Web 应用防火墙

产品简介

产品简介

什么是Web应用防火墙

云盾Web应用防火墙（Web Application Firewall, 简称 WAF）基于云安全大数据能力，用于防御SQL注入、XSS跨站脚本、常见Web服务器插件漏洞、木马上传、非授权核心资源访问等OWASP常见攻击，并过滤海量恶意CC攻击，避免您的网站资产数据泄露，保障网站的安全与可用性。

您购买Web应用防火墙后，把域名解析到Web应用防火墙提供的CNAME地址上，并配置源站服务器IP，即可启用Web应用防火墙。启用之后，您网站所有的公网流量都会先经过Web应用防火墙，恶意攻击流量在Web应用防火墙上被检测过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。

功能特性

Web应用防火墙（WAF）帮助您轻松应对各类Web应用攻击，确保网站的Web安全与可用性。

- 核心攻防+大数据能力驱动Web安全
- 新时代的云WAF
- 一款淘宝天猫都在用的WAF

WAF支持以下功能：

业务配置

支持对网站的HTTP、HTTPS（高级版及以上）流量进行Web安全防护。

Web应用安全防护

常见Web应用攻击防护

- **防御OWASP常见威胁**，包括：SQL注入、XSS跨站、Webshell上传、后门隔离保护、命令注入、非法HTTP协议请求、常见Web服务器漏洞攻击、核心文件非授权访问、路径穿越、扫描防护等。
- **网站隐身**：不对攻击者暴露站点地址、避免其绕过Web应用防火墙直接攻击。

- **0day补丁定期及时更新**：防护规则与淘宝同步，及时更新最新漏洞补丁，第一时间全球同步下发最新补丁，对网站进行安全防护。
- **友好的观察模式**：针对网站新上线的业务开启观察模式，对于匹配中防护规则的疑似攻击只告警不阻断，方便统计业务误报状况。

CC恶意攻击防护

- 对单一源IP的访问频率进行控制，基于重定向跳转验证，人机识别等。
- 针对海量慢速请求攻击，根据统计响应码及URL请求分布、异常Referer及User-Agent特征识别，结合网站精准防护规则进行综合防护。
- 充分利用阿里云大数据安全优势，建立威胁情报与可信访问分析模型，快速识别恶意流量。

精准访问控制

- 提供友好的配置控制台界面，支持IP、URL、Referer、User-Agent等HTTP常见字段的条件组合，配置强大的精准访问控制策略；支持盗链防护、网站后台保护等防护场景。
- 与Web常见攻击防护、CC防护等安全模块结和，搭建多层综合保护机制；依据需求，轻松识别可信与恶意流量。

虚拟补丁

在Web应用漏洞补丁发布和修复之前，通过调整Web防护策略实现快速防护。

攻击事件管理

支持对攻击事件、攻击流量、攻击规模的集中管理统计。

可靠性

- **支持负载均衡**：以集群方式提供服务，多台机器负载均衡，支持多种负载均衡策略。
- **支持平滑扩容**：可根据实际流量情况，缩减或增加集群机器的数量，进行服务能力弹性扩容。
- **无单点问题**：单台机器宕机或者下线维修，均不影响正常服务。

更多产品信息，请查看Web应用防火墙产品页面。

产品优势

五分钟体验网站安全

- 无需安装任何软、硬件。
- 无需更改网站配置、代码。

- 只需修改DNS记录，五分钟实现网站Web安全。

强大Web防御能力

- 内置近千条安全防护规则，每周均有规则的新增和优化。
- Web 0Day漏洞补丁修复，24小时内防护，全球同步。
- 专业攻防团队进行漏洞研究，捕获0Dday漏洞并生成防护规则。
- 通过大数据平台分析规则优化，整体误报率控制在十万分之一以内。

