Web 应用防火墙

用户指南

文档版本 06

发布日期 2023-10-30

华为云计算技术有限公司

商标声明


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

注意

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

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

目 录

1 产品简介

1.1 Web 应用防火墙

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

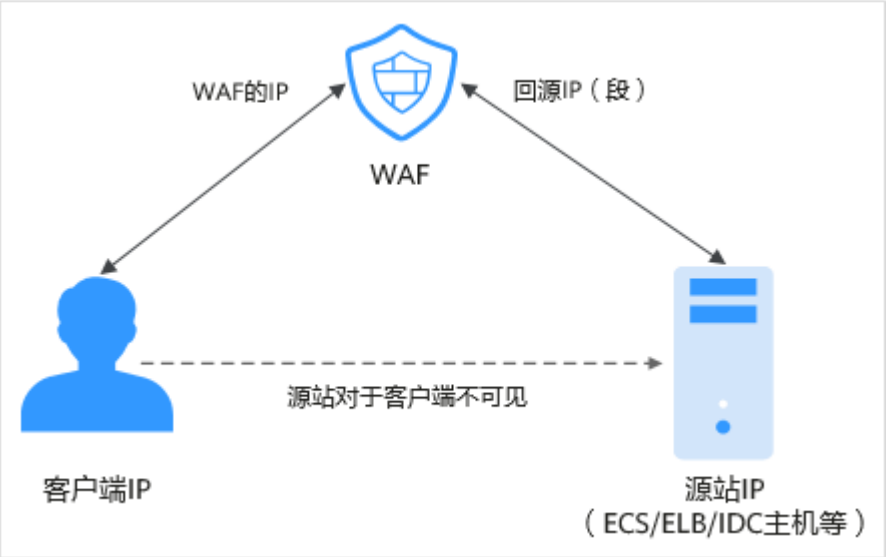
防护原理

开通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 CNAME 接入、独享模式接入防护原理

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支持云模式、独享模式两种部署模式，各部署模式支持防护的对象说明如下：

- 云模式：域名，云上或云下的Web业务。
- 独享模式：域名或IP，云上的Web业务。

1.2 功能特性

通过Web应用防火墙，轻松应对各种Web安全风险。

域名（泛域名、一级域名、二级域名等各级域名）/IP 防护

WAF支持云模式和独享模式两种部署模式，各部署模式支持防护的对象说明如下：

- 云模式：域名，云上或云下的Web业务
- 独享模式：域名或IP，云上的Web业务

HTTP/HTTPS 业务防护

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

支持 WebSocket/WebSockets 协议

WAF支持WebSocket/WebSockets协议，且默认为开启状态。

PCI DSS/PCI 3DS 合规认证和 TLS

- TLS支持TLS v1.0、TLS v1.1和TLS v1.2三个版本和七种加密套件，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。

Web 基础防护

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

- 全面的攻击防护

  支持SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、目录（路径）遍历、敏感文件访问、命令/代码注入、网页木马上传、后门隔离保护、非法HTTP协议请求、第三方漏洞攻击等威胁检测和拦截。

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

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

CC 攻击防护

CC攻击防护规则支持通过限制单个IP/Cookie/Referer访问者对防护网站上特定路径（URL）的访问频率，精准识别CC攻击以及有效缓解CC攻击，阻挡暴力破解、探测和统计弱密码撞库等高频攻击。支持人机验证、阻断、动态阻断和仅记录防护动作。

- 策略配置灵活

  可以根据IP、Cookie或者Referer字段名设置灵活的限速策略。

- 阻断页面可定制

  阻断页面可自定义内容和类型，满足业务多样化需要。

安全可视化

提供简洁友好的控制界面，实时查看攻击信息和事件日志。

- 策略事件集中配置

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

- 流量及事件统计信息

  实时查看访问次数、安全事件的数量与类型、详细的日志信息。

非标准端口防护

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

表 1-1 WAF 支持的端口

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

部署模式	端口分类	HTTP协议	HTTPS协议	端口防护限制数
	非标准端口（**86个**）	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805	**20个**
独享模式	标准端口	80	443	不限制

部署模式	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

精准访问防护

基于丰富的字段和逻辑条件组合，打造强大的精准访问控制策略。

- 支持丰富的字段条件

  支持IP、URL、Referer、User Agent、Params、Header等HTTP常见参数和字段的条件组合。

- 支持多种条件逻辑

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

扫描器爬虫防护

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

IP 黑白名单设置

添加始终拦截与始终放行的黑白名单IP/IP地址段，增加防御准确性。

攻击惩罚

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

连接保护

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

手动设置网站连接超时时间

- 浏览器到WAF引擎的连接超时时长是120秒，该值不可以手动设置。
- WAF到客户源站的连接超时时长默认为60秒，该值可以手动设置，但仅“独享模式”和“云模式”的专业版（原企业版）、铂金版（原旗舰版）支持手动设置连接超时时长。

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

地理位置访问控制

可以针对国家、地区地理位置来源IP进行自定义访问控制。

网页防篡改

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

网站反爬虫

动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。

- 特征反爬虫

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

  通过自定义规则识别并阻断JS脚本爬虫行为。

全局白名单（原误报屏蔽）规则

针对特定请求忽略某些攻击检测规则，用于处理误报事件。

隐私屏蔽

避免在防护事件日志中，出现用户名或者密码等敏感信息。

防敏感信息泄露

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

稳定可靠

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

告警通知

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

管理防护事件

- 当Web应用防火墙拦截或者仅记录的攻击事件为误报时，用户可通过Web应用防火墙处理误报事件、查看事件详情。
- 用户可以通过Web应用防火墙服务下载5天内的全量防护事件数据。

1.3 服务版本差异

Web应用防火墙支持云模式和独享模式两种部署方式，部署模式的差异说明如**云模式、独享模式使用说明**。

云模式、独享模式使用说明

请您根据业务需求选择使用云模式或独享模式，您也可以同时使用两种模式， 两种模式的部署架构如图1-3所示，主要差异说明如表1-2所示。

图 1-3 云模式和独享模式部署架构

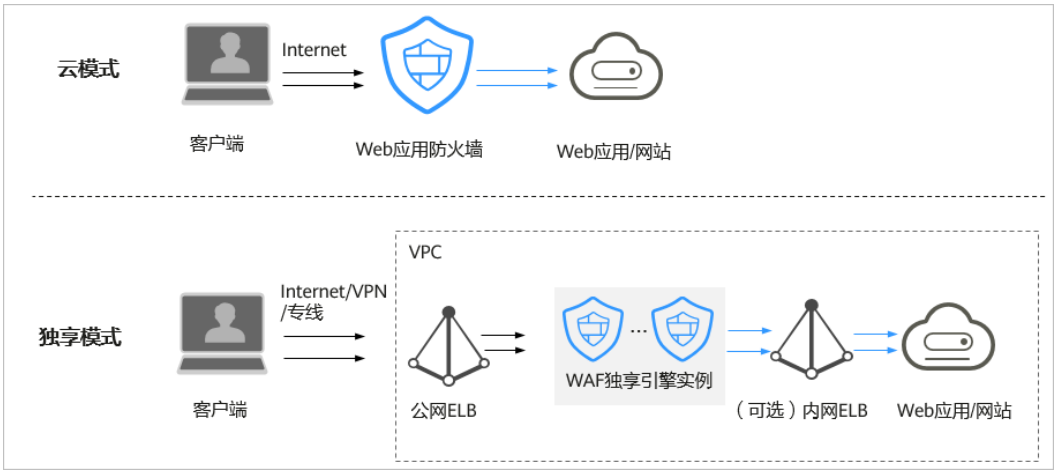


表 1-2 各模式使用说明

项目	云模式	独享模式
计费方式	按需计费	按需计费
使用场景	业务服务器部署在云上或线下。	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制定个性化防护规则的安全需求。
防护对象	域名	• 域名 • IP
优势	• 弹性扩容能力强，通过升级规格可以扩容防护能力 • 可以防护云上和云下的Web业务	• 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

各版本支持的业务规格

云模式、独享模式适用的业务规格如表1-3所示。

表 1-3 适用的业务规格

业务规格	云模式	独享模式
正常业务请求峰值	-	以下数据为单实例规格： ● 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 **须知** 极限值为实验室测试值，高敏感业务请以实际业务测试数据为准。实际QPS与业务请求数据大小、自定义防护规则种类及数量相关
业务带宽阈值（源站服务器部署在云上）	-	● 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	30个（支持3个一级域名）	2,000个（支持2,000个一级域名）
回源IP（单个防护域名支持的回源服务器IP个数）	20个	-
支持的端口个数	-	● 标准端口：80、443 ● 非标准端口：不限制数量
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
CC攻击防护规则	200条	100条
精准访问防护规则	1000条	100条

业务规格	云模式	独享模式
引用表规则	1000条	100条
IP黑白名单规则	2000条	100条
地理位置封禁规则	200条	100条
网页防篡改规则	200条	100条
防敏感信息泄露	200条	100条
全局白名单规则	2000条	1000条
隐私屏蔽规则	200条	100条

1.4 产品优势

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

精准高效的威胁检测

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

保护用户数据隐私

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

1.5 应用场景

常规防护

帮助用户防护常见的Web安全问题，比如命令注入、敏感文件访问等高危攻击。

电商抢购秒杀防护

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

0Day 漏洞爆发防范

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

防数据泄露

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

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

防网页篡改

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

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

1.6 计费说明

Web应用防火墙支持按需计费（后付费）和按月计费两种计费方式。

计费项

图 1-4 WAF 的计费方式

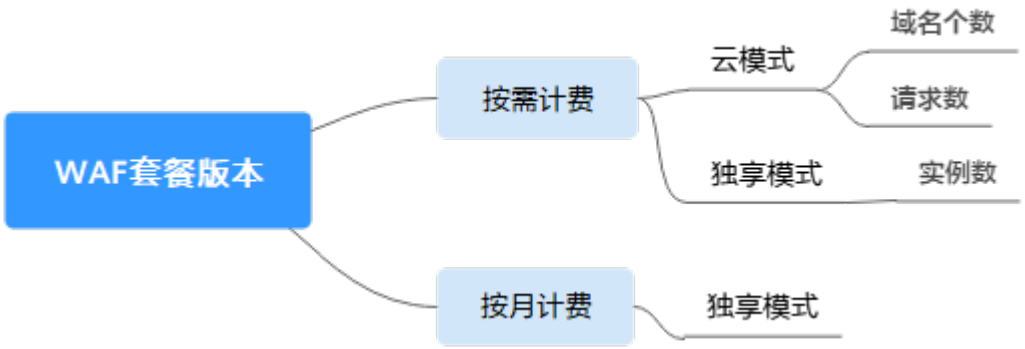


表 1-4 计费项信息

模式	计费模式	计费项目	计费说明
云模式	按需计费	• 域名个数 • 请求数	• 域名个数：按小时结算。在结算期间内，如果添加域名后立即删除，该域名也会计费。 • 请求数：按1个月累计结算。
独享模式	按需计费	实例数	按实际使用时长计费。
	按月计费	实例数	按申请的实例数量和实例规格计费。

计费模式

- 按月计费：使用越久越便宜。按申请的实例数量和实例规格计费。
- 按需计费：购买方式比较灵活，可以即开即停。
  - 云模式：从开通并使用WAF开始计费到关闭按需计费时结束计费，按实际添加的域名个数、和使用的请求数计费。
  - 独享模式：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。

FAQ

更多计费相关FAQ，请参见**WAF常见问题**。

1.7 项目和企业项目

项目

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

企业项目

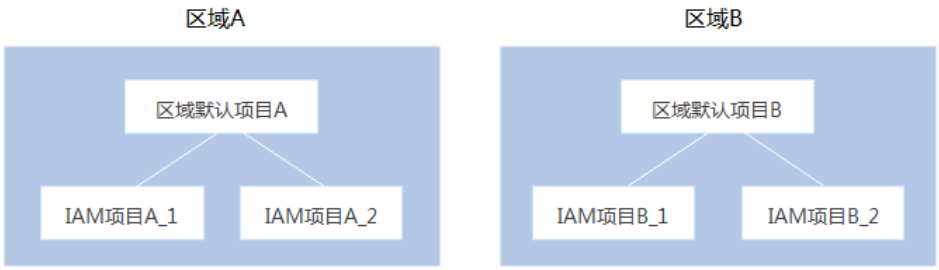
企业管理中的企业项目是对多个资源进行分组和管理，在目标区域中同一类型的资源可以划分到一个企业项目中，且主机安全服务的使用不受企业项目的划分影响。

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

项目与企业项目的区别

- IAM项目

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



- 企业项目

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

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

1.8 访问和使用

1.8.1 如何访问

请使用管理控制台访问Web应用防火墙。如果用户已注册公有云，可直接登录管理控制台。

- 云模式：从主页选择“安全 > Web应用防火墙”。
- 独享模式：从主页选择“安全 > Web应用防火墙 (独享)”。

1.8.2 如何使用

由于黑客技术泛滥，导致互联网安全事件频发，Web服务面临黑客入侵威胁，Web应用防火墙为Web服务提供基础安全防护措施。

用户使用Web应用防火墙服务后，可以配置并开启防护策略检测SQL注入、XSS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、CSRF等攻击，保护Web服务安全稳定。

用户可以查看Web服务防护事件日志及统计报告，及时了解Web服务的安全情况，并可对误报事件进行屏蔽处理或者添加白名单对误报进行忽略。

1.9 与其他云服务的关系

本章节介绍Web应用防火墙与其他云服务的关系。

与云审计服务的关系

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

表 1-5 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
修改告警通知设置	alertNoticeConfig	modifyAlertNoticeConfig
添加证书	certificate	createCertificate
修改证书名称	certificate	modifyCertificate
删除证书	certificate	deleteCertificate
创建CC规则	policy	createCc
修改CC规则	policy	modifyCc
删除CC规则	policy	deleteCc
创建精准防护规则	policy	createCustom
修改精准防护规则	policy	modifyCustom
删除精准防护规则	policy	deleteCustom
创建IP黑白名单规则	policy	createWhiteblackip
修改IP黑白名单规则	policy	modifyWhiteblackip
删除IP黑白名单规则	policy	deleteWhiteblackip
创建/刷新网页防篡改规则	policy	createAntitamper
删除网页防篡改规则	policy	deleteAntitamper

操作名称	资源类型	事件名称
创建全局白名单（原误报屏蔽）规则	policy	createIgnore
删除全局白名单（原误报屏蔽）规则	policy	deleteIgnore
创建隐私屏蔽规则	policy	createPrivacy
修改隐私屏蔽规则	policy	modifyPrivacy
删除隐私屏蔽规则	policy	deletePrivacy

与云监控服务的关系

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

有关WAF监控指标的详细介绍，请参见**监控指标**。

与标签管理服务的关系

标签管理服务是一种将标签集中管理的快速便捷的可视化服务，方便用户通过标签标识管理web应用防火墙实例。

表 1-6 标签管理服务支持的 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标签	Tag	createResourceTag
删除Web应用防火墙防护实例标签	Tag	deleteResourceTag

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，详细内容请参考《统一身份认证服务用户指南》。

与消息通知服务的关系

消息通知服务（Simple Message Notification，简称SMN）提供消息通知功能。Web应用防火墙开启通知设置后，如果防护的域名受到事件攻击时用户会收到短信或邮件的提醒信息。有关SMN的详细内容，请参见《消息通知服务用户指南》。

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。

与企业管理的关系

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

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

1.10 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1-7所示。

表 1-7 个人数据范围列表

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

类型	收集方式	是否可以修改	是否必须
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。

1.11 权限管理

1.11.1 用户权限（云模式）

系统默认提供两种权限：用户管理权限和资源管理权限。用户管理权限可以管理用户、用户组及用户组的权限。资源管理权限可以控制用户对云服务资源执行的操作。

1.11.2 WAF 权限管理（独享模式）

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

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

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

WAF 权限

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

WAF部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生

效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问WAF时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

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

如**表1-8**所示，包括了WAF的所有系统角色。

表 1-8 WAF 系统角色

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

相关链接

- **WAF自定义策略**
- **WAF权限及授权项**

2 监控指标

功能说明

本节定义了Web应用防火墙服务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应用防火墙服务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。

云模式监控指标

表 2-1 监控指标

指标ID	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
attacks	attacks	统计防护域名在周期内被攻击的总次数	>=0 count	测量对象：防护域名 测量维度：waf_instance_id	5分钟
requests	requests	统计防护域名在周期内被请求的总次数	>=0 count	测量对象：防护域名 测量维度：waf_instance_id	5分钟

独享引擎实例监控指标

表 2-2 WAF 独享引擎实例支持的监控指标

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
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

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_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字节数。 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
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

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_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
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

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）
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

表 2-3 维度

Key	Value
waf_instance_id	域名ID。
instance_id	WAF独享引擎实例ID

3 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3-1所示。

表 3-1 WAF 支持的端口

部署模式	端口分类	HTTP协议	HTTPS协议	端口防护限制数
云模式	标准端口	80	443	不限制
	非标准端口（**86个**）	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805	**20个**
独享模式	标准端口	80	443	不限制

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

4 云模式 WAF

4.1 入门

4.1.1 概述

使用Web应用防火墙（WAF）服务前，您需要根据入门中的操作步骤将您的网站域名接入WAF进行防护。

Web应用防火墙的使用概览如**表4-1**所示。

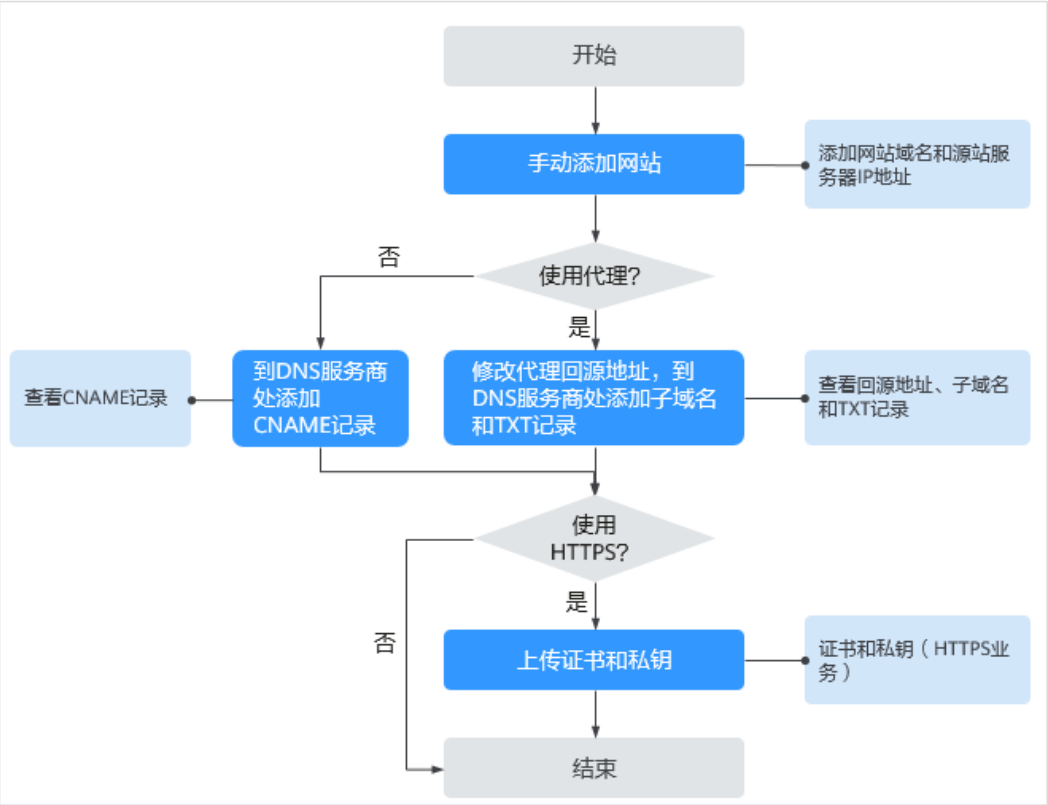
表 4-1 Web 应用防火墙的使用概览

子流程	说明
添加防护域名	开通WAF后，添加需要防护的域名或网站。详细操作请参见**添加防护域名**。
开启WAF防护	添加防护域名后，可开启WAF防护，保护网站业务安全稳定。详细操作请参见**开启防护**。 **说明** • 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。 • WAF根据QPS（HTTP GET请求量）或者业务带宽（所有该WAF防护的域名、站点中正常业务流量的大小）进行收费，且QPS的上限为10,000QPS（Query Per Second，即每秒钟的请求量，例如一个HTTP GET请求就是一个Query），带宽的上限为300Mbit/s。
配置自定义规则	WAF除了内置的防护规则外，还提供了丰富全面的自定义防护配置规则，全方位的防护您的网站。详细操作请参见**配置防护规则**。
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。详细操作请参见**开启告警通知**。

子流程	说明
处理误报事件	WAF拦截或者记录的攻击事件为误报时，可对误报进行屏蔽处理。详细操作请参见**处理误报事件**。
安全总览	可查看到昨天、今天、3天、7天或者30天范围内的访问与攻击统计次数、攻击分布、攻击源IP TOP5的次数。详细操作请参见**安全总览**。

网站接入WAF的操作流程图如**图4-1**所示。

图 4-1 网站接入 WAF 的操作流程图



4.1.2 添加防护域名

该任务指导用户在Web应用防火墙添加并接入域名。域名接入WAF后，WAF作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。

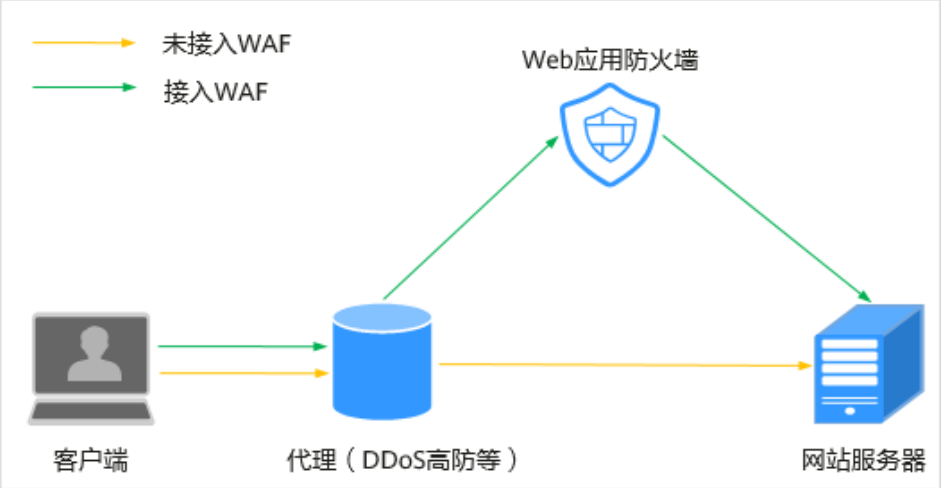
前提条件

已获取管理控制台的账号和密码。

配置防护域名原理图

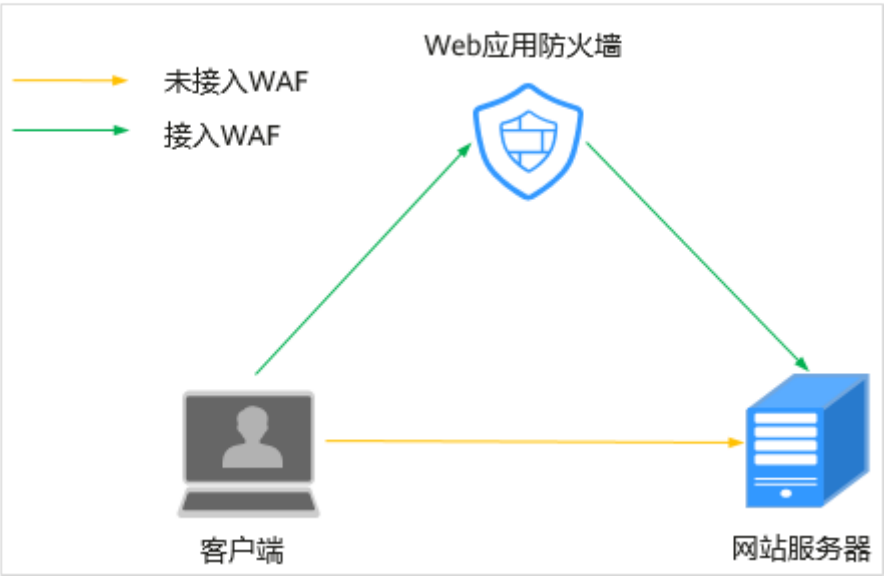
- 若在客户端和Web应用防火墙之间使用了代理，可参照图4-2配置。

图 4-2 使用代理配置原理图



  - 当网站没有接入到WAF前，DNS解析到DDoS高防等代理，流量先经过DDoS高防等代理，DDoS高防等代理再将流量直接转到源站。
  - 网站接入WAF后，需要将域名解析到WAF，这样流量才会被DDoS高防等代理转发到WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。
    i. 将DDoS高防等代理回源地址修改为WAF的“接入地址”。
    ii. 在DNS服务商处添加一条WAF的子域名和TXT记录。
- 若在客户端和Web应用防火墙之间未使用代理，可参照图4-3配置。

图 4-3 未使用代理配置原理图



  - 当网站没有接入到WAF前，DNS直接解析到源站的IP，用户直接访问服务器。

- 当网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“域名配置”，进入“域名配置”页面。

步骤5 在页面的右上角，单击“创建防护域名”。

步骤6 在“创建防护域名”页面配置域名基本信息。相关参数说明如**表4-2**所示。

表 4-2 基本信息参数说明

参数	参数说明	取值样例
防护域名	可防护的域名，支持单域名和泛域名。 ● 单域名：输入防护的单域名。例如：www.example.com。 ● 泛域名 – 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：*.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。	单域名：www.example.com 泛域名：*.example.com
非标准端口	可选参数，仅当用户勾选“非标准端口”时需要配置。 ● “对外协议”选择“HTTP”时，WAF默认防护“80”标准端口的业务，如需配置除“80”以外的端口，勾选“非标准端口”，在“端口”下拉列表中选择非标准端口。 ● “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“443”以外的端口，勾选“非标准端口”，在“端口”下拉列表中选择非标准端口。 Web应用防火墙可支持的非标准端口请参见**Web应用防火墙**章节。	4443

参数	参数说明	取值样例
服务器配置	网站服务器地址的配置。包括对外协议、源站协议、源站地址和源站端口。 • “对外协议”：客户端协议类型。包括“HTTP”、“HTTPS”两种协议类型。 • “源站协议”：服务器协议类型，WAF转发客户端请求的协议。包括“HTTP”、“HTTPS”两种协议类型。 **说明** 对外协议与源站协议的具体配置规则，请参见**对外协议与源站协议配置规则**。 • “源站地址”：客户端访问的网站服务器的IP地址（一般对应该域名接入WAF之前的A记录）或者域名（一般对应该域名接入前的CNAME）。 **说明** WAF不支持健康检查，如需使用，请配合ELB使用。ELB配置完成后，再将ELB的EIP作为源站地址的IP地址，接入WAF，实现健康检查。 • “源站端口”：客户端访问的网站服务器的端口号。	对外协议：HTTPS 源站协议：HTTP 源站地址：XXX.XXX.1.1 源站端口：80
证书名称	“对外协议”设置为“HTTPS”时，需要选择已有证书或导入新证书，导入新证书的操作请参见**步骤7**。	-

步骤7 （可选）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“上传证书”，在弹出的“上传证书”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。

   WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**表4-3**将证书转换为PEM格式，再上传。

   表 4-3 证书转换命令

格式类型	转换方式（通过openssl工具进行转换）
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	– 提取私钥命令，以“cert.pfx”转换为“cert.key”为例。**openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** – 提取证书命令，以“cert.pfx”转换位“cert.pem”为例。**openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。**openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。

格式类型	转换方式（通过openssl工具进行转换）
DER	– 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**

2. 单击“确定”，上传证书。

步骤8 选择“是否已使用代理”，默认为“否”。

须知

当在Web应用防火墙前使用代理时，不能切换为“Bypass”工作模式。

- 若接入Web应用防火墙的网站已使用高防、CDN（Content Delivery Network，内容分发网络）、云加速等代理，为了保证WAF的安全策略能够针对真实源IP生效，请务必选择“是”，如果选择“否”，则Web应用防火墙无法获取Web访问者请求的真实IP地址。

  说明

  当在Web应用防火墙前使用CDN等代理时，WAF服务默认从HTTP Header“X-Forwarded-For”获取访问者真实源IP地址。当网站代理不使用“X-Forwarded-For”标识客户端原始IP地址时，需在“真实源IP头”所在行的“X-Forwarded-For”后单击 ，在弹出的对话框中，选择已有的source IP header或选择“自定义”后输入自定义的source IP header。
- 若接入Web应用防火墙的网站未使用任何代理，请选择“否”。

步骤9 单击“立即创建”，进入“域名接入”页面，同时在页面的右上角，会弹出“域名添加成功”。

说明

如果暂时不接入域名，可跳过本步骤，直接单击“下一步”后单击“完成”。后续再参照域名接入章节完成域名接入，此时，“DNS”解析状态显示“异常”。

- 若使用了CDN或高防等代理类服务，需要配置回源地址、子域名和TXT记录。
  a. 配置网站使用代理的“回源地址”。
     将CDN或高防等代理中的回源地址修改为WAF生成的回源地址。
  b. 配置“子域名”和“TXT记录”。
     前往您的DNS服务商处，添加一个“子域名”，并为该子域名添加一条“TXT记录”。

须知

WAF的多AZ灾备机制依赖DNS解析。请不要使用固定IP访问业务，否则会影响服务的灾备可靠性。

- 未使用代理，需要配置CNAME记录。

  a. 到该域名的DNS服务商处，配置防护域名的别名解析，具体操作请咨询您的域名服务提供商。

  须知

  WAF的多AZ灾备机制依赖DNS解析。请不要使用固定IP访问业务，否则会影响服务的灾备可靠性，因此：

  1. 请不要用修改hosts记录的方式替代DNS解析配置。
  2. 请不要用A记录替代CNAME记录。

  以下为当前主流的域名服务商的CNAME绑定方法，仅供参考。如与实际配置不符，请以各自域名服务商的信息为准。

  i. 登录域名服务提供商的管理控制台。

  ii. 进入域名解析记录页。

  iii. 设置CNAME解析记录。

  - “记录类型”选择为“CNAME”。
  - “主机记录”一般填写域名前缀，例如：防护域名为“admin.demo.com”，“主机记录”填写为“admin”。
  - “记录值”填写为WAF生成的CNAME。
  - “解析线路”，“TTL” 保持默认值即可。

  iv. 填写完成后，单击“保存”，完成解析设置。

  须知

  以上解析方法为第三方解析方法。本文档不对任何第三方内容进行控制或负责，包括但不限于其准确性、兼容性、可靠性、可用性、合法性、适当性、性能、不侵权、更新状态等。

  b. 验证域名的CNAME是否配置成功。

  i. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”。

  ii. 执行以下命令，查询CNAME。如果回显的域名是配置的CNAME，则表示配置成功。

  nslookup www.*domain*.com

步骤10 域名接入完成后，单击“下一步”。

步骤11 单击“完成”，防护域名添加成功。

用户可在域名列表中查看已添加防护域名的“DNS解析状态”和“工作模式”。

说明

- 若用户的服务器在使用其他网络防火墙，请将其关闭或者将WAF的IP网段添加到网络防火墙的IP白名单中。
- 若用户的服务器上已安装个人版安全软件，建议将其更换为企业版安全软件，并将WAF的IP网段添加到该软件的IP白名单中。
- 若防护域名已接入WAF，“DNS解析状态”为“正常”。如果“DNS解析状态”仍然为“异常”，可在目标域名所在行的“操作”列，单击“更多 > 检查DNS”，检查“DNS解析状态”，如果仍然为“异常”，可参照**如何处理DNS解析状态异常?** 重新进行域名接入。
- 域名添加成功后，Web应用防火墙默认开启防护。其中，Web基础防护开启“仅记录”（发现攻击行为后只记录不阻断攻击）防护模式，且WAF默认为该域名添加一条CC防护规则，该规则默认为500次/5s，最大可以调整到10000次/5s，可联系管理员调整上限，该规则只能修改不能删除。

----结束

对外协议与源站协议配置规则

根据您的业务场景的不同，WAF提供灵活的协议类型配置。假设您的网站为www.example.com，WAF可配置如下四种访问模式：

- HTTP访问模式。

  “对外协议”和“源站协议”都为“HTTP”。

  须知

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

- HTTPS访问模式，客户端协议全部配置为HTTPS时，当使用HTTP协议访问服务器时，会强制跳转为HTTPS协议。

  须知

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

- HTTP/HTTPS分别转发模式。

  服务器配置两条，一条“对外协议”和“源站协议”都为“HTTP”，一条“对外协议”和“源站协议”都为“HTTPS”。

  须知

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

- 使用WAF做HTTPS卸载模式。
  “对外协议”为“HTTPS”，和“源站协议”为“HTTP”。

须知

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

4.1.3 放行 WAF 回源 IP

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

须知

网站以“云模式”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WAF回源IP的访问控制策略。

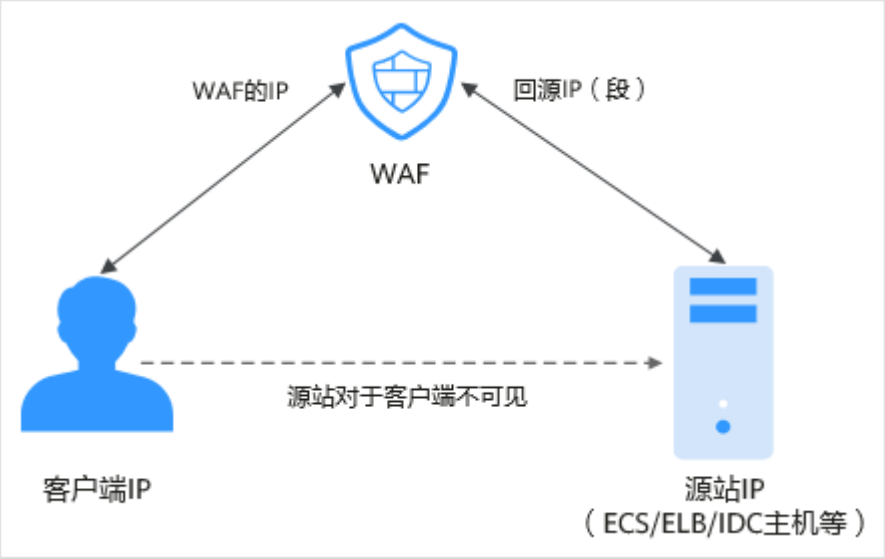
什么是回源 IP?

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

说明

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

图 4-4 回源 IP



回源 IP 检测机制

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

说明

Web应用防火墙的回源IP网段会定期更新，请及时将更新后的回源IP网段添加至相应的安全组规则中，避免出现误拦截。

为什么需要放行回源 IP 段?

