

Web 应用防火墙

用户指南

文档版本 01
发布日期 2024-04-13



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。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 产品介绍	1
1.1 什么是 Web 应用防火墙	1
1.2 产品规格	2
1.3 功能特性	4
1.4 产品优势	7
1.5 应用场景	7
1.6 个人数据保护机制	8
1.7 WAF 权限管理	9
2 WAF 使用概览	11
3 申请 WAF 独享引擎	15
4 接入 WAF	18
4.1 WAF 支持的端口	18
4.2 网站接入 WAF	19
4.2.1 网站接入流程（独享模式）	19
4.2.2 步骤一：添加防护网站	20
4.2.3 步骤二：配置负载均衡	25
4.2.4 步骤三：为弹性负载均衡绑定弹性公网 IP	26
4.2.5 步骤四：放行独享引擎回源 IP	27
5 管理防护域名	30
5.1 查看基本信息	30
5.2 切换工作模式	31
5.3 配置 TLS 最低版本和加密套件	32
5.4 配置网站连接超时时间	37
5.5 配置连接保护	38
5.6 更新证书	39
5.7 配置攻击惩罚的流量标识	40
5.8 修改服务器配置信息	42
5.9 修改拦截返回页面	43
5.10 删除防护域名	44
6 管理证书	45
6.1 上传证书	45

6.2 删除证书.....	47
6.3 查看证书信息.....	48
7 管理黑白名单 IP 地址组.....	50
7.1 添加黑白名单 IP 地址组.....	50
7.2 修改或删除黑白名单 IP 地址组.....	50
8 配置防护规则.....	52
8.1 配置引导.....	52
8.2 配置 Web 基础防护规则.....	56
8.3 配置 CC 攻击防护规则.....	59
8.4 配置精准访问防护规则.....	64
8.5 创建引用表.....	69
8.6 配置 IP 黑白名单规则.....	71
8.7 配置攻击惩罚标准.....	73
8.8 配置地理位置访问控制规则.....	75
8.9 配置网页防篡改规则.....	77
8.10 配置网站反爬虫防护规则.....	79
8.11 配置防敏感信息泄露规则.....	81
8.12 配置全局白名单（原误报屏蔽）规则.....	83
8.13 配置隐私屏蔽规则.....	86
9 安全总览.....	89
10 管理防护事件.....	92
10.1 查看防护日志.....	92
10.2 处理误报事件.....	94
10.3 下载防护事件数据.....	96
11 开启告警通知.....	99
12 策略管理.....	101
12.1 新增防护策略.....	101
12.2 批量添加防护规则.....	102
12.3 添加策略适用的防护域名.....	103
13 管理独享引擎.....	104
14 查看产品信息.....	106
15 权限管理.....	107
15.1 WAF 自定义策略.....	107
15.2 WAF 权限及授权项.....	108
16 常见问题.....	112
16.1 产品咨询.....	112
16.1.1 功能说明类.....	112
16.1.1.1 Web 应用防火墙是否能防护 IP?	112

16.1.1.2 Web 应用防火墙支持对哪些对象进行防护？	112
16.1.1.3 Web 应用防火墙支持哪些操作系统？	112
16.1.1.4 Web 应用防火墙提供的是几层防护？	112
16.1.1.5 Web 应用防火墙是否支持文件缓存？	112
16.1.1.6 Web 应用防火墙攻击防护类问题	113
16.1.1.7 Web 应用防火墙是否支持 SSL 双向认证？	113
16.1.1.8 Web 应用防火墙支持基于应用层协议和内容的访问控制吗？	113
16.1.1.9 Web 应用防火墙是否可以对用户添加的 Post 的 body 进行检查？	113
16.1.1.10 Web 应用防火墙可以限制域名访问速度吗？	114
16.1.1.11 Web 应用防火墙可以拦截 multipart/form-data 格式的数据包吗？	114
16.1.1.12 Web 应用防护墙可以部署在 VPC 内网吗？	114
16.1.1.13 Web 应用防火墙支持拦截包含特殊字符的 URL 请求吗？	114
16.1.1.14 Web 应用防火墙可以防止垃圾注册和恶意注册吗？	114
16.1.1.15 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？	114
16.1.1.16 Web 应用防火墙可以配置会话 Cookie 吗？	114
16.1.1.17 Web 应用防火墙支持自定义 POST 拦截吗？	115
16.1.1.18 Web 应用防火墙可以设置域名限制访问吗？	116
16.1.1.19 Web 应用防火墙有 IPS 入侵防御系统模块吗？	116
16.1.1.20 Web 应用防火墙支持哪些 Web 服务框架/协议？	117
16.1.1.21 WAF 可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗？	117
16.1.1.22 WAF 转发和 Nginx 转发有什么区别？	117
16.1.1.23 WAF 会缓存网站数据吗？	118
16.1.1.24 Web 应用防火墙是硬防火墙还是软防火墙？	118
16.1.1.25 HTTP 2.0 业务接入 WAF 防护是否会对源站有影响？	118
16.1.1.26 WAF 对 SQL 注入、XSS 跨站脚本攻击的检测原理？	118
16.1.1.27 WAF 是否可以防护 Apache Struts2 远程代码执行漏洞 (CVE-2021-31805) ？	119
16.1.1.28 独享版 WAF 是否支持跨 VPC 防护？	119
16.1.2 使用说明类	119
16.1.2.1 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？	119
16.1.2.2 使用 Web 应用防火墙对邮件收发和邮件端口有影响吗？	120
16.1.2.3 如何获取访问者真实 IP？	120
16.1.2.4 Web 应用防火墙如何拦截请求内容？	120
16.1.2.5 本地文件包含和远程文件包含是指什么？	120
16.1.2.6 QPS 和请求次数有什么区别？	121
16.1.2.7 什么是并发数？	121
16.1.2.8 如果证书挂载在 ELB 上，WAF 可以根据请求内容进行拦截吗？	121
16.1.2.9 接入 WAF 对现有业务和服务器运行有影响吗？	121
16.1.2.10 仅放行通过 WAF 的访问请求，如何配置？	121
16.1.2.11 为什么 Cookie 中有 HWWAFSESID 或 HWWAFSESTIME 字段？	121
16.1.2.12 网站部署了反向代理服务器，如何配置 WAF？	122
16.1.2.13 泛域名和单域名都接入 WAF，WAF 如何转发访问请求？	122
16.1.2.14 使用 WAF 是否影响内网向外发送数据？	122

16.1.2.15 源站 IP 地址服务器更换安全组后，在 WAF 中需要做更改吗？	122
16.2 网站接入配置	122
16.2.1 域名/端口类	122
16.2.1.1 域名/IP 如何接入 Web 应用防火墙？	122
16.2.1.2 Web 应用防火墙支持哪些非标准端口？	124
16.2.1.3 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？	125
16.2.1.4 如何在添加域名中配置防护域名？	126
16.2.1.5 添加域名时，防护网站端口需要和源站端口配置一样吗？	126
16.2.1.6 多个端口的服务器，如果某个端口不需要 WAF 防护，如何处理？	127
16.2.1.7 域名/IP 接入 WAF 前需要准备哪些数据？	127
16.2.1.8 删除防护域名时应该注意哪些事项？	127
16.2.1.9 域名添加到 WAF 后，域名是否可以修改？	127
16.2.1.10 后端服务器配置多个源站地址时的注意事项？	127
16.2.1.11 Web 应用防火墙支持配置泛域名吗？	127
16.2.1.12 一个独享 WAF 实例可以接入多个 ELB 吗？	128
16.2.1.13 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？	128
16.2.2 证书管理	128
16.2.2.1 配置泛域名时，如何选择证书？	128
16.2.2.2 ELB 已上传的证书，在 Web 应用防火墙上需要重新导入上传吗？	128
16.2.2.3 如何将非 PEM 格式的证书转换为 PEM 格式？	128
16.3 业务中断排查	129
16.3.1 如何排查 404/502/504 错误？	129
16.3.2 域名/IP 接入状态显示“未接入”，如何处理？	132
16.3.3 WAF 误拦截了正常访问请求，如何处理？	134
16.3.4 WAF 误拦截了“非法请求”访问请求，如何处理？	135
16.3.5 连接超时时长是多少，是否可以手动设置该时长？	135
16.3.6 如何解决重定向次数过多？	135
16.3.7 如何解决 HTTPS 请求在部分手机访问异常？	135
16.3.8 如何解决证书链不完整？	136
16.3.9 如何解决证书与密钥不匹配问题？	140
16.3.10 如何处理 418 错误码问题？	140
16.3.11 如何处理 523 错误码问题？	141
16.3.12 如何处理域名接入 WAF 后，登录首页不停地刷新？	141
16.3.13 如何解决 HTTP 配置转发策略后程序访问页面卡顿？	141
16.3.14 使用 WAF 后如何处理网站的文件不能上传？	141
16.3.15 如何解决“网站被检测到：SSL/TLS 存在 Bar Mitzvah Attack 漏洞”？	141
16.4 防护规则配置	142
16.4.1 Web 基础防护类	142
16.4.1.1 如何将 Web 基础防护的仅记录模式切换为拦截模式？	142
16.4.1.2 Web 基础防护支持设置哪几种防护等级？	142
16.4.2 CC 攻击防护规则类	143
16.4.2.1 如何配置 CC 防护规则？	143

16.4.2.2 在什么情况下使用 Cookie 区分用户?	143
16.4.2.3 CC 规则里“限速频率”和“放行频率”的区别?	143
16.4.3 精准访问规则类.....	144
16.4.3.1 精准访问防护规则可以设置在指定的时间段生效吗?	144
16.4.4 网站反爬虫类.....	144
16.4.4.1 开启网站反爬虫后, 为什么有些请求被 WAF 拦截但查不到拦截记录?	144
16.4.5 其他类.....	144
16.4.5.1 哪些情况会造成 WAF 配置的防护规则不生效?	144
16.4.5.2 防护规则的路径是否区分大小写?	145
16.4.5.3 Web 应用防火墙支持哪些防护规则?	145
16.4.5.4 Web 应用防火墙的哪些防护规则支持仅记录模式?	145
16.4.5.5 开启网页防篡改后, 为什么刷新页面失败?	145
16.4.5.6 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?	146
16.4.5.7 如何处理 Appscan 等扫描器检测结果为 Cookie 缺失 Secure/HttpOnly?	147
A 修订记录.....	148

1 产品介绍

1.1 什么是 Web 应用防火墙

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

开通Web应用防火墙后，在WAF管理控制台将网站添加并接入WAF，即可启用Web应用防火墙。启用之后，您网站所有的公网流量都会先经过Web应用防火墙，恶意攻击流量在Web应用防火墙上被检测过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。

防护原理

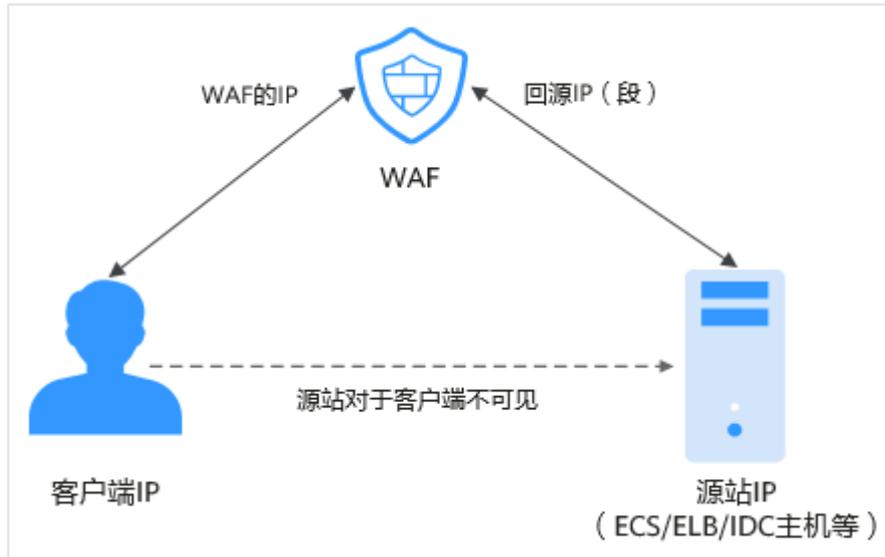
申请WAF后，在WAF管理控制台将网站添加并接入WAF。网站成功接入WAF后，网站所有访问请求将先流转至WAF，WAF检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

图 1-1 网站接入 WAF 防护原理



流量经WAF返回源站的过程称为回源。WAF通过回源IP代替客户端发送请求到源站服务器，接入WAF后，在客户端看来，所有的目标IP都是WAF的IP，从而隐藏源站IP。

图 1-2 回源 IP



防护对象

WAF支持的防护对象：域名或IP，云上或云下的Web业务。

1.2 产品规格

Web应用防火墙采用独享模式部署，有关独享模式和业务规格说明如下。

独享模式说明

独享模式相关说明如表1-1所示。

表 1-1 独享模式说明

项目	说明
部署方式	独享引擎
使用场景	业务服务器部署在云上。 大型企业网站，具备较大的业务规模且基于业务特性具有定制化的安全需求。
防护对象	域名或IP
优势	<ul style="list-style-type: none">● 部署灵活● 独享引擎实例资源由用户独享● 可以满足大规模流量攻击场景防护需求● 独享引擎实例部署在VPC内，网络链路时延低

业务规格

WAF支持的业务规格如表1-2所示。

表 1-2 适用的业务规格

业务指标	规格
正常业务请求峰值	<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 8,00；极限QPS 1,600 Websocket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>
业务带宽阈值	<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
域名个数	2,000个（支持2,000个一级域名）
支持的端口个数	<ul style="list-style-type: none"> 标准端口：不限制 非标准端口：不限制
CC攻击防护峰值	<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	100条
精准访问防护规则	100条
引用表规则	100条
IP黑白名单规则	1000条
地理位置封禁规则	100条

业务指标	规格
网页防篡改规则	100条
防敏感信息泄露	100条
误报屏蔽	1000条
隐私屏蔽规则	100条

须知

- 域名个数为一级域名（例如，example.com）、单域名/子域名（例如，www.example.com）和泛域名（例如，*.example.com）的总数。
- 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。

1.3 功能特性

通过Web应用防火墙，轻松应对各种Web安全风险，Web应用防火墙支持功能如下表。

功能类别	功能说明
业务配置	域名（泛域名、一级域名、二级域名等各级域名）/IP防护
	WAF支持的防护对象：域名或IP，云上或云下的Web业务。
	HTTP/HTTPS业务防护
	WAF可以防护HTTP/HTTPS业务，通过对HTTP/HTTPS请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。
	支持WebSocket/WebSockets协议
	WAF支持WebSocket/WebSockets协议，且默认为开启状态。
	非标端口防护
	Web应用防火墙除了可以防护标准的80，443端口外，还支持非标准端口的防护。

功能类别	功能说明	
Web应用安全防护	Web基础防护 说明 防护动作作为“拦截”时，可使用攻击惩罚标准功能，即当恶意请求被拦截时，可自动封禁访问者一段时间。	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。 <ul style="list-style-type: none"> ● 全面的攻击防护 支持SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、目录（路径）遍历、敏感文件访问、命令/代码注入、网页木马上传、后门隔离保护、非法HTTP协议请求、第三方漏洞攻击等威胁检测和拦截。 ● Webshell检测 防护通过上传接口植入网页木马。 ● 识别精准 <ul style="list-style-type: none"> - 内置语义分析+正则双引擎，黑白名单配置，误报率更低。 - 支持防逃逸，自动还原常见编码，识别变形攻击能力更强。 默认支持的编码还原类型： url_encode、Unicode、xml、OCT（八进制）、HEX（十六进制）、html转义、base64、大小写混淆、javascript/shell/php等拼接混淆。 ● 深度检测 深度反逃逸识别（支持同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等的防护）。 ● header全检测 支持对请求里header中所有字段进行攻击检测。
	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 说明 防护动作作为“阻断”时，可使用攻击惩罚标准功能，即当恶意请求被拦截时，可自动封禁访问者一段时间。	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。

功能类别		功能说明
	黑白名单规则 说明 防护动作作为“拦截”时，可使用攻击惩罚标准功能，即当恶意请求被拦截时，可自动封禁访问者一段时间。	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。
	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（原误报屏蔽）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。
连接保护		网站接入WAF防护之后，若您访问网站时出现大量的502 Bad Gateway, 504 Gateway Timeout错误或者等待处理的请求，为了保护源站的安全，可使用WAF的宕机保护和连接保护功能。当502/504请求数量或读等待URL请求数量以及占比阈值达到您设置的值时，将触发WAF熔断功能开关，实现宕机保护和读等待URL请求保护。
手动设置网站连接超时时间		<ul style="list-style-type: none"> 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60秒，该值可以在WAF界面手动设置。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。

功能类别	功能说明
防护事件管理	<ul style="list-style-type: none">当Web应用防火墙拦截或者仅记录的攻击事件为误报时，用户可通过Web应用防火墙处理误报事件、查看事件详情。用户可以通过Web应用防火墙服务下载5天内的全量防护事件数据。
安全可视化	提供简洁友好的控制界面，实时查看攻击信息和事件日志。 <ul style="list-style-type: none">策略事件集中配置 在Web应用防火墙服务的控制台集中配置适用于多个防护域名的策略，快速下发，快速生效。流量及事件统计信息 实时查看访问次数、安全事件的数量与类型、详细的日志信息。
灵活性、可靠性	多区域多集群部署，支持负载均衡，可在线平滑扩容，没有单点故障，最大限度保护业务运行稳定。

1.4 产品优势

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

精准高效的威胁检测

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

保护用户数据隐私

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

1.5 应用场景

常规防护

帮助用户防护常见的Web安全问题，比如命令注入、敏感文件访问等高危攻击。

电商抢购秒杀防护

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

0Day 漏洞爆发防范

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

防数据泄露

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

- 精准识别
采用语义分析+正则表达式双引擎，对流量进行多维度精确检测，精准识别攻击流量。
- 变形攻击检测
支持7种编码还原，可识别更多变形攻击，降低Web应用防火墙被绕过的风险。

防网页篡改

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

- 挂马检测
检测恶意攻击者在网站服务器注入的恶意代码，保护网站访问者安全。
- 页面不被篡改
保护页面内容安全，避免攻击者恶意篡改页面，修改页面信息或在网页上发布不良信息，影响网站品牌形象。

1.6 个人数据保护机制

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

收集范围

对于触发攻击告警的请求，WAF在事件日志中会记录相关请求记录，收集及产生的个人数据如表1-3所示。

表 1-3 个人数据范围列表

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

存储方式

对敏感字段提供了脱敏配置，其他字段在日志中明文保存。

访问权限控制

用户只能查看自己业务的相关日志。

1.7 WAF 权限管理

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

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

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

WAF 权限

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

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

根据授权精细程度分为角色和策略。

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

如表1-4所示，包括了WAF的所有系统角色。

表 1-4 WAF 系统角色

系统角色/策略名称	描述	类别	依赖关系
WAF Administrator	Web应用防火墙服务的管理员权限。	系统角色	依赖Tenant Guest和Server Administrator角色。 <ul style="list-style-type: none">● Tenant Guest：全局级角色，在全局项目中勾选。● Server Administrator：项目级角色，在同项目中勾选。
WAF FullAccess	Web应用防火墙服务的所有权限。	系统策略	无。
WAF ReadOnlyAccess	Web应用防火墙的只读访问权限。	系统策略	

2 WAF 使用概览

开通Web应用防火墙（WAF）服务后并将您的网站域名接入WAF，使网站的访问流量全部流转到WAF进行防护。

网站业务梳理

建议您对所需接入WAF进行防护的网站业务情况进行全面梳理，帮助您了解当前业务状况和具体数据，为后续配置WAF的防护策略提供依据。

表 2-1 网站业务梳理

梳理项	说明
网站和业务信息	
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	判断风险时间点，并且可作为WAF实例的业务带宽和业务QPS规格的选择依据。 说明 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，QPS将直接透传到源站，影响网站/应用业务的防护。
业务的主要用户群体（例如，访问用户的主要来源地区）	判断非法攻击来源，后续可使用地理位置访问控制功能屏蔽非法来源地区。
业务是否为C/S架构	如果是C/S架构，进一步明确是否有App客户端、Windows客户端、Linux客户端、代码回调或其他环境的客户端。
源站部署的具体位置	判断申请哪种实例region。
源站服务器的操作系统（Linux、Windows）和所使用的Web服务中间件（Apache、Nginx、IIS等）	判断源站是否存在访问控制策略，避免源站误拦截WAF回源IP转发的流量。

梳理项	说明
域名使用协议	<p>判断所使用的通信协议WAF是否支持。</p> <p>说明 网站的“对外协议”、“源站协议”必须要根据防护网站的实际情况配置正确，WAF才会正常防护您的网站。</p> <ul style="list-style-type: none"> 对外协议，即客户端（例如浏览器）请求访问网站的协议类型。可选择“HTTP”、“HTTPS”两种协议类型。 源站协议，即WAF转发客户端（例如浏览器）请求的协议类型。可选择“HTTP”、“HTTPS”两种协议类型。
业务端口	<p>判断需要防护的业务端口是否在WAF支持的端口范围内。</p> <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。
业务是否使用TLS 1.0或弱加密套件	判断业务使用的加密套件是否支持。
业务在接入WAF前，是否已接入DDoS高防、CDN等服务。	接入WAF时，判断如何选择“是否已使用代理”，以及正确进行域名解析。
（针对HTTPS业务）客户端是否支持SNI标准	对于支持HTTPS协议的域名，接入WAF后，客户端和服务端都需要支持SNI标准。
业务交互过程	了解业务交互过程、业务处理逻辑，便于后续配置针对性防护策略。
活跃用户数量	便于后续在处理紧急攻击事件时，判断事件严重程度，以采取风险较低的应急处理措施。
业务及攻击情况	
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻击防护过程中分析攻击特征。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
用户群体属性	例如，个人用户、网吧用户、或通过代理访问的用户。
业务是否遭受过大流量攻击、攻击类型和最大的攻击流量峰值	判断是否需要增加DDoS防护服务，并根据攻击流量峰值判断需要的DDoS防护规格。
业务是否遭受过CC攻击和最大的CC攻击峰值QPS	通过分析历史攻击特征，配置预防性策略。

