Web 应用防火墙

产品介绍

文档版本 58

发布日期 2022-05-12

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 什么是 Web 应用防火墙

Web应用防火墙（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

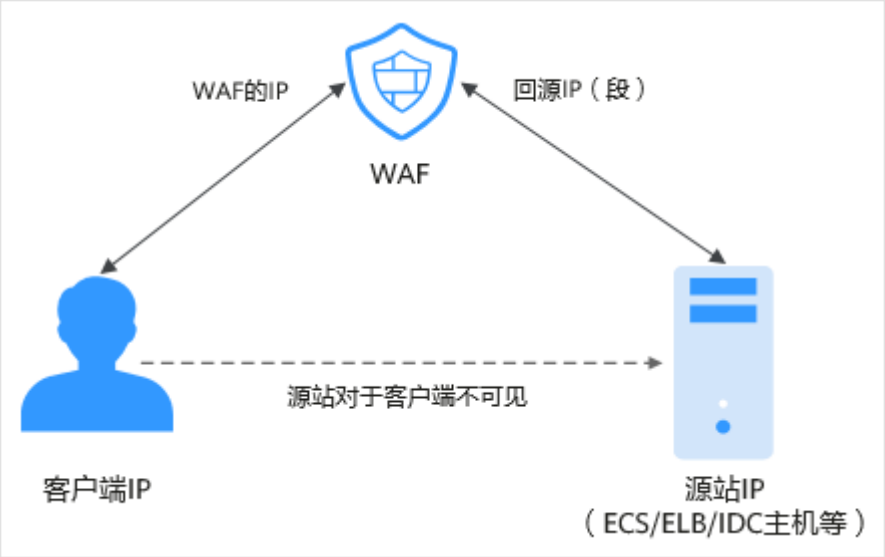
防护原理

购买WAF后，在WAF管理控制台将网站添加并接入WAF。网站成功接入WAF后，网站所有访问请求将先流转到WAF，WAF检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

图 1-1 网站接入 WAF 防护原理

流量经WAF返回源站的过程称为回源。WAF通过回源IP代替客户端发送请求到源站服务器，在源站服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，进而隐藏源站。

图 1-2 回源 IP



防护对象

WAF支持云模式、独享模式和ELB模式三种部署模式，各部署模式支持防护的对象说明如下：

- 云模式：域名，华为云、非华为云或云下的Web业务
- 独享模式/ELB模式：域名或IP，华为云上的Web业务

2 服务版本差异

Web应用防火墙支持云模式、独享模式和ELB模式三种部署方式，部署模式的差异说明如**云模式、独享模式和ELB模式使用说明**。

云模式、独享模式和 ELB 模式使用说明

请您根据业务需求选择使用云模式、独享模式或ELB模式（ELB模式为七层负载均衡，支持HTTP和HTTPS协议，监听器收到访问请求后，需要识别并通过HTTP/HTTPS协议报文头中的相关字段，进行数据的转发），您也可以同时使用三种模式， 三种模式的部署架构如**图2-1**所示，主要差异说明如**表2-1**所示。

须知

使用独享模式或ELB模式前，请确认已**提交工单**申请开通独享模式或ELB模式。否则，您将无法购买独享模式或ELB模式。

图 2-1 云模式、独享模式和 ELB 模式部署架构

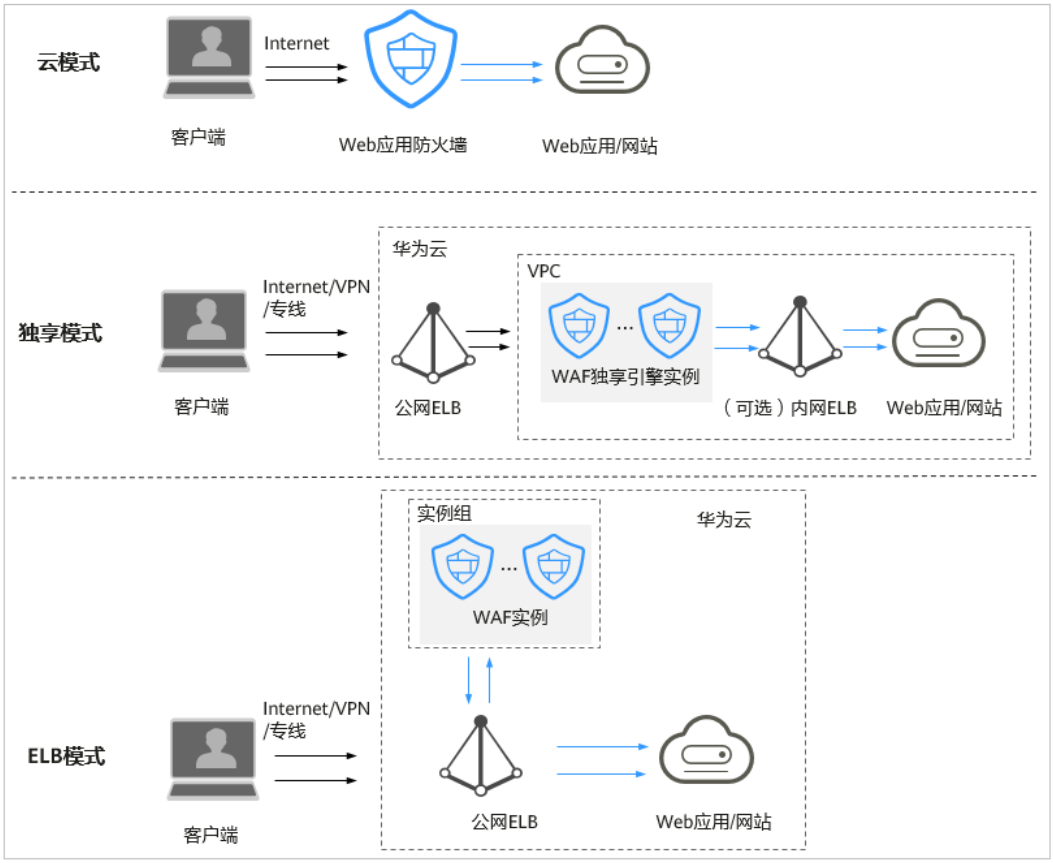


表 2-1 各模式使用说明

项目	云模式	独享模式	ELB模式
计费方式	包周期（包年/包月）	按需计费	按需计费
服务版本	• 检测版 • 标准版（原专业版） • 专业版（原企业版） • 铂金版（原旗舰版）	-	-

