

Web 应用防火墙

常见问题

文档版本 148
发布日期 2024-04-10



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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云计算技术有限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，华为云计算技术有限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 高频常见问题	1
2 产品咨询	3
2.1 新手入门常见问题	3
2.2 功能说明类	9
2.2.1 Web 应用防火墙是否能防护 IP?	9
2.2.2 Web 应用防火墙支持对哪些对象进行防护?	10
2.2.3 Web 应用防火墙支持自定义 POST 拦截吗?	10
2.2.4 Web 应用防火墙是否支持 IPv4 和 IPv6 共存?	11
2.2.5 WAF 和 HSS 的网页防篡改有什么区别?	12
2.2.6 Web 应用防火墙支持哪些 Web 服务框架/协议?	13
2.2.7 WAF 可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗?	13
2.2.8 WAF 转发和 Nginx 转发有什么区别?	13
2.2.9 Web 应用防火墙和云防火墙有什么区别?	14
2.2.10 Web 应用防火墙可以配置会话 Cookie 吗?	16
2.2.11 WAF 对 SQL 注入、XSS 跨站脚本和 PHP 注入攻击的检测原理?	16
2.2.12 WAF 是否可以防护 Apache Struts2 远程代码执行漏洞 (CVE-2021-31805)?	17
2.3 使用说明类	18
2.3.1 接入 WAF 后为什么漏洞扫描工具扫描出未开通的非标准端口?	18
2.3.2 多 Project 下使用 Web 应用防火墙的限制条件?	18
2.3.3 如何获取访问者真实 IP?	18
2.3.4 Web 应用防火墙切换为 Bypass 模式后会放行流量吗?	19
2.3.5 本地文件包含和远程文件包含是指什么?	19
2.3.6 QPS 和请求次数有什么区别?	20
2.3.7 Web 应用防火墙支持自定义授权策略吗?	20
2.3.8 仅放行通过 WAF 的访问请求, 如何配置?	20
2.3.9 为什么 Cookie 中有 HWWAFSESID 或 HWWAFSESTIME 字段?	21
2.3.10 云模式、独享模式可以互相切换吗?	21
2.3.11 同一防护域名/IP 可以添加到不同的账号进行防护吗?	21
2.3.12 网站部署了反向代理服务器, 如何配置 WAF?	22
2.3.13 泛域名和单域名都接入 WAF, WAF 如何转发访问请求?	22
2.4 区域与可用区	22
2.4.1 什么是区域和可用区?	22
2.4.2 Web 应用防火墙可以跨区域使用吗?	23

2.4.3 Web 应用防火墙支持防护哪些区域?	24
2.5 IPv6 配置.....	24
2.5.1 哪些版本支持 IPv6 防护?	24
2.5.2 如何测试在 WAF 中配置的源站 IP 是 IPv6 地址?	25
2.5.3 业务使用了 IPv6, WAF 中的源站地址如何配置?	25
2.5.4 WAF 如何解析/访问 IPv6 源站?	26
2.6 企业项目.....	26
2.6.1 WAF 可以跨企业项目使用吗?	26
2.6.2 购买或升级 WAF 时选择了企业项目, 其他企业项目可以使用该企业项目的 WAF 吗?	26
3 购买 WAF.....	28
3.1 同一账号可以购买多个 Web 应用防火墙吗?	28
3.2 主账号与子账号的权限有哪些区别?	28
3.3 Web 应用防火墙是否支持多个账号共享使用?	28
3.4 WAF 是如何计算域名个数的?	29
4 业务请求/规格.....	30
4.1 变更规格类.....	30
4.1.1 如何降低 Web 应用防火墙的版本和规格?	30
4.1.2 防护规则条数不够用时, 如何处理?	30
4.1.3 若流量超过 Web 应用防火墙的业务请求限制, 该如何处理?	31
4.1.4 QPS 超过当前 WAF 版本支持的峰值时有什么影响?	31
4.1.5 续费时如何变更 Web 应用防火墙的规格?	32
4.1.6 Web 应用防火墙最多可以添加多少条规则?	32
4.1.7 如何购买域名扩展包/QPS 扩展包/规则扩展包?	36
4.2 业务请求类.....	37
4.2.1 购买 WAF 时如何选择业务 QPS?	37
4.2.2 选择业务 QPS 时是按照入流量计算还是出流量计算?	38
4.2.3 WAF 对防护带宽/共享带宽有限制吗?	39
4.2.4 如何查看防护网站的入带宽和出带宽信息?	39
5 网站接入配置.....	40
5.1 域名/端口类.....	40
5.1.1 域名/IP 如何接入 Web 应用防火墙?	40
5.1.2 Web 应用防火墙支持哪些非标准端口?	42
5.1.3 独享模式如何防护不支持的非标准端口?	46
5.1.4 如何在添加域名中配置防护域名?	47
5.1.5 添加域名时, 防护网站端口需要和源站端口配置一样吗?	48
5.1.6 添加防护域名时如何配置非标准端口?	48
5.1.7 多个端口的服务器, 如果某个端口不需要 WAF 防护, 如何处理?	51
5.1.8 域名/IP 接入 WAF 前需要准备哪些数据?	51
5.1.9 删除防护域名时应该注意哪些事项?	53
5.1.10 删除防护域名后 CNAME 记录会保留多久?	54
5.1.11 域名添加到 WAF 后, 域名是否可以修改?	54

5.1.12 后端服务器配置多个源站地址时的注意事项？	54
5.1.13 Web 应用防火墙支持配置泛域名吗？	54
5.1.14 Web 应用防火墙支持防护中文域名吗？	54
5.1.15 如何使网站流量切入云模式 Web 应用防火墙？	55
5.1.16 添加域名时提示“非法的源站地址”，如何处理？	56
5.1.17 添加域名时，为什么还有域名配额却提示域名配额不足呢？	56
5.1.18 一个独享 WAF 实例可以接入多个 ELB 吗？	56
5.1.19 添加防护域名时，提示“其他人已经添加了该域名，请确认该域名是否属于你”，如何处理？	56
5.2 证书管理	56
5.2.1 为什么华为云 SCM 上的 SSL 证书在 WAF 上不能查看？	57
5.2.2 配置泛域名时，如何选择证书？	57
5.2.3 如何修改已绑定域名的证书？	57
5.2.4 ELB 已上传的证书，在 Web 应用防火墙上需要重新导入上传吗？	57
5.2.5 如何将非 PEM 格式的证书转换为 PEM 格式？	57
5.2.6 为什么非 default 企业项目不能使用华为云 SCM 推送的 SSL 证书？	58
5.2.7 添加防护域名时，为什么无法选择 SCM 证书？	58
5.3 服务器配置类	58
5.3.1 如何配置对外协议与源站协议？	59
5.3.2 添加域名时，为什么不能选择对外协议？	61
5.3.3 云模式服务器的源站地址可以配置成 CNAME 吗？	61
5.4 域名解析类	61
5.4.1 如何在华为云的云解析服务上修改 DNS 解析？	61
5.4.2 如何在华为云的云解析服务上进行 DNS 验证？	63
5.4.3 如何在华为云的云解析服务上配置 TXT 记录的值？	65
5.4.4 未配置子域名和 TXT 记录的影响？	66
5.4.5 如何查询域名提供商？	68
5.4.6 如何使用 A 记录进行域名解析？	68
5.4.7 新旧 CNAME 的区别？	68
5.5 接入后处理	69
5.5.1 域名接入 Web 应用防火墙后，能通过 IP 访问网站吗？	69
5.5.2 如何在本地测试 Web 应用防火墙？	69
5.5.3 如何设置使流量不经过 WAF，直接访问源站？	69
5.5.4 域名接入 WAF 后，为什么无法开启防护模式？	72
6 业务中断排查	73
6.1 如何排查 404/502/504 错误？	73
6.2 域名/IP 接入状态显示“未接入”，如何处理？	81
6.3 WAF 误拦截了正常访问请求，如何处理？	85
6.4 WAF 误拦截了“非法请求”访问请求，如何处理？	86
6.5 为什么误报处理不能使用了？	87
6.6 如何放行云模式 WAF 的回源 IP 段？	88
6.7 连接超时时长是多少，是否可以手动设置该时长？	92
6.8 如何解决重定向次数过多？	92

6.9 如何解决 HTTPS 请求在部分手机访问异常?	93
6.10 如何解决证书链不完整?	93
6.11 如何解决证书与密钥不匹配问题?	98
6.12 如何处理 418 错误码问题?	98
6.13 如何处理 523 错误码问题?	98
6.14 如何处理域名接入 WAF 后, 登录首页不停地刷新?	100
6.15 如何解决 HTTP 配置转发策略后程序访问页面卡顿?	100
6.16 使用 WAF 后如何处理网站的文件不能上传?	100
6.17 如何处理接入 WAF 后报错 414 Request-URI Too Large?	101
6.18 如何处理“协议不受支持, 客户端和服务端不支持一般 SSL 协议版本或加密套件”?	102
6.19 访问独享引擎页面时提示“IAM 未授权”?	103
6.20 如何解决“网站被检测到: SSL/TLS 存在 Bar Mitzvah Attack 漏洞”?	103
6.21 如何解决“源站服务器 CPU 使用率高达 100%”问题?	103
6.22 域名接入 WAF 后, 漏扫工具为什么扫不到用户真实的业务?	104
7 防护规则配置.....	106
7.1 Web 基础防护类.....	106
7.1.1 如何将 Web 基础防护的仅记录模式切换为拦截模式?	106
7.1.2 Web 基础防护支持设置哪几种防护等级?	106
7.2 CC 攻击防护规则类.....	107
7.2.1 CC 攻击的防护峰值是多少?	107
7.2.2 如何配置 CC 防护规则?	108
7.2.3 在什么情况下使用 Cookie 区分用户?	108
7.2.4 CC 规则里“限速频率”和“放行频率”的区别?	109
7.2.5 配置“人机验证”CC 防护规则后, 验证码不能刷新, 验证一直不通过, 如何处理?	109
7.3 精准访问规则类.....	111
7.3.1 精准访问防护规则可以设置在指定的时间段生效吗?	111
7.3.2 精准访问防护规则添加的路径中带有#能匹配吗?	111
7.3.3 如何不拦截带有.js 的文件?	112
7.4 IP 黑白名单类.....	112
7.4.1 Web 应用防火墙可以批量配置黑白名单吗?	112
7.4.2 Web 应用防火墙可以导入/导出黑白名单吗?	112
7.4.3 如何对异常 IP 进行封堵?	112
7.5 网站反爬虫类.....	114
7.5.1 开启 JS 脚本反爬虫后, 为什么客户端请求获取页面失败?	114
7.5.2 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗?	114
7.5.3 JS 脚本反爬虫的检测机制是怎么样的?	115
7.6 其他类.....	116
7.6.1 哪些情况会造成 WAF 配置的防护规则不生效?	116
7.6.2 如果只允许指定地区的 IP 可以访问, 如何设置防护策略?	116
7.6.3 Web 应用防火墙支持哪些工作模式和防护模式?	118
7.6.4 Web 应用防火墙支持哪些防护规则?	119
7.6.5 Web 应用防火墙的哪些防护规则支持仅记录模式?	120

7.6.6 拦截所有来源 IP 或仅允许指定 IP 访问防护网站，WAF 如何配置？	120
7.6.7 系统自动生成策略包括哪些防护规则？	125
7.6.8 开启网页防篡改后，为什么刷新页面失败？	125
7.6.9 黑白名单规则和精准访问防护规则的拦截指定 IP 访问请求，有什么差异？	126
7.6.10 如何处理 Appscan 等扫描器检测结果为 Cookie 缺失 Secure/HttpOnly？	127
8 防护日志.....	128
8.1 Web 应用防火墙支持记录防护日志吗？	128
8.2 Web 应用防火墙的日志是否可以通过 API 的方式获取？	128
8.3 如何获取拦截的数据？	128
8.4 防护事件列表中，防护动作为“不匹配”是什么意思呢？	128
8.5 WAF 获取真实 IP 是从报文中哪个字段获取到的？.....	129
8.6 Web 应用防火墙的日志可以转储到 OBS 吗？	129
8.7 Web 应用防火墙支持日志转发到 Syslog Server 吗？	129
8.8 Web 应用防火墙的防护日志可以存储多久？	129
8.9 Web 应用防火墙可以同时查询多个指定 IP 的防护事件吗？	130
8.10 Web 应用防火墙会记录未拦截的事件吗？	130
8.11 为什么 WAF 显示的流量大小与源站上显示的不一致？	130
8.12 为什么“安全总览”和全量日志统计的日志个数不一致？	131
8.13 如何处理导出的防护事件数据乱码？	131
9 WAF 与其他华为云服务同时部署.....	133
9.1 CDN+WAF 如何配置？	133
A 修订记录.....	134

1 高频常见问题

购买 WAF

- [Web应用防火墙可以跨区域使用吗？](#)
- [Web应用防火墙支持防护哪些区域？](#)
- [同一账号可以购买多个Web应用防火墙吗？](#)
- [Web应用防火墙支持自定义授权策略吗？](#)
- [域名扩展包说明](#)
- [QPS扩展包说明](#)

变更规格

- [如何降低Web应用防火墙的版本和规格？](#)
- [若流量超过Web应用防火墙的业务请求限制，该如何处理？](#)
- [续费时如何变更Web应用防火墙的规格？](#)

网站接入配置

- [域名/IP接入WAF前需要准备哪些数据？](#)
- [Web应用防火墙支持哪些非标准端口？](#)
- [域名/IP如何接入Web应用防火墙？](#)
- [如何配置对外协议与源站协议？](#)
- [添加域名时提示“非法的源站地址”，如何处理？](#)
- [域名/IP接入状态显示“未接入”，如何处理？](#)
- [域名接入WAF后，为什么无法开启防护模式？](#)
- [业务使用了IPv6，WAF中的源站地址如何配置？](#)

业务中断处理

- [使用WAF后如何处理网站的文件不能上传？](#)
- [如何排查404/502/504错误？](#)
- [连接超时时长是多少，是否可以手动设置该时长？](#)
- [如何处理523错误码问题？](#)

- [如何解决重定向次数过多？](#)
- [如何放行云模式WAF的回源IP段？](#)

防护规则

- [哪些情况会造成WAF配置的防护规则不生效？](#)
- [开启JS脚本反爬虫后，为什么客户端请求获取页面失败？](#)
- [CC规则里“限速频率”和“放行频率”的区别？](#)
- [配置“人机验证”CC防护规则后，验证码不能刷新，验证一直不通过，如何处理？](#)

防护日志

- [Web应用防火墙的防护日志可以存储多久？](#)
- [Web应用防火墙的日志可以转储到OBS吗？](#)

WAF 与其他云服务同时部署

- [CDN+WAF如何配置？](#)

2 产品咨询

2.1 新手入门常见问题

本章节为您罗列了WAF入门级的常见问题。

Web 应用防火墙是硬防火墙还是软防火墙？

Web应用防火墙是软防火墙。当您购买WAF后，只需要将域名接入WAF，就可以使用WAF防护功能。

有关域名接入WAF的详细操作，请参见[添加防护域名](#)。

接入 WAF 对现有业务和服务器运行有影响吗？

接入WAF不需要中断现有业务，不会影响源站服务器的运行状态，即不需要对源站服务站进行任何操作（例如关机或重启）。

须知

以云模式的CNAME接入方式接入WAF时，您需要修改DNS解析使流量经过WAF进行转发。修改DNS解析可能会影响网站访问业务，建议您在业务量少时进行修改。有关网站接入WAF的详细操作，请参见[域名接入配置](#)。

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

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务
- 独享模式：域名或IP，华为云的Web业务

Web 应用防护墙可以部署在 VPC 内网吗？

可以。独享版WAF的独享引擎实例部署在VPC内。

独享版 WAF 是否支持跨 VPC 防护？

如果WAF独享引擎实例与源站不在同一个VPC中，可通过[对等连接](#)打通两个VPC之间网络，但受限于网络的不稳定性，建议WAF独享引擎实例与源站在同一个VPC中。

Web 应用防火墙是否支持防护非华为云和云下服务器？

WAF云模式可以跨云使用，支持防护非华为云和云下服务器，但是该服务器必须已连接互联网。

WAF云模式是基于域名进行防护的，只要有域名就能防护，不区分云上云下服务器，也不受Region、Project和账户的影响。

Web 应用防火墙支持哪些操作系统？

Web应用防火墙部署在云端，即与操作系统没有关系。故Web应用防火墙支持任意操作系统，任意操作系统上的域名服务器都可以接入WAF做防护。

Web 应用防火墙提供的是几层防护？

Web应用防火墙提供的是七层（物理层、数据链路层、网络层、传输层、会话层、表示层和应用层）防护。

Web 应用防火墙如何拦截请求内容？

WAF对请求的首部和body体都会进行检测。例如body的表单、xml、json等数据都会被WAF检测，WAF通过检测对不符合防护规则的请求内容进行拦截。

有关WAF防护流程的详细介绍，请参见[配置引导](#)。

Web 应用防火墙是否支持文件缓存？

WAF只缓存配置了网页防篡改的静态网页，用于将缓存的未被篡改的网页返回给Web访问者，以达到防篡改的目的。

如果您需要缓存所有的网站内容，可以选择部署CDN，WAF部署在CDN和源站之间，具体的配置方式请参见[同时部署CDN和WAF的配置指导](#)。

WAF 会缓存网站数据吗？

WAF的网页防篡改功能，可以为用户提供应用层的防护，只对网站的静态网页进行缓存，当用户访问网站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。

WAF不会缓存网站数据。如果你需要绑在网站内容，可以使用[CDN](#)，或者同时部署WAF和CDN。

有关同时部署CDN和WAF的详细介绍，请参见[“CDN+WAF”联动提升网站防护能力和访问速度](#)。

Web 应用防火墙是否支持健康检查？

WAF目前暂不支持健康检查的功能，如果您希望服务器有健康性检查的功能，建议您将弹性负载均衡（ELB）和WAF搭配使用，ELB配置完成后，再将ELB的EIP作为服务器的IP地址，接入WAF，实现健康检查。

Web 应用防火墙是否支持 SSL 双向认证？

不支持。您可以在WAF上配置单向的SSL证书。

📖 说明

添加防护网站时，如果“对外协议”使用了HTTPS协议，您需要上传证书使证书绑定到防护网站。

建议您使用ELB+独享WAF的模式，在ELB上配置双向认证，具体的操作如下：

1. [购买WAF独享模式](#)。
2. 将网站接入WAF并配置负载均衡（ELB），具体请参见[网站接入流程（独享模式）](#)。
3. 在ELB上配置双向认证，具体请参见[HTTPS双向认证](#)。

Web 应用防火墙支持基于应用层协议和内容的访问控制吗？

WAF支持应用层协议和内容的访问控制，应用层协议支持HTTP和HTTPS。

Web 应用防火墙是否可以对用户添加的 Post 的 body 进行检查？

WAF的内置检测会检查Post数据，webshell是Post提交的文件。Post类型提交的表单、json等数据，都会被WAF的默认策略检查。

您可以通过配置精准访问防护规则，对添加的Post的body进行检查。有关配置精准访问防护规则的详细操作，请参见[配置精准访问防护规则](#)。

Web 应用防火墙可以限制域名访问速度吗？

不支持。WAF支持通过自定义CC防护规则，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。

有关CC防护规则的详细介绍，请参见[配置CC攻击防护规则](#)。

Web 应用防火墙支持拦截包含特殊字符的 URL 请求吗？

WAF不支持将拦截请求URL中含有特殊字符作为拦截条件，即URL请求中有特殊字符，WAF不会拦截。WAF可以对来源IP进行检测和限制。

Web 应用防火墙可以防止垃圾注册和恶意注册吗？

WAF不能防止垃圾注册和恶意注册等业务层面攻击行为。建议您在网站配置注册验证机制，以防止垃圾注册和恶意注册。

WAF通过对HTTP(S)请求进行检测，可以识别并阻断Web服务的网络攻击（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）。

Web 应用防火墙可以拦截 Web 页面调用其他接口的请求数据吗？

当Web页面调用其他接口的请求数据在WAF防护域名内时，该请求数据将经过WAF，WAF会检测并阻断该请求数据。

如果Web页面调用其他接口的请求数据不在WAF防护域名内，则该请求数据不经过WAF，WAF不会拦截该请求数据。

Web 应用防火墙可以设置域名限制访问吗？

WAF不能直接通过域名限制访问。WAF支持配置黑白名单规则（即设置IP黑/白名单），阻断、仅记录或放行指定IP或IP段的访问请求。

您可以通过配置黑白名单规则，阻断、仅记录或放行域名对应的IP或IP段的访问请求。

Web 应用防火墙有 IPS 入侵防御系统模块吗？

Web应用防火墙没有传统防火墙的IPS模块，不支持IPS入侵防御，仅支持对HTTP/HTTPS协议的入侵检测。

WAF 支持弹性伸缩功能吗？

WAF暂不支持弹性伸缩功能。

WAF支持云模式和独享模式，请根据您的业务需求和资源，选择WAF模式。

HTTP 2.0 业务接入 WAF 防护是否会对源站有影响？

HTTP 2.0业务接入WAF防护对源站有影响。HTTP 2.0业务接入WAF防护表示WAF可以处理客户端的HTTP 2.0请求，而WAF目前仅支持以HTTP 1.0/1.1协议转发回源请求，即WAF与源站间暂不支持HTTP 2.0。因此，如果您将HTTP 2.0业务接入WAF防护，则源站的HTTP 2.0特性将会受到影响，例如，源站HTTP 2.0的多路复用特性可能失效，造成源站业务请求量上升。

WAF 中的防 SQL 注入攻击和 DBSS 中的 SQL 注入的区别？

WAF支持对SQL注入攻击进行防护，防止恶意SQL命令的执行。具体的防护检测原理参见[WAF针对SQL注入攻击的检测原理](#)。

数据库安全审计(DBSS)提供SQL注入库，可以基于SQL命令特征或风险等级，发现数据库异常行为立即告警。

使用 Web 应用防火墙对邮件收发和邮件端口有影响吗？

WAF是对Web应用网页进行防护，当您的网站接入WAF后，对邮件收发和邮件端口不会产生影响。

在安全组中配置 WAF 白名单，需要开放所有端口吗？

可以开放所有端口。为了降低网络安全风险，建议只开放80和443端口。

什么是并发数？

并发数指系统能够同时处理请求的数目。对于网站而言，并发数即网站并发用户数，指同时提交请求的用户数目。

WAF对QPS有限制，各版本支持的QPS和业务带宽说明，请参见[服务版本差异](#)。

如果证书挂载在 ELB 上，WAF 可以根据请求内容进行拦截吗？

如果证书挂载在ELB上，通过WAF的请求都是加密的。对于HTTPS的业务，您必须将证书上传到WAF上，WAF才能根据解密之后的请求判断是否进行拦截。

源站 IP 地址服务器更换安全组后，在 WAF 中需要做更改吗？

添加到WAF的网站的源站IP地址服务器更换安全组后，在WAF中不需要做任何操作，但是需要在源站放行WAF的回源IP或者实例IP。

不同WAF模式的操作方法如下：

- 云模式：[放行WAF回源IP](#)。
- 独享模式：[放行独享引擎回源IP](#)。

WAF 配置多个源站时如何负载？

如果您配置了多个源站IP地址，WAF默认使用加权轮询的方式对访问请求进行负载均衡。您也可以根据需求自定义负载均衡算法。更多信息，请参见[修改负载均衡算法](#)。

源站开启 gzip 对 WAF 有影响吗？

如果源站开启gzip，WAF可能误拦截源站正常访问请求。如果确认拦截的为正常访问请求，您可以参照[处理误报事件](#)将该事件处理为误报事件。处理后，WAF将不再拦截该事件，即“防护事件”页面中将不再显示该攻击事件，您也不会收到该攻击事件的告警通知。

使用 WAF 是否影响内网向外发送数据？

使用WAF不会影响内网机器向外发送数据。以云模式的CNAME方式或独享模式将网站成功接入WAF后，WAF对网站的HTTP(S)请求进行检测，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。

多个域名对应同一源站，Web 应用防火墙可以防护这些域名吗？

可以。不同域名对应同一个源站时，您可以将这些域名都接入WAF进行防护。

WAF的防护对象是域名或IP，如果是多个域名使用了同一个EIP对外提供服务，必须将多个域名都接入WAF才能对所有域名进行防护。

什么是防护 IP？

防护IP是指需要保护的网站的IP地址。

云模式 WAF 提供的解析地址是固定 IP 吗？

将域名通过云模式添加到WAF后，WAF会随机分配一个CNAME值给域名，用作域名解析，该CNAME值是WAF IP池内随机分配的，不是固定的。

源站 IP 更改后是否会改变 CNAME 值？

通过云模式WAF接入网站，源站IP更改后，不会改变WAF分配给该网站的CNAME值。

更换 IP 后，需要重新将域名添加到 WAF 吗？

如果网站所在的IP没有发生变化则无需重新在WAF中重新配置，如果网站解析到了新IP则需要重新配置。

WAF 需要绑定 EIP 吗？

WAF云模式无需绑定EIP，独享WAF需要和七层的独享型ELB进行联动，ELB需要有公网IP地址作为业务地址。详细的操作请参见[为弹性负载均衡绑定弹性公网IP](#)。

Web 应用防火墙支持漏洞检测吗？

WAF的网站反爬虫防护功能可以对第三方漏洞攻击等威胁进行检测和拦截。在配置网站反爬虫防护规则时，如果您开启了扫描器，WAF将对扫描器爬虫，如OpenVAS、Nmap等进行检测。

有关网站反爬虫防护规则的详细操作，请参见[配置网站反爬虫防护规则](#)。

Web 应用防火墙是否支持 Exchange 里的相关协议？

WAF支持exchange里登录网页webmail时的http和https协议；WAF不支持exchange里的SMTP、POP3、IMAP等邮件相关的协议。

Web 应用防火墙是否支持防御 XOR 注入攻击？

Web应用防火墙支持防御XOR注入。

为什么域名接入 WAF 后，有的攻击场景还是触发不了拦截呢？

大概率是因为客户没有开启Web基础防护的header全检测。在header自定义字段中携带攻击载荷，“header全检测”必须开启拦截模式，才可以拦截此类攻击。具体的操作请参见[配置Web基础防护规则](#)。

如何理解 WAF 日志里的 bind_ip 参数？

网站接入WAF后，WAF作为反向代理存在客户端与源站服务器之间，检测过滤恶意攻击流量，用bind_ip（WAF的回源IP）将正常的流量转发传输到源站。参考[如何放行云模式WAF的回源IP段？](#) 查看WAF的回源IP并放行回源IP。

通过 IP 接入 WAF 后，WAF 可以防护映射到这个 IP 的所有域名吗？

不支持。

WAF的独享模式支持源站IP接入WAF防护，且该IP支持私网IP或者内网IP，但WAF仅防护通过IP访问的流量，不能防护映射到这个IP的域名，如需防护域名，需要单独将域名接入WAF进行防护。

如果业务超时数据较多，如何处理？

云模式WAF为多租共享，随着其他客户业务的增长，可能会影响业务转发的时延，如果您对时延要求严格，建议您使用WAF的独享模式，该模式不会因其他客户业务增长而受到影响。

WAF 是否支持 HTTP/3 协议吗？

目前WAF最高支持HTTP/2协议，还不支持HTTP/3协议。

WAF 是否支持防护 CS 架构的网站？

如果该网站的CS架构是七层HTTP/HTTPS协议，则WAF可以防护，否则不支持防护。

WAF 云模式是否能防护其他账号下的域名？

可以。WAF云模式的防护对象是域名，只需要将该域名在当前账号下添加到WAF云模式中进行防护即可。

如何查看当前 WAF 业务 QPS 的使用情况和流入的流量？

您可以在源站上，查看源站IP地址的带宽/QPS使用情况流入的流量。

Web 应用防火墙可以拦截 multipart/form-data 格式的数据包吗？

WAF支持拦截multipart/form-data格式的数据包。

Multipart/form-data是浏览器使用表单上传文件的方式。例如，在写邮件时，如果邮件添加了附件，附件通常使用multipart/form-data格式上传到服务器。

Web 应用防火墙支持跨域禁止访问功能吗？

WAF不支持配置跨域禁止访问功能。有关WAF功能的详细介绍，请参见[功能特性](#)。

WAF 支持防御哪些 CVE 漏洞？

WAF支持防御的CVE漏洞：CVE-2017-7525、CVE-2019-17571、CVE-2018-1270、CVE-2016-1000027、CVE-2022-22965、CVE-2022-22968、CVE-2018-20318。

2.2 功能说明类

2.2.1 Web 应用防火墙是否能防护 IP？

WAF可以对IP进行防护。

云模式-CNAME 接入

WAF不能防护IP，只能基于域名进行防护。

在WAF中配置的源站IP只支持公网IP，不支持私网IP或者内网IP。

若您需要减少公网IP的数量，可以购买ELB（Elastic Load Balance，简称ELB）搭建负载均衡，代理后端私网IP，并将EIP（公网IP）设置为源站地址。

独享模式/云模式-ELB 接入

WAF可以对IP或域名进行防护。

在WAF中配置的源站IP支持私网IP或者内网IP。

有关域名接入WAF的流程说明，请参见[域名/IP如何接入Web应用防火墙？](#)。

2.2.2 Web 应用防火墙支持对哪些对象进行防护？

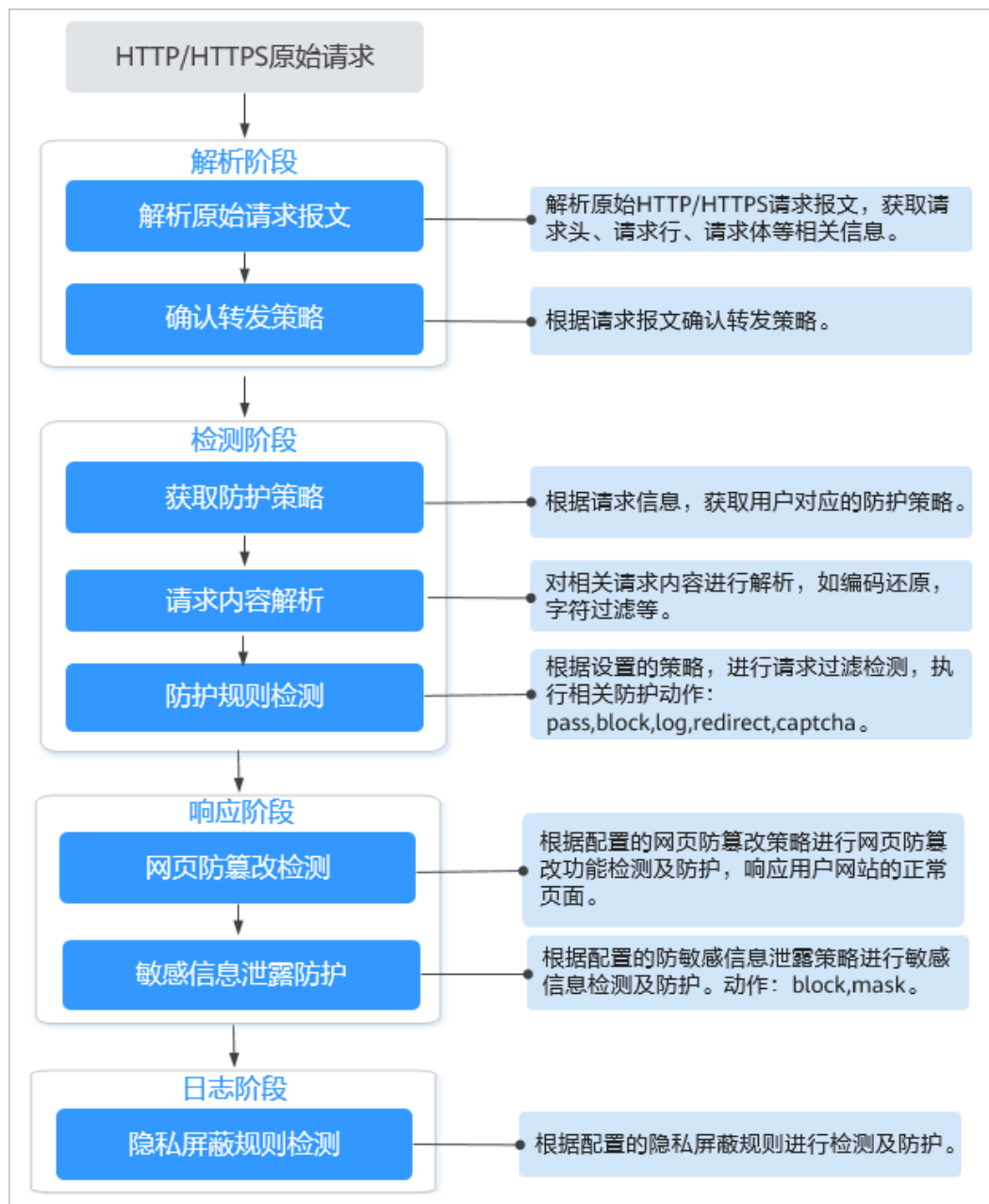
WAF支持对域名或IP进行防护，相关说明如下：

- 云模式的CNAME接入只能基于域名进行防护
在WAF中配置的源站IP只支持公网IP。例如，源站服务器部署了华为云弹性负载均衡（Elastic Load Balance，简称ELB）时，只要ELB（经典型、共享型或独享型）有公网IP，云模式就可以对域名进行防护。
- 独享模式和云模式的ELB接入可以对域名或IP进行防护

