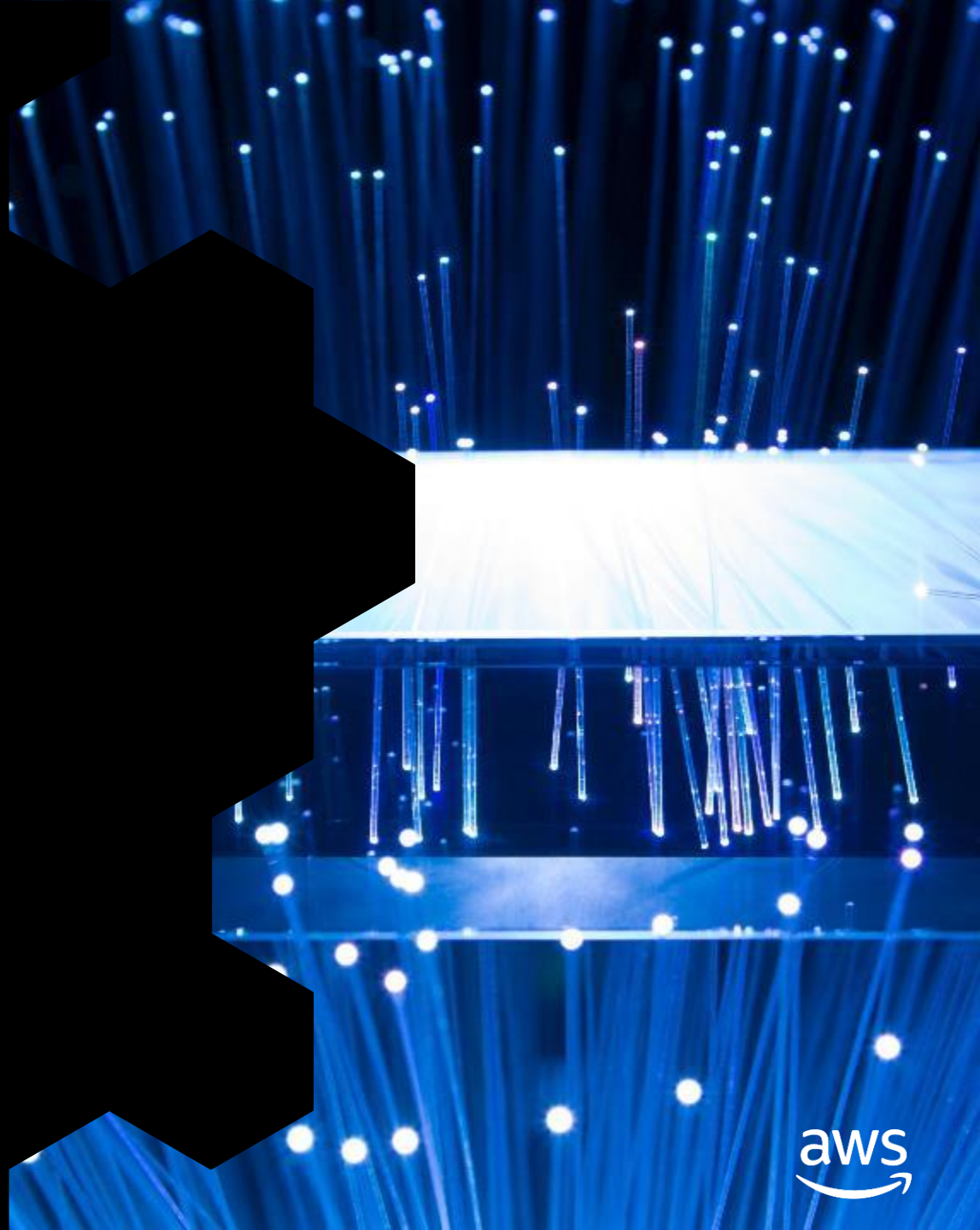
如何在全球范围内抵御 DDoS 攻击

童轶 AWS 解决方案架构师

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

日程

- DDoS 常见的攻击类型
- AWS DDoS 攻击最佳实践
- 云原生的游戏安全防御解决方案

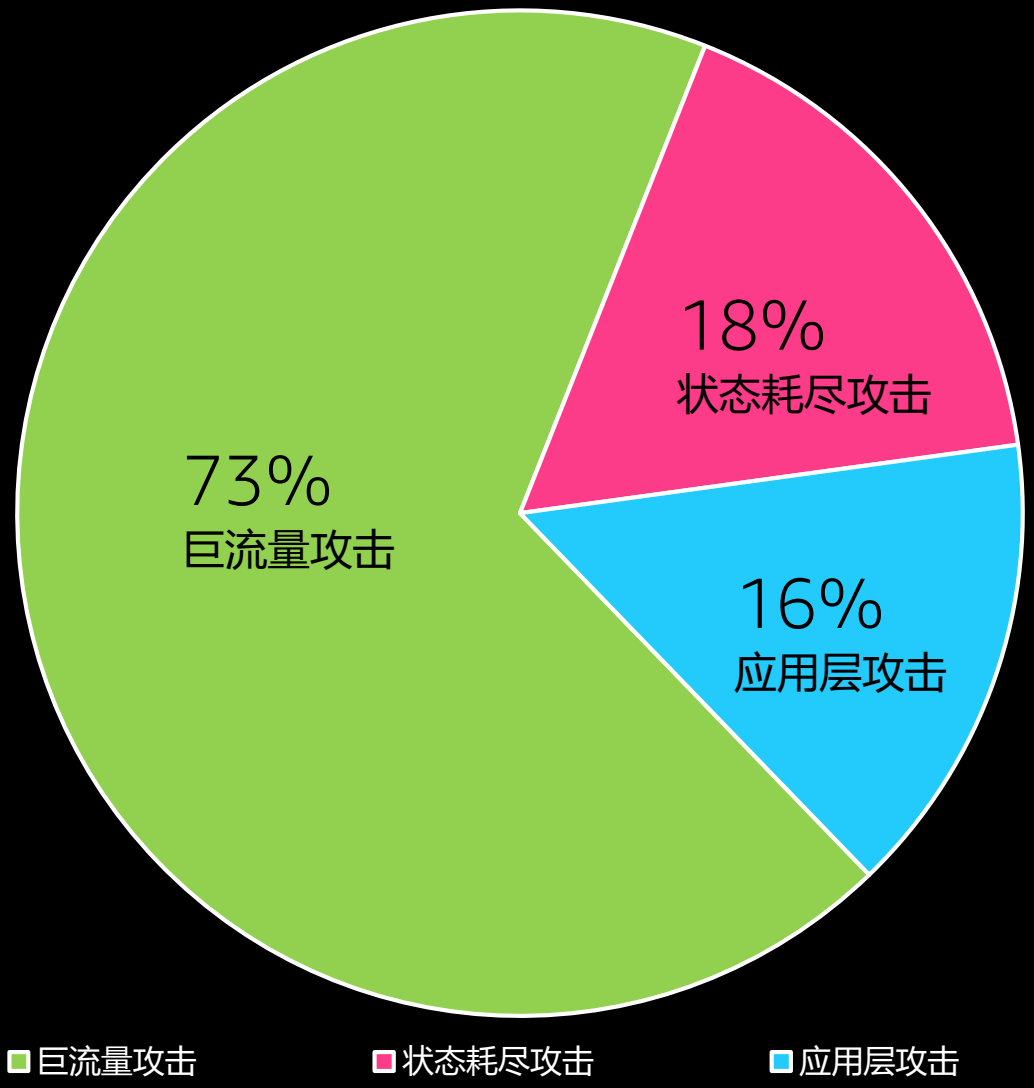


- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 常见的攻击类型

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS攻击趋势



- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 攻击的类型 1 — 网络层攻击

巨流量 DDoS 攻击：带宽消耗

通过超过你的处理能力的流量

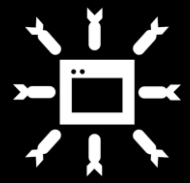
来撑爆你的网络

例如，UDP反射攻击

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 网络层攻击方法——UDP 反射攻击

攻击者不直接把攻击包发给受害者，而是冒充受害者给反射器发包，然后再反射给受害者。



攻击者
192.0.2.1

受害者
198.51.100.4

源 = 198.51.100.4
目的 = 203.0.113.32

反射器 (NTP servers)
203.0.113.32

NTP
DNS
SNMP
SSDP
Memcached

带宽放大因子
(BAF, Bandwidth Amplification Factor)

