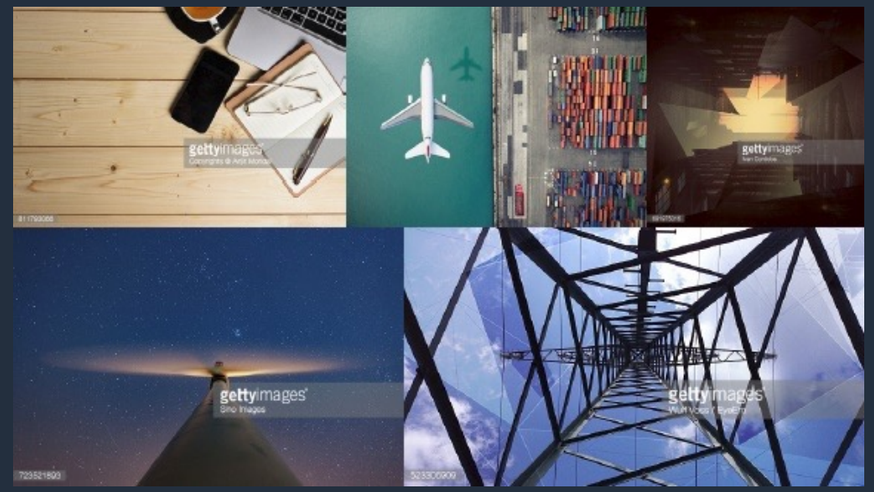
亚马逊云科技

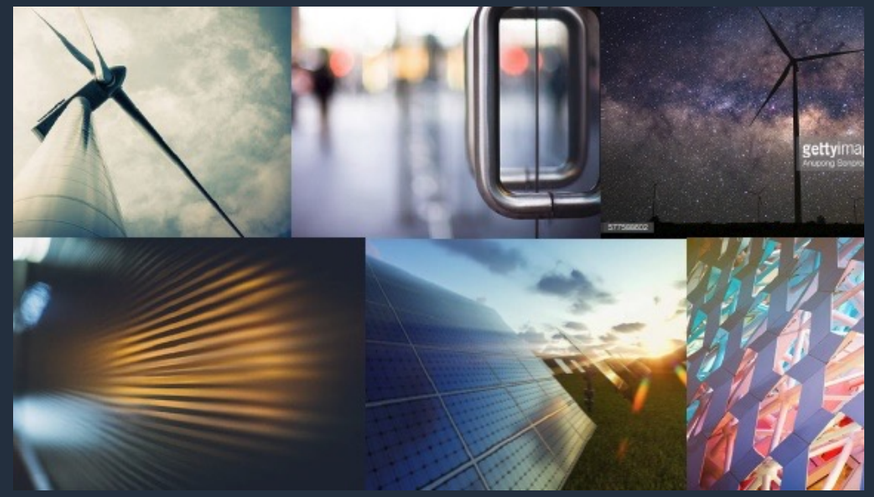
Amazon Shield/WAF 介绍

叶明
亚马逊云科技中国 边缘产品架构师

企业上云的安全挑战

- 企业上云为我们带来了新的机遇 – 互联网的机遇
- 企业上云同时也带来了新的挑战 – 互联网的安全威胁





来自互联网的安全事件规模

亚马逊云科技2020年Q1监测数据

单次攻击最大流量

2.3T

事件总数

31万次

互联网安全威胁的多样性

CC攻击

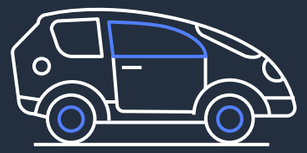
“海量仿真”

DNS劫持

“流量误导”

勒索事件

“交钱解锁”



漏洞渗入

“信息窃取”

僵尸病毒

“你花钱我办事”

亚马逊云科技互联网安全防护理念

"打铁还需自身硬"

25 Launched Regions Each with multiple Availability Zones (AZ's)	**81 Availability Zones**	**5 Local Zones** **13 Wavelength Zones** For ultralow latency applications	**7 Announced Regions** **12 Announced Local Zones**
2x More Regions With multiple AZ's than the next largest cloud provider	**245 Countries and Territories Served**	**108 Direct Connect Locations**	**230+ Points of Presence** 218+ Edge Locations and 12 Regional Edge Caches

