



Web 应用防火墙（独享版）

用户使用指南

天翼云科技有限公司

目 录

1 产品介绍	7
1.1 什么是 Web 应用防火墙	7
1.2 内容安全检测	8
1.3 产品规格	9
1.4 相关概念	12
1.5 功能特性	15
1.6 产品优势	19
1.7 应用场景	19
1.8 个人数据保护机制	20
1.9 用户权限	21
1.10 与其他云服务的关系	22
2 计费说明	23
3 WAF 操作指引	25
4 申请 WAF 独享引擎	28
5 网站接入 WAF	32
5.1 将网站接入 WAF 防护	32
5.1.1 网站接入流程（独享模式）	32
5.1.2 步骤一：添加防护网站	35
5.1.3 步骤二：配置负载均衡	40
5.1.4 步骤三：为弹性负载均衡绑定弹性公网 IP	42
5.1.5 步骤四：放行独享引擎回源 IP	43
5.1.6 步骤五：独享引擎本地验证	46
5.2 WAF 支持的端口范围	48
6 查看防护事件	50
6.1 查询防护事件	50
6.2 处理误报事件	52
6.3 下载防护事件	59
6.4 通过 LTS 记录 WAF 全量日志	61

7 配置防护策略	73
7.1 防护配置概述	73
7.2 配置 Web 基础防护规则防御常见 Web 攻击	77
7.3 配置 CC 攻击防护规则防御 CC 攻击	81
7.4 配置精准访问防护规则定制化防护策略	88
7.5 配置 IP 黑白名单规则拦截/放行指定 IP	97
7.6 配置地理位置访问控制规则拦截/放行特定区域请求	104
7.7 配置网页防篡改规则避免静态网页被篡改	111
7.8 配置网站反爬虫防护规则防御爬虫攻击	114
7.9 配置防敏感信息泄露规则避免敏感信息泄露	122
7.10 配置全局白名单规则对误报进行忽略	126
7.11 配置隐私屏蔽规则防隐私信息泄露	131
7.12 创建引用表对防护指标进行批量配置	135
7.13 配置攻击惩罚标准封禁访问者指定时长	139
7.14 条件字段说明	143
8 查看总览	146
9 网站设置	150
9.1 网站接入后推荐配置	150
9.1.1 配置 PCI DSS/3DS 合规与 TLS	150
9.1.2 开启 IPv6 防护	158
9.1.3 配置 WAF 到网站服务器的连接超时时间	160
9.1.4 开启连接保护功能保护源站安全	161
9.1.5 配置攻击惩罚的流量标识	163
9.1.6 修改拦截返回页面	165
9.1.7 开启 Cookie 安全属性	167
9.2 网站管理	168
9.2.1 查看网站基本信息	168
9.2.2 切换工作模式	170
9.2.3 更新网站绑定的证书	170
9.2.4 修改服务器配置信息	173
9.2.5 删除防护网站	174
10 策略管理	176
10.1 新增防护策略	176
10.2 添加策略适用的防护域名	177
10.3 批量添加防护规则	178
11 高阶功能	180
11.1 配置内容安全检测	180

12 对象管理	184
12.1 管理证书.....	184
12.1.1 上传证书.....	184
12.1.2 查看证书信息.....	186
12.1.3 删除证书.....	187
12.2 管理黑白名单 IP 地址组.....	188
12.2.1 添加黑白名单 IP 地址组.....	188
12.2.2 修改或删除黑白名单 IP 地址组.....	189
13 系统管理	191
13.1 管理独享引擎.....	191
13.2 查看产品信息.....	195
13.3 开启告警通知.....	195
14 权限管理	198
14.1 IAM 权限管理.....	198
14.1.1 WAF 自定义策略.....	198
14.1.2 WAF 权限及授权项.....	199
15 监控与审计	203
15.1 监控.....	203
15.1.1 WAF 监控指标说明.....	203
15.1.2 设置监控告警规则.....	215
15.1.3 查看监控指标.....	216
15.2 审计.....	217
15.2.1 云审计服务支持的 WAF 操作列表.....	217
15.2.2 在 CTS 事件列表查看云审计事件.....	218
16 常见问题	221
16.1 产品咨询.....	221
16.1.1 WAF 基础知识.....	221
16.1.2 Web 应用防火墙是否能防护 IP?	225
16.1.3 Web 应用防火墙支持对哪些对象进行防护?	226
16.1.4 Web 应用防火墙支持自定义 POST 拦截吗?	226
16.1.5 Web 应用防火墙是否支持 IPv4 和 IPv6 共存?	227
16.1.6 WAF 和 HSS 的网页防篡改有什么区别?	228
16.1.7 Web 应用防火墙支持哪些 Web 服务框架/协议?	229
16.1.8 WAF 可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗?	229
16.1.9 WAF 转发和 Nginx 转发有什么区别?	229
16.1.10 Web 应用防火墙和云防火墙有什么区别?	230
16.1.11 Web 应用防火墙可以配置会话 Cookie 吗?	231
16.1.12 WAF 对 SQL 注入、XSS 跨站脚本和 PHP 注入攻击的检测原理?	232

16.1.13 WAF 是否可以防护 Apache Struts2 远程代码执行漏洞（CVE-2021-31805）？	233
16.1.14 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？	233
16.1.15 本地文件包含和远程文件包含是指什么？	234
16.1.16 QPS 和请求次数有什么区别？	234
16.1.17 为什么 Cookie 中有 HWWAFSESID 或 HWWAFSESTIME 字段？	235
16.2 购买和变更规格	235
16.2.1 主账号与子账号的权限有哪些区别？	235
16.2.2 Web 应用防火墙是否支持多个账号共享使用？	235
16.2.3 QPS 超过当前 WAF 版本支持的峰值时有什么影响？	236
16.2.4 如何查看防护网站的入带宽和出带宽信息？	236
16.3 计费	237
16.3.1 Web 应用防火墙可以免费使用吗？	237
16.3.2 Web 应用防火墙如何收费？	237
16.3.3 如何退订 Web 应用防火墙？	237
16.4 网站接入	238
16.4.1 独享模式如何防护不支持的非标准端口？	238
16.4.2 如何在添加域名中配置防护域名？	239
16.4.3 添加域名时，防护网站端口需要和源站端口配置一样吗？	240
16.4.4 后端服务器配置多个源站地址时的注意事项？	240
16.4.5 Web 应用防火墙支持配置泛域名吗？	241
16.4.6 泛域名和单域名都接入 WAF，WAF 如何转发访问请求？	241
16.4.7 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？	241
16.4.8 域名接入 Web 应用防火墙后，能通过 IP 访问网站吗？	242
16.5 防护规则	242
16.5.1 Web 基础防护支持设置哪几种防护等级？	242
16.5.2 CC 攻击的防护峰值是多少？	242
16.5.3 在什么情况下使用 Cookie 区分用户？	246
16.5.4 CC 规则里“限速频率”和“放行频率”的区别？	246
16.5.5 配置“人机验证”CC 防护规则后，验证码不能刷新，验证一直不通过，如何处理？	246
16.5.6 开启 JS 脚本反爬虫后，为什么客户端请求获取页面失败？	249
16.5.7 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗？	249
16.5.8 JS 脚本反爬虫的检测机制是怎么样的？	250
16.5.9 哪些情况会造成 WAF 配置的防护规则不生效？	251
16.5.10 开启网页防篡改后，为什么刷新页面失败？	251
16.5.11 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？	252
16.5.12 如何处理 Appscan 等扫描器检测结果为 Cookie 缺失 Secure/HttpOnly？	253
16.6 IPv6 防护	253
16.6.1 哪些版本支持 IPv6 防护？	253
16.6.2 如何测试在 WAF 中配置的源站 IP 是 IPv6 地址？	253

16.6.3 业务使用了 IPv6，WAF 中的源站地址如何配置？	254
16.6.4 WAF 如何解析/访问 IPv6 源站？	254
16.7 证书管理	255
16.8 防护日志	256
16.8.1 Web 应用防火墙支持记录防护日志吗？	256
16.8.2 如何获取拦截的数据？	256
16.8.3 防护事件列表中，防护动作为“不匹配”是什么意思呢？	256
16.8.4 Web 应用防火墙的防护日志可以存储多久？	256
16.8.5 Web 应用防火墙可以同时查询多个指定 IP 的防护事件吗？	256
16.8.6 Web 应用防火墙会记录未拦截的事件吗？	257
16.8.7 为什么 WAF 显示的流量大小与源站上显示的不一致？	257
16.9 内容安全检测服务	257
16.9.1 购买内容安全检测服务时，如何确定网站检测配额？	257
16.9.2 内容安全检测服务对网站的检测范围是什么？	259
16.9.3 购买内容安全检测服务后，多长时间能出报告？	260
16.9.4 购买内容安全检测服务后，什么时候扣费？	260
16.10 网站接入异常排查	260
16.10.1 域名/IP 接入状态显示“未接入”，如何处理？	260
16.10.2 如何解决网站接入 WAF 后程序访问页面卡顿？	262
16.10.3 如何处理网站接入 WAF 后，文件不能上传？	262
16.11 证书/加密套件问题排查	263
16.11.1 如何解决证书链不完整？	263
16.11.2 如何解决证书与密钥不匹配问题？	267
16.11.3 如何解决 HTTPS 请求在部分手机访问异常？	268
16.11.4 如何处理“协议不受支持，客户端和服务端不支持一般 SSL 协议版本或加密套件”？	268
16.11.5 如何解决“网站被检测到：SSL/TLS 存在 Bar Mitzvah Attack 漏洞”？	270
16.12 流量转发异常排查	270
16.12.1 如何排查 404/502/504 错误？	270
16.12.2 如何处理 418 错误码问题？	274
16.12.3 如何处理 523 错误码问题？	274
16.12.4 如何解决重定向次数过多？	276
16.12.5 如何处理接入 WAF 后报错 414 Request-URI Too Large？	276
16.12.6 连接超时时长是多少，是否可以手动设置该时长？	278
16.13 误拦截正常请求排查	278
16.13.1 WAF 误拦截了正常访问请求，如何处理？	278
16.13.2 WAF 误拦截了“非法请求”访问请求，如何处理？	279
A 修订记录	281

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

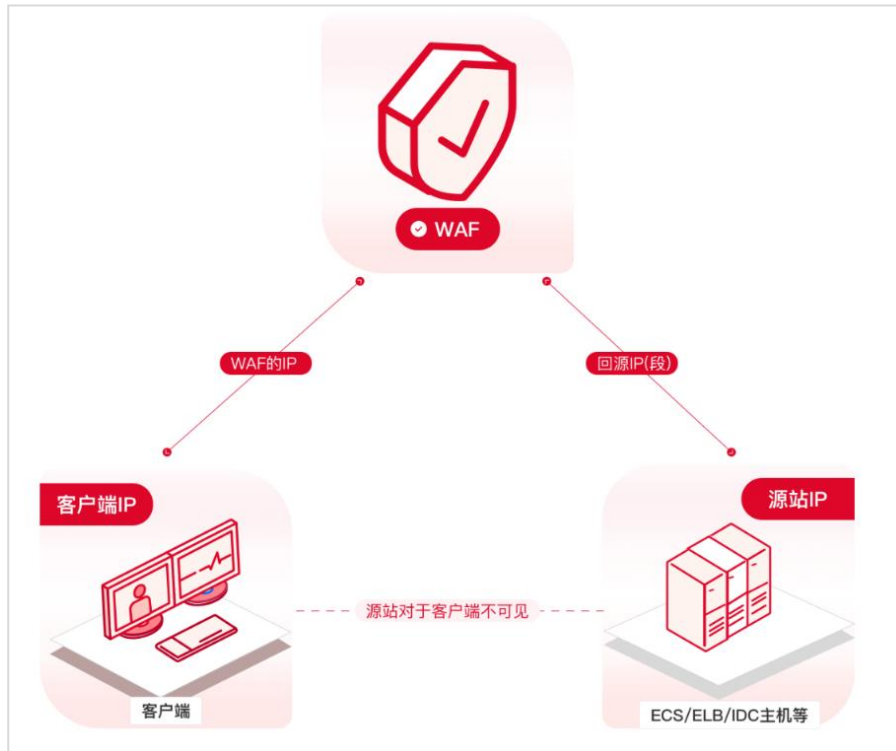
申请 WAF 后，在 WAF 管理控制台将网站添加并接入 WAF。网站成功接入 WAF 后，网站所有访问请求将先流转到 WAF，WAF 检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

图 1-1 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 内容安全检测

内容安全检测服务，基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出 Web 网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、涉政、惊悚、违禁广告等敏感违规内容，并提供文本内容纠错审校（错别字、生僻字、语法表述不当等有违准确性内容）。并提供专业检测报告助您自纠自查，降低内容违规风险。

特性说明

表 1-1 特性说明

特性	说明
检测位置	检测 Web 网站和新媒体平台发布的内容。
检测范围	内容的合法合规性、准确性。
检测技术	机器检测：基于丰富的违规样例库进行机器初审核。

特性	说明
	人工审核：内容审核专家基于多年经验对机器检测结果进行再审核。
交付形式	Word 形式的检测报告。 <ul style="list-style-type: none">“检测类型”选择“内容安全单次检测（按需）”时，下单后的 7 个工作日内出报告。“检测类型”选择“文本安全监测（按月/按年）”时，下单后的检测周期（1 个月）后的 7 个工作日内出报告。
计费模式	包年/包月（预付费）和按需计费（后付费）两种计费方式。 <ul style="list-style-type: none">文本安全监测（按年）文本安全监测（按月）内容安全单次检测（按需） 按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。例如：单次配置了 10 个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行 10 次收费。

应用场景

网站/新媒体内容安全检测

- 内容合法合规性检测

国家政策要求各地方机构要认真落实意识形态工作和网络内容安全工作责任制。为响应国家政策，内容安全检测服务可对网站/新媒体内容进行合法合规检测，主要对文本、图片、视频、语音进行检测和识别是否包含色情、涉政、暴力、惊悚、不宜广告、垃圾信息、不良内容等，有效帮助您降低内容风险。

- 内容准确性检测

对网站/主流新媒体平台的内容进行准确性检测，主要对文本、图片、视频、语音进行表述规范审核，如对错别字、生僻字、词法表述、语法表述等内容进行检测审核。

1.3 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 1-2 所示。

表 1-2 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	<ul style="list-style-type: none">• 域名• 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 1-3 所示。

表 1-3 业务规格说明

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 800；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</p> <p>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>

业务指标	规格
业务带宽阈值（源站服务器部署在云内）	<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）
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
IP 黑白名单规则	100 条
地理位置封禁规则	100 条
网页防篡改规则	100 条
防敏感信息泄露	100 条
误报屏蔽规则	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。

表 1-4 安全功能特性

功能模板	相关文档
支持添加泛域名	5.1.2 步骤一：添加防护网站
非 80、443 标准端口防护	5.2WAF 支持的端口范围
支持 IPv6 防护	9.1.2 开启 IPv6 防护
批量灵活配置防护策略	10.3 批量添加防护规则

功能模板	相关文档
常见的 Web 应用攻击防护，包括 XSS 攻击、SQL 注入、爬虫检测等	7.2 配置 Web 基础防护规则防御常见 Web 攻击
云端自动更新最新 0Day 漏洞防护规则，及时下发 0Day 漏洞虚拟补丁	
Webshell 检测	
CC 攻击防护	7.3 配置 CC 攻击防护规则防御 CC 攻击
精准访问防护	7.4 配置精准访问防护规则定制化防护策略
引用表管理	7.12 创建引用表对防护指标进行批量配置
IP 黑白名单设置	7.5 配置 IP 黑白名单规则拦截/放行指定 IP
支持对指定国家、省份的 IP 自定义访问控制	7.6 配置地理位置访问控制规则拦截/放行特定区域请求
网页防篡改	7.7 配置网页防篡改规则避免静态网页被篡改
基于人机识别和数据风控的动态反爬虫	7.8 配置网站反爬虫防护规则防御爬虫攻击
防敏感信息泄露	7.9 配置防敏感信息泄露规则避免敏感信息泄露
误报屏蔽	7.10 配置全局白名单规则对误报进行忽略
隐私屏蔽	7.11 配置隐私屏蔽规则防隐私信息泄露

1.4 相关概念

本文为您介绍 Web 应用防火墙相关名词的主要含义。

CC 攻击

CC 攻击是针对 Web 服务器或应用程序的攻击，利用获取信息的标准的 GET/POST 请求，如请求涉及数据库操作的 URI（Universal Resource Identifier）或其他消耗系统资源的 URI，造成服务器资源耗尽，无法响应正常请求。

跨站请求伪造

跨站请求伪造攻击是一种常见的 WEB 攻击手法。攻击者通过伪造非受害者意愿的请求数据，诱导受害者访问，如果受害者浏览器保持目标站点的认证会话，则受害者在访问攻击者构造的页面或 URL 的同时，携带自己的认证身份向目标站点发起了攻击者伪造的请求。

扫描器

扫描器是一类自动检测本地或远程主机安全弱点的程序，它能够快速的准确的发现扫描目标存在的漏洞并提供给使用者扫描结果。

网页防篡改

网页防篡改为用户的文件提供保护功能，避免指定目录中的网页、电子文档、图片、数据库等类型的文件被黑客、病毒等非法篡改和破坏。

跨站脚本攻击

一种网站应用程序的安全漏洞攻击，攻击者将恶意代码注入到网页上，用户在浏览网页时恶意代码会被执行，从而达到恶意盗取用户信息的目的。

SQL 注入

SQL 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 Web 后台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。

命令注入

利用各种调用系统命令的 Web 应用接口，通过命令拼接、绕过黑名单等方式在服务端形成对业务服务攻击的系统命令，从而实现对业务服务的攻击。

代码注入

利用 Web 应用在输入校验上的逻辑缺陷，或者部分脚本函数本身存在的代码执行漏洞，而实现的攻击手法。

敏感文件访问

一些涉及操作系统、应用服务框架的配置文件、权限管理文件等作为业务核心敏感的文件不应该被 Internet 上的请求所访问，否则会影响业务的安全。

服务端请求伪造

一种由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF 攻击的目标是从外网无法访问的内部系统。SSRF 形成的原因是服务端提供了从其他服务器应用获取数据的功能，在用户可控的情况下，未对目标地址进行过滤与限制，导致此漏洞的产生。

网站后门

Webshell 是一种 Web 入侵的脚本攻击工具，攻击者在入侵了一个网站后，将 asp、php、jsp 或者 cgi 等脚本文件与正常的网页文件混在一起，然后使用浏览器来访问 asp 或者 php 后门，得到一个命令执行环境，以达到控制网站服务器的目的。因此也有人称之为网站的后门工具。

盗链

盗链是指对方网站直接链接您网站上的文件，而不是将其置于自己的服务器上。一般而言，盗链的对象大多为耗带宽的大体积文件，如图片、视频等。从某种意义上说，造成了让您为其访问流量买单，不仅您的服务器带宽被无任何回报地占用，而且往往会在很大程度上影响您网站的访问速度。

多模匹配

利用高效的多模匹配算法，对请求流量进行特征检测，极大提升了检测引擎的性能。

精准访问防护

支持对 HTTP 请求的多个常用字段（URL、IP、Params、Cookie、Referer、User-Agent、Header）的自定义检测策略，并且支持多逻辑检测策略。

黑白名单

IP 黑白名单包括 IP 白名单和 IP 黑名单配置，其中 IP 白名单即指定 IP 为可信 IP，源 IP 为可信 IP 的流量不进行攻击检测。IP 黑名单即指定 IP 为恶意 IP，源 IP 为恶意 IP 的流量需要根据检测策略执行相应的动作。

智能解码

智能识别请求中的多种编码无限次多层混淆，对其进行深度解码，从而获取攻击者原始的攻击意图。

基于语义分析检测

基于语义上下文构建语法树，分析并判断是否为攻击载荷。

访问频率控制

通过访问控制策略，限制接口的访问的频率。

反爬虫

丰富的爬虫特征库，检测各种类别的爬虫（引擎爬虫，脚本爬虫，扫描工具）。

A 记录

A（Address）记录是地址记录，用来指定主机名（或域名）对应的 IP 地址记录，通过 A 记录，可以设置不同域名指向不同的 IP。

SQL 注入攻击

通过输入域或页面请求的查询字符串，欺骗服务器执行恶意的 SQL 命令。

非标准端口

除“80”、“443”以外的端口。

1.5 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	支持对网站的 HTTP、HTTPS 流量进行安全防护。
	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	<p>覆盖 OWASP（Open Web Application Security Project，简称 OWASP）TOP 10 中常见安全威胁，通过预置丰富的信誉库，对漏洞攻击、网页木马等威胁进行检测和拦截。</p> <ul style="list-style-type: none"> • 常规检测 防护 SQL 注入、XSS 跨站脚本、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。 • 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。 <p>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。</p> • 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	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	对常见的 HTTP 字段（如 IP、路径、Referer、User Agent、Params 等）进行条件组合，配置强大的精准访问控制策略；支持盗链防护、空字段拦截等防护场景。
	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。

功能类别		功能说明
	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。
高级配置	PCI DSS/PCI 3DS 合规认证和 TLS	<ul style="list-style-type: none"> TLS 支持 TLS v1.0、TLS v1.1 和 TLS v1.2 三个版本和七种加密套件，可以满足各种行业客户的安全需求。 WAF 支持 PCI DSS 和 PCI 3DS 合规认证功能。
	IPv6 防护	<ul style="list-style-type: none"> Web 应用防火墙支持 IPv6/IPv4 双栈，针对同一域名可以同时提供 IPv6 和 IPv4 的流量防护。 针对仍然使用 IPv4 协议栈的 Web 业务，Web 应用防火墙支持 NAT64 机制（NAT64 是一种通过网络地址转换（NAT）形式促成 IPv6 与 IPv4 主机间通信的 IPv6 转换机制），即 WAF 可以将 IPv4 源站转化成 IPv6 网站，将外部 IPv6 访问流量转化成对内的 IPv4 流量。
	连接保护	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。

功能类别		功能说明
	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。
	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 30 秒，该值可以在 WAF 界面手动设置。
高阶功能	内容安全检测服务	基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出 Web 网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、违禁等敏感违规内容，并提供文本内容纠错审校，助您降低内容违规风险
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。
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。
安全可视化		<p>提供简洁友好的控制界面，实时查看攻击信息和事件日志。</p> <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。

1.6 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。

0day 漏洞快速修复

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

保护用户数据隐私

- 支持用户对攻击日志中的账号、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。

1.7 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。

内容安全检测

网站/新媒体内容安全检测

- 内容合法合规性检测

国家政策要求各地方机构要认真落实意识形态工作和网络内容安全工作责任制。为响应国家政策，内容安全检测服务可对网站/新媒体内容进行合法合规检测，主要对文本、图片、视频、语音进行检测和识别是否包含色情、涉政、暴力、惊悚、不宜广告、垃圾信息、不良内容等，有效帮助您降低内容风险。

- 内容准确性检测

对网站/主流新媒体平台的内容进行准确性检测，主要对文本、图片、视频、语音进行表述规范审核，如对错别字、生僻字、词法表述、语法表述等内容进行检测审核。

1.8 个人数据保护机制

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

收集范围

对于触发攻击告警的请求，WAF 在事件日志中会记录相关请求记录，收集及产生的个人数据如表 1-5 所示。

表 1-5 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
----	------	--------	------

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。

1.9 用户权限

系统默认提供两种权限策略：系统策略和自定义策略。系统策略是 IAM 预置的策略，用户只能使用不能修改。如果系统策略不满足授权要求，用户可以创建自定义策略，自由搭配需要授予的权限集。

用户组配置权限策略后，将用户加入用户组中，可以使该用户获得权限策略中定义的操作权限。

1.10 与其他云服务的关系

本章节介绍 Web 应用防火墙与其他云服务的关系。

与弹性云主机的关系

Web 应用防火墙为弹性云主机提供 Web 安全防护服务。

与云审计的关系

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

与云监控服务的关系

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

与弹性负载均衡的关系

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

与统一身份认证服务的关系

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

2 计费说明

Web 应用防火墙支持按需计费（后付费）计费方式。

计费项

WAF 根据计费项目进行计费。

表 2-1 计费项信息

模式	计费模式	计费项目	计费说明
独享模式	按需计费	实例数	按实际使用时长计费。
内容安全检测服务	包周期（按月/按年）	文本安全监测	按购买的检测类型计费。
	按需计费	检测次数	单次扫描，按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。 例如：单次配置了 10 个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行 10 次收费。

计费模式

- 独享模式：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。
- 内容安全检测服务：包年/包月（预付费）和按需计费（后付费）两种计费方式。
 - 文本安全监测（按年）
 - 文本安全监测（按月）
 - 内容安全单次检测（按需）

按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。例如：单次配置了 10 个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行 10 次收费。

3 WAF 操作指引

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至 WAF 进行防护。

使用流程

相关流程如图 3-1，具体说明如图 3-1 表 3-1 所示。

图 3-1 WAF 使用流程



表 3-1 WAF 使用流程说明

操作	说明
4 申请 WAF 独享引擎	通过申请独享引擎开通 WAF。
5 网站接入 WAF	添加需要防护的网站，WAF 保护网站业务安全稳定。 详细操作请参见 5.1.2 步骤一：添加防护网站。 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。
7 配置防护策略	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。
6 查看防护事件	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，通过查看并分析防护日志，对网站的防护策略进行调整，也可以对误报时间进行屏蔽。
13.3 开启告警通知	开启告警通知后，用户可以第一时间接收被拦截和仅记录的攻击日志。

配套功能

按照[使用流程](#)完成网站配置后，您也可以使用以下功能增强网站的安全性能。

表 3-2 配套功能

功能	说明
1111.1 配置内容安全检测	Web 应用防火墙提供内容安全检测服务，基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出 Web 网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、涉政、惊悚、违禁广告等敏感违规内容，并提供文本内容纠错审校（错别字、生僻字、语法表述不当等有违准确性内容）。并提供专业检测报告助您自纠自查，降低内容违规风险。
8 查看总览	可查看到昨天、今天、3 天、7 天或者 30 天范围内的防护数据。

功能	说明
99.19.1.1 配置 PCI DSS/3DS 合规与 TLS	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。
9.1.2 开启 IPv6 防护	开启 IPv6 防护后，WAF 将为域名分配 IPv6 的接入地址，WAF 直接通过 IPv6 地址访问源站。
9.1.3 配置 WAF 到网站服务器的连接超时时间	<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 30 秒，该值可以在 WAF 界面手动设置。
9.1.4 开启连接保护功能保护源站安全	网站接入 WAF 防护之后，如果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。
9.1.5 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。
9.1.6 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。
1212.1 管理证书	将证书上传到 WAF，添加防护网站时可直接选择上传到 WAF 的证书。
1313.1 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。
13.2 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。

4 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 单击管理控制台右上角的，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（独享版）”。
- 步骤 4 在界面右上角，单击“申请独享引擎”。
- 步骤 5 配置 WAF 实例参数，如图 4-1 所示，相关参数说明如图 4-1 表 4-1 所示。

图 4-1 配置 WAF 独享引擎实例

可用区 **可用区1**
如何选择可用区?

WAF实例名称前缀

WAF实例数量 如果被防护的业务为生产业务，为保证业务SLA，请至少申请部署两个实例节点，避免单点故障

WAF实例规格 **WI-500** WI-100
单实例性能参考，吞吐量：500 Mbps，QPS：5,000，极限 10,000 ?
单实例可支持回源长连接：60,000（每实例），5,000（每域名） ?

WAF实例创建类别 **资源租户类** 普通租户类
WAF实例将通过弹性网卡接入租户网络（若使用ELB接入，那么仅支持独享型ELB）

CPU架构 **X86计算** **ARM计算**

虚拟私有云 [查看虚拟私有云](#)

子网 [C](#)

安全组 ? [管理安全组](#)

表 4-1 WAF 独享引擎实例参数说明

参数名称	说明
计费模式	<ul style="list-style-type: none"> 包年/包月 “WAF 实例创建类别”：只支持“资源租户类”。 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。 “WAF 实例创建类别”：支持“资源租户类”和“普通租户类”。
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。只提供已授权的可用分区。
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。

参数名称	说明
WAF 实例规格	<p>选择实例的规格。WAF 支持 500Mbit/s 和 100Mbit/s 两种规格。</p> <ul style="list-style-type: none"> WI-500 单实例性能参考，吞吐量：500 Mbps，QPS：10,000 单实例可支持回源长连接：60,000（每实例），5,000（每域名） WI-100 单实例性能参考，吞吐量：100 Mbps，QPS：2,000 单实例可支持回源长连接：60,000（每实例），5,000（每域名）
WAF 实例创建类别	<ul style="list-style-type: none"> 资源租户类 WAF 实例将通过弹性网卡接入租户网络（如果使用 ELB 接入，那么仅支持独享型 ELB） 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。支持“X86 计算”和“ARM 计算”。
ECS 规格	“WAF 实例创建类别”选择“普通租户类”时，需要配置此参数。选择实例的 ECS 规格。
虚拟私有云	选择源站所在的 VPC。
子网	选择 VPC 中已配置的子网。
安全组	<p>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。</p> <p>须知</p> <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。
服务授权	首次购买 WAF 时，可配置此参数。勾选后，WAF 将代您在 IAM 中创建委托，开通相关权限。
反亲和	开启后，独享引擎在创建时，将尽量分散地创建在不同的物理主机上，以提高业务的可靠性。

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。

---**结束**

5 网站接入 WAF

5.1 将网站接入 WAF 防护

5.1.1 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至 WAF 进行监控防护。

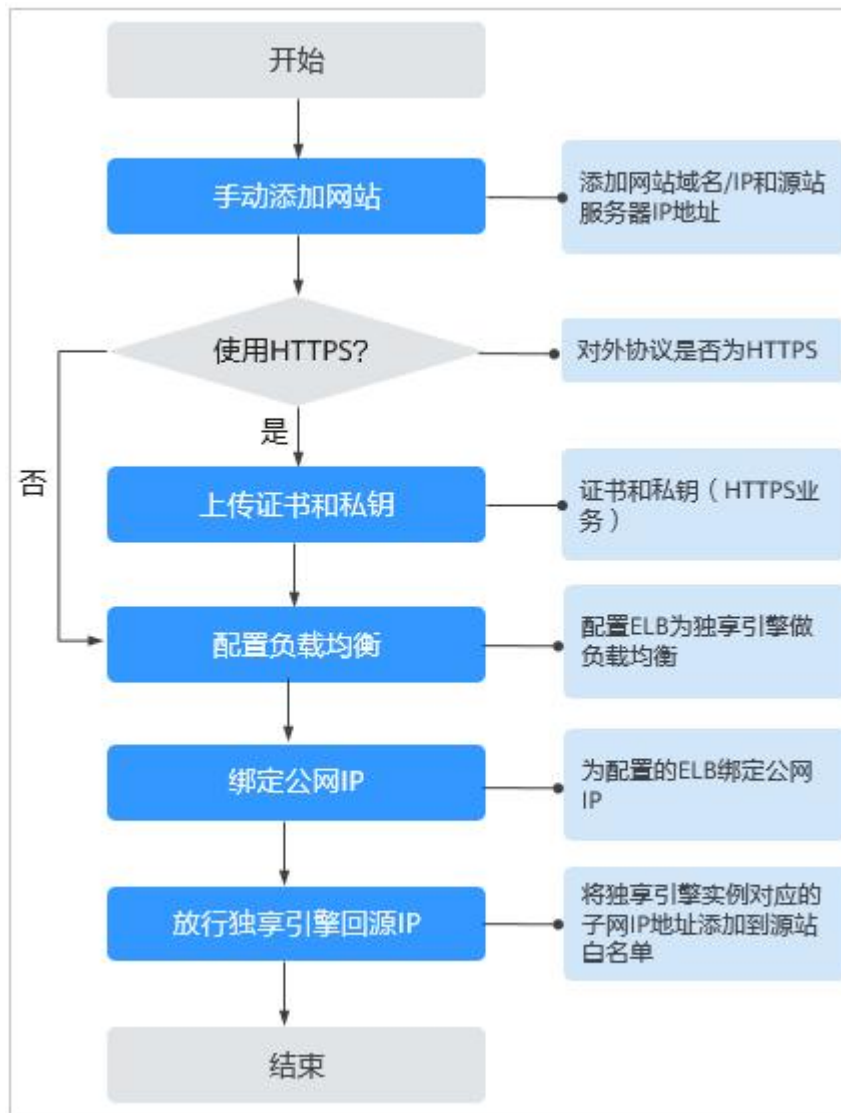
使用场景

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 5-1 所示的配置流程，快速使用 WAF。

图 5-1 网站接入 WAF 的操作流程图-独享模式



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 5-1 所示相关信息。

表 5-1 准备防护域名/IP 相关信息

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

获取信息	参数	说明	示例
	防护对象端口	<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 <p>须知 如果防护域名使用非标准端口, 请查看 5.2WAF 支持的端口范围, 确保购买的 WAF 版本支持防护该非标准端口。</p>	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	<p>网站服务器的私网 IP 地址。</p> <p>登录 ECS 或 ELB 控制台, 在实例列表中查看对应服务器的私有 IP 地址。</p> <p>说明 源站地址不能与防护对象一致。</p>	192.168.1.1
(可选) 证书	证书名称	<p>对外协议选择“HTTPS”时, 需要在 WAF 上配置证书, 将证书绑定到防护域名。</p> <p>须知 WAF 当前仅支持 PEM 格式证书。如果证书为非 PEM 格式, 请参考如何将非 PEM 格式的证书转换为 PEM 格式? 转化证书格式。</p>	-

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 16.1016.10.1 域名/IP 接入状态显示“未接入”，如何处理？排查处理。

5.1.2 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

- 已申请独享型 ELB（Elastic Load Balance）。
- 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”。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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（独享版）”。

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”，如 图 5-2 所示。

- “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

- WAF 支持添加“*”泛域名，表示可以防护任意的域名。“防护对象”配置为“*”时，只能防护除 80、443 端口以外的非标端口。
- 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。

图 5-2 配置域名信息

域名信息

网站名称 test

* 防护对象 192.168.3.1

网站备注 test

步骤 7 源站配置，如图 5-3 所示，参数说明如图 5-3 表 5-2 所示。

图 5-3 源站配置

源站配置

* 防护对象端口 标准端口

* 服务器配置

对外协议 ? 源站协议 ? VPC 源站地址 ? 源站端口 ?

