阿里云云计算ACP认证培训

阿里云安全

为了无法计算的价值 | 阿里云

课程目标

学习完本课程后，你将能够：

1. 了解云上安全形势及阿里云安全体系
2. 掌握阿里云主要安全产品的功能、特点及操作
3. 掌握阿里云监控与报警平台基本内容

目录

云计算面临的安全威胁

- 可用性
  - ✓安全威胁：大规模分布式拒绝服务攻击（DDoS）、僵尸网络（Botnet）
  - ✓影响：网站业务不可用
- 完整性
  - ✓安全威胁：网站入侵、服务器口令暴力破解
  - ✓影响：网站页面被篡改和植入后门
- 保密性
  - ✓安全威胁：网站后门、数据库非法访问（拖库）
  - ✓影响：用户帐户信息和敏感数据泄露

NO	安全威胁
T1	数据泄露
T2	身份、凭证和访问管理不足
T3	不安全的接口和应用程序编程接口（API）
T4	系统漏洞
T5	账户劫持
T6	恶意的内部人员
T7	高级持续性威胁（APT）
T8	数据丢失
T9	尽职调查不足
T10	滥用和恶意使用云服务
T11	拒绝服务（DoS）
T12	共享的技术漏洞

CSA发布12大云计算安全威胁

近几年的安全事件

事件一、1•21中国互联网DNS大劫难

几乎每一次上网都需要DNS

2014年1月21日下午3点10分左右，国内很多.Cn域名解析出现异常，超过85%的用户遭遇了DNS故障，引发网速变慢和打不开网站的情况，持续数小时。

事件二、某旅游公司漏洞事件

上旅游网，银行卡信息泄露了

2014年3月22日，某旅游公司被爆“安全支付日志可遍历下载导致大量用户银行卡信息泄露（包含持卡人姓名身份证、银行卡号、卡CVV码、6位卡Bin）”的漏洞。

事件三、某开源软件包心脏出血漏洞

网银、电商、金融、保险

2014年4月爆出了Heartbleed漏洞，该漏洞是近年来影响范围最广的高危漏洞，涉及各大网银、门户网站等。该漏洞可被用于窃取服务器敏感信息，实时抓取用户的账号密码。

开发者vs黑客：一场实力悬殊的战争

安全是动态的攻防对抗过程!

应用开发者

- 没有应用安全攻防经验
- 没有精力和时间投入到应用安全防护中
- 缺乏相应的防护工具

黑色产业

- 专业的应用攻防能力
- 100%的精力投入
- 完整的产业链结构与分工
- 各种先进的检测工具

目录

责任分担，共建安全（公有云）

阿里云云安全体系


云安全体系
云安全运营
云盾
云产品安全
数据库防火墙
数据库审计
3副本
快照
备份
清零
加密
数据安全
Web应用防火墙
Web弱点分析
安全开发生命周期（SDL）
应用安全
主机入侵防护
堡垒机
双因素认证
多租户隔离
自动宕机迁移
安全镜像
主机安全
DDoS防护
网络流量监控
防地址欺骗
VPC隔离
安全组防火墙
网络安全
操作系统加固
内核防提权
主机入侵防护
沙箱
漏洞热修复
多租户隔离
云操作系统安全
统一账号管理
双因素认证
集中权限管理
三权分立
堡垒机
日志审计
安全运维

阿里云安全产品体系

安全服务


安全众测


等保合规


应急响应


安全培训

阿里云.云盾

 态势感知	 SDL平台	 安全管家	**安全管理**
 业务风控	 内容安全	 实人认证	**业务安全**
 加密服务	 数据脱敏	 数据库审计	**数据安全**
 Web应用防火墙	 证书服务	 漏洞扫描	**应用安全**
 安骑士	 容器安全	 堡垒机	**主机安全**
 DDoS防护	 云防火墙	 SCDN	**网络安全**