2.2.3 Web 应用防火墙支持自定义 POST 拦截吗？

WAF不支持自定义POST拦截。针对HTTP/HTTPS原始请求，WAF引擎内置防护规则的检测流程如[图2-1](#)所示。

图 2-1 WAF 引擎检测图



有关WAF防护流程的详细介绍，请参见[配置引导](#)。

2.2.4 Web 应用防火墙是否支持 IPv4 和 IPv6 共存？

WAF支持IPv4和IPv6共存，针对同一域名可以同时提供IPv6和IPv4的流量防护。

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考[功能总览](#)。

须知

仅云模式专业版和铂金版支持IPv6防护。

2.2.5 WAF 和 HSS 的网页防篡改有什么区别？

HSS网页防篡改版是专业的锁定文件不被修改，实时监控网站目录，并可以通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，是政府、院校及企业等组织必备的安全服务。

WAF网页防篡改为用户提供应用层的防护，对网站的静态网页进行缓存，当用户访问网站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。

网页防篡改的区别

HSS与WAF网页防篡改的区别，如表2-1所示。

表 2-1 HSS 和 WAF 网页防篡改的区别

类别	HSS	WAF
静态网页	锁定驱动级文件目录、Web文件目录下的文件，禁止攻击者修改。	缓存服务端静态网页
动态网页	<ul style="list-style-type: none">动态数据防篡改 提供tomcat应用运行时自我保护，能够检测针对数据库等动态数据的篡改行为。特权进程管理 配置特权进程白名单后，网页防篡改功能将主动放行可信任的进程，确保正常业务进程的运行。	不支持
备份恢复	<ul style="list-style-type: none">主动备份恢复 若检测到防护目录下的文件被篡改时，将立即使用本地主机备份文件自动恢复被非法篡改的文件。远端备份恢复 若本地主机上的文件目录和备份目录失效，可通过远端备份服务恢复被篡改的网页。	不支持
防护对象	网站防护要求高，手动恢复篡改能力差	网站防护要求低，仅需要对应用层进行防护

如何选择网页防篡改

防护对象	选择网页防篡改
普通网站	WAF网页防篡改+HSS企业版

防护对象	选择网页防篡改
网站防护+高要求网页防篡改	WAF网页防篡改+HSS网页防篡改

2.2.6 Web 应用防火墙支持哪些 Web 服务框架/协议？

Web应用防火墙部署在云端，与Web服务框架没有关系。

WAF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。

WAF支持防护的协议类型说明如下：

- WebSocket/WebSockets协议，且默认为开启状态
 - “对外协议”选择“HTTP”时，默认支持WebSocket
 - “对外协议”选择“HTTPS”时，默认支持WebSockets
- HTTP/HTTPS协议

2.2.7 WAF 可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗？

可以。WAF支持防护HTTP/HTTPS协议业务。

- 网站选择使用HSTS（HTTP Strict Transport Security，HTTP严格传输安全协议）策略后，会强制要求客户端（如浏览器）使用HTTPS协议与网站进行通信，以减少会话劫持风险。配置HSTS策略的网站使用的是HTTPS协议，WAF可以防护。
- NTLM（New Technology LAN Manager，Windows NT LAN管理器）代理是Windows平台下HTTP代理的一种认证方式，其认证方式与Windows远程登录的认证方式是一样的，客户端（如浏览器）和代理之前需要三次握手才开始传递信息。

对于客户端（如浏览器）和代理之前使用NTLM认证的业务，WAF可以防护。

2.2.8 WAF 转发和 Nginx 转发有什么区别？

WAF转发和Nginx转发的主要区别为Nginx是直接转发访问请求到源站服务器，而WAF会先检测并过滤恶意流量，再将过滤后的访问请求转发到源站服务器，详细说明如下：

- WAF转发
网站接入WAF后，所有访问请求将先经过WAF，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流量后，将正常流量返回给源站，从而确保Web应用安全、稳定、可用。

图 2-2 防护原理



- Nginx转发

即反向代理（Reverse Proxy）方式转发。反向代理服务器接受客户端访问请求后，直接将访问请求转发给Web服务器，并将从Web服务器上获取的结果返回给客户端。反向代理服务器安装在网站机房，代理Web服务器接收访问请求，并对访问请求进行转发。

反向代理可以防止外网对内网服务器的恶性攻击，缓存以减少内网服务器压力，还可以实现访问安全控制和负载均衡。

图 2-3 Nginx 转发原理



2.2.9 Web 应用防火墙和云防火墙有什么区别？

Web应用防火墙和云防火墙是华为云推出的两款不同的产品，分别针对您的Web服务，互联网边界和VPC边界的流量进行防护。

WAF和CFW的主要区别说明如[表2-2](#)所示。

表 2-2 WAF 和 CFW 的主要区别说明

类别	Web应用防火墙	云防火墙
定义	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。	云防火墙（Cloud Firewall, CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。
防护机制	网站成功接入WAF后，WAF作为一个反向代理存在于客户端和服务端之间，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。	CFW可对全流量进行精细化管控，包括互联网边界防护，跨VPC，跨VM的流量，防止外部入侵、内部渗透攻击和从内到外的非法访问。
部署模式	WAF支持云模式、独享模式和ELB模式。 <ul style="list-style-type: none"> ● 云模式-CNAME接入：业务服务器部署在华为云、非华为云或线下，且防护对象为域名。各服务版本推荐使用的场景说明如下： <ul style="list-style-type: none"> - 标准版 中小型网站，对业务没有特殊的安全需求 - 专业版 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 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 ● 云模式-ELB接入：业务服务器部署在华为云，防护对象为域名或IP。大型企业网站，对业务稳定性有较高要求的安全防护需求。 ● 独享模式：业务服务器部署在华为云，防护对象为域名或IP。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。 	互联网边界和VPC边界

类别	Web应用防火墙	云防火墙
防护对象	<ul style="list-style-type: none">云模式-CNAME接入：域名。独享模式/云模式-ELB接入：域名或IP。	弹性公网IP
功能特性	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防护。	<ul style="list-style-type: none">资产管理与入侵防御：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。访问控制：支持互联网边界访问流量的访问控制。流量分析与日志审计：VPC间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。

2.2.10 Web 应用防火墙可以配置会话 Cookie 吗？

WAF不支持配置会话Cookie。

WAF可以通过配置CC攻击防护规则，限制单个Cookie字段特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击。例如，您可以通过配置CC攻击规则，使Cookie标识为name的用户在60秒内访问域名的“/admin*”页面超过10次时，封禁该用户访问域名600秒。

有关配置CC攻击防护规则的详细操作，请参见[配置CC攻击防护规则](#)。

什么是 Cookie

Cookie是网站为了辨别用户身份，进行Session跟踪而储存在用户本地终端上的数据（通常经过加密），Cookie由Web服务器发送到浏览器，可以用来记录用户个人信息。

Cookie由一个名称（Name）、一个值（Value）和其它几个用于控制Cookie有效期、安全性、使用范围的可选属性组成。Cookie分为会话Cookie和持久性Cookie两种类型，详细说明如下：

- 会话Cookie
临时的Cookie，不包含到期日期，存储在内存中。当浏览器关闭时，Cookie将被删除。
- 持久性Cookie
包含到期日期，存储在磁盘中，当到达指定的到期日期时，Cookie将从磁盘中被删除。

2.2.11 WAF 对 SQL 注入、XSS 跨站脚本和 PHP 注入攻击的检测原理？

SQL（Structured Query Language）注入攻击是一种常见的Web攻击方法，攻击者通过把SQL命令注入到数据库的查询字符串中，最终达到欺骗服务器执行恶意SQL命令的

目的。例如，可以从数据库获取敏感信息，或者利用数据库的特性执行添加用户、导出文件等一系列恶意操作，甚至有可能获取数据库乃至系统用户最高权限。

XSS攻击通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、VBScript、ActiveX、Flash 或者甚至是普通的HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和Cookie等各种内容。

WAF 针对 SQL 注入攻击的检测原理

WAF针对SQL注入攻击的检测原理是检测SQL关键字、特殊符号、运算符、操作符、注释符的相关组合特征，并进行匹配。

- SQL关键字（如 union, Select, from, as, asc, desc, order by, sort, and , or, load, delete, update, execute, count, top, between, declare, distinct, distinctrow, sleep, waitfor, delay, having, sysdate, when, dba_user, case, delay 等）
- 特殊符号（' " ; ()）
- 运算符（±*/%|）
- 操作符（=, >, <, >=, <=, !=, +=, -=）
- 注释符（-, /**/）

WAF 针对 XSS 攻击的检测原理

WAF对XSS跨站脚本攻击的检测原理主要是针对HTML脚本标签、事件处理器、脚本协议、样式等进行检测，防止恶意用户通过客户端请求注入恶意XSS语句。

- XSS关键字（javascript、script、object、style、iframe、body、input、form、onerror、alert等）；
- 特殊字符（<、>、'、"）；
- 外部链接（href="http://xxx/"，src="http://xxx/attack.js"）。

📖 说明

如果业务需要上传富文本，可以用multipart方式上传，不用body方式上传，放在表单里，即使base64编码也会解码。分析业务场景，建议限制引号、尖括号输入。

WAF 针对 PHP 攻击的检测原理

如果请求中包含类似于system(xx) 关键字，该关键字具有PHP注入攻击风险，因此，WAF会拦截了该类请求。

2.2.12 WAF 是否可以防护 Apache Struts2 远程代码执行漏洞（CVE-2021-31805）？

WAF的Web基础防护规则可以防护Apache Struts2远程代码执行漏洞（CVE-2021-31805）。

配置方法

- 步骤1 [购买WAF](#)。

步骤2 将网站域名添加到WAF中并完成域名接入，详细操作请参见[添加防护域名](#)。

步骤3 将Web基础防护的状态设置为“拦截”模式，详细操作请参见[配置Web基础防护规则](#)。

----结束

2.3 使用说明类

2.3.1 接入 WAF 后为什么漏洞扫描工具扫描出未开通的非标准端口？

问题现象

域名接入WAF通过第三方漏洞扫描工具扫描后，扫描结果显示了域名的标准端口（例如443）和非标准端口（例如8000、8443等）。

可能原因

由于WAF的非标准端口引擎是所有用户间共享的，即通过第三方漏洞扫描工具可以检测到所有已在WAF中使用的非标准端口。域名的端口检测，应以源站IP开通的端口为准，即引擎的端口检测并不影响源站的使用安全，且WAF保证客户解析CNAME返回的引擎IP的安全性。

处理建议

无需处理

2.3.2 多 Project 下使用 Web 应用防火墙的限制条件？

各Project是相互独立的，创建的策略、证书都不可互用。

- 策略不可互用，例如，主Project创建的policy A，则子Project创建的规则都不能属于policy A，只能单独创建策略。
- 证书不可互用，主Project和子Project创建的证书无法相互推送，则只能使用各自Project创建的证书。

2.3.3 如何获取访问者真实 IP？

网站接入WAF后，WAF作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

通常情况下，网站访问并不是简单地从用户的浏览器直达服务器，中间可能部署有CDN、WAF、高防。例如，采用这样的架构：“用户 > CDN/WAF/高防 > 源站服务器”。那么，在经过多层代理之后，服务器如何获取发起请求的真实客户端IP呢？

一个透明的代理服务器在把用户的HTTP请求转到下一环节的服务器时，会在HTTP的头部中加入一条“X-Forwarded-For”记录，用来记录用户的真实IP，其形式为“X-Forwarded-For: 访问者的真实IP, 代理服务器1-IP, 代理服务器2-IP, 代理服务器3-IP, ……”。

因此，访问者的真实IP可以通过获取“X-Forwarded-For”对应的第一个IP来得到。

可参考最佳实践[获取访问者真实IP](#)。

2.3.4 Web 应用防火墙切换为 Bypass 模式后会放行流量吗？

WAF云模式下，防护的“工作模式”切换为“Bypass”后，该域名的请求直接到达其后端服务器，不再经过WAF。

只有出现以下情况，才能将“工作模式”切换为“Bypass”：


- 当有测试等特殊场景，需要将业务恢复到没有接入WAF的状态，可以通过Bypass功能切换。
- 排查网站异常，例如报502、504或其他不兼容等问题。
- 在Web应用防火墙前面未使用代理。


Bypass 模式生效时间

当您将“工作模式”切换为“Bypass”后，等待约3~5分钟后，Bypass模式生效。

切换为 Bypass 模式

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。


步骤5 在目标域名所在行的“工作模式”列，单击 ，选择“Bypass”。

图 2-4 切换工作模式



---结束

2.3.5 本地文件包含和远程文件包含是指什么？

您可以在WAF的防护事件中查看文件包含等安全事件，快速定位攻击源或对攻击事件进行分析。

文件包含是指程序开发人员一般会把重复使用的函数写到单个文件中，需要使用某个函数时直接调用此文件，而无需再次编写，这种文件调用的过程一般被称为文件包含。文件包含分为本地文件包含和远程文件包含，说明如下：

- 当被包含的文件在服务器本地时，称为本地文件包含。
- 当被包含的文件在第三方服务器时，称为远程文件包含。

文件包含漏洞是指通过函数包含文件时，由于没有对包含的文件名进行有效的过滤处理，被攻击者利用从而导致了包含了Web根目录以外的文件进来，导致文件信息的泄露甚至注入了恶意代码。

有关查看防护日志的详细操作，请参见[查看防护日志](#)。

2.3.6 QPS 和请求次数有什么区别？

QPS (Queries Per Second) 即每秒钟的请求量，例如一个HTTP GET请求就是一个Query。请求次数是间隔时间内请求的总量。

QPS是单个进程每秒请求服务器的成功次数。

📖 说明

QPS = 请求数/秒 (req/sec)

“安全总览”页面中QPS的计算方式说明如[表2-3](#)所示。

表 2-3 QPS 取值说明

时间段	QPS平均取值说明	QPS峰值取值说明
“昨天”、“今天”	间隔1分钟，取1分钟内的平均值	间隔1分钟，取1分钟内的最大值
“3天”	间隔5分钟，取5分钟内的平均值	间隔5分钟，取5分钟内的最大值
“7天”	间隔10分钟，取每5分钟内平均值的最大值	间隔10分钟，取10分钟内最大值
“30天”	间隔1小时，取每5分钟内平均值的最大值	间隔1小时，取1小时内最大值

WAF各版本支持的QPS指标说明，请参见[服务版本差异](#)。

2.3.7 Web 应用防火墙支持自定义授权策略吗？

WAF支持自定义授权策略，通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用WAF资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将WAF资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

有关创建WAF权限策略的详细介绍，请参见[创建用户组并授权使用WAF](#)。

2.3.8 仅放行通过 WAF 的访问请求，如何配置？

您可以在源站服务器上配置只放行WAF回源IP的访问控制策略，即仅允许通过WAF的请求访问到源站，防止黑客获取源站IP后绕过WAF直接攻击源站，以确保源站安全、稳定、可用。

放行WAF回源IP的访问控制策略操作说明如下：

- 源站服务器配置放行WAF回源IP的访问控制策略。
 - 云模式：请参见[如何放行云模式WAF的回源IP段？](#)。
 - 独享模式：请参见[放行独享引擎回源IP](#)。
- 建议您关闭防火墙和服务器安全防护软件。

2.3.9 为什么 Cookie 中有 HWWAFSESID 或 HWWAFSESTIME 字段？

HWWAFSESID：会话ID；HWWAFSESTIME：会话时间戳，这两个字段用于标记请求，如CC防护规则中用户计数。

防护域名/IP接入WAF后，WAF会在客户请求Cookie中插入HWWAFSESID（会话ID），HWWAFSESTIME（会话时间戳）等字段，这些字段服务于WAF统计和安全特性，不插入这些字段将会影响CC人机验证、攻击惩罚、动态反爬虫的功能使用。

2.3.10 云模式、独享模式可以互相切换吗？

不能直接切换。添加防护域名/IP时，您需要根据业务实际情况，选择部署模式：云模式-CNAME接入、云模式-ELB接入或独享模式。防护域名添加到WAF后，部署模式不能切换。

如果您需要更换防护域名/IP的部署模式，请确保业务已部署到对应模式。在WAF的网站配置列中删除添加的防护域名/IP后，再以对应的部署方式重新添加该防护域名/IP，完成部署模式切换。例如，“www.example.com”防护域名以云模式添加到WAF，如果您希望“www.example.com”切换到独享模式，请先确保当前业务支持独享模式部署方式，申请独享模式后，您需要先删除“www.example.com”防护域名，然后再重新以独享模式方式重新添加“www.example.com”防护域名。

须知

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

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务
- 独享模式：域名或IP，华为云的Web业务

2.3.11 同一防护域名/IP 可以添加到不同的账号进行防护吗？

当防护域名以云模式添加到WAF时，不能再重复添加该防护域名进行防护。因此，同一防护域名不能添加到不同的账号进行防护。

当防护域名/IP以独享模式或云模式的ELB接入添加到WAF时，可以添加到不同的账号进行防护。

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

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务

- 独享模式：域名或IP，华为云的Web业务

须知

同一个域名/IP对应不同端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个防护配额。如果您需要防护同一域名/IP的多个端口，您需要将该域名/IP和端口逐一添加到WAF。

2.3.12 网站部署了反向代理服务器，如何配置 WAF？

如果网站部署了反向代理服务器，网站接入WAF后不会影响反向代理服务器。以云模式的CNAME接入将网站接入WAF后，WAF作为一个反向代理部署在客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

防护域名/IP接入WAF的操作流程请参见[域名/IP如何接入Web应用防火墙？](#)。

2.3.13 泛域名和单域名都接入 WAF，WAF 如何转发访问请求？

单域名和泛域名都接入WAF后，WAF优先将防护网站的访问请求转发到单域名，如果不能识别单域名，访问请求将转发到泛域名。

例如，单域名a.example.com和泛域名*.example.com接入WAF，访问请求将优先通过单域名a.example.com进行转发。

泛域名配置说明如下：

- 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。
- 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。

2.4 区域与可用区

2.4.1 什么是区域和可用区？

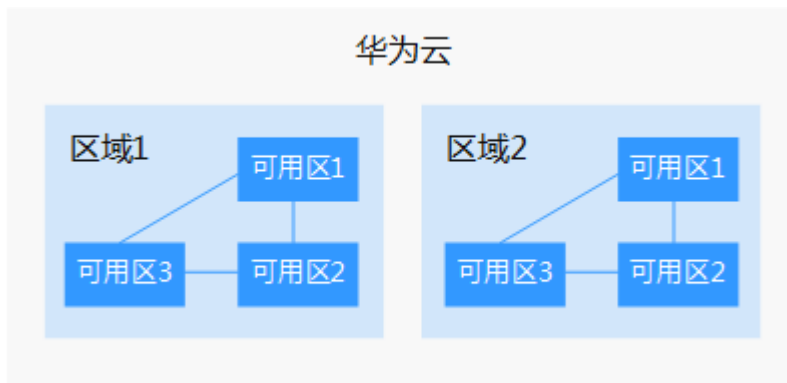
什么是区域、可用区？

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图2-5阐明了区域和可用区之间的关系。

图 2-5 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域？

选择区域时，您需要考虑以下几个因素：

- 地理位置
 - 一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。
 - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
 - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
 - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。
- 资源的价格
 - 不同区域的资源价格可能有差异，请参见[华为云服务价格详情](#)。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅[地区和终端节点](#)。

2.4.2 Web 应用防火墙可以跨区域使用吗？

原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。

例如，如果买一个WAF能同时覆盖不同地域的业务（如北京和上海），但是若购买北京region的WAF，对于客户在上海的业务，可能转发时长相比于北京的业务会更长。为了提高转发效率，建议您购买2个WAF（北京region的WAF和上海region的WAF），分别防护北京和上海的业务。

2.4.3 Web 应用防火墙支持防护哪些区域？

Web应用防火墙支持防护所有区域。

须知

- 购买WAF后，区域不能修改。如果您需要修改购买WAF的区域，您可以退订后重新购买。
- 同一账号在同一个大区域（例如，华东区域（华东-上海一、华东-上海二））只能购买一个服务版本。

购买 WAF 时如何选择区域

原则上，在任何一个区域购买的WAF支持防护所有区域的Web业务。但是为了提高WAF的转发效率，建议您在购买WAF时，根据防护业务的所在区域就近选择购买的WAF区域。

例如，如果您只购买了北京region的WAF，需要同时覆盖不同地域的业务（如北京和上海），对于客户在上海的业务，可能转发时长相比于北京的业务会更长。为了提高转发效率，建议您购买2个WAF（北京region的WAF和上海region的WAF），分别防护北京和上海的业务。

2.5 IPv6 配置

2.5.1 哪些版本支持 IPv6 防护？

WAF支持IPv6防护，详细说明如下：

- 云模式的CNAME接入的专业版和铂金版支持IPv6的防护。
- 独享模式/云模式-ELB接入没有公网IP，公网IP绑定在ELB的弹性公网IP上，如果独享模式/模式-ELB接入所在的ELB支持IPv6，那么独享模式/模式-ELB接入也支持IPv6。

须知

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考[功能总览](#)。

2.5.2 如何测试在 WAF 中配置的源站 IP 是 IPv6 地址？

执行此操作前，请确认已在WAF中添加了域名并完成了域名接入。

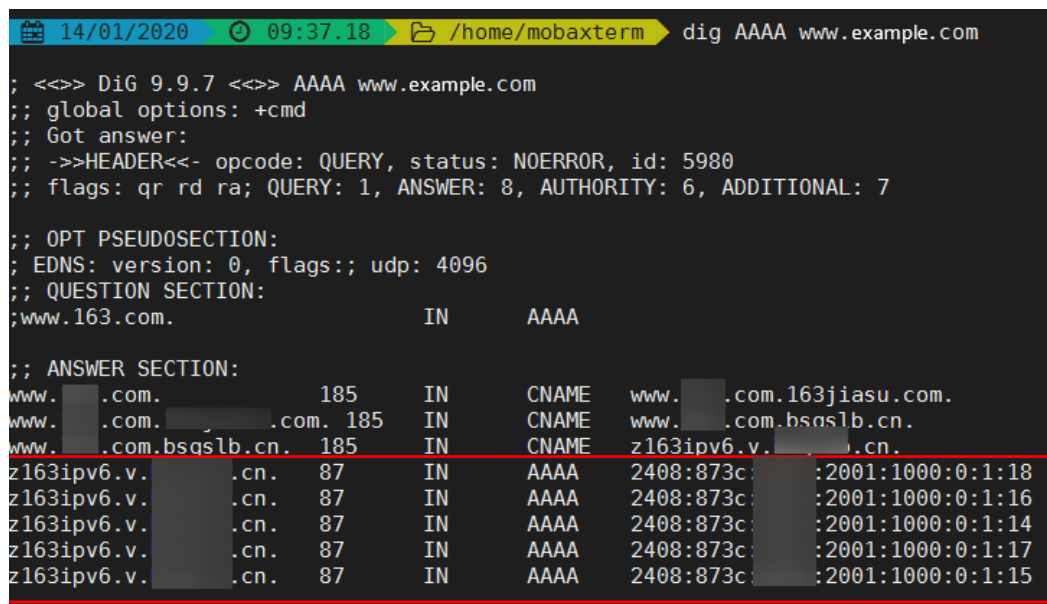
假如已在WAF中添加域名www.example.com。通过以下方法可以测试配置的源站IP是否是IPv6地址：

步骤1 在Windows中打开cmd命令行工具。

步骤2 执行dig AAAA www.example.com命令。

若返回的结果里有IPv6格式的IP地址，如图2-6所示，则证明配置的源站IP是IPv6地址。

图 2-6 测试结果



```
14/01/2020 09:37.18 /home/mobaxterm dig AAAA www.example.com
; <<>> DiG 9.9.7 <<>> AAAA www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5980
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 6, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;www.163.com.                IN      AAAA

;; ANSWER SECTION:
www.163.com.                 185     IN      CNAME   www.163jiasu.com.
www.163.com.                 185     IN      CNAME   www.163bsqslb.cn.
www.163.com.bsqslb.cn.      185     IN      CNAME   z163ipv6.vip.163.com.cn.
z163ipv6.vip.163.com.cn.    87      IN      AAAA    2408:873c:163:163::2001:1000:0:1:18
z163ipv6.vip.163.com.cn.    87      IN      AAAA    2408:873c:163:163::2001:1000:0:1:16
z163ipv6.vip.163.com.cn.    87      IN      AAAA    2408:873c:163:163::2001:1000:0:1:14
z163ipv6.vip.163.com.cn.    87      IN      AAAA    2408:873c:163:163::2001:1000:0:1:17
z163ipv6.vip.163.com.cn.    87      IN      AAAA    2408:873c:163:163::2001:1000:0:1:15

---结束
```

---结束

2.5.3 业务使用了 IPv6，WAF 中的源站地址如何配置？

如果域名已接入了WAF（源站地址配置为IPv4地址）进行防护，当业务开启了IPv6时，WAF中配置的源站地址可以保持原IPv4地址，也可以修改为IPv6地址。

WAF支持IPv6/IPv4双栈模式和NAT64机制，详细说明如下：

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考[功能总览](#)。

须知

仅专业版和铂金版支持IPv6防护。

2.5.4 WAF 如何解析/访问 IPv6 源站?

当防护网站的源站地址配置为IPv6地址时，WAF直接通过IPv6地址访问源站。WAF默认在CNAME中增加IPv6地址解析，IPv6的所有访问请求将先流转到WAF，WAF检测并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。

WAF支持IPv6/IPv4双栈模式和NAT64机制，详细说明如下：

- 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可以将外部IPv6访问流量转化成对内的IPv4流量。
- 哪些Region支持IPv6防护请参考[功能总览](#)。

须知

仅专业版和铂金版支持IPv6防护。

2.6 企业项目

2.6.1 WAF 可以跨企业项目使用吗?

不同的WAF模式，是否支持跨企业项目使用，详情如下：

- 云模式
 - 云模式-CNAME接入：支持跨企业项目使用。
 - 云模式-ELB接入：通过WAF防护的ELB与购买的ELB实例组必须在同一个VPC内，才支持跨企业项目使用。
- 独享模式

通过WAF购买的独享引擎实例到源站的VPC网络是互通的，则支持跨企业项目使用。否则，在某个企业项目下购买的WAF独享引擎实例，在其他企业项目下不能使用。

📖 说明

如果独享引擎实例到源站的VPC网络不互通，且您又想跨企业项目使用WAF实例的话，您可以在“企业项目管理”页面将购买的WAF迁入目标企业项目，使目标企业项目可以使用购买或升级的WAF。

2.6.2 购买或升级 WAF 时选择了企业项目，其他企业项目可以使用该企业项目的 WAF 吗?

[开通企业管理功能](#)后，WAF可以按企业项目分配管理。

- 云模式（CNAME接入和ELB接入）

购买或升级WAF时如果您选中了某一个企业项目，其他企业项目可以使用该企业项目的WAF。

- 独享模式

通过WAF购买的独享引擎实例到源站的VPC网络是互通的，则支持跨企业项目使用。否则，在某个企业项目下购买的WAF独享引擎实例，在其他企业项目下不能使用。

 **说明**

如果独享引擎实例到源站的VPC网络不互通，且您又想跨企业项目使用WAF实例的话，您可以在“企业项目管理”页面将购买的WAF迁入目标企业项目，使目标企业项目可以使用购买或升级的WAF。

3 购买 WAF

3.1 同一账号可以购买多个 Web 应用防火墙吗？

购买云模式时，同一账号在同一个大区域（例如华东区域）只能选择一个服务版本。购买云模式后，您可以升级云模式版本和规格。

同一账号可以同时购买云模式、独享模式和ELB模式。其中，独享模式实例可以购买多个。

3.2 主账号与子账号的权限有哪些区别？

企业为了方便管理，在IAM注册账号时，提供多个账号之间形成企业主子关系的能力，如果多个账号属于同一组织架构，可以将多个账号创建关联关系。

主账号可以给予子账号划拨费用，并由子账号独立进行资源管理，子账号的作用是方便主账号进行费用管理以及成本核算。

主账号与子账号中都可以再创建更小层级的IAM用户，这些IAM用户分别属于对应的账号，可以帮助账号管理资源。企业主账号只能管理企业主账号创建的IAM用户，无法管理子账号创建的IAM用户。

主账号与子账号的权限区别取决于企业授予了该账号什么权限，账号本身并无权限区别。

关于WAF账号权限的详细介绍，请参见[WAF权限管理](#)。

3.3 Web 应用防火墙是否支持多个账号共享使用？

WAF不支持多个账号共享使用，每个账号需要单独购买WAF进行部署。但是支持多个IAM用户共享使用。

多个 IAM 用户共享使用

例如，您通过注册华为云创建了1个账号（“domain1”），且由“domain1”账号在IAM中创建了2个IAM用户（“sub-user1a”和“sub-user1b”），如果您授权了“sub-user1b”用户WAF的权限策略，则“sub-user1b”用户可以使用“sub-user1a”用户的WAF。

有关WAF权限管理的详细操作，请参见[创建用户组并授权使用WAF](#)。

3.4 WAF 是如何计算域名个数的？

WAF支持的防护域名个数计算方式说明如下：

- 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，标准版支持防护10个域名，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。
- WAF支持上传的证书套数和WAF支持防护的域名的个数相同。例如，购买了标准版WAF（支持防护10个域名）、1个独享版WAF（支持防护2,000个域名）和域名扩展包（20个域名），WAF可以防护2,030个域名，则WAF支持上传2,030套证书。

有关WAF各版本支持防护的域名个数的详细说明，请参见[服务版本差异](#)。

4 业务请求/规格

4.1 变更规格类

4.1.1 如何降低 Web 应用防火墙的版本和规格？

WAF云模式提供了标准版、专业版和铂金版三种服务版本。WAF支持降低WAF的版本和域名扩展包、QPS扩展包、规则扩展包的数量，如果您需要降低当前的WAF版本和规格，在页面的右上角，单击“变更”，进入“变更Web应用防火墙规格”页面进行操作。

- **变更版本：**在“版本”所在行的“变更详情”列，单击“变更版本”，选择规格版本并单击“确定”。
- **变更扩展包：**分别在“域名额度”、“QPS额度”、“规则额度”所在行的变更详情列，增加或减少扩展包数量。
默认不支持将扩展包数量降到0，如果您需要将扩展包数量降到0，单击“退订”进行处理。
- **计费信息：**变更规格不改变计费模式与到期时间。

注意

- 已到期的服务版本，不支持变更规格，请先完成续费再变更规格。
- 扩展包只能退订未使用的扩展包。

- 有关WAF各版本规格的详细说明，请参见[服务版本差异](#)。
- 有关退订的详细操作，请参见[如何退订Web应用防火墙？](#)。
- 有关退订重购后，原配置数据的相关说明，请参见[退订后重购WAF，原配置数据可以保存吗？](#)。

4.1.2 防护规则条数不够用时，如何处理？

Web应用防火墙云模式提供了标准版、专业版和铂金版三种服务版本。各服务版本针对各种规则的配置条数请参见[服务版本差异](#)。如果您所购买的服务版本支持的规则条数不能满足您业务的需要，您可以升级服务版本。

4.1.3 若流量超过 Web 应用防火墙的业务请求限制，该如何处理？

如果您的正常业务流量超过您已购买的WAF版本的业务请求限制，您在WAF中配置的全部业务的流量转发将可能受到影响。

超出业务请求限制后，可能出现限流、随机丢包、自动Bypass等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。

📖 说明

超出业务请求限制后，WAF不会发告警通知，当QPS超过版本支持的峰值且受到攻击时，WAF会发送告警通知。有关告警通知的详细介绍，请参见[开启告警通知](#)。

如果出现这种情况，您需要升级WAF版本或者扩展业务QPS，避免正常业务流量超出业务带宽限制所产生的影响。

有关升级版本的详细介绍，请参见[升级服务版本](#)。

4.1.4 QPS 超过当前 WAF 版本支持的峰值时有什么影响？

如果您选择的QPS规格不足以支撑网站/应用业务每天的流量峰值，对超出当前WAF版本支持峰值的QPS，WAF将不再防护网站，可能出现限流、随机丢包、自动Bypass等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。

WAF各版本支持的QPS规格说明如[表4-1](#)所示。

表 4-1 WAF 支持的 QPS 规格说明

服务版本	正常业务请求峰值	CC攻击防护峰值
标准版	2,000QPS	100,000QPS
专业版	5,000QPS	200,000QPS
铂金版	10,000QPS	1,000,000QPS