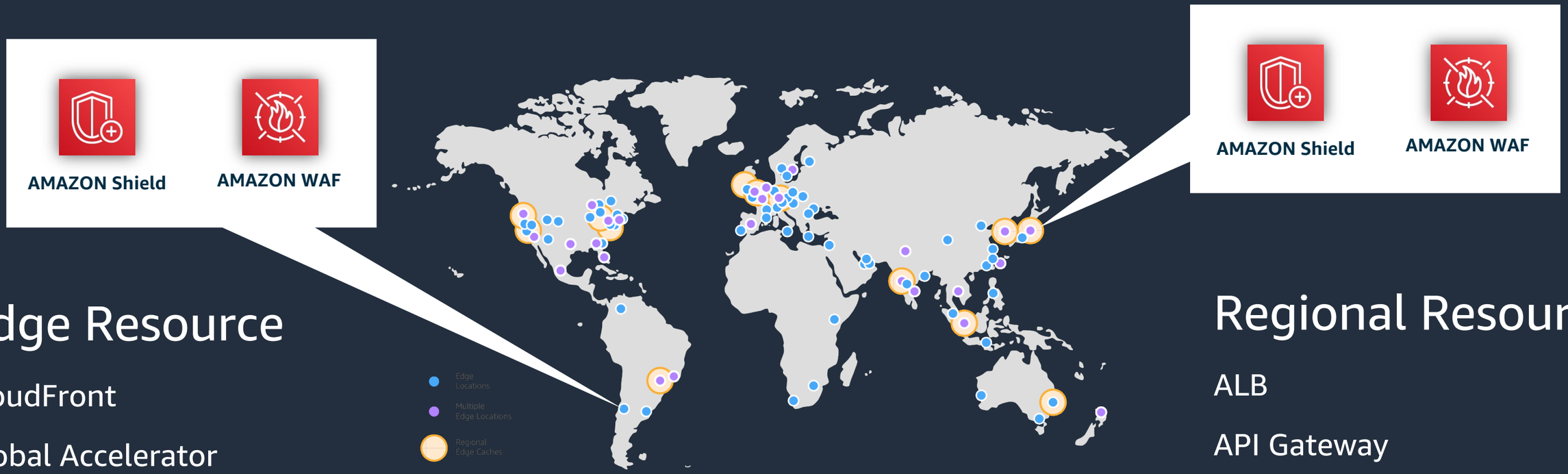
完善的基础设施

"植入式"安全

亚马逊云科技

亚马逊云科技互联网安全防护理念

"安全防护从边缘做起"



Edge Resource

CloudFront

Global Accelerator

Regional Resource

ALB

API Gateway

亚马逊云科技互联网安全防护产品

WAF

WEB 安全防护

Shield Standard

IP/TCP/UDP 基本安全防护

Shield Advanced

高级安全防护

Firewall Manager

安全管理

中国区WAF已经可以提供服务

2021年6月

亚马逊云科技
北京区和宁夏区
WAF

WAF

亚马逊云科技

亚马逊云科技 WAF的特点

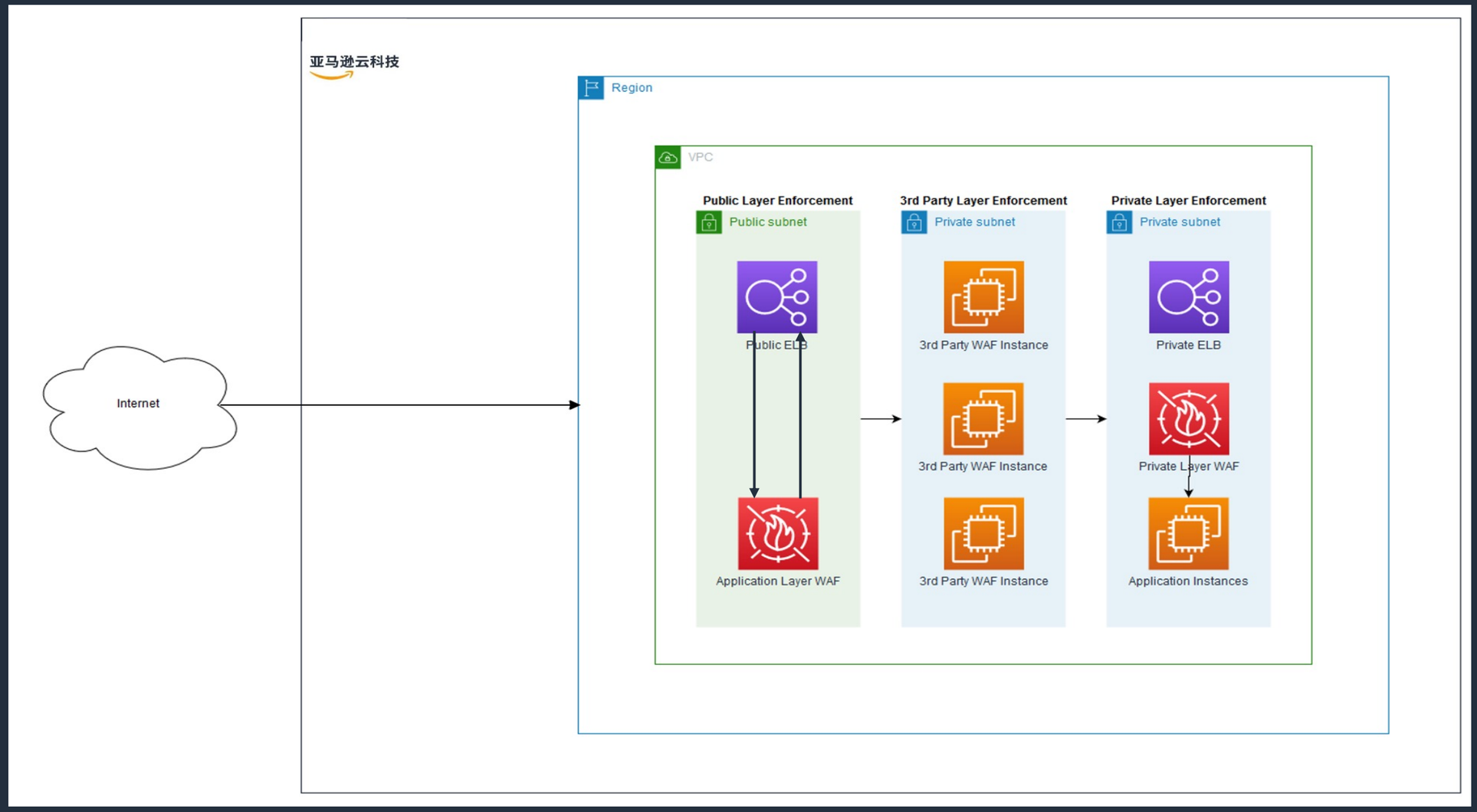
部署方便: 无需改动现有云上架构，旁路式部署无需安装TLS/SSL证书，可以和已部署的WAF实例共存