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

说明

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“域名配置”，进入“域名配置”页面。

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

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

步骤7 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

----结束

4.1.4 本地验证

该章节指导用户在本地模拟接入WAF，然后访问被防护网站，验证WAF是否正常转发。

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

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

前提条件

- 已获取管理控制台的账号和密码。

- 已在WAF中添加了未使用其他代理的防护域名。

本地接入 WAF

步骤1 获取CNAME值。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。
3. 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，单击“域名配置”，进入“域名配置”页面。
4. 在目标域名所在行的“防护域名”列中，单击目标域名，进入域名基本信息页面。
5. 在“CNAME”信息行，单击，复制“CNAME”值。

步骤2 ping“CNAME”值并记录“CNAME”对应的IP地址（例如：192.168.0.1）。

步骤3 在本地修改hosts文件，将域名及“CNAME”对应的WAF回源IP添加到“hosts”文件。

1. 用记事本或notepad++等文本编辑器打开hosts文件，hosts文件一般位于“C:\Windows\System32\drivers\etc\”路径下。
2. 在hosts文件添加如**图5 追加记录**内容，前面的IP地址即在**步骤2**中获取的WAF回源IP地址，后面的域名即被防护的域名。

   图 4-5 追加记录

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [illegible].94.97      [illegible].acme.com          # source server
#       [illegible].63.10      [illegible]e.com              # x client host

# localhost name resolution is handled within DNS itself.
#   [illegible].0.1       localhost
#   ::1             localhost