协议	理论 BAF
NTP	556
DNS	28.7 ~ 54.6
SSDP	30.8
SNMP	6.3
Memcached	可达数万

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 攻击的类型 2 — 传输层攻击

状态耗尽 DDoS 攻击：协议耗尽

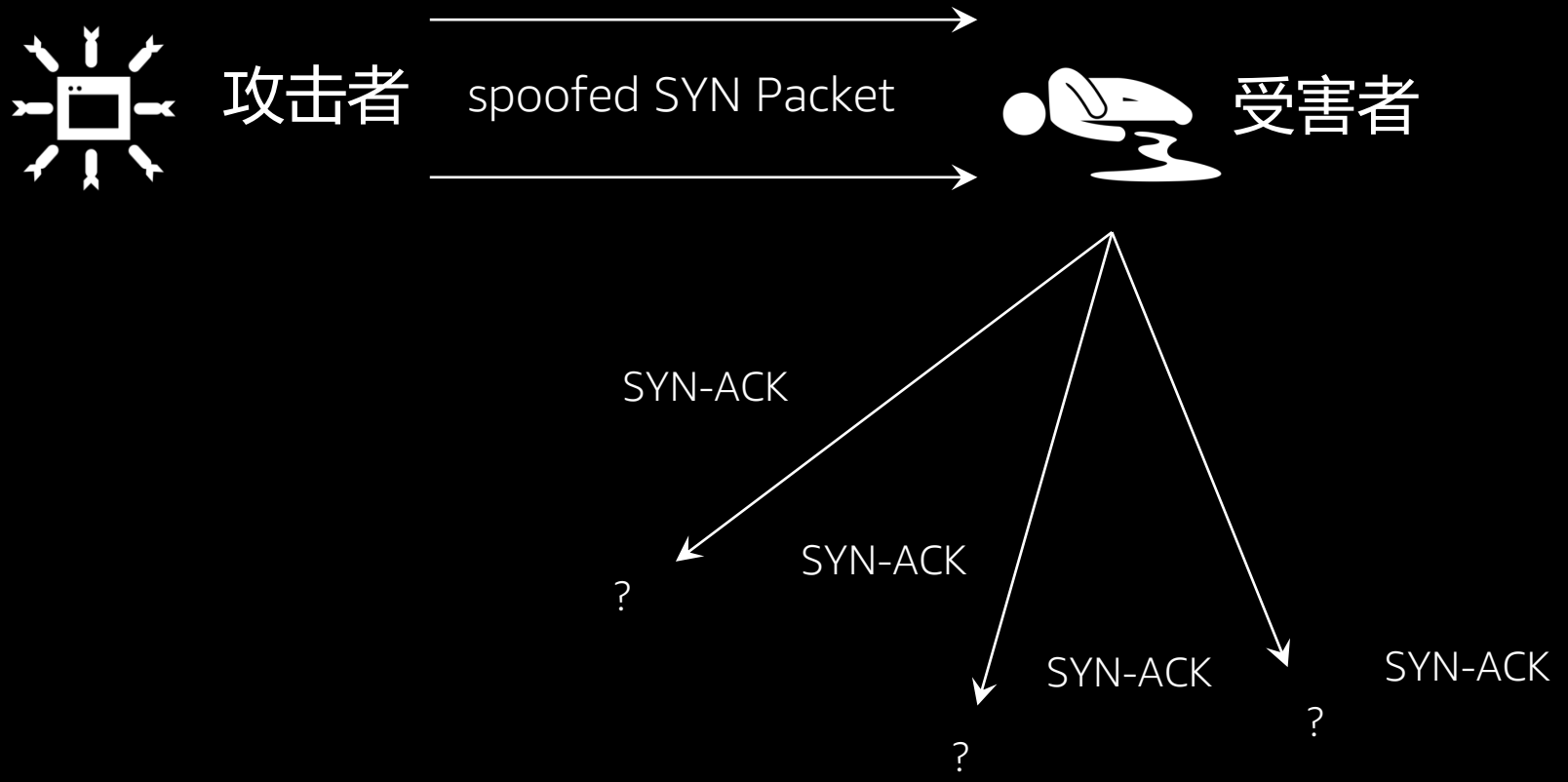
滥用协议的一些弱点，试图压垮系统（如防火墙，负载均衡等）

例如 TCP SYN 泛洪（SYN Flood）

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 传输层攻击方法 — SYN Flood