项目	云模式	独享模式	ELB模式
使用场景	业务服务器部署在华为云上、非华为云或线下。 各服务版本推荐使用的场景说明如下： ● 检测版 个人网站防护 ● 标准版（原专业版） 中小型网站，对业务没有特殊的安全需求 ● 专业版（原企业版） 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 ● 铂金版（原旗舰版） 中大型企业网站，具备较大的业务规模，或是具有制定个性化防护的安全需求	业务服务器部署在华为云上。 大型企业网站，具备较大的业务规模且基于业务特性具有制定个性化防护规则的安全需求。	业务服务器部署在华为云上。 大型企业网站，对业务稳定性有较高要求的安全防护需求。
防护对象	域名	域名或IP	域名或IP
优势	● 弹性扩容能力强，通过升级规格可以扩容防护能力 ● 可以防护华为云、非华为云和云下的Web业务 ● 支持IPv6防护	● 部署灵活 ● 独享引擎实例资源由用户独享 ● 可以满足大规模流量攻击场景防护需求 ● 独享引擎实例部署在VPC内，网络链路时延低	● 不改变业务架构，水平扩展防护能力 ● 旁路部署，业务零影响 ● 可靠性高 当WAF发生故障时，流量将直接通过ELB发送给后端，不影响客户正常业务。

各版本支持的业务规格

云模式各个版本、独享模式和ELB模式适用的业务规格如**表2-2**所示。其中，购买云模式时您可以选择购买域名扩展包、带宽扩展包和规则扩展包，以满足更多域名、更大

流量的防护需求，也可以购买额外的扩展包或者通过**升级云模式版本和规格**从较低版本升级到任一更高版本。

扩展包限制和规格说明如下：

- 一个域名包支持10个域名，限制仅支持1个一级域名和与一级域名相关的子域名或泛域名。
- 一个带宽扩展包包含20Mbit/s/50Mbit/s（华为云外/华为云内）或者1,000QPS（Query Per Second，即每秒钟的请求量，例如一个HTTP GET请求就是一个Query）。

  说明

  - 华为云外：源站服务器部署在非华为云或云下（线下）。
  - 华为云内：源站服务器部署在华为云上。
- 一个规则扩展包包含10条IP黑白名单防护规则。

须知

- 域名个数为一级域名（例如，example.com）、单域名/二级域名等子域名（例如，www.example.com）和泛域名（例如，*.example.com）的总数。例如，标准版（原专业版）支持防护10个域名，则标准版（原专业版）可以添加10个单域名或泛域名，也可以添加1个一级域名和9个与其相关的子域名或泛域名。
- 同一个域名对应不同端口视为不同的域名，例如www.example.com:8080和www.example.com:8081视为两个不同的域名，将占用两个不同的域名防护额度。

表 2-2 适用的业务规格

业务规格	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享模式	ELB模式
正常业务请求峰值	• 100 QPS业务请求 • 6,000回源长连接（每域名）	• 2,000 QPS • 6,000回源长连接（每域名）	• 5,000 QPS业务请求 • 6,000回源长连接（每域名）	• 10,000 QPS业务请求 • 6,000回源长连接（每域名）	• WAF实例规格选择WI-500，参考性能： – 吞吐量：500 Mbps，QPS：10,000 – 单实例可支持回源长连接：60,000（每实例），5,000（每域名） • WAF实例规格选择WI-100，参考性能： – 吞吐量：100 Mbps，QPS：2,000 – 单实例可支持回源长连	• WAF实例规格选择WI-500，参考性能 – 吞吐量：500 Mbit/s – QPS：10,000 • WAF实例规格选择WI-100，参考性能 – 吞吐量：100 Mbit/s – QPS：2,000

业务规格	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享模式	ELB模式
					接:60,000（每实例），5,000（每域名）	

业务规格	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享模式	ELB模式
业务带宽阈值（源站服务器部署在华为云）	10Mbit/s	100Mbit/s	200Mbit/s	300Mbit/s	• WAF实例规格选择WI-500，参考性能： – 吞吐量：500 Mbps，QPS：10,000 – 单实例可支持回源长连接：60,000（每实例），5,000（每域名） • WAF实例规格选择WI-100，参考性能： – 吞吐量：100 Mbps，QPS：2,000 – 单实例可支持回源长连接：	• WAF实例规格选择WI-500，参考性能 – 吞吐量：500 Mbit/s – QPS：10,000 • WAF实例规格选择WI-100，参考性能 – 吞吐量：100 Mbit/s – QPS：2,000