HTTP HTTP vpc-gz IPv4 80

+ 添加 您还可以添加79个源站地址

表 5-2 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。 <p>说明 WAF 支持 WebSocket/WebSockets 协议，且默认为开启状态。</p> <ul style="list-style-type: none"> 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：网站服务器的私有 IP 地址。 登录 ECS 或 ELB 控制台，在实例列表中查看对应服务器的私有 IP 地址。 <p>说明 源站地址不能与防护对象一致。 支持以下两种 IP 格式：</p> <ul style="list-style-type: none"> IPv4，例如：XXX.XXX.1.1 IPv6，例如： fe80:0000:0000:0000:0000:0000:0000:0000 <ul style="list-style-type: none"> 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>成功导入的新证书，将添加到“证书管理”页面的证书列表中。有关证书管理的操作，请参见1212.112.1.1 上传证书。</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。

- “是否已使用代理”：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。

可根据界面提示，完成配置负载均衡、为弹性负载均衡绑定弹性公网 IP 和放行独享引擎回源 IP 的操作，建议单击“稍后”。后续参照 2.5.1.3 步骤二：配置负载均衡、5.1.4 步骤三：为弹性负载均衡绑定弹性公网 IP 和 5.1.5 步骤四：放行独享引擎回源 IP 完成相关操作。

---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 独享引擎时，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。然后输入“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。

图 5-4 导入新证书



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 5-3 在本地将证书转换为 PEM 格式，再上传。

表 5-3 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
P7B	<ol style="list-style-type: none">证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer将“cert.cer”证书文件直接重命名为“cert.pem”。

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.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

📖 说明

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

5.1.3 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。

约束条件

- 配置健康检查后，独享引擎实例的“健康检查结果”的“状态”必须为“正常”，否则会导致网站不能正常接入 WAF。
- 后端服务器的“业务端口”需要与 WAF 独享引擎实例实际监听的业务端口一致，即与 5.1.2 步骤一：添加防护网站时设置的“防护对象端口”保持一致。
- 由于 WAF 是七层代理产品，配置监听器时，“前端协议”只能选择 HTTP 或 HTTPS 协议。

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”，配置监听器名称、前端协议/前端端口信息。
- 步骤 6 单击“下一步”，配置后端主机组和健康检查，如图 5-5 和图 5-6 所示。

图 5-5 配置后端主机组



后端主机组

* 名称

* 后端协议

* 分配策略类型

会话保持

描述

0/255

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。

图 5-6 健康检查配置



步骤 7 单击“完成”后再单击“确定”，监听器添加成功。

步骤 8 在添加的监听器页面，选择“后端主机组”页签后，单击“添加”。

步骤 9 在弹出的“添加后端主机”对话框中，选择已创建的 WAF 独享引擎实例。

步骤 10 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。

5.1.4 步骤三：为弹性负载均衡绑定弹性公网 IP

如果 WAF 独享引擎实例已配置负载均衡，请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 2.5.1.3 步骤二：配置负载均衡上。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。


本章节以解绑源站服务器的弹性公网 IP（Elastic IP，简称 EIP），将解绑的 EIP 绑定到 WAF 独享引擎的弹性负载均衡（Elastic Load Balance，简称 ELB）上为例说明，具体操作请以实际业务为准。


前提条件

已为 WAF 独享引擎实例 2.5.1.3 步骤二：配置负载均衡。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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，解绑源站服务器的弹性公网 IP。

- 解绑 IPv4 公网 IP，在目标源站的负载均衡器所在行“操作”列，选择“更多 > 解绑 IPv4 公网 IP”。
- 解绑 IPv6 公网 IP，在目标源站的负载均衡器所在行“操作”列，选择“更多 > 解绑 IPv6 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，找到 WAF 独享引擎的 ELB 的负载均衡器，绑定源站服务器的弹性公网 IP。

- 绑定 IPv4 公网 IP，在 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 公网 IP”。
- 绑定 IPv6 公网 IP，在 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 IPv6 公网 IP”。

步骤 7 在弹出对话框中，选择**步骤 4**中解绑的 EIP，单击“确定”，绑定 EIP。

---结束

5.1.5 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 (独享版)”。


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。

图 5-7 独享引擎列表



实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	规格	计费模式	操作
1026-fyV 388ad33ce22438b657b67a95...	未发配	vpc-iv-test	subnet-e2db	192.168.0.8...	未接入	运行中	--	标准模式 (反向代理)	s7n.2large.2	按量计费	升级 删除 切换安全组
102703100-fA3n 112f93259ec4892810227460a95...	未发配	vpc-iv-test	subnet-e2db	192.168.0.2...	未接入	运行中	--	标准模式 (反向代理)	c7n.large.4	包年包月	升级 续费 更多

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 > 弹性云主机”。

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 5-4 所示。

表 5-4 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 单击页面左上方的 ，选择“安全 > Web 应用防火墙 (独享版)”。


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。

图 5-8 独享引擎列表



实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	规格	计费模式	操作
1026-kyiv 388a9c3e9e2243d8e57ab7a96...	未发现	vpc-ky-test	subnet-e2db	192.168.0.8...	未接入	运行中	--	标准模式 (反向代理)	s7n.2large.2	按量计费	升级 删除 切换安全组
102703100-4A3d 11f2f3258e488281022f460a09...	未发现	vpc-ky-test	subnet-e2db	192.168.0.2...	未接入	运行中	--	标准模式 (反向代理)	c7n.large.4	包年包月	升级 续费 更多

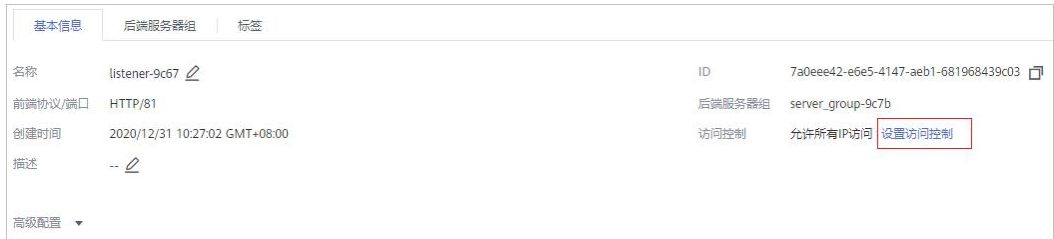
步骤 5 在独享引擎列表的“IP 地址”栏，获取所有创建的独享引擎对应的子网 IP 地址。

步骤 6 单击页面左上方的 ，选择“网络 > 弹性负载均衡”。

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”。

图 5-9 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

5.1.6 步骤五：独享引擎本地验证

添加防护网站后，为了确保 WAF 转发正常，建议您先通过本地验证确保防护网站一切配置正常。

前提条件

已完成 5.1.2 步骤一：添加防护网站~ 5.1.5 步骤四：放行独享引擎回源 IP 的操作。

（可选）验证独享 WAF 是否正常工作

步骤 1 创建一台与独享 WAF 实例在同一 VPC 下的 ECS 用于发送请求。

步骤 2 通过步骤 1 中创建的 ECS 向独享 WAF 发送请求。

- 转发测试

```
curl -kv -H "Host: {添加到 WAF 的防护对象}" {服务器配置中的对外协议}://{独享 WAF 的 IP}:{防护对象端口}
```

例如：

```
curl -kv -H "Host: a.example.com" http://192.168.0.1
```

返回码为 200 则说明转发成功。

- 攻击拦截测试。
 - a. 确保网站对应策略已开启基础防护的拦截模式。



Web基础防护
防护常见的Web应用攻击，如SQL注入、XSS攻击、网页木马检查等。



- b. 执行以下命令：

```
curl -kv -H "Host: {添加到WAF的防护对象}" {服务器配置中的对外协议}://{独享WAF的IP}:{防护对象端口} --data "id=1 and 1='1"
```

例如：

```
curl -kv -H "Host: a.example.com" http://192.168.X.X --data "id=1 and 1='1"
```

返回码为 418 则说明拦截成功，独享 WAF 工作正常。

---结束

验证独享 WAF 和 ELB 是否都正常工作

- 转发测试

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB私网的IP}:{ELB监听端口}
```

如果 ELB 添加了 EIP，可以使用任意公网机器直接进行测试。

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB公网的IP}:{ELB监听端口}
```

例如：

```
curl -kv -H "Host: a.example.com" http://192.168.X.Y  
curl -kv -H "Host: a.example.com" http://100.10.X.X
```

返回码为 200 则说明转发成功。

在确保独享引擎工作正常的情况下，如果转发失败，则优先检查 ELB 配置是否有误（如果 ELB 健康检查异常可先关闭 ELB 健康检查再重新执行以上的操作）。

- 攻击拦截测试
 - a. 确保网站对应策略已开启基础防护的拦截模式。



Web基础防护
防护常见的Web应用攻击，如SQL注入、XSS攻击、网页木马检查等。



- b. 执行以下命令：

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB私网的IP}:{ELB监听端口} --data "id=1 and 1='1"
```

如果 ELB 添加了 EIP，可以使用任意公网机器直接进行测试。

```
curl -kv -H "Host: {添加到WAF的防护对象}" {ELB对外协议}://{ELB公网的IP}:{ELB监听端口} --data "id=1 and 1='1"
```

例如：

