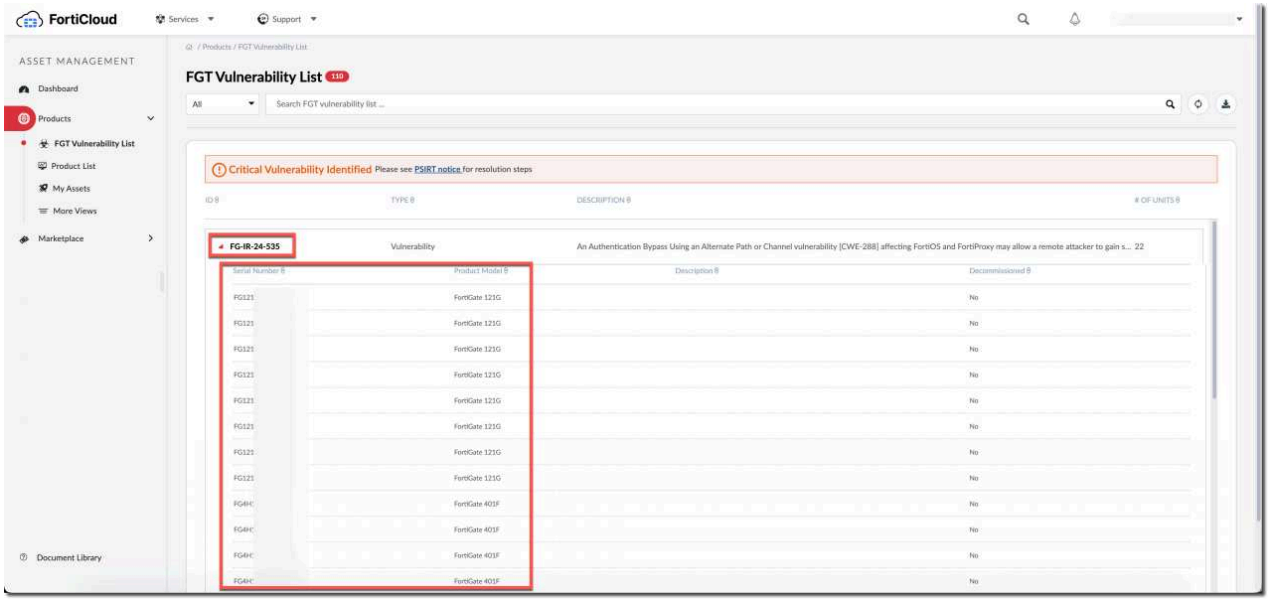
高频关注

版本漏洞查询

1. 使用设备注册的FortiCloud账户登录https://support.fortinet.com/asset/#/views/products ↗，如果当前账户中检测到至少一个已存在漏洞的设备时，导航菜单中的“Product”中将会出现“FGT Vulnerability List”页面，该页面会显示所有相关漏洞信息。如下所示，FortiCloud账户中存在FortiOS版本为7.0.15的设备，该版本存在的漏洞会被列出。

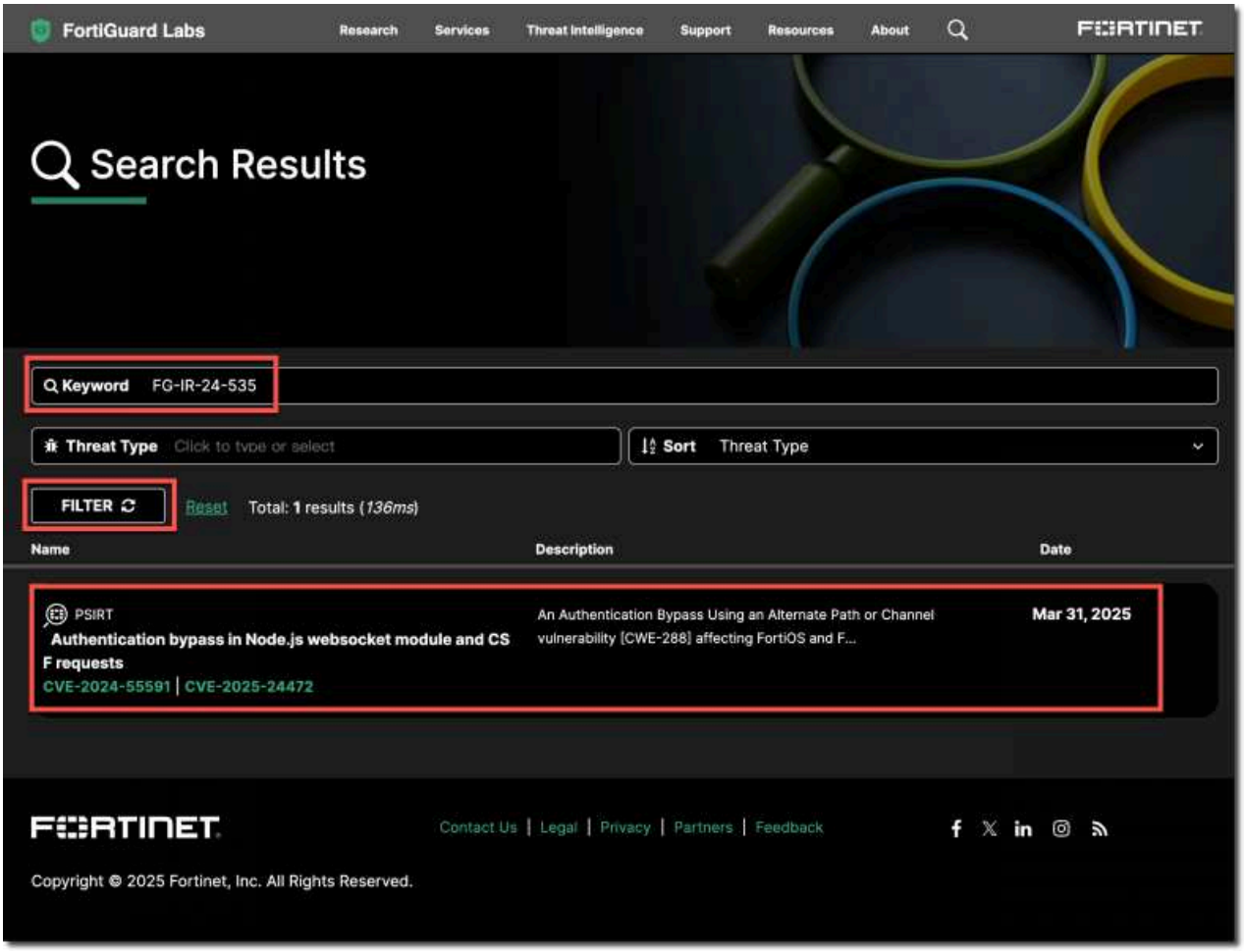


2. 点开某个漏洞ID的折叠项，漏洞列表包括已确定存在关键漏洞的设备列表以及漏洞相关信息。



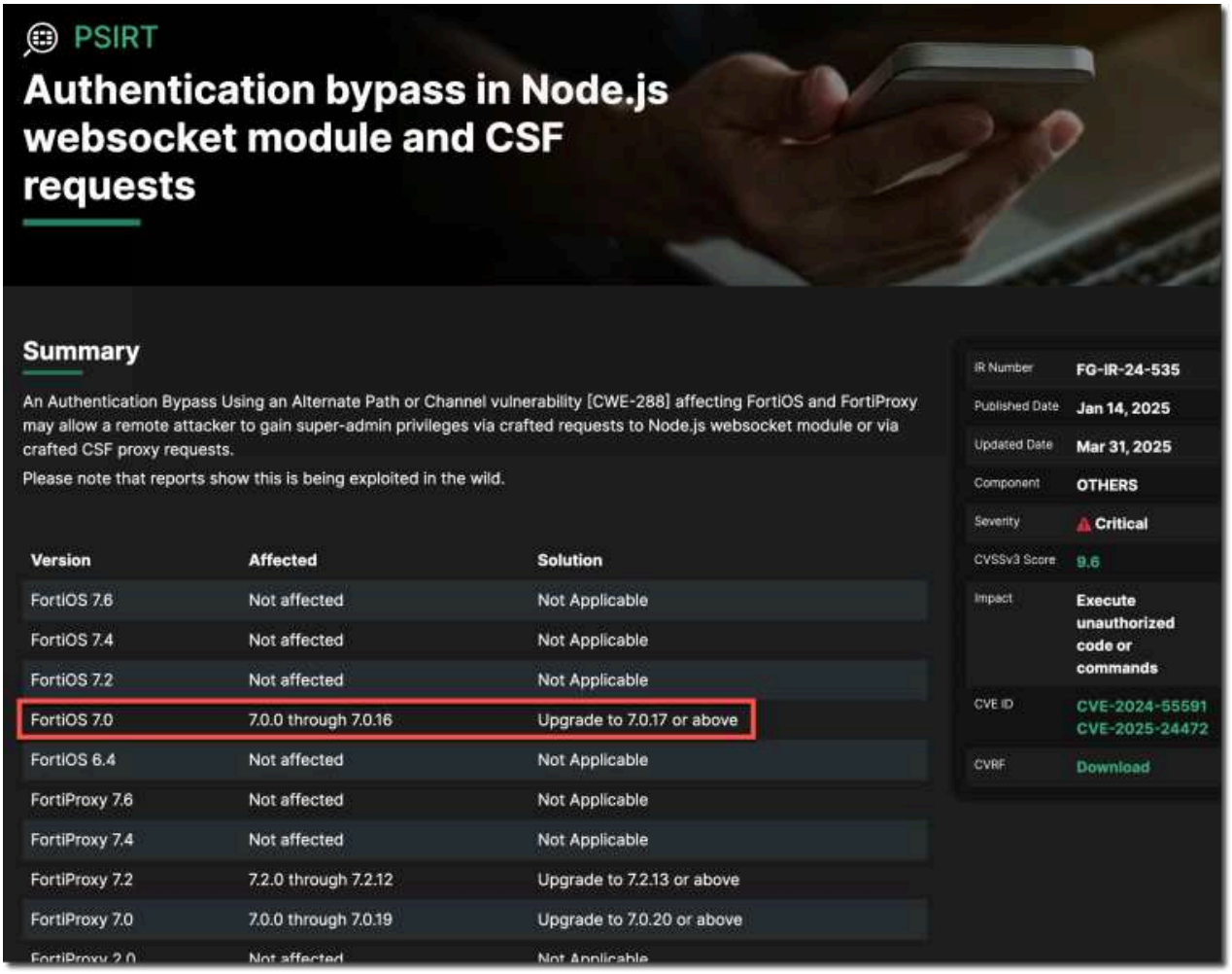
3. 如果您在以上页面中发现存在漏洞的设备版本，请访问https://fortiguard.fortinet.com/search ↗，搜索漏洞ID（如 `FG-IR-24-535` ）。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



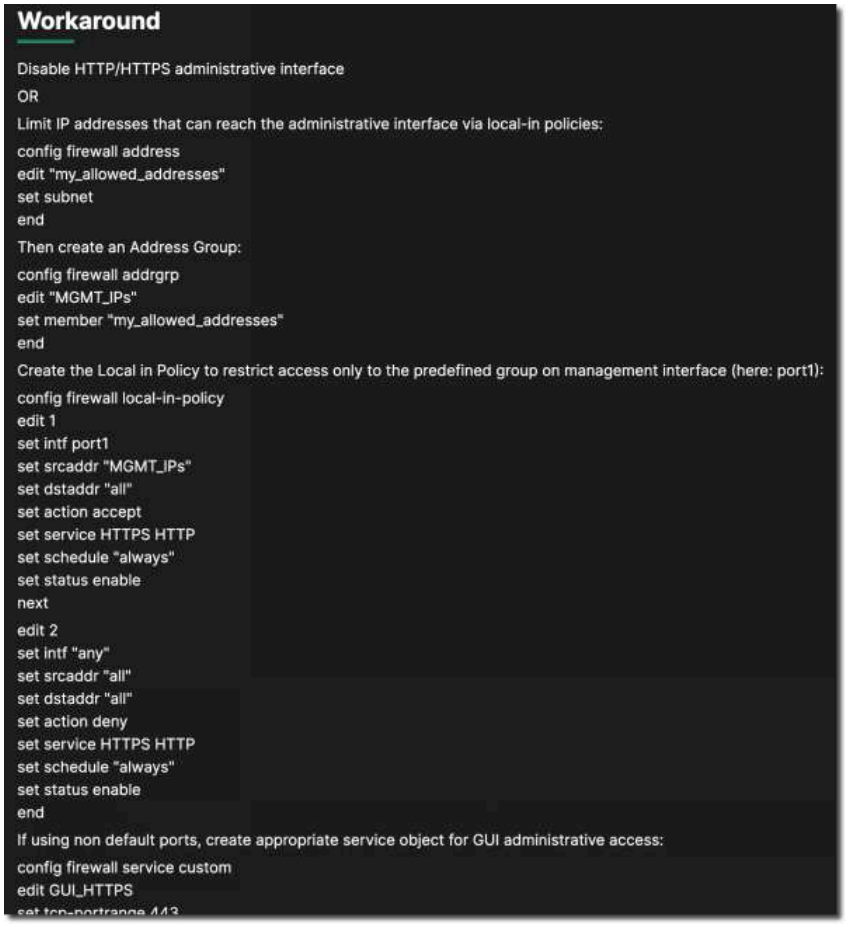
4. 点击进入该漏洞详情，可以查询该漏洞的升级解决方案、Workaround等信息。如下所示，FortiOS需要升级至7.0.17版本以解决该漏洞。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