阿里云.云产品


RDS.
SQL审计


KMS


RDS.透
明加密


安全组


VPC

云盾起源：十年攻防，一朝成盾

护航集团业务

阿里安全团队护航阿里巴巴集团内部
所有业务系统的信息安全

云盾 v 0.6

DDoS防护
主机安全防护
Web漏洞监测服务

云盾 v 1.6

云平台整体云防护

云盾 v 3.0

态势感知
安全大数据分析
感知现在，预测未来

云盾 v 1.0

云平台恶意攻击检测

云盾 v 2.0

云平台恶意软件查杀
云平台漏洞快速修复

全球首家获得云安全国际认证金牌（CSA STAR Certification）的云服务供应商

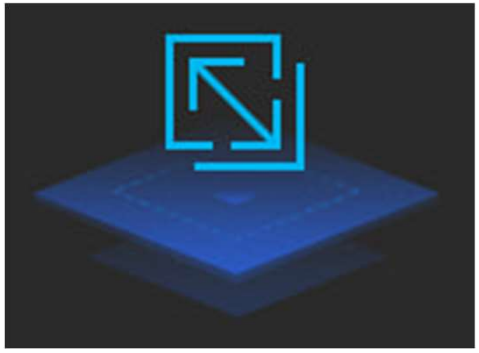
全国首个通过公安部等级保护测评（DJCP）的云计算系统

全国首家获得ISO27001信息安全管理体系 国际认证的云安全服务供应商

全国首批获得可信云权威机构认证，政企采购阿里云服务有据可依

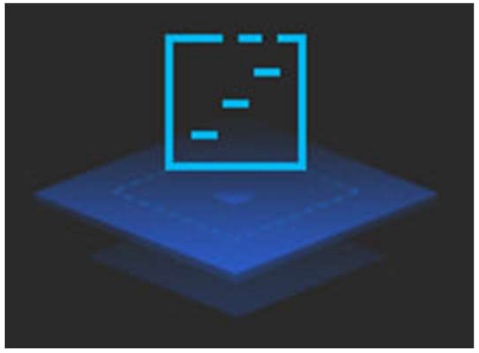
目录

云环境面临新的安全问题



边界和责任越来越模糊

资产业务的多元化

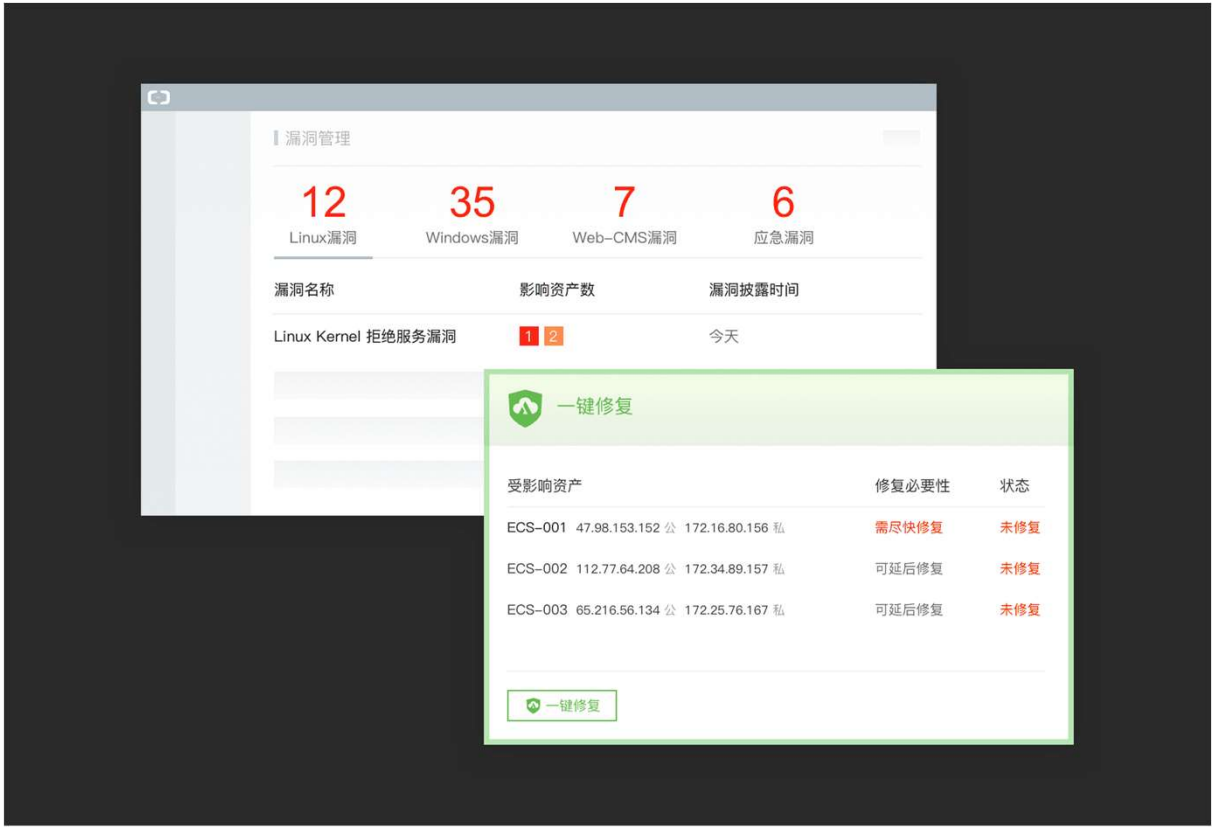


安全威胁的预谋化

- 云的边界/安全责任（共担模型）越来越模糊，用户的保护资产涉及云上云下资产，且资产类型将越来越多元化。
- 云环境安全威胁、传统环境安全威胁攻击方式和手段由原先的撒网式无差别扫描攻击转向有预谋的定向攻击，且随着资产的变化也在随之变化，例如IoT、移动安全 以上是挑战同时也是机遇，新的安全场景需要由新的方式来进行解决

云安全中心应用场景及功能：安全预防

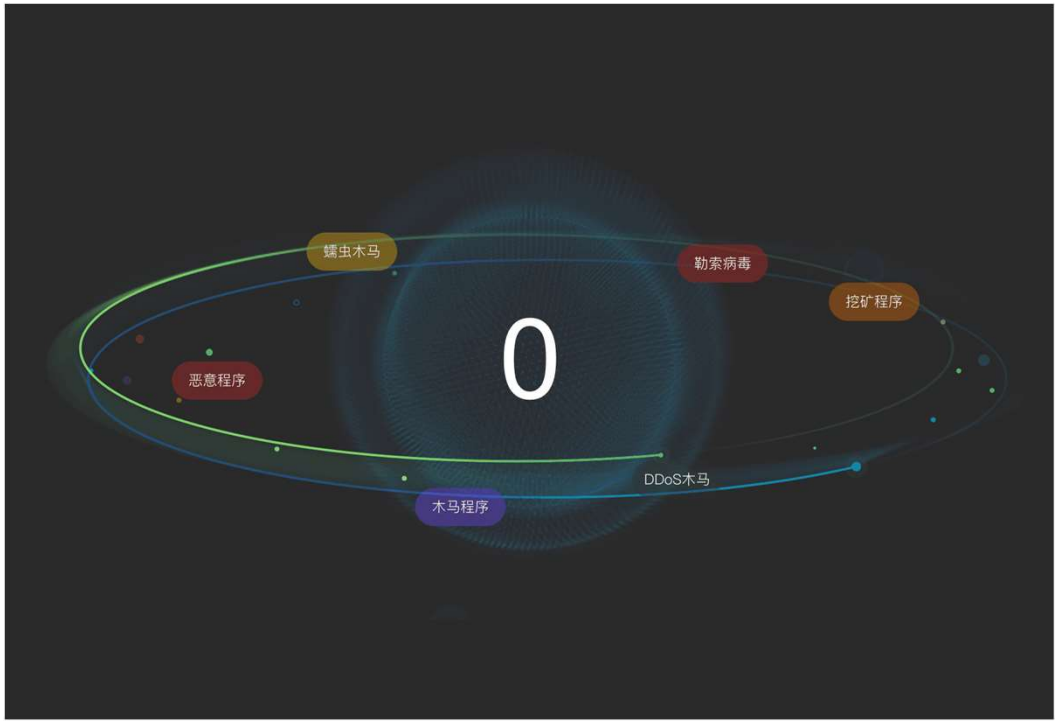
- **实现云产品联动，形成安全闭环**
  - **云平台最佳安全实践：**基于云平台最佳实践能力，联动云产品能力形成安全闭环
  - **漏洞管理与修复：**主流系统、软件漏洞识别，并支持漏洞一键修复
  - **基线检查：**基于阿里云最佳配置核查清单，降低配置不当引起的风险



云安全中心应用场景及功能：主动防御

- **基于系统内核分析技术实现防勒索、防病毒、防篡改**

- **防勒索、防病毒：**实时拦截已知勒索病毒、挖矿、蠕虫、DDoS等七类病毒
- **防篡改：**防止网站被植入涉恐涉政、暗链、后门等，保障网页正常
- **应用白名单：**防止未经授权的应用异常启动，影响业务正常运行