```
curl -kv -H "Host: a.example.com" http:// 192.168.0.2 --data "id=1 and 1='1"  
curl -kv -H "Host: a.example.com" http:// 100.10.X.X --data "id=1 and 1='1"
```

返回码为 418 则说明拦截成功，独享 WAF、ELB 均工作正常。

5.2 WAF 支持的端口范围

Web 应用防火墙（Web Application Firewall，简称 WAF）支持防护标准端口和非标端口。您在网站接入配置中添加防护网站对应的业务端口，WAF 将通过您设置的业务端口为网站提供流量的接入与转发服务。本文介绍 WAF 支持防护的标准端口和非标端口。

Web 应用防火墙可防护的端口如表 5-5 所示。

表 5-5 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

6 查看防护事件

6.1 查询防护事件

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。

前提条件


5 网站接入 WAF


约束条件

- 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。
- 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。

查看防护日志

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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攻击事件、受攻击站点、攻击源 IP、受攻击 URL 的 TOP 10 网站进行统计，单击可复制统计图表的数据。

图 6-1 防护事件



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“确定”后，匹配条件会展示在事件列表的上方，条件字段参数说明如 表 6-2 所示。
- 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。

表 6-1 支持筛选搜索的条件字段

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、不匹配等。 <ul style="list-style-type: none"> ● 人机验证：CC 防护规则中，“防护动作”支持配置“人机验证”。即当访问的请求频率超过设定的“限速频率”后将弹出验证码提示，输入正确的验证码，请求将不受访问限制。 ● 不匹配：配置网页防篡改、防敏感信息泄露、隐私屏蔽防护规则后，如果访问请求命中这些防护规则，则防护日志中记录的防护事件，“防护动作”显示为“不匹配”。
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 6-2 防护事件列表可展示字段参数说明

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
规则 ID	内置 Web 基础防护规则 ID。	-
URL	攻击的防护域名的 URL。	/admin
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

6.2 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），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，您也不会收到该攻击事件的告警通知。

当 WAF 根据内置的 Web 基础防护规则和网站反爬虫的特征反爬虫，以及自定义防护规则（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 基础防护规则和网站反爬虫的特征反爬虫拦截或记录的攻击事情可以进行“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，您也不会收到该类事件的告警通知。
- 独享模式 2022 年 6 月之前的版本“不检测模块”不支持配置“所有检测模块”选项，仅支持配置“Web 基础防护模块”。


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。

处理误报事件

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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。

图 6-2 误报处理

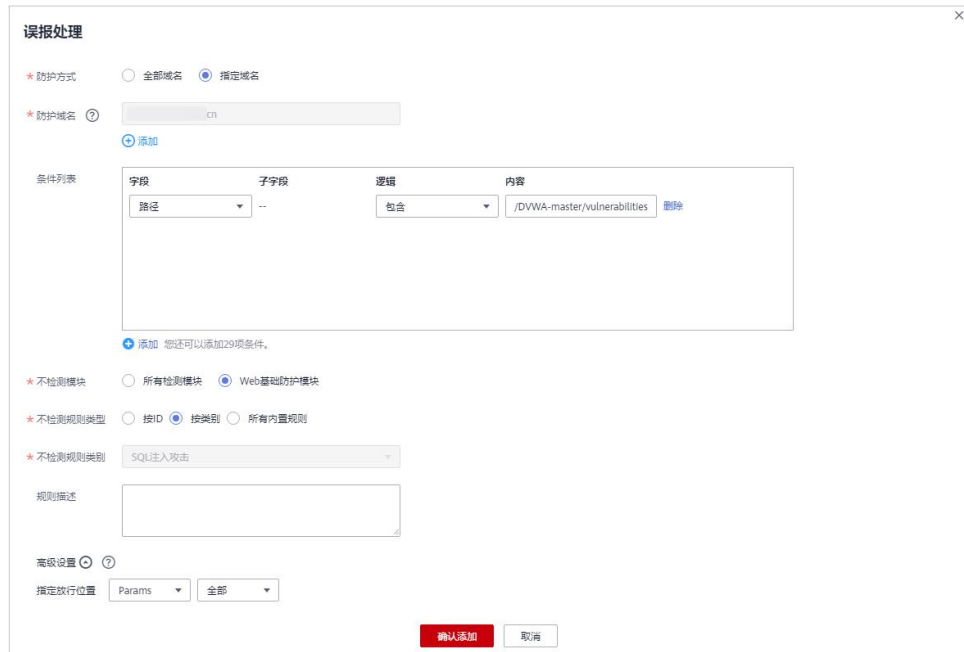


表 6-3 参数说明

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	“防护方式”选择“指定域名”时，需要配置此参数。 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。	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</p> <p>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：7.2 配置 Web 基础防护规则防御常见 Web 攻击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。建议您直接在防护事件页面进行误报处理。</p>	041046

参数	参数说明	取值样例
不检测规则类别	<p>当“不检测规则类型”选择“按类别”时，需要配置此参数。</p> <p>在下拉框中选择事件类别。</p> <p>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。</p>	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	<p>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。</p> <p>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。</p> <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。 <p>说明</p> <p>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。</p>	Params 全部

- 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。

图 6-3 添加至地址组

添加至地址组

将攻击源IP添加至地址组，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。

* 攻击源IP 49

* 添加方式 **选择已有地址组** 新建地址组

* 地址组名称 th812-test 应用于1个策略

确认 取消

- 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。

图 6-4 添加至黑白名单

添加至黑白名单 ✕

将攻击源IP添加至对应防护域名下的策略，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。

防护域名 hkh4 防护策略 hkhtest1

您还可以添加 4,284 个IP/IP段。如需增加配额，请购买 规则扩展包

* 攻击源IP 49.

* 添加方式 选择已有规则 新建规则

* 规则名称 waftest

* IP/IP段或地址组 IP/IP段 地址组

* 防护动作 拦截 ▼

攻击惩罚 无攻击惩罚 ▼

规则描述

确认
取消

表 6-4 参数说明

参数	参数说明
添加方式	<ul style="list-style-type: none"> • 选择已有规则 • 新建规则
规则名称	<ul style="list-style-type: none"> • 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”。

参数	参数说明
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。。
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规则列表中，您可以在“防护策略”界面的全局白名单页面查看、关闭、删除或修改该规则。有关配置全局白名单规则的详细操作，请参见 7.10 配置全局白名单规则对误报进行忽略。

6.3 下载防护事件

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

- 5 网站接入 WAF。
- 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。

下载防护事件数据



- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的，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 (独享版)”。
- 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 6-5。

表 6-5 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

字段	字段说明	示例
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。	d5580c8f6cd4403ebbf85892d4bbb8e4
request_line	攻击者的请求行。	GET /
rule	防护事件对应的规则编号。	81066
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。	/

6.4 通过 LTS 记录 WAF 全量日志

启用 WAF 全量日志功能后，您可以将攻击日志、访问日志记录到云日志服务（Log Tank Service，简称 LTS）中，通过 LTS 记录的 WAF 日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。

LTS 对于采集的日志数据，通过海量日志数据的分析与处理，可以为您提供一个实时、高效、安全的日志处理能力。LTS 默认存储日志的时间为 7 天，存储时间可以在 1~30 天之间进行设置，超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），LTS 提供转储功能，可以将日志转储至对象存储服务（OBS）或者数据接入服务（DIS）中长期保存。

前提条件


- 已申请 WAF。
- 5 网站接入 WAF。


系统影响

开启全量日志功能是将 WAF 日志记录到 LTS，不影响 WAF 性能。

将防护日志配置到 LTS

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（独享版）”。

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“全量日志”页签，开启全量日志 ，并选择日志组和日志流，相关参数说明如图 6-5 表 6-6 所示。

图 6-5 配置全量日志



表 6-6 全量日志配置参数

参数	参数说明	取值样例
选择日志组	选择已创建的日志组。	lts-group-waf
记录攻击日志	选择已创建的日志流。 攻击日志记录每一个攻击告警信息，包括攻击事件类型、防护动作、攻击源 IP 等信息。	lts-topic-waf-attack
记录访问日志	选择已创建的日志流。 访问日志记录每一个 HTTP 访问的关键信息，包括访问时间、访问客户端 IP、访问资源 URL 等信息。	lts-topic-waf-access

步骤 6 单击“确定”，全量日志配置成功。

您可以在 LTS 管理控制台查看 WAF 的防护日志。


----结束


在 LTS 上查看并下载 WAF 防护日志

当您将 WAF 防护日志配置记录到 LTS 上后，请参考以下操作步骤，在 LTS 管理控制台查看、分析、下载记录的 WAF 日志数据。

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“管理与部署 > 云日志服务”，进入“日志管理”页面。

步骤 4 在日志组列表中，单击  展开 waf 日志组（例如，“lts-group-waf”）。

步骤 5 在日志流列表，单击日志流名称，进入日志流日志页面，查看并分析日志。

---结束

WAF 访问日志 access_log 字段说明

字段	类型	字段说明	描述
access_log.requestid	string	随机 ID 标识	与攻击日志的“req_id”字段末尾 8 个字符一致。
access_log.time	string	访问请求的时间	日志内容记录的 GMT 时间。
access_log.connection_requests	string	标识该长链接第几个请求	-
access_log.eng_ip	string	WAF 引擎 IP	-
access_log.pid	string	标识处理该请求的引擎	引擎（worker PID）。
access_log.hostid	string	访问请求的域名标识	防护域名 ID(upstream_id)。
access_log.tenantiid	string	防护域名的租户 ID	一个账号对应一个租户 ID。
access_log.projectid	string	防护域名的项目 ID	用户在对应区域下的项目 ID。
access_log.remote_ip	string	标识请求的四层远端 IP	请求的客户端 IP。 须知 如果在 WAF 前部署了 7 层代理，本字段表示最靠近 WAF 的代理节点的 IP 地址。此时，真实访问者 IP 参考“x-forwarded-for”，“x_real_ip”字段。
access_log.remote_port	string	标识请求的四层远端端口号	请求的客户端端口号。
access_log.sip	string	标识请求的客户端 IP	如，XFF 等。

字段	类型	字段说明	描述
access_log.scheme	string	请求协议类型	请求所使用的协议有： <ul style="list-style-type: none"> • http • https
access_log.response_code	string	请求响应码	源站返回给 WAF 的响应状态码。
access_log.method	string	请求方法	请求行中的请求类型。通常为“GET”或“POST”。
access_log.http_host	string	请求的服务器域名	浏览器的地址栏中输入的地址，域名或 IP 地址。
access_log.url	string	请求 URL	URL 链接中的路径（不包含域名）。
access_log.request_length	string	请求的长度	包括请求地址、HTTP 请求头和请求体的字节数。
access_log.bytes_sent	string	发送给客户端的总字节数	WAF 返回给客户端的总字节数。
access_log.body_bytes_sent	string	发送给客户端的响应体字节数	WAF 返回给客户端的响应体字节数。
access_log.upstream_addr	string	选择的后端服务器地址	请求所对应的源站 IP。例如，WAF 回源到 ECS，则返回源站 ECS 的 IP。
access_log.request_time	string	标识请求处理时间	从读取客户端的第一个字节开始计时（单位：s）。
access_log.upstream_response_time	string	标识后端服务器响应时间	后端服务器响应 WAF 请求的时间（单位：s）。
access_log.upstream_status	string	标识后端服务器的响应码	后端服务器返回给 WAF 的响应状态码。
access_log.upstream_connect_time	string	源站与后端服务建立连接的时间，单位为秒。	在使用 SSL 的情况下，握手过程所消耗的时间也会被记录下来。多次请求建立的时间，使用逗号分隔。

字段	类型	字段说明	描述
access_log.upstream_header_time	string	后端服务器接收到第一个响应头字节的用时，单位为秒。	多次请求响应的的时间，使用逗号分隔。
access_log.bind_ip	string	WAF 引擎回源 IP	引擎回源用网卡的具体 IP 值，若引擎通过挂载 EIP 回源，此值并非 EIP 的值。
access_log.group_id	string	对接 LTS 服务的日志组 ID	WAF 对接云日志服务日志组 ID。
access_log.access_stream_id	string	日志流 ID	与“group_id”相关，是日志组下用户的 access_stream 的 ID。
access_log.engine_id	string	WAF 引擎标识	WAF 引擎的唯一标识。
access_log.time_iso8601	string	日志的 ISO 8601 格式时间	-
access_log.sni	string	通过 SNI 请求的域名	-
access_log.tls_version	string	建立 SSL 连接的协议版本	请求所使用的 TLS 协议版本。
access_log.ssl_curves	string	客户端支持的曲线列表	-
access_log.ssl_session_reused	string	SSL 会话是否被重用。	表示 SSL 会话是否被重用。 r: 是 . : 否
access_log.process_time	string	引擎的检测用时（单位：ms）	-
access_log.args	string	标识 URL 中的参数数据	-

字段	类型	字段说明	描述
access_log.x_forwarded_for	string	当 WAF 前部署代理时，代理节点 IP 链	代理节点 IP 链，为 1 个或多个 IP 组成的字符串。 最左边为最原始客户端的 IP 地址，代理服务器每成功收到一个请求，就将请求来源 IP 地址添加到右边。
access_log.cdn_src_ip	string	当 WAF 前部署 CDN 时 CDN 识别到的客户端 IP	当 WAF 前部署 CDN 时，此字段记录的为 CDN 节点识别到的真实客户端 IP。 须知 部分 CDN 厂商可能使用其他字段，WAF 仅记录最常见的字段。
access_log.x_real_ip	string	当 WAF 前部署代理时，真实的客户端 IP	代理节点识别到的真实客户端 IP。
access_log.intel_crawler	string	用于情报反爬虫分析	-
access_log.ssl_ciphers_md5	string	标识 ssl_ciphers 的 md5 值	-
access_log.ssl_cipher	string	标识使用的 ssl_cipher	-
access_log.web_tag	string	标识网站名称	-
access_log.user_agent	string	标识请求 header 中的 user-agent	-
access_log.upstream_response_length	string	标识后端响应的大小	-
access_log.region_id	string	标识请求所属 Region	-
access_log.enterprise_project_id	string	标识请求域名所属企业项目 ID	-

字段	类型	字段说明	描述
access_log.referer	string	标识请求头中的 Referer 内容	最大长度为 128 字符，大于 128 字符会被截断。
access_log.rule	string	标识请求命中的规则	命中多条规则此处也只会显示一条。
access_log.category	string	标识请求命中的日志分类	-
access_log.waf_time	string	访问请求的时间	-

WAF 攻击日志 attack_log 字段说明

字段	类型	字段说明	描述
attack_log.category	string	日志分类	值为“attack”。
attack_log.time	string	日志时间	-
attack_log.time_iso8601	string	日志的 ISO 8601 格式时间	-
attack_log.policy_id	string	防护策略 ID	-
attack_log.level	string	防护策略层级	表示 Web 基础防护策略级别。 <ul style="list-style-type: none"> • 1: 宽松 • 2: 中等 • 3: 严格

字段	类型	字段说明	描述
attack_log.attack	string	发生攻击的类型	<p>发生攻击的类型，仅在攻击日志中出现。</p> <ul style="list-style-type: none"> • default: 默认 • sqli: SQL 注入攻击 • xss: 跨站脚本攻击 • webshell: WebShell 攻击 • robot: 恶意爬虫 • cmdi: 命令注入攻击 • rfi: 远程文件包含 • lfi: 本地文件包含 • illegal: 非法请求 • vuln: 漏洞攻击 • cc: 命中 CC 防护规则 • custom_custom: 命中精准防护规则 • custom_whiteblackip: 命中 IP 黑白名单规则 • custom_geoip: 命中地理位置控制规则 • antitamper: 命中网页防篡改规则 • anticrawler: 命中 JS 挑战反爬虫规则 • leakage: 命中敏感信息泄露规则 • antiscan_high_freq_scan: 防扫描-高频扫描攻击。 • followed_action: 攻击惩罚。
attack_log.action	string	防护动作	<p>WAF 防护攻击动作。</p> <ul style="list-style-type: none"> • block: 拦截 • log: 仅记录 • captcha: 人机验证
attack_log.sub_type	string	爬虫的子类型	<p>当 attack 为 robot 时，该字段不为空。</p> <ul style="list-style-type: none"> • script_tool: 脚本工具 • search_engine: 搜索引擎 • scanner: 扫描工具 • uncategorized: 其他爬虫
attack_log.rule	string	触发的规则 ID 或者自定义的策略类型描述	-

字段	类型	字段说明	描述
attack_log.rule_name	string	标识自定义的策略类型描述。	命中基础防护规则时该字段为空。
attack_log.location	string	触发恶意负载的位置	-
attack_log.req_body	string	标识请求体	-
attack_log.resp_headers	string	响应头	-
attack_log.hit_data	string	触发恶意负载的字符串	-
attack_log.resp_body	string	响应体	-
attack_log.backend.protocol	string	标识当前后端协议	-
attack_log.backend.alive	string	标识当前后端状态	-
attack_log.backend.port	string	标识当前后端端口	-
attack_log.backend.host	string	标识当前后端 Host 值	-
attack_log.backend.type	string	标识当前后端 Host 类型	IP 或域名
attack_log.backend.weight	number	标识当前后端权重	-
attack_log.status	string	请求的响应状态码	-
attack_log.upstream_status	string	标识请求的源站响应状态码	-
attack_log.reqid	string	随机 ID 标识	由引擎 IP 尾缀、请求时间戳、NGINX 分配的请求 ID 组成。
attack_log.requestid	string	标识请求唯一 ID	NGINX 分配的请求 ID。
attack_log.id	string	攻击 ID	攻击的 ID 标识。
attack_log.method	string	请求方法	-

字段	类型	字段说明	描述
attack_log.sip	string	客户端请求 IP	-
attack_log.sport	string	客户端请求端口	-
attack_log.host	string	请求的服务器域名	-
attack_log.http_host	string	请求的服务器域名	-
attack_log.hport	string	请求的服务器端口	-
attack_log.uri	string	请求 URL	不包括域名。
attack_log.header	json string , decode 后为 json table	请求 header 信息	-
attack_log.multipart	json string , decode 后为 json table	请求 multipart header	用于文件上传。
attack_log.cookie	json string , decode 后为 json table	请求 Cookie 信息	-
attack_log.params	json string , decode 后为 json table	请求 URI 后的参数信息	-
attack_log.body_bytes_sent	string	发送给客户端的响应体字节数	WAF 发送给客户端的响应体字节数。

字段	类型	字段说明	描述
attack_log.upstream_response_time	string	后端服务器从上游服务接收响应内容所经过的时间，单位为秒。	多次请求响应的时间，使用逗号分隔。
attack_log.engine_id	string	引擎的唯一标识	-
attack_log.region_id	string	标识引擎所在 region 的 ID	-
attack_log.engine_ip	string	标识引擎 IP	-
attack_log.process_time	string	引擎的检测用时	-
attack_log.remote_ip	string	标识请求的四层客户端 IP	-
attack_log.x_forwarded_for	string	标识请求头中“X-Forwarded-For”的内容	-
attack_log.cdn_src_ip	string	标识请求头中“Cdn-Src-Ip”的内容	-
attack_log.x_real_ip	string	标识请求头中“X-Real-IP”的内容	-
attack_log.group_id	string	日志组 ID	对接 LTS 服务的日志组 ID。
attack_log.attack_stream_id	string	日志流 ID	与“group_id”相关，是日志组下用户的 access_stream 的 ID。
attack_log.hostid	string	防护域名 ID (upstream_id)	-
attack_log.tenant_id	string	防护域名的租户 ID	-
attack_log.project_id	string	防护域名的项目 ID	-
attack_log.enterprise_project_id	string	标识请求域名所属企业项目 ID	-

字段	类型	字段说明	描述
attack_log.web_tag	string	标识网站名称	-
attack_log.req_body	string	识请求体（超过 1K 记录时会被截断）	-

7

配置防护策略

7.1 防护配置概述

本文介绍 Web 应用防火墙（Web Application Firewall，WAF）服务的防护策略的配置流程以及 WAF 引擎检测机制及规则的检测顺序。

策略配置流程

网站接入 WAF 防护后，您需要为网站配置防护策略。

表 7-1 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。	7.2 配置 Web 基础防护规则防御常见 Web 攻击
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。	7.3 配置 CC 攻击防护规则防御 CC 攻击
精准访问防护规则	精准访问防护策略可对 HTTP 首部、Cookie、访问 URL、请求参数或者客户端 IP 进行条件组合，定制化防护策略，为您的网站带来更精准的防护。	7.4 配置精准访问防护规则定制化防护策略

防护规则	说明	参考文档
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。	7.5 配置 IP 黑白名单规则拦截/放行指定 IP
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。	7.13 配置攻击惩罚标准封禁访问者指定时长
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。	7.6 配置地理位置访问控制规则拦截/放行特定区域请求
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。	7.7 配置网页防篡改规则避免静态网页被篡改
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。	7.8 配置网站反爬虫防护规则防御爬虫攻击
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。	7.9 配置防敏感信息泄露规则避免敏感信息泄露
全局白名单规则	针对特定请求忽略某些攻击检测规则，用于处理误报事件。	7.10 配置全局白名单规则对误报进行忽略
隐私屏蔽规则	隐私信息屏蔽，避免用户的密码等信息出现在事件日志中。	7.11 配置隐私屏蔽规则防隐私信息泄露

WAF 引擎规则检测顺序

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 7-2 所示，自定义规则的检测顺序如图 7-3 所示。

说明

在防护配置页面，勾选“按检测顺序排序”，所有的防护规则将按 WAF 的检测顺序进行重新排序。

图 7-2 WAF 引擎检测图

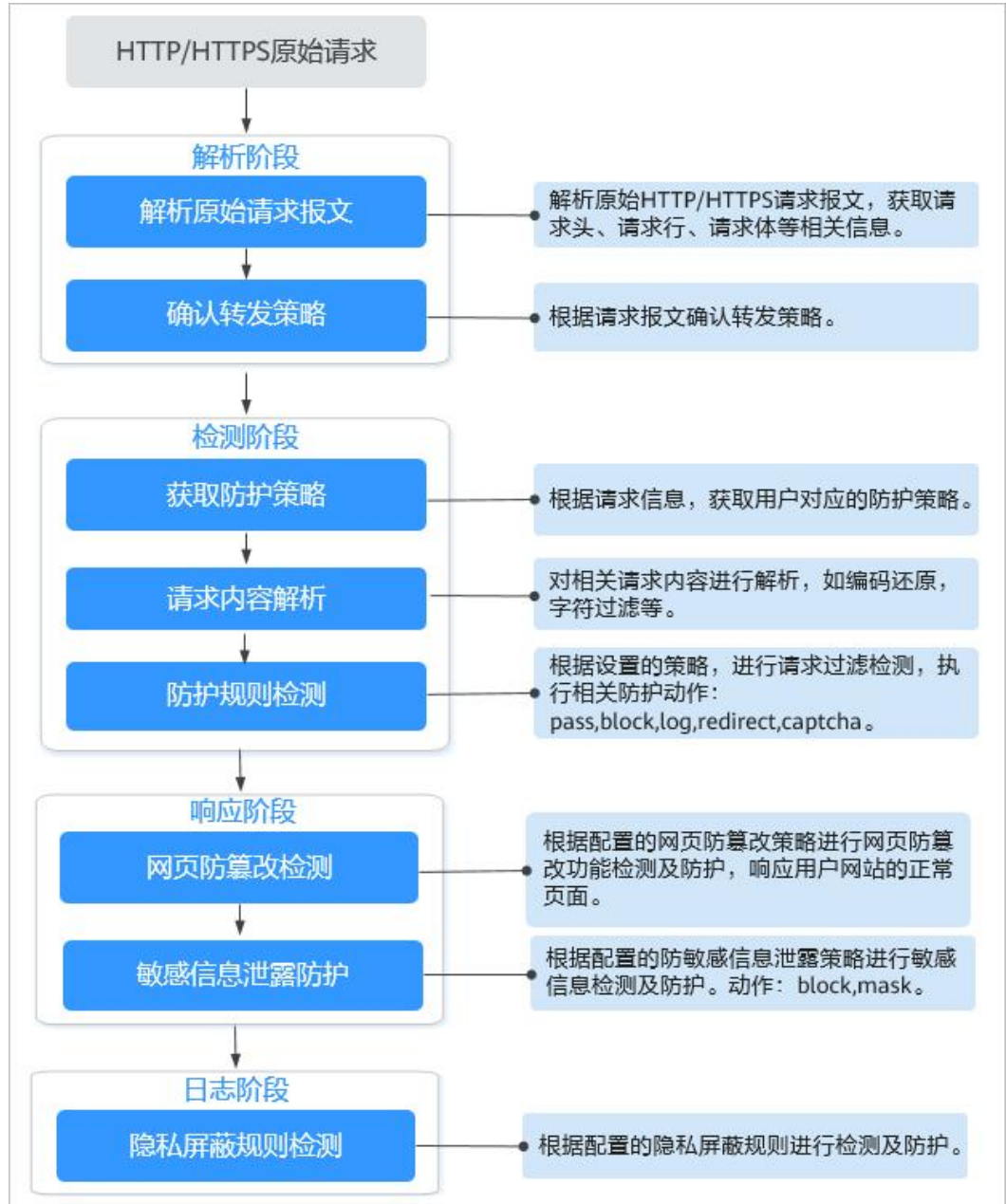


图 7-3 防护规则的检测顺序



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。

7.2 配置 Web 基础防护规则防御常见 Web 攻击

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。

前提条件


已添加防护网站。


约束条件

- Web 基础防护支持“拦截”和“仅记录”模式。
- 当 Web 基础防护设置为“拦截”模式时，您可以 7.13 配置攻击惩罚标准封禁访问者指定时长。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。

开启 Web 基础防护规则

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“Web 基础防护”配置框中，用户可根据自己的需要参照图 7-4 表 7-2 更改 Web 基础防护的“状态”和“模式”。

图 7-4 Web 基础防护配置框

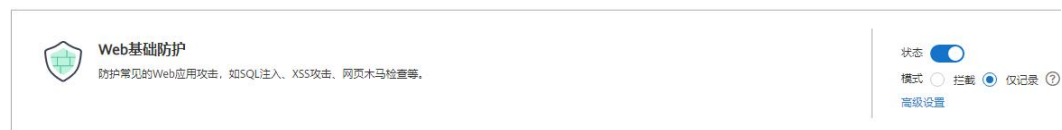




表 7-2 防护动作参数说明

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

参数	说明
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，如图 7-5 所示，检测项说明如 3.表 7-4 所示。

图 7-5 Web 基础防护



1. 防护动作设置。

- 拦截：发现攻击行为后立即阻断并记录。
 设置为“拦截”时，您可以根据需要选择已配置的攻击惩罚。有关配置攻击惩罚的详细操作，请参见 7.13 配置攻击惩罚标准封禁访问者指定时长。
- 仅记录：发现攻击行为后只记录不阻断攻击。

2. 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 7-3 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规则，再开启“严格”模式，使 WAF 能有效防护更多攻击。

3. 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 7-4 开启其他需要防护的检测类型。

表 7-4 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

使用建议

- 如果您对自己的业务流量特征还不完全清楚，建议先切换到“仅记录”模式进行观察。一般情况下，建议您观察一至两周，然后分析仅记录模式下的攻击日志。
 - 如果没有发现任何正常业务流量被拦截的记录，则可以切换到“拦截”模式启用拦截防护。
 - 如果发现攻击日志中存在正常业务流量，建议调整防护等级或者设置全局白名单来避免正常业务的误拦截。
- 业务操作方面应注意以下问题：

- 正常业务的 HTTP 请求中尽量不要直接传递原始的 SQL 语句、JavaScript 代码。
- 正常业务的 URL 尽量不要使用一些特殊的关键字（UPDATE、SET 等）作为路径，例如：“https://www.example.com/abc/update/mod.php?set=1”。
- 如果业务中需要上传文件，不建议直接通过 Web 方式上传超过 50M 的文件，建议使用对象存储服务或者其他方式上传。

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 5.1.2 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。

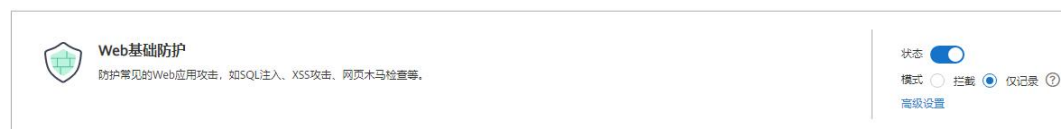
---结束

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。

图 7-6 Web 基础防护配置框



- 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 7-7 所示。

图 7-7 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

7.3 配置 CC 攻击防护规则防御 CC 攻击

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源端的访问频率，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。

CC 攻击防护规则可以添加引用表，引用表防护规则对所有防护域名都生效，即所有防护域名都可以使用 CC 攻击防护规则的引用表。

前提条件


已添加防护网站。


约束条件

- 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 7.12 创建引用表对防护指标进行批量配置。
- 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。

配置 CC 攻击防护规则

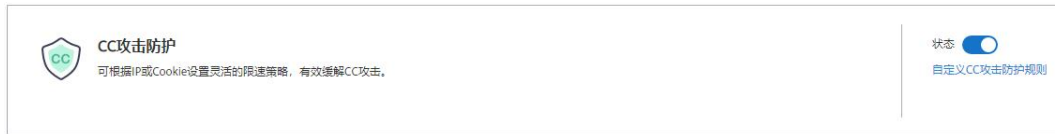
步骤 1 登录管理控制台。

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 (独享版)”。

- 步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。
- 步骤 5 单击目标策略名称，进入目标策略的防护配置页面。
- 步骤 6 在“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。

图 7-8 CC 防护规则配置框



- 步骤 7 在“CC 攻击防护”规则配置列表左上方，单击“添加规则”。
- 步骤 8 在弹出的对话框中，根据图 7-9 表 7-5 配置 CC 防护规则。

图 7-9 添加 CC 防护规则



表 7-5 CC 防护规则参数说明

参数	参数说明	取值样例
规则描述	可选参数，设置该规则的备注信息。	--

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>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：如果用户不希望访问者从“www.test.com”访问网站，则“Referer”对应的“内容”设置为“http://www.test.com”。</p>	--
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，那么可以用 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

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 • 子字段：当“字段”选择 IPv4、IPv6、Cookie、Header、Params 时，请根据实际需求配置子字段。 <p>须知</p> <p>子字段的长度不能超过 2048 字节。</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> <p>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 7.12 创建引用表对防护指标进行批量配置。</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/”
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
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。人机验证目前支持英文。 • 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。 	阻断

参数	参数说明	取值样例
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</p> <p>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，需要设置该参数，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
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。	<p>不同页面类型对应的页面内容样式：</p> <ul style="list-style-type: none"> text/html: <pre><html><body>Forbidden</body></html></pre> application/json: <pre>{"msg": "Forbidden"}</pre> text/xml: <pre><?xml version="1.0" encoding="utf-8"?><error> <msg>Forbidden </msg></error></pre>

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”，如果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”。

- 如果需要修改添加的 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。
- 如果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”，且配置了如 步骤 8 图 7-9 所示“阻断”防护动作的 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 5.1.2 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；60 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。

---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。

图 7-10 添加“人机验证”防护规则

添加CC防护规则

* 用户标识

当不存在这个字段时，不参与计数；当字段存在但内容为空时，会参与计数

* 限速条件

字段	子字段	逻辑	内容
IPv4	客户端IP	等于	<input type="text"/>

[添加引用表](#)

+ 添加 您还可以添加29项条件。(多个条件同时成立才生效)

* 限速速率 次 秒

* 防护动作 人机验证 阻断 动态阻断 仅记录

* 生效时间 立即生效

步骤 2 开启 CC 攻击防护。

图 7-11 CC 防护规则配置框

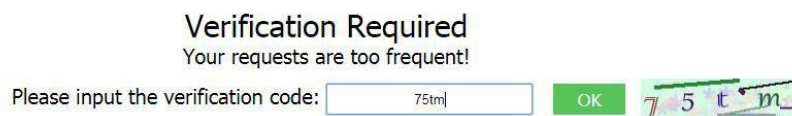
CC攻击防护

可根据IP或Cookie设置灵活的限速策略，有效缓解CC攻击。

状态 自定义CC攻击防护规则

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

7.4 配置精准访问防护规则定制化防护策略

精准访问防护规则可对常见的 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。

精准访问防护规则可以添加引用表，引用表防护规则对所有防护域名都生效，即所有防护域名都可以使用精准防护规则的引用表。

前提条件

已添加防护网站。

约束条件


- 当精准访问防护规则的“防护动作”设置为“阻断”时，您可以 7.13 配置攻击惩罚标准封禁访问者指定时长。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。
- 配置的“路径”的“内容”不能包含特殊字符（<>*）。
- 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。


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。

配置精准访问防护规则

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，选择区域或项目。

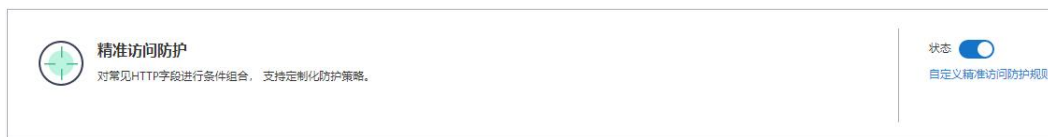
步骤 3 单击页面左上方的，选择“安全 > Web 应用防火墙 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“精准访问防护”配置框中，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。

图 7-12 精准访问防护配置框



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”规则配置列表左上方，单击“添加规则”。

步骤 9 在弹出的对话框中，根据图 7-13 表 7-6 添加精准访问防护规则。

以图 7-13 的配置为例，其含义为：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。

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”。

图 7-13 添加精准访问防护规则

添加精准访问防护规则

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

规则描述

* 条件列表

字段	子字段	逻辑	内容
路径	--	包含	/admin

[添加引用表](#)

[添加](#) 您还可以添加29项条件。(多个条件同时成立，才执行防护动作)

* 防护动作

* 攻击惩罚

* 优先级 值越小，优先级越高

* 生效时间 立即生效 自定义

表 7-6 规则参数说明

参数	参数说明	取值样例
规则描述	可选参数，设置该规则的备注信息。	--

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。 • 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 7.12 创建引用表对防护指标进行批量配置。 • “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。 • 内容：输入或者选择条件匹配的内容。 <p>说明</p> <p>具体的配置请参见 表 7-17。</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”
防护动作	<ul style="list-style-type: none"> • 阻断：表示拦截命中规则的请求，并向发起请求的客户端返回拦截响应页面。WAF 默认使用统一的拦截响应页面，您也可以自定义拦截响应页面。 • 放行：表示不拦截命中规则的请求，直接放行。 • 仅记录：表示不拦截命中规则的请求，只通过日志记录请求命中了规则。您可以通过 WAF 日志，查询命中当前规则请求，分析规则的防护效果。例如，是否有误拦截等。 	“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
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> <p>须知</p> <p>如果多条精准访问控制规则的优先级取值相同，则 WAF 将根据添加防护规则的先后顺序进行排序匹配。</p>	5
生效模式	<p>用户可以选择“立即生效”或者自定义设置生效时间段。</p> <p>自定义设置的时间只能为将来的某一时间段。</p>	“立即生效”

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”，如果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”。
- 如果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。
- 如果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”，且配置了如 步骤 9 图 7-13 所示的精准访问防护规则。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 5.1.2 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。

---结束

配置示例-拦截特定的攻击请求

通过分析某类特定的 WordPress 反弹攻击，发现其特征是 User-Agent 字段都包含 WordPress，如图 7-14 所示。

图 7-14 WordPress 反弹攻击

UA
WordPress/4.2.10; http://[redacted].s.vn; verifying pingback from [redacted] 249.54
WordPress/4.0.1; http://[redacted]:90; verifying pingback from [redacted] 249.54