服务版本	正常业务请求峰值	CC攻击防护峰值
独享版	<p>以下数据为单实例规格：</p> <ul style="list-style-type: none">WAF实例规格选择WI-500，参考性能：<ul style="list-style-type: none">HTTP业务：建议QPS 5,000；极限QPS 10,000HTTPS业务：建议QPS 4,000；极限QPS 8,000Websocket业务：支持最大并发连接5,000最大回源长连接：60,000WAF实例规格选择WI-100，参考性能：<ul style="list-style-type: none">HTTP业务：建议QPS 1,000；极限QPS 2,000HTTPS业务：建议QPS 800；极限QPS 1,600Websocket业务：支持最大并发连接1,000最大回源长连接：60,000	<ul style="list-style-type: none">WAF实例规格选择WI-500，参考性能：防护峰值：20,000QPSWAF实例规格选择WI-100，参考性能：防护峰值：4,000QPS

有关WAF各版本规格的详细介绍，请参见[服务版本差异](#)。

4.1.5 续费时如何变更 Web 应用防火墙的规格？

您只能为当前的WAF云模式进行续费，续费时不能直接变更WAF的规格。即WAF会按照当前WAF的版本、购买的域名/QPS/规则扩展包的数量进行续费。如果您需要在续费时变更WAF的规格，可参见[升级云模式版本和规格](#)先进行操作后再进行续费操作。

须知

如果重购的WAF与原WAF不在同一区域，原WAF配置数据将不能保存。当您重新购买WAF后，您需要将防护域名重新接入WAF，并根据防护需求为域名配置相应的防护规则，详细说明请参见[退订后重购WAF，原配置数据可以保存吗？](#)。

4.1.6 Web 应用防火墙最多可以添加多少条规则？

根据不同的版本不同的配置规则，可添加的规则条数不同。具体的版本规格说明如[表 4-2](#)所示。

表 4-2 适用的业务规格

业务规格	标准版	专业版	铂金版	云模式 (按需 计费)	独享模式
正常业务请求峰值	<ul style="list-style-type: none"> • 2,000 QPS业务请求 • 6,000回源长连接 (每域名) 	<ul style="list-style-type: none"> • 5,000 QPS业务请求 • 6,000回源长连接 (每域名) 	<ul style="list-style-type: none"> • 10,000 QPS业务请求 • 6,000回源长连接 (每域名) 	6,000回源长连接 (每域名)	<p>以下数据为单实例规格:</p> <ul style="list-style-type: none"> • WAF实例规格选择 WI-500, 参考性能: <ul style="list-style-type: none"> - HTTP业务: 建议 QPS 5,000; 极限QPS 10,000 - HTTPS业务: 建议 QPS 4,000; 极限QPS 8,000 - Websocket业务: 支持最大并发连接 5,000 - 最大回源长连接: 60,000 • WAF实例规格选择 WI-100, 参考性能: <ul style="list-style-type: none"> - HTTP业务: 建议 QPS 1,000; 极限QPS 2,000 - HTTPS业务: 建议 QPS 800; 极限 QPS 1,600 - Websocket业务: 支

业务规格	标准版	专业版	铂金版	云模式 (按需 计费)	独享模式
					持最大并发连接 1,000 - 最大回源长连接: 60,000 须知 极限值为实验室测试值, 高敏感业务请以实际业务测试数据为准。实际QPS与业务请求数据大小、自定义防护规则种类及数量相关
业务带宽阈值 (源站服务器部署在华为云)	100Mbit/s	200Mbit/s	300Mbit/s	-	<ul style="list-style-type: none"> WAF实例规格选择 WI-500, 参考性能: 吞吐量: 500 Mbps WAF实例规格选择 WI-100, 参考性能: 吞吐量: 100 Mbps
业务带宽阈值 (源站服务器未部署在华为云)	30Mbit/s	50Mbit/s	100Mbit/s	-	-
域名个数	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)	30个 (支持3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)	20个	50个	80个	20个	-

业务规格	标准版	专业版	铂金版	云模式 (按需 计费)	独享模式
支持的端口 个数 说明 云模式的专业版和铂金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。	<ul style="list-style-type: none"> 标准端口：2个（80，443） 非标准端口：可任意使用WAF支持的端口列表中的端口，不限制数量。 	<ul style="list-style-type: none"> 标准端口：2个（80，443） 非标准端口：可任意使用WAF支持的端口列表中的端口，不限制数量。 	<ul style="list-style-type: none"> 标准端口：2个（80，443） 非标准端口：可任意使用WAF支持的端口列表中的端口，不限制数量。 	-	<ul style="list-style-type: none"> 标准端口：2个（80，443） 非标准端口：可任意使用WAF支持的端口列表中的端口，不限制数量。
CC攻击防护峰值	100,000QPS	200,000 QPS	1,000,000 QPS	-	<ul style="list-style-type: none"> WAF实例规格选择 WI-500，参考性能：防护峰值：20,000QPS WAF实例规格选择 WI-100，参考性能：防护峰值：4,000QPS
CC攻击防护规则	20条	50条	100条	200条	100条
精准访问防护规则	20条	50条	100条	200条	100条
引用表规则	-	50条	100条	200条	100条
IP黑白名单规则	1000条	2000条	5000条	200条	1000条

业务规格	标准版	专业版	铂金版	云模式 (按需 计费)	独享模式
地理位置封禁规则	-	50条	100条	200条	100条
网页防篡改规则	20条	50条	100条	200条	100条
JS脚本反爬虫规则	-	50条	100条	200条	100条
防敏感信息泄露	-	50条	100条	200条	100条
全局白名单规则	1000条	1000条	1000条	2000条	1000条
隐私屏蔽规则	20条	50条	100条	200条	100条
安全报告模板	5个	10个	20个	-	20个

4.1.7 如何购买域名扩展包/QPS 扩展包/规则扩展包？

购买或升级WAF云模式的标准版、专业版和铂金版时，您可以选择购买域名扩展包、QPS扩展包或规则扩展包。


有关域名扩展包、QPS扩展包或规则扩展包的详细介绍，请参见[域名扩展包说明](#)、[QPS扩展包说明](#)和[规则扩展包说明](#)。


须知

WAF独享模式不支持购买扩展包，因此，如果您需要扩展QPS，只能购买多个WAF独享引擎实例。

购买云模式时同时购买扩展包

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在界面右上角，单击“购买WAF实例”。

步骤5 在“购买Web应用防火墙”界面，选择“云模式”。

步骤6 在“购买Web应用防火墙”界面，选择“区域”和服务版本。

步骤7 可以选择“域名扩展包”、“QPS扩展包”和“规则扩展包”的数量。

步骤8 选择“购买时长”后，按界面提示付款。


说明


扩展包购买时长和购买WAF时长一致。

----结束

升级时购买扩展包

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全 > Web应用防火墙 WAF”。

步骤4 在左侧导航栏中，选择“系统管理 > 产品信息”，进入产品信息页面。

步骤5 单击“规格变更”，进入“变更Web应用防火墙规格”页面。

- **变更版本**：在“版本”所在行的“变更详情”列，单击“变更版本”，选择规格版本并单击“确定”。
- **变更扩展包**：分别在“域名额度”、“QPS额度”、“规则额度”所在行的变更详情列，增加或减少扩展包数量。
默认不支持将扩展包数量降到0，如果您需要将扩展包数量降到0，单击“退订”进行处理。
- **计费信息**：变更规格不改变计费模式与到期时间。

步骤6 分别在“域名额度”、“QPS额度”、“规则额度”所在行的变更详情列，增减扩展包数量。

步骤7 在页面右下角，单击“立即购买”，按界面提示完成付款。

说明

扩展包购买时长和购买WAF时长一致。

----结束

4.2 业务请求类

4.2.1 购买 WAF 时如何选择业务 QPS?

WAF对防护带宽/共享带宽没有限制，对业务带宽和业务QPS请求数有限制。WAF各版本支持的业务QPS请求数规格请参见[服务版本差异](#)。

什么是 QPS?

WAF的业务QPS是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为QPS。一个QPS扩展包的QPS限制和带宽限制：

- 对于部署在华为云的Web应用
业务带宽：50Mbit/s

每秒钟的请求量：1000QPS（Query Per Second，例如一个HTTP GET请求就是一个Query）

- 对于未部署在华为云的Web应用

业务带宽：20Mbit/s

每秒钟的请求量：1000QPS（Query Per Second，例如一个HTTP GET请求就是一个Query）

须知

- 购买了云模式标准版、专业版或铂金版后，才支持使用ELB接入方式，域名、QPS、规则扩展包的配额与云模式的CNAME接入方式共用，且ELB接入方式的业务规格与购买的云模式版本的对应规格一致。
- 带宽限制仅对云模式-CNAME接入的网站有限制，通过ELB接入方式接入的网站，没有带宽限制，仅有QPS限制。

有关QPS扩展包的详细介绍，请参见[QPS扩展包说明](#)。

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。

什么是流量？

流量指的是业务去掉攻击流量后的正常流量。例如，您需要将所有站点对外访问的流量都接入WAF进行防护，在正常访问（未遭受攻击）时，WAF将这些正常访问流量回源到源站ECS实例；而当站点遭受攻击（CC攻击或DDoS攻击）时，WAF将异常流量拦截、过滤后，将正常流量回源到源站ECS实例。因此，您在云服务器（ECS）管理控制台中查看您源站ECS实例的入方向及出方向的流量就是正常的业务流量。如果存在多个源站ECS实例，则需要统计所有源站ECS实例流量的总和。例如：假设您需要通过WAF配置防护六个站点，每个站点的出方向的正常业务流量峰值都不超过2,000QPS，流量总和不超过12,000QPS。这种情况下，您只需选择购买Web应用防火墙铂金版套餐即可。

说明

一般情况下，出方向的流量会比较大。

超过业务带宽限制和请求限制会有什么影响

如果您的正常业务流量超过您已购买的WAF版本的业务带宽和请求限制，您在WAF中配置的全部业务的流量转发将可能受到影响。

超出业务请求限制后，可能出现限流、随机丢包等现象，导致您的正常业务在一定时间内不可用、卡顿、延迟等。

如果出现这种情况，您需要升级WAF版本或者扩展业务请求，避免正常业务流量超出业务请求限制所产生的影响。

4.2.2 选择业务 QPS 时是按照入流量计算还是出流量计算？

WAF的业务QPS是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为QPS。

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。

流量指的是业务去掉攻击流量后的正常流量。例如，您需要将所有站点对外访问的流量都接入WAF进行防护，在正常访问（未遭受攻击）时，WAF将这些正常访问流量回源到源站ECS实例；而当站点遭受攻击（CC攻击或DDoS攻击）时，WAF将异常流量拦截、过滤后，将正常流量回源到源站ECS实例。因此，您在云服务器（ECS）管理控制台中查看您源站ECS实例的入方向及出方向的流量就是正常的业务流量。如果存在多个源站ECS实例，则需要统计所有源站ECS实例流量的总和。例如：假设您需要通过WAF配置防护六个站点，每个站点的出方向的正常业务流量峰值都不超过2,000QPS，流量总和不超过12,000QPS。这种情况下，您只需选择购买Web应用防火墙铂金版套餐即可。

说明

一般情况下，出方向的流量会比较大。

有关QPS的详细介绍，请参见[QPS扩展包说明](#)。

4.2.3 WAF 对防护带宽/共享带宽有限制吗？

WAF对防护带宽/共享带宽没有限制，WAF对业务带宽和QPS有限制。

WAF的业务QPS是指所有该WAF防护的域名、站点中正常业务流量的大小，单位为QPS。

购买WAF时，您需要提前考虑准备通过WAF配置防护的所有站点的日常入方向和出方向总流量的峰值，确保您选购的WAF所对应的业务带宽限制大于入、出方向总流量峰值中较大的值。


有关WAF各版本防护规格的详细介绍，请参见[服务版本差异](#)。

4.2.4 如何查看防护网站的入带宽和出带宽信息？

在“安全总览”页面，您可以查看防护网站或实例的带宽信息，操作步骤如下。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”，进入“安全总览”页面。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目的安全总览信息。

步骤4 在网站或实例下拉列表中，选择要查看的网站或实例，并选择查看的时间段（昨天、今天、3天、7天、30天）。

步骤5 在“安全统计”区域框中，选择“发送/接收字节数”页签，可以查看防护网站或实例的入带宽和出带宽信息。

----结束

5 网站接入配置

5.1 域名/端口类

5.1.1 域名/IP 如何接入 Web 应用防火墙？

域名或IP以云模式-CNAME接入或者独享模式接入WAF后，WAF作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

域名或IP以云模式-ELB接入接入WAF后，WAF通过内嵌在ELB网关中的SDK提取流量并进行检测和防护，由ELB根据WAF的检测结果决定是否将客户端请求转发到源站。WAF不参与流量转发，避免因额外引入一层转发而带来各种兼容性和稳定性问题。

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

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务
- 独享模式：域名或IP，华为云的Web业务

须知

- WAF支持防护多级别单域名（例如，一级域名example.com，二级域名www.example.com和泛域名*.example.com）。各类型域名接入WAF的流程是相同的。
 - 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。
 - 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。
- 同一防护域名不能重复添加到WAF云模式。
 同一个域名对应不同非标准端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个域名防护配额。如果您需要防护同一域名的多个端口，您需要将该域名和端口逐一添加到WAF。

有关云模式、独享模式的应用场景和差异的详细说明，请参见[服务版本差异](#)。

网站接入WAF各模式的流程如下图所示。

图 5-1 网站接入 WAF 的操作流程图-云模式（CNAME 接入）

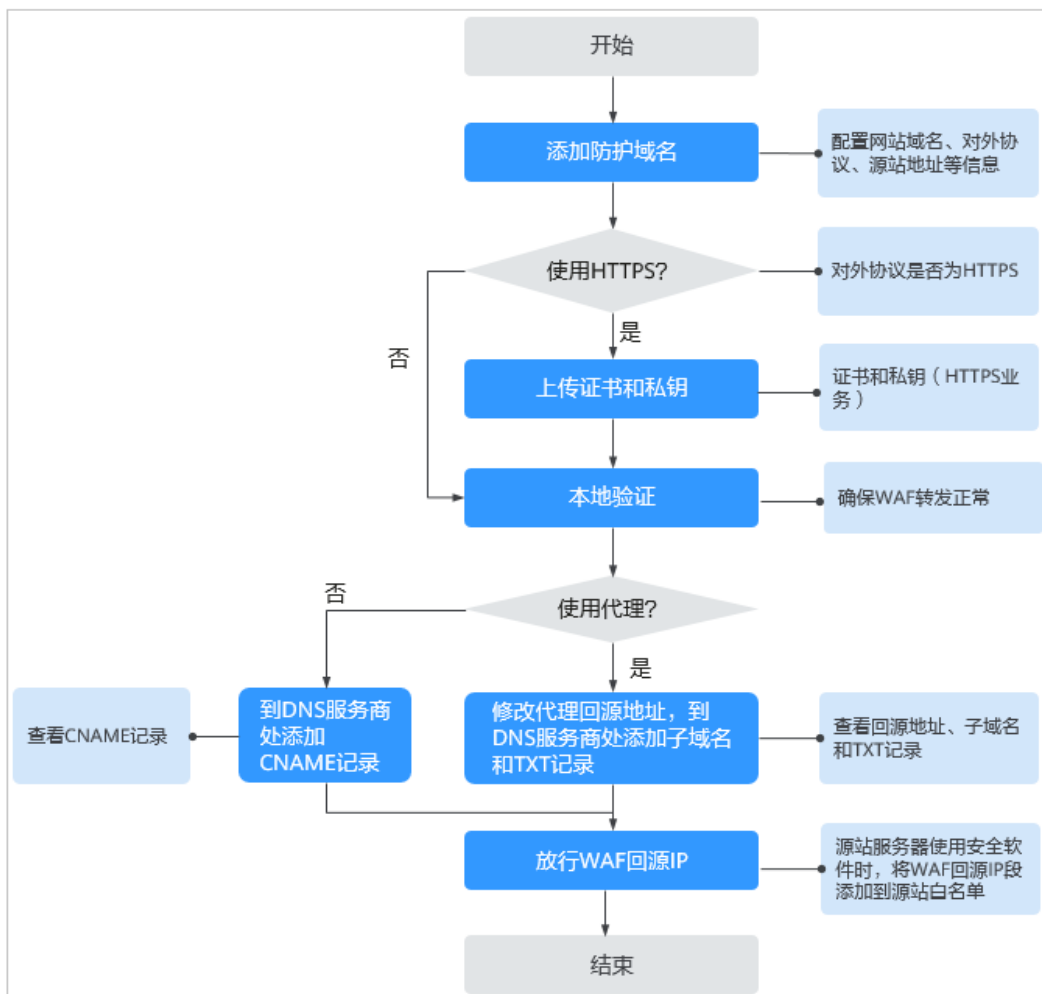
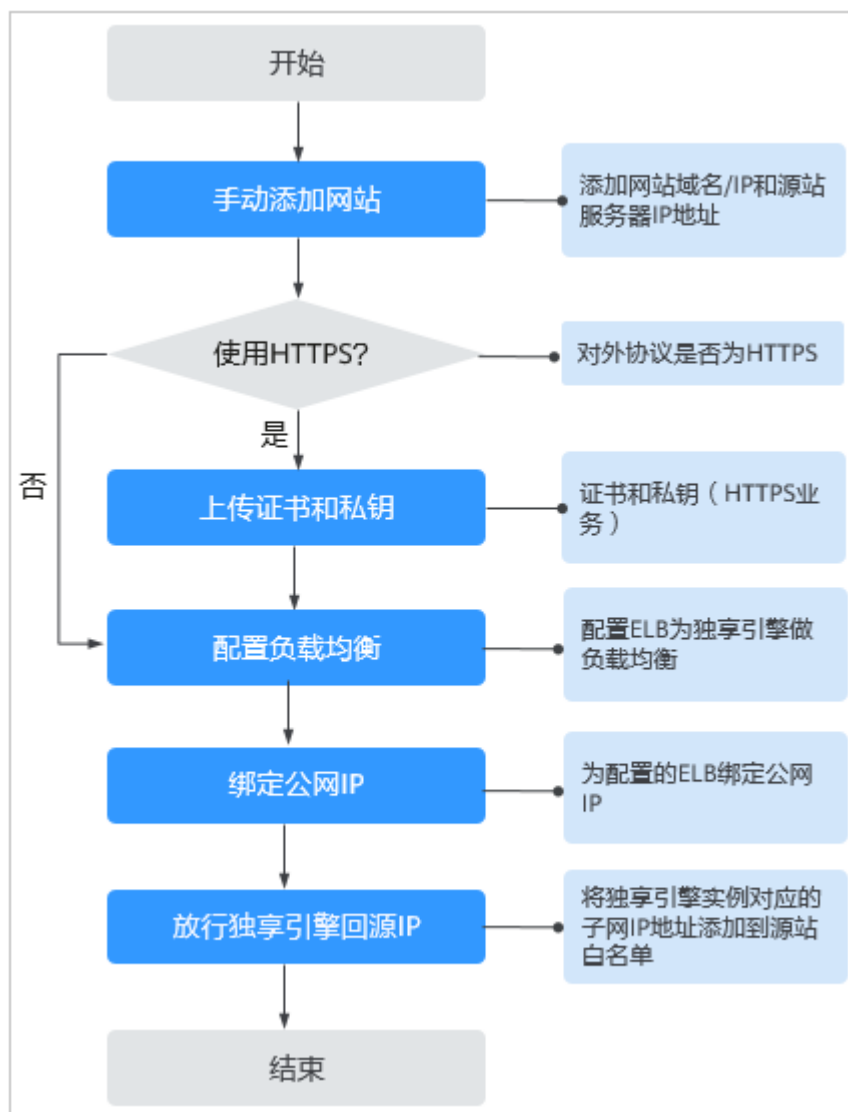


图 5-2 网站接入 WAF 的操作流程图-独享模式



有关域名接入WAF的详细介绍，请参见[添加防护域名](#)。

- 如果网站接入WAF失败，即防护网站“接入状态”显示“未接入”，请参见[域名/IP接入状态显示“未接入”，如何处理？](#) 排查处理。
- 如果网站接入WAF后访问网站报错，请参见[如何排查404/502/504错误？](#) 进行处理。

5.1.2 Web 应用防火墙支持哪些非标准端口？

WAF支持防护采用WebSocket/WebSockets（默认为开启状态）/HTTP/HTTPS协议的Web应用，WAF可以防护标准的80，443端口外，还支持非标准端口的防护，且不同版本支持的端口有所差异。

同一个域名对应不同非标准端口视为不同的防护对象，例如www.example.com:8080和www.example.com:8081为两个不同的防护对象，且占用两个域名防护配额。如果您需要防护同一域名的多个端口，您需要将该域名和端口逐一添加到WAF。

须知

不同Region支持的端口范围略有差异，以实际的支持范围为准。

标准端口

WAF支持防护如下标准端口：

- HTTP协议端口：80
- HTTPS协议端口：443

云模式支持防护的非标端口

云模式支持的非标端口是由WAF指定的任意非标端口，而不是您业务中的任意一个自定义非标端口。不同版本的WAF支持的非标准端口范围有所不同。

表 5-1 云模式支持的非标端口

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
标准版/按需计费	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 7009, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8999, 9001	4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8712, 8803, 8804, 8805, 8843, 9443, 8553, 8663, 9553, 9663, 18000, 18110, 18381, 18443, 18980, 19000, 28443

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
专业版	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888 , 1000, 1090, 1135, 1139, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 55222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 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, 7080, 77081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 9770, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18180, 18280, 19101, 19501, 21028, 23333, 27777, 28080, 30002, 30086, 33332, 33334, 33702, 40010, 48299, 48800, 52725, 52726, 60008, 60010	447, 882, 1818, 4006, 4430, 4443, 5048, 5049, 5100, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 9005, 9053, 9090, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 14443, 17618, 17718, 17818, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 20000, 28443, 60009

服务版本	支持的非标端口范围	
	HTTP协议	HTTPS协议
铂金版	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888 , 1000, 1090, 1135, 1139, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 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, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8899, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18180, 18280, 23333, 27777, 28080, 30086, 33702, 48299, 48800	447, 882, 1818, 4006, 4430, 4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 8848, 8910, 8920, 8950, 9005, 9053, 9090, 9182, 9184, 9190, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 17618, 17718, 17818, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 28443, 60009

独享模式支持防护的非标端口

使用独享模式接入WAF时，支持防护表5-2中的任意非标端口。

表 5-2 独享模式支持的非标端口

HTTP协议	HTTPS协议
81, 82, 83, 84, 86, 87, 88, 89, 97, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 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, 7080, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9945, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 10000, 10001, 10080, 12601, 19101, 19501, 19998, 21028, 28080, 30002, 33332, 33334, 33702, 40010, 48800, 52725, 52726, 60008, 60010	4443, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8843, 9443, 9553, 9663, 9999, 18000, 18010, 18110, 18381, 18443, 18980, 19000, 28443

5.1.3 独享模式如何防护不支持的非标准端口？

当独享模式不支持防护域名的非标准端口时，您可以通过配置ELB将流量引流到独享模式任一支持的非标准端口，以防护不支持的非标准端口。有关独享模式支持防护的非标准端口，请参见[Web应用防火墙支持哪些非标准端口？](#)。

例如，客户端请求到独享引擎使用的协议为HTTP，您需要对“www.example.com:1234”进行防护，而独享模式不支持非标准端口“1234”。此时，您可以通过配置ELB将流量引流到独享模式支持的任一非标准端口（如“81”），以实现防护非标准端口“1234”。


须知

为了确认配置生效，添加防护域名时，“防护域名”建议填写为防护域名对应的泛域名。例如，您需要对“www.example.com:1234”进行防护，则“防护域名”需要填写为“*.example.com”。

请参照以下操作步骤进行配置。


步骤1 登录管理控制台。

步骤2 在WAF管理控制台添加防护域名。

1. 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。
2. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
3. 在网站列表左上角，单击“添加防护网站”，选择“独享模式”后，添加“www.example.com:1234”对应的泛域名“*.example.com”，在“防护对象端口”下拉框中选择任一端口（如“81”）。
4. “是否已使用代理”，选择“七层代理”，单击“确认”，防护网站添加成功。
5. 关闭弹出的对话框。

您可以在防护网站列表中查看已添加防护网站。

步骤3 在ELB管理控制台配置负载均衡。

1. 单击页面左上方的 ，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。
2. 在负载均衡器所在行的“名称”列，单击目标负载均衡器名称，进入ELB“基本信息”页面。
3. 在“跨VPC后端”所在行，单击“跨VPC后端”，并在弹框中单击“确定”，开启跨VPC后端。
4. 选择“监听器”页签后，单击“添加监听器”，配置监听器端口为“1234”。
5. 单击“下一步：配置后端分配策略”，配置后端分配策略。
6. 单击“下一步：添加后端服务器”，并选择“跨VPC后端”页签，添加跨VPC后端和健康检查。
7. 单击“添加跨VPC后端”，在弹出的弹框中，配置“跨VPC的后端IP”和“后端端口”。
 - 跨VPC后端IP：WAF独享引擎的IP（在“独享引擎”列表中获取）。
 - 后端端口：“81”（与步骤2.3中配置的端口一致）。
8. 单击“确定”，配置完成。
9. 单击“下一步：确认配置”后单击“提交”。

步骤4 解绑源站服务器的弹性公网IP，将解绑的弹性公网IP绑定到WAF独享引擎实例配置的负载均衡上。

----结束

5.1.4 如何在添加域名中配置防护域名？

在使用WAF防护前，您需要根据您的Web业务防护需求，在WAF中添加防护域名，WAF支持添加单域名和泛域名。本章节为您介绍如何配置防护域名。

相关概念

- 泛域名
泛域名是指带1个通配符“*”且以“.”号开头的域名。
例如：“*.example.com”是正确的泛域名，但“**.example.com”则是不正确的。

📖 说明

一个泛域名算一个域名。

- 单域名

单域名又称普通域名，是相对泛域名来说的，是一个具体的域名或者说不是通配符域名。

例如：“www.example.com”或“example.com”都算一个单域名。

📖 说明

如“www.example.com”或“a.www.example.com”各个明细子域名都算一个域名。

如何选择域名类型

WAF支持防护单域名和泛域名。

在DNS服务商处购买的域名为单域名（example.com），WAF中添加的域名形式可以为example.com、子域名（例如：a.example.com）、泛域名（*.example.com），可根据以下场景选择配置域名的类型：

- 如果防护的域名业务相同：输入单域名。例如：防护www.example.com的业务都是8080端口的业务，则“防护域名”直接配置为单域名“www.example.com”。
- 如果各子域名对应的服务器IP地址相同：输入防护的泛域名。例如：a.example.com、b.example.com和c.example.com对应的服务器IP地址相同，则“防护域名”可配置为泛域名“*.example.com”。
- 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条添加。

📖 说明

建议添加的“防护域名”与在DNS服务商处设置的域名保持一致。

同时在 WAF 中添加单域名和泛域名，WAF 会优先检测哪个域名？

WAF会先检测精准度高的域名。例如，www.example.com、*.a.example.com、*.example.com都添加到WAF，WAF的检测顺序为：www.example.com > *.a.example.com > *.example.com。

5.1.5 添加域名时，防护网站端口需要和源站端口配置一样吗？

端口为实际防护网站的端口，源站端口是WAF转发客户端请求到服务器的业务端口。两者不用配置为一样，端口配置说明如下：

- “对外协议”选择“HTTP”时，WAF默认防护“80”标准端口的业务；“对外协议”选择“HTTPS”时，WAF默认防护“443”标准端口的业务。
- 如需配置除“80”/“443”以外的端口，在“防护对象端口”或者“防护域名端口”下拉列表中选择非标准端口。

Web应用防火墙支持的非标准端口请参见[Web应用防火墙支持哪些非标准端口？](#)。

5.1.6 添加防护域名时如何配置非标准端口？

端口为实际防护网站的端口，端口配置说明如下：

- “对外协议”选择“HTTP”时，WAF默认防护“80”标准端口的业务；“对外协议”选择“HTTPS”时，WAF默认防护“443”标准端口的业务。
- 如需配置除“80”/“443”以外的端口，在“防护对象端口”或者“防护域名端口”下拉列表中选择非标准端口。

示例一：防护同一端口的不同源站 IP 的标准端口业务

1. 在“防护域名端口”下拉框中，选择“标准端口”。
2. “对外协议”统一选择“HTTP”或者“HTTPS”。HTTP标准端口防护配置如图5-3所示，HTTPS标准端口防护配置如图5-4所示。

图 5-3 80 端口业务

源站配置						
* 防护域名端口	标准端口					
* 服务器配置	对外协议	源站协议	源站地址	源站端口	权重	
	HTTP	HTTP	IPv4	36	80	1
	HTTP	HTTP	IPv4	9	80	1

+ 添加 您还可以添加78个源站地址

图 5-4 443 端口业务

源站配置						
* 防护域名端口	标准端口					
* 服务器配置	对外协议	源站协议	源站地址	源站端口	权重	
	HTTPS	HTTP	IPv4	36	80	1
	HTTPS	HTTP	IPv4	9	80	1

+ 添加 您还可以添加78个源站地址

说明

- “对外协议”选择“HTTPS”时，需要配置证书。
3. 访问网站时，域名后可以不加端口号进行访问。例如，在浏览器中直接输入“http://www.example.com”访问网站。

示例二：防护同一端口的不同源站 IP 的非标准端口业务

1. 在“防护域名端口”下拉框中，选择需要防护的非标准端口。
2. “对外协议”全部选择“HTTP”或者“HTTPS”。HTTP协议的非标准端口的配置如图5-5，HTTPS协议的非标准端口的配置如图5-6。

图 5-5 除 80 端口的其他 HTTP 协议端口的业务

对外协议	源站协议	源站地址	源站端口	权重
HTTP	HTTP	IPv4 36	80	1
HTTP	HTTP	IPv4 9	80	1

图 5-6 除 443 端口的其他 HTTPS 协议端口的业务

对外协议	源站协议	源站地址	源站端口	权重
HTTPS	HTTP	IPv4 36	80	1
HTTPS	HTTP	IPv4 9	80	1

说明

“对外协议”选择“HTTPS”时，需要配置证书。

- 访问网站时，域名后必须加上配置的非标准端口，否则会报404错误。假如配置的非标准端口为8080，则在浏览器中直接输入的地址为“http://www.example.com:8080”。

示例三：防护不同的业务端口

如果防护的业务端口不一样，则需要分别添加域名进行配置，如：域名www.example.com需要同时防护8080端口和6443端口，配置如图5-7和图5-8所示。

图 5-7 8080 端口

对外协议	源站协议	源站地址	源站端口	权重
HTTP	HTTP	IPv4 36	80	1

图 5-8 6443 端口

对外协议	源站协议	源站地址	源站端口	权重
HTTPS	HTTP	IPv4 36	80	1

5.1.7 多个端口的服务器，如果某个端口不需要 WAF 防护，如何处理？

防护网站是通过域名+端口方式接入WAF进行防护的。在添加防护域名时，您只需要配置域名+需要防护的端口即可。防护网站接入WAF后，流量不会通过其他端口转发到WAF。

有关域名接入WAF的详细操作，请参见[添加防护域名](#)。

5.1.8 域名/IP 接入 WAF 前需要准备哪些数据？

请根据购买的WAF模式，在域名/IP接入WAF前收集相关信息。

- 云模式-CNAME接入

表 5-3 准备防护域名相关信息

获取信息	参数	说明	示例
域名是否使用代理	代理	域名在接入WAF前，是否已接入CDN、云加速等提供七层Web代理的产品，如果是，请务必配置成“七层代理”。	-
配置参数	防护域名	由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。	www.example.com
	防护域名端口	需要防护的域名对应的业务端口。 <ul style="list-style-type: none">• 标准端口<ul style="list-style-type: none">- 80: HTTP对外协议默认使用端口- 443: HTTPS对外协议默认使用端口• 非标准端口 80/443以外的端口 须知 如果防护域名使用非标准端口，请查看 Web应用防火墙支持哪些非标准端口? ，确保购买的WAF版本支持防护该非标准端口。	80
	HTTP2协议	HTTP2协议仅适用于客户端到WAF之间的访问，且“对外协议”必须包含HTTPS才能支持使用。	-
	对外协议	客户端（例如浏览器）请求访问网站的协议类型。WAF支持“HTTP”、“HTTPS”两种协议类型。	HTTP

获取信息	参数	说明	示例
	源站协议	WAF转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站地址	客户端（例如浏览器）访问网站所在源站服务器的 公网IP地址 （一般对应该域名在DNS服务商处配置的A记录）或者域名（一般对应该域名在DNS服务商处配置的CNAME）。	XXX.XXX.1.1
（可选）证书	证书名称	<p>对外协议选择“HTTPS”时，需要在WAF上配置证书，将证书绑定到防护域名。</p> <p>须知 WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考如何将非PEM格式的证书转换为PEM格式? 转化证书格式。</p>	-