SYN flood 或称 SYN 洪水、SYN 洪泛是一种阻断服务攻击，起因于攻击者传送一系列的 SYN 请求到目标系统



- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 攻击的类型 3 — 应用层攻击

应用消耗

使用格式良好但恶意的请求

来规避防御，并消耗应用程序资源

例如 HTTP GET 泛洪（GET Flood）、DNS 查询泛洪（DNS Query Flood）

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

DDoS 应用层攻击方法 — HTTP 攻击

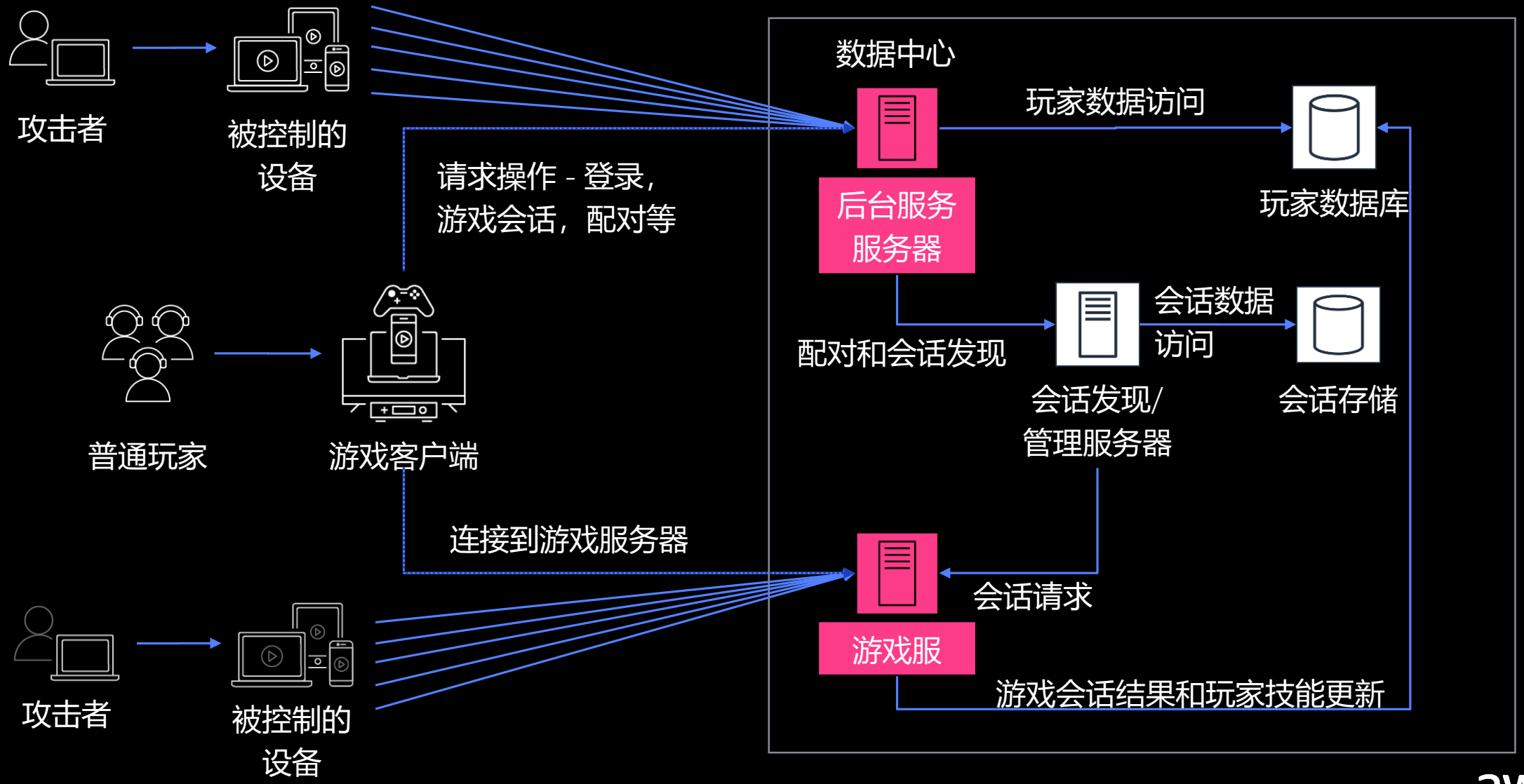
慢攻击工具的原理就是想办法让服务器等待，当服务器在保持连接等待时，自然就消耗了资源。