业务规格	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享模式	ELB模式
					60,000（每实例），5,000（每域名）	
业务带宽阈值（源站服务器未部署在华为云）	10Mbit/s	30Mbit/s	50Mbit/s	100Mbit/s	-	-
域名个数	10个（支持1个一级域名）	10个（支持1个一级域名）	50个（支持5个一级域名）	80个（支持8个一级域名）	2,000个（支持2,000个一级域名）	2,000个（支持2,000个一级域名）
回源IP（单个防护域名支持的回源服务器IP个数）	10个	20个	50个	80个	-	-
支持的端口个数	标准端口：不限制	• 标准端口：不限制 • 非标准端口：10个	• 标准端口：不限制 • 非标准端口：18个	• 标准端口：不限制 • 非标准端口：58个	• 标准端口：不限制 • 非标准端口：不限制	不限制
CC攻击防护峰值	-	100,000QPS	300,000QPS	1,000,000QPS	500,000QPS	500,000QPS

业务规格	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享模式	ELB模式
CC攻击防护规则	-	20条	50条	100条	100条	100条
精准访问防护规则	-	20条	50条	100条	100条	100条
引用表规则	-	-	50条	100条	100条	100条
IP黑白名单规则	-	20条	100条	1000条	1000条	1000条
地理位置封禁规则	-	-	50条	100条	100条	100条
网页防篡改规则	-	20条	50条	100条	100条	-
防敏感信息泄露	-	-	50条	100条	100条	-
误报屏蔽规则	1000条	1000条	1000条	1000条	1000条	1000条
隐私屏蔽规则	-	20条	50条	100条	100条	100条

各版本支持的功能特性

云模式各个版本、独享模式和ELB模式适用的安全功能特性如**表2-3**所示，请您根据业务需求选择对应的服务版本。其中，云模式支持检测版、标准版（原专业版）、专业版（原企业版）和铂金版（原旗舰版）四种版本，您可以通过**升级云模式版本和规格**从较低版本升级到任一更高版本，以满足更多防护功能需求。

须知

云模式的专业版（原企业版）和铂金版（原旗舰版）支持定制非标准端口，您可以**提交工单**申请开通定制的非标准端口。定制的非标准端口数将统计到非标准端口配额中（铂金版支持防护58个非标准端口），例如，如果您添加了6个铂金版支持的非标准端口，2个定制的非标准端口，则您还可以添加50个非标准端口。

标识说明：

- √：表示在当前版本中支持。
- ×：表示在当前版本中不支持。

表 2-3 安全功能特性

功能模板	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享版	ELB模式
域名/带宽/规则扩展包	×	√	√	√	×	×
域名备案检查	√	√	√	√	×	×
支持添加泛域名	×	√	√	√	√	√
非80、443标准端口防护	×	√	√	√	√	√
非80、443标准端口定制	×	×	√	√	×	×
批量灵活配置防护策略	√（仅支持批量配置误报屏蔽策略）	×	√	√	√	√
为防护策略批量配置适用的防护域名	×	×	√	√	√	√
支持IPv6防护 **须知** 当前仅“华东”和“华北”区域支持IPv4/6双栈和NAT64。	×	×	√	√	×	×
常见的Web应用攻击防护，包括SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等	√（只检测，不支持拦截）	√	√	√	√	√
云端自动更新最新0Day漏洞防护规则，及时下发0Day漏洞虚拟补丁	×	√	√	√	√	√
Webshell检测	√（只检测，不支持拦截）	√	√	√	√	√

功能模板	检测版	标准版（原专业版）	专业版（原企业版）	铂金版（原旗舰版）	独享版	ELB模式
深度检测，同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸检测	√（只检测，不支持拦截）	√	√	√	√	√
header全检测，对请求里header中所有字段进行攻击检测	√（只检测，不支持拦截）	√	√	√	√	√
CC攻击防护	×	√	√	√	√	√
精准访问防护	×	√（不支持全检测）	√	√	√	√
引用表管理	×	×	√	√	√	√
IP黑白名单设置，支持批量导入IP地址/IP地址段	×	√	√	√	√	√
支持对指定国家、省份的IP自定义访问控制	×	×	√	√	√	√
网页防篡改	×	√	√	√	√	×
检测并拦截搜索引擎、扫描器、脚本工具、其它爬虫等爬虫行为	×	×	√	√	√	√
检测并拦截JS脚本反爬虫检测行为	×	×	√	√	√	×
防敏感信息泄露	×	×	√	√	√	×
误报屏蔽	√	√	√	√	√	√
隐私屏蔽	×	√	√	√	√	√

3 功能特性

通过Web应用防火墙，轻松应对各种Web安全风险。

域名（泛域名、一级域名、二级域名等各级域名）/IP 防护

WAF支持云模式、独享模式和ELB模式三种部署模式，各部署模式支持防护的对象说明如下：

- 云模式：域名，华为云、非华为云或云下的Web业务
- 独享模式/ELB模式：域名或IP，华为云上的Web业务

HTTP/HTTPS 业务防护

WAF可以防护HTTP/HTTPS业务，通过对HTTP/HTTPS请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

支持 WebSocket/WebSockets 协议

WAF支持WebSocket/WebSockets协议，且默认为开启状态。

域名备案检查

WAF云模式支持域名备案检查，添加防护域名时，WAF会检查域名备案情况，未备案域名将无法添加到WAF。

PCI DSS/PCI 3DS 合规认证和 TLS

- TLS支持TLS v1.0、TLS v1.1和TLS v1.2三个版本和五种加密套件，可以满足各种行业客户的安全需求。
- WAF支持PCI DSS和PCI 3DS合规认证功能。

Web 基础防护

覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对漏洞攻击、网页木马等威胁进行检测和拦截。

- 全面的攻击防护

  支持SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录（路径）遍历、敏感文件访问、命令/代码注入、XML/Xpath注入等攻击检测和拦截。

