# 目录

# 产品概述

Web应用防火墙（Web Application Firewall，简称 WAF）可以帮助用户解决Web攻击防护、业务访问风险、漏洞利用、后门入侵等安全问题。通过修改DNS解析，将Web业务流量牵引到云端WAF防护集群，流量经过层层清洗后，将正常、安全的流量回注到源站。接入WAF即可分钟级获取Web应用攻击防护能力，避免网站服务器被恶意入侵，为客户网站及Web业务安全运营保驾护航。

本文档能够帮助您了解WAF产品的功能特点，指导您使购买并使用WAF。

# 产品功能

Web应用防火墙基于金山云安全团队防护经验内置规则集，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。本文档介绍了WAF的产品功能。

## Web应用攻击防护

### 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。
- 0day补丁定期及时更新：防护规则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。

### 精准访问控制

- 提供友好的配置控制台界面，支持IP、Path、Referer、User-Agent等HTTP常见字段，配置强大的精准访问控制策略。
- 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。

### 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。
- 对URL+cookie的访问频率进行控制，支持人机识别、拦截防护动作。

### 高级的Web攻击防护

- 地域封禁：使用封禁地区可以对指定的中国大陆各省份以及全球多达247个国家或地区的来源IP进行一键黑名单封禁，阻断所有来自指定地区的访问请求。

## 全量日志支持

支持全量日志实时存储和查询服务，保障业务情况安全可控可视。

# 新版WAF

Web应用防护墙（Web Application Firewall，简称WAF）默认提供高级版、企业版套餐，您可以根据要防护的业务规模和安全防护需求选择合适套餐。

本文档介绍了不同WAF套餐适用的业务规模和支持的防护功能。

## WAF3版本规格

| 功能详情 | 高级版 | 企业版 |
| --- | --- | --- |
| 全面检测SQL注入、XSS、WebShell上传、恶意爬虫等OWASP常见威胁 | √ | √ |
| 支持0Day漏洞虚拟补丁，云端同步更新最新Web漏洞规则 | √ | √ |
| 支持扫描工具屏蔽，屏蔽SqlMap等常见扫描工具 | √ | √ |
| 可针对特定的URL路径实现自定义匹配规则、识别方式 | √ | √ |
| 自由设置访问频率限制和阻断时间、方式，实现规则自由定义 | √ | √ |

| | | |
|---|---|---|
| 支持自定义设置人机识别算法，动态拉黑非法IP | √ | √ |
| 可针对常见HTTP字段实现精准访问控制，添加黑白名单，阻止不合规请求 | 支持IP、URL、Referer、User-Agent基础字段 | 包含基础字段外的更多HTTP字段 |
| 免费域名包 | 1个（支持10个域名防护，仅限1个一级域名，支持泛域名） | 1个（支持10个域名防护，仅限1个一级域名，支持泛域名） |
| 支持正常业务QPS阈值 | 5000QPS | 8000QPS |
| 免费IPv4防护带宽 | 10M | 30M |
| 免费日志存储时长 | 180天 | 360天 |
| 支持地域封禁功能，支持一键封禁海外地区 | - | √ |
| 支持一键开启HTTPS强制跳转、HTTP回源转换 | - | √ |
| 支持非标端口 | - | √ |

# 旧版WAF

Web应用防护墙（Web Application Firewall，简称WAF）分为SLB_WAF和云WAF两种实例类型，默认提供高级版、企业版套餐，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实例类型及套餐。

本文档介绍了不同WAF实例及其套餐适用的业务规模和支持的防护功能。

## WAF2实例类型

金山云Web应用防护墙分为SLB_WAF和云WAF两种实例类型，不同实例类型的应用场景和计费模式有一定区别。

### SLB_WAF

- 适用于源站在金山云数据中心内部，可以一键解绑定弹性EIP，内网回源，仅使用HTTP协议转发回源（包括HTTP和HTTPS请求），默认回源端口为80
- SLB_WAF需绑定VPC实例，回源防护只支持添加同VPC环境下的后端服务器，支持添加内网IP或弹性IP（过期或被删除的弹性IP，将从SLB_WAF回源记录中删除，建议添加内网IP）

### 云WAF

- 不限制源站在金山云内，可添加任意公网源站进行防护，HTTPS请求回源转发协议默认为HTTPS
- 不支持一键解绑定弹性IP
- 云WAF对超出赠送的业务带宽将收取带宽费用

## WAF2版本规格

| 规格 | 高级版 | 企业版 |
|---|---|---|
| 支持一键解绑定弹性EIP，作为SLB使用 | 仅SLB_WAF | 仅SLB_WAF |
| Web应用攻击基础防护，全面检测SQL注入、XSS、WebShell上传、文件包含、命令执行等OWASP常见威胁 | 支持 | 支持 |
| 敏感文件下载防护，阻止攻击者对网站敏感信息（如Git、SVN、配置、数据库等）进行下载尝试 | 支持 | 支持 |
| 支持常见HTTP字段的精准访问控制，阻止不合规（RFC、用户自定义）的HTTP/HTTPS请求 | 支持 | 支持 |
| 扫描工具屏蔽，屏蔽SqlMap等常见扫描工具 | 支持 | 支持 |
| 云端同步更新最新Web漏洞规则，支持0Day漏洞虚拟补丁 | 支持 | 支持 |
| 支持一键开启关闭域名防护 | 支持 | 支持 |
| 多协议支持：支持HTTP/HTTP 2.0/HTTPS协议 | 支持 | 支持 |
| 支持自定义设置人机识别算法，动态拉黑非法IP | - | 支持 |
| 支持多种人机识别算法进行业务风控，防黄牛、防刷单、防恶意注册等业务防护 | - | 支持 |
| 支持URI粒度的单IP/单用户CC自定义访问频率设置 | - | 支持 |
| 支持地域封禁功能，支持一键封禁海外地区 | - | 支持 |
| 免费域名包（1个域名防护包支持绑定10个域名,仅限1个一级域名，支持泛域名配置） | 1个 | 1个 |
| 正常业务QPS阈值 | 2000QPS | 5000QPS |
| 免费业务带宽 | 10Mbps（仅云WAF） | 30Mbps（仅云WAF） |

# 术语说明

本文档主要介绍了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。

## 源站

源站指提供服务的后端服务器。

## 常见攻击

| 攻击类型 | 解释 |
| --- | --- |
| SQL注入 | 通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令 |
| 跨站脚本攻击 | 即XSS攻击，攻击者在Web页面中插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的 |
| 文件包含 | 攻击者通过网站注入一段受控制的恶意脚本或代码文件，并让服务端执行 |
| 远程命令执行 | 程序对传数过滤不严，导致攻击者能控制最终执行的命令，进而入侵系统 |
| 敏感信息泄露 | 用户或企业的私密信息，通过漏洞被攻击者获取 |
| 恶意扫描 | 通过自动化扫描工具探测网站是否存在可利用的Web 漏洞 |
| CC攻击 | 攻击者借助代理服务器生成指向Web服务器的合法请求，导致服务器无法处理正常访问请求 |