云安全中心应用场景及功能：威胁检测

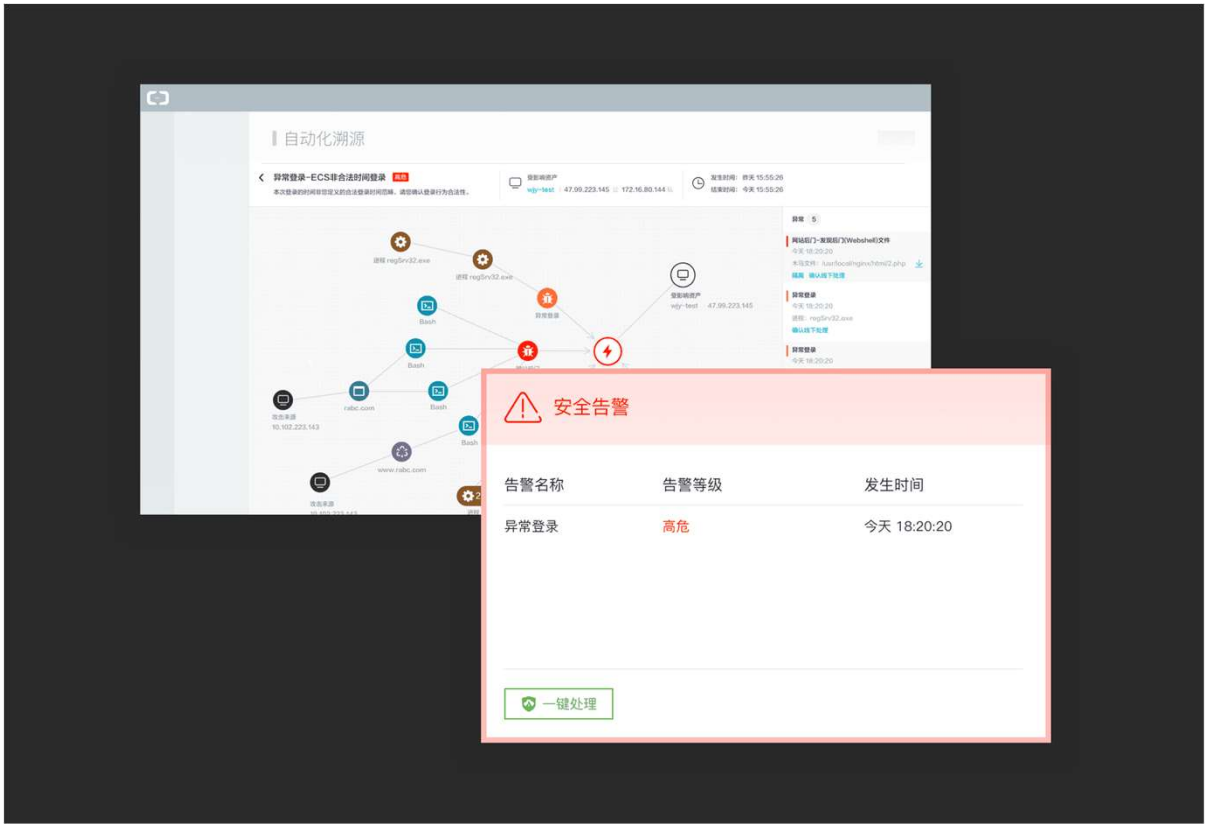
- **海量告警可自动关联分析，人工分析复杂告警成过去时，提升效率**

- **告警自动化分析关联**：自动关联告警、识别低危异常形成的入侵，提升运营效率
- **自定义告警**：第三方数据上云实时分析关联聚合，自定义告警规则
- **可视化态势**：安全大屏知己、知彼、知威胁多维度展现网络安全态势

云安全中心应用场景及功能：调查响应

- **基于攻击链自动化回溯攻击源头和原因，快速响应决策**

- **自动化攻击溯源**：自动溯源攻击源和原因，帮用户了解入侵威胁，快速响应
- **日志分析&审计**：提供日志审计、分析能力，提供攻击追溯、合规的平台

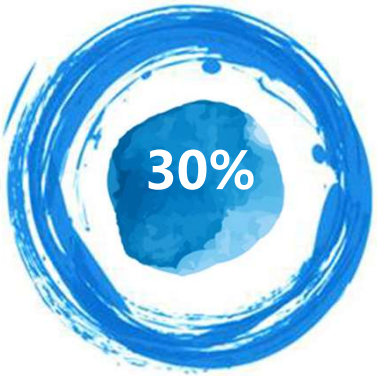


为什么要使用WAF?

Web应用防火墙(Web Application Firewall, 简称 WAF)：是一款网站必备的安全产品。
传统Web应用防火墙用户的痛点：

用不上
无法应用复杂业务
误报机率大

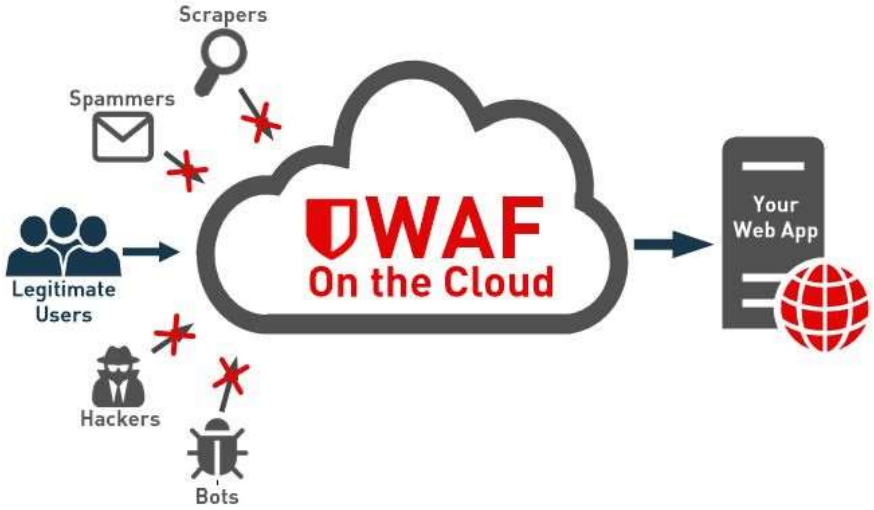
无专人后续运维
产品升级慢、流程复杂
不能及时防护最新漏洞



紧急问题响应慢
不能第一时间定位问题
原因、影响业务

什么是云盾WAF?

