ALIBABA CLOUD

阿里云

Web应用防火墙

产品简介

文档版本：20201106

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是Web应用防火墙

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。

- 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。

计费概述

WAF支持包年包月（预付费）、按量计费（后付费）的计费方式。包年包月计费方式支持按一个月、三个月、半年和一年购买。详细内容，请参见计费方式。

2.功能特性

Web应用防火墙（Web Application Firewall，简称WAF）使用核心攻防和大数据能力来驱动Web安全，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。本文介绍了WAF的功能特性。

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：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。

3.套餐规格与功能说明

Web应用防火墙包年包月服务默认提供高级版、企业版、旗舰版等套餐（独享版需要提交工单申请后才支持开通）。通过包年包月方式开通WAF时，您可以根据要防护的业务规模和安全防护需求选择合适的套餐。本文介绍了不同WAF套餐适用的业务规模和支持的防护功能。

适用的业务规模

下表描述了不同WAF套餐适用的业务规模。一般情况下，对于中型规模的企业网站，推荐您选择企业版或者旗舰版。

> **说明** 独享版需要工单申请后才支持开通。

业务规格	高级版	企业版	旗舰版	独享版（仅支持工单开通）
站点规模	中小型网站，对业务没有特殊的安全需求	中型企业级网站或服务对互联网公众开放，关注数据安全且具有高标准的安全需求	中大型企业网站，具备较大的业务规模，或是具有特殊定制的安全需求	大型企业网站，具备较大的业务规模且基于业务特性具有定制化的配置需求
业务并发请求峰值	2,000 QPS	5,000 QPS	超过10,000 QPS	5,000 QPS
业务带宽阈值（源站服务器部署在阿里云）	50 Mbps	100 Mbps	200 Mbps	100 Mbps
业务带宽阈值（源站服务器未部署在阿里云）	10 Mbps	30 Mbps	50 Mbps	30 Mbps
默认可防护的一级域名个数	1个	1个	1个	1,000个
默认可防护的总域名个数（支持泛域名）	10个	10个	10个	1,000个

关于如何开通Web应用防火墙服务，请参见开通Web应用防火墙。

套餐功能列表（中国内地）

下表描述了Web应用防火墙中国内地实例（购买包年包月实例时选择**中国内地**地域）及按量计费实例的主要功能模块在不同套餐中的支持情况。更详细的套餐功能说明，请参见Web应用防火墙产品定价页面。

标识说明：

- √：表示在当前套餐中支持。
- ×：表示在当前套餐中不支持。
- ○：表示需要额外付费开启的增值服务。您可以在购买WAF实例时开启增值服务，或者在购买WAF实例后使用升级功能开启增值服务。
- △：表示需要在开通按量计费WAF后，通过**功能与规格设置**单独开启的特性。

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）	按量计费
业务接入						
HTTPS安全防护	全站一键实现HTTPS防护。	√	√	√	√	△
非标准端口防护	支持防护80、8080、443、8443以外的特定非标准端口上的业务。	×	√	√	√	△
IPv6防护	支持IPv6访问流量的安全检测与防护。	×	√	√	√	×
智能负载均衡	通过多节点智能接入技术，实现源站服务器多节点、多线路自动调度容灾。	○	○	○	○	×
域名独享资源包	支持为域名开启独享IP防护。	○	○	○	○	△
独享集群	基于业务特性的定制化接入和防护能力。	×	×	×	√	×
资产识别	主动发现和管理站点资产，支持一键接入防护。	√	√	√	√	√
透明接入	直接牵引源站ECS的流量到Web应用防火墙进行防护。	×	√	√	√	×
网站防护						
正则防护引擎	防御常见的Web攻击，例如SQL注入、XSS等。	√	√	√	√	√
	自动更新Web 0day漏洞攻击防护规则。	√	√	√	√	√
防护规则组	支持自定义防护规则组。	×	√	√	√	×
大数据深度学习引擎	依托于大数据深度学习引擎的0day漏洞风险检测。	×	√	√	√	×
主动防御	基于网站访问流量的深度学习，提供主动防御能力。	×	×	√	√	×
网站防篡改	锁定网站页面，防止内容被恶意篡改。	√	√	√	√	△
防敏感信息泄露	防敏感隐私数据泄露，包括电话号码、身份证、银行卡等重要隐私数据。	√	√	√	√	△

