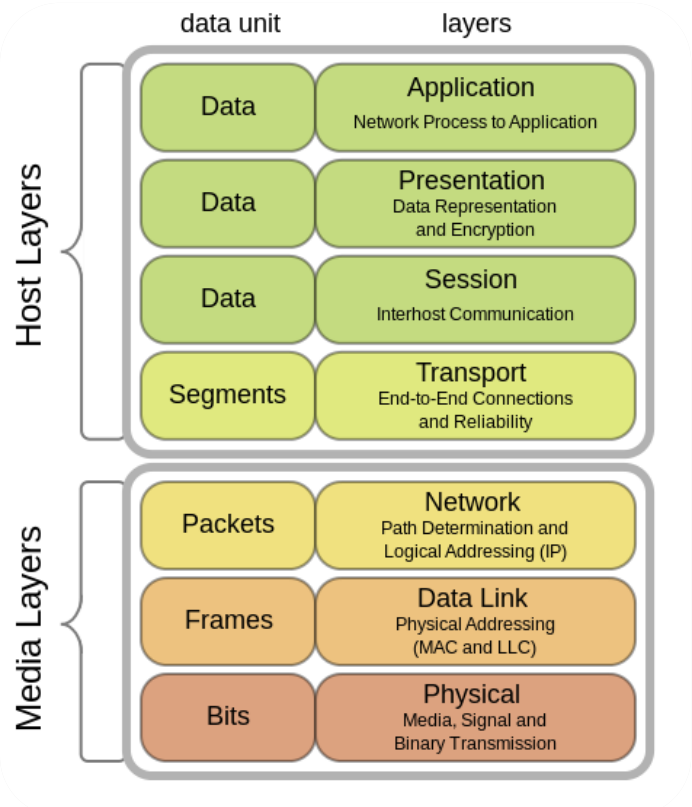
游戏行业DDOS在AWS的解决方案

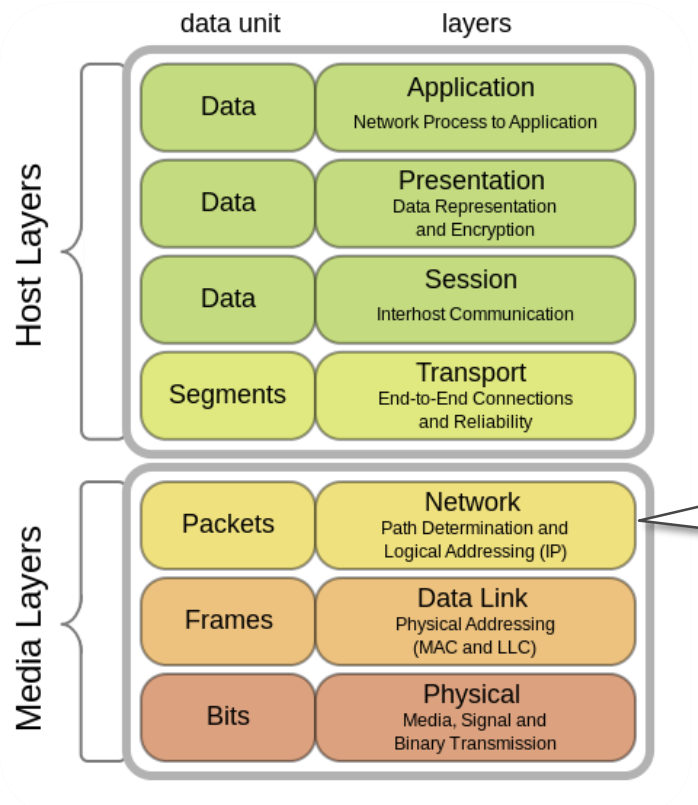
狄颖伟，AWS解决方案架构师
Yingwei Di, Solution Architect, Amazon Web Services

2017年7月18日
18th July , 2017

DDoS 攻击类型


data unit
layers
Host Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Media Layers
Packets
Network
Path Determination and Logical Addressing (IP)
Frames
Data Link
Physical Addressing (MAC and LLC)
Bits
Physical
Media, Signal and Binary Transmission

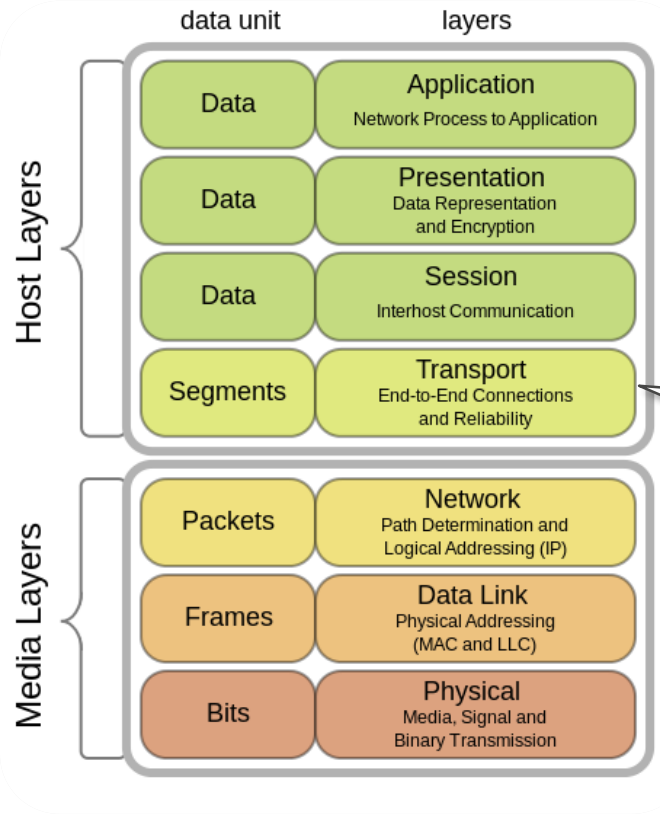
DDoS攻击类型



流量 DDoS 攻击

通过大流量造成网络拥塞 (e.g., UDP reflection attacks)

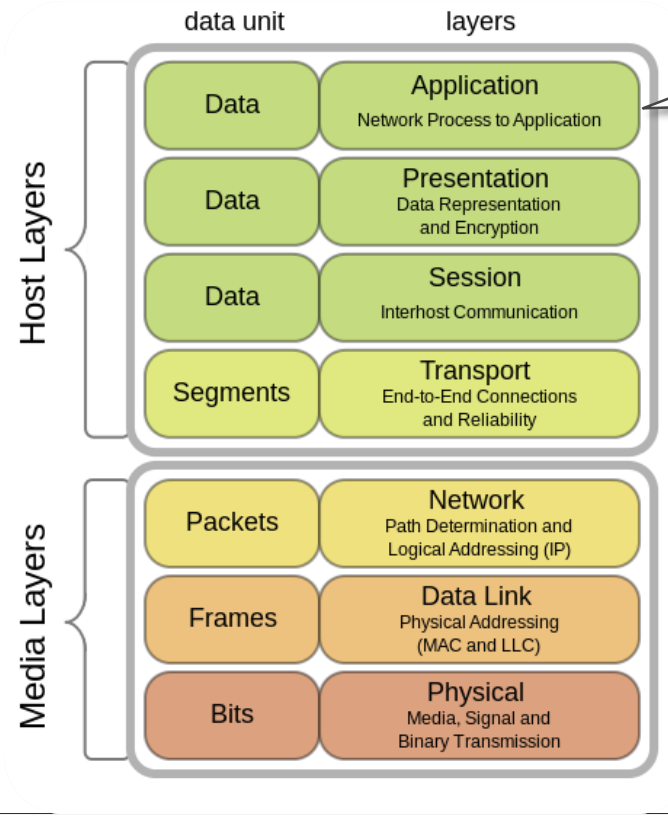
DDoS 攻击类型



资源耗尽 DDoS 攻击

通过网络协议使得诸如防火墙，负载均衡等设备资源耗尽 (e.g., TCP SYN flood)