- **阿里云.云盾Web应用防火墙：**是阿里云提供的一款新型WAF产品，它基于云安全大数据能力实现运营+数据+攻防体系，综合打造网站应用安全。



网站/APP
应用防护

云盾WAF的应用场景

网站变卡、打不开

恶意海量肉鸡访问
网站资源被耗尽

账号数据、资金损失

官网充值、商品交易、恶意免费/低价成交、盗取用户账户数据

网站数据被恶意爬取
短信流量被滥刷

数据接口被刷，如：短信流量滥刷、用户数据信息被恶意爬取

获取服务器管理员权限
篡改网站数据、页面

利用最新0day漏洞、命令执行注入、获取服务器管理权限、获取数据、篡改页面等各种危害

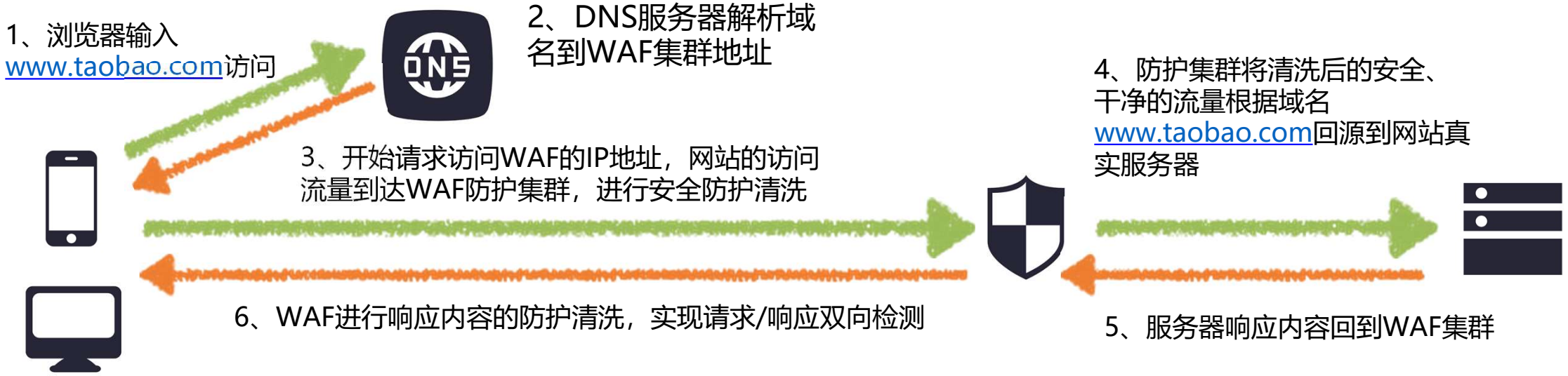
云盾WAF的产品功能

核心能力

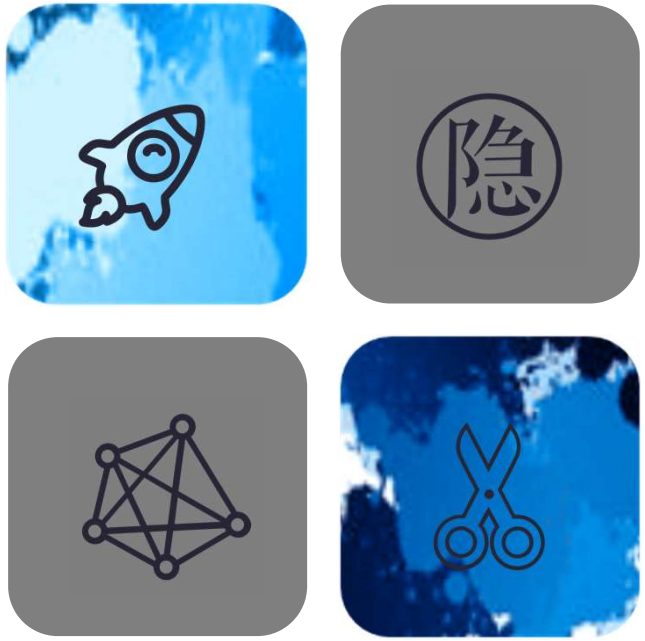
- 0DAY漏洞防护：
  推出最新曝出的Web 0day漏洞自动防御补丁规则、防护黑客的定向攻击
- Web应用防护：
  防御OWASP常见威胁、避免注入类攻击导致的数据泄露
- CC防护：
  针对恶意肉鸡发起的消耗网站资源海量请求进行拦截，并对IP进行封禁处罚
- 业务风控：
  - 防刷：针对用户注册及登录页面、避免网站的手机用户数据泄露、短信流量恶意消耗
  - 防爬：避免恶意爬虫抓取网站数据
  - 防撞库：缓解对登录页面的Web暴力破解