192.168.0.1       www.example.com
```

3. 修改hosts文件后保存，然后本地ping一下被防护的域名。

   预期此时解析到的IP地址应该是**2**中绑定的WAF回源IP地址。如果依然是源站地址，可尝试刷新本地的DNS缓存（Windows的cmd下可以使用**ipconfig/flushdns**命令）。

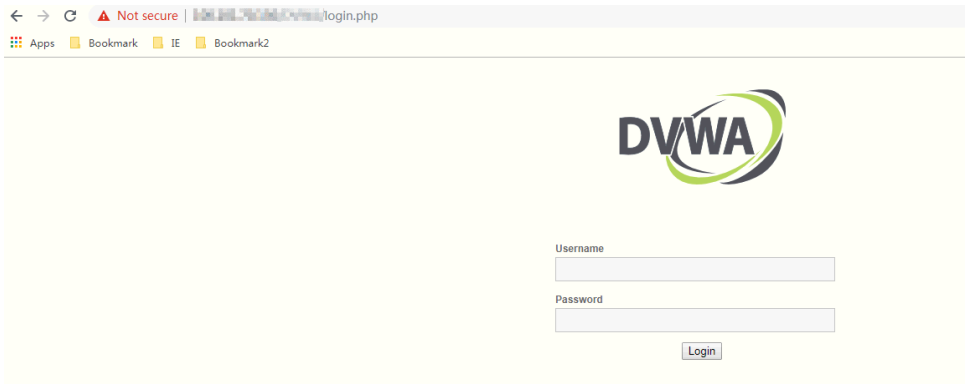
----结束

验证 WAF 转发正常

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。

如果hosts绑定已经生效（域名已经本地解析为WAF回源IP）且WAF的配置正确，访问该域名，预期网站能够正常打开。

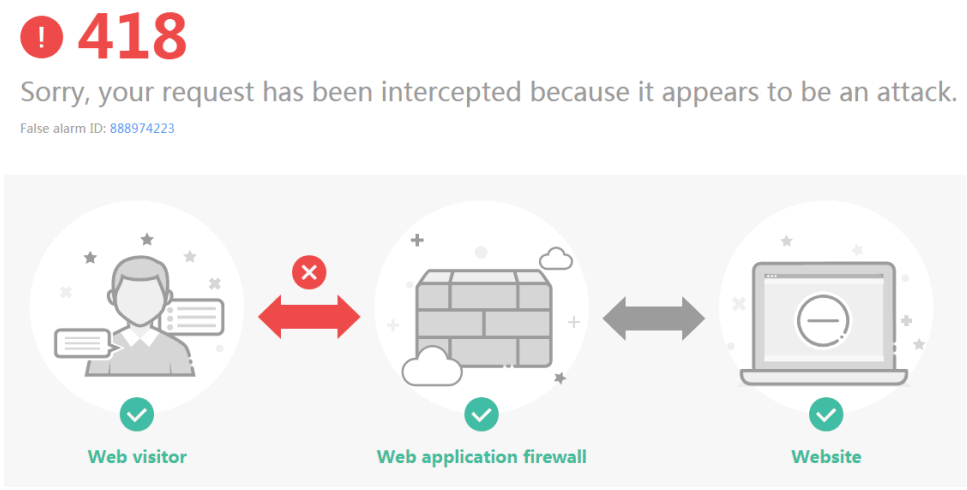
图 4-6 正常访问的网页



步骤2 手动模拟简单的web攻击命令，测试Web攻击请求。

1. 将Web基础防护的状态设置为“拦截”模式，具体方法请参见**配置Web基础防护规则**。
2. 清理浏览器缓存，在浏览器中输入“http://www.test.com?id=1%20or%201%20=1”模拟SQL注入攻击，测试WAF是否拦截了此条攻击，如**图4-7**所示。

图 4-7 访问被拦截



3. 在左侧导航树中，选择“防护事件”，查看防护域名测试的各项数据。

----结束

4.1.5 域名接入

该任务指导用户进行域名接入，使网站流量接入Web应用防火墙。

域名接入前，为了确保WAF转发正常，建议您先参照**本地验证**通过本地验证确保一切配置正常。

工作原理

- 未使用代理

  当网站没有接入到WAF前，DNS直接解析到源站的IP，所以当网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

- 使用了DDoS高防等代理

  当网站没有接入到WAF前，DNS解析到DDoS高防等代理，流量先经过DDoS高防等代理，DDoS高防等代理再将流量直接转到源站。网站接入WAF后，需要将DDoS高防等代理回源地址修改为WAF的“接入地址”，并且需要在DNS服务商处添加一条WAF的子域名和TXT记录，将域名解析到WAF，这样流量才会被DDoS高防等代理转发到WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名且域名未接入成功。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“防护域名”列中，单击域名名称，进入域名基本信息页面，完成域名接入。

- 未使用代理

  a. 在“CNAME”行中，单击，复制“CNAME”值。

  b. 到该域名的DNS服务商处，配置防护域名的别名解析，具体操作请咨询您的域名服务提供商。

  须知

  WAF的多AZ灾备机制依赖DNS解析。请不要使用固定IP访问业务，否则会影响服务的灾备可靠性，因此：

  1. 请不要用修改hosts记录的方式替代DNS解析配置。
  2. 请不要用A记录替代CNAME记录。

  以下为当前主流的域名服务商的CNAME绑定方法，仅供参考。如与实际配置不符，请以各自域名服务商的信息为准。

  i. 登录域名服务提供商的管理控制台。

  ii. 进入域名解析记录页。

  iii. 设置CNAME解析记录。

  - “记录类型”选择为“CNAME”。

- “主机记录”一般填写域名前缀，例如：防护域名为“admin.demo.com”，“主机记录”填写为“admin”。
- “记录值”填写为WAF生成的CNAME。
- “解析线路”，“TTL” 保持默认值即可。

iv. 填写完成后，单击“保存”，完成解析设置。

须知

以上解析方法为第三方解析方法。本文档不对任何第三方内容进行控制或负责，包括但不限于其准确性、兼容性、可靠性、可用性、合法性、适当性、性能、不侵权、更新状态等。

c. 验证域名的CNAME是否配置成功。

i. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”。

ii. 执行以下命令，查询CNAME。如果回显的域名是配置的CNAME，则表示配置成功。

nslookup www.*domain*.com

- 使用代理

a. 在接入地址、子域名、TXT记录所在行中，单击，复制“接入地址”、“子域名”和“TXT记录”。

b. 将使用的代理类服务（高防DDoS、CDN服务等）的回源地址修改为复制的目标域名的接入地址，并且前往您的DNS服务商处添加子域名，并为它配置TXT记录。域名接入成功后，网站流量正常接入Web应用防火墙。

须知

WAF的多AZ灾备机制依赖DNS解析。请不要使用固定IP访问业务，否则会影响服务的灾备可靠性。

说明

默认情况下，服务每隔一小时就会自动检测每个防护域名的DNS解析状态。如果您确认已完成域名接入，“DNS解析状态”为“正常”，则表示域名接入成功。

----结束

4.2 证书管理

4.2.1 上传证书

本章节指导用户如何上传证书。

前提条件

已获取管理控制台的账号和密码。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“证书管理”，进入“证书管理”界面。

步骤5 在页面的右上角，单击“上传证书”，进入“上传证书”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。

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**表4-4**将证书转换为PEM格式，再上传。

表 4-4 证书转换命令

格式类型	转换方式（通过openssl工具进行转换）
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	• 提取私钥命令，以“cert.pfx”转换为“cert.key”为例。 **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -nodes** • 提取证书命令，以“cert.pfx”转换位“cert.pem”为例。 **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	• 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**

步骤6 单击“确定”，上传证书成功。

说明

- 当导入的证书达到使用限额时，可以参照**删除证书**删除未绑定域名的证书后，再导入证书。
- 单击“证书名称”列中证书名称后的，可以修改证书名称。

----结束

4.2.2 删除证书

本章节指导用户如何删除证书，只能删除未使用的证书。

前提条件

- 已获取管理控制台的账号和密码。
- 待删除的证书未绑定域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”。

步骤4 在左侧导航树中，选择“证书管理”，进入“证书管理”界面。

步骤5 在待删除证书所在行的“操作”列，单击“删除”。

步骤6 在弹出的对话框中，单击“是”，证书删除成功。

----结束

4.3 管理防护域名

4.3.1 查看基本信息

本任务指导用户通过Web应用防火墙查看防护域名的基本信息，编辑域名的服务器信息。

前提条件

已获取管理控制台的账号和密码。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面，参数说明如表4-5所示。

表 4-5 参数说明

参数名称	参数说明
防护域名	防护域名。

参数名称	参数说明
工作模式	防护模式。 ● “开启防护”：开启状态。 ● “暂停防护”：关闭状态。 ● “Bypass”：该域名的请求直接到达其后端服务器，不再经过WAF。
DNS解析状态	DNS解析状态。 ● “异常”：域名未接入WAF或者接入不成功，DNS解析状态异常，参照**如何处理DNS解析状态异常?** 进行处理。 ● “正常”：域名接入WAF成功，DNS解析状态正常。
最近三天防护监控	该域名3天内的防护情况。可在“操作”列，单击“更多 > 查看攻击详情”查看具体的防护日志。
防护策略	防护策略配置情况。可单击“配置防护策略”配置具体的防护规则，具体的配置方法参见**配置防护规则**。

步骤4 在目标域名所在行的“防护域名”列中，单击目标域名，进入域名基本信息页面。

步骤5 查看防护域名的基本信息。

1. 查看“基本信息”和“Web应用防火墙信息”。

   在页面的右上方，单击 ，可刷新页面信息。

   说明

   - 域名ID：随机生成的唯一标识域名的ID。
   - 创建日期：添加域名的时间。
   - 用户可单击 ，复制“接入地址”、“子域名”、“TXT记录”或“Web应用防火墙IP段”。
   - 当客户端协议选择HTTPS时，若需要更新证书，在“证书名称”所在行的证书名称后，单击 ，在弹出的对话框中，重新选择已有证书。
   - 如果不需要使用代理，在“是否已使用代理”所在行，单击 ，在弹出的对话框中，选择“否”。

   说明

   - 域名ID：随机生成的唯一标识域名的ID。
   - 创建日期：添加域名的时间。
   - 用户可单击 ，复制“CNAME”或“Web应用防火墙IP段”。
   - 当客户端协议选择HTTPS时，若需要更新证书，在“证书名称”所在行的证书名称后，单击 ，在弹出的对话框中，重新选择已有证书。
   - 如果不需要使用代理，在“是否已使用代理”所在行，单击 ，在弹出的对话框中，选择“是”。

2. 查看服务器信息。

   单击“修改服务器信息”，进入“修改服务器信息”页面，根据需要修改服务器的各项配置（对外协议、已绑定的域名证书等）。

----结束

相关操作

在域名列表的“操作”列，可执行以下操作：

- 单击“切换”，可切换WAF的防护模式。
- 单击“配置防护策略”，可灵活配置WAF防护规则。
- 单击“更多 > 检查DNS”，可检测DNS的接入状态。
- 单击“更多 > 查看攻击详情”，可查看WAF的防护日志。
- 单击“更多 > 查看指标”，可查看WAF的监控日志，具体请参见《云监控服务用户指南》。
- 单击“更多 > 删除”，可删除防护域名。

4.3.2 开启防护

该任务指导用户通过Web应用防火墙服务开启防护。

说明

- 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。
- WAF根据QPS（HTTP GET请求量）或者业务带宽（所有该WAF防护的域名、站点中正常业务流量的大小）进行收费，且QPS的上限为10,000QPS（Query Per Second，即每秒钟的请求量，例如一个HTTP GET请求就是一个Query），带宽的上限为300Mbit/s。

前提条件

- 已获取管理控制台的账号和密码。
- 防护域名的“工作模式”为“暂停防护”或者“Bypass”。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”列，单击“切换”。

步骤5 在弹出的“切换工作模式”对话框中，选择“开启防护”，单击“确定”，启用防护操作成功。

----结束

4.3.3 停止防护

该任务指导用户通过Web应用防火墙服务停止防护。该模式下，WAF对所有的流量请求只转发不检测。

前提条件

- 已获取管理控制台的账号和密码。
- 防护域名的“工作模式”为“开启防护”或者“Bypass”。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”列，单击“切换”。

步骤5 在弹出的“切换工作模式”对话框中，选择“暂停防护”，单击“确定”，停止防护操作成功。

----结束

4.3.4 Bypass 模式设置

该任务指导用户通过Web应用防火墙服务进行Bypassed设置，即该域名的请求直接到达其后端服务器，不再经过WAF。

说明

当有测试等特殊场景，需要将业务恢复到没有接入WAF的状态，可以通过Bypass功能切换。

前提条件

- 已获取管理控制台的账号和密码。
- 防护域名的“工作模式”为“开启防护”或者“暂停防护”。
- Web应用防火墙之前未使用代理。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”列，单击“切换”。

步骤5 在弹出的对话框中，选择“Bypass”，单击“确定”，Bypass模式设置成功。

----结束

4.3.5 删除防护域名

该任务指导用户通过Web应用防火墙服务对不再防护的域名执行删除操作。

须知

- 如果要删除的防护域名已经接入Web应用防火墙，在删除防护域名前，请您先到DNS服务商处将域名重新解析，指向源站服务器IP地址，否则该域名的流量将无法切回服务器，影响正常访问。
- 删除域名后，1分钟内生效，且不可恢复，请谨慎删除防护域名。

前提条件

- 已获取管理控制台的账号和密码。
- 待删除域名已指向源站服务器地址。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标防护域名所在行的“操作”列中，单击“更多 > 删除”，进入删除防护域名对话框界面。

- 未使用代理

  说明

  - 确保已完成并勾选“已经在DNS服务商处将域名的CNAME删除并配置A记录到源站地址，或该域名业务已下线”。
  - 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”。

- 使用代理

  说明

  - 确保已完成并勾选“已经在高防、CDN或云加速等代理处将域名回源到源站，或该域名业务已下线”。
  - 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5 单击“是”，页面右上角弹出“删除成功”，则说明删除防护域名操作成功。

----结束

4.4 配置防护规则

本章节指导用户配置Web应用防火墙服务的各项防护规则。

4.4.1 配置 Web 基础防护规则

该任务指导用户通过Web应用防火墙服务配置Web基础防护。

Web基础防护开启后，可防范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，以及支持Webshell检测、搜索引擎、扫描器、脚本工具、其它爬虫等Web基础防护。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 在“Web基础防护”配置框中，用户可根据自己的需要参照表4-6更改Web基础防护的“状态”和“模式”，配置完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存相关设置，如果是误操作，单击“取消”取消相关配置。

表 4-6 防护动作参数说明

参数	说明
状态	Web应用防护攻击的状态。
模式	• 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6 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，根据您的业务场景，开启合适的防护功能。

说明

如果用户更改了5的“状态”和“模式”后，未单击“保存”，单击“高级设置”时，会弹出“警告”对话框。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

表 4-7 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。
Webshell检测	防护通过上传接口植入网页木马。
搜索引擎	为搜索引擎执行页面内容爬取任务，如Googlebot、Baiduspider。
扫描器	执行漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap。
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。 **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。

1. 防护等级设置。

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

   表 4-8 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。 当需要更严格地防护SQL注入、跨站脚本、命令注入等攻击行为时，建议使用“严格”模式。

2. 防护检测类型设置。

   默认开启“常规检测”和“扫描器”防护检测，用户可根据业务需要，单击  开启其他需要防护的检测类型。

3. 配置完成后，在页面的右上方，单击“保存”，Web基础防护配置成功，如果是误操作，单击“取消”取消相关配置。

----结束

4.4.2 配置 CC 攻击防护规则

该任务指导用户通过Web应用防火墙服务配置CC（Challenge Collapsar）攻击防护规则。

CC攻击防护规则根据IP、Cookie或者Referer字段设置灵活的限速策略，精准识别CC攻击以及有效缓解CC攻击。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 在“CC攻击防护”配置框中，用户可根据自己的需要更改“状态”，修改完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存，如果是误操作，单击“取消”取消相关配置。

步骤6 单击“自定义CC攻击防护规则”，进入CC防护规则配置页面，在“CC攻击防护”配置页面左上角，单击“添加规则”。

说明

如果用户修改了5的“状态”后，未单击“保存”，单击“自定义CC攻击防护规则”时，会弹出“警告”对话框。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

WAF默认添加一条CC防护规则，该规则默认为500次/5s，最大可以调整到10000次/5s，可联系管理员调整上限，只能修改不能删除。

步骤7 在弹出的对话框中，添加CC防护规则，请根据表4-9配置参数。

表 4-9 CC 防护规则参数说明

参数	参数说明	取值样例
路径	CC防护的URL链接，不包含域名。 ● 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”。 **说明** ● 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”，WAF引擎会将“///”转为“/”。	/admin*
限速模式	● IP限速：根据IP区分单个Web访问者。 ● 用户限速：根据Cookie键值区分单个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。 **说明** 当“防护模式”选择“其他”时，“Referer”对应的“Content”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，“Content”里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。 例如：防护路径设置为“/admin”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“Content”设置为“http://www.test.com”	用户限速
用户标识	“防护模式”选择“用户限速”时，需要设置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。如果用户没有设置Cookie键值，WAF会自动分配一个值。 例如：如果网站使用Cookie中的某个字段，name唯一标识用户，那么可以选取name字段来区分Web访问者。	name

参数	参数说明	取值样例
限速频率	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应用防火墙服务将暂停该Web访问者的访问。	10次/60秒
防护动作	当访问超过限制频率时，进行“人机验证”或者“阻断”。 • 人机验证：表示在指定时间内访问超过次数限制后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。 • 阻断：表示在指定时间内访问超过次数限制将直接阻断。 **说明** 当“防护模式”选择“其他”时，“防护动作”只能选择“阻断”。	阻断
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	当“防护动作”选择“阻断”时，需要设置，即当访问超过限速频率时，返回的错误页面。 • 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。	<html><body>Forbidden</body></html>

步骤8 单击“确认添加”，CC攻击防护规则添加成功，添加的CC攻击防护规则展示在CC规则列表中。

- 若需要修改添加的CC攻击防护规则时，可单击待修改的CC攻击防护规则所在行的“修改”，修改CC攻击防护规则。
- WAF默认添加的一条CC防护规则，只能修改不能删除。
- 若需要删除用户自行添加的CC攻击防护规则时，可单击待删除的CC攻击防护规则所在行的“删除”，删除CC攻击防护规则。

----结束

4.4.3 配置精准访问防护规则

该任务指导用户通过Web应用防火墙服务配置精准访问防护规则。

精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者IP进行条件组合，定制化防护策略，为用户的网站带来更精准的防护。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 在“精准访问防护”配置框中，用户可根据自己的需要更改精准访问防护的“状态”，配置完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存相关设置，如果是误操作，单击“取消”取消相关配置。

步骤6 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，设置“检测模式”。

说明

如果用户修改了步骤4的“状态”后，未单击“保存”，单击“自定义精准访问防护规则”时，会弹出“警告”对话框。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

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。

默认为“ 短路检测”检测模式，修改检测模式后需要单击“保存”，保存配置。

步骤7 在“精准访问防护配置”页面左上角，单击“添加规则”。

步骤8 在弹出的对话框中，添加精准访问防护规则，参数说明如表4-10所示。

表 4-10 规则参数说明

参数	参数说明	取值样例
规则名称	用户自定义为规则的名字。	waftest
防护动作	可选择“阻断”或者“放行”。默认为“阻断”。	“阻断”

参数	参数说明	取值样例
生效时间	用户可以选择“立即生效”或者自定义设置生效时间段。 自定义设置的时间只能为将来的某一时间段。	“立即生效”
条件列表	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。 ● 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。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 ● 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。 **说明** 具体的配置请参见**表4-11**。	● “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“Nessus”
优先级	设置该条件规则检测的顺序值。 值越小，优先级越高；值相同时，规则创建时间越早，优先级越高。	50

表 4-11 条件列表配置

字段	子字段（举例）	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”）	--	“包含”、“不包含”、“等于”、“不等于”、“前缀为”、“前缀不为”、“后缀为”、“后缀不为”。	/buy/phone/

字段	子字段（举例）	逻辑	内容（举例）
User Agent：设置为需要防护的扫描器的用户代理。	--	“包含”、“不包含”、“等于”、“不等于”、“前缀为”、“前缀不为”、“后缀为”、“后缀不为”。	Mozilla/5.0 (Windows NT 6.1)
IP：设置为需要防护的访问者IP地址。	--	“等于”、“不等于”。	192.168.2.3
Params：设置为需要防护的请求参数。	sttl	“包含”、“不包含”、“等于”、“不等于”、“前缀为”、“前缀不为”、“后缀为”、“后缀不为”。	201901150929
Cookie：根据Cookie区分的Web访问者。	name	“包含”、“不包含”、“等于”、“不等于”、“前缀为”、“前缀不为”、“后缀为”、“后缀不为”。	Nessus
Referer：设置为需要防护的自定义请求访问的来源。 例如：防护路径设置为“/admin/xxx”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“Content”设置为“http://www.test.com”。	--	“包含”、“不包含”、“等于”、“不等于”、“前缀为”、“前缀不为”、“后缀为”、“后缀不为”。	http://www.test.com
Header：设置为需要防护的自定义HTTP首部。	Accept	“包含”、“不包含”、“等于”、“不等于”、“前缀为”、“前缀不为”、“后缀为”、“后缀不为”。	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8

步骤9 单击“确认添加”，精准访问防护规则添加成功。

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

----结束

4.4.4 配置黑白名单规则

该任务指导用户通过Web应用防火墙服务配置黑白名单规则，阻断或放行指定IP的访问请求，即设置IP黑/白名单。

符合设置的黑白名单IP或者IP段规则，Web应用防火墙将拦截或者放行IP的访问。

IP黑白名单仅针对配置的特定域名生效。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 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”，设置完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存，如果是误操作，单击“取消”取消相关配置。

步骤6 单击“自定义黑白名单设置规则”，进入黑白名单设置规则页面，在“黑白名单”设置规则页面左上角，单击“添加规则”。

说明

如果用户修改了5的“状态”后，未单击“保存”，单击“自定义黑白名单设置规则”时，会弹出“警告”对话。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

步骤7 在弹出的对话框中，添加黑白名单规则，参数说明如表4-12所示。

表 4-12 黑白名单参数说明

参数	参数说明	取值样例
IP地址或IP地址段	• IP地址：添加黑名单或者白名单的IP地址。 • IP地址段：IP地址与子网掩码。	• XXX.XXX.1.1 • XXX.XXX.1.0/24
类型（防护动作）	IP地址或IP地址段设置的是白名单，则类型选择“Whitelist”。 IP地址或IP地址段设置的是黑名单，则类型选择“Blacklist”。	黑（拦截）

步骤8 单击“确认添加”，黑白名单添加成功。

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

----结束

4.4.5 配置网页防篡改规则

该任务指导用户通过Web应用防火墙服务配置网页防篡改规则。

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。

网页防篡改具有以下优势：

- 加速请求的响应

  当配置网页防篡改规则后，Web应用防火墙缓存服务端的静态网页，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

  当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，保证Web访问者访问的是正确的页面。

  Web应用防火墙具有随机抽取Web访问者的一个请求，将请求的页面与服务端页面进行对比的功能，若发现页面被篡改，将以短信或者Email的形式通知用户，告警通知的设置请参考**开启告警通知**。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 在“网页防篡改”配置框中，用户可根据自己的需要更改“状态”，设置完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存，如果是误操作，单击“取消”取消相关配置。

步骤6 单击“自定义网页防篡改规则”，进入网页防篡改规则的配置页面，在“网页防篡改”规则的配置页面左上角，单击“添加规则”。

说明

如果用户修改了5的“状态”后，未单击“保存”，单击“自定义网页防篡改规则”时，会弹出“警告”对话框。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

步骤7 在弹出的对话框中，添加网页防篡改规则，参数说明如表4-13所示。

表 4-13 参数说明

参数	参数说明	取值样例
域名	设置防篡改的域名。	www.example.com
路径	设置防篡改的URL链接，不包含域名。 **说明** • 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 例如：需要防护的URL为“http://www.example.com/admin”，则“路径”设置为“/admin”。

步骤8 单击“确认添加”，网页防篡改规则添加成功。

- 若防篡改的网页内容有修改，需要WAF重新缓存网页内容，可单击待更新的网页防篡改规则所在行的“更新缓存”。
- 若需要删除添加的网页防篡改规则时，可单击待删除的网页防篡改规则所在行的“删除”，删除网页防篡改规则。

----结束

4.4.6 配置误报屏蔽规则

该任务指导用户通过Web应用防火墙服务配置误报屏蔽规则。

对于误报情况，可以添加白名单对误报进行忽略，对某些事件ID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）。

仅WAF预置的Web基础防护规则可通过配置误报屏蔽规则进行屏蔽，用户自己添加的防护规则，若需要屏蔽，可将添加的防护规则删除。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 在“误报屏蔽”配置框中，用户可根据自己的需要更改“状态”，设置完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存，如果是误操作，单击“取消”取消相关配置。

步骤6 单击“自定义误报屏蔽规则”，进入“误报屏蔽”规则配置页面，在“误报屏蔽”规则配置页面左上角，单击“添加规则”。

说明

如果用户修改了5的“状态”后，未单击“保存”，单击“自定义误报屏蔽规则”时，会弹出“警告”对话框。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

步骤7 添加误报屏蔽规则，参数说明如表4-14所示。

说明

仅WAF预置的Web基础防护规则可通过配置误报屏蔽规则进行屏蔽，用户自己添加的防护规则，若需要屏蔽，可将添加的防护规则删除。

表 4-14 添加误报屏蔽规则参数说明

参数	参数说明	取值样例
路径	误报路径，完整的URL链接，不包含域名。 ● 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”。 **说明** ● 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“/”。	/admin 例如：需要防护的URL为“http://www.example.com/admin”，则“路径”设置为“/admin”。
事件ID	需要进行误报屏蔽处理的攻击事件所对应的内置规则ID。 **说明** 到“防护事件”的“查询”页面，在该攻击事件所在行的“操作”列，单击“误报处理”，可获取该攻击事件对应的规则编号ID。	0000-0000-0000-14-6faa68ff067b246a555a3efbb9fb83dc

步骤8 单击“确认添加”，在页面右上角弹出“添加成功”，则表示添加误报屏蔽规则成功。

若需要删除添加的误报屏蔽规则时，可单击待删除的误报屏蔽规则所在行的“删除”，删除误报屏蔽规则。

----结束

4.4.7 配置隐私屏蔽规则

该任务指导用户通过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

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“域名配置”，进入“域名配置”页面。

步骤4 在目标域名所在行的“操作”栏中，单击“配置防护策略”，进入“防护配置”页面。

步骤5 在“隐私屏蔽”配置框中，用户可根据自己的需要更改“状态”，设置完成后在“防护配置”列表的右上角，单击“保存”，并在弹出的对话框中，单击“是”保存，如果是误操作，单击“取消”取消相关配置。

步骤6 单击“自定义隐私屏蔽规则”进入隐私屏蔽规则配置页面，在“隐私屏蔽”规则配置页面左上角，单击“添加规则”。

说明

如果用户修改了5的“状态”后，未单击“保存”，单击“自定义隐私屏蔽规则”时，会弹出“警告”对话框。

- 单击“是”，取消之前的配置。
- 单击“否”后再单击“保存”，保存相关配置。

步骤7 添加隐私屏蔽规则，根据表4-15配置参数。

表 4-15 添加隐私屏蔽规则参数说明

参数	参数说明	取值样例
路径	完整的URL链接，不包含域名。 • 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”。 **说明** • 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“/”。	/admin/login.php 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”。

参数	参数说明	取值样例
屏蔽字段	设置为屏蔽的字段。 ● Params：请求参数。 ● Header：自定义HTTP首部。	● “屏蔽字段”为“Params”时，“子字段”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。 ● “Header”时，“子字段”请根据实际使用需求设置，如果设置为“Accept”，设置后，与“Accept”匹配的内容将被屏蔽。
子字段	根据“屏蔽字段”设置字段名，被屏蔽的字段将不会出现在日志中。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。	

步骤8 单击“确认添加”，隐私屏蔽规则添加成功。

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

----结束

4.5 策略管理

4.5.1 添加防护策略

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。该任务指导用户通过Web应用防火墙添加防护策略。

前提条件

已获取管理控制台的账号和密码。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“防护策略”，进入“防护策略”页面。

步骤4 在列表的右上角，单击“创建防护策略”。

步骤5 在弹出的对话框中，输入策略名称，单击“确定”。

步骤6 在目标策略所在行，单击策略名称，进入防护规则配置页面，参见**配置防护规则**为策略添加防护规则。

说明

- 若想修改策略名称，单击目标策略名称后的 ，在弹出的对话框中，重新输入新的策略名称即可。
- 防护策略添加成功后，Web应用防火墙默认开启防护。其中，Web基础防护开启“仅记录”（发现攻击行为后只记录不阻断攻击）防护模式；且WAF默认为该策略添加一条CC防护规则，该规则只能修改不能删除。

----结束

4.5.2 添加策略适用的防护域名

该任务指导用户通过Web应用防火墙服务添加策略适用的防护域名。

前提条件

- 已获取管理控制台的账号和密码。
- 已添加防护域名。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“防护策略”，进入“防护策略”页面。

步骤4 在目标策略名称所在行的“操作”列，单击“绑定防护域名”。

步骤5 在“防护域名”下拉框中选择适用于该策略的防护域名。

如果想了解所有域名的信息，单击“查看所有防护域名”，返回域名列表，查看详情。

须知

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

步骤6 单击“确定”，策略适用的防护域名添加成功。

----结束

4.6 安全总览

该任务指导用户通过Web应用防火墙服务查看防护日志，可查看到昨天、今天、3天、7天或者30天的访问与攻击统计次数、攻击分布、攻击源IP TOP5的次数。

前提条件

已获取管理控制台的账号和密码。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，进入Web应用防火墙“安全总览”页面。

步骤4 在域名下拉列表中，选择待查看的防护域名的防护日志，可查看“昨天”、“今天”、“3天”“7天”或者“30天”的防护概况。

说明

可在防护域名下拉列表中查看“所有域名”或者某一个域名的防护日志。

表 4-16 防护日志参数说明

参数	说明	界面说明
请求次数	访问者访问指定域名的总次数。 若“所有域名”下拉列表中选择的是“所有域名”，则统计的是访问所有域名的总次数。	-
请求峰值	每秒访问指定域名的最高的次数。	-
攻击次数	攻击指定域名的次数。	-
攻击源个数	攻击指定域名的攻击源个数。	-
攻击次数统计	攻击次数趋势图。	默认展示攻击次数统计趋势图。
访问次数统计	访问次数趋势图。	单击“访问次数统计”，查看访问次数统计趋势图。
事件分布	查看攻击事件类型。	• 单击“事件分布”中的其中一个颜色区域，可查看指定域名被攻击的类型、攻击的次数、以及攻击占比。 • 当不需要展示某种类型的攻击时，单击事件分布图右侧攻击类型对应的颜色方块，取消在事件分布圆环中的展示。

参数	说明	界面说明
攻击源IP TOP5(次)	攻击源IP TOP5的攻击次数统计。	-

----结束

4.7 管理防护事件

4.7.1 处理误报事件

当Web应用防火墙拦截或者记录的攻击事件为误报时，用户可通过Web应用防火墙对误报进行屏蔽。该任务指导用户通过Web应用防火墙处理误报事件、查看事件详情。

前提条件

- 已获取管理控制台的账号和密码。
- 事件详情列表中包含误报攻击事件。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“防护事件”，进入“防护事件”页面。

步骤4 选择“查询”页签，在域名下拉列表中选择待查看的防护域名或“所有域名”，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，参数说明如表4-17和表4-18所示。

在事件列表的右上角，单击“通过ID查询”，可以通过事件ID来查询防护事件。

表 4-17 防护事件参数说明

参数名称	参数说明
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。
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。

表 4-18 日志列表参数说明

参数名称	参数说明
时间	发生本次攻击的时间。
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。
URL	攻击的防护域名的URL。
恶意负载	发生攻击的恶意负载位置。
事件类型	发生攻击的类型。
防护动作	防护配置中设置的防护动作。

说明

如果需要查看目标域名攻击事件详情，可在事件列表中的“操作”列，单击“详情”。

步骤5 当攻击事件属于误报时，在该攻击事件所在行的“操作”列，可单击“误报处理”，添加误报屏蔽策略，参数说明如表4-19所示。

说明

- 仅WAF预置的Web基础防护规则可添加误报进行屏蔽，用户自己添加的规则无法执行误报屏蔽操作，若需要屏蔽，可将添加的防护规则删除。
- 在“误报处理”对话框右上方，单击“误报屏蔽”，可以跳转到误报屏蔽页面，您可以在误报屏蔽页面添加误报屏蔽规则。

表 4-19 误报处理参数说明

参数	参数说明	取值样例
防护对象	发生攻击事件的域名，系统自动获取。	--
路径	误报事件的URL路径，不包含域名。 • 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”。 **说明** • 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”，WAF引擎会将“///”转为“/”。	/admin*

参数	参数说明	取值样例
事件ID	自动读取的内置的规则ID。	0000-0000-0000-14-a77516b2df8a3324461edb9140d8c45b

步骤6 单击“确认添加”，处理误报，攻击事件详情列表中不再出现此误报。

说明

用户可以进入“域名列表”页面，在对应防护域名的所在行的“操作”列中，单击“配置防护策略”，在“误报屏蔽”栏中，单击“自定义误报屏蔽规则”，进入误报屏蔽列表，查看已添加的误报屏蔽事件。

----结束

4.7.2 下载防护事件数据

该任务指导用户通过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天内的所有防护域名的防护事件数据，当天的防护事件数据，在次日凌晨（UTC 01:00）生成防护事件数据文件。

前提条件

- 已获取管理控制台的账号和密码。
- 已生成了防护事件数据文件。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“防护事件”，进入“防护事件”页面，选择“下载”页签，参数说明如表4-20所示。

表 4-20 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10000，超过10000就会生成另一个文件。

步骤4 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

4.7.3 开启告警通知

该任务指导用户通过Web应用防火墙服务对攻击日志进行通知设置。Web应用防火墙可将仅记录和拦截的攻击日志通过用户设置的邮箱或者手机号发送给用户。

前提条件

- 已获取管理控制台的账号和密码。
- 已开通消息通知服务。

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 单击页面上方的“服务列表”，选择“安全 > Web应用防火墙”，在左侧导航树中选择“防护事件”，进入“防护事件”页面。

步骤4 选择“通知”页签，配置告警通知，根据表4-21配置参数。

表 4-21 通知设置参数说明

参数	参数说明
通知ID	告警事件ID。
通知状态	是否开启通知。
通知群组	单击下拉列表选择已创建的群组，或者单击“查看主题”创建新的群组。 更多信息，请参见《消息通知服务用户指南》。
告警频率	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	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。 详细的事件类型请参见表4-22。

表 4-22 事件类型列表

事件类型	说明
CC攻击	CC攻击事件，当客户发现网站处理速度下降，网络带宽占用过高时，很有可能已经遭受CC攻击。
命令注入	命令注入攻击是通过命令拼接、绕过黑名单等方式在服务端形成对业务攻击的系统命令，利用各种系统命令调用Web应用接口，从而实现对业务的攻击。

事件类型	说明
精准防护	精准访问防护事件。
非法请求	非法请求事件，例如，参数个数大于512个。
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。
本地文件包含	所谓的本地文件包含漏洞，其实就是你在Web端可以显现出某服务器本地的一些文件，或者可以下载获得一些敏感的配置之类的漏洞，主要是由于没有严格的过滤造成的。
恶意爬虫	扫描器爬虫攻击事件。
网页防篡改	网页防篡改攻击事件。
远程文件包含	远程文件包含攻击事件。
其他类型攻击	其它类型攻击，不容易区分类型的攻击事件，例如，SQL Injection和Command Injection的混合攻击，特定的CVE漏洞。
XSS攻击	跨站脚本攻击是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。
IP黑白名单	黑白名单事件。
网站木马	Webshell是一种Web入侵的脚本攻击工具，攻击者在入侵一个网站后，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。

步骤5 配置完成后，单击“保存”，告警通知设置成功。

----结束

5 独享模式 WAF

5.1 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到WAF进行防护。

使用流程

相关流程如**图5-1**，具体说明如**表5-1**所示。

图 5-1 WAF 使用流程

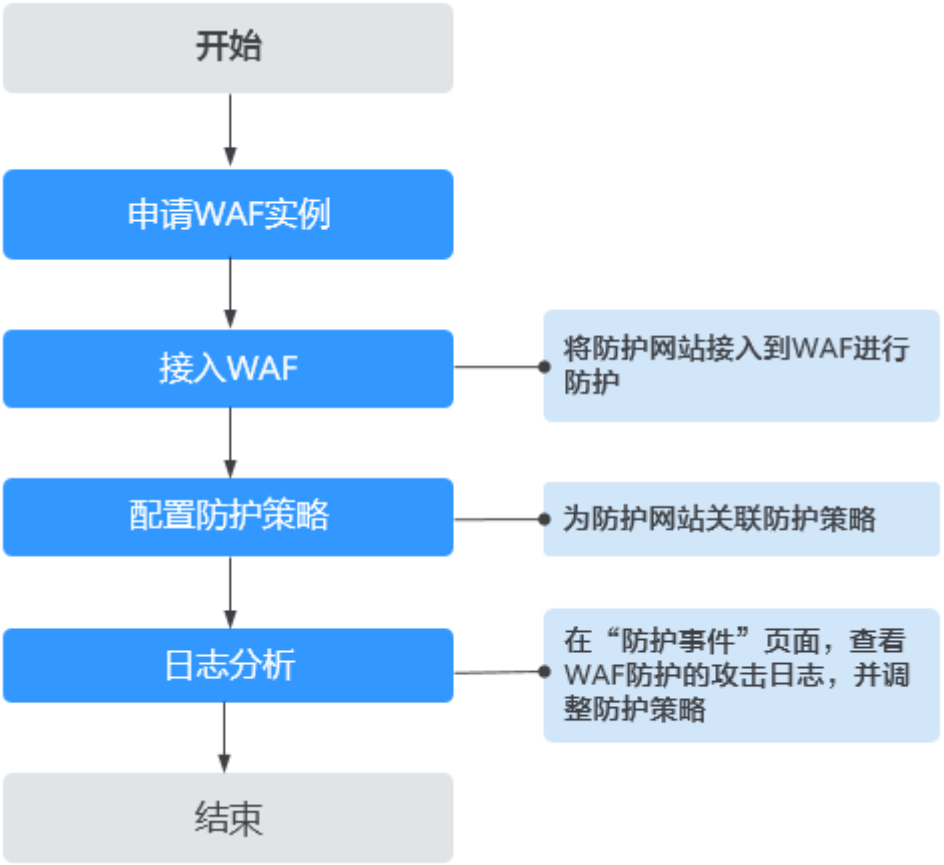


表 5-1 WAF 使用流程说明

操作	说明
申请WAF实例	通过申请独享引擎开通WAF。
接入WAF	添加需要防护的网站，WAF保护网站业务安全稳定。 **说明** • WAF引擎不是运行在客户的Web服务器上的，所以对客户的Web服务器的资源性能没有影响。 • 接入WAF之后，根据请求页面的大小和数量，会有几十毫秒的延迟。
配置防护策略	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。
日志分析	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。

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 5-2 配套功能

功能	说明
安全总览	可查看到昨天、今天、3天、7天或者30天范围内的防护数据。
配置PCI DSS/3DS合规与TLS配置TLS最低版本和加密套件	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。
配置网站连接超时时间	• 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。
配置连接保护	网站接入WAF防护之后，若您访问网站时出现大量的502 Bad Gateway，504 Gateway Timeout错误或者等待处理的请求，为了保护源站的安全，可使用WAF的宕机保护和连接保护功能。当502/504请求数量或读等待URL请求数量以及占比阈值达到您设置的值时，将触发WAF熔断功能开关，实现宕机保护和读等待URL请求保护。
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。
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。
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。
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、查看实例的监控信息、升级实例版本以及删除实例。
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。

5.2 申请 WAF 独享引擎实例

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

前提条件

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

操作须知

申请成功后，独享引擎实例规格不能修改。

须知

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙（独享）”。

步骤4 配置WAF实例参数，相关参数说明如表5-3所示。

表 5-3 WAF 独享引擎实例参数说明

参数名称	说明
WAF模式	独享模式
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	选择当前区域中的可用区。
WAF实例名称前缀	设置WAF实例名称前缀，申请多个实例时，实例前缀名称相同。
WAF实例数量	设置申请的WAF实例个数。
WAF实例规格	选择实例的规格。WAF支持500Mbit/s和100Mbit/s两种规格。
WAF实例创建类别	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	选择实例的CPU架构。
ECS规格	选择实例的ECS规格。
虚拟私有云	选择源站所在的VPC。

参数名称	说明
子网	选择VPC中已配置的子网。
安全组	选择区域中已有的安全组，或者单击“管理安全组”，跳转到VPC管理控制台创建新的安全组。选择安全组后，该实例将受到该安全组访问规则的保护。 **须知** • 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。 • 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。
标签	如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。
服务授权	勾选“我同意 WAF（Web应用防火墙）获取访问我的云资源权限：Tenant Guest、Server Administrator、VPCAdministrator、ELB Administrator”。 同意授权后，WAF将在IAM为您创建委托。

步骤5 确认参数配置无误后，在页面右下角单击“立即创建”。

步骤6 确认订单详情无误，单击“去创建”。

步骤7 单击“返回独享引擎列表”，在独享引擎实例列表界面，可以查看实例的创建情况。

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

----结束

5.3 安全总览

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。

说明

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

前提条件

- 已添加了防护域名并已完成了域名接入。
- WAF防护已开启。

- 已为防护域名添加了一个或者多个防护规则。

规格限制

在“安全总览”界面，最多可以查看30天的防护数据。

QPS 计算方式

不同时间段的QPS计算方式不同，QPS在各时间段的取值说明如表5-4所示。

表 5-4 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在页面上方，选择“企业项目”，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”：统计的是选择的企业项目下，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。

步骤5 查看统计的总的请求次数、攻击次数以及各类型攻击的页面总数。

- “请求次数”中统计的次数为网站的PV（Page Views）值，即用户每次访问网站，在某个时间内被访问的页面总数。
- “攻击次数”中统计的次数为网站被各类型攻击的总次数。

- 各攻击类型统计的次数为用户每次访问网站，在某个时间内被该类型攻击的页面总数。
- 单击“查看网站TOP统计”，可查看请求次数、攻击次数、Web基础防护、精准防护、CC攻击防护、爬虫攻击防护排名TOP 10的数据。

步骤6 “安全统计”模块数据展示。

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

- “昨天”、“今天”：间隔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。

表 5-5 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）。
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。

参数	说明
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

5.4 防护事件

5.4.1 查看防护日志

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

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目的防护日志。

前提条件

防护网站已接入WAF。

约束条件

- 下载防护事件文件时，如果您本地安装的安全软件拦截了下载文件，请关闭该软件后重新下载防护事件文件。
- 在WAF控制台只能查看所有防护域名最近30天的防护事件数据。您可以通过开启全量日志长期保存日志，并查看攻击日志和访问日志的详细信息。有关开启全量日志的详细操作，请参见**开启全量日志**。
- 如果您将防护网站的“工作模式”切换为“暂停防护”模式，WAF将对该防护网站所有的流量请求只转发不检测，同时，日志也不会记录。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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5-7**所示。
- 在事件列表的左上角，单击“导出”，可导出防护事件列表数据，防护事件数据小于200条将直接导出到本地；防护事件数据大于等于200条时，将在“下载”页面生成一条防护事件数据，您可以在下载页面去下载防护事件数据。
- 单击 ，可选择防护事件列表展示的字段。
- 在目标事件的“操作”列单击“详情”，可查看目标域名攻击事件详情。

表 5-6 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、人机验证等。 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。
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 5-7 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。	-

参数	说明	示例
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
状态码	拦截页面返回的HTTP状态码。	418
恶意负载	本次攻击对防护域名造成伤害的位置、组成部分或访问URL的次数。 **说明** • 对于CC攻击事件，恶意负载表示当时访问URL的次数。 • 对于黑名单防护事件，恶意负载为空。	id=1 and 1='1
企业项目	网站所在的企业项目。	default

----结束

5.4.2 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，则您可以通过设置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。

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。

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，才能处理该企业项目下的误报事件。

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。
- 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全 > Web应用防火墙 (独享)”。

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“更多 > 误报处理”，添加误报处理策略。

表 5-8 参数说明

参数	参数说明	取值样例
防护方式	- “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	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。 条件设置参数说明如下： - 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。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 - 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	- “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	“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： - 按ID：按攻击事件的ID进行配置。 - 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 - 所有内置规则：**Web基础防护规则**里开启的所有防护规则。	按类别
不检测规则ID	当“不检测规则类型”选择“按ID”时，需要配置此参数。 “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。	041046

参数	参数说明	取值样例
不检测规则类别	当“不检测规则类型”选择“按类别”时，需要配置此参数。 在下拉框中选择事件类别。 WAF支持的防护事件类别有：XSS攻击、网站木马、其他类型攻击、SQL注入攻击、恶意爬虫、远程文件包含、本地文件包含、命令注入攻击。	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	不拦截SQL注入攻击
高级设置	如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，WAF将不再拦截指定字段的攻击事件。 在左边第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。 – 当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。 – 当选择“Body”或“Multipart”字段时，可以配置“全部”。 – 当选择“Cookie”字段时，“防护域名”可以为空。 **说明** 当字段配置为“全部”时，配置完成后，WAF将不再拦截该字段的所有攻击事件。	Params 全部

- 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“更多 > 添加到地址组”，添加成功后将根据该地址组所应用的防护策略进行拦截或放行。

  “添加方式”可选择已有地址组或者新建地址组。
- 将源IP添加至对应防护域名下的黑白名单策略。在目标防护事件所在行的“操作”列，单击“更多 > 添加至黑白名单”，添加成功后该策略将始终对添加的攻击源IP进行拦截或放行。

表 5-9 参数说明

参数	参数说明
添加方式	– 选择已有规则 – 新建规则

参数	参数说明
规则名称	– 添加方式选择“选择已有规则”时，在下拉框中选择规则名称 。 – 添加方式选择“新建规则”时，自定义黑白名单规则的名字。
IP/IP段或地址组	添加方式选择“新建规则”时，需要配置此参数。 支持添加黑白名单规则的方式，“IP/IP段”或“地址组”。
地址组名称	“IP/IP段或地址组”选择“地址组”时，需要配置此参数。 在下拉列表框中选择已添加的地址组。。
防护动作	– 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**配置全局白名单规则对误报进行忽略**。

5.4.3 下载防护事件数据

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

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，才能下载该企业项目的防护事件数据。

前提条件

- 已添加防护网站。
- 已生成了防护事件数据文件。

规格限制

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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5-10。

表 5-10 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

字段	字段说明	示例
id	标识防护事件的ID。	02-11-16-20201121060347-feb42002
payload	攻击者对防护网站造成伤害的组成部分。	python-requests/2.20.1
payload_location	攻击者对防护网站造成伤害的位置或访问URL的次数。	user-agent
policyid	标识防护策略ID。	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。	/

5.4.4 开启全量日志

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

- 已添加防护网站。

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)”。

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，相关参数说明如表5-11所示。

表 5-11 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 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 查看WAF防护日志。

- 查看攻击日志
  a. 在日志流列表，单击配置的攻击日志流名称。
  b. 查看攻击日志。
- 查看访问日志
  a. 在日志流列表，单击配置的访问日志流名称。
  b. 查看访问日志。

----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.tenantid	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。
access_log.scheme	string	请求协议类型	请求所使用的协议有： ● 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”。

字段	类型	字段说明	描述
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_send	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。
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。	多次请求响应的时间，使用逗号分隔。
access_log.bind_ip	string	WAF引擎回源IP	WAF引擎所使用的回源IP。
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。

字段	类型	字段说明	描述
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	-
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。

字段	类型	字段说明	描述
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	-
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。

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	-

字段	类型	字段说明	描述
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。 ● 1：宽松 ● 2：中等 ● 3：严格
attack_log.attack	string	发生攻击的类型	发生攻击的类型，仅在攻击日志中出现。 ● 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	WAF防护攻击动作。 ● block：拦截 ● log：仅记录 ● captcha：人机验证

字段	类型	字段说明	描述
attack_log.sub_type	string	爬虫的子类型	当attack为robot时，该字段不为空。 ● script_tool：脚本工具 ● search_engine：搜索引擎 ● scaner：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	-
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	sting	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	-

字段	类型	字段说明	描述
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	-
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.mutipart	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	-

字段	类型	字段说明	描述
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。
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。

字段	类型	字段说明	描述
attack_log.hostid	string	防护域名ID（upstream_id）	-
attack_log.tenantid	string	防护域名的租户ID	-
attack_log.projectid	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	-
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）	-

5.5 防护策略

5.5.1 防护配置引导

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 5-12 可配置的防护规则

防护规则	说明	参考文档
Web基础防护规则	覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对恶意扫描器、IP、网马等威胁进行检测和拦截。	**配置Web基础防护规则防御常见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。	**配置CC攻击防护规则防御CC攻击**

防护规则	说明	参考文档
精准访问防护规则	精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者客户端IP进行条件组合，定制化防护策略，为您的网站带来更精准的防护。	配置精准访问防护规则定制化防护策略
黑白名单规则	配置黑白名单规则，阻断、仅记录或放行指定IP的访问请求，即设置IP黑/白名单。	配置IP黑白名单规则拦截/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。	配置攻击惩罚标准自动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。	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。	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。	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： • 敏感信息过滤。配置后可对返回页面中包含的敏感信息做屏蔽处理，防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。 • 响应码拦截。配置后可拦截指定的HTTP响应码页面。	配置防敏感信息泄露规则避免敏感信息泄露
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。	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。	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5-2所示，自定义规则的检测顺序如图5-3所示。

图 5-2 WAF 引擎检测图

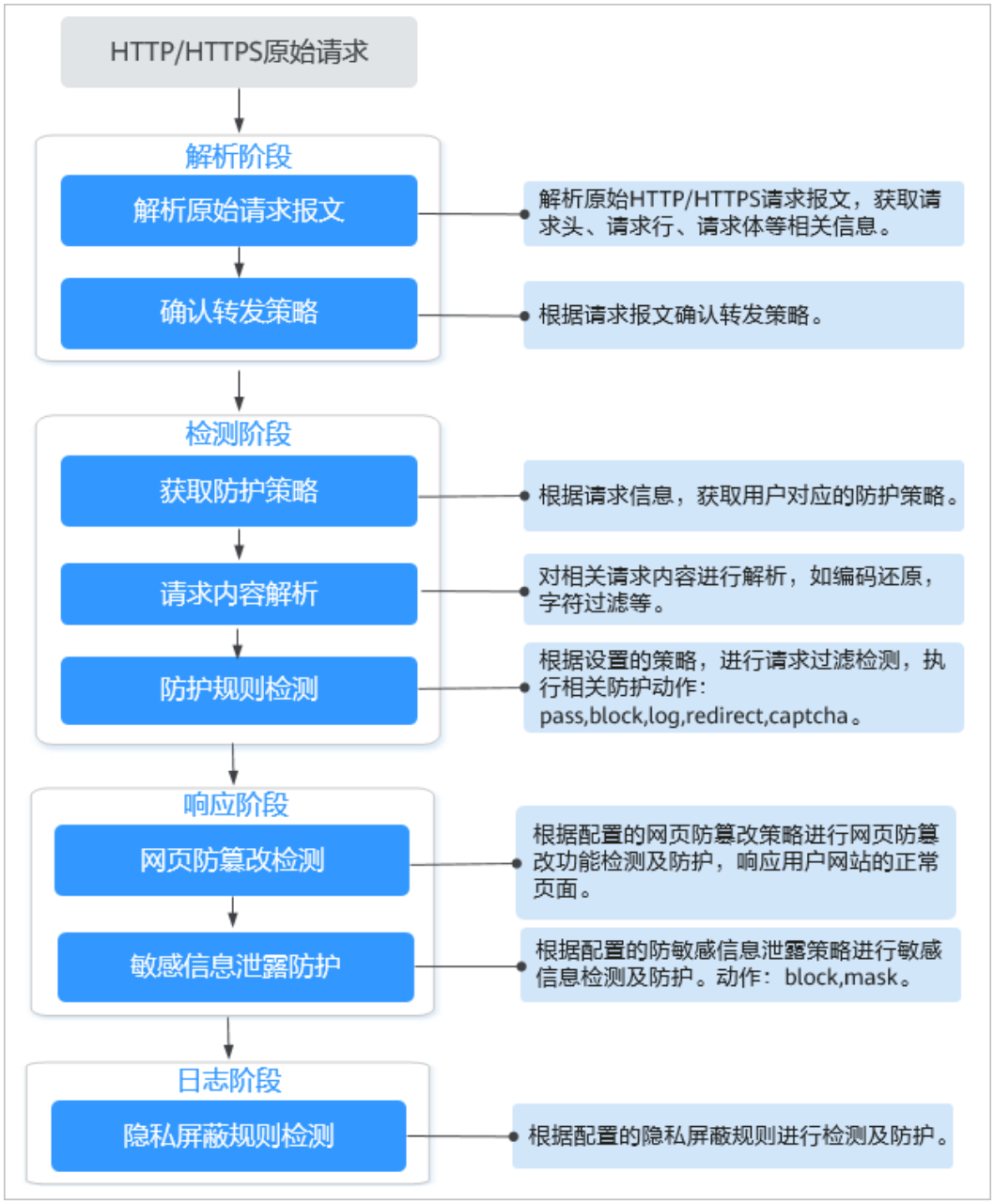
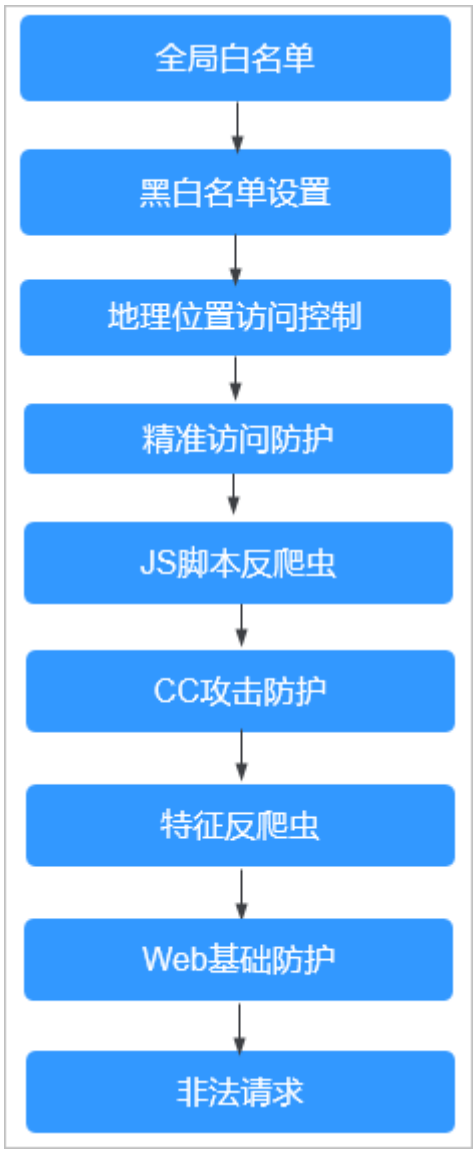


图 5-3 防护规则的检测顺序



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。

5.5.2 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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**新增防护策略**。

约束条件

- Web基础防护支持“拦截”和“仅记录”模式。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当Web基础防护设置为“拦截”模式时，您可以**配置攻击惩罚标准**。配置攻击惩罚后，如果访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据攻击惩罚设置的拦截时长来封禁访问者。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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**表5-13**更改Web基础防护的“状态”和“模式”。

表 5-13 防护动作参数说明

参数	说明
状态	Web应用防护攻击的状态。 •  ：开启状态 •  ：关闭状态
模式	• 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 选择“防护配置”页签，根据您的业务场景，开启合适的防护功能，检测项说明如**表5-15**所示。

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**配置攻击惩罚标准自动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 5-14 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5-15**开启其他需要防护的检测类型。

   表 5-15 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。

检测项	说明
深度检测	防护同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸。 **说明** 开启“深度检测”后，WAF将对深度反逃逸进行检测防护。
header全检测	默认关闭。关闭状态下WAF会检测常规存在注入点的header字段，包含User-Agent、Content-type、Accept-Language和Cookie。 **说明** 开启“header全检测”后，WAF将对请求里header中所有字段进行攻击检测。

----结束

防护效果

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

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

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

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

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

----结束

配置示例-拦截 SQL 注入攻击

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

步骤1 开启Web基础防护的“常规检测”，并将防护模式设置为“拦截”。

步骤2 开启Web基础防护。

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

WAF将拦截该访问请求，拦截页面示例如**图5-4**所示。

图 5-4 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

5.5.3 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

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当“逻辑”关系选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，需要选择引用表，创建引用表的详细操作请参见**创建引用表对防护指标进行批量配置**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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，根据表5-16配置CC防护规则。

表 5-16 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。	--
限速模式	• “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。 **说明** 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“/”。 例如：若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”。	--
用户标识	“限速模式”选择“用户限速”时，需要配置此参数： • 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	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。 ● 字段 ● 子字段：当“字段”选择IPv4、Cookie、Header、Params时，请根据实际需求配置子字段。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 ● 逻辑：在“逻辑”下拉列表中选择需要的逻辑关系。 **说明** 当“逻辑”关系选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，需要选择引用表，创建引用表的详细操作请参见**创建引用表对防护指标进行批量配置**。 ● 内容：输入或者选择条件匹配的内容。	“路径”包含“/admin/”
限速频率	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。	10次/60秒
防护动作	当访问的请求频率超过“限速频率”时，可设置以下防护动作： ● 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。可**下载防护事件数据**查看域名的防护日志。	阻断

参数	参数说明	取值样例
放行频率	当“防护动作”选择“动态阻断”时，可配置放行频率。 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”。 “放行频率”小于等于“限速频率”。 **说明** 当“放行频率”设置为0时，表示如果上一个限速周期发生过拦截后，下一个限速周期所有的请求都不放行。	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	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。 ● 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。	不同页面类型对应的页面内容样式： ● text/html：<html><body>Forbidden</body></html> ● application/json：{"msg": "Forbidden"} ● text/xml：<?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>

步骤9 单击“确认”，添加的CC攻击防护规则展示在CC规则列表中。

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

- 若需要删除用户自行添加的CC攻击防护规则时，可单击待删除的CC攻击防护规则所在行的“删除”，删除CC攻击防护规则。

----结束

防护效果

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

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

- 不能正常访问，参照章节**步骤一：添加防护网站（独享模式）**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，您也可以**下载防护事件数据**。

----结束

配置示例-人机验证

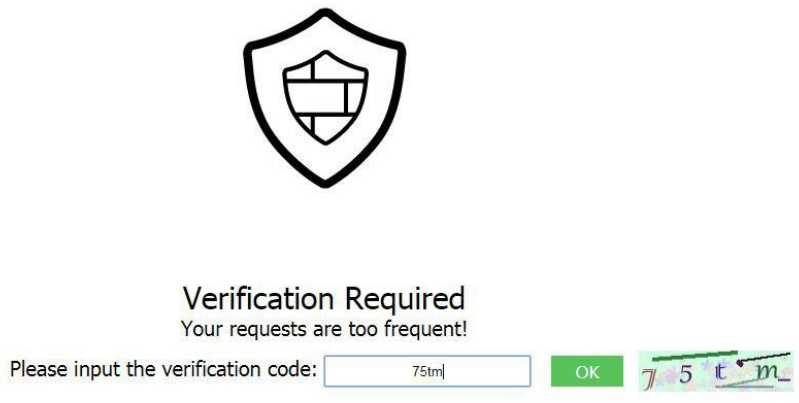
假如防护域名“www.example.com”已接入WAF，您可以参照以下操作步骤验证人机验证防护效果。

步骤1 添加防护动作为“人机验证”CC防护规则。

步骤2 开启CC攻击防护。

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

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



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

----结束

5.5.4 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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**新增防护策略**。

约束条件

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 当精准访问防护规则的“防护动作”设置为“阻断”时，您可以**配置攻击惩罚标准自动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（' "<>&*#%\?）。

应用场景

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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，根据表5-17添加精准访问防护规则。

须知

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

表 5-17 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	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。 条件设置参数说明如下： ● 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。 **说明** – 选择“包含任意一个”、“不包含所有”、“等于任意一个”、“不等于所有”、“前缀为任意一个”、“前缀不为所有”、“后缀为任意一个”或者“后缀不为所有”时，“内容”需要选择引用表名称，创建引用表的详细操作请参见**创建引用表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。 **说明** 具体的配置请参见**表5-28**。	“路径”包含“/admin/”
防护动作	● 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，具体操作请参见**修改拦截返回页面**。 ● 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，查询命中当前规则的请求，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	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。 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。 **须知** 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。	5
生效时间	用户可以选择“立即生效”或者自定义设置生效时间段。 自定义设置的时间只能为将来的某一时间段。	“立即生效”

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

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的精准访问防护规则时，可单击待修改的精准访问防护规则所在行的“修改”，修改精准访问防护规则。
- 若需要删除添加的精准访问防护规则时，可单击待删除的精准访问防护规则所在行的“删除”，删除精准访问防护规则。

----结束

防护效果

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

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

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

步骤2 清理浏览器缓存，在浏览器中访问“http://www.example.com/admin”页面或者包含/admin的任意页面，正常情况下，WAF会阻断满足条件的访问请求，返回拦截页面。

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

----结束

配置示例-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5-5**所示。

图 5-5 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。

5.5.5 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。

前提条件

已添加防护网站或已**新增防护策略**。

约束条件

- WAF不支持批量导入黑白名单，如果您需要配置多个IP/IP地址段规则，请逐条添加黑白名单防护规则，放行或拦截指定IP/IP地址段。
- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 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**配置攻击惩罚标准自动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。

系统影响

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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，参数说明如表5-18所示。

说明

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

表 5-18 黑白名单参数说明

参数	参数说明	取值样例
规则名称	用户自定义黑白名单规则的名字。	WAF
IP/IP段	支持IP地址或IP地址段。 • IP地址：添加黑名单或者白名单的IP地址。 • IP地址段：IP地址与子网掩码。	XXX.XXX.2.3

参数	参数说明	取值样例
防护动作	• 拦截：IP地址或IP地址段设置的是黑名单且需要拦截，则选择“拦截”。 • 放行：IP地址或IP地址段设置的是白名单，则选择“放行”。 • 仅记录：需要观察的IP地址或IP地址段，可选择“仅记录”。再根据**防护事件数据**判断该IP地址或IP地址段是黑名单还是白名单。	拦截
攻击惩罚	当“防护动作”设置为“拦截”时，您可以设置攻击惩罚标准。设置攻击惩罚后，当访问者的IP、Cookie或Params恶意请求被拦截时，WAF将根据惩罚标准设置的拦截时长来封禁访问者。	长时间IP拦截
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 输入完成后，单击“确认”，添加的黑白名单展示在黑白名单规则列表中。

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

----结束

防护效果

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

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

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

步骤2 参照**操作步骤**，将您的客户端IP配置为黑名单。

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

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

----结束

5.5.6 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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**新增防护策略**。

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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，根据**表5-19**配置参数。

表 5-19 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
规则描述	可选参数，设置该规则的备注信息。	waf
地理位置	IP访问的地理范围。	-
防护动作	可以根据需要选择“拦截”、“放行”或者“仅记录”。	“拦截”

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

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的地理位置访问控制规则时，可单击待修改的地理位置访问控制规则所在行的“修改”，修改地理位置访问控制规则。
- 若需要删除添加的地理位置访问控制规则时，可单击待删除的地理位置访问控制规则所在行的“删除”，删除地理位置访问控制规则。

----结束

防护效果

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

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

- 不能正常访问，参照**步骤一：添加防护网站（独享模式）**重新完成域名接入。
- 能正常访问，执行**2**。

步骤2 参照**操作步骤**，将您的客户端IP来源地配置为拦截。

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

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

----结束

5.5.7 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。

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，才能为该企业项目下域名配置防护策略。

工作原理

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

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

前提条件

已添加防护网站或已**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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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**表5-20**所示。

表 5-20 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	设置防篡改的URL链接中的路径（不包含域名）。 URL用来定义网页的地址。基本的URL格式如下： 协议名://域名或IP地址[:端口号]/[路径名/…/文件名]。 例如，URL为“http://www.example.com/admin”，则“路径”设置为“/admin”。 **说明** • 该路径不支持正则。 • 路径里不能含有连续的多条斜线的配置，如“///admin”，WAF引擎会将“///”转为“/”。	/admin
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的网页防篡改规则展示在网页防篡改规则列表中。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若被防护页面进行了内容修改，必须单击待更新的网页防篡改规则所在行的“更新缓存”来更新缓存，如果您在页面更新后未更新缓存，WAF将始终返回最近一次缓存的页面内容。
- 若需要删除添加的网页防篡改规则时，可单击待删除的网页防篡改规则所在行的“删除”，删除网页防篡改规则。

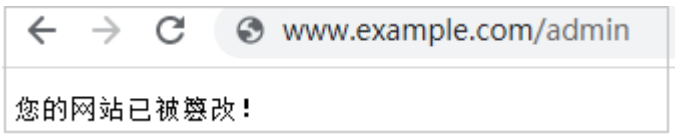
配置示例-静态页面防篡改

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

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

此时，显示的是被篡改的页面。

图 5-6 静态页面被篡改示例



步骤2 添加一条网页防篡改规则。

步骤3 开启网页防篡改。

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

步骤5 在浏览器中访问篡改后的页面。

此时，显示的是被篡改前的页面。

----结束

5.5.8 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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**新增防护策略**。

约束条件

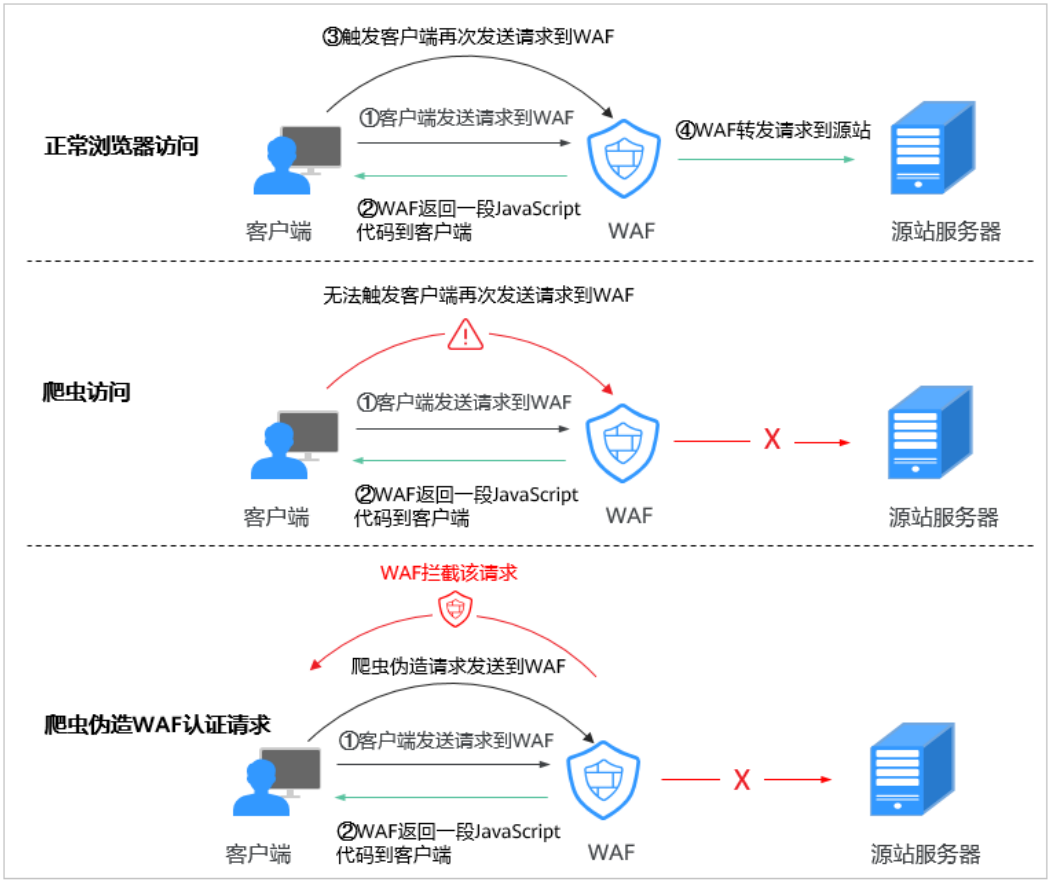
- JS脚本反爬虫依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用。
- 如果您的业务接入了CDN服务，请谨慎使用JS脚本反爬虫。

  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”的防护动作为仅记录，WAF不支持配置“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5-7**所示，其中，①和②称为“js挑战”，③称为“js验证”。

图 5-7 JS 脚本检测流程说明



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

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

通过统计“js挑战”和“js验证”，就可以汇总出JS脚本反爬虫防御的请求次数。例如，图5-8中JS脚本反爬虫共记录了18次事件，其中，“js挑战”（WAF返回JS代码）为16次，“js验证”（WAF完成JS验证）为2次，“其他”（即爬虫伪造WAF认证请求）为0次。

图 5-8 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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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“网站反爬虫设置”，进入网站反爬虫规则配置页面。

步骤7 选择“特征反爬虫”页签，根据您的业务场景，开启合适的防护功能，检测项说明如表5-21所示。

特征反爬虫规则提供了两种防护动作：

- 拦截

  发现攻击行为后立即阻断并记录。

  注意

  开启拦截后，可能会有以下影响：

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

- 仅记录
  默认防护动作，发现攻击行为后只记录不阻断攻击。

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

表 5-21 特征反爬虫检测项说明

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

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。
- 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，相关参数说明如表5-22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”。

- 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”。

表 5-22 JS 脚本反爬虫防护规则参数说明

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** • 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。	-
生效时间	立即生效	立即生效

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的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。
- 若需要删除添加的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）。

步骤3 开启网站反爬虫。

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

5.5.9 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（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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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，参数说明如表5-23所示。

“防敏感信息泄露”规则既能防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露，也能够拦截指定的HTTP响应码页面。

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

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

表 5-23 参数说明

参数名称	参数说明	取值样例
路径	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。 ● 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”。 **说明** – 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*
类型	● 敏感信息过滤：防止用户的敏感信息（例如：身份证号、电话号码、电子邮箱等）泄露。 ● 响应码拦截：拦截指定的HTTP响应码页面。	敏感信息过滤
内容	防护“类型”对应的防护内容，支持多选。	身份证号码
规则描述	可选参数，设置该规则的备注信息。	--

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

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 当您需要修改添加的防敏感信息泄露规则时，在待修改的防敏感信息泄露规则所在行，单击“修改”，修改防敏感信息泄露规则。

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

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。

步骤2 开启防敏感信息泄露。

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

5.5.10 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）。

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，才能为该企业项目下域名配置防护策略。

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。

- 添加或修改防护规则后，规则生效需要等待几分钟。规则生效后，您可以在“防护事件”页面查看防护效果。
- 您可以通过**处理误报事件**来配置全局白名单规则，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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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**表5-24**所示。

表 5-24 参数说明

参数	参数说明	取值样例
防护方式	• “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	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。 条件设置参数说明如下： ● 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。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。 ● 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	● “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	“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： ● 按ID：按攻击事件的ID进行配置。 ● 按类别：按攻击事件类别进行配置，如：XSS、SQL注入等。一个类别会包含一个或者多个规则id。 ● 所有内置规则：**Web基础防护规则**里开启的所有防护规则。	按类别
不检测规则ID	当“不检测规则类型”选择“按ID”时，需要配置此参数。 “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。	041046

参数	参数说明	取值样例
不检测规则类别	当“不检测规则类型”选择“按类别”时，需要配置此参数。 在下拉框中选择事件类别。 WAF支持的防护事件类别有：XSS攻击、网站木马、其他类型攻击、SQL注入攻击、恶意爬虫、远程文件包含、本地文件包含、命令注入攻击。	SQL注入攻击
规则描述	可选参数，设置该规则的备注信息。	不拦截SQL注入攻击
高级设置	如果您只想忽略来源于某攻击事件下指定字段的攻击，可在“高级设置”里选择指定字段进行配置，配置完成后，WAF将不再拦截指定字段的攻击事件。 在左边第一个下拉列表中选择目标字段。支持的字段有：Params、Cookie、Header、Body、Multipart。 ● 当选择“Params”、“Cookie”或者“Header”字段时，可以配置“全部”或根据需求配置子字段。 ● 当选择“Body”或“Multipart”字段时，可以配置“全部”。 ● 当选择“Cookie”字段时，“防护域名”可以为空。 **说明** 当字段配置为“全部”时，配置完成后，WAF将不再拦截该字段的所有攻击事件。	Params 全部

步骤9 单击“确认”。

----结束

相关操作

- 规则添加成功后，默认的“规则状态”为“已开启”，若您暂时不想使该规则生效，可在目标规则所在行的“操作”列，单击“关闭”。
- 若需要修改添加的全局白名单规则时，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。
- 若需要删除添加的**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。

5.5.11 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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**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。

系统影响

配置隐私屏蔽规则后，防护事件中将屏蔽敏感数据，防止用户隐私泄露。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用 防火墙 (独享)”。

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。

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**表5-25**配置参数。

表 5-25 添加隐私屏蔽规则参数说明

参数	参数说明	取值样例
路径	完整的URL链接，不包含域名。 ● 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”。 **说明** ● 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“/”。	/admin/login.php 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”。
屏蔽字段	设置为屏蔽的字段。 ● 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。	● “屏蔽字段”为“Params”时，屏蔽字段名请根据实际使用需求设置，如果设置为“id”，设置后，与“id”匹配的内容将被屏蔽。 ● “屏蔽字段”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。
屏蔽字段名	根据“屏蔽字段”设置字段名，被屏蔽的字段将不会出现在日志中。 **须知** 子字段的长度不能超过2048字节，且只能由数字、字母、下划线和中划线组成。	
规则描述	可选参数，设置该规则的备注信息。	--

步骤9 单击“确认”，添加的隐私屏蔽规则展示在隐私屏蔽规则列表中。

----结束

相关操作

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

5.5.12 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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**新增防护策略**。

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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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**表5-26**所示。

表 5-26 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	• 路径：设置的防护路径，不包含域名。 • User Agent：设置为需要防护的扫描器的用户代理。 • IP：设置为需要防护的访问者IP地址。 • Params：设置为需要防护的请求参数。 • Cookie：根据Cookie区分的Web访问者。 • Referer：设置为需要防护的自定义请求访问的来源。例如：防护路径设置为“/admin/xxx”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“值”设置为“http://www.test.com”。 • Header：设置为需要防护的自定义HTTP首部。	路径
值	对应“类型”的取值，该值不支持通配符。 **说明** 可单击“添加”设置多个值。	/buy/phone/

步骤10 单击“确认”，添加的引用表展示在引用表列表。

----结束

相关操作

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