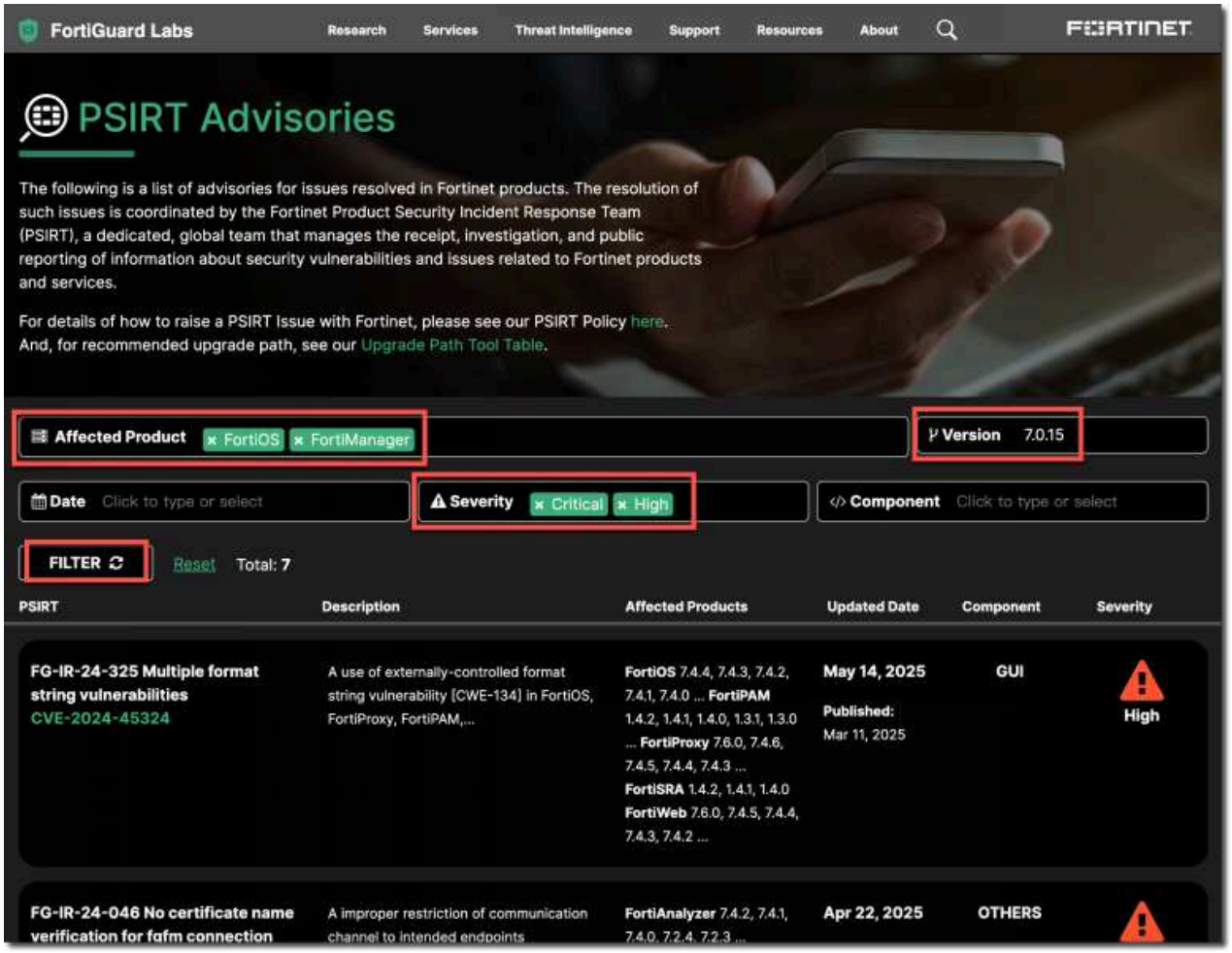
5. 也可以根据页面内的Workaround（如果有）暂时规避该漏洞。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



6. 访问此链接：https://www.fortiguard.com/psirt ↗ ，可以通过过滤特定产品/版本/严重程度等信息，查询相关的漏洞信息。

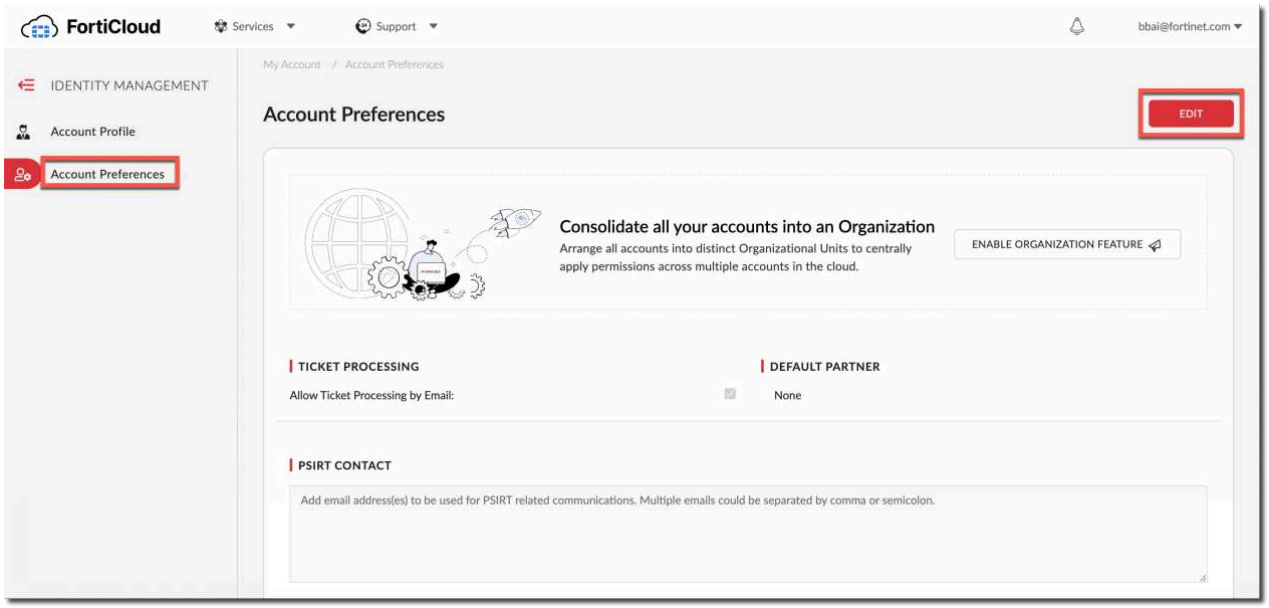
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



订阅漏洞更新

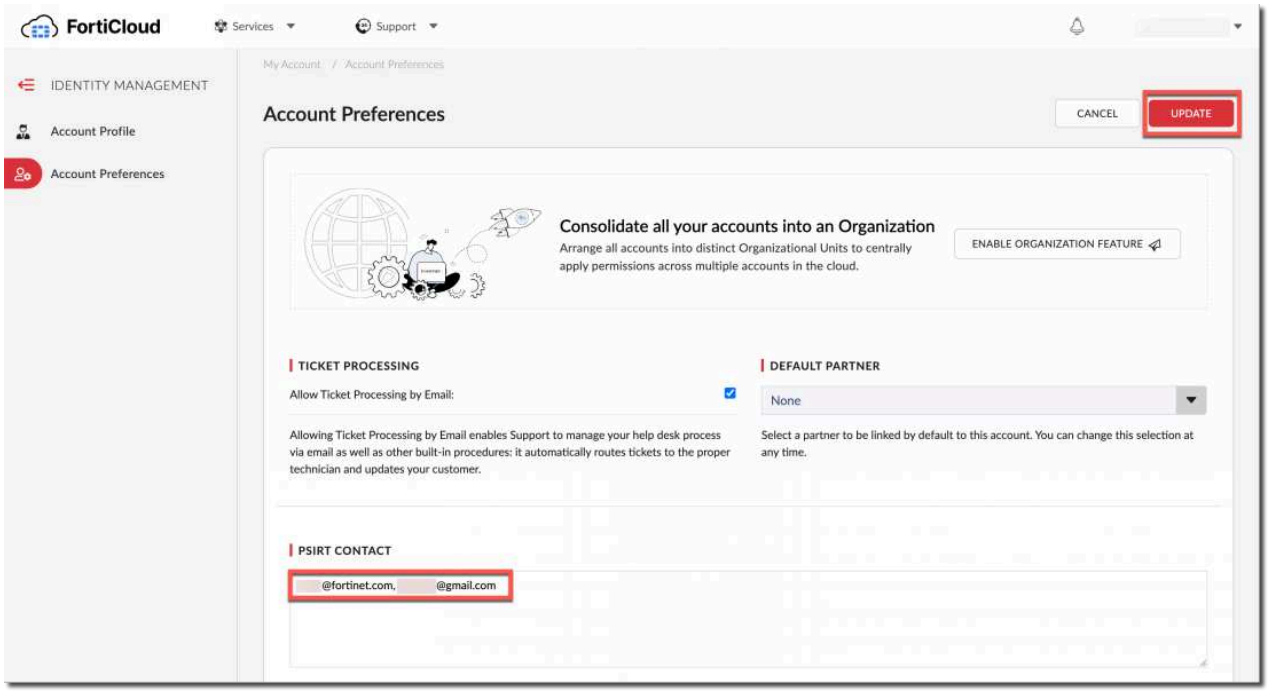
Email订阅

1. 使用设备注册的FortiCloud账户登录https://support.fortinet.com/cred/#/sec/my-account/account-preferences ↗ （Account Preferences页面），点页面击右上角的“EDIT”按钮。

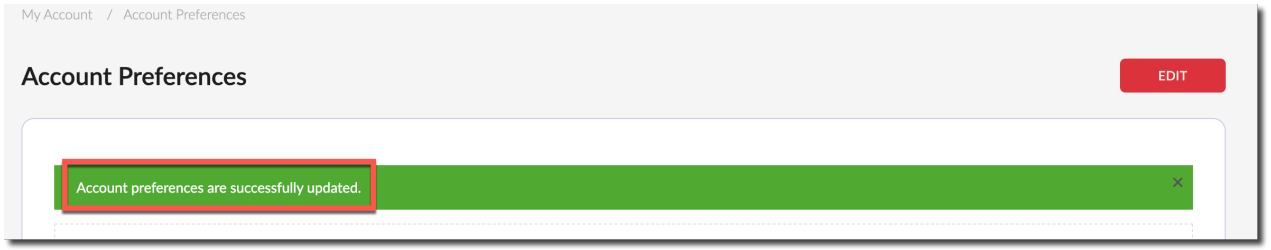


2. 在“PSIRT CONTACT”处填写需要接收漏洞公告的邮箱，可以填写多个邮箱，以英文`,`或`;`分隔。填写完成后，点击页面右上角的“UPDATE”按钮。

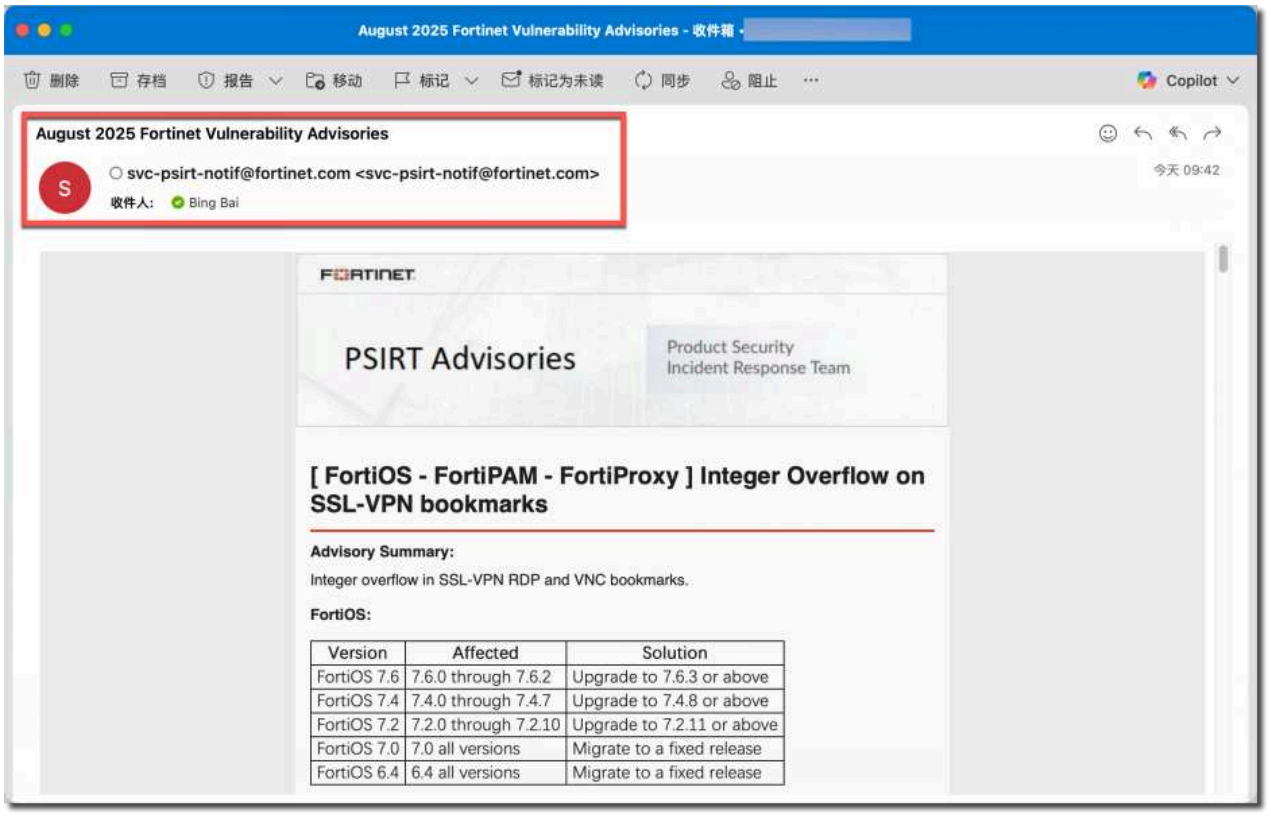
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