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）	按量计费
CC安全防护	防御常见的CC攻击，支持内置的防护和防护-紧急模式。	√	√	√	√	√
IP黑名单	一键封禁特定的IP地址和地址段的访问能力。	√	√	√	√	△
	包含上述特性，且支持一键封禁指定地理区域IP的访问能力。	×	√	√	√	△
扫描防护	支持高频Web攻击封禁（默认规则）、目录遍历封禁（默认规则）、扫描工具封禁、协同防御。	√	√	√	√	△
	包含上述特性，且支持自定义高频Web攻击封禁、目录遍历封禁规则。	×	√	√	√	△
自定义防护策略	基于基础字段（包含IP、URL、Referer、User-Agent、Params）的ACL访问控制。	√	√	√	√	√
	包含基础字段，且支持高级字段（例如Cookie、Content-Type、Header、Http-Method等）。	×	√	√	√	√
	自定义CC防护规则，设置基于IP和Session进行请求次数统计的频率控制策略。	×	√	√	√	√
	包含IP和Session，且支持基于自定义字段进行请求次数统计。	×	×	√	√	√
数据风控	防御网站关键业务（例如注册、登录、活动、论坛）中可能发生的机器爬虫欺诈行为。	○	○	○	○	△
Bot管理	提供针对自动化攻击或Bot流量的智能防护方案，缓解机器流量对业务造成的安全威胁。支持人机识别，防黄牛、防恶意注册场景。	○	○	○	○	×
App防护	专门针对原生APP端，提供可信通信，防机器脚本滥刷等安全防护，可以有效识别代理、模拟器、非法签名的请求。	○	○	○	○	×

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）	按量计费
账户安全	支持识别与账户关联的业务接口（例如注册、登录等）上的撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷事件。	√	√	√	√	×
API安全	支持上传自定义的API规则文件，确保只有符合规则的API请求才会被执行。	×	√	√	√	×
安全分析和支持						
日志服务	支持采集WAF所有的日志信息并存储至日志服务中，提供准实时查询分析和在线报表展示等功能。	○	○	○	○	△
可视化大屏服务	提供网站整体业务及安全状况的可视化大屏分析。	○	○	○	○	×
产品专家服务	由阿里云安全专家提供钉钉群咨询服务，负责产品配置、策略优化、日常监控等技术支持。	○	○	○	○	×

套餐功能列表（海外地区）

下表描述了Web应用防火墙海外地区实例（购买包年包月实例时选择**海外地区**地域）的主要功能模块在不同套餐中的支持情况。更详细的套餐功能说明，请参见Web应用防火墙产品定价页面。

标识说明：

- √：表示在当前套餐中支持。
- ×：表示在当前套餐中不支持。
- ○：表示需要额外付费开启的增值服务。您可以在购买WAF实例时开启增值服务，或者在购买WAF实例后使用升级功能开启增值服务。
- △：表示需要在开通按量计费WAF后，通过**功能与规格设置**单独开启的特性。

> **说明** 海外地区WAF实例不支持按量计费。

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）
业务接入					
HTTPS安全防护	全站一键实现HTTPS防护。	√	√	√	√

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）
非标准端口防护	支持防护80、8080、443、8443以外的特定非标准端口上的业务。	×	√	√	√
IPv6防护	支持IPv6访问流量的安全检测与防护。	×	×	×	×
智能负载均衡	通过多节点智能接入技术，实现源站服务器多节点、多线路自动调度容灾。	×	○	○	○
域名独享资源包	支持为域名开启独享IP防护。	○	○	○	○
独享集群	基于业务特性的定制化接入和防护能力。	×	×	×	√
资产识别	主动发现和管理站点资产，支持一键接入防护。	×	×	×	×
透明接入	直接牵引源站ECS的流量到Web应用防火墙进行防护。	×	×	×	×
网站防护					
正则防护引擎	防御常见的Web攻击，例如SQL注入、XSS等。	√	√	√	√
	自动更新Web 0day漏洞攻击防护规则。	√	√	√	√
防护规则组	支持自定义防护规则组。	×	×	√	√
大数据深度学习引擎	依托于大数据深度学习引擎的0day漏洞风险检测。	×	×	×	×
主动防御	基于网站访问流量的深度学习，提供主动防御能力。	×	×	×	×
网站防篡改	锁定网站页面，防止内容被恶意篡改。	×	×	√	√
防敏感信息泄露	防敏感隐私数据泄露，包括电话号码、身份证、银行卡等重要隐私数据。	×	√	√	√
CC安全防护	防御常见的CC攻击，支持内置的防护和防护-紧急模式。	√	√	√	√
IP黑名单	一键封禁特定的IP地址和地址段的访问能力。	√	√	√	√
	包含上述特性，且支持一键封禁指定地理区域IP的访问能力。	×	√	√	√