可扩展性: Managed cluster，no need to prewarm

兼顾易用性和复杂度: 使用托管规则进行快速部署，使用自定义规则进行限速和过滤

支持Devops方式部署: API 驱动自动化部署

WAF部署架构



亚马逊云科技WAF托管规则

常用
托管规则

OWASP Top 10

PHP / SQLi

Linux / Admin Page

威胁IP地址库

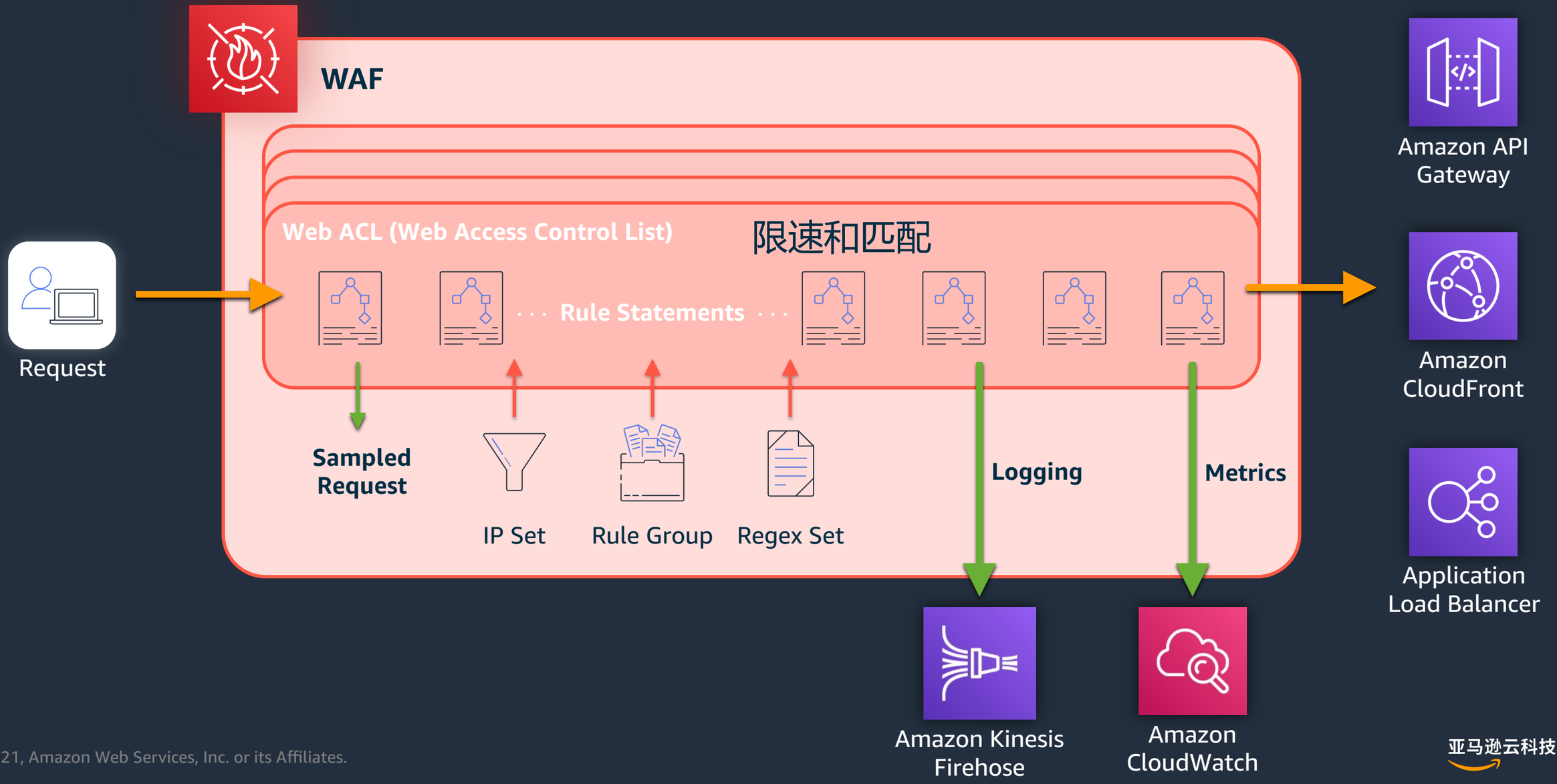
.....