云盾WAF的工作原理

以用户访问 www.taobao.com 站点为例：



云盾WAF的产品特性



产品特性

一键接入：

无需部署软、硬件；无需修改配置；

DNS切换、五分钟实现网站安全

网站隐身：

隐藏源站地址、避免攻击者直接攻击服务器

协同防御：

共享国内近一半网站的防护策略、最新0day漏洞攻击第一时间防护

精准防护：

针对黑客发起的定向攻击、根据攻击特征(IP/URL/UA/Referer）一键过滤

云盾WAF的服务优势

应用防护规则只针对有攻击性行为阻拦，避免过度规则的滥用、降低业务误报

每日及时更新Web 0day漏洞防护规则避免服务器遭受黑客全网扫描、中招

特定接口防护规则专家级定制、让WAF真正被用起来

针对高端企业用户提供VIP服务迅速响应、及时处理网站问题

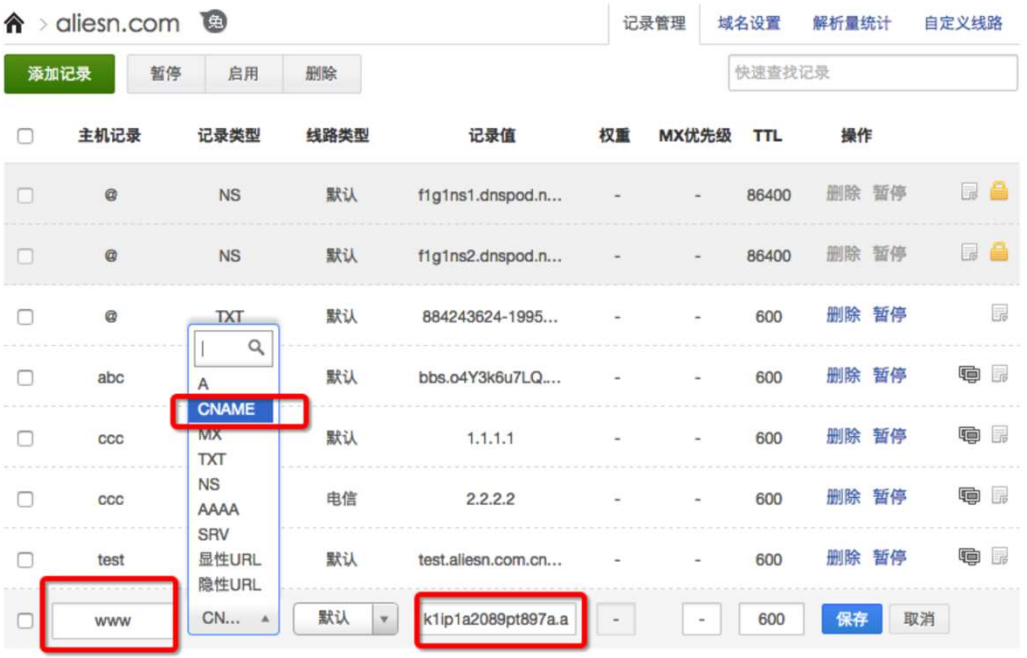
云盾WAF的配置方法

阿里云 aliyun.com

Step 1：添加域名及服务器公网IP

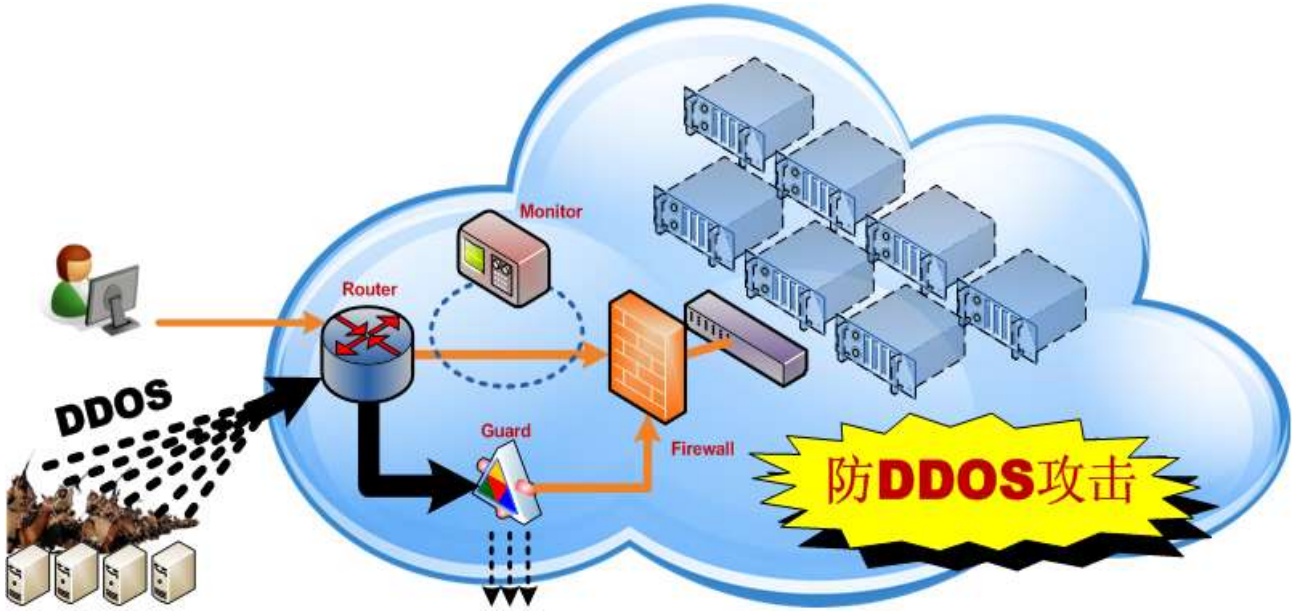
Step 2：获取域名对应的Cname地址

Step 3：针对域名添加对应的Cname记录，将流量牵引到WAF防护集群

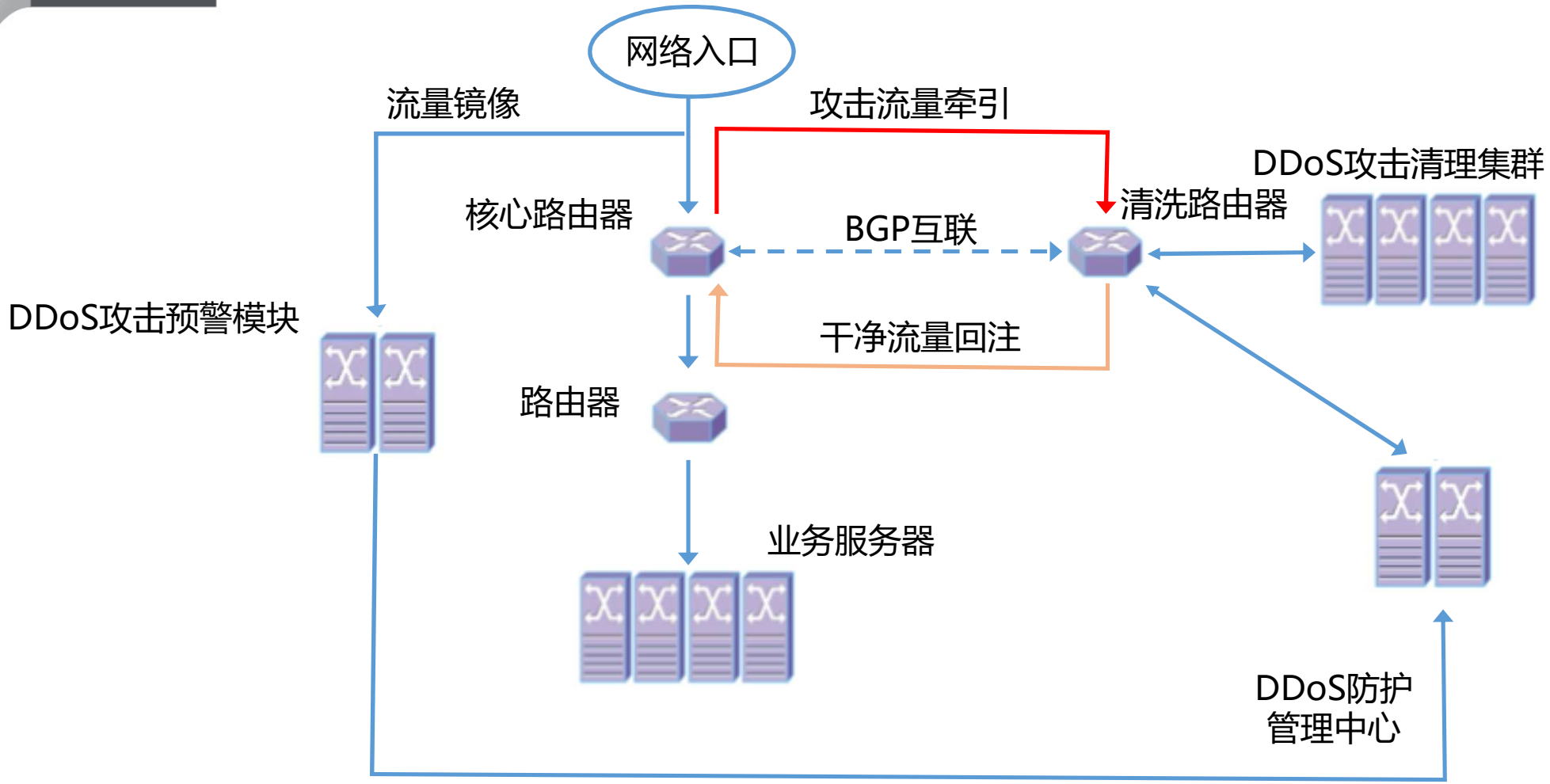


DDoS攻击是什么?