梳理项	说明
业务是否已完成压力测试	评估源站服务器的请求处理性能，帮助后续判断是否因遭受攻击导致业务发生异常。

WAF 的使用概览

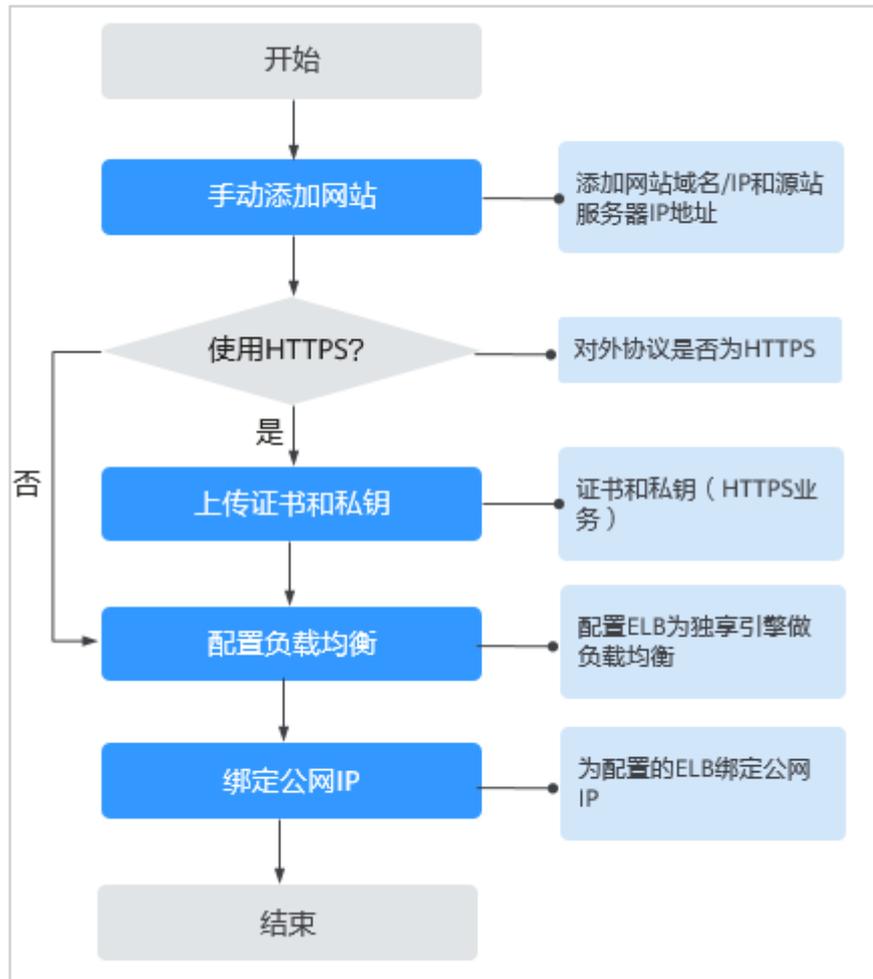
Web应用防火墙的使用概览如表2-2所示。

表 2-2 Web 应用防火墙的使用概览

子流程	说明
申请独享引擎	通过申请独享引擎开通WAF。 详细操作请参见 申请WAF独享引擎 。
添加防护网站	添加需要防护的网站。 详细操作请参见 步骤一：添加防护网站 。
开启WAF防护	添加防护域名后，可开启WAF防护，保护网站业务安全稳定。 说明 <ul style="list-style-type: none">WAF引擎不是运行在客户的Web服务器上的，所以对客户的Web服务器的资源性能没有影响。接入WAF之后，根据请求页面的大小和数量，会有几十毫秒的延迟。
配置自定义规则	WAF除了内置的防护规则外，还提供了丰富全面的自定义防护配置规则，全方位的防护您的网站。详细操作请参见 配置防护规则 。
处理误报事件	WAF拦截或者记录的攻击事件为误报时，可对误报进行屏蔽处理。 详细操作请参见 处理误报事件 。
安全总览	可查看到昨天、今天、3天、7天或者30天范围内的防护数据。详细操作请参见 安全总览 。

网站接入WAF的操作流程图如图2-1所示。

图 2-1 网站接入 WAF 的操作流程图



3 申请 WAF 独享引擎

如果您的业务服务器部署在云上，您可以通过申请WAF独享引擎实例对重要的域名或仅有IP的Web服务进行防护。

前提条件

- 已获取管理控制台的登录账号（配置WAF Administrator或WAF FullAccess权限策略）与密码。
- 已成功申请虚拟私有云VPC。
- 已创建了资源集。

操作须知

申请成功后，独享引擎实例规格不能修改。

须知

创建实例大约需要10分钟。当实例的运行状态为“运行中”时，说明实例已经创建成功。

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 > Web应用防火墙”。

步骤4 首次申请独享引擎时，在界面左侧，单击“立即申请独享模式”。

说明

重新申请独享引擎时，请在界面右上角，单击“创建WAF实例”。

步骤5 在“申请Web应用防火墙”界面，配置WAF实例参数，相关参数说明如[表3-1](#)所示。

表 3-1 WAF 独享引擎实例参数说明

参数名称	说明
计费模式	WAF独享引擎实例为按需计费，实例从创建成功开始计费到删除实例时结束计费，按实际使用时长（精确到秒）计费。
区域	原则上，在任何一个区域申请的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，建议您在申请WAF时，根据防护业务的所在区域就近选择申请的WAF区域。
可用区	选择区域中的可用区。
WAF实例名称前缀	设置WAF实例名称前缀，申请多个实例时，实例前缀名称相同。
WAF实例数量	设置申请的WAF实例个数。
WAF实例规格	选择实例的规格。WAF支持500Mbit/s和100Mbit/s两种规格。
WAF实例创建类别	普通租户类。 WAF实例将直接创建在租户ECS中，租户可以在ECS服务页面看到WAF实例所在的弹性云服务器
CPU架构	选择实例的CPU架构。
ECS规格	选择实例的ECS规格。
预计最终规格	吞吐量的性能参考值。
虚拟私有云	选择源站所在的VPC。 须知 如果您选择支持IPv6的VPC，勾选“开启ipv6”，独享引擎实例将支持IPv6防护。
子网	选择VPC中已配置的子网。
安全组	选择区域中已有的安全组，或者单击“管理安全组”，跳转到VPC管理控制台创建新的安全组。选择安全组后，该实例将受到该安全组访问规则的保护。 须知 <ul style="list-style-type: none">安全组建议配置以下访问规则：<ul style="list-style-type: none">入方向规则 根据业务需求添加指定端口入方向规则，放通指定端口入方向网络流量。例如，需要放通“80”端口时，您可以添加“策略”为“允许”的“TCP”、“80”协议端口规则。出方向规则 默认。放通全部出方向网络流量。如果WAF独享引擎实例与源站在不在同一个VPC中，需要在安全组中设置实例与源站的子网互通。

步骤6 确认参数配置无误后，在页面右下角单击“下一步”。

步骤7 确认订单详情无误，单击“立即申请”。

步骤8 单击“返回独享引擎列表”，在独享引擎实例列表界面，可以查看实例的创建情况。

创建实例大约需要10分钟。当实例的运行状态为“运行中”时，说明实例已经创建成功。

----**结束**

4 接入 WAF

4.1 WAF 支持的端口

Web应用防火墙可防护的端口如[表4-1](#)所示。

表 4-1 WAF 支持的端口

端口分类	HTTP协议	HTTPS协议	端口防护限制数
标准端口	80	443	不限制

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

4.2 网站接入 WAF

4.2.1 网站接入流程（独享模式）

申请WAF独享模式后，您需要将防护域名接入WAF，使网站的访问流量全部流转到WAF进行监控防护。

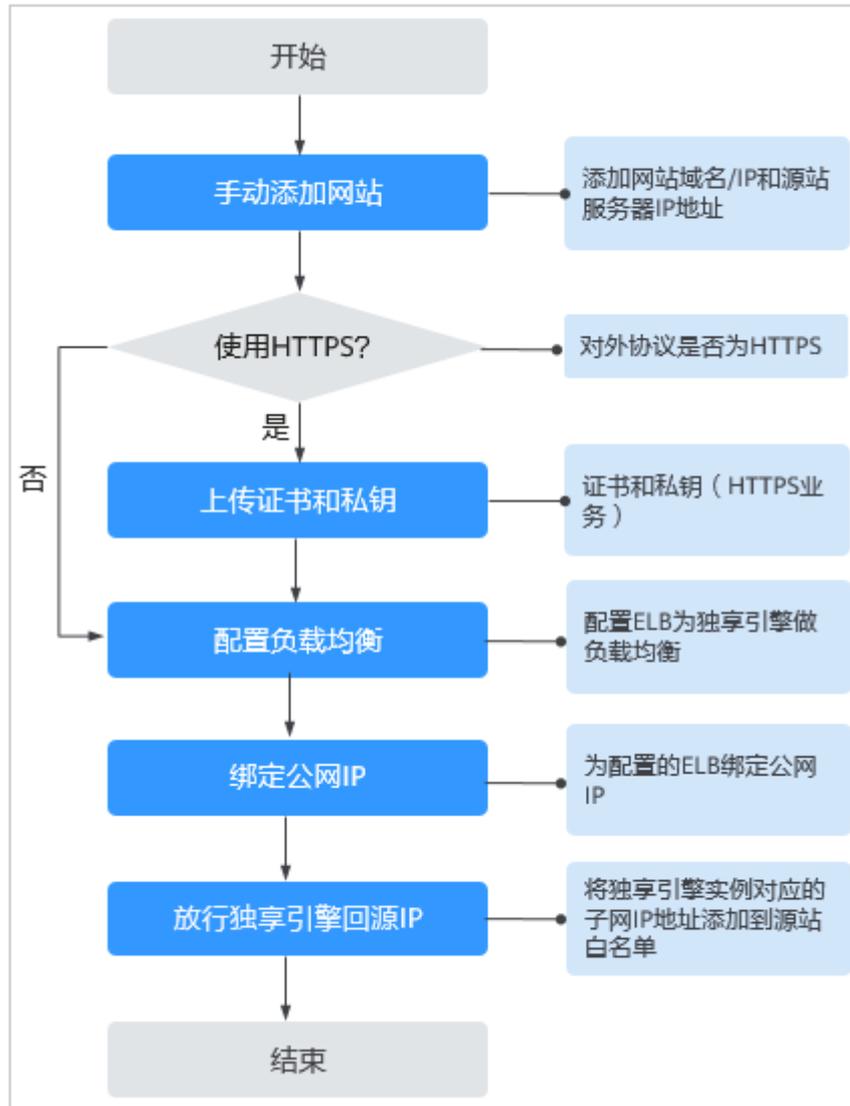
约束限制

WAF独享模式可以防护通过域名或IP访问的Web应用/网站。

网站接入流程说明

申请WAF独享模式后，您可以参照图4-1所示的配置流程，快速使用WAF。

图 4-1 网站接入 WAF 的操作流程图-独享模式



接入失败处理

如果域名接入失败，即域名接入状态为“未接入”，请参考[域名/IP接入状态显示“未接入”，如何处理?](#) 排查处理。

4.2.2 步骤一：添加防护网站

如果您的业务服务器部署在云上，您可以将网站的域名或IP添加到WAF，使网站流量切入WAF。

前提条件

已申请WAF独享引擎实例。

约束条件

- 接入Web应用防火墙的网站已使用公网ELB（Elastic Load Balance）代理用作负载均衡。
- 为了保证WAF的安全策略能够针对真实源IP生效，成功获取Web访问者请求的真实IP地址，如果WAF前没有使用CDN、云加速等七层代理服务器，且ELB使用的是四层负载均衡（NAT等方式），“是否已使用代理”务必选择“否”，其他情况，“是否已使用代理”选择“是”。

收集防护域名/IP 的配置信息

在添加防护域名/IP前，请获取防护域名/IP如表4-2所示相关信息。

表 4-2 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	防护域名	<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
	防护对象端口	<p>需要防护的域名对应的业务端口。</p> <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	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	选择申请的独享引擎实例所在的VPC。	vpc-default
	源站地址	客户端（例如浏览器）访问的网站服务器的私网IP地址。	192.168.1.1

获取信息	参数	说明	示例
(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 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。	-

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 > 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 在网站列表左上角，单击“添加防护网站”。

步骤6 配置“域名信息”。

- “网站名称”：可选参数，自定义网站名称。
- “防护对象”：防护的域名或IP，域名支持单域名和泛域名。

说明

- 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。
- “网站备注”：可选参数，网站的备注信息。

步骤7 源站配置，参数说明如[表4-3](#)所示。

表 4-3 基本信息参数说明

参数	参数说明	取值样例
防护对象 端口	在下拉框中选择面要防护的端口。 配置80/443端口，在下拉框中选择“标准端口”。	81

参数	参数说明	取值样例
服务器配置	<p>网站服务器地址的配置。包括对外协议、源站协议、VPC、源站地址和源站端口。</p> <ul style="list-style-type: none"> 对外协议：客户端请求访问服务器的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 源站协议：Web应用防火墙转发客户端请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。 VPC：选择独享引擎实例所在的VPC。 <p>说明 为了实现业务双活，避免业务单点故障，建议在同一VPC下申请两个WAF实例。</p> <ul style="list-style-type: none"> 源站地址：客户端（例如浏览器）访问的网站服务器的私网/内网IP地址。支持以下两种IP格式： <ul style="list-style-type: none"> IPv4，例如：XXX.XXX.1.1 IPv6，例如： fe80:0000:0000:0000:0000:0000:0000 源站端口：WAF独享引擎转发客户端请求到服务器的业务端口。 	<p>对外协议： HTTP</p> <p>源站协议： HTTP</p> <p>源站地址： XXX.XXX.1.1</p> <p>源站端口：80</p>
证书名称	<p>“对外协议”设置为“HTTPS”时，需要选择证书。您可以选择已创建的“国际证书”和“国密证书”或选择导入的新证书。导入新证书的操作请参见导入新证书。</p> <p>须知</p> <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，请参考导入新证书将证书转换为PEM格式，再上传。 如果您的证书即将到期，为了不影响网站的使用，建议您在到期前重新使用新的证书，并在WAF中同步更新网站绑定的证书。 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。 	--

步骤8 高级配置。

- “代理”：为了保证WAF的安全策略能够针对真实源IP生效，成功获取Web访问者请求的真实IP地址，如果WAF前已使用如CDN、云加速等提供七层Web代理的产品，请务必选择“是”。
- 选择“策略配置”：默认为“系统自动生成策略”，您也可以选择已创建的防护策略或在域名接入后根据防护需求配置防护规则。

系统自动生成的策略说明如下：

- 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。

步骤9 单击“确认”，添加域名完成。

---结束

生效条件

防护网站的初始“接入状态”为“未接入”，配置完负载均衡以及为弹性负载均衡绑定弹性IP后，当访问请求到达该网站的WAF专享引擎时，该防护网站的接入状态将自动切换为“已接入”。

导入新证书

当“对外协议”设置为“HTTPS”时，可以导入新证书。

1. 单击“导入新证书”，打开“导入新证书”对话框。
 - “类型”选择“国密证书”时，输入“证书名称”，并将“签名证书”、“签名私钥”、“加密证书”和“加密私钥”分别粘贴到对应的文本框中。
 - “类型”选择“国际证书”时，输入“证书名称”，并将“证书文件”和“证书私钥”分别粘贴到对应的文本框中。

📖 说明

Web应用防火墙将对私钥进行加密保存，保障证书私钥的安全性。

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考[表4-4](#)在本地将证书转换为PEM格式，再上传。

表 4-4 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”。
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">1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer2. 将“cert.cer”证书文件直接重命名为“cert.pem”。

格式类型	转换方式
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.der”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.der -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。
2. 单击“确认”，上传证书。

4.2.3 步骤二：配置负载均衡

添加防护网站后，您需要使用云上弹性负载均衡（Elastic Load Balance，简称ELB）为WAF独享引擎实例配置负载均衡和健康检查，以确保WAF的可靠性和稳定性。

前提条件

- 已添加独享模式防护网站。
- 已成功申请ELB实例。
- 在该独享引擎实例所在安全组中已放开了相关端口。

安全组建议配置以下访问规则：

- 入方向规则

根据业务需求添加指定端口入方向规则，放通指定端口入方向网络流量。例如，需要放通“80”端口时，您可以添加“策略”为“允许”的“TCP”、“80”协议端口规则。

- 出方向规则

默认。放通全部出方向网络流量。

系统影响

“分配策略类型”选择“加权轮询算法”时，请关闭“会话保持”，如果开启会话保持，相同的请求会转发到相同的WAF独享引擎实例上，当WAF独享引擎实例出现故障时，再次到达该引擎的请求将会出错。

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“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

- 步骤4** 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。
- 步骤5** 选择“监听器”页签后，单击“添加监听器”，配置监听器信息。
- 步骤6** 单击“下一步：配置后端分配策略”，配置后端分配策略。

须知

“分配策略类型”选择“轮询算法”时，请关闭“会话保持”，如果开启会话保持，相同的请求会转发到相同的WAF独享引擎实例上，当WAF独享引擎实例出现故障时，再次到达该引擎的请求将会出错。

- 步骤7** 单击“下一步：添加后端服务器”，添加云服务器并配置健康检查。
- 步骤8** 单击“下一步：确认配置”。
- 步骤9** 单击“提交”，监听器添加成功。
- 步骤10** 在添加的监听器页面，选择“后端服务器组”页签后，单击“添加”。
- 步骤11** 在弹出的“添加后端服务器”对话框中，选择已创建的WAF独享引擎实例。
- 步骤12** 单击“下一步”，为独享引擎配置端口。

须知

独享引擎监听端口需要与**步骤一：添加防护网站**时设置的端口保持一致。如果防护网站配置的是标准端口，则HTTP协议监听端口配置为“80”，HTTPS协议监听端口配置为“443”。

- 步骤13** 单击“完成”，配置完成。

----结束

生效条件

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。

4.2.4 步骤三：为弹性负载均衡绑定弹性公网 IP

WAF独享引擎实例配置负载均衡后，您还需要解绑源站服务器的弹性公网IP（Elastic IP，简称EIP），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。绑定后，请求流量会先经过WAF独享引擎进行攻击检测，然后转发到源站服务器，从而确保源站安全、稳定、可用。

前提条件

已为WAF独享引擎实例**配置负载均衡**。

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“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

步骤4 在“负载均衡器”页面，目标源站的负载均衡器所在行“操作”列，选择“更多 > 解绑IPv4/6公网IP”。

步骤5 在弹出的对话框中，单击“是”，解绑EIP。

步骤6 在“负载均衡器”页面，WAF独享引擎的ELB的负载均衡器所在行“操作”列，选择“更多 > 绑定IPv4/6公网IP”。

步骤7 在“绑定弹性公网IP”对话框中，选择**步骤4**中解绑的EIP，单击“确定”，绑定EIP。

----结束

4.2.5 步骤四：放行独享引擎回源 IP

网站以“独享模式”成功接入WAF后，建议您在源站服务器上配置只放行独享引擎回源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

网站以“独享模式”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独享引擎回源IP的访问控制策略。

为什么需要放行回源 IP

网站以“独享模式”成功接入WAF后，所有网站访问请求将先经过独享引擎配置的ELB然后流转到独享引擎实例进行监控，经独享引擎实例过滤后再返回到源站服务器，流量经独享引擎实例返回源站的过程称为回源。在服务器看来，接入WAF后所有源IP都会变成独享引擎实例的回源IP（即独享引擎实例对应的子网IP），以防止源站IP暴露后被黑客直接攻击。

源站服务器上的安全软件很容易认为独享引擎的回源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，网站以“独享模式”接入WAF防护后，您需要在源站服务器上设置放行创建的独享引擎实例对应的子网IP，不然可能会出现网站打不开或打开极其缓慢等情况。

前提条件

网站以“独享模式”成功接入WAF。

回源到 ECS

如果您的源站服务器直接部署在ECS上，请参考以下操作步骤设置安全组规则，放行独享模式回源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 > Web应用防火墙”。
- 步骤4** 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。
- 步骤5** 在独享引擎列表的“IP地址”栏，获取所有创建的独享引擎对应的子网IP地址。
- 步骤6** 单击页面左上方的 ，选择“计算 > 弹性云服务器 ECS”。
- 步骤7** 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8** 选择“安全组”页签，单击“更改安全组”。
- 步骤9** 在“更改安全组”对话框中，选择目标安全组或新建安全组并单击“确定”。
- 步骤10** 单击安全组ID，进入安全组基本信息页面。
- 步骤11** 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，参数配置说明如表4-5所示。

表 4-5 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5中获取的所有独享引擎实例的子网IP地址。 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12** 单击“确定”，安全组规则添加完成。

成功添加安全组规则后，安全组规则将允许独享引擎回源IP地址的所有入方向流量。

您可以使用Telnet工具测试已接入WAF防护的源站IP对应的业务端口是否能成功建立连接验证配置是否生效。

例如，执行以下命令，测试已接入WAF防护的源站IP对外开放的443端口是否能成功建立连接。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示安全组规则配置成功。

Telnet 源站IP 443

----结束

回源到 ELB

如果您的源站服务器使用ELB进行流量分发，请参考以下操作步骤设置访问控制（白名单）策略，只放行独享模式回源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 击页面左上方的 ，选择“安全 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