网站专属防护

- 支持业务精准防护、快速过滤恶意流量、如保护管理后台、恶意IP封禁、特定URL加白等功能。

大数据安全能力

- 每日对数十亿条数据进行安全分析，提取规则同步到所有用户，进行协同防御。
- 不断通过大数据分析丰富恶意IP库、恶意样本库，建立网站的可信源。

检测快、防护稳

- 一毫秒内检测攻击并防护生效，防护无延时。
- 新的防护规则一分钟内全球同步。
- 覆盖OWASP常见的10余种威胁攻击。
- 全年稳定在线可用。

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。
- 清洗服务可用性高达99.99%。

应用场景

阿里云云盾Web应用防火墙适用于阿里云以及阿里云外所有用户。

Web应用防火墙服务主要适用于金融、电商、o2o、互联网+、游戏、政府、保险等行业各类网站的Web应用安全防护。

Web应用防火墙可以帮助您解决以下问题：

防数据泄密，避免因黑客的注入入侵攻击，导致网站核心数据被拖库泄露。

防恶意CC，通过阻断海量的恶意请求，保障网站可用性。

阻止木马上传网页篡改，保障网站的公信力。

提供虚拟补丁，针对网站被曝光的最新漏洞，最大可能地提供快速修复的规则。

更新公告

版本号	发布日期	发布说明
V3.6	2017-04-12	新增以下功能： - WAF所有版本均支持8080、8443端口的HTTP/HTTPS业务安全防护。企业版及旗舰版支持更多自定义非标端口。具体支持的端口可在控制台查看，或者参考非标端口支持。 - 一键将网站HTTPS，无需修改服务器配置，即支持将HTTP流量强制转换为HTTPS访问。 - HTTPS流量支持HTTP回到源站。
V3.5	2017-03-08	新增以下功能： 允许针对阿里云万网接入DNS的网站（当客户进行授权后）一键智能解析到Web应用防火墙节点，无需您手工进行DNS配置，让接入更简单方便。
V3.4	2017-02-09	新增以下功能： 在得到用户授权后，Web应用防火墙会保存用户该域名下的全量访问日志并提供一键智能搜索功能，快速定位运维问题和安全

		拦截事件。
V3.3	2017-02-04	新增以下功能： Web应用防火墙已打通阿里云账号限制，允许回源IP填写不同的阿里云账号下ECS或者SLB公网地址。
V3.2	2017-02-09	新增以下功能： Web应用防火墙具备网页防篡改能力，避免网站遭到恶意攻击后对外显示篡改后的非法页面。在网站遭受到恶意篡改后，Web应用防火墙能够利用缓存检测技术，使对外提供服务的页面显示为篡改前的正常页面。
V3.1	2016-12-21	新增以下功能： - 支持基于省份地理位置的IP区域封禁功能，并且支持封禁海外IP访问。 - 支持在控制台自主配置CC自定义规则，针对单IP的访问频率做限制。 - 支持包括参数等更多HTTP字段的访问控制。新增了长度、严格匹配等多种逻辑符。 - 提供版本支持的参数规格，包括支持的带宽、QPS限制等。 包含以下产品改进： 风险预警：总结出最主要的攻击如变种CC、短信恶意注册、撞库、爬虫扫描等主要安全事件。
V3.0	2016-10-12	新增以下功能： - 支持Web攻击中的Post内容展示，帮助用户快速分析定位攻击原因。 - 访问控制事件能够清晰展示匹配次数及匹配中的规则内容。 - 所有攻击类型（Web攻击、CC攻击、访问控制）均支持

		历史攻击概况的详情统计，统计数据包括攻击总次数及攻击源IP个数，时间维度为“天、周、月”，并支持自定义时间的查询。 包含以下产品改进： - 将产品分为“安全总览”、“业务分析”、“域名配置”三部分。第一优先展示“安全总览”，帮助用户快速准确的熟悉网站当前安全状况。 - 新版本依靠大数据平台，提供了更为丰富的攻击数据及访问数据统计能力。 - Web攻击详情的查询时间，由之前的“最近3天”延长到“最近30天”。 - Web攻击详情支持按IP查询最后一次攻击时间以及攻击总次数的排序。 - CC攻击由之前的攻击事件展示变为攻击次数的展示，对CC攻击事件有了明确定义（攻击时间持续超过三分钟，每秒攻击请求数大于100）。 - 业务分析中的访问数据准实时动态更新，时间维度支持“天、周、月”。各类Top数据能方便您快速熟悉业务访问状况并做出对应措施。 - 在网站域名的管理配

		置中，提供了友好的引导提示帮助，帮助用户更顺利的将网站接入防护。 - 突出产品工具栏中的帮助指导及安全通告，帮助用户快速的了解安全动态，在对产品的使用上更加游刃有余。
V2.5	2016-09-09	新增以下功能： WAF高级版及更高版本目前已支持业务风控防护能力，在无需改造业务代码的情况下，通过滑块验证等一系列手段解决“短信轰炸”、“刷库撞库”、“恶意注册”、“营销作弊”等常见的业务风险问题。
V2.0	2016-06-23	新增以下功能： - 支持对网站发起频繁Web攻击的IP自动封禁。 - Web安全日志支持一个月的安全事件概览统计。 - 针对域名粒度，提供高、中、低三种级别的Web防护策略，适应不同的业务场景。 包含以下产品改进： - 支持高防+WAF或CDN+WAF的网站架构，支持通过CDN、高防后，针对真实访问源IP的防护以及安全日志展示。（已添加的域名可以点击“编辑”修改默认配置）。 - 界面优化、安全日志的查询速度优化，支持泛域名攻击查询。

V1.0	20116-04-11	新增以下功能： - 为网站提供常见的Web攻击防护能力、CC防护以及精准访问控制功能。 - 是否支持HTTPS，支持防护的域名个数，回源IP个数，访问控制功能，业务分析能力等参数规格受套餐规格约束。 - 用户可以通过控制台查看不同时间范围内的日志报表。