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

游戏服务常见的受攻击点

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

游戏服务的攻击点



- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

AWS DDoS攻击最佳实践

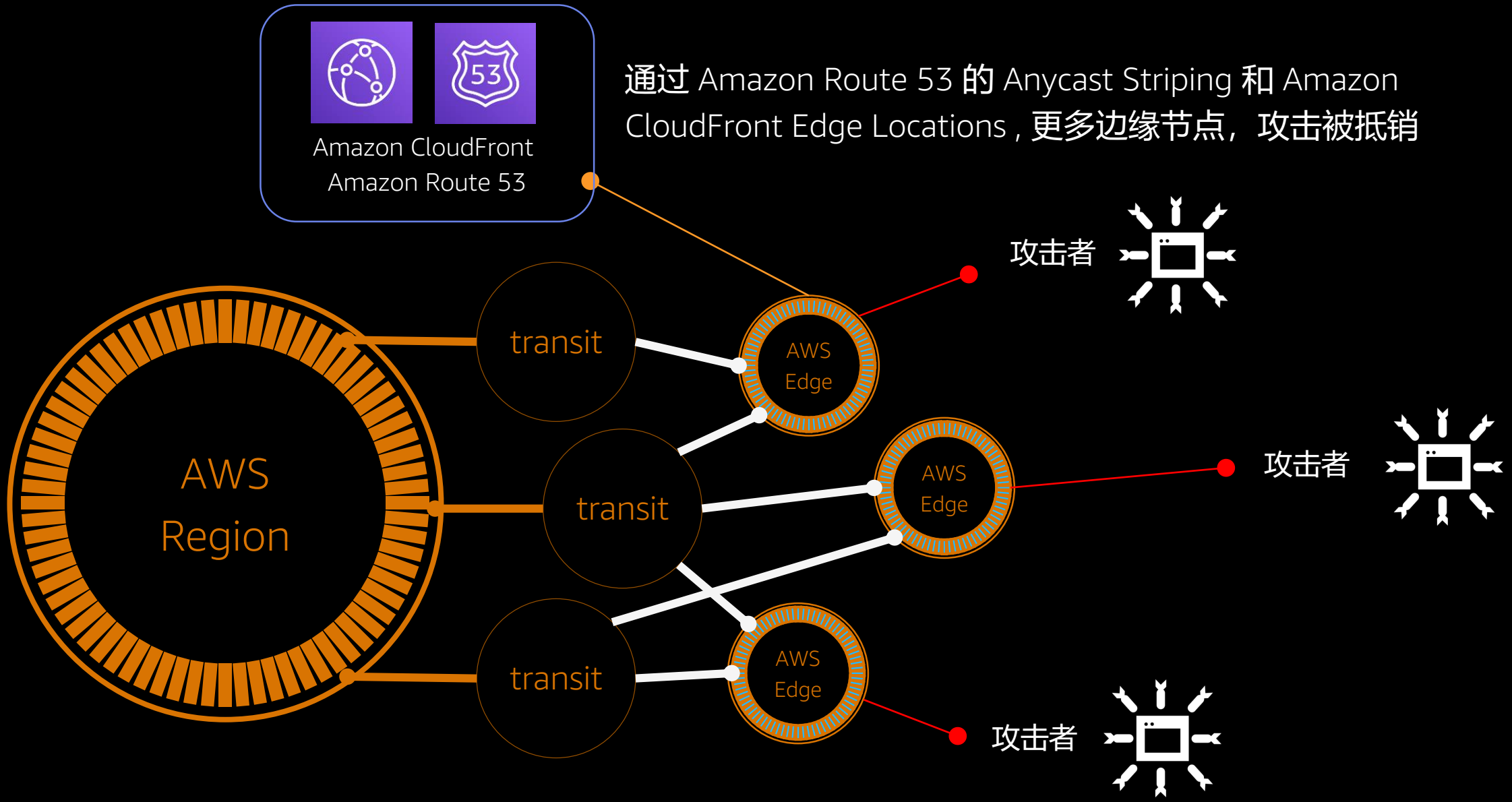
- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

AWS 全球基础架构
已内置 DDoS 防御能力（AWS Shield）

- ✓ DDoS 防御能力已内置集成到 AWS 的网络服务（CloudFront, Route53, ELB）；
- ✓ DDoS 防御一直开启，快速抵御，无需人工干预或进行外部路由；
- ✓ 充分利用 AWS 数据中心的冗余互联网连接和超高带宽；
- ✓ 自动抵御最常见的攻击，如：SYN/ACK 泛洪、UDP 泛洪、反射攻击等；
- ✓ 无需额外费用。