- 云模式-ELB接入

表 5-4 准备防护域名/IP 相关信息

参数	说明	示例
域名/IP	<ul style="list-style-type: none"> • 域名：由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。 • IP：访问网站所使用的IP地址。 	www.example.com

- 独享模式

表 5-5 准备防护域名/IP 相关信息

获取信息	参数	说明	示例
配置参数	防护对象	<ul style="list-style-type: none"> • 域名：由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。 • IP：访问网站所使用的IP地址。 	www.example.com

获取信息	参数	说明	示例
	防护对象端口	需要防护的域名对应的业务端口。 <ul style="list-style-type: none">标准端口<ul style="list-style-type: none">80: HTTP对外协议默认使用端口443: HTTPS对外协议默认使用端口非标准端口 80/443以外的端口 须知 如果防护域名使用非标准端口，请查看 Web应用防火墙支持哪些非标准端口? ，确保购买的WAF版本支持防护该非标准端口。	80
	对外协议	客户端（例如浏览器）请求访问网站的协议类型。WAF支持“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站协议	WAF转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。	HTTP
	VPC	选择购买的独享引擎实例所在的VPC。	vpc-default
	源站地址	网站服务器的私网IP地址。	192.168.1.1
（可选）证书	证书名称	对外协议选择“HTTPS”时，需要在WAF上配置证书，将证书绑定到防护域名。 须知 <ul style="list-style-type: none">WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考如何将非PEM格式的证书转换为PEM格式?转化证书格式。目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能选择使用SCM推送的SSL证书。	-

5.1.9 删除防护域名时应该注意哪些事项？

删除网站的具体操作请参见[删除防护域名](#)，删除网站前的注意事项如下：

- 防护网站“部署模式”为“云模式”时，如果要删除的防护网站已经接入Web应用防火墙，在删除防护网站前，请您先到DNS服务商处将域名重新解析，指向源站服务器IP地址，否则该域名的流量将无法切回服务器，影响正常访问。

- 勾选“强制删除WAF的接入CNAME”后，WAF不再检测业务域名解析配置，立即删除WAF的CNAME，如果业务域名解析未做修改，可能会导致业务异常。
- 删除网站后，1分钟内生效，且不可恢复，请谨慎删除防护网站。

5.1.10 删除防护域名后 CNAME 记录会保留多久？

删除防护域名时，如果您没有勾选“强制删除WAF的接入CNAME”，WAF会将该域名的CNAME保留约30天后再删除该CNAME。

但是如果您在删除防护域名时，勾选了“强制删除WAF的接入CNAME”，WAF不再检测业务域名解析配置，立即删除WAF的CNAME，如果业务域名解析未做修改，可能会导致业务异常。

5.1.11 域名添加到 WAF 后，域名是否可以修改？

防护域名添加到WAF后，您不能修改防护域名的名称。如果您需要修改防护域名的名称，建议您删除原域名后再重新添加待防护的域名。

5.1.12 后端服务器配置多个源站地址时的注意事项？

- 同一个域名在后端配置多个源站地址时，请注意：
 - 域名对应的业务端口为非标准端口
对外协议、源站协议和源站端口必须都相同
 - 域名对应的业务端口为标准端口
对外协议、源站协议和源站端口可不相同
- 添加域名时，WAF支持添加多个服务器IP，多个服务器之间，WAF采用轮询的方式回源，这样有助于减少服务器的压力，起到保护源站的作用。例如，后端添加了两个服务器IP（IP-A，IP-B），当有10个请求访问该域名时，5个请求会被WAF转发到IP-A，其余5个请求会被WAF转发到IP-B。

5.1.13 Web 应用防火墙支持配置泛域名吗？

在WAF中添加防护的域名时，您可以根据业务需求配置单域名或泛域名，说明如下：

- 单域名
配置待防护的单域名。例如：www.example.com。
- 泛域名
配置泛域名可以使泛域名下的多级域名经过WAF防护。
 - 如果各子域名对应的服务器IP地址相同：配置防护的泛域名。例如：子域名a.example.com，b.example.com和c.example.com对应的服务器IP地址相同，可以直接添加泛域名*.example.com。
 - 如果各子域名对应的服务器IP地址不相同：请将子域名按“单域名”方式逐条配置。

有关添加防护域名的详细操作，请参见[添加防护域名](#)。

5.1.14 Web 应用防火墙支持防护中文域名吗？

WAF不支持中文域名。防护的域名只能由字母、数字、-、_和.组成，且域名的字符长度不能超过63个字符长度。

WAF支持防护单域名和泛域名。

- 单域名：输入防护的单域名。
- 泛域名：输入防护的泛域名。泛域名不支持下划线（_）。

5.1.15 如何使网站流量切入云模式 Web 应用防火墙？

将您的网站以云模式的CNAME接入方式添加到WAF后，还需要完成域名接入，使网站流量切入WAF。流量切入WAF后，WAF帮助您过滤恶意请求，放行合法的访问请求至源站服务器。

工作原理

- 未使用代理
当网站没有接入到WAF前，DNS直接解析到源站的IP，所以当网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。
- 使用了DDoS高防等代理
当网站没有接入到WAF前，DNS解析到高防等代理，流量先经过高防等代理，高防等代理再将流量直接转到源站。网站接入WAF后，需要将高防等代理回源地址修改为WAF的“CNAME”，这样流量才会被高防等代理转发到WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

📖 说明

- 为了确保WAF转发正常，在修改DNS解析配置前，建议您参照[本地验证](#)进行本地验证确保一切配置正常。
- 为了防止其他用户提前将您的域名配置到Web应用防火墙上，从而对您的域名防护造成干扰，建议您到DNS服务商处添加“子域名”，并为它配置“TXT记录”。WAF会据此判断域名的所有权真正属于哪个用户。具体的配置方法请参见[未配置子域名和TXT记录的影响](#)。

操作指导

添加域名后，WAF会根据添加的域名是否已在WAF前使用了代理，生成CNAME值或者CNAME、子域名和TXT记录，用于域名解析，使网站流量切入WAF，相关操作指导参见[表5-6](#)。

表 5-6 操作指导

场景	生成的参数值	域名解析的相关操作
未使用代理	CNAME	把DNS解析到WAF的“CNAME”。
使用代理	CNAME、子域名和TXT记录	<ul style="list-style-type: none">• 将DDoS高防等代理回源地址修改为WAF的“CNAME”。• （可选）在DNS服务商处添加一条WAF的“子域名”和“TXT记录”。

操作步骤

具体的操作步骤请参见[域名接入WAF](#)。

5.1.16 添加域名时提示“非法的源站地址”，如何处理？

故障现象

添加防护域名时，无法添加域名，提示“非法的源站地址”。

可能原因

- “源站地址”配置为内部保留的私网IP地址。
- “防护对象”和“源站地址”配置成了一样。

处理建议

将“源站地址”配置为真实的源站IP地址（公网IP地址）或单独的回源域名（回源域名不能和“防护域名”相同）。

5.1.17 添加域名时，为什么还有域名配额却提示域名配额不足呢？

添加域名时，如果您还有域名配额却提示域名配额不足，可能是因为你添加的是一级域名，而一级域名配额已经用完。

在“网站设置”页面，可查看您的域名配额情况。



5.1.18 一个独享 WAF 实例可以接入多个 ELB 吗？

多个ELB可以共用一个WAF独享引擎实例，将独享WAF实例添加到对应的ELB后端服务器组即可。

将网站以独享模式接入WAF的具体操作请参见[网站接入WAF（独享模式）](#)。

5.1.19 添加防护域名时，提示“其他人已经添加了该域名，请确认该域名是否属于你”，如何处理？

添加防护域名时，如果不能正常添加域名，而提示：其他人已经添加了该域名，请确认该域名是否属于您，如果是，请联系服务人员帮您解决。可能是由于您的域名已在其他账号下添加到了WAF，如果您想将该域名添加到当前账号下进行使用，需要将该域名在其他账号下的相关配置进行删除，删除后再在当前账号下重新将域名添加到WAF。

5.2 证书管理

5.2.1 为什么华为云 SCM 上的 SSL 证书在 WAF 上不能查看？

华为云SCM上的SSL证书签发后或成功上传后，您需要将证书一键推送到WAF中，才能在华为云WAF中使用。

目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能使用SCM推送的SSL证书。

有关推送SSL证书的详细操作，请参见[推送证书到云产品](#)。

5.2.2 配置泛域名时，如何选择证书？


域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有泛域名证书，只有单域名对应的证书，则只能在WAF中按照单域名的方式逐条添加域名进行防护。


5.2.3 如何修改已绑定域名的证书？

如果您购买的证书即将到期，为了不影响域名的使用，建议您在到期前重新购买证书，并在WAF中同步更新域名绑定的证书。

执行以下操作修改已绑定域名的证书。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤6 单击“源站服务器”后的编辑图标，若“对外协议”选择的是“HTTPS”，可在证书的下拉框中重新选择证书或者导入新的证书。

----结束

5.2.4 ELB 已上传的证书，在 Web 应用防火墙上需要重新导入上传吗？

在选择证书时，您可以选择已创建证书或选择导入的新证书。在ELB上已上传的证书，还需要在WAF上导入上传。

5.2.5 如何将非 PEM 格式的证书转换为 PEM 格式？

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考[表5-7](#)在本地将证书转换为PEM格式，再上传。

表 5-7 证书转换命令

格式类型	转换方式
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。

格式类型	转换方式
PFX	<ul style="list-style-type: none">提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	<ol style="list-style-type: none">证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	<ul style="list-style-type: none">提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

📖 说明

- 执行openssl命令前，请确保本地已安装[openssl](#)。
- 如果本地为Windows操作系统，请进入“命令提示符”对话框后，再执行证书转换命令。

5.2.6 为什么非 default 企业项目不能使用华为云 SCM 推送的 SSL 证书？

目前华为云SCM证书只能推送到“default”企业项目下。如果您使用其他企业项目，则不能使用SCM推送的SSL证书。

有关SCM证书推送的详细介绍，请参见[推送证书到云产品](#)。

5.2.7 添加防护域名时，为什么无法选择 SCM 证书？

现象

在WAF中添加防护域名时，在证书下拉框中选择SCM证书时，提示“用户角色无权限访问该接口 scm cert download”。

原因

该用户使用的账号没有“SCM Administrator”和“SCM FullAccess”这两个权限。

解决办法

在IAM中授予该账号“SCM Administrator”和“SCM FullAccess”权限，即可在添加防护域名时选择同一账号下的SCM证书。

5.3 服务器配置类

5.3.1 如何配置对外协议与源站协议？

本节介绍如何配置WAF的对外协议与源站协议。

根据您的业务场景的不同，WAF提供灵活的协议类型配置。假设您网站为www.example.com，WAF可配置以下模式：

HTTP 访问模式-302 跳转响应

“对外协议”和“源站协议”都配置为“HTTP”，如图5-9所示。

须知

此种配置表示用户只能通过http://www.example.com访问网站，如果用户通过https://www.example.com访问网站，会收到302跳转响应，浏览器跳转到http://www.example.com。

图 5-9 HTTP 协议访问模式

域名信息				
网站名称	您可以为域名自定义名称			
* 防护域名	www.example.com			
网站备注				
源站配置				
* 防护域名端口	标准端口			
* 服务器配置				
对外协议	源站协议	源站地址	源站端口	权重
HTTP	HTTP	IPv4	80	1
+ 添加 您还可以添加79个源站地址				

HTTPS 访问强制跳转模式

“对外协议”和“源站协议”都配置为“HTTPS”，如图5-10所示。当使用HTTP协议访问服务器时，会强制跳转为HTTPS协议。

须知

- 用户直接通过https://www.example.com访问网站，网站返回正常内容。
- 用户通过http://www.example.com访问网站，用户会收到302跳转响应，浏览器跳转到https://www.example.com。

图 5-10 HTTPS 协议访问强制跳转模式

The screenshot shows a configuration page for a website. It is divided into two main sections: "域名信息" (Domain Information) and "源站配置" (Source Site Configuration).
Under "域名信息":

- 网站名称: 您可以为域名自定义名称 (Website Name: You can customize the domain name)
- * 防护域名: www.example.com (Protection Domain: www.example.com)
- 网站备注: (Website Remark)

Under "源站配置":

- * 防护域名端口: 标准端口 (Protection Domain Port: Standard Port)
- * 服务器配置 (Server Configuration):

对外协议 ?	源站协议 ?	源站地址 ?	源站端口 ?	权重 ?
HTTPS	HTTPS	IPv4	443	1
- 底部提示: + 添加 您还可以添加79个源站地址 (Add: You can also add 79 source site addresses)

HTTP/HTTPS 分别转发模式

“对外协议”和“源站协议”配置的协议如图5-11所示。

须知

- 用户通过http://www.example.com访问网站，网站返回正常内容，没有跳转，网站内容不加密传输。
- 用户通过https://www.example.com访问网站，网站返回正常内容，没有跳转，网站内容加密传输。

图 5-11 HTTP/HTTPS 分别转发模式

The screenshot shows a configuration page for a website, similar to Figure 5-10. It is divided into "域名信息" and "源站配置".
Under "域名信息":

- 网站名称: 您可以为域名自定义名称
- * 防护域名: www.example.com
- 网站备注:

Under "源站配置":

- * 防护域名端口: 标准端口
- * 服务器配置:

对外协议 ?	源站协议 ?	源站地址 ?	源站端口 ?	权重 ?
HTTP	HTTP	IPv4	80	1
HTTPS	HTTPS	IPv4	443	1
- 底部提示: + 添加 您还可以添加78个源站地址

HTTPS 卸载模式

“对外协议”配置为“HTTPS”且“源站协议”配置为“HTTP”，如图5-12所示。

须知

用户通过https://www.example.com访问网站，但是WAF到源站依然使用HTTP协议。

图 5-12 使用 WAF 做 HTTPS 卸载模式

The screenshot shows a configuration form for WAF. It is divided into two main sections: '域名信息' (Domain Information) and '源站配置' (Origin Configuration). Under '域名信息', there are fields for '网站名称' (Website Name) with a placeholder '您可以为域名自定义名称', '防护域名' (Protection Domain) with the value 'www.example.com', and '网站备注' (Website Remark). Under '源站配置', there is a dropdown for '防护域名端口' (Protection Domain Port) set to '标准端口' (Standard Port). Below this is a table for '服务器配置' (Server Configuration) with columns: '对外协议' (Outward Protocol) set to 'HTTPS', '源站协议' (Origin Protocol) set to 'HTTP', '源站地址' (Origin Address) set to 'IPv4', '源站端口' (Origin Port) set to '80', and '权重' (Weight) set to '1'. At the bottom, there is a link to add more origin addresses: '+ 添加 您还可以添加79个源站地址'.

5.3.2 添加域名时，为什么不能选择对外协议？

添加防护域名时，如果配置了非标准端口，当对外协议（HTTP/HTTPS）不支持该非标准端口时，您将不能选择对外协议。建议在配置非标准端口时，确认对外协议（HTTP/HTTPS）支持该非标准端口。

有关WAF支持的非标准端口的详细介绍，请参见[Web应用防火墙支持哪些非标准端口？](#)。

5.3.3 云模式服务器的源站地址可以配置成 CNAME 吗？

可以。如果服务器的源站地址配置为CNAME，添加域名后会多经历一层DNS解析，即先将CNAME解析为IP地址，DNS解析会增加时延，故推荐您将源站地址配置成公网IP地址。

添加域名的相关配置请参见[添加防护域名](#)。

5.4 域名解析类

5.4.1 如何在华为云的云解析服务上修改 DNS 解析？

如果网站在接入WAF前用户通过客户端（例如浏览器）直接访问网站服务器，当选择WAF添加防护域名后，您还需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

本章节以华为云的云解析服务为例介绍如何修改DNS解析，具体操作请根据域名提供商进行相应操作。

前提条件


- 已选择“云模式-CNAME”部署方式添加防护域名。
- 为了确保WAF转发正常，在修改DNS解析配置前，建议您参照[本地验证](#)进行本地验证确保一切配置正常。

约束条件

- 对于同一个主机记录，CNAME解析记录不能重复，您需要将已存在的解析记录的CNAME修改为WAF CNAME地址。

- 同一解析记录下，不同DNS解析记录类型间可能存在冲突。例如，对于同一个主机记录，CNAME记录与A记录、MX记录、TXT记录等其他记录互相冲突。在无法直接修改记录类型的情况下，您可以先删除存在冲突的其他记录，再添加一条新的CNAME记录。删除其他解析记录并新增CNAME解析记录的过程应尽可能在短时间内完成。如果删除A记录后没有添加CNAME解析记录，可能导致域名无法正常解析。详细介绍请参见[添加记录集时，为什么会提示“与已有解析记录冲突”？](#)。
- 为了防止其他用户提前将您的域名配置到Web应用防火墙上，从而对您的域名防护造成干扰，建议您到DNS服务商处添加“子域名”，并为其配置“TXT记录”，WAF会据此判断域名的所有权真正属于哪个用户。具体的配置方法请参见[未配置子域名和TXT记录的影响](#)。
- 修改域名解析记录后，理论上生效的最长时间是解析记录修改或删除前设置的TTL值。如果运营商强制设置了更长的域名解析记录的缓存时间，也会导致修改解析记录生效的延迟。

操作步骤

进入“网站设置”页面后，在目标域名的“接入状态”所在行单击，复制“CNAME”值。

请参考以下操作步骤修改DNS解析。

1. 进入云解析页面的入口，如[图5-13](#)所示。

图 5-13 云解析页面入口



2. 在目标域名所在行的“操作”列，单击“修改”，进入“修改记录集”页面。
3. 在弹出的“修改记录集”对话框中修改记录值，如[图5-14](#)所示。
 - “主机记录”：在WAF中配置的域名。
 - “类型”：选择“CNAME-将域名指向另外一个域名”。
 - “线路类型”：全网默认。
 - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
 - “值”：修改为已复制的WAF CNAME地址。
 - 其他的设置保持不变。

说明

关于修改解析记录：

- 对于同一个主机记录，CNAME解析记录不能重复，您需要将已存在的解析记录的CNAME修改为WAF CNAME地址。
- 同一解析记录下，不同DNS解析记录类型间可能存在冲突。例如，对于同一个主机记录，CNAME记录与A记录、MX记录、TXT记录等其他记录互相冲突。在无法直接修改记录类型的情况下，您可以先删除存在冲突的其他记录，再添加一条新的CNAME记录。删除其他解析记录并新增CNAME解析记录的过程应尽可能在短时间内完成。如果删除A记录后没有添加CNAME解析记录，可能导致域名无法正常解析。

域名解析类型的限制规则请参见[添加记录集时，为什么会提示“与已有解析记录冲突”？](#)。

图 5-14 修改记录集

修改记录集

主机记录

类型

别名 是 否

线路类型

* TTL (秒)

* 值

权重

其他配置

4. 单击“确定”，完成DNS配置，等待DNS解析记录生效。

5.4.2 如何在华为云的云解析服务上进行 DNS 验证？

DNS验证一般需要由您的域名管理人员进行相关操作。如果您是在华为云平台管理您的域名，并且您的域名在您的华为账号中，请参见本章节在华为云的云解析服务上进行DNS验证。

须知

如果您是在其他域名管理平台（如万网、新网、DNSPod等）管理您的域名，请在相应的平台上进行DNS验证。例如，域名托管在阿里云，则需要到阿里云的云解析DNS控制台进行相关配置。

以下操作步骤是以申请证书的域名“domain3.com”添加一条DNS记录“2019030700000022ams1xbyevidn4jvahact9xzpicb565k9443mryw2qe99mbzpb”（记录类型为TXT）为例说明，在华为云的云解析服务上进行DNS验证的操作步骤。

前提条件

已获取域名验证所需的配置信息（“主机记录”和“记录值”）。

操作步骤

步骤1 登录管理控制台。

步骤2 选择“网络 > 云解析服务”，进入“云解析”页面。

步骤3 在左侧树状导航栏，选择“公网域名”，进入“公网域名”页面。

步骤4 在“公网域名”页面的域名列表中，单击需要解析的域名“domain3.com”，进入“解析记录”页面。

步骤5 在“解析记录”页面的左上角，单击“添加记录集”，进入“添加记录集”页面。

📖 说明

如果在“解析记录”的域名列表中，已存在域名“domain3.com”的TXT记录值，直接在目标域名的“操作”列，单击“修改”，进入“修改记录集”页面。

- “主机记录”：“域名验证”页面，域名服务商返回的“主机记录”的前缀。

根据域名服务商不同，返回的“主机记录”不同，以下仅为两个样例。

举例：

- 如果域名服务商返回的“主机记录”为“_dnsauth.domain3.com”，则主机记录填写“_dnsauth”。
- 如果域名服务商返回的“主机记录”为“domain3.com”，则“主机记录”为空，不需要填写。

- “类型”：选择“TXT - 设置文本记录”。
- “线路类型”：全网默认。
- “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
- “值”：“域名验证”页面，域名服务商返回的“记录值”。

📖 说明

记录值必须用英文引号引用后粘贴在文本框中。

- 其他的设置保持不变。

图 5-15 添加记录集

添加记录集

主机记录

* 类型

* 别名 ? 是 否

* 线路类型

* TTL (秒) ?

* 值 ?

权重 ?

其他配置

步骤6 单击“确定”，记录集添加成功。

当记录集的状态显示为“正常”时，表示记录集添加成功。

📖 说明

- 该DNS配置记录在证书颁发或吊销后才可以删除。
- 请您务必检查是否正确配置了DNS记录，DNS没有配置正确是无法签发证书的。
- 验证完成后，CA机构可能还需要2-3个工作日审核域名信息，请耐心等待，在此期间，证书状态为“待完成域名验证”。CA机构审核通过后，证书审核才可以进入“待完成组织验证”状态。

----结束

5.4.3 如何在华为云的云解析服务上配置 TXT 记录的值？

如果您在WAF中添加了使用了DDoS高防等相关代理的域名，请在您的DNS服务商处配置“子域名”和“TXT记录”，以避免其他用户在WAF中配置了相同的域名而对您的域名防护造成干扰。

如果您使用了华为云的云解析服务，配置TXT类型的记录值时，需要将TXT记录加上引号后粘贴在对应的文本框，例如，“37c795804124dd4a0dd88defff8941f”，如图5-16所示。

图 5-16 添加记录集

添加记录集

主机记录 .example_com ?

* 类型

* 别名 ? 是 否

* 线路类型 ?

* TTL (秒) ?

* 值 ?

权重

其他配置

有关在华为云的云解析服务上配置子域名和TXT记录的详细操作，请参见[未配置子域名和TXT记录的影响?](#)。

5.4.4 未配置子域名和 TXT 记录的影响?

如果在WAF中添加的域名，已使用了DDoS高防等相关代理产品，但是没有在DNS服务商处配置“子域名”和“TXT记录”，WAF将无法判断域名的所有权。

因此，为了防止其他用户提前将您的域名配置到Web应用防火墙上，干扰WAF对您的域名进行防护，请在DNS服务商处添加一条“子域名”，并为该子域名配置一条“TXT记录”，WAF会据此判断域名的所有权真正属于哪个用户。

如何判断



目标域名在域名列表中被置灰，“工作模式”为“暂停防护”，且无法切换为“开启防护”模式。如果出现此种现象，则说明您的域名被其他用户占用了。

解决办法

前往您的DNS服务商处，添加一条“子域名”，并为该子域名配置一条“TXT记录”，以下以目标域名“www.example.com”为例，描述如何在华为云的云解析服务DNS进行配置。

步骤1 获取“子域名”和“TXT记录”值。

1. [登录管理控制台](#)。

- 单击页面左上方的 ，在右侧弹框中选择“安全与合规 > Web应用防火墙 WAF”，在左侧导航树中选择“网站设置”，进入“网站设置”页面。
- 在目标域名“www.example.com”所在行中，单击目标域名，进入域名基本信息页面。
- 在页面顶部，单击“未接入”旁边的 ，在弹出的对话框中，复制“子域名”和“TXT记录”。

步骤2 在DNS服务商添加一条WAF的子域名和TXT记录。

- 在目标域名“www.example.com”的“操作”列，单击“解析”，如 [图5-17](#)所示。

图 5-17 云解析页面入口



- 在页面的左上角，单击“添加记录集”，进入“添加记录集”页面，配置模式如 [图5-18](#)所示。
 - “主机记录”：将 [步骤1.4](#)中复制的TXT记录粘贴到文本框中。
 - “类型”：选择“TXT-设置文本记录”。
 - “别名”：选择“否”。
 - “线路类型”：全网默认。
 - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
 - “值”：将 [步骤1.4](#)中复制的TXT记录加上引号后粘贴在对应的文本框，例如，“37c795804124dd4a0dd88defff8941f”。
 - 其他的设置保持不变。

图 5-18 添加记录集

The screenshot shows a configuration window titled "添加记录集" (Add Record Set). It contains the following fields and options:

- 主机记录 (Host Record): 37c795804124dd4a0dd88defff8941f example_com
- * 类型 (Type): TXT - 设置文本记录
- * 别名 (Alias): 是 否
- * 线路类型 (Line Type): 全网默认
- * TTL (秒): 300, 5分钟 (selected), 1小时, 12小时, 1天
- * 值 (Value): "37c795804124dd4a0dd88defff8941f"
- 权重 (Weight): 1
- 其他配置 (Other Settings):

Buttons at the bottom: 确定 (Confirm), 取消 (Cancel).

3. 单击“确定”，完成子域名配置。

----结束

5.4.5 如何查询域名提供商？

用户可以通过查询域名注册信息，确认域名所属的DNS服务器信息，然后再根据域名所属的DNS服务器信息进行DNS验证的相关操作。

有关查询域名提供商的详细操作，请参见[如何查询域名提供商？](#)。

5.4.6 如何使用 A 记录进行域名解析？

当客户端和Web应用防火墙之间未使用代理时，当网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

在配置域名接入时，您需要到该域名的DNS服务商处，配置防护域名的别名解析。如果您之前在DNS云解析服务上添加的域名主机记录的“类型”为“A-将域名指向IPv4地址”，请参照[A记录接入](#)完成域名配置。

5.4.7 新旧 CNAME 的区别？

背景

为了提高域名解析的可靠性，WAF针对CNAME做了升级。

为了不影响已添加域名的使用，WAF在已添加域名的基本信息页面保留了旧的CNAME，并呈现了新的CNAME。

新旧 CNAME 的区别

新CNAME实现了双活，即双DNS，为异构的两个DNS解析服务。提高了域名解析的可靠性。

建议您在做域名解析时，选择新的CNAME。

5.5 接入后处理

5.5.1 域名接入 Web 应用防火墙后，能通过 IP 访问网站吗？

域名接入到Web应用防火墙后，可以直接在浏览器的地址栏输入源站IP地址进行访问。但是这样容易暴露您的源站IP，使攻击者可以绕过Web应用防火墙直接攻击您的源站。

建议您参照[源站保护最佳实践](#)配置源站保护。

5.5.2 如何在本地测试 Web 应用防火墙？

把业务流量切到WAF之前，为了确保WAF转发正常，建议您先通过本地验证确保一切配置正常。

进行此操作前，确保添加的防护域名（例如：www.example5.com）的源站服务器协议、地址、端口配置正确，如果“对外协议”类型选择了“HTTPS”，也必须确保上传证书的证书文件和私钥正确。

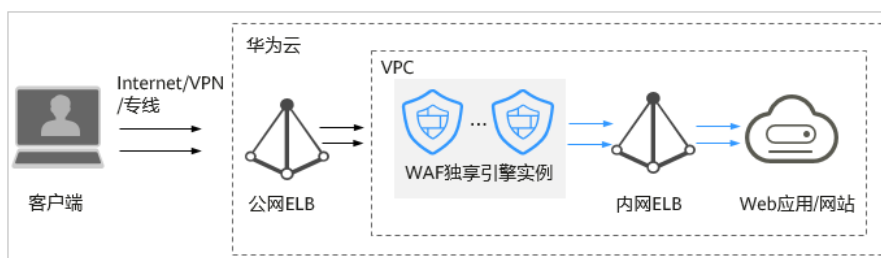
具体的操作步骤请参见[本地验证](#)。

5.5.3 如何设置使流量不经过 WAF，直接访问源站？

当防护网站的“部署模式”为“云模式-CNAME接入”或“独享模式”时，您可以通过以下方式，使访问防护网站的流量不经过WAF，直接访问源站。

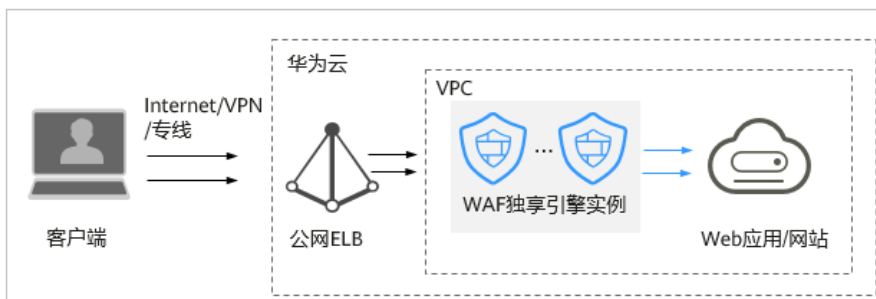
- 云模式-CNAME接入
将防护网站的“工作模式”切换为“Bypass”，使网站的请求直接到达其后端服务器，不再经过WAF。防护网站切换为Bypass工作模式，约3分~5分后开始生效。
- 独享模式
 - 当网站的部署架构如[图5-19](#)所示时（即独享引擎实例后端部署了内网ELB），将EIP从公网ELB上解绑，然后再绑定到内网ELB上，使业务请求绕过WAF，直接到达源站。

图 5-19 独享模式部署架构（独享引擎实例后端部署了内网 ELB）



- 当网站的部署架构如图5-20所示时（即独享引擎实例后端未部署内网ELB），将公网ELB上添加的独享引擎实例移除后，再将源站添加到公网ELB，使业务请求绕过WAF，直接到达源站。

图 5-20 独享模式部署架构（独享引擎实例后端未部署内网 ELB）



约束条件


当防护网站的“部署模式”为“云模式”时，只有有出现以下情况，才能将“工作模式”切换为“Bypass”：


- 当有测试等特殊场景，需要将业务恢复到没有接入WAF的状态，可以通过Bypass功能切换。
- 排查网站异常，例如报502、504或其他不兼容等问题。
- 在Web应用防火墙前面未使用代理。

云模式-CNAME 接入的配置操作

通过将防护网站的“工作模式”切换为“Bypass”，使访问防护网站的流量不经过WAF，直接访问源站。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“工作模式”列，单击 ，选择工作模式。

图 5-21 切换工作模式



----结束

独享模式配置操作-独享引擎实例后端部署了内网 ELB

通过将EIP从公网ELB上解绑，然后再绑定到内网ELB上，使访问防护网站的流量不经过WAF，直接访问源站。



- 步骤1** 单击管理控制台左上角的 ，选择区域或项目。
- 步骤2** 单击页面左上方的 ，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。
- 步骤3** 在“负载均衡器”页面，目标公网ELB所在行“操作”列，选择“更多 > 解绑IPv4公网IP”，如图5-22所示。

图 5-22 解绑公网 ELB 上绑定的 EIP

名称	状态	实例规格类型	规格	应用型(HTTP/HTTPS) 大型 I	10.100.100.243 (IPv4私有IP) vpc-waf-only (虚拟私有云)	Listener-81 (HTTP/81) Listener-57a8 (HTTP/80)	IPv4 100 Mbit/s 按量 按带宽	计费模式 2021/07/02 12:...	default	修改IPv4带宽 删除 更多
elb-waf-only	运行中	独享型	应用型(HTTP/HTTPS) 大型 I elbv3.basic.1az 200 LCU	10.100.100.243 (IPv4私有IP) vpc-waf-only (虚拟私有云)	Listener-81 (HTTP/81) Listener-57a8 (HTTP/80)	IPv4 100 Mbit/s 按量 按带宽	...	default	修改IPv4带宽 删除 更多	
elb-icst-test2	运行中	共享型	--	192.168.10.147 (IPv4私有IP) vpc-e936 (虚拟私有云)	Listener-53ac (TCP/80)	IPv4 1 Mbit/s 按量 按带宽	...	default	修改IPv4带宽 修改IPv4公网IP 修改IPv4私有IP 变更规格	
resource-tenant	运行中	共享型	--	192.168.10.59 (IPv4私有IP) vpc-e936 (虚拟私有云)	Listener-7777 (HTTP/7777) Listener-6868 (HTTP/6868)	--	...	default	修改IPv4带宽	

- 步骤4** 在弹出的提示框中，单击“是”，将EIP从公网ELB上解绑。
- 步骤5** 在“负载均衡器”页面，内网ELB所在行“操作”列，选择“更多 > 绑定IPv4公网IP”。
- 步骤6** 在弹出的“绑定IPv4公网IP”对话框中，选择步骤3解绑的公网IP后，单击“确定”，将EIP绑定到内网ELB。

----结束

独享模式配置操作-独享引擎实例后端未部署内网 ELB

通过将公网ELB上添加的独享引擎实例移除，再将源站添加到公网ELB，使业务请求绕过WAF，直接到达源站。



- 步骤1** 单击管理控制台左上角的 ，选择区域或项目。
- 步骤2** 单击页面左上方的 ，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。
- 步骤3** 在负载均衡器所在行的“名称”列，单击目标负载均衡器名称，进入ELB“基本信息”页面。

图 5-23 负载均衡器列表

名称	状态	实例规格类型	规格	应用型(HTTP/HTTPS) 小型 I	10.100.100.73 (IPv4私有IP) vpc-waf-only (虚拟私有云)	Listener-80 (HTTP/80)	公网计费信息	计费模式 2022/01/05 17:...	default	修改IPv4带宽 删除 更多
elb-waf-only-2	运行中	独享型	应用型(HTTP/HTTPS) 小型 I elbv3.basic.1az 10 LCU	10.100.100.73 (IPv4私有IP) vpc-waf-only (虚拟私有云)	Listener-80 (HTTP/80)	--	...	default	修改IPv4带宽 删除 更多	
elb-shared	运行中	共享型	--	10.100.100.6 (IPv4私有IP) vpc-waf-only (虚拟私有云)	Listener-9acb (TCP/80)	--	...	default	修改IPv4带宽 删除 更多	
elb-front-end	运行中	共享型	--	10.100.100.187 (IPv4私有IP) vpc-waf-only (虚拟私有云)	Listener-80 (HTTP/80)	--	...	default	修改IPv4带宽 删除 更多	

- 步骤4** 选择“后端服务器组”页签，勾选待移除的独享引擎实例后，单击“移除”，如图5-24所示。

图 5-24 移除公网 ELB 上添加的独享引擎实例



步骤5 在弹出的提示框中，单击“是”，将独享引擎实例从公网ELB移除。

步骤6 单击“添加云服务器”，在弹出的“添加后端服务器”对话框中，选择源站服务器。

步骤7 单击“下一步”，设置后端端口后，单击“完成”，将源站服务器添加到公网ELB。

图 5-25 添加源站服务器



----结束

5.5.4 域名接入 WAF 后，为什么无法开启防护模式？

其他客户在WAF配置了同样的域名，导致域名所有权被另外一个租户占有了。此时，您需要前往您的DNS服务商处，添加一条“子域名”，并为该子域名配置一条“TXT记录”。

具体的配置方法请参见[未配置子域名和TXT记录的影响？](#)。

6 业务中断排查

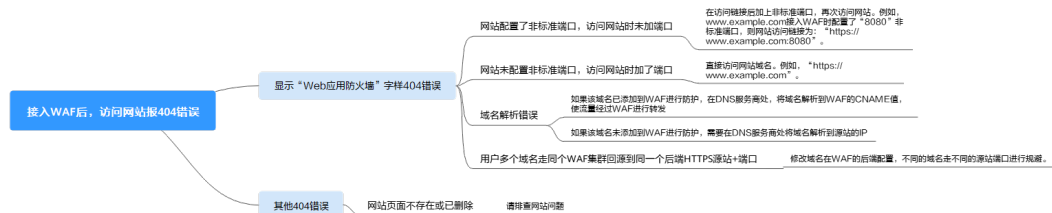
6.1 如何排查 404/502/504 错误?