WordPress/4.6.1; https://[redacted].sabt.com; verifying pingback from [redacted] 249.54
WordPress/4.5.3; http://[redacted].lib.umd.edu; verifying pingback from [redacted] 9.54
WordPress/3.5.1; http://[redacted].o.com
WordPress/4.2.4; http://[redacted].t.tw; verifying pingback from [redacted] 249.54
WordPress/4.6.1; http://[redacted].om; verifying pingback from [redacted] 249.54

因此，可以设置精准访问控制规则，拦截该类 WordPress 反弹攻击请求。

图 7-15 User Agent 配置

* 防护动作	阻断								
* 生效时间	<input checked="" type="radio"/> 立即生效 <input type="radio"/> 自定义								
* 条件列表	<table border="1"><thead><tr><th>字段</th><th>子字段</th><th>逻辑</th><th>内容</th></tr></thead><tbody><tr><td>User Agent</td><td>--</td><td>包含</td><td>WordPress</td></tr></tbody></table>	字段	子字段	逻辑	内容	User Agent	--	包含	WordPress
字段	子字段	逻辑	内容						
User Agent	--	包含	WordPress						

配置示例-拦截特定的 URL 请求

如果您遇到有大量 IP 在访问某个特定且不存在的 URL，您可以通过配置以下精准访问防护规则直接阻断所有该类请求，降低源站服务器的资源消耗，如图 7-16 所示。

图 7-16 特定的 URL 拦截

添加精准访问防护规则

不同模式使用限制和注意事项 [?](#)

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容
路径	--	包含	/XXXX

[添加引用表](#)

[+](#) 添加 您还可以添加29项条件。(多个条件同时成立，才执行防护动作)

* 防护动作

配置示例-拦截字段为空值的请求

如果您需要拦截某个为空值的字段，您可以通过配置精准访问防护规则直接阻断该类请求，如图 7-17 所示。

图 7-17 Referer 空值拦截

添加精准访问防护规则

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 生效时间 立即生效 自定义

* 条件列表

字段	子字段	逻辑	内容
Header	自定义	referer	不存在

[添加引用表](#)

[+](#) 添加 您还可以添加29项条件。(多个条件同时成立，才执行防护动作)

* 防护动作

* 攻击惩罚

* 优先级 值越小，优先级越高

配置示例-拦截指定文件类型（zip、tar、docx 等）

通过配置路径字段匹配的文件类型，您可以阻断特定的文件类型。例如，您需要拦截“.zip”格式文件，您可以配置精准防护规则阻断“.zip”文件类型访问请求，如图 7-18 所示。

图 7-18 阻断特定文件类型请求

添加精准访问防护规则

不同模式使用限制和注意事项 ?

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容
路径	--	后缀为	zip

+ 添加 您还可以添加29项条件。（多个条件同时成立，才执行防护动作）

* 防护动作

配置示例-防盗链

通过配置 Referer 匹配字段的访问控制规则，您可以阻断特定网站的盗链。例如，您发现“https://abc.blog.com”大量盗用本站的图片，您可以配置精准访问防护规则阻断相关访问请求。

图 7-19 防盗链

添加精准访问防护规则

不同模式使用限制和注意事项 ?

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称

规则描述

* 条件列表

字段	子字段	逻辑	内容
Referer	--	包含	https://abc.blog.com

+ 添加 您还可以添加29项条件。（多个条件同时成立，才执行防护动作）

* 防护动作

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，如图 7-20 所示，一条单独放行指定 IP 的访问，如图 7-21 所示。

图 7-20 阻断所有的请求

添加精准访问防护规则

不同模式使用限制和注意事项 ?

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称: waftest

规则描述:

* 条件列表

字段	子字段	逻辑	内容
路径	--	包含	/

+ 添加 您还可以添加29项条件。(多个条件同时成立，才执行防护动作)

* 防护动作: 阻断

图 7-21 放行指定 IP

添加精准访问防护规则

不同模式使用限制和注意事项 ?

下面条件同时满足，此规则生效，一条规则最多支持30个条件。

* 规则名称: waftest

规则描述:

* 条件列表

字段	子字段	逻辑	内容
IPv4	客户端IP	等于	192.168.2.3

+ 添加 您还可以添加29项条件。(多个条件同时成立，才执行防护动作)

* 防护动作: 放行

配置示例-放行指定 IP 的特定 URL 请求

通过配置多条“条件列表”，当访问请求同时满足条件列表时，可以实现放行指定 IP 的特定 URL 请求，如图 7-22 所示。

图 7-22 放行指定 IP 访问特定路径

添加精准访问防护规则

不同模式使用限制和注意事项 ⓘ

下面条件同时满足，此规则生效。一条规则最多支持30个条件。

* 规则名称: waftest

规则描述:

* 条件列表

字段	子字段	逻辑	内容	
IPv4	客户端IP	等于	192.168.2.3	删除
路径	--	包含	/admin	删除

添加 您还可以添加28项条件。(多个条件同时成立，才执行防护动作)

* 防护动作: 放行

7.5 配置 IP 黑白名单规则拦截/放行指定 IP

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，白名单规则优先级高于黑名单规则。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 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，请添加地址组，详细操作请参见 12.212.2.1 添加黑白名单 IP 地址组。
- WAF 黑白名单规则不支持配置 0.0.0.0/0 IP 地址段，且白名单规则优先级高于黑名单规则。如果您需要放行某个网段指定的 IP 并拦截某个网段其他所有 IP，请先添加黑名单规则，拦截该网段的所有 IP，然后添加白名单规则，放行指定 IP。
- 当黑白名单规则的“防护动作”设置为“拦截”时，您可以 7.13 配置攻击惩罚标准封禁访问者指定时长，但攻击惩罚的“拦截类型”不支持选择“长时间 IP 拦截”和“短时间 IP 拦截”。配置攻击惩罚后，如果访问者的 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。
- 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。


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。

配置 IP 黑白名单规则

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，选择区域或项目。

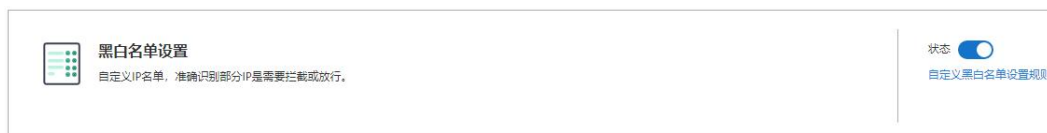
步骤 3 单击页面左上方的，选择“安全 > Web 应用防火墙 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“黑白名单设置”配置框中，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。

图 7-23 黑白名单配置框



步骤 7 在“黑白名单设置”配置列表的左上方，单击“添加规则”。

步骤 8 在弹出的对话框中，添加黑白名单规则，参数说明如 图 7-24 表 7-7 所示。

说明

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

图 7-24 添加黑白名单规则

表 7-7 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。	wafest
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 地址或 IP 地址段	<p>当“IP/IP 段或地址组”选择“IP/IP 段”时需要设置该参数。</p> <p>支持 IPv4 和 IPv6 格式的 IP 地址或 IP 地址段。</p> <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。 	<ul style="list-style-type: none"> IPv4 格式： <ul style="list-style-type: none"> 192.168.2.3 10.1.1.0/24 IPv6 格式： <ul style="list-style-type: none"> fe80:0000:0000:0000:0000:0000:0000:0000

参数	参数说明	取值样例
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 12.212.2.1 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	<p>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 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。</p> <p>说明 不支持选择“长时间 IP 拦截”和“短时间 IP 拦截”。</p>	长时间 Cookie 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”，如果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”。
- 如果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。
- 如果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

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 5.1.2 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 参照配置 IP 黑白名单规则，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。

---结束

配置示例-放行指定 IP

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放行指定 IP 防护效果。

- 步骤 1 添加以下 2 条黑白名单规则，拦截所有来源 IP。

图 7-25 拦截 1.0.0.0/1 IP 地址段

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

- 规则名称 (Rule Name): all01
- IP/IP段或地址组 (IP/IP Range or Address Group): IP/IP段 (selected), 地址组 (Address Group)
- IP/IP段 (IP/IP Range): 1.0.0.0/1
- 防护动作 (Protection Action): 拦截 (Intercept)
- 攻击惩罚 (Attack Penalty): 无攻击惩罚 (No Attack Penalty)
- 规则描述 (Rule Description): (empty field)

At the bottom, there are two buttons: 确认 (Confirm) and 取消 (Cancel).

图 7-26 拦截 128.0.0.0/1 IP 地址段

The screenshot shows a configuration window titled "添加黑白名单设置规则" (Add Whitelist Rule). It contains the following fields and options:

- 规则名称 (Rule Name): all02
- IP/IP段或地址组 (IP/Segment or Address Group): IP/IP段 (selected), 地址组 (Address Group)
- IP/IP段 (IP/Segment): 128.0.0.0/1
- 防护动作 (Protection Action): 拦截 (Intercept)
- 攻击惩罚 (Attack Penalty): 无攻击惩罚 (No Attack Penalty)
- 规则描述 (Rule Description): (empty)

Buttons at the bottom: 确认 (Confirm) and 取消 (Cancel).

您也可以通过添加一条精准访问防护规则，拦截所有访问请求，如图 7-27 所示。

图 7-27 拦截所有访问请求

The screenshot shows a configuration window titled "添加精准访问防护规则" (Add Precise Access Protection Rule). It contains the following fields and options:

- 规则名称 (Rule Name): waftest
- 规则描述 (Rule Description): (empty)
- 条件列表 (Conditions List):

字段 (Field)	子字段 (Sub-field)	逻辑 (Logic)	内容 (Content)
路径 (Path)	-	包含 (Contains)	/
- 防护动作 (Protection Action): 阻断 (Block)

Buttons at the bottom: 添加 (Add), 删除 (Delete), 重置 (Reset), 取消 (Cancel).

有关配置精准访问防护规则的详细介绍，请参见 7.4 配置精准访问防护规则定制化防护策略。

步骤 2 参照图 7-28 示例添加黑白名单规则，放行指定 IP，例如，XXX.XXX.2.3。

图 7-28 放行指定 IP



The screenshot shows a dialog box titled "添加黑白名单设置规则" (Add Whitelist Rule). It contains the following fields and controls:

- * 规则名称** (Rule Name): A text input field containing "fx001".
- * IP/IP段或地址组** (IP/IP Range or Address Group): Two radio buttons, "IP/IP段" (selected) and "地址组" (Address Group).
- * IP/IP段** (IP/IP Range): A text input field containing "3".
- * 防护动作** (Protection Action): A dropdown menu with "放行" (Allow) selected.
- 规则描述** (Rule Description): An empty text input field.
- At the bottom, there are two buttons: "确认" (Confirm) in red and "取消" (Cancel) in white.

步骤 3 开启黑白名单防护规则。

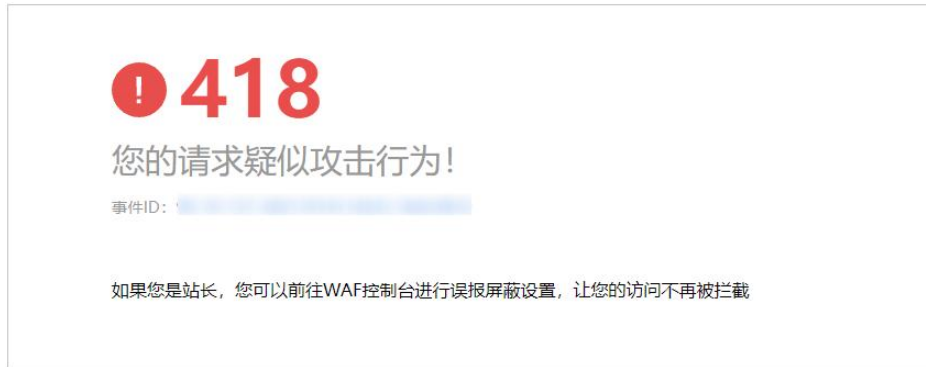
图 7-29 黑白名单配置框



步骤 4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当访问者的源 IP 不属于步骤 2 中设置的放行 IP 地址时，WAF 将拦截该访问请求，拦截页面示例如图 7-30 所示。

图 7-30 WAF 拦截攻击请求



步骤 5 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

7.6 配置地理位置访问控制规则拦截/放行特定区域请求

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。

配置地理位置访问防护规则

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的🏠，选择区域或项目。

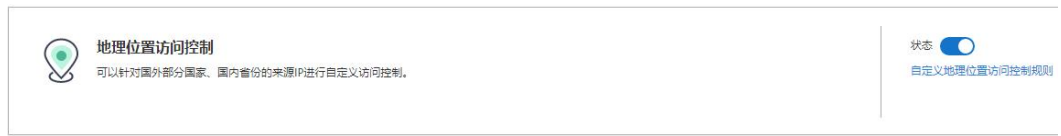
步骤 3 单击页面左上方的☰，选择“安全 > Web 应用防火墙 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“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。

图 7-31 地理位置访问控制配置框



步骤 7 在“地理位置访问控制”配置列表的左上方，单击“添加规则”。

步骤 8 在弹出的对话框中，添加地理位置访问控制规则，如图 7-32 所示，根据图 7-32 表 7-8 配置参数。

图 7-32 添加地理位置访问控制规则

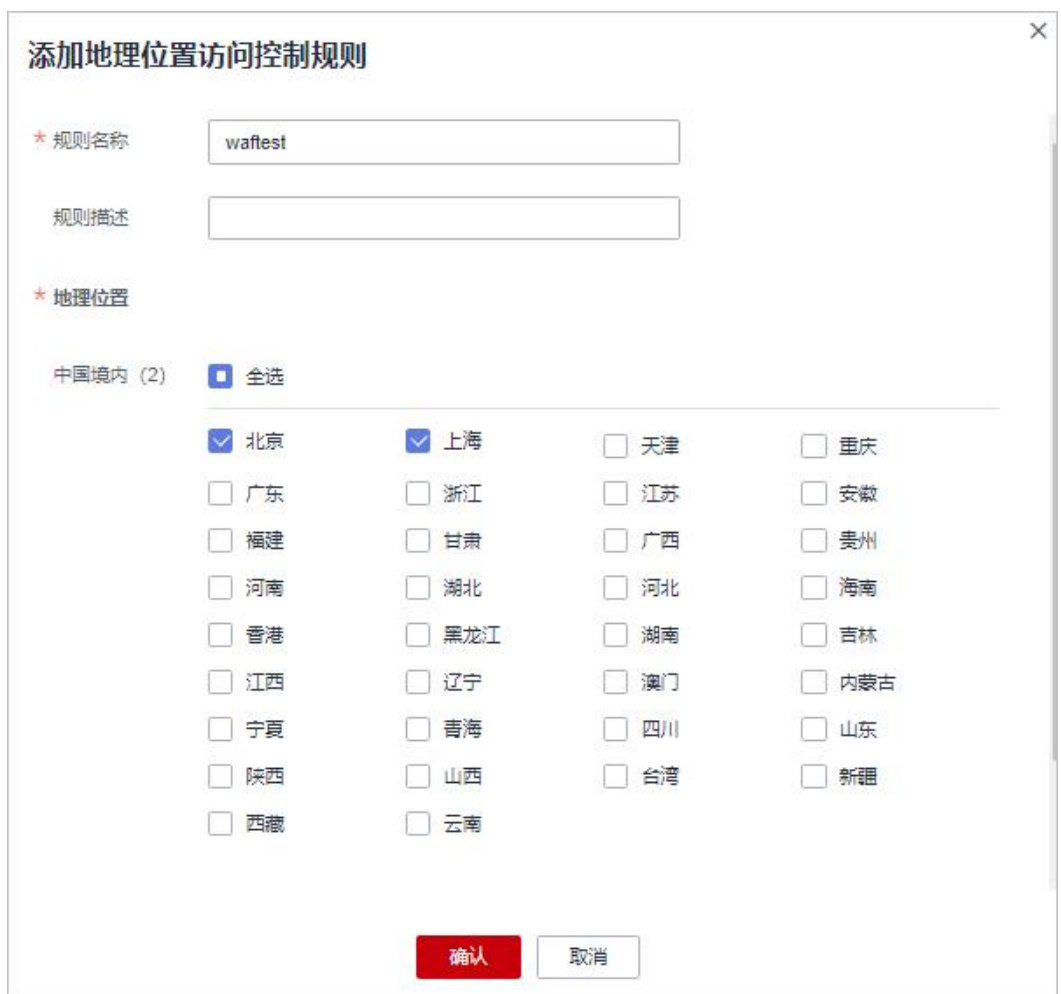


表 7-8 添加地理位置访问控制规则参数说明

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。	waf

参数	参数说明	取值样例
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，可以选择“中国境内”和“中国境外”地区。	-
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”，如果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”。
- 如果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。
- 如果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

配置示例-仅允许某一地区来源 IP 访问请求

假如防护域名“www.example.com”已接入 WAF，当您只允许某一地区的 IP 可以访问防护域名，例如，只允许来源“上海”地区的 IP 可以访问防护域名，请参照以下步骤处理。

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

图 7-33 添加“放行”防护动作

添加地理位置访问控制规则

* 地理位置

中国境内 (1) 全选

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

中国境外 (0)

* 防护动作

步骤 2 开启地理位置访问控制。

图 7-34 地理位置访问控制配置框

地理位置访问控制

可以针对国外部分国家、国内省份的来源IP进行自定义访问控制。

状态 自定义地理位置访问控制规则

步骤 3 配置一条精准访问防护规则，拦截所有的请求。

图 7-35 拦截所有访问请求



步骤 4 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

当非“上海”地区的源 IP 访问页面时，WAF 将拦截该访问请求，拦截页面示例如图 7-36 所示。

图 7-36 WAF 拦截攻击请求



步骤 5 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，您可以查看到非“上海”地区的源 IP 都被拦截。

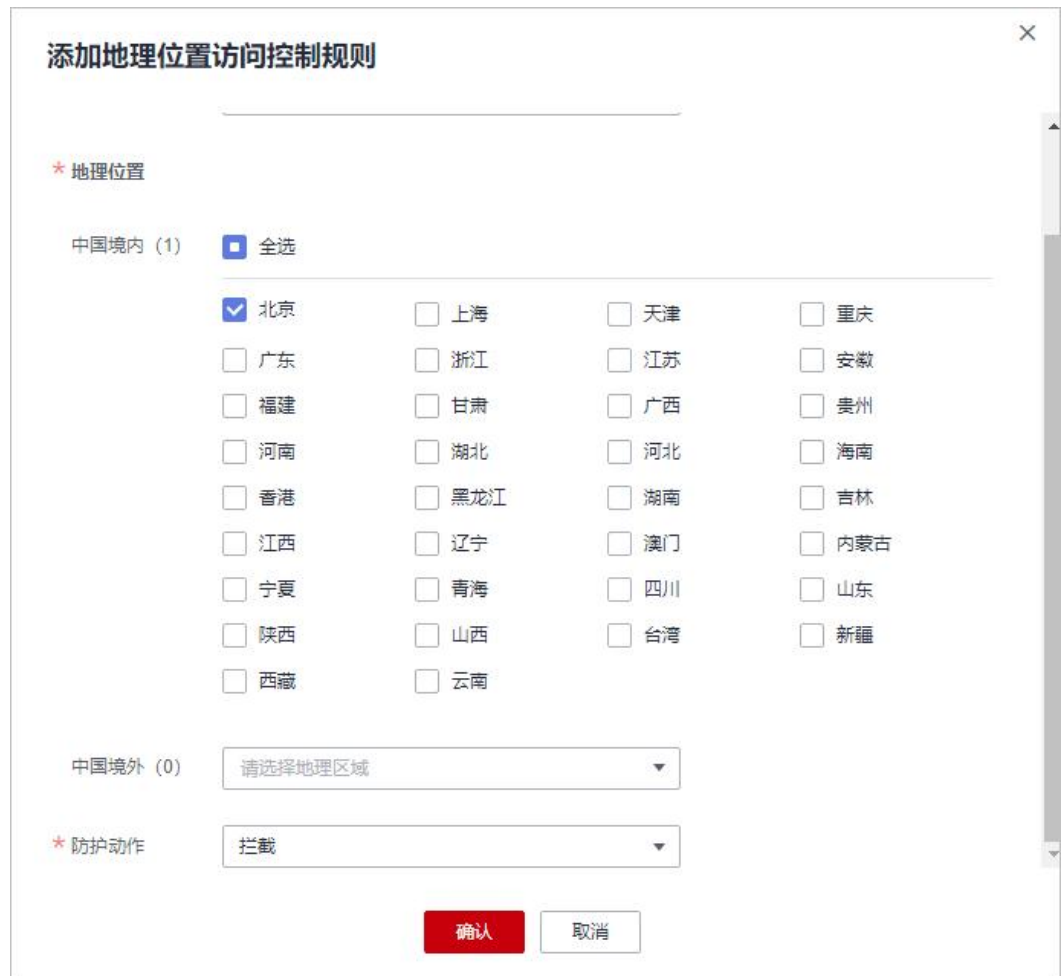
---结束

配置示例-拦截某一地区来源 IP 访问请求

假如防护域名“www.example.com”已接入 WAF，您需要拦截所有来源“北京”地区的 IP 访问防护域名，可以参照以下操作步骤验证防护效果。

步骤 1 添加一条地理位置访问控制规则，设置“北京”地区“拦截”动作。

图 7-37 拦截某一地区访问请求



步骤 2 开启地理位置访问控制。

图 7-38 地理位置访问控制配置框



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

当“北京”地区的源 IP 访问页面时，WAF 将拦截该访问请求，拦截页面示例如图 7-39 所示。

图 7-39 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。

图 7-40 查看防护事件-拦截某一地区 IP 访问请求

时间	源IP	地理位置	防护域名	URL	恶意负载	事件类型	防护动作	操作
2021/11/19 15:24:37 GMT...	[REDACTED]	北京	www.example.com	/		地理访问控制	拦截	详情 误报处理
2021/11/19 15:24:37 GMT...	[REDACTED]	北京	www.example.com	/		地理访问控制	拦截	详情 误报处理
2021/11/19 01:13:22 GMT...	[REDACTED]	北京	www.example.com	/		地理访问控制	拦截	详情 误报处理
2021/11/19 00:19:23 GMT...	[REDACTED]	北京	www.example.com	/		地理访问控制	拦截	详情 误报处理
2021/11/19 00:19:22 GMT...	[REDACTED]	北京	www.example.com	/		地理访问控制	拦截	详情 误报处理

---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 5.1.2 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** 参照配置地理位置访问防护规则，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。

---结束

7.7 配置网页防篡改规则避免静态网页被篡改

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。
即如果请求中 `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

已添加防护网站或已 1010.1 新增防护策略。

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。

配置网页防篡改规则

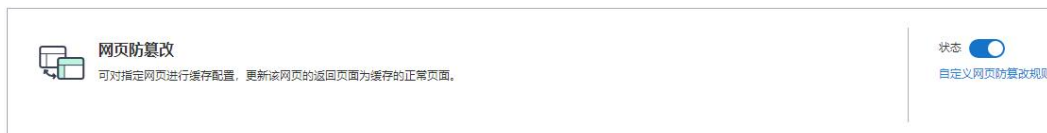
步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

- 步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。
- 步骤 5 单击目标策略名称，进入目标策略的防护配置页面。
- 步骤 6 在“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。

图 7-41 网页防篡改配置框



- 步骤 7 在“网页防篡改”规则配置列表的左上方，单击“添加规则”。
- 步骤 8 在弹出的对话框中，添加网页防篡改规则，参数说明如图 7-42 表 7-9 所示。

图 7-42 添加网页防篡改规则



表 7-9 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

参数	参数说明	取值样例
路径	<p>设置防篡改的 URL 链接中的路径（不包含域名）。</p> <p>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]。</p> <p>例如，URL 为 “http://www.example.com/admin”，则“路径”设置为 “/admin”。</p> <p>说明</p> <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”，如果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”。
- 如果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。
- 如果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，需要防止“/admin”静态页面被篡改，您可以参照以下操作步骤验证防护效果。

步骤 1 添加一条网页防篡改规则。

图 7-43 添加网页防篡改规则



添加网页防篡改规则

* 域名

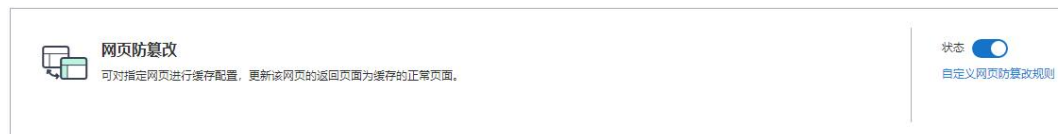
* 路径

规则描述

确认添加 取消

步骤 2 开启网页防篡改。

图 7-44 网页防篡改配置框



步骤 3 模拟篡改“http://www.example.com/admin”网页。

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

7.8 配置网站反爬虫防护规则防御爬虫攻击

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，以及自定义 JS 脚本反爬虫防护规则。

前提条件

已添加防护网站。

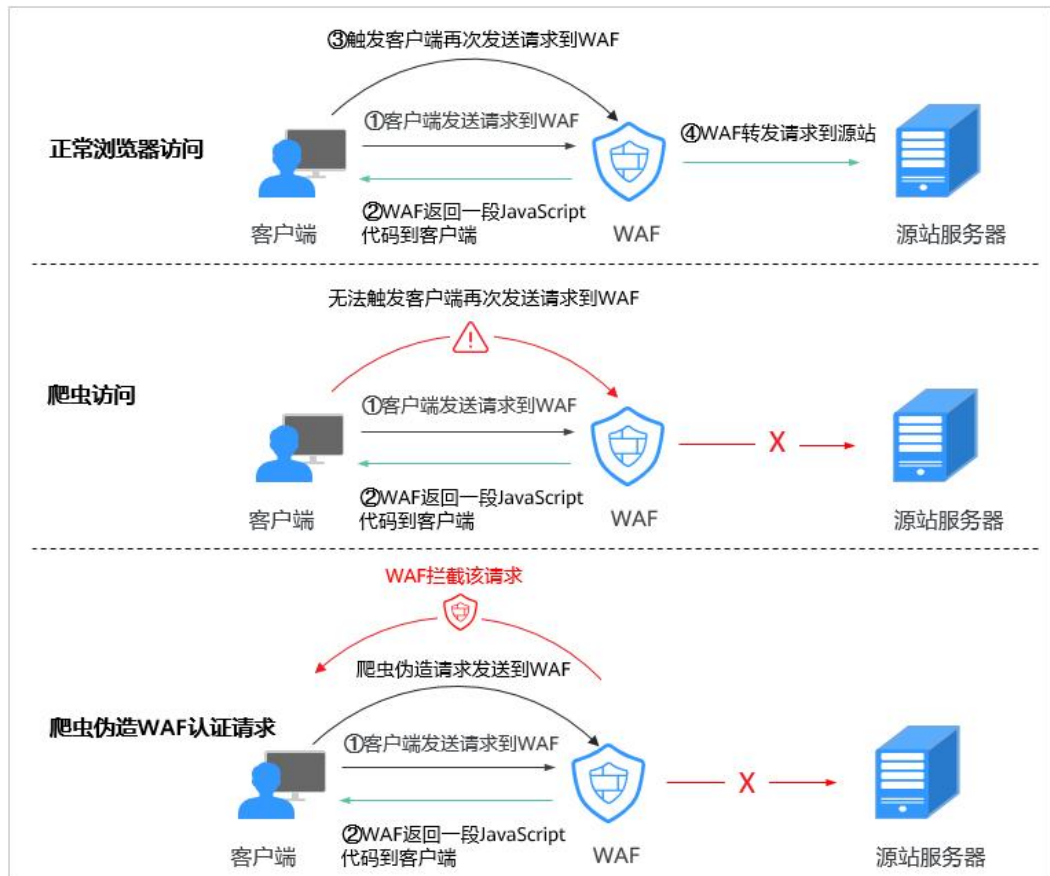
约束条件

- JS 脚本反爬虫依赖浏览器的 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，开启后会造成永远无法访问源站。
- 如果您的业务接入了 CDN 服务，请谨慎使用 JS 脚本反爬虫。
由于 CDN 缓存机制的影响，JS 脚本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。
- 网站反爬虫“js 挑战”和“js 验证”的防护动作默认为“仅记录”，WAF 不支持手动配置“js 挑战”和“js 验证”的防护动作。
- WAF 的 JS 脚本反爬虫功能只支持 get 请求，不支持 post 请求。

JS 脚本反爬虫检测机制

JS 脚本检测流程如图 7-45 所示，其中，①和②称为“js 挑战”，③称为“js 验证”。

图 7-45 JS 脚本检测流程说明



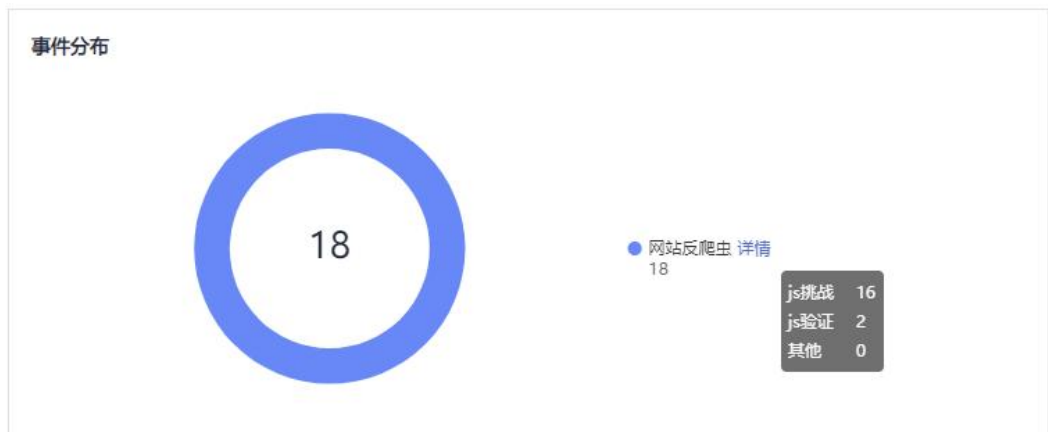
开启 JS 脚本反爬虫后，当客户端发送请求时，WAF 会返回一段 JavaScript 代码到客户端。

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

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

通过统计“js 挑战”和“js 验证”，就可以汇总出 JS 脚本反爬虫防御的请求次数。例如，图 7-46 中 JS 脚本反爬虫共记录了 18 次事件，其中，“js 挑战”（WAF 返回 JS 代码）为 16 次，“js 验证”（WAF 完成 JS 验证）为 2 次，“其他”（即爬虫伪造 WAF 认证请求）为 0 次。

图 7-46 JS 脚本反爬虫防护数据



须知

“js 挑战”和“js 验证”的防护动作为仅记录，WAF 不支持配置“js 挑战”和“js 验证”的防护动作。

配置网站反爬虫防护规则

- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的📍，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 (独享版)”。
- 步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。
- 步骤 5 单击目标策略名称，进入目标策略的防护配置页面。
- 步骤 6 在“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。

图 7-47 网站反爬虫配置框



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，如 图 7-48 所示，检测项说明如 图 7-48 表 7-10 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。

图 7-48 特征反爬虫防护

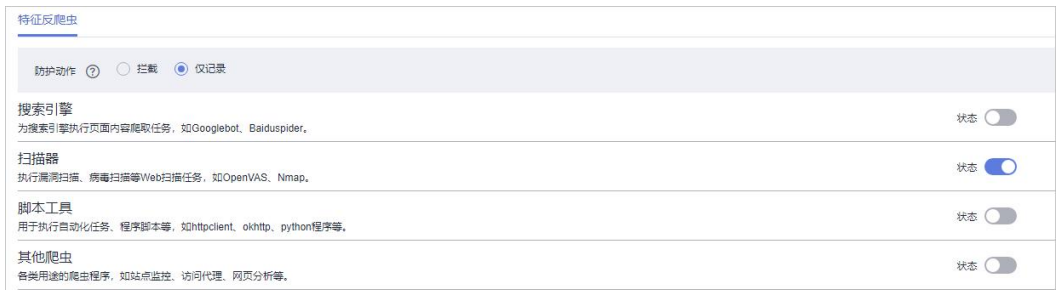




表 7-10 特征反爬虫检测项说明

检测项	说明	功能说明
-----	----	------

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，如果您希望拦截百度爬虫的 POST 请求，可参照 配置示例-搜索引擎 进行配置。
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。

步骤 8 选择“JS 脚本反爬虫”页签，用户可根据业务需求更改 JS 脚本反爬虫的“状态”。

默认关闭 JS 脚本反爬虫，单击 ，在弹出的“警告”提示框中，单击“确定”，开启 JS 脚本反爬虫 。

须知

- JS 脚本反爬虫依赖浏览器的 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，开启后会造成永远无法访问源站。
- 如果您的业务接入了 CDN 服务，请谨慎使用 JS 脚本反爬虫。

由于 CDN 缓存机制的影响，JS 脚本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。

步骤 9 根据业务配置 JS 脚本反爬虫规则，相关参数说明如 图 7-50 表 7-11 所示。

JS 脚本反爬虫规则提供了“防护所有请求”和“防护指定请求”两种防护动作。

- 除了指定路径以外，防护其他所有路径
“防护模式”选择“防护所有请求”，单击“添加排除请求规则”，配置防护路径后，单击“确认”。

图 7-49 添加排除请求规则

不同模式使用限制和注意事项 ?

* 规则名称

* 路径

* 逻辑

规则描述

* 生效时间 立即生效

确认 取消

- 只防护指定路径时
“防护模式”选择“防护指定请求”，单击“添加请求规则”，配置防护路径后，单击“确认”。

图 7-50 添加请求规则

不同模式使用限制和注意事项 ?

* 规则名称

* 路径

* 逻辑

规则描述

* 生效时间 立即生效

确认 取消

表 7-11 JS 脚本反爬虫防护规则参数说明

参数	参数说明	示例
----	------	----

参数	参数说明	示例
规则名称	自定义规则名称。	wafjs
路径	设置 JS 脚本反爬虫的 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
逻辑	在“逻辑”下拉列表中选择需要的逻辑关系。	包含
规则描述	规则备注信息。	-

---结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，如果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”。
- 如果需要修改添加的 JS 脚本反爬虫规则，可单击待修改的路径规则所在行的“修改”，修改该规则。
- 如果需要删除添加的 JS 脚本反爬虫规则时，可单击待删除的路径规则所在行的“删除”，删除该规则。

配置示例-仅记录脚本工具爬虫

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反爬虫防护效果。

步骤 1 执行 JS 脚本工具，爬取网页内容。

步骤 2 在“特征反爬虫”页签，开启“脚本工具”，“防护动作”设置为“仅记录”（WAF 检测为攻击行为后，只记录不阻断）。

图 7-51 开启“脚本工具”



步骤 3 开启网站反爬虫。

图 7-52 网站反爬虫配置框




步骤 4 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

配置示例-搜索引擎

放行百度或者谷歌的搜索引擎，同时拦截百度的 POST 请求。

步骤 1 参照步骤 6 将“搜索引擎”设置为放行，即将“搜索引擎”的“状态”设置为 。

步骤 2 参照 7.4 配置精准访问防护规则定制化防护策略配置如图 7-53 的规则。

图 7-53 拦截 POST 请求

---结束

7.9 配置防敏感信息泄露规则避免敏感信息泄露

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（身份证号、电话号码、电子邮箱）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

已添加防护网站或已 1010.1 新增防护策略。

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。

配置防敏感信息泄露规则

- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的，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 (独享版)”。
- 步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。
- 步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

- 步骤 6 在“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。

图 7-54 防敏感信息泄露配置框



- 步骤 7 在“防敏感信息泄露”规则配置列表的左上方，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，如图 7-55 和图 7-56 所示，参数说明如图 7-56 表 7-12 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。

图 7-55 敏感信息泄露



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。

图 7-56 响应码拦截

表 7-12 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”，如果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。

配置示例-敏感信息过滤

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敏感信息过滤防护效果。

步骤 1 添加一条敏感信息过滤规则。

图 7-57 敏感信息泄露

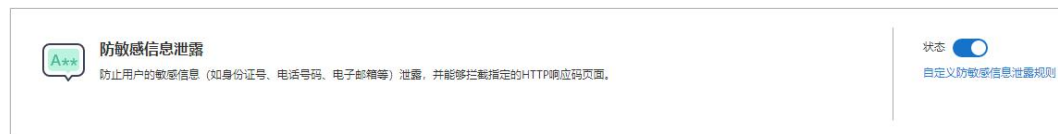


The screenshot shows a configuration window titled "添加防敏感信息泄露规则" (Add Sensitive Information Leakage Rule). It contains the following fields and options:

- * 路径** (Path): An empty text input field.
- * 类型** (Type): A dropdown menu with "敏感信息过滤" (Sensitive Information Filtering) selected.
- * 内容** (Content): A section with three checked checkboxes: "身份证号" (ID Number), "电话号码" (Phone Number), and "电子邮箱" (Email Address).
- 规则描述** (Rule Description): An empty text area.
- Buttons: "确认" (Confirm) and "取消" (Cancel).

步骤 2 开启防敏感信息泄露。

图 7-58 防敏感信息泄露配置框



The screenshot shows a configuration panel for "防敏感信息泄露" (Sensitive Information Leakage). It includes:

- A status indicator "A**" and a description: "防止用户的敏感信息（如身份证号、电话号码、电子邮箱等）泄露，并能够拦截指定的HTTP响应页面。" (Prevent sensitive information from leaking and intercept specified HTTP response pages).
- A toggle switch labeled "状态" (Status) which is turned on, with the text "自定义防敏感信息泄露规则" (Custom Sensitive Information Leakage Rule) below it.

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

该页面的电子邮箱、电话号码和身份号码信息被屏蔽。

---结束

7.10 配置全局白名单规则对误报进行忽略

当 WAF 根据您配置的 Web 基础防护规则或网站反爬虫的“特征反爬虫”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。

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

- 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。
- 您可以通过 6.2 处理误报事件来配置全局白名单规则，处理误报事件后，您可以在全局白名单规则列表中查看该误报事件对应的全局白名单规则。
- 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。

配置全局白名单规则

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，选择区域或项目。

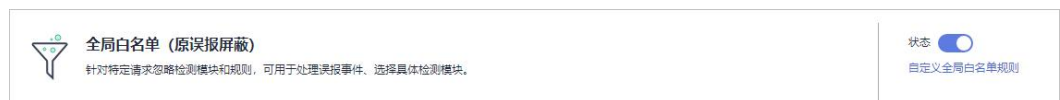
步骤 3 单击页面左上方的，选择“安全 > Web 应用防火墙 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“全局白名单”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。

图 7-59 全局白名单配置框



步骤 7 在“全局白名单”规则配置列表的左上方，单击“添加规则”。

步骤 8 添加全局白名单规则，参数说明如图 7-60 表 7-13 所示。

图 7-60 添加全局白名单规则

The screenshot shows a configuration window titled "添加全局白名单规则" (Add Global Whitelist Rule). It contains several sections:

- * 防护方式** (Protection Mode): Radio buttons for "全部域名" (All domains) and "指定域名" (Specify domain), with "指定域名" selected.
- * 防护域名** (Protection Domain): A text input field containing "cn".
- 条件列表** (Condition List): A table with columns "字段" (Field), "子字段" (Sub-field), "逻辑" (Logic), and "内容" (Content). One rule is shown: Field "路径" (Path), Sub-field "--", Logic "包含" (Contains), Content "/product".
- * 不检测模块** (Do not check modules): Radio buttons for "所有检测模块" (All detection modules) and "Web基础防护模块" (Web basic protection modules), with the latter selected.
- * 不检测规则类型** (Do not check rule types): Radio buttons for "按ID" (By ID), "按类别" (By category), and "所有内置规则" (All built-in rules), with "按类别" selected.
- * 不检测规则类别** (Do not check rule categories): A dropdown menu showing "XSS攻击" (XSS attack).
- 规则描述** (Rule description): A text area.
- 高级设置** (Advanced settings): Includes "指定放行位置" (Specify allow location) with dropdowns for "Params" and "全部" (All).

Buttons at the bottom include "确认添加" (Confirm add) and "取消" (Cancel).

表 7-13 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</p> <p>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：7.2 配置 Web 基础防护规则防御常见 Web 攻击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。建议您直接在防护事件页面进行误报处理。</p>	041046

参数	参数说明	取值样例
不检测规则类别	<p>当“不检测规则类型”选择“按类别”时，需要配置此参数。</p> <p>在下拉框中选择事件类别。</p> <p>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。</p>	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	<p>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。</p> <p>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。</p> <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。 <p>说明</p> <p>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。</p>	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”，如果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”。
- 如果需要修改添加的全局白名单规则时，可单击待修改的全局白名单规则所在行的“修改”，修改全局白名单规则。
- 如果需要删除添加的全局白名单规则时，可单击待删除的全局白名单规则所在行的“删除”，删除全局白名单规则。

7.11 配置隐私屏蔽规则防隐私信息泄露

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。

配置隐私屏蔽规则

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，选择区域或项目。

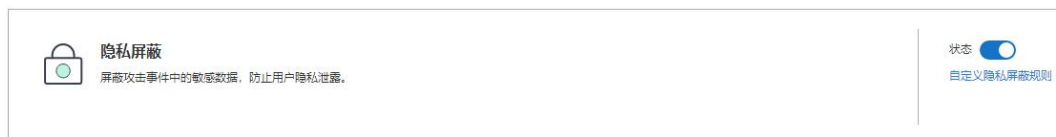
步骤 3 单击页面左上方的，选择“安全 > Web 应用 防火墙 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“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。

图 7-61 隐私设置配置框



步骤 7 在“隐私屏蔽”规则配置列表的左上方，单击“添加规则”。

步骤 8 添加隐私屏蔽规则，根据图 7-62 表 7-14 配置参数。

图 7-62 添加隐私屏蔽规则

表 7-14 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>
屏蔽字段	<p>设置为屏蔽的字段。</p> <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。

参数	参数说明	取值样例
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。	<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

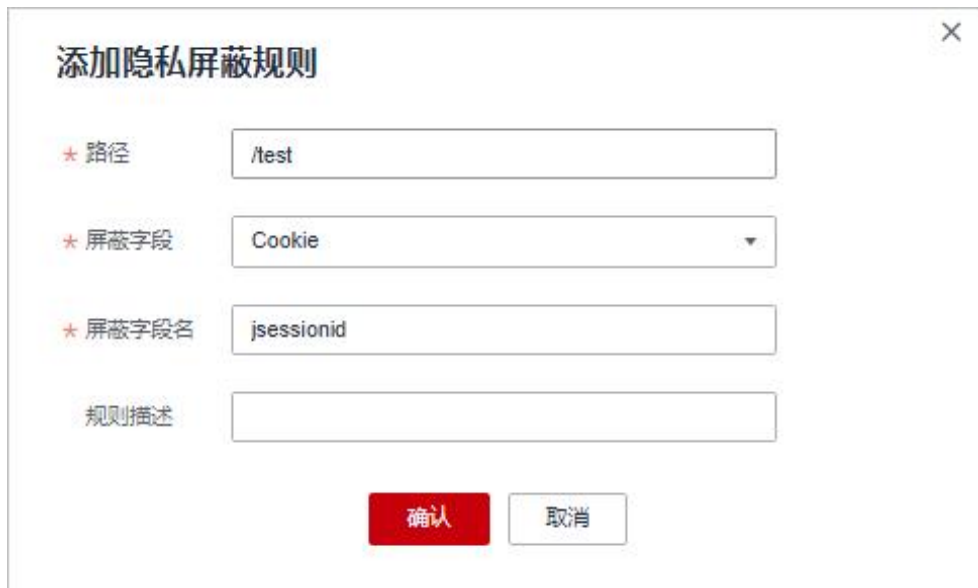
- 规则添加成功后，默认的“规则状态”为“已开启”，如果您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 如果需要修改添加的隐私屏蔽规则时，可单击待修改的隐私屏蔽规则所在行的“修改”，修改隐私屏蔽规则。
- 如果需要删除添加的隐私屏蔽规则时，可单击待删除的隐私屏蔽规则所在行的“删除”，删除隐私屏蔽规则。

配置示例-屏蔽 Cookie 字段

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屏蔽 Cookie 字段名“jsessionid”防护效果。

步骤 1 添加一条隐私屏蔽规则。

图 7-63 添加“jsessionId”字段名隐私屏蔽规则



添加隐私屏蔽规则

* 路径 /test

* 屏蔽字段 Cookie

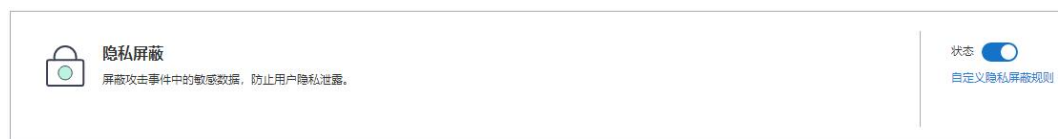
* 屏蔽字段名 jsessionId

规则描述

确认 取消

步骤 2 开启隐私屏蔽。

图 7-64 隐私设置配置框



隐私屏蔽
屏蔽攻击事件中的敏感数据，防止用户隐私泄露。

状态 自定义隐私屏蔽规则

步骤 3 在左侧导航树中，单击“防护事件”，进入“防护事件”页面。

步骤 4 在目标防护事件所在行的“操作”列中，单击“详情”，查看事件详细信息。

该防护事件的 Cookie 字段名“jsessionId”信息被屏蔽。

图 7-65 查看防护事件-隐私屏蔽

事件信息

时间	2021/11/18 20:15:58 GMT+08:00	事件类型	SQL注入攻击
源IP	[REDACTED]	地理位置	江苏
防护域名	[REDACTED]	URL	/test
恶意负载位置	body	防护动作	拦截
事件ID	[REDACTED]	状态码	418
响应时间 (毫秒)	0	返回大小 (字节)	3,533

恶意负载

