什么是Web应用防火墙

更新时间：2020-11-03 13:57:00

[**本页目录**](javascript:void(0))

* [主要功能](https://help.aliyun.com/document_detail/28517.html?spm=a2c4g.11174283.6.555.61ce644dXxQk9l#title-pcs-cra-i3p)
* [如何使用WAF](https://help.aliyun.com/document_detail/28517.html?spm=a2c4g.11174283.6.555.61ce644dXxQk9l#title-qun-6yz-gme)
* [计费概述](https://help.aliyun.com/document_detail/28517.html?spm=a2c4g.11174283.6.555.61ce644dXxQk9l#title-kj8-nxw-5w9)

Web应用防火墙（Web Application Firewall，简称 WAF）为您的网站或App业务提供一站式安全防护。WAF可以有效识别Web业务流量的恶意特征，在对流量进行清洗和过滤后，将正常、安全的流量返回给服务器，避免网站服务器被恶意入侵导致服务器性能异常等问题，保障网站的业务安全和数据安全。

**主要功能**

* 提供Web应用攻击防护。
* 缓解恶意CC攻击，过滤恶意的Bot流量，保障服务器性能正常。
* 提供业务风控方案，解决业务接口被恶意滥刷等业务安全风险。
* 提供网站一键HTTPS和HTTP回源，降低源站负载压力。
* 支持对HTTP和HTTPS流量进行精准的访问控制。
* 支持超长时长的全量日志实时存储、分析和自定义报表服务，支持日志线上同步第三方平台，助力满足等保合规要求。

**如何使用WAF**

您购买WAF后，可以通过CNAME接入或透明接入的方式，把网站域名接入到WAF集群进行防护。

* CNAME接入

把域名解析到WAF提供的CNAME地址上，并配置源站服务器IP，即可启用WAF。启用WAF后，您网站所有的公网流量都会先经过WAF，恶意攻击流量在WAF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。

详细内容，请参见[网站接入](https://help.aliyun.com/document_detail/97063.html#task-1796689)。

* 透明接入

如果您的源站服务器部署在阿里云公网SLB上，那么除了使用CNAME接入，您还可以选择云原生的透明接入方式，实现WAF对网站的防护。在这种模式下，您无需修改域名DNS解析、设置源站保护，同时无需改变服务器获取真实源IP的方式，保护您SLB上的Web业务正常运转。

详细内容，请参见[SLB透明接入](https://help.aliyun.com/document_detail/171452.html" \l "task-2538763" \o "Web应用防火墙（WAF）提供CNAME接入和透明接入两种方式，使您的网站流量可以受到WAF的保护。如果您的源站服务器部署在阿里云公网SLB上，那么除了使用CNAME接入，您还可以选择云原生的透明接入方式。在这种模式下，无需修改域名DNS解析、设置源站保护，同时无需改变服务器获取真实源IP的方式，保护您SLB上的Web业务正常运转。)。

## Web应用安全防护

**常见Web应用攻击防护**

* 防御OWASP常见威胁：支持防御以下常见威胁：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。

**深度精确防护**

* 支持全解析多种常见HTTP协议数据提交格式：任意头部字段、Form表单、Multipart、JSON、XML。
* 支持解码常见编码类型：URL编码、Java Script Unicode编码、HEX编码、HTML实体编码、Java序列化编码、PHP序列化编码、base64编码、UTF-7编码、混合嵌套编码。
* 支持预处理机制：空格压缩、注释删减、特殊字符处理，向上层多种检测引擎提供更为精细、准确的数据源。
* 在准确性上，优化引擎解析HTTP协议的能力，支持复杂格式数据环境下的检测能力；抽象复杂格式数据中用户可控部分，降低上层检测逻辑的复杂度，避免过多检测数据导致的误报，降低多倍的误报率；在全面性上，支持多种形式数据编码的自适应解码，避免利用各种编码形式的绕过。

**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防护等安全模块结合，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，请参见[Web应用防火墙产品页面](http://www.aliyun.com/product/waf/)。