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）
扫描防护	支持高频Web攻击封禁（默认规则）、目录遍历封禁（默认规则）、扫描工具封禁、协同防御。	√	√	√	√
	包含上述特性，且支持自定义高频Web攻击封禁、目录遍历封禁规则。	×	√	√	√
自定义防护策略	基于基础字段（包含IP、URL、Referer、User-Agent、Params）的ACL访问控制。	√	√	√	√
	包含基础字段，且支持高级字段（例如Cookie、Content-Type、Header、Http-Method等）。	×	√	√	√
	自定义CC防护规则，设置基于IP和Session进行请求次数统计的频率控制策略。	×	√	√	√
	包含IP和Session，且支持基于自定义字段进行请求次数统计。	×	×	√	√
数据风控	防御网站关键业务（例如注册、登录、活动、论坛）中可能发生的机器爬虫欺诈行为。	×	×	×	×
Bot管理	提供针对自动化攻击或Bot流量的智能防护方案，缓解机器流量对业务造成的安全威胁。支持人机识别，防黄牛、防恶意注册场景。	○	○	○	○
App防护	专门针对原生APP端，提供可信通信，防机器脚本滥刷等安全防护，可以有效识别代理、模拟器、非法签名的请求。	○	○	○	○
账户安全	支持识别与账户关联的业务接口（例如注册、登录等）上的撞库、暴力破解、垃圾注册、弱口令嗅探和短信验证码接口滥刷事件。	√	√	√	√
API安全	支持上传自定义的API规则文件，确保只有符合规则的API请求才会被执行。	×	×	√	√
安全分析和支持					
日志服务	支持采集WAF所有的日志信息并存储至日志服务中，提供准实时查询分析和在线报表展示等功能。	○	○	○	○

功能模块	描述	高级版	企业版	旗舰版	独享版（仅支持工单开通）
可视化大屏服务	提供网站整体业务及安全状况的可视化大屏分析。	×	○	○	○
产品专家服务	由阿里云安全专家提供钉钉群咨询服务，负责产品配置、策略优化、日常监控等技术支持。	○	○	○	○

4.产品优势

云盾Web应用防火墙具有部署简易、防护及时精确、大数据驱动、高可靠等优势。

10年以上网络安全经验

- 建立在阿里巴巴集团10年以上的网络安全经验上，提供与淘宝、天猫、支付宝等成功应用案例同样的安全体验。
- 由来自全球的安全专家组建的专业安全团队向您提供服务。
- 完全抵御已知的OWASP漏洞并不断提供针对最新披露漏洞的更新。

防御CC攻击和爬虫攻击

- 帮助您抵御和减缓CC攻击。
- 帮助您防御网络爬虫，避免网络资源消耗。
- 检测和阻挡恶意请求，帮助您减少带宽消耗、防止数据库/SMS/API资源亏空、减少响应延时、避免宕机等。
- 针对多样业务场景支持自定义防护规则。

集成大数据能力

- 阿里云托管着37%左右的中国境内网站。
- 阿里云每天约抵御8亿次网络攻击。
- 阿里云拥有中国最受欢迎的IP数据库。
- 阿里云拥有广泛的应用案列，对各类常见网络攻击的模式、方法和签名有大量研究。
- 阿里云大数据分析不断整合最先进的技术。

简易性可靠性

- 5分钟内部署和激活。
- 无需安装任何软硬件或调整路由配置。
- 通过防护集群作用，避免单点故障和冗余。
- 可圈可点的处理性能。

5.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。

> **说明** 云盾Web应用防火墙仅支持通过域名方式进行防护，不支持使用IP直接接入。

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规则。

6.常见术语

本文主要介绍了Web应用防火墙的常见术语。

回源IP

回源IP指Web应用防火墙用来与源站服务器建立网络连接的IP地址。

Web应用防火墙使用特定的回源IP段将经过防护引擎检测后的正常流量转发到网站域名的源站服务器。在将网站业务接入Web应用防火墙进行防护后，建议您在源站服务器上设置放行Web应用防火墙的回源IP，防止Web应用防火墙转发回源站的正常流量被误拦截。更多信息，请参见放行WAF回源IP段。

源站

源站指提供服务的后端服务器。

Web应用

Web应用指用户通过Web浏览器即可访问的应用程序。

四层代理

四层代理指代理服务器只分析请求报文中的目的地址和端口信息，结合服务器选择规则，直接将访问请求转发到源站服务器。

七层代理

七层代理指代理服务器在分析请求报文中的应用层内容后，根据报文中的特定字段以及服务器选择规则，将访问请求转发到源站服务器。