3. 页面提示账户更新成功。



4. 在新的PSIRT更新发布后，相关邮箱可以收到PSIRT更新邮件，发件人为`svc-psirt-notif@fortinet.com`。

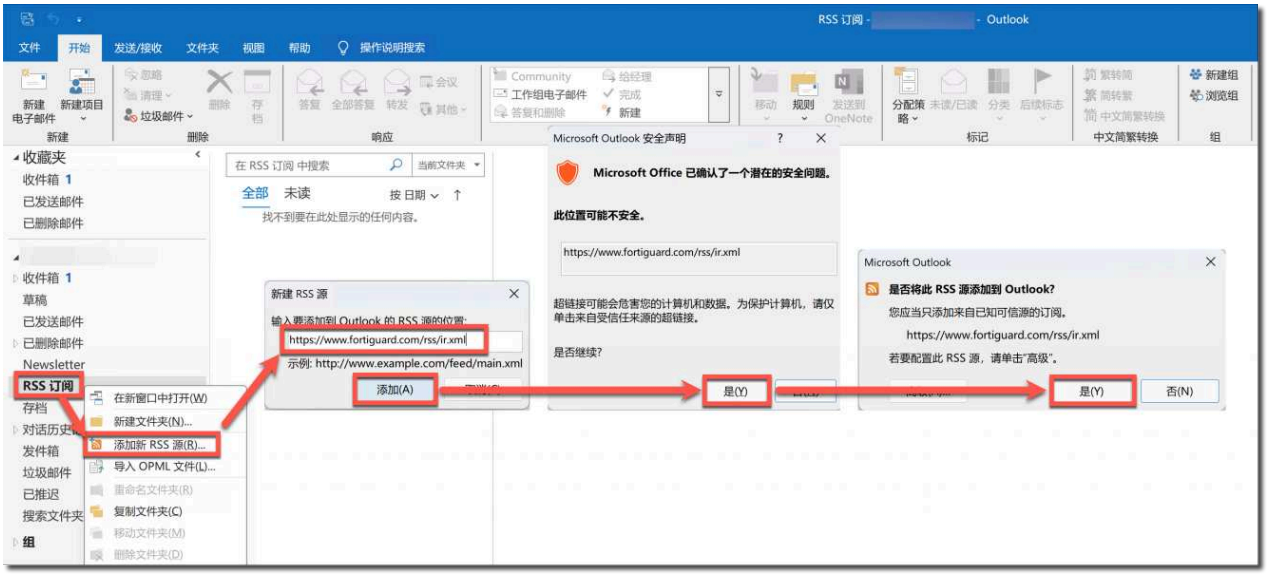


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

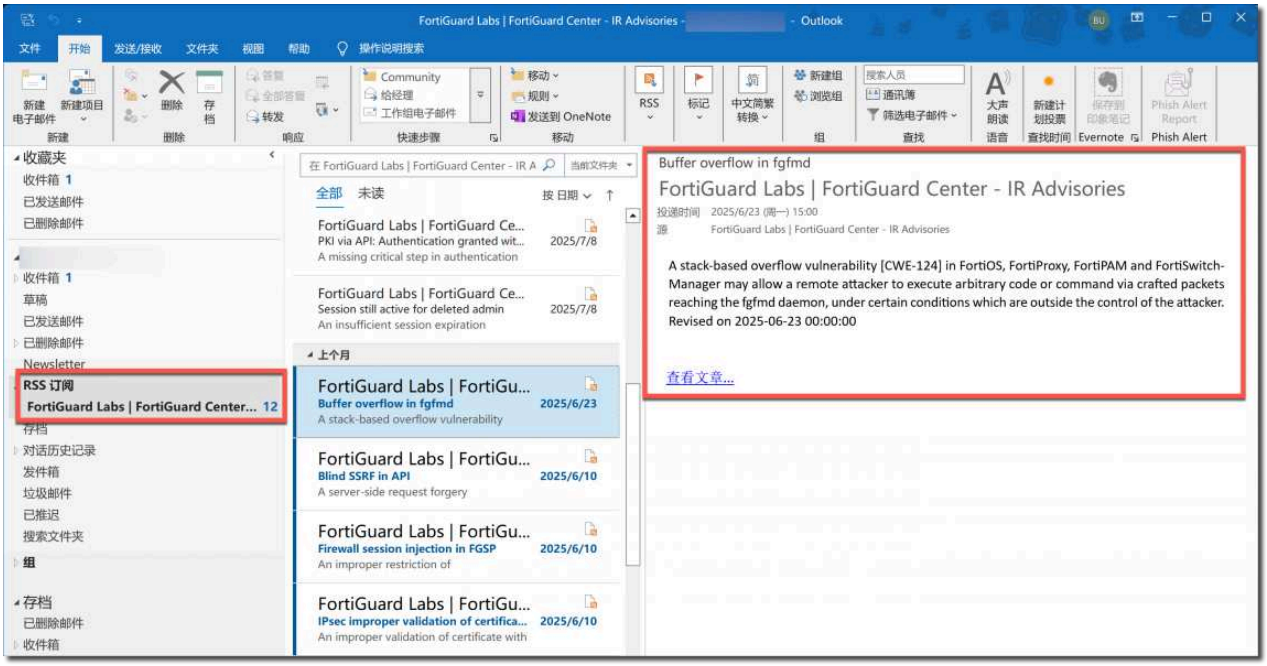
RSS订阅

1. RSS源（`https://www.fortiguard.com/rss/ir.xml`），包含所有漏洞的链接，可在所选RSS阅读器中进行通知。

2. 以Outlook为例，右键点击“开始→RSS订阅”，选择“添加新RSS源”，输入FortiGuard PSIRT RSS源（`https://www.fortiguard.com/rss/ir.xml`），点击“添加”按钮，随后在弹出的“Microsoft Outlook安全声明”窗口中点击“是”，随后再次在弹出的窗口中点击“是”。



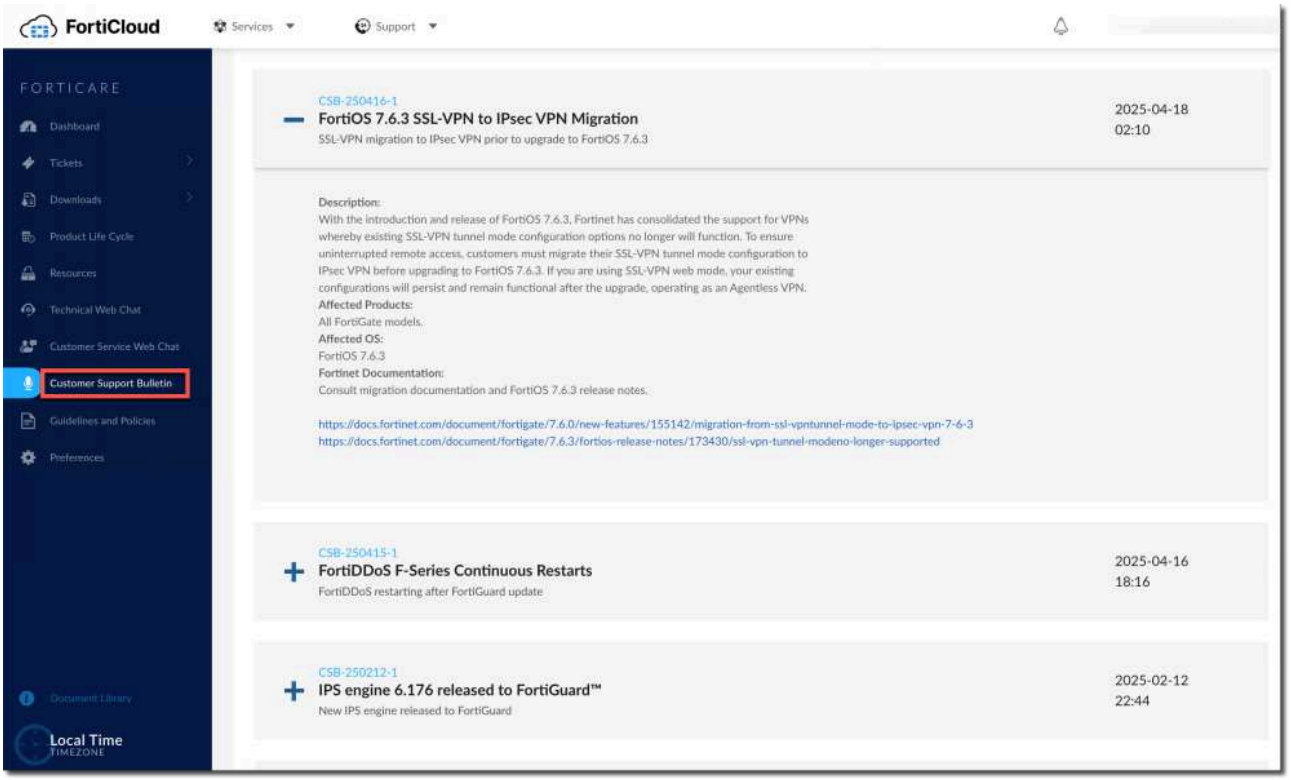
3. RSS订阅添加成功，Outlook自动下载了历史所有的PSIRT公告，并会在新的PSIRT公告发布后自动更新。



重要事件公告

使用设备注册的FortiCloud账户登录https://support.fortinet.com/support/#/bulletin ↗ ，可以查看Fortinet各个产品发布的新功能、错误修复、版本漏洞发布、版本注意事项等信息。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

运维注意事项

请参考运维注意事项↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2GB内存设备配置优化

简介

本文介绍如何减少2GB内存入门级FortiGate设备在进入内存保护模式前的内存使用率。当前≤2GB设备的型号如下：

30D/30E/30G/40C/40F/50E/50G/60D/60E/61E/60F/61F/70D/80C/80D/80E/81E/90D/91/92D

这类设备的一个突出问题是：基础内存占用就很高（约50%～70%），预留的内存空间有限。一旦遭遇突发事件，如网络流量突然增加、大量并发会话、攻击或短时高峰流量，内存极易飙升至阈值，从而触发“内存保护”模式。进入该模式后，设备会作为保护措施阻止新的连接请求，虽然能避免系统崩溃，但也可能影响业务连续性。这种情况在低端型号中尤为常见，因此必须特别关注内存的合理使用和优化。

查看内存大小

要检查FortiGate的内存大小与使用情况，可在设备CLI下运行`diagnose hardware sysinfo memory`（或`get hardware memory`、`fnsysctl cat /proc/meminfo`）命令，如下所示，FortiGate-60F的总内存大小为2GB：

```bash
FortiGate-60F # diagnose hardware sysinfo memory
MemTotal:        1963616 kB
MemFree:          493552 kB
Buffers:           39388 kB
Cached:           537824 kB
SwapCached:            0 kB
Active:           675400 kB
Inactive:         126488 kB
Active(anon):     485728 kB
Inactive(anon):    42588 kB
Active(file):     189672 kB
Inactive(file):    83900 kB
Unevictable:      190276 kB
Mlocked:           20400 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                76 kB
Writeback:             0 kB
AnonPages:        414976 kB
Mapped:           135568 kB
Shmem:            121484 kB
Slab:             209332 kB
SReclaimable:      16468 kB
SUnreclaim:       192864 kB
KernelStack:        3968 kB
PageTables:        31116 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:      981808 kB
Committed_AS:   13450496 kB
VmallocTotal:   260046784 kB
VmallocUsed:      126860 kB
VmallocChunk:   259812288 kB
```

优化建议

使用推荐版本或型号

- 建议在网络规划阶段评估业务需求，并根据性能要求选择合适规格的FortiGate型号，以避免后续扩容风险。设备选型请联系[se_china@fortinet.com](mailto: se_china_fortinet.com)。
- 强烈建议在FortiGate上使用推荐的FortiOS版本。推荐版本通常包含对内存相关问题的修复和优化，可提升系统稳定性与可靠性。FortiGate各型号版本推荐请参考：系统管理→固件与配置管理→固件版本管理→固件下载↗章节。

FortiGuard更新

1. 优化FortiGuard更新相关配置。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```bash
config system fortiguard
    set webfilter-cache-ttl 600              ←——减小WebFilter缓存时间，默认值3600
    set antispam-cache-ttl 600               ←——减小反垃圾邮件缓存时间，默认值1800
    set outbreak-prevention-cache-ttl 300    ←——减小病毒爆发防御缓存时间，默认值300
    set update-ffdb disable                  ←——只在设备未进入“内存保护模式”时更新ISDB
end
```

2. 修改FortiGuard更新间隔。

```bash
config system autoupdate schedule
    set frequency daily                      ←——将FortiGuard自动更新间隔增加到每天
    set time 03:00                           ←——FortiGuard自动更新时间为凌晨3:00
end
```

会话时间

1. 减少TCP会话相关状态的超时时间，更快释放内存。请根据FortiGate的实际流量情况调整以下值：

```bash
config system global
    set reset-sessionless-tcp disable
    set tcp-halfclose-timer 30  ←——减小TCP halfclose超时时间，默认值120
    set tcp-halfopen-timer 5    ←——减小TCP halfopen超时时间，默认值10
    set tcp-timewait-timer 0    ←——减小TCP timewait超时时间，默认值1
    set udp-idle-timer 60       ←——减小UDP超时时间，默认值180
end
```

2. 减少TCP会话和DNS会话的老化时间。