第三方
托管规则

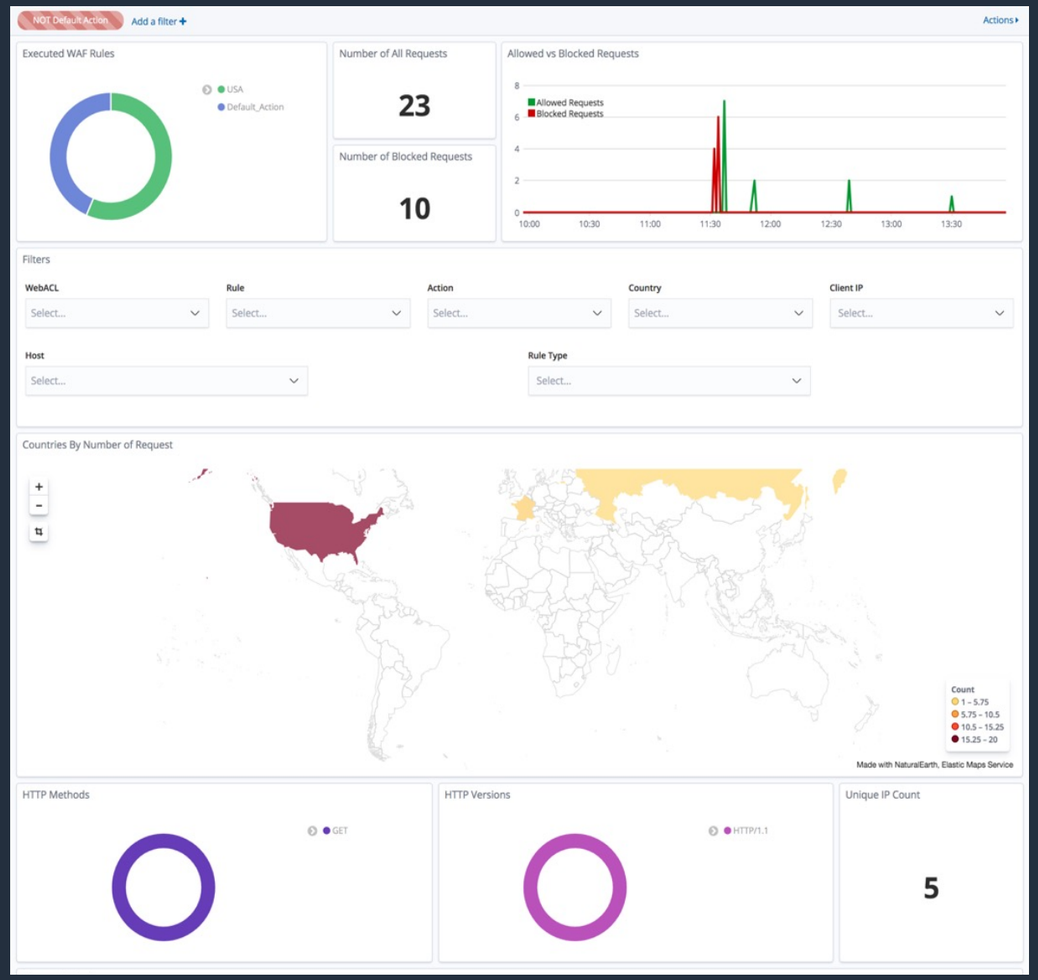
机器人
托管规则

聊天机器人
广告机器人
爬虫机器人
扫描机器人
… …

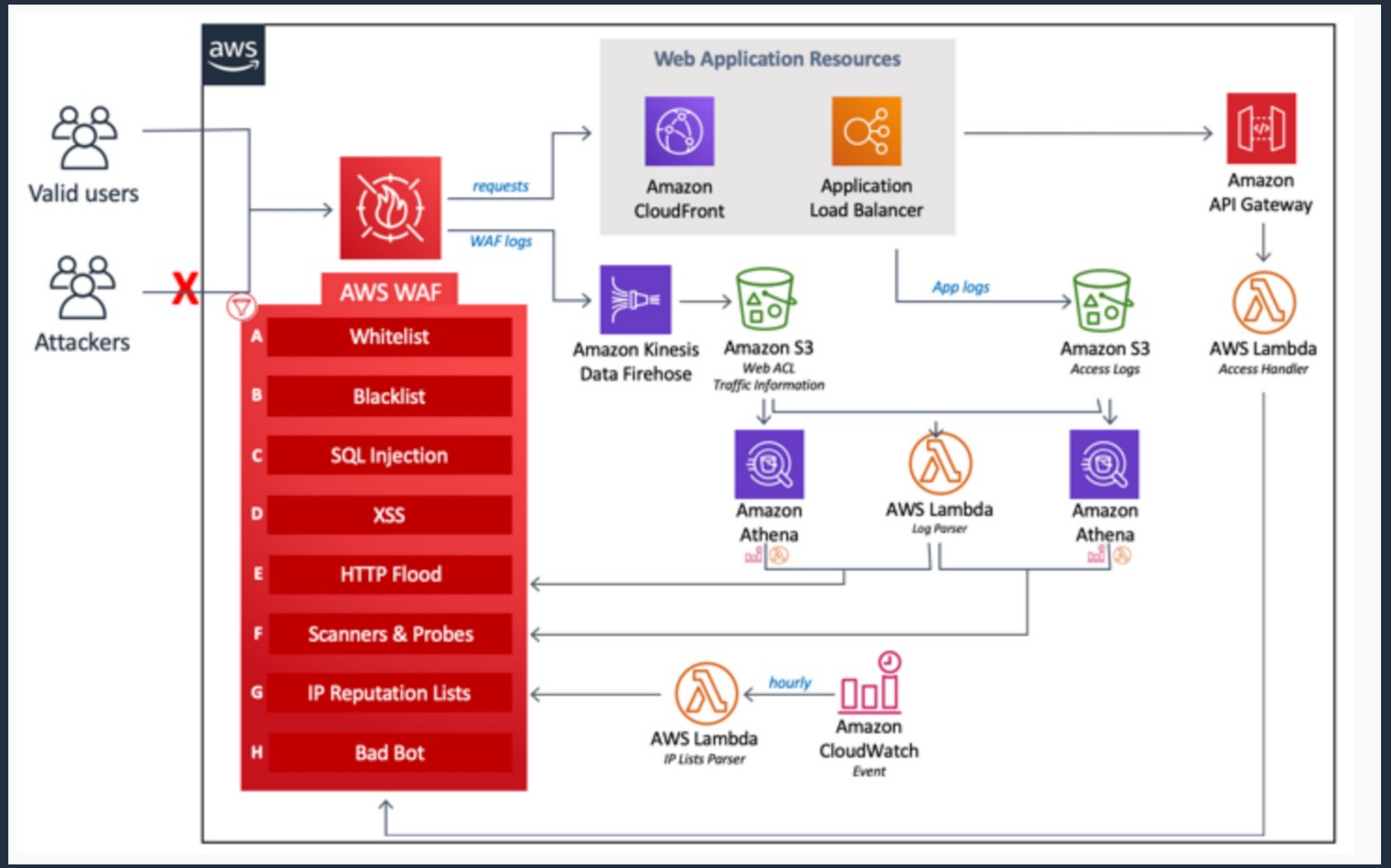
亚马逊云科技WAF自定义规则和数据获取



WAF 扩展监控：Kinesis + ELK



WAF自动化：Lambda + WAF API



Shield Advance

亚马逊云科技