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

aws



了解详情，请访问：https://d1.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

如何缓解 DDoS 攻击

— 针对 HTTPS 攻击

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

针对 HTTP Flood, AWS 提供的 DDoS 防御能力

使攻击面最小化

创建 DMZ 区，将攻击阻挡在外层
并通过 Security Group 限定进入流量


ELB


SSH Bastion


NAT Gateway

保护暴露的资源

Web Application Firewall 检测并过滤
应用层流量 HTTP & HTTPS


WAF

定制 AWS WAF 规则，SQLi, XSS, 限速机制，黑名单

自动扩展应对攻击

通过自动扩展与快速分布的资源，将
攻击威力分散与减弱


Edge location

Route 53


ELB

对攻击制订对应策略

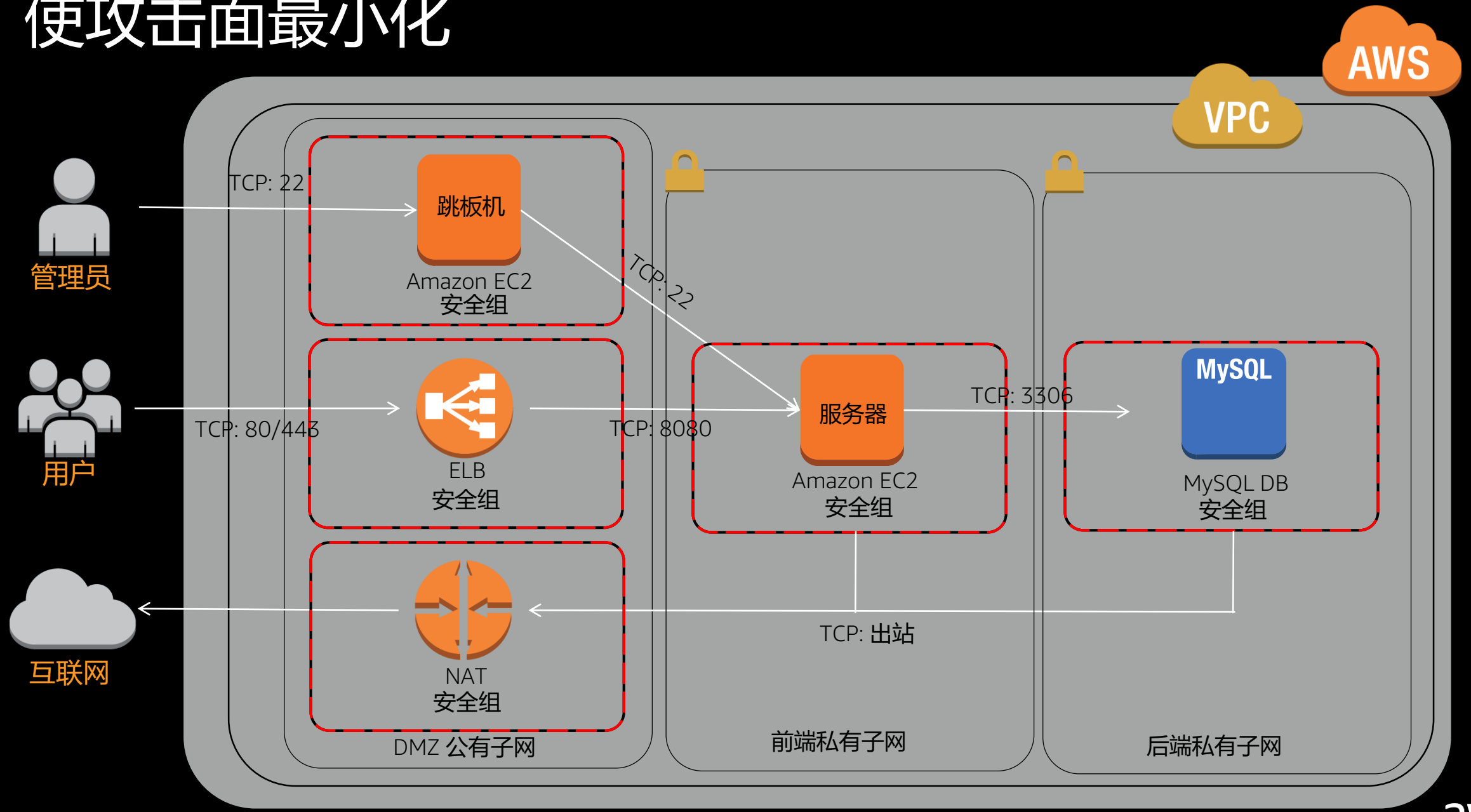
对服务正常的行为模式了如指掌，对
于异常状况就能快速反应


AWS Shield


CloudWatch

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

使攻击面最小化



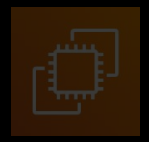
- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

针对 HTTP Flood, AWS 提供的 DDoS 防御能力

使攻击面最小化

创建 DMZ 区，将攻击阻挡在外层
并通过 Security Group 限定进入流量


ELB


SSH Bastion


NAT Gateway

保护暴露的资源

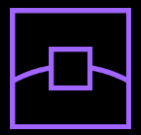
Web Application Firewall 检测并过滤
应用层流量 HTTP & HTTPS