5.5.13 配置攻击惩罚标准自动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。

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，才能为该企业项目下域名配置防护策略。

前提条件

已添加防护网站或已**新增防护策略**。

约束条件

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

规格限制

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

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**表5-27**所示。

表 5-27 攻击惩罚参数说明

参数	参数说明	取值样例
拦截类型	支持以下拦截方式： ● 长时间IP拦截 ● 短时间IP拦截 ● 长时间Cookie拦截 ● 短时间Cookie拦截 ● 长时间Params拦截 ● 短时间Params拦截	长时间IP拦截
拦截时长（秒）	拦截时长需要设置为整数，且设置范围为： ● 300<长时间拦截时长≤1800 ● 短时间拦截时长≤300	500
规则描述	可选参数，设置该规则的备注信息。	-

步骤9 输入完成后，单击“确认”，添加的攻击惩罚标准展示在列表中。

----结束

相关操作

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

配置示例-Cookie 拦截攻击惩罚

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

步骤1 在“网站设置”页面，单击“www.example.com”，进入域名基本信息页面。

步骤2 配置防护域名的Cookie流量标识，即“Session标记”。

步骤3 添加一条拦截时长为600秒的“长时间Cookie拦截”的攻击惩罚标准。

步骤4 开启攻击惩罚。

步骤5 添加一条黑白名单规则，拦截XXX.XXX.248.195，且“攻击惩罚”选择“长时间Cookie拦截”。

步骤6 清理浏览器缓存，在浏览器中访问“http://www.example.com”页面。

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

图 5-9 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

5.5.14 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**CC攻击防护规则**、**精准访问防护规则**或**配置误报屏蔽规则**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 5-10 条件字段

条件字段由字段、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“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 5-28 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** • 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（' "<>&*#% \?）。
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。	• 客户端IP • X-Forwarded-For • TCP连接IP		XXX.XXX.1.1
Params：设置为需要防护的请求参数。	• 所有字段 • 任意子字段 • 自定义		201901150929
Referer：设置为需要防护的自定义请求访问的来源。 例如：防护路径设置为“/admin/xxx”，若用户不希望访问者从“www.test.com”访问该页面，则“Referer”对应的“内容”设置为“http://www.test.com”。	--		http://www.test.com
Cookie：根据Cookie区分的Web访问者。	• 所有字段 • 任意子字段 • 自定义		jsessionid

字段	子字段	逻辑	内容（举例）
Header：设置为需要防护的自定义HTTP首部。	• 所有字段 • 任意子字段 • 自定义		*text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8*
Method：需要防护的自定义请求的方法。	--		GET、POST、PUT、DELETE、PATCH
Request Line：需要防护的自定义请求行的长度。	--		50
Request：需要防护的自定义请求的长度。包含请求头、请求行、请求体。	--		--
Protocol：需要防护的请求的协议。	--		http

5.6 管理策略

5.6.1 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。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为该企业项目添加防护策略。

前提条件

已添加防护网站。

约束条件

一个防护域名只能绑定一条防护策略。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“安全 > Web应用防火墙 (独享)”。

步骤3 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤4 在列表的左上角，单击“添加防护策略”。

步骤5 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6 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**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”。

5.6.2 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，才能为该企业项目批量添加防护规则。

前提条件

已添加防护网站。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 在目标策略名称所在行的“操作”列，单击“添加防护域名”。

步骤6 在“防护域名”下拉框中选择适用于该策略的防护域名。

须知

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

步骤7 单击“确认”。

----结束

5.6.3 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。

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，才能为该企业项目批量添加防护规则。

前提条件

已添加防护网站。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

步骤8 完成除“策略名称”以外其它参数的配置。

- “CC攻击防护”请参见**表5-16**进行参数配置。
- “精准访问防护”请参见**表5-17**进行参数配置。
- “黑白名单设置”请参见**表5-18**进行参数配置。
- “地理位置访问控制”请参见**表5-19**进行参数配置。
- “网页防篡改”请参见**表5-20**进行参数配置。
- “防敏感信息泄露”请参见**表5-23**进行参数配置。
- “全局白名单”请参见**表5-24**进行参数配置。
- “隐私屏蔽”请参见**表5-25**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

5.7 网站设置

5.7.1 网站接入 WAF（独享模式）

5.7.1.1 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到WAF进行监控防护。

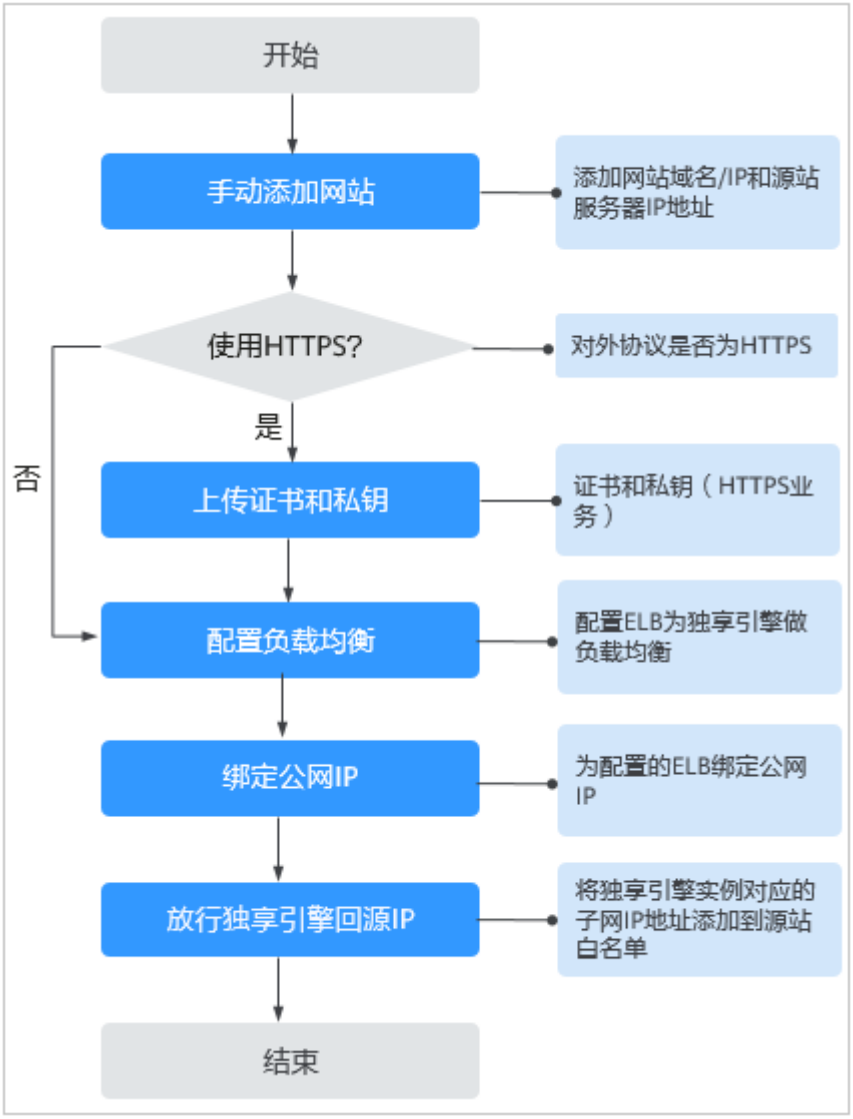
约束限制

- WAF独享模式可以防护通过域名或IP访问的Web应用/网站。
- 准备以独享模式接入WAF的网站已经使用独享型ELB（Elastic Load Balance）作为负载均衡。

网站接入流程说明

申请WAF独享模式后，您可以参照**图5-11**所示的配置流程，快速使用WAF。

图 5-11 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5-29所示相关信息。

表 5-29 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	• 域名：由一串用点分隔的英文字母组成（以字符串的形式来表示服务器IP），用户通过域名来访问网站。 • IP：访问网站所使用的IP地址。	www.example.com

获取信息	参数	说明	示例
	防护对象端口	需要防护的域名对应的业务端口。 • 标准端口 – 80：HTTP对外协议默认使用端口 – 443：HTTPS对外协议默认使用端口 • 非标准端口 80/443以外的端口	80
	对外协议	客户端（例如浏览器）请求访问网站的协议类型。WAF支持“HTTP”、“HTTPS”两种协议类型。	HTTP
	源站协议	WAF转发客户端（例如浏览器）请求的协议类型。包括“HTTP”、“HTTPS”两种协议类型。	HTTP
	VPC	选择申请的独享引擎实例所在的VPC。	vpc-default
	源站地址	网站服务器的私网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。 **说明** 源站地址不能与防护对象一致。	192.168.1.1
（可选）证书	证书名称	对外协议选择“HTTPS”时，需要在WAF上配置证书，将证书绑定到防护域名。 **须知** 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。	-

接入失败处理

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

5.7.1.2 步骤一：添加防护网站（独享模式）

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。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，在该企业项目下添加防护网站。

前提条件

已申请WAF独享引擎实例。

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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 在页面配置域名基本信息，相关参数说明如表5-30所示。

表 5-30 参数说明

参数	参数说明	取值样例
网站名称	自定义网站名称	WAF-OCB

参数	参数说明	取值样例
防护对象	防护的域名或IP，域名支持单域名和泛域名。 ● 单域名：输入防护的单域名。例如：www.example.com。 ● 泛域名 **说明** WAF不支持添加带有下划线（_）的泛域名。 – 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。	单域名：www.example.com 泛域名：*.example.com IP：XXX.XXX.1.1
网站备注	网站补充信息。	test
防护对象端口	在下拉框中选择面要防护的端口。 配置80/443端口，在下拉框中选择“Standard port”。	标准端口
服务器配置	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。 ● 对外协议：客户端请求到WAF独享引擎使用的协议。包括“HTTP”、“HTTPS”两种协议类型。 ● 源站协议：客户端请求经过WAF独享引擎转发到源站时使用的协议。包括“HTTP”、“HTTPS”两种协议类型。 **说明** WAF支持WebSocket/WebSockets协议，且默认为开启状态。 ● VPC：选择独享引擎实例所在的VPC。 ● 源站地址：客户端（例如浏览器）访问的网站服务器的私网IP地址。 ● 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。	对外协议：HTTP 源站协议：HTTP VPC：vpc-default 源站地址：192.168.1.1 源站端口：80

参数	参数说明	取值样例
证书名称	“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**。 创建证书的操作，请参见**上传证书**。 **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**导入新证书**将证书转换为PEM格式，再上传。 • 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7 选择“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前没有使用CDN、云加速等七层等代理服务器，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”。

步骤8 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”，防护网站添加成功。

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**步骤二：配置负载均衡**和**步骤三：为弹性负载均衡绑定弹性公网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。

   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5-31**在本地将证书转换为PEM格式，再上传。

   表 5-31 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	• 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	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	• 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。

5.7.1.3 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。
- 监听器的“后端端口”需要与WAF独享引擎实例实际监听的业务端口一致，即与**步骤一：添加防护网站（独享模式）**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。

添加监听器

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。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的  ，选择区域或项目。

步骤3 单击页面左上方的  ，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

步骤4 在负载均衡器所在行的“名称”列，单击目标负载均衡器名称，进入ELB“基本信息”页面。

步骤5 选择“监听器”页签后，单击“添加监听器”，配置监听器信息。

- “前端端口”：配置为WAF中配置的源站端口。
- “前端协议”：只能选择HTTP或HTTPS协议 。

步骤6 单击“下一步：配置后端分配策略”，配置后端服务器组。

须知

“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。

步骤7 单击“下一步：添加后端服务器”，配置健康检查。

须知

- 配置健康检查后，“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。

步骤8 单击“下一步：确认配置”。

步骤9 单击“提交”，监听器添加成功。

----结束

将 WAF 实例添加到 ELB

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)”。

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 > 添加到ELB”。

步骤6 在“添加到ELB”页面中，选择**添加监听器**中配置的“ELB（负载均衡器）”、“ELB监听器”和“后端服务器组”。

须知

“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。

步骤7 单击“确认”，为WAF实例配置业务端口，“业务端口”需要配置为WAF独享引擎实例实际监听的业务端口，即**步骤一：添加防护网站（独享模式）**中配置的“防护对象端口”。

----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。

5.7.1.4 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**配置的负载均衡**上。绑定后，请求流量会先经过WAF独享引擎进行攻击检测，然后转发到源站服务器，从而确保源站安全、稳定、可用。

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**配置负载均衡**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。

步骤4 在“负载均衡器”页面，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

5.7.1.5 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。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，在该企业项目下放行独享引擎回源IP。

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)”。

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

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

步骤6 单击页面左上方的，选择“计算 > 弹性云服务器”。

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5-32所示。

表 5-32 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)”。

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

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

步骤6 单击页面左上方的，选择“网络 > 弹性负载均衡”。

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

步骤8 选择“监听器”页签，在“访问控制”列单击“设置访问控制”。

步骤9 在弹出的对话框中，“访问策略”选择“白名单”。

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

步骤10 单击“确定”，白名单访问控制策略添加完成。

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

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

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

Telnet *源站IP* 443

----结束

5.7.1.6 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**步骤一：添加防护网站（独享模式）**~**步骤四：放行独享引擎回源IP**的操作。

（可选）单独验证独享 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。

  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。

  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。

5.7.2 高级配置

5.7.2.1 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，将无法正常访问网站，以满足行业客户的安全需求。

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

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，才能为该企业项目下的域名配置PCI DSS/3DS合规与TLS。

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。

应用场景

WAF默认配置的最低TLS版本为“TLS v1.0”，为了确保网站安全，建议您根据业务实际需求进行配置，推荐配置的最低TLS版本如表5-33所示。

表 5-33 推荐配置的最低 TLS 版本说明

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

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5-34所示。

说明

加密套件配置值中，带“!”的表示不支持。例如，!MD5表示不支持MD5算法。

表 5-34 加密套件说明

加密套件名称	加密套件配置值	说明
默认加密套件	• ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH • !MD5 • !aNULL • !eNULL • !NULL • !DH • !EDH • !AESGCM	• 兼容性：较好，支持的客户端较为广泛 • 安全性：一般
加密套件1	• ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH • !MEDIUM • !LOW • !aNULL • !eNULL • !DES • !MD5 • !PSK • !RC4 • !kRSA • !SRP • !3DES • !DSS • !EXP • !CAMELLIA • @STRENGTH	推荐配置。 • 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	• EECDH+AESGCM • EDH+AESGCM	• 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

加密套件名称	加密套件配置值	说明
加密套件3	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • RC4 • HIGH • !MD5 • !aNULL • !eNULL • !NULL • !DH • !EDH	• 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4	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH • !MD5 • !aNULL • !eNULL • !NULL • !EDH	• 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。

加密套件名称	加密套件配置值	说明
加密套件5	• AES128-SHA:AES256-SHA • AES128-SHA256:AES256-SHA256 • HIGH • !MEDIUM • !LOW • !aNULL • !eNULL • !EXPORT • !DES • !MD5 • !PSK • !RC4 • !DHE • @STRENGTH	仅支持RSA-AES-CBC算法。
加密套件6	• 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	• 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5-35**所示。

须知

建议您以实际客户端环境测试的兼容情况为准，避免影响现网业务。

表 5-35 加密套件不兼容的浏览器/客户端参考说明（TLS v1.0）

浏览器/客户端	默认加密套件	加密套件1	加密套件2	加密套件3	加密套件4
Google Chrome 63 /macOS High Sierra 10.13.2	×	√	√	√	×
Google Chrome 49/ Windows XP SP3	×	×	×	×	×
Internet Explorer 6/Windows XP	×	×	×	×	×
Internet Explorer 8/Windows XP	×	×	×	×	×
Safari 6/iOS 6.0.1	√	√	×	√	√
Safari 7/iOS 7.1	√	√	×	√	√
Safari 7/OS X 10.9	√	√	×	√	√
Safari 8/iOS 8.4	√	√	×	√	√
Safari 8/OS X 10.10	√	√	×	√	√
Internet Explorer 7/Windows Vista	√	√	×	√	√
Internet Explorer 8～10/Windows 7	√	√	×	√	√
Internet Explorer 10/Windows Phone 8.0	√	√	×	√	√
Java 7u25	√	√	×	√	√
OpenSSL 0.9.8y	×	×	×	×	×
Safari 5.1.9/OS X 10.6.8	√	√	×	√	√
Safari 6.0.4/OS X 10.8.4	√	√	×	√	√

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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

- 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。

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。

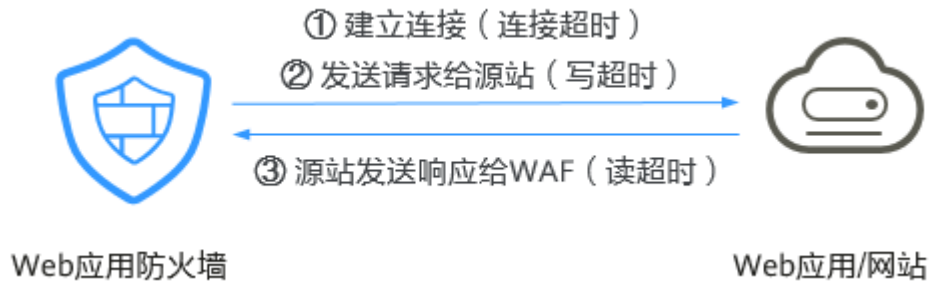
5.7.2.2 配置 WAF 到网站服务器的连接超时时间

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，若在设定的写超时时间内源站未接收到请求，则认为连接超时。
- **读超时**：WAF从源站读取响应的超时时间，若在设定的读超时时间内未收到来自源站的响应，则认为连接超时。

WAF转发请求给源站的三个步骤如图5-12所示。

图 5-12 WAF 转发请求给源站



说明

- 浏览器到WAF引擎的连接超时时长是120秒，该值取决于浏览器的配置，该值在WAF界面不可以手动设置。
- WAF到客户源站的连接超时时长默认为30秒，该值可以参考本章节进行手动设置。

前提条件

已添加防护网站。

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击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)”。

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

5.7.2.3 开启连接保护

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

前提条件

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

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击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)”。

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。

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5-36**所示。

表 5-36 连接保护参数说明

参数		参数说明	示例
宕机保护	502/504数量阈值	每30s累加的502/504数量阈值	1000
	502/504数量占比(%)	总请求数量中502/504数量占比达到所设定值，并且与数量阈值同时满足时触发宕机保护。	90
	初次保护时间(秒)	初次触发宕机的保护时间，即WAF将停止转发用户请求的时间。	180
	连续触发叠加系数	连续触发时，保护时间延长最大倍数，叠加周期为3600s。 例如，“初次保护时间”设置为180s，“连续触发叠加系数”设置为3。 ● 当触发次数为2（即小于3）时，保护时间为360s。 ● 当次数大于等于3时，保护时间为540s。 ● 当累计保护时间超过1小时（3600s），叠加次数会从头计数。	3
连接保护	读等待URL请求数量阈值	读等待URL请求数量到达设定值即触发连接保护	6000
	保护时间(秒)	达到数量阈值所触发的保护时间，即WAF将停止转发用户请求的时间。	60

----结束

5.7.2.4 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。

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，才能为该企业项目下的域名配置攻击惩罚的流量标识。

前提条件

已添加防护网站。

约束条件

- 使用Cookie或Params恶意请求的攻击惩罚功能前，您需要分别配置对应域名的Session标记或User标记。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

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

步骤6 在“流量标识”栏中，单击“IP标记”、“Session标记”或“User标记”后的，分别设置流量标记，相关参数说明如表5-37所示。

表 5-37 流量标识参数说明

标识	说明	配置样例
IP标记	客户端最原始的IP地址的HTTP请求头字段。 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）。 **须知** • 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。	jssessionid
User标记	用于Params恶意请求的攻击惩罚功能。在选择Params拦截的攻击惩罚功能前，必须配置该标识。	name

步骤7 单击“确认”，完成标记信息配置。

----结束

5.7.2.5 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。

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，才能为该企业项目下域名修改拦截返回页面。

前提条件

已添加防护网站。

约束条件

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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

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

步骤7 单击“确认”，告警页面配置成功。

----结束

5.7.3 基本信息维护

5.7.3.1 查看基本信息

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

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目下域名。

前提条件

已成功添加防护网站。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 查看防护网站信息，参数说明如表5-38所示。

表 5-38 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	防护模式。单击，可选择以下两种防护模式： • “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。 详细操作请参见切换工作模式。

参数名称	参数说明
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。
企业项目	域名所在企业项目。

步骤6 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。

步骤7 查看防护网站的信息。

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。

----结束

5.7.3.2 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。

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，才能切换该企业项目下域名的工作模式。

前提条件

防护域名已接入WAF。

应用场景

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“工作模式”列，单击，选择工作模式。

----结束

5.7.3.3 更新证书

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

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

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，才能为该企业项目下的域名更新证书。

前提条件

- 已添加防护网站。
- 防护网站的“对外协议”使用了HTTPS协议。

约束条件

- 域名和证书需要一一对应，泛域名只能使用泛域名证书。如果您没有泛域名证书，只有单域名对应的证书，则只能在WAF中按照单域名的方式逐条添加域名进行防护。
- WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**步骤6**将证书转换为PEM格式，再上传。

系统影响

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

  WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**表5-39**在本地将证书转换为PEM格式，再上传。

  表 5-39 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	– 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	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	– 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。

- “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

5.7.3.4 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**更新证书**。

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，才能为该企业项目下域名的服务器配置信息。

前提条件

已添加防护网站。

系统影响

修改服务器配置信息对业务无影响。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

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

步骤6 在“服务器信息”栏中，单击。

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

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

步骤8 单击“确认”，完成服务器信息修改。

----结束

5.7.3.5 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。

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，才能删除该企业项目下域名。

前提条件

已添加防护域名。

系统影响

删除网站后，1分钟内生效，且不可恢复，请谨慎删除防护网站。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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

5.8 管理证书

5.8.1 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。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为该企业项目上传证书。

前提条件

已获取证书文件和证书私钥信息。

规格限制

WAF支持创建的证书套数和WAF支持防护的域名的个数相同。例如，WAF支持防护10个域名，则WAF支持创建10套证书。

约束条件

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

应用场景

当域名的“对外协议”设置为“HTTPS”时，需要配置证书。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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

步骤5 在证书列表左上方，单击“上传证书”，弹出添加证书的对话框。

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。

WAF当前仅支持PEM格式证书。如果证书为非PEM格式，请参考**表5-40**在本地将证书转换为PEM格式，再上传。

表 5-40 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	• 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	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	• 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“应用”，您可以将证书绑定到对应的域名。
- 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。

5.8.2 绑定证书到防护网站

当您的防护网站“对外协议”为“HTTPS”时，您可以将上传的证书绑定到防护网站。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，为该企业项目绑定证书到防护网站。

前提条件

- 证书未到期。
- 防护网站的“对外协议”使用了HTTPS协议。

约束条件

- 同一证书可以绑定多个防护网站。
- 同一防护网站只能绑定一个证书。

应用场景

当域名的“对外协议”设置为“HTTPS”时，需要配置证书。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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“应用”。

步骤6 在弹出的“应用域名”对话框中，选择应用该证书的防护网站。

步骤7 单击“确认”，将证书绑定到防护网站。

----结束

生效条件

证书的“应用域名”列显示已应用该证书的防护网站。

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。

5.8.3 删除证书

当证书过期或证书无效时，您可以删除该证书。

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，才能删除该企业项目下的证书。

前提条件

证书没有被使用，即证书未绑定防护网站。

约束条件

如果证书已绑定防护网站，删除证书前需要解除该证书与域名绑定关系。

系统影响

- 删除证书不会影响业务。
- 证书删除后不可恢复，请谨慎删除证书。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全 > Web应用防火墙 (独享)”。

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

5.8.4 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。

说明

如果您已开通企业项目，您可以在“企业项目”下拉列表中选择您所在的企业项目，查看该企业项目下的证书信息。

前提条件

在WAF上创建了证书。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的 ，选择区域或项目。

步骤3 单击页面左上方的 ，选择“安全 > Web应用防火墙 (独享)”。

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5-41所示。

表 5-41 证书参数说明

参数名称	参数说明
名称	证书名称。

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

----结束

相关操作

- 当鼠标移到目标证书的名称后时，单击，您可以修改证书的名称。

  须知

  如果证书正在使用中，请先解除域名和证书的绑定关系，否则无法修改证书名称。

- 在目标证书所在行的“操作”列中，单击“查看”，您可以查看证书的证书文件和证书私钥信息。
- 在目标证书所在行的“操作”列中，单击“应用”，您可以将证书绑定到对应的域名。
- 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。

5.9 系统管理

5.9.1 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、查看实例的监控信息、升级实例版本以及删除实例。

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，才能管理该企业项目下的独享引擎。

前提条件

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

查看独享引擎实例信息

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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

步骤5 查看独享引擎实例信息，如表5-42所示。

表 5-42 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。	-
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

查看独享实例的云监控信息

当实例的“运行状态”为“运行中”时，您可以查看实例的云监控信息。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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“云监控”，跳转到云监控，查看实例的CPU、内存、带宽等监控信息。

----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。根据独享引擎实例个数不同选择不同升级方法：

- **单独享引擎实例节点升级**
- **多独享引擎实例节点升级**

说明

当独享引擎实例为最新版本时，“升级”按钮为灰化状态。

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)”。

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 > 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)”。

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 > 删除”。

步骤6 在弹出的对话框中，输入“DELETE”后单击“确认”。

----结束

5.9.2 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。

说明

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

前提条件

已申请Web应用防火墙实例。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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

5.10 授权并关联企业项目

企业管理服务提供统一的云资源按企业项目管理，以及企业项目内的资源管理、成员管理，企业项目可以授权给一个或者多个用户组进行管理。您可以在企业管理服务创建相关WAF的企业项目来集中管理您的WAF资源。

创建企业项目并授权

- 创建企业项目

  进入管理控制台页面，单击右上方的“企业 > 项目管理”，进入企业项目管理页面。单击“创建企业项目”，输入名称。

  说明

  开通了企业项目的客户，或者权限为企业主账号的客户才可以看到控制台页面上方的“企业”入口。

- 授权

  通过为企业项目添加用户组，并设置策略，实现企业项目和用户组的关联。将用户加入到用户组，使用户具有用户组中的权限，从而精确地控制用户所能访问的项目，以及所能操作的资源。具体步骤如下：

  a. 在新创建的企业项目所在行，单击操作列的“更多 > 查看用户组”，进入“用户组”区域。单击“添加用户组”，在左侧选择目标用户组，移入右侧区域。继续下一步设置策略，选择需要的云资源权限集。

b. 进入“人员管理 > 用户管理” 页面，选择目标用户，单击操作列的“加入到用户组”，在左侧区域选择已设置策略的用户组，移入右侧区域，完成授权过程。

- 关联资源与企业项目

  企业项目可以将云资源按企业项目统一管理。

  - 申请Web应用防火墙时选择企业项目
  - 资源迁入

    对于账号下申请的WAF计费资源，您可以在“企业项目管理”页面将资源迁入目标企业项目。

    “default”为默认企业项目，账号下原有资源和未选择企业项目的资源均在默认企业项目内。

5.11 审计

5.11.1 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 5-43 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

操作名称	资源类型	事件名称
删除CC规则	policy	deleteCc
创建精准防护规则	policy	createCustom
修改精准防护规则	policy	modifyCustom
删除精准防护规则	policy	deleteCustom
创建IP黑白名单规则	policy	createWhiteblackip
修改IP黑白名单规则	policy	modifyWhiteblackip
删除IP黑白名单规则	policy	deleteWhiteblackip
创建/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	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

5.11.2 查看云审计日志

开启了云审计服务后，系统开始记录WAF资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 WAF 的云审计日志

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，在右方的弹框中选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。

步骤4 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤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”。
  - “事件类型”选择“管理事件”。
  - “事件来源”选择“WAF”。
  - “筛选类型”选择“按资源ID”时，还需手动输入某个具体的资源ID。
- “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”：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

步骤6 单击“查询”，查看对应的操作事件。

步骤7 在需要查看的记录左侧，单击 展开该记录的详细信息，展开记录如图5-13所示。

图 5-13 展开记录

步骤8 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如图5-14所示，显示了该操作事件结构的详细信息。

图 5-14 查看事件

----结束

6 最佳实践

6.1 Web 漏洞防护最佳实践

6.1.1 Java Spring 框架远程代码执行高危漏洞

Spring是一款主流的Java EE轻量级开源框架，面向服务器端开发设计。近日，Spring框架被曝出可导致RCE远程代码执行的漏洞，该漏洞攻击面较广，潜在危害严重，对JDK 9及以上版本皆有影响。

漏洞名称

Spring框架RCE 0day安全漏洞

影响范围

- JDK 9及以上的。
- 使用了Spring框架或衍生框架。

防护建议

步骤1 **申请WAF独享引擎实例**。

步骤2 将网站域名添加到WAF中并完成域名接入。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

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

须知

目前，该漏洞存在两种攻击payload，是否开启“header全检测”根据攻击payload的方式而定：

- 第一种是通过在参数提交中携带攻击载荷。此时，“header全检测”可以不开启拦截。
- 第二种是在header自定义字段中携带攻击载荷。此时，“header全检测”必须开启拦截模式，才可以拦截此类攻击。

第二种攻击方式对第一种有依赖，所以是否要开启“header全检测”，您可以根据您的业务需求进行选择。

----结束

6.1.2 Apache Dubbo 反序列化漏洞

2020年02月10日，云安全团队监测到Apache Dubbo官方发布了CVE-2019-17564漏洞通告，漏洞等级中危。当用户选择http协议进行通信时，攻击者可以通过发送POST请求的时候来执行一个反序列化的操作，由于没有任何安全校验，该漏洞可以造成反序列化执行任意代码。目前，Web应用防火墙（Web Application Firewall，WAF）提供了对该漏洞的防护。

影响的版本范围

漏洞影响的Apache Dubbo产品版本包括： 2.7.0～2.7.4、2.6.0～2.6.7、2.5.x的所有版本。

安全版本

Apache Dubbo 2.7.5版本。

解决方案

建议您将Apache Dubbo升级到2.7.5版本。

如果您无法快速升级版本，或者希望防护更多其他漏洞，可以使用Web应用防火墙对该漏洞进行防护，请参照以下步骤进行防护：

步骤1 **申请WAF独享引擎实例**。

步骤2 将网站域名添加到WAF中并完成域名接入。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

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

----结束

6.1.3 开源组件 Fastjson 拒绝服务漏洞

2019年09月03日，云安全团队检测到应用较广的开源组件Fastjson的多个版本出现拒绝服务漏洞。攻击者利用该漏洞，可构造恶意请求发给使用了Fastjson的服务器，使其

内存和CPU耗尽，最终崩溃，造成用户业务瘫痪。目前，Web应用防火墙（Web Application Firewall，WAF）提供了对该漏洞的防护。

影响的版本范围

漏洞影响的产品版本包括：Fastjson 1.2.60以下版本，不包括Fastjson 1.2.60版本。

安全版本

Fastjson 1.2.60版本。

官方解决方案

建议用户将开源组件Fastjson升级到1.2.60版本。

防护建议

WAF支持对该漏洞的检测和防护，步骤如下：

步骤1 **申请WAF独享引擎实例**。

步骤2 将网站域名添加到WAF中并完成域名接入。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

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

----结束

6.1.4 开源组件 Fastjson 远程代码执行漏洞

2019年07月12日，云应急响应中心检测到开源组件Fastjson存在远程代码执行漏洞，此漏洞为2017年Fastjson 1.2.24版本反序列化漏洞的延伸利用，可直接获取服务器权限，危害严重。

影响的版本范围

漏洞影响的产品版本包括：Fastjson 1.2.51以下的版本，不包括Fastjson 1.2.51版本。

安全版本

Fastjson 1.2.51版本及以上的版本。

官方解决方案

建议用户将开源组件Fastjson升级到1.2.51版本或者最新的1.2.58版本。

防护建议

Web应用防火墙内置的防护规则支持对该漏洞的防护，参照以下步骤进行防护：

步骤1 **申请WAF独享引擎实例**。

步骤2 将网站域名添加到WAF中并完成域名接入。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

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

----结束

6.1.5 Oracle WebLogic wls9-async 反序列化远程命令执行漏洞（CNVD-C-2019-48814）

Oracle WebLogic wls9-async组件在反序列化处理输入信息时存在缺陷，攻击者可以发送精心构造的恶意HTTP请求获取目标服务器权限，在未授权的情况下远程执行命令，CNVD对该漏洞的综合评级为“高危”。

漏洞编号

CNVD-C-2019-48814

漏洞名称

Oracle WebLogic wls9-async反序列化远程命令执行漏洞

漏洞描述

WebLogic wls9-async组件存在缺陷，通过WebLogic Server构建的网站存在安全隐患。攻击者可以构造HTTP请求获取目标服务器的权限，在未授权的情况下远程执行命令。

影响范围

- Oracle WebLogic Server 10.X
- Oracle WebLogic Server 12.1.3

官方解决方案

官方暂未发布针对此漏洞的修复补丁。

防护建议

通过WAF的精准访问防护功能，参考**图6-1**和**图6-2**分别配置限制访问路径前缀为/_async/和/wls-wsat/的请求，拦截利用该漏洞发起的远程命令执行攻击请求。

图 6-1 async 配置

图 6-2 wls-wsat 配置

6.2 通过配置 TLS 最低版本和加密套件提升客户端访问域名的通道安全

HTTPS协议是由TLS（Transport Layer Security，传输层安全性协议）+HTTP协议构建的可进行加密传输、身份认证的网络协议。当添加防护域名时，如果客户端采用HTTPS协议请求访问服务器，即防护域名的“对外协议”配置为“HTTPS”时，您可以通过为域名配置最低TLS版本和加密套件来确保网站安全，详细说明如下：

- 最低TLS版本

  最低TLS版本是客户端通过TLS访问网站时，被允许访问网站的最低TLS版本。配置最低TLS版本后，只有满足最低TLS版本的请求，才能正常访问网站，可以满足行业网站的安全需求。

说明

- 截止目前，TLS已发布了三个版本（TLS v1.0、TLS v1.1、TLS v1.2），TLS v1.0和TLS v1.1版本由于发布时间久远，某些加密算法（如SHA1、RC4算法）很容易被黑客攻击，且在性能上，TLS v1.0和TLS v1.1已经无法满足呈几何级增长的数据传输加密，存在安全隐患。同时，为了保障通信协议的安全，满足支付卡行业数据安全标准（PCI DSS），支付卡行业安全标准委员会（PCI SSC）规定，TLS v1.0安全通信协议于2018年6月30日不再生效。火狐、Safari、Chrome、Edge等主流浏览器厂商也声明将于2020年全面停止支持TLS v1.0和TLS v1.1。
- 您可以通过**查看网站TLS版本**，检测网站支持的TLS版本。

- 加密套件

  加密套件是多种加密算法的集合。配置安全性更高的加密套件，可以保障网站的保密性和数据完整性。

推荐配置的最低 TLS 版本说明

为了确保网站安全，建议您根据业务实际需求进行配置，推荐配置的最低TLS版本如**表6-1**所示。

表 6-1 推荐配置的最低 TLS 版本说明

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

推荐配置的加密套件说明

WAF默认配置的加密套件为“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6-2**所示。

说明

加密套件配置值中，带“!”的表示不支持。例如，!MD5表示不支持MD5算法。

表 6-2 加密套件说明

加密套件名称	加密算法	说明
默认加密套件	ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM	• 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	加密算法	说明
加密套件1	ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH	推荐配置。 • 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	EECDH+AESGCM:EDH+AESGCM	• 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	ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH	• 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，不支持CBC算法。
加密套件4	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH	• 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	AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4:!DHE:@STRENGTH	仅支持RSA-AES-CBC算法。
加密套件6	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	• 兼容性：一般 • 安全性：较好

WAF提供的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。TLS版本不同，加密套件的浏览器或客户端兼容情况也不同。以TLS v1.0协议为例，加密套件的浏览器及客户端兼容性说明如**表6-3**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 6-3 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
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	×	×	×	×	×
Safari 5.1.9/OS X 10.6.8	√	√	×	√	√
Safari 6.0.4/OS X 10.8.4	√	√	×	√	√

配置 TLS 最低版本和加密套件

以独享WAF介绍如何配置TLS最低版本为“TLS v1.2”，加密套件为“加密套件1”，以及如何验证配置效果。

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)”。

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“TLS配置”所在行，单击。

说明

WAF支持一键开启PCI DSS和PCI 3DS合规认证功能，开启合规认证后，可以满足PCI DSS和PCI 3DS合规认证要求。

- 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。

步骤7 在弹出的“TLS配置”对话框中，选择最低TLS版本“TLS v1.2”和“加密套件1”。

步骤8 单击“确认”，TLS配置完成。

----结束

效果验证

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

您可以在本地通过命令行方式，验证TLS是否配置成功。在验证前，请确保您本地已安装**openssl**。

步骤1 复制防护域名的CNAME值，用于获取WAF的回源IP。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。
3. 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。
4. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
5. 在目标网站所在行的“域名”列中，单击目标网站，进入域名基本信息页面。

6. 在“CNAME”信息行，单击，复制“CNAME”值。

步骤2 获取WAF的回源IP。

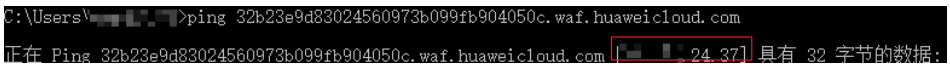
- 云模式

  在Windows操作系统的命令行窗口，执行以下命令，获取WAF的回源IP。

  ping *CNAME值*

  在界面回显信息中获取WAF回源IP，如图6-3所示。

  图 6-3 ping cname

- 独享模式

  a. 在左侧导航树中，选择“系统管理 > 独享引擎”，进入独享引擎实例列表页面。

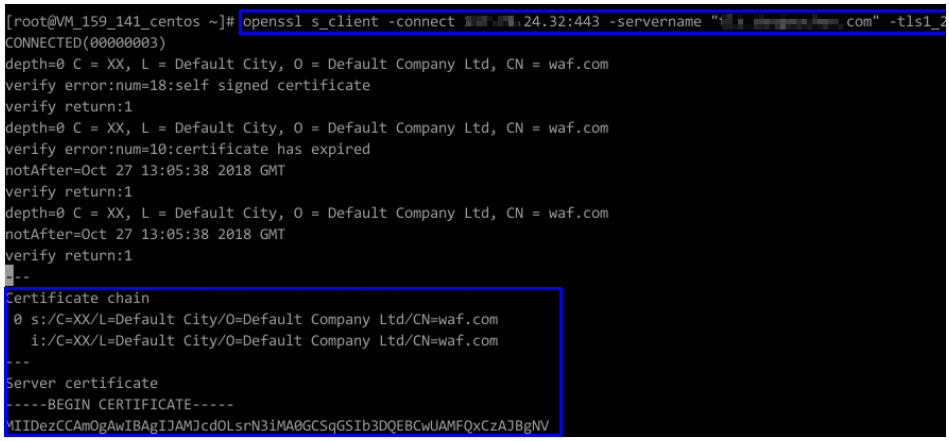
  b. 在独享引擎列表的“IP地址”栏，获取所有创建的独享引擎对应的子网IP地址，即独享引擎实例对应的回源IP。

步骤3 执行以下命令，验证“TLS v1.2”协议可以访问目标网站。

openssl s_client -connect *WAF回源IP* **-servername** "*防护域名*" **-tls1_2**

界面返回证书相关信息，如图6-4所示，说明“TLS v1.2”协议可以访问目标网站。

图 6-4 验证 TLS v1.2

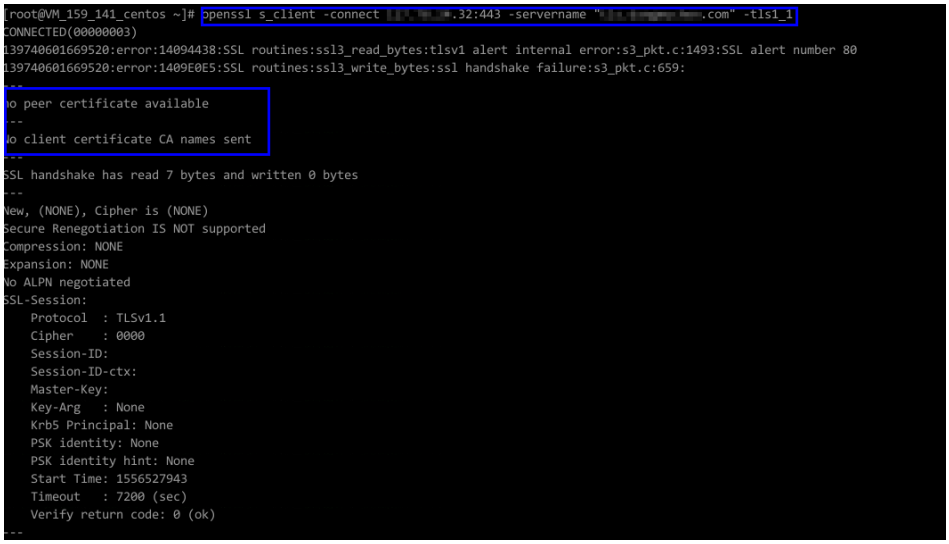


步骤4 执行以下命令，验证“TLS v1.1”协议不能访问目标网站。

openssl s_client -connect *WAF回源IP* **-servername** "*防护域名*" **-tls1_1**

界面未返回证书相关信息，如图6-5所示，说明WAF拦截了“TLS v1.1”的访问。

图 6-5 验证 TLS v1.1



----结束

6.3 CC 攻击防御最佳实践

6.3.1 简介

本手册基于Web应用防火墙实践所编写，指导您在遭遇CC（Challenge Collapsar）攻击时，完成基于IP限速和基于Cookie字段识别的防护规则的配置。

如何判断是否遭受 CC 攻击?

当客户发现网站处理速度下降，网络带宽占用过高时，很有可能已经遭受CC攻击，此时可查看Web服务器的访问日志或网络连接数量，如果访问日志或网络连接数量显著增加，则可确定已遭受CC攻击，可以按照以下策略进行配置，利用WAF阻断CC攻击，保障网站业务的正常运行。

说明

- WAF防护应用层流量的拒绝服务攻击，适合防御HTTP Get攻击等。
- WAF服务并不提供针对四层及以下流量的防护，例如：ACK Flood、UDP Flood等攻击，这类攻击建议使用DDoS及IP高防服务进行防护。

6.3.2 基于 IP 限速的配置

当WAF与访问者之间并无代理设备时，通过源IP来检测攻击行为较为精确，建议直接使用IP限速的方式进行访问频率限制。

实践案例

竞争对手控制数台主机，持续向网站“www.example.com”发起HTTP Post请求，网站并无较大的负载能力，网站连接数、带宽等资源均被该攻击者大量占用，正常用户无法访问网站，最终竞争力急剧下降。

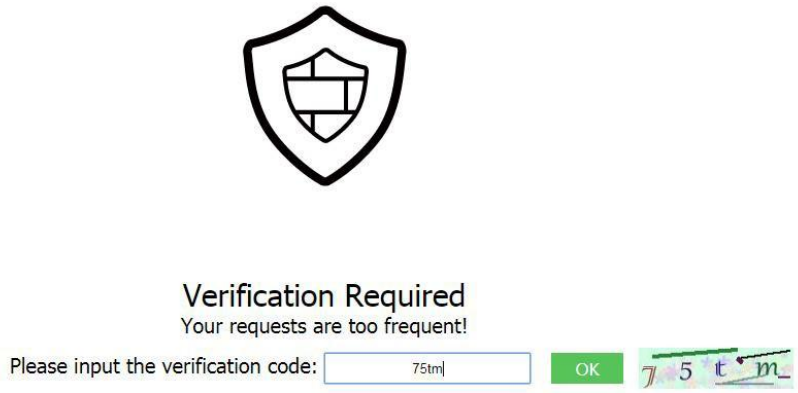
防护措施

1. 根据服务访问请求统计，判断网站是否有大量单IP请求发生，如果有则说明网站很有可能遭受了CC攻击。
2. 登录管理控制台，将您的网站成功接入Web应用防火墙。
   - 云模式：**添加防护域名**。
   - 独享模式：**步骤一：添加防护网站（独享模式）**。
3. 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面，确认“CC攻击防护”的“状态”为“开启”  。
4. 开启WAF的“CC攻击防护”后，添加CC防护规则，配置对域名下的请求进行基于IP限速的检测，针对业务特性，设置限速频率，并配置人机验证，防止误拦截正常用户，针对网站所有url进行防护，配置如**图6-6**所示。

图 6-6 IP 限速

   - 限速模式：选择“IP限速”，根据IP区分单个Web访问者。
   - 限速频率：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应用防火墙服务将暂停该Web访问者的访问。
   - 防护动作：防止误拦截正常用户，选择“人机验证”。
     - 人机验证：表示在指定时间内访问超过次数限制后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。
     - 阻断：表示在指定时间内访问超过次数限制将直接阻断。
     - 仅记录：表示在指定时间内访问超过次数限制将只记录不阻断。

当用户访问超过限制后需要输入验证码才能继续访问。



进入防护事件页面，可以查看攻击事件详情。

6.3.3 基于 Cookie 字段的配置

对于有些网站，源IP无法精准获取。例如：存在未在header中插入“X-Forwarded-For”字段的Proxy或其他原因，建议使用配置Cookie字段实现用户标识并开启“全局计数”。

实践案例

竞争对手控制数台主机，与大多普通访客一样，共用同一IP，或通过代理频繁更换源IP，持续向网站“www.example.com”发起HTTP Post请求，网站并无较大的负载能力，网站连接数、带宽等资源均被该攻击者大量占用，正常用户无法访问网站，最终竞争力急剧下降。

防护措施

1. 根据服务访问请求统计，判断网站是否有大量同一IP请求发生，如果有则说明网站很有可能遭受了CC攻击。
2. 登录管理控制台，将您的网站成功接入Web应用防火墙。
   - 云模式：**添加防护域名**。
   - 独享模式：**步骤一：添加防护网站（独享模式）**。
3. 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面，确认“CC攻击防护”的“状态”为“开启”  。
4. 开启WAF的“CC攻击防护”后，添加CC防护规则，配置“用户限速”模式，输入用户标识，即Cookie字段中的变量名。为了更加有效的标识用户，建议使用“sessionid”或“token”这类标识网站后台颁发给用户的唯一标识字段。

   说明

   “防护模式”选择“阻断”模式，设置“阻断时长”，能够在攻击被拦截后，攻击者需额外等待一段时间， 该设置能进一步对攻击者行为进行限制，建议对安全要求非常高的用户设置。

   - 限速模式：选择“用户限速”，根据Cookie键值区分单个Web访问者。
   - 用户标识：为了更加有效的标识用户，建议使用“sessionid”或“token”这类标识网站后台颁发给用户的唯一标识字段。

- 限速频率：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应用防火墙服务将暂停该Web访问者的访问。
- 防护动作：选择“阻断”模式。该模式可设置“阻断时长”，在攻击被拦截后，攻击者需额外等待一段时间才能访问正常的网页， 该设置能进一步对攻击者行为进行限制，建议对安全要求非常高的用户设置。
  - 人机验证：表示在指定时间内访问超过次数限制后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。
  - 阻断：表示在指定时间内访问超过次数限制将直接阻断。
  - 仅记录：表示在指定时间内访问超过次数限制将只记录不阻断。
- 阻断页面：可选择“默认设置”或者“自定义”。

6.3.4 通过业务 Cookie 和 HWWAFSESID 联合配置限制恶意抢购、下载

本文档通过CC防护规则配置业务Cookie和HWWAFSESID限制恶意抢购、下载等。

业务场景

- **场景一：**限制同一个账号切换IP、终端的恶意请求（抢购、下载等）。
  防护措施：**使用业务Cookie（或者用户id）基于路径配置CC限速**
- **场景二：**限制恶意人员在同一个PC多个账号不停切换的恶意请求（抢购、下载等）。
  防护措施：**使用HWWAFSESID基于路径配置CC限速**

使用业务 Cookie（或者用户 id）基于路径配置 CC 限速

步骤1 登录管理控制台，将您的网站成功接入到WAF。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

步骤2 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤3 在“CC攻击防护”配置框中，确认“CC攻击防护”的状态为开启，单击“自定义CC攻击防护规则”，进入CC防护规则配置页面。

步骤4 在“CC攻击防护”规则配置页面左上角，单击“添加规则”。

步骤5 根据业务情况，使用业务Cookie（或者用户id）基于路径配置CC限速，参考如**图6-7**进行配置。

根据实际情况配置以下参数。

图 6-7 业务 Cookie 配置

步骤6 单击“确认”，完成配置。

----结束

使用 HWWAFSESID 基于路径配置 CC 限速

步骤1 登录管理控制台，将您的网站成功接入到WAF。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

步骤2 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤3 在“CC攻击防护”配置框中，确认“CC攻击防护”的“状态”为“开启”，单击“自定义CC攻击防护规则”，进入CC防护规则配置页面。

步骤4 在“CC攻击防护”规则配置页面左上角，单击“添加规则”。

步骤5 根据业务情况，使用HWWAFSESID基于路径配置CC限速，参考如**图6-8**进行配置。

- “用户标识”：选择“Cookie”，配置为“HWWAFSESID”。
- 其他参数根据业务实际情况进行配置。

图 6-8 HWWAFSESID 配置

步骤6 单击“确认”，完成配置。

----结束

6.4 通过配置反爬虫防护策略阻止爬虫攻击

网络爬虫为网络信息收集与查询提供了极大的便利，但同时也对网络安全产生以下负面影响：

- 网络爬虫会根据特定策略尽可能多的“爬过”网站中的高价值信息，占用服务器带宽，增加服务器的负载
- 恶意用户利用网络爬虫对Web服务发动DoS攻击，可能使Web服务资源耗尽而不能提供正常服务
- 恶意用户利用网络爬虫抓取各种敏感信息，造成网站的核心数据被窃取，损害企业经济利益

Web应用防火墙可以通过Robot检测（识别User-Agent）、网站反爬虫（检查浏览器合法性）和CC攻击防护（限制访问频率）三个反爬虫策略，全方位帮您解决业务网站遭受的爬虫问题。

前提条件

域名已成功接入WAF。

开启 Robot 检测（识别 User-Agent）

开启Robot检测后，WAF可以检测和拦截恶意爬虫、扫描器、网马等威胁。

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)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤6 确认“Web基础防护”的状态为。

步骤7 单击“高级设置”，在“防护配置”页面，开启“常规检测”和“Webshell检测”开关。

步骤8 在“网站反爬虫”配置框中，开启网站反爬虫。单击“网站反爬虫设置”，进入网站反爬虫规则配置页面。

步骤9 在“特征反爬虫”页面，根据您的业务场景，开启合适的防护功能。

----结束

当WAF检测到恶意爬虫、扫描器等对网站进行爬取时，将立即拦截并记录该事件，您可以在“防护事件”页面查看爬虫防护日志。

开启网站反爬虫（检查浏览器合法性）

开启网站反爬虫，WAF可以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。

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)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

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

步骤7 根据业务配置JS脚本反爬虫规则，相关参数说明如**表6-4**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”。

- 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”。

表 6-4 JS 脚本反爬虫防护规则参数说明

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** • 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。	-
生效时间	立即生效	立即生效

----结束

配置 CC 攻击防护（限制访问频率）

开启CC攻击防护，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，缓解CC攻击对业务的影响。

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)”。

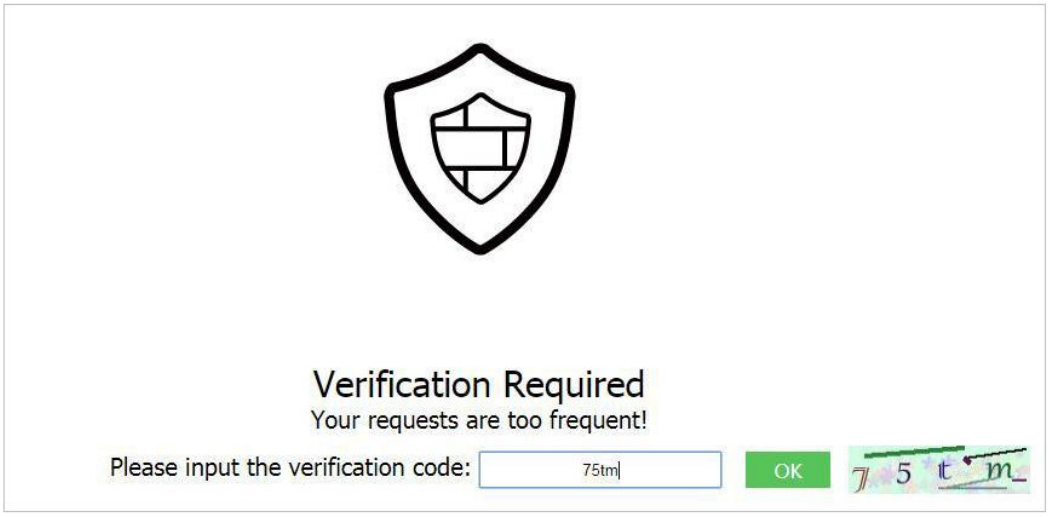
步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面，确认“CC攻击防护”的“状态”为“开启”。

步骤6 在“CC攻击防护”规则配置列表的左上方，单击“添加规则”。以IP限速和人机验证为例，添加IP限速规则，如图6-9所示。

图 6-9 IP 限速

设置成功后，当用户访问超过限制后需要输入验证码才能继续访问。



----结束

6.5 通过配置 ECS/ELB 访问控制策略保护源站安全

网站已接入Web应用防火墙（Web Application Firewall，简称WAF）进行安全防护后，您可以通过设置源站服务器的访问控制策略，只放行WAF回源IP段，防止黑客获取您的源站IP后绕过WAF直接攻击源站。

本章节介绍了源站服务器部署在弹性云服务器（以下简称ECS）时或弹性负载均衡（以下简称ELB）后面时，如何判断源站存在泄漏风险，以及如何配置访问控制策略保护源站安全。

说明

- 网站已接入WAF进行安全防护后，无论您是否配置源站保护，都不影响正常业务的转发。没有配置源站保护可能导致攻击者在源站IP暴露的情况下，绕过WAF直接攻击您的源站。
- 如果在ECS前使用了NAT网关做转发，也需要**设置ECS入方向规则**在ECS的安全组配置只允许放行WAF的回源IP地址段，保护源站安全。

操作须知

- 在配置源站保护前，请确保该ECS或ELB实例上的所有网站域名都已经接入WAF，保证网站能正常访问。
- 配置安全组存在一定风险，避免出现以下问题：
  - 您的网站设置了Bypass回源，但未取消安全组和网络ACL等配置，这种情况下，可能会导致源站无法从公网访问。
  - 当WAF有新增的回源网段时，如果源站已配置安全组防护，可能会导致频繁出现5xx错误。

如何判断源站存在泄露风险

您可以直接使用Telnet工具连接源站公网IP地址的业务端口（或者直接在浏览器中输入访问Web应用的IP），查看是否建立连接成功。

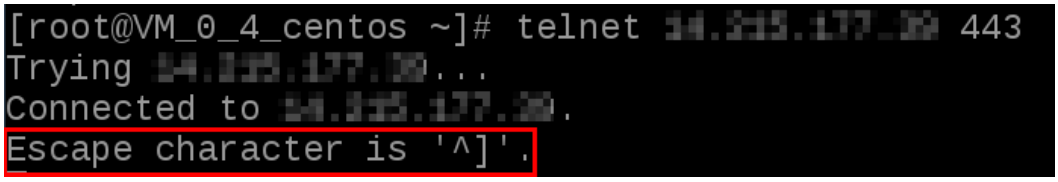
- 如果可以连通

  表示源站存在泄露风险，一旦黑客获取到源站公网IP就可以绕过WAF直接访问。
- 如果无法连通

  表示当前不存在源站泄露风险。

例如，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，显示如**图6-10**所示类似信息，说明端口可连通，表示该源站存在泄露风险。

图 6-10 测试源站泄露风险



获取 WAF 回源 IP 地址

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

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)”。

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

说明

Web应用防火墙的回源IP网段会定期更新，及时将更新后的回源IP网段添加至相应的安全组规则中，避免出现误拦截。

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

----结束

设置 ECS 入方向规则

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，只放行WAF回源IP段。

须知

请确保所有WAF回源IP段都已通过源站ECS的安全组规则设置了入方向的允许策略，否则可能导致网站访问异常。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“计算 > 弹性云服务器 ECS”。

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

步骤5 选择“安全组”页签，单击“更改安全组”。

步骤6 单击安全组ID，进入安全组基本信息页面。

步骤7 选择“入方向规则”页签，单击“添加规则”，进入“添加入方向规则”页面，参数配置说明如表6-5所示。

表 6-5 入方向规则参数配置说明

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

步骤8 单击“确定”，安全组规则添加完成。

成功添加安全组规则后，安全组规则将允许WAF回源IP段的所有入方向流量。

您可以参考**如何判断源站存在泄露风险**，通过测试已接入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。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示源站保护配置成功。

----结束

开启 ELB 访问控制

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

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“网络 > 弹性负载均衡 ELB”。

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

步骤5 选择“监听器”页签，在“访问控制”列单击“设置访问控制”。

步骤6 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6**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6.1**中创建的IP地址组。

步骤7 单击“确定”，白名单访问控制策略添加完成。

您可以参考**如何判断源站存在泄露风险**，通过测试已接入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。如果显示端口无法直接连通，但网站业务仍可正常访问，则表示源站保护配置成功。

----结束

6.6 Web 基础防护功能最佳实践

本文介绍了WAF的Web攻击防护最佳实践，主要从应用场景、防护策略、防护效果三个方面进行介绍。

应用场景

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

防护策略

步骤1 登录管理控制台。

步骤2 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤3 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤4 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面。

步骤5 在“Web基础防护”配置框中，查看Web应用攻击防护的防护状态。

Web基础防护功能默认为开启状态，并使用“仅记录”模式的防护规则策略。

- 状态
  -  ：表示WAF的Web基础防护的防护模块已开启。
  -  ：表示该防护模块处理关闭状态。
- 模式：分为拦截和仅记录两种模式。
  - “拦截”模式表示当遭受Web攻击时，WAF立即拦截攻击请求，并在后台记录攻击日志。
  - “仅记录”模式表示当遭受Web攻击时，WAF不会拦截攻击请求，仅在后台记录攻击日志。

步骤6 单击“高级设置”，进入“Web基础防护”界面。

- “防护等级”：分为宽松、中等、严格三种模式，默认为“中等”防护模式。

  表 6-6 防护等级说明

防护等级	说明
宽松	防护粒度较粗，只拦截攻击特征比较明显的请求。 当误报情况较多的场景下，建议选择“宽松”模式。
中等	默认为“中等”防护模式，满足大多数场景下的Web防护需求。
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。 当需要更严格地防护SQL注入、跨站脚本、命令注入等攻击行为时，建议使用“严格”模式。

- 灵活设置防护检测类型。

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

----结束

使用建议

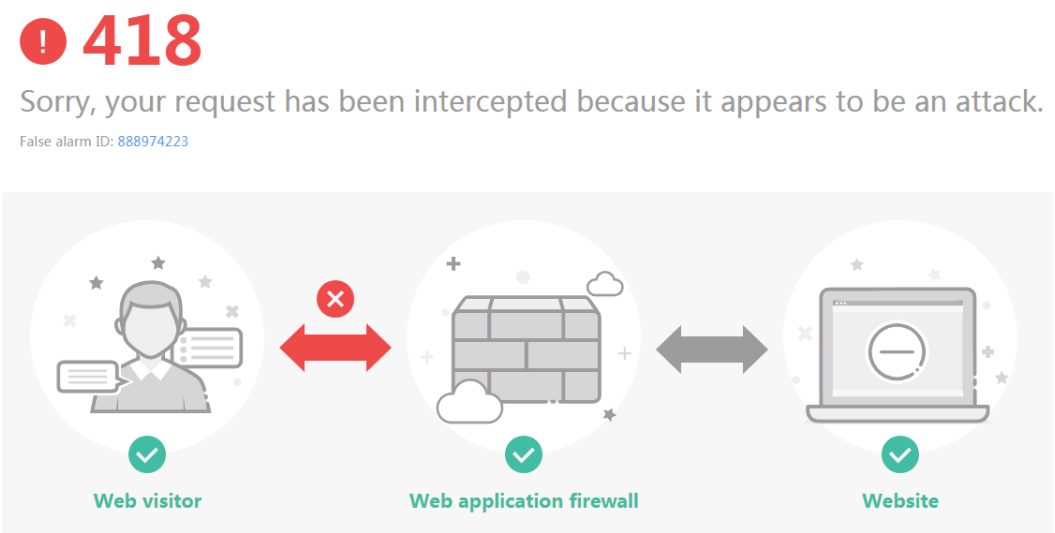
- 如果您对自己的业务流量特征还不完全清楚，建议先切换到“仅记录”模式进行观察。一般情况下，建议您观察一至两周，然后分析仅记录模式下的攻击日志。
  - 如果没有发现任何正常业务流量被拦截的记录，则可以切换到“拦截”模式启用拦截防护。
  - 如果发现攻击日志中存在正常业务流量，建议调整防护等级或者设置全局白名单来避免正常业务的误拦截。
- 业务操作方面应注意以下问题：

- 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

开启Web基础防护功能后，在浏览器中输入模拟SQL注入攻击的测试域名，WAF将拦截了此条攻击。您可以在“安全总览”页面，查看攻击的拦截日志。

图 6-11 SQL 攻击拦截



在“防护事件”页面，您可查看“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。

6.7 通过误报处理提升 Web 基础防护效果

当您的网站接入Web应用防火墙（Web Application Firewall，简称WAF）并开启Web基础防护后，WAF会根据您设置的Web基础防护规则检测并拦截命中规则的请求。如果业务正常请求命中Web基础防护规则被WAF误拦截，可能导致正常请求访问网站显示异常，此时，您可以通过误报处理使WAF不再拦截该请求，提升Web基础防护效果。

前提条件

“防护事件”页面可以查看误拦截事件。

约束条件

同一个事件不能重复进行误报处理，即如果该事件已进行了误报处理，则不能再对该事件进行误报处理。

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。

系统影响

- 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。
- 拦截事件处理为误报后，该误报事件对应的规则将添加到全局白名单（原误报屏蔽）规则列表中，您可以在“防护策略”界面的“全局白名单（原误报屏蔽）”页面查看、关闭、删除或修改该规则。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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 在防护事件列表中，根据防护网站、事件类型、源IP、URL等信息筛选误拦截事件。

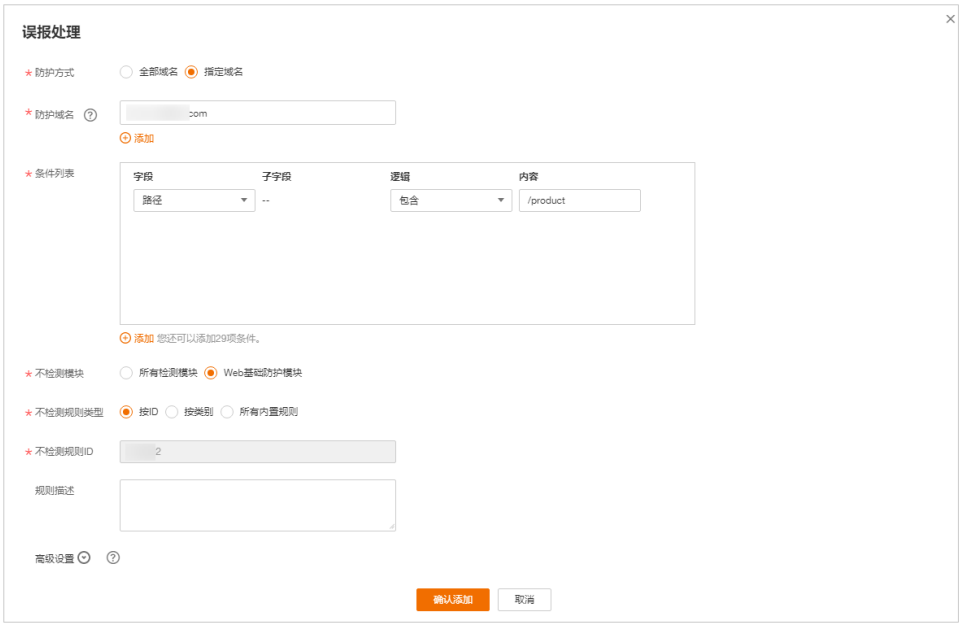
步骤6 在误拦截事件所在行的“操作”列中，单击“详情”，查看事件详细信息，确认为误拦截事件。

图 6-12 查看拦截事件详细信息

步骤7 在误拦截事件所在行的“操作”列中，单击“更多 > 误报处理”。

步骤8 在弹出的对话框中，添加误报处理策略，详细的操作请参见**处理误报事件**。

图 6-13 添加全局白名单规则



----结束

生效条件

设置误报处理后，1分钟左右生效，防护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，重新访问设置了误报处理的页面，如果访问正常，说明配置成功。

Web 基础防护检测项说明

Web基础防护覆盖OWASP（Open Web Application Security Project）常见安全威胁，内置语义分析+正则双引擎，可以对恶意扫描器、IP、网马等威胁进行检测并拦截。请根据业务使用场景开启相应的检测项，详细的检测项说明如表6-7所示。

表 6-7 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。

检测项	说明
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。

Web 基础防护等级

Web基础防护支持三种防护等级：“宽松”、“中等”、“严格”，默认防护等级为“中等”。宽松的防护等级可能降低误报率，但可能导致漏报率增高；严格的防护等级可能增高误报率，但可以降低漏报率。防护等级的详细说明如表6-8所示。

表 6-8 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。 当需要更严格地防护SQL注入、跨站脚本、命令注入等攻击行为时，建议使用“严格”模式。

6.8 使用 Postman 工具模拟业务验证全局白名单（原误报屏蔽）规则

当防护网站成功接入WAF后，您可以使用接口测试工具模拟用户发起各类HTTP(S)请求，以验证配置的WAF防护规则是否生效，即验证配置防护规则的防护效果。本实践以Postman工具为例，说明如何验证全局白名单（原误报屏蔽）规则。

应用示例

例如，您的业务部署在“/product”路径下，由于生态开发，针对参数ID存在用户提交脚本或富文本的业务场景，为了确保业务正常运行，您需要对用户提交的内容进行误报屏蔽，以屏蔽误拦截的访问请求，提升WAF防护效果。

前提条件

- 防护网站已成功接入WAF。
- 已开启“Web基础防护”，且防护模式为“拦截”。同时，“常规检测”已开启。

操作步骤

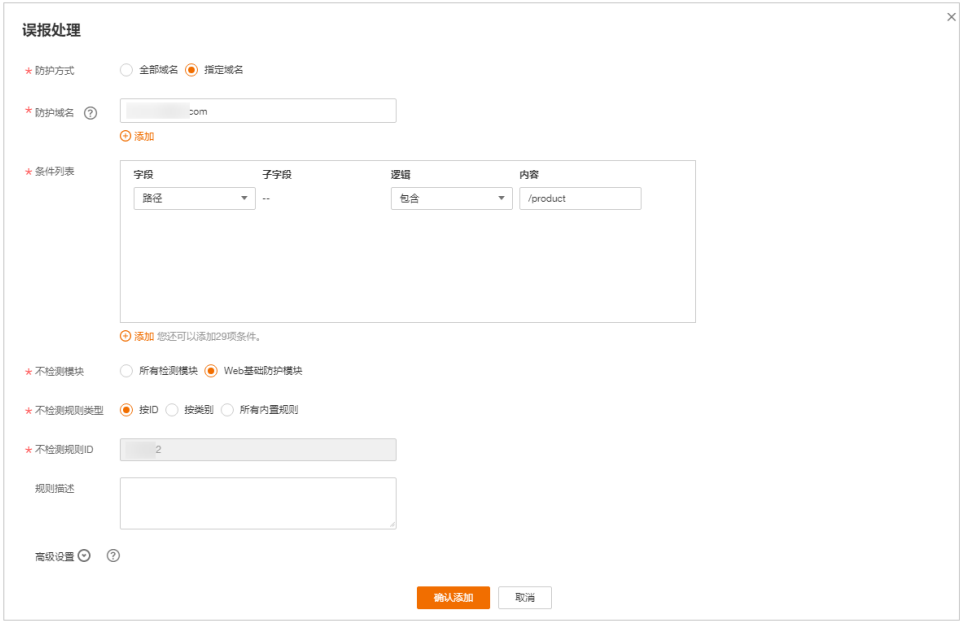
步骤1 下载并安装Postman。

步骤2 在Postman上设置请求路径为“/product”，参数ID为普通测试脚本，防护网站的访问请求被拦截。

步骤3 处理误报事件。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。
3. 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。
4. 在左侧导航树中，选择“防护事件”，进入“防护事件”页面。
5. 在防护事件页面，WAF拦截的防护事件命中了“XSS攻击”的“010000”规则。
6. 在该防护事件所在行的“操作”列中，单击“更多 > 误报处理”。
7. 在弹出的“误报处理”对话框中，添加如图6-14所示全局白名单规则。

图 6-14 添加全局白名单规则

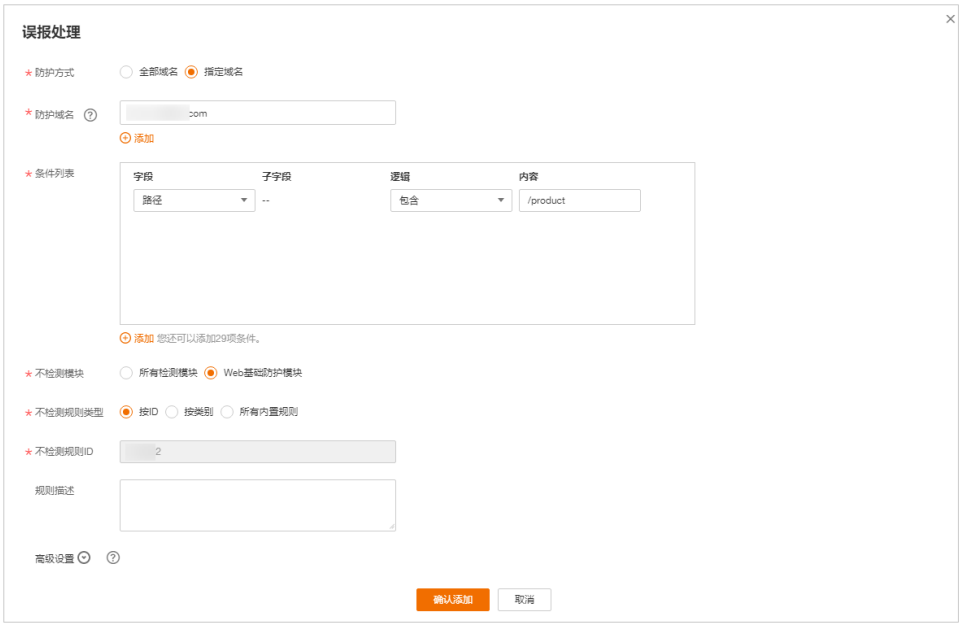


8. 单击“确认添加”。
   防护规则生效需要5分钟左右。

步骤4 在Postman上再次设置请求路径为“/product”，参数ID为普通测试脚本，防护网站的访问请求还是被拦截。

步骤5 参照步骤3，查看防护事件，处理命中“XSS攻击”的“110053”规则的误报防护事件。

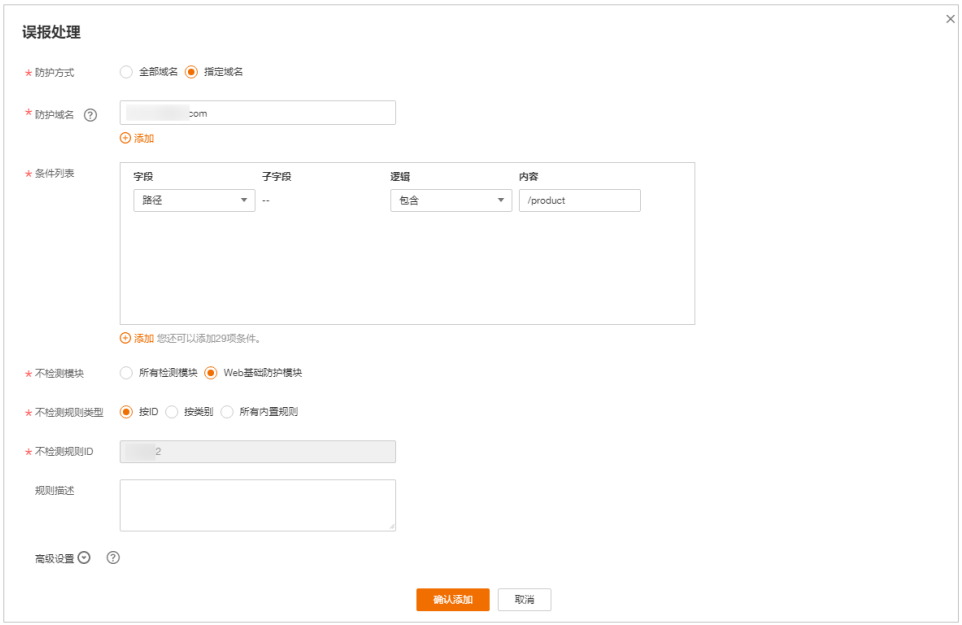
图 6-15 添加全局白名单规则



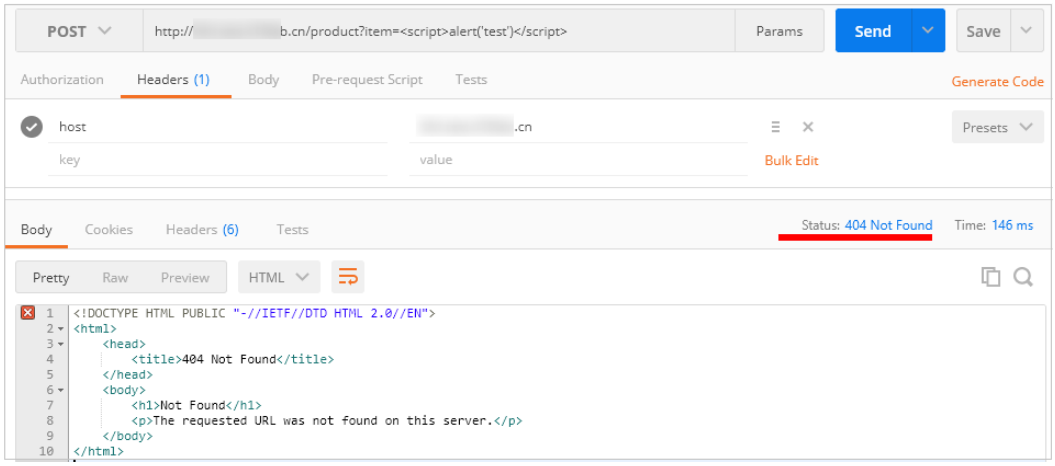
步骤6 在Postman上第三次设置请求路径为“/product”，参数ID为普通测试脚本，防护网站的访问请求仍被拦截。

步骤7 参照**步骤3**，查看防护事件，处理命中“XSS攻击”的“110060”规则的误报防护事件。

图 6-16 添加全局白名单规则



步骤8 在Postman上第四次设置请求路径为“/product”，参数ID为普通测试脚本。此时，防护网站的访问请求不再被拦截，说明所有全局白名单规则都已生效。



同时，查看“防护事件”页面，防护事件列表也没有新增的XSS攻击防护事件。

步骤9 在Postman上模拟攻击，验证设置的全局白名单（原误报屏蔽）规则不会影响WAF拦截其他参数的XSS攻击事件。

1. 在Postman上设置请求路径为“/product”，参数item为普通测试脚本，防护网站的访问请求被拦截。
2. 查看“防护事件”页面，WAF拦截参数item的XSS攻击事件。

步骤10 在Postman上模拟攻击，验证设置的全局白名单（原误报屏蔽）规则不会影响WAF拦截其他路径的XSS攻击事件。

1. 在Postman上设置请求路径为“/order”，参数ID为普通测试脚本，防护网站的访问请求被拦截。
2. 查看“防护事件”页面，WAF拦截“URL”为“/order”、参数ID的XSS攻击事件。

----结束

6.9 WAF 云模式接入配置

6.9.1 准备阶段

将网站域名接入Web应用防火墙（Web Application Firewall，WAF），能够帮助您的网站防御常见的Web攻击和恶意CC攻击流量，避免网站遭到入侵导致数据泄露，全面保障您网站的安全性和可用性。

网站业务梳理

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

表 6-9 网站业务梳理

梳理项	说明
网站和业务信息	

梳理项	说明
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	判断风险时间点，并且可作为WAF实例的业务带宽和业务QPS规格的选择依据。 **说明** 如果您选择的QPS规格不足以支撑网站/应用业务每天的流量峰值，对超出当前WAF版本支持峰值的QPS，WAF将不再防护网站，QPS将直接透传到源站，影响网站/应用业务的防护。
业务的主要用户群体（例如，访问用户的主要来源地区）	判断非法攻击来源，后续可使用地理位置访问控制功能屏蔽非法来源地区。
业务是否为C/S架构	如果是C/S架构，进一步明确是否有App客户端、Windows客户端、Linux客户端、代码回调或其他环境的客户端。
源站部署的具体位置	判断购买哪种实例region。
源站服务器的操作系统（Linux、Windows）和所使用的Web服务中间件（Apache、Nginx、IIS等）	判断源站是否存在访问控制策略，避免源站误拦截WAF回源IP转发的流量。
域名使用协议	判断所使用的通信协议WAF是否支持。 **说明** 网站的“对外协议”、“源站协议” 必须要根据防护网站的实际情况配置正确，WAF才会正常防护您的网站。 • 对外协议，即客户端（例如浏览器）请求访问网站的协议类型。可选择“HTTP”、“HTTPS”两种协议类型。 • 源站协议，即WAF转发客户端（例如浏览器）请求的协议类型。可选择“HTTP”、“HTTPS”两种协议类型。
业务端口	判断需要防护的业务端口是否在WAF支持的端口范围内。 • 标准端口 – 80：HTTP对外协议默认使用端口 – 443：HTTPS对外协议默认使用端口 • 非标准端口 80/443以外的端口
业务是否使用TLS 1.0或弱加密套件	判断业务使用的加密套件是否支持。
业务在接入WAF前，是否已接入DDoS高防、CDN等服务。	接入WAF时，判断如何选择“是否已使用代理”，以及正确进行域名解析。
（针对HTTPS业务）客户端是否支持SNI标准	对于支持HTTPS协议的域名，接入WAF后，客户端和服务端都需要支持SNI标准。
业务交互过程	了解业务交互过程、业务处理逻辑，便于后续配置针对性防护策略。

梳理项	说明
活跃用户数量	便于后续在处理紧急攻击事件时，判断事件严重程度，以采取风险较低的应急处理措施。
业务及攻击情况	
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻击防护过程中分析攻击特征。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
用户群体属性	例如，个人用户、网吧用户、或通过代理访问的用户。
业务是否遭受过大流量攻击、攻击类型和最大的攻击流量峰值	判断是否需要增加DDoS防护服务，并根据攻击流量峰值判断需要的DDoS防护规格。
业务是否遭受过CC攻击和最大的CC攻击峰值QPS	通过分析历史攻击特征，配置预防性策略。
业务是否已完成压力测试	评估源站服务器的请求处理性能，帮助后续判断是否因遭受攻击导致业务发生异常。

准备工作

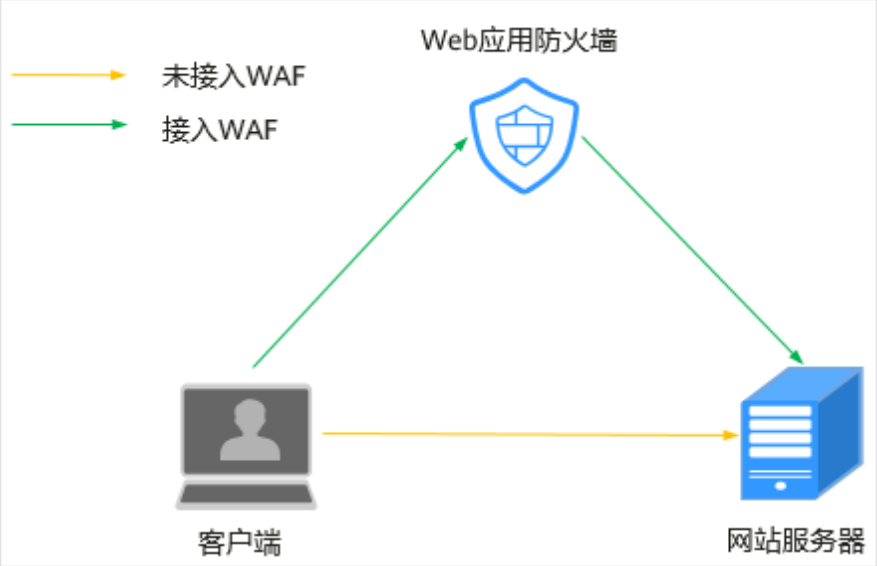
- 已将域名信息（源站服务器的IP、端口等信息）以“云模式”的方式添加到WAF。
- 具有网站DNS域名解析管理员的账号，用于修改DNS解析记录将网站流量切换至WAF。
- 推荐在将网站业务接入前，完成压力测试。
- 检查网站业务是否已有信任的访问客户端（例如监控系统、通过内部固定IP或IP段调用的API接口、固定的程序客户端请求等）。在将业务接入后，需要将这些信任的客户端IP加入白名单。

6.9.2 单独使用 WAF 配置指导

当网站没有接入到WAF前，DNS直接解析到源站的IP。网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。本文介绍通过DNS配置模式接入WAF时，如何在已添加网站配置后，配置域名解析，实现业务接入。

原理图

图 6-17 未使用代理配置原理图



前提条件

- 已有网站域名。
- 在域名的DNS服务商处有更新DNS记录的权限。
- （可选）放行WAF回源段IP。源站服务器上已启用安全软件（如安全狗、云锁）时，您需要在这些软件上设置放行WAF回源段IP，防止由WAF转发到源站的正常业务流量被拦截。具体请参考**通过配置ECS/ELB访问控制策略保护源站安全**。
- （可选）进行本地验证。通过本地验证确保WAF转发规则配置正常后，再修改网站域名的DNS解析记录，防止因配置错误导致业务中断。具体请参考**本地验证**。

操作背景

- 如果您之前在DNS云解析服务上添加的域名主机记录的“类型”是“CNAME-将域名指向另外一个域名”，可参照**CNAME接入**完成配置。

CNAME 接入

如果您之前在DNS云解析服务上添加的域名主机记录的“类型”是“CNAME-将域名指向另外一个域名”，请参照以下操作步骤接入WAF。

以下为当前主流的域名服务商的CNAME绑定方法，仅供参考。如与实际配置不符，请以各自域名服务商的信息为准。

步骤1 获取CNAME值。

1. 单击管理控制台左上角的，选择区域或项目。
2. 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。
3. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

4. 在目标网站所在行的“域名”列中，单击目标网站，进入网站基本信息页面。
5. 在“CNAME”行中，单击，复制“CNAME”值。

步骤2 域名解析。

1. 登录域名服务提供商的管理控制台。
2. 进入域名解析记录页。
3. 在弹出的“修改记录集”对话框中修改记录值。
   - “主机记录”：在WAF中配置的域名。
   - “类型”：选择“CNAME-将域名指向另外一个域名”。
   - “线路类型”：全网默认。
   - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
   - “值”：修改为已复制的WAF CNAME地址。
   - 其他的设置保持不变。

说明

关于修改解析记录：

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

步骤3 （可选）验证DNS配置。您可以Ping网站域名验证DNS解析是否生效。

说明

由于DNS解析记录生效需要一定时间，如果验证失败，您可以等待5分钟后重新检查。

----结束

6.10 独享引擎实例升级配置

当您的防护网站以独享模式部署到WAF后，您可以在WAF管理控制台上通过升级操作，将WAF独享引擎实例升级到最新版本，以获取独享引擎实例最新防护性能。为了提升业务的高可靠性，请您参照以下操作指导完成独享引擎实例升级操作。

须知

对于可靠性要求较高的业务，建议您至少申请2个独享引擎实例部署为双活或多活高可靠架构。如果业务部署单引擎实例，当实例对应的ECS发生故障时，WAF将不可用。

前提条件

防护网站以“独享模式”接入WAF。

单独享引擎实例节点升级

如果您的业务只部署了一个独享引擎实例，请参照以下操作升级实例。

步骤1 建议参见**申请WAF独享引擎实例**申请一个新的独享引擎实例。

- 新申请的独享引擎实例为最新版本。当实例为最新版本时，“升级”按钮为灰化状态。
- 确保新申请的实例，虚拟私有云，子网，安全组等配置，与原实例一致。在这些参数都一致的情况下，新实例会自动同步原实例的所有WAF防护配置。

步骤2 在原独享引擎实例所属VPC下的任一台ECS上，执行curl命令，验证业务是否正常。

- HTTP业务

  curl http://*WAF独享引擎实例IP.业务端口* -H "host：*业务域名*" -H "User-Agent: Test"

- HTTPS业务

  curl https://*WAF独享引擎实例IP.业务端口* -H "host：业务域名" -H "User-Agent: Test"

检查业务是否正常，如果业务正常，请执行**步骤3**；如果业务异常，请参照**域名/IP接入状态显示“未接入”，如何处理?** 和**如何排查500/502/504错误?** 排查故障后，再执行**步骤3**。

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。

步骤3 将新购买的独享引擎实例添加到ELB的后端服务器上。

以添加共享型后端服务器为例说明，添加后端服务器操作步骤如下。

1. 单击页面左上方的 ☰，选择“安全 > Web应用防火墙 (独享)”。
2. 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。
3. 在目标实例所在行的“操作”列，单击“更多 > 添加到ELB”。
4. 在“添加到ELB”页面中，选择原独享引擎实例配置的“ELB（负载均衡器）”、“ELB监听器”和“后端服务器组”。
5. 单击“确认”，为WAF实例配置业务端口，“业务端口”需要配置为原WAF独享引擎实例实际监听的业务端口。

步骤4 在ELB管理控制台上，将原独享引擎实例的流量权重设置为“0”。

新的请求不会转发到权重为0的后端。

步骤5 待业务流量降下来后，删除原独享引擎实例。

查看独享实例的云监控信息，“新建连接数”较小时（例如，小于5），说明业务流量已经降下来。

1. 在WAF控制台的左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。
2. 在目标实例所在行的“操作”列，单击“更多 > 删除”。

3. 在弹出的提示框中，单击“确认”。

   删除实例后，该实例上的资源将被释放且不可恢复。

----结束

多独享引擎实例节点升级

如果您的业务部署了多个独享引擎实例，请参照以下操作升级实例。

步骤1 在ELB管理控制台上，记录任一独享引擎实例的流量权重后，将该实例的流量权重设置为“0”。

新的请求不会转发到权重为0的后端。

步骤2 待业务流量降下来后，升级独享引擎实例版本。

查看独享实例的云监控信息，“新建连接数”较小时（例如，小于5），说明业务流量已经降下来。

1. 在WAF控制台的左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。
2. 在目标实例所在行的“操作”列，单击“升级”。
3. 在弹出的对话框中，确认并勾选业务已满足提示框中所描述的相关配置后，单击“确认”，升级实例版本。

   升级大约需要5分钟。

步骤3 在独享引擎实例所属VPC下的任一台ECS上，执行curl命令，验证业务是否正常。

- HTTP业务

  curl http://*WAF独享引擎实例IP.业务端口* -H "host：*业务域名*" -H "User-Agent: Test"

- HTTPS业务

  curl https://*WAF独享引擎实例IP.业务端口* -H "host：业务域名" -H "User-Agent: Test"

检查业务是否正常，如果业务正常，请执行**步骤4**；如果业务异常，请参照**域名/IP接入状态显示“未接入”，如何处理？**和**如何排查500/502/504错误？**排查故障后，再执行**步骤4**。

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。

步骤4 在ELB管理控制台上，将引擎实例的流量权重从0调整为**步骤1**中记录的原值。

步骤5 参照**步骤1**~**步骤4**，分别对其他独享引擎实例节点执行升级操作。

----结束

6.11 获取客户端真实 IP

客户端IP指的是访问者（用户设备）的IP地址。在Web应用开发中，通常需要获取客户端真实的IP地址。例如，投票系统为了防止刷票，需要通过获取客户端真实IP地址，限制每个客户端IP地址只能投票一次。

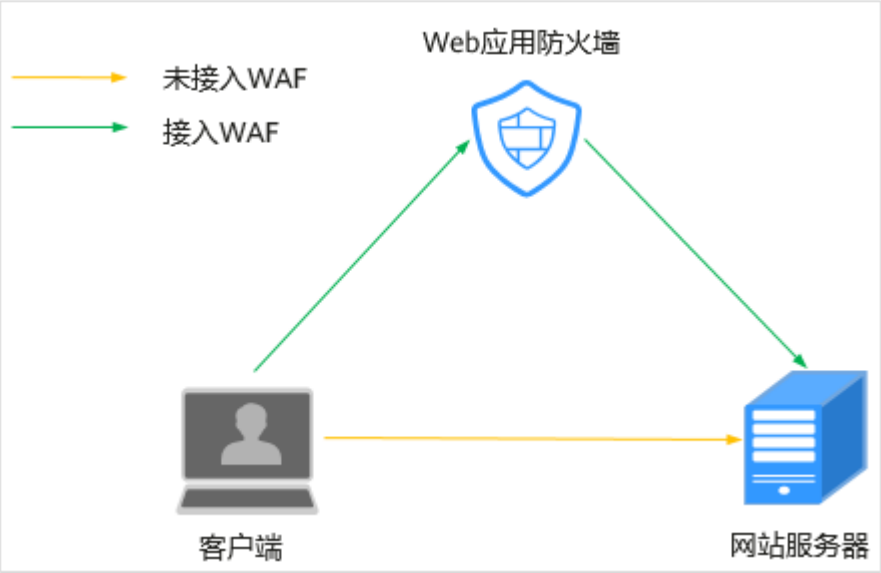
当您的网站已接入Web应用防火墙（Web Application Firewall，简称WAF）进行安全防护后，WAF作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。此时，您可直接通过WAF获取客户端的真实IP，也可以通过配置网站服务器获取客户端的真实IP。

本章节介绍了通过WAF直接获取真实IP的方法，以及不同类型的Web应用服务器（包括Tomcat、Apache、Nginx、IIS 6和IIS 7）如何进行相关设置，以获取客户端的真实IP。

背景信息

通常情况下，网站访问并不是简单地从用户的浏览器直达服务器，中间可能部署有CDN、WAF、高防等代理服务器（架构为“用户 > CDN/WAF/高防等代理服务 > 源站服务器”）。以WAF为例，部署示意图如图6-18所示。

图 6-18 部署 WAF 原理图



说明

- 当网站没有接入到WAF前，DNS直接解析到源站的IP，用户直接访问服务器。
- 当网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

在这种情况下，访问请求到达源站服务器之前可能经过了多层安全代理转发或加速代理转发，服务器如何获取发起请求的真实客户端IP呢?

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

Forwarded-For：客户端的真实IP，代理服务器1-IP， 代理服务器2-IP，代理服务器3-IP，……”。

因此，您可以通过获取“X-Forwarded-For”对应的第一个IP来得到客户端的真实IP。

约束条件

- 添加域名时“是否已使用代理”配置错误将导致无法成功获取Web访问者请求的真实IP地址。

  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前使用了CDN、云加速等七层代理的产品，“是否已使用代理”务必选择“是”，其他情况，“是否已使用代理”选择“否”。
- 常规情况下，X-Forwarded-For字段中，第一个IP就是客户端真实IP，当IPV6地址长度超过X-Forwarded-For字段长度限制时，将读取不到IP地址；另外，nat64下，ELB是IPv4的监听器，也读不到ipv6地址。

通过 WAF 直接获取客户端真实 IP

网站接入WAF后，WAF作为一个反向代理部署于客户端和服务器之间，实现网站安全防护。

下面为您介绍如何通过X-Forwarded-For和X-Real-IP变量获取客户端真实IP地址的方法：

- WAF使用X-Forwarded-For的方式获取客户端的真实IP地址。

  WAF将“真实的客户端IP”放在HTTP头部的“X-Forwarded-For”字段，格式如下：