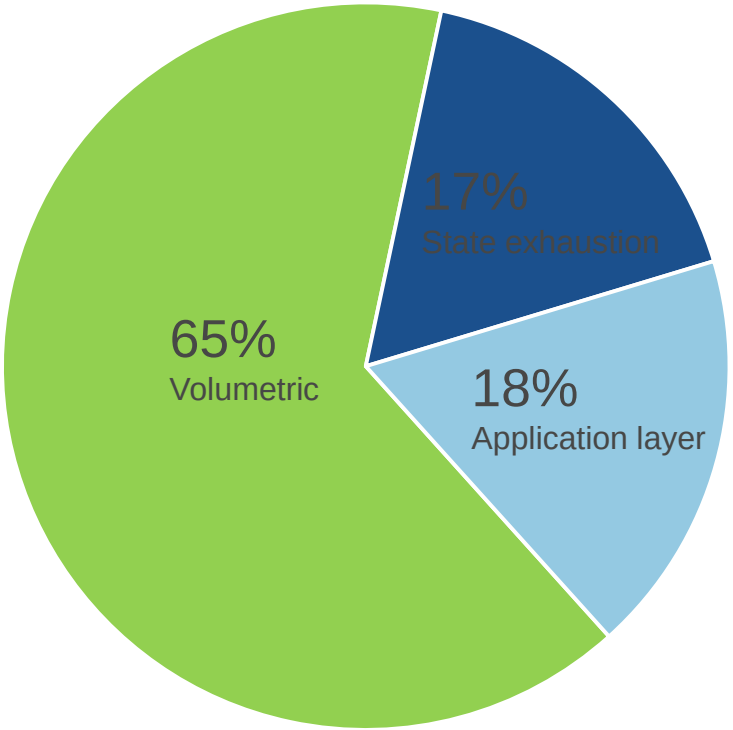
DDoS攻击类型



应用层 DDoS 攻击

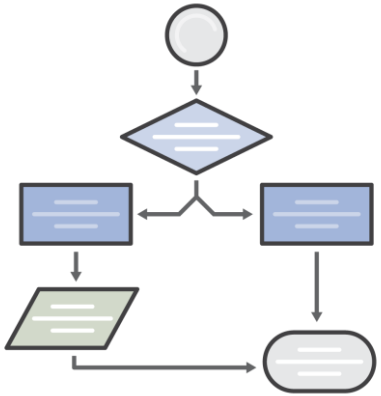
用大量的真实请求消耗应用资源 (e.g., HTTP GET)

DDoS攻击趋势


17%
State exhaustion
65%
Volumetric
18%
Application layer
Volumetric
State exhaustion
Application layer

应对DDoS攻击的挑战

- 难以处理



Complex set-up

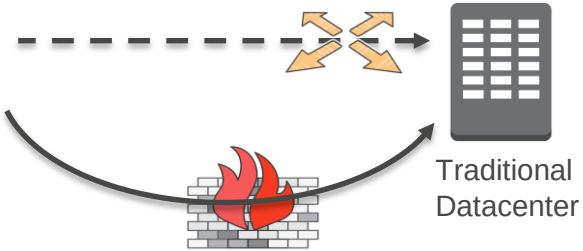
Provision bandwidth capacity

Application re-architecture

应对DDoS攻击的挑战

- 人工介入

Operator involvement to initiate mitigation



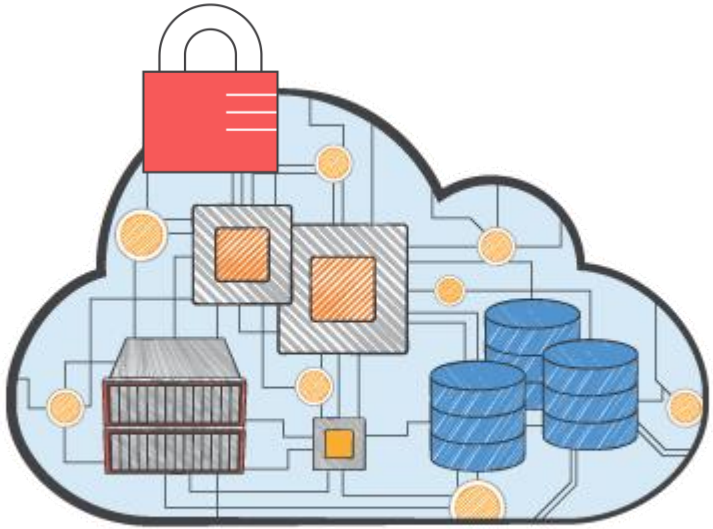
Re-route traffic via distant scrubbing location

