Web 应用防火墙

最佳实践

文档版本 71

发布日期 2024-05-09

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 Solution as Code 一键式部署类最佳实践

为帮助企业高效上云，华为云Solution as Code萃取丰富上云成功实践，提供一系列基于华为云可快速部署的解决方案，帮助用户降低上云门槛。同时开放完整源码，支持个性化配置，解决方案开箱即用，所见即所得。

表 1-1 Solution as Code 一键式部署类最佳实践汇总

场景类型	一键式部署方案	说明	相关服务
网站防护	Web网站基础安全防护	帮助企业网站业务流量进行多维度检测和防护，全面避免网站被黑客恶意攻击和入侵。	WAF、ECS、EIP
	防勒索病毒安全解决方案	该解决方案能帮您为华为云上部署的服务器提供事前安全加固、事中主动防御、事后备份恢复的防勒索病毒方案，抵御勒索软件入侵，营造主机资产安全运行环境。	WAF、HSS、SMN
等保	等保二级解决方案	该解决方案能帮您在华为云上快速部署等保二级合规解决方案，帮助客户快速、低成本完成安全整改，轻松满足等保二级合规要求。	WAF、CFW、HSS、SCM、SA、MTD
	等保三级解决方案	该解决方案依托华为云自身安全能力与安全合规生态，为用户提供一站式的等保三级安全解决方案	WAF、HSS、SCM、SA、MTD、CFW、CBH、DBS、CodeArts Inspector

2 WAF 云模式接入配置

2.1 准备阶段

将网站域名接入华为云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 2-1 网站业务梳理

梳理项	说明
网站和业务信息	
网站/应用业务每天的流量峰值情况，包括Mbps、QPS	判断风险时间点，并且可作为WAF实例的业务带宽和业务QPS规格的选择依据。 **说明** 如果您选择的QPS规格不足以支撑网站/应用业务每天的流量峰值，对超出当前WAF版本支持峰值的QPS，WAF将不再防护网站，QPS将直接透传到源站，影响网站/应用业务的防护。
业务的主要用户群体（例如，访问用户的主要来源地区）	判断非法攻击来源，后续可使用地理位置访问控制功能屏蔽非法来源地区。
业务是否为C/S架构	如果是C/S架构，进一步明确是否有App客户端、Windows客户端、Linux客户端、代码回调或其他环境的客户端。
源站部署的具体位置	判断购买哪种实例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。

梳理项	说明
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 **说明** 如果防护域名使用非标准端口，请查看**WAF支持哪些非标准端口?**，确保购买的WAF版本支持防护该非标准端口。
业务是否使用TLS 1.0或弱加密套件	判断业务使用的加密套件是否支持。
业务在接入WAF前，是否已接入DDoS高防、CDN等服务。	接入WAF时，判断如何选择“是否已使用代理”，以及正确进行域名解析。
（针对HTTPS业务）客户端是否支持SNI标准	对于支持HTTPS协议的域名，接入WAF后，客户端和服务端都需要支持SNI标准。
业务交互过程	了解业务交互过程、业务处理逻辑，便于后续配置针对性防护策略。
活跃用户数量	便于后续在处理紧急攻击事件时，判断事件严重程度，以采取风险较低的应急处理措施。
业务及攻击情况	
业务类型及业务特征（例如，游戏、棋牌、网站、App等业务）	便于在后续攻击防护过程中分析攻击特征。
单用户、单IP的入方向流量范围和连接情况	帮助后续判断是否可针对单个IP制定限速策略。
用户群体属性	例如，个人用户、网吧用户、或通过代理访问的用户。
业务是否遭受过大流量攻击、攻击类型和最大的攻击流量峰值	判断是否需要增加DDoS防护服务，并根据攻击流量峰值判断需要的DDoS防护规格。

梳理项	说明
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

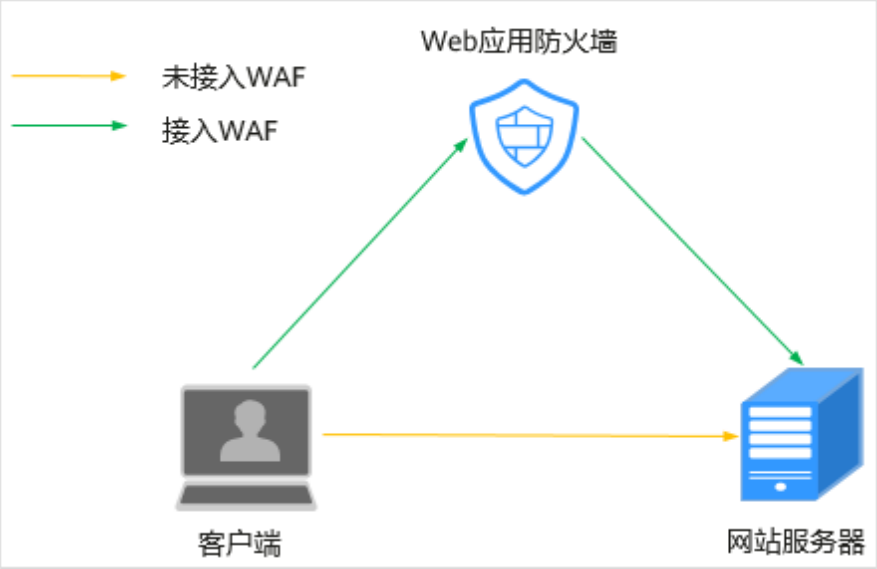
- 已将域名信息（源站服务器的IP、端口等信息）以“云模式-CNAME接入”的方式添加到WAF。
- 具有网站DNS域名解析管理员的账号，用于修改DNS解析记录将网站流量切换至WAF。
- 推荐在将网站业务接入前，完成压力测试。
- 检查网站业务是否已有信任的访问客户端（例如监控系统、通过内部固定IP或IP段调用的API接口、固定的程序客户端请求等）。在将业务接入后，需要将这些信任的客户端IP加入白名单。