  ```
  X-Forwarded-For: 用户真实IP, 代理服务器1-IP， 代理服务器2-IP，...
  ```

  说明

  当使用此方式获取客户端真实IP时，获取的第一个地址就是客户端真实IP。

  各种语言通过调用SDK接口获取X-Forwarded-For字段的方式：

  - **ASP：**
    ```
    Request.ServerVariables("HTTP_X_FORWARDED_FOR")
    ```
  - **ASP.NET(C#)：**
    ```
    Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
    ```
  - **PHP：**
    ```
    $_SERVER["HTTP_X_FORWARDED_FOR"]
    ```
  - **JSP:**
    ```
    request.getHeader("HTTP_X_FORWARDED_FOR")
    ```
- WAF服务还支持使用X-Real-IP变量，获取客户的来源IP（使用过程中考虑了后面经过的多层反向代理对该变量的修改）。

  各种语言通过调用SDK接口获取X-Real-IP字段的方式：

  - **ASP：**
    ```
    Request.ServerVariables("HTTP_X_REAL_IP")
    ```
  - **ASP.NET(C#)：**
    ```
    Request.ServerVariables["HTTP_X_REAL_IP"]
    ```
  - **PHP：**
    ```
    $_SERVER["HTTP_X_REAL_IP"]
    ```
  - **JSP:**
    ```
    request.getHeader("HTTP_X_REAL_IP")
    ```


Tomcat 如何在访问日志中获取客户端真实 IP

如果您的源站部署了Tomcat服务器，可通过启用Tomcat的X-Forwarded-For功能，获取客户端的真实IP地址。

步骤1 打开“server.xml”文件（“tomcat/conf/server.xml”），AccessLogValue日志记录功能部分内容如下：

