阿里云

2021阿里云开发者大会
ALIBABA CLOUD DEVELOPER CONFERENCE

云原生网络安全开发应用

CODE FUTURE_

轻盈如薄纱，坚固若磐石

朱家睿

高级产品专家

1、云上安全运维困难和挑战

安全与业务的割裂

安全是纵深在整条业务架构中的必要因素，但与业务的割裂导致安全建设和运维成本高

计费模式的割裂	部署形式的割裂	安全能力的割裂	业务变革的安全挑战
缺少安全效果计费	部署对架构入侵大	基础安全能力部分缺失	业务边缘化的安全挑战
计费模式的不统一	缺少混合云统一管理	安全生态能力融合难	容器和硬件安全需求

传统网络安全方案部署时遇到的挑战

用不了

因域名、DNS、端口、SNI等无法接入

- 没有域名、纯IP访问
- 不能修改DNS
- 非标端口
- 客户端不支持SNI

因资产规模、业务模型复杂等无法接入

- 多资产多端口
- 不能换IP
- 不希望改变网络架构
- 延迟不能增加

用不爽

接入后需要复杂配置、有扫描风险等

- 获取真实IP麻烦
- 防绕过额外增加配置
- TLS1.0、弱算法风险
- 证书多处维护

接入效率低，链路复杂度增加

- 大带宽业务成本高
- 被攻击换IP手忙脚乱
- 运维复杂度大大增加
- 额外增加链路故障风险

2.阿里云-原生网络安全方案

阿里云-原生网络安全方案

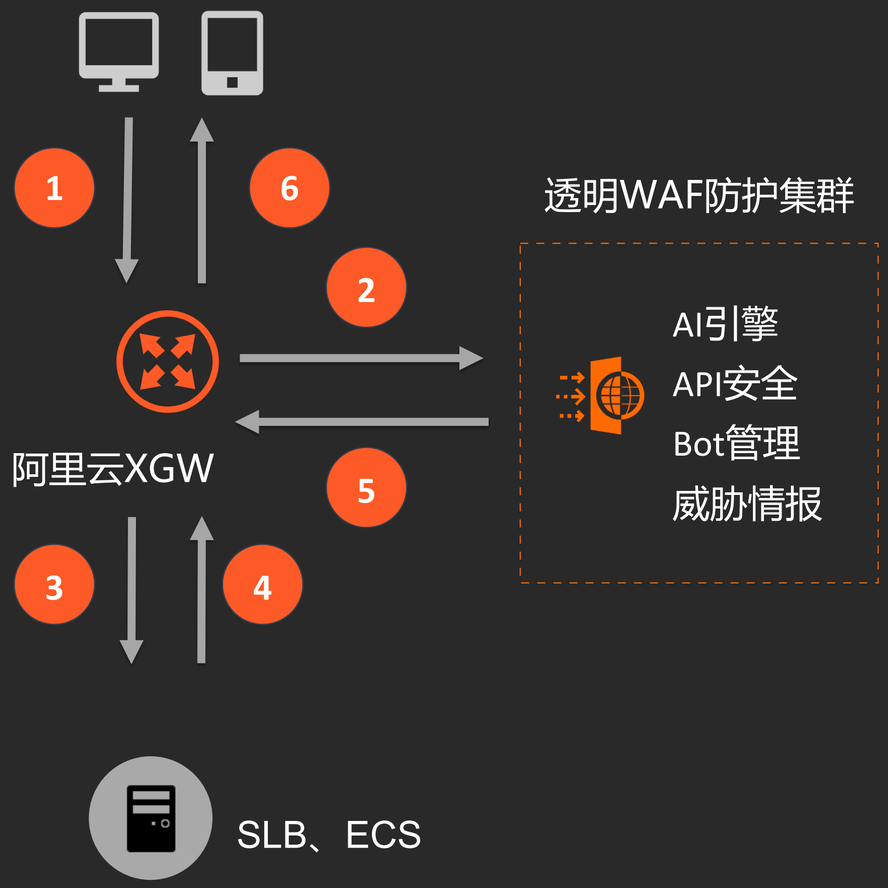
阿里云-原生安全帮助客户在现有业务架构基础上提供无缝部署、快速启用、按需付费的安全能力