WAF

定制 AWS WAF 规则，SQLi, XSS, 限速机制，黑名单

自动扩展应对攻击

通过自动扩展与快速分布的资源，将
攻击威力分散与减弱


Edge location

Route 53


ELB

对攻击制订对应策略

对服务正常的行为模式了如指掌，对
于异常状况就能快速反应

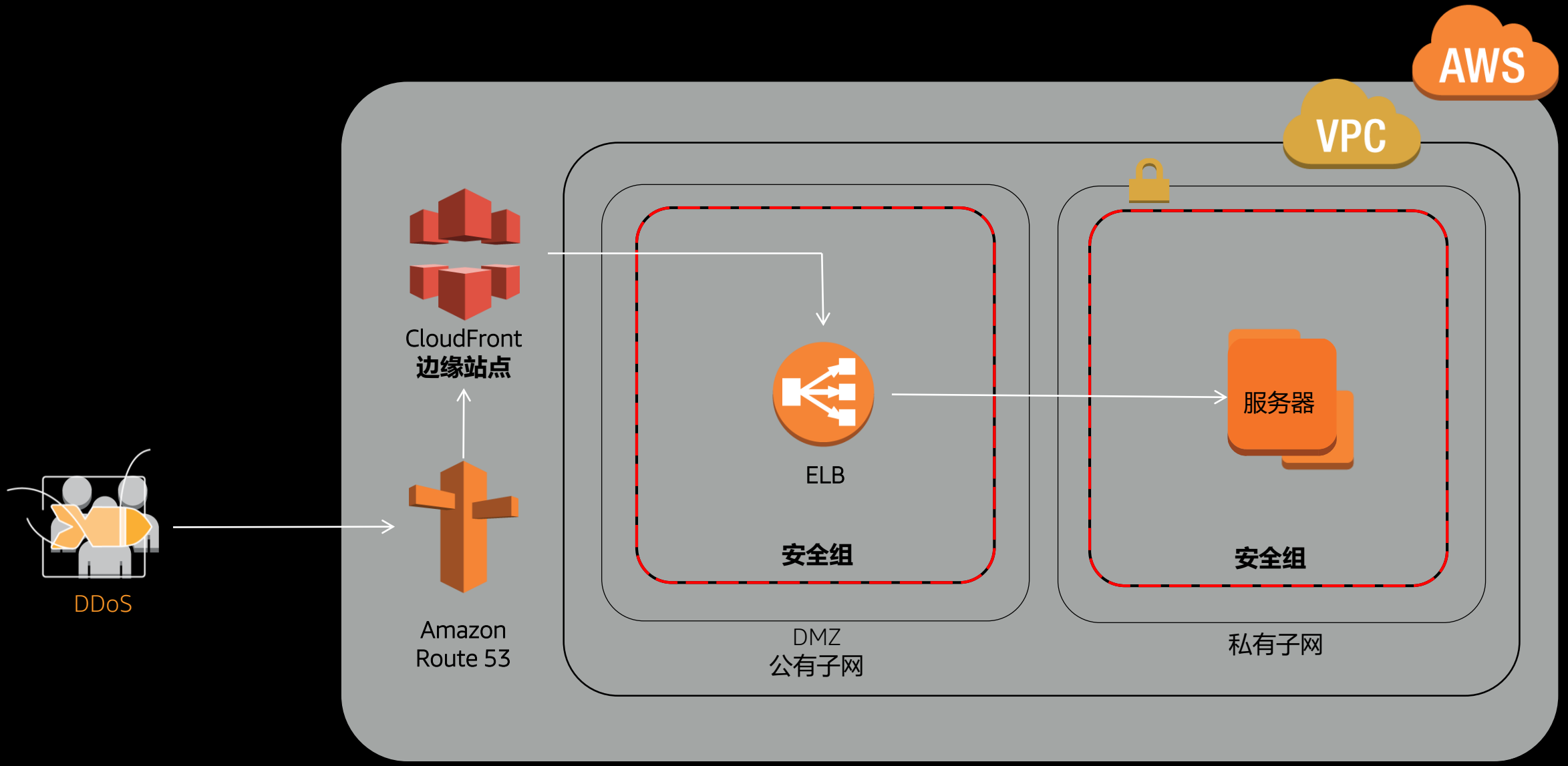

AWS Shield


CloudWatch

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

aws

自动扩展应对攻击



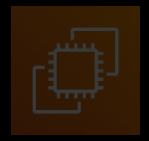
- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

针对 HTTP Flood, AWS 提供的 DDoS 防御能力

使攻击面最小化

创建 DMZ 区，将攻击阻挡在外层
并通过 Security Group 限定进入流量


ELB


SSH Bastion


NAT Gateway

保护暴露的资源

Web Application Firewall 检测并过滤
应用层流量 HTTP & HTTPS


WAF

定制 AWS WAF 规则，SQLi, XSS, 限速机制，黑名单

自动扩展应对攻击

通过自动扩展与快速分布的资源，将
攻击威力分散与减弱


Edge location

Route 53


ELB

对攻击制订对应策略

对服务正常的行为模式了如指掌，对
于异常状况就能快速反应


AWS Shield


CloudWatch

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

aws

如何缓解 DDoS 攻击

—针对 TCP 与 UDP 攻击

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

使用 TCP 协议的 Game Server，建议的 DDoS 防御措施

Amazon VPC

- ✓ 正确设置安全组及 VPC Network ACLs，禁用 UDP/ICMP 以及用不到的 TCP 端口
- ✓ 免费的 UDP 泛洪和反射攻击防护，以及 ICMP 泛洪

AWS ELB

- ✓ 使用 ELB/NLB 可以帮助支撑更多的 SYN Flood 流量，更大的吞吐和包处理能力

Amazon EC2

- ✓ Amazon Linux 默认打开 SYN Cookie (net.ipv4.tcp_syncookies = 1)
- ✓ 提供很高的小包吞吐能力吸收 SYN 泛洪，ACK 泛洪

AWS Shield Advanced

- ✓ AWS Shield Advanced 能够提供 SYN 限速的功能

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

使用 TCP 协议的 Game Server，建议的 DDoS 防御措施

Amazon VPC

- ✓ 正确设置安全组及 VPC Network ACLs，禁用 UDP/ICMP 以及用不到的 TCP 端口
- ✓ 免费的 UDP 泛洪和反射攻击防护，以及 ICMP 泛洪

AWS ELB

- ✓ 使用 ELB/NLB 可以帮助支撑更多的 SYN Flood 流量，更大的吞吐和包处理能力

Amazon EC2

- ✓ Amazon Linux 默认打开 SYN Cookie (net.ipv4.tcp_syncookies = 1)
- ✓ 提供很高的小包吞吐能力吸收 SYN 泛洪，ACK 泛洪

AWS Shield Advanced

- ✓ AWS Shield Advanced 能够提供 SYN 限速的功能

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

使用 TCP 协议的 Game Server，建议的 DDoS 防御措施

Amazon VPC

- ✓ 正确设置安全组及 VPC Network ACLs，禁用 UDP/ICMP 以及用不到的 TCP 端口
- ✓ 免费的 UDP 泛洪和反射攻击防护，以及 ICMP 泛洪

AWS ELB

- ✓ 使用 ELB/NLB 可以帮助支撑更多的 SYN Flood 流量，更大的吞吐和包处理能力

Amazon EC2

- ✓ Amazon Linux 默认打开 SYN Cookie (net.ipv4.tcp_syncookies = 1)
- ✓ 提供很高的小包吞吐能力吸收 SYN 泛洪，ACK 泛洪

AWS Shield Advanced

- ✓ AWS Shield Advanced 能够提供 SYN 限速的功能

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

使用 TCP 协议的 Game Server，建议的 DDoS 防御措施

Amazon VPC

- ✓ 正确设置安全组及 VPC Network ACLs，禁用 UDP/ICMP 以及用不到的 TCP 端口
- ✓ 免费的 UDP 泛洪和反射攻击防护，以及 ICMP 泛洪

AWS ELB

- ✓ 使用 ELB/NLB 可以帮助支撑更多的 SYN Flood 流量，更大的吞吐和包处理能力

Amazon EC2

- ✓ Amazon Linux 默认打开 SYN Cookie (net.ipv4.tcp_syncookies = 1)
- ✓ 提供很高的小包吞吐能力吸收 SYN 泛洪，ACK 泛洪