Increased time to mitigate

应对DDoS攻击的挑战

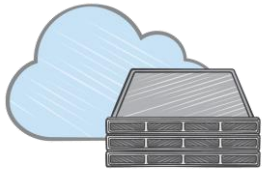
- 成本

AWS 应对方法

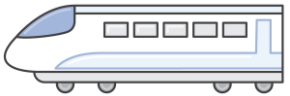


AWS DDoS防护

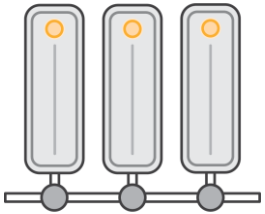
- 与全球基础资源集成



- 快速响应

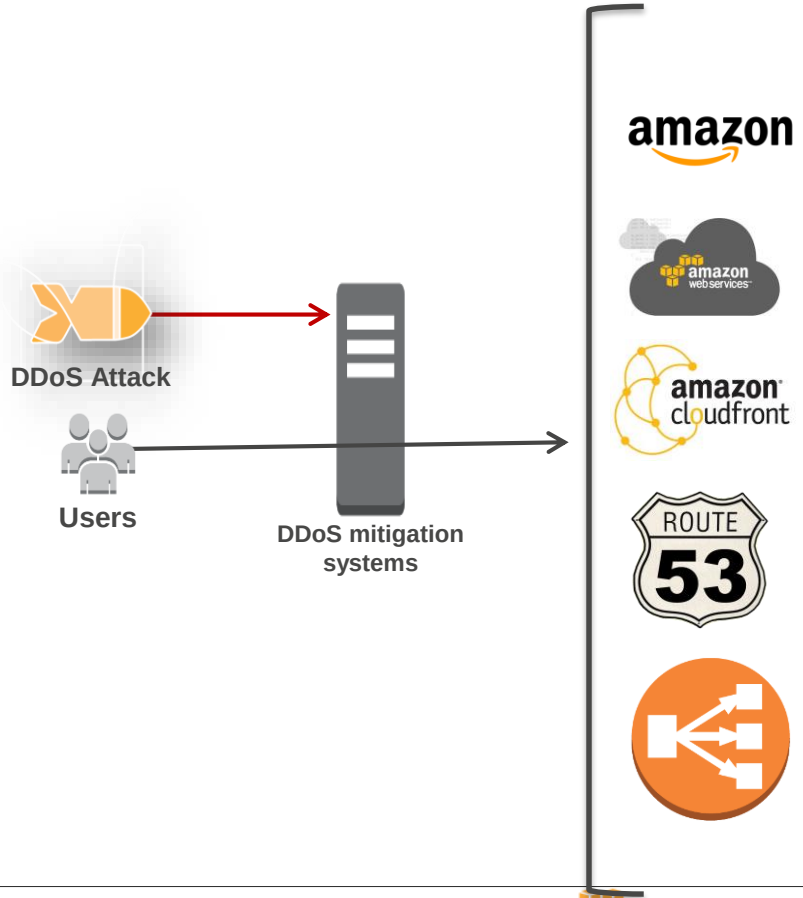


- 链路冗余



AWS内置DDoS防护

- ✓ 防护对基础设施的攻击
- ✓ 应对SYN/ACK Floods, UDP Floods, 等攻击
- ✓ 无额外费用

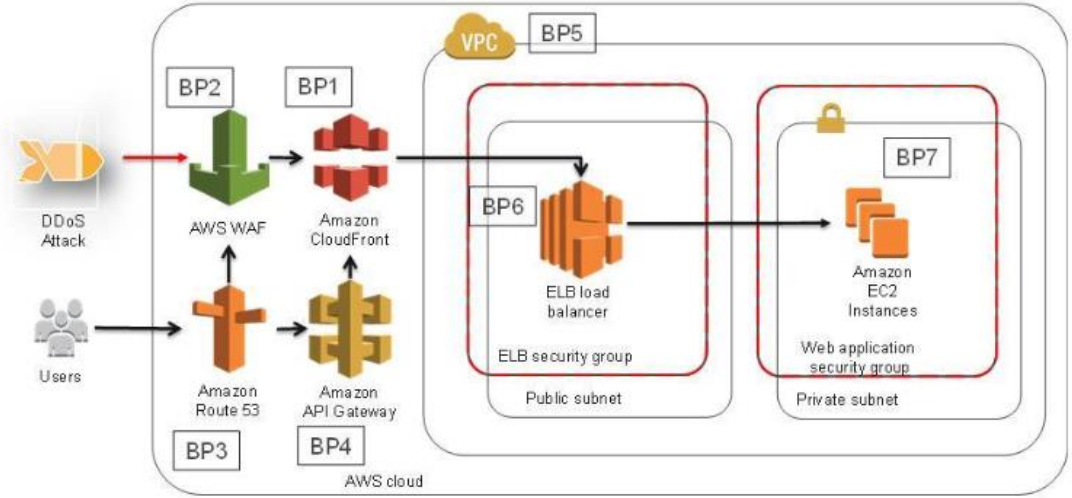


AWS WAF

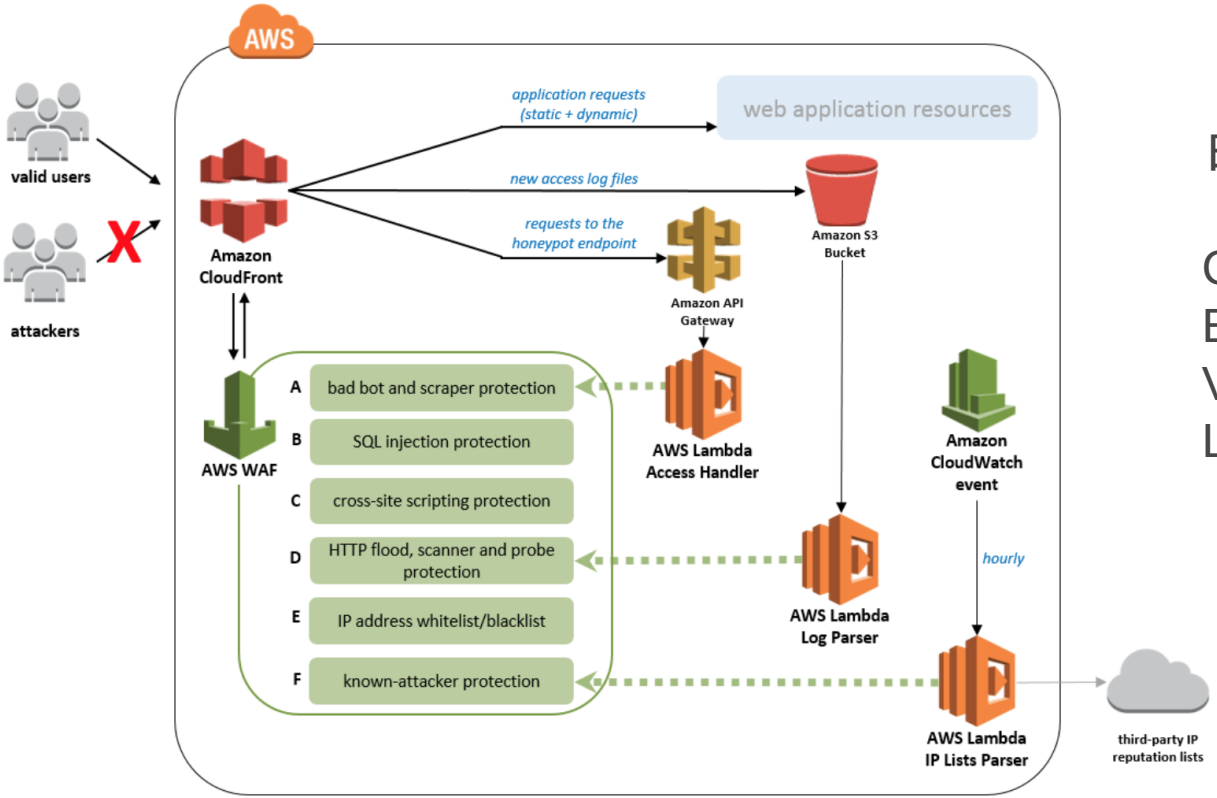
- 与CloudFront，ALB集成
- 支持API
- 策略
  - SQL注入
  - CSRF
  - IP地址
  - 数据包特性

AWS最佳实践

- 最小化受攻击面
- 吸收
- 重点保护暴露的资源
- 熟悉正常网络情况
- 应对计划



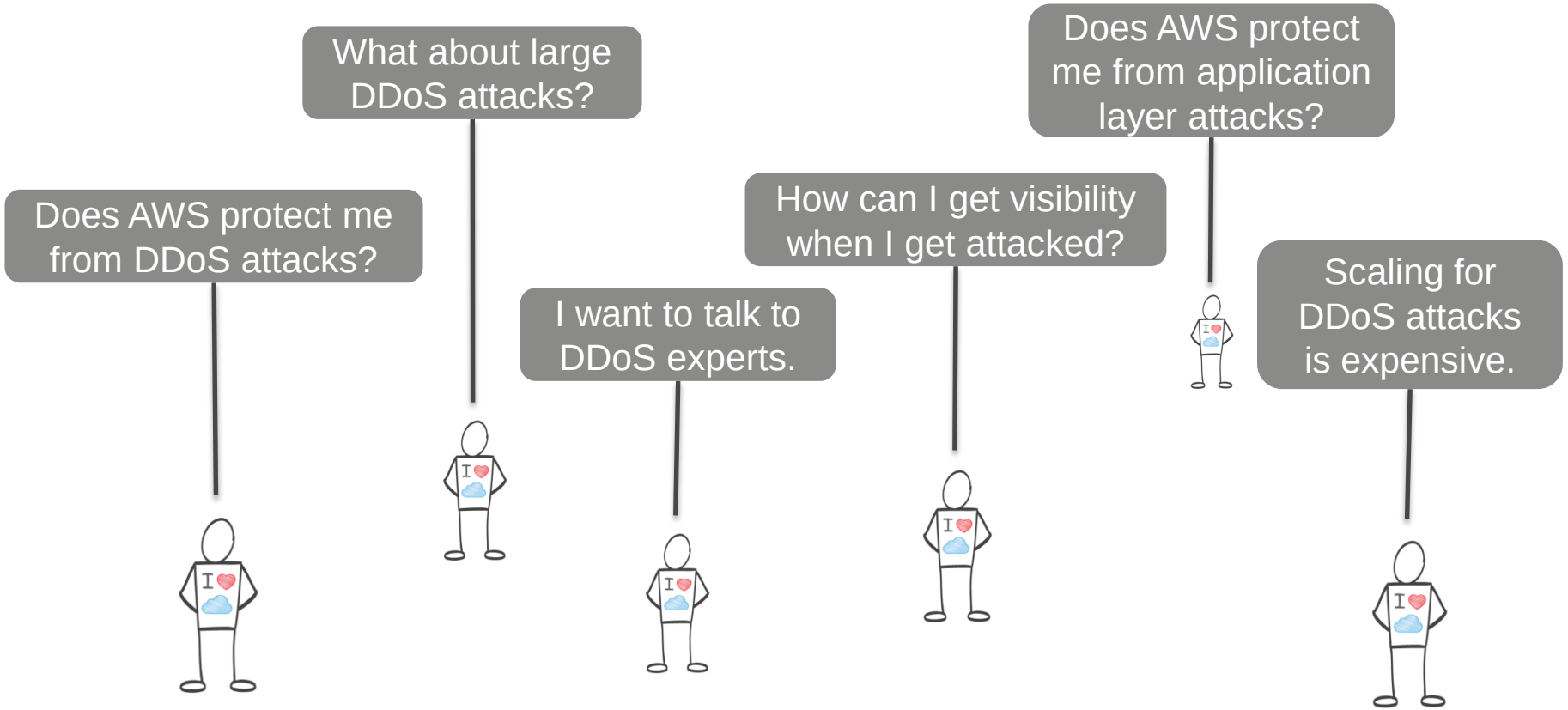
自动化防御



日志分析

CF log - S3 - Lambda
ELB log - S3 - Lambda
VPC flow log – CloudWatch Log - Lambda

客户还关心…


Does AWS protect me from DDoS attacks?
What about large DDoS attacks?
I want to talk to DDoS experts.
How can I get visibility when I get attacked?
Does AWS protect me from application layer attacks?
Scaling for DDoS attacks is expensive.