- Webshell检测

  防护通过上传接口植入网页木马。

- 识别精准
  - 内置语义分析+正则双引擎，黑白名单配置，误报率更低。
  - 支持防逃逸，自动还原常见编码，识别变形攻击能力更强。

    默认支持的编码还原类型：url_encode、Unicode、xml、OCT（八进制）、HEX（十六进制）、html转义、base64、大小写混淆、javascript/shell/php等拼接混淆。

- 深度检测

  深度反逃逸识别（支持同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等的防护）。

- header全检测

  支持对请求里header中所有字段进行攻击检测。

IPv6 防护

Web应用防火墙支持防护IPv6环境下发起的攻击，帮助您的源站实现对IPv6流量的安全防护。

随着IPv6协议的迅速普及，新的网络环境以及新兴领域均面临着新的安全挑战，Web应用防火墙的IPv6防护功能帮助您轻松构建覆盖全球的安全防护体系。

- Web应用防火墙支持IPv6/IPv4双栈，针对同一域名可以同时提供IPv6和IPv4的流量防护。
- 针对仍然使用IPv4协议栈的Web业务，Web应用防火墙支持NAT64机制（NAT64是一种通过网络地址转换（NAT）形式促成IPv6与IPv4主机间通信的IPv6转换机制），即WAF可以将IPv4源站转化成IPv6网站，将外部IPv6访问流量转化成对内的IPv4流量。

CC 攻击防护

CC攻击防护规则支持通过限制单个IP/Cookie/Referer访问者对防护网站上特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击。支持人机验证、阻断、动态阻断和仅记录防护动作。

- 策略配置灵活

  可以根据IP、Cookie或者Referer字段名设置灵活的限速策略。

- 阻断页面可定制

  阻断页面可自定义内容和类型，满足业务多样化需要。

安全可视化

提供简洁友好的控制界面，实时查看攻击信息和事件日志。

- 策略事件集中配置

在Web应用防火墙服务的控制台集中配置适用于多个防护域名的策略，快速下发，快速生效。

- 流量及事件统计信息

  实时查看访问次数、安全事件的数量与类型、详细的日志信息。

非标准端口防护

Web应用防火墙除了可以防护标准的80，443端口外，还支持非标准端口的防护。

表 3-1 WAF 支持的端口

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
检测版	标准端口	80	443	不限制
标准版（原专业版）	标准端口	80	443	不限制
	非标准端口（**86个**）	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805	**10个**
专业版（原企业版）	标准端口	80	443	不限制

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
	非标准端口（**182个**）	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	**18个**

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
铂金版（原旗舰版）	标准端口	80	443	不限制

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
	非标准端口（**199个**）	8899, 8006, 9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014,	8750, 9190, 9184, 9182, 8950, 8920, 8910, 8848, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999, 8244, 8224, 8281, 8211, 8243, 8221, 8231	**58个**

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
		8015, 8016, 8017, 8070, 8232		
独享模式	标准端口	80	443	不限制

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
	非标准端口（**182个**）	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	不限制

服务版本	端口分类	HTTP协议	HTTPS协议	端口防护限制数
ELB模式	端口	1~65535	1~65535	不限制

精准访问防护

基于丰富的字段和逻辑条件组合，打造强大的精准访问控制策略。

- 支持丰富的字段条件

  支持IP、URL、Referer、User Agent、Params、Header等HTTP常见参数和字段的条件组合。
- 支持多种条件逻辑

  支持包含、不包含、等于、不等于、前缀为、前缀不为等逻辑条件，设置阻断或放行策略。

IP 黑白名单设置

添加始终拦截与始终放行的黑白名单IP/IP地址段，增加防御准确性。WAF支持批量导入IP地址/IP地址段。

攻击惩罚

- 当访问者的IP、Cookie或Params恶意请求被WAF拦截时，您可以通过配置攻击惩罚，使WAF按配置的攻击惩罚时长来自动封禁访问者。
- Web基础防护、精准访问防护和黑白名单设置支持攻击惩罚功能。

地理位置访问控制

可以针对国家、地区地理位置来源IP进行自定义访问控制。

网页防篡改

对网站的静态网页进行缓存配置，当用户访问时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

网站反爬虫

动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别700+种爬虫行为。

- 特征反爬虫

  自定义扫描器与爬虫规则，用于阻断网页爬取行为，添加定制的恶意爬虫、扫描器特征，使爬虫防护更精准。
- JS脚本反爬虫

  通过自定义规则识别并阻断JS脚本爬虫行为。

误报屏蔽

针对特定请求忽略某些攻击检测规则，用于处理误报事件。

隐私屏蔽

避免在防护事件日志中，出现用户名或者密码等敏感信息。

防敏感信息泄露

防止在页面中泄露用户的敏感信息，例如：用户的身份证号码、手机号码、电子邮箱等。

稳定可靠

多区域多集群部署，支持负载均衡，可在线平滑扩容，没有单点故障，最大限度保护业务运行稳定。

告警通知

用户可以通过Web应用防火墙服务对攻击日志进行通知设置。开启告警通知后，Web应用防火墙将仅记录和拦截的攻击日志通过用户设置的接收通知方式发送给用户。

管理防护事件

- 当Web应用防火墙拦截或者仅记录的攻击事件为误报时，用户可通过Web应用防火墙处理误报事件、查看事件详情。
- 用户可以通过Web应用防火墙服务下载5天内的全量防护事件数据。
- WAF支持全量日志功能，您可以将攻击日志、访问日志记录到华为云的云日志服务（ Log Tank Service，简称LTS ）。

4 产品优势

Web应用防火墙对网站业务流量进行多维度检测和防护，降低数据被篡改、失窃的风险。

精准高效的威胁检测

- 采用规则和AI双引擎架构，默认集成华为最新的防护规则和优秀实践。
- 企业级用户策略定制，支持拦截页面自定义、多条件的CC防护策略配置、海量IP黑名单等，使网站防护更精准。