网站接入WAF防护之后，若您访问网站时出现404 Not Found、502 Bad Gateway，504 Gateway Timeout等错误，请参考以下方法解决。

404 Not Found 错误排查思路和处理建议

网站接入WAF后，访问网站时出现404 Not Found错误，请参考图6-1进行排查处理。

图 6-1 404 错误排查思路



- 如果访问网站返回如图6-2所示页面，原因和处理建议说明如下：

图 6-2 404 页面



原因一：添加防护域名到WAF时，配置了非标准端口，例如配置了如图6-3所示的非标准端口业务，访问网站时未加端口用“https://www.example.com”或者“https://www.example.com:80”访问网站。

图 6-3 非标准端口配置

The screenshot shows the WAF configuration page for the domain 'www.example.com'. Under the 'Source Configuration' (源站配置) section, the 'Protection Port' (防护域名端口) is set to '8080'. Below this, the 'Server Configuration' (服务器配置) table is visible, with columns for 'Outward Protocol' (对外协议), 'Source Protocol' (源站协议), 'Source Address' (源站地址), 'Source Port' (源站端口), and 'Weight' (权重). The first row shows 'HTTP' for both protocols, 'IPv4' for the address, and '80' for the port. A '+ Add' button is at the bottom.

处理建议：在访问链接后加上非标准端口，再次访问源站，如“https://www.example.com:8080”。

原因二：添加防护域名到WAF时，没有配置非标准端口，访问时使用了非标准端口或者“源站端口”配置的非标准端口，例如配置了如图6-4所示的防护业务，用“https://www.example.com:8080”访问网站。

图 6-4 未配置非标准端口

The screenshot shows the WAF configuration page for the domain 'www.example.com'. Under the 'Source Configuration' (源站配置) section, the 'Protection Port' (防护域名端口) is set to 'Standard Port' (标准端口). The 'Server Configuration' (服务器配置) table below shows 'HTTP' for both protocols, 'IPv4' for the address, and '80' for the port. A '+ Add' button is at the bottom.

说明

没有配置非标准端口的情况下，WAF默认防护80/443端口的业务。其他端口的业务不能正常访问，如果您需要防护其他非标准端口的业务，请重新进行域名配置。

处理建议：直接访问网站域名，如“https://www.example.com”。

原因三：域名解析错误。

处理建议：

- 如果该域名已添加到WAF进行防护，参照[域名解析](#)重新完成域名接入的操作，使流量经过WAF进行转发。
- 如果该域名未添加到WAF进行防护，需要在DNS服务商处将域名解析到源站的IP。

原因四：用户多个域名走同个WAF集群回源到同一个后端HTTPS源站+端口，由于WAF回源是长连接复用的，后端源站节点无法分辨是哪个域名（nginx通过Host和

SNI分辨)，会有一些几率出现A域名的请求转发到B域名的后端，所以会出现404。

处理建议：修改域名在WAF的后端配置，不同的域名走不同的源站端口进行规避。

- 如果访问网站时，返回的不是图6-2所示的404页面，原因和处理建议说明如下：
 - 原因：**网站页面不存在或已删除。
 - 处理建议：**请排查网站问题。

502 Bad Gateway 错误排查思路和处理建议

完成WAF配置之后网站访问正常，但过一段时间，访问页面返回502，或者大概率出现502，请参考图6-5进行排查处理。

图 6-5 502 错误排查思路

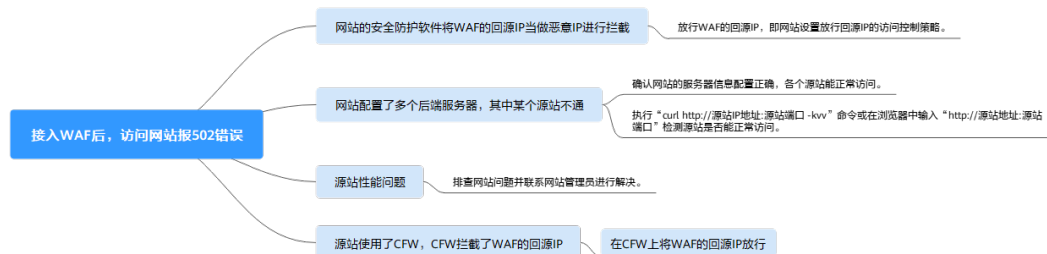


表 6-1 502 错误问题处理


可能原因	处理建议
原因一：网站使用了其他的安全防护软件（如360、安全狗、云锁或云盾等安全防护软件），这些软件把WAF的回源IP当成了恶意IP，拦截了WAF转发的请求	源站服务器配置放行WAF回源IP的访问控制策略。 <ul style="list-style-type: none"> 云模式：请参见如何放行云模式WAF的回源IP段？。 独享模式：请参见放行独享引擎回源IP。
原因二：网站的后端配置了多个服务器，其中某个源站不通	请参照 步骤1~步骤8 ，确保所有源站都可以正常访问。
原因三：网站服务器性能问题	排查网站问题并联系您的网站管理员进行解决。
原因四：源站使用了CFW，CFW拦截了WAF的回源ip	该问题有以下排查方法： <ul style="list-style-type: none"> 如果源站使用了CFW，在CFW的控制台查看拦截日志，排查是否有相关的事件产生。 查看CFW的访问控制策略，排查是否配置了拦截WAF的回源IP 在CFW上将WAF的回源IP放行，具体操作请参见 配置访问控制策略


当网站的后端配置了多个服务器，其中某个源站不通时，请参照以下操作步骤，检查网站的服务器是否配置正确。

须知

修改服务器信息，大约需要2分钟同步生效。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行中，单击目标域名，进入域名基本信息页面。


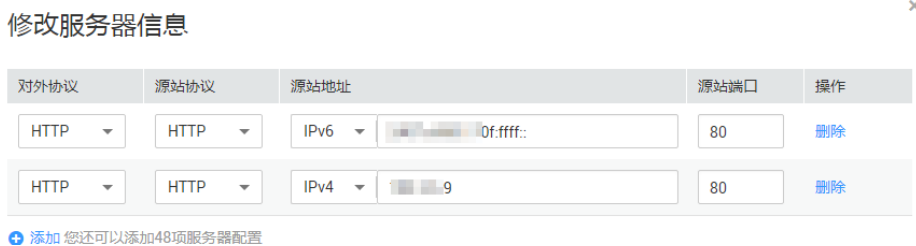
步骤6 在“源站服务器”栏中，单击 ，进入“修改服务器信息”页面，确保对外协议、源站协议、源站地址、端口等信息配置正确。

图 6-6 服务器配置



步骤7 检测各个源站是否能正常访问。

- 在主机上执行以下命令进行检测。

```
curl http://xx.xx.xx.xx:yy -kvv
```

说明

- xx.xx.xx.xx代表源站服务器的源站IP地址，yy代表源站服务器的源站端口，xx.xx.xx.xx和yy必须是同一个服务器的源站地址和端口。
- 执行curl命令的主机需要满足以下条件：
 - 网络通信正常。
 - 已安装curl命令。Windows操作系统的主机需要手动安装curl，其他操作系统自带curl。

图 6-7 检测源站

```
[root@localhost ~]# curl http://[REDACTED].47.58:8080 -kvv
* About to connect() to [REDACTED].47.58 port 8080 (#0)
* Trying [REDACTED].47.58...
* Connection refused
* Failed connect to [REDACTED].47.58:8080; Connection refused
* Closing connection 0
curl: (7) Failed connect to [REDACTED].47.58:8080; Connection refused
```

- 如果回显信息提示连接正常表示可以正常访问网站。
- 如果回显信息提示“connection refused”表示源站不通，不能正常访问网站，请执行**步骤8**。

- 在浏览器中输入“http://源站地址:源站端口”进行检测。
 - 如果可以访问，表示网站访问正常。
 - 如果不能访问，表示源站不通，不能正常访问网站，请执行**步骤8**。

步骤8 检测服务器是否运行正常。

如果运行不正常，请尝试重启服务器。

----结束

504 Gateway Timeout 错误排查思路和处理建议

完成WAF域名接入配置之后，业务正常，但当业务量增加时，发生504错误的概率增加，直接访问源站IP也有一定概率出现504错误，请参考**图6-8**进行排查处理。

图 6-8 504 错误排查思路



表 6-2 504 错误问题处理

可能原因	排查方法	处理建议
原因一：后端服务器性能问题（连接数，CPU 内存占用过大等）	源站性能问题，可以排查源站访问日志以及访问流量情况，定性分析。	<ul style="list-style-type: none"> 优化服务器的相关配置，包括TCP网络参数的优化配置，ulimit相关参数设置等。 如果是云模式部署方式，建议在ELB上增加后端服务器组或创建新的ELB，支撑大量增长的业务量。 <ul style="list-style-type: none"> 增加后端服务器组的详细操作，请参见添加或删除后端服务器（共享型）。 配置新ELB的操作，请参考步骤1~步骤8。 如果“对外协议”是HTTPS，建议在WAF设置HTTPS转发，回源走HTTP协议即“源站协议”设置为HTTP，降低后端服务器的计算压力。 修改服务器信息的详细操作，请参见修改服务器信息。 使用CC防护规则，拦截恶意流量。
原因二： <ul style="list-style-type: none"> 安全组未将WAF回源IP设置为白名单或未放开端口 源站有防火墙设备，且该防火墙设备拦截了WAF的回源IP 	建议采用以下方法进行排查： <ul style="list-style-type: none"> 排查客户源站是否有安全组，防火墙，服务器安全软件等。 在客户端与WAF上同时进行抓包分析，排查源站防火墙等设备对WAF的长连接是否有主动丢包的现象。 	<ul style="list-style-type: none"> 源站服务器配置放行WAF回源IP的访问控制策略。 <ul style="list-style-type: none"> 云模式：请参见如何放行云模式WAF的回源IP段？。 独享模式：请参见放行独享引擎回源IP。 建议您关闭防火墙和服务器安全防护软件。

可能原因	排查方法	处理建议
<p>原因三：连接超时、read超时</p> <p>说明</p> <ul style="list-style-type: none"> 源站响应时间过长导致504（数据库查询时间过长，大文件上传时间过长，源站故障等）。 WAF回源到客户源站超时时间大多为60秒或180秒，若超时则会报错504。 	<p>该问题有以下排查方法：</p> <ul style="list-style-type: none"> 绕过WAF，直接访问客户源站，查看响应时长 查看全量日志里面访问日志源站响应时长 建议客户绕过WAF测试上传功能，并检查客户上传文件大小 	<ul style="list-style-type: none"> 数据库查询时间过长： <ul style="list-style-type: none"> 调整优化业务，尽量缩短查询时长，优化用户体验。 修改请求的交互方式，让这种长连接在 60s 内能有一些数据交互（如，ack报文、心跳包、keep-alive等任何可以维持会话的报文）。 大文件上传时间过长： <ul style="list-style-type: none"> 调整优化业务，尽量缩短文件上传时间。 建议使用FTP方式上传文件。 直接通过IP上传，或者使用没有被WAF防护的域名上传。 使用WAF的独享模式，独享WAF回源超时默认为180s。 源站故障类：检查源站业务是否正常。
<p>原因四：源站带宽不足，访问量过大，带宽超限制</p>	<p>该问题有以下排查方法：</p> <ul style="list-style-type: none"> 若客户配置的WAF后端为7层ELB，则可以在ELB上查504相关日志 若客户配置的WAF后端为4层ELB，则可以在ELB上查“Traffic exceeded the bandwidth threshold”相关字段日志 若客户配置的WAF后端为EIP，则在504高峰查看EIP流量监控。 	<p>扩展源站服务器带宽。</p>

可能原因	排查方法	处理建议
原因五：源站使用了CFW，CFW拦截了WAF的回源ip	该问题有以下排查方法： <ul style="list-style-type: none">如果源站使用了CFW，在CFW的控制台查看拦截日志，排查是否有相关的事件产生。查看CFW的访问控制策略，排查是否配置了拦截WAF的回源IP	在CFW上将WAF的回源IP放行，具体操作请参见 配置访问控制策略


创建新的ELB，参照以下方法将ELB的EIP作为服务器的IP地址，接入WAF。

须知

修改服务器信息，大约需要2分钟同步生效。

步骤1 [创建共享型负载均衡器](#)。

步骤2 [登录管理控制台](#)。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“域名”列中，单击目标域名，进入域名基本信息页面。


步骤6 在“源站服务器”栏中，单击 ，进入“修改服务器信息”页面，单击“添加”，新增后端服务器。

图 6-9 服务器配置



步骤7 将“源站地址”设置为ELB的弹性公网IP地址。

步骤8 单击“确定”，服务器信息修改成功。


----结束

6.2 域名/IP 接入状态显示“未接入”，如何处理？

故障现象

添加防护域名或IP后，域名或IP接入WAF失败，即防护网站“域名接入进度”没有显示“已接入”。

须知

- WAF每隔一小时就会自动检测防护网站的“接入状态”，当WAF统计防护网站在5分钟内达到20次访问请求时，将认定该防护网站已成功接入WAF。
- WAF默认只检测两周内新增或更新的域名的“接入状态”，如果域名创建时间在两周前，且最近两周内没有任何修改，您可以在“域名接入”进度栏，单击，手动刷新接入状态。

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

- 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
- 云模式-ELB接入：域名或IP，华为云的Web业务
- 独享模式：域名或IP，华为云的Web业务



云模式排查思路和处理建议

防护网站的“部署模式”为“云模式”时，请参考图6-10和表6-3进行排查处理。

图 6-10 云模式排查思路



表 6-3 接入 WAF 失败问题处理

可能原因	处理建议
原因一：域名“接入状态”未刷新	在防护网站“接入状态”栏，单击  刷新状态。
原因二：访问量未达到WAF统计要求 须知 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	<ol style="list-style-type: none"> 在1分钟内多次访问防护网站。 在防护网站“接入状态”栏，单击  刷新状态。
原因三：域名参数配置错误	<p>须知</p> <p>WAF支持防护以下类型域名：</p> <ul style="list-style-type: none"> 一级域名，例如，example.com 单域名/二级域名等子域名，例如，www.example.com 泛域名，例如，*.example.com <p>example.com与www.example.com是不同的域名，请确认“防护域名”配置正确。</p> <p>请参照以下步骤确保域名参数配置正确。</p> <ol style="list-style-type: none"> 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”，进入命令提示符窗口。 运行ping 域名在WAF对应的CNAME值（例如ping e59e684e2278043ae98a5423aef8ee329.vip.huaweicloudwaf.com），获取WAF的回源IP。 用文本编辑器打开hosts文件，hosts文件一般位于“C:\Windows\System32\drivers\etc\”路径下。 在hosts文件添加记录：防护域名 域名对应的WAF回源IP。 修改hosts文件后保存，在命令提示符窗口中运行ping 防护域名（例如ping www.example.com）。 <p>如果回显信息中的IP地址为2中的WAF回源IP地址，说明域名参数配置正确。</p> <p>详细操作请参见本地验证。</p> <p>如果域名参数配置错误，删除该域名后重新添加防护网站。</p>

可能原因	处理建议
原因四：未配置域名解析或代理回源地址	<p>确认接入WAF的网站是否使用高防、CDN、云加速等代理。</p> <ul style="list-style-type: none"> 是：确保网站的“是否已使用代理”已配置为“四层代理”或“七层代理”。 <ul style="list-style-type: none"> 将CDN等代理回源地址修改为WAF的“CNAME”。 （可选）在DNS服务商处添加一条WAF的“子域名”和“TXT记录”。 否：到该域名的DNS服务商处，配置防护域名的别名解析。 <p>详细操作请参见域名接入WAF。</p>
原因五：域名解析或代理回源地址配置错误	<p>请参照以下步骤验证域名的CNAME是否配置成功。</p> <ol style="list-style-type: none"> 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”，进入命令提示符窗口。 执行nslookup命令，查询CNAME。如果回显信息的域名在WAF上的CNAME，则表示配置成功。 <p>以域名www.example.com为例。 <pre>nslookup www.example.com</pre></p> <p>如果CNAME配置失败，请参见域名接入WAF重新修改DNS解析或回源地址。</p>



独享模式排查思路和处理建议

防护网站的“部署模式”为“独享模式”时，请参考[图6-11](#)和[表6-4](#)进行排查处理。

图 6-11 独享模式排查思路



表 6-4 独享模式接入 WAF 失败问题处理

可能原因	处理建议
原因一：域名/IP “接入状态” 未刷新	在防护网站“接入状态”栏，单击  刷新状态。
原因二：访问流量未达到WAF统计要求 须知 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击  刷新状态。
原因三：域名/IP参数配置错误	查看基本信息 ，检查域名/IP参数是否正确。 如果域名/IP配置错误，删除该域名/IP后重新添加防护网站。
原因四：没有为独享模式实例配置负载均衡，配置的负载均衡未绑定弹性公网IP	1. 为独享引擎实例 配置负载均衡 。 2. 为弹性负载均衡绑定弹性公网IP 。
原因五：独享模式实例负载均衡配置错误或负载均衡绑定弹性公网IP错误	<ul style="list-style-type: none"> ● 配置负载均衡后，当WAF独享引擎实例的“健康检查结果”为“正常”时，说明弹性负载均衡配置成功。健康检查异常的排查思路请参见健康检查异常。 ● 为弹性负载均衡绑定弹性公网IP后，可以查看绑定的弹性公网IP，说明绑定成功。

云模式-ELB 接入排查思路和处理建议

防护网站的“部署模式”为“云模式-ELB接入”时，请参考图6-12和表6-5进行排查处理。

图 6-12 ELB 模式排查思路

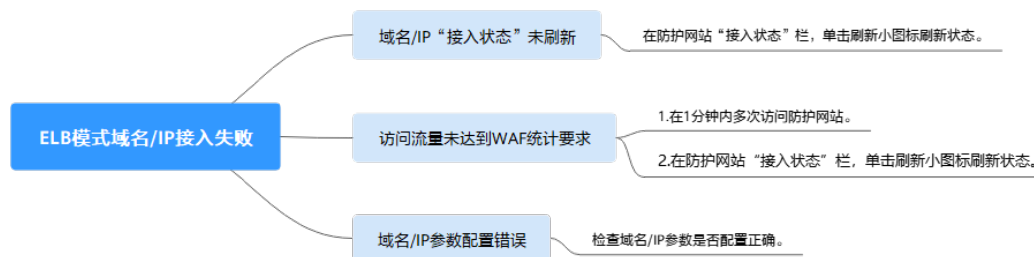




表 6-5 ELB 模式接入 WAF 失败问题处理

可能原因	处理建议
原因一：域名/IP“接入状态”未刷新	在防护网站“接入状态”栏，单击  刷新状态。
原因二：访问流量未达到WAF统计要求 须知 防护网站接入WAF后，当WAF统计防护网站在5分钟内 有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击  刷新状态。
原因三：域名/IP参数配置错误	查看域名基本信息 ，检查域名/IP参数是否正确。 如果域名/IP配置错误，删除该域名/IP后重新添加防护网站。

6.3 WAF 误拦截了正常访问请求，如何处理？

当WAF根据您配置的防护规则检测到符合规则的恶意攻击时，会按照规则中的防护动作（仅记录、拦截等），在“防护事件”页面中记录检测到的攻击事件。

须知

如果您已开通企业项目，请务必在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能处理该企业项目下的误报事件。有关企业项目的详细介绍，请参见[管理项目和企业项目](#)。

在误拦截事件所在行的“操作”列中，单击“详情”，查看事件详细信息。如果确认该防护事件为误报事件时，您可以参照[表6-6](#)对该事件进行误报处理。处理后，WAF将不再拦截该事件，即“防护事件”页面中将不再显示该攻击事件，您也不会收到该攻击事件的告警通知。

表 6-6 误报处理说明

命中规则类型	命中规则	处理方式
WAF内置防护规则	<ul style="list-style-type: none">Web基础防护规则 防范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/代码注入等常规的Web攻击，以及Webshell检测、深度反逃逸检测等Web基础防护。网站反爬虫的“特征反爬虫”规则 可防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫。	在该攻击事件所在行的“操作”列，单击“误报处理”，详细操作请参见 处理误报事件 。
自定义防护规则	<ul style="list-style-type: none">CC攻击防护规则精准访问防护规则黑白名单规则地理位置访问控制规则网页防篡改规则网站反爬虫的“JS脚本反爬虫”规则防敏感信息泄露规则隐私屏蔽规则	在拦截该攻击事件的防护规则页面，删除对应的防护规则。
其他	<p>“非法请求”访问请求</p> <p>说明 当遇到以下情况时，WAF将判定该访问请求为非法请求并拦截该访问请求：</p> <ul style="list-style-type: none">POST/PUT使用“form-data”时，表单的参数个数多于8192个。URI的参数个数多于2048个。Header个数超过512个。	“误报处理”按钮置灰不能使用，请参见 配置精准访问防护规则 放行该访问请求。

6.4 WAF 误拦截了“非法请求”访问请求，如何处理？

问题现象

防护网站接入WAF后，访问请求被WAF拦截，在“防护事件”页面查看防护日志，显示访问请求为“非法请求”且误报处理按钮置灰不能使用，如图6-13所示。

图 6-13 非法请求被 WAF 拦截

时间	源IP	地理位置	防护域名	URL	恶意负载	事件类型	防护动作	操作
2021/05/13 17:25:59 GMT...	10.25.63.141	Reserved IP	www.huaweicloud.com	/<script>alert()</script>	/<script>alert()</script>	XSS攻击	拦截	详情 误报处理
2021/05/11 18:06:05 GMT...	10.142.204.230	Reserved IP	www.huaweicloud.com	/123		非法请求	拦截	详情 误报处理

可能原因

当遇到以下情况时，WAF将判定该访问请求为非法请求并拦截该访问请求：

- POST/PUT使用“form-data”时，表单的参数个数多于8192个。
- URI的参数个数多于2048个。
- Header个数超过512个。

处理建议

当确认访问请求为正常请求时，请通过[配置精准访问防护规则](#)放行该访问请求。

6.5 为什么误报处理不能使用了？

误报处理不能使用时，请先确认登录管理控制台账号是否授予了使用WAF的权限，有关WAF权限的详细介绍，请参见[WAF权限管理](#)。

须知

如果您已开通企业项目，处理误报事件时请在“企业项目”下拉列表中选择您所在的企业项目。

- 基于自定义规则（CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则等）拦截或记录的攻击事件，无法执行“误报处理”操作，如果您确认该攻击事件为误报，可在自定义规则页面，将该攻击事件对应的防护规则删除或关闭。
- 防护网站接入WAF后，当WAF检测到访问请求的以下参数超过512个时，WAF将判定该访问请求为非法请求并拦截该访问请求，且误报处理按钮置灰不能使用：
 - POST/PUT使用“form-data”时，表单的参数个数多于8192个。
 - URI的参数个数多于2048个。
 - Header个数超过512个。

图 6-14 非法请求被 WAF 拦截

时间	源IP	地理位置	防护域名	URL	恶意负载	事件类型	防护动作	操作
2021/05/13 17:25:59 GMT...	10.25.63.141	Reserved IP	www.huaweicloud.com	/<script>alert()</script>	/<script>alert()</script>	XSS攻击	拦截	详情 误报处理
2021/05/11 18:06:05 GMT...	10.142.204.230	Reserved IP	www.huaweicloud.com	/123		非法请求	拦截	详情 误报处理

有关非法请求的处理建议，请参见[WAF误拦截了“非法请求”访问请求，如何处理？](#)。

6.6 如何放行云模式 WAF 的回源 IP 段？

网站以“云模式-CNAME”方式成功接入WAF后，建议您在源站服务器上配置只放行WAF回源IP的访问控制策略，防止黑客获取源站IP后绕过WAF直接攻击源站，以确保源站安全、稳定、可用。

须知

网站成功接入WAF后，如果访问网站频繁出现502/504错误，建议您检查并确保源站服务器已配置了放行WAF回源IP的访问控制策略。

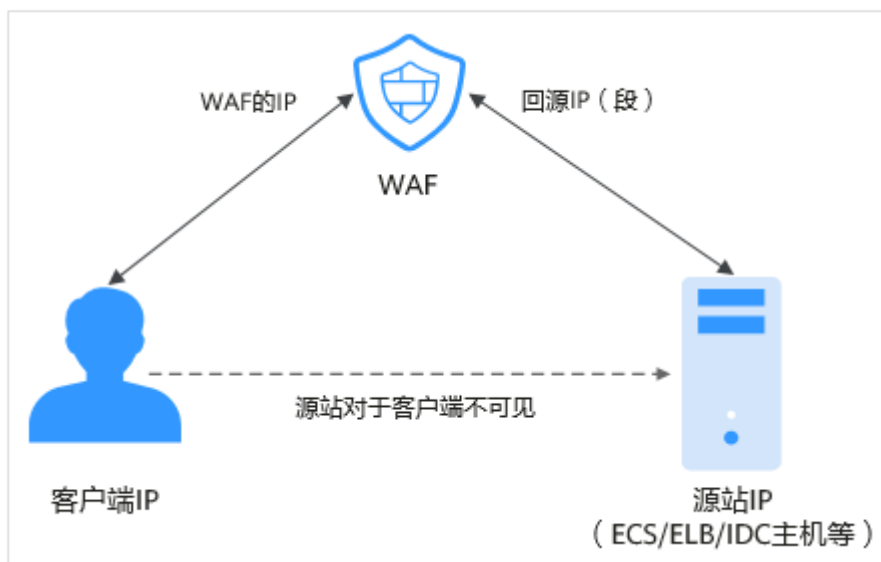
什么是回源 IP？

回源IP是WAF用来代理客户端请求服务器时用的源IP，在服务器看来，接入WAF后所有源IP都会变成WAF的回源IP，而真实的客户端地址会被加在HTTP头部的XFF字段中。

说明

- WAF的回源IP会因为扩容/新建集群而增加，对于一个客户的存量域名，一般回源IP会固定在2~4个集群的几个C类IP地址（192.0.0.0~223.255.255.255）上。
- 一般情况下，在没有灾备切换或其他调度切换集群的场景下，回源IP不会变。且WAF后台做集群切换时，会探测源站安全组配置，确保不会因为安全组配置导致业务整体故障。

图 6-15 回源 IP



回源 IP 检测机制

回源IP（该IP在回源IP段中）是随机分配的。回源时WAF会监控回源IP的状态，如果该IP异常，WAF将剔除该异常IP并随机分配正常的回源IP接收/转发访问请求。

为什么需要放行回源 IP 段？


WAF实例的IP数量有限，且源站服务器收到的所有请求都来自这些IP。在源站服务器上的安全软件很容易认为这些IP是恶意IP，有可能触发屏蔽WAF回源IP的操作。一旦WAF的回源IP被屏蔽，WAF的请求将无法得到源站的正常响应，因此，在接入WAF防护后，您需要在源站服务器的安全软件上设置放行所有WAF回源IP，不然可能会出现网站打不开或打开极其缓慢等情况。


说明

网站接入WAF后，建议您卸载源站服务器上的其他安全软件，或者配置只允许来自WAF的访问请求访问您的源站，这样既可保证访问不受影响，又能防止源站IP暴露后被黑客直接攻击。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在网站列表上方，单击“Web应用防火墙回源IP网段”，查看Web应用防火墙所有回源IP段。

图 6-16 回源 IP 网段



步骤6 在“Web应用防火墙的回源IP网段”对话框，单击“复制IP段”，复制所有回源IP。

图 6-17 Web 应用防火墙的回源 IP 网段



步骤7 打开源站服务器上的安全软件，将复制的IP段添加到白名单。


- 源站服务器部署在华为云ECS上，请参考[源站服务器部署在ECS上，放行WAF回源IP](#)进行操作。
- 源站服务器部署在华为云ELB上，请参考[源站服务器部署在华为云ELB上，放行WAF回源IP](#)进行操作。
- 如果您同时使用了华为云云防火墙（CFW），请参考[添加防护规则](#)放行WAF的回源IP。
- 如果后端资源在其他云厂商，请在对应安全组、访问控制等中添加信任WAF的回源IP。
- 如果源站服务器只安装了个人版杀毒软件，通常这些软件没有配置加白IP的界面。如果是对外提供Web业务的服务器，建议您安装服务器版本的企业安全软件，或华为云主机安全服务产品，这些产品会识别一些请求量较大的IP的socket，并偶发断开连接，一般情况下不会拦截WAF的回源IP。


----结束

源站服务器部署在 ECS 上，放行 WAF 回源 IP

如果您的源站服务器直接部署在华为云ECS上，请参考以下操作步骤设置安全组规则，只放行WAF回源IP段。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“计算 > 弹性云服务器 ECS”。