```bash
config system session-ttl
    set default 300
    config port
        edit 0
            set protocol 17
            set timeout 10
            set end-port 53
            set start-port 53
        next
    end
end
```

系统配置

1. 关闭安全评级相关功能。

```bash
config system global
    set internet-service-database on-demand        ←——仅下载已使用的ISDB条目
    set security-rating-result-submission disable  ←——关闭安全评级结果提交
    set security-rating-run-on-schedule disable    ←——关闭安全评级执行计划
end
```

2. 减少部分系统进程的数量。如果FortiGate上某些进程同时运行多个实例，应适当减少其数量（谨慎操作）。

```bash
config system global
    set miglogd-children 1
    set sslvpn-max-worker-count 1
    set wad-worker-count 1
    set scanunit-count 2
end
```

3. 减少DNS缓存条目的老化时间。

```bash
config system dns
    set dns-cache-limit 600  ←——DNS缓存条目最大数，默认值5000
    set dns-cache-ttl 600    ←——DNS缓存条目老化时间，默认值1800
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

日志相关

1. 关闭报告功能。对于2GB或4GB内存型号，不建议启用报告功能，会消耗较多比例的内存。

```bash
config report setting
    set pdf-report disable
    set fortiview disable
end

diagnose report-runner clean  ←——删除之前已生成的报告文件
```

2. 关闭内存日志，关闭硬盘日志记录流量日志，推荐将日志发送到FortiAnalyzer或syslog服务器。

```bash
config log memory setting
    set status disable
end

config log disk filter
    set forward-traffic disable
end
```

UTM相关

1. 启用IPS的`fail-open`，设备进入“内存保护模式”后bypass需要检测的流量。

```bash
config ips global
    set fail-open enable
    set cp-accel-mode none
end
```

2. 关闭AV启发式扫描。

```bash
config antivirus settings
    set machine-learning-detection disable
end
```

3. 缺省的AV扫描文件大小为10 MB，可能会导致内存消耗太多进入“内存保护模式”。根据病毒要求传播快的特点，一般病毒文件都不会太大，所以可以调整扫描文件的大小：
   - 配置自定义的profile-protocol-options，设置各个应用的扫描阈值为1 MB，大于1 MB的文件会被AV bypass：

```bash
config firewall profile-protocol-options
    edit "av-profile-options"
        set oversize-log enable
        config http
            set ports 80
            set options clientcomfort servercomfort chunkedbypass
            unset post-lang
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
            set stream-based-uncompressed-limit 2
        end
        config ftp
            set ports 21
            set options clientcomfort splice
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
            set stream-based-uncompressed-limit 2
        end
        config imap
            set ports 143
            set options fragmail
            set oversize-limit 1
            set uncompressed-oversize-limit 2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            set uncompressed-nest-limit 2
        end
        config mapi
            set ports 135
            set options fragmail
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
        end
        config pop3
            set ports 110
            set options fragmail
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
        end
        config smtp
            set ports 25
            set options fragmail splice
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
        end
        config nntp
            set ports 119
            set options splice
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
        end
        config ssh
            unset options
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
            set stream-based-uncompressed-limit 2
        end
        config dns
            set ports 53
        end
        config cifs
            set ports 445
            unset options
            set oversize-limit 1
            set uncompressed-oversize-limit 2
            set uncompressed-nest-limit 2
        end
    next
end
```

- 需要在防火墙策略内调用相应的profile-protocol-options才能生效。

```bash
config firewall policy
    edit <policy_id>
          set profile-protocol-options av-profile-options
    next
end
```

自动化重启IPS

结合正常期间的内存占用，调整内存利用率高的阈值，当内存高时，自动触发IPS engine重启并释放内存。重启IPS engine不会影响业务流量。

1. 降低进入“内存保护模式”的green和red阈值，内存值到达`memory-use-threshold-red`设置的75%时，会进入“内存保护模式”，当FortiGate进入“内存保护模式”后，如果内存在red和extreme之间时，新会话不会被丢弃，继续转发，当内存到达extreme时开始丢弃新会话。

```bash
config system global
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 70  ←——默认值82
    set memory-use-threshold-red 75    ←——默认值88
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

2. 配置自动化触发器，触发条件为设备进入了“内存保护模式”。

```bash
config system automation-trigger
    edit "Enters_Conserve_Mode"
        set event-type low-memory
    next
end
```

3. 配置自动化动作，动作内容为重启IPS Engine。

```bash
config system automation-action
    edit "RestartIPS"
        set action-type cli-script
        set script "config global    ←——如果未开启多VDOM，则不需要此行
diagnose test application ipsmonitor 99"
        set accprofile "super_admin"
    next
end
```

4. 配置自动化工作流，绑定触发条件和动作。

```bash
config system automation-stitch
    edit "Restart_IPS_during_Conserve_Mode"
        set trigger "Enters_Conserve_Mode"
        config actions
            edit 1
                set action "RestartIPS"
            next
        end
    next
end
```

5. 补充：也可以设置一个周期性重启IPS的自动化（可以与上述脚本同时使用），如下所示，每天凌晨4点重启IPS engine。

```bash
config system automation-trigger
    edit "4AM"
        set trigger-type scheduled
        set trigger-hour 4
    next
end

config system automation-action
    edit "RestartIPS"
        set action-type cli-script
        set script "config global    ←——如果未开启多VDOM，则不需要此行
diagnose test application ipsmonitor 99"
        set accprofile "super_admin"
    next
end

config system automation-stitch
    edit "RestartIPS"
        set trigger "4AM"
        config actions
            edit 1
                set action "RestartIPS"
            next
        end
    next
end
```

注意事项

1. 上述优化配置的具体参数应根据您的实际网络状态进行调整。
2. 从FortiOS 7.4.4版本开始，从 ≤ 2GB内存的设备上移除了代理相关的功能。
3. 从FortiOS 7.6.3版本开始，从 ≤ 2GB内存的设备上移除了部分Security Fabric相关功能。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

常用维护命令

请参考：常用维护命令手册 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

收集客户信息

在项目实施前，请先确认以下关键信息是否有遗漏，并提前做好上点规划，避免上线后出现问题。同时为后续可能出现故障问题能快速排查定位打下铺垫。

1. 网络拓扑信息（了解网络拓扑信息有助于网络方案的规划）

2. 环境信息（了解部署位置、部署模式、最大吞吐、最大用户数有助于对设备性能的评估）

3. 客户需求，对FortiGate部署的功能要求（了解客户要求部署上FortiGate后需要开启哪些功能和访问控制策略以明确配置思路）

4. FortiGate设备的IP地址规划（了解FortiGate设备部署时所需要的基本网络配置，如IP地址、子网掩码、网关、路由、DNS以确定具体配置内容）

5. FortiGate接入链路信息（了解现网的链路及接口状态，提前确认设备接口是否能够满足）

6. 收集好割接前后的业务访问信息，如ping包延时、网页打开速度等信息，割接后对网络的性能做对比 。

记录项目	ping包延时	
	平时	高峰
割接前	网站Ping延时 ping www.sina.com 延时：XXms ping www.baidu.com 延时：XXms	网站Ping延时 ping www.sina.com 延时：XXms ping www.baidu.com 延时：XXms
割接后	网站Ping延时 ping www.sina.com 延时：XXms ping www.baidu.com 延时：XXms 与割接前进行对比，确认延时浮动是否会超过10ms以上	网站Ping延时 ping www.sina.com 延时：XXms ping www.baidu.com 延时：XXms 与割接前进行对比，确认延时浮动是否会超过10ms以上

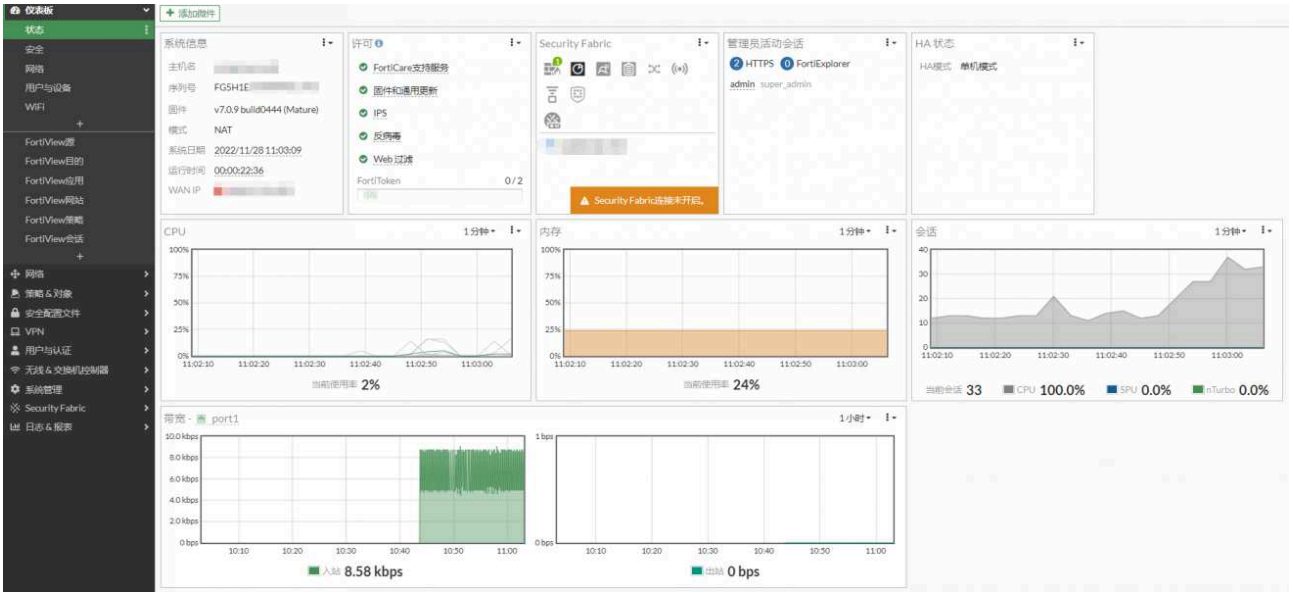
记录项目	网页打开速度	
	平时	高峰
割接前	记录打开网页的体验 打开 www.163.com 延时：XXms 打开 www.sina.com 延时：XXms	记录打开网页的体验 打开 www.163.com 延时：XXms 打开 www.sina.com 延时：XXms
割接后	记录打开网页的体验 打开 www.163.com 延时：XXms 打开 www.sina.com 延时：XXms 与割接前进行对比，确认网页打开时间是否会比割接前慢5秒以上	记录打开网页的体验 打开 www.163.com 延时：XXms 打开 www.sina.com 延时：XXms 与割接前进行对比，确认网页打开时间是否会比割接前慢5秒以上

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

设备软件检查

首页信息

进入系统首页可以产看 设备的型号、硬件序列号、软件序列号、系统版本、运行时间、系统时间、HA模式、运行模式、接口状态、系统资源：cpu、内存、磁盘使用情况，告警信息等。

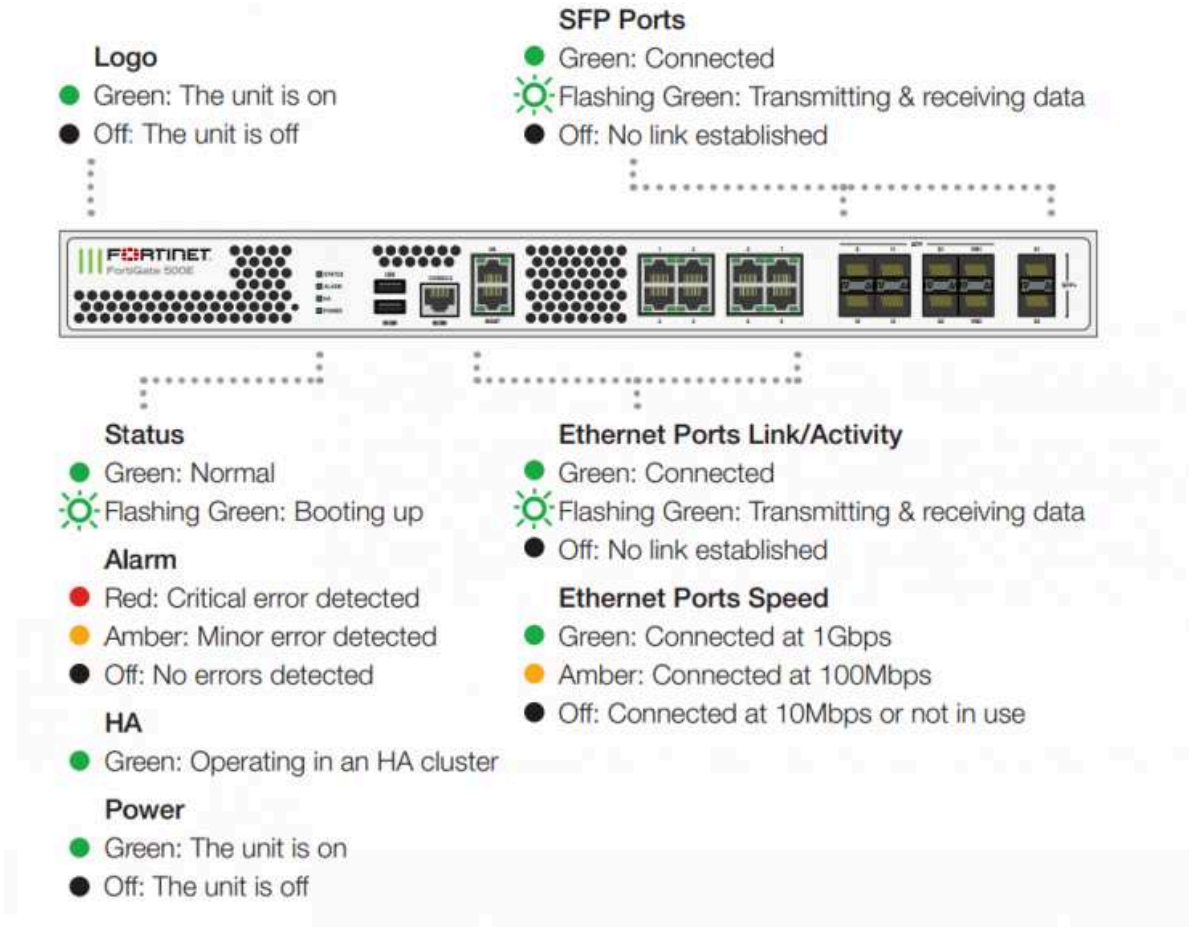


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

设备硬件检查

环境/指示灯维护

1. 清洁状况：设备外壳、设备内部、机架内各防尘网、地板等都应干净整洁无明显尘土附着。注意机柜防尘网的清洁状况，及时清洗更换，以免影响机柜门及风扇框的通风散热。
2. 散热状况：设备正常工作时，要求保持风扇正常运转，擅自关闭风扇会引起设备温度升高，并可能损坏设备。不要在设备子架上通风口处放置杂物，还应定期清理风扇的防网。
3. 设备指示灯及状态，请参考设备硬件指南：https://docs.fortinet.com/product/fortigate/hardware ↗ ，如FortiGate 500E



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

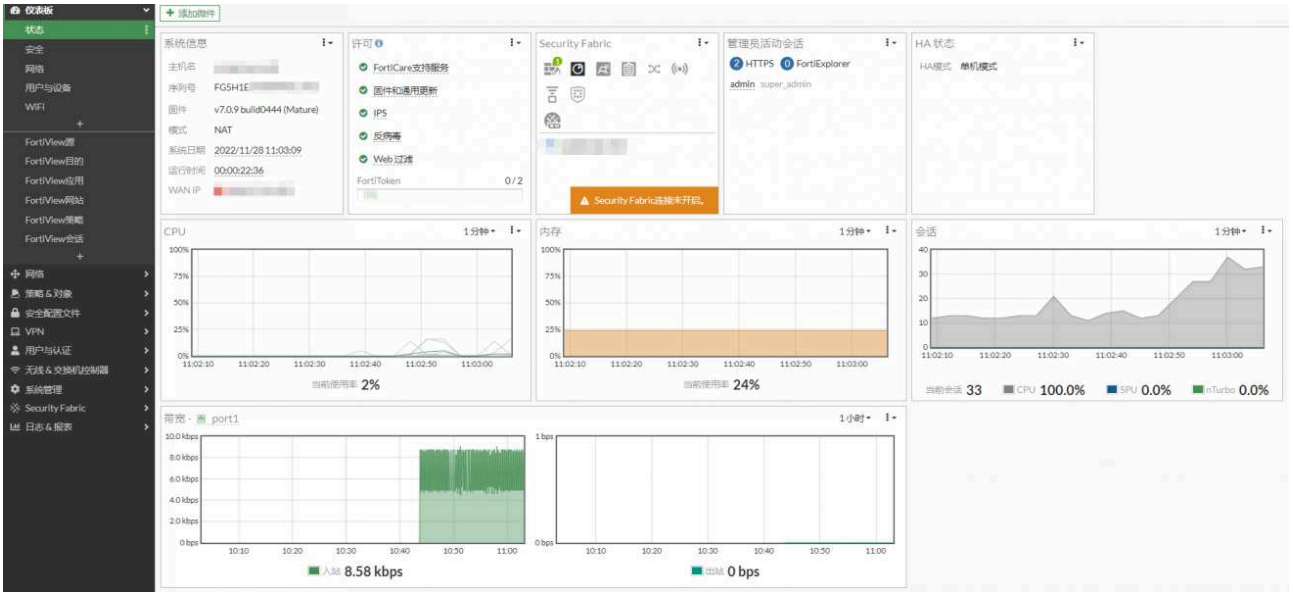
"状态"界面，通过添加"微件"的方式，如接口流量，如下图，查看cpu、内存、接口流量和会话数。 CPU和内存利用率通常应低于80%，如果CPU或者内存长时间利用率高，应分析原因。 image-20221128112105632">"状态"界面，通过添加"微件"的方式，如接口流量，如下图，查看cpu、内存、接口流量和会话数。 CPU和内存利用率通常应低于80%，如果CPU或者内存长时间利用率高，应分析原因。 image-20221128112105632">

基础检查

2025/10/29 小于 1 分钟

在"仪表板"-->"状态"界面，通过添加"微件"的方式，如接口流量，如下图，查看cpu、内存、接口流量和会话数。

CPU和内存利用率通常应低于80%，如果CPU或者内存长时间利用率高，应分析原因。



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

运行情况

使用命令行的方式查看更详细的信息

1. 查看系统基本信息