```
id=' and 1=1--
```

请求详情

```
POST /test
authorization: Basic cm9vdDpyb290
content-length: 14
accept-language: zh-CN,zh;q=0.9, zh-CN,zh;q=0.9
host: [REDACTED]
upgrade-insecure-requests: 1
content-type: application/x-www-form-urlencoded
connection: Keep-Alive
cache-control: max-age=0
user-agent: Mozilla/5.0 (Linux; U; Android 10; id-id; Redmi 9C Build/QP1A.190711.020) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/89.0.4389.116 Mobile Safari/537.36 XiaoMi/MiuiBrowser/12.13.0-gn
via: proxy A
Cookie: HWWAFESID=f3ece7308c3e8feff3; HWWAFESTIME=1637135543680; jsessionid=***mask***
```

---结束

7.12 创建引用表对防护指标进行批量配置

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、精准访问防护规则所引用。

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。

应用场景

CC 攻击防护规则、精准访问防护规则批量配置防护字段时，可以使用引用表。

创建引用表



- 步骤 1** 登录管理控制台。
- 步骤 2** 单击管理控制台右上角的，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 (独享版)”。
- 步骤 4** 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。
- 步骤 5** 单击目标策略名称，进入目标策略的防护配置页面。
- 步骤 6** 在“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，参数说明如图 7-66 表 7-15 所示。

图 7-66 添加引用表

添加引用表

* 名称

* 类型

* 值

+ 添加 您还可以添加29项条件。

规则描述

确认 取消

表 7-15 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

参数名称	参数说明	取值样例
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。支持 IPv4 和 IPv6 两种格式的 IP 地址。<ul style="list-style-type: none">- IPv4, 例如: 192.168.1.1- IPv6, 例如: fe80:0000:0000:0000:0000:0000:0000:0000• 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”, 如果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

- 如果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。
- 如果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。

7.13 配置攻击惩罚标准封禁访问者指定时长

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 黑白名单等规则使用。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。

须知

黑白名单规则中，不支持选择“长时间 IP 拦截”和“短时间 IP 拦截”的攻击惩罚。


- 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 9.1.5 配置攻击惩罚的流量标识。
- 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。


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。

配置攻击惩罚标准

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“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。

图 7-67 攻击惩罚配置框



步骤 7 在“攻击惩罚”列表的左上方，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，参数说明如图 7-68 表 7-16 所示。

图 7-68 添加攻击惩罚



表 7-16 攻击惩罚参数说明

参数	参数说明	取值样例
----	------	------

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 <p>须知</p> <p>黑白名单规则中，不支持选择“长时间 IP 拦截”和“短时间 IP 拦截”的攻击惩罚。</p>	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 • 0<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 配置完成后，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

- 如果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。
- 如果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”。

图 7-69 流量标识



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。

图 7-70 添加 Cookie 拦截攻击惩罚



步骤 4 开启攻击惩罚。

图 7-71 攻击惩罚配置框



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 7-72 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

7.14 条件字段说明

您在设置 CC 攻击防护规则、精准访问防护规则或全局白名单规则时，需要在规则中配置条件字段，定义要匹配的请求特征。本文介绍了规则匹配条件支持使用的字段及其释义。

什么是条件字段

条件字段指需要 WAF 检测的请求特征。您在设置 7.3 配置 CC 攻击防护规则防御 CC 攻击、7.4 配置精准访问防护规则定制化防护策略或 7.10 配置全局白名单规则对误报进行忽略时，通过定义条件字段，指定要检测的请求特征。如果某个请求满足规则中设置的条件，则该请求命中对应规则；WAF 会依据规则中设置的规则动作，对请求执行相应处置（例如，放行、拦截、仅记录等）。

图 7-73 条件字段



条件字段由字段、子字段、逻辑、和内容组成。配置示例如下：

- 示例 1：“字段”为“路径”、“逻辑”为“包含”、内容为“/admin”，表示被请求的路径包含“/admin”时，则请求命中该规则。
- 示例 2：“字段”为“IPv4”、“子字段”为“客户端 IP”、“逻辑”为“等于”、内容为“192.XX.XX.3”，表示当发起连接的客户端 IP 为 192.XX.XX.3 时，则请求命中该规则。

支持的条件字段

表 7-17 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。	/buy/phone/ 须知 <ul style="list-style-type: none"> ● 路径设置为“/”时，表示防护网站所有路径。 ● 配置的“路径”的“内容”不能包含特殊字符 (<math>< > * </math>)。
User Agent：设置为需要防护的扫描器的用户代理。	--		Mozilla/5.0 (Windows NT 6.1)
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）
<p>Referer: 设置为需要防护的自定义请求访问的来源。</p> <p>例如：防护路径设置为“/admin/xxx”，如果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>	--		http://www.test.com
<p>Cookie: 根据 Cookie 区分的 Web 访问者。</p>	<ul style="list-style-type: none"> • 所有字段 • 任意子字段 • 自定义 		jsessionId
<p>Header: 设置为需要防护的自定义 HTTP 首部。</p>	<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>
<p>Method: 需要防护的自定义请求的方法。</p>	--		GET、POST、PUT、DELETE、PATCH
<p>Request Line: 需要防护的自定义请求行的长度。</p>	--		50
<p>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。</p>	--		--
<p>Protocol: 需要防护的请求的协议。</p>	--		http

8 查看总览

在“安全总览”页面，您可以查看昨天、今天、3天、7天或者30天内所有防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类型统计次数，QPS 信息，以及事件分布、受攻击域名 Top10、攻击源 IP Top10、受攻击 URL Top10 等防护数据。

前提条件

- 已 5 网站接入 WAF。
- 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 8-1 所示。

表 8-1 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


📖 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。

查看安全总览

步骤 1 登录管理控制台。

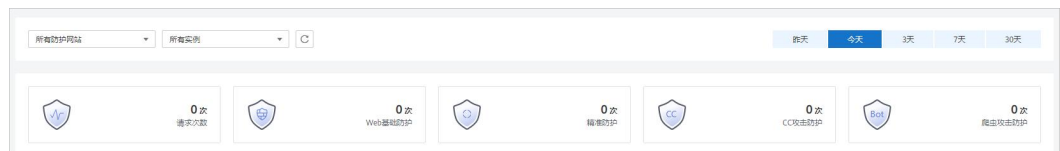
步骤 2 单击管理控制台右上角的，选择区域或项目。

步骤 3 单击页面左上方的，选择“安全 > Web 应用防火墙 (独享版)”。

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”：统计的是选择添加到 WAF 的防护网站的接入信息。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。

图 8-2 查询条件设置



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。

图 8-3 防护统计数据



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 1 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。

图 8-4 安全统计

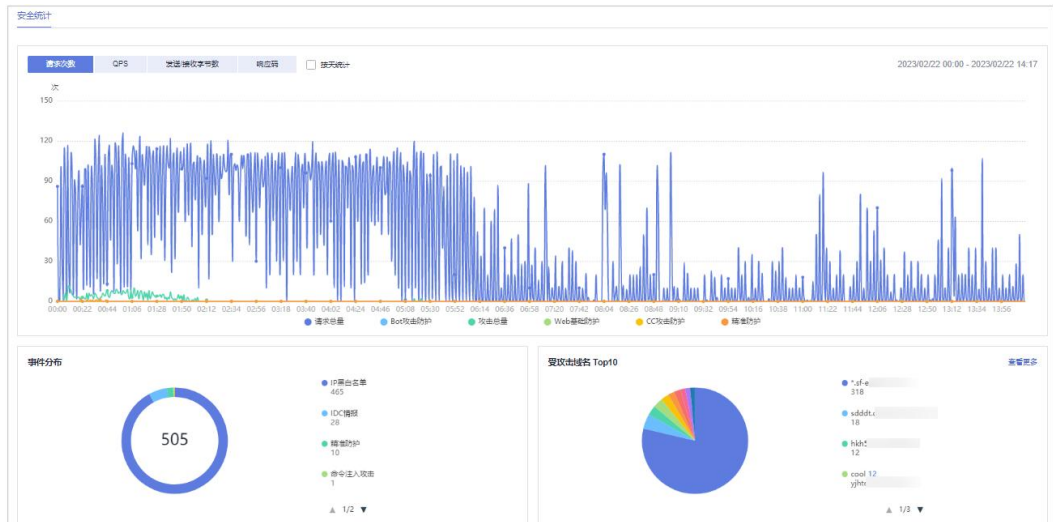


表 8-2 安全统计参数说明

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。
发送/接收字节数	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。
响应码	可以查看“WAF 返回客户端”和“源站返回给 WAF”对应响应码以及响应次数。 响应码的数量是按照图表下方响应码的顺序（从左至右）累加进行显示，对应响应码的数量是为两条线的差值（如果某个响应码值为 0，会与前一个的响应码显示的线重合）。

参数	说明
事件分布	查看攻击事件类型。 单击“事件分布”中的任意一个区域，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

9 网站设置

9.1 网站接入后推荐配置

9.1.1 配置 PCI DSS/3DS 合规与 TLS

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。

约束条件

- 当防护网站的“对外协议”为“HTTP”时，HTTP 协议不涉及 TLS，请忽略该章节。
- 如果防护网站配置了多个服务器时，“对外协议”都配置为“HTTPS”时，才支持配置 PCI DSS/3DS 合规。
- 开启 PCI DSS/3DS 合规后，将不支持修改“对外协议”，也不支持添加服务器。

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，支持配置的最低 TLS 版本如表 9-1 所示。

表 9-1 支持配置的最低 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。

📖 说明

在配置 TLS 前，您可以先[查看网站 TLS 版本](#)。

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 9-2 所示。

表 9-2 加密套件说明

加密套件名称	支持的加密算法	不支持的加密算法	说明
默认加密套件 说明 WAF 默认给网站配置的是“加密套件 1”，但是如果请求信息不携带 sni 信息，WAF 就会选择缺省的“默认加密套件”。	<ul style="list-style-type: none">• ECDHE-RSA-AES256-SHA384• AES256-SHA256• RC4• HIGH	<ul style="list-style-type: none">• 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	不支持的加密算法	说明
加密套件 1	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH 	<ul style="list-style-type: none"> • MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • 3DES • DSS • EXP • CAMELLIA 	<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 • RC4 • HIGH 	<ul style="list-style-type: none"> • 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	不支持的加密算法	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 • RC4 • HIGH 	<ul style="list-style-type: none"> • 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。
加密套件 5	<ul style="list-style-type: none"> • AES128-SHA:AES256-SHA • AES128-SHA256:AES256-SHA256 • HIGH 	<ul style="list-style-type: none"> • MEDIUM • LOW • aNULL • eNULL • EXPORT • DES • MD5 • PSK • RC4 • DHE 	仅支持 RSA-AES-CBC 算法。
加密套件 6	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 	-	<ul style="list-style-type: none"> • 兼容性：一般 • 安全性：较好

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 9-3 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 9-3 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	加密套件 5	加密套件 6
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	√	√	×	√	√	√	√
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	×	×	×	×	×	×	×


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	加密套件 5	加密套件 6
Safari 5.1.9/OS X 10.6.8	√	√	×	√	√	×	√
Safari 6.0.4/OS X 10.8.4	√	√	×	√	√	×	√


系统影响

- PCI DSS
 - 开启 PCI DSS 合规认证后，不能修改 TLS 最低版本和加密套件，且最低 TLS 版本将设置为“TLS v1.2”，加密套件设置为 EECDH+AESGCM:EDH+AESGCM。
 - 开启 PCI DSS 合规认证后，如果您需要修改 TLS 最低版本和加密套件，请关闭该认证。
- PCI 3DS
 - 开启 PCI 3DS 合规认证后，不能修改 TLS 最低版本，且最低 TLS 版本将设置为“TLS v1.2”。
 - 开启 PCI 3DS 合规认证后，您将不能关闭该认证，请根据业务实际需求进行操作。

配置 PCI DSS/3DS 合规与 TLS

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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，也可以在“TLS 配置”所在行，单击修改 TLS 配置。

图 9-2 修改 TLS 配置

基本信息

网站名称	--
防护域名	0910. .com
网站备注	--
对外协议类型	HTTPS
合规认证	<input type="checkbox"/> PCI DSS <input type="checkbox"/> PCI 3DS
国际证书	证书名称 dmc0909
	TLS配置 TLS v1.0 加密套件1
是否已使用代理	否
策略名称	policy_NXiqWhDp
告警页面	系统默认

- 勾选“PCI DSS”，系统弹出“警告”对话框，单击“确定”，开启该合规认证。



须知

选择开启 PCI DSS 合规认证后，您将不能修改 TLS 最低版本和加密套件。

- 勾选“PCI 3DS”，系统弹出“警告”对话框，单击“确定”，开启该合规认证。

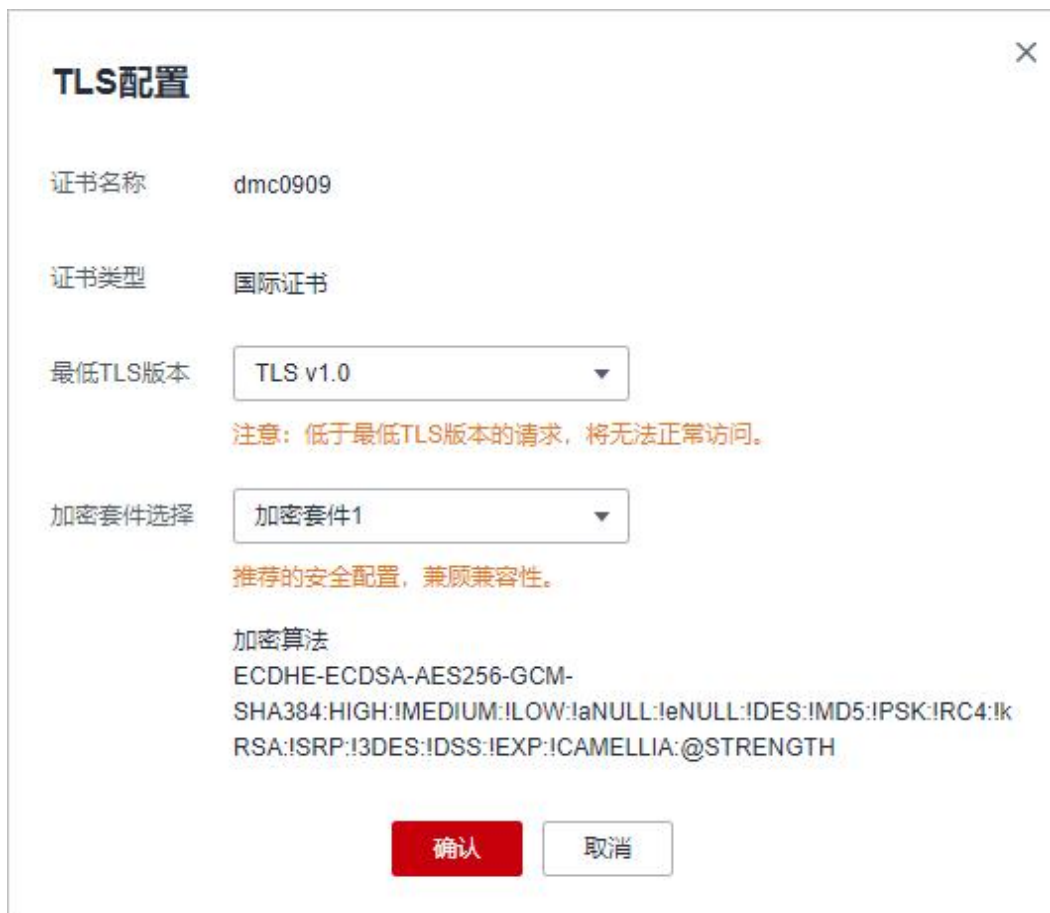


须知

- 选择开启 PCI 3DS 合规认证后，您将不能修改 TLS 最低版本。
- 选择开启 PCI 3DS 合规认证后，您将不能关闭该认证，请根据业务实际需求进行操作。

步骤 7 在弹出的“TLS 配置”对话框中，选择最低 TLS 版本和加密套件，如图 9-3 所示。

图 9-3 “TLS 配置”对话框



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。

步骤 8 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。

9.1.2 开启 IPv6 防护

如果您的网站需要 IPv6 的防护，可以参考本章节开启 IPv6 防护，开启后，WAF 将为域名分配 IPv6 的接入地址，WAF 默认在 CNAME 中增加 IPv6 地址解析，IPv6 的所有访问请求将先流转到 WAF，WAF 检测并过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

- 当防护网站的源站地址配置为 IPv6 地址时，默认开启 IPv6 防护。WAF 使用 IPv6 回源地址和源站发起连接。

图 9-4 源站地址只有 IPv6 时



- 当防护网站的源站地址配置为 IPv4 地址时，手动开启 IPv6 防护后，WAF 将通过 NAT64 机制（NAT64 是一种通过网络地址转换（NAT）形式促成 IPv6 与 IPv4 主机间通信的 IPv6 转换机制）将外部 IPv6 访问流量转化成对内的 IPv4 流量。WAF 使用 IPv4 回源地址和源站发起连接。

图 9-5 源站地址只有 IPv4 时




前提条件

5 网站接入 WAF

开启 IPv6 防护

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 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“IPv6 防护”所在行，单击，在弹出的对话框中，选择“开启”并单击“确定”。

---结束

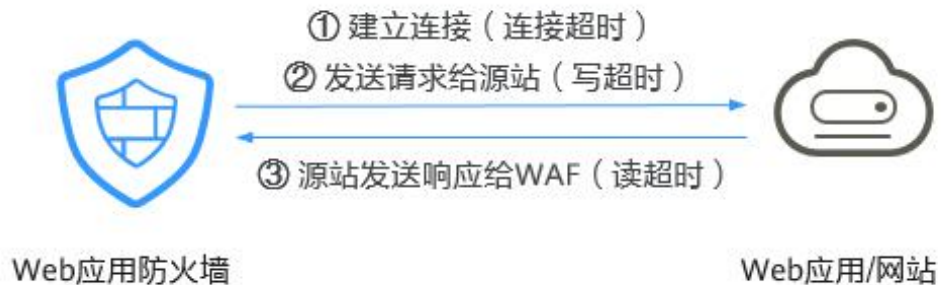
9.1.3 配置 WAF 到网站服务器的连接超时时间

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，如果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，如果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 9-6 所示。

图 9-6 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。

前提条件


5 网站接入 WAF


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。

配置 WAF 到网站服务器的连接超时时间


步骤 1 登录管理控制台。



步骤 2 单击管理控制台右上角的，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 (独享版)”。

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“超时配置”所在行，单击 ，开启超时配置。

步骤 7 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

9.1.4 开启连接保护功能保护源站安全

网站接入 WAF 防护之后，如果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 5 网站接入 WAF。
- 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](#)。


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。

开启连接保护

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的 ，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 (独享版)”。

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“连接保护”所在行，单击“启用状态”图标，开启连接保护。

图 9-7 连接保护





步骤 7 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 9-4 所示。

表 9-4 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

参数		参数说明	示例
	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

📖 说明

以 步骤 6 图 9-7 中设置的值为例进行解释：

- “宕机保护”：当防护网站的 502/504 错误返回量达到 1000 条以上且占网站的所有访问请求量的 90%及以上时，第一次触发时，WAF 将停止转发用户请求 180s（即阻止用户访问网站 180s）；连续第二次触发时，WAF 将停止转发用户请求 360s；连续第三次及以上触发时，WAF 将停止转发用户请求 540s。当累计保护时间超过 1 小时（3600s），叠加次数会从头计数。
- “连接保护”：访问网站的读等待 URL 请求数量达到 6000 以上时，WAF 将停止转发用户请求 60s，并将返回网站的维护页面。

---结束

9.1.5 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

5 网站接入 WAF

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。

配置攻击惩罚的流量标识




- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的, 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 (独享版)”。
- 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, 分别设置流量标识, 相关参数说明如图 9-8 表 9-5 所示。

图 9-8 流量标识



表 9-5 流量标识参数说明

标识	说明	配置样例
----	----	------

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>该字段用于保存客户端的真实 IP 地址，可自定义字段名且支持配置多个字段（多个字段名以英文逗号隔开），配置后，WAF 优先从配置的字段中获取客户端真实 IP（配置多个字段时，WAF 从左到右依次读取）。</p> <p>须知</p> <ul style="list-style-type: none">• 如果想以 TCP 连接 IP 作为客户端 IP，“IP 标记”应配置为“\$remote_addr”。• 如果报文存在 TOA，而不想以“TCP Option Address”作为客户端 IP，“IP 标记”应配置为“\$remote_sockaddr”，并将独享引擎版本升级到 24 年 5 月及之后的版本，配置后会以报文的 3 层源 IP 作为客户端 IP。• 如果从自定义字段中未获取到客户端真实 IP，WAF 将依次从 cdn-src-ip, x-real-ip, x-forwarded-for, \$remote_addr 字段获取客户端 IP。	X-Forwarded-For
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

9.1.6 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


5 网站接入 WAF


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”。

修改拦截返回页面

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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，单击编辑图标，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，如-图 9-9 所示。
 - HTTP 返回码：自定义页面配置的返回码。
 - 响应标头：单击“添加响应标头字段”，可配置响应标头参数及参数值。
 - 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。

图 9-9 自定义告警页面

告警页面

页面模板 系统默认 自定义 重定向

HTTP返回码

页面类型

页面内容 ?

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>错误</title>
</head>
<body>

</body>

</html>
</html>
```

确定 取消

- “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

9.1.7 开启 Cookie 安全属性

当“对外协议”配置为 HTTPS 时，WAF 支持开启“Cookie 安全属性”，开启后会将 Cookie 的 `HttpOnly` 和 `Secure` 属性设置为 `true`。

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。


约束条件

- “对外协议”包含“HTTP”时，“Cookie 安全属性”默认为关闭状态，不支持开启。

开启 Cookie 安全属性

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（独享版）”。

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。


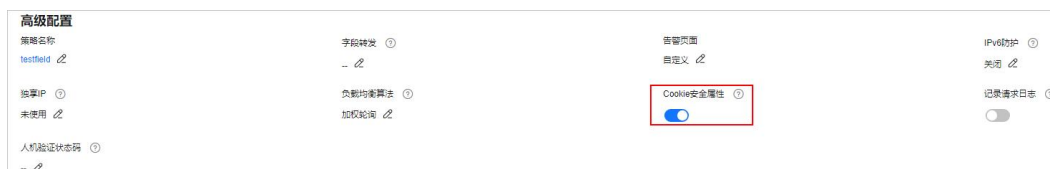
步骤 6 在“高级配置”栏中“Cookie 安全属性”列单击 ，开启 Cookie 安全属性

图 9-10 开启 Cookie 安全属性



---结束

9.2 网站管理

9.2.1 查看网站基本信息


您可以通过 WAF 管理控制台，查看防护域名的对外协议类型、策略名称、告警页面、CNAME、CNAME IP 等信息。


前提条件

5 网站接入 WAF

查看网站基本信息

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的 ，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（独享版）”。

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 9-6 所示。

表 9-6 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”。
源站 IP/端口	客户端访问的网站服务器的公网 IP 地址和 WAF 转发客户端请求到服务器的业务端口。
证书	绑定该域名的证书，单击证书名称，可跳转到“证书管理”页面。
近 3 天威胁	该域名 3 天内的防护情况。
工作模式	<p>防护模式。单击 ▼，可选择以下两种防护模式：</p> <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规则处理正常业务拦截问题。 <p>详细操作请参见 9.2.2 切换工作模式。</p>
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。
域名接入进度	网站接入 WAF 未完成的步骤或者接入状态。
创建时间	该域名添加到 WAF 的时间。

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 查看防护域名的信息，如图 9-11 所示。

如果需要修改某项信息，在目标参数所在行，单击编辑按钮进行修改。

图 9-11 查看基本信息



---结束

9.2.2 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

5 网站接入 WAF

应用场景


- 开启防护：开启后，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规则处理正常业务拦截问题。

切换工作模式

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

步骤 4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

---结束

9.2.3 更新网站绑定的证书

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。

更新网站绑定的证书

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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 在证书所在行的证书名称后，单击编辑图标，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。

- “更新方式”选择“添加证书”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。

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。

图 9-12 导入证书



WAF 当前仅支持 PEM 格式证书。如果证书为非 PEM 格式，请参考表 9-7 在本地将证书转换为 PEM 格式，再上传。

表 9-7 证书转换命令

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

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。
- “更新方式”选择“选择已有证书”时，在“证书”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

9.2.4 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 9.2.3 更新网站绑定的证书。

前提条件

5 网站接入 WAF

约束条件


开启 PCI DSS/3DS 合规后，将不支持修改“对外协议”，也不支持添加源站地址。



系统影响

修改服务器配置信息对业务无影响。

修改服务器配置信息

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。
- 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 9.2.3 更新网站绑定的证书。
 - 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。
 - 如果需要开启 IPv6 防护，在“IPv6 防护”所在行，单击“开启”。
- 步骤 8** 单击“确认”，完成服务器信息修改。

---结束

9.2.5 删除防护网站

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。



前提条件

5 网站接入 WAF

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。

删除防护网站

- 步骤 1** 登录管理控制台。
- 步骤 2** 单击管理控制台右上角的 ，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 (独享版)”。
- 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

相关操作

如果您想批量删除域名，批量勾选域名后，在网站列表上方，单击“批量删除”。

10 策略管理



10.1 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。

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 单击管理控制台右上角的，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 (独享版)”。
- 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 7 配置防护策略为策略添加防护规则。

---结束

相关操作

- 如果您想修改策略名称，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。
- 如果您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”。
- 如果您想批量删除防护策略，勾选需要删除的策略，单击策略列表上方的“批量删除”。

10.2 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，添加的域名将从原有策略迁移到当前策略。



说明

如果您已开通企业项目，您需要在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能为企业项目批量添加防护规则。

前提条件

5 网站接入 WAF

添加策略适用的防护域名

- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的，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 (独享版)”。
- 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。
- 如果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”。

图 10-1 添加策略适用的防护域名



步骤 7 单击“确认”。

---结束

10.3 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。

批量添加防护规则



- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的, 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 (独享版)”。
- 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 在策略列表左上方, 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。

图 10-2 批量添加防护规则

批量添加CC防护规则

如果使用独享引擎，请您确认引擎是否全部升级到最新版本。否则该功能将不生效。

规则描述

* 策略名称

* 限速模式 IP限速 用户限速 其他

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

* 限速条件

字段	子字段	逻辑	内容
路径	--	包含	<input type="text"/>

添加 您还可以添加29项条件。（多个条件同时成立才生效）

* 限速频率 次 秒

* 防护动作 人机验证 阻断 动态阻断 仅记录

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 步骤 8 图 7-9 表 7-5 进行参数配置。
- “精准访问防护”请参见 步骤 9 图 7-13 表 7-6 进行参数配置。
- “黑白名单设置”请参见 图 7-24 表 7-7 进行参数配置。
- “地理位置访问控制”请参见 步骤 8 图 7-32 表 7-8 进行参数配置。
- “网页防篡改”请参见 步骤 8 图 7-42 表 7-9 进行参数配置。
- “防敏感信息泄露”请参见 步骤 8 图 7-56 表 7-12 进行参数配置。
- “全局白名单”请参见 步骤 8 图 7-60 表 7-13 进行参数配置。
- “隐私屏蔽”请参见 7.11 步骤 8 图 7-62 表 7-14 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

11 高阶功能

11.1 配置内容安全检测

Web 应用防火墙提供内容安全检测服务，基于丰富的违规样例库和内容审核专家经验，通过机器审核加人工审核结合的方式，帮助您准确检测出 Web 网站和新媒体平台上的关于涉黄、涉赌、涉毒、暴恐、涉政、惊悚、违禁广告等敏感违规内容，并提供文本内容纠错审校（错别字、生僻字、语法表述不当等有违准确性内容）。并提供专业检测报告助您自纠自查，降低内容违规风险。

使用须知

- 购买内容安全检测服务后，系统立即执行检测。
- 检测过程中，不支持修改检测域名、暂停任务、退费等操作。
- 确定网站检测配额，请参见 16.916.9.1 购买内容安全检测服务时，如何确定网站检测配额？。
- “检测类型”选择“内容安全单次检测（按需）”时，下单后的 7 个工作日内出报告。
- “检测类型”选择“文本安全监测（按月/按年）”时，下单后的检测周期（1 个月）后的 7 个工作日内出报告。
- 10 个工作日内检测完成。

计费模式

包年/包月（预付费）和按需计费（后付费）两种计费方式。

内容安全检测服务支持三种检测类型：内容安全单次检测（按需）、文本安全监测（按月）、文本安全监测（按年）。选择“内容安全单次检测（按需）”时，内容安全检测服务按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。网站检测配额请参见 16.916.9.1 购买内容安全检测服务时，如何确定网站检测配额？。


例如：单次配置了 10 个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行 10 次收费。


步骤一：购买内容安全检测

购买内容安全检测，配置“检测类型”和“检测对象”，可对“检测对象”对应的文本类型进行安全检测。

支持批量购买内容安全检测，可一次输入一个或多个“检测对象”进行安全检测。

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

步骤 4 在左侧导航栏，选择“高阶功能 > 内容安全检测”，进入“内容安全检测”页面。

步骤 5 在页面右上角，单击“购买内容安全检测服务”，进入购买页面，参见图 11-1 表 11-1 配置相关参数。

图 11-1 购买内容安全检测服务



图 11-1 展示了购买内容安全检测服务的配置界面。界面主要分为两个部分：检测类型选择和检测对象配置。

检测类型选择：

- 内容安全单次检测 (按需)：**检测完成后提供一份内容检测报告。可检测：图片、文字、视频、音频。
- 文本安全监测 (按月)：**提供内容监测月报。可检测：文字。
- 文本安全监测 (按年)：**提供内容监测月报、年报。可检测：文字。

检测对象配置：

- 检测对象类型：**选择“网站”。
- 检测对象：**输入框，支持批量输入。示例说明：每一行表示一个检测网址，多个网址以回车换行分割，同一行内的网址和备注之间以英文逗号分割，格式如下：
http://域名1,备注
https://域名2,备注
.....
- 检测网站的数量：**1/100

表 11-1 参数说明

参数	说明
区域	在下拉框选择区域。

参数	说明
检测类型	<ul style="list-style-type: none"> “内容安全单次检测（按需）”：针对单个网站或新媒体账号的文字、图片、音频、视频内容进行检测，检测完成后提供一份内容检测报告。 “文本安全监测（按月）”：针对单个网站或新媒体账号的文字内容进行内容安全监测，并在一个自然月后输出内容监测月报。 “文本安全监测（按年）”：针对单个网站或新媒体账号的文字内容进行内容安全监测，并在每一个自然月后输出内容监测月报，一个自然年后输出内容监测年报。
伙伴	<p>以下两个伙伴供您选择：</p> <ul style="list-style-type: none"> “蜜度”：语言智能科技企业，致力于为政企客户提供全方位的数据智能服务。 “汉雅星空”：面向文旅、广电等行业领域，提供内容安全审核解决方案的运营服务商。
检测对象类型	<p>检测对象类型包含：</p> <ul style="list-style-type: none"> “网站”：支持网站内容审查，可根据 URL 检测网站内容，可自行排查检测站内网页、链接内容，包括文本、图片、音频、视频等。 “新媒体”：支持主流新媒体平台的内容审查，包括文本、图片、音频、视频等。
检测对象	<ul style="list-style-type: none"> “检测对象类型”选择“新媒体”时：输入需要检测的账号名称，并备注新媒体平台。 <p>说明</p> <p>每一行表示一个新媒体账号，多个新媒体账号以回车换行分割；同一行内的新媒体账号和备注之间以英文逗号分割，每行最多支持 500 个英文字符（1 个中文字符等于 2 个英文字符）。</p> <ul style="list-style-type: none"> “检测对象类型”选择“网站”时：输入被检测网站完整域名与备注信息。 <p>说明</p> <p>每一行表示一个检测网址，多个网址以回车换行分割；同一行内的网址和备注之间以英文逗号分割，如无备注，可只输入网址，每行最多支持 500 个英文字符（1 个中文字符等于 2 个英文字符）。</p>

步骤 6 请仔细阅读“重要提示”内容并勾选“我已知晓”。

 **注意**

检测任务创建后，一次性扣费，不支持修改和暂停任务，请您仔细核对检测信息。

步骤 7 确认订单详情无误后，单击“立即使用”，进入检测数量确认界面。

步骤 8 确认检测数量后，单击“确认”，完成购买操作。

---结束

步骤二：下载检测报告

步骤 1 在左侧导航栏选择“高阶功能 > 内容安全检测”，进入“内容安全检测”页面。

步骤 2 在目标检测对象所在行的“操作”列，单击“下载报告”，可将检测报告下载到本地。

报告中呈现检测出的合规性风险、内容安全风险等相关内容。用户根据报告内容选择整改或者保留。

 **说明**

“检测状态”为“检测完成”时，才支持下载报告。

---结束

其他操作

如果您需要对检测对象进行再次检测时，在该检测对象所在行的“操作”列，单击“复购”。

12 对象管理

12.1 管理证书

12.1.1 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。

将证书上传到 WAF，添加防护网站时可直接选择上传到 WAF 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。

上传证书

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，选择区域或项目。

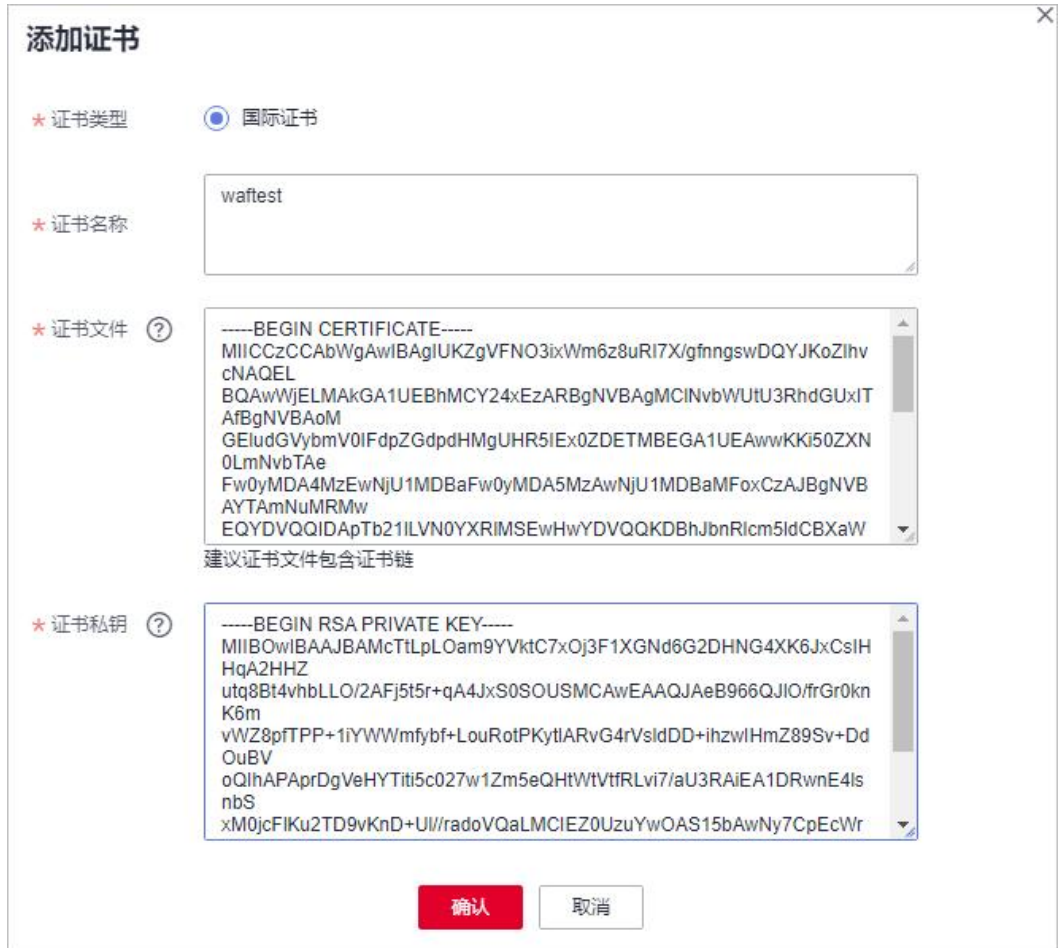
步骤 3 单击页面左上方的，选择“安全 > Web 应用防火墙 (独享版)”。

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“添加证书”，弹出添加证书的对话框。

步骤 6 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。

图 12-1 “上传证书”对话框



WAF 当前仅支持 PEM 格式证书。如果证书为非 PEM 格式，请参考表 12-1 在本地将证书转换为 PEM 格式，再上传。

表 12-1 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

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。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	<ul style="list-style-type: none">提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

📖 说明

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


步骤 7 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。

12.1.2 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

在 WAF 上创建了证书。

查看证书信息




- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的，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 (独享版)”。
- 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 12-2 所示。

表 12-2 证书参数说明

参数名称	参数说明
名称	证书名称。
证书类型	仅支持“国际证书”。
到期时间	证书到期时间。 证书过期后，对源站的影响是毁灭性的，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 9.2.3 更新网站绑定的证书。
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。

12.1.3 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。

删除证书

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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

12.2 管理黑白名单 IP 地址组



12.2.1 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。

添加黑白名单 IP 地址组

- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的，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（独享版）”。
- 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 在地址组列表左上方，单击“添加地址组”。
- 步骤 6 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 7 单击“确认”，地址组创建成功。

---结束

12.2.2 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

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。

修改或删除黑白名单 IP 地址组

- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台右上角的，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（独享版）”。
- 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 12-3 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。

参数名称	参数说明
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“确定”。

---**结束**

13 系统管理

13.1 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 单击管理控制台右上角的，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 (独享版)”。
- 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。

图 13-1 独享引擎列表



实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	规格	计费模式	操作
1029-5ny 388a4c3ce42243d0a57bb7a95...	未发配	vpc-iv-test	subnet-e2db	192.168.0.8...	未接入	运行中	-	标准模式 (反向代理)	s7n.2xlarge.2	按量计费	升级 删除 切换安全组
102703100-4A3d f102f3258ec488281022f460a90...	未发配	vpc-iv-test	subnet-e2db	192.168.0.2...	未接入	运行中	-	标准模式 (反向代理)	c7n.large.4	包年包月	升级 续费 更多

- 步骤 5 查看独享引擎实例信息，如表 13-1 所示。

表 13-1 独享引擎实例关键参数说明

参数	说明	示例
实例名	创建实例时自动生成的名称。	-

参数	说明	示例
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
版本	独享引擎版本。	202304
模式	实例的部署模式。	标准模式(反向代理)
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。

须知

- 升级大约需要 5 分钟，执行升级前请注意：
- 当业务部署多个独享引擎实例时，如果您已经在 ELB 上配置了健康检查策略，系统会自动将流量切换到其它正在运行的独享引擎实例上，业务几乎无影响（可能会出现几秒的请求闪断重连）。
- 当业务只部署一个独享引擎实例，为了避免升级导致业务中断，在升级前请先配置 ELB，使流量不经过 WAF，然后再执行升级操作。当升级完成后，再配置 ELB 使流量切入 WAF。
- 当实例为最新版本时，“升级”按钮为灰化状态。

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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。

图 13-2 独享引擎列表

实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	报价	计费模式	操作
102b-6yY 3884dc3ee224380b57ba7e45...	未设置	vpc-4-test	subnet-e2db	192.168.0.8...	未接入	运行中	--	标准模式 (反向代理)	s7n.2large.2	按需计费	升级 删除 切换安全组
102703100-4A3q f1f2f3258ec488281022f40a90...	未设置	vpc-4-test	subnet-e2db	192.168.0.2...	未接入	运行中	--	标准模式 (反向代理)	c7n.large.4	包年包月	升级 续费 更多

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。

图 13-3 升级独享引擎实例版本

你确认要升级以下实例吗?