步骤4 在目标ECS所在行的“名称/ID”列中，单击目标ECS实例名称，进入ECS实例的详情页面。

步骤5 选择“安全组”页签，单击“更改安全组”。

步骤6 单击安全组名称，进入安全组基本信息页面。

步骤7 选择“入方向规则”页签，单击“添加规则”，进入“添加入方向规则”页面，如图 6-18 所示，参数配置说明如表 6-7 所示。

图 6-18 添加入方向规则

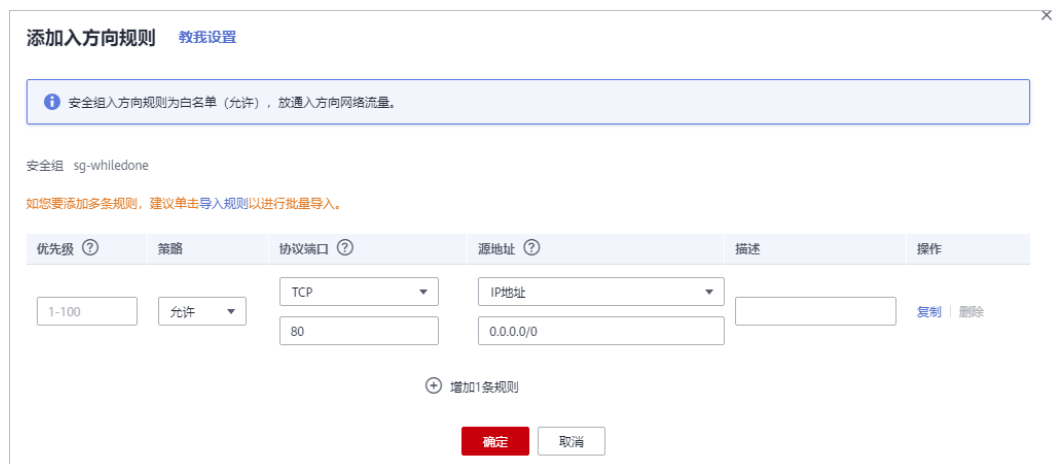


表 6-7 入方向规则参数配置说明

参数	配置说明
协议端口	安全组规则作用的协议和端口。选择“自定义TCP”后，在TCP框下方输入源站的端口。
源地址	逐一添加步骤6中复制的所有WAF回源IP段。 说明 一条规则配置一个IP。单击“增加1条规则”，可配置多条规则，最多支持添加10条规则。

步骤8 单击“确定”，安全组规则添加完成。


成功添加安全组规则后，安全组规则将允许WAF回源IP段的所有入方向流量。


----结束

源站服务器部署在华为云 ELB 上，放行 WAF 回源 IP

如果您的源站服务器直接部署在华为云ELB上，请参考以下操作步骤设置访问控制（白名单）策略，只放行WAF回源IP段。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“网络 > 弹性负载均衡 ELB”。

步骤4 在目标ELB所在行的“监听器”列中，单击监听器名称，进入监听器的详情页面。

步骤5 在目标监听器所在行的“访问控制”列，单击“设置”。

图 6-19 监听器列表



步骤6 在弹出的对话框中，“访问控制”选择“白名单”。



1. 单击“创建IP地址组”，将**步骤6**中独享引擎实例的回源IP地址添加到“IP地址组”。
2. 在“IP地址组”的下拉框中选择**步骤6.1**中创建的IP地址组。

步骤7 单击“确定”，白名单访问控制策略添加完成。

----结束

6.7 连接超时时长是多少，是否可以手动设置该时长？

- 浏览器到WAF引擎的连接超时时长默认是120秒，该值取决于浏览器的配置，该值在WAF界面不可以手动设置。
- WAF到客户源站的连接超时时长默认为30秒，该值可以在WAF界面手动设置，但仅“独享模式”和“云模式”的专业版、铂金版支持手动设置连接超时时长。

在域名的基本信息页面，开启“超时配置”并单击 ，设置“连接超时”、“读超时”、“写超时”的时间，并单击  保存设置。

6.8 如何解决重定向次数过多？

在WAF中完成了域名接入后，请求访问目标域名时，如果提示“重定向次数过多”，一般是由于您在服务器后端配置了HTTP强制跳转HTTPS，在WAF上只配置了一条HTTPS（对外协议）到HTTP（源站协议）的转发，强制WAF将用户的请求进行跳转，所以造成死循环。可在WAF中**修改服务器信息**，配置两条HTTP（对外协议）到HTTP（源站协议）和HTTPS（对外协议）到HTTPS（源站协议）的服务器信息。配置完成后，服务器信息如**图6-20**所示。

图 6-20 配置示例

修改服务器信息

对外协议	源站协议	源站地址	源站端口	权重	主备
HTTP	HTTP	IPv4 1.	80	1	主用服务器
HTTPS	HTTPS	IPv4 12	443	1	主用服务器

添加 您还可以添加48个源站地址
若您的源站服务器配置了多个不同的主备服务器，请确保不同“对外协议-源站地址”组合下至少有一台主用服务器。

IPv6防护 开启 关闭

您的域名对外协议支持HTTPS，域名使用证书

国际证书 已有证书/12222

国密证书 请选择证书

若您选用国密证书WAF将会切换至国密集群，证书切换会影响服务端与客户端的TLS握手过程，请谨慎使用

导入新证书

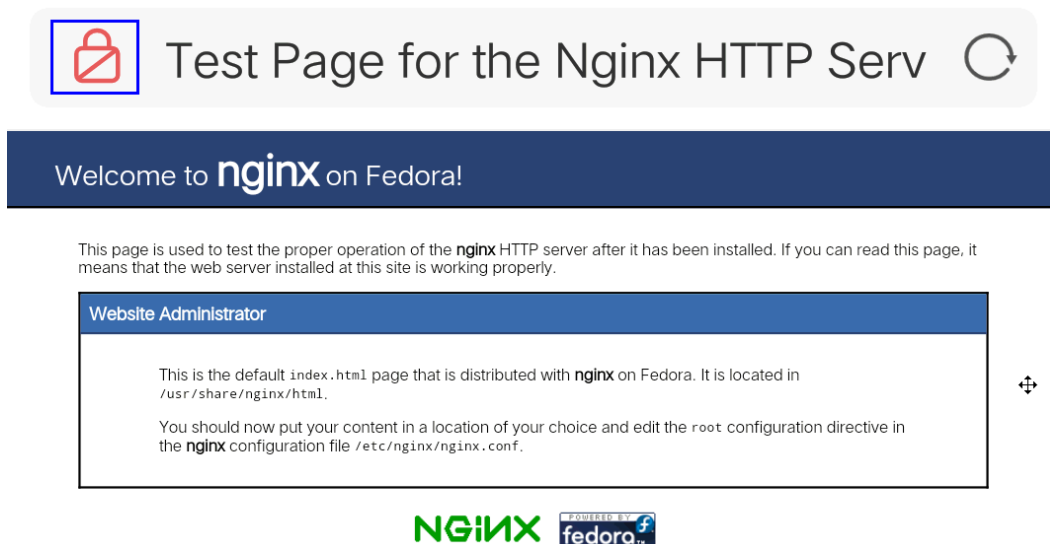
您对服务器配置已进行了修改，如需应用请点击确定，撤销请点击取消。

确认 取消

6.9 如何解决 HTTPS 请求在部分手机访问异常？

打开手机浏览器，访问防护域名，如果出现类似于图6-21所示的页面，则表示该手机上HTTPS请求访问异常，该问题是由于上传的证书链不完整，可参照[如何解决证书链不完整？](#)解决。

图 6-21 访问异常



6.10 如何解决证书链不完整？

如果证书机构提供的证书在用户平台内置信任库中查询不到，且证书链中没有颁发机构，则证明该证书是不完整的证书。使用不完整的证书，当用户访问防护域名对应的浏览器时，因不受信任而不能正常访问防护域名对应的浏览器。

按以下两种方法可解决此问题：

- 手动构造完整证书链，并上传证书。（WAF自动补全证书链功能正在开发中，敬请期待！）
- 重新上传正确的证书。

Chrome最新版本一般是支持自动验证信任链，以华为的证书为例，手工构造完整的证书链步骤如下：

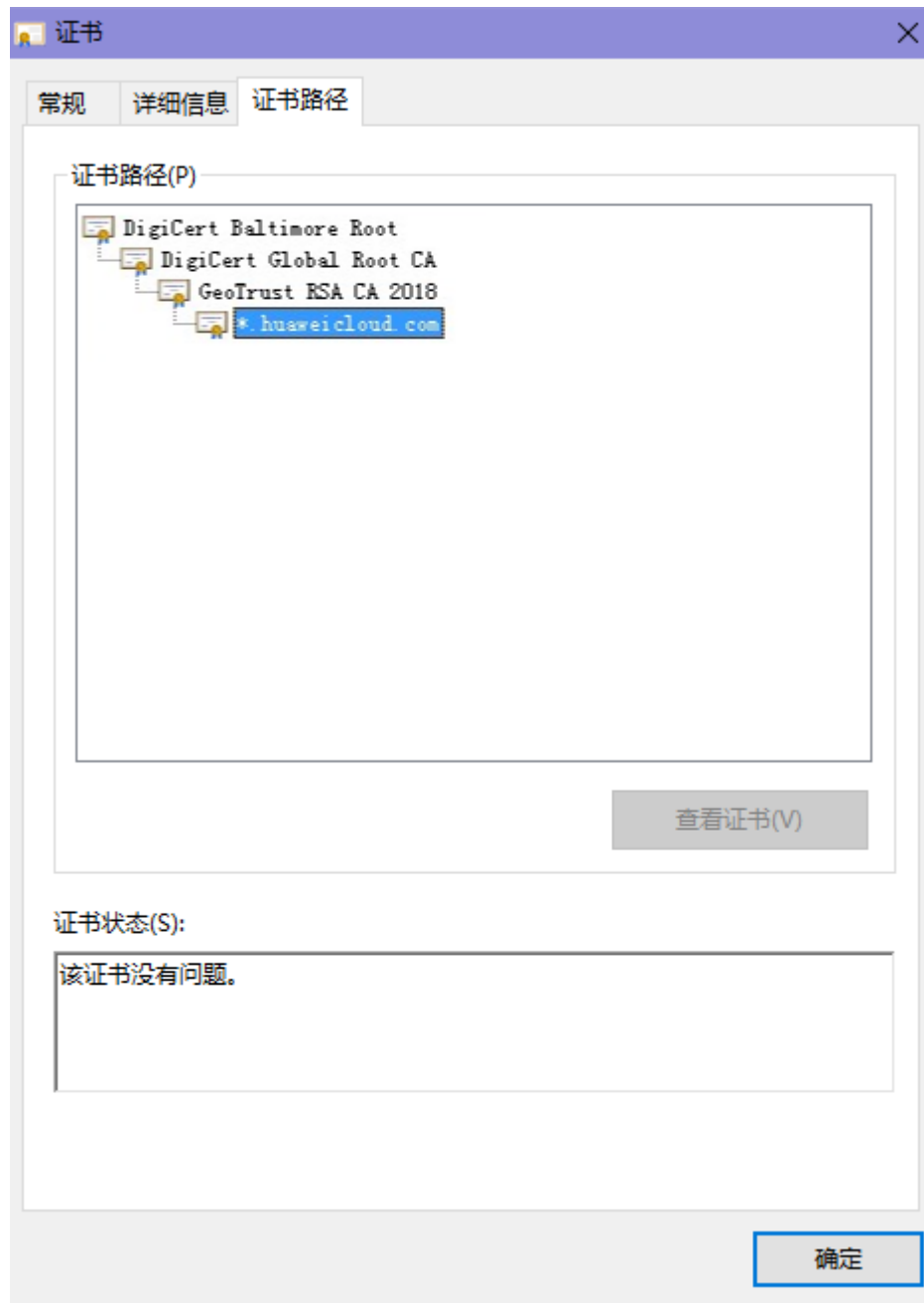
步骤1 查看证书。单击浏览器前的锁，可查看证书状况。

图 6-22 查看证书



步骤2 查看证书链。单击“证书”，并选中“证书路径”页签，可单击证书名称查看证书状态，如图6-23所示。

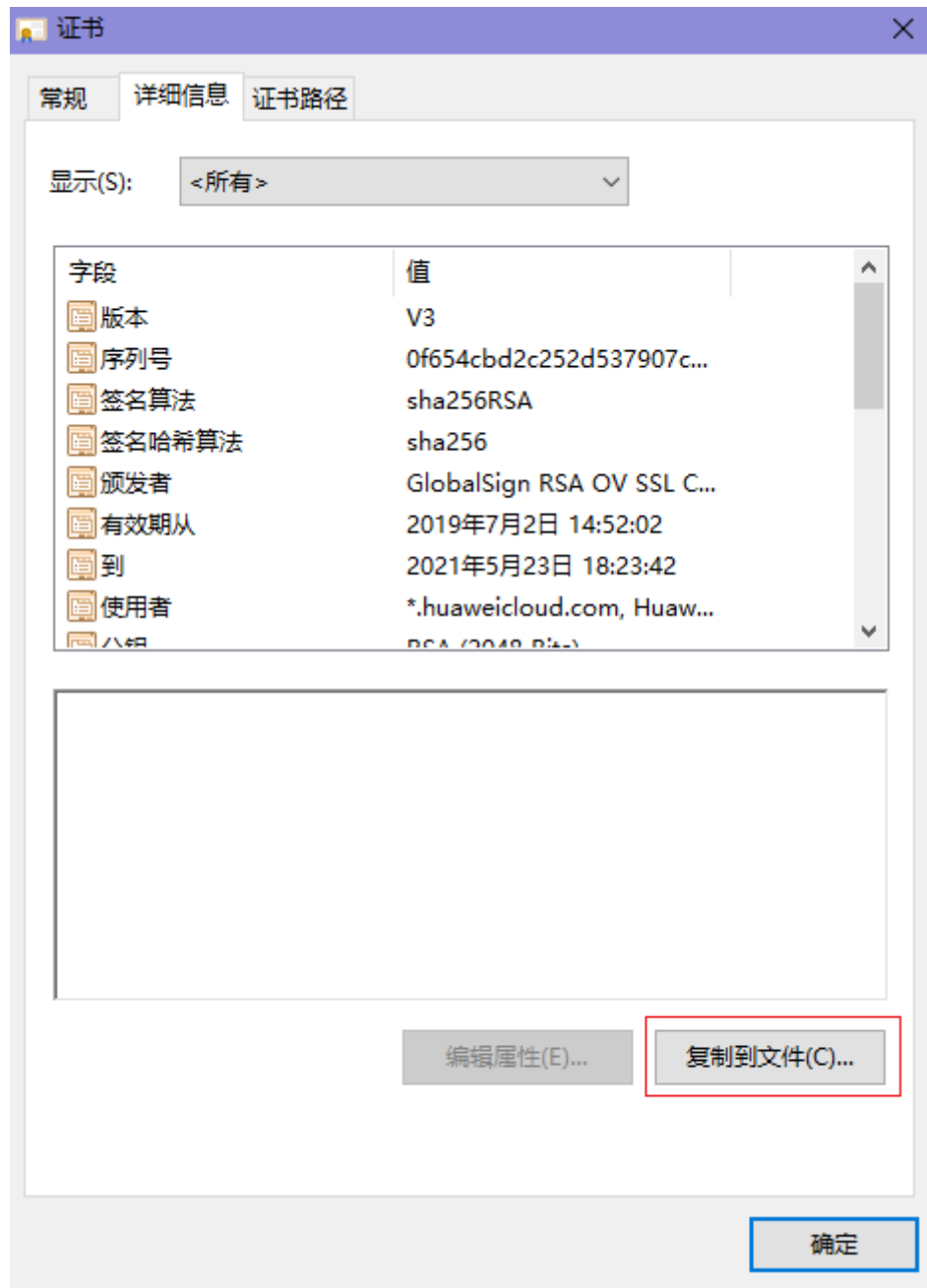
图 6-23 查看证书链



步骤3 逐一将证书另存到本地。

1. 选中证书名称，单击“详细信息”页签，如图6-24所示。

图 6-24 详细信息



2. 单击“复制到文件”，按照界面提示，单击“下一步”。
3. 选择“Base64编码”，单击“下一步”，如图6-25所示。

图 6-25 证书导出向导



步骤4 证书重构。证书全部导出到本地后，用记事本打开证书文件，按图6-26重组证书顺序，完成证书重构。

图 6-26 证书重构



步骤5 重新上传证书。

----结束

6.11 如何解决证书与密钥不匹配问题？

在DDoS高防控制台、WAF控制台上传HTTPS证书后，收到证书和密钥不匹配的提示。

解决方案

可能的原因	修复建议
您上传的证书与私钥内容不匹配	<ol style="list-style-type: none">1. 执行以下命令，分别查看证书和私钥文件的MD5值： <pre>openssl x509 -noout -modulus -in <证书文件> openssl md5 openssl rsa -noout -modulus -in <私钥文件> openssl md5</pre>2. 判断证书和私钥文件的MD5值是否一致，如果不一致，表示证书文件和私钥文件关联了不同的域名，证书和私钥内容不匹配。3. 如果确认证书和私钥文件内容不匹配，建议您重新上传正确的证书和私钥文件。
RSA私钥格式错误	<ol style="list-style-type: none">1. 执行以下命令，生成一个新的私钥： <pre>openssl rsa -in <私钥文件> -out <新私钥文件></pre>2. 重新上传私钥。

相关操作

- [如何解决证书链不完整？](#)
- [如何解决HTTPS请求在部分手机访问异常？](#)

6.12 如何处理 418 错误码问题？

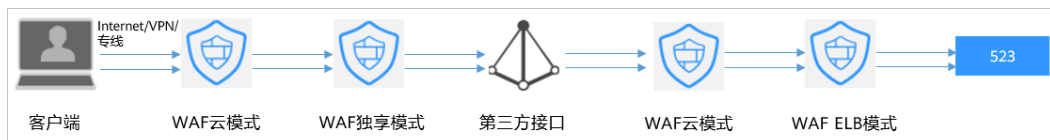
如果请求本身含有恶意负载被WAF拦截，此时访问WAF防护的域名时会出现418的错误。您可以通过查看WAF的防护日志，查看拦截原因。有关查看防护日志的详细操作，请参见[查看防护日志](#)。

- 如果您判断该请求为业务正常请求调用，可以通过误报处理操作对该路径的对应规则进行放行处理，避免同样问题再次发生。
有关处理误报事件的详细操作，请参见[处理误报事件](#)。
- 如果确认有问题，说明您的网站受到了攻击，并被WAF拦截。

6.13 如何处理 523 错误码问题？

523错误码是由于同一个访问请求四次经过了WAF引起，为了避免出现死循环现象，WAF会拦截该请求。如果您在访问网站时出现了523错误码问题，请先梳理流量图，查出流量串接多个华为云WAF的原因。

可能导致523错误码的示例流量图如下：



原因一：将同一个网站接入 WAF 4 次以上

通过WAF的各种模式（云模式-CNAME接入、云模式-ELB接入、独享模式），将同一个网站接入WAF 4次以上。

解决办法：

梳理流量图，将用户流量绕过多余WAF，具体操作如下：

步骤1 登录WAF管理控制台。

步骤2 在左侧导航树中，选择“网站设置”，进入网站设置列表。

步骤3 找到出现523问题的防护网站，保留一个配置，删除多余的防护网站，具体操作请参见[删除防护网站](#)。

防止删除网站后造成业务中断，在删除网站前，需要完成以下操作：

云模式：请您先到DNS服务商处将域名重新解析，指向源站服务器IP地址，否则该域名的流量将无法切回服务器，影响正常访问。

独享模式：修改ELB的后端服务器组，不再接入WAF实例节点，具体操作请参见[更换后端服务器组](#)。

----结束

原因二：调用了第三方接口且第三方接口也使用了华为云 WAF

将用户的请求在转发给第三方接口时仅修改了host，而header、cookie执行了原样转发，导致保留了WAF原有的计数器。

解决办法：

修改反向代理请求中的header字段，具体操作如下：

须知

用户的流量链路上，在WAF后如果有NGINX，才可用此方法。

步骤1 通过使用“proxy_set_header”来重定义发往代理服务器的请求头，执行以下命令打开nginx配置文件。

以Nginx安装在“/opt/nginx/”目录为例，具体情况需要依据实际目录调整。

vi /opt/nginx/conf/nginx.conf

步骤2 在nginx配置文件中加入proxy_set_header X-CloudWAF-Traffic-Tag 0;，示例如下：

```
location ^~/test/ {
    .....
    proxy_set_header Host    $proxy_host;
    proxy_set_header X-CloudWAF-Traffic-Tag 0;
    .....
}
```

```
proxy_pass http://x.x.x.x;  
}
```

----结束

原因三：源站 IP 误配置为 WAF 的回源 IP 或 WAF 前代理的 IP

如果“源站地址”误配置为WAF的回源IP或WAF前代理的IP，会造成访问死循环，报523错误。

解决办法：

检测源站服务器的配置，将“源站地址”修改为正确的源站IP，具体操作请参见[修改服务器配置信息](#)。

图 6-27 修改源站地址



6.14 如何处理域名接入 WAF 后，登录首页不停地刷新？

域名接入WAF后，所有网站访问请求将先流转到WAF进行监控，经WAF过滤后再返回到源站服务器。对于客户端的每一个请求，WAF会根据请求访问的IP地址和用户代理（User Agent）生成一个识别码，而WAF有多个回源IP（随机分配），当回源IP发生变化时请求的识别码也会不同，将导致会话被WAF直接删除，登录首页不停地刷新，为了避免出现该问题，建议您使用会话Cookie进行会话保持。

6.15 如何解决 HTTP 配置转发策略后程序访问页面卡顿？

如果HTTP配置转发策略后程序访问页面卡顿，请添加HTTP到HTTP和HTTPS到HTTPS这两条转发协议规则。

有关配置转发规则的详细操作，请参见[如何解决重定向次数过多？](#)。

6.16 使用 WAF 后如何处理网站的文件不能上传？

将网站接入WAF后，网站的文件上传请求限制为10G。

如果需要上传超过10G的文件，视频，建议不使用WAF防护的域名上传，可采用以下三种方式上传：

- 直接通过IP上传。
- 使用没有被WAF防护的域名上传。
- 采用ftp协议上传。

6.17 如何处理接入 WAF 后报错 414 Request-URI Too Large?

故障现象

防护网站接入WAF后，用户不能正常访问网站，提示“414 Request-URI Too Large”错误，如图6-28所示。

图 6-28 提示“414 Request-URI Too Large”错误

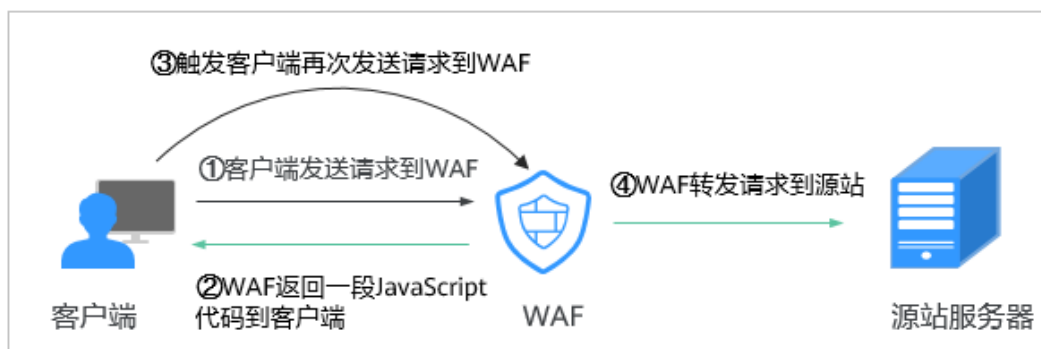


可能原因

防护网站开启了“JS脚本反爬虫”，由于用户的客户端浏览器没有JavaScript解析能力，客户端会缓存包含WAF返回JavaScript代码的页面，而用户每次访问防护网站时都会访问该缓存页面，WAF由此判定用户访问请求为非法的浏览器或爬虫工具，访问请求验证一直失败，造成无限循环，最终导致URI长度超出浏览器限制，访问网站失败。

开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成JS验证，并将该请求转发给源站，如图6-29所示。

图 6-29 JS 脚本反爬虫正常检测流程





- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。
- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

处理建议

当客户端的浏览器没有JavaScript解析能力时，请参照以下操作步骤关闭JS脚本反爬虫。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网站反爬虫”配置框，用户可根据自己的需要开启或关闭网站反爬虫策略。

- ：开启状态。
- ：关闭状态。


步骤7 选择“JS脚本反爬虫”页签，关闭JS脚本反爬虫，即JS脚本反爬虫的“状态”为 ，如图6-30所示。

图 6-30 关闭 JS 脚本反爬虫



----结束

6.18 如何处理“协议不受支持，客户端和服务端不支持一般SSL 协议版本或加密套件”？

现象

域名接入WAF后，不能正常访问网站，提示“协议不受支持，客户端和服务端不支持一般 SSL 协议版本或加密套件”。

解决办法

建议您在TLS配置里，将“加密套件”切换为“默认加密套件”，具体操作请参见[配置 PCI DSS/3DS合规与TLS](#)。

图 6-31 TLS 配置



6.19 访问独享引擎页面时提示“IAM 未授权”？

问题现象

当访问“系统管理”下的“独享引擎”页面时，提示“调用IAM失败，请检查当前用户是否具有IAM权限”时。

可能的原因

登录账号未授予“IAM ReadOnly”权限。

解决办法

为您的账号授予“IAM ReadOnly”权限，具体的操作方法请参见[给IAM用户授权](#)。

6.20 如何解决“网站被检测到：SSL/TLS 存在 Bar Mitzvah Attack 漏洞”？

SSL/TLS 存在Bar Mitzvah Attack漏洞是由RC4加密算法中一个问题所导致的。该问题能够在某些情况下泄露SSL/TLS加密流量中的密文，从而将账户用户密码、信用卡数据和其他敏感信息泄露给黑客。

解决办法

建议您在TLS配置里，将“最低TLS版本”配置为“TLS v1.2”，“加密套件”配置为“加密套件2”，具体操作如请参见[配置PCI DSS/3DS合规与TLS](#)。

6.21 如何解决“源站服务器 CPU 使用率高达 100%”问题？

问题现象

网站遭受攻击，网站已接入WAF，但防护没起作用，源站服务器CPU使用率高达100%，怎么办？

可能原因

网站可能遭受了CC攻击。

当发现网站处理速度下降，网络带宽占用过高时，很有可能已经遭受CC攻击，此时可查看Web服务器的访问日志或网络连接数量，如果访问日志或网络连接数量显著增加，则可确定遭受CC攻击。

解决办法

步骤1 确认WAF的防护策略的配置规则都开启了拦截模式。

步骤2 配置一条“路径”包含“/”的CC策略对网站的全路径进行防护，限速频率设置严格一些，观察请求流量，确认攻击是否缓减，并根据防护效果调整策略，配置如图6-32所示。

图 6-32 全路径防护

添加CC防护规则

* 限速模式 **源限速** 目的限速

对源端限速，如某IP（或用户）的访问频率超过限速频率，就会对该IP（或用户）的访问限速。

IP限速 用户限速 其他

* 域名聚合统计

当开启时，如配置的泛域名为“.a.com”，会将所有子域名（b.a.com, c.a.com）的请求一起聚合统计。

* 限速条件

字段	子字段	逻辑	内容
路径	--	包含	/

添加 您还可以添加29项条件。（多个条件同时成立才生效）

* 限速频率

- 10 + 次 - 60 + 秒 全局计数

确认 取消

步骤3 查看防护日志，对于攻击量大的IP，把IP加入黑名单，进行立即拦截。黑名单的配置请参见[配置IP黑白名单规则](#)。

----结束

6.22 域名接入 WAF 后，漏扫工具为什么扫不到用户真实的业务？

将域名以云模式-CNAME方式接入WAF后，使用漏洞扫描工具扫描网站域名时，扫描不到网站的真实业务，只能扫描到WAF的IP。

解决方案

方案一：在WAF控制台，将工作模式切换为Bypass，具体操作请参见[切换工作模式](#)。

须知

Bypass后，该域名的请求直接到达其后端服务器，不再经过WAF，此时需要先放通源站业务的安全策略端口，才能保证模式切换后，业务运行正常。

方案二：将网站IP添加到漏洞扫描工具进行扫描。以漏洞管理服务为例，将网站IP添加到漏洞管理服务进行扫描。

7 防护规则配置

7.1 Web 基础防护类


7.1.1 如何将 Web 基础防护的仅记录模式切换为拦截模式？

本节介绍如何将Web基础防护的仅记录模式切换为拦截模式。

执行以下操作完成Web基础防护的防护模式切换：

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“Web基础防护”配置框，“防护动作”选择“拦截”模式。

----结束

7.1.2 Web 基础防护支持设置哪几种防护等级？

Web基础防护设置了三种防护等级：“宽松”、“中等”、“严格”，默认为“中等”。防护等级相关说明如[表7-1](#)所示。

表 7-1 防护等级说明

防护等级	说明
宽松	防护粒度较粗，只拦截攻击特征比较明显的请求。 当误报情况较多的场景下，建议选择“宽松”模式。
中等	默认为“中等”防护模式，满足大多数场景下的Web防护需求。

防护等级	说明
严格	防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求，例如jolokia网络攻击、探测CGI漏洞、探测 Druid SQL注入攻击。 建议您等待业务运行一段时间后，根据防护效果配置全局白名单规则，再开启“严格”模式，使WAF能有效防护更多攻击。

有关配置Web基础防护规则的详细操作，请参见[配置Web基础防护规则](#)。

7.2 CC 攻击防护规则类

7.2.1 CC 攻击的防护峰值是多少？

各版本对应的CC攻击防护峰值如[表1 CC攻击的防护峰值](#)所示。

表 7-2 CC 攻击的防护峰值

服务版本	正常业务请求峰值	CC攻击防护峰值
入门版本	<ul style="list-style-type: none">100 QPS业务请求6,000 回源长连接（每域名）	-
标准版	<ul style="list-style-type: none">2,000 QPS6,000回源长连接（每域名）	100,000QPS
专业版	<ul style="list-style-type: none">5,000 QPS业务请求6,000 回源长连接（每域名）	300,000QPS
铂金版	<ul style="list-style-type: none">10,000 QPS业务请求6,000 回源长连接（每域名）	1,000,000QPS

服务版本	正常业务请求峰值	CC攻击防护峰值
独享版	<p>以下数据为单实例规格：</p> <ul style="list-style-type: none">WAF实例规格选择WI-500，参考性能：<ul style="list-style-type: none">HTTP业务：建议QPS 5,000；极限QPS 10,000HTTPS业务：建议QPS 4,000；极限QPS 8,000Websocket业务：支持最大并发连接5,000最大回源长连接：60,000WAF实例规格选择WI-100，参考性能：<ul style="list-style-type: none">HTTP业务：建议QPS 1,000；极限QPS 2,000HTTPS业务：建议QPS 800；极限QPS 1,600Websocket业务：支持最大并发连接1,000最大回源长连接：60,000 <p>须知 极限值为实验室测试值，高敏感业务请以实际业务测试数据为准。实际QPS与业务请求数据大小、自定义防护规则种类及数量相关</p>	<ul style="list-style-type: none">WAF实例规格选择WI-500，参考性能：防护峰值：20,000QPSWAF实例规格选择WI-100，参考性能：防护峰值：4,000QPS

7.2.2 如何配置 CC 防护规则？

当业务接口被HTTP Flood攻击时，可以通过Web应用防火墙Console界面设置CC防护规则，从而缓解业务压力。

用户可根据业务类型，配置CC防护规则，可配置以下内容：

- 每个Web访问者在规定时间内允许访问的次数。
- 根据IP、Cookie或者Referer字段区分Web访问者。
- 当访问超过限制时，对其访问进行阻断或者发送验证码验证。

具体的配置规则请参见[配置CC攻击防护规则](#)。

7.2.3 在什么情况下使用 Cookie 区分用户？

在配置CC防护规则时，当IP无法精确区分用户，例如多个用户共享一个出口IP时，用户可以使用Cookie区分用户。

用户使用Cookie区分用户时，如果Cookie中带有用户相关的“session”等“key”值，直接设置该“key”值作为区分用户的依据。

须知

如果CC防护策略中配置的URL请求是被其他服务调用的API接口，可能不支持Cookie方式。

7.2.4 CC 规则里“限速频率”和“放行频率”的区别？

“限速频率”是单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，WAF将根据配置的CC攻击防护规则“防护动作”来处理。例如，“限速频率”设置为“10次/60秒”，“防护动作”设置为“阻断”，则表示60秒只能有10次访问请求，一旦在60秒内访问请求超过10次，WAF就直接阻断该Web访问者访问目标URL。

配置CC防护规则时，如果选择了“高级”工作模式，且“防护动作”配置为“动态阻断”，则除了需要配置“限速频率”外，还需要配置“放行频率”。

如果在一个限速周期内，访问的请求频率超过“限速频率”触发了拦截，那么，在下一个限速周期内，拦截阈值将动态调整为“放行频率”。且“放行频率”为0时，表示上个周期发生拦截后，下一个周期所有满足规则条件的请求都会被拦截。