- **AWS Shield**
- ***A Managed DDoS Protection Service***

AWS Shield

标准保护

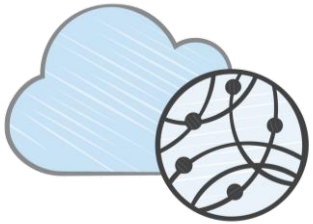
- *提供给所有客户，无额外费用*

高级保护

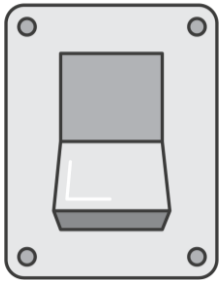
付费服务，提供额外的服务和功能

AWS Shield

特点…



与AWS服务集成
Integration
DDoS protection without infrastructure changes



持续侦测和压制
Minimize impact on application latency

经济
Don't force unnecessary trade-offs between cost and availability

灵活
Customize protections for your applications

- **AWS Shield 标准版**

AWS Shield 标准版

3/4层保护

- ✓ Automatic detection & mitigation
- ✓ Protection from most common attacks (SYN/UDP Floods, Reflection Attacks, etc.)
- ✓ Built into AWS services

7层保护

- ✓ AWS WAF for Layer 7 DDoS attack mitigation
- ✓ Self-service & pay-as-you-go

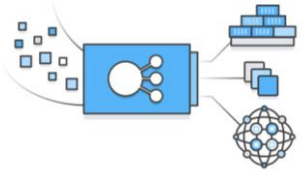
AWS Shield 标准版

- 更好的保护您运行在AWS上的资源
- 通过BlackWatch systems提升效果
- 持续监控和压制
- 无额外费用

- **AWS Shield Advanced**
- ***Managed DDoS Protection***

AWS Shield 高级版

- 与AWS服务结合，需要business support



Application Load Balancer

Classic Load Balancer

Amazon CloudFront

Amazon Route 53

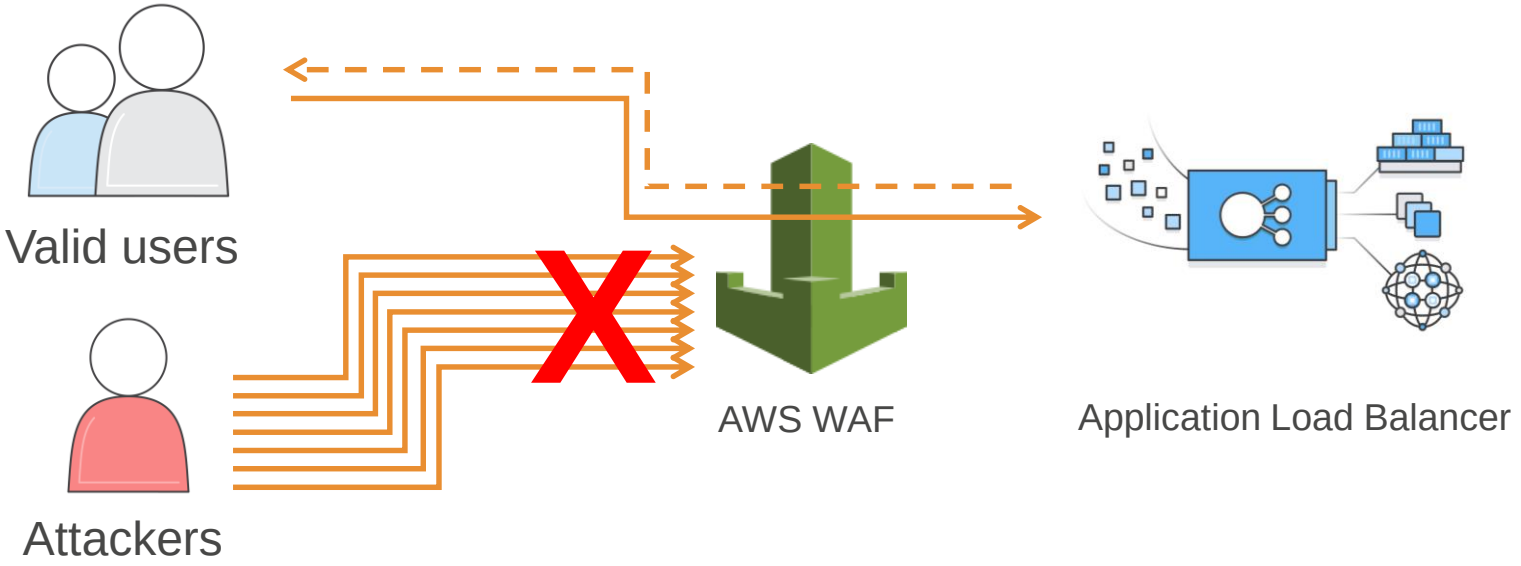
AWS Shield 高级版

- 支持的区域

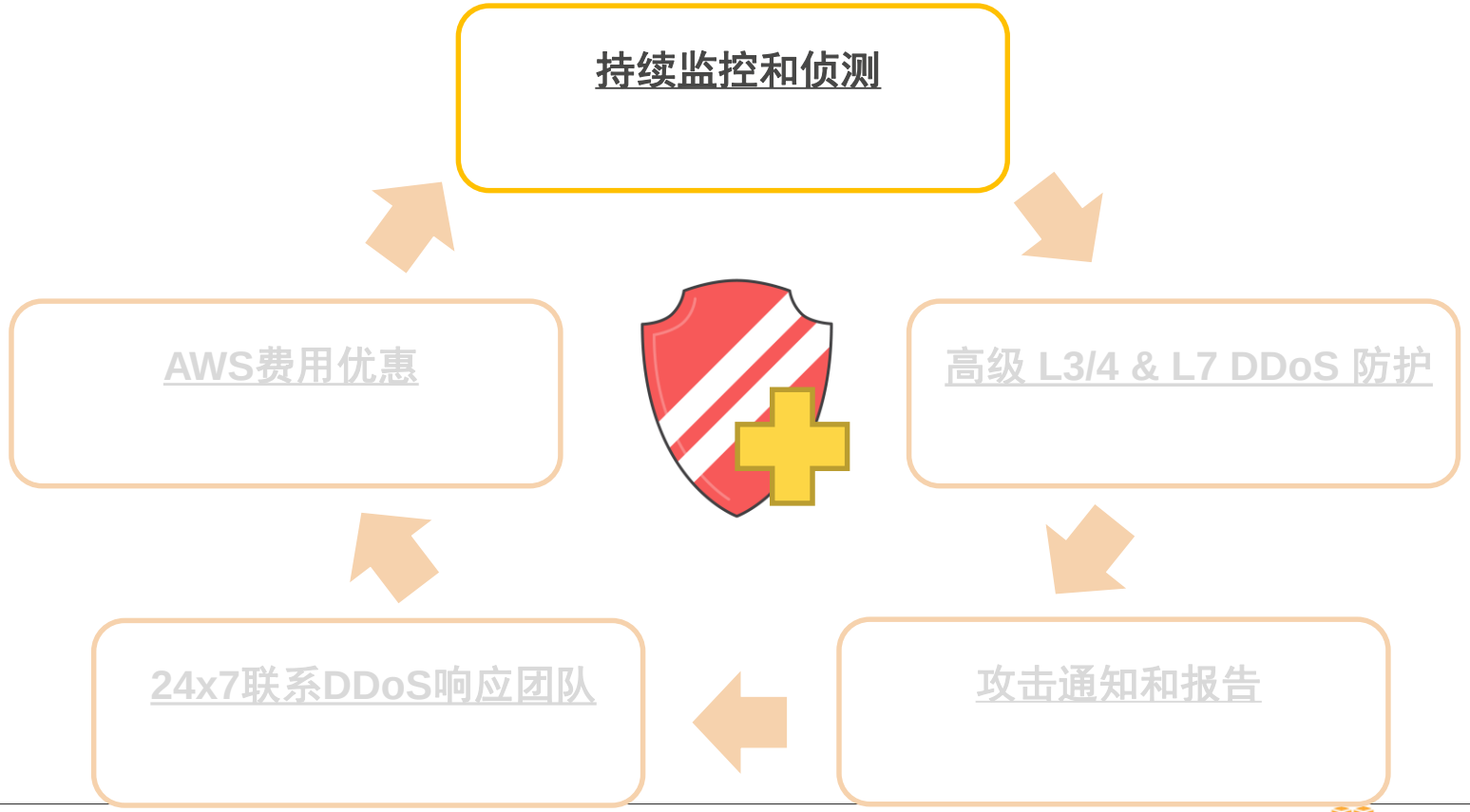
US East (N. Virginia)	us-east-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Tokyo)	ap-northeast-1

AWS Shield 高级版

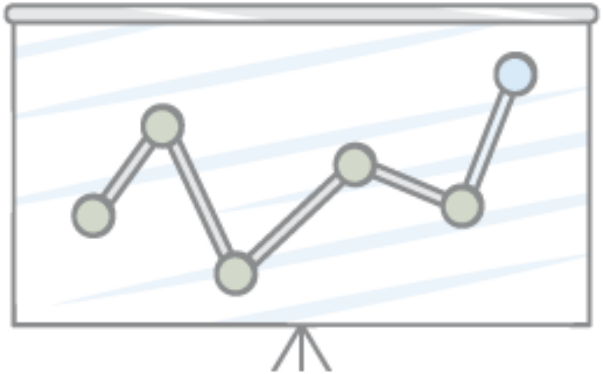
- **AWS WAF与Application Load Balancer集成**