```
<Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
      <Valve className="org.apache.catalina.values.AccessLogValue" directory="logs"
            prefix="localhost_access_log." suffix=".txt"
            pattern="%h %l %u %t "%r" %s %b" />
```

步骤2 在pattern中增加“%{X-Forwarded-For}i”，修改后的server.xml为：

```
<Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
      <Valve className="org.apache.catalina.valves.AccessLogValue" directory="logs"
            prefix="localhost_access_log." suffix=".txt"
            pattern="%{X-Forwarded-For}i %h %l %u %t "%r" %s %b" />
</Host>
```

步骤3 查看“localhost_access_log”日志文件，可获取**X-Forwarded-For**对应的访问者真实IP。

----结束

Apache 如何在访问日志中获取客户端真实 IP

如果源站部署的Apache服务器为2.4及以上版本，您可以使用Apache安装包中自带“remoteip_module”模块文件“mod_remoteip.so”，获取客户端IP地址。

- CentOS 7.6
  a. 编辑“httpd.conf”配置文件，在文件中添加以下内容：

     ```
     LoadModule remoteip_module modules/mod_remoteip.so  ##加载mod_remoteip.so模块
     RemoteIPHeader X-Forwarded-For   ##设置RemoteIPHeader头部
     RemoteIPInternalProxy WAF的回源IP段  ##设置WAF回源IP段
     ```

     说明

     - “mod_remoteip.so”模块已默认加载在以下文件：“/etc/httpd/conf.modules.d/00-base.conf:46”
     - 多个回源IP段请使用空格分隔。

  b. 修改配置文件日志格式，即将日志格式文件中的“%h”修改为“%a”。

     ```
     LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
     LogFormat "%a %l %u %t \"%r\" %>s %b" common
     ```

  c. 重启Apache服务，使配置生效。
- Ubuntu 20.04.2
  a. 编辑“apache2.conf”配置文件，在文件中添加以下内容：

     ```
     ln -s ../mods-available/remoteip.load /etc/apache2/mods-enabled/remoteip.load  ##加载mod_remoteip.so模块
     RemoteIPHeader X-Forwarded-For   ##设置RemoteIPHeader头部
     RemoteIPInternalProxy WAF的回源IP段  ##设置WAF回源IP段
     ```

     说明

     - 您也可以添加以下内容加载mod_remoteip.so模块：

       LoadModule remoteip_module /usr/lib/apache2/modules/mod_remoteip.so
     - 多个回源IP段请使用空格分隔。

b. 修改配置文件日志格式，即将日志格式文件中的“%h”修改为“%a”。

```
LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%a %l %u %t \"%r\" %>s %b" common
```

c. 重启Apache服务，使配置生效。

如果源站部署的Apache服务器为2.2及以下版本，您可通过运行命令安装Apache的第三方模块mod_rpaf，并修改“http.conf”文件获取客户IP地址。

步骤1 执行以下命令安装Apache的一个第三方模块mod_rpaf。

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar xvfz mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/local/apache/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

步骤2 打开“httpd.conf”配置文件，并将文件内容修改为如下内容：

```
LoadModule rpaf_module   modules/mod_rpaf-2.0.so ##加载mod_rpaf模块
<IfModule mod_rpaf.c>
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 127.0.0.1 <反向代理IPs>
RPAFheader X-Forwarded-For
</IfModule>
```

步骤3 定义日志格式。

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" common
```

步骤4 启用自定义格式日志。

```
CustomLog "/[apache目录]/logs/$access.log" common
```

步骤5 重启Apache，使配置生效。

```
/[apached目录]/httpd/bin/apachectl restart
```

步骤6 查看“access.log”日志文件，可获取**X-Forwarded-For**对应的客户端真实IP。

----结束

Nginx 如何在访问日志中获取客户端真实 IP

如果您的源站部署了Nginx反向代理，可通过在Nginx反向代理配置Location信息，后端Web服务器即可通过类似函数获取客户的真实IP地址。

步骤1 根据源站Nginx反向代理的配置，在Nginx反向代理的相应location位置配置如下内容，获取客户IP的信息。

```
Location ^ /<uri> {
    proxy_pass  ....;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

步骤2 后端Web服务器通过定义Nginx日志参数**$http_x_forwarded_for**来获取客户的真实IP。

示例：

```
log_format main ' "<$http_Cdn_Src_IP>" "{$http_x_real_ip}" "[$http_x_forwarded_for]" "$remote_addr"
' '$http_user_agent - $remote_user [$time_local] "$request" '    ' $status $body_bytes_sent "$http_referer" ';
```

----结束

IIS 6 如何在访问日志中获取客户端真实 IP

如果您的源站部署了IIS 6服务器，您可以通过安装“F5XForwardedFor.dll”插件，从IIS 6服务器记录的访问日志中获取客户端真实的IP地址。

步骤1 下载F5XForwardedFor模块。

步骤2 根据您服务器的操作系统版本将“x86\Release”或者“x64\Release”目录中的“F5XForwardedFor.dll”文件拷贝至指定目录（例如，“C:\ISAPIFilters”），同时确保IIS进程对该目录有读取权限。

步骤3 打开IIS管理器，找到当前开启的网站，在该网站上右键选择“属性”，打开“属性”页面。

步骤4 在“属性”页面，切换至“ISAPI筛选器”，单击“添加”，在弹出的窗口中，配置如下信息：

- “筛选器名称”：“F5XForwardedFor”；
- “可执行文件”：“F5XForwardedFor.dll”的完整路径，例如：“C:\ISAPIFilters\F5XForwardedFor.dll”。

步骤5 单击“确定”，重启IIS 6服务器。

步骤6 查看IIS 6服务器记录的访问日志（默认的日志路径为：“C:\WINDOWS\system32\LogFiles\ ”，IIS日志的文件名称以“.log”为后缀），可获取**X-Forwarded-For**对应的客户端真实IP。

----结束

IIS 7 如何在访问日志中获取客户端真实 IP

如果您的源站部署了IIS 7服务器，您可以通过安装“F5XForwardedFor”模块，从IIS 7服务器记录的访问日志中获取客户端真实的IP地址。

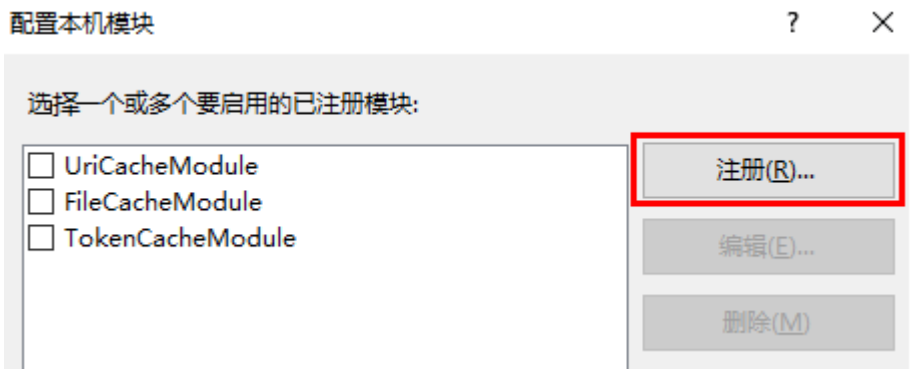
步骤1 下载F5XForwardedFor模块。

步骤2 根据服务器的操作系统版本将“x86\Release”或者“x64\Release”目录中的“F5XFFHttpModule.dll”和“F5XFFHttpModule.ini”文件拷贝到指定目录（例如，“C:\x_forwarded_for\x86”或“C:\x_forwarded_for\x64”），并确保IIS进程对该目录有读取权限。

步骤3 在IIS服务器的选择项中，双击“模块”，进入“模块”界面。

步骤4 单击“配置本机模块”，在弹出的对话框中，单击“注册”。

图 6-19 注册模块



步骤5 在弹出的对话框中，按操作系统注册已下载的DLL文件后，单击“确定”。

- x86操作系统：注册模块“x_forwarded_for_x86”

  - 名称：x_forwarded_for_x86
  - 路径：“C:\x_forwarded_for\x86\F5XFFHttpModule.dll”
- x64操作系统：注册模块“x_forwarded_for_x64”
  - 名称：x_forwarded_for_x64
  - 路径：“C:\x_forwarded_for\x64\F5XFFHttpModule.dll”

步骤6 注册完成后，勾选新注册的模块（“x_forwarded_for_x86”或“x_forwarded_for_x64”）并单击“确定”。

步骤7 在“ISAPI和CGI限制”中，按操作系统添加已注册的DLL文件，并将其“限制”改为“允许”。

- x86操作系统：
  - ISAPI或CGI路径：“C:\x_forwarded_for\x86\F5XFFHttpModule.dll”
  - 描述：x86
- x64操作系统：
  - ISAPI或CGI路径：“C:\x_forwarded_for\x64\F5XFFHttpModule.dll”
  - 描述：x64

步骤8 重启IIS 7服务器，等待配置生效。

步骤9 查看IIS 7服务器记录的访问日志（默认的日志路径为：“C:\WINDOWS\system32\LogFiles\”，IIS日志的文件名称以“.log”为后缀），可获取**X-Forwarded-For**对应的客户端真实IP。

----结束

6.12 通过 LTS 快速查询分析 WAF 访问日志

开启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。

本实践以日志组“lts-waf”的访问日志流“lts-waf-access”为例，说明如何通过LTS快速查询分析日志。

前提条件

- 防护网站已成功接入WAF。
- WAF已**开启全量日志**。

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“管理与监管 > 云日志服务”，进入“日志管理”页面。

步骤4 在“日志组名称”列，单击访问日志流所在的日志组名称（例如，“lts-waf”），进入日志流页面。

步骤5 在“日志流名称”列，单击访问日志流名称（例如，“lts-waf-access”），进入“日志流”页面。

步骤6 在日志流详情页面，单击右上角 ，在弹出页面中，选择“云端结构化解析”页签，进入日志结构化配置页面。

步骤7 选择“JSON”日志结构化方式，如图6-20所示。

图 6-20 选择 JSON 格式

步骤8 在“步骤1 选择示例”日志区域，单击“从已有日志中选择”，在弹出“选择已有日志”对话框中任选一条日志后，单击“确定”。

步骤9 在“步骤2 字段提取”区域，单击“智能提取”，开启需要快速分析的字段（例如，“remote_ip”）。

“remote_ip”：访问请求的客户端IP地址。

步骤10 单击“保存”，LTS将对周期内的日志进行快速分析、统计。

步骤11 在左侧导航树中，选择“可视化”，在页面右侧选择日志查询时间段，在搜索框中输入SQL语句后单击“执行查询”，查询指定日志。

您可以在搜索框中输入如下SQL语句，查询指定IP的日志：

select * where remote_ip = 'xx.xx.xx.xx' 或者select * where remote_ip like 'xx.xx.xx%'

----结束

6.13 通过 LTS 实时分析 Spring core RCE 漏洞的拦截情况

开启WAF全量日志功能后，您可以将攻击日志（attack）记录到云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的WAF攻击日志数据，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。

本实践通过将WAF的攻击日志开启LTS快速分析，再通过Spirng规则ID快速查询并分析被拦截的Spring core RCE漏洞的日志。

前提条件

- 防护网站已成功接入WAF。
- WAF已开启全量日志，将WAF的攻击日志流对接到LTS。
- 已获取Spirng规则ID。

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“管理与监督 > 云日志服务”，进入“日志管理”页面。

步骤4 在日志组列表中，展开waf日志组，选择日志流“attack”。

步骤5 在日志流详情页面，单击右上角，在弹出页面中，选择“云端结构化解析”页签，进入日志结构化配置页面。

步骤6 选择“JSON”日志结构化方式，单击“从已有日志中选择”，在右侧弹框中任意选择一条日志。

步骤7 单击“智能提取”，筛选出需要“快速分析”的字段，打开这些字段在“快速分析”列的开关，打开后，可以对周期类日志进行统计分析。

步骤8 找到“category”字段，单击该字段“别名”列的，修改该字段名称并单击保存设置。

说明

该字段名称与系统内置字段 category 重复了，需要修改后才能保存成功。

步骤9 在列表右下方，单击“保存”，LTS将对周期内的日志进行快速分析、统计。

步骤10 在左侧导航树中，选择“可视化”，输入以下命令，并单击“执行查询”，可查看到被拦截的Spring core RCE漏洞的日志。

select rule, hit_data where rule IN('XX','XX','XX','XX',)

----结束

6.14 通过 LTS 配置 WAF 规则的拦截告警

开启WAF全量日志功能后，您可以将攻击日志、访问日志记录到日志服务（Log Tank Service，简称LTS）中，通过LTS记录的WAF攻击日志数据，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。

本实践通过将WAF的攻击日志开启LTS快速分析，再配置告警规则，实现WAF规则拦截日志的分析及告警，实时洞察您的业务在WAF中的防护情况并作出决策分析。

前提条件

- 防护网站已成功接入WAF。
- WAF的攻击日志流已对接到LTS。
- 已开通消息通知服务。

快速分析规则拦截日志

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“管理与监督 > 云日志服务”，进入“日志管理”页面。

步骤4 在日志组列表中，展开waf日志组，选择日志流“attack”。

步骤5 在日志流详情页面，单击右上角，在弹出页面中，选择“云端结构化解析”页签，进入日志结构化配置页面。

步骤6 选择“JSON”日志结构化方式，单击“从已有日志中选择”，在右侧弹框中任意选择一条日志。

步骤7 单击“智能提取”，筛选出需要“快速分析”的字段，打开这些字段在“快速分析”列的开关，打开后，可以对周期类日志进行统计分析。

步骤8 找到“category”字段，单击该字段“别名”列的，修改该字段名称并单击保存设置。

说明

该字段名称与系统内置字段 category 重复了，需要修改后才能保存成功。

步骤9 在列表右下方，单击“保存”，LTS将对周期内的日志进行快速分析、统计。

步骤10 在左侧导航树中，选择“可视化”，在页面右侧选择日志查询时间段，在搜索框中输入SQL语句后单击“执行查询”。

您可以根据 rule 和 uri 进行分组，在搜索框中输入如下SQL语句，查询指定规则的日志：

select rule, uri, count(*) as cnt where action = 'block' group by rule, uri order by cnt desc

----结束

配置告警规则

步骤1 单击页面左上方的，选择“管理与监督 > 云日志服务”，进入“日志管理”页面。

步骤2 在左侧导航树中，选择“告警”，并选择“告警规则”页签。

步骤3 单击“创建”，在右侧弹框中配置相关参数，参数说明如表6-10所示。

表 6-10 关键参数说明

参数名称	参数说明	样例
规则名称	自定义该规则的名称。	WAF告警
统计类型	选择“SQL统计”。	SQL统计

参数名称	参数说明	样例
相关图表	单击“直接添加”。 • 选择需要配置拦截告警的“日志组名称”和“日志流名称”。 • “查询时间”：日志统计时间周期。 • “查询语句”：步骤10中配置好的SQL语句，如**select rule,uri,count(*) as cnt where action='block' group by rule,uri order by cnt desc**	-
统计周期	告警触发的周期。一般选择“固定间隔”，5分钟。	固定间隔 5 分钟
条件表达式	配置告警阈值	cnt>5
触发告警级别	根据该拦截规则的紧急程选择告警级别，可选择“紧急”、“重要”、“次要”、“提示。”	重要
发送通知	选择“发送”。	发送
告警主题	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》。	-
时区/语言	可单击“修改”配置消息接收的语言和时区。	-
消息模板	在下拉框中选择已有的模板或者单击“创建消息模板”创建新的模板。	sql模板

步骤4 参数配置好后，单击“确定”，告警规则配置完成。当触发该告警规则时，您会收到告警邮件或者短信。

----结束

6.15 “独享 WAF+7 层 ELB”联动，实现防护任意非标端口

如果您需要防护WAF支持的端口范围以外的非标端口，可参考本章节配置WAF的独享模式和7层ELB联动，可实现任意端口业务的防护。

防护场景

假设需要将“www.example.com:9876”配置到WAF进行防护，但WAF不支持“9876”非标端口的防护，则可以按以下的方法进行配置，实现“9876”非标端口的防护。

前提条件

- 已有合适的负载均衡器类型。
- 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。

操作步骤

步骤1 **申请WAF独享引擎实例**。

步骤2 将网站“www.example.com”接入WAF，选择任意的非标准端口，如“86”端口，“源站端口”配置为“9876”，“是否已使用代理”选择，其他参数的配置参见**步骤一：添加防护网站（独享模式）**。

步骤3 为ELB配置监听器和后端服务器组。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。
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。
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。
5. 选择“监听器”页签后，单击“添加监听器”，配置监听器信息，“前端端口”配置为您想防护的端口，如此处配置为“9876”。
6. 单击“下一步：配置后端分配策略”，配置后端服务器组。

   须知

   “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。
7. 单击“下一步：配置后端服务器”后直接单击“下一步：确认配置”。

步骤4 将WAF实例添加到ELB。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域或项目。
3. 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。
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。

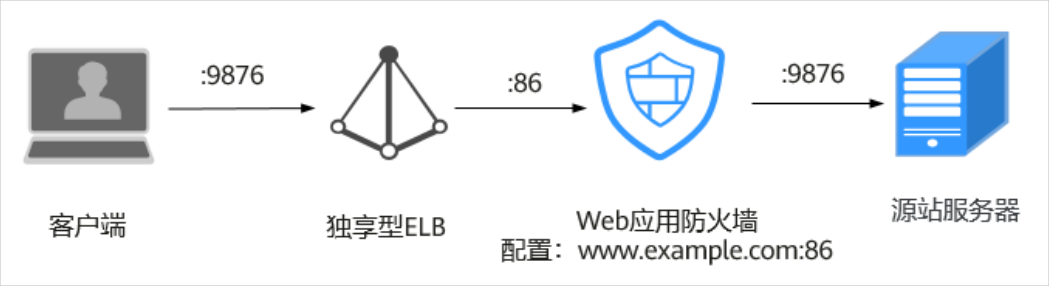
5. 在目标实例所在行的“操作”列，单击“更多 > 添加到ELB”。
6. 在“添加到ELB”页面中，选择**步骤3**中配置的“ELB（负载均衡器）”、“ELB监听器”和“后端服务器组”。
7. 单击“确认”，为WAF实例配置业务端口，“业务端口”需要配置为WAF独享引擎实例实际监听的业务端口，即**步骤2**中配置的86端口。
8. 单击“确认”，配置完成。

步骤5 **为弹性负载均衡绑定弹性公网IP**。

步骤6 **放行独享引擎回源IP**。

----结束

配置完成后流量防护原理图



6.16 “WAF+HSS”联动，提升网页防篡改能力

当攻击者企图通过SQL注入等攻击手段篡改网页时，WAF通过对HTTP(S)请求进行检测，及时识别并阻断攻击，防止攻击渗透进入系统层。

即使攻击突破了第一层防护也不用慌，企业主机安全网页防篡改早已提前帮您驱动及锁定Web文件目录下的文件，只有网站管理员可通过特权进程更新网站内容；除了锁定文件，企业主机安全网页防篡改还同时在本地主机和远端做了备份，一旦发生非法篡改，可以立即通过备份目录进行恢复；对于web服务器里的应用程序等动态网页，企业主机安全网页防篡改采用RASP检测应用程序行为，能够检测针对数据库等动态数据的篡改行为，实时阻断攻击者通过应用程序篡改网页内容的行为。

企业主机安全网页防篡改和Web应用防火墙双剑合璧，杜绝网页篡改事件发生。

什么是网页篡改&网页被篡改的后果

网页篡改是一种通过网页应用中的漏洞获取权限，通过非法篡改Web应用中的内容、植入暗链等，传播恶意信息，危害社会安全并牟取暴利的网络攻击行为。

如果网页被篡改，可能导致网页被植入色情、诈骗等非法信息的链接，从而对企业、社会造成不良影响，损害企业的品牌形象。

HSS 和 WAF 的网页防篡改的区别

表 6-11 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	• 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	• 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	支持预防篡改和恢复篡改能力，适用于对网站防护要求高的用户。	适用于对网站防护要求低，仅需要对应用层进行防护的用户。

配置 WAF 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)”。

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。

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，参数说明如表6-12所示。

表 6-12 参数说明

参数	参数说明	取值样例
域名	设置防篡改的域名。	www.example.com
路径	设置防篡改的URL链接中的路径（不包含域名）。 URL用来定义网页的地址。基本的URL格式如下： 协议名://域名或IP地址[:端口号]/[路径名/…/文件名]。 例如，URL为“http://www.example.com/admin”，则“路径”设置为“/admin”。 **说明** ● 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

开启 HSS 网页防篡改

步骤1 。

步骤2 在左侧导航树中，选择“主动防御 > 网页防篡改”，进入“网页防篡改”界面，单击“添加防护服务器”。

步骤3 在“添加防护服务器”页面，选择“可添加服务器”页签，勾选需要开启防护的服务器，选择目标配额，可默认随机选择，单击“添加并开启防护”。

步骤4 开启“网页防篡改”防护服务后，请在控制台上查看的开启状态。

“网页防篡改版”开启后，旗舰版防护会同步开启。

- 选择“主动防御 > 网页防篡改”，目标服务器所在行的“防护状态”为“防护中”，则表示网页防篡改版已开启。

----结束

须知

- 关闭网页防篡改防护服务前，请对主机执行全面的检测，处理已知风险并记录操作信息，避免运维失误，使您的主机遭受攻击。
- 关闭网页防篡改防护服务后，网页应用被篡改的可能性将大大提高，请及时清理主机中的重要数据、关停主机中的重要业务并断开主机与外部网络的连接，避免因主机遭受攻击而承担不必要的损失。
- 执行关闭网页防篡改操作后，防护目录下的文件将不再受“网页防篡改”功能的防护，建议您提前处理防护目录下的文档，再对文档执行暂停防护、编辑或删除的相关操作。
- 执行关闭网页防篡改操作后，若您的文档不慎被删除，请在主机本地备份或远端主机的备份路径中查找。
- 当用户关闭网页防篡改时会同步关闭旗舰版防护。

7 IAM 权限管理

7.1 创建用户组并授权使用 WAF

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，简称IAM），通过IAM，您可以：

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

如果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。

本章节为您介绍对用户授权的方法，操作流程如**图7-1**所示。

前提条件

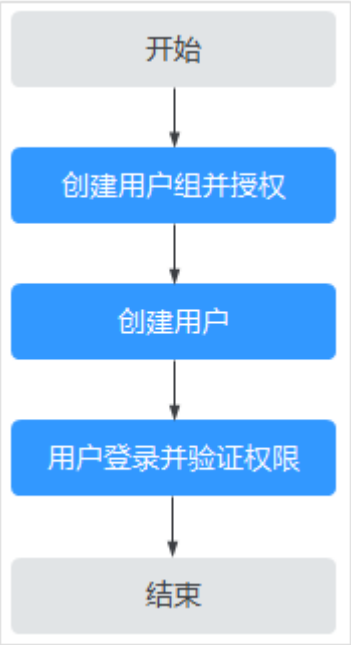
表 7-1 WAF 系统角色

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

系统角色/策略名称	描述	类别	依赖关系
WAF ReadOnlyAccess	Web应用防火墙的只读访问权限。	系统策略	

示例流程

图 7-1 给用户授权服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予Web应用防火墙权限“WAF Administrator”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，切换至授权区域，验证权限：
   在“服务列表”中选择除Web应用防火墙外（假设当前策略仅包含“WAF Administrator”）的任一服务，若提示权限不足，表示“WAF Administrator”已生效。

7.2 WAF 自定义策略

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

目前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。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的WAF自定义策略样例。

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"
            ]
        }
    ]
}
```

7.3 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最初提供的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

权限	授权项
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
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

权限	授权项
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
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

8 常见问题

8.1 产品咨询

8.1.1 新手入门常见问题

本章节为您罗列了WAF入门级的常见问题。

Web 应用防火墙是硬防火墙还是软防火墙?