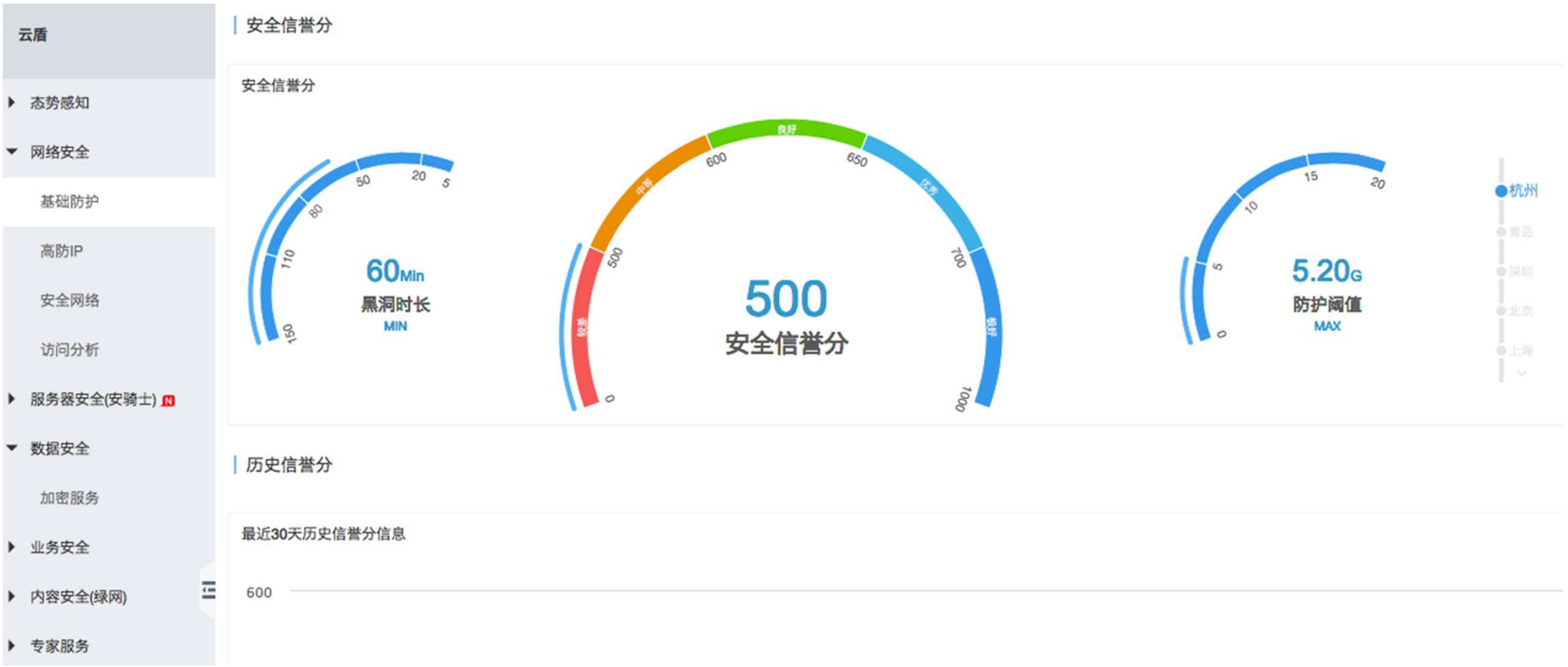
- DDoS（Distributed Denial of Service）即分布式拒绝服务攻击。
- 攻击主要目的是让指定目标无法提供正常服务，是最强大、最难防御的攻击之一。
- 近年出现的DRDoS（分布式反射攻击）让DDoS攻击水平迅速提升，互联网安全被网络暴力所威胁。



基础DDoS防护的实现流程



基础DDoS防护主页

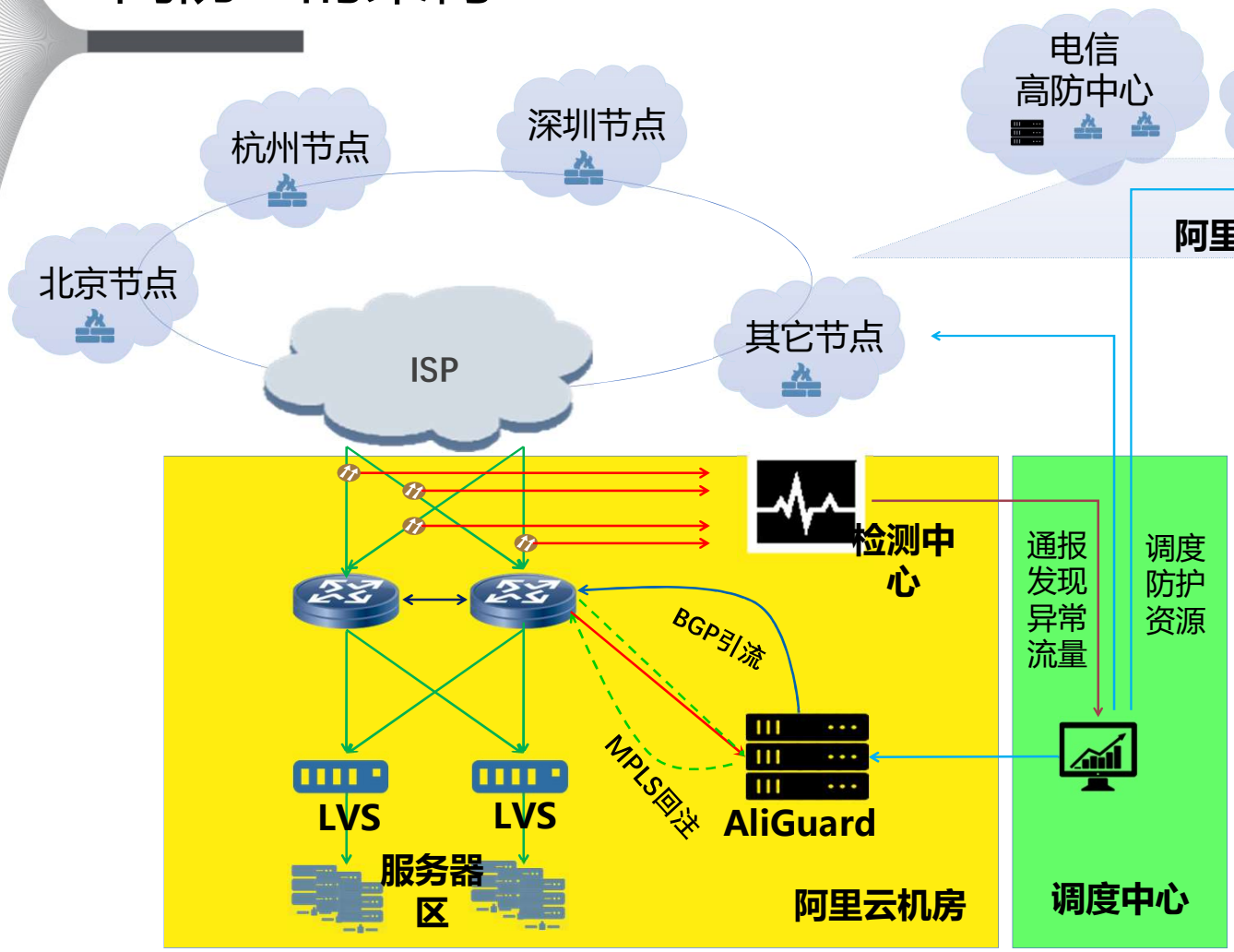

云盾
态势感知
网络安全
基础防护
高防IP
安全网络
访问分析
服务器安全(安骑士)
数据安全
加密服务
业务安全
内容安全(绿网)
专家服务
安全信誉分
安全信誉分
60Min
黑洞时长
MIN
500
安全信誉分
5.20G
防护阈值
MAX
杭州
历史信誉分
最近30天历史信誉分信息
600

为什么要使用DDoS高防?