```
# get system status
Version: FortiGate-501E v7.0.9,build0444,221121 (GA.M)
Firmware Signature: certified
Virus-DB: 90.08232(2022-11-27 22:26)
Extended DB: 90.08232(2022-11-27 22:26)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 2.08576(2022-11-27 21:45)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 22.00446(2022-11-24 01:49)
APP-DB: 22.00444(2022-11-22 02:49)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 4.00543(2022-11-27 12:14)
Serial-Number: FG5H1Exxxxxx
BIOS version: 05000005
System Part-Number: P21592-08
Log hard disk: Available
Hostname: FGTxxxxxx
Private Encryption: Disable
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0444
Release Version Information: GA
FortiOS x86-64: Yes
System time: Mon Nov 28 14:49:17 2022
Last reboot reason: warm reboot
```

2. 查看硬件状态

```
# get hardware status
Model name: FortiGate-501E
ASIC version: CP9
ASIC SRAM: 64M
CPU: Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
Number of CPUs: 8
RAM: 16047 MB
Compact Flash: 15331 MB /dev/sdc
Hard disk: 228936 MB /dev/sda
USB Flash: not available
Network Card chipset: Intel(R) Gigabit Ethernet Linux Driver (rev.0003)
Network Card chipset: FortiASIC NP6 Adapter (rev.)
```

3. 查看CPU和内存利用率

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU2 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU4 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU5 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU6 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU7 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 16432720k total, 4086464k used (24.9%), 11961200k free (72.8%), 385056k freeable (2.3%)
Average network usage: 191 / 2 kbps in 1 minute, 263 / 11 kbps in 10 minutes, 268 / 4 kbps in 30 minutes
Maximal network usage: 283 / 42 kbps in 1 minute, 553 / 1422 kbps in 10 minutes, 553 / 1422 kbps in 30 minutes
Average sessions: 11 sessions in 1 minute, 10 sessions in 10 minutes, 8 sessions in 30 minutes
Maximal sessions: 16 sessions in 1 minute, 19 sessions in 10 minutes, 19 sessions in 30 minutes
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes, 0
sessions per second in last 30 minutes
Maximal session setup rate: 3 sessions per second in last 1 minute, 3 sessions per second in last 10 minutes, 3
sessions per second in last 30 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Average nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal nTurbo sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days,  4 hours,  10 minutes
```

4. 查看会话状态

```
# diagnose sys session full-stat
session table:           table_size=4194304 max_depth=1 used=66
misc info:       session_count=35 setup_rate=0 exp_count=0 clash=0
        memory_tension_drop=0 ephemeral=0/1113088 removeable=0 extreme_low_mem=0
        npu_session_count=0
        nturbo_session_count=0
delete=6, flush=5, dev_down=98/137 ses_walkers=0
TCP sessions:
         11 in ESTABLISHED state
         1 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ips_recv=00000000
policy_deny=00006bae
av_recv=00000000
fqdn_count=00000001
fqdn6_count=00000000
```

5. 查看HA状态

```
# get system ha status
HA Health Status: OK
Model: FortiGate-501E
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:21:11
Cluster state change time: 2022-11-28 15:13:06
Primary selected using:
    <2022/11/28 15:13:06> FG5H1ExxxxxxB is selected as the primary because its uptime is larger than peer member
FG5H1E5819904211.
    <2022/11/28 15:13:06> FG5H1ExxxxxxA is selected as the primary because its override priority is larger than
peer member FG5H1E5819904036.
    <2022/11/28 15:10:15> FG5H1ExxxxxxA is selected as the primary because it's the only member in the cluster.
ses_pickup: disable
override: disable
Configuration Status:
    FG5H1ExxxxxxA(updated 4 seconds ago): out-of-sync
    FG5H1ExxxxxxB(updated 0 seconds ago): in-sync
System Usage stats:
    FG5H1ExxxxxxA(updated 4 seconds ago):
        sessions=11, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=24%
    FG5H1ExxxxxxB(updated 0 seconds ago):
        sessions=17, average-cpu-user/nice/system/idle=0%/0%/1%/98%, memory=21%
HBDEV stats:
    FG5H1ExxxxxxA(updated 4 seconds ago):
        port6: physical/1000full, up, rx-bytes/packets/dropped/errors=47426063/99344/0/0, tx=461507/1005/0/0
    FG5H1ExxxxxxB(updated 0 seconds ago):
        port6: physical/1000full, up, rx-bytes/packets/dropped/errors=1169224/2536/0/0, tx=3000908/6578/0/0
Secondary   : FGT1, FG5H1ExxxxxxA, HA cluster index = 0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
Primary     : FGT2, FG5H1ExxxxxxB, HA cluster index = 1
number of vcluster: 1
vcluster 1: standby 169.254.0.2
Secondary: FG5H1ExxxxxxA, HA operating index = 1
Primary: FG5H1ExxxxxxA, HA operating index = 0
```

6. 查看crashlog是否异常

```
# diagnose debug crashlog read
1: 2022-11-23 17:32:57 the killed daemon is /bin/sflowd: status=0×0
2: 2022-11-23 17:34:55 the killed daemon is /bin/dhcpd: status=0×0
3: 2022-11-23 01:38:40 the killed daemon is /bin/getty: status=0×0
4: 2022-11-23 01:41:32 the killed daemon is /bin/fgfmd: status=0×0
5: 2022-11-28 10:41:47 the killed daemon is /bin/sflowd: status=0×0
Crash log interval is 3600 seconds
Max crash log line number: 16384
```