区别

- “放行频率”和“限速频率”的限速周期一致。
- “放行频率”小于等于“限速频率”，且“放行频率”可为0。

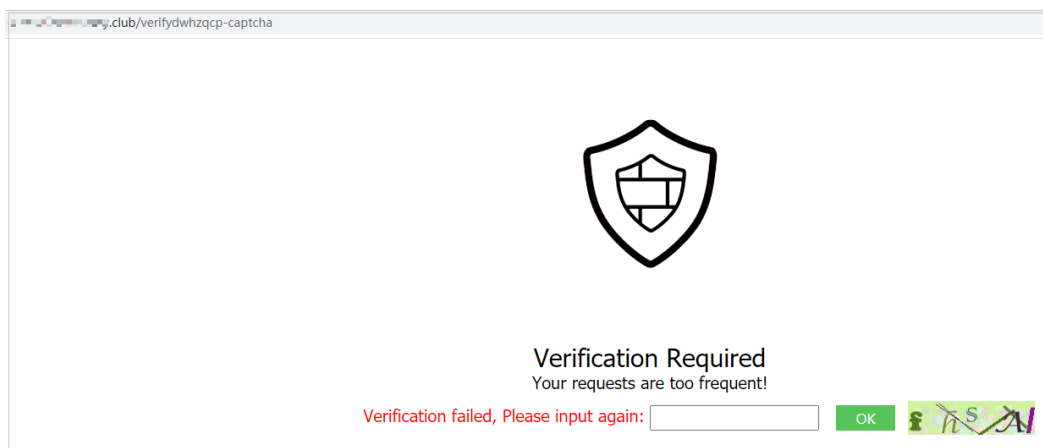
有关配置CC攻击防护规则的详细介绍，请参见[配置CC攻击防护规则](#)。

7.2.5 配置“人机验证”CC防护规则后，验证码不能刷新，验证一直不通过，如何处理？

故障现象

在WAF上开启“CC攻击防护”，添加“防护动作”为“人机验证”的规则后，访问网站，验证码不能刷新，验证一直不通过，如[图7-1](#)所示。

图 7-1 验证码一直验证不通过



配置“人机验证”后，在配置的指定时间内当用户访问网站超过配置的次数限制后，将弹出验证码进行人机验证，完成验证后，请求将不受访问限制。

有关配置CC攻击防护规则的详细操作，请参见[配置CC攻击防护规则](#)。

可能原因

域名同时接入WAF和CDN（Content Delivery Network，内容分发网络），CC攻击防护规则的“路径”中包含静态页面，静态页面被CDN缓存，导致验证码不能刷新，验证不能通过。


处理建议


在CDN上，将缓存的静态URL设置为放行，操作步骤如下。

须知

配置完成后，请等待3~5分钟，待配置的缓存策略生效后，再访问网站使用验证码功能。

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“CDN与智能边缘 > 内容分发网络 CDN”，进入CDN页面。

步骤4 在左侧导航树中，选择“域名管理”，进入“域名管理”页面。

步骤5 在“域名”列，单击目标域名的名称，进入域名配置页面。

步骤6 选择“缓存配置”页签，单击“编辑”，系统弹出“配置缓存策略”对话框。

步骤7 单击“添加”，添加两条缓存策略规则，如[图7-2](#)所示，相关参数说明如[表7-3](#)所示。

图 7-2 “配置缓存策略”对话框



类型	内容	优先级	缓存过期时间	URL参数	URL参数值	缓存排除网站	操作
文件名后缀	.php, .jsp, .asp, .aspx	2	0 秒	不忽略参数		<input type="checkbox"/>	删除
所有文件		1	30 天	不忽略参数		<input type="checkbox"/>	删除
全路径	/verifydwhzqcp-cap	1-100整数	0 天	不忽略参数		<input type="checkbox"/>	删除
全路径	/getdwhzqcp-captct	1-100整数	0 天	不忽略参数		<input type="checkbox"/>	删除

表 7-3 配置静态 URL 缓存策略参数说明

参数	配置说明
类型	选择“全路径”。
内容	依次添加的两条规则的内容为： <ul style="list-style-type: none">“/verifydwhzqcp-captcha”“/getdwhzqcp-captcha.jpg”
优先级	将两条规则设置为最高的优先级。
缓存过期时间	设置为“0”，不缓存静态URL。

步骤8 单击“确定”，完成缓存规则配置，如图7-3所示。

图 7-3 完成缓存规则配置

类型	内容	优先级	缓存间隔时间
所有文件		1	3分
文件名后缀	.php;.jsp;.asp;.aspx;.html	2	0秒
全路径	/verifydwhzqcp-captcha	3	0秒
全路径	/getdwhzqcp-captcha.jpg	4	0秒

配置完成后，请等待3~5分钟，待配置的缓存策略生效后，再访问网站使用验证码功能。

---结束

7.3 精准访问规则类

7.3.1 精准访问防护规则可以设置在指定的时间段生效吗？

WAF支持精准防护访问规则在指定的时间段生效。

您可以通过设置精准访问防护规则，对常见的HTTP字段（如IP、路径、Referer、User Agent、Params等）进行条件组合，筛选访问请求，并对命中条件的请求设置放行或阻断操作。

有关配置精准访问防护规则的详细操作，请参见[配置精准访问防护规则](#)。

7.3.2 精准访问防护规则添加的路径中带有#能匹配吗？

在精准访问防护规则中添加路径的内容不能包含特殊字符（' "<>*&#%\'?）。

#号是客户端参数，#号之后的参数就不会传入到服务端，用于网页位置定位；WAF和浏览器均不认为#后面的内容为url参数，因此获取不到。

添加精准访问防护规则

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容	添加引用表
路径	--	包含	<input type="text" value="/#userlogin "/>	

不能包含特殊字符 ("<-`?)"，且不能超过2,048 个字符长度。

7.3.3 如何不拦截带有.js 的文件？

您可以通过WAF的精准访问防护规则配置放行路径后缀为.js的条件，具体配置如下：

添加精准访问防护规则

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容	添加引用表
路径	--	后缀为	<input type="text" value=".js"/>	

添加 您还可以添加29项条件。（多个条件同时成立，才执行防护动作）

* 防护动作

7.4 IP 黑白名单类

7.4.1 Web 应用防火墙可以批量配置黑白名单吗？

WAF支持批量配置黑白名单。您可以通过添加地址组，批量设置IP/IP段黑白规则，阻断、仅记录或放行指定IP/IP段的访问请求。您也可以为每一个IP/IP段分别配置黑白名单规则。

有关配置黑白名单规则的详细操作，请参见[配置黑白名单规则](#)。

7.4.2 Web 应用防火墙可以导入/导出黑白名单吗？

WAF支持导入黑白名单，您可以在添加黑白名单规则时选择通过“地址组”方式导入黑白名单。WAF不支持导出黑白名单。


有关配置黑白名单的详细操作，请参见[配置黑白名单规则](#)。


7.4.3 如何对异常 IP 进行封堵？

对于异常的IP，您可以将该IP配置为黑名单。该IP配置为黑名单后，来自该IP的访问，WAF将直接拦截。

请参照以下操作步骤配置黑名单。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“黑白名单设置”配置框，用户可根据自己的需要开启或关闭黑白名单策略。

- ：开启状态。
- ：关闭状态。

步骤7 在“黑白名单设置”配置列表的左上方，单击“添加规则”。

步骤8 在弹出的对话框中，添加黑白名单规则，如**图7-4**所示。

说明

- 将IP配置为仅记录后，来自该IP的访问，WAF将根据防护规则进行检测并记录该IP的防护事件数据。
- 其他的IP将根据配置的WAF防护规则进行检测。

图 7-4 添加黑白名单规则



添加黑白名单设置规则

* 规则名称

* IP/IPv4或地址组 IP/IPv4 地址组

* IP/IPv4

* 防护动作

攻击惩罚 [添加攻击惩罚](#)

规则描述

* 生效时间 立即生效 自定义

步骤9 输入完成后，单击“确认”，添加的黑白名单展示在黑白名单规则列表中。

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的黑白名单规则时，可单击待修改的黑白名单IP规则所在行的“修改”，修改黑白名单规则。

- 若需要删除添加的黑白名单规则时，可单击待删除的黑白名单IP规则所在行的“删除”，删除黑白名单规则。

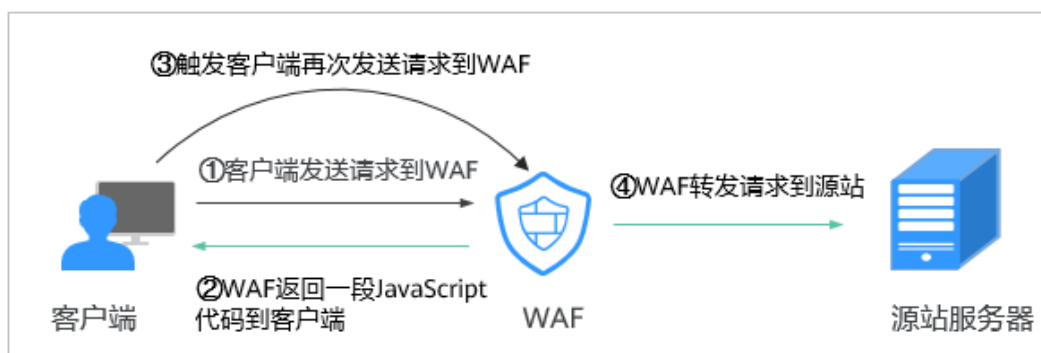
----结束

7.5 网站反爬虫类

7.5.1 开启 JS 脚本反爬虫后，为什么客户端请求获取页面失败？

开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成JS验证，并将该请求转发给源站，如图7-5所示。

图 7-5 JS 脚本反爬虫正常检测流程



- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。
- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

须知

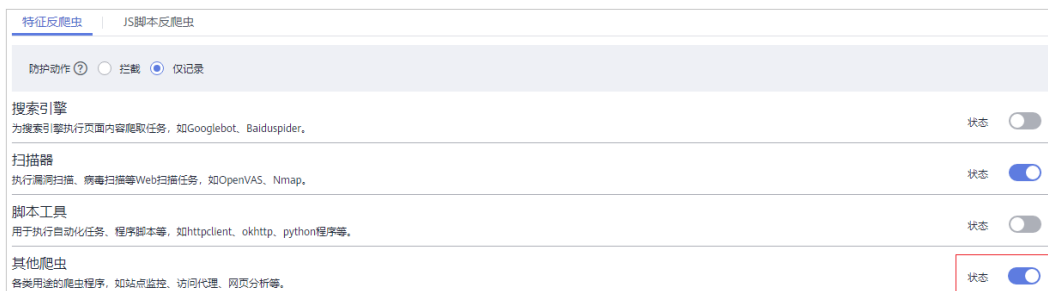
- 开启JS脚本反爬虫，要求客户端浏览器具有JavaScript的解析能力，并开启了Cookie。
- 如果客户端不满足以上要求，则只能完成①和②，此时客户端请求将不能成功获取到页面。

请您排查业务侧是否存在这种场景。如果您的网站有非浏览器访问的场景，建议您关闭JS脚本反爬虫功能。

7.5.2 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗？

在配置网站反爬虫的“特征反爬虫”时，如果开启了“其他爬虫”，WAF将对各类用途的爬虫程序（例如，站点监控、访问代理、网页分析）进行检测。开启该防护，不影响用户正常访问网页，也不影响用户访问网页的浏览速度。

图 7-6 开启“其他爬虫”

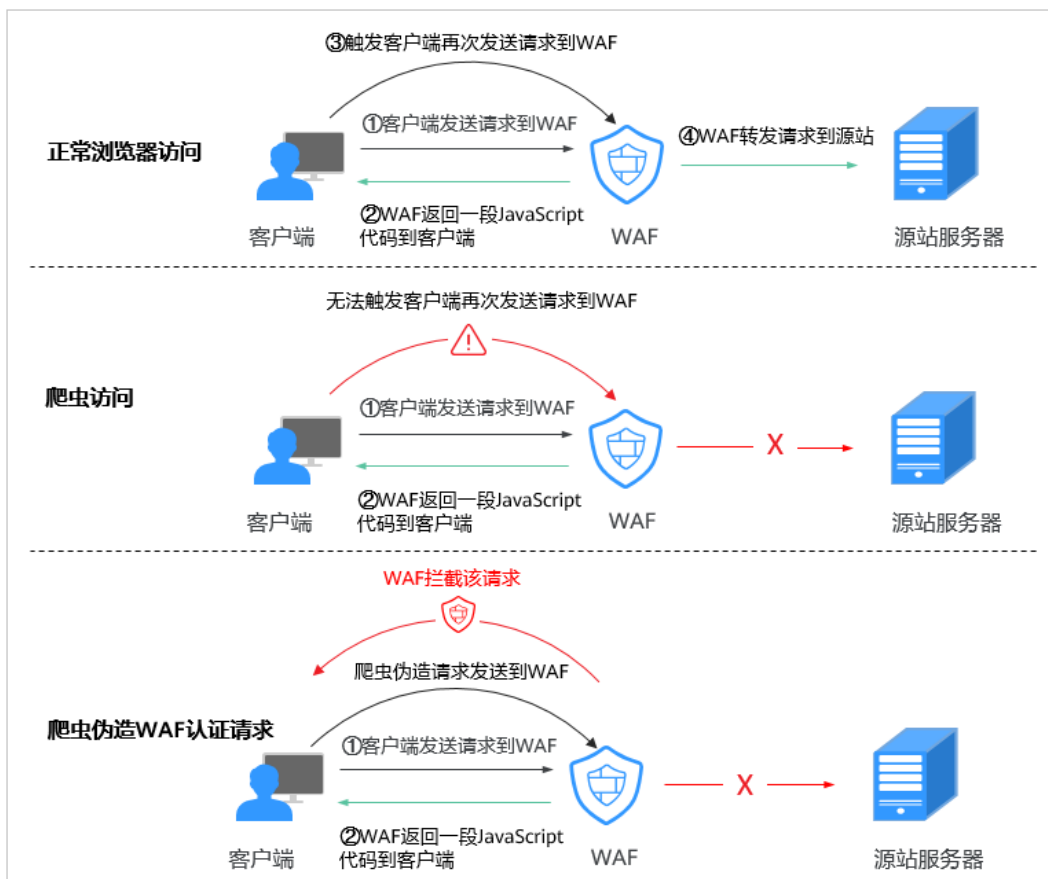


有关配置网站反爬虫的详细操作，请参见[配置网站反爬虫规则](#)。

7.5.3 JS 脚本反爬虫的检测机制是怎么样的？

JS脚本检测流程如图7-7所示，其中，①和②称为“js挑战”，③称为“js验证”。

图 7-7 JS 脚本检测流程说明



开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。

- 如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成js验证，并将该请求转发给源站。
- 如果客户端是爬虫访问，就无法触发这段JavaScript代码再发送一次请求到WAF，即WAF无法完成js验证。

- 如果客户端爬虫伪造了WAF的认证请求，发送到WAF时，WAF将拦截该请求，js验证失败。

通过统计“js挑战”和“js验证”，就可以汇总出JS脚本反爬虫防御的请求次数。例如，图7-8中JS脚本反爬虫共记录了18次事件，其中，“js挑战”（WAF返回JS代码）为16次，“js验证”（WAF完成JS验证）为2次，“其他”（即爬虫伪造WAF认证请求）为0次。

图 7-8 JS 脚本反爬虫防护数据



须知

网站反爬虫“js挑战”的防护动作为“仅记录”，“js验证”的防护动作为人机验证（即js验证失败后，弹出验证码提示，输入正确的验证码，请求将不受访问限制）。

7.6 其他类

7.6.1 哪些情况会造成 WAF 配置的防护规则不生效？

域名成功接入WAF后，正常情况下，域名的所有访问请求流量都会经过WAF检测并转发到服务器。但是，如果网站在WAF前使用了CDN，对于静态缓存资源的请求，由于CDN直接返回给客户端，请求没有到WAF，所以这些请求的安全策略不会生效。

7.6.2 如果只允许指定地区的 IP 可以访问，如何设置防护策略？

如果您只允许某一地区的IP访问防护域名，例如，只允许来源“上海”地区的IP可以访问防护域名，请参照以下步骤处理。

说明

由于地理位置访问控制的优先级高于内置规则的检测，配置了该地区IP放行后，WAF将不再检测其他的Web基础防护策略，直接放行。

步骤1 添加一条地理位置访问控制规则，添加“上海”地区的“放行”防护动作，如图7-9所示。

图 7-9 添加“放行”防护动作

添加地理位置访问控制规则

* 地理位置

中国境内 (1) 全选

<input type="checkbox"/> 北京	<input checked="" type="checkbox"/> 上海	<input type="checkbox"/> 天津	<input type="checkbox"/> 重庆
<input type="checkbox"/> 广东	<input type="checkbox"/> 浙江	<input type="checkbox"/> 江苏	<input type="checkbox"/> 安徽
<input type="checkbox"/> 福建	<input type="checkbox"/> 甘肃	<input type="checkbox"/> 广西	<input type="checkbox"/> 贵州
<input type="checkbox"/> 河南	<input type="checkbox"/> 湖北	<input type="checkbox"/> 河北	<input type="checkbox"/> 海南
<input type="checkbox"/> 香港	<input type="checkbox"/> 黑龙江	<input type="checkbox"/> 湖南	<input type="checkbox"/> 吉林
<input type="checkbox"/> 江西	<input type="checkbox"/> 辽宁	<input type="checkbox"/> 澳门	<input type="checkbox"/> 内蒙古
<input type="checkbox"/> 宁夏	<input type="checkbox"/> 青海	<input type="checkbox"/> 四川	<input type="checkbox"/> 山东
<input type="checkbox"/> 陕西	<input type="checkbox"/> 山西	<input type="checkbox"/> 台湾	<input type="checkbox"/> 新疆
<input type="checkbox"/> 西藏	<input type="checkbox"/> 云南		

中国境外 (0) 请选择地理区域

* 防护动作 放行

确认 取消

步骤2 配置一条精准访问防护规则，拦截所有的请求，如图7-10所示。

图 7-10 拦截所有访问请求

添加精准访问防护规则

不同模式使用限制和注意事项 ⓘ

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称 wafest

规则描述

字段	子字段	逻辑	内容
路径	-	包含	/

添加引用表

添加 您还可以添加29项条件。(多个条件同时成立，才执行防护动作)

* 防护动作 阻断

确定 取消

----结束

7.6.3 Web 应用防火墙支持哪些工作模式和防护模式？

域名接入WAF后，WAF作为一个反向代理部署在客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

WAF支持以下几种工作模式：

- 开启防护
- 暂停防护
- Bypass

须知

- 如果“部署模式”为“云模式”的网站在接入WAF前使用了代理，则不能切换为“Bypass”工作模式。
- “部署模式”为“独享模式”的网站不支持“Bypass”工作模式。

有关切换WAF工作模式的详细操作，请参见[切换工作模式](#)。

WAF防护规则支持的防护模式说明如[表7-4](#)所示。

表 7-4 支持的防护模式说明

防护规则	防护模式
Web基础防护规则	<ul style="list-style-type: none">• 拦截• 仅记录
CC攻击防护规则	<ul style="list-style-type: none">• 人机验证• 阻断• 动态阻断• 仅记录
精准访问防护规则	<ul style="list-style-type: none">• 阻断• 放行• 仅记录
黑白名单规则	<ul style="list-style-type: none">• 拦截• 放行• 仅记录
地理位置访问控制规则	<ul style="list-style-type: none">• 拦截• 放行• 仅记录 <p>须知 WAF专业版、铂金版、独享版和ELB模式支持配置该规则。</p>

防护规则	防护模式
网站反爬虫规则	特征反爬虫支持以下防护动作： <ul style="list-style-type: none">● 拦截● 仅记录 须知 WAF专业版、铂金版、独享版和ELB模式支持配置该规则。

说明

- 拦截：发现攻击行为后立即阻断并记录。
- 仅记录：发现攻击行为后只记录不阻断攻击。

7.6.4 Web 应用防火墙支持哪些防护规则？

Web应用防火墙支持的防护规则如[表7-5](#)所示。

表 7-5 可配置的防护规则

防护规则	说明
Web基础防护规则	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，对恶意扫描器、IP、网马等威胁进行检测和拦截。
CC攻击防护规则	可以自定义CC防护规则，限制单个IP/Cookie/Referer访问者对您的网站上特定路径（URL）的访问频率，WAF会根据您配置的规则，精准识别CC攻击以及有效缓解CC攻击。
精准访问防护规则	精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者客户端IP进行条件组合，定制化防护策略，为您的网站带来更精准的防护。
黑白名单规则	配置黑白名单规则，阻断、仅记录或放行指定IP的访问请求，即设置IP黑/白名单。
攻击惩罚规则	当恶意请求被拦截时，可设置自动封禁访问者一段时间，该功能和其他规则结合使用。
地理位置访问控制规则	针对指定国家、地区的来源IP自定义访问控制。
网页防篡改规则	当用户需要防护静态页面被篡改时，可配置网页防篡改规则。
网站反爬虫规则	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，精准识别爬虫行为。

防护规则	说明
防敏感信息泄露规则	该规则可添加两种类型的防敏感信息泄露规则： <ul style="list-style-type: none">敏感信息过滤。配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。响应码拦截。配置后可拦截指定的HTTP响应码页面。
全局白名单规则	针对特定请求忽略某些攻击检测规则，用于处理误报事件。
隐私屏蔽规则	隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。

7.6.5 Web 应用防火墙的哪些防护规则支持仅记录模式？

WAF的Web基础防护规则支持“仅记录”模式。


WAF的CC攻击防护规则、精准访问防护规则、黑白名单规则、地理位置访问控制规则和网站反爬虫支持“仅记录”防护动作。


7.6.6 拦截所有来源 IP 或仅允许指定 IP 访问防护网站，WAF 如何配置？

防护网站接入WAF后，您可以通过配置黑白名单规则或精准访问防护规则，使WAF仅允许指定IP访问防护网站，即WAF拦截除指定IP外的所有来源IP。

通过配置 IP 黑白名单规则拦截除指定 IP 外的所有来源 IP

步骤1 [登录管理控制台](#)。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 在“黑白名单设置”配置框中，开启防护规则。

图 7-11 黑白名单配置框



步骤7 单击“自定义黑白名单设置规则”，进入黑白名单设置规则页面，在黑白名单设置规则页面左上角，单击“添加规则”。

步骤8 在弹出的“添加黑白名单设置规则”对话框中，添加2条黑名单规则，拦截所有来源IP，如图7-12和图7-13所示。

图 7-12 拦截 1.0.0.0/1 IP 地址段



图 7-13 拦截 128.0.0.0/1 IP 地址段

The dialog box titled "添加黑白名单设置规则" (Add Black and White List Rule) contains the following fields and options:

- 规则名称 (Rule Name): all01
- IP/IP段或地址组 (IP/Segment or Address Group): IP/IP段, 地址组
- IP/IP段 (IP/Segment): 128.0.0.0/1
- 防护动作 (Protection Action): 拦截 (Intercept)
- 攻击惩罚 (Attack Penalty): 无攻击惩罚 (No Attack Penalty), with a "添加攻击惩罚" (Add Attack Penalty) button.
- 规则描述 (Rule Description): (Empty text box)

Buttons: 确认 (Confirm), 取消 (Cancel)

步骤9 单击“添加规则”，在弹出的“添加黑白名单设置规则”对话框中，分别添加放行指定IP或IP地址段的防护规则。

例如，如果您需要放行XXX.XXX.2.3，添加一条如图7-14所示防护规则。

图 7-14 放行指定 IP

The dialog box titled "添加黑白名单设置规则" (Add Black and White List Rule) contains the following fields and options:


- 规则名称 (Rule Name): all01
- IP/IP段或地址组 (IP/Segment or Address Group): IP/IP段, 地址组
- IP/IP段 (IP/Segment): .2.3
- 防护动作 (Protection Action): 放行 (Allow)
- 规则描述 (Rule Description): (Empty text box)


Buttons: 确认 (Confirm), 取消 (Cancel)

----结束

通过配置精准访问防护规则拦截除指定 IP 外的所有来源 IP

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 在“精准访问防护”配置框中，开启防护规则。

图 7-15 精准访问防护配置框



步骤7 单击“自定义精准访问防护规则”，进入精准访问防护规则配置页面，在精准访问防护规则页面左上角，单击“添加规则”。

步骤8 在弹出的“添加精准访问防护规则”对话框中，添加如图7-16所示防护规则，阻断所有请求。

注意

因为配置精准防护白名单放行的优先级要高于拦截的优先级且“优先级”值越小优先级越高，因此此处配置的“优先级”值应大于步骤9中“优先级”配置的值。

图 7-16 阻断所有的请求

添加精准访问防护规则

不同模式使用限制和注意事项 ?

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容
路径	--	包含	/

添加引用表

+ 添加 您还可以添加29项条件。（多个条件同时成立，才执行防护动作）

* 防护动作

步骤9 单击“添加规则”，在弹出的“添加精准访问防护规则”对话框中，分别添加放行指定IP的防护规则。

例如，如果您需要放行192.168.2.3，添加一条如图7-17所示防护规则。

注意

因为配置精准防护白名单放行的优先级要高于拦截的优先级且“优先级”值越小优先级越高，因此此处配置的“优先级”值应小于步骤8中“优先级”配置的值。

图 7-17 放行指定 IP

添加精准访问防护规则

不同模式使用限制和注意事项 ?

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容
IPv4	客户端IP	等于	192.168.2.3

添加引用表

+ 添加 您还可以添加29项条件。（多个条件同时成立，才执行防护动作）

* 防护动作

您也可以参照步骤9，在黑白名单中添加防护规则，放行指定IP或IP地址段。

----结束

7.6.7 系统自动生成策略包括哪些防护规则？

在添加防护网站进行“策略配置”时，您可以选择已创建的防护策略或默认的“系统自动生成策略”，系统自动生成的策略相关说明如表7-6所示。

须知

标准版只能选择“系统自动生成策略”。

您也可以在域名接入后根据防护需求配置防护规则。

表 7-6 系统自动生成策略说明

版本	防护策略	策略说明
标准版	Web基础防护（“仅记录”模式、常规检测）	仅记录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/代码注入等攻击行为。
专业版、铂金版/独享模式	Web基础防护（“仅记录”模式、常规检测）	仅记录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/代码注入等攻击行为。
	网站反爬虫（“仅记录”模式、扫描器）	仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。


说明


“仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。

7.6.8 开启网页防篡改后，为什么刷新页面失败？

WAF网页防篡改仅支持对网站的静态网页进行缓存。如果您配置网页防篡改规则后，刷新页面访问的还是未更新的页面，请参考以下步骤处理：

步骤1 [登录管理控制台](#)。




步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网页防篡改”配置框，检查是否已开启网页防篡改。。

- ：开启状态，表示已开启，请执行**步骤7**。
- ：关闭状态，表示已关闭，单击  开启网页防篡改，等待几分钟后，刷新页面后重新访问。。

步骤7 查看目标规则配置的域名和路径是否配置正确。

- 如果配置正确，请执行**步骤8**。
- 如果配置不正确，在目标网页防篡改规则所在行的“操作”列中，单击“删除”，删除该防护规则后，在列表上方单击“添加规则”，重新配置网页防篡改规则。有关配置网页防篡改规则的详细操作，请参见[配置网页防篡改规则](#)。规则添加成功，等待几分钟后，刷新页面后重新访问。

步骤8 在目标网页防篡改规则所在行的“操作”列中，单击“更新缓存”。

当防护页面内容进行了修改，请务必更新缓存，否则WAF将始终返回最近一次缓存的页面内容。

此时，刷新页面后重新访问，如果还是未更新的页面，请联系技术支持。

----结束

7.6.9 黑白名单规则和精准访问防护规则的拦截指定 IP 访问请求，有什么差异？

黑白名单规则和精准访问防护规则都可以拦截指定IP访问请求，两者的区别说明如表 7-7所示。

表 7-7 黑白名单规则和精准访问防护规则区别

防护规则	防护功能	WAF检测顺序
黑白名单规则	只能阻断、仅记录或放行指定IP地址/IP地址段的访问请求。	最高 WAF根据配置的防护规则，按照防护规则检测顺序，进行访问请求过滤检测。
精准访问防护规则	对常见的HTTP字段（如IP、路径、Referer、User Agent、Params等）进行条件组合，用来筛选访问请求，并对命中条件的请求设置放行或阻断操作。	低于黑白名单规则

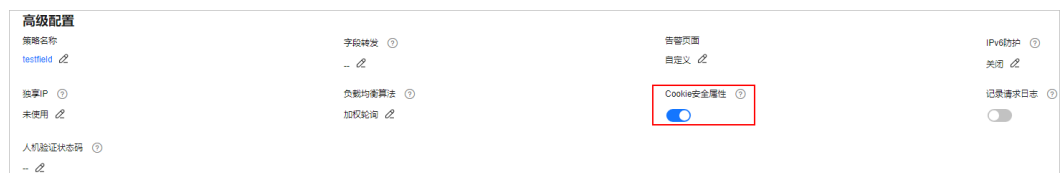
7.6.10 如何处理 Appscan 等扫描器检测结果为 Cookie 缺失 Secure/HttpOnly?