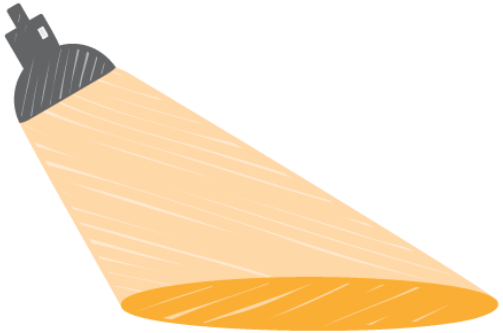
AWS Shield 高级版



持续监控和侦测



Network flow monitoring



Application traffic monitoring

持续监控和侦测

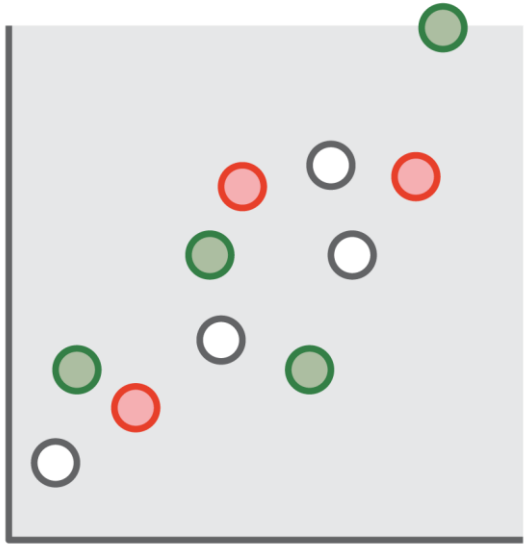
异常检测

- Detects anomalies based on attributes such as:
- Source IP
- Source ASN
- Traffic levels
- Validated sources

持续监控和侦测

基线

- Continuously baselining normal traffic patterns
- HTTP Requests per second
- Source IP Address
- URLs
- User-Agents



AWS WAF支持基于rate的过滤

AWS Shield 高级版

增强DDoS防护

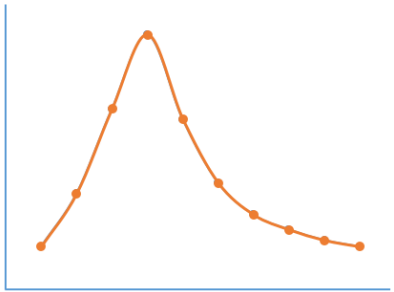
Layer 3/4 infrastructure protection

Layer 7 application protection

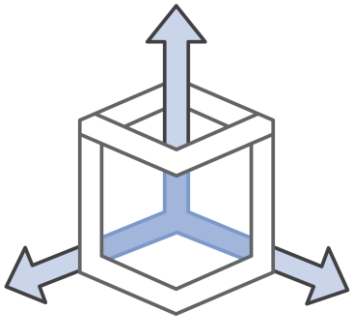
3/4层基础设施防护

高级防护技术技术

Deterministic filtering



Traffic prioritization based on scoring



Advanced routing policies

3/4层基础设施防护

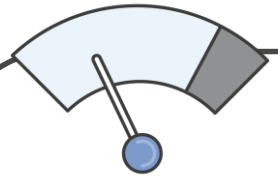
过滤技术

- Automatically filters malformed TCP packets

- IP checksum
- TCP valid flags
- UDP payload length
- DNS request validation

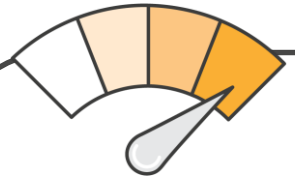
3/4层基础设施防护

流量优先级



Low suspicion attributes

- Normal packet or request header
- Traffic composition and volume is typical given its source
- Traffic valid for its destination



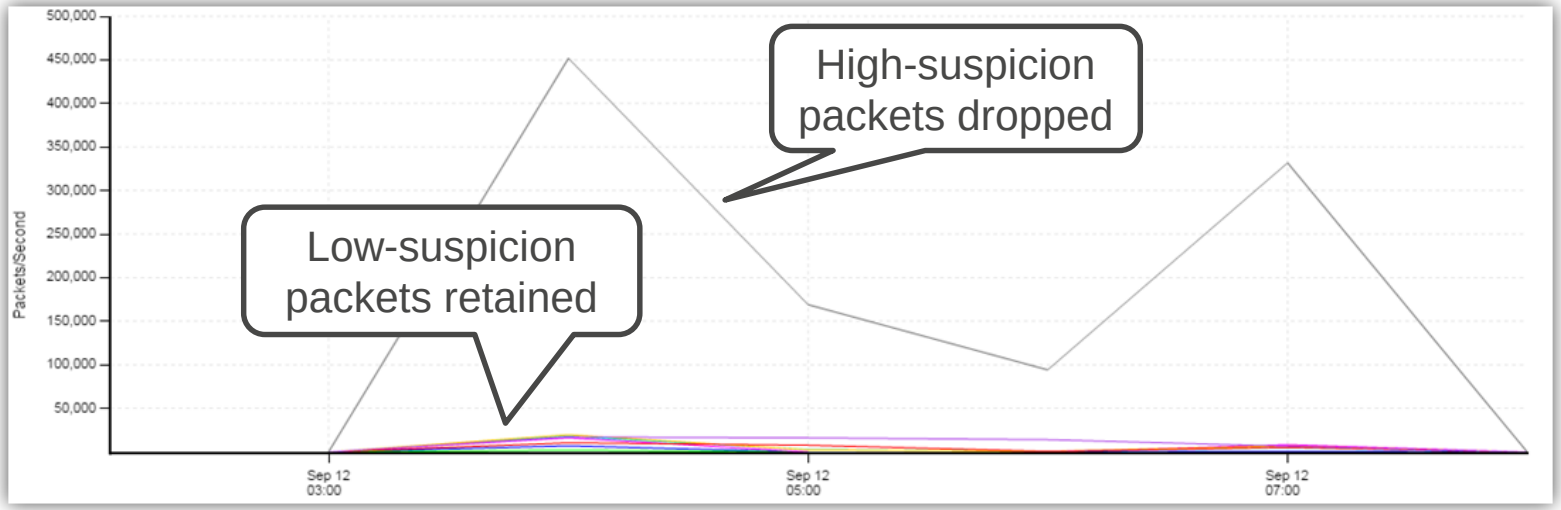
High suspicion attributes

- Suspicious packet or request headers
- Entropy in traffic by header attribute
- Entropy in traffic source and volume
- Traffic source has a poor reputation
- Traffic invalid for its destination
- Request with cache-busting

3/4层基础设施防护

流量优先级

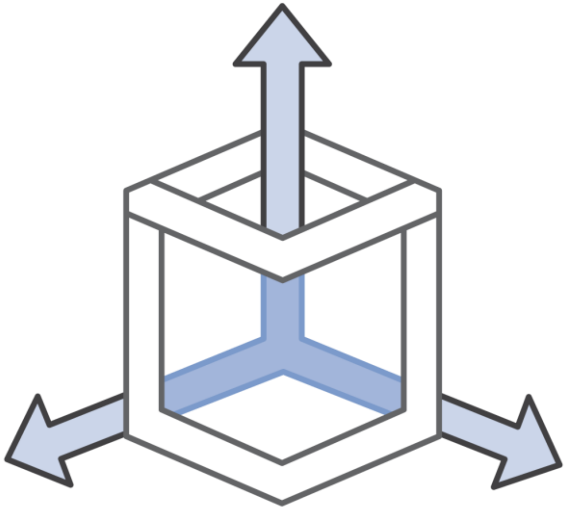
- Inline inspection and scoring
- Preferentially discard lower priority (attack) traffic



3/4层基础设施防护

高级路由策略

- Distributed scrubbing and bandwidth capacity
- Automated routing policies to absorb large attacks
- Manual traffic engineering