为了获得更高DDoS防护能力，唯有补上“木桶”的“短板”

- **更强的服务能力**
- **突破设备性能**
- **突破机房带宽瓶颈**

高防IP的架构



- **小流量攻击**

  攻击小于5G，由云中心出口初级检测清洗设备完成清洗

- **大流量攻击**

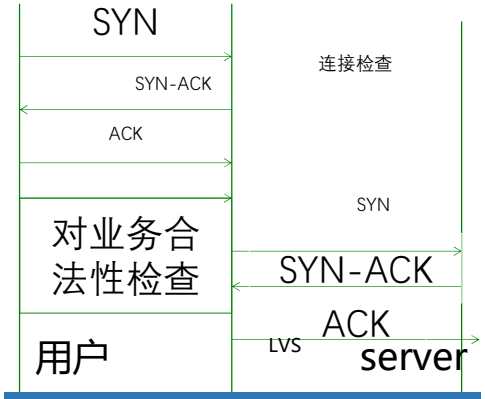
  攻击流量大于等于5G，

  - ✓ **黑洞**
  - ✓ **高防**，购买高防服务，由高防进行高等级清洗

- **强大云端高防**

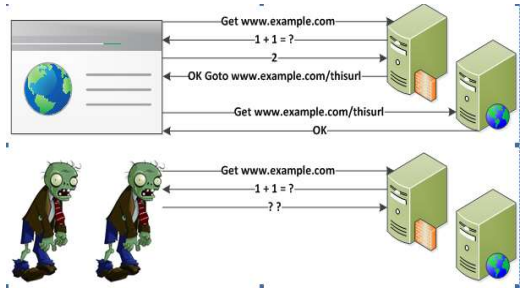
  建设电信、联通多个高防中心，释放用户防护带宽、防护性能压力

DDoS高防IP的功能



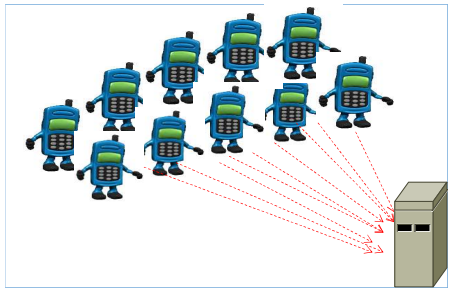
游戏空连接

- 防御空连接
- 防御慢连接
- 针对游戏的恶意连接
- 对报文合法性检查



防御CC攻击

- 1000万QPS
- IP+cookie的频率
- IP+key的认证
- 黑名单处罚
- 验证码、防爬



防御僵尸网络

- 全球僵尸网络库
- 与淘宝共享资源
- 神盾局攻击溯源

防御WEB攻击

- 防御SQL注入
- 防御XSS
- 防御跨站攻击

高防IP特点汇总

- **防护海量DDoS攻击**

  多个高防中心，电信、联通、BGP、海外线路，新节点持续建设

  有效抵御所有各类基于网络层、传输层及应用层的DDoS攻击

  超大DDoS防护经验丰富，平均每天防护2次200G以上攻击

- **专业团队运营**

  7x24专业团队随时应对

- **源站IP隐藏**

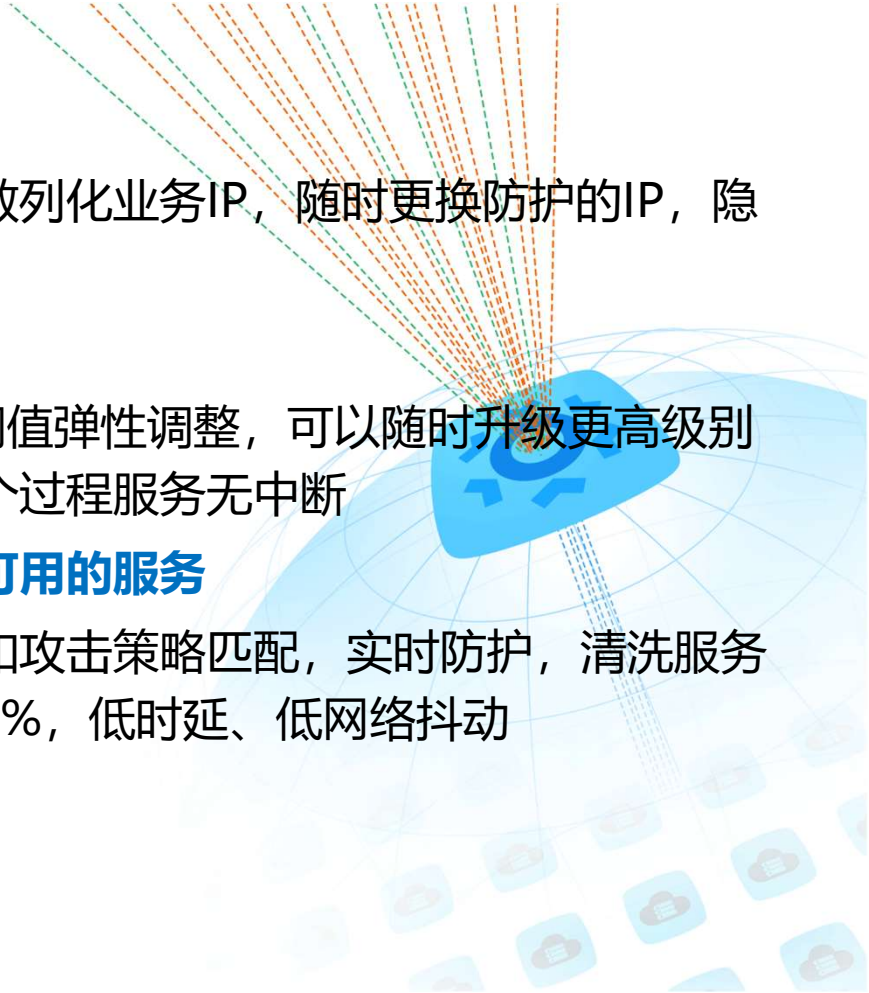
  高防服务可散列化业务IP，随时更换防护的IP，隐藏源站网络

- **弹性防护**

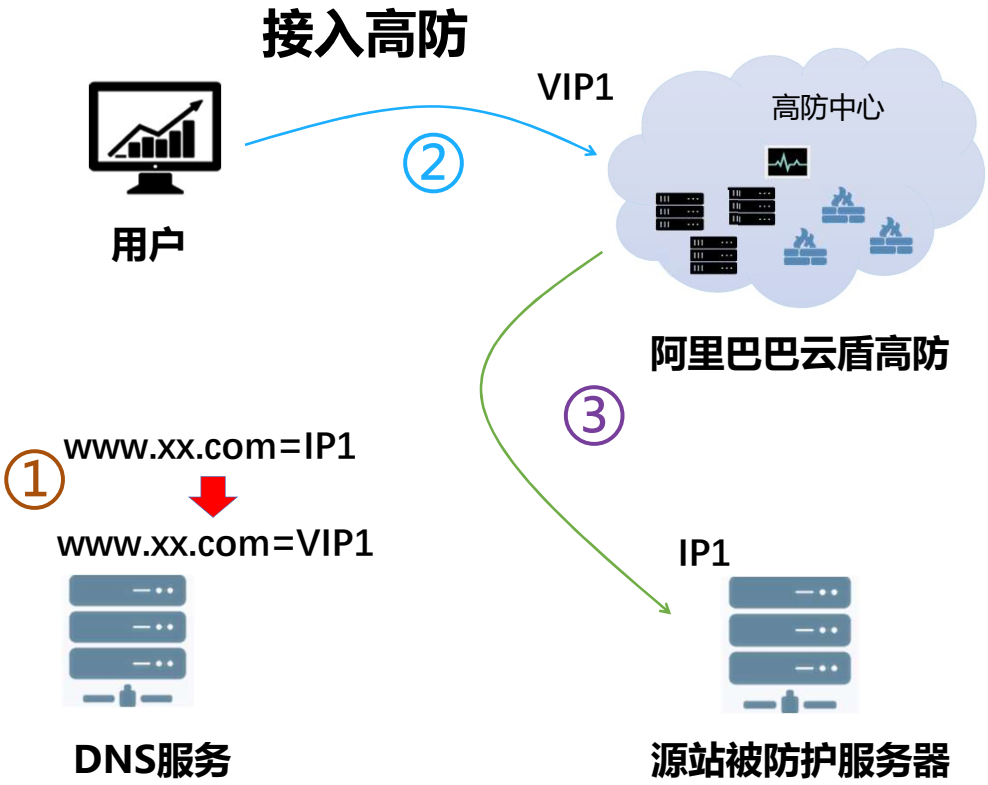
  DDoS防护阈值弹性调整，可以随时升级更高级别的防护，整个过程服务无中断

- **高可靠、高可用的服务**

  全自动检测和攻击策略匹配，实时防护，清洗服务可用性99.99%，低时延、低网络抖动



高防IP接入流程



高防接入步骤

①**DNS服务器更换对外服务IP。**根据高防提VIP1，在DNS服务器把原域名IP1更换为VIP1

②**流量完成切换。**客户端向源站的访问流量直接流向VIP1，安全防护由高防接管。

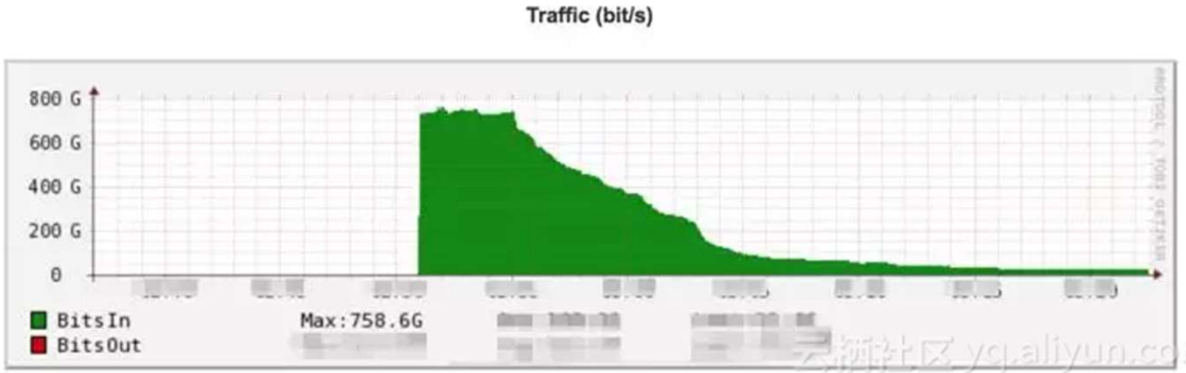
③**回源正常用户。**回注方式与传统方式不同,传统是要打上VPN标签进行回注隔离主机路由，我们采用协议栈更换技术，把处理完成的流量再送给源站IP1实现回注。