0day 漏洞快速修复

专业安全团队7*24小时运营，实现紧急0day漏洞2小时内修复完成，帮助用户快速抵御最新威胁。

保护用户数据隐私

- 支持用户对攻击日志中的帐号、密码等敏感信息进行脱敏。
- 支持PCI-DSS标准的SSL安全配置。
- 支持TLS协议版本和加密套件的配置。

助力企业安全合规

帮助企业满足等保测评、PCI-DSS等安全标准的技术要求。

5 应用场景

常规防护

帮助用户防护常见的Web安全问题，比如命令注入、敏感文件访问等高危攻击。

电商抢购秒杀防护

当业务举办定时抢购秒杀活动时，业务接口可能在短时间承担大量的恶意请求。Web应用防火墙可以灵活设置CC攻击防护的限速策略，能够保证业务服务不会因大量的并发访问而崩溃，同时尽可能地给正常用户提供业务服务。

0Day 漏洞爆发防范

当第三方Web框架、插件爆出高危漏洞，业务无法快速升级修复，Web应用防火墙会第一时间升级预置防护规则，保障业务安全稳定。WAF相当于第三方网络架构加了一层保护膜，和直接修复第三方架构的漏洞相比，WAF创建的规则能更快的遏制住风险。

防数据泄露

恶意访问者通过SQL注入，网页木马等攻击手段，入侵网站数据库，窃取业务数据或其他敏感信息。用户可通过Web应用防火墙配置防数据泄露规则，以实现：

- 精准识别

  采用语义分析+正则表达式双引擎，对流量进行多维度精确检测，精准识别攻击流量。
- 变形攻击检测

  支持7种编码还原，可识别更多变形攻击，降低Web应用防火墙被绕过的风险。

防网页篡改

攻击者利用黑客技术，在网站服务器上留下后门或篡改网页内容，造成经济损失或带来负面影响。用户可通过Web应用防火墙配置网页防篡改规则，以实现：

- 挂马检测

  检测恶意攻击者在网站服务器注入的恶意代码，保护网站访问者安全。
- 页面不被篡改

保护页面内容安全，避免攻击者恶意篡改页面，修改页面信息或在网页上发布不良信息，影响网站品牌形象。

6 计费说明

Web应用防火墙云模式支持包年/包月（预付费）计费方式，独享模式和ELB模式支持按需计费（后付费）计费方式。

有关Web应用防火墙详细的服务资费费率标准请参见**产品价格详情**。

计费项

WAF根据购买方式和计费模式进行计费。

图 6-1 WAF 的计费方式

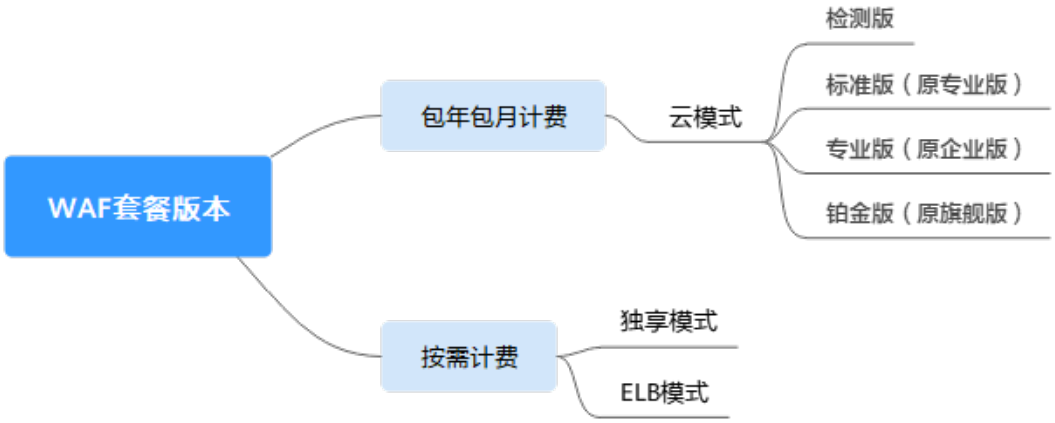


表 6-1 计费项信息

购买模式	计费模式	计费项目	计费说明
云模式	包周期（包年/包月）	服务版本（必选）	按购买的服务版本：检测版、标准版（原专业版）、专业版（原企业版）、铂金版（原旗舰版）计费。 各服务版本支持的业务规格和功能，请参见**服务版本差异**。
		域名扩展包（可选）	按购买的个数计费。

购买模式	计费模式	计费项目	计费说明
		带宽扩展包（可选）	按购买的个数计费。
		规则扩展包（可选）	按购买的个数计费。
		购买时长	提供包月和包年的购买模式。
独享模式	按需计费	实例个数	按实际使用时长计费。
ELB模式	按需计费	实例个数	按实际使用时长计费。

计费模式

- 包周期（包年/包月）：云模式计费模式，使用越久越便宜。包周期计费按照订单的购买周期来进行结算。
- 按需计费：独享模式和ELB模式计费模式，这种购买方式比较灵活，可以即开即停。

  实例从创建成功开始计费到删除实例时结束计费，按实际使用时长（精确到秒）计费。

变更配置

- 以包年/包月方式购买云模式，您可以通过升级规格操作，将WAF从较低版本升级到任一更高版本，也可以根据业务需求增加域名扩展包、带宽扩展包和规则扩展包的数量。
- 退订：以包年/包月方式购买云模式后，如需停止使用，请到费用中心执行**退订**操作。