7. 查看进程状态

```
# diagnose sys top 3 100 3    可判断每个进程的cpu和内存的利用率，敲一次c 按cpu高低排序；敲一次m，按mem高低排序，敲q退出
第一个3是间隔3s，100是显示的进程数，最后一个3是执行3次
Run Time:  0 days, 4 hours and 16 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 16047T, 11679F
       ipshelper      228      S <     0.0     1.6    0
       ipsengine      357      S <     0.0     0.5    1
       ipsengine      360      S <     0.0     0.5    4
       ipsengine      363      S <     0.0     0.5    6
       ipsengine      358      S <     0.0     0.5    2
       ipsengine      361      S <     0.0     0.5    7
       ipsengine      362      S <     0.0     0.5    5
       ipsengine      359      S <     0.0     0.5    3
            node      215      S       0.0     0.3    1
         cmdbsvr      180      S       0.0     0.3    2
         miglogd      234      S       0.0     0.2    0
             wad      284      S       0.0     0.2    7
             wad      283      S       0.0     0.2    4
             wad      285      S       0.0     0.2    2
             wad      286      S       0.0     0.2    0
             wad      287      S       0.0     0.2    3
             wad      289      S       0.0     0.2    2
             wad      290      S       0.0     0.2    0
             wad      288      S       0.0     0.2    4
       scanunitd      238      S <     0.0     0.2    2
         miglogd      298      S       0.0     0.2    4
         miglogd      299      S       0.0     0.2    1
         miglogd      301      S       0.0     0.2    1
         miglogd      300      S       0.0     0.2    6
       forticron      222      S       0.0     0.1    2
       extenderd      266      S       0.0     0.1    0
          cw_acd      257      S       0.0     0.1    0
         updated      239      S       0.0     0.1    5
           fgfmd      256      S       0.0     0.1    0
          httpsd      214      S       0.0     0.1    4
         reportd      235      S       0.0     0.1    5
          newcli     1330      S       0.0     0.1    6
       scanunitd     1318      S <     0.0     0.1    6
       scanunitd     1319      S <     0.0     0.1    1
       scanunitd     1320      S <     0.0     0.1    6
       scanunitd     1321      S <     0.0     0.1    6
       scanunitd     1322      S <     0.0     0.1    2
       scanunitd     1323      S <     0.0     0.1    0
       scanunitd     1324      S <     0.0     0.1    2
       scanunitd     1325      S <     0.0     0.1    4
       forticldd      223      S       0.0     0.1    2
 initXXXXXXXXXXX        1      S       0.0     0.1    2
        dnsproxy      268      S       0.0     0.1    2
             wad      281      S       0.0     0.0    6
          cu_acd      261      S       0.0     0.0    0
          httpsd     1300      S       0.0     0.0    2
          fnbamd      220      S       0.0     0.0    2
           autod      267      S       0.0     0.0    2
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
            authd      224      S       0.0     0.0    0
           newcli     1357      R       0.0     0.0    1
            authd      312      S       0.0     0.0    5
            authd      311      S       0.0     0.0    2
            authd      313      S       0.0     0.0    1
            authd      314      S       0.0     0.0    2
        eap_proxy      255      S       0.0     0.0    1
       wf_monitor      245      S       0.0     0.0    2
          foauthd      225      S       0.0     0.0    0
              wad      237      S       0.0     0.0    6
             sshd      247      S       0.0     0.0    2
            voipd      236      S       0.0     0.0    2
            snmpd      240      S       0.0     0.0    6
           fcnacd      230      S       0.0     0.0    0
              nsm      198      S       0.0     0.0    0
         syslogd      219      S       0.0     0.0    2
           flcfgd      262      S       0.0     0.0    2
            radvd      251      S       0.0     0.0    4
            dhcpd      241      S       0.0     0.0    6
       urlfilter      377      S <     0.0     0.0    2
          wpad_ac      259      S       0.0     0.0    4
      fortilinkd      260      S       0.0     0.0    1
  zebos_launcher      193      S       0.0     0.0    2
           quard      250      S       0.0     0.0    0
   cw_acd_helper      258      S       0.0     0.0    7
            ntpd      246      S <     0.0     0.0    0
        dnsproxy      253      S       0.0     0.0    6
          lldptx      243      S       0.0     0.0    3
    ipmc_sensord      212      S       0.0     0.0    2
            sshd     1329      S       0.0     0.0    0
          lldprx      242      S       0.0     0.0    2
          flpold      263      S       0.0     0.0    6
         uploadd      211      S       0.0     0.0    6
      ipsmonitor      217      S       0.0     0.0    5
             acd      244      S       0.0     0.0    2
           getty      216      S <     0.0     0.0    4
       alertmail      252      S       0.0     0.0    6
             fsd      265      S       0.0     0.0    0
           fsvrd      249      S       0.0     0.0    2
             fas      229      S       0.0     0.0    6
             wad      279      S       0.0     0.0    4
         telnetd      248      S       0.0     0.0    3
  merged_daemons      218      S       0.0     0.0    6
      clearpass      226      S       0.0     0.0    1
      fsso_ldap      232      S       0.0     0.0    1
       kmiglogd      213      S       0.0     0.0    2
           xcvrd      233      S       0.0     0.0    4
        httpclid      227      S       0.0     0.0    2
       fclicense      221      S       0.0     0.0    6
             imi      210      S       0.0     0.0    6
            bgpd      203      S <     0.0     0.0    5
            pimd      205      S       0.0     0.0    0
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

日志查看

查看FortiGate各日志模块是否有异常日志，如系统事件，HA事件，入侵防御，反病毒等。



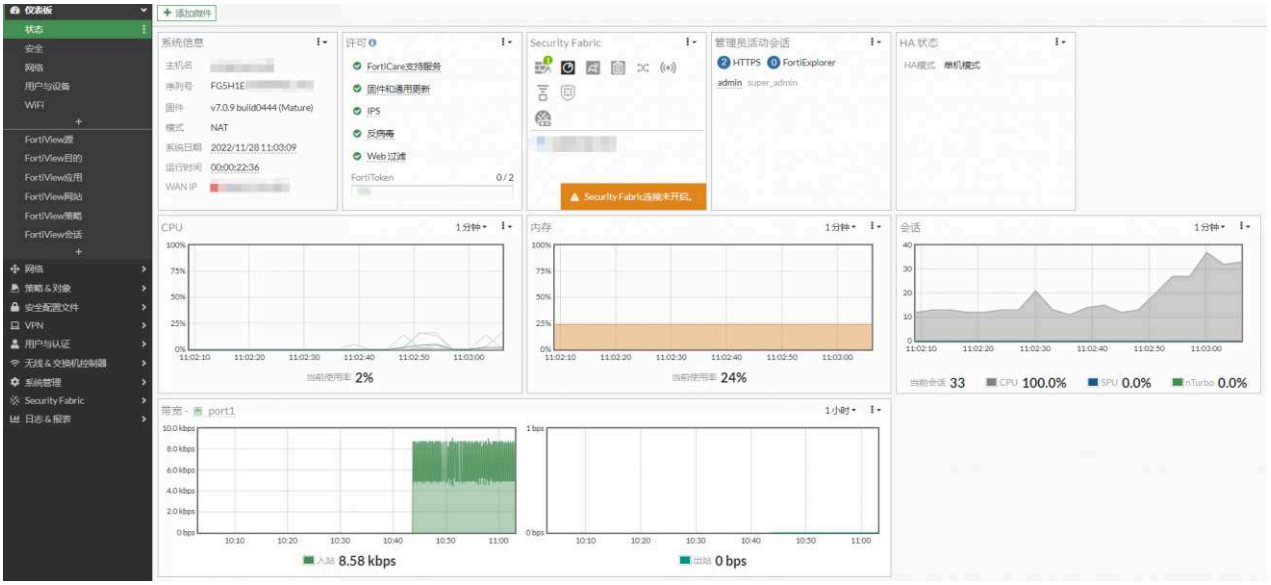
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

"状态"界面，通过添加"微件"的方式，如接口流量，如下图，查看cpu、内存、接口流量和会话数。 image-20221128112105632 如何查看设备接口的流量 答：在仪表板-->状态，选择“添加微件”，点击“接口带宽”，选择对应的业务接口。image-20221202143609105 image-202212021...">"状态"界面，通过添加"微件"的方式，如接口流量，如下图，查看cpu、内存、接口流量和会话数。 image-20221128112105632 如何查看设备接口的流量 答：在仪表板-->状态，选择“添加微件”，点击“接口带宽”，选择对应的业务接口。image-20221202143609105 image-202212021...">

运维监控

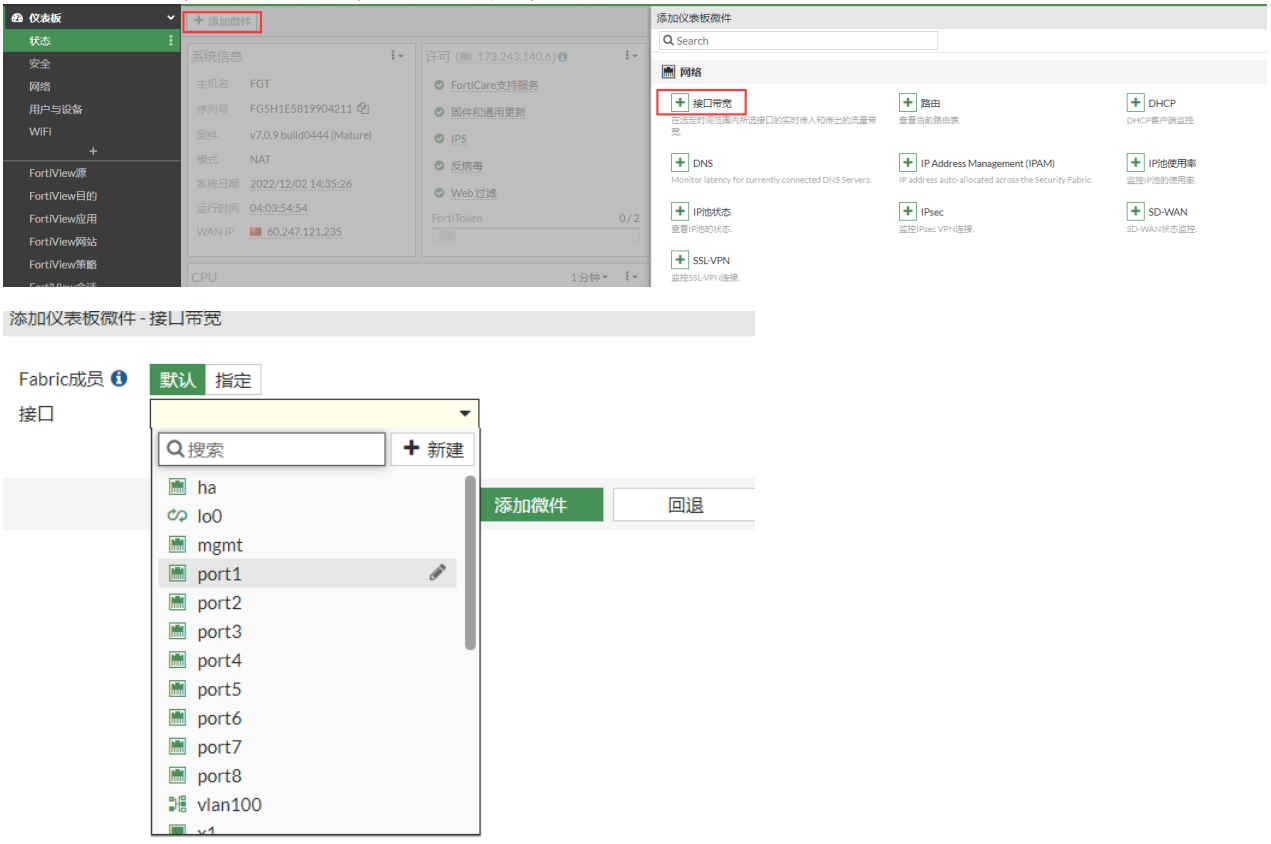
2025/10/29 大约 1 分钟

1. 在"仪表板"-->"状态"界面，通过添加"微件"的方式，如接口流量，如下图，查看cpu、内存、接口流量和会话数。



2. 如何查看设备接口的流量

答：在仪表板-->状态，选择“添加微件”，点击“接口带宽”，选择对应的业务接口。



3. 如何通过SNMP管理并监控FortiGate的系统运行及性能情况。

答：a.开启设备的SNMP，配置步骤请参考系统管理→SNMP→SNMP的设置 ↗。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

b.在SNMP配置界面下方可直接下载FortiGate SNMP MIB文件，并将MIB文件导入进MIB Browser、PRTG Network Monitor、Cacti等MIB管理监控工具。

c.通过MIB工具可读取出设备的相关CPU使用率、MEM使用率、硬盘使用率、新建会话数、并发会话数等关键参数， 以下为整理出来的常用MIB OID参数值。

```
FortiGate设备名称          sysName          OID: 1.3.6.1.2.1.1.5
FortiGate设备序列号        fnSysSerial      OID: 1.3.6.1.4.1.12356.100.1.1.1
FortiGate设备软件版本      fgSysVersion     OID: 1.3.6.1.4.1.12356.101.4.1.1
FortiGate设备运行时间      sysUpTime        OID: 1.3.6.1.2.1.1.3
CPU 使用率                 fgSysCpuUsage    OID: 1.3.6.1.4.1.12356.101.4.1.3
MEM使用率                  fgSysMemUsage    OID: 1.3.6.1.4.1.12356.101.4.1.4
硬盘使用率                 fgSysDiskUsage   OID: 1.3.6.1.4.1.12356.101.4.1.6
IPv4并发会话数             fgSysSesCount    OID: 1.3.6.1.4.1.12356.101.4.1.8
IPv4新建会话数（1分钟）     fgSysSesRate1    OID: 1.3.6.1.4.1.12356.101.4.1.11
IPv6并发会话数             fgSysSes6Count   OID: 1.3.6.1.4.1.12356.101.4.1.15
IPv6新建会话数（1分钟）     fgSysSesRate1    OID: 1.3.6.1.4.1.12356.101.4.1.16
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

FortiGate通用多运营商路由导入脚本

运营商地址列表

电信、网通的路由表是不断在更新的，可以通过https://ispip.clang.cn/ ↗ 查看运营商的地址列表

ISP IP列表 HTML格式 CIDR

文件	描述	数据	更新时间	大小
all_cn_cidr.html	中国大陆所有IP地址	5441条	2022-11-23 00:33:36	85.57 KB
chinatelecom_cidr.html	中国电信	1724条	2022-11-23 00:33:36	28.48 KB
unicom_cnc_cidr.html	中国联通/网通	655条	2022-11-23 00:33:36	12.77 KB
cmcc_cidr.html	中国移动	46条	2022-11-23 00:33:36	3.68 KB
crtc_cidr.html	中国铁通	17条	2022-11-23 00:33:36	3.23 KB
cernet_cidr.html	中国教育网	81条	2022-11-23 00:33:36	4.17 KB
gwbn_cidr.html	长城宽带/鹏博士	172条	2022-11-23 00:33:36	5.64 KB
othernet_cidr.html	中国其他ISP	3290条	2022-11-23 00:33:36	53.71 KB
hk_cidr.html	中国香港	2250条	2022-11-23 00:33:36	37.86 KB
mo_cidr.html	中国澳门	29条	2022-11-23 00:33:36	3.44 KB
tw_cidr.html	中国台湾	657条	2022-11-23 00:33:36	13.08 KB

ISP IP列表 TXT格式 CIDR

文件	描述	数据	更新时间	大小
all_cn_cidr.txt	中国大陆所有IP地址	5441条	2022-11-23 00:33:36	82.58 KB
chinatelecom_cidr.txt	中国电信	1724条	2022-11-23 00:33:36	25.49 KB
unicom_cnc_cidr.txt	中国联通/网通	655条	2022-11-23 00:33:36	9.77 KB
cmcc_cidr.txt	中国移动	46条	2022-11-23 00:33:36	710 B

如点击“unicom_cnc_cidr.html”，就可以看到联通的地址列表

ispip.clang.cn/unicom_cnc.html

```
#################################################################
# ISP 中国联通(网通) 所有IP地址段表
# 数据来自于：https://ispip.clang.cn/
# 数据生成时间:2022-11-23 00:33:36
# 共计数据 890 条
# 脚本自动生成,如有错漏或任何建议,请联系admin[at]clang.cn
#################################################################
1.24.0.0/13
1.56.0.0/13
1.188.0.0/14
14.204.0.0/15
27.0.128.0/22
27.8.0.0/13
27.36.0.0/14
27.40.0.0/13
27.50.128.0/17
27.54.192.0/18
27.98.224.0/19
27.112.0.0/18
27.115.0.0/17
27.192.0.0/11
36.32.0.0/14
36.248.0.0/14
39.64.0.0/11
42.1.128.0/17
42.4.0.0/14
42.48.0.0/15
```