增强DDoS防护

Layer 3/4 infrastructure protection

Layer 7 application protection

AWS WAF – 7层应用防护

Web traffic filtering with custom rules

Malicious request blocking

Active monitoring and tuning

AWS WAF – 7层应用防护

- **三种操作模式**

Self-service

Engage DDoS experts

Proactive DRT engagement

AWS WAF – 7层应用防护

自服务

- AWS WAF included at no additional cost

AWS WAF – 7层应用防护

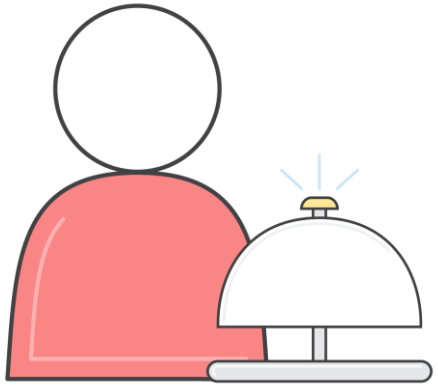
引入DDoS专家

1. You engage the AWS DDoS Response Team (DRT)
2. DRT triages attack
3. DRT assists you with creating AWS WAF rules

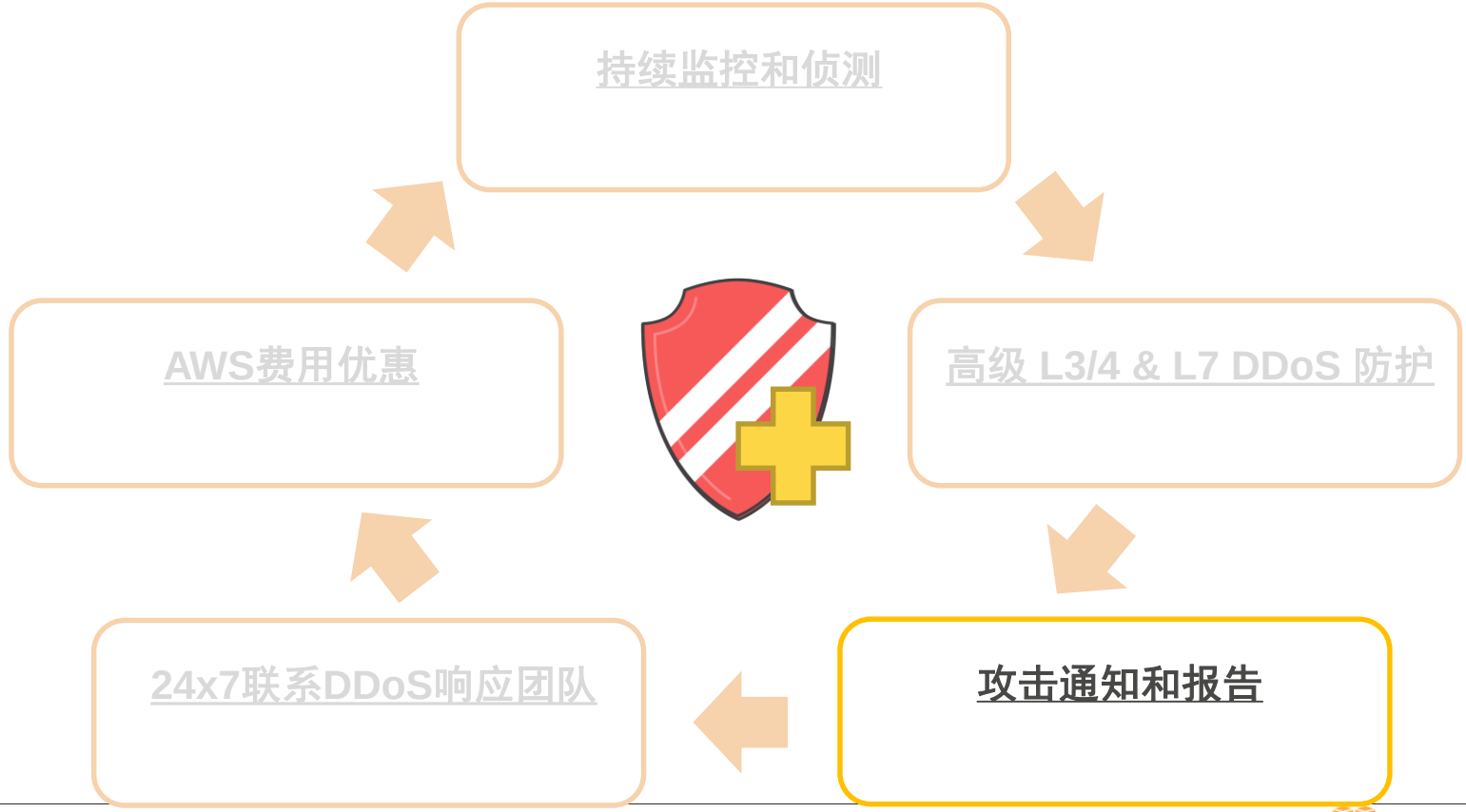
AWS WAF – 7层应用防护

预先引入DRT

1. Always-on monitoring engages the AWS DDoS Response Team (DRT)
2. DRT proactively triages DDoS attack
3. DRT creates AWS WAF rules (prior authorization required)