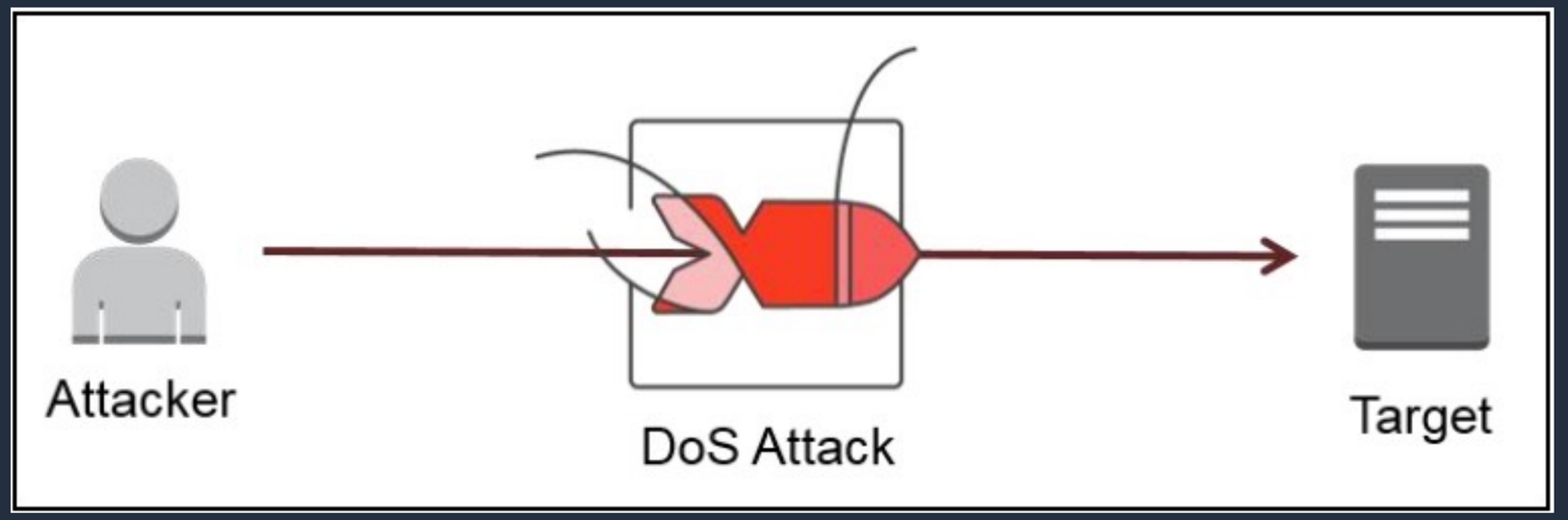
拒绝服务攻击——DoS（Denial of Service）

通过各种手段，使网络服务无法使用或不可用的行为

如果攻击来源单一，
可以简单拦截IP防范

Service Unavailable

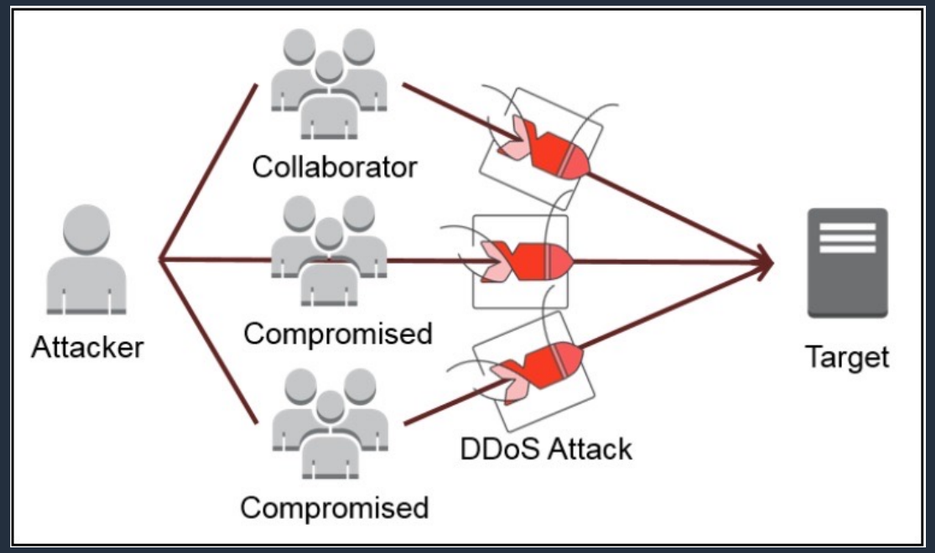
HTTP Error 503. The service is unavailable.