2.2 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 2-1 未使用代理配置原理图



前提条件

- 已有网站域名。
- 已**购买WAF**。
- 已将网站信息（源站服务器的IP、端口等信息）**添加到WAF**。
- 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非华为云安全软件（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。

有关DNS云解析服务的记录集类型和规则的详细介绍，请参见**记录集类型及配置规则**。

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。

以下操作以华为云云解析DNS为例介绍修改域名CNAME解析记录的方法。如果您的域名的DNS解析托管在华为云云解析DNS上，您可以直接参照以下步骤进行操作；若您使用华为云以外的DNS服务，请参考以下步骤在域名的DNS服务商的系统上进行类似配置。

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“安全与合规 > Web应用防火墙 WAF”。
3. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
4. 在目标域名所在行中，单击目标域名名称，进入域名基本信息页面。

图 2-2 查看基本信息

5. 在“CNAME”信息行，单击，复制“CNAME”值。

步骤2 域名解析。

1. 进入云解析页面的入口，如图2-3所示。

图 2-3 云解析页面入口

2. 在目标域名所在行的“操作”列，单击“修改”，进入“修改记录集”页面。
3. 在弹出的“修改记录集”对话框中修改记录值，如图2-4所示。
   - “主机记录”：在WAF中配置的域名。
   - “类型”：选择“CNAME-将域名指向另外一个域名”。
   - “线路类型”：全网默认。
   - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
   - “值”：修改为已复制的WAF CNAME地址。
   - 其他的设置保持不变。

说明

关于修改解析记录：

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

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

图 2-4 修改记录集

4. 单击“确定”，完成DNS配置，等待DNS解析记录生效。

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

3 网站防护最佳实践

当您首次完成网站接入，面对网站防护策略配置时，可能会不知道如何下手。本文将引导您从不同场景、角色的视角快速熟悉Web应用防火墙（Web Application Firewall，简称WAF）的防护规则，帮助您从自己最关心的需求入手，了解WAF的防护逻辑。

前提条件

- **已完成网站接入**。
- 您所购买的WAF版本，支持相应的防护功能。WAF各版本之间的功能特性差异请参见**各版本支持的功能特性**。

概述

本文从以下不同角色视角或业务需求视角出发，提供了网站防护的设置建议。您可以选择最贴近您自身实际需求的场景，了解相关的防护设置：

- **我是新手，不懂安全，也没有特殊需求**
- **我是专业的安全人员，需要做全面的Web入侵运营**
- **我的业务需要严格的安全防护，有攻击时宁可错杀不可漏掉**
- **我的业务经常受到爬虫骚扰或面临数据泄露、被篡改的风险**

我是新手，不懂安全，也没有特殊需求

您可能是基于等保要求或出于提升企业安全水位（达到预防目的）等考虑购买了Web应用防火墙。这种情况下，您可以在完成网站接入后直接使用WAF的默认基础防护设置，不做任何调整。WAF提供的默认防护能力足够为网站抵御绝大部分的基础Web威胁。

建议您多关注Web应用防火墙控制台的“安全总览”和“防护事件”页面，了解业务情况和攻击情况。具体操作可参见以下文档：

- **安全总览**
- **查看防护日志**

我是专业的安全人员，需要做全面的 Web 入侵运营

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

- **Web基础防护**：帮助您防范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，并支持深度反逃逸识别、对请求里header中所有字段进行攻击检测、Shiro解密检测、Webshell检测。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“Web基础防护”区域，选择“拦截”或者“仅记录”模式，开启所有的检测项。具体的操作请参见**配置Web基础防护规则**。
- **自定义防护策略（自由组合防护配置规则）**：防护配置规则的自由组合配置，为您的网站定制适合的防护策略，全方位的防护您的网站。

  操作导航：在“防护策略”页面，进行相关的配置，具体的操作请参见**防护配置引导**。

我的业务需要严格的安全防护，有攻击时宁可错杀不可漏掉

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

- **Web基础防护（拦截模式）**：帮助您防范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，并支持深度反逃逸识别、对请求里header中所有字段进行攻击检测、Shiro解密检测、Webshell检测。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“Web基础防护”区域，选择“拦截”模式，开启所有的检测项。具体的操作请参见**配置Web基础防护规则**。
- **CC攻击防护（阻断模式）**：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，精准识别并阻断CC攻击。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“CC攻击防护”区域，添加规则，“防护动作”配置为“阻断”。具体的操作请参见**配置CC攻击防护规则**。
- **精准访问防护（阻断模式）**：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。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“精准访问防护”区域，添加规则，“防护动作”配置为“阻断”。具体的操作请参见**配置精准访问防护规则**。
- **IP黑白名单设置（拦截模式）**：封禁与业务不相关的IP地址和地址段。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“黑白名单设置”区域，添加规则，“防护动作”配置为“拦截”。具体的操作请参见**配置IP黑白名单规则**。
- **地理位置访问控制（拦截模式）**：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。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“地理位置访问控制”区域，添加规则，“防护动作”配置为“拦截”。具体的操作请参见**配置地理位置访问控制规则**。

我的业务经常受到爬虫骚扰或面临数据泄露、被篡改的风险

针对您的需求，推荐您在完成网站接入后，为网站设置以下防护功能：

- **网页防篡改**：帮助您锁定需要保护的网站页面，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。