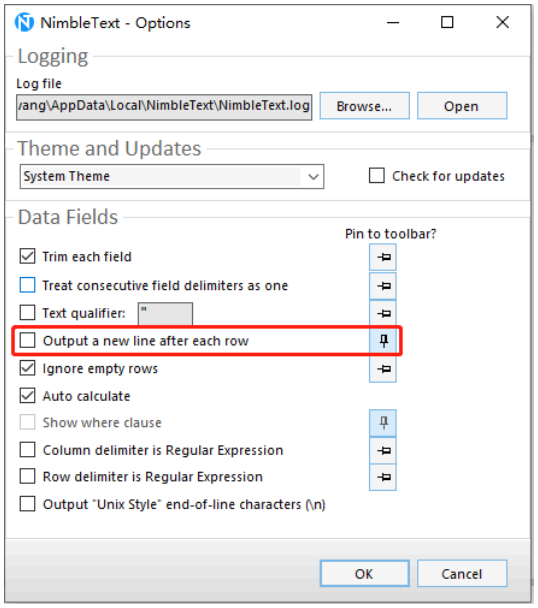
生成运营商路由脚本

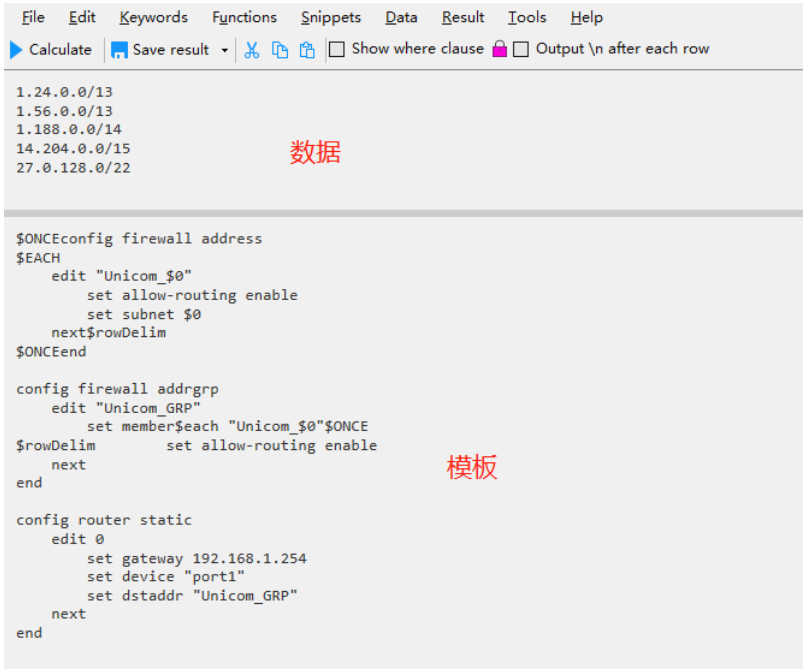
根据运营商地址列表，在FortiGate中生成对应的运营商路由。可以python，NimbleText等工具生成，这里使用NimbleText，其官网链接：http://nimbletext.com/ ↗

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

1. 通过NimbleText生成地址对象条目，这里截取联通地址列表的一部分做示范，其他的同理。

   在NimbleText选择“Tools”，点击“options...”，取消勾选“Output a new line after each row”





Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

Calculate auto

```
config firewall address
    edit "Unicom_1.24.0.0/13"
        set allow-routing enable
        set subnet 1.24.0.0/13
    next
    edit "Unicom_1.56.0.0/13"
        set allow-routing enable
        set subnet 1.56.0.0/13
    next
    edit "Unicom_1.188.0.0/14"
        set allow-routing enable
        set subnet 1.188.0.0/14
    next
    edit "Unicom_14.204.0.0/15"
        set allow-routing enable
        set subnet 14.204.0.0/15
    next
    edit "Unicom_27.0.128.0/22"
        set allow-routing enable
        set subnet 27.0.128.0/22
    next
end

config firewall addrgrp
    edit "Unicom_GRP"
        set member "Unicom_1.24.0.0/13" "Unicom_1.56.0.0/13" "Unicom_1.188.0.0/14" "Unicom_14.204.0.0/15" "Unicom_27.0.128.0/22"
        set allow-routing enable
    next
end

config router static
    edit 0
        set gateway 192.168.1.254
        set device "port1"
        set dstaddr "Unicom_GRP"
    next
end
```

结果

模板中的脚本，其中config router static下的gateway和device需要根据现场的环境修改

```
$ONCEconfig firewall address
$EACH
    edit "Unicom_$0"
        set allow-routing enable
        set subnet $0
    next$rowDelim
$ONCEend

config firewall addrgrp
    edit "Unicom_GRP"
        set member$each "Unicom_$0"$ONCE
$rowDelim        set allow-routing enable
    next
end

config router static
    edit 0
        set gateway 192.168.1.254       #改为现场环境使用的网关ip
        set device "port1"              #改为现场环境使用的接口
        set dstaddr "Unicom_GRP"
    next
end
```

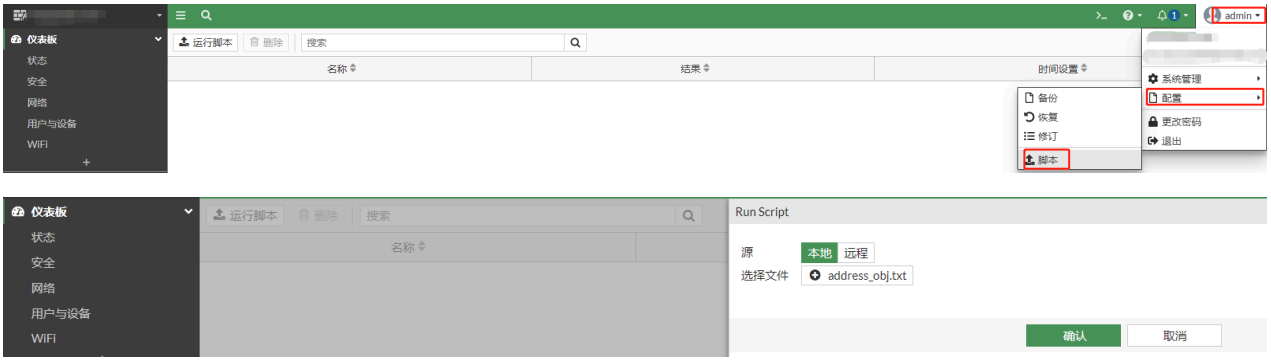
2. 将生成的结果保存在notepad++中，然后点击“编码”-->“使用UTF-8编码“并保存



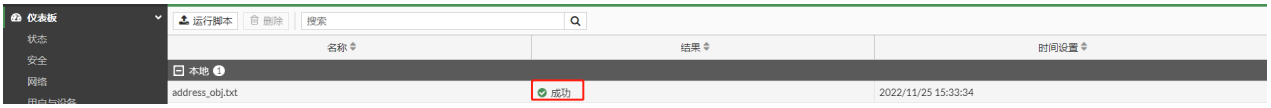
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall address
    edit "Unicom_1.24.0.0/13"
        set allow-routing enable
        set subnet 1.24.0.0/13
    next
    edit "Unicom_1.56.0.0/13"
        set allow-routing enable
        set subnet 1.56.0.0/13
    next
    edit "Unicom_1.188.0.0/14"
        set allow-routing enable
        set subnet 1.188.0.0/14
    next
    edit "Unicom_27.8.0.0/13"
        set allow-routing enable
        set subnet 27.8.0.0/13
    next
end

config firewall addrgrp
    edit "Unicom_GRP"
        set member "Unicom_1.24.0.0/13" "Unicom_1.56.0.0/13" "Unicom_1.188.0.0/14" "Unicom_27.8.0.0/13"
        set allow-routing enable
    next
end

config router static
    edit 0
        set gateway 192.168.1.254
        set device "port1"
        set dstaddr "Unicom_GRP"
    next
end
```

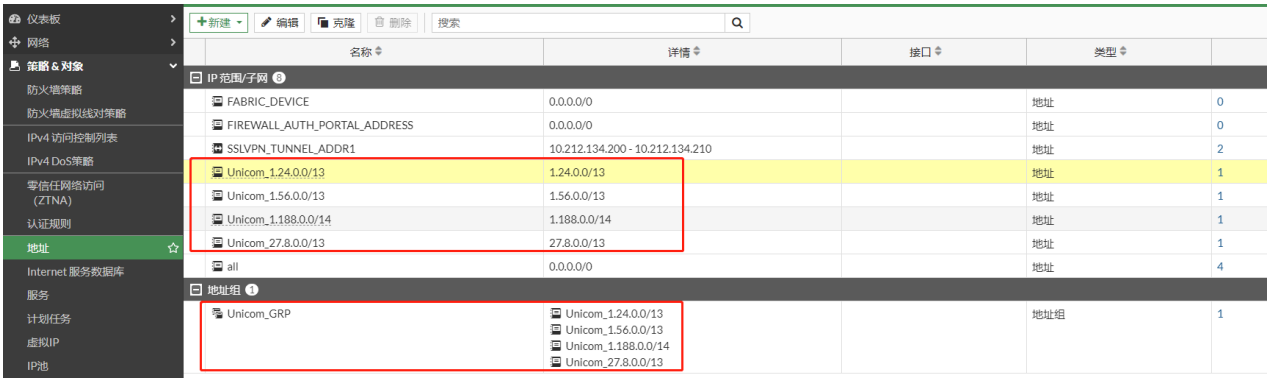
3. 点击FortiGate右上角账号旁边的下拉箭头，选择“配置”-->“脚本”，点击“运行脚本”



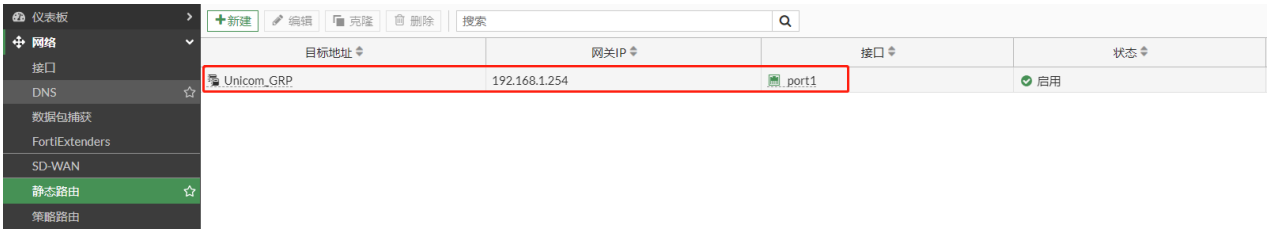
4. 脚本上传成功后会显示“成功”的字样



5. 在FortiGate地址对象界面查看刚刚上传的地址对象，地址对象组，路由



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

命令行脚本批量转换工具说明

说明

通常使用NimbleText工具生成相应的脚本，然后使用Notepad++保存脚本。

NimbleText：用于批量生成命令行脚本。官网链接：http://nimbletext.com/

Notepad++：文本编辑器，保存配置脚本，保存成.txt格式，编码为“UTF-8编码”。官网链接：https://notepad-plus-plus.org/

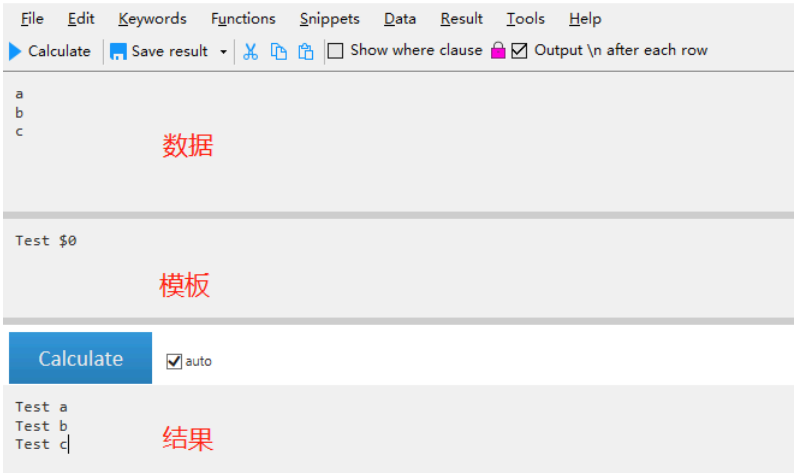
NimbleText的脚本编辑举例

NimbleText帮助文档：

https://nimbletext.com/Help/Keywords

https://nimbletext.com/help

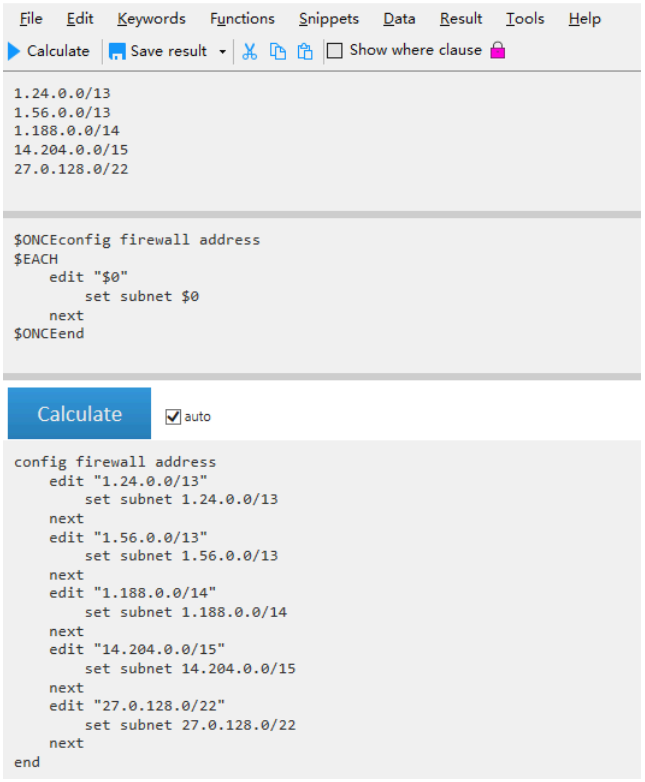
NimbleText的界面分成三个部分：数据，模板，结果，NimbleText就是将数据和模板结合生成对应的结果。



1. 批量生成地址对象