续费

包年/包月方式购买的云模式到期后，如果没有按时续费，公有云平台会提供一定的保留期。

保留期的时长由客户等级来定，详细信息请参见“**保留期**”。

- 冻结期内，WAF只转发流量，但用户配置的各种防护策略将不再生效。
- 冻结期满，进入资源清理期，域名的所有配置将会被全部删除。清除资源的时候，默认会把域名指回源站，但由于用户配置的协议和端口可能存在不一致的情况，所以不能保证该域名的业务能正常运行。

为了防止造成不必要的损失，请您及时续费。如果未续费，您将不能使用WAF服务，不影响您的网站访问业务。

如需续费，请在管理控制台续费管理页面进行续费操作。详细操作请参考**续费管理**。

到期与欠费

- 服务到期

  若包年/包月方式购买的云模式到期后，如果没有按时续费，公有云平台会提供一定的保留期，请参考**保留期**。

- 欠费

  若包年/包月方式购买的云模式已欠费，可以查看欠费详情。为了网站安全，建议您及时进行充值，详细操作请参考**欠费还款**。

FAQ

更多计费相关FAQ，请参见**WAF常见问题**。

7 项目和企业项目

项目

IAM中的项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。一个帐户中可以创建多个项目。

企业项目

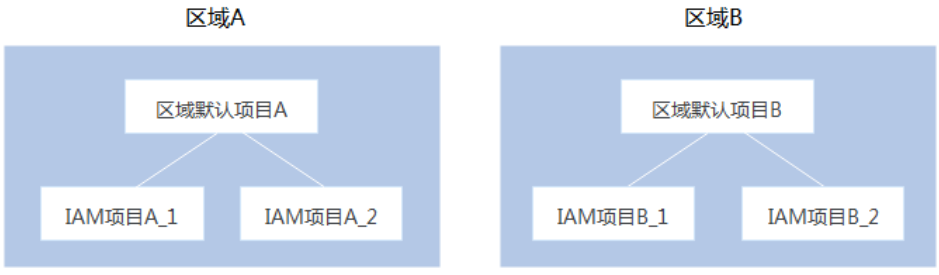
企业管理中的企业项目是对多个资源进行分组和管理，在目标区域中同一类型的资源可以划分到一个企业项目中，且主机安全服务的使用不受企业项目的划分影响。

企业可以根据不同的部门或项目组，将相关的资源放置在相同的企业项目内进行管理，并支持资源在企业项目之间迁移。

项目与企业项目的区别

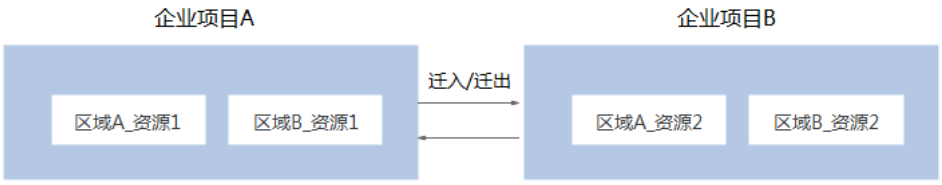
- IAM项目

  IAM项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。



- 企业项目

  企业项目是IAM项目的升级版，是针对企业不同项目间资源的分组和管理。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。如果您开通了企业管理，将不能创建新的IAM项目（只能管理已有项目）。未来IAM项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。



项目和企业项目都可以授权给一个或者多个用户组进行管理，管理企业项目的用户归属于用户组。通过给用户组授予策略，用户组中的用户就能在所属项目/企业项目中获得策略中定义的权限。

有关创建项目、企业项目，以及授权的详细操作，请参见**管理项目和企业项目**。

8 个人数据保护机制

为了确保网站访问者的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，WAF通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

对于触发攻击告警的请求，WAF在事件日志中会记录相关请求记录，收集及产生的个人数据如表8-1所示。

表 8-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
请求源IP	攻击防护域名时，被WAF拦截或者记录的攻击者IP。	否	是
URL	攻击的防护域名的URL，被WAF拦截或者记录的防护域名的URL。	否	是
HTTP/HTTPS Header信息（包括Cookie）	用户在配置CC攻击、精准访问防护规则时，在配置界面输入的Cookie值和Header值。	否	否 如果配置的Cookie和Header信息不含有用户的个人信息，则WAF记录的相关请求中不会收集及产生用户的个人数据。
请求参数（Get、Post）	防护日志里，WAF记录的请求详情。	否	否 如果请求参数里不含有用户的个人信息，则WAF记录的相关请求中不会收集及产生用户的个人数据。

存储方式

对敏感字段提供了脱敏配置，其他字段在日志中明文保存。

访问权限控制

用户只能查看自己业务的相关日志。

9 WAF 权限管理

如果您需要对华为云上购买的WAF资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云帐号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望这些员工拥有WAF的使用权限，但是不希望这些员工拥有删除WAF等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用WAF，但是不允许删除WAF的权限，控制员工对WAF资源的使用范围。

如果华为云帐号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用WAF的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

WAF 权限

默认情况下，创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

WAF部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问WAF时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对WAF服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，WAF支持的API授权项请参见**WAF权限及授权项**。

如表9-1所示，包括了WAF的所有系统角色。

表 9-1 WAF 系统角色

系统角色/策略名称	描述	类别	依赖关系
WAF Administrator	Web应用防火墙服务的管理员权限。	系统角色	依赖Tenant Guest和Server Administrator角色。 • Tenant Guest：全局级角色，在全局项目中勾选。 • Server Administrator：项目级角色，在同项目中勾选。
WAF FullAccess	Web应用防火墙服务的所有权限。	系统策略	无。
WAF ReadOnlyAccess	Web应用防火墙的只读访问权限。	系统策略	