升级过程中实例不可用，请谨慎操作。

实例名	当前版本	待更新版本	版本信息
waf-gm-filemode-QEws	202304	202304	查看版本详情

为保证业务不受影响，升级前，请确认满足以下条件：


- 实例所在的ELB后端服务器组中存在多个活动实例，或该实例未接入业务
如果您的ELB后端服务器组中只存在单个实例，升级过程中服务页面无法正常加载。为避免对您业务的影响，请确保后端服务器组中存在多个活动实例。
- ELB已开启HTTP/HTTPS健康检查
配置健康检查后，ELB不会将流量分发到正在升级的实例，而是分发到健康检查正常的实例。实例升级完成后ELB会将其自动恢复到负载均衡服务中，承载业务流量。
- ELB已关闭会话保持
如果流量分配策略采用轮询模式，请关闭会话保持。会话保持开启后，一系列相关联的访问请求会保持分配到同一台实例上，升级时到达该实例的请求会发生异常。


---结束

回退独享引擎实例版本

仅支持回退到升级前的版本。

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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“更多 > 回退”。

步骤 6 在弹出的对话框中，确认满足并勾选以下三个条件后单击“确认”。

必须满足以下条件，才支持回退实例：


- 实例所在的 ELB 后端服务器组中存在多个活动实例，或该实例未接入业务。
- ELB 已开启 HTTP/HTTPS 健康检查。
- ELB 已关闭会话保持。


----结束

切换独享引擎实例安全组

当“实例类别”为“资源租户类”时，您可以切换独享引擎所属的安全组。切换安全组后，实例将受到该安全组访问规则的保护。

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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。

图 13-4 独享引擎列表



实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	规格	计费模式	操作
1026-kyv 388a9c3ee2243db0e57ab7a96...	未发现	vpc-ky-test	subnet-e2db	192.168.0.8...	未接入	运行中	--	标准模式 (反向代理)	s7n.2large.2	按量计费	升级 删除 切换安全组
102703100-4A3d 112f43258ec488281022f460a0...	未发现	vpc-ky-test	subnet-e2db	192.168.0.2...	未接入	运行中	--	标准模式 (反向代理)	c7n.large.4	包年包月	升级 续费 更多

步骤 5 在目标实例所在行的“操作”列，单击“更多 > 切换安全组”。

步骤 6 在弹出的对话框中，选择目标安全组后，单击“确认”，切换独享引擎实例安全组。

----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 单击管理控制台右上角的，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 (独享版)”。

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。

图 13-5 独享引擎列表



实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	规格	计费模式	操作
1028-9-V 3889dc3ce2243d2e572a7a95...	未设置	vpc-iv-test	subnet-e2db	192.168.0.8...	未接入	运行中	--	独享模式 (反向代理)	s7n.2xlarge.2	按量计费	升级 删除 切换安全组
102703100-4A3d 112f43258ec488281022f480a0...	未设置	vpc-iv-test	subnet-e2db	192.168.0.2...	未接入	运行中	--	独享模式 (反向代理)	c7n.large.4	包年包月	升级 续费 更多

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，输入“DELETE”后单击“确认”。

---结束

13.2 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。

查看产品信息

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的 ，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 (独享版)”。

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

13.3 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。

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。

开启告警通知

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 (独享版)”。

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，参数说明如图 13-6 表 13-2。

图 13-6 添加通知



添加通知

通知类型 **防护事件**

* 通知名称

通知描述
0/256

企业项目  

通知群组  [查看主题](#)

告警频率 分钟 次
在该时间间隔内，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 **全部** 自定义

确认

表 13-2 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。
企业项目	在下拉框中选择企业项目，该通知在选择的企业项目下生效。
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。

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

14 权限管理

14.1 IAM 权限管理

14.1.1 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 14.1.2 WAF 权限及授权项。

目前云服务平台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"
      ]
    }
  ]
}
```

14.1.2 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

权限	授权项
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
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:geoIpRule: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:geoIpRule: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
查询全局白名单规则列表	waf:falseAlarmMaskRule:list

权限	授权项
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:geoIpRule:list
查询防护域名列表	waf:instance:list
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

15 监控与审计

15.1 监控

15.1.1 WAF 监控指标说明

功能说明

本节定义了 Web 应用防火墙上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供管理控制台或 API 接口来检索 Web 应用防火墙产生的监控指标和告警信息。

命名空间

SYS.WAF

说明

命名空间是对一组资源和对象的抽象整合。在同一个集群内可创建不同的命名空间，不同命名空间中的数据彼此隔离。使得它们既可以共享同一个集群的服务，也能够互不干扰。

防护域名监控指标

表 15-1 WAF 防护域名监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
requests	请求量	该指标用于统计测量对象近 5 分钟内 WAF 返回的请求量的总数。 单位：次 采集方式：统计防护域名请求量的总数	≥ 0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_http_2xx	WAF 返回码 (2XX)	该指标用于统计测量对象近 5 分钟内 WAF 返回的 2XX 状态码的数量。 单位：次 采集方式：统计 WAF 引擎返回的 2XX 系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5 分钟
waf_http_3xx	WAF 返回码 (3XX)	该指标用于统计测量对象近 5 分钟内 WAF 返回的 3XX 状态码的数量。 单位：次 采集方式：统计 WAF 引擎返回的 3XX 系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5 分钟
waf_http_4xx	WAF 返回码 (4XX)	该指标用于统计测量对象近 5 分钟内 WAF 返回的 4XX 状态码的数量。 单位：次 采集方式：统计 WAF 引擎返回的 4XX 系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5 分钟
waf_http_5xx	WAF 返回码 (5XX)	该指标用于统计测量对象近 5 分钟内 WAF 返回的 5XX 状态码的数量。 单位：次 采集方式：统计 WAF 引擎返回的 5XX 系列状态响应码的数量	≥0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_fused_counts	WAF 熔断量	该指标用于统计测量对象近 5 分钟内被 WAF 熔断保护的请求数量。 单位：次 采集方式：统计防护域名被熔断保护的请求数量	≥ 0 次 值类型： Float	防护域名	5 分钟
inbound_traffic	入网总流量	该指标用于统计测量对象近 5 分钟内总入带宽的大小。 单位：Mbit 采集方式：统计近 5 分钟内总入带宽的大小	≥ 0 Mbit 值类型： Float	防护域名	5 分钟
outbound_traffic	出网总流量	该指标用于统计测量对象近 5 分钟内总出带宽的大小。 单位：Mbit 采集方式：统计近 5 分钟内总出带宽的大小	≥ 0 Mbit 值类型： Float	防护域名	5 分钟
waf_process_time_0	WAF 处理时延-区间 [0-10ms)	该指标用于统计测量对象近 5 分钟内 WAF 处理时延在区间 [0-10ms) 内的总数量。 单位：次 采集方式：统计近 5 分钟内 WAF 处理时延在区间 [0-10ms) 内的总数量	≥ 0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_process_time_10	WAF 处理时延-区间 [10-20ms)	该指标用于统计测量对象近 5 分钟内 WAF 处理时延在区间[10-20ms)内的总数量。 单位：次 采集方式：统计近 5 分钟内 WAF 处理时延在区间[10-20ms)内的总数量	≥0 次 值类型： Float	防护域名	5 分钟
waf_process_time_20	WAF 处理时延-区间 [20-50ms)	该指标用于统计测量对象近 5 分钟内 WAF 处理时延在区间[20-50ms)内的总数量。 单位：次 采集方式：统计近 5 分钟内 WAF 处理时延在区间[20-50ms)内的总数量	≥0 次 值类型： Float	防护域名	5 分钟
waf_process_time_50	WAF 处理时延-区间 [50-100ms)	该指标用于统计测量对象近 5 分钟内 WAF 处理时延在区间[50-100ms)内的总数量。 单位：次 采集方式：统计近 5 分钟内 WAF 处理时延在区间[50-100ms)内的总数量	≥0 次 值类型： Float	防护域名	5 分钟
waf_process_time_100	WAF 处理时延-区间 [100-1000ms)	该指标用于统计测量对象近 5 分钟内 WAF 处理时延在区间[100-1000ms)内的总数量。 单位：次 采集方式：统计近 5 分钟内 WAF 处理时延在区间[100-1000ms)内的总数量	≥0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
waf_process_time_1000	WAF 处理时延-区间 [1000+ms)	该指标用于统计测量对象近 5 分钟内 WAF 处理时延在区间[1000+ms)内的总数量。 单位：次 采集方式：统计近 5 分钟内 WAF 处理时延在区间 [1000+ms)内的总数量	≥0 次 值类型： Float	防护域名	5 分钟
qps_peak	QPS 峰值	该指标用于统计近 5 分钟内防护域名的 QPS 峰值。 单位：次 采集方式：统计近 5 分钟内防护域名的 QPS 峰值	≥0 次 值类型： Float	防护域名	5 分钟
qps_mean	QPS 均值	该指标用于统计近 5 分钟内防护域名的 QPS 均值。 单位：次 采集方式：统计近 5 分钟内防护域名的 QPS 均值	≥0 次 值类型： Float	防护域名	5 分钟
waf_http_0	无返回的 WAF 状态码	该指标用于统计测量对象近 5 分钟内 WAF 无返回的状态响应码的数量。 单位：次 采集方式：统计近 5 分钟内 WAF 无返回的状态响应码的数量	≥0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
upstream_code_2xx	业务返回码 (2XX)	该指标用于统计测量对象近 5 分钟内业务返回的 2XX 系列状态响应码的数量。 单位：次 采集方式：统计近 5 分钟内业务返回的 2XX 系列状态响应码的数量	≥ 0 次 值类型： Float	防护域名	5 分钟
upstream_code_3xx	业务返回码 (3XX)	该指标用于统计测量对象近 5 分钟内业务返回的 3XX 系列状态响应码的数量。 单位：次 采集方式：统计近 5 分钟内业务返回的 3XX 系列状态响应码的数量	≥ 0 次 值类型： Float	防护域名	5 分钟
upstream_code_4xx	业务返回码 (4XX)	该指标用于统计测量对象近 5 分钟内业务返回的 4XX 系列状态响应码的数量。 单位：次 采集方式：统计近 5 分钟内业务返回的 4XX 系列状态响应码的数量	≥ 0 次 值类型： Float	防护域名	5 分钟
upstream_code_5xx	业务返回码 (5XX)	该指标用于统计近 5 分钟内业务返回的 5XX 系列状态响应码的数量。 单位：次 采集方式：统计近 5 分钟内业务返回的 5XX 系列状态响应码的数量	≥ 0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
upstream_code_0	无返回的业务状态码	该指标用于统计测量对象近 5 分钟内业务无返回的状态响应码的数量。 单位：次 采集方式：统计近 5 分钟内业务无返回的状态响应码的数量	≥ 0 次 值类型： Float	防护域名	5 分钟
inbound_traffic_peak	入网流量的峰值	该指标用于统计近 5 分钟内防护域名入网流量的峰值。 单位：Mbit/s 采集方式：统计近 5 分钟内防护域名入网流量的峰值	≥ 0 Mbit/s 值类型： Float	防护域名	5 分钟
inbound_traffic_mean	入网流量的均值	该指标用于统计近 5 分钟内防护域名入网流量的均值。 单位：Mbit/s 采集方式：统计近 5 分钟内防护域名入网流量的均值	≥ 0 Mbit/s 值类型： Float	防护域名	5 分钟
outbound_traffic_peak	出网流量的峰值	该指标用于统计近 5 分钟内防护域名出网流量的峰值。 单位：Mbit/s 采集方式：统计近 5 分钟内防护域名出网流量的峰值	≥ 0 Mbit/s 值类型： Float	防护域名	5 分钟
outbound_traffic_mean	出网流量的均值	该指标用于统计近 5 分钟内防护域名出网流量的均值。 单位：Mbit/s 采集方式：统计近 5 分钟内防护域名出网流量的均值	≥ 0 Mbit/s 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
attacks	攻击总次数	该指标用于统计近 5 分钟内防护域名攻击请求量的总数。 单位：次 采集方式：统计近 5 分钟内防护域名攻击请求量的总数	≥0 次 值类型： Float	防护域名	5 分钟
crawlers	爬虫攻击次数	该指标用于统计近 5 分钟内防护域名爬虫攻击请求量的总数。 单位：次 采集方式：统计近 5 分钟内防护域名爬虫攻击请求量的总数	≥0 次 值类型： Float	防护域名	5 分钟
base_protection_counts	web 基础防护次数	该指标用于统计近 5 分钟内由 Web 基础防护规则防护的攻击数量。 单位：次 采集方式：统计近 5 分钟内由 Web 基础防护规则防护的攻击数量	≥0 次 值类型： Float	防护域名	5 分钟
precise_protection_counts	精准防护次数	该指标用于统计近 5 分钟内由精准防护规则防护的攻击数量。 单位：次 采集方式：统计近 5 分钟内由精准防护规则防护的攻击数量	≥0 次 值类型： Float	防护域名	5 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
cc_protection_counts	cc 防护次数	该指标用于统计近 5 分钟内由 CC 防护规则防护的攻击数量。 单位：次 采集方式：统计近 5 分钟内由 CC 防护规则防护的攻击数量。	≥0 次 值类型： Float	防护域名	5 分钟

独享引擎实例监控指标

表 15-2 WAF 独享引擎实例监控指标

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
cpu_util	CPU 使用率	该指标用于统计测量对象的 CPU 利用率。 单位：百分比 采集方式： 100%减去空闲 CPU 占比	0~100 % 值类型： Float	独享引擎实例	1 分钟
mem_util	内存使用率	该指标用于统计测量对象的内存利用率。 单位：百分比 采集方式： 100%减去空闲内存占比	0~100 % 值类型： Float	独享引擎实例	1 分钟
disk_util	磁盘使用率	该指标用于统计测量对象的磁盘利用率。 单位：百分比 采集方式： 100%减去空闲磁盘占比	0~100 % 值类型： Float	独享引擎实例	1 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
disk_avail_size	磁盘可用空间	该指标用于统计测量对象的磁盘可用空间。 单位：byte、KB、MB、GB、TB、PB 采集方式：空闲磁盘空间大小	≥ 0 byte 值类型： Float	独享引擎实例	1 分钟
disk_read_bytes_rate	磁盘读速率	该指标用于统计测量对象每秒从磁盘读取的字节数。 单位：byte/s、KB/s、MB/s、GB/s 采集方式：每秒从磁盘读取的字节数	≥ 0 byte/s 值类型： Float	独享引擎实例	1 分钟
disk_write_bytes_rate	磁盘写速率	该指标用于统计测量对象每秒写入磁盘的字节数。 单位：byte/s、KB/s、MB/s、GB/s 采集方式：每秒写入磁盘的字节数	≥ 0 byte/s 值类型： Float	独享引擎实例	1 分钟
disk_read_requests_rate	磁盘读操作速率	该指标用于统计测量对象每秒从磁盘读取的请求数。 单位：请求/秒 采集方式：每秒磁盘处理的读取请求数	≥ 0 request/s 值类型： Float	独享引擎实例	1 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
disk_write_requests_rate	磁盘写操作速率	该指标用于统计测量对象每秒写入数据到磁盘的请求次数。 单位：请求/秒 采集方式：每秒磁盘处理的写入请求数	≥ 0 request/s 值类型： Float	独享引擎实例	1 分钟
network_incoming_bytes_rate	网络流入速率	该指标用于统计测量对象每秒流入测量对象的网络流量。 单位： byte/s、KB/s、MB/s、GB/s 采集方式：每秒从网络适配器输入的流量	≥ 0 byte/s 值类型： Float	独享引擎实例	1 分钟
network_outgoing_bytes_rate	网络流出速率	该指标用于统计测量对象每秒流出测量对象的网络流量。 单位： byte/s、KB/s、MB/s、GB/s 采集方式：每秒从网络适配器输出的流量	≥ 0 byte/s 值类型： Float	独享引擎实例	1 分钟
network_incoming_packets_rate	网络流入包速率	该指标用于统计测量对象每秒流入测量对象的数据包数量。 单位： packet/s 采集方式：每秒从网络适配器流入的数据包数	≥ 0 packet/s 值类型： Int	独享引擎实例	1 分钟

指标 ID	指标名称	指标含义	取值范围	测量对象	监控周期 (原始指标)
network_outgoing_packets_rate	网络流出包速率	该指标用于统计测量对象每秒流出测量对象的数据包数量。 单位： packet/s 采集方式：每秒从网络适配器流出的数据包数	≥0 packet/s 值类型： Int	独享引擎实例	1 分钟
concurrent_connections	并发连接数	该指标用于统计测量对象当前处理的并发连接数量。 单位：count 采集方式：系统当前的并发连接数量	≥0 count 值类型： Int	独享引擎实例	1 分钟
active_connections	活跃连接数	该指标用于统计测量对象当前打开的连接数量。 单位：count 采集方式：系统当前的活跃连接数量	≥0 count 值类型： Int	独享引擎实例	1 分钟
latest_policy_sync_time	最近一次策略同步的耗时	该指标用于统计测量对象最近一次同步 WAF 策略的耗时。 单位：ms 采集方式：最近一次同步 WAF 策略的耗时	≥0 ms 值类型： Int	独享引擎实例	1 分钟

维度

Key	Value
instance_id	WAF 独享引擎实例 ID

Key	Value
waf_instance_id	WAF 防护网站 ID

监控指标原始数据格式样例