Web应用防火墙是软防火墙。

接入 WAF 对现有业务和服务器运行有影响吗?

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

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的请求内容进行拦截。

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。

WAF 配置多个源站时如何负载?

如果您配置了多个源站IP地址，WAF默认使用加权轮询的方式对访问请求进行负载均衡。您也可以根据需要自定义负载均衡算法。

源站开启 gzip 对 WAF 有影响吗?

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

使用 WAF 是否影响内网向外发送数据?

使用WAF不会影响内网机器向外发送数据。以云模式的CNAME方式或独享模式将网站成功接入WAF后，WAF对网站的HTTP(S)请求进行检测，网站所有访问请求将先流转到WAF，WAF检测过滤恶意攻击流量后，将正常流量返回给源站，从而确保源站安全、稳定、可用。

多个域名对应同一源站，Web 应用防火墙可以防护这些域名吗?

可以。不同域名对应同一个源站时，您可以将这些域名都接入WAF进行防护。

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

防护规则的路径是否区分大小写?

WAF所有需要配置路径的防护规则，配置的防护路径都区分大小写。

什么是防护 IP?

防护IP是指需要保护的网站的IP地址。

云模式 WAF 提供的解析地址是固定 IP 吗?

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

源站 IP 更改后是否会改变 CNAME 值?

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

更换 IP 后，需要重新将域名添加到 WAF 吗?

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

WAF 需要绑定 EIP 吗?

WAF云模式无需绑定EIP，独享WAF需要和七层的独享型ELB进行联动，EIB需要有公网IP地址作为业务地址。

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。参考**如何放行云模式WAF的回源IP段?** 查看WAF的回源IP并放行回源IP。

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

不支持。

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

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。

8.1.2 功能说明类

8.1.2.1 Web 应用防火墙是否能防护 IP?

WAF可以对IP进行防护。

云模式

WAF不能防护IP，只能基于域名进行防护。

在WAF中配置的源站IP只支持公网IP，不支持私网IP或者内网IP。

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

独享模式

WAF可以对IP或域名进行防护。

在WAF中配置的源站IP支持私网IP或者内网IP。

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

8.1.2.2 Web 应用防火墙支持对哪些对象进行防护?

WAF支持对域名或IP进行防护，相关说明如下：

- 云模式的CNAME接入只能基于域名进行防护

  在WAF中配置的源站IP只支持公网IP。例如，源站服务器部署了弹性负载均衡（Elastic Load Balance，简称ELB）时，只要ELB（经典型、共享型或独享型）有公网IP，云模式就可以对域名进行防护。
- 独享模式可以对域名或IP进行防护

8.1.2.3 Web 应用防火墙攻击防护类问题

什么是防护 IP?

防护IP是指需要保护的网站的IP地址。

云模式 WAF 提供的解析地址是固定 IP 吗?

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

源站 IP 更改后是否会改变 CNAME 值?

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

更换 IP 后，需要重新将域名添加到 WAF 吗?

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

WAF 需要绑定 EIP 吗?

WAF云模式无需绑定EIP，独享WAF需要和七层的独享型ELB进行联动，EIB需要有公网IP地址作为业务地址。

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。参考**如何放行云模式WAF的回源IP段?** 查看WAF的回源IP并放行回源IP。

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

不支持。

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

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。

8.1.2.4 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

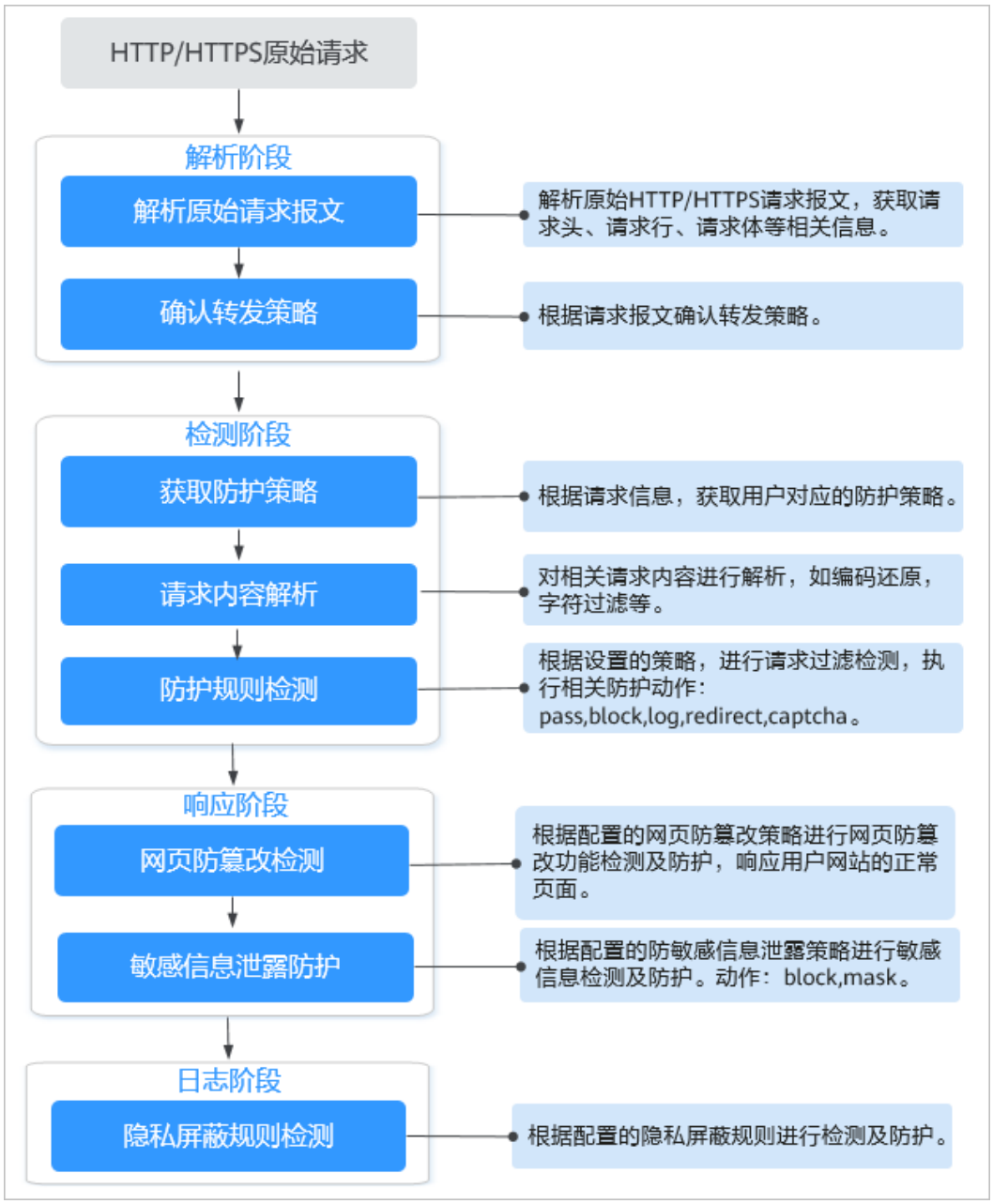
  临时的Cookie，不包含到期日期，存储在内存中。当浏览器关闭时，Cookie将被删除。
- 持久性Cookie

  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。

8.1.2.5 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8-1**所示。

图 8-1 WAF 引擎检测图



8.1.2.6 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8-1所示。

表 8-1 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	• 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	• 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

8.1.2.7 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

8.1.2.8 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。

8.1.2.9 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 8-2 CNAME 接入、独享模式接入防护原理

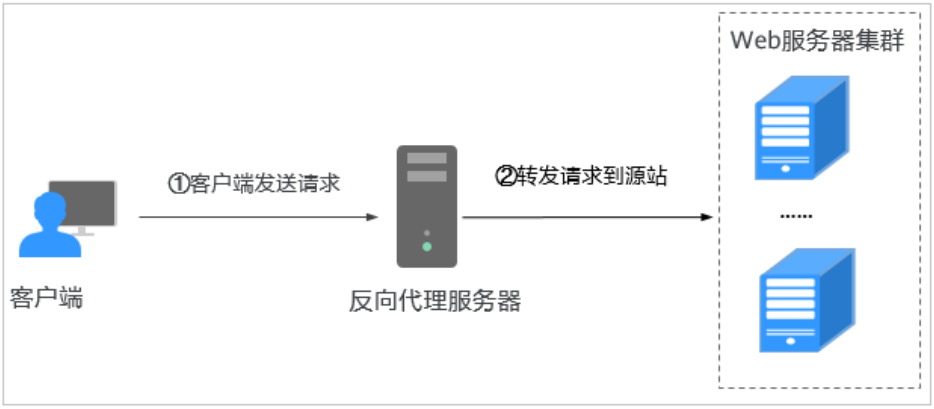
  

- Nginx转发

  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 8-3 Nginx 转发原理



8.1.2.10 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。

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

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

配置方法

步骤1 **申请WAF独享引擎实例**。

步骤2 将网站域名添加到WAF中并完成域名接入。

- 云模式：**添加防护域名**。
- 独享模式：**步骤一：添加防护网站（独享模式）**。

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

----结束

8.1.3 使用说明类

8.1.3.1 接入 WAF 后为什么漏洞扫描工具扫描出未开通的非标准端口?

问题现象

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

可能原因

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

处理建议

无需处理

8.1.3.2 如何获取访问者真实 IP?

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

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

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

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

8.1.3.3 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。

8.1.3.4 QPS 和请求次数有什么区别?

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

QPS是单个进程每秒请求服务器的成功次数。

说明

QPS = 请求数/秒（req/sec ）

“安全总览”页面中QPS的计算方式说明如表8-2所示。

表 8-2 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

时间段	QPS平均取值说明	QPS峰值取值说明
“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

8.1.3.5 Web 应用防火墙支持自定义授权策略吗?

WAF支持自定义授权策略，通过IAM，您可以：

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

8.1.3.6 同一防护域名/IP 可以添加到不同的账号进行防护吗?

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

当防护域名/IP以独享模式添加到WAF时，可以添加到不同的账号进行防护。

须知

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

8.1.3.7 仅放行通过 WAF 的访问请求，如何配置?

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

8.1.3.8 为什么 Cookie 中有 HWWAFSESID 或 HWWAFSESTIME 字段?

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

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

8.1.3.9 云模式、独享模式可以互相切换吗?

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

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

8.1.3.10 网站部署了反向代理服务器，如何配置 WAF?

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

8.1.3.11 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。

8.1.4 企业项目

8.1.4.1 WAF 可以跨企业项目使用吗?

不同的WAF模式，是否支持跨企业项目使用，详情如下：

- 云模式

  支持跨企业项目使用。

- 独享模式

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

  说明

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

8.2 业务请求/规格

8.2.1 变更规格类

8.2.1.1 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

8.2.2 业务请求类

8.2.2.1 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。

8.2.2.2 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 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4 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

8.3 计费相关

8.3.1 Web 应用防火墙如何收费?

WAF云模式支持“按需计费”，按实际添加的域名个数、和使用的请求数计费。

WAF独享模式支持“按需计费”和“按月计费”两种计费方式。

- 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。
- 按月计费：按申请的实例数量和实例规格计费

更多关于计费的详细信息，请参见**计费说明**。

8.3.2 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应用防火墙云模式支持按需计费（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，按实际添加的域名个数和使用的请求数计费，独享模式支持“按需计费”和“按月计费”两种计费方式。

更多关于计费的详细信息，请参见**计费说明**。

8.4 网站接入配置

8.4.1 域名/端口类

8.4.1.1 域名/IP 如何接入 Web 应用防火墙?

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

WAF支持云模式和独享模式两种部署模式，各部署模式支持防护的对象说明如下：

- 云模式：域名，云上或云下的Web业务
- 独享模式：域名或IP，云上的Web业务

须知

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

网站接入WAF各模式的流程如下图所示。

图 8-4 网站接入 WAF 的操作流程图-云模式（CNAME 接入）

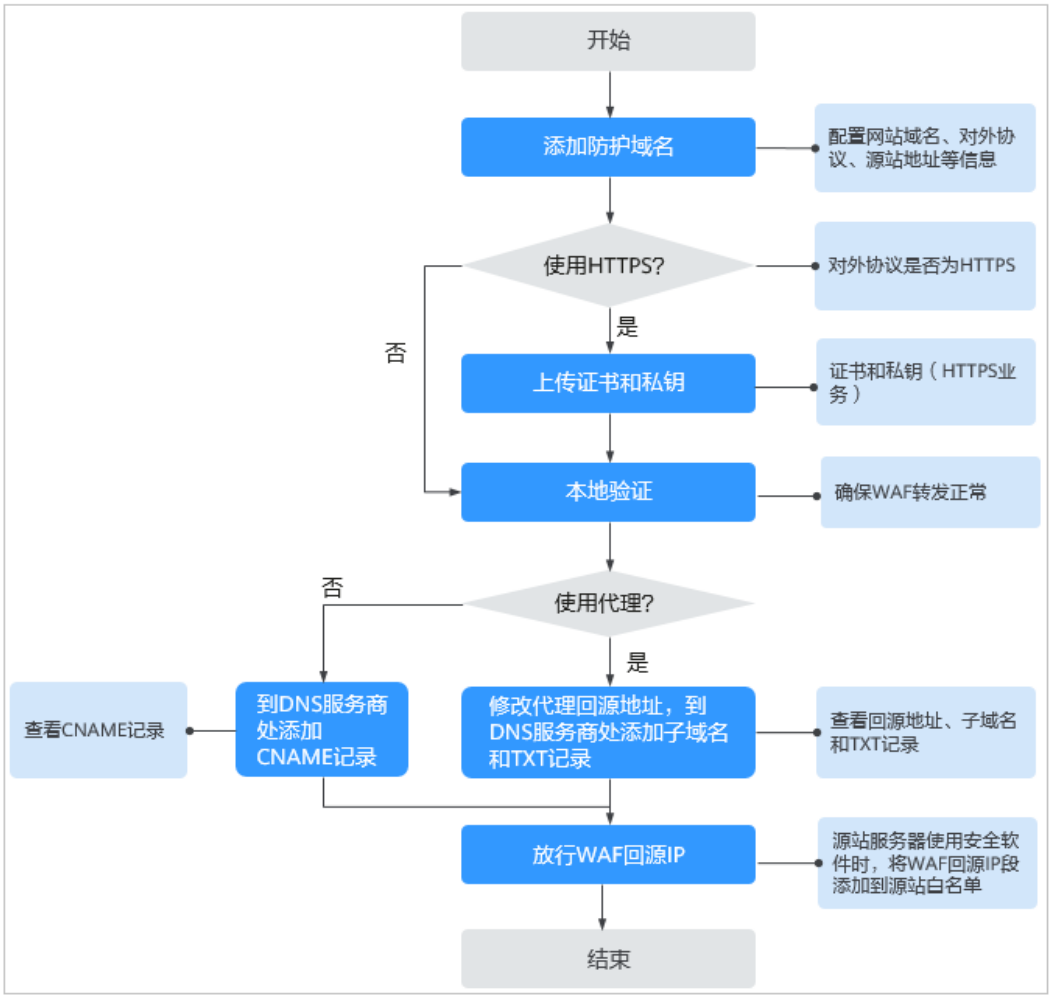
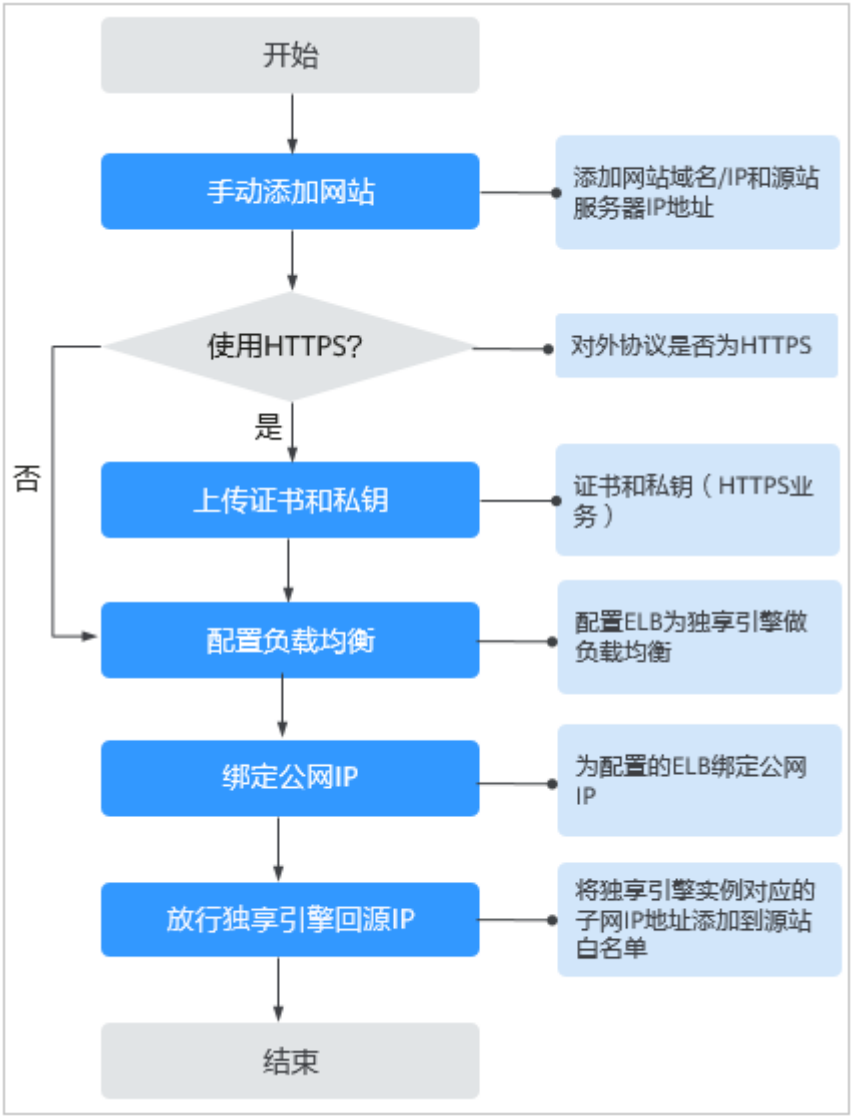


图 8-5 网站接入 WAF 的操作流程图-独享模式



- 如果网站接入WAF失败，即防护网站“接入状态”显示“未接入”，请参见**域名/IP接入状态显示“未接入”，如何处理?** 排查处理。
- 如果网站接入WAF后访问网站报错，请参见**如何排查500/502/504错误?** 进行处理。

8.4.1.2 Web 应用防火墙支持哪些非标准端口?

Web应用防火墙除了可以防护标准的80，443端口外，还支持非标准端口的防护，且不同版本支持的端口有所差异。

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

WAF 支持的端口

Web应用防火墙可防护的端口如**表8-3**所示。

表 8-3 WAF 支持的端口

部署模式	端口分类	HTTP协议	HTTPS协议	端口防护限制数
云模式	标准端口	80	443	不限制
	非标准端口（**86个**）	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805	**20个**
独享模式	标准端口	80	443	不限制

部署模式	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

8.4.1.3 独享模式如何防护不支持的非标准端口?

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

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

须知

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

请参照以下操作步骤进行配置。

步骤1 登录管理控制台。

步骤2 在WAF管理控制台添加防护域名。

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

   您可以在防护网站列表中查看已添加防护网站。

步骤3 在ELB管理控制台配置负载均衡。

1. 单击页面左上方的 ☰，选择“网络 > 弹性负载均衡”，进入“负载均衡器”页面。
2. 在负载均衡器所在行的“名称”列，单击目标负载均衡器名称，进入ELB“基本信息”页面。
3. 在“跨VPC后端”所在行，单击“跨VPC后端”，并在弹框中单击“确定”，开启跨VPC后端。
4. 选择“监听器”页签后，单击“添加监听器”，配置监听器端口为“1234”。
5. 单击“下一步：配置后端分配策略”，配置后端分配策略。
6. 单击“下一步：添加后端服务器”，并选择“跨VPC后端”页签，添加跨VPC后端和健康检查。
7. 单击“添加跨VPC后端”，在弹出的弹框中，配置“跨VPC的后端IP”和“后端端口”。

- 跨VPC后端IP：WAF独享引擎的IP（在“独享引擎”列表中获取）。
- 后端端口：“81”（与步骤2.3中配置的端口一致）。

8. 单击“确定”，配置完成。
9. 单击“下一步：确认配置”后单击“提交”。

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

----结束

8.4.1.4 如何在添加域名中配置防护域名?

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

相关概念

- 泛域名

  泛域名是指带1个通配符“*”且以“*.”号开头的域名。

  例如：“*.example.com”是正确的泛域名，但“*.*.example.com”则是不正确的。

  说明

  一个泛域名算一个域名。

- 单域名

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

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

  说明

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

如何选择域名类型

WAF支持防护单域名和泛域名。

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

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

说明

建议添加的“防护域名”与在DNS服务商处设置的域名保持一致。

同时在 WAF 中添加单域名和泛域名，WAF 会优先检测哪个域名?

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

8.4.1.5 添加域名时，防护网站端口需要和源站端口配置一样吗?

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

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

8.4.1.6 添加防护域名时如何配置非标准端口?

端口为实际防护网站的端口，端口配置说明如下：

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

8.4.1.7 多个端口的服务器，如果某个端口不需要 WAF 防护，如何处理?

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

8.4.1.8 域名/IP 接入 WAF 前需要准备哪些数据?

请根据申请的WAF模式，在域名/IP接入WAF前收集相关信息。

接入WAF前需要准备以下数据：

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

8.4.1.9 删除防护域名时应该注意哪些事项?

删除网站的具体的操作请参见**删除防护网站**，删除网站前的注意事项如下：

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

8.4.1.10 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。

8.4.1.11 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。

8.4.1.12 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。

8.4.1.13 如何使网站流量切入云模式 Web 应用防火墙?

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

工作原理

- 未使用代理

  当网站没有接入到WAF前，DNS直接解析到源站的IP，所以当网站接入WAF后，需要把DNS解析到WAF的CNAME，这样流量才会先经过WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。
- 使用了DDoS高防等代理

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

说明

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

操作指导

添加域名后，WAF会根据添加的域名是否已在WAF前使用了代理，生成CNAME值或者CNAME、子域名和TXT记录，用于域名解析，使网站流量切入WAF，相关操作指导参见**表8-4**。

表 8-4 操作指导

场景	生成的参数值	域名解析的相关操作
未使用代理	CNAME	把DNS解析到WAF的“CNAME”。
使用代理	CNAME、子域名和TXT记录	• 将DDoS高防等代理回源地址修改为WAF的“CNAME”。 • （可选）在DNS服务商处添加一条WAF的“子域名”和“TXT记录”。

操作步骤

具体的操作步骤请参见**域名接入**。

8.4.1.14 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。

8.4.2 证书管理

8.4.2.1 配置泛域名时，如何选择证书?

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

8.4.2.2 如何修改已绑定域名的证书?

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

以独享WAF为例，执行以下操作修改已绑定域名的证书。

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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“防护网站”列中，单击目标网站，进入网站基本信息页面。

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

----结束

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

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

8.4.2.4 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8-5在本地将证书转换为PEM格式，再上传。

表 8-5 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	• 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	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	• 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。

8.4.3 服务器配置类

8.4.3.1 如何配置对外协议与源站协议?

本节介绍如何配置WAF的对外协议与源站协议。

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

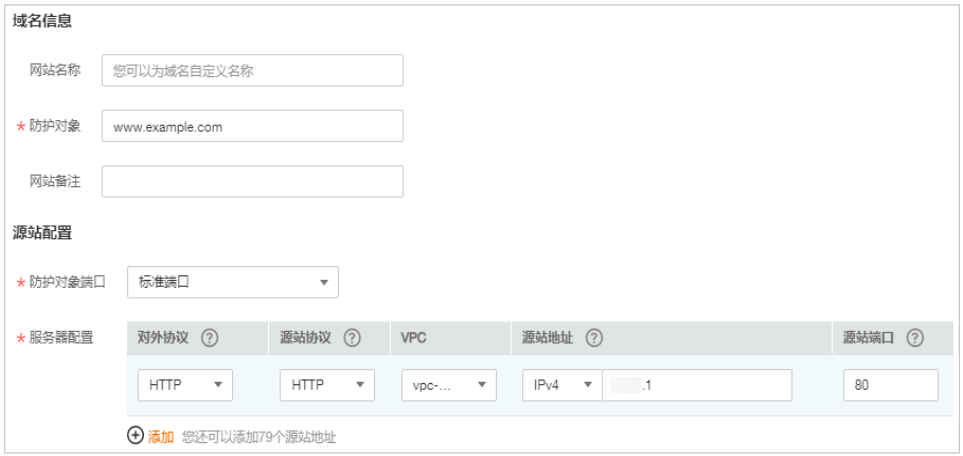
HTTP 访问模式-302 跳转响应

“对外协议”和“源站协议”都配置为“HTTP”，如图8-6所示。

须知

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

图 8-6 HTTP 协议访问模式



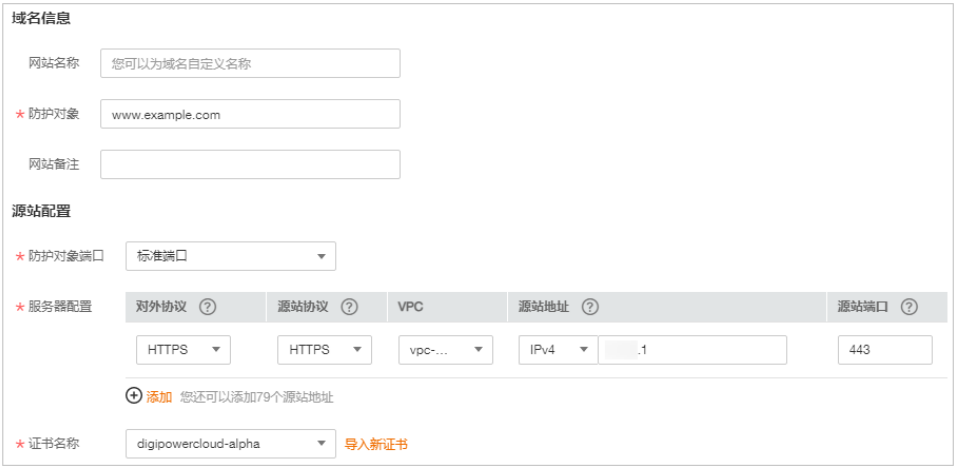
HTTPS 访问强制跳转模式

“对外协议”和“源站协议”都配置为“HTTPS”，如图8-7所示。当使用HTTP协议访问服务器时，会强制跳转为HTTPS协议。

须知

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

图 8-7 HTTPS 协议访问强制跳转模式



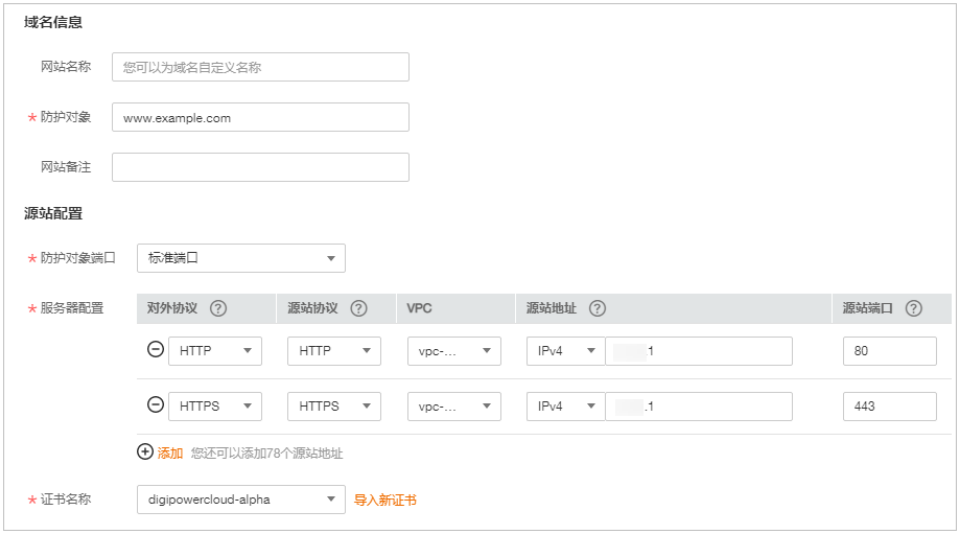
HTTP/HTTPS 分别转发模式

“对外协议”和“源站协议”配置的协议如图8-8所示。

须知

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

图 8-8 HTTP/HTTPS 分别转发模式



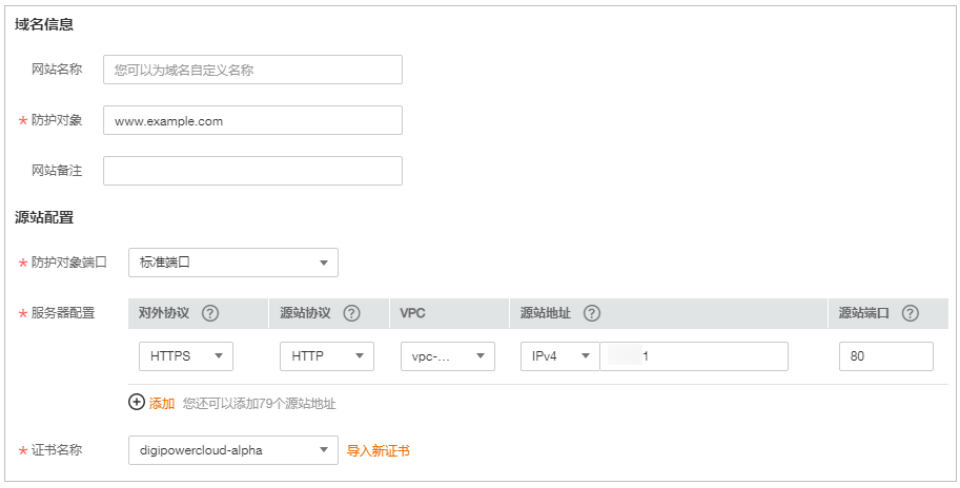
HTTPS 卸载模式

“对外协议”配置为“HTTPS”且“源站协议”配置为“HTTP”，如图8-9所示。

须知

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

图 8-9 使用 WAF 做 HTTPS 卸载模式



8.4.3.2 添加域名时，为什么不能选择对外协议?

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

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

8.4.3.3 云模式服务器的源站地址可以配置成 CNAME 吗?

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

8.4.4 域名解析类

8.4.4.1 如何处理 DNS 解析状态异常?

如果DNS解析状态异常，表示未完成域名解析，即域名接入WAF失败，可参照以下步骤重新完成域名接入。

- 若使用了CDN或高防等代理类服务，需要配置回源地址、子域名和TXT记录。
  a. 配置网站使用代理的“回源地址”。
     将CDN或高防等代理中的回源地址修改为WAF生成的回源地址。
  b. 配置“子域名”和“TXT记录”。
     前往您的DNS服务商处，添加一个“子域名”，并为该子域名添加一条“TXT记录”。

  须知

  WAF的多AZ灾备机制依赖DNS解析。请不要使用固定IP访问业务，否则会影响服务的灾备可靠性。

- 未使用代理，需要配置CNAME记录。
  a. 到该域名的DNS服务商处，配置防护域名的别名解析，具体操作请咨询您的域名服务提供商。

  须知

  WAF的多AZ灾备机制依赖DNS解析。请不要使用固定IP访问业务，否则会影响服务的灾备可靠性，因此：
  1. 请不要用修改hosts记录的方式替代DNS解析配置。
  2. 请不要用A记录替代CNAME记录。

  以下为当前主流的域名服务商的CNAME绑定方法，仅供参考。如与实际配置不符，请以各自域名服务商的信息为准。
  i. 登录域名服务提供商的管理控制台。
  ii. 进入域名解析记录页。
  iii. 设置CNAME解析记录。
     - “记录类型”选择为“CNAME”。
     - “主机记录”一般填写域名前缀，例如：防护域名为“admin.demo.com”，“主机记录”填写为“admin”。
     - “记录值”填写为WAF生成的CNAME。

- “解析线路”，“TTL” 保持默认值即可。

iv. 填写完成后，单击“保存”，完成解析设置。

须知

以上解析方法为第三方解析方法。本文档不对任何第三方内容进行控制或负责，包括但不限于其准确性、兼容性、可靠性、可用性、合法性、适当性、性能、不侵权、更新状态等。

b. 验证域名的CNAME是否配置成功。

i. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”。

ii. 执行以下命令，查询CNAME。如果回显的域名是配置的CNAME，则表示配置成功。

nslookup www.*domain*.com

8.4.5 接入后处理

8.4.5.1 域名接入 Web 应用防火墙后，能通过 IP 访问网站吗?

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

8.4.5.2 如何在本地测试 Web 应用防火墙?

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

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

具体的操作步骤请参见**本地验证**。

8.4.5.3 域名接入 WAF 后，为什么无法开启防护模式?

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

8.5 业务中断排查

8.5.1 如何排查 500/502/504 错误?

业务接入WAF防护之后，访问网站如果出现500 Internal Server Error，502 Bad Gateway，504 Gateway Timeout等错误，请参考以下方法排查错误。

现象一

完成WAF配置之后正常，但是一段时间后就报502，或者大概率出现502。

- 可能原因

  防火墙、后端服务器安全防护软件、业务限速策略拦截。

- 解决方法

  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。

现象二

完成WAF配置之后，访问页面返回502/500，或者大概率出现502/500（当后端配置了多个服务器的情况）。

- 可能原因

  源站配置错误。

- 解决方法

  在“域名配置”列表中找到相应的域名记录，单击域名名称，进入域名基本信息页面，在“服务器信息”栏中，确认源站协议、IP、端口等信息是否正确。

  可在浏览器访问源站IP地址来检查后端业务端口是否打开。

现象三

完成WAF配置之后，HTTPS业务大概率返回502，而直接通过IP访问源站正常。

- 可能原因

  HTTPS采用不安全的协议版本。

- 解决方法

  SSL低版本的协议存在严重的安全隐患，Web应用防火墙支持TLS1.2及以上版本的协议。如果您的业务服务器的SSL版本较低，接入WAF之后则会出现502错误，需要您升级解决。您可以在通过“https://www.ssllabs.com/ssltest/index.html”检查网站服务的SSL版本信息：

  - 如果你的Web服务器是Windows 2008以前的版本，SSL协议不支持TLS1.2及以上。您需要将服务器版本升级到Windows 2008以上（或Linux较新版本的操作系统），并在IIS等服务中开启TLS1.2。
  - 如果您的Web服务是其他系统，请确认SSL协议是否是TLS1.2或以上。

现象四

完成WAF配置之后，业务正常。但业务量增加时，502/504比例增加。直接访问源站也有一定概率出现502/504的返回码。

- 可能原因

  后端服务器性能问题。

- 解决方法

  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. 对后端ECS扩容来支撑业务增长，WAF支持配置多个后端服务器。

c. 如果业务为HTTPS，可考虑在WAF设置HTTPS转发，回源走HTTP协议，降低后端服务器的计算压力。

8.5.2 域名/IP 接入状态显示“未接入”，如何处理?