AWS Shield Advanced

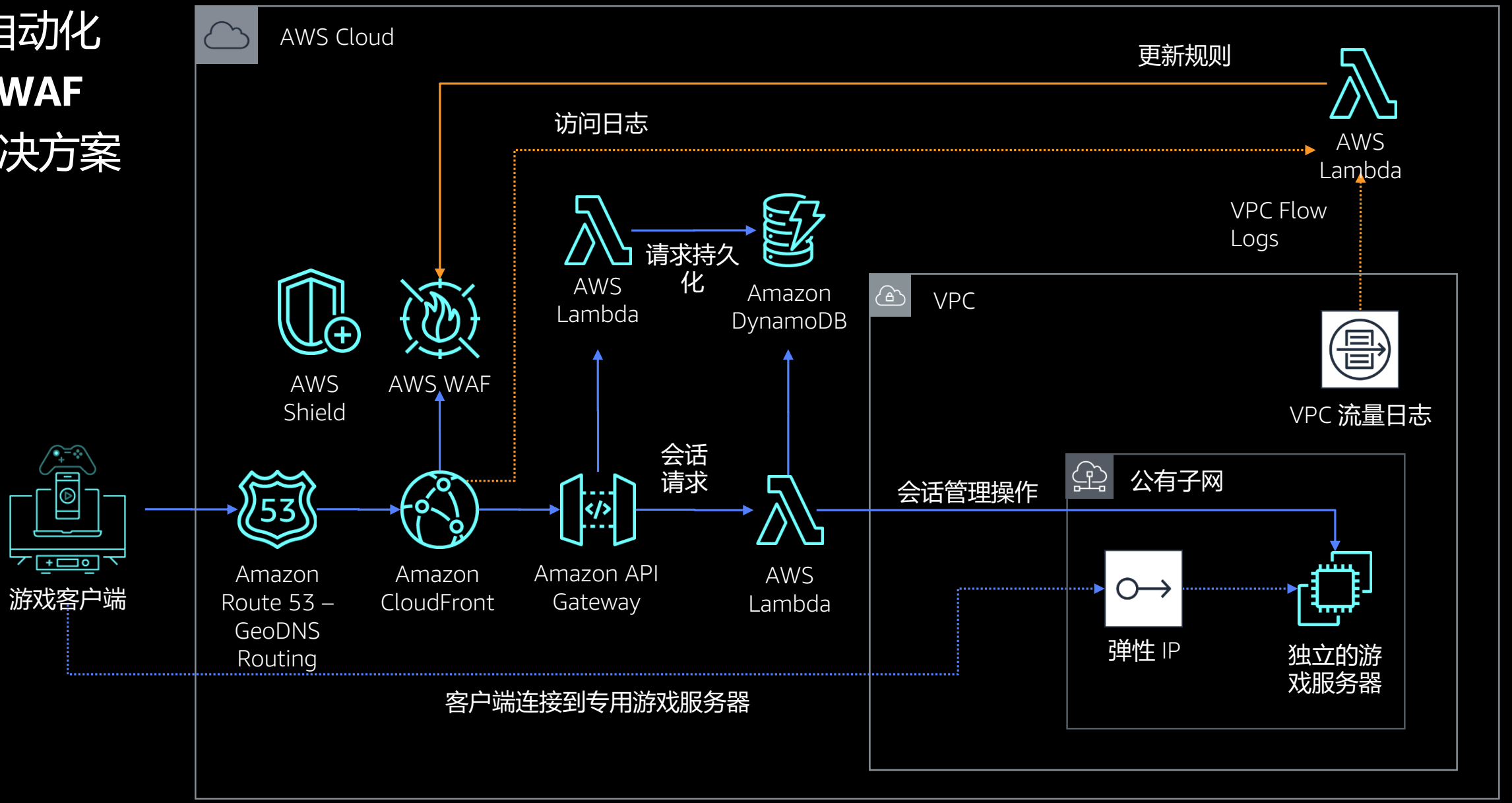
- ✓ AWS Shield Advanced 能够提供 SYN 限速的功能
- ✓ Byte Match 、针对特定的 Magic Salt 进行白名单，其余UDP包抛弃

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

云原生的游戏安全防御解决方案

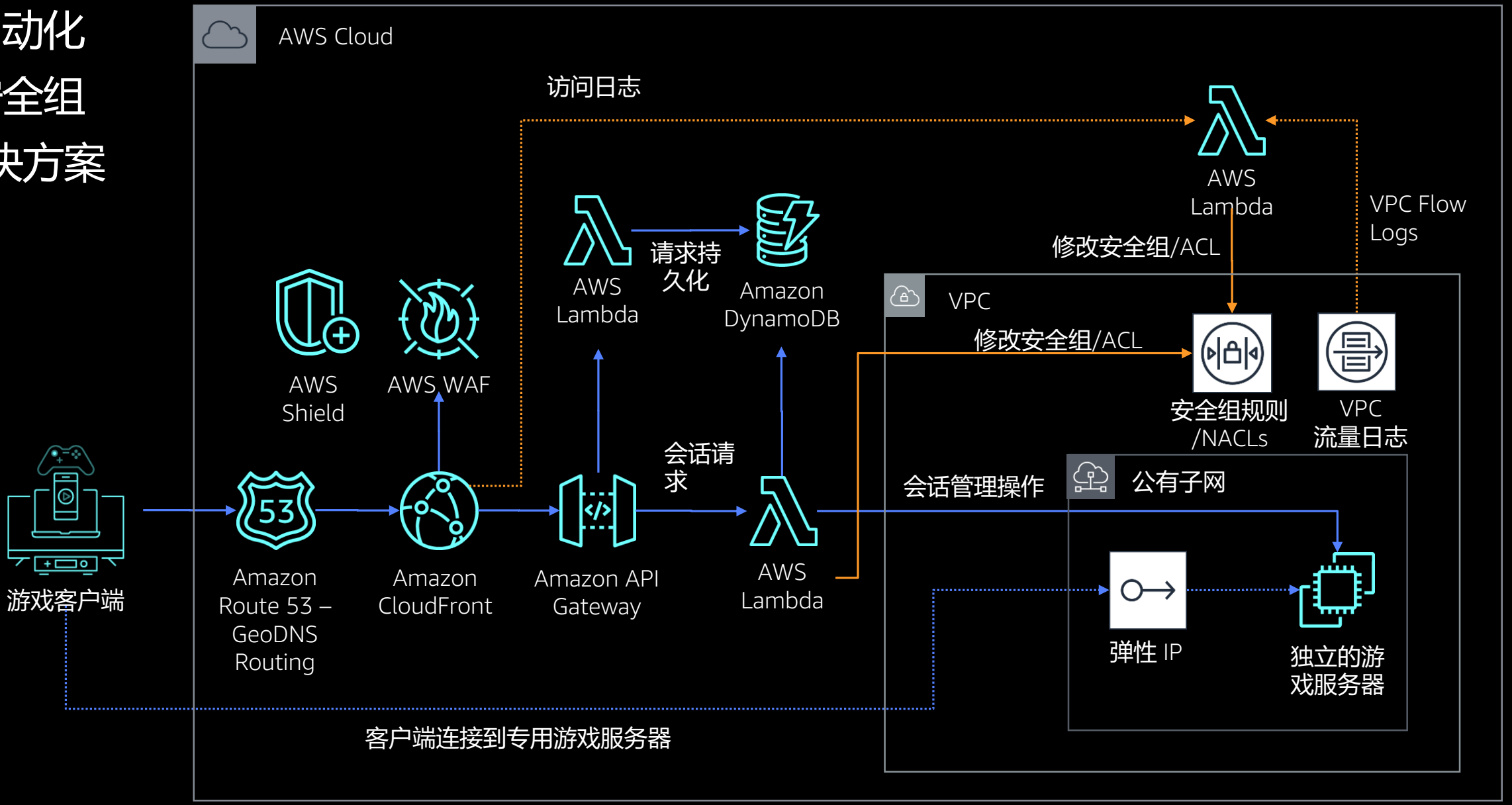
- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