相关链接

- IAM产品介绍
- 创建用户组、用户并授予WAF权限
- WAF自定义策略
- WAF权限及授权项

WAF FullAccess 策略内容

```
{    "Version": "1.1",
     "Statement": [
         {
            "Action": [
              "waf:*:*",
              "lts:groups:get",
              "lts:groups:list",
              "lts:topics:get",
              "lts:topics:list",
              "smn:*:list*",
              "vpc:*:get*",
              "vpc:*:list*",
              "ecs:*:get*",
              "ecs:*:list*",
              "elb:*:get*",
              "elb:*:list*"
            ],
              "Effect": "Allow"
         }
              ]
}
```

WAF ReadOnlyAccess 策略内容

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "waf:*:get*",
            "waf:*:list*",
            "lts:groups:get",
            "lts:groups:list",
            "lts:topics:get",
            "lts:topics:list",
            "smn:*:list*",
            "vpc:*:get*",
            "vpc:*:list*",
            "ecs:*:get*",
            "ecs:*:list*",
            "elb:*:get*",
            "elb:*:list*"
       ],
            "Effect": "Allow"
      }
   ]
}
```


10 与其他云服务的关系

本章节介绍Web应用防火墙与其他云服务的关系。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录了Web应用防火墙相关的操作事件，方便用户日后的查询、审计和回溯。

须知

目前以下区域支持云审计功能：

- 华北-北京一
- 华北-北京四
- 华东-上海一
- 华东-上海二
- 华南-广州
- 中国-香港
- 亚太-曼谷
- 亚太-新加坡
- 非洲-约翰内斯堡
- 拉美-圣地亚哥

表 10-1 云审计服务支持的 WAF 操作列表

操作名称	资源类型	事件名称
创建Web应用防火墙防护实例	instance	createInstance
删除Web应用防火墙防护实例	instance	deleteInstance
更新Web应用防火墙防护实例	instance	modifyInstance

操作名称	资源类型	事件名称
修改Web应用防火墙防护实例的防护状态	instance	modifyProtectStatus
修改Web应用防火墙防护实例的接入状态	instance	modifyAccessStatus
创建Web应用防火墙防护策略	policy	createPolicy
应用Web应用防火墙防护策略	policy	applyToHost
更新Web应用防火墙防护策略	policy	modifyPolicy
删除Web应用防火墙防护策略	policy	deletePolicy
修改告警通知设置	alertNoticeConfig	modifyAlertNoticeConfig
添加证书	certificate	createCertificate
修改证书名称	certificate	modifyCertificate
删除证书	certificate	deleteCertificate
创建CC规则	policy	createCc
修改CC规则	policy	modifyCc
删除CC规则	policy	deleteCc
创建精准防护规则	policy	createCustom
修改精准防护规则	policy	modifyCustom
删除精准防护规则	policy	deleteCustom
创建IP黑白名单规则	policy	createWhiteblackip
修改IP黑白名单规则	policy	modifyWhiteblackip
删除IP黑白名单规则	policy	deleteWhiteblackip
创建网页防篡改规则	policy	createAntitamper
刷新网页防篡改规则	policy	refreshAntitamper
删除网页防篡改规则	policy	deleteAntitamper
创建误报屏蔽规则	policy	createIgnore
删除误报屏蔽规则	policy	deleteIgnore
创建隐私屏蔽规则	policy	createPrivacy
修改隐私屏蔽规则	policy	modifyPrivacy
删除隐私屏蔽规则	policy	deletePrivacy

与云监控服务的关系

云监控服务可以监控Web应用防火墙的相关指标，用户可以通过指标及时了解Web应用防火墙防护状况，并通过这些指标设置防护策略。具体请参见《云监控服务用户指南》。

有关WAF监控指标的详细介绍，请参见**WAF监控指标说明**。

与弹性负载均衡的关系

Web应用防火墙通过绑定**弹性负载均衡**（Elastic Load Balance，以下简称ELB），使流量通过ELB后先发送给WAF检测，再发送给应用端，以提升防护性能和确保业务稳定运行。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为Web应用防火墙服务提供了权限管理的功能。需要拥有WAF Administrator权限的用户才能使用WAF服务。如需开通该权限，请联系拥有Security Administrator权限的用户。

与云日志服务的关系

云日志服务（Log Tank Service，简称LTS）用于收集来自主机和云服务的日志数据。Web应用防火墙可以设置将攻击日志、访问日志记录到LTS中，为您提供一个实时、高效、安全的日志处理功能。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN）提供消息通知功能。Web应用防火墙开启通知设置后，如果防护的域名受到事件攻击时，告警信息会通过用户设置的接收通知方式发送给用户。

与企业管理的关系