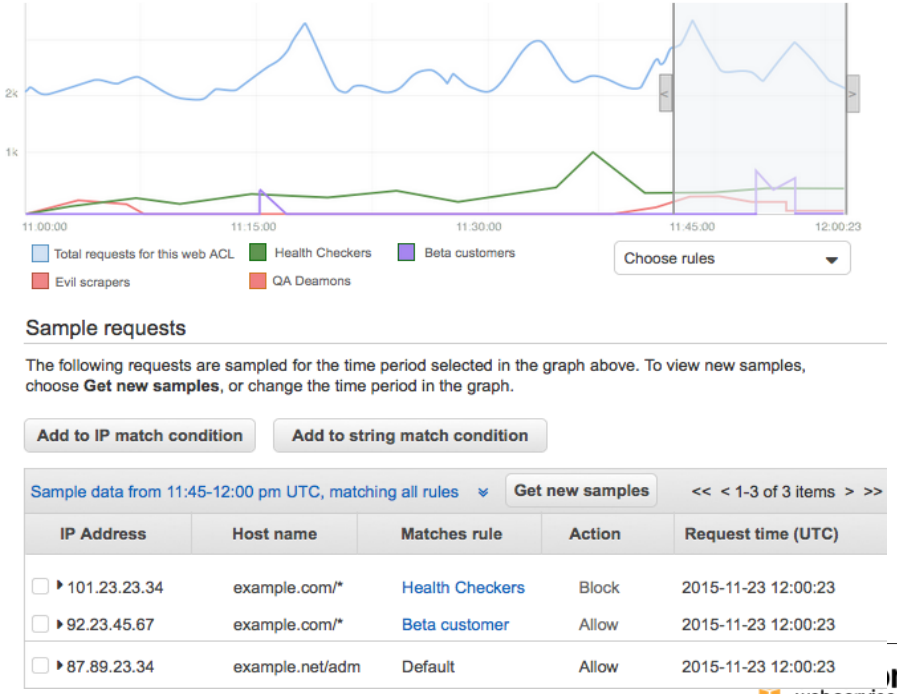
AWS Shield 高级版



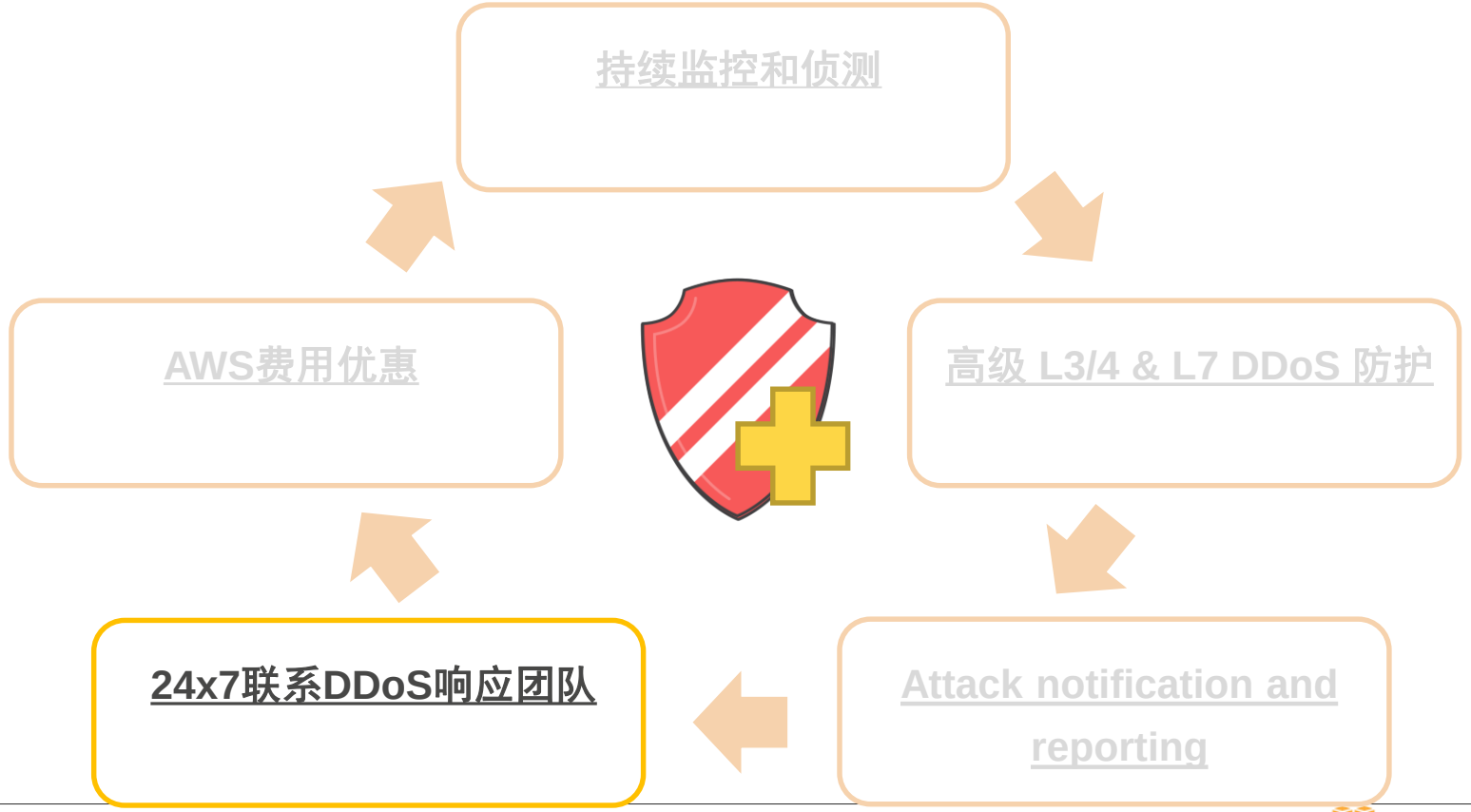
攻击通知和报告

- Real-time notification of attacks via Amazon CloudWatch
- Near real-time metrics and packet captures for attack forensics
- Historical attack reports

Attack monitoring and detection



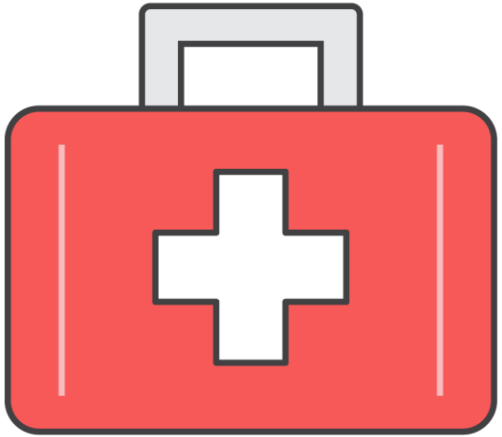
AWS Shield 高级版



24x7 联系DDoS 响应团队

- 关键、紧急事件迅速响应，直接与DRT专家沟通

- 复杂可由DTR 专家处理，DRT专家在保护AWS和amazon.com具有丰富的实践经验



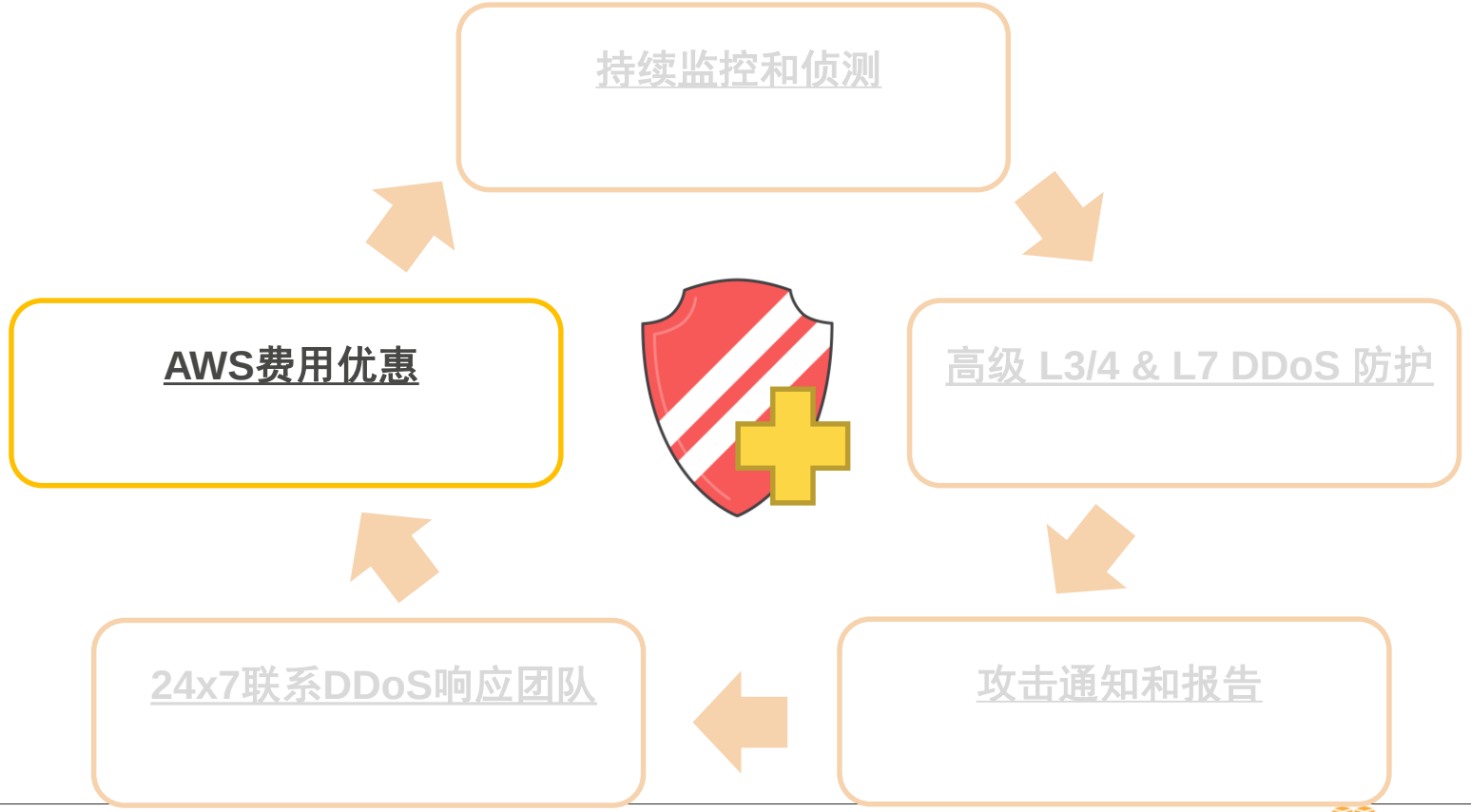
24x7 联系DDoS 响应团队

事前
Proactive consultation and best practice guidance

事中
Attack mitigation

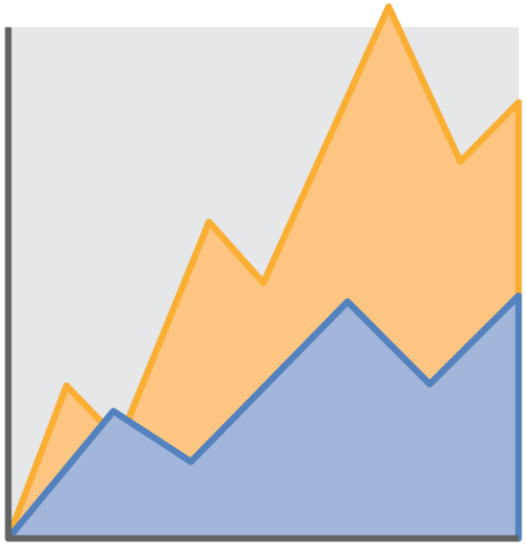
事后
Post-mortem analysis

AWS Shield 高级版



AWS 费用减免

- 减免因DDoS攻击造成的扩展费用
  - Amazon CloudFront
  - Elastic Load Balancer
  - Application Load Balancer
  - Amazon Route 53