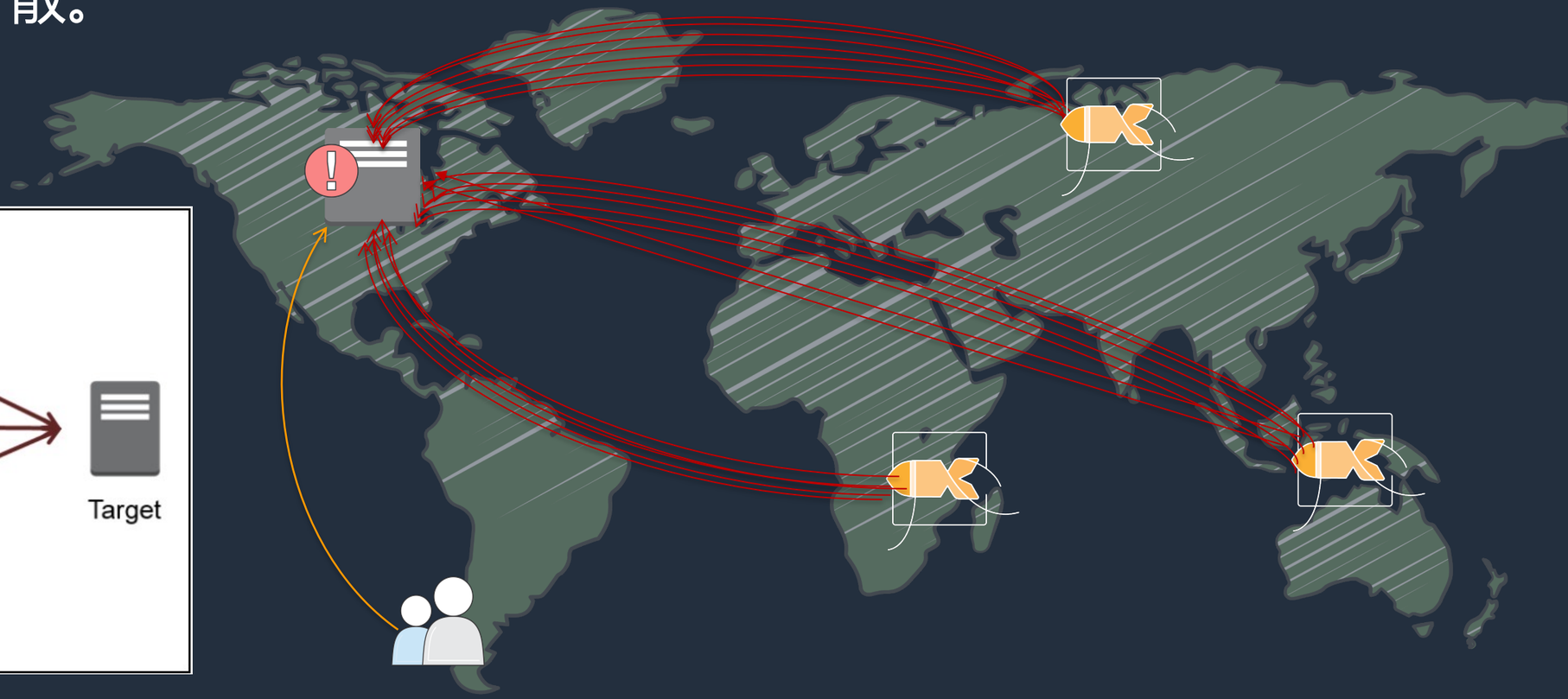


分布式拒绝服务攻击——DDoS(Distributed Denial Of Service)