不仅为用户实现了攻击防护，同时，做为业务前置，把源站网络完全对外隐藏，降低安全风险

成功案例：成功防御国内最大规模DDoS攻击

2018年3月1日，阿里云已经成功监控和防御一起流量高达758.6Gbps的Memcached DDoS反射攻击

有别于NTP和SSDP反射攻击一般只能放大数十倍到数百倍，利用Memcached可以数万倍的放大报文；整个互联网可以用于Memcached反射的IP达到数十万，为攻击者提供了海量的军火库。



目录

传统监控的不足

- 每套监控系统的监控对象单一，多套监控系统难以统一管理。出现故障时，无法快速准确定位问题。

- 大都采用手动操作，当系统达到一定规模后，IT管理和运维成本也随之增长，对运维人员来说是噩梦。

- 监控数据和IT管理系统未打通，监控数据无法用于改善IT管理，价值无法体现。

云计算环境下监控的特点

云监控基本概念

云监控(CloudMonitor)是一项针对阿里云资源和互联网应用进行监控的服务。
云监控服务可用于收集获取阿里云资源的监控指标，探测互联网服务可用性，以及针对指标设置警报。

模块	功能
概览	云监控总览页，展示站点监控、云服务监控主要产品、自定义监控的监控信息和报警信息概览
站点监控	探测URL、IP的可用性，支持创建HTTP、ICMP、TCP、UDP、DNS、POP3、SMTP、FTP 8种探测点，获取探测对象的状态码和响应时间
云服务监控	为阿里云服务用户提供各个产品的性能指标查看和报警功能。当前支持11种产品的相关性能指标
自定义监控	用户可根据自身业务，定义监控指标，并通过脚本上报数据。满足用户业务层面的监控需求
报警联系人	用于管理报警规则的通知对象。报警规则与联系组关联，用户通过维护联系人信息和联系组信息，来管理对应的报警规则需要发送给哪些通知对象
事件订阅	事件订阅是除手机、邮箱、旺旺外的另一种报警通知接收方式。用户通过事件订阅功能，可通过MNS消息队列中间件来消费报警通知，对接自己的报警服务平台。主要满足大用户的混合云场景。

云监控的优势

- ✓ 无需特意开通，使用阿里云产品后直接到云监控查看产品运行状态并设置报警规则。
- ✓ 通过Dashboard提供丰富的图表，满足各种场景下的监控数据可视化需求。

- ✓ 设置报警规则和通知方式后，一旦发生异常便立刻报警，方便用户及时知晓并处理异常，提高用户产品的可用性。
- ✓ 云监控支持您通过 Dashboard 对监控数据进行时间维度和空间维度的聚合处理。

小结

1、用户使用阿里云搭建了网站，主机安全问题由谁负责?

2、云盾产品按照其防护层次划分，可以分为哪几类?

3、安骑士、DDoS高防、WAF的功能和应用场景分别是什么?

4、阿里云云监控的功能和优点有哪些?

为了无法计算的价值 | 阿里云