自动化 WAF 解决方案



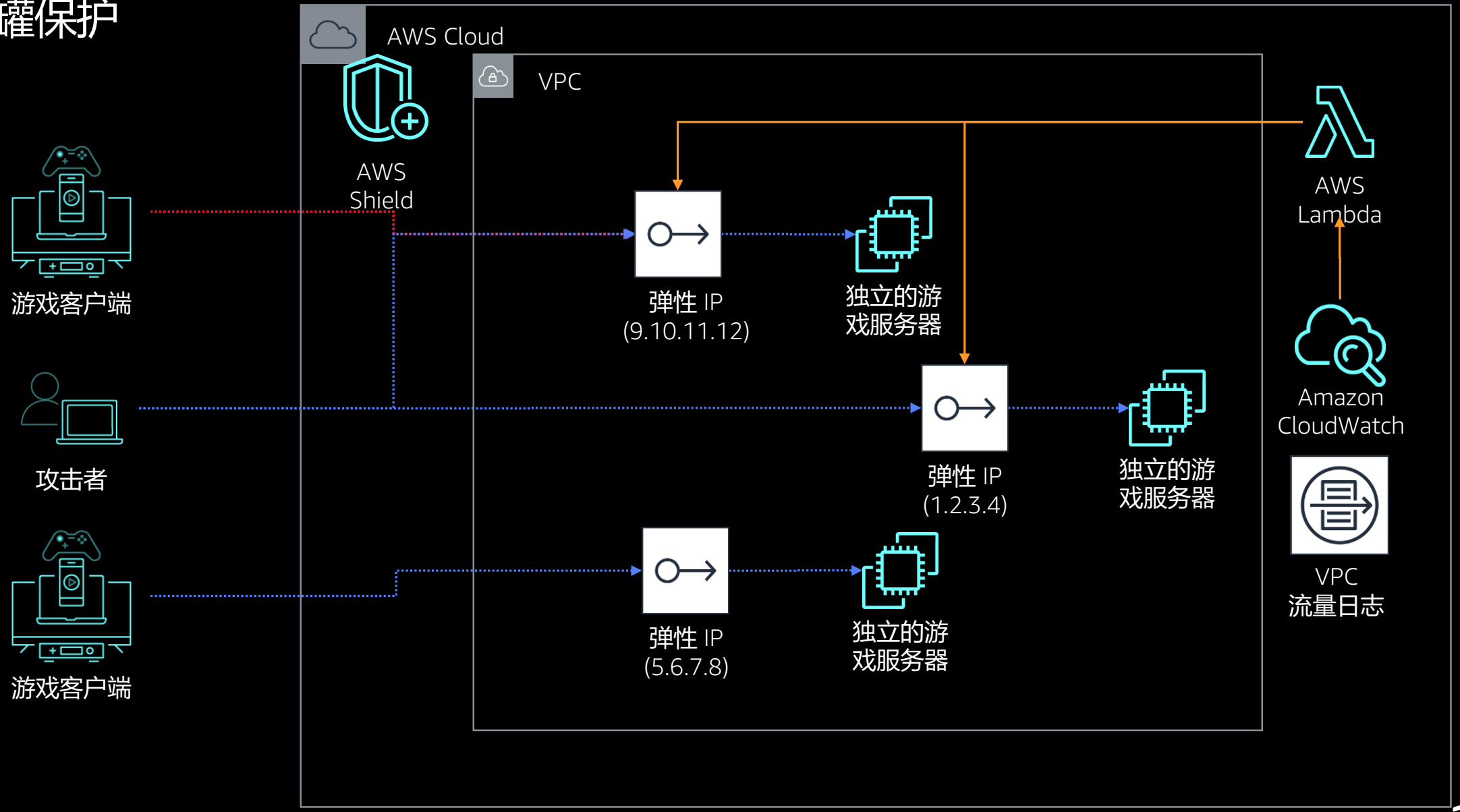
- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

自动化安全组解决方案



- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

蜜罐保护



- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营

Thank you!

- AWS中国（宁夏）区域由西云数据运营
- AWS中国（北京）区域由光环新网运营