```
[
  {
    "metric": {
      // 命名空间
      "namespace": "SYS.WAF",
      "dimensions": [
        {
          // 维度名称, 例如防护网站
          "name": "waf_instance_id",
          // 该维度下的监控对象 ID, 例如防护网站 ID
          "value": "082db2f542e0438aa520035b3e99cd99"
        }
      ],
      // 指标 ID
      "metric_name": "waf_http_2xx"
    },
    // 生存时间, 指标预定义
    "ttl": 172800,
    // 指标值
    "value": 0.0,
    // 指标单位
    "unit": "Count",
    // 指标值类型
    "type": "float",
    // 指标采集时间
    "collect_time": 1637677359778
  }
]
```

15.1.2 设置监控告警规则


通过设置 WAF 告警规则，用户可自定义监控目标与通知策略，设置告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数，帮助您及时了解 WAF 防护状况，从而起到预警作用。


前提条件

5 网站接入 WAF

设置监控告警规则

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“管理与部署 > 云监控服务 CES”。
- 步骤 4** 在左侧导航树栏，选择“告警 > 告警规则”，进入“告警规则”页面。
- 步骤 5** 在页面右上方，单击“创建告警规则”，进入“创建告警规则”界面。
- 步骤 6** 配置相关参数。
- 名称：自定义规则名称。
 - 告警类型：选择“指标”。
 - 云产品：选择“Web 应用防火墙-独享实例”或“Web 应用防火墙-防护域名”。
 - 独享实例监控指标选择“Web 应用防火墙-独享实例”。
 - 防护域名监控指标选择“Web 应用防火墙-防护域名”。
 - 监控范围：全部资源。
 - 触发规则：选择“关联模板”，或者自定义创建模板。
 - 发送通知：如果希望实时收到告警信息，开启该选项，并选择通知方式。
 - 其他参数：根据实际情况配置。
- 步骤 7** 单击“立即创建”，在弹出的提示框中，单击“确定”，告警规则创建成功。

---结束



15.1.3 查看监控指标

您可以通过 CES 管理控制台，查看 WAF 的相关指标，及时了解 WAF 防护状况，并通过指标设置防护策略。

前提条件

WAF 已对接云监控，即已在云监控页面设置监控告警规则。有关设置监控告警规则的详细操作，请参见 1515.115.1.2 设置监控告警规则。

查看监控指标

- 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“管理与部署 > 云监控服务 CES”。
- 步骤 4** 在左侧导航树栏，选择“云服务监控 > Web 应用防火墙”，进入“云服务监控”页面。
- 步骤 5** 在目标独享实例或防护域名所在行的“操作”列中，单击“查看监控指标”，查看对象的指标详情。

说明

在“网站设置”列表中，目标域名所在行的“操作”列，单击“云监控”，可直接查看单个网站的监控信息。

---结束

15.2 审计

15.2.1 云审计服务支持的 WAF 操作列表

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

表 15-3 云审计服务支持的 WAF 操作列表

操作名称	资源类型	事件名称
创建 Web 应用防火墙防护实例	instance	createInstance
删除 Web 应用防火墙防护实例	instance	deleteInstance
更新 Web 应用防火墙防护实例	instance	alterInstanceName
修改 Web 应用防火墙防护实例的防护状态	instance	modifyProtectStatus
修改 Web 应用防火墙防护实例的接入状态	instance	modifyAccessStatus
创建 Web 应用防火墙防护策略	policy	createPolicy
应用 Web 应用防火墙防护策略	policy	applyToHost
更新 Web 应用防火墙防护策略	policy	modifyPolicy
删除 Web 应用防火墙防护策略	policy	deletePolicy
添加证书	certificate	createCertificate
修改证书名称	certificate	modifyCertificate
删除证书	certificate	deleteCertificate
创建 CC 规则	policy	createCc
修改 CC 规则	policy	modifyCc
删除 CC 规则	policy	deleteCc
创建精准防护规则	policy	createCustom
修改精准防护规则	policy	modifyCustom
删除精准防护规则	policy	deleteCustom
创建 IP 黑白名单规则	policy	createWhiteblackip
修改 IP 黑白名单规则	policy	modifyWhiteblackip

操作名称	资源类型	事件名称
删除 IP 黑白名单规则	policy	deleteWhiteblackip
创建/刷新网页防篡改规则	policy	createAntitamper
删除网页防篡改规则	policy	deleteAntitamper
创建全局白名单规则	policy	createIgnore
删除全局白名单规则	policy	deleteIgnore
创建隐私屏蔽规则	policy	createPrivacy
修改隐私屏蔽规则	policy	modifyPrivacy
删除隐私屏蔽规则	policy	deletePrivacy

15.2.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对 OBS 桶中数据的操作。云审计服务管理控制台会保存最近 7 天的操作记录。


本节介绍如何在云审计服务管理控制台查看或导出最近 7 天的操作记录：




- [在新版事件列表查看审计事件](#)
- [在旧版事件列表查看审计事件](#)

使用限制


- 用户通过云审计控制台只能查询最近 7 天的操作记录。如果需要查询超过 7 天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在 OBS 桶或 LTS 日志组里面查看历史事件信息。否则，您将无法追溯 7 天以前的操作记录。
- 云上操作后，1 分钟内可以通过云审计控制台查询管理类事件操作记录，5 分钟后才可通过云审计控制台查询数据类事件操作记录。



在新版事件列表查看审计事件

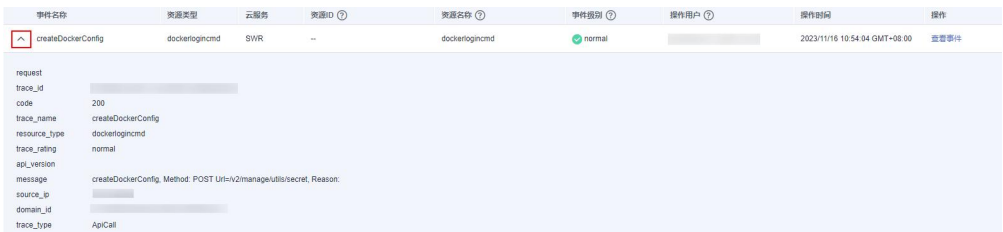
1. 登录管理控制台。
2. 单击左上角 ，选择“管理与部署 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
 - 事件名称：输入事件的名称。

- 事件 ID: 输入事件 ID。
 - 资源名称: 输入资源的名称, 当该事件所涉及的云资源无资源名称或对应的 API 接口操作不涉及资源名称参数时, 该字段为空。
 - 资源 ID: 输入资源 ID, 当该资源类型无资源 ID 或资源创建失败时, 该字段为空。
 - 云服务: 在下拉框中选择对应的云服务名称。
 - 资源类型: 在下拉框中选择对应的资源类型。
 - 操作用户: 在下拉框中选择一个或多个具体的操作用户。
 - 事件级别: 可选项为“normal”、“warning”、“incident”, 只可选择其中一项。
 - normal: 表示操作成功。
 - warning: 表示操作失败。
 - incident: 表示比操作失败更严重的情况, 例如引起其他故障等。
 - 时间范围: 可选择查询最近 1 小时、最近 1 天、最近 1 周的操作事件, 也可以自定义最近 7 天内任意时间段的操作事件。
5. 在事件列表页面, 您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
- 在搜索框中输入任意关键字, 按下 Enter 键, 可以在事件列表搜索符合条件的数据。
 - 单击“导出”按钮, 云审计服务会将查询结果以.xlsx 格式的表格文件导出, 该.xlsx 文件包含了本次查询结果的所有事件, 且最多导出 5000 条信息。
 - 单击  按钮, 可以获取到事件操作记录的最新信息。
 - 单击  按钮, 可以自定义事件列表的展示信息。启用表格内容折行开关 , 可让表格内容自动折行, 禁用此功能将会截断文本, 默认停用此开关。
6. 关于事件结构的关键字段详解, 请参见“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
7. (可选) 在新版事件列表页面, 单击右上方的“返回旧版”按钮, 可切换至旧版事件列表页面。

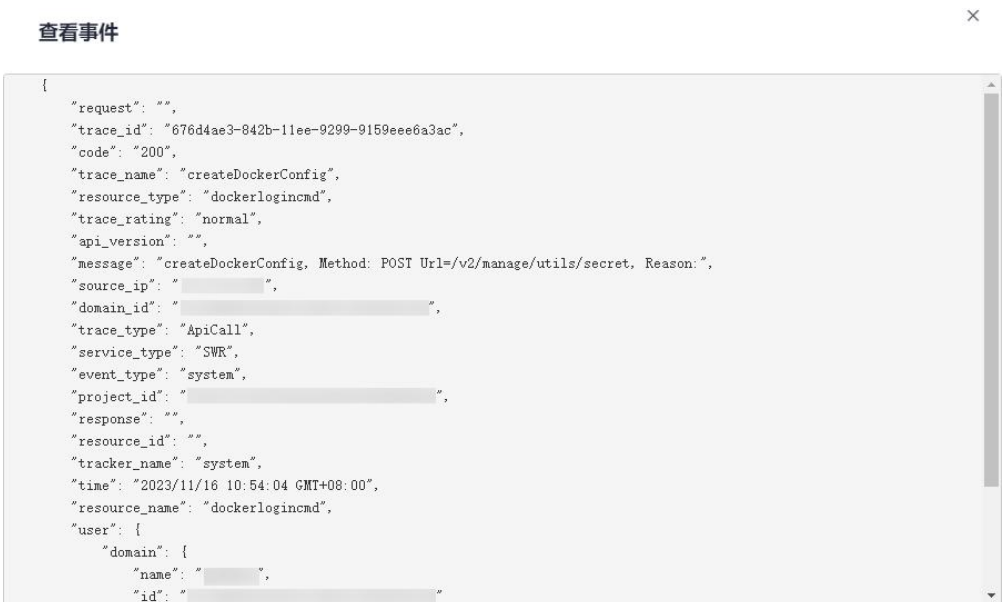
在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 , 选择“管理与部署 > 云审计服务 CTS”, 进入云审计服务页面。
3. 单击左侧导航树的“事件列表”, 进入事件列表信息页面。
4. 用户每次登录云审计控制台时, 控制台默认显示新版事件列表, 单击页面右上方的“返回旧版”按钮, 切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询, 详细信息如下:
 - 事件类型、事件来源、资源类型和筛选类型, 在下拉框中选择查询条件。
 - 筛选类型按资源 ID 筛选时, 还需手动输入某个具体的资源 ID。
 - 筛选类型按事件名称筛选时, 还需选择某个具体的事件名称。

- 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
 - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
 - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
 - 时间范围：可选择查询最近 1 小时、最近 1 天、最近 1 周的操作事件，也可以自定义最近 7 天内任意时间段的操作事件。
 - 单击“导出”按钮，云审计服务会将查询结果以 CSV 格式的表格文件导出，该 CSV 文件包含了本次查询结果的所有事件，且最多导出 5000 条信息。
6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
- 单击“导出”按钮，云审计服务会将查询结果以 CSV 格式的表格文件导出，该 CSV 文件包含了本次查询结果的所有事件，且最多导出 5000 条信息。
 - 单击  按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击  展开该记录的详细信息。



9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的“云审计服务事件参考 > 事件结构”章节和“云审计服务事件参考 > 事件样例”章节。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

16 常见问题

16.1 产品咨询

16.1.1 WAF 基础知识

本章节为您罗列了 WAF 入门级的常见问题。

Web 应用防火墙是硬防火墙还是软防火墙？

Web 应用防火墙是软防火墙。

有关域名接入 WAF 的详细操作，请参见 9 网站设置。

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器进行任何操作（例如关机或重启）。

Web 应用防护墙可以部署在 VPC 内网吗？

可以。独享版 WAF 的独享引擎实例部署在 VPC 内。

独享版 WAF 是否支持跨 VPC 防护？

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不在同一个 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。

Web 应用防火墙支持哪些操作系统？

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

Web 应用防火墙提供的是几层防护？

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

Web 应用防火墙如何拦截请求内容？

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

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。

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。

Web 应用防火墙是否支持健康检查？

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

Web 应用防火墙是否支持 SSL 双向认证？

不支持。您可以在 WAF 上配置单向的 SSL 证书。

说明

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

Web 应用防火墙支持基于应用层协议和内容的访问控制吗？

WAF 支持应用层协议和内容的访问控制，应用层协议支持 HTTP 和 HTTPS。

Web 应用防火墙是否可以对用户添加的 Post 的 body 进行检查？

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

您可以通过配置精准访问防护规则，对添加的 Post 的 body 进行检查。

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。

Web 应用防火墙支持拦截包含特殊字符的 URL 请求吗？

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

Web 应用防火墙可以防止垃圾注册和恶意注册吗？

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

WAF 通过对 HTTP(S)请求进行检测，可以识别并阻断 Web 服务的网络攻击（SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等）。

Web 应用防火墙可以拦截 Web 页面调用其他接口的请求数据吗？

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

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

Web 应用防火墙可以设置域名限制访问吗？

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

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

Web 应用防火墙有 IPS 入侵防御系统模块吗？

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

WAF 支持弹性伸缩功能吗？

WAF 暂不支持弹性伸缩功能。

HTTP 2.0 业务接入 WAF 防护是否会对源站有影响？

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

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。

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。

如果证书挂载在 ELB 上，WAF 可以根据请求内容进行拦截吗？

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

源站 IP 地址服务器更换安全组后，在 WAF 中需要做更改吗？

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

源站开启 gzip 对 WAF 有影响吗？

如果源站开启 gzip，WAF 可能误拦截源站正常访问请求。如果确认拦截的为正常访问请求，您可以参照 6.2 处理误报事件将该事件处理为误报事件。处理后，WAF 将不再拦截该事件，即“防护事件”页面中将不再显示该攻击事件，您也不会收到该攻击事件的告警通知。

多个域名对应同一源站，Web 应用防火墙可以防护这些域名吗？

可以。不同域名对应同一个源站时，您可以将这些域名都接入 WAF 进行防护。

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

什么是防护 IP？

防护 IP 是指需要保护的网站的 IP 地址。

更换 IP 后，需要重新将域名添加到 WAF 吗？

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

Web 应用防火墙支持漏洞检测吗？

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

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。

WAF 是否支持防护 CS 架构的网站？

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

如何查看当前 WAF 业务 QPS 的使用情况和流入的流量？

您可以在源站上，查看源站 IP 地址的带宽/QPS 使用情况流入的流量。

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

WAF 支持拦截 multipart/form-data 格式的数据包。

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

WAF 支持防御哪些 CVE 漏洞？

WAF 支持防御的 CVE 漏洞：CVE-2017-7525、CVE-2019-17571、CVE-2018-1270、CVE-2016-100027、CVE-2022-22965、CVE-2022-22968、CVE-2018-20318。

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。

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。

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。

16.1.2 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。

16.1.3 Web 应用防火墙支持对哪些对象进行防护？

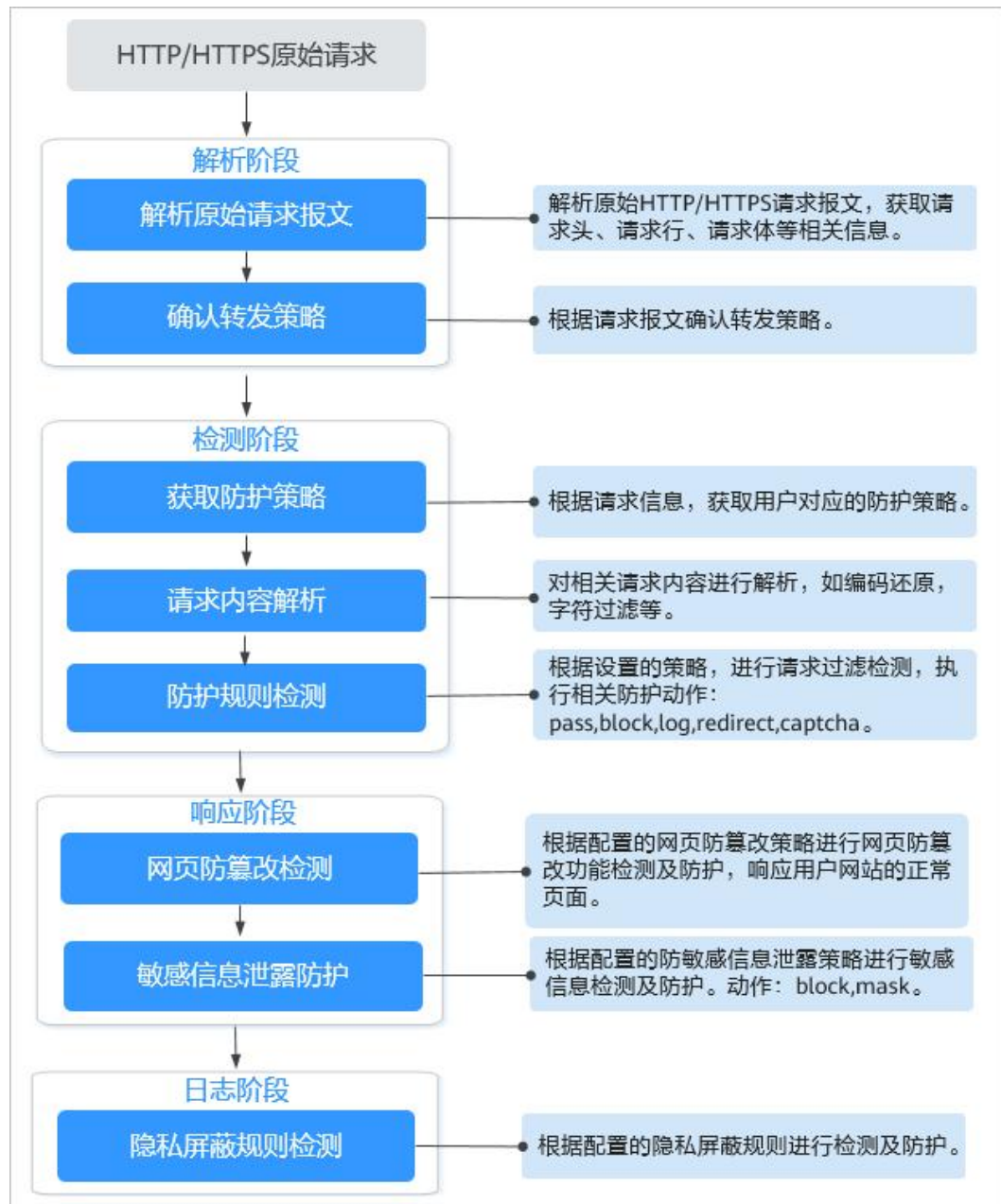
WAF 支持对域名或 IP 进行防护。

16.1.4 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



16.1.5 Web 应用防火墙是否支持 IPv4 和 IPv6 共存？

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

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

16.1.6 WAF 和 HSS 的网页防篡改有什么区别？

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

WAF 网页防篡改为用户提供应用层的防护，对网站的静态网页进行缓存，当用户访问网站时返回给用户缓存的正常页面，并随机检测网页是否被篡改。

网页防篡改的区别

HSS 与 WAF 网页防篡改的区别，如表 16-1 所示。

表 16-1 HSS 和 WAF 网页防篡改的区别

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

如何选择网页防篡改

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

16.1.7 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

16.1.8 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。

16.1.9 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 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



16.1.10 Web 应用防火墙和云防火墙有什么区别？

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

WAF 和 CFW 的主要区别说明如表 16-2 所示。

表 16-2 WAF 和 CFW 的主要区别说明

类别	Web 应用防火墙	云防火墙
----	-----------	------

类别	Web 应用防火墙	云防火墙
定义	Web 应用防火墙（Web Application Firewall, WAF），通过对 HTTP(S) 请求进行检测，识别并阻断 SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护 Web 服务安全稳定。	云防火墙（Cloud Firewall, CFW）是新一代的云原生防火墙，提供云上互联网边界和 VPC 边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持 AI 提升智能防御能力满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。
防护机制	网站成功接入 WAF 后，WAF 作为一个反向代理存在于客户端和服务器之间，网站所有访问请求将先流转到 WAF，WAF 检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。	CFW 可对全流量进行精细化管理，包括互联网边界防护，跨 VPC，NAT 流量防护，防止外部入侵、内部渗透攻击和从内到外的非法访问。
部署模式	业务服务器部署在天翼云，防护对象为域名或 IP。大型企业网站，具备较大的业务规模且基于业务特性具有制定个性化防护规则的安全需求。	互联网边界和 VPC 边界
防护对象	域名或 IP	弹性公网 IP 和 VPC
功能特性	SQL 注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC 攻击、恶意爬虫扫描、跨站请求伪造等攻击防护。	<ul style="list-style-type: none"> ● 资产管理与入侵防御：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 ● 访问控制：支持互联网边界访问流量的访问控制。 ● 流量分析与日志审计：VPC 间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。

16.1.11 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。

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

SQL（Structured Query Language）注入攻击是一种常见的 Web 攻击方法，攻击者通过把 SQL 命令注入到数据库的查询字符串中，最终达到欺骗服务器执行恶意 SQL 命令的目的。例如，可以从数据库获取敏感信息，或者利用数据库的特性执行添加用户、导出文件等一系列恶意操作，甚至有可能获取数据库乃至系统用户最高权限。

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

WAF 针对 SQL 注入攻击的检测原理

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

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

WAF 针对 XSS 攻击的检测原理

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

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

说明

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

WAF 针对 PHP 攻击的检测原理

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

16.1.13 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）。

参考以下配置方法完成配置。

配置方法

步骤 1 4 申请 WAF 独享引擎。

步骤 2 将网站域名添加到 WAF 中并完成域名接入，详细操作请参见 55.1 将网站接入 WAF 防护。

步骤 3 将 Web 基础防护的状态设置为“拦截”模式，详细操作请参见 7.2 配置 Web 基础防护规则防御常见 Web 攻击。

---结束

16.1.14 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

16.1.15 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。

16.1.16 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

$$\text{QPS} = \text{请求数/秒 (req/sec)}$$

“安全总览”页面中 QPS 的计算方式说明如表 16-3 所示。

表 16-3 QPS 取值说明

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

时间段	QPS 平均取值说明	QPS 峰值取值说明
“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

16.1.17 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。

📖 说明

以下配置中，WAF 不会在客户请求 Cookie 中插入 HWWAFSESID（会话 ID），HWWAFSESTIME（会话时间戳）字段：

- 防护动作配置为“放行”的规则。
- 全局白名单规则中“不检测模块”选择了“所有检测模块”。
- 防护模式为“暂停防护”。
- 未开启 Web 基础防护。

16.2 购买和变更规格

16.2.1 主账号与子账号的权限有哪些区别？

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

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

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

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

16.2.2 Web 应用防火墙是否支持多个账号共享使用？

WAF 不支持多个账号共享使用，每个账号需要单独购买 WAF 进行部署。

16.2.3 QPS 超过当前 WAF 版本支持的峰值时有什么影响？

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

独享版 WAF 支持的 QPS 规格说明：


- 单实例规格的正常业务请求峰值：
 - WAF 实例规格选择 WI-500，参考性能：
 - 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：
 - HTTP 业务：建议 QPS 1,000；极限 QPS 2,000
 - HTTPS 业务：建议 QPS 800；极限 QPS 1,600
 - Websocket 业务：支持最大并发连接 1,000
 - 最大回源长连接：60,000
- CC 攻击防护峰值：
 - 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

16.2.4 如何查看防护网站的入带宽和出带宽信息？

在“安全总览”页面，您可以查看防护网站或实例的带宽信息，操作步骤如下。

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角的 ，选择区域或项目。

步骤 3 单击页面左上方的 ，选择“安全 > Web 应用防火墙 (独享版)”。

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

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

---结束

16.3 计费

16.3.1 Web 应用防火墙可以免费使用吗？

WAF 为收费服务，需要购买后才能使用。Web 应用防火墙独享模式支持按需计费（后付费）模式，从开通并使用 WAF 开始计费到关闭按需计费时结束计费，按实际使用时长计费。

内容安全检测支持包年/包月（预付费）和按需计费（后付费）两种计费方式。

- 文本安全监测（按年）
- 文本安全监测（按月）
- 内容安全单次检测（按需）

按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。例如：单次配置了 10 个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行 10 次收费。

16.3.2 Web 应用防火墙如何收费？

Web 应用防火墙独享模式支持按需计费（后付费）模式，从开通并使用 WAF 开始计费到关闭按需计费时结束计费，按实际使用时长计费。

内容安全检测支持包年/包月（预付费）和按需计费（后付费）两种计费方式。

- 文本安全监测（按年）
- 文本安全监测（按月）
- 内容安全单次检测（按需）


按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。例如：单次配置了 10 个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行 10 次收费。


16.3.3 如何退订 Web 应用防火墙？

如果您需要退订以按需计费方式购买的独享模式 WAF，前往“独享引擎”页面，直接删除独享引擎实例即可，删除实例后，将停止计费。

操作步骤

步骤 1 登录管理控制台。

步骤 2 单击管理控制台右上角的，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 (独享版)”。

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。

图 16-4 独享引擎列表



实例名	防护网站	VPC	子网	IP地址	接入状态	运行状态	版本	模式	计费	操作
10276-6vY 3884dc3ee2243db657ba7e65...	未设置	vpc-9-test	subnet-e2db	192.168.0.8...	未接入	运行中	--	标准模式 (反向代理)	按量计费	升级 删除 切换安全组
102703100-4A3q 1f12f3258ec488281022f4ba0a0...	未设置	vpc-9-test	subnet-e2db	192.168.0.2...	未接入	运行中	--	标准模式 (反向代理)	包年包月	升级 续费 更多

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，输入“DELETE”后单击“确认”。

---结束

16.4 网站接入

16.4.1 独享模式如何防护不支持的非标准端口？

当独享模式不支持防护域名的非标准端口时，您可以通过配置 ELB 将流量引流到独享模式任一支持的非标准端口，以防护不支持的非标准端口。有关独享模式支持防护的非标准端口，请参见 5.2WAF 支持的端口范围。

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



须知

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

请参照以下操作步骤进行配置。


步骤 1 登录管理控制台。

步骤 2 在 WAF 管理控制台添加防护域名。

- 单击页面左上方的 ，选择“安全 > Web 应用防火墙”。
- 单击页面左上方的 ，选择“安全 > Web 应用防火墙 (独享版)”。
- 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
- 在网站列表左上角，单击“添加防护网站”，选择“独享模式”后，添加“www.example.com:1234”对应的泛域名“*.example.com”，在“防护对象端口”下拉框中选择任一端口（如“81”）。
- “是否已使用代理”，选择“是”，单击“确认”，防护网站添加成功。

6. 关闭弹出的对话框。
您可以在防护网站列表中查看已添加防护网站。

步骤 3 在 ELB 管理控制台配置负载均衡。

1. 单击页面左上方的 ，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。
2. 在负载均衡器所在行的“名称”列，单击目标负载均衡器名称，进入 ELB “基本信息”页面。
3. 在“跨 VPC 后端”所在行，单击“跨 VPC 后端”，并在弹框中单击“确定”，开启跨 VPC 后端。
4. 选择“监听器”页签后，单击“添加监听器”，配置监听器端口为“1234”。
5. 单击“下一步：配置后端分配策略”，配置后端分配策略。
6. 单击“下一步：添加后端服务器”，并选择“跨 VPC 后端”页签，添加跨 VPC 后端和健康检查。
7. 单击“添加跨 VPC 后端”，在弹出的弹框中，配置“跨 VPC 的后端 IP”和“后端端口”。
 - 跨 VPC 后端 IP：WAF 独享引擎的 IP（在“独享引擎”列表中获取）。
 - 后端端口：“81”（与步骤 2.4 中配置的端口一致）。
8. 单击“确定”，配置完成。
9. 单击“下一步：确认配置”后单击“提交”。

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

---结束

16.4.2 如何在添加域名中配置防护域名？

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

相关概念

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

说明

一个泛域名算一个域名。

- 单域名
单域名又称普通域名，是相对泛域名来说的，是一个具体的域名或者说不是通配符域名。
例如：“www.example.com”或“example.com”都算一个单域名。

📖 说明

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

如何选择域名类型

WAF 支持防护单域名和泛域名。

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

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

📖 说明

建议添加的“防护域名”与在 DNS 服务商处设置的域名保持一致。

同时在 WAF 中添加单域名和泛域名，WAF 会优先检测哪个域名？

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

16.4.3 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，在防护端口下拉列表中选择非标准端口。

16.4.4 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。

16.4.5 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。

16.4.6 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。

16.4.7 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？

背景

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。

原因

可能是由于您的域名已在其他账号下添加到了 WAF。同一个域名不支持重复添加到 WAF。

解决办法

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。

16.4.8 域名接入 Web 应用防火墙后，能通过 IP 访问网站吗？

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

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。

16.5 防护规则

16.5.1 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 16-4 所示。

表 16-4 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规则，再开启“严格”模式，使 WAF 能有效防护更多攻击。

16.5.2 CC 攻击的防护峰值是多少？

各版本对应的 CC 攻击防护峰值如表 16-5 所示。

表 16-5 适用的业务规格

业务规格	独立模式
------	------

业务规格	独享模式
正常业务请求峰值	以下数据为单实例规格： <ul style="list-style-type: none">•

16.5.3 在什么情况下使用 Cookie 区分用户？

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

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

16.5.4 CC 规则里“限速频率”和“放行频率”的区别？

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

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

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

区别

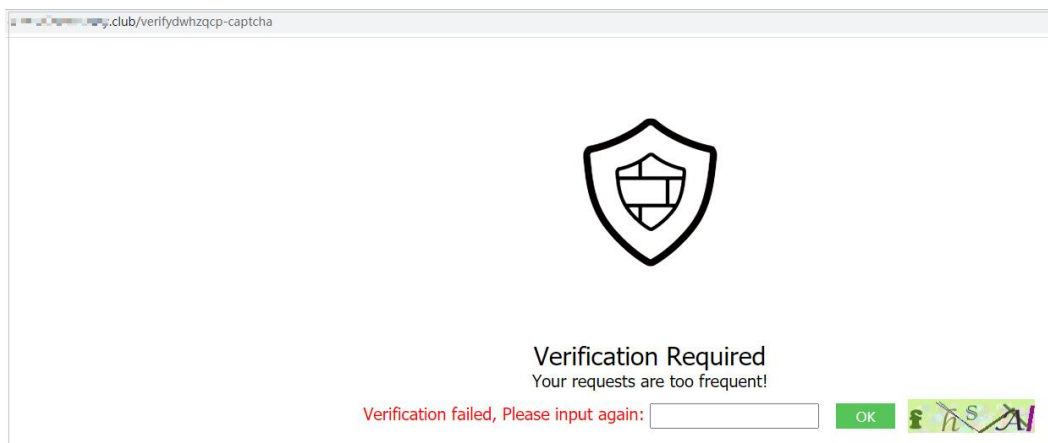
- “放行频率”和“限速频率”的限速周期一致。
- “放行频率”小于等于“限速频率”，且“放行频率”可为 0。

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

故障现象

在 WAF 上开启“CC 攻击防护”，添加“防护动作”为“人机验证”的规则后，访问网站，验证码不能刷新，验证一直不通过，如图 16-5 所示。

图 16-5 验证码一直验证不通过



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

可能原因

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

处理建议

在 CDN 上，将缓存的静态 URL 设置为放行，操作步骤如下。

须知

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



- 步骤 1 登录管理控制台。
- 步骤 2 单击管理控制台左上角的 ，选择区域或项目。
- 步骤 3 单击页面左上方的 ，选择“CDN 与智能边缘 > 内容分发网络 CDN”，进入 CDN 页面。
- 步骤 4 在左侧导航树中，选择“域名管理”，进入“域名管理”页面。
- 步骤 5 在“域名”列，单击目标域名的名称，进入域名配置页面。
- 步骤 6 选择“缓存配置”页签，单击“编辑”，系统弹出“配置缓存策略”对话框。
- 步骤 7 单击“添加”，添加两条缓存策略规则，如图 16-6 所示，相关参数说明如图 16-6 表 16-6 所示。

图 16-6 “配置缓存策略”对话框



表 16-6 配置静态 URL 缓存策略参数说明

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

步骤 8 单击“确定”，完成缓存规则配置，如图 16-7 所示。

图 16-7 完成缓存规则配置



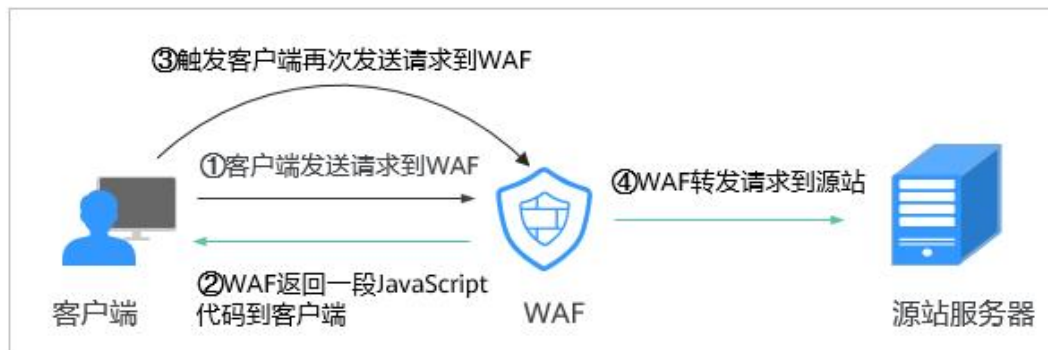
配置完成后，请等待 3~5 分钟，待配置的缓存策略生效后，再访问网站使用验证码功能。

---结束

16.5.6 开启 JS 脚本反爬虫后，为什么客户端请求获取页面失败？

开启 JS 脚本反爬虫后，当客户端发送请求时，WAF 会返回一段 JavaScript 代码到客户端。如果客户端是正常浏览器访问，就可以触发这段 JavaScript 代码再发送一次请求到 WAF，即 WAF 完成 JS 验证，并将该请求转发给源站，如图 16-8 所示。

图 16-8 JS 脚本反爬虫正常检测流程



须知

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

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

16.5.7 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗？

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

图 16-9 开启“其他爬虫”

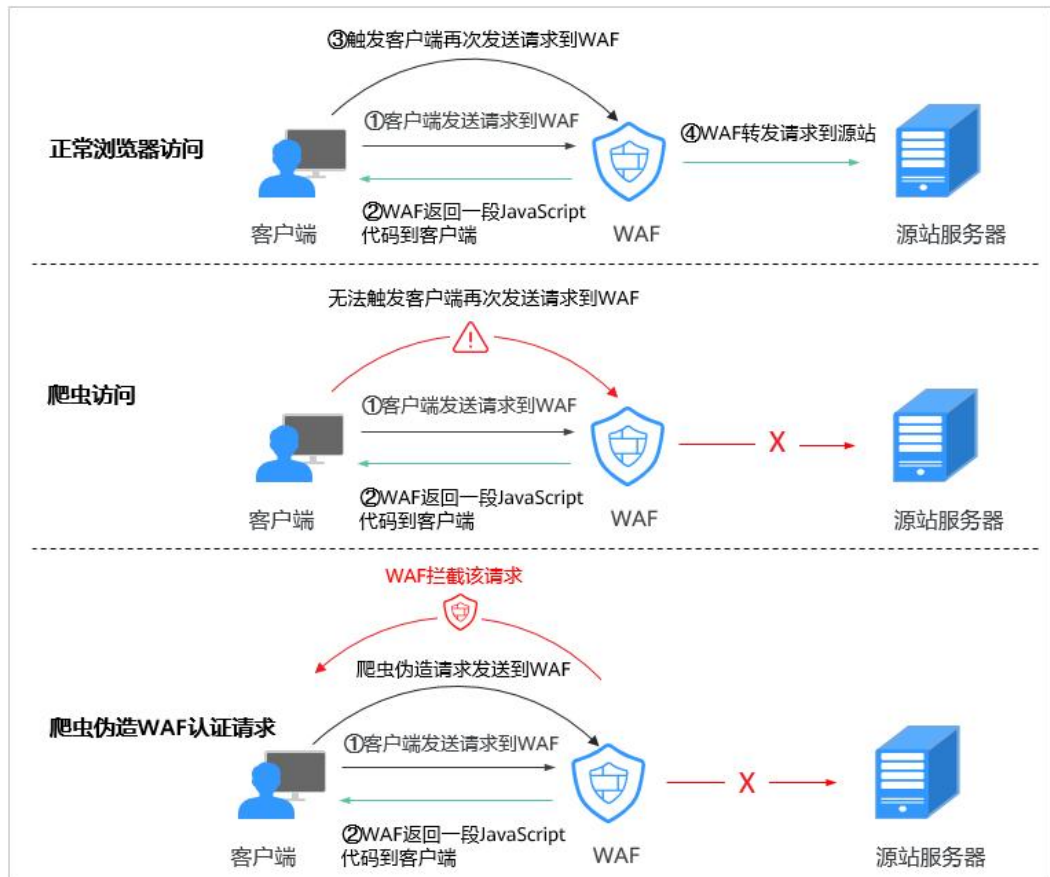


有关配置网站反爬虫的详细操作，请参见 7.8 配置网站反爬虫防护规则防御爬虫攻击。

16.5.8 JS 脚本反爬虫的检测机制是怎么样的？

JS 脚本检测流程如图 16-10 所示，其中，①和②称为“js 挑战”，③称为“js 验证”。

图 16-10 JS 脚本检测流程说明



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

- 如果客户端是正常浏览器访问，就可以触发这段 JavaScript 代码再发送一次请求到 WAF，即 WAF 完成 js 验证，并将该请求转发给源站。
- 如果客户端是爬虫访问，就无法触发这段 JavaScript 代码再发送一次请求到 WAF，即 WAF 无法完成 js 验证。
- 如果客户端爬虫伪造了 WAF 的认证请求，发送到 WAF 时，WAF 将拦截该请求，js 验证失败。

通过统计“js 挑战”和“js 验证”，就可以汇总出 JS 脚本反爬虫防御的请求次数。例如，图 16-11 中 JS 脚本反爬虫共记录了 18 次事件，其中，“js 挑战”（WAF 返回 JS 代码）为 16 次，“js 验证”（WAF 完成 JS 验证）为 2 次，“其他”（即爬虫伪造 WAF 认证请求）为 0 次。

图 16-11 JS 脚本反爬虫防护数据



须知

“js 挑战”和“js 验证”的防护动作为仅记录，WAF 不支持配置“js 挑战”和“js 验证”的防护动作。


16.5.9 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。

16.5.10 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 单击管理控制台右上角的，选择区域或项目。

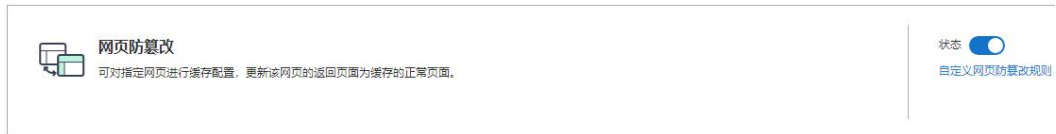
步骤 3 单击页面左上方的，选择“安全 > Web 应用防火墙 (独享版)”。




步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“网页防篡改”配置框中，检查是否已开启网页防篡改。

图 16-12 网页防篡改配置框



- 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，查看目标规则配置的域名和路径是否配置正确。

- 如果配置正确，请执行步骤 8。
- 如果配置不正确，在目标网页防篡改规则所在行的“操作”列中，单击“删除”，删除该防护规则后，在列表上方单击“添加规则”，重新配置网页防篡改规则。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

16.5.11 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

16.5.12 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。

16.6 IPv6 防护

16.6.1 哪些版本支持 IPv6 防护?

须知

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

16.6.2 如何测试在 WAF 中配置的源站 IP 是 IPv6 地址?

执行此操作前，请确认已在 WAF 中添加了域名并完成了域名接入。

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

步骤 1 在 Windows 中打开 `cmd` 命令行工具。

步骤 2 执行 `dig AAAA www.example.com` 命令。

如果返回的结果里有 IPv6 格式的 IP 地址，如图 16-13 所示，则证明配置的源站 IP 是 IPv6 地址。

图 16-13 测试结果