步骤5 在独享引擎列表的“IP地址”栏，获取所有创建的独享引擎对应的子网IP地址。

步骤6 单击页面左上方的 ，选择“网络 > 弹性负载均衡 ELB”。

步骤7 在独享引擎绑定的ELB所在行的“名称”列中，单击ELB名称，进入ELB的详情页面。

步骤8 选择“监听器”页签，在“访问控制”列单击“设置访问控制”。

步骤9 在弹出的对话框中，“访问策略”选择“白名单”。

1. 单击“创建IP地址组”，将**步骤5**中独享引擎实例的回源IP地址添加到“IP地址组”中。
2. 在“IP地址组”的下拉框中选择**步骤9.1**中创建的IP地址组。

步骤10 单击“确定”，白名单访问控制策略添加完成。

成功配置访问控制策略后，访问控制策略将允许独享引擎回源IP地址的所有入方向流量。

您可以使用Telnet工具测试已接入WAF防护的源站IP对应的业务端口是否能成功建立连接验证配置是否生效。

例如，执行以下命令，测试已接入WAF防护的源站IP对外开放的443端口是否能成功建立连接。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示安全组规则配置成功。

Telnet 源站IP 443

----结束

5 管理防护域名

5.1 查看基本信息

您可以通过Web应用防火墙查看防护域名的基本信息、切换工作模式、删除防护域名。

前提条件

已成功添加防护网站。

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 > Web应用防火墙”。

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 查看防护网站信息，参数说明如表5-1所示。

表 5-1 参数说明

参数名称	参数说明
域名	防护的域名或IP。
部署模式	防护网站的部署模式，仅支持“独享模式”。
近3天威胁	该域名3天内的防护情况。

参数名称	参数说明
工作模式	防护模式。单击▼，可以选择以下三种防护模式： <ul style="list-style-type: none">“开启防护”：开启状态。“暂停防护”：关闭状态。如果大量的正常业务被拦截，比如大量返回418返回码，可以将“工作模式”切换为“暂停防护”。该模式下，WAF对所有的流量请求只转发不检测。该模式存在风险，建议您优先选择全局白名单（原误报屏蔽）规则处理正常业务拦截问题。
防护策略	显示通过WAF配置的防护策略总数。单击数字可跳转到规则配置页面，配置具体的防护规则，具体的配置方法参见 配置防护规则 。
域名接入进度	展示网站接入WAF未完成的步骤或者接入状态。 <ul style="list-style-type: none">“未接入”：网站未接入WAF或者接入不成功。“已接入”：网站接入WAF成功。 须知 防护网站“部署模式”为“独享模式”时，防护网站的初始接入状态为“未接入”，当访问请求到达该网站的实例时，该防护网站的接入状态将自动切换为“已接入”。
操作	单击“删除”，可删除目标防护网站。

步骤6 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7 查看防护网站的信息。

- 当客户端协议选择HTTPS时，若需要更新证书，在“国际证书”或者“国密证书”所在行的证书名称后，单击，在弹出的对话框中，上传新证书或者选择已有证书。关于证书更新的详细内容请参见[更新证书](#)。
- 当客户端协议选择HTTPS时，若需要更新访问源站的TLS版本和TLS的加密套件，单击，在弹出的对话框中，重新选择TLS版本和TLS的加密套件。关于配置TLS的详细内容请参见[配置TLS最低版本和加密套件](#)。
- 若需要修改“是否已使用代理”，可以单击，在弹出的对话框中，重新配置是否需要使用代理，如果需要使用代理，设置成“是”。
- “告警页面”默认为“系统默认”的页面，您也可以单击，在弹出的对话框中，配置“自定义”或者“重定向”页面。
- 如果您需要针对域名的每个请求设置超时时间，开启“超时配置”并单击，设置“连接超时”、“读超时”、“写超时”的时间。开启后不支持关闭，具体的操作请参见[配置网站连接超时时间](#)。

----结束

5.2 切换工作模式

您可以通过Web应用防火墙服务切换工作模式。Web应用防火墙提供开启防护和暂停防护两种工作模式。

前提条件

防护域名已接入WAF。

应用场景

- 开启防护：开启防护模式后，WAF会根据您配置的策略进行攻击检测。
- 暂停防护：如果大量的正常业务被拦截，比如大量返回418返回码，可以将“工作模式”切换为“暂停防护”。该模式下，WAF对所有的流量请求只转发不检测，日志也不会记录。该模式存在风险，建议您优先选择全局白名单（原误报屏蔽）规则处理正常业务拦截问题。

系统影响

切换为暂停模式后，WAF只转发流程请求，网站安全可能存在风险，建议您优先选择全局白名单（原误报屏蔽）规则处理正常业务拦截问题。

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 > Web应用防火墙”。

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。

----结束

5.3 配置 TLS 最低版本和加密套件

安全传输层协议（Transport Layer Security，TLS）在两个通信应用程序之间提供保密性和数据完整性。HTTPS协议是由TLS+HTTP协议构建的可进行加密传输、身份认证的网络协议。当防护网站的“对外协议”使用了“HTTPS”时，您可以通过WAF为网站设置最低TLS版本和加密套件（多种加密算法的集合），对于低于最低TLS版本的请求，将无法正常访问网站，以满足行业客户的安全需求。

WAF默认配置的最低TLS版本为TLS v1.0，加密套件为加密套件1，为了确保网站安全，建议您将网站的最低TLS版本和TLS加密套件配置为安全性更高TLS版本和加密套件。

前提条件

- 已添加防护网站。
- 防护网站的“对外协议”使用了HTTPS协议。

应用场景

WAF默认配置的最低TLS版本为“TLS v1.0”，为了确保网站安全，建议您根据业务实际需求进行配置，推荐配置的最低TLS版本如[表5-2](#)所示。

表 5-2 推荐配置的最低 TLS 版本说明

场景	最低TLS版本（推荐）	防护效果
网站安全性能要求很高（例如，银行金融、证券、电子商务等有重要商业信息和重要数据的行业）	TLS v1.2	WAF将自动拦截TLS v1.0和TLS v1.1协议的访问请求。
网站安全性能要求一般（例如，中小企业门户网站）	TLS v1.1	WAF将自动拦截TLS1.0协议的访问请求。
客户端APP无安全性要求，可以正常访问网站	TLS v1.0	所有的TLS协议都可以访问网站。

WAF推荐配置的加密套件为“加密套件1”，可以满足浏览器兼容性和安全性，各加密套件相关说明如表5-3所示。

表 5-3 加密套件说明

加密套件名称	支持的加密算法	说明
默认加密套件	<ul style="list-style-type: none"> ● ECDHE-RSA-AES256-SHA384 ● AES256-SHA256 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH ● !AESGCM 	<ul style="list-style-type: none"> ● 兼容性：较好，支持的客户端较为广泛 ● 安全性：一般

加密套件名称	支持的加密算法	说明
加密套件1	<ul style="list-style-type: none"> ● ECDHE-ECDSA-AES256-GCM-SHA384 ● HIGH ● !MEDIUM ● !LOW ● !aNULL ● !eNULL ● !DES ● !MD5 ● !PSK ● !kRSA ● !SRP ● !3DES ● !DSS ● !EXP ● !CAMELLIA ● @STRENGTH 	<p>推荐配置。</p> <ul style="list-style-type: none"> ● 兼容性：较好，支持的客户端较为广泛 ● 安全性：较高
加密套件2	<ul style="list-style-type: none"> ● ECDH+AESGCM ● EDH+AESGCM 	<ul style="list-style-type: none"> ● 兼容性：一般，严格符合 PCI DSS的FS要求，较低版本浏览器可能无法访问。 ● 安全性：高
加密套件3	<ul style="list-style-type: none"> ● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES256-SHA384 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH 	<ul style="list-style-type: none"> ● 兼容性：一般，较低版本浏览器可能无法访问。 ● 安全性：高，支持ECDHE、DHE-GCM、RSA-AES-GCM多种算法。

加密套件名称	支持的加密算法	说明
加密套件4	<ul style="list-style-type: none"> • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • HIGH • !MD5 • !aNULL • !eNULL • !NULL • !EDH 	<ul style="list-style-type: none"> • 兼容性：较好，支持的客户端较为广泛 • 安全性：一般，新增支持GCM算法。

WAF提供的TLS加密套件对于高版本的浏览器及客户端都可以兼容，不能兼容部分老版本的浏览器，以TLS v1.0协议为例，加密套件不兼容的浏览器及客户端参考说明如表5-4所示。

须知

建议您以实际客户端环境测试的兼容情况为准，避免影响现网业务。

表 5-4 加密套件不兼容的浏览器/客户端参考说明 (TLS v1.0)

浏览器/客户端	默认加密套件	加密套件 1	加密套件 2	加密套件 3	加密套件 4
Google Chrome 63 /macOS High Sierra 10.13.2	×	√	√	√	×
Google Chrome 49/ Windows XP SP3	×	×	×	×	×
Internet Explorer 6/Windows XP	×	×	×	×	×
Internet Explorer 8/Windows XP	×	×	×	×	×
Safari 6/iOS 6.0.1	√	√	×	√	√
Safari 7/iOS 7.1	√	√	×	√	√

浏览器/客户端	默认加密套件	加密套件 1	加密套件 2	加密套件 3	加密套件 4
Safari 7/OS X 10.9	√	√	×	√	√
Safari 8/iOS 8.4	√	√	×	√	√
Safari 8/OS X 10.10	√	√	×	√	√
Internet Explorer 7/Windows Vista	√	√	×	√	√
Internet Explorer 8~10/Windows 7	√	√	×	√	√
Internet Explorer 10/Windows Phone 8.0	√	√	×	√	√
Java 7u25	√	√	×	√	√
OpenSSL 0.9.8y	×	×	×	×	×
Safari 5.1.9/OS X 10.6.8	√	√	×	√	√
Safari 6.0.4/OS X 10.8.4	√	√	×	√	√

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 > Web应用防火墙”。

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 在“合规认证”行，可以勾选“PCI DSS”或“PCI 3DS”开启合规认证。

步骤7 在“国际证书”或者“国密证书”所在行的加密套件后，单击 。

步骤8 在弹出的“TLS配置”对话框中，选择TLS版本和加密套件。

1. “证书类型”为“国际证书”时，选择最低TLS版本和加密套件。

选择“最低TLS版本”，相关说明如下：

- 默认为TLS v1.0版本，TLS v1.0及以上版本的请求可以访问域名。
- 选择TLS v1.1版本时，TLS v1.1及以上版本的请求可以访问域名。
- 选择TLS v1.2版本时，TLS v1.2及以上版本的请求可以访问域名。

- “证书类型”为“国密证书”时，仅支持“gmtls”的TLS版本和默认的加密套件。

步骤9 单击“确认”，TLS配置完成。

----结束

生效条件

如果“最低TLS版本”配置为“TLS v1.2”，则TLS v1.2协议可以正常访问网站，TLS v1.1及以下协议不能正常访问网站。

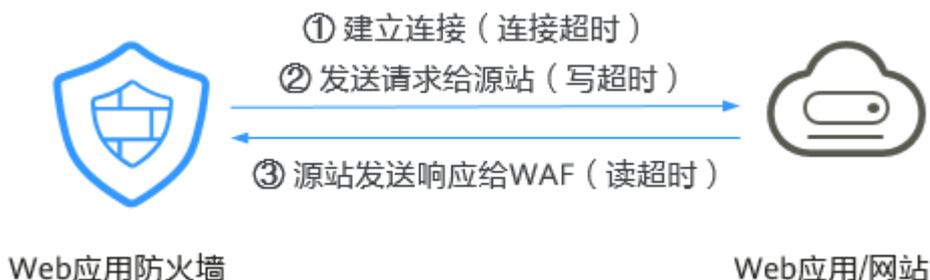
5.4 配置网站连接超时时间

如果您需要针对域名的每个请求设置超时时间，可参考本章节开启WAF到客户源站的“超时配置”并设置“连接超时”、“读超时”、“写超时”的时间。开启后不支持关闭。

- 连接超时**：WAF转发客户端请求时，TCP三次握手超时时间。
- 写超时**：WAF向源站发送请求的超时时间，若在设定的写超时时间内源站未接收到请求，则认为连接超时。
- 读超时**：WAF从源站读取响应的超时时间，若在设定的读超时时间内未收到来自源站的响应，则认为连接超时。

WAF转发请求给源站的三个步骤如**图5-1**所示。

图 5-1 WAF 转发请求给源站



说明

- 浏览器到WAF引擎的连接超时时长是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60秒，该值可以参考本章节进行手动设置。

前提条件

已添加防护网站。

约束条件

- WAF不支持手动设置浏览器到WAF引擎的连接超时时长，仅支持配置WAF到客户源站的连接超时时长。

- 开启后不支持关闭。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“安全 > Web应用防火墙”。

步骤3 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤4 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5 在“超时配置”所在行，单击“启用状态”图标，开启超时配置。

步骤6 单击 ，设置“连接超时”、“读超时”、“写超时”的时间，并单击  保存设置。

----结束

5.5 配置连接保护

网站接入WAF防护之后，若您访问网站时出现大量的502 Bad Gateway，504 Gateway Timeout错误或者等待处理的请求，为了保护源站的安全，可使用WAF的宕机保护和连接保护功能。当502/504请求数量或读等待URL请求数量以及占比阈值达到您设置的值时，将触发WAF熔断功能开关，实现宕机保护和读等待URL请求保护。

前提条件

- 已添加防护网站。
- 已将独享引擎版本升级到最新版本，具体的操作请参见[升级独享引擎实例版本](#)。

约束条件

- 防护网站的部署模式为“独享模式”。
- 开启“连接保护”前，必须将[将独享引擎实例版本升级到最新版本](#)，否则开启后可能会对业务产生影响。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“安全 > Web应用防火墙”。

步骤3 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤4 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5 在“连接保护”所在行，单击“启用状态”图标，开启连接保护。

步骤6 根据业务需要，在各参数所在行，单击 ，配置“宕机保护”和“连接保护”参数值，并单击  保存设置，参数说明如[表5-5](#)所示。

表 5-5 连接保护参数说明

参数		参数说明	示例
宕机保护	502/504数量阈值	每30s累加的502/504数量阈值	1000
	502/504数量占比(%)	总请求数量中502/504数量占比达到所设定值，并且与数量阈值同时满足时触发宕机保护。	90
	初次保护时间(秒)	初次触发宕机的保护时间，即WAF将停止转发用户请求的时间。	180
	连续触发叠加系数	连续触发时，保护时间延长最大倍数，叠加周期为3600s。 例如，“初次保护时间”设置为180s，“连续触发叠加系数”设置为3。 <ul style="list-style-type: none"> 当触发次数为2（即小于3）时，保护时间为360s。 当次数大于等于3时，保护时间为540s。 当累计保护时间超过1小时（3600s），叠加次数会从头计数。 	3
连接保护	读等待URL请求数量阈值	读等待URL请求数量到达设定值即触发连接保护	6000
	保护时间(秒)	达到数量阈值所触发的保护时间，即WAF将停止转发用户请求的时间。	60

----结束

5.6 更新证书

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

- 如果您的证书即将到期，为了不影响网站的使用，建议您在到期前重新使用新的证书，并在WAF中同步更新网站绑定的证书。
- 如果您需要更新网站绑定证书的信息，可以在WAF中为网站绑定新的证书。

前提条件

- 已添加防护网站。
- 防护网站的“对外协议”使用了HTTPS协议。

约束条件

- 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。
- WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考[步骤6](#)将证书转换为PEM格式，再上传。

系统影响

- 证书过期后，对源站的影响是覆灭性的，比主机崩溃和网站无法访问的影响还要大，且会造成WAF的防护规则不生效，故建议您在证书到期前及时更新证书。
- 更新证书不会影响业务，更换过程中会使用旧证书，更新成功后，自动切为新证书，新证书立刻生效。

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 > Web应用防火墙”。

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 在“国际证书”或者“国密证书”的证书名称后，单击 ，在弹出的“更新证书”对话框中，上传新证书或者选择已有证书。

- 更新国际证书，“更新方式”选择“上传证书”时，在对话框中输入“证书名称”，并将证书内容和私钥内容粘贴到对应的文本框中。
- 更新国密证书，“更新方式”选择“上传证书”时，在对话框中输入“证书名称”，将签名证书、签名私钥、加密证书和加密私钥的内容粘贴到对应的文本框中。
- “更新方式”选择“选择已有证书”时，在“证书选择”的下拉框中选择已有的证书。

步骤7 单击“确认”，证书更新完成。

----结束

5.7 配置攻击惩罚的流量标识

WAF根据配置的流量标识识别客户端IP、Session或User标记，以分别实现IP、Cookie或Params恶意请求的攻击惩罚功能。

前提条件

已添加防护网站。

约束条件

- 如果配置了IP标记，为了确保IP标记生效，请您确认防护网站在接入WAF前已使用了7层代理，且防护网站的“是否已使用代理”为“是”。
如果未配置IP标记，WAF默认通过客户端IP进行识别。
- 使用Cookie或Params恶意请求的攻击惩罚功能前，您需要分别配置对应域名的Session标记或User标记。

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 > Web应用防火墙”。

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 在“流量标识”栏中，单击“IP标记”、“Session标记”或“User标记”后的 ，分别设置流量标记，相关参数说明如表5-6所示。

表 5-6 流量标识参数说明

标识	说明	配置样例
IP标记	<p>客户端最原始的IP地址的HTTP请求头字段。</p> <p>如果配置该标识，请确保网站在接入WAF前已使用了7层代理，且防护网站的“是否已使用代理”为“是”，IP标记功能才能生效。</p> <p>开启了代理后，WAF获取客户端的策略如下。</p> <ol style="list-style-type: none">1. 配置了IP标记后，WAF将优先取“upstream”中配置的源IP头列表，如果未取到，执行步骤6.22. 取config中配置的源IP头列表“cdn-src-ip”字段对应的值，未取到，执行步骤6.3。3. 取“x-real-ip”字段的值，未取到，执行步骤6.4。4. 取“x-forwarded-for”字段左边开始第一个公网IP，未取到，执行步骤6.5。5. 取WAF看到的TCP连接IP，“remote_addr”字段对应的值。	X-Forwarded-For

标识	说明	配置样例
Session标记	用于Cookie恶意请求的攻击惩罚功能。在选择Cookie拦截的攻击惩罚功能前，必须配置该标识。	jsessionid
User标记	用于Params恶意请求的攻击惩罚功能。在选择Params拦截的攻击惩罚功能前，必须配置该标识。	name

步骤7 单击“确认”，完成标记信息配置。

----结束

5.8 修改服务器配置信息

当您需要修改防护网站的服务器信息或者需要添加服务器信息时，可参考本章节进行操作。

本章节可对以下场景提供指导：

- 修改服务器信息，即修改对外协议、源站协议、VPC、源站地址、源站端口。
- 添加服务器配置。
- 更新证书，关于证书更新的详细内容可参见[更新证书](#)。

前提条件

已添加防护网站。

系统影响

修改服务器配置信息对业务无影响。

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 > Web应用防火墙”。

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 在“服务器信息”栏中，单击 。

步骤7 在“修改服务器信息”页面，根据需要修改服务器的各项配置以及已绑定的证书。

- 关于证书更新的详细内容可参见[更新证书](#)。
- WAF支持配置多个后端服务器，如果需要增加后端服务器，可单击“添加”，增加服务器。

步骤8 单击“确认”，完成服务器信息修改。

----结束

5.9 修改拦截返回页面

当访问者触发WAF拦截时，默认返回WAF“系统默认”的拦截返回页面，您也可以根据自己的需要，配置“自定义”或者“重定向”的拦截返回页面。

前提条件

已添加防护网站。

约束条件

- “自定义”的拦截返回页面支持配置text/html、text/xml和application/json三种页面类型的页面内容。
- “重定向”地址的根域名必须和当前被防护的域名（包括泛域名）保持一致。例如，被防护的域名为www.example.com，端口为8080，则重定向URL可设置为“http://www.example.com:8080/error.html”。

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 > Web应用防火墙”。

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 在“告警页面”所在行的页面模板名称后，单击 ，在弹出的“告警页面”对话框中，选择“页面模板”进行配置。

- “页面模板”选择“系统默认”时，默认返回WAF内置的HTTP返回码为418的拦截页面。
- “页面模板”选择“自定义”时。
 - HTTP返回码：自定义页面配置的返回码。
 - 页面类型：可选择text/html、text/xml和application/json三种类型。
 - 页面内容：根据选择的“页面类型”配置对应的页面内容。
- “页面模板”选择“重定向”时，根据界面提示配置重定向URL。

重定向URL的根域名必须和当前被防护的域名（包括泛域名）保持一致。例如，被防护的域名为www.example.com，端口为8080，则重定向URL可设置为“http://www.example.com:8080/error.html”。

步骤7 单击“确认”，告警页面配置成功。

----结束

5.10 删除防护域名

您可以通过Web应用防火墙服务对不再防护的网站执行删除操作。

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。

前提条件

已添加防护域名。

系统影响

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。

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 > Web应用防火墙”。

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 在目标防护域名所在行的“操作”列中，单击“删除”，进入删除防护域名对话框界面。

步骤6 在删除防护网站对话框中，确认删除防护网站。

如果需要保留该域名绑定的防护策略，可以勾选“保留该域名的防护策略”。

步骤7 单击“确定”，页面右上角弹出“删除成功”，则说明删除操作成功。

----结束

6 管理证书

6.1 上传证书

添加防护网站时，如果“对外协议”选择“HTTPS”协议，需要选择证书使证书绑定到防护网站。

您可以通过上传证书，将证书上传到WAF，使防护网站直接选择上传的证书。

前提条件

已获取证书文件和证书私钥信息。

规格限制

WAF支持上传的证书套数和WAF支持防护的域名的个数相同。

约束条件

添加防护网站或更新证书时导入的新证书，将直接添加到“证书管理”页面的证书列表中，且导入的新证书会统计到创建的证书套数中。

应用场景

当域名的“对外协议”设置为“HTTPS”时，需要配置证书。

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 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。