亮点
最小化业务架构变化部署安全
一键启用
按需使用

客户价值
简化安全建设和运维，专注业务
建设安全能力，效果驱动付费
安全投入与业务发展阶段匹配
统一管理云上和云下安全能力
加速企业云化

原生透明WAF解决方案架构

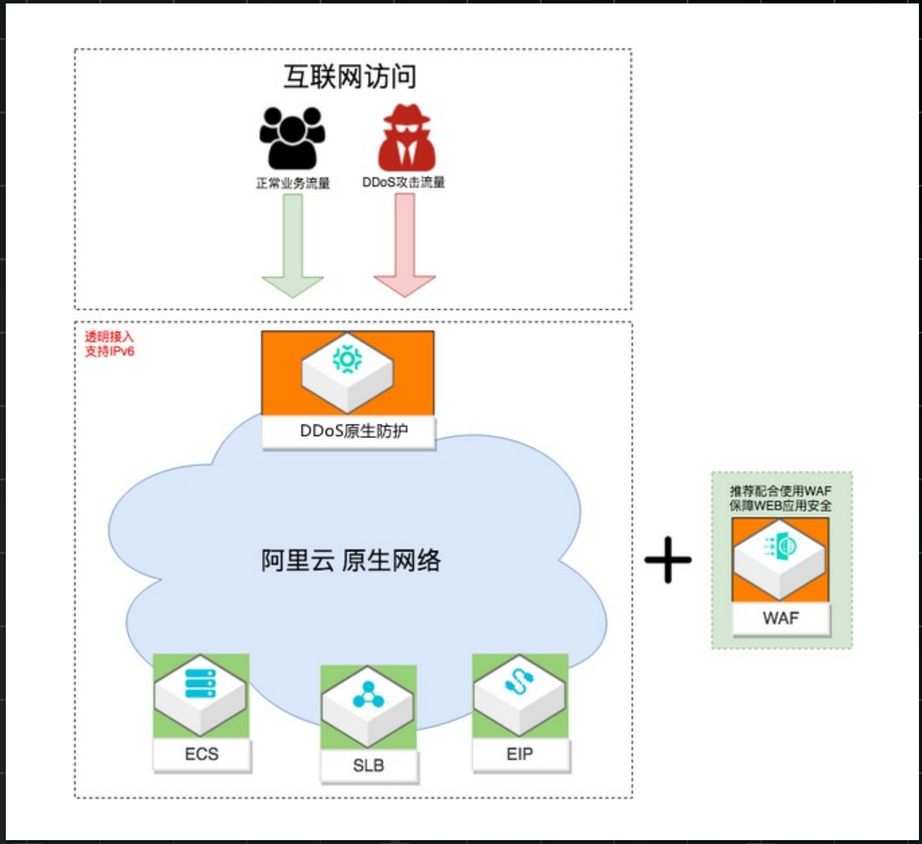
透明WAF业务数据流向图



- 不需要修改DNS接入
- 任何端口都可以接入WAF
- 不需要更换IP
- 不需要兼容SNI
- 不需要修改客户端和服务器逻辑

- 通过XGW技术将去往SLB的公网IP流量先牵引到WAF集群
- 安全检测后，流量回注到SLB并修改IP，让SLB看到真实客户端IP
- 在七层SLB(开启HTTP/S协议)上的端口、证书、TLS等设置均自动同步到WAF、无需额外配置
- 按量计费、根据防护需求按需定制合适的防护策略,进一步降低用户接入成本