```
地址列表
1.24.0.0/13
1.56.0.0/13
1.188.0.0/14
14.204.0.0/15
27.0.128.0/22

FortiGate地址对象配置示例
config firewall address
    edit "1.1.1.0/24"
        set subnet 1.1.1.0/24
    next
end

根据地址对象命令分析，config firewall address和end不需要重复执行，对于edit和set subnet需要根据地址列表的变化而重复。
$ONCEconfig firewall address
$EACH
    edit "$0"
        set subnet $0
    next
$ONCEend

$ONCE，$EACH，$0都是NimbleText的关键字
$ONCE:任何在'$ONCE'关键字之后的文本将只输出一次，不管有多少行，到'$EACH'关键字或者到文件末尾为止。
$EACH:在'$EACH'关键字之后的任何文本将为每行输出一次（默认会换行），不管有多少行，到'$ONCE'关键字或者到文件末尾为止。
可以随意交错任意多的“$ONCE”和“$EACH”。
$0，$1:$0是第1列的数据，$1是第2列的数据，依次类推。
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

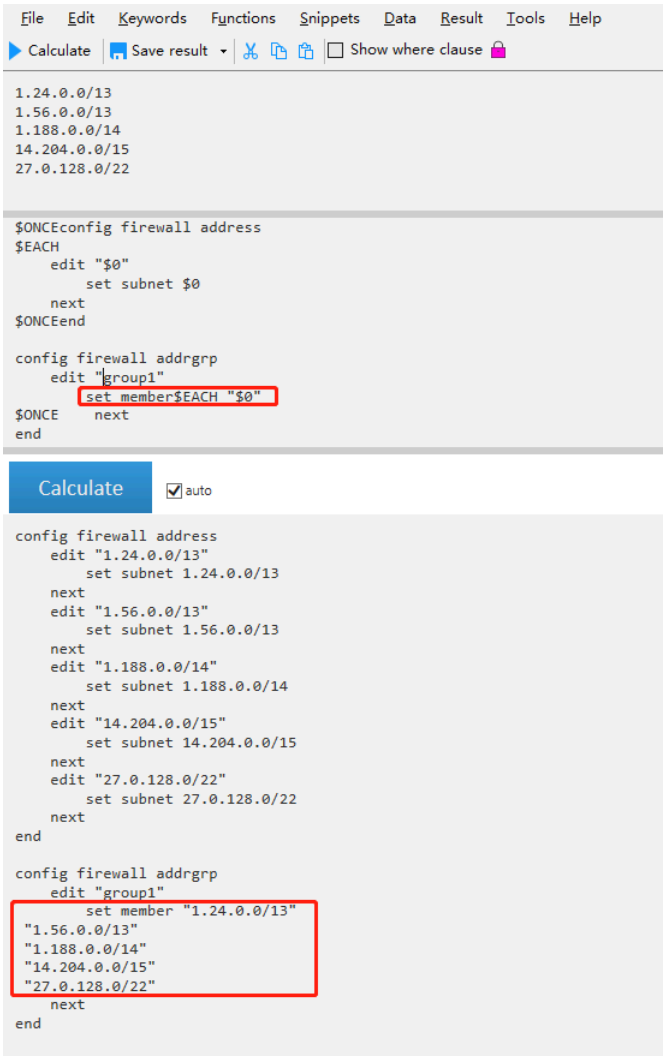


2.批量生成地址对象，并将其加入地址对象组

```
地址列表
1.24.0.0/13
1.56.0.0/13
1.188.0.0/14
14.204.0.0/15
27.0.128.0/22

FortiGate地址对象,地址对象组配置示例
config firewall address
    edit "1.1.1.0/24"
        set subnet 1.1.1.0/24
    next
    edit "1.1.2.0/24"
        set subnet 1.1.2.0/24
    next
end
config firewall addrgrp
    edit "group1"
        set member "1.1.1.0/24" "1.1.2.0/24"
    next
end
```

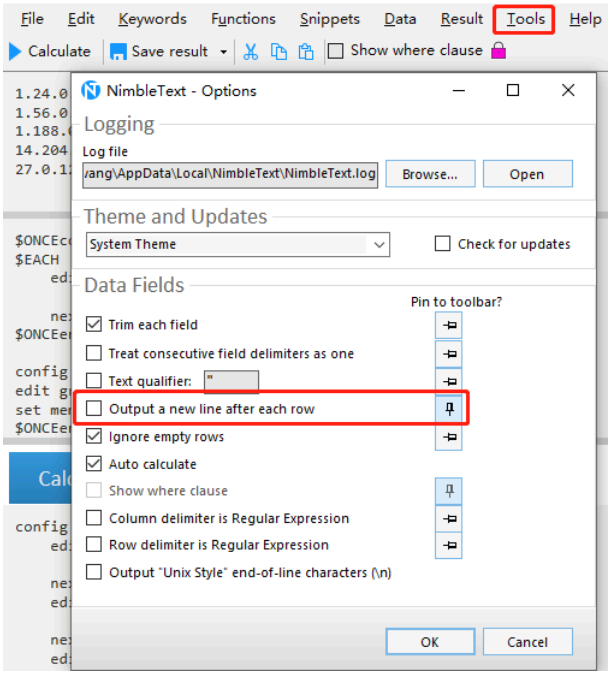
按照示例1的方式，NimbleText输出如下：

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



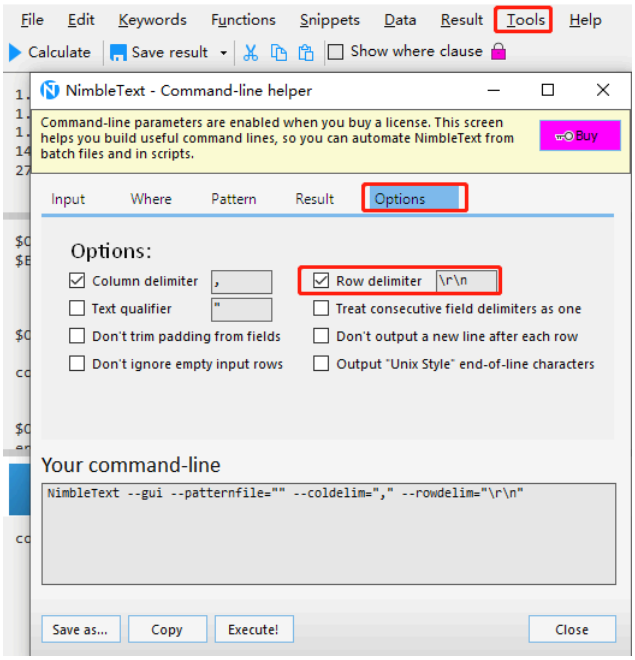
在地址对象配置中edit "$0"和set subnet $0循环第1列数据时，需要换行；在地址对象组set member$EACH $0 循环第1列的数据时，不需要换行。因此需要解决$EACH关键自动换行的问题。

修改$EACH关键字的输出不自动换行，选择”Tools“-->“Options...”，取消勾选“Output a new line after each row”



$rowDelim：行分隔符，这里利用这个关键字来换行。选择“Tools”-->“Command-line helper”，点击“Options”可以看出行分隔符是\r\n。

Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.



NimbleText修改后模板脚本如下：

```
$ONCEconfig firewall address
$EACH
    edit "$0"
        set subnet $0
    next$rowDelim
$ONCEend

config firewall addrgrp
    edit "group1"
        set member$EACH "$0"
$ONCE$rowDelim    next
end
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

File Edit Keywords Functions Snippets Data Result Tools Help

Calculate | Save result | Show where clause

```
1.24.0.0/13
1.56.0.0/13
1.188.0.0/14
14.204.0.0/15
27.0.128.0/22
```

```
$ONCEconfig firewall address
$EACH
    edit "$0"
        set subnet $0
    next$rowDelim
$ONCEend

config firewall addrgrp
    edit "group1"
        set member$EACH "$0"
$ONCE$rowDelim    next
end
```

Calculate auto

```
config firewall address
    edit "1.24.0.0/13"
        set subnet 1.24.0.0/13
    next
    edit "1.56.0.0/13"
        set subnet 1.56.0.0/13
    next
    edit "1.188.0.0/14"
        set subnet 1.188.0.0/14
    next
    edit "14.204.0.0/15"
        set subnet 14.204.0.0/15
    next
    edit "27.0.128.0/22"
        set subnet 27.0.128.0/22
    next
end

config firewall addrgrp
    edit "group1"
        set member "1.24.0.0/13" "1.56.0.0/13" "1.188.0.0/14" "14.204.0.0/15" "27.0.128.0/22"
    next
end
```

Notepad++保存脚本并导入

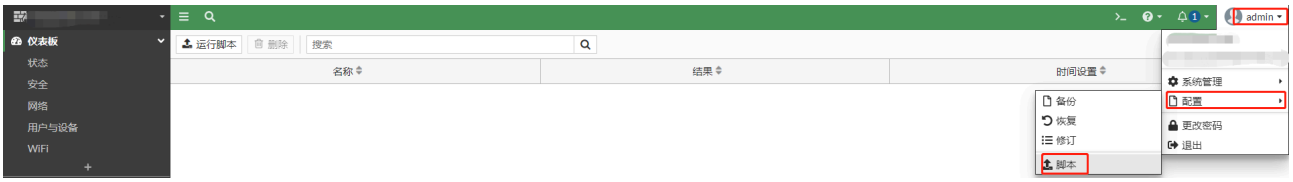
将NimbleText的输出保存在notepadd++中，选择“编码”-->“使用UTF-8编码”，并保存。

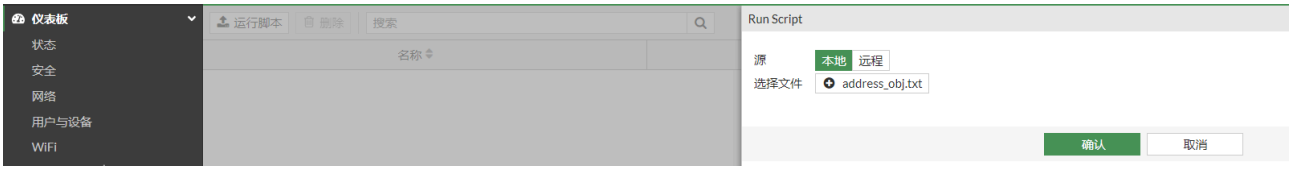


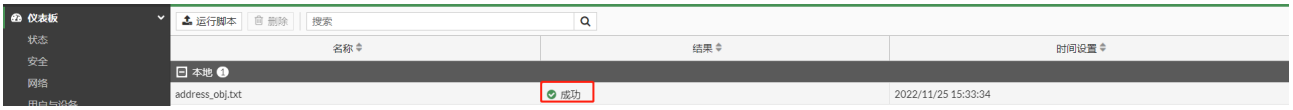
Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
config firewall address
    edit "1.24.0.0/13"
        set subnet 1.24.0.0/13
    next
    edit "1.56.0.0/13"
        set subnet 1.56.0.0/13
    next
    edit "1.188.0.0/14"
        set subnet 1.188.0.0/14
    next
    edit "14.204.0.0/15"
        set subnet 14.204.0.0/15
    next
    edit "27.0.128.0/22"
        set subnet 27.0.128.0/22
    next
end

config firewall addrgrp
    edit "group1"
        set member "1.24.0.0/13" "1.56.0.0/13" "1.188.0.0/14" "14.204.0.0/15" "27.0.128.0/22"
    next
end
```

点击右上角下拉箭头，选择”配置“-->”脚本“，点击”运行脚本“，上传address_obj.txt，脚本上传成功后会显示“成功”的字样。

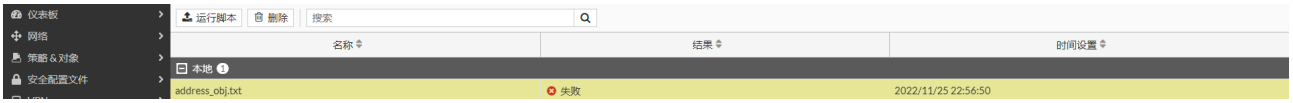






上传脚本失败排查

脚本上传显示“失败”的字样，即该脚本有问题。



在上传时，通过ssh或者web console登录FortiGate命令行，可以通过debug命令查看具体是哪一行有问题。

```
# diagnose debug  cli 8
# diagnose debug  enable
在diagnose debug cli 8的输出中，只有值为0才是成功的。

cmd=/tmp/monitor_upload_nRf481
0: config firewall address
0:     edit "1.24.0.0/13"
0:         set subnet 1.24.0.0/13
0:     next
0:     edit "1.56.0.0/13"
0:         set subnet 1.56.0.0/13
0:     next
0:     edit "1.188.0.0/14"
0:         set subnet 1.188.0.0/14
0:     next
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.

```
0:     edit "14.204.0.0/15"
0:         set subnet 14.204.0.0/15
0:     next
0:     edit "27.0.128.0/22"
-160:         set subnet 27.0.128.0     #从这里可以看出这个地址没有掩码，修改后就能够正常上传了
1:     next
0: end
0:
0: config firewall addrgrp
0:     edit "group1"
-3:         set member "1.24.0.0/13" "1.56.0.0/13" "1.188.0.0/14" "14.204.0.0/15" "27.0.128.0/22"
1:     next
0: end
0:
```


Copyright © 2025 Fortinet Inc. All rights reserved. Powered by Fortinet TAC Team.