企业中有多个项目，多个项目的资源需要分开结算，且分属不同人员进行管理。同时项目可以单独启动或停止，对其他项目没有影响。**企业管理**可以针对企业中的每个项目，分别建立企业项目，管理各自的资源，并且针对不同的企业项目，设置不同的人员进行管理。

Web应用防火墙支持企业管理，您可以将Web应用防火墙上的资源按照企业项目进行管理，并设置每个企业项目的用户权限。

须知

目前华北-乌兰察布一区域不支持企业管理功能。

A 修订记录

发布日期	修改说明
2022-05-12	第五十八次正式发布。 修改如下章节： • **服务版本差异** • **计费说明** • **产品优势**
2022-05-07	第五十七次正式发布。 修改**个人数据保护机制**章节。
2022-03-07	第五十六次正式发布。 支持独享模式，修改如下章节： • **服务版本差异** • **计费说明**
2022-02-10	第五十五次正式发布。 **服务版本差异**，优化内容描述。
2022-01-21	第五十四次正式发布。 **服务版本差异**，优化内容描述。
2021-12-30	第五十三次正式发布。 **与其他云服务的关系**，新增与云监控服务相关内容。
2021-12-10	第五十二次正式发布。 **服务版本差异**，修改规格描述。
2021-11-08	第五十一次正式发布。 **服务版本差异**，修改规格描述。
2021-11-04	第五十次正式发布。 **服务版本差异**，修改规格描述。

发布日期	修改说明
2021-10-12	第四十九次正式发布。 **功能特性**，优化部分文字描述。
2021-09-23	第四十八次正式发布。 **WAF权限管理**，修改策略内容描述。
2021-09-17	第四十七次正式发布。 **服务版本差异**，优化部分文字描述。
2021-08-12	第四十六次正式发布。 **服务版本差异**，优化部分文字描述。
2021-08-06	第四十五次正式发布。 云模式服务版本名称变更：原专业版变更为标准版、原企业版变更为专业版、原旗舰版变更为铂金版。
2021-08-02	第四十四次正式发布。 **功能特性**，优化部分文字内容描述。
2021-07-06	第四十三次正式发布。 **什么是Web应用防火墙**，优化部分文字内容描述。
2021-06-16	第四十二次正式发布。 **服务版本差异**，优化部分文字内容描述。
2021-05-27	第四十一次正式发布。 **服务版本差异**，优化部分文字内容描述。
2021-05-24	第四十次正式发布。 **功能特性**，新增功能特性描述。
2021-05-18	第三十九次正式发布。 **什么是Web应用防火墙**，新增防护对象内容描述。
2021-04-30	第三十八次正式发布。 **计费说明**，增加带宽扩展包计费说明。
2021-04-07	第三十七次正式发布。 **服务版本差异**，新增安全特性描述。
2021-03-02	第三十六次正式发布。 **服务版本差异**，修改部署架构图。
2021-02-25	第三十五次正式发布。 • 新增**项目和企业项目**。 • **与其他云服务的关系**，增加与企业管理关系说明。
2021-02-23	第三十四次正式发布。 **服务版本差异**，修改内容描述。

发布日期	修改说明
2021-02-05	第三十三次正式发布。 **服务版本差异**，优化部分文字内容描述。
2021-01-25	第三十二次正式发布。 **服务版本差异**，优化部分文字内容描述。
2020-12-31	第三十一次正式发布。 **功能特性**，优化部分文字内容描述。
2020-12-25	第三十次正式发布。 • **服务版本差异**，新增ELB模式相关内容。 • **计费说明**，新增ELB模式相关内容。
2020-12-11	第二十九次正式发布。 删除云模式按需计费相关描述。
2020-10-22	第二十八次正式发布。 **服务版本差异**，修改按需计费规格。
2020-09-23	第二十七次正式发布。 **与其他云服务的关系**，优化部分文字内容描述。
2020-09-11	第二十六次正式发布。 • **功能特性**，补充云模式按需计费支持端口说明。 • **计费说明**，补充云模式按需计费相关内容说明。
2020-07-31	第二十五次正式发布。 **计费说明**，优化部分文字内容描述。
2020-07-08	第二十四次正式发布。 • **服务版本差异**，补充独享模式相关内容描述。 • **计费说明**，优化部分文字内容描述。
2020-06-24	第二十三次正式发布。 **服务版本差异**，补充检测版内容。
2020-06-22	第二十二次正式发布。 **WAF权限管理**，补充细粒度策略内容。
2020-06-16	第二十一次正式发布。 **服务版本差异**，优化域名描述。
2020-06-11	第二十次正式发布。 **服务版本差异**，优化部分文字内容描述。
2020-05-26	第十九次正式发布。 **计费说明**，优化部分文字内容描述。

发布日期	修改说明
2020-05-19	第十八次正式发布。 新增**计费说明**。
2020-03-19	第十七次正式发布。 **功能特性**，修改非标准端口。
2020-01-20	第十六次正式发布。 **WAF权限管理**，优化部分文字内容描述。
2019-12-26	第十五次正式发布。 **功能特性**，优化部分文字内容描述。
2019-12-09	第十四次正式发布。 • **服务版本差异**，优化部分文字内容描述。 • **功能特性**，优化部分文字内容描述。
2019-11-28	第十三次正式发布。 • **功能特性**，优化部分文字内容描述。 • **服务版本差异**，优化部分文字内容描述。
2019-10-25	第十二次正式发布。 新增**个人数据保护机制**。
2019-10-14	第十一次正式发布。 • **什么是Web应用防火墙**，优化部分文字内容描述。 • **功能特性**，优化部分文字内容描述。 • **服务版本差异**，优化部分文字内容描述。 • **应用场景**，优化部分文字内容描述。
2019-05-16	第十次正式发布。 **功能特性**，优化部分文字内容描述。
2019-05-14	第九次正式发布。 • 新增**功能特性**。 • **什么是Web应用防火墙**，优化部分文字内容描述。 • **与其他云服务的关系**，优化部分文字内容描述。
2018-11-08	第八次正式发布。 设置短描述和关键字。
2018-10-29	第七次正式发布。 **什么是Web应用防火墙**，优化部分文字内容描述。
2018-04-26	第六次正式发布。 新增**WAF权限管理**。

发布日期	修改说明
2018-04-12	第五次正式发布。 **什么是Web应用防火墙**，增加防敏感信息泄露相关内容。
2018-04-02	第四次正式发布。 **什么是Web应用防火墙**，优化部分文字内容描述。
2018-03-27	第三次正式发布。 • **什么是Web应用防火墙**，增加功能介绍内容描述。 • 删除“概念”章节。
2018-01-11	第二次正式发布。 **与其他云服务的关系**，增加与云审计服务的关系描述内容。
2017-10-30	第一次正式发布。