攻击者会使用大量广泛分布的僵尸网络、肉机等发起对目标的攻击

其来源分布一般比较分散。
因此难以简单防范。





Shield：L3/4层防护

- 异常发现
- 数据清洗
- 数据限速
- 连接验证

Shield

Amazon CloudFront

Amazon Route 53

Elastic Load Balancing

Global Accelerator

Elastic IP Address

Shield Advance：完整安全防护

Shield

定制化L3/L4防护

WAF

定制化L7防护

SRT

攻击前/中/后响应

安全架构

TCP/UDP类应用

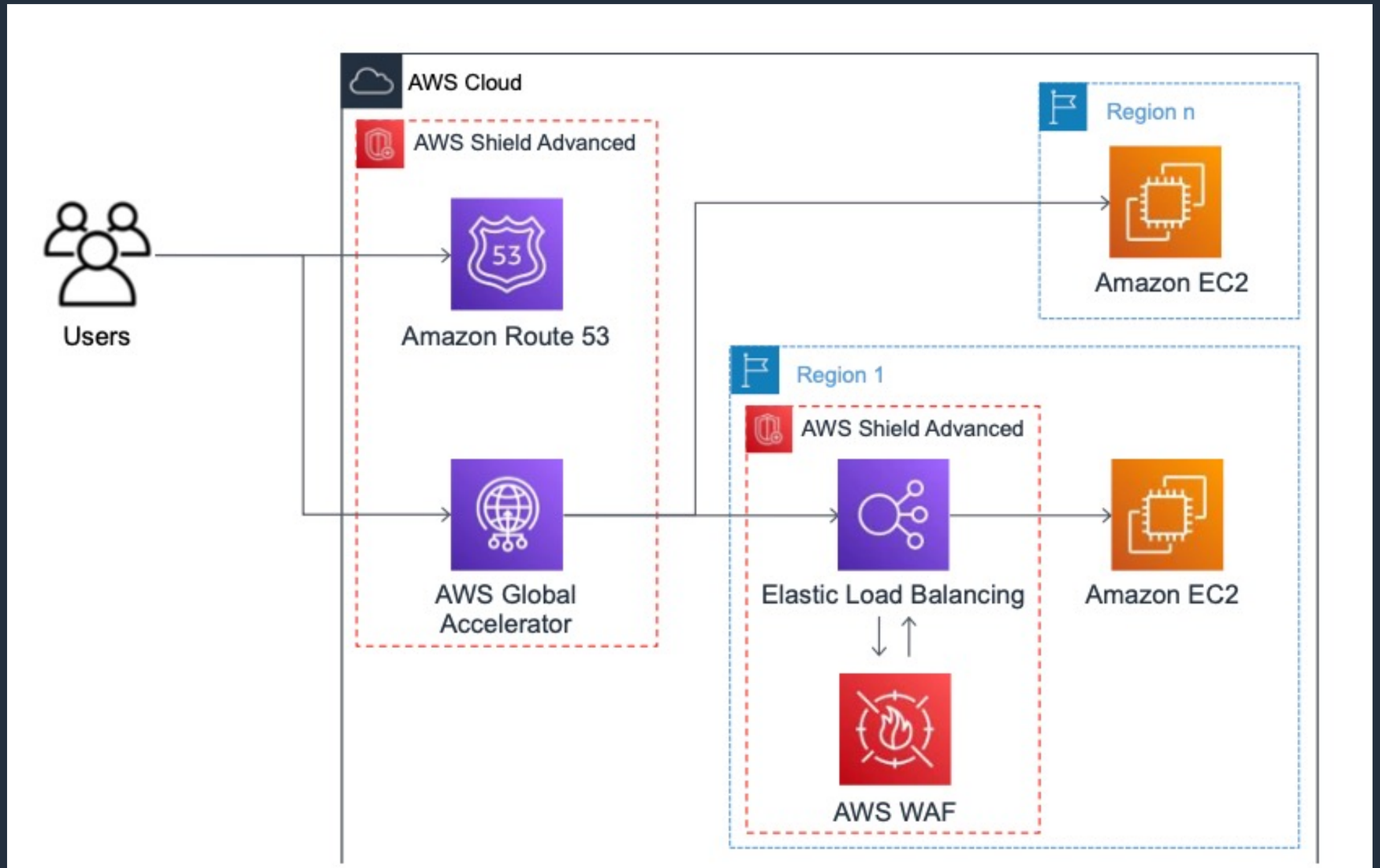


Figure 3 – Architecting DDoS resiliency for TCP and UDP applications

Web类应用

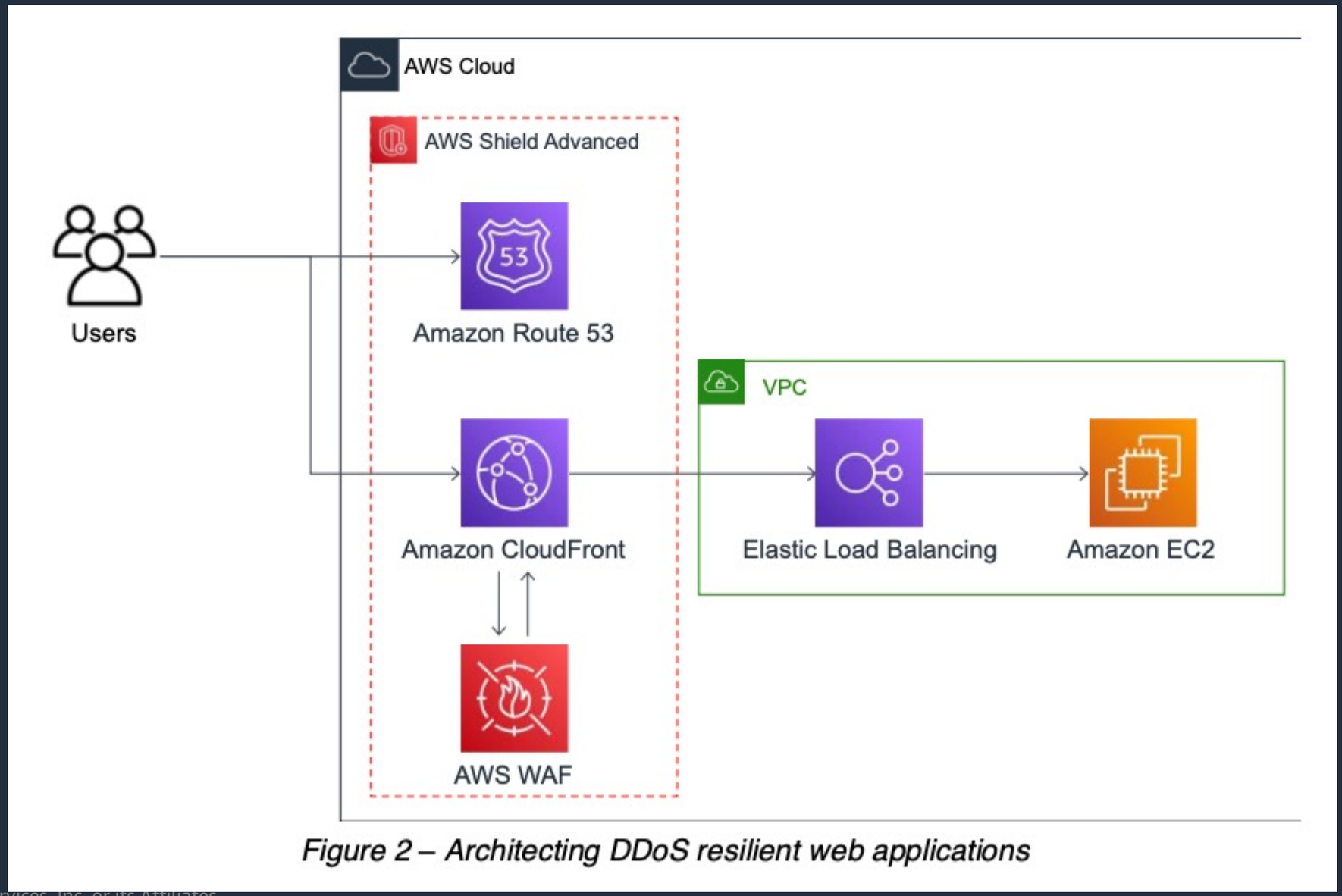


Figure 2 – Architecting DDoS resilient web applications