Cookie是后端Web Server插入的，可以通过框架配置或set-cookie实现，其中，Cookie中配置Secure，HttpOnly有助于防范XSS等攻击获取Cookie，对于Cookie劫持有一定的防御作用。

Appscan扫描器在扫描网站后发现客户站点没有向扫描请求Cookie中插入HttpOnly Secure等安全配置字段将记录为安全威胁。

当“对外协议”配置为HTTPS时，WAF支持在网站基本信息页面，开启“Cookie安全属性”，开启后会将Cookie的HttpOnly和Secure属性设置为true。

图 7-18 开启 Cookie 安全属性



8 防护日志

8.1 Web 应用防火墙支持记录防护日志吗？

在WAF管理控制台，您可以免费查看最近30天的防护日志、下载5天内的所有防护域名的防护日志数据。

如果您需要长期保存防护日志，您可以将WAF的防护日志记录到单独收费的云日志服务（Log Tank Service，简称LTS）上。LTS默认存储日志的时间为7天，存储时间可以在1~30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

- 有关查看防护日志的详细操作，请参见[查看防护日志](#)。
- 有关下载防护日志的详细操作，请参见[下载防护事件数据](#)。
- 有关WAF日志配置到LTS的详细操作，请参见[开启全量日志](#)。

8.2 Web 应用防火墙的日志是否可以通过 API 的方式获取？

您可以通过API的方式查看WAF的防护日志。

您也可以通过Web应用防火墙服务的控制台下载防护事件，具体您可参考[下载防护事件数据](#)章节。

8.3 如何获取拦截的数据？

通过Web应用防火墙服务可下载5天内的所有防护域名的仅记录和拦截的攻击事件数据，当天的防护事件数据，在次日凌晨生成防护事件数据的CSV文件。

可参照[下载防护事件数据](#)章节获取拦截数据。

8.4 防护事件列表中，防护动作为“不匹配”是什么意思呢？

配置网页防篡改、防敏感信息泄露、隐私屏蔽防护规则后，如果访问请求命中这些防护规则，则防护日志中记录的防护事件，“防护动作”显示为“不匹配”。

8.5 WAF 获取真实 IP 是从报文中哪个字段获取到的？

WAF引擎会根据防护规则确定是否代理转发请求去后端，如果WAF配置了基于IP的规则（比如黑白名单、地理位置、基于IP的精准访问防护规则），那么WAF引擎就会获取真实IP后才能放行或者拦截代理请求。获取真实IP的方法基于以下原则：

- 在WAF中开启了代理，即添加域名时，“是否已使用代理”选择了“四层代理”或“七层代理”，按以下顺序获取源IP：
 - a. 优先取“upstream”中配置的源IP头列表，即在域名的基本信息页面配置的“IP标记”，具体的操作请参见[配置攻击惩罚的流量标识](#)。如果未取到，执行**b**。

📖 说明

如果想以TCP连接IP作为客户端IP，“IP标记”应配置为“remote_addr”。

- b. 取config中配置的源IP头列表“cdn-src-ip”字段对应的值，未取到，执行**c**。
 - c. 取“x-real-ip”字段的值，未取到，执行**d**。
 - d. 取“x-forwarded-for”字段左边开始第一个公网IP，未取到，执行**e**。
 - e. 取WAF看到的TCP连接IP，“remote_addr”字段对应的值。
- 在WAF中未开启代理，即添加域名时，“是否已使用代理”选择了“无代理”，直接取“remote_ip”字段的值为真实IP。

8.6 Web 应用防火墙的日志可以转储到 OBS 吗？

您可以先将日志配置到LTS，然后在LTS上将WAF转储到OBS。

- 有关WAF日志配置到LTS的详细操作，请参见[防护日志记录到LTS](#)。
- 有关LTS日志转储至OBS的详细操作，请参见[LTS日志转储至OBS](#)。

8.7 Web 应用防火墙支持日志转发到 Syslog Server 吗？

WAF不支持日志转发到Syslog Server。

您可以下载WAF防护日志，详细操作请参见[下载防护事件数据](#)。

8.8 Web 应用防火墙的防护日志可以存储多久？

在WAF管理控制台，您可以免费查看最近30天的防护日志、下载5天内的所有防护域名的防护日志数据。

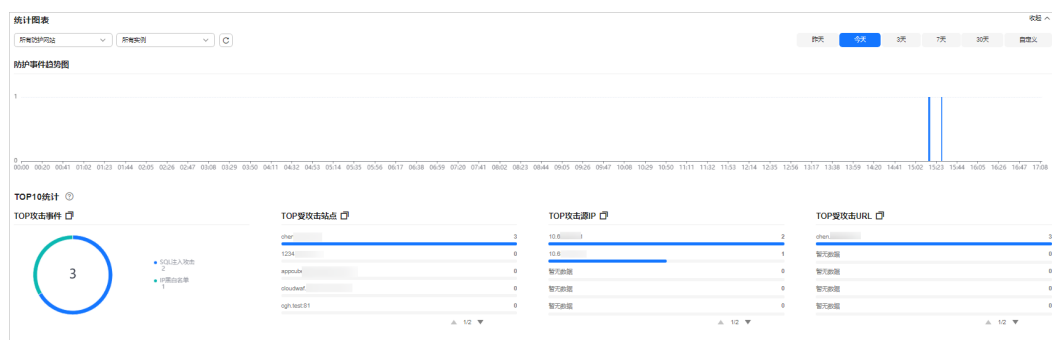
您可以将WAF的防护日志记录到单独收费的云日志服务（Log Tank Service，简称LTS），LTS默认存储日志的时间为7天，存储时间可以在1~30天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

- 有关WAF日志配置到LTS的详细操作，请参见[防护日志记录到LTS](#)。
- 有关LTS日志转储至OBS的详细操作，请参见[LTS日志转储至OBS](#)。

8.9 Web 应用防火墙可以同时查询多个指定 IP 的防护事件吗？

WAF不支持同时查询多个指定IP的防护事件。您可以在“防护事件”页面，通过“事件类型”、“防护动作”、“源IP”、“URL”、“事件ID”组合条件，查看防护域名相应的防护事件。

图 8-1 防护事件



有关查看防护事件的详细操作，请参见[查看防护日志](#)。

8.10 Web 应用防火墙会记录未拦截的事件吗？

WAF根据配置的防护规则拦截攻击事件，并将拦截或者仅记录攻击的事件记录在防护日志中，不会记录未拦截的事件。

有关查看防护日志的详细操作，请参见[查看防护日志](#)。

8.11 为什么 WAF 显示的流量大小与源站上显示的不一致？

WAF“安全总览”页面显示的流量大小与源站上显示的不同，主要原因说明如下：

- 网页压缩
WAF默认开启压缩，客户端（如浏览器）与WAF之间进行通信的网页可能被压缩（依赖浏览器压缩选项），而源站服务器可能不支持压缩。
- 连接复用
WAF与源站服务器之间会复用socket连接，这样会降低源站服务器与WAF之间的带宽消耗。
- 攻击请求
攻击请求被WAF拦截，而这种请求不会消耗源站服务器的带宽。
- 其他异常请求
如果源站服务器存在超时，无法连接等情况，这种情况不会消耗源站服务器的带宽。
- TCP层的重传等

WAF统计的带宽是7层的数据，而源站服务器网卡统计的是4层的数据。当网络通信质量差时，会出现TCP重传，网卡统计的带宽会重复计算，而7层传输的数据不会重复计算。在这种情况下，WAF上显示的带宽会低于源站上显示的带宽。

8.12 为什么“安全总览”和全量日志统计的日志个数不一致？

当攻击源、匹配规则、负载位置、URL等信息一致时，全量日志只记录一条日志。因此，全量日志显示的日志个数可能会低于“安全总览”显示的日志个数。

8.13 如何处理导出的防护事件数据乱码？

如果您需要将防护事件导出到本地，可在“防护事件”页面，单击“导出”。如果导出的防护事件数据，用Excel工具打开时，有乱码情况，可参照本章节处理。



原因

导出的防护事件数据为CSV格式，如果使用Excel工具打开该文件，可能会出现中文乱码的情况。这是因为通过WAF控制台导出的CSV文件使用了UTF-8编码格式，而Excel是以ANSI格式打开的，没有做编码识别。

图 8-2 导出防护事件数据



解决方案

方案一：

1. 打开csv文件时，对Excel进行如下设置：
 - a. 新建Excel。
 - b. 选择“数据 > 自文本”。
 - c. 选择导出的防护事件数据CSV文件，单击“导入”，进入“文本导入向导”页面。
 - d. 选择“分隔符号”，单击“下一步”。
 - e. 去勾选“Tab键”，勾选“逗号”，单击“下一步”。
 - f. 单击“完成”。
 - g. 在“导入数据”对话框里，单击“确定”。
2. 完成1后，使用记事本等文本编译器直接打开，或使用WPS打开。

方案二：

1. 使用记事本文本编译器打开导出的防护事件数据CSV文件。
2. 选择“文件 > 另存为”。
3. “编码”选择“ANSI”，修改文件名（后缀依然是.csv），避免覆盖原文件，单击“保存”。
使用Excel打开修改后CSV文件，一般中文就可以正常显示了。

9 WAF 与其他华为云服务同时部署

9.1 CDN+WAF 如何配置？

CDN+WAF配置后，流量被CDN加速后转发到WAF，WAF再将流量转到源站，在提升用户访问网站的响应速度与网站的可用性的同时，实现网站流量检测和攻击拦截。



有关同时部署CDN和WAF的详细介绍，请参见“[CDN+WAF](#)”[联动提升网站防护能力和访问速度](#)。

A 修订记录

发布日期	修改说明
2024-04-10	第一百四十八次正式发布。 修改： <ul style="list-style-type: none">• 连接超时时长是多少，是否可以手动设置该时长？• 如何处理Appscan等扫描器检测结果为Cookie缺失Secure/HttpOnly？
2024-01-31	第一百四十七次正式发布。 <ul style="list-style-type: none">• 新增：新手入门常见问题，同类问题进行了整合。• 修改：域名/IP接入状态显示“未接入”，如何处理？
2023-11-30	第一百四十六次正式发布。 修改： <ul style="list-style-type: none">• 如何将Web基础防护的仅记录模式切换为拦截模式？• 如何对异常IP进行封堵？• 拦截所有来源IP或仅允许指定IP访问防护网站，WAF如何配置？• 同时在WAF中添加单域名和泛域名，WAF会优先检测哪个域名？
2023-11-10	第一百四十五次正式发布。 <ul style="list-style-type: none">• 新增： 如何处理导出的防护事件数据乱码？• 修改：<ul style="list-style-type: none">- Web应用防火墙是否能防护IP？- 业务请求/规格
2023-09-18	第一百四十四次正式发布。 修改： 如何处理523错误码问题？

发布日期	修改说明
2023-09-05	<p>第一百四十三次正式发布。</p> <p>修改：</p> <ul style="list-style-type: none"> • Web应用防火墙支持漏洞检测吗？ • WAF是否支持防护CS架构的网站？
2023-09-01	<p>第一百四十二次正式发布。</p> <ul style="list-style-type: none"> • 修改如何排查404/502/504错误？。 • 增加WAF对SQL注入、XSS跨站脚本和PHP注入攻击的检测原理？。
2023-08-16	<p>第一百四十一次正式发布。</p> <p>增加如何解决“源站服务器CPU使用率高达100%”问题？。</p>
2023-08-08	<p>第一百四十次正式发布。</p> <p>增加：</p> <ul style="list-style-type: none"> • 云模式WAF提供的解析地址是固定IP吗？ • 源站IP更改后是否会改变CNAME值？ • 更换IP后，需要重新将域名添加到WAF吗？ • 如何不拦截带有.js的文件？
2023-07-20	<p>第一百三十九次正式发布。</p> <ul style="list-style-type: none"> • 增加： <ul style="list-style-type: none"> - WAF是否支持防护CS架构的网站？ - WAF云模式是否能防护其他账号下的域名？ - WAF需要绑定EIP吗？ • 修改： <ul style="list-style-type: none"> - 独享版WAF是否支持跨VPC防护？ - 如何购买域名扩展包/QPS扩展包/规则扩展包？ - Web应用防火墙支持哪些非标准端口？ - QPS超过当前WAF版本支持的峰值时有什么影响？
2023-06-30	<p>第一百三十八次正式发布。</p> <p>修改：</p> <ul style="list-style-type: none"> • WAF获取真实IP是从报文中哪个字段获取到的？ • 域名/IP接入状态显示“未接入”，如何处理？
2023-06-25	<p>第一百三十七次正式发布。</p> <p>修改未配置子域名和TXT记录的影响？</p>

发布日期	修改说明
2023-06-19	<p>第一百三十六次正式发布。</p> <ul style="list-style-type: none"> 增加： 精准访问防护规则添加的路径中带有#能匹配吗？ 修改： 添加域名时提示“非法的源站地址”，如何处理？
2023-06-14	<p>第一百三十五次正式发布。</p> <p>修改：</p> <ul style="list-style-type: none"> 如何将Web基础防护的仅记录模式切换为拦截模式？ CC攻击防护规则类 变更规格类
2023-06-01	<p>第一百三十四次正式发布。</p> <ul style="list-style-type: none"> 增加： <ul style="list-style-type: none"> 一个独享WAF实例可以接入多个ELB吗？ 添加防护域名时，提示“其他人已经添加了该域名，请确认该域名是否属于你”，如何处理？ WAF是否支持HTTP/3协议吗？ 删除防护域名后CNAME记录会保留多久？ 如何解决“网站被检测到：SSL/TLS 存在Bar Mitzvah Attack漏洞”？ 修改： <ul style="list-style-type: none"> 主账号与子账号的权限有哪些区别？
2023-04-30	<p>第一百三十二次正式发布。</p> <ul style="list-style-type: none"> 修改： <ul style="list-style-type: none"> 使用WAF后如何处理网站的文件不能上传？ Web应用防火墙支持哪些非标准端口？ 拦截所有来源IP或仅允许指定IP访问防护网站，WAF如何配置？ 增加： 访问独享引擎页面时提示“IAM未授权”？
2023-04-21	<p>第一百三十一次正式发布。</p> <p>修改WAF误拦截了“非法请求”访问请求，如何处理？</p>
2023-04-12	<p>第一百三十次正式发布。</p> <p>修改如何购买域名扩展包/QPS扩展包/规则扩展包？</p>
2023-03-28	<p>第一百二十九次正式发布。</p> <p>修改：</p> <ul style="list-style-type: none"> 添加域名时，防护网站端口需要和源站端口配置一样吗？ 连接超时时长是多少，是否可以手动设置该时长？

发布日期	修改说明
2023-03-03	第一百二十八次正式发布。 修改： <ul style="list-style-type: none"> ● 如何将Web基础防护的仅记录模式切换为拦截模式？ ● CC攻击防护规则类 ● 变更规格类
2023-02-22	第一百二十七次正式发布。 修改： 如何排查404/502/504错误？
2023-02-08	第一百二十六次正式发布。 修改： <ul style="list-style-type: none"> ● Web应用防火墙是否支持防护非华为云和云下服务器？ ● 网站接入配置
2023-01-31	第一百二十五次正式发布。 修改以下问题： <ul style="list-style-type: none"> ● Web应用防火墙是否支持健康检查？ ● 如何排查404/502/504错误？
2022-12-22	第一百二十四次正式发布。 修改 WAF获取真实IP是从报文中哪个字段获取到的？ 。
2022-11-18	第一百二十三次正式发布。 新增以下问题： <ul style="list-style-type: none"> ● 防护事件列表中，防护动作为“不匹配”是什么意思呢？ ● WAF获取真实IP是从报文中哪个字段获取到的？
2022-11-02	第一百二十二次正式发布。 新增以下问题： <ul style="list-style-type: none"> ● 独享版WAF是否支持跨VPC防护？ ● WAF中的防SQL注入攻击和DBSS中的SQL注入的区别？ ● 如何处理“协议不受支持，客户端和服务端不支持一般SSL协议版本或加密套件”？
2022-10-25	第一百二十一次正式发布。 修改以下问题： <ul style="list-style-type: none"> ● 业务使用了IPv6，WAF中的源站地址如何配置？ ● 如何放行云模式WAF的回源IP段？ ● 如何降低Web应用防火墙的版本和规格？ ● 哪些版本支持IPv6防护？

发布日期	修改说明
2022-09-13	第一百二十次正式发布。 修改 WAF对SQL注入、XSS跨站脚本和PHP注入攻击的检测原理? ：增加“WAF针对XSS攻击的检测原理”。
2022-09-07	第一百一十九次正式发布。 修改 Web应用防火墙支持哪些非标准端口?
2022-09-05	第一百一十八次正式发布。 修改以下常见问题： <ul style="list-style-type: none"> • 域名/IP接入状态显示“未接入”，如何处理? • 域名/IP如何接入Web应用防火墙? • 如何排查404/502/504错误?
2022-08-30	第一百一十七次正式发布。 <ul style="list-style-type: none"> • 修改：多个域名对应同一源站，Web应用防火墙可以防护这些域名吗? • 增加：添加域名时，为什么还有域名配额却提示域名配额不足呢?
2022-08-03	第一百一十六次正式发布。 修改常见问题 Web应用防火墙支持防护哪些区域? 。
2022-07-18	第一百一十五次正式发布。 <ul style="list-style-type: none"> • 增加如下常见问题： <ul style="list-style-type: none"> - 如何理解WAF日志里的bind_ip参数? - 通过IP接入WAF后，WAF可以防护映射到这个IP的所有域名吗? - 如果业务超时数据较多，如何处理?
2022-07-06	第一百一十四次正式发布。 修改 为什么误报处理不能使用了? ：增加了区域限制的描述。
2022-07-04	第一百一十三次正式发布。 修改如下章节： <ul style="list-style-type: none"> • Web基础防护支持设置哪几种防护等级? • Web应用防火墙最多可以添加多少条规则?
2022-06-28	第一百一十二次正式发布。 修改如下章节： Web应用防火墙是否支持防御XOR注入攻击?
2022-06-15	第一百一十一次正式发布。 修改如下章节： <ul style="list-style-type: none"> • Web应用防火墙支持防护哪些区域? • Web应用防火墙攻击防护类问题

发布日期	修改说明
2022-06-09	第一百一十次正式发布。 修改 Web应用防火墙支持哪些非标准端口? 章节: 增加了新的端口。
2022-05-30	第一百零九次正式发布。 修改 Web应用防火墙支持哪些非标准端口? 章节。
2022-05-26	第一百零八次正式发布。 增加如下问题: <ul style="list-style-type: none">● WAF对SQL注入、XSS跨站脚本和PHP注入攻击的检测原理?● WAF是否可以防护Apache Struts2远程代码执行漏洞 (CVE-2021-31805)?
2022-05-13	第一百零七次正式发布。 修改如下问题: <ul style="list-style-type: none">● Web应用防火墙最多可以添加多少条规则?● 如何解决证书与密钥不匹配问题?● HTTP 2.0业务接入WAF防护是否会对源站有影响?● WAF配置多个源站时如何负载?
2022-05-05	第一百零六次正式发布。 修改如下问题: <ul style="list-style-type: none">● Web应用防火墙有IPS入侵防御系统模块吗?● 连接超时时长是多少, 是否可以手动设置该时长?
2022-04-25	第一百零五次正式发布。 修改 WAF可以跨企业项目使用吗? , 优化了相关描述。
2022-04-21	第一百零四次正式发布。 增加如下常见问题: <ul style="list-style-type: none">● 源站IP地址服务器更换安全组后, 在WAF中需要做更改吗?● 如何查看Web应用防火墙的到期时间?
2022-04-19	第一百零三次正式发布。 修改如下问题: <ul style="list-style-type: none">● Web应用防火墙支持哪些Web服务框架/协议?● 连接超时时长是多少, 是否可以手动设置该时长?
2022-04-07	第一百零二次正式发布。 修改如下问题: <ul style="list-style-type: none">● 如何排查404/502/504错误?, 增加了504的排查方法。● 独享模式排查思路和处理建议, 增加该问题的排查思路和建议。

发布日期	修改说明
2022-03-17	第一百次正式发布。 修改如下问题： <ul style="list-style-type: none"> • WAF可以跨企业项目使用吗？ • 购买或升级WAF时选择了企业项目，其他企业项目可以使用该企业项目的WAF吗？
2022-03-07	第九十九次正式发布。 支独享模式，修改了相关章节。
2022-02-25	第九十八次正式发布。 增加CC攻击的防护峰值是多少？
2022-01-06	第九十七次正式发布。 如何设置使流量不经过WAF，直接访问源站？ ，优化内容描述。
2021-12-20	第九十六次正式发布。 新增 如何查看防护网站的入带宽和出带宽信息？
2021-11-17	第九十五次正式发布。 新增： <ul style="list-style-type: none"> • 源站开启gzip对WAF有影响吗？ • 新增黑白名单规则和精准访问防护规则的拦截指定IP访问请求，有什么差异？ • 新增为什么“安全总览”和全量日志统计的日志个数不一致？
2021-11-08	第九十四次正式发布。 新增 为什么WAF显示的流量大小与源站上显示的不一致？
2021-11-02	第九十三次正式发布。 <ul style="list-style-type: none"> • 选择业务QPS时是按照入流量计算还是出流量计算？，优化内容描述。 • 新增泛域名和单域名都接入WAF，WAF如何转发访问请求？
2021-10-21	第九十二次正式发布。 Web应用防火墙可以批量配置黑白名单吗？ ，优化内容描述。
2021-10-12	第九十一次正式发布。 新增 开启网页防篡改后，为什么刷新页面失败？
2021-09-27	第九十次正式发布。 WAF误拦截了正常访问请求，如何处理？ ，新增误报处理方式表格。

发布日期	修改说明
2021-09-15	第八十九次正式发布。 新增 多个端口的服务器，如果某个端口不需要WAF防护，如何处理？
2021-08-31	第八十八次正式发布。 新增 购买或升级WAF时选择了企业项目，其他企业项目可以使用该企业项目的WAF吗？
2021-08-12	第八十七次正式发布。 <ul style="list-style-type: none"> 新增同一防护域名/IP可以添加到不同的账号进行防护吗？ 新增网站部署了反向代理服务器，如何配置WAF？
2021-08-06	第八十六次正式发布。 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	第八十五次正式发布。 系统自动生成策略包括哪些防护规则？ ，优化内容描述。
2021-07-19	第八十四次正式发布。 更新管理控制台入口描述。
2021-07-14	第八十三次正式发布。 新增： <ul style="list-style-type: none"> WAF会缓存网站数据吗？ 仅放行通过WAF的访问请求，如何配置？
2021-06-30	第八十二次正式发布。 如何排查404/502/504错误？ ，优化内容描述。
2021-06-23	第八十一次正式发布。 新增 为什么非default企业项目不能使用华为云SCM推送的SSL证书？
2021-06-02	第八十次正式发布。 新增： <ul style="list-style-type: none"> WAF转发和Nginx转发有什么区别？ 接入WAF对现有业务和服务器运行有影响吗？
2021-05-27	第七十九次正式发布。 新增 WAF误拦截了“非法请求”访问请求，如何处理？
2021-05-24	第七十八次正式发布。 <ul style="list-style-type: none"> 新增系统自动生成策略包括哪些防护规则？ 域名/IP接入状态显示“未接入”，如何处理？，优化内容描述。

发布日期	修改说明
2021-05-18	第七十七次正式发布。 新增 WAF和HSS的网页防篡改有什么区别?
2021-05-14	第七十六次正式发布。 新增 WAF可以防护使用HSTS策略/NTLM代理认证访问的网站吗?
2021-04-15	第七十四次正式发布。 Web应用防火墙可以拦截Web页面调用其他接口的请求数据吗?，优化内容描述。
2021-04-07	第七十三次正式发布。 <ul style="list-style-type: none"> 新增接入WAF后为什么漏洞扫描工具扫描出未开通的非标准端口? 如何排查404/502/504错误?，优化内容描述。
2021-03-03	第七十二次正式发布。 JS脚本反爬虫的检测机制是怎么样的? ，更新界面截图。
2021-02-25	第七十一次正式发布。 Web应用防火墙支持防护哪些区域? ，优化内容描述。
2021-02-19	第七十次正式发布。 新增 拦截所有来源IP或仅允许指定IP访问防护网站，WAF如何配置?
2021-02-05	第六十九次正式发布。 新增“Web应用防火墙包年/包月和按需计费模式是否支持互相切换?”
2021-01-25	第六十八次正式发布。 Web应用防火墙的防护日志可以存储多久? ，优化内容描述。
2020-12-31	第六十七次正式发布。 <ul style="list-style-type: none"> 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗?，更新界面截图。
2020-12-25	第六十六次正式发布。 调整文档框架。
2020-12-11	第六十五次正式发布。 删除云模式按需计费模式相关内容描述。
2020-11-18	第六十四次正式发布。 新增： <ul style="list-style-type: none"> Web应用防火墙可以防止垃圾注册和恶意注册吗? 添加域名时，防护网站端口需要和源站端口配置一样吗?

发布日期	修改说明
2020-11-09	第六十三次正式发布。 新增 域名/IP接入状态显示“未接入”，如何处理？
2020-10-22	第六十二次正式发布。 Web应用防火墙支持哪些Web服务框架/协议？ ，优化内容描述。
2020-09-23	第六十一次正式发布。 如何排查404/502/504错误？ ，更新界面截图。
2020-09-11	第六十次正式发布。 修改以下常见问题。 <ul style="list-style-type: none">• Web应用防火墙如何收费？• 如何退订Web应用防火墙？• 退订后重购WAF，原配置数据可以保存吗？
2020-08-12	第五十九次正式发布。 修改以下常见问题。 为什么华为云SCM上的SSL证书在WAF上不能查看？
2020-07-20	第五十八次正式发布。 新增 配置“人机验证”CC防护规则后，验证码不能刷新，验证一直不通过，如何处理？
2020-07-16	第五十七次正式发布。 新增：Web应用防火墙可以拦截multipart/form-data格式的数据包吗？
2020-07-08	第五十六次正式发布。 <ul style="list-style-type: none">• 新增开启JS脚本反爬虫后，为什么客户端请求获取页面失败？• Web应用防火墙是否支持防护非华为云和云下服务器？，优化内容描述。• Web应用防火墙是否能防护IP？，优化内容描述。• Web应用防火墙支持对哪些对象进行防护？，优化内容描述。• Web应用防火墙是否支持健康检查？，优化内容描述。
2020-06-24	第五十五次正式发布。 新增 添加域名时提示“非法的源站地址”，如何处理？
2020-06-16	第五十四次正式发布。 如何配置对外协议与源站协议？ ，调整章节架构。

发布日期	修改说明
2020-06-08	<p>第五十三次正式发布。</p> <p>新增以下常见问题。</p> <ul style="list-style-type: none"> • Web应用防火墙切换为Bypass模式后会放行流量吗？ • Web应用防火墙支持哪些工作模式和防护模式？
2020-06-02	<p>第五十二次正式发布。</p> <p>新增以下常见问题。</p> <ul style="list-style-type: none"> • Web应用防火墙可以导入/导出黑白名单吗？ • Web应用防火墙支持配置泛域名吗？ • Web应用防火墙可以配置会话Cookie吗？ • Web应用防火墙可以同时查询多个指定IP的防护事件吗？ • 如何在华为云的云解析服务上配置TXT记录的值？ • Web基础防护支持设置哪几种防护等级？ • Web应用防火墙的日志可以转储到OBS吗？
2020-05-26	<p>第五十一次正式发布。</p> <p>新增以下常见问题。</p> <ul style="list-style-type: none"> • QPS超过当前WAF版本支持的峰值时有什么影响？ • 本地文件包含和远程文件包含是指什么？ • Web应用防火墙可以批量配置黑白名单吗？ • 使用Web应用防火墙对邮件收发和邮件端口有影响吗？
2020-03-31	<p>第五十次正式发布。</p> <p>更新界面截图。</p>
2020-03-19	<p>第四十九次正式发布。</p> <ul style="list-style-type: none"> • Web应用防火墙支持哪些非标准端口？，修改非标准端口。 • 什么是区域和可用区？，优化内容描述。
2020-03-06	<p>第四十八次正式发布。</p> <p>新增以下常见问题。</p> <ul style="list-style-type: none"> • 购买WAF时如何选择业务QPS？ • 若流量超过Web应用防火墙的业务请求限制，该如何处理？ • 域名/IP如何接入Web应用防火墙？ • CDN+WAF如何配置？
2020-03-03	<p>第四十七次正式发布。</p> <ul style="list-style-type: none"> • 调整文档架构。 • 修改未配置子域名和TXT记录的影响？，更新界面截图并优化内容描述。

发布日期	修改说明
2020-01-10	第四十六次正式发布。 <ul style="list-style-type: none"> 新增Web应用防火墙是否支持多个账号共享使用? 修改Web应用防火墙是否能防护IP?，优化内容描述。
2019-12-26	第四十五次正式发布。 修改 Web应用防火墙支持哪些非标准端口? ，优化内容描述。
2019-12-20	第四十四次正式发布。 修改 Web应用防火墙支持哪些非标准端口? ，优化内容描述。
2019-12-16	第四十三次正式发布。 操作入口连环图更新。
2019-12-09	第四十二次正式发布。 <ul style="list-style-type: none"> 新增连接超时时长是多少，是否可以手动设置该时长? 新增域名/IP接入WAF前需要准备哪些数据? 修改：Web应用防火墙是否支持防护非华为云和云下服务器? 修改Web应用防火墙是否能防护IP?，优化内容描述。
2019-11-14	第四十一次正式发布。 修改 Web应用防火墙支持哪些非标准端口? ，优化内容描述。
2019-11-07	第四十次正式发布。 新增 CC规则里“限速频率”和“放行频率”的区别?
2019-11-05	第三十九次正式发布。 修改 如何排查404/502/504错误? ，优化内容描述。
2019-11-04	第三十八次正式发布。 新增： <ul style="list-style-type: none"> Web应用防火墙有IPS入侵防御系统模块吗? Web应用防火墙是否支持防护非华为云和云下服务器? Web应用防火墙是否支持文件缓存? 防护规则的路径是否区分大小写?

发布日期	修改说明
2019-10-30	<p>第三十七次正式发布。</p> <ul style="list-style-type: none"> 新增域名接入WAF后，为什么无法开启防护模式？ 新增如何在华为云的云解析服务上进行DNS验证？ 新增Web应用防火墙支持对哪些对象进行防护？ 新增配置泛域名时，如何选择证书？ 新增Web应用防火墙最多可以添加多少条规则？ 新增：Web应用防火墙是否支持健康检查？ 新增Web应用防火墙的防护日志可以存储多久？ 新增如何获取拦截的数据？ 新增Web应用防火墙支持记录防护日志吗？ 新增Web应用防火墙的日志是否可以通过API的方式获取？
2019-10-21	<p>第三十六次正式发布。</p> <p>新增未配置子域名和TXT记录的影响？</p>
2019-10-17	<p>第三十五次正式发布。</p> <ul style="list-style-type: none"> 修改如何使网站流量切入云模式Web应用防火墙？，优化内容描述。 删除“如何处理DNS解析状态异常？”。
2019-10-14	<p>第三十四次正式发布。</p> <p>修改：</p> <ul style="list-style-type: none"> Web应用防火墙支持哪些非标准端口？，优化内容描述。 如何排查404/502/504错误？，优化内容描述。 Web应用防火墙支持哪些操作系统？，优化内容描述。 Web应用防火墙支持哪些Web服务框架/协议？，优化内容描述。
2019-09-12	<p>第三十三次正式发布。</p> <p>新增：</p> <ul style="list-style-type: none"> 如何处理Appscan等扫描器检测结果为Cookie缺失Secure/HttpOnly？ 选择业务QPS时是按照入流量计算还是出流量计算？ 主账号与子账号的权限有哪些区别？
2019-09-06	<p>第三十二次正式发布。</p> <p>新增：</p> <ul style="list-style-type: none"> 新旧CNAME的区别？ 云模式服务器的源站地址可以配置成CNAME吗？ 修改如何排查404/502/504错误？，优化内容描述。 修改如何修改已绑定域名的证书？，优化内容描述。

发布日期	修改说明
2019-08-28	第三十一次正式发布。 <ul style="list-style-type: none"> 修改如何排查404/502/504错误?，优化内容描述。 修改如何获取访问者真实IP?，增加最佳实践的链接。 修改如何配置CC防护规则?，增加关联章节的链接。 修改如何使网站流量切入云模式Web应用防火墙?，增加关联章节的链接。
2019-08-20	第三十次正式发布。 文档优化：使用连环图。
2019-08-15	第二十九次正式发布。 <ul style="list-style-type: none"> 新增如何解决重定向次数过多? 修改如何使网站流量切入云模式Web应用防火墙?，优化内容描述。
2019-07-15	第二十八次正式发布。 <ul style="list-style-type: none"> 新增“如何为Web应用防火墙续费？” 新增“如何退订Web应用防火墙？” 修改如何在添加域名中配置防护域名?，优化内容描述。
2019-07-11	第二十七次正式发布。 修改 如何在添加域名中配置防护域名? ，优化内容描述。
2019-07-02	第二十六次正式发布。 新增 如何在添加域名中配置防护域名?
2019-07-01	第二十五次正式发布。 <ul style="list-style-type: none"> 新增后端服务器配置多个源站地址时的注意事项? 修改如何排查404/502/504错误?，优化内容描述。
2019-06-18	第二十四次正式发布。 <ul style="list-style-type: none"> 新增多Project下使用Web应用防火墙的限制条件? 新增哪些情况会造成WAF配置的防护规则不生效?
2019-06-06	第二十三次正式发布。 <ul style="list-style-type: none"> 新增Web应用防火墙支持防护哪些区域? 新增使用WAF后如何处理网站的文件不能上传? 修改Web应用防火墙支持哪些非标准端口?，优化内容描述。
2019-05-30	第二十二次正式发布。 修改 如何使网站流量切入云模式Web应用防火墙? ，优化内容描述。

发布日期	修改说明
2019-05-16	第二十一正式发布。 修改 如何使网站流量切入云模式Web应用防火墙? ，优化内容描述。
2019-05-14	第二十正式发布。 修改 如何排查404/502/504错误? ，优化内容描述。
2019-05-05	第十九正式发布。 <ul style="list-style-type: none"> 新增如何放行云模式WAF的回源IP段? 新增如何解决HTTPS请求在部分手机访问异常? 修改如何排查404/502/504错误?，优化内容描述。 修改Web应用防火墙支持哪些非标准端口?，优化内容描述。 修改如何使网站流量切入云模式Web应用防火墙?，优化内容描述。
2019-02-20	第十八次发布。 <ul style="list-style-type: none"> 修改Web应用防火墙支持哪些非标准端口?，优化内容描述。 修改“Web应用防火墙如何收费?”，优化内容描述。
2019-01-03	第十七正式发布。 调整文档布局。
2018-11-08	第十六正式发布。 设置短描述和关键字。
2018-10-29	第十五正式发布。 修改 Web应用防火墙支持哪些非标准端口? ，优化内容描述。
2018-09-12	第十四正式发布。 新增 如何解决证书链不完整?
2018-07-19	第十三次发布。 <ul style="list-style-type: none"> 新增如何获取访问者真实IP? 修改如何修改已绑定域名的证书?，优化内容描述。 根据界面变化修改了截图。
2018-07-05	第十二次发布。 <ul style="list-style-type: none"> 修改如何使网站流量切入云模式Web应用防火墙?，优化内容描述。 修改如何在本地测试Web应用防火墙?，优化内容描述。
2018-06-14	第十一次发布。 根据界面变化修改了截图。

发布日期	修改说明
2018-06-07	第十次发布。 新增 如何修改已绑定域名的证书?
2018-05-31	第九次正式发布。 新增 如何排查404/502/504错误?
2018-05-17	第八次正式发布。 新增 如何配置对外协议与源站协议?
2018-04-12	第七次正式发布。 修改“Web应用防火墙支持哪些防护规则? ”，增加防敏感信息泄露相关内容描述。
2018-04-02	第六次正式发布。 <ul style="list-style-type: none"> 修改Web应用防火墙支持哪些非标准端口?，优化内容描述。 根据界面变化更新了界面描述和截图。
2018-03-31	第五次正式发布。 <ul style="list-style-type: none"> 新增如何将Web基础防护的仅记录模式切换为拦截模式? 根据界面变化更新了界面描述和截图。
2018-03-27	第四次正式发布。 <ul style="list-style-type: none"> 新增Web应用防火墙支持哪些非标准端口? 新增如何使网站流量切入云模式Web应用防火墙? 新增如何在本地测试Web应用防火墙? 新增删除防护域名时应该注意哪些事项? 删除“如何开启WAF防护?”。 根据界面变化更新了界面描述和截图。
2018-01-16	第三次正式发布。 新增 Web应用防火墙是否能防护IP?
2018-01-11	第二次正式发布。 新增：Web应用防火墙提供的是几层防护?
2017-10-30	第一次正式发布。