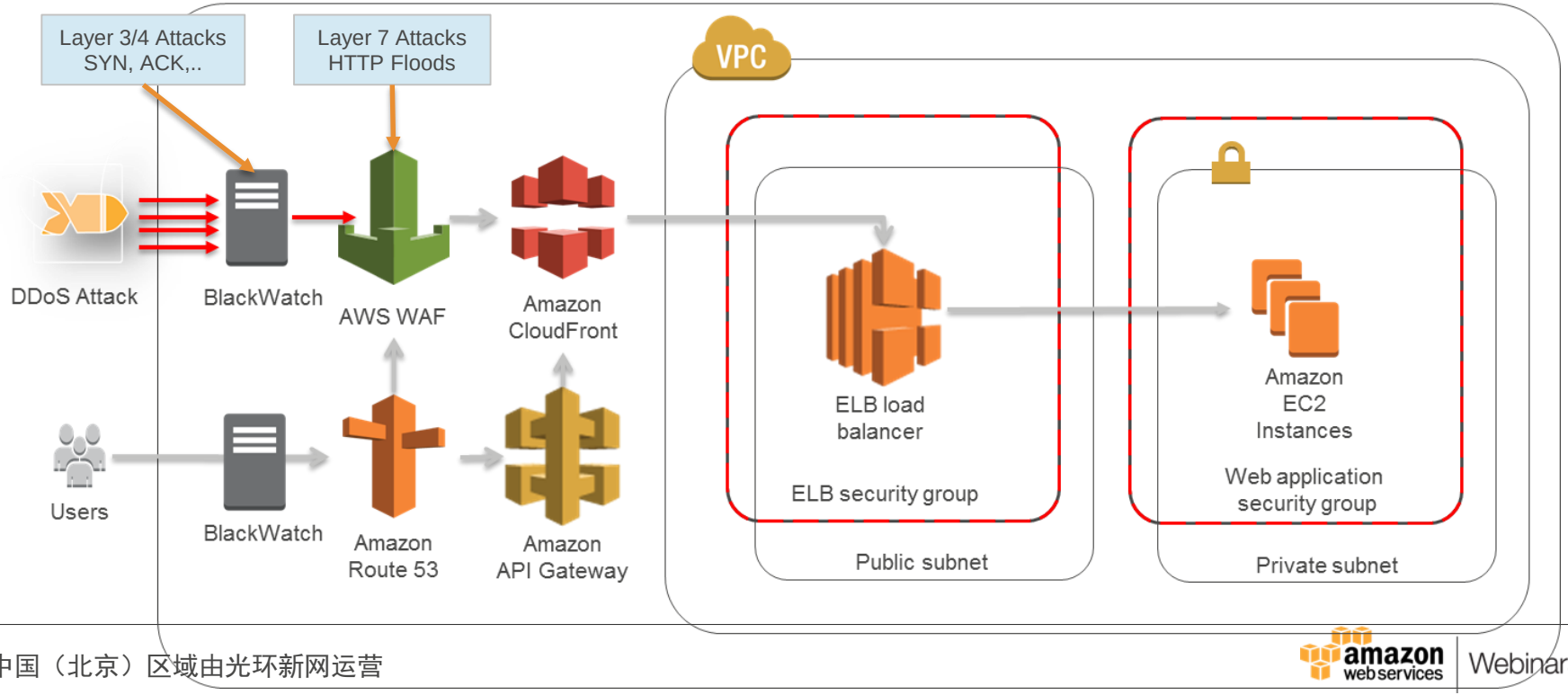


游戏DDoS防护

- **游戏应用组成**
- Web Portal – HTTP(S)
- Backend services, like Matchmaking – HTTP(S) / TCP
- Dedicated Game Servers - UDP
- Multiplayer Relay Servers - UDP

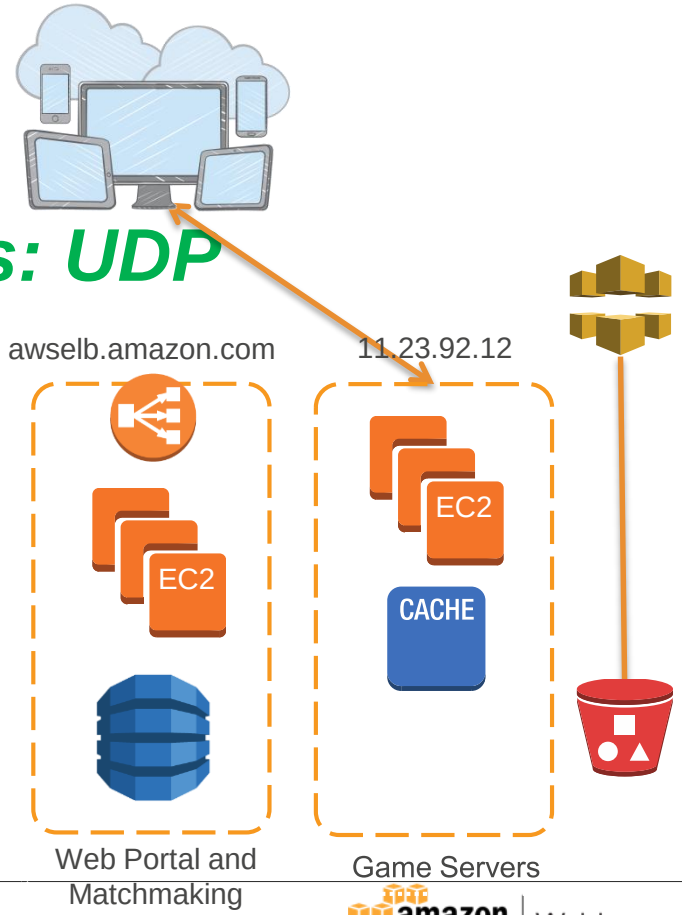
游戏DDoS防护

- ***Web Portal and Match-Making***

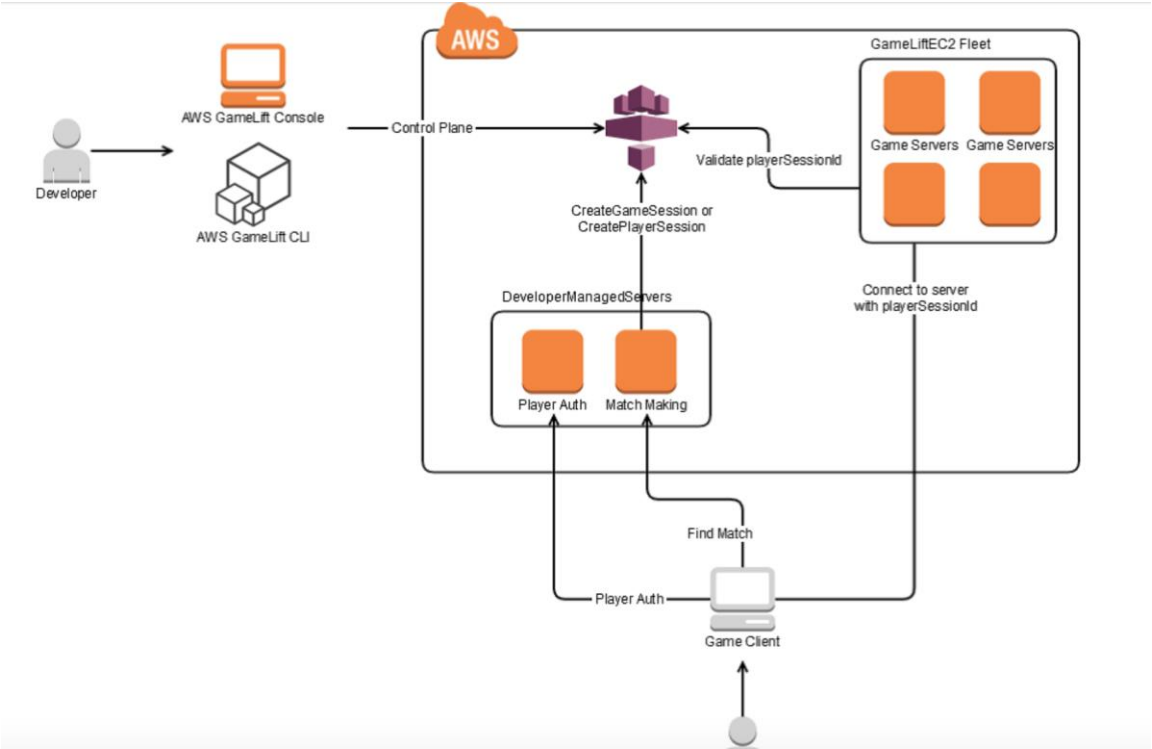


游戏DDoS防护

- ***Game Servers & Relay Servers: UDP***
- EC2 Traffic Shaping
- Auto-Mitigation



游戏DDoS防护—GameLift



Thank You!