步骤5 在证书列表左上方，单击“上传证书”，弹出“上传证书”对话框。

- “类型”选择“国密证书”时，输入“证书名称”，并将“签名证书”、“签名私钥”、“加密证书”和“加密私钥”分别粘贴到对应的文本框中。
- “类型”选择“国际证书”时，输入“证书名称”，并将“证书文件”和“证书私钥”分别粘贴到对应的文本框中。

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考表6-1在本地将证书转换为PEM格式，再上传。

表 6-1 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”。
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">1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer2. 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.der”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.der -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。

步骤6 单击“确认”，证书创建成功。

----结束

生效条件

成功创建的证书将显示在证书列表中。

相关操作

- 当鼠标移到目标证书的名称后时，单击，您可以修改证书的名称。

须知

如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。
- 在目标证书所在行的“操作”列中，单击“删除”，您可以删除该证书。

6.2 删除证书

当证书过期或证书无效时，您可以删除该证书。

前提条件

证书没有被使用，即证书未绑定防护网站。

约束条件

如果证书已绑定防护网站，删除证书前需要解除该证书与域名绑定关系。

系统影响

- 删除证书不会影响业务。
- 证书删除后不可恢复，请谨慎删除证书。

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 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。

步骤5 在目标证书所在行的“操作”列中，单击“删除”。

步骤6 在弹出的提示框中，单击“确认”，删除证书。

----结束

相关操作

如果证书已绑定防护网站，删除证书前需要解除该证书与域名绑定关系。

请参考以下操作步骤，解除证书与域名绑定关系。

步骤1 在目标证书所在行的“应用域名”列中，单击防护域名，进入域名基本信息页面。

步骤2 在“证书名称”后单击 ，在弹出的对话框中，上传新证书或者选择其他已有证书。

----结束

6.3 查看证书信息

您可以查看证书的名称、绑定的域名和到期时间等详细信息。

前提条件

已推送证书到WAF或在WAF上创建了证书。

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 > Web应用防火墙”。
- 步骤4** 在左侧导航树中，选择“对象管理 > 证书管理”，进入“证书管理”页面。
- 步骤5** 查看证书信息，相关参数说明如表6-2所示。

表 6-2 证书参数说明

参数名称	参数说明
名称	证书名称。
证书类型	支持“国际证书”和“国密证书”。
到期时间	证书到期时间。 证书过期后，对源站的影响是覆灭性的，比主机崩溃和网站无法访问的影响还要大，且会造成WAF的防护规则不生效，建议您在证书到期前及时更新证书。有关更新证书的详细操作，请参见 更新证书 。
应用域名	已使用该证书的域名。域名与证书是一一对应的，同一个证书可以绑定到多个域名。

----结束

相关操作

- 当鼠标移到目标证书的名称后时，单击 ，您可以修改证书的名称。

须知

如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。

- 在目标证书所在行的“操作”列中，单击“删除”，您可以删除该证书。

7 管理黑白名单 IP 地址组

7.1 添加黑白名单 IP 地址组

IP地址组集中管理IP地址或网段，被黑白名单规则引用时可以批量设置IP/IP地址段。

前提条件

已申请Web应用防火墙实例。

约束条件

添加IP地址组时，请确保IP/IP地址段未添加到其他IP地址组，重复添加同一IP/IP地址段会导致添加IP地址组失败。

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 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 地址组管理”，进入“地址组管理”页面。

步骤5 选择“我的地址组”页签，进入地址组页面。

步骤6 在我的地址组列表左上方，单击“添加地址组”。

步骤7 在弹出的“添加地址组”对话框中，输入“地址组名称”和“IP/IP段”。

步骤8 单击“确认”，地址组创建成功。

----结束

7.2 修改或删除黑白名单 IP 地址组

您可以通过修改或删除IP地址，管理IP地址组信息。

前提条件

已成功创建地址组。

约束条件

- 修改IP地址组时，请确保IP地址组中的IP/IP地址段未添加到其他IP地址组，重复添加同一IP/IP地址段会导致添加IP地址组失败。
- 如果地址组已被黑白名单规则引用，删除地址组前需要解除该地址组与黑白名单规则的绑定关系。

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 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“对象管理 > 地址组管理”，进入“地址组管理”页面。

步骤5 在地址组列表中，查看地址组信息。

表 7-1 参数说明

参数名称	参数说明
地址组名称	用户自定义的地址组名称。
IP/IP段	地址组添加的IP地址/IP地址段。
应用规则	引用地址组的防护规则。
备注	地址组补充信息。

步骤6 修改或删除IP地址组。

- 修改地址组

在目标地址组所在行的“操作”列中，单击“修改”，在弹出的“修改地址组”对话框中，修改地址组名称或IP地址/IP地址段后，单击“确认”。

- 删除地址组

在目标地址组所在行的“操作”列中，单击“删除”，在弹出的提示框中，单击“确认”。

----结束

8 配置防护规则

8.1 配置引导

WAF 引擎检测机制

Web应用防火墙内置的防护规则，可帮助您防范常见的Web应用攻击，包括XSS攻击、SQL注入、爬虫检测、Webshell检测等。同时，您也可以根据自己网站防护的需要，灵活配置防护规则，Web应用防火墙根据您配置的防护规则更好的防护您的网站业务。WAF引擎内置防护规则的检测流程如[图8-1](#)所示，自定义规则的检测顺序如[图8-2](#)所示。

图 8-1 WAF 引擎检测图

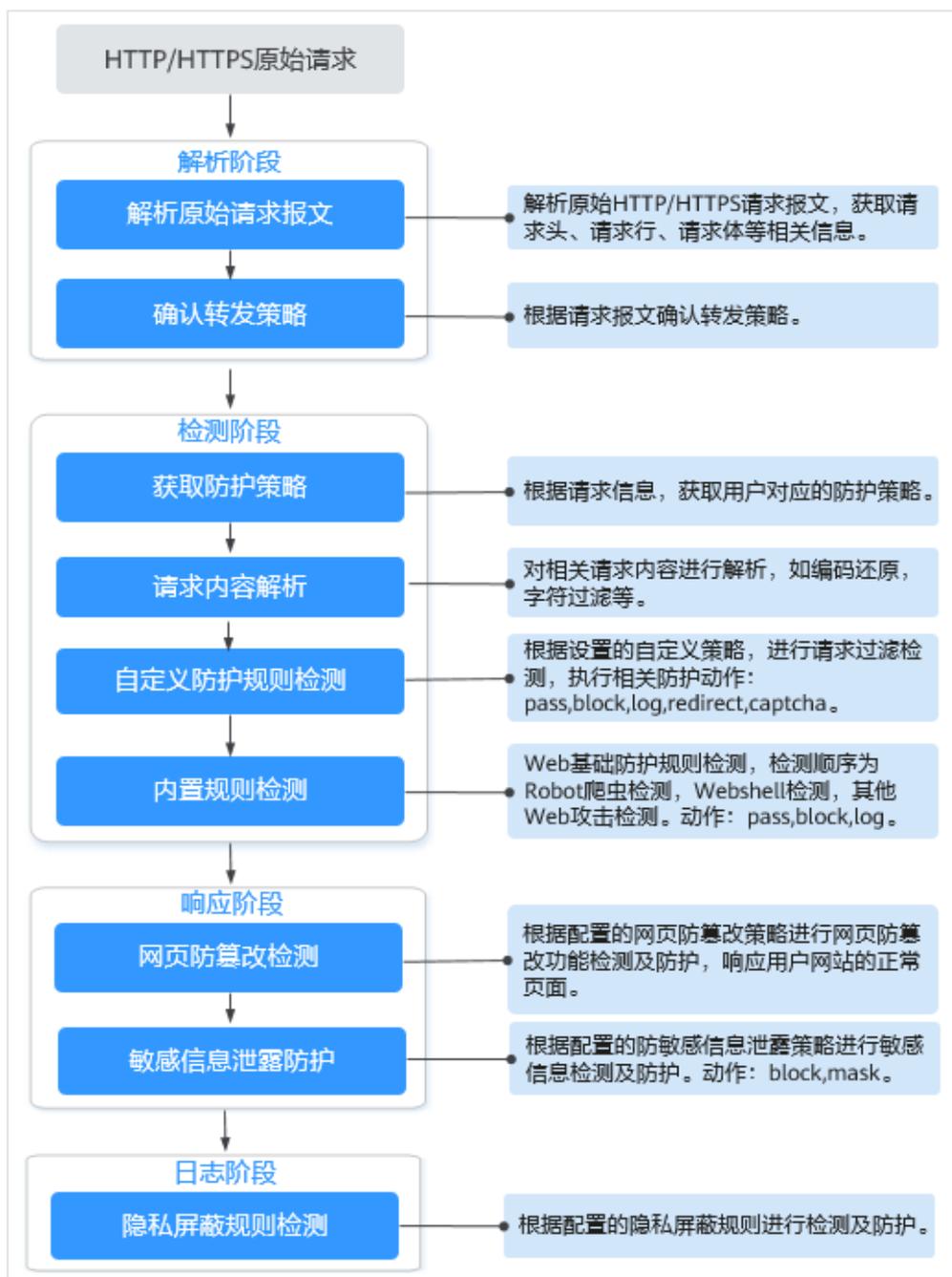


图 8-2 自定义防护规则的检测顺序



响应动作：

- pass：命中规则后无条件放行当前请求。
- block：命中规则后拦截当前请求。
- captcha：命中规则后执行人机验证动作。
- redirect：命中规则后通知客户端执行重定向动作。
- log：命中规则后仅记录攻击信息。
- mask：命中规则后对相关敏感信息进行脱敏处理。

防护规则配置方式

为了简化您的配置过程，WAF提供了以下两种自定义防护规则的配置方式，请根据您的业务合理选择配置方式。

方式一：单个域名配置防护规则

此种方式适合域名业务较少或者域名业务适用的配置规则不相同的用户。

📖 说明

域名添加到WAF后，WAF会自动为该域名绑定一个防护策略，为域名配置的防护规则默认也添加到绑定该域名的防护策略。如果以后有适用于该防护策略的域名，可直接通过该策略添加防护域名，具体的操作请参见[添加策略适用的防护域名](#)。

- 入口
 - a. 在左侧导航树中选择“网站设置”，进入“网站设置”页面。
 - b. 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。
- 进入规则配置页面可配置的防护规则

表 8-1 可配置的防护规则

防护规则	说明	参考文档
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。	配置Web基础防护规则
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。	配置CC攻击防护规则
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。	配置精准访问防护规则
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。	配置IP黑白名单规则
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。	配置攻击惩罚标准
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。	配置地理位置访问控制规则
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。	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。	配置网站反爬虫防护规则

防护规则	说明	参考文档
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。	配置防敏感信息泄露规则
全局白名单（原误报屏蔽）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。	配置全局白名单（原误报屏蔽）规则
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。	配置隐私屏蔽规则

方式二：批量配置防护规则

此种方式适用于域名业务较多且多个域名需要防护的策略配置相同的用户。该方式可大大减少用户相同重复的配置工作，增强防护的效率性。

- 入口
在左侧导航树中选择“防护策略”，进入“防护策略”页面。
- 操作步骤：
 - 新建策略。具体的操作请参见[添加防护策略](#)。
 - 配置防护规则。具体的操作请参见[批量添加防护规则](#)。
 - 批量添加策略适用的防护域名。具体操作请参见[添加策略适用的防护域名](#)。

8.2 配置 Web 基础防护规则

Web基础防护开启后，默认防范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。您还可以根据实际使用需求，开启Webshell检测、深度反逃逸检测和header全检测等Web基础防护。

须知

Web基础防护支持“拦截”和“仅记录”模式。

前提条件

已添加防护网站。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“Web基础防护”配置框中，用户可根据自己的需要参照表8-2更改Web基础防护的“状态”和“模式”。

表 8-2 防护动作参数说明

参数	说明
状态	Web应用防护攻击的状态。 <ul style="list-style-type: none">：开启状态。：关闭状态。
模式	<ul style="list-style-type: none">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。

步骤7 在“Web基础防护”配置框中，单击“高级设置”，进入“Web基础防护”界面。

步骤8 根据您的业务场景，开启合适的防护功能，检测项说明如表8-4所示。

1. 防护等级设置。

在页面上方，选择防护等级，Web基础防护设置了三种防护等级：“宽松”、“中等”、“严格”，默认情况下，选择“中等”。

表 8-3 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。
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（原误报屏蔽）规则，再开启“严格”模式，使WAF能有效防护更多攻击。

2. 防护检测类型设置。

须知

默认开启“常规检测”防护检测，用户可根据业务需要，参照表8-4开启其他需要防护的检测类型。

表 8-4 检测项说明

检测项	说明
常规检测	防护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。其中，SQL注入攻击主要基于语义进行检测。 说明 开启“常规检测”后，WAF将根据内置规则对常规检测项进行检测。
Webshell检测	防护通过上传接口植入网页木马。 说明 开启“Webshell检测”后，WAF将对通过上传接口植入的网页木马进行检测。
深度检测	防护同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸。 说明 开启“深度检测”后，WAF将对深度反逃逸进行检测防护。
header全检测	默认关闭。关闭状态下WAF会检测常规存在注入点的header字段，包含User-Agent、Content-type、Accept-Language和Cookie。 说明 开启“header全检测”后，WAF将对请求里header中所有字段进行攻击检测。

----结束

防护效果

假如已添加域名“www.example.com”，且已开启了Web基础防护的“常规检测”，防护模式为“拦截”。您可以参照以下步骤验证WAF防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照章节[步骤一：添加防护网站](#)重新完成域名接入。
- 能正常访问，执行2。

步骤2 清理浏览器缓存，在浏览器中输入“http://www.example.com?id=1%27%20or%201=1”模拟SQL注入攻击。

步骤3 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志，您也可以[下载防护事件数据](#)。

----结束

配置示例-拦截 SQL 注入攻击

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证WAF拦截SQL注入攻击。

步骤1 开启Web基础防护的“常规检测”，并将防护模式设置为“拦截”。

步骤2 开启Web基础防护。

步骤3 清理浏览器缓存，在浏览器中输入模拟SQL注入攻击（例如，http://www.example.com?id=' or 1=1）。

WAF将拦截该访问请求，拦截页面示例如图8-3所示。

图 8-3 WAF 拦截攻击请求



步骤4 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

8.3 配置 CC 攻击防护规则

CC攻击防护规则支持通过限制单个IP/Cookie/Referer访问者对防护网站上特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击。当您配置完CC攻击防护规则并开启CC攻击防护后，WAF才能根据您配置的CC攻击防护规则进行CC攻击防护。

前提条件

已添加防护网站。

约束条件

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 网站同时接入WAF和CDN（Content Delivery Network，内容分发网络）时，如果“防护动作”配置为“人机验证”，建议防护规则的“路径”配置为动态页面。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“CC攻击防护”配置框中，用户可根据自己的需要更改“状态”，单击“自定义CC攻击防护规则”，进入CC防护规则配置页面。

步骤7 在“CC攻击防护”规则配置页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，根据表8-5配置CC防护规则。

例如，Cookie标识为“name”字段的同一值的用户访问目标地址（以/admin为前缀的地址，例如，https://www.example.com/adminlogic）时，一旦在60秒内访问超过10次，就直接阻断该Cookie用户访问目标URL地址，阻断操作持续600秒，阻断页面返回自定义的页面内容。

表 8-5 CC 防护规则参数说明

参数	参数说明	取值样例
限速模式	<ul style="list-style-type: none">IP限速：根据IP区分单个Web访问者。用户限速：根据Cookie键值或者Header区分单个Web访问者。其他：根据Referer（自定义请求访问的来源）字段区分单个Web访问者。 <p>说明</p> <p>当“防护模式”选择“其他”时，“Referer”对应的“内容”填写为包含域名的完整URL链接，仅支持前缀匹配和精准匹配的逻辑，“内容”里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。</p> <p>例如：防护路径设置为“/admin”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“内容”设置为“http://www.test.com”。</p>	用户限速

参数	参数说明	取值样例
限速条件	<p>单击“添加”增加新的条件，至少配置一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。</p> <ul style="list-style-type: none"> • 字段：路径、IP、Cookie、Header、Params。 • 子字段：当“字段”选择“Cookie”、“Header”、“Params”时，请根据实际需求配置子字段。 <p>须知 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。</p> <ul style="list-style-type: none"> • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 <p>说明 当“逻辑”关系选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，需要选择引用表，创建引用表的详细操作请参见创建引用表。</p> <ul style="list-style-type: none"> • 内容：输入或者选择条件匹配的内容。 	“路径”包含“/admin/”
用户标识	<p>“限速模式”选择“用户限速”时，需要配置此参数：</p> <ul style="list-style-type: none"> • 选择Cookie时，设置Cookie字段名，即用户需要根据网站实际情况配置唯一可识别Web访问者的Cookie中的某属性变量名。用户标识的Cookie，不支持正则，必须完全匹配。 例如：如果网站使用Cookie中的某个字段name唯一标识用户，那么可以选取name字段来区分Web访问者。 • 选择Header时，设置需要防护的自定义HTTP首部，即用户需要根据网站实际情况配置可识别Web访问者的HTTP首部。 	name
限速频率	<p>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，Web应用防火墙服务将根据配置的“防护动作”来处理。</p>	10次/60秒

参数	参数说明	取值样例
防护动作	<p>当访问的请求频率超过“限速频率”时，可设置以下防护动作：</p> <ul style="list-style-type: none"> ● 人机验证：表示超过“限速频率”后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。 ● 阻断：表示超过“限速频率”将直接阻断。 ● 动态阻断：上一个限速周期内，请求频率超过“限速频率”将被阻断，那么在下一个限速周期内，请求频率超过“放行频率”将被阻断。 ● 仅记录：表示超过“限速频率”将只记录不阻断。可下载防护事件数据查看域名的防护日志。 	阻断
放行频率	<p>当“防护动作”选择“动态阻断”时，可配置放行频率。</p> <p>如果在一个限速周期内，访问超过“限速频率”触发了拦截，那么，在下一个限速周期内，拦截阈值动态调整为“放行频率”。</p> <p>“放行频率”小于等于“限速频率”。</p> <p>说明 当“放行频率”设置为0时，表示如果上一个限速周期发生过拦截后，下一个限速周期所有的请求都不放行。</p>	8次/60秒
阻断时长	当“防护动作”选择“阻断”时，可设置阻断后恢复正常访问页面的时间。	600秒
阻断页面	<p>当“防护动作”选择“阻断”时，需要设置，即当访问超过限速频率时，返回的错误页面。</p> <ul style="list-style-type: none"> ● 当选择“默认设置”时，返回的错误页面为系统默认的阻断页面。 ● 当选择“自定义”，返回错误信息由用户自定义。 	自定义
页面类型	当“阻断页面”选择“自定义”时，可选择阻断页面的类型“application/json”、“text/html”或者“text/xml”。	text/html

参数	参数说明	取值样例
页面内容	当“阻断页面”选择“自定义”时，可设置自定义返回的内容。	不同页面类型对应的页面内容样式： <ul style="list-style-type: none">• text/html: <html><body>Forbidden</body></html>• application/json: {"msg": "Forbidden"}• text/xml: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的CC攻击防护规则展示在CC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CC攻击防护规则时，可单击待修改的CC攻击防护规则所在行的“修改”，修改CC攻击防护规则。
- 若需要删除用户自行添加的CC攻击防护规则时，可单击待删除的CC攻击防护规则所在行的“删除”，删除CC攻击防护规则。

----结束

防护效果

假如已添加域名“www.example.com”，且配置了CC防护规则。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照章节[步骤一：添加防护网站](#)重新完成域名接入。
- 能正常访问，执行2。

步骤2 清理浏览器缓存，在浏览器中访问满足Cookie条件的“http://www.example.com/admin”页面，在60秒内刷新页面10次，正常情况下，在第11次访问该页面时，返回自定义的拦截页面；600秒后刷新目标页面，页面访问正常。

如果您设置了“人机验证”防护动作，当用户访问超过限制后需要输入验证码才能继续访问。

步骤3 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志，您也可以[下载防护事件数据](#)。

----结束

配置示例-人机验证

假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证人机验证防护效果。

步骤1 添加防护动作为“人机验证”CC防护规则。

步骤2 开启CC攻击防护。

步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin/”页面。

当您在60秒内访问页面10次，在第11次访问该页面时，页面弹出验证码。此时，您需要输入验证码才能继续访问。



步骤4 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

8.4 配置精准访问防护规则

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。

精准访问防护规则允许您设置访问防护规则，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仅记录、放行或阻断操作。

前提条件

已添加防护网站。

约束条件

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当精准访问防护规则的“防护动作”设置为“阻断”时，您可以[配置攻击惩罚标准](#)。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据攻击惩罚设置的拦截时长来封禁访问者。

应用场景

精准访问防护支持业务场景定制化的防护策略，可用于盗链防护、网站管理后台保护等场景。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“精准访问防护”配置框中，用户可根据自己的需要更改“状态”，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。

步骤7 在“精准访问防护配置”页面，设置“检测模式”。

精准访问防护规则提供了两种检测模式：

- 短路检测：当用户的请求符合精准防护中的拦截条件时，便立刻终止检测，进行拦截。
- 全检测：当用户的请求符合精准防护中的拦截条件时，不会立即拦截，它会继续执行其他防护的检测，待其他防护的检测完成后进行拦截。

步骤8 在“精准访问防护配置”页面左上角，单击“添加规则”。

步骤9 在弹出的对话框中，根据表8-6添加精准访问防护规则。

须知

如果不确定配置的精准访问防护规则是否会使WAF误拦截正常的访问请求，您可以先将精准访问防护规则的“防护动作”设置为“仅记录”，在“防护事件”页面查看防护事件，确认WAF不会误拦截正常的访问请求后，再将该精准访问防护规则的“防护动作”设置为“阻断”。

例如，当用户访问目标域名下包含“/admin”的URL地址时，WAF将阻断该用户访问目标URL地址。

表 8-6 规则参数说明

参数	参数说明	取值样例
防护动作	可选择“阻断”、“放行”或者“仅记录”。默认为“阻断”。	“阻断”