故障现象

添加防护域名或IP后，域名或IP接入WAF失败，即防护网站“域名接入进度/状态”显示“未接入”。

须知

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

云模式排查思路和处理建议

防护网站的“部署模式”为“云模式”时，请参考图8-10和表8-6进行排查处理。

图 8-10 云模式排查思路

表 8-6 接入 WAF 失败问题处理

可能原因	处理建议
原因一：**域名**“接入状态”**未刷新**	在防护网站“接入状态”栏，单击刷新状态。

可能原因	处理建议
原因二：**访问流量未达到WAF统计要求** **须知** 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击刷新状态。
原因三：**域名参数配置错误**	**须知** WAF支持防护以下类型域名： • 一级域名，例如，example.com • 单域名/二级域名等子域名，例如，www.example.com • 泛域名，例如，*.example.com example.com与www.example.com是不同的域名，请确认“防护域名”配置正确。 请参照以下步骤确保域名参数配置正确。 1. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”，进入命令提示符窗口。 2. 运行**ping** *域名在WAF对应的CNAME值*，获取WAF的回源IP。 3. 用文本编辑器打开hosts文件，hosts文件一般位于“C:\Windows\System32\drivers\etc\”路径下。 4. 在hosts文件添加记录：***防护域名 域名对应的WAF回源IP***。 5. 修改hosts文件后保存，在命令提示符窗口中运行**ping** *防护域名*（例如ping www.example.com）。 如果回显信息中的IP地址为2中的WAF回源IP地址，说明域名参数配置正确。 如果域名参数配置错误，删除该域名后重新添加防护网站。
原因四：**未配置域名解析或代理回源地址**	确认接入WAF的网站是否使用高防、CDN、云加速等代理。 • 是 – 将CDN等代理回源地址修改为WAF的“CNAME”。 – （可选）在DNS服务商处添加一条WAF的“子域名”和“TXT记录”。 • 否：到该域名的DNS服务商处，配置防护域名的别名解析。

可能原因	处理建议
原因五：**域名解析或代理回源地址配置错误**	请参照以下步骤验证域名的CNAME是否配置成功。 1. 在Windows操作系统中，选择“开始 > 运行”，在弹出框中输入“cmd”，按“Enter”，进入命令提示符窗口。 2. 执行**nslookup**命令，查询CNAME。如果回显信息的域名在WAF上的CNAME，则表示配置成功。 以域名www.example.com为例。 **nslookup** www.example.com

独享模式排查思路和处理建议

防护网站的“部署模式”为“独享模式”时，请参考图8-11和表8-7进行排查处理。

图 8-11 独享模式排查思路

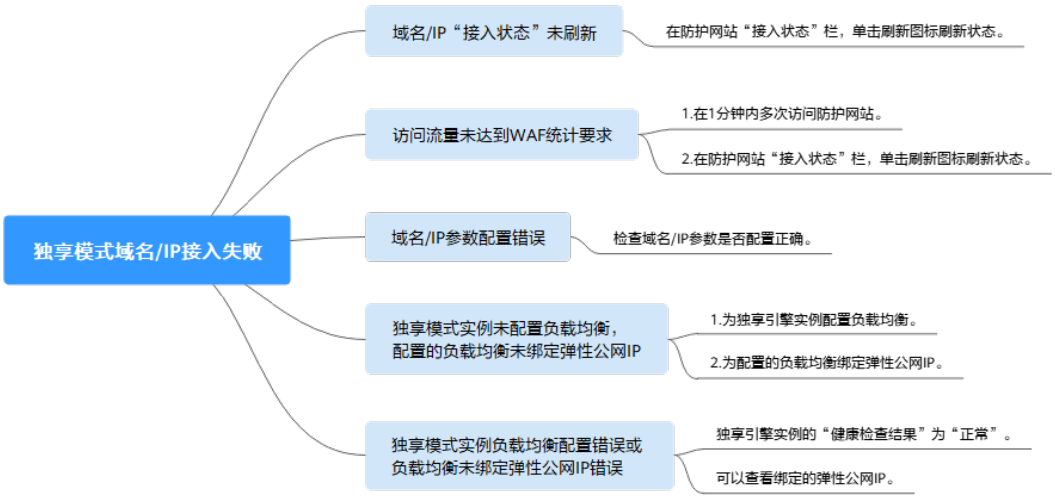


表 8-7 独享模式接入 WAF 失败问题处理

可能原因	处理建议
原因一：**域名/IP“接入状态”未刷新**	在防护网站“接入状态”栏，单击刷新状态。
原因二：**访问流量未达到WAF统计要求** **须知** 防护网站接入WAF后，当WAF统计防护网站在5分钟内有20次请求时，将认定该防护网站已接入WAF。	1. 在1分钟内多次访问防护网站。 2. 在防护网站“接入状态”栏，单击刷新状态。

可能原因	处理建议
原因三：**域名/IP参数配置错误**	检查域名/IP参数是否正确。 如果域名/IP配置错误，删除该域名/IP后重新添加防护网站。
原因四：**没有为独享模式实例配置负载均衡，配置的负载均衡未绑定弹性公网IP**	1. 为独享引擎实例**配置负载均衡**。 2. **为弹性负载均衡绑定弹性公网IP**。
原因五：**独享模式实例负载均衡配置错误或负载均衡绑定弹性公网IP错误**	• **配置负载均衡**后，当WAF独享引擎实例的“健康检查结果”为“正常”时，说明弹性负载均衡配置成功。 • **为弹性负载均衡绑定弹性公网IP**后，可以查看绑定的弹性公网IP，说明绑定成功。

8.5.3 WAF 误拦截了正常访问请求，如何处理?

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

须知

如果您已开通企业项目，请务必在“企业项目”下拉列表中选择您所在的企业项目并确保已开通操作权限，才能处理该企业项目下的误报事件。

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8-8**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。

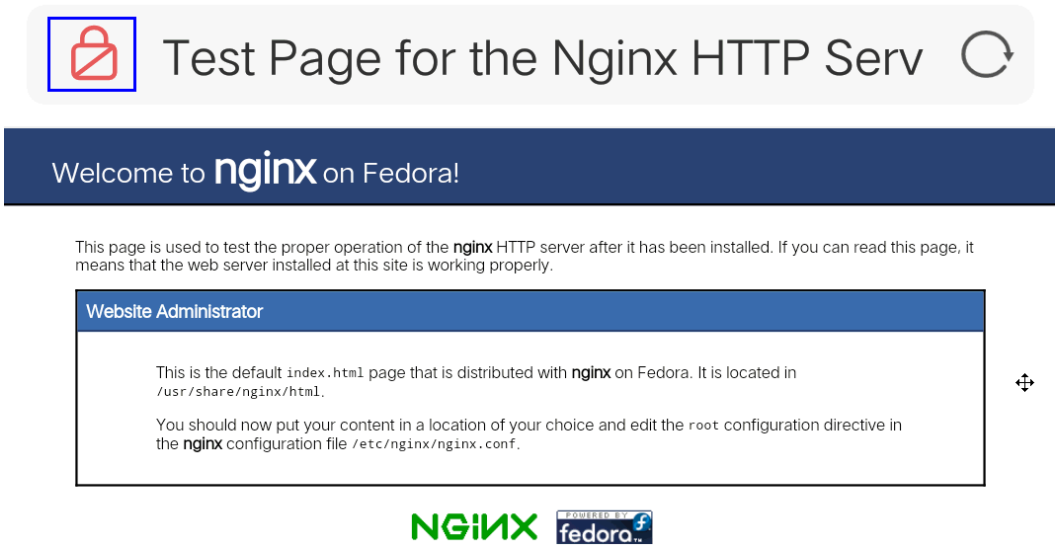
表 8-8 误报处理说明

命中规则类型	命中规则	处理方式
WAF内置防护规则	• Web基础防护规则 防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击，以及Webshell检测、深度反逃逸检测等Web基础防护。 • 网站反爬虫的“特征反爬虫”规则 可防护搜索引擎、扫描器、脚本工具、其它爬虫等爬虫。	在该攻击事件所在行的“操作”列，单击“误报处理”，详细操作请参见**处理误报事件**。
自定义防护规则	• 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	“非法请求”访问请求 **说明** 当遇到以下情况时，WAF将判定该访问请求为非法请求并拦截该访问请求： • POST/PUT使用“form-data”时，表单的参数个数多于8192个。 • URI的参数个数多于2048个。 • Header个数超过512个。	“误报处理”按钮置灰不能使用，请参见**配置精准访问防护规则定制化防护策略**放行该访问请求。

8.5.4 如何解决 HTTPS 请求在部分手机访问异常?

打开手机浏览器，访问防护域名，如果出现类似如**图8-12**所示的页面，则表示该手机上HTTPS请求访问异常，该问题是由于上传的证书链不完整，可参照**如何解决证书链不完整?** 解决。

图 8-12 访问异常



8.5.5 如何解决证书链不完整?

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

按以下两种方法可解决此问题：

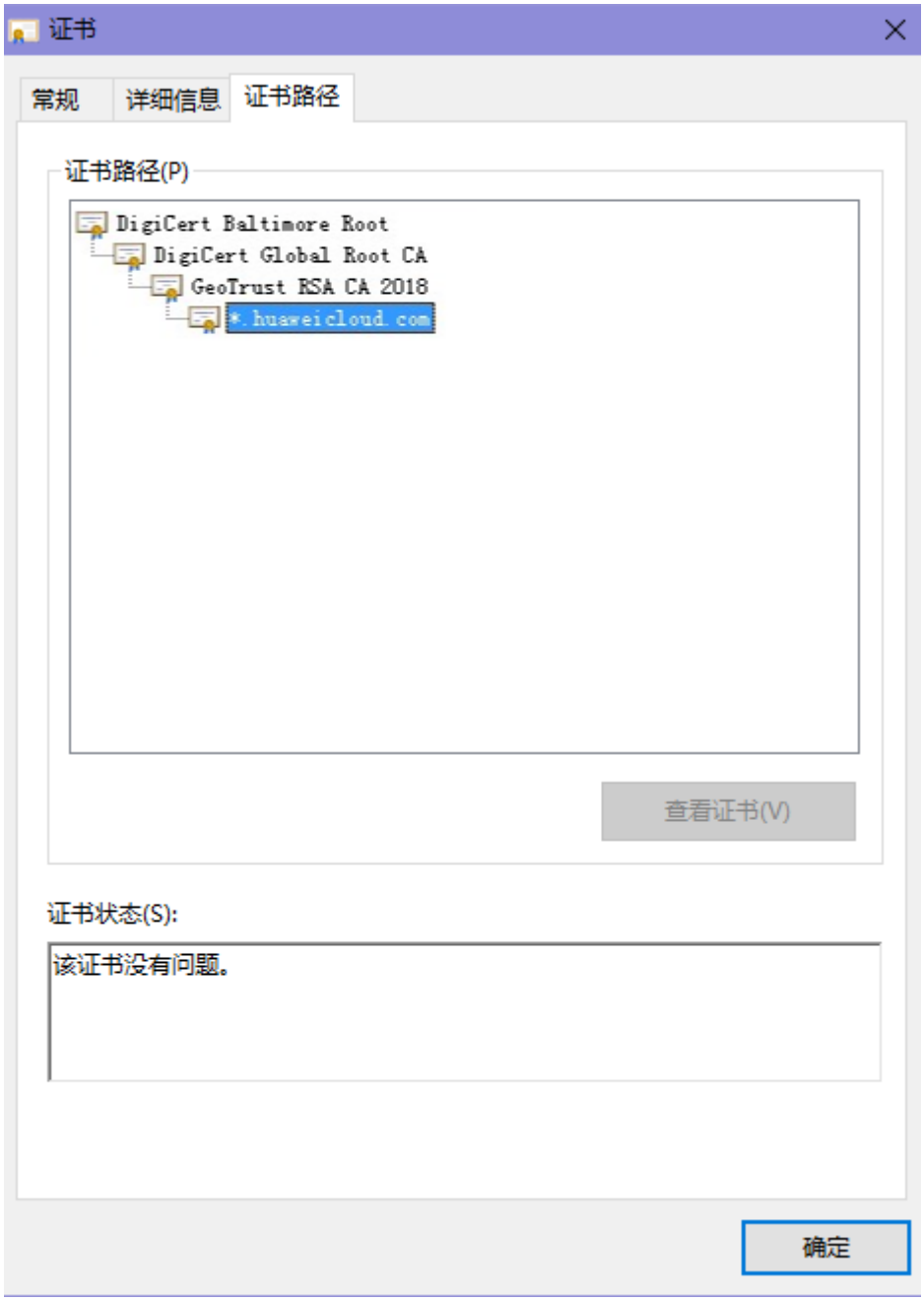
- 手动构造完整证书链，并上传证书。（WAF自动补全证书链功能正在开发中，敬请期待！）
- 重新上传正确的证书。

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

步骤1 **查看证书**。单击浏览器前的锁，可查看证书状况。

步骤2 **查看证书链**。单击“证书”，并选中“证书路径”页签，可单击证书名称查看证书状态，如图8-13所示。

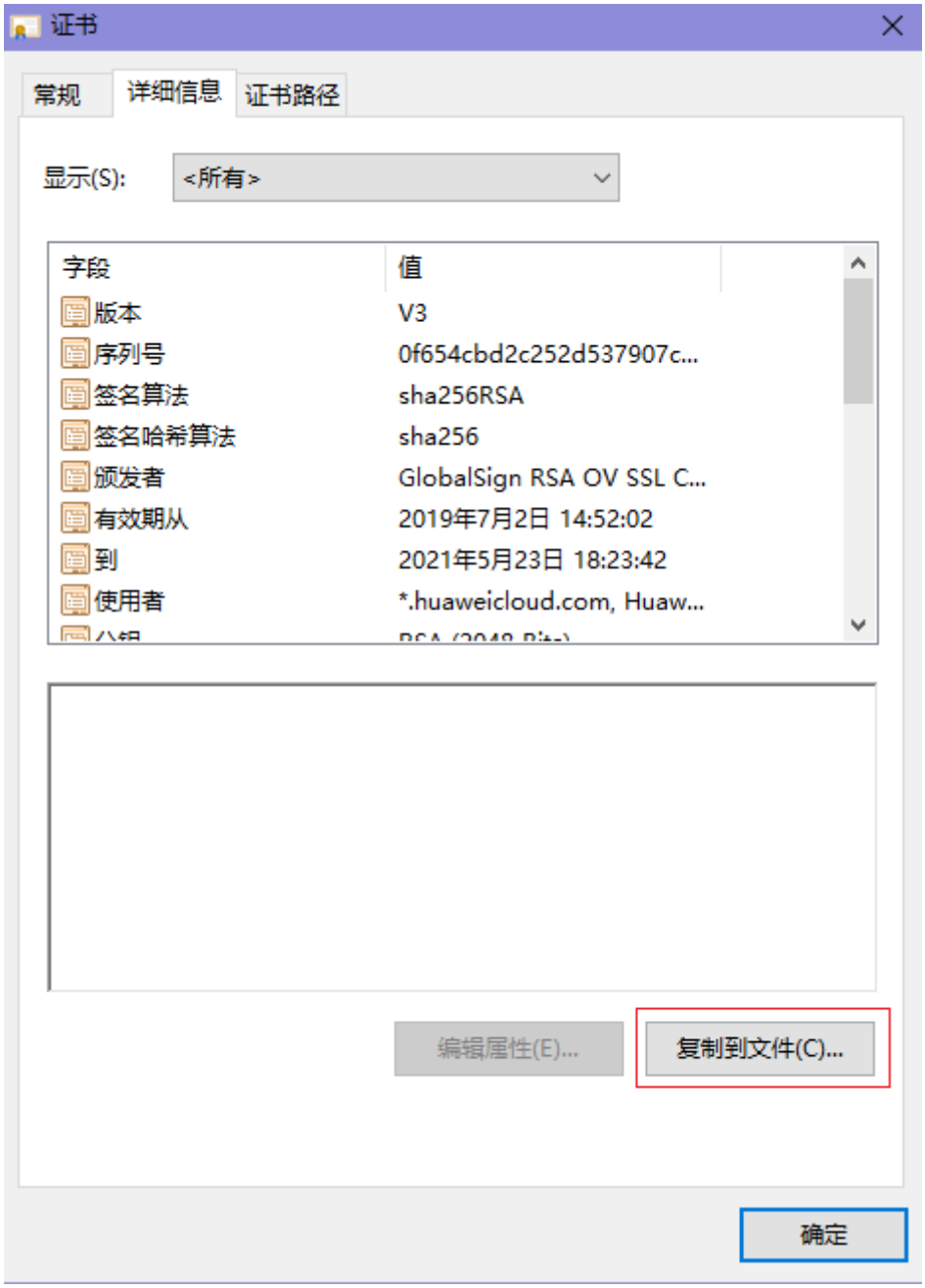
图 8-13 查看证书链



步骤3 逐一将证书另存到本地。

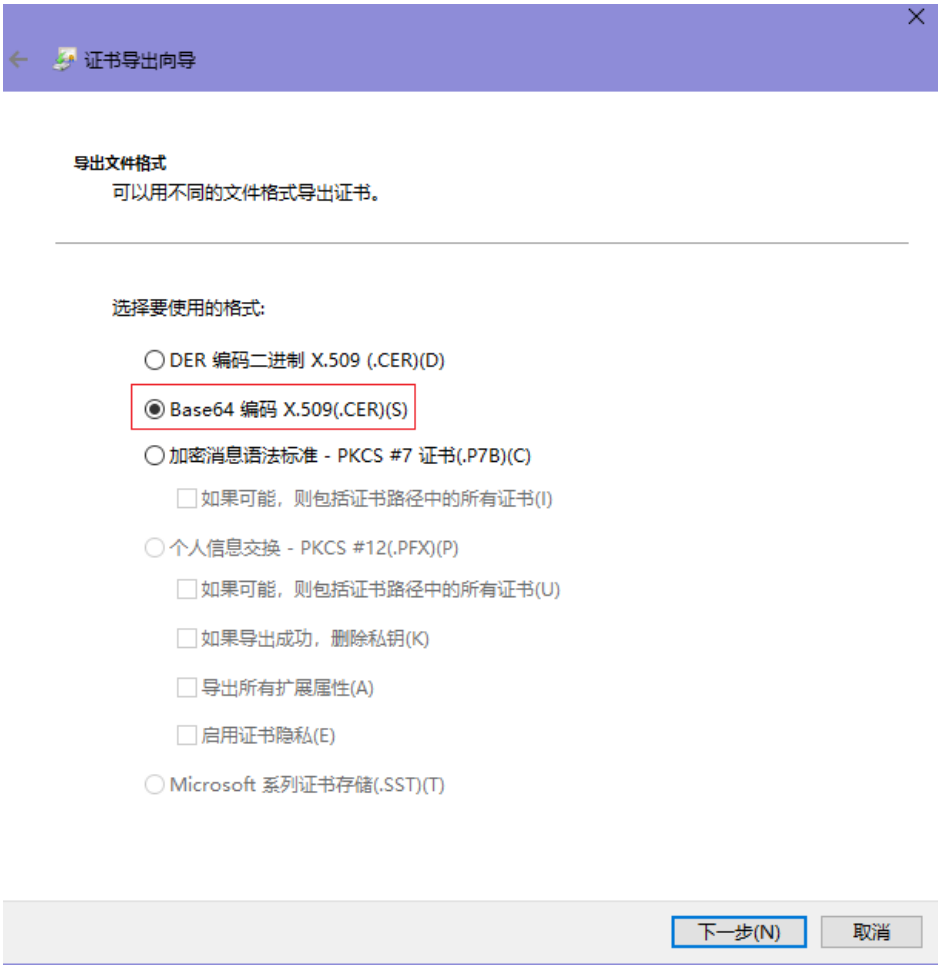
1. 选中证书名称，单击“详细信息”页签，如图8-14所示。

图 8-14 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8-15所示。

图 8-15 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8-16重组证书顺序，完成证书重构。

图 8-16 证书重构

步骤5 **重新上传证书。**

----结束

8.5.6 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	1. 执行以下命令，分别查看证书和私钥文件的MD5值：
	`openssl x509 -noout -modulus -in <证书文件>|openssl md5`
	`openssl rsa -noout -modulus -in  <私钥文件>|openssl md5`
	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	1. 执行以下命令，生成一个新的私钥： `openssl rsa -in <私钥文件> -out <新私钥文件>` 2. 重新上传私钥。

相关操作

- 如何解决证书链不完整?
- 如何解决HTTPS请求在部分手机访问异常?

8.5.7 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。

8.5.8 使用 WAF 后如何处理网站的文件不能上传?

将网站接入WAF后，网站的文件上传请求限制为10G 。

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

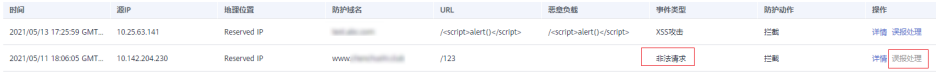
- 直接通过IP上传。
- 使用没有被WAF防护的域名上传。
- 采用ftp协议上传。

8.5.9 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8-17所示。

图 8-17 非法请求被 WAF 拦截



可能原因

当遇到以下情况时，WAF将判定该访问请求为非法请求并拦截该访问请求：

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

处理建议

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

8.5.10 如何放行云模式 WAF 的回源 IP 段?

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

须知

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

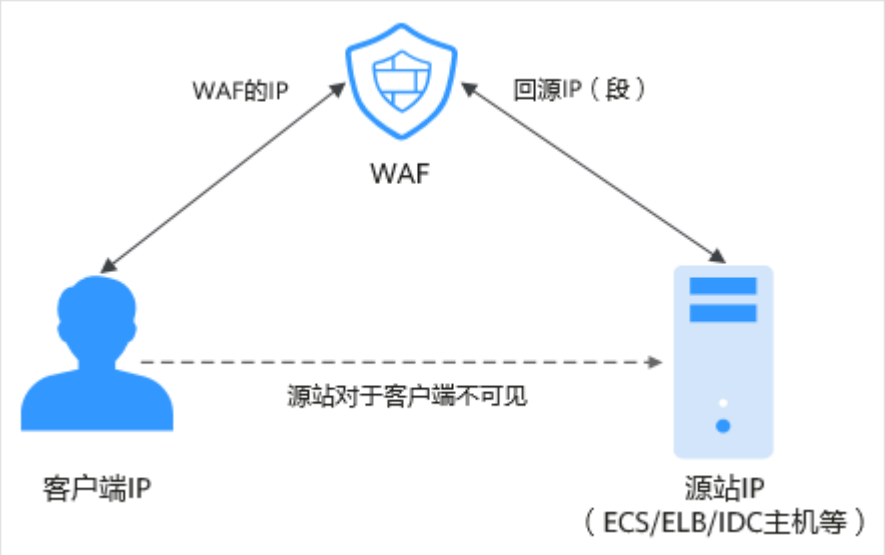
什么是回源 IP?

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

说明

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

图 8-18 回源 IP



回源 IP 检测机制

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

为什么需要放行回源 IP 段?

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

说明

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

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

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

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

步骤7 打开源站服务器上的安全软件，将复制的IP段添加到白名单。

----结束

8.5.11 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。

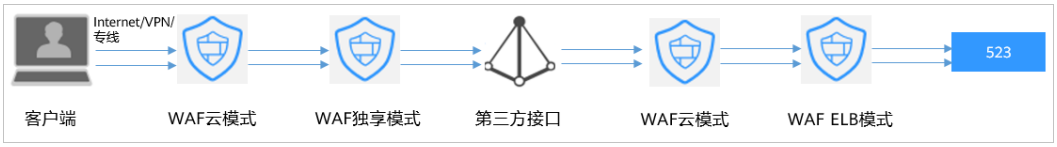
  在域名的基本信息页面，开启“超时配置”并单击，设置“连接超时”、“读超时”、“写超时”的时间，并单击保存设置。

8.5.12 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。

8.5.13 如何处理 523 错误码问题?

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

防止删除网站后造成业务中断，在删除网站前，需要完成以下操作:

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

----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。

8.5.14 如何处理域名接入 WAF 后，登录首页不停地刷新?

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

8.5.15 如何解决 HTTP 配置转发策略后程序访问页面卡顿?

如果HTTP配置转发策略后程序访问页面卡顿，请添加HTTP到HTTP和HTTPS到HTTPS这2条转发协议规则。

有关配置转发规则的详细操作，请参见**如何解决重定向次数过多?** 。

8.5.16 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8-19**所示。

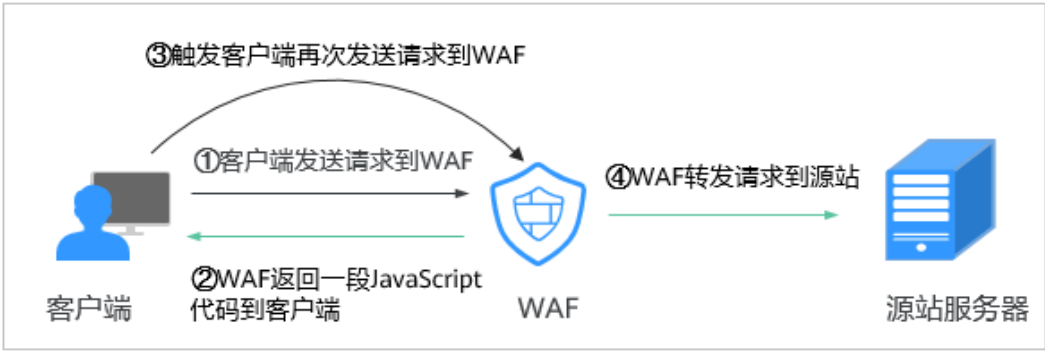
图 8-19 提示“414 Request-URI Too Large”错误

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8-20所示。

图 8-20 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)”。

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“网站反爬虫设置”，进入网站反爬虫规则配置页面。

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。

----结束

8.5.17 如何处理“协议不受支持，客户端和服务器不支持一般 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，客户端和服务器不支持一般 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。

8.5.18 访问独享引擎页面时提示“IAM 未授权”？

问题现象

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

可能的原因

登录账号未授予“IAM ReadOnly”权限。

处理办法

为您的账号授予“IAM ReadOnly”权限。

8.5.19 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”。

8.6 防护规则配置

8.6.1 Web 基础防护类

8.6.1.1 如何将 Web 基础防护的仅记录模式切换为拦截模式?

本节介绍如何将Web基础防护的仅记录模式切换为拦截模式。

执行以下操作完成Web基础防护的防护模式切换：

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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，选择“拦截”模式。

须知

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

----结束

8.6.1.2 Web 基础防护支持设置哪几种防护等级?

Web基础防护设置了三种防护等级：“宽松”、“中等”、“严格”，默认为“中等”。防护等级相关说明如表8-9所示。

表 8-9 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。

8.6.2 CC 攻击防护规则类

8.6.2.1 CC 攻击的防护峰值是多少?

各版本对应的CC攻击防护峰值如表8-10所示。

表 8-10 适用的业务规格

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： ● 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 **须知** 极限值为实验室测试值，高敏感业务请以实际业务测试数据为准。实际QPS与业务请求数据大小、自定义防护规则种类及数量相关
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

8.6.2.2 如何配置 CC 防护规则?

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

用户可根据业务类型，配置CC防护规则，可配置以下内容：

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

8.6.2.3 在什么情况下使用 Cookie 区分用户?

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

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

8.6.2.4 CC 规则里“限速频率”和“放行频率”的区别?

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

请求，一旦在60秒内访问请求超过10次，WAF就直接阻断该Web访问者访问目标URL。

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

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

区别

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

8.6.3 精准访问规则类

8.6.3.1 精准访问防护规则可以设置在指定的时间段生效吗?

WAF支持精准防护访问规则在指定的时间段生效。

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

8.6.3.2 精准访问防护规则添加的路径中带有#能匹配吗?

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

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

8.6.3.3 如何不拦截带有.js 的文件?

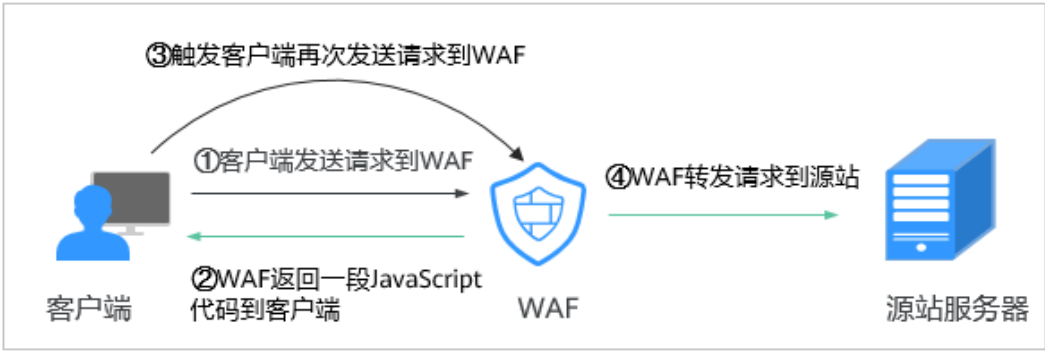
您可以通过WAF的精准访问防护规则配置放行路径后缀为.js的条件，具体配置如下：

8.6.4 网站反爬虫类

8.6.4.1 开启 JS 脚本反爬虫后，为什么客户端请求获取页面失败?

开启JS脚本反爬虫后，当客户端发送请求时，WAF会返回一段JavaScript代码到客户端。如果客户端是正常浏览器访问，就可以触发这段JavaScript代码再发送一次请求到WAF，即WAF完成JS验证，并将该请求转发给源站，如图8-21所示。

图 8-21 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。

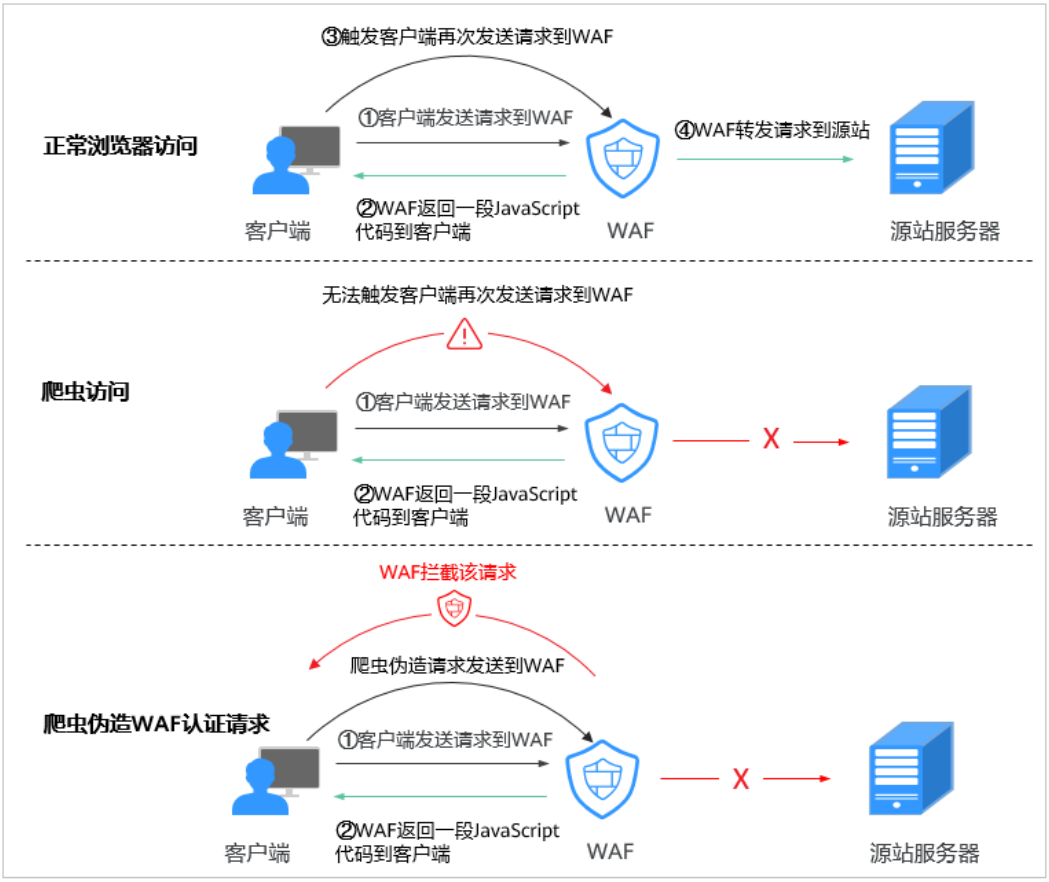
8.6.4.2 开启网站反爬虫中的“其他爬虫”会影响网页的浏览速度吗?

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

8.6.4.3 JS 脚本反爬虫的检测机制是怎么样的?

JS脚本检测流程如图8-22所示，其中，①和②称为“js挑战”，③称为“js验证”。

图 8-22 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8-23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 8-23 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。

8.6.5 其他类

8.6.5.1 哪些情况会造成 WAF 配置的防护规则不生效?

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

8.6.5.2 是否可以导出/备份 WAF 的配置?

当前WAF的配置，不支持导出和备份功能。

8.6.5.3 Web 应用防火墙支持哪些工作模式和防护模式?

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

WAF支持以下几种工作模式：

- 开启防护
- 暂停防护

WAF防护规则支持的防护模式说明如表8-11所示。

表 8-11 支持的防护模式说明

防护规则	防护模式
Web基础防护规则	• 拦截 • 仅记录

防护规则	防护模式
CC攻击防护规则	• 人机验证 • 阻断 • 动态阻断 • 仅记录
精准访问防护规则	• 阻断 • 放行 • 仅记录
黑白名单规则	• 拦截 • 放行 • 仅记录
地理位置访问控制规则	• 拦截 • 放行 • 仅记录
网站反爬虫规则	特征反爬虫支持以下防护动作： • 拦截 • 仅记录

8.6.5.4 系统自动生成策略包括哪些防护规则?

在添加防护网站进行“策略配置”时，您可以选择已创建的防护策略或默认的“系统自动生成策略”，系统自动生成的策略相关说明如表8-12所示。

须知

标准版只能选择“系统自动生成策略”。

您也可以在域名接入后根据防护需求配置防护规则。

表 8-12 系统自动生成策略说明

版本	防护策略	策略说明
云模式	Web基础防护（“仅记录”模式、常规检测）	仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。

版本	防护策略	策略说明
独享模式	Web基础防护（“仅记录”模式、常规检测）	仅记录SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击行为。
	网站反爬虫（“仅记录”模式、扫描器）	仅记录漏洞扫描、病毒扫描等Web扫描任务，如OpenVAS、Nmap的爬虫行为。

说明

“仅记录”模式：发现攻击行为后WAF只记录攻击事件不阻断攻击。

8.6.5.5 Web 应用防火墙支持哪些防护规则?

Web应用防火墙支持的防护规则如表8-13所示。

表 8-13 可配置的防护规则

防护规则	说明
Web基础防护规则	覆盖OWASP（Open Web Application Security Project，简称OWASP）TOP 10中常见安全威胁，通过预置丰富的信誉库，对恶意扫描器、IP、网马等威胁进行检测和拦截。
CC攻击防护规则	可以自定义CC防护规则，限制单个IP/Cookie/Referer访问者对您的网站上特定路径（URL）的访问频率，WAF会根据您配置的规则，精准识别CC攻击以及有效缓解CC攻击。
精准访问防护规则	精准访问防护策略可对HTTP首部、Cookie、访问URL、请求参数或者客户端IP进行条件组合，定制化防护策略，为您的网站带来更精准的防护。
黑白名单规则	配置黑白名单规则，阻断、仅记录或放行指定IP的访问请求，即设置IP黑/白名单。
攻击惩罚规则	当恶意请求被拦截时，可设置自动封禁访问者一段时间，该功能和其他规则结合使用。
地理位置访问控制规则	针对指定国家、地区的来源IP自定义访问控制。
网页防篡改规则	当用户需要防护静态页面被篡改时，可配置网页防篡改规则。
网站反爬虫规则	动态分析网站业务模型，结合人机识别技术和数据风控手段，精准识别爬虫行为。

防护规则	说明
防敏感信息泄露规则	该规则可添加两种类型的防敏感信息泄露规则： ● 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。

8.6.5.6 Web 应用防火墙的哪些防护规则支持仅记录模式?

WAF的Web基础防护规则支持“仅记录”模式。

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

8.6.5.7 开启网页防篡改后，为什么刷新页面失败?

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

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“安全 > Web应用防火墙 (独享)”。

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。

- 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

8.6.5.8 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8-14**所示。

表 8-14 黑白名单规则和精准访问防护规则区别

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

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

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

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

A 修订记录

发布日期	修改说明
2023-10-30	第六次正式发布。 ● 架构调整。 ● 增加： – 开启全量日志 – 通过LTS快速查询分析WAF访问日志 – 通过LTS实时分析Spring core RCE漏洞的拦截情况 – 通过LTS配置WAF规则的拦截告警 – 云模式WAF提供的解析地址是固定IP吗? – 源站IP更改后是否会改变CNAME值? – 更换IP后，需要重新将域名添加到WAF吗? – 如何不拦截带有.js的文件? ● 修改： – 步骤二：配置负载均衡 – 配置PCI DSS/3DS合规与TLS配置TLS最低版本和加密套件 – 配置CC攻击防护规则（HC&HK&OCB） – 开启网站反爬虫配置网站反爬虫防护规则 – 安全总览 – 查看防护日志 – 管理独享引擎 – CC攻击防御最佳实践 – 独享引擎实例升级最佳实践
2023-06-15	第五次正式发布。 ● 修改“服务版本差异”：修改截图。 ● 补充相关截图。

发布日期	修改说明
2023-03-30	第四次正式发布。 ● 新增“最佳实践”章节。 ● 修改“什么是Web应用防火墙”：增加云服务原理图。 ● 增加“服务版本差异”章节。 ● 增加“WAF支持的端口”章节。 ● 增加“云审计服务支持的关键操作”章节。 ● 增加“个人数据保护机制”章节。 ● 增加以下常见问题： – Web应用防火墙攻击防护类问题 – Web应用防火墙可以拦截multipart/form-data格式的数据包吗? – 独享版WAF是否支持跨VPC防护? – WAF转发和Nginx转发有什么区别? – Web应用防火墙支持自定义POST拦截吗? – Web应用防火墙有IPS入侵防御系统模块吗? – HTTP 2.0业务接入WAF防护是否会对源站有影响? – WAF是否可以防护Apache Struts2远程代码执行漏洞（CVE-2021-31805）? – 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? – Web应用防火墙如何拦截请求内容? – 如果证书挂载在ELB上，WAF可以根据请求内容进行拦截吗? – 接入WAF对现有业务和服务器运行有影响吗? – 仅放行通过WAF的访问请求，如何配置? – 为什么Cookie中有HWWAFSESID或HWWAFSESTIME字段? – 网站部署了反向代理服务器，如何配置WAF? – 源站IP地址服务器更换安全组后，在WAF中需要做更改吗? – Web应用防火墙支持哪些非标准端口? – 独享模式如何防护不支持的非标准端口? – 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? – 添加域名时，端口需要和源站端口配置一样吗? – 多个端口的服务器，如果某个端口不需要WAF防护，如何处理? – 删除防护域名时应该注意哪些事项? – ELB已上传的证书，在Web应用防火墙上需要重新导入上传吗?

发布日期	修改说明
	– 如何配置对外协议与源站协议? – 添加域名时，为什么不能选择对外协议? – 云模式服务器的源站地址可以配置成CNAME吗? – 域名接入Web应用防火墙后，能通过IP访问网站吗? – 域名/IP接入状态显示“未接入”，如何处理? – WAF误拦截了“非法请求”访问请求，如何处理? – 连接超时时长是多少，是否可以手动设置该时长? – 如何解决重定向次数过多? – 如何处理域名接入WAF后，登录首页不停地刷新? – 如何解决HTTP配置转发策略后程序访问页面卡顿? – 如何处理523错误码问题? – 防护规则配置类的常见问题
2022-12-28	第三次正式发布。 ● 新增“独享模式 WAF”。 ● 新增“监控指标”章节。 ● 新增“权限管理”章节。 ● “常见问题”调整架构并新增若干常见问题。
2022-05-06	第二次正式发布。 修改“概述”章节：增加WAF的计费模式和带宽说明。
2021-07-14	第一次正式发布。