DDoS原生防护解决方案



全账号全资产

- 账号级防护，支持防御数百上千云资产
- 支持全类型云产品，包括ECS、VPC、EIP、SLB、WAF、NAT等

不改架构 不增延迟

- 基于云原生，无需改变IP，一步完成
- 不增加延迟，不改变网络结构

费用可控

- 全力防护模式，不产生攻击后付费，无需升级弹性防护
- 部分开放按量计费模式

支持大型业务

- 适配所有业务规模，从100Mbps到1000Gbps，都可以合理成本接入

3、云原生网络安全产品使用介绍

透明WAF使用介绍

1.添加网站时，选择透明接入模式，完成相关授权

2.明确网站解析在哪个SLB实例和端口

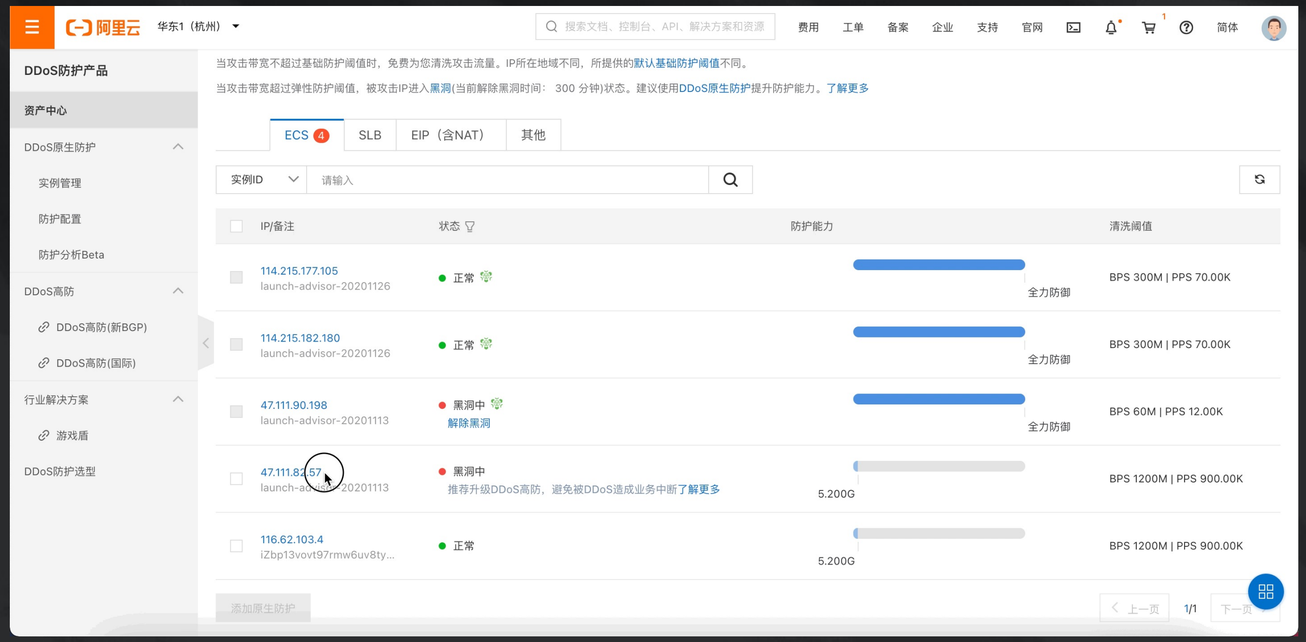
3.勾选对应端口、点击保存即完成引流防护

4.七层SLB实例下，无需选择协议、上传证书、选择负载算法等，所有配置均从SLB自动同步

DDoS原生防护使用介绍

1.选择对应资产，一键启动防护

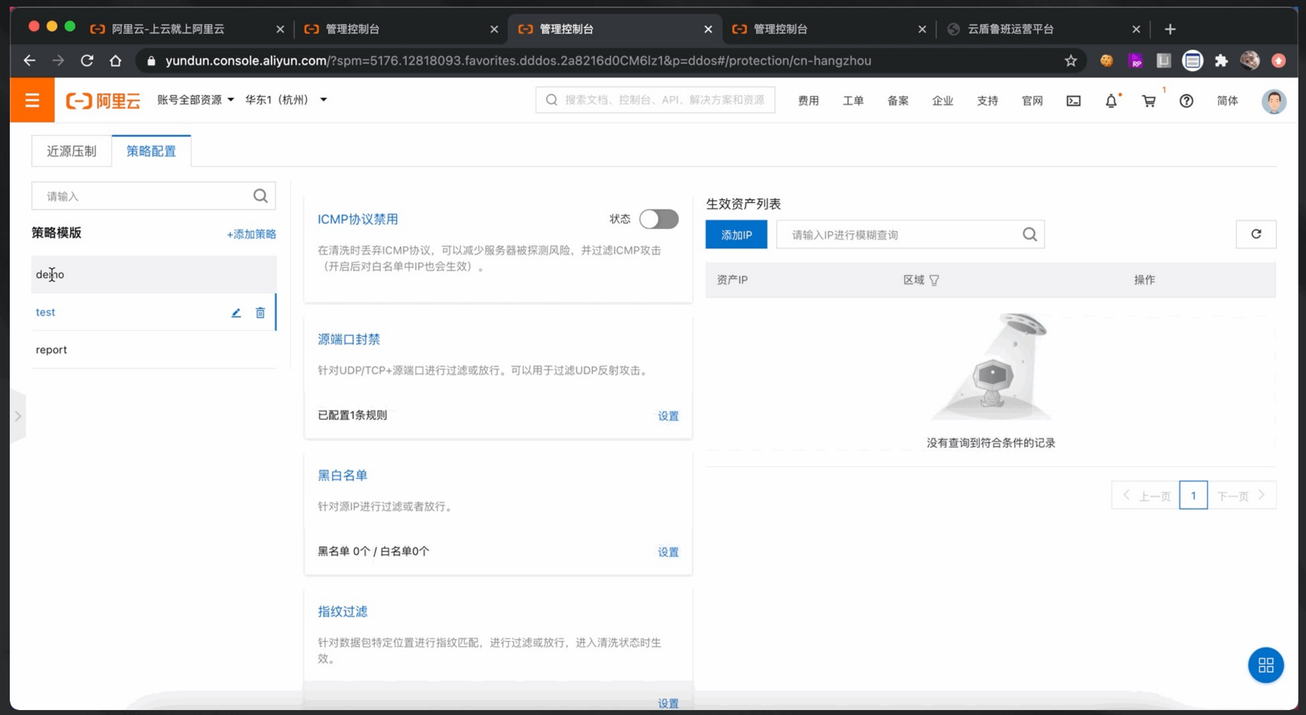