参数	参数说明	取值样例
攻击惩罚	当“防护动作”设置为“阻断”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。	长时间IP拦截
生效时间	用户可以选择“立即生效”或者自定义设置生效时间段。 自定义设置的时间只能为将来的某一时间段。	“立即生效”
条件列表	<p>单击“添加”增加新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。</p> <p>条件设置参数说明如下：</p> <ul style="list-style-type: none"> • 字段 • 子字段：当字段选择“IP”、“Params”、“Cookie”、“Response Header”或者“Header”时，请根据实际使用需求配置子字段。 <p>须知 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。</p> <ul style="list-style-type: none"> • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 <p>说明</p> <ul style="list-style-type: none"> - 选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，“内容”需要选择引用表名称，创建引用表的详细操作请参见创建引用表。 - “不包含所有”、“不等于所有”、“前缀不为所有”、“后缀不为所有”是指当访问请求中字段不包含、不等于、前/后缀不为引用表中设置的任何一个值时，WAF将进行防护动作（阻断、放行或仅记录）。例如，设置“路径”字段的逻辑为“不包含所有”，选择了“test”引用表，如果“test”引用表中设置的值为test1、test2和test3，则当访问请求的路径不包含test1、test2或test3时，WAF将进行防护动作。 <ul style="list-style-type: none"> • 内容：输入或者选择条件匹配的内容。 <p>说明 具体的配置请参见表8-7。</p>	<ul style="list-style-type: none"> • “路径”包含“/admin/” • “User Agent”前缀不为“mozilla/5.0” • “IP”等于“192.168.2.3” • “Cookie[key1]”前缀不为“jsessionid”

参数	参数说明	取值样例
优先级	<p>设置该条件规则检测的顺序值。如果您设置了多条规则，则多条规则间有先后匹配顺序，即访问请求将根据您设定的精准访问控制规则优先级依次进行匹配，优先级较小的精准访问控制规则优先匹配。</p> <p>您可以通过优先级功能对所有精准访问控制规则进行排序，以获得最优的防护效果。</p>	5
规则描述	可选参数，设置该规则的备注信息。	--

表 8-7 条件列表配置

字段	子字段	逻辑	内容（举例）
路径：设置的防护路径，不包含域名，仅支持精准匹配（需要防护的路径需要与此处填写的路径完全相等。例如，需要防护的路径为“/admin”，该规则必须填写为“/admin”）	--	在“逻辑”下拉列表框中选择逻辑关系。	<i>/buy/phone/</i> 须知 路径设置为“/”时，表示防护网站所有路径。
User Agent：设置为需要防护的扫描器的用户代理。	--		<i>Mozilla/5.0 (Windows NT 6.1)</i>
IP：设置为需要防护的访问者IP地址。	--		XXX.XXX.1.1
Params：设置为需要防护的请求参数。	<ul style="list-style-type: none"> ● 所有字段 ● 任意子字段 ● 自定义 		201901150929

字段	子字段	逻辑	内容（举例）
Referer: 设置为需要防护的自定义请求访问的来源。 例如: 防护路径设置为“/admin/xxx”, 若用户不希望访问者从“www.test.com”访问该页面, 则“Referer”对应的“内容”设置为“http://www.test.com”。	--		http://www.test.com
Cookie: 根据Cookie区分的Web访问者。	<ul style="list-style-type: none"> • 所有字段 • 任意子字段 • 自定义 		jsessionId
Header: 设置为需要防护的自定义HTTP首部。	<ul style="list-style-type: none"> • 所有字段 • 任意子字段 • 自定义 		<i>text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8</i>
Method: 需要防护的自定义请求的方法。	--		GET、POST、PUT、DELETE、PATCH
Request Line: 需要防护的自定义请求行的长度。	--		50
Request: 需要防护的自定义请求的长度。包含请求头、请求行、请求体。	--		--
Protocol: 需要防护的请求的协议。	--		http

步骤10 单击“确认”，添加的精准访问防护规则展示在精准访问防护规则列表中。

- 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”。
- 若需要修改添加的精准访问防护规则时，可单击待修改的精准访问防护规则所在行的“修改”，修改精准访问防护规则。

- 若需要删除添加的精准访问防护规则时，可单击待删除的精准访问防护规则所在行的“删除”，删除精准访问防护规则。

----结束

防护效果

假如已添加域名“www.example.com”，且配置了精准访问防护规则。可参照以下步骤验证防护效果：

- 步骤1** 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。
- 不能正常访问，参照章节[步骤一：添加防护网站](#)重新完成域名接入。
 - 能正常访问，执行**2**。
- 步骤2** 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin”页面或者包含/admin的任意页面，正常情况下，WAF会阻断满足条件的访问请求，返回拦截页面。
- 步骤3** 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志，您也可以[下载防护事件数据](#)。

----结束

配置示例-单独放行指定 IP 的访问

配置两条精准访问防护规则，一条拦截所有的请求和一条单独放行指定IP的访问。

8.5 创建引用表

该章节指导您创建引用表，即可对路径、User Agent、IP、Params、Cookie、Referer、Header这些单一类型的防护指标进行批量配置，引用表能够被CC攻击防护规则和精准访问防护中的规则所引用。

创建的引用表会同步给CC攻击防护规则、精准访问防护规则使用。当配置CC攻击防护规则、精准访问防护规则时，“条件列表”中的“逻辑”关系选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，可在“内容”的下拉框中选择适合的引用表名称。

前提条件

已添加防护网站。

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 > Web应用防火墙”。
- 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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。
- 步骤6** 在“CC攻击防护”或者“精准访问防护”配置框中，单击“自定义CC攻击防护规则”或者“自定义精准访问防护规则”，进入规则配置页面。
- 步骤7** 在列表左上角，单击“引用表管理”。
- 步骤8** 在“引用表管理”界面，单击“添加引用表”。
- 步骤9** 在弹出的“添加引用表”对话框中，添加引用表，参数说明如表8-8所示。

表 8-8 添加引用表参数说明

参数名称	参数说明	取值样例
名称	用户自定义引用表的名字。	test
类型	<ul style="list-style-type: none">• 路径：设置的防护路径，不包含域名。• User Agent：设置为需要防护的扫描器的用户代理。• IP：设置为需要防护的访问者IP地址。• Params：设置为需要防护的请求参数。• Cookie：根据Cookie区分的Web访问者。• Referer：设置为需要防护的自定义请求访问的来源。 例如：防护路径设置为“/admin/xxx”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“值”设置为“http://www.test.com”。• Header：设置为需要防护的自定义HTTP首部。	路径
值	对应“类型”的取值，该值不支持通配符。 说明 可单击“添加”设置多个值。	/buy/phone/

- 步骤10** 单击“确认”，添加的引用表展示在引用表列表。

----结束

相关操作

- 若需要修改创建的引用表，可单击待修改的引用表所在行的“修改”，修改引用表。

- 若需要删除创建的引用表，可单击待删除的引用表所在行的“删除”，删除引用表。

8.6 配置 IP 黑白名单规则

您可以通过配置黑白名单规则，阻断、仅记录或放行指定IP地址/IP地址段的访问请求。配置黑白名单规则时，WAF支持单个添加或通过引用地址组批量导入黑白名单IP地址/IP地址段。

前提条件

已添加防护网站。

约束条件

- WAF不支持批量导入黑白名单，如果您需要配置多个IP/IP地址段规则，请逐条添加黑白名单防护规则，放行或拦截指定IP/IP地址段。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当黑白名单规则的“防护动作”设置为“拦截”时，您可以[配置攻击惩罚标准](#)。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据攻击惩罚设置的拦截时长来封禁访问者。

系统影响

将IP或IP地址段配置为黑名单/白名单后，来自该IP或IP地址段的访问，WAF将不会做任何检测，直接拦截/放行。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“黑白名单设置”配置框中，用户可根据自己的需要更改“状态”，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。

步骤7 在“黑白名单”页面左上角，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，参数说明如[表8-9](#)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。

表 8-9 黑白名单参数说明

参数	参数说明	取值样例
规则名称	用户自定义黑白名单规则的名字。	WAF
IP/IP段或地址组	支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。	IP/IP段
IP/IP段	当“IP/IP段或地址组”选择“IP/IP段”时需要设置该参数。 支持IP地址或IP地址段。 <ul style="list-style-type: none"> IP地址：添加黑名单或者白名单的IP地址。 IP地址段：IP地址与子网掩码。 	XXX.XXX.2.3
选择地址组	当“IP/IP段或地址组”选择“地址组”时需要设置该参数，在下拉列表框中选择已添加的地址组。您也可以单击“添加地址组”创建新的地址组，详细操作请参见 添加黑白名单IP地址组 。	groupwaf
防护动作	<ul style="list-style-type: none"> 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。再根据防护事件数据判断该IP地址或IP地址段是黑名单还是白名单。 	拦截
攻击惩罚	当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。	长时间IP拦截
规则描述	可选参数，设置该规则的备注信息。	--

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

配置示例-放行指定 IP

假如您仅需要放行3个IP，其他的IP全部拦截。

配置方法：利用[精准访问防护规则](#)，配置阻断所有的请求的规则；再将三个IP分别配置为白名单。

防护效果

假如已添加域名“www.example.com”。可参照以下步骤验证防护效果：

步骤1 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

- 不能正常访问，参照章节[步骤一：添加防护网站](#)重新完成域名接入。
- 能正常访问，执行**2**。

步骤2 参照[操作步骤](#)，将您的客户端IP配置为黑名单。

步骤3 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面，正常情况下，WAF会阻断该IP的访问请求，返回拦截页面。

步骤4 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志，您也可以[下载防护事件数据](#)。

----结束

8.7 配置攻击惩罚标准

当访问者的IP、Cookie或Params恶意请求被WAF拦截时，您可以通过配置攻击惩罚，使WAF按配置的攻击惩罚时长来自动封禁访问者。例如，访问者的源IP为恶意请求，如果您配置了IP攻击惩罚拦截时长为500秒，该攻击惩罚生效后，则该IP被WAF拦截时，WAF将封禁该IP，时长为500秒。

配置的攻击惩罚标准规则会同步给Web基础防护规则、精准访问防护规则和IP黑白名单规则使用。当配置Web基础防护规则、精准访问防护规则和IP黑白名单规则时，防护动作为“拦截”或“阻断”时，可使用攻击惩罚标准功能。

前提条件

已添加防护网站。

约束条件

- Web基础防护、精准访问防护和黑白名单设置支持攻击惩罚功能，当攻击惩罚标准配置完成后，您还需要在Web基础防护、精准访问防护或黑白名单规则中选择攻击惩罚，该功能才能生效。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 在配置Cookie或Params恶意请求的攻击惩罚标准前，您需要在域名详情页面设置对应的流量标识。相关操作请参见[配置攻击惩罚的流量标识](#)。

规格限制

- WAF支持设置6种拦截类型，每个拦截类型只能设置一条攻击惩罚标准。
- 最大拦截时长为30分钟。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“攻击惩罚”配置框中，用户可根据自己的需要更改“状态”，单击“自定义攻击惩罚标准”，进入攻击惩罚标准页面。

步骤7 在攻击惩罚标准的列表左上角，单击“添加攻击惩罚”。

步骤8 在弹出的对话框中，添加攻击惩罚标准，参数说明如表8-10所示。

表 8-10 攻击惩罚参数说明

参数	参数说明	取值样例
拦截类型	支持以下拦截方式： <ul style="list-style-type: none">• 长时间IP拦截• 短时间IP拦截• 长时间Cookie拦截• 短时间Cookie拦截• 长时间Params拦截• 短时间Params拦截	长时间IP拦截
拦截时长（秒）	拦截时长需要设置为整数，且设置范围为： <ul style="list-style-type: none">• 300<长时间拦截时长≤1800• 短时间拦截时长≤300	500
规则描述	可选参数，设置该规则的备注信息。	-

步骤9 输入完成后，单击“确认”，添加的攻击惩罚标准展示在列表中。

----结束

相关操作

- 若需要修改添加的攻击惩罚标准，可单击待修改的攻击惩罚标准所在行的“修改”，修改该标准的拦截时长。
- 若需要删除添加的攻击惩罚标准，可单击待删除的攻击惩罚标准所在行的“删除”，删除该标准。

配置示例-Cookie 拦截攻击惩罚

假如防护域名“www.example.com”已接入WAF，访问者IP XXX.XXX.248.195为恶意请求，而您需要对来自该IP地址Cookie标记为jsessionid的访问请求封禁10分钟。您可以参照以下操作步骤验证封禁效果。

- 步骤1** 在“网站设置”页面，单击“www.example.com”，进入域名基本信息页面。
- 步骤2** 配置防护域名的Cookie流量标识，即“Session标记”。
- 步骤3** 添加一条拦截时长为600秒的“长时间Cookie拦截”的攻击惩罚标准。
- 步骤4** 开启攻击惩罚。
- 步骤5** 添加一条黑白名单规则，拦截XXX.XXX.248.195，且“攻击惩罚”选择“长时间Cookie拦截”。
- 步骤6** 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当XXX.XXX.248.195源IP访问页面时，会被WAF拦截。当WAF检测到来自该源IP的Cookie标记为jsessionid访问请求时，WAF将封禁该访问请求，时长为10分钟。

图 8-4 WAF 拦截攻击请求



- 步骤7** 返回Web应用防火墙管理控制台，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，您可以查看该防护事件。

----结束

8.8 配置地理位置访问控制规则

网站接入Web应用防火墙后，您可以设置地理位置访问控制规则，WAF通过识别客户端访问请求的来源区域，一键封禁来自特定区域的访问或者允许特定区域的来源IP的访问，解决部分地区高发的恶意请求问题。可针对指定国家、地区的来源IP自定义访问控制。

前提条件

已添加防护网站。

约束条件

- 同一个地区只能配置到一条地理位置访问控制规则中。
- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“地理位置访问控制”配置框中，用户可根据自己的需要更改“状态”，单击“自定义地理位置访问控制规则”，进入“地理位置访问控制”页面。

步骤7 在“地理位置访问控制”页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，添加地理位置访问控制规则，根据表8-11配置参数。

表 8-11 添加地理位置访问控制规则参数说明

参数	参数说明	取值样例
规则名称	用户自定义地理位置控制规则的名字。	dlfw
规则描述	可选参数，设置该规则的备注信息。	waf
地理位置	IP访问的地理范围。	-
防护动作	可以根据需要选择“拦截”、“放行”或者“仅记录”。	“拦截”

步骤9 单击“确认”，添加的地理位置访问控制规则展示在地理位置访问控制规则列表中。

- 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”。
- 若需要修改添加的地理位置访问控制规则时，可单击待修改的地理位置访问控制规则所在行的“修改”，修改地理位置访问控制规则。
- 若需要删除添加的地理位置访问控制规则时，可单击待删除的地理位置访问控制规则所在行的“删除”，删除地理位置访问控制规则。

----结束

防护效果

假如已添加域名“www.example.com”。可参照以下步骤验证防护效果：

- 步骤1** 清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。
 - 不能正常访问，参照[步骤一：添加防护网站](#)重新完成域名接入。
 - 能正常访问，执行2。
- 步骤2** 参照[操作步骤](#)，将您的客户端IP来源地配置为拦截。
- 步骤3** 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面，正常情况下，WAF会阻断该来源地IP的访问请求，返回拦截页面。
- 步骤4** 返回Web应用防火墙控制界面，在左侧导航树中，单击“防护事件”，进入“防护事件”页面，查看防护域名拦截日志，您也可以[下载防护事件数据](#)。

----结束

8.9 配置网页防篡改规则

网站接入WAF后，您可以通过设置网页防篡改规则，锁定需要保护的网站页面（例如敏感页面）。当被锁定的页面在收到请求时，返回已设置的缓存页面，预防源站页面内容被恶意篡改。

工作原理

- 当WAF接收到正常的访问请求时，直接将缓存的网页返回给Web访问者，加速请求响应。
- 如果攻击者篡改了网站的静态网页，WAF将缓存的未被篡改的网页返回给Web访问者，保证Web访问者访问的是正确的页面。
- WAF将对页面路径下的所有相关资源进行防护。例如，对“www.example.com/index.html”静态页面配置了网页防篡改规则，则WAF将防护“/index.html”的网页以及这个网页关联的相关资源。

即若请求中Referer请求头的值中的URL路径与您配置的防篡改路径一致，如“/index.html”，则该请求命中的资源（结尾为png、jpg、jpeg、gif、bmp、css、js的所有资源）也会同时被缓存下来。

前提条件

已添加防护网站。

约束条件

- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 请确保源站响应中包括Content-Type响应头，否则可能导致WAF无法缓存源站响应。

应用场景

- 加速请求的响应

配置网页防篡改规则后，Web应用防火墙将对服务端的静态网页进行缓存。当Web应用防火墙接收到Web访问者的请求时，直接将缓存的网页返回给Web访问者。

- 网页防篡改

攻击者将服务端的静态网页篡改后，Web应用防火墙将缓存的未被篡改的网页返回给Web访问者，以保证Web访问者访问的是正确的页面。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“网页防篡改”配置框中，用户可根据自己的需要更改“状态”，单击“自定义网页防篡改”，进入网页防篡改规则的配置页面。

步骤7 在“网页防篡改”规则的配置页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，添加网页防篡改规则，参数说明如表8-12所示。

表 8-12 参数说明

参数	参数说明	取值样例
域名	设置防篡改的域名。	www.example.com
路径	设置防篡改的URL链接中的路径（不包含域名）。 URL用来定义网页的地址。基本的URL格式如下： 协议名://域名或IP地址[:端口号]/[路径名/.../文件名]。 例如，URL为“http://www.example.com/admin”，则“路径”设置为“/admin”。 说明 <ul style="list-style-type: none">• 该路径不支持正则。• 路径里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。	/admin
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的网页防篡改规则展示在网页防篡改规则列表中。

----结束

相关操作

- 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”。
- 若被防护页面进行了内容修改，必须单击待更新的网页防篡改规则所在行的“更新缓存”来更新缓存，如果您在页面更新后未更新缓存，WAF将始终返回最近一次缓存的页面内容。
- 若需要删除添加的网页防篡改规则时，可单击待删除的网页防篡改规则所在行的“删除”，删除网页防篡改规则。

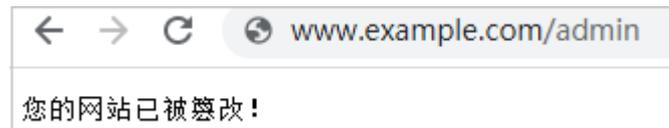
配置示例-静态页面防篡改

假如防护域名“www.example.com”已接入WAF，“/admin”静态页面已被篡改，您可以参照以下操作步骤验证防护效果。

步骤1 在浏览器中访问“http://www.example.com/admin”静态页面。

此时，显示的是被篡改的页面。

图 8-5 静态页面被篡改示例



步骤2 添加一条网页防篡改规则。

步骤3 开启网页防篡改。

步骤4 在浏览器中访问“http://www.example.com/admin”，等待WAF缓存静态页面。

步骤5 在浏览器中访问篡改后的页面。

此时，显示的是被篡改前的页面。

----结束

8.10 配置网站反爬虫防护规则

您可以通过配置网站反爬虫防护规则，防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫。

前提条件

已添加防护网站。

约束条件

- 本功能依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用。

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 如果您的业务接入了CDN服务，请谨慎使用此功能。
由于CDN缓存机制的影响，WAF的网站反爬虫特性将无法达到预期效果，并且有可能造成页面访问异常。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“网站反爬虫”配置框中，用户可根据自己的需要更改网站反爬虫的“状态”，单击“BOT设置”，进入网站反爬虫规则配置页面。

步骤7 选择“特征反爬虫”页签，根据您的业务场景，开启合适的防护功能，检测项说明如 [表8-13](#)所示。

特征反爬虫规则提供了两种防护动作：

- 拦截
发现攻击行为后立即阻断并记录。

注意

开启拦截后，可能会有以下影响：

- 拦截搜索引擎请求，可能影响网站的搜索引擎优化。
- 拦截脚本工具，可能会影响部分APP访问（部分APP的User-Agent未做修改，会匹配脚本工具类爬虫规则）。

- 仅记录
默认防护动作，发现攻击行为后只记录不阻断攻击。

默认开启“扫描器”防护检测，用户可根据业务需要，配置防护动作并开启其他需要防护的检测类型。

表 8-13 特征反爬虫检测项说明

检测项	说明	功能说明
搜索引擎	搜索引擎执行页面内容爬取任务，如Googlebot、Baiduspider。	开启后，WAF将检测并阻断搜索引擎爬虫。 说明 如果不开启“搜索引擎”，WAF针对谷歌和百度爬虫不会拦截。
扫描器	执行漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap。	开启后，WAF将检测并阻断扫描器爬虫。
脚本工具	用于执行自动化任务、程序脚本等，如httpclient、okhttp、python程序等。	开启后，WAF将检测并阻断执行自动化任务、程序脚本等。 说明 如果您的应用程序中使用了httpclient、okhttp、python程序等脚本工具，建议您关闭“脚本工具”，否则，WAF会将使用了httpclient、okhttp、python程序等脚本工具当成恶意爬虫，拦截该应用程序。
其他爬虫	各类用途的爬虫程序，如站点监控、访问代理、网页分析等。 说明 “访问代理”是指当网站接入WAF后，为避免爬虫被WAF拦截，爬虫者使用大量IP代理实现爬虫的一种技术手段。	开启后，WAF将检测并阻断各类用途的爬虫程序。

---结束

8.11 配置防敏感信息泄露规则

您可以添加两种类型的防敏感信息泄露规则：

- 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。

前提条件

已添加防护网站。

约束条件

- 添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“防敏感信息泄露”的配置框中，用户可根据自己的需要更改“状态”，单击“自定义防敏感信息泄露规则”，进入“防敏感信息泄露”规则配置页面。