```
14/01/2020 09:37.18 /home/mobaxterm dig AAAA www.example.com
; <<>> DiG 9.9.7 <<>> AAAA www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5980
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 6, ADDITIONAL: 7
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 4096
;; QUESTION SECTION:
;www.163.com.                IN      AAAA
;; ANSWER SECTION:
www.163.com.                185     IN      CNAME   www.163jiasu.com.
www.163.com.                185     IN      CNAME   www.bsqs1b.cn.
www.bsqs1b.cn.             185     IN      CNAME   z163ipv6.v163.com.cn.
z163ipv6.v163.com.cn.     87      IN      AAAA    2408:873c:0000:0000:0000:0000:2001:1000:0:1:18
z163ipv6.v163.com.cn.     87      IN      AAAA    2408:873c:0000:0000:0000:0000:2001:1000:0:1:16
z163ipv6.v163.com.cn.     87      IN      AAAA    2408:873c:0000:0000:0000:0000:2001:1000:0:1:14
z163ipv6.v163.com.cn.     87      IN      AAAA    2408:873c:0000:0000:0000:0000:2001:1000:0:1:17
z163ipv6.v163.com.cn.     87      IN      AAAA    2408:873c:0000:0000:0000:0000:2001:1000:0:1:15
```

---结束

16.6.3 业务使用了 IPv6，WAF 中的源站地址如何配置？

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

WAF 支持 IPv6/IPv4 双栈模式和 NAT64 机制，详细说明如下：

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

16.6.4 WAF 如何解析/访问 IPv6 源站？

当防护网站的源站地址配置为 IPv6 地址时，WAF 直接通过 IPv6 地址访问源站。WAF 默认在 CNAME 中增加 IPv6 地址解析，IPv6 的所有访问请求将先流转到 WAF，WAF 检测并过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

WAF 支持 IPv6/IPv4 双栈模式和 NAT64 机制，详细说明如下：

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

16.7 证书管理

本章节为您罗列了证书使用过程中遇到的一些常见问题。

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。

ELB 已上传证书，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。

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 16-8 在本地将证书转换为 PEM 格式，再上传。

表 16-8 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">证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	<ul style="list-style-type: none">提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

说明

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

16.8 防护日志

16.8.1 Web 应用防火墙支持记录防护日志吗？

在 WAF 管理控制台，您可以免费查看最近 30 天的防护日志。

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

有关 WAF 日志配置到 LTS 的详细操作，请参见 6.4 通过 LTS 记录 WAF 全量日志。

16.8.2 如何获取拦截的数据？

16.8.3 防护事件列表中，防护动作为“不匹配”是什么意思呢？

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

16.8.4 Web 应用防火墙的防护日志可以存储多久？

在 WAF 管理控制台，您可以免费查看最近 30 天的防护日志。

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

16.8.5 Web 应用防火墙可以同时查询多个指定 IP 的防护事件吗？

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

图 16-14 防护事件



16.8.6 Web 应用防火墙会记录未拦截的事件吗？

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

16.8.7 为什么 WAF 显示的流量大小与源站上显示的不一致？

WAF “安全总览” 页面显示的流量大小与源站上显示的不同，主要原因说明如下：

- 网页压缩
WAF 默认开启压缩，客户端（如浏览器）与 WAF 之间进行通信的网页可能被压缩（依赖浏览器压缩选项），而源站服务器可能不支持压缩。
- 连接复用
WAF 与源站服务器之间会复用 socket 连接，这样会降低源站服务器与 WAF 之间的带宽消耗。
- 攻击请求
攻击请求被 WAF 拦截，而这种请求不会消耗源站服务器的带宽。
- 其他异常请求
如果源站服务器存在超时，无法连接等情况，这种情况不会消耗源站服务器的带宽。
- TCP 层的重传等
WAF 统计的带宽是 7 层的数据，而源站服务器网卡统计的是 4 层的数据。当网络通信质量差时，会出现 TCP 重传，网卡统计的带宽会重复计算，而 7 层传输的数据不会重复计算。在这种情况下，WAF 上显示的带宽会低于源站上显示的带宽。

16.9 内容安全检测服务

16.9.1 购买内容安全检测服务时，如何确定网站检测配额？

WAF 内容安全检测服务按新媒体账号或网站地址个数确定检测配额，1 个新媒体账号或 1 个网站地址占 1 个检测配额。

基于网站内容来判定配置几个检测网站，同一个组织和同一类内容被认定成一个网站，具体可参见以下几个场景。

说明

- WAF 支持批量购买内容安全检测服务，可一次输入一个或多个检测对象（新媒体或网站）进行安全检测，最多支持一次输入 100 个检测对象。
- “检测对象类型”为“网站”时，检测对象的每一行表示一个检测网址，多个网址以回车换行分割；同一行内的网址和备注之间以英文逗号分割，如无备注，可只输入网址，每行最多支持 500 个英文字符（1 个中文字符等于 2 个英文字符）。
- “检测对象类型”为“新媒体”时，检测对象的每一行表示一个新媒体账号，多个新媒体账号以回车换行分割；同一行内的新媒体账号和备注之间以英文逗号分割，每行最多支持 500 个英文字符（1 个中文字符等于 2 个英文字符）。

场景一：同一官网域名对应的内容，占一个网站检测配额

举例：XX 官网里有“产品中心”、“品牌活动”、“网络商城”等板块，但这些板块都同属于官网域名，算一个网站，占一个检测网站配额，即在购买内容安全检测服务时，“检测对象类型”选择“网站”，“检测对象”配置为 XX 官网的网址即可。

场景二：不同域名对应的网站，检测配额独立计算

举例：某官网（<http://www.example.com>）是一个网站，该网站下有链接到运营商 BG（<https://carrier.example.com/>）、企业 BG（<https://e.example.com/>）、消费者 BG（<https://consumer.example.com/>）三个网站，三个网站对应三个不同的域名，则占 4 个检测网站配额，即在购买内容安全检测服务时，“检测对象类型”选择“网站”，“检测对象”配置如图 16-15 所示。

图 16-15 检测对象配置

* 检测对象类型: 网站

* 检测对象 ?

http://www.example.com,某官网
https://carrier.example.com,运营商BG
https://e.example.com,企业BG
https://consumer.example.com,消费者BG

检测网站的数量: 4/100

场景三：域名相同但网站名称不同，检测配额独立计算

举例：某省省法院官网（<https://www.example.com/index.html>），市法院官网（<https://www.example.com/test.html>），虽然属于同一个域名，但官网名称不同，则判定为 2 个网站，占 2 个检测网站配额，即在购买内容安全检测服务时，“检测对象类型”选择“网站”，“检测对象”配置如图 16-16 所示。

图 16-16 网站配置



16.9.2 内容安全检测服务对网站的检测范围是什么？

内容安全检测服务可对网站/新媒体平台发布的内容进行合法合规检测，主要对文本、图片、视频、语音进行检测和识别是否包含色情、涉政、暴力、惊悚、不宜广告、垃圾信息、不良内容等，有效帮助您降低内容风险。

- 内容合法合规性检测

国家政策要求各地方机构要认真落实意识形态工作和网络内容安全工作责任制。为响应国家政策，内容安全检测服务可对网站/新媒体内容进行合法合规检测，主要对文本、图片、视频、语音进行检测和识别是否包含色情、涉政、暴力、惊悚、不宜广告、垃圾信息、不良内容等，有效帮助您降低内容风险。

- 内容准确性检测

对网站/主流新媒体平台的内容进行准确性检测，主要对文本、图片、视频、语音进行表述规范审核，如对错别字、生僻字、词法表述、语法表述等内容进行检测审核。

网站目录的检测范围

检测同一个网站域名下的所有目录（检测的域名和网站名称完全一致）。例如，
`http://www.example.com/a/`、`http://www.example.com/a/b/`、
`http://www.example.com/a/b/c/`都属于同一个域名的检测范围。

- 不检测链接到其它域名的 URL（检测的域名不一致）。例如，检测域名是“`http://www.example.com`”，不检测链接到“`http://e.example.com`”的页面和资源。
- 不检测链接到其它网站的 URL（域名相同，但网站名称不一致的）。例如，检测域名是“`https://www.example.com/index.html`”（网站名称是某省省法院官网），不检

测链接到“<https://www.example.com/test.html>”（网站名称是市法院官网）的页面和资源，此类网站多见于政务、学校网站。

16.9.3 购买内容安全检测服务后，多长时间能出报告？

“检测类型”选择“内容安全单次检测（按需）”时，下单后7个工作日内出报告；“检测类型”选择“文本安全监测（按月/按年）”时，下单后的检测周期（1个自然月）后的7个工作日内出报告。可在WAF控制台内容安全检测页面下载检测报告，详细操作参见[下载检测报告](#)。

16.9.4 购买内容安全检测服务后，什么时候扣费？

购买内容安全检测服务后，系统立即执行检测并扣费，且检测过程中，不支持修改检测域名、暂停任务、退费等操作。

内容安全检测服务支持三种检测类型：内容安全单次检测（按需）、文本安全监测（按月）、文本安全监测（按年）。选择“内容安全单次检测（按需）”时，内容安全检测服务按“检测对象”的总个数进行收费。同一个对象再次进行扫描时，需要重新收费。网站检测配额请参见 [16.9.16.9.1 购买内容安全检测服务时，如何确定网站检测配额？](#)。

例如：单次配置了10个检测对象（新媒体账号或网站网址），每个检测对象检测一次，则需要进行10次收费。

详细的计费说明请参见[计费项](#)。

16.10 网站接入异常排查

16.10.1 域名/IP 接入状态显示“未接入”，如何处理？

故障现象

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

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 16-17 和图 16-17 表 16-9 进行排查处理。

图 16-17 独享模式排查思路

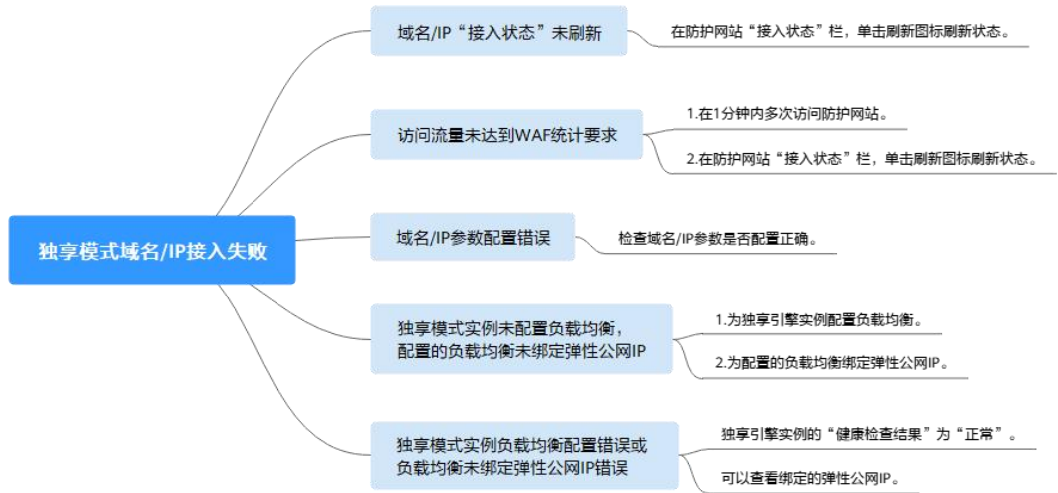




表 16-9 独享模式接入 WAF 失败问题处理

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 2.5.1.3 步骤二：配置负载均衡。 2. 5.1.4 步骤三：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"> 2.5.1.3 步骤二：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。 5.1.4 步骤三：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。

16.10.2 如何解决网站接入 WAF 后程序访问页面卡顿？

问题现象

网站接入 WAF 后程序访问页面卡顿。

可能的原因

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。

解决办法

请添加 HTTP 到 HTTP 和 HTTPS 到 HTTPS 这 2 条转发协议规则。具体操作如下：


- 步骤 1 登录 WAF 控制台。
- 步骤 2 在左侧导航栏中，选择“网站设置”，进入网站设置页面。
- 步骤 3 在“服务器信息”栏中，单击 。
- 步骤 4 在“修改服务器信息”页面，添加 HTTP 到 HTTP 和 HTTPS 到 HTTPS 这 2 条转发协议规则。

图 16-18 配置示例



---结束

有关配置转发规则的详细操作，请参见 16.12.4 如何解决重定向次数过多？。

16.10.3 如何处理网站接入 WAF 后，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。

16.11 证书/加密套件问题排查

16.11.1 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。
- 重新上传正确的证书。

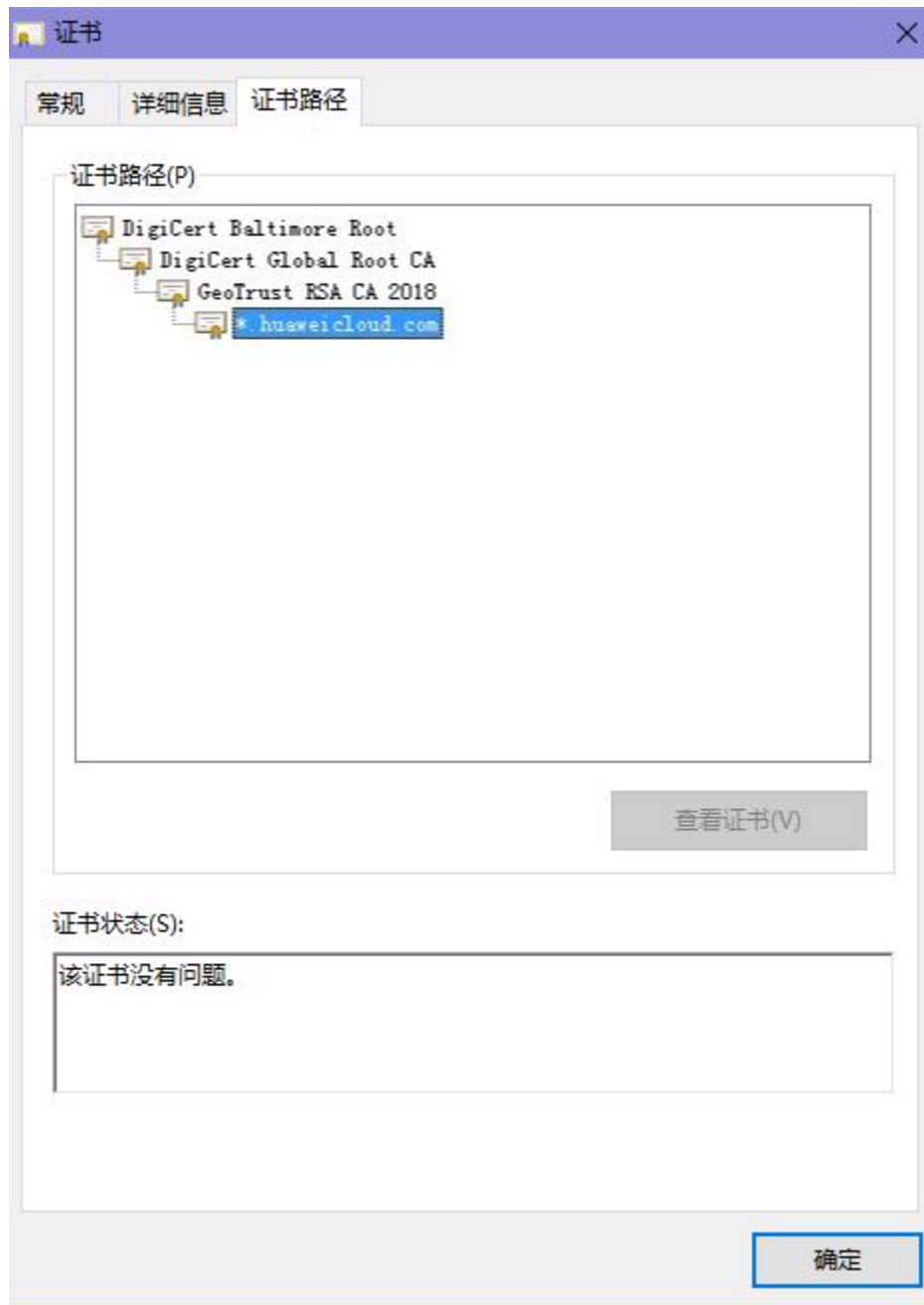
Chrome 最新版本一般是支持自动验证信任链，手工构造完整的证书链步骤如下：

步骤 1 查看证书并导出证书。

1. 单击浏览器前的锁，可查看证书状况。
2. 在“连接是安全的”所在行，单击 , 并单击“证书有效”。
3. 选择“详细信息”页签，在页面右下角单击“导出”，将证书导出到本地。

步骤 2 查看证书链。在本地打开导出的证书，并选中“证书路径”页签，可单击证书名称查看证书状态，如图 16-19 所示。

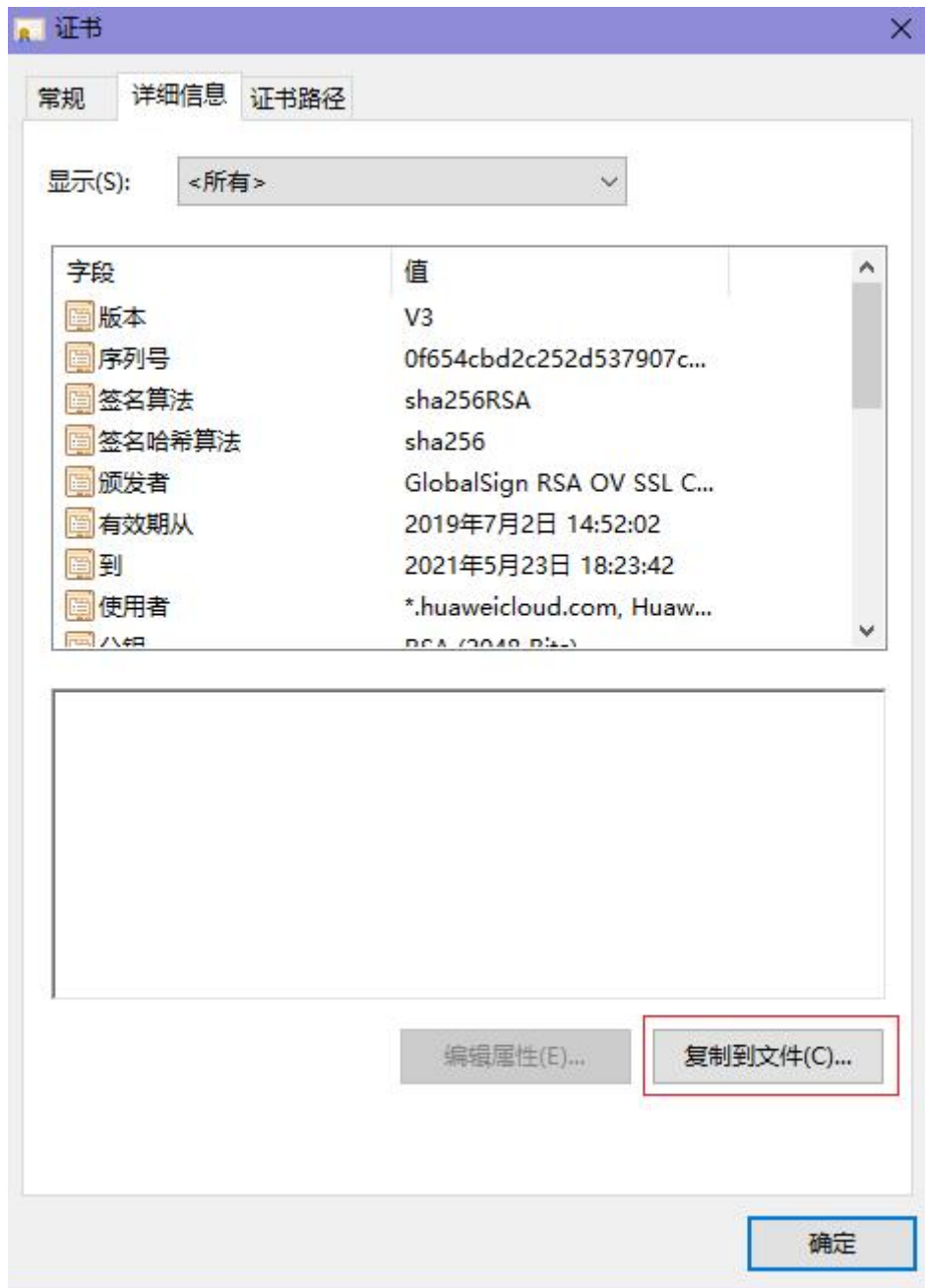
图 16-19 查看证书链



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 16-20 所示。

图 16-20 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 16-21 所示。

图 16-21 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 16-22 重组证书顺序，完成证书重构。

图 16-22 证书重构



步骤 5 重新上传证书。

----结束

16.11.2 如何解决证书与密钥不匹配问题？

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

解决方案

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

相关操作

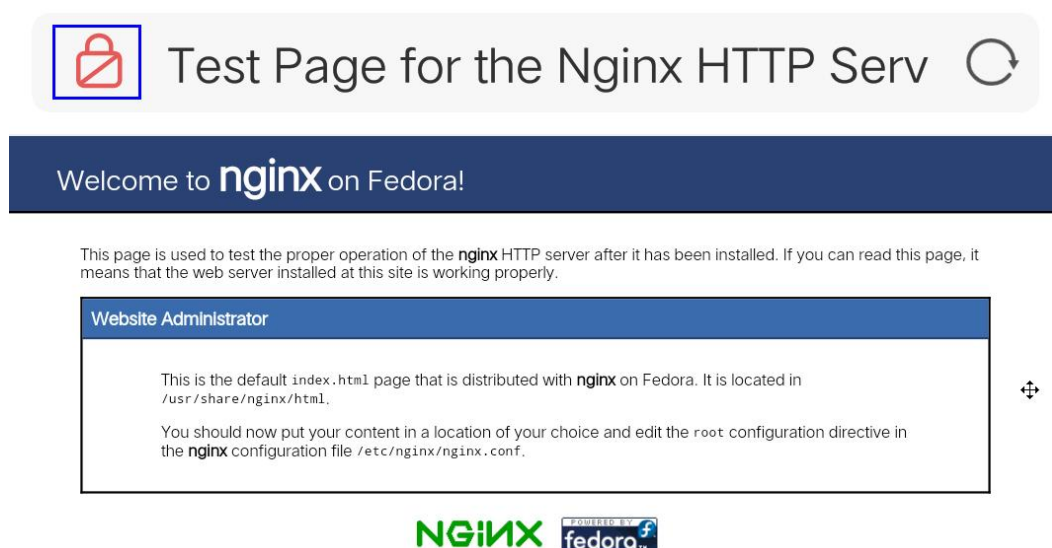
- 16.1116.11.1 如何解决证书链不完整？
- 16.11.3 如何解决 HTTPS 请求在部分手机访问异常？

16.11.3 如何解决 HTTPS 请求在部分手机访问异常？

问题现象

打开手机浏览器，访问防护域名，如果出现类似如图 16-23 所示的页面，则表示该手机上 HTTPS 请求访问异常。

图 16-23 访问异常



原因

该问题是由于上传的证书链不完整，

解决办法

可参照 16.1116.11.1 如何解决证书链不完整？解决。

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

现象

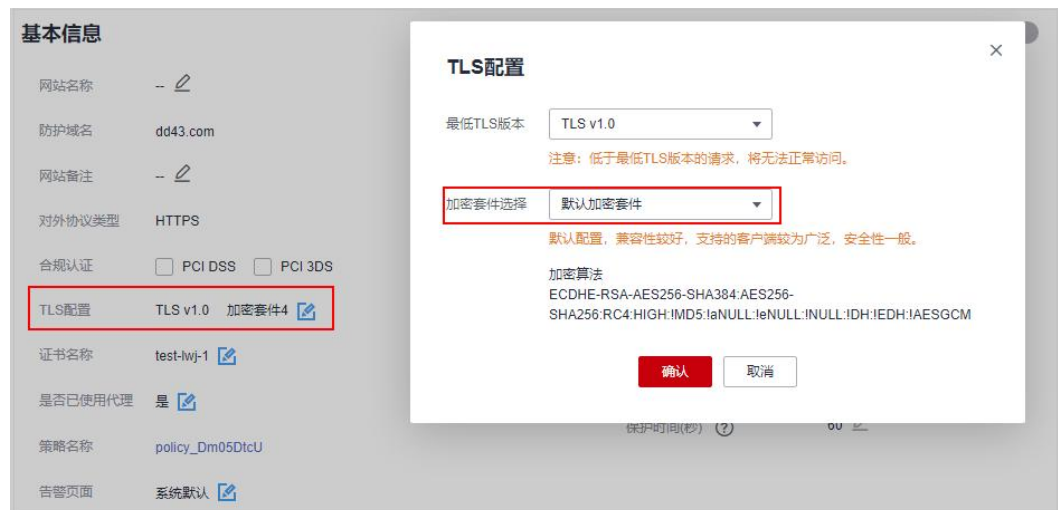
域名接入 WAF 后，不能正常访问网站，提示“协议不受支持，客户端和服务端不支持一般 SSL 协议版本或加密套件”。



解决办法

建议您在 TLS 配置里，将“加密套件”切换为“默认加密套件”，具体操作请参见 99.19.1.1 配置 PCI DSS/3DS 合规与 TLS。

图 16-24 TLS 配置



16.11.5 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”。

16.12 流量转发异常排查

16.12.1 如何排查 404/502/504 错误？

网站接入 WAF 防护之后，如果您访问网站时出现 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 16-25 所示的页面。

图 16-25 404 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 16.1216.12.1 图 16-25 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. 单击页面左上方的 ，选择“安全 > Web 应用防火墙”。
- 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“域名”列中，单击目标域名，进入域名基本信息页面。
- d. 在“服务器”栏中，单击 ，进入“修改服务器信息”页面，确保对外协议、源站协议、源站地址、端口等信息配置正确。

图 16-26 服务器配置

修改服务器信息

对外协议	源站协议	源站地址	源站端口	操作
HTTP	HTTP	xx.xx.xx.101	80	删除
HTTP	HTTP	xx.xx.xx.22	80	删除

+ 添加 您还可以添加18项服务器配置

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 -kvv
```

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。

图 16-27 检测源站

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

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. 单击页面左上方的 ，选择“安全 > Web 应用防火墙”。
 - 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“域名”列中，单击目标域名，进入域名基本信息页面。
 - iv. 在“服务器”栏中，单击 ，进入“修改服务器信息”页面，单击“添加”，新增后端服务器。

图 16-28 服务器配置



- 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。
- **原因六：独享模式下，源站安全组或源站网络 ACL 未放开。**
解决办法：放开安全组端口（例如 80 、443），网络 ACL 放通源站子网。

16.12.2 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。

16.12.3 如何处理 523 错误码问题？

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



原因一：将同一个网站接入 WAF 4 次以上

通过 WAF 的各种模式，将同一个网站接入 WAF 4 次以上。

解决办法：

梳理流量图，将用户流量绕过多余 WAF，具体操作如下：

- 步骤 1** 登录 WAF 管理控制台。
- 步骤 2** 在左侧导航树中，选择“网站设置”，进入网站设置列表。
- 步骤 3** 找到出现 523 问题的防护网站，保留一个配置，删除多余的防护网站，具体操作请参见 9.2.5 删除防护网站。

防止删除网站后造成业务中断，在删除网站前，需要完成以下操作：

独享模式：修改 ELB 的后端服务器组，不再接入 WAF 实例节点。

---结束

原因二：调用了第三方接口且第三方接口也使用了 WAF

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

解决办法：

修改反向代理请求中的 header 字段，具体操作如下：

须知

用户的流量链路上，在 WAF 后如果有 NGINX，才可用此方法。

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

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

```
vi /opt/nginx/conf/nginx.conf
```

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

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

---结束

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

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

解决办法：

检测源站服务器的配置，将“源站地址”修改为正确的源站 IP。

图 16-29 修改源站地址



16.12.4 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。配置完成后，服务器信息如图 16-30 所示。

图 16-30 配置示例



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

故障现象

防护网站接入 WAF 后，用户不能正常访问网站，提示“414 Request-URI Too Large”错误，如图 16-31 所示。

图 16-31 提示“414 Request-URI Too Large”错误



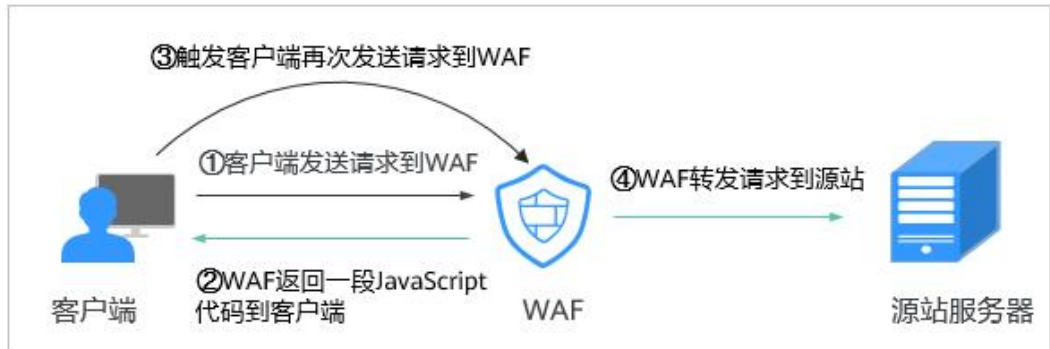
可能原因

防护网站开启了“JS 脚本反爬虫”，由于用户的客户端浏览器没有 JavaScript 解析能力，客户端会缓存包含 WAF 返回 JavaScript 代码的页面，而用户每次访问防护网站时都会

访问该缓存页面，WAF 由此判定用户访问请求为非法的浏览器或爬虫工具，访问请求验证一直失败，造成无限循环，最终导致 URI 长度超出浏览器限制，访问网站失败。

开启 JS 脚本反爬虫后，当客户端发送请求时，WAF 会返回一段 JavaScript 代码到客户端。如果客户端是正常浏览器访问，就可以触发这段 JavaScript 代码再发送一次请求到 WAF，即 WAF 完成 JS 验证，并将该请求转发给源站，如图 16-32 所示。


图 16-32 JS 脚本反爬虫正常检测流程




处理建议

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

步骤 1 登录管理控制台。

步骤 2 单击管理控制台左上角的 ，选择区域或项目。

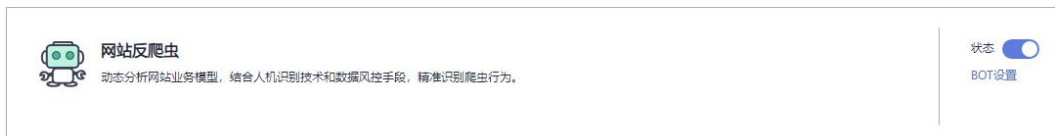
步骤 3 单击页面左上方的 ，选择“安全 > Web 应用防火墙 (独享版)”。

步骤 4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤 5 单击目标策略名称，进入目标策略的防护配置页面。

步骤 6 在“网站反爬虫”配置框中，单击“BOT 设置”，进入网站反爬虫规则配置页面。

图 16-33 网站反爬虫配置框






步骤 7 选择“JS 脚本反爬虫”页签，关闭 JS 脚本反爬虫，即 JS 脚本反爬虫的“状态”为 ，如图 16-34 所示。

图 16-34 关闭 JS 脚本反爬虫



---结束

16.12.6 连接超时时长是多少，是否可以手动设置该时长？

- 浏览器到 WAF 引擎的连接超时时长默认是 120 秒，该值取决于浏览器的配置，该值在 WAF 界面不可以手动设置。
- WAF 到客户源站的连接超时时长默认为 30 秒，该值可以在 WAF 界面手动设置。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。

16.13 误拦截正常请求排查

16.13.1 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。

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 16-10 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 16-10 误报处理说明

命中规则类型	命中规则	处理方式
--------	------	------

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 6.2 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”访问请求说明</p> <p>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。 • URL 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 7.4 配置精准访问防护规则定制化防护策略放行该访问请求。

16.13.2 WAF 误拦截了“非法请求”访问请求，如何处理？

问题现象

防护网站接入 WAF 后，访问请求被 WAF 拦截，在“防护事件”页面查看防护日志，显示访问请求为“非法请求”且误报处理按钮置灰不能使用，如图 16-35 所示。

图 16-35 非法请求被 WAF 拦截

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

可能原因

当遇到以下情况时，WAF 将判定该访问请求为非法请求并拦截该访问请求：

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

处理建议

当确认访问请求为正常请求时，请通过 7.4 配置精准访问防护规则定制化防护策略放行该访问请求。

A 修订记录

发布日期	修改说明
2024-09-05	第八次正式发布。 增加： <ul style="list-style-type: none">9.1.2 开启 IPv6 防护16.6IPv6 防护
2024-07-16	第七次正式发布。 <ul style="list-style-type: none">增加：<ul style="list-style-type: none">9.1.7 开启 Cookie 安全属性回退独享引擎实例版本修改：<ul style="list-style-type: none">8 查看总览66.1 查询防护事件6.2 处理误报事件7.3 配置 CC 攻击防护规则防御 CC 攻击7.4 配置精准访问防护规则定制化防护策略7.5 配置 IP 黑白名单规则拦截/放行指定 IP7.8 配置网站反爬虫防护规则防御爬虫攻击
2024-03-28	第六次正式发布。 增加：15 监控与审计章节。
2024-02-04	第五次正式发布。 <ul style="list-style-type: none">增加：<ul style="list-style-type: none">6.4 通过 LTS 记录 WAF 全量日志16.816.8.1Web 应用防火墙支持记录防护日志吗？16.816.8.2 如何获取拦截的数据？修改：<ul style="list-style-type: none">16.816.8.4Web 应用防火墙的防护日志可以存储多久？

发布日期	修改说明
2023-11-30	<p>第四次正式发布。</p> <ul style="list-style-type: none">• 架构调整。• 增加：<ul style="list-style-type: none">- 11.2 内容安全检测- 2.5.1.6 步骤五：独享引擎本地验证- 9.1.3 配置 WAF 到网站服务器的连接超时时间- 9.1.4 开启连接保护功能保护源站安全- 9.1.5 配置攻击惩罚的流量标识- 1111.1 配置内容安全检测- 13.2 查看产品信息- 13.3 开启告警通知- 1616.116.1.1WAF 基础知识- 16.1.10Web 应用防火墙和云防火墙有什么区别？- 16.1.6WAF 和 HSS 的网页防篡改有什么区别？- 16.9 内容安全检测服务- 16.12.5 如何处理接入 WAF 后报错 414 Request-URI Too Large？- 16.11.5 如何解决“网站被检测到：SSL/TLS 存在 Bar Mitzvah Attack 漏洞”？- 精准访问防护规则添加的路径中带有#能匹配吗？- 如何不拦截带有.js 的文件？- 12.2 管理黑白名单 IP 地址组• 修改：<ul style="list-style-type: none">- 11.2 内容安全检测- 1.7 应用场景- 2 计费说明- 1.5 功能特性- 3WAF 操作指引- 66.1 查询防护事件- 6.2 处理误报事件- 10 策略管理- 99.19.1.1 配置 PCI DSS/3DS 合规与 TLS- 9.2 网站管理- 1212.1 管理证书- 1313.1 管理独享引擎- -16.316.3.1Web 应用防火墙可以免费使用吗？- 16.3.2Web 应用防火墙如何收费？

发布日期	修改说明
2023-05-25	第三次正式发布。 修改： <ul style="list-style-type: none">• 2.5.1.3 步骤二：配置负载均衡• 5.1.4 步骤三：为弹性负载均衡绑定弹性公网 IP• 5.1.5 步骤四：放行独享引擎回源 IP• 8 查看总览• 6 查看防护事件
2022-02-25	第二次正式发布。 新增 16.1.8 WAF 可以防护使用 HSTS 策略/NTLM 代理认证访问的网站吗？
2021-01-29	第一次正式发布。