2.按需启用网络边界流量过滤



DDoS原生防护使用介绍

1.选择对应资产，一键启动防护

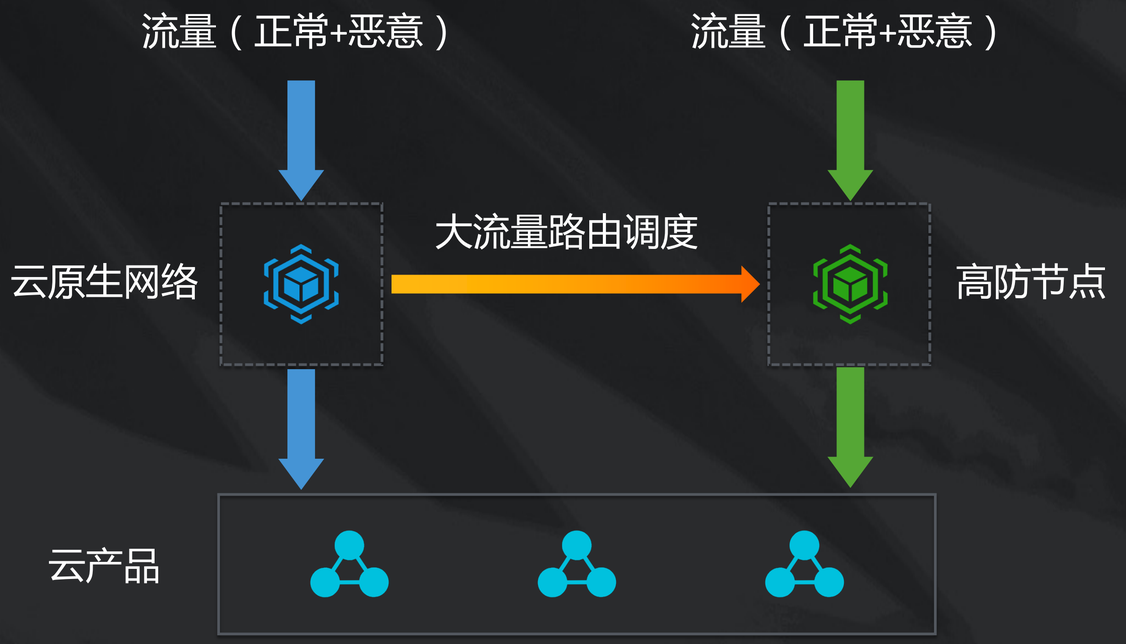
2.按需启用网络边界流量过滤



4、典型场景

典型场景：游戏行业防御DDoS攻击

场景需求
1.多IP、多端口，不要通过代理模式接入
2.游戏上量快，尽量轻量化部署，多区域统一方案
3.对延迟和稳定性要求高，不要改变网络架构



防护调度：

采用路由代播技术，网络入口调度高防节点，对客户透明

典型场景：无法修改DNS一键启用WAF

场景需求

1.不做DNS修改，接入WAF

业务流量走向：

业务流量走向不发生变化；

可提供全量请求日志与攻击防护日志；

安全防护：

流量进行分析bot流量与WEB攻击流量进行分析后，可进行观察、系统默认拦截，自定义拦截等；

提供AI智能防护，主动防御、全局流量限速、0Day默认防护等安全能；

阿里云

2021阿里云开发者大会
ALIBABA CLOUD DEVELOPER CONFERENCE

Thanks_

C{}DE FUTURE_