步骤7 在“防敏感信息泄露”规则配置页面左上角，单击“添加规则”。

步骤8 在弹出的对话框，添加防敏感信息泄露规则，参数说明如表8-14所示。

“防敏感信息泄露”规则既能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，也能够拦截指定的HTTP响应码页面。

敏感信息过滤：针对网站页面中可能存在的电话号码和身份证等敏感信息，配置相应的规则对其进行屏蔽处理。例如，您可以通过设置以下防护规则，屏蔽身份证号、电话号码和电子邮箱敏感信息。

响应码拦截：针对特定的HTTP请求状态码，可配置规则将其拦截，避免服务器敏感信息泄露。例如，您可以通过设置以下防护规则，拦截HTTP 404、502、503状态码。

表 8-14 参数说明

参数名称	参数说明	取值样例
路径	<p>需要过滤敏感信息（例如：身份证号、电话号码、电子邮箱等）或者拦截响应码的URL不包含域名的路径。</p> <ul style="list-style-type: none">前缀匹配：填写的路径前缀与需要防护的路径相同即可。 如果防护路径为“/admin”，该规则填写为“/admin*”，该规则生效。精准匹配：需要防护的路径需要与此处填写的路径完全相等。 如果防护路径为“/admin”，该规则必须填写为“/admin”。 <p>说明</p> <ul style="list-style-type: none">该路径不支持正则，仅支持前缀匹配和精准匹配的逻辑。路径里不能含有多条斜线的配置，如“///admin”，访问时，引擎会将“///”转为“/”。	/admin*

参数名称	参数说明	取值样例
类型	<ul style="list-style-type: none">敏感信息过滤：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：拦截指定的HTTP响应码页面。	敏感信息过滤
内容	防护“类型”对应的防护内容，支持多选。	身份证号码
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的防敏感信息泄露规则展示在防敏感信息泄露规则列表中。

----结束

相关操作

- 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”。
- 当您需要修改添加的防敏感信息泄露规则时，在待修改的防敏感信息泄露规则所在行，单击“修改”，修改防敏感信息泄露规则。
- 当您需要删除添加的防敏感信息泄露规则时，在待删除的防敏感信息泄露规则所在行，单击“删除”，删除防敏感信息泄露规则。

8.12 配置全局白名单（原误报屏蔽）规则

对于误报情况，您可以添加白名单对误报进行忽略，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。

- “不检测模块”选择“所有检测模块”时：通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。
- “不检测模块”选择“Web基础防护模块”时：可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。

前提条件

已添加防护网站。

约束条件

- 仅对WAF预置的Web基础防护规则拦截或记录的攻击事件可以配置误报屏蔽规则。
- 当“不检测模块”配置为“所有检测模块”时，通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。
- 当“不检测模块”配置为“Web基础防护模块”时，仅对WAF预置的Web基础防护规则和网站反爬虫的“特征反爬虫”拦截或记录的攻击事件可以配置全局白名单（原误报屏蔽）规则，防护规则相关说明如下：

- 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。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 您可以通过[处理误报事件](#)来配置全局白名单（原误报屏蔽）规则，处理误报事件后，您可以在全局白名单（原误报屏蔽）规则列表中查看该误报事件对应的全局白名单（原误报屏蔽）规则。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“全局白名单（原误报屏蔽）”配置框中，用户可根据自己的需要更改“状态”，单击“自定义全局白名单规则”，进入规则配置页面。

步骤7 在“全局白名单”规则配置页面左上角，单击“添加规则”。

步骤8 添加全局白名单规则，参数说明如[表8-15](#)所示，

表 8-15 参数说明

参数	参数说明	取值样例
防护方式	<ul style="list-style-type: none"> • “全部域名”：默认防护当前策略下绑定的所有域名。 • “指定域名”：选择策略绑定的防护域名或手动输入泛域名对应的单域名。 	指定域名
防护域名	<p>“防护方式”选择“指定域名”时，需要配置此参数。</p> <p>需要手动输入当前策略下绑定的需要防护的泛域名对应的单域名，且需要输入完整的域名。</p>	www.example.com

参数	参数说明	取值样例
条件列表	<p>单击“添加”增加新的条件，一个防护规则至少包含一项条件，最多可添加30项条件，多个条件同时满足时，本条规则才生效。</p> <p>条件设置参数说明如下：</p> <ul style="list-style-type: none"> • 字段 • 子字段：当字段选择“Params”、“Cookie”或者“Header”时，请根据实际使用需求配置子字段。 <p>须知 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。</p> <ul style="list-style-type: none"> • 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 • 内容：输入或者选择条件匹配的内容。 	“路径”包含“/product”
不检测模块	<ul style="list-style-type: none"> • “所有检测模块”：通过WAF配置的其他所有的规则都不会生效，WAF将放行该域名下的所有请求流量。 • “Web基础防护模块”：选择此参数时，可根据选择的“不检测规则类型”，对某些规则ID或者事件类别进行忽略设置（例如，某URL不进行XSS的检查，可设置屏蔽规则，屏蔽XSS检查）。 	Web基础防护模块
不检测规则类型	<p>“不检测模块”选择“Web基础防护模块”时，您可以选择以下三种方式进行配置：</p> <ul style="list-style-type: none"> • 按ID：按攻击事件的ID进行配置。 • 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 • 所有内置规则：Web基础防护规则里开启的所有防护规则。 	按类别
不检测规则ID	<p>当“不检测规则类型”选择“按ID”时，需要配置此参数。</p> <p>“防护事件”列表中事件类型为非自定义规则的攻击事件所对应的规则编号。单击该攻击事件所在行的“误报处理”获取ID编号。建议您直接参照处理误报事件在防护事件页面配置全局白名单（原误报屏蔽）规则。</p>	041046

参数	参数说明	取值样例
不检测规则类别	当“不检测规则类型”选择“按类别”时，需要配置此参数。 在下拉框中选择事件类别。 WAF支持的防护事件类别有：XSS攻击、网站木马、其他类型攻击、SQL注入攻击、恶意爬虫、远程文件包含、本地文件包含、命令注入攻击。	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	不拦截SQL注入攻击
高级设置	如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，WAF将不再拦截指定字段的攻击事件。 在左边第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。 <ul style="list-style-type: none">当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。当选择“Body”或“Multipart”字段时，可以配置“全部”。当选择“Cookie”字段时，“防护域名”可以为空。 说明 当字段配置为“全部”时，配置完成后，WAF将不再拦截该字段的所有攻击事件。	Params 全部

步骤9 单击“确认添加”。

----结束

相关操作

- 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”。
- 若需要修改添加的全局白名单（原误报屏蔽）规则时，可单击待修改的全局白名单（原误报屏蔽）规则所在行的“修改”，修改全局白名单（原误报屏蔽）规则。
- 若需要删除添加的全局白名单（原误报屏蔽）规则时，可单击待删除的全局白名单（原误报屏蔽）规则所在行的“删除”，删除全局白名单（原误报屏蔽）规则。

8.13 配置隐私屏蔽规则

您可以通过Web应用防火墙服务配置隐私屏蔽规则。隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。

前提条件

已添加防护网站。

约束条件

添加或修改防护规则后，规则生效需要几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。

系统影响

配置隐私屏蔽规则后，防护事件中将屏蔽敏感数据，防止用户隐私泄露。

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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“隐私屏蔽”配置框中，用户可根据自己的需要更改“状态”，单击“自定义隐私屏蔽规则”，进入隐私屏蔽规则配置页面。

步骤7 在“隐私屏蔽”规则配置页面左上角，单击“添加规则”。

步骤8 添加隐私屏蔽规则，根据表8-16配置参数。

表 8-16 添加隐私屏蔽规则参数说明

参数	参数说明	取值样例
路径	<p>完整的URL链接，不包含域名。</p> <ul style="list-style-type: none">前缀匹配：以*结尾代表以该路径为前缀。例如，需要防护的路径为“/admin/test.php”或“/adminabc”，则路径可以填写为“/admin*”。精准匹配：需要防护的路径需要与此处填写的路径完全相等。例如，需要防护的路径为“/admin”，该规则必须填写为“/admin”。 <p>说明</p> <ul style="list-style-type: none">该路径不支持正则，仅支持前缀匹配和精准匹配的逻辑。路径里不能含有连续的多条斜线的配置，如“///admin”，访问时，引擎会将“///”转为“/”。	<p>/admin/login.php</p> <p>例如：需要防护的URL为“http://www.example.com/admin/login.php”，则“路径”设置为“/admin/login.php”。</p>

参数	参数说明	取值样例
屏蔽字段	设置为屏蔽的字段。 <ul style="list-style-type: none"> Params: 请求参数。 Cookie: 根据Cookie区分的Web访问者。 Header: 自定义HTTP首部。 Form: 表单参数。 	<ul style="list-style-type: none"> “屏蔽字段”为“Params”时，屏蔽字段名请根据实际使用需求设置，如果设置为“id”，设置后，与“id”匹配的内容将被屏蔽。
屏蔽字段名	根据“屏蔽字段”设置字段名，被屏蔽的字段将不会出现在日志中。 须知 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。	<ul style="list-style-type: none"> “屏蔽字段”为“Cookie”时，屏蔽字段名请根据实际使用需求设置，如果设置为“name”，设置后，与“name”匹配的内容将被屏蔽。
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的隐私屏蔽规则展示在隐私屏蔽规则列表中。

----结束

相关操作

- 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”。
- 若需要修改添加的隐私屏蔽规则时，可单击待修改的隐私屏蔽规则所在行的“修改”，修改隐私屏蔽规则。
- 若需要删除添加的隐私屏蔽规则时，可单击待删除的隐私屏蔽规则所在行的“删除”，删除隐私屏蔽规则。

9 安全总览

您通过Web应用防火墙服务查看防护日志，可查看到昨天、今天、3天、7天或者30天的访问与攻击统计次数、攻击分布、受攻击域名 TOP10、攻击源IP TOP10和受攻击URL TOP10的次数。

前提条件

- 已添加了防护域名并已完成了域名接入。
- WAF防护已开启。
- 已为防护域名添加了一个或者多个防护规则。

规格限制

在“安全总览”界面，最多可以查看30天的防护数据。

QPS 计算方式

不同时间段的QPS计算方式不同，QPS在各时间段的取值说明如表9-1所示。

表 9-1 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分钟内最大值的最大值
“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小时内最大值的最大值

说明

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。

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 > Web应用防火墙”，进入“安全总览”页面。

步骤4 在页面上方，设置要查询的网站、实例以及查询时间。

- 默认统计的是该账号所有项目下添加到WAF的所有网站的相关数据。
- “域名接入”：统计的是添加到WAF的防护域名的接入信息。单击“查看”跳转到“网站设置”界面，可以查看防护域名详细信息。
- 查询时间：可选择昨天、今天、3天、7天、30天。

步骤5 查看统计的总的请求次数、攻击次数以及各类型攻击的页面总数。

- “请求次数”中统计的次数为网站的PV (Page Views) 值，即用户每次访问网站，在某个时间内被访问的页面总数。
- “攻击次数”中统计的次数为网站被各类型攻击的总次数。
- 各攻击类型统计的次数为用户每次访问网站，在某个时间内被该类型攻击的页面总数。
- 单击“查看网站TOP统计”，可查看请求次数、攻击次数、Web基础防护、精准防护、CC攻击防护、爬虫攻击防护排名TOP 10的数据。

步骤6 “安全统计”模块数据展示。

“按天统计”：勾选后，显示的是间隔一天统计一次的数据；不勾选，统计的数据周期根据选择的时间段而定，具体如下：

- “昨天”、“今天”：间隔两分钟统计一次数据。
- “3天”：间隔5分钟统计一次数据。
- “7天”：间隔10分钟统计一次数据。
- “30天”：间隔1小时统计一次数据。

表 9-2 安全统计参数说明

参数	说明
请求次数	统计的是域名被访问的总请求量、攻击总量以及被各类攻击类型攻击的页面总数。
QPS	域名平均每秒钟的请求量。QPS的取值说明参考 QPS计算方式 。 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。

参数	说明
带宽	域名访问的占用带宽。 发送、接收字节数是通过request_length, upstream_bytes_received按时间进行累加统计, 与EIP上监控的网络带宽值存在差异。此外, 造成两者差异的原因, 还可能跟网页压缩、连接复用、TCP重传等因素相关。
事件分布	查看攻击事件类型。 单击“事件分布”中的任一个区域, 可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。
受攻击域名 Top10	受攻击统计次数Top 10的域名以及各域名受攻击的次数。 单击“查看更多”, 可以跳转到“防护事件”页面, 查看更多防护数据。
攻击源IP Top10	攻击次数Top 10的攻击源IP以及各源IP发起的攻击次数。 单击“查看更多”, 可以跳转到“防护事件”页面, 查看更多防护数据。
受攻击URL Top10	受攻击统计次数Top 10的URL以及各URL受攻击的次数。 单击“查看更多”, 可以跳转到“防护事件”页面, 查看更多防护数据。

----结束

10 管理防护事件

10.1 查看防护日志

Web应用防火墙将拦截或者仅记录攻击事件记录在“防护事件”页面。您可以查看WAF的防护日志，包括事件发生的时间、源IP、源IP所在地理位置、恶意负载、命中规则等信息。

须知

在WAF控制台只能查看所有防护域名最近30天的防护事件数据。

前提条件

防护网站已接入WAF。

约束条件

- 下载防护事件文件时，如果您本地安装的安全软件拦截了下载文件，请关闭该软件后重新下载防护事件文件。
- 在WAF控制台只能查看所有防护域名最近30天的防护事件数据。
- 如果您将防护网站的“工作模式”切换为“暂停防护”模式，WAF将对该防护网站所有的流量请求只转发不检测，同时，日志也不会记录。

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 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。

步骤5 选择“查询”页签，在网站或实例下拉列表中选择待查看的防护网站，可查看“昨天”、“今天”、“3天”、“7天”、“30天”或者自定义时间范围内的防护日志。

- “防护事件趋势图”：展示所选网站在选择的时间段内WAF的防护情况。
- “TOP10统计”：针对当前所选时间段的TOP10网站统计。

步骤6 在“防护事件列表”中，查看防护详情。

- 根据筛选条件字段匹配值进行筛选，可设置多项匹配条件，单击“添加”后，匹配条件会展示在事件列表的上方，确认后单击“查询”，条件字段参数说明如表 10-1所示。
- 在事件列表的右上角，单击，可导出防护事件列表数据，防护事件数据小于200条将直接导出到本地；防护事件数据大于等于200条时，将在“下载”页面生成一条防护事件数据，您可以在下载页面去下载防护事件数据。
- 单击，可选择防护事件列表展示的字段。
- 在目标事件的“操作”列单击“详情”，可查看目标域名攻击事件详情。
- 单击“源IP”旁边的，可根据源站IP的升序或降序对事件列表进行重新排序。

表 10-1 条件字段参数说明

参数名称	参数说明
事件ID	标识该防护事件的ID。
事件类型	发生攻击的类型。 默认选择“全部”，查看所有攻击类型的日志信息，也可以根据需要，选择攻击类型查看攻击日志信息。
规则ID	内置Web基础防护规则ID。
防护动作	防护配置中设置的防护动作，包含：拦截、仅记录、人机验证等。
源IP	Web访问者的公网IP地址（攻击者IP地址）。 默认选择“全部”，查看所有的日志信息，也可以根据需要，选择或者自定义攻击者IP地址查看攻击日志信息。
URL	攻击的防护域名的URL。

表 10-2 防护事件列表参数说明

参数	说明	示例
时间	本次攻击发生的时间。	2021/02/04 13:20:04
源IP	Web访问者的公网IP地址（攻击者IP地址）。	-
防护域名	被攻击的防护域名。	www.example.com
地理位置	攻击者来源IP所在地区。	-
URL	攻击的防护域名的URL。	/admin

参数	说明	示例
事件类型	发生攻击的类型。	SQL注入攻击
防护动作	防护配置中设置的防护动作，包含： 拦截、仅记录、人机验证等。 说明 配置网页防篡改、防敏感信息泄露、隐私屏蔽防护规则后，如果访问请求命中防护规则，则防护动作显示为“不匹配”。	拦截

---结束

10.2 处理误报事件

对于“防护事件”页面中的攻击事件，如果排查后您确认该攻击事件为误报事件，即未发现该攻击事件相关的恶意链接、字符等，您可以通过设置URL和规则ID的忽略（Web基础防护规则）、删除或关闭对应的防护规则（自定义防护规则）、将攻击源IP添加至黑白名单地址组或黑白名单策略中，屏蔽该攻击事件。将攻击事件处理为误报事件后，“防护事件”页面中将不再出现该攻击事件。

当WAF根据内置的Web基础防护规则和自定义防护规则（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）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。

前提条件

事件详情列表中包含误报攻击事件。

约束条件

- 仅基于WAF内置的Web基础防护规则拦截或记录的攻击事件可以进行“误报处理”操作。
- 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。
- 同一个攻击事件不能重复进行误报处理，即如果该攻击事件已进行了误报处理，则不能再对该攻击事件进行误报处理。
- 拦截事件处理为误报后，“防护事件”页面中将不再出现该事件。

使用场景

业务正常请求被WAF拦截。例如，您在ECS服务器上部署了一个Web应用，将该Web应用对应的公网域名接入WAF并开启Web基础防护后，该域名的请求流量命中了Web基础防护规则被WAF误拦截，导致通过域名访问网站显示异常，但直接通过IP访问网站正常。

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 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。

步骤5 选择“查询”页签，在网站或实例下拉列表中选择待查看的防护网站，可查看“昨天”、“今天”、“3天”、“7天”、“30天”或者自定义时间范围内的防护日志。

步骤6 在“防护事件列表”中，根据实际情况对防护事件进行处理。

- 确认事件为误报，在目标防护事件所在行的“操作”列，单击“事件处理 > 误报处理”，添加误报处理策略。
- 将源IP添加到地址组。在目标防护事件所在行的“操作”列，单击“事件处理 > 添加到地址组”，添加成功后将根据该地址组所应用的防护策略进行拦截或放行。
“添加方式”可选择已有地址组或者新建地址组。
- 将源IP添加至对应防护域名下的黑白名单策略。在目标防护事件所在行的“操作”列，单击“事件处理 > 添加至黑白名单”，添加成功后该策略将始终对添加的攻击源IP进行拦截或放行。

表 10-3 参数说明

参数	参数说明
添加方式	- 选择已有规则 - 新建规则
规则名称	- 添加方式选择“选择已有规则”时，在下拉框中选择规则名称。 - 添加方式选择“新建规则”时，自定义黑白名单规则的名字。
IP/IP段或地址组	添加方式选择“新建规则”时，需要配置此参数。支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。
地址组名称	“IP/IP段或地址组”选择“地址组”时，需要配置此参数。 在下拉列表框中选择已添加的地址组。您也可以单击“添加地址组”创建新的地址组，详细操作请参见 添加黑白名单IP地址组 。

参数	参数说明
防护动作	<ul style="list-style-type: none">- 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。- 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。- 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。
攻击惩罚	当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。
规则描述	可选参数，设置该规则的备注信息。

----结束

生效条件

设置误报处理后，1分钟左右生效，攻击事件详情列表中将不再出现此误报。您可以刷新浏览器缓存，重新访问设置了全局白名单（原误报屏蔽）规则的页面，验证是否配置成功。

相关操作

拦截事件处理为误报后，该误报事件对应的规则将添加到全局白名单（原误报屏蔽）规则列表中，您可以在“防护策略”界面的全局白名单（原误报屏蔽）页面查看、关闭、删除或修改该规则。有关配置全局白名单（原误报屏蔽）规则的详细操作，请参见[配置全局白名单（原误报屏蔽）规则](#)。

10.3 下载防护事件数据

该章节指导您通过Web应用防火墙服务下载仅记录和拦截的攻击事件数据，可下载5天内的全量防护事件数据，当天的防护事件数据，在次日凌晨生成到防护事件数据csv文件。

前提条件

- 已添加防护网站。
- 已生成了防护事件数据文件。

规格限制

- 单个文件的事件总数量最大值为5000，超过5000就会生成另一个文件。
- 在WAF控制台只能下载5天内的全量防护事件数据。

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 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。

步骤5 选择“下载”页签，下载防护数据文件，参数说明如表10-4。

表 10-4 防护数据参数说明

参数名称	参数说明
文件名称	样式为文件名称.csv。
事件数量	被拦截和仅记录的事件总数量。 说明 单个文件的事件总数量最大值为5,000，超过5,000就会生成另一个文件。

步骤6 在目标时间段所在行的“操作”列，单击“下载数据”，下载到本地。

----结束

防护数据文件字段参数说明

字段	字段说明	示例
action	防护事件的防护动作。	block
attack	攻击的类型。	SQL Injection
body	攻击者的请求实体内容。	-
cookie	攻击者的Cookie。	-
headers	攻击者的消息头。	-
host	防护的网站域名或IP。	www.example.com
id	标识防护事件的ID。	02-11-16-20201121060347-feb42002
payload	攻击者对防护网站造成伤害的组成部分。	python-requests/2.20.1
payload_location	攻击者对防护网站造成伤害的位置或访问URL的次数。	user-agent
policyid	标识防护策略ID。	d5580c8f6cd4403ebbf85892d4bb8e4
request_line	攻击者的请求行。	GET /
rule	防护事件对应的规则编号。	81066

字段	字段说明	示例
sip	Web访问者的公网IP地址（攻击者IP地址）。	-
time	防护事件发生的时间。	2020/11/21 0:20:44
url	防护域名的URL。	/

11 开启告警通知

通过对攻击日志进行通知设置，WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户。

同时，您也可以配置证书到期通知，证书即将到期时，WAF将通过用户设置的接收通知方式（例如邮件或短信）通知用户。

📖 说明

- 在设置告警通知前，建议您先在“消息通知服务”中创建“消息主题”。

前提条件

已开通消息通知服务。

约束条件

在设置时间间隔内，当攻击次数大于或等于您设置的阈值时才会发送告警通知。

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 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“系统管理 > 告警通知”，进入“告警通知”页面。

步骤5 单击“添加通知”，配置告警通知参数，参数说明如[表11-1](#)。

表 11-1 通知设置参数说明

参数	参数说明
通知类型	选择告警通知的类型： <ul style="list-style-type: none">防护事件：WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户。证书到期：证书即将到期时，WAF将通过用户设置的接收通知方式（例如邮件或短信）通知用户。
通知名称	自定义该条告警的名称。
通知描述	可选参数，备注该条告警的用途。
通知群组	单击下拉列表选择已创建的主题或者单击“查看主题”创建新的主题，用于配置接收告警通知的终端。更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。
告警频率	“通知类型”选择“防护事件”时，需要设置告警频率。 说明 在设置时间间隔内，当攻击次数大于或等于您设置的阈值时才会发送告警通知。
事件类型	“通知类型”选择“防护事件”时，需要配置此参数。 设置告警的事件类型，系统默认选择“全部”，用户也可以单击“自定义”，勾选需要告警的事件类型。
到期提前通知	“通知类型”选择“证书到期”时，需要配置此参数。 在下拉框中选择证书到期提前通知的时间，可选择“1周”、“1个月”、“2个月”。 例如：选择“1周”，那么证书到期前1周时，WAF将以短信或邮件的方式通知您更换证书。
提前通知频率	“通知类型”选择“证书到期”时，需要配置此参数。 在下拉框中选择证书到期提前通知的频率，可配置为“每周”或“每天”。

步骤6 配置完成后，单击“确认”，告警通知设置成功。

- 如果需要关闭该告警通知，在目标告警所在行的“操作”列，单击“关闭”。
- 如果需要删除该告警通知，在目标告警所在行的“操作”列，单击“删除”。
- 如果需要修改该告警通知，在目标告警所在行的“操作”列，单击“修改”。

---结束

12 策略管理

12.1 新增防护策略

防护策略是多种防护规则的合集，用于配置和管理Web基础防护、黑白名单、精准访问防护等防护规则，一条防护策略可以适用于多个防护域名，但一个防护域名只能绑定一个防护策略。该任务指导您通过Web应用防火墙添加防护策略。

前提条件

已添加防护网站。

约束条件

一个防护域名只能绑定一条防护策略。

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 > Web应用防火墙”。

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 在列表的左上角，单击“添加防护策略”。

步骤6 在弹出的对话框中，输入策略名称，单击“确认”，添加的策略会展示在策略列表中。

步骤7 在目标策略所在行，单击策略名称，进入防护规则配置页面，参见[配置防护规则](#)为策略添加防护规则。

----结束

相关操作

- 若想修改策略名称，单击目标策略名称后的 ，在弹出的对话框中，重新输入新的策略名称即可。
- 若想删除添加的防护策略，在目标策略所在行的“操作”列，单击“删除”。

12.2 批量添加防护规则

您可以通过Web应用防火墙服务为防护策略批量添加防护规则。

前提条件

已添加防护网站。

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 > Web应用防火墙”。

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 在页面左上角，单击“所有策略规则”。

步骤6 在待配置规则列表的左上角，单击“批量添加”，进入对应的规则配置页面。

步骤7 选择策略名称，在“策略名称”的下拉框中选择策略名，可批量多选。

步骤8 完成除“策略名称”以外其它参数的配置。

- “CC攻击防护”请参见[表8-5](#)进行参数配置。
- “精准访问防护”请参见[表8-6](#)进行参数配置。
- “黑白名单设置”请参见[表8-9](#)进行参数配置。
- “地理位置访问控制”请参见[表8-11](#)进行参数配置。
- “网页防篡改”请参见[表8-12](#)进行参数配置。
- “防敏感信息泄露”请参见[表8-14](#)进行参数配置。
- “全局白名单”请参见[表8-15](#)进行参数配置。
- “隐私屏蔽”请参见[表8-16](#)进行参数配置。

步骤9 单击“确认”，批量添加防护规则成功。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该策略生效，可在目标策略所在行的“操作”列，单击“关闭”，也可以批量勾选多条策略规则，单击列表上方的“批量关闭”，同时关闭多条策略规则。

- 当您需要修改添加的规则时，在待修改的规则所在行，单击“修改”，修改规则，也可以批量勾选不同策略下的多条规则，单击列表上方的“批量修改”，同时修改多条策略规则。
- 当您需要删除添加的规则时，在待删除的规则所在行，单击“删除”，删除规则，也可以批量勾选多条策略规则，单击列表上方的“批量删除”，同时删除多条策略规则。

12.3 添加策略适用的防护域名

您可以通过Web应用防火墙服务添加策略适用的防护域名。

前提条件

已添加防护网站。

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 > Web应用防火墙”。

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 在目标策略名称所在行的“操作”列，单击“添加防护域名”。

步骤6 在“防护域名”下拉框中选择适用于该策略的防护域名。

须知

- 一个防护域名有且只能配置一条防护策略。
- 一条防护策略可以适用于多个防护域名。
- 若想删除已绑定域名的防护策略，请先将此防护策略绑定的所有域名添加到其它防护策略，再在目标策略名称所在行的“操作”列中，单击“删除”。

步骤7 单击“确认”。

----结束

13 管理独享引擎

创建WAF独享引擎实例后，您可以查看实例信息、升级实例版本以及删除实例。

前提条件

- 已申请独享引擎实例。
- 登录账号已授予“IAM ReadOnly”权限。

查看独享引擎实例信息

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”。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

步骤5 查看独享引擎实例信息，如表13-1所示。

表 13-1 独享引擎实例信息说明

参数	说明	示例
实例名	创建实例时自动生成的名称。	-
防护网站	实例当前防护的网站。	www.example.com
VPC	实例所在的VPC。	vpc-waf
子网	实例所在的子网。	subnet-62bb
IP地址	实例所在业务VPC的子网IP地址。	192.168.0.186
接入状态	实例的接入状态。	已接入
运行状态	实例的运行状态。	运行中
模式	实例的部署模式。	标准模式(反向代理)

参数	说明	示例
规格	实例的资源规格。	8vCPUs 16GB

----结束

升级独享引擎实例版本

当实例的“运行状态”为“运行中”时，您可以通过升级操作，将WAF独享引擎实例升级到最新版本。

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”。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

步骤5 在目标实例所在行的“操作”列，单击“升级”。

步骤6 在弹出的对话框中，确认并勾选业务满足后对话框所描述的条件后，单击“确认”，升级实例版本。

单击“查看版本详情”，可查看独享引擎版本迭代详情。

----结束

删除独享引擎实例

当您不需要使用独享引擎实例时，您可以删除实例，删除实例时WAF将停止防护。

须知

删除实例后，该实例上的资源将被释放且不可恢复，请谨慎操作。

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”。

步骤4 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

步骤5 在目标实例所在行的“操作”列，单击“删除”。

步骤6 在弹出的对话框中，单击“确认”。

----结束

14 查看产品信息

您可以在产品信息界面查看WAF产品信息，包括申请的WAF版本、域名规格等信息。

前提条件

已申请Web应用防火墙实例。

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 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“系统管理 > 产品信息”，进入“产品信息”页面。

步骤5 在“产品信息”界面，查看WAF版本、产品规格、到期时间等信息。

- 单击“规格详情”，可以查看当前WAF版本的详细规格信息。

----结束

15 权限管理

15.1 WAF 自定义策略

如果系统预置的WAF权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见[WAF权限及授权项](#)。

目前支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

WAF 自定义策略样例

- 示例1：授权用户查询防护域名列表

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:instance:list"
      ]
    }
  ]
}
```

- 示例2：拒绝用户删除网页防篡改规则

拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

如果您给用户授予“WAF FullAccess”的系统策略，但不希望用户拥有“WAF FullAccess”中定义的删除网页防篡改规则的权限

（waf:antiTamperRule:delete），您可以创建一条相同Action的自定义策略，并将自定义策略的Effect设置为“Deny”，然后同时将“WAF FullAccess”和拒绝策略授予用户，根据Deny优先原则用户可以对WAF执行除了删除网页防篡改规则的所有操作。以下策略样例表示：拒绝用户删除网页防篡改规则。

```
{
  "Version": "1.1",
  "Statement": [
```

```
{
  "Effect": "Deny",
  "Action": [
    "waf:antiTamperRule:delete"
  ]
},
]
```

- 多个授权项策略

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务。多个授权语句策略描述如下：

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:instance:get",
        "waf:certificate:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:switchVersion",
        "hss:hosts:manualDetect",
        "hss:manualDetectStatus:get"
      ]
    }
  ]
}
```

15.2 WAF 权限及授权项

如果您需要对您所拥有的WAF进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management, IAM），如果登录账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用WAF服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为角色和策略。角色以服务为粒度，是IAM最初提供了一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

权限	授权项
查询防敏感信息泄漏规则	waf:antiLeakageRule:get
查询网页防篡改规则	waf:antiTamperRule:get
查询CC攻击防护规则	waf:ccRule:get
查询精准访问防护规则	waf:preciseProtectionRule:get
查询全局白名单（原误报屏蔽）规则	waf:falseAlarmMaskRule:get
查询隐私屏蔽规则	waf:privacyRule:get
查询黑白名单规则	waf:whiteBlackIpRule:get
查询地址位置访问控制规则	waf:geoIpRule:get
查询证书	waf:certificate:get
修改WAF证书	waf:certificate:put
查询防护事件	waf:event:get
查询防护域名	waf:instance:get
查询防护策略	waf:policy:get
查询用户套餐信息	waf:bundle:get
查询防护事件下载链接	waf:dumpEventLink:get
查询页面配置信息	waf:consoleConfig:get
查询回源IP段	waf:sourceIp:get
更新防敏感信息泄漏规则	waf:antiLeakageRule:put
更新网页防篡改规则	waf:antiTamperRule:put
更新CC攻击防护规则	waf:ccRuleRule:put
更新精准访问防护规则	waf:preciseProtectionRule:put
更新全局白名单（原误报屏蔽）规则	waf:falseAlarmMaskRule:put
更新隐私屏蔽规则	waf:privacyRule:put
更新黑白名单规则	waf:whiteBlackIpRule:put
更新地址位置访问控制规则	waf:geoIpRule:put
更新防护域名	waf:instance:put
更新防护策略	waf:policy:put
删除防敏感信息泄漏规则	waf:antiLeakageRule:delete
删除网页防篡改规则	waf:antiTamperRule:delete

权限	授权项
删除CC攻击防护规则	waf:ccRule:delete
删除精准访问防护规则	waf:preciseProtectionRule:delete
删除全局白名单（原误报屏蔽）规则	waf:falseAlarmMaskRule:delete
删除隐私屏蔽规则	waf:privacyRule:delete
删除黑白名单规则	waf:whiteBlackIpRule:delete
删除地址位置访问控制规则	waf:geolpRule:delete
删除防护域名	waf:instance:delete
删除防护策略	waf:policy:delete
创建防敏感信息泄漏规则	waf:antiLeakageRule:create
创建网页防篡改规则	waf:antiTamperRule:create
创建CC攻击防护规则	waf:ccRule:create
创建精准访问防护规则	waf:preciseProtectionRule:create
创建全局白名单（原误报屏蔽）规则	waf:falseAlarmMaskRule:create
创建隐私屏蔽规则	waf:privacyRule:create
创建黑白名单规则	waf:whiteBlackIpRule:create
创建地址位置访问控制规则	waf:geolpRule:create
创建证书	waf:certificate:create
创建防护域名	waf:instance:create
创建防护策略	waf:policy:create
查询防敏感信息泄漏规则列表	waf:antiLeakageRule:list
查询网页防篡改规则列表	waf:antiTamperRule:list
查询CC攻击防护规则列表	waf:ccRuleRule:list
查询精准访问防护规则列表	waf:preciseProtectionRule:list
查询全局白名单（原误报屏蔽）规则列表	waf:falseAlarmMaskRule:list
查询隐私屏蔽规则列表	waf:privacyRule:list
查询黑白名单规则列表	waf:whiteBlackIpRule:list
查询地址位置访问控制规则列表	waf:geolpRule:list
查询防护域名列表	waf:instance:list

权限	授权项
查询防护策略列表	waf:policy:list
查询独享引擎实例列表	waf:premiumInstance:list
查询独享引擎	waf:premiumInstance:get
创建独享引擎实例	waf:premiumInstance:create
删除独享引擎实例	waf:premiumInstance:delete
更新独享引擎	waf:premiumInstance:put

16 常见问题

16.1 产品咨询

16.1.1 功能说明类

16.1.1.1 Web 应用防火墙是否能防护 IP?

WAF可以对IP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？](#)。

16.1.1.2 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。

16.1.1.3 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。

16.1.1.4 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。

16.1.1.5 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。

16.1.1.6 Web 应用防火墙攻击防护类问题

什么是防护 IP？

防护IP是指需要保护的网站的IP地址。

Web 应用防火墙支持漏洞检测吗？

WAF的Web基础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Web基础防护规则时，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。

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。

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。

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。

16.1.1.7 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。

16.1.1.8 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。

16.1.1.9 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。

16.1.1.10 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。

16.1.1.11 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。

16.1.1.12 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。

16.1.1.13 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。

16.1.1.14 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）。

16.1.1.15 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。

16.1.1.16 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。

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。

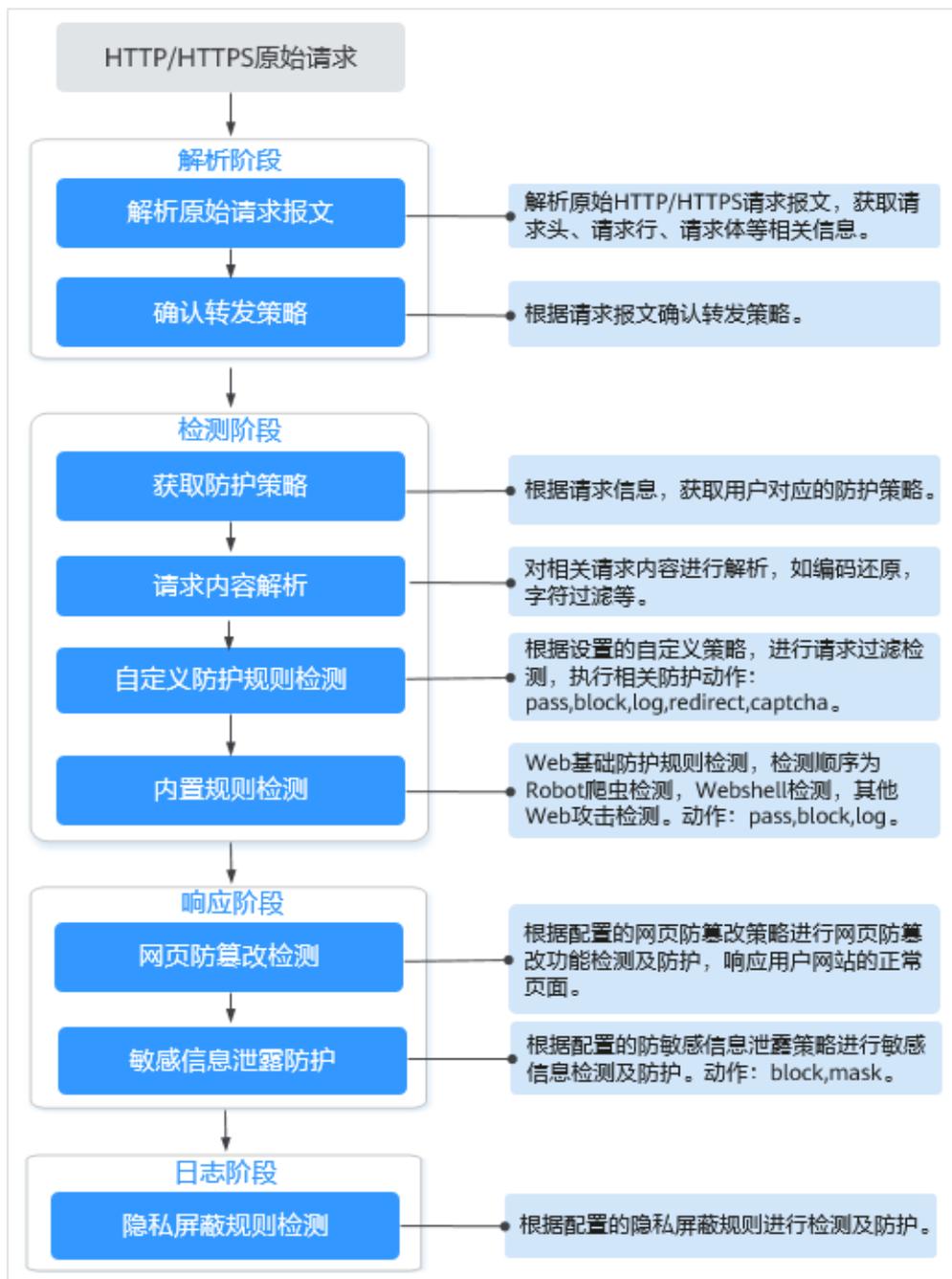
Cookie由一个名称（Name）、一个值（Value）和其它几个用于控制Cookie有效期、安全性、使用范围的可选属性组成。Cookie分为会话Cookie和持久性Cookie两种类型，详细说明如下：

- 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。

16.1.1.17 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16-1](#)所示。

图 16-1 WAF 引擎检测图



16.1.1.18 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。

16.1.1.19 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。

16.1.1.20 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

16.1.1.21 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。

16.1.1.22 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 16-2 网站接入 WAF 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 16-3 Nginx 转发原理



16.1.1.23 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。

16.1.1.24 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。

16.1.1.25 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，造成源站业务带宽上升。

16.1.1.26 WAF 对 SQL 注入、XSS 跨站脚本攻击的检测原理？

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。

16.1.1.27 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）。

16.1.1.28 独享版 WAF 是否支持跨 VPC 防护？

WAF独享引擎不支持跨VPC防护的场景。如果WAF独享引擎实例与源站在同一个VPC中，建议您重新申请与源站在同一VPC下的WAF独享引擎实例进行防护。

16.1.2 使用说明类

16.1.2.1 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

16.1.2.2 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。

16.1.2.3 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。

16.1.2.4 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。

16.1.2.5 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。

16.1.2.6 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16-1](#)所示。

表 16-1 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

16.1.2.7 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。

16.1.2.8 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。

16.1.2.9 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）。

16.1.2.10 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。

16.1.2.11 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。

16.1.2.12 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。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。

16.1.2.13 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。

16.1.2.14 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。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至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。

16.1.2.15 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的域名/IP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。

16.2 网站接入配置

16.2.1 域名/端口类

16.2.1.1 域名/IP 如何接入 Web 应用防火墙？

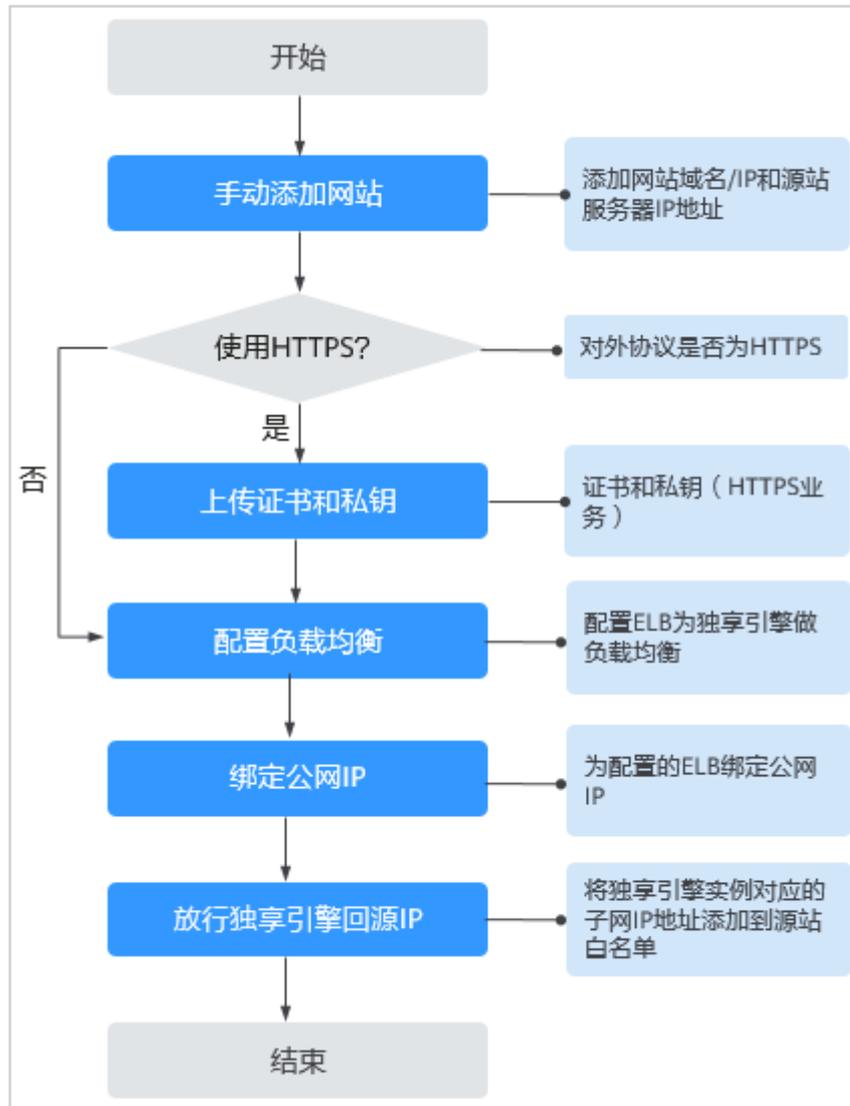
域名或IP接入WAF后，WAF作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

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。

网站接入WAF各模式的流程如下图所示。

图 16-4 网站接入 WAF 的操作流程图-独享模式



- 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。

16.2.1.2 Web 应用防火墙支持哪些非标准端口？

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

WAF 支持的端口

Web应用防火墙可防护的端口如[表16-2](#)所示。

表 16-2 WAF 支持的端口

端口分类	HTTP协议	HTTPS协议	端口防护限制数
标准端口	80	443	不限制
非标准端口 (182个)	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	不限制

16.2.1.3 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。

16.2.1.4 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。

16.2.1.5 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”下拉列表中选择非标准端口。

16.2.1.6 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。

16.2.1.7 域名/IP 接入 WAF 前需要准备哪些数据？

请根据申请的WAF模式，在域名/IP接入WAF前收集相关信息。

接入WAF前需要准备以下数据：

- 域名/IP
- 端口：需要防护的域名对应的业务端口，WAF支持防护非标准端口。
- 服务器信息：
 - 对外协议：客户端请求访问服务器的协议类型。
 - 源站协议：WAF转发客户端请求到服务器的协议类型。
 - 源站地址：客户端访问的网站服务器的IP地址或域名。
 - 源站端口：WAF转发客户端请求到服务器的业务端口。
- 证书：如果“对外协议”使用HTTPS，则需要为该域名绑定证书。

16.2.1.8 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：

- 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。

16.2.1.9 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。

16.2.1.10 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。

16.2.1.11 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。

16.2.1.12 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。

16.2.1.13 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。

16.2.2 证书管理

16.2.2.1 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。

16.2.2.2 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。

16.2.2.3 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16-3在本地将证书转换为PEM格式，再上传。

表 16-3 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”。
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

格式类型	转换方式
P7B	<ol style="list-style-type: none">证书转换，以“cert.p7b”转换为“cert.cer”为例。 <code>openssl pkcs7 -print_certs -in cert.p7b -out cert.cer</code>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。 <code>openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem</code>提取证书命令，以“cert.der”转换为“cert.pem”为例。 <code>openssl x509 -inform der -in cert.der -out cert.pem</code>

📖 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。

16.3 业务中断排查

16.3.1 如何排查 404/502/504 错误?

域名接入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

现象一：访问网站时，返回如图16-5所示的页面。

图 16-5 404 页面



原因：访问地址增加的端口错误。

- 添加防护域名到WAF时，配置了非标准端口，访问网站时未加端口或使用源站端口，而不是非标准端口，用“https://www.example.com”或者“https://www.example.com:80”访问网站。

解决办法：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”。

- 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，用“https://www.example.com:8080”访问网站。

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。

解决办法：直接访问网站域名，如“https://www.example.com”。

现象二：访问网站时，返回的不是图16-5所示的页面，而是其他的404页面。

原因：网站页面不存在或已删除。

解决办法：请排查网站问题。

502 Bad Gateway

现象：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。

说明

如果您的网站不是部署在云上，建议您咨询服务器服务商，该服务器是否存在默认的防护拦截并要求服务商解除默认拦截。

这种情况一般有三种原因：

- **原因一：**您的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，导致不能正常访问。

解决办法：将WAF的回源IP网段添加到防火墙（硬件或软件）、安全防护软件、业务限速模块的白名单中。

- **原因二：**网站的后端配置了多个服务器，其中某个源站不通。

按以下方法检测源站配置是否正确：

- a. 登录管理控制台，单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，进入Web应用防火墙控制界面。
- b. 在左侧导航树中选择“网站设置”，进入“网站设置”页面。
- c. 在目标域名所在行的“防护网站”列中，单击目标域名，进入域名基本信息页面。
- d. 在“服务器信息”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。
- e. 在主机上执行curl命令检测各个源站是否能正常访问。

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

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。

📖 说明

- 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。
- 您也可以在浏览器中输入“http://源站地址:源站端口”检测源站是否能正常访问。

如果显示“connection refused”表示源站不通，不能正常访问网站。按以下方法处理：

- 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。
- 将WAF的回源IP网段添加到防火墙（硬件或软件）、安全防护软件、业务限速模块的白名单中。
- **原因三：源站性能问题。**
解决办法：排查网站问题并联系您的网站负责人进行解决。

504 Gateway Timeout

现象：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的返回码。

可能有以下几个原因：

- **原因一：后端服务器性能问题（连接数，CPU内存占用过大等）。**
解决办法：
 - a. 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。
 - b. 为了支撑业务量的大量增长，可按照**方法一**或者**方法二**进行处理。
方法一：在ELB上增加后端服务器组。
方法二：创建新的ELB，并参照以下方法将ELB的EIP作为服务器的IP地址，接入WAF。
 - i. 登录管理控制台，单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，进入Web应用防火墙控制界面。
 - ii. 在左侧导航树中选择“网站设置”，进入“网站设置”页面。
 - iii. 在目标域名所在行的“防护网站”列中，单击目标域名，进入域名基本信息页面。
 - iv. 在“服务器信息”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。
 - c. 如果客户端协议即“对外协议”是HTTPS协议，可考虑在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。
- **原因二：安全组未将WAF回源IP设置为白名单或未放开口。**
解决办法：将WAF的回源IP在网站所在的ECS的安全组里设置为白名单。
- **原因三：源站有防火墙设备，且该防火墙设备拦截了WAF的回源IP。**

解决办法：将WAF的回源IP在网站所在的ECS的安全组里设置为白名单或者卸载除WAF以外其他防火墙软件。

- **原因四：**连接超时、read超时。

解决办法：

- 数据库查询时间过长：

- 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：

- 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。

- **原因五：**源站超带宽。

解决办法：扩展源站服务器带宽。

16.3.2 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”未显示“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。

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16-6](#)和[表16-4](#)进行排查处理。

图 16-6 独享模式排查思路



表 16-4 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	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。 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。

16.3.3 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。

当某种业务频繁误报时，可以在事件日志中，进行误报处理。通过设置URL和规则ID的忽略，以后该URL再次被攻击时，WAF不再阻断。

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16-5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 16-5 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。

16.3.4 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。

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，请参见[配置精准访问防护规则](#)放行该访问请求。

16.3.5 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60秒，该值可以在WAF界面手动设置。

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。

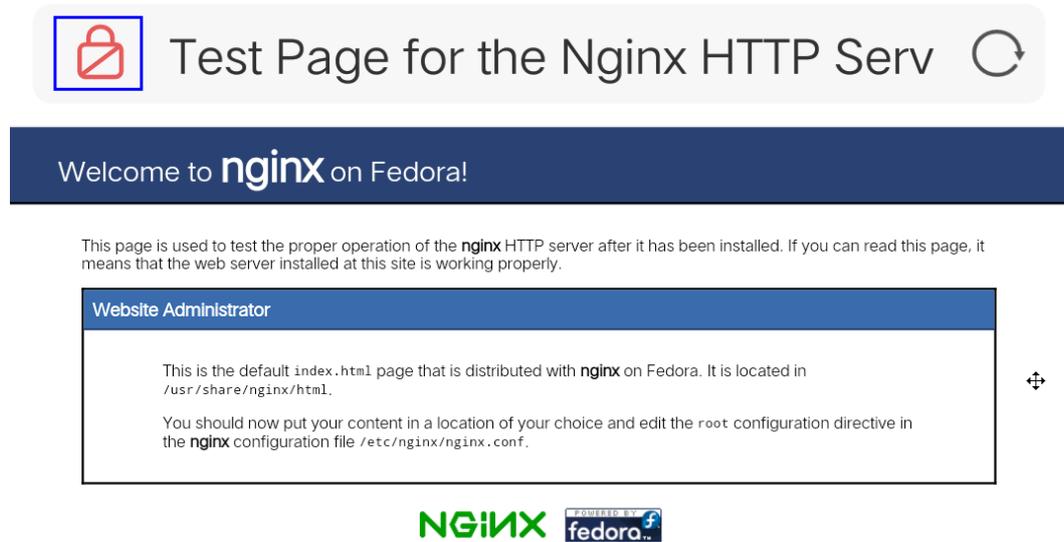
16.3.6 如何解决重定向次数过多？

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。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。

16.3.7 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，如果出现类似如[图16-7](#)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 16-7 访问异常



16.3.8 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：

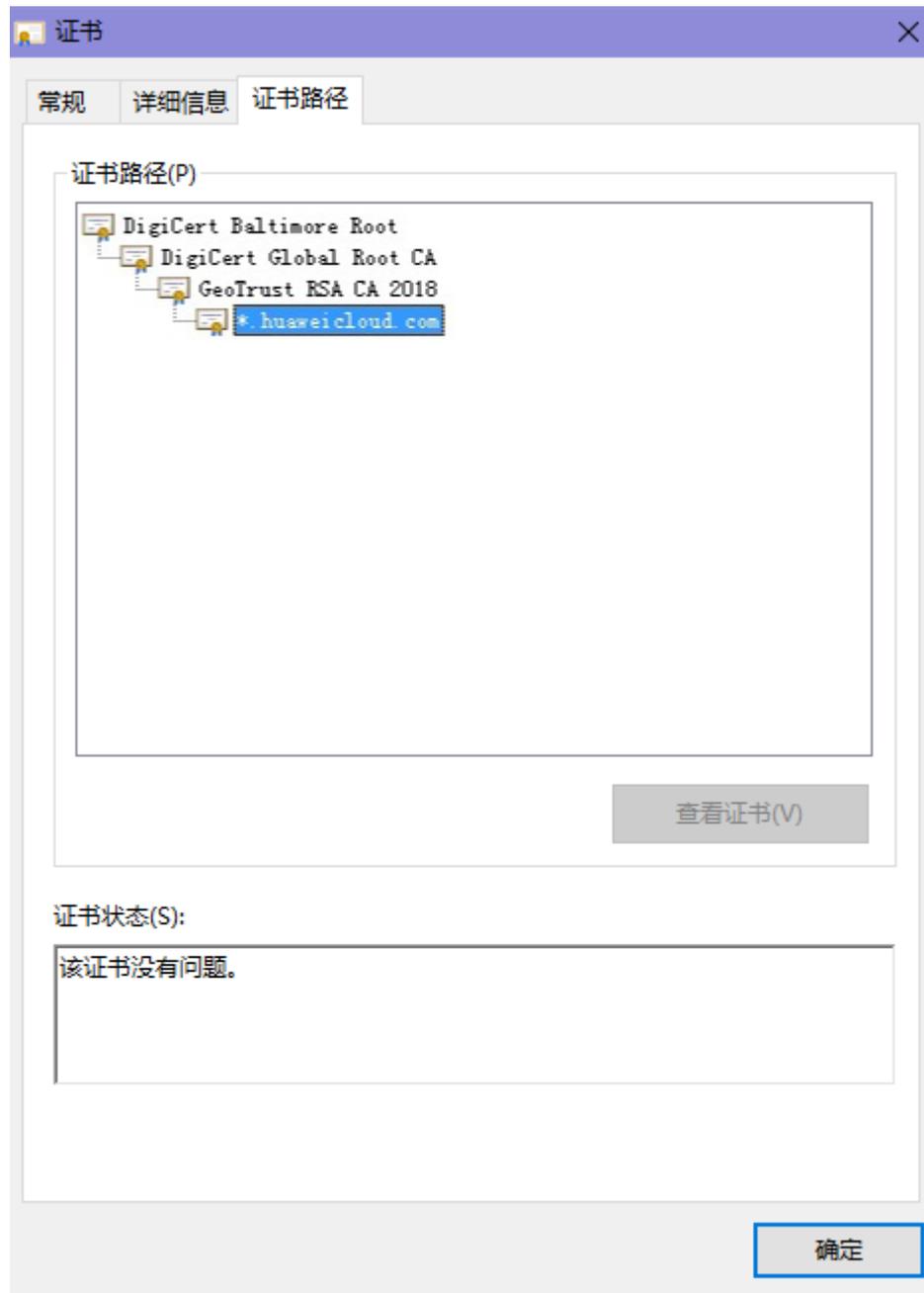
- 手动构造完整证书链，并上传证书。（WAF自动补全证书链功能正在开发中，敬请期待！）
- 重新上传正确的证书。

Chrome最新版本一般是支持自动验证信任链，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。

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16-8所示。

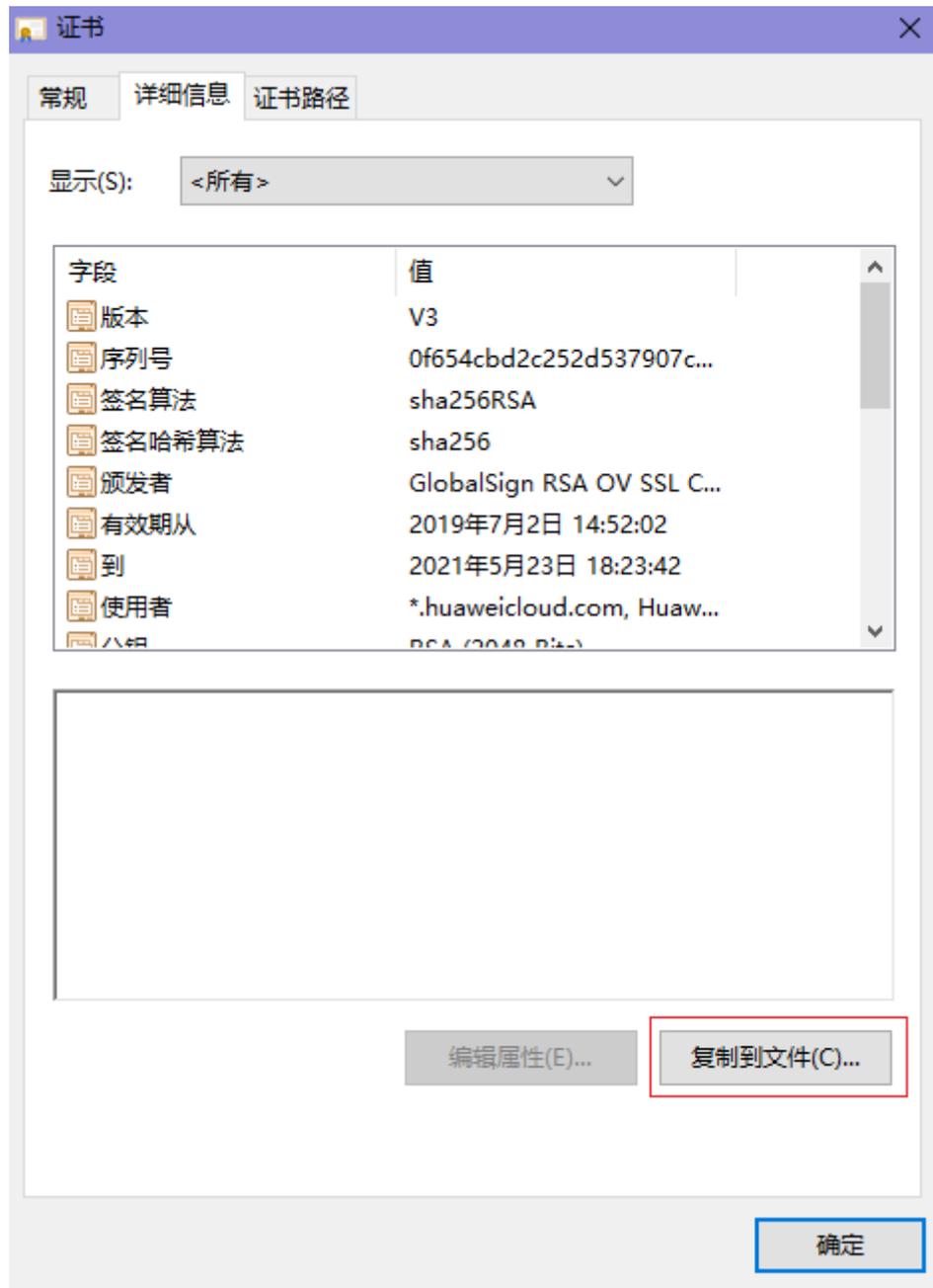
图 16-8 查看证书链



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16-9所示。

图 16-9 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16-10所示。

图 16-10 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16-11重组证书顺序，完成证书重构。

图 16-11 证书重构

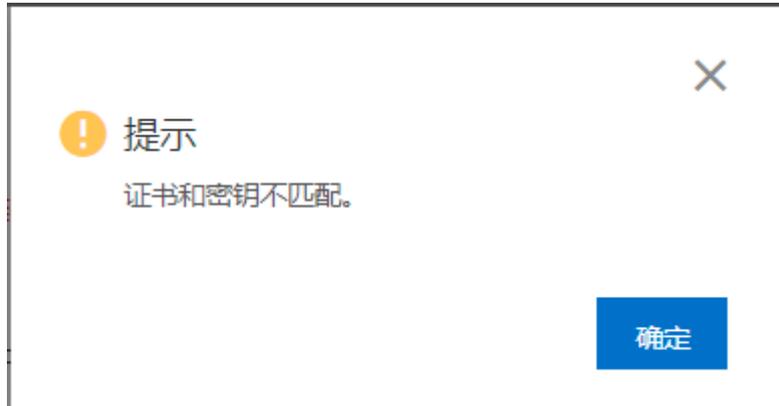


步骤5 重新上传证书。

----结束

16.3.9 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： <code>openssl x509 -noout -modulus -in <证书文件> openssl md5</code> <code>openssl rsa -noout -modulus -in <私钥文件> openssl md5</code>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： <code>openssl rsa -in <私钥文件> -out <新私钥文件></code>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？](#)

16.3.10 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。

- 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。

- 如果确认有问题，说明您的网站受到了攻击，并被WAF拦截。

16.3.11 如何处理 523 错误码问题？

如果同一个访问请求四次经过了WAF，为了避免出现死循环现象，WAF会拦截该请求，此时如果您访问网站会出现523错误。

您可以通过以下两种方法解决523错误码问题。

- 方法一：将域名配置为内网解析，不经过公网转发。
- 方法二：配置源站服务器的hosts文件。

以Windows操作系统为例，配置hosts文件的操作步骤如下。

- a. 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。
- b. 在hosts文件添加一条记录：域名对应的源站IP地址。
- c. 保存后退出。

16.3.12 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。

16.3.13 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？](#)。

16.3.14 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。

16.3.15 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”。

16.4 防护规则配置

16.4.1 Web 基础防护类

16.4.1.1 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 > Web应用防火墙”。

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“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 在“Web基础防护”配置框中，选择“拦截”模式。

须知

仅记录模式和拦截模式只适用于Web基础防护，CC攻击防护和精准访问防护都有各自的防护动作。

----结束

16.4.1.2 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16-6](#)所示。

表 16-6 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（原误报屏蔽）规则，再开启“严格”模式，使WAF能有效防护更多攻击。

16.4.2 CC 攻击防护规则类

16.4.2.1 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](#)章节。

16.4.2.2 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。

16.4.2.3 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。

16.4.3 精准访问规则类

16.4.3.1 精准访问防护规则可以设置在指定的时间段生效吗？

WAF不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。

16.4.4 网站反爬虫类

16.4.4.1 开启网站反爬虫后，为什么有些请求被 WAF 拦截但查不到拦截记录？

当您开启网站反爬虫后，WAF将对该域名的第一个访问请求返回一个JavaScript代码，然后根据浏览器解析执行结果返回的数据来判断是否为合法的浏览器或爬虫工具。

网站反爬虫正常的检测流程如下：

1. 客户端访问网站，实际请求首先发送到WAF上。
2. WAF返回JavaScript代码到客户端。
3. 客户端解析JavaScript代码，并将执行结果返回给WAF。
4. WAF根据客户端返回的结果判断客户端是否为合法的浏览器。
 - 如果合法，则WAF将请求发送给源站服务器。
 - 如果非法，则WAF产生告警日志。

须知

- 开启网站反爬虫，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：
 - 对于客户端，请求没有成功获取到页面。
 - 对于WAF，客户端并没有发送解析JavaScript代码的执行结果，因此没有拦截日志记录。

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，建议您关闭网站反爬虫功能。

16.4.5 其他类

16.4.5.1 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。

16.4.5.2 防护规则的路径是否区分大小写？

WAF所有需要配置路径的防护规则，配置的防护路径都区分大小写。

16.4.5.3 Web 应用防火墙支持哪些防护规则？

本节介绍Web应用防火墙支持的防护规则。

- Web基础防护
可防范常规的web应用攻击，如SQL注入攻击、XSS跨站攻击等，可检测webshell，检查HTTP上传通道中的网页木马，打开开关即实时生效。
- CC攻击防护
可根据IP、Cookie或者Referer字段名设置灵活的限速策略，有效缓解CC攻击。
- 精准访问防护
对常见HTTP字段进行条件组合，支持定制化防护策略如CSRF防护，通过自定义规则的配置，更精准的识别恶意伪造请求、保护网站敏感信息、提高防护精准性。
- IP黑白名单
添加终拦截与始终放行的黑白名单IP，增加防御准确性。
- 地理位置访问控制
添加地理位置访问控制规则，针对来源IP进行自定义访问控制。
- 网页防篡改
对网站的静态网页进行缓存配置，当用户访问时返回给用户缓存的正常页面，并随机检测网页是否被篡改。
- 网站反爬虫
动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。
- 全局白名单（原误报屏蔽）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
隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。
- 防敏感信息泄露
防止在页面中泄露用户的敏感信息，例如：用户的身份证号码、手机号码、电子邮箱等。

16.4.5.4 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。

16.4.5.5 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 > Web应用防火墙”。

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“防护策略”栏中，单击“配置防护策略”，进入“防护策略”页面。

步骤6 在“网页防篡改”配置框中，检查是否已开启网页防篡改。

- 如果状态为 ，表示已开启，请执行**步骤7**。
- 如果状态为 ，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 单击“自定义网页防篡改”，进入网页防篡改规则的配置页面，查看规则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。

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

16.4.5.6 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 16-7所示。

表 16-7 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，按照配置引导防护规则检测顺序，进行访问请求过滤检测。

防护规则	防护功能	WAF检测顺序
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

16.4.5.7 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。

A 修订记录

发布日期	修改说明
2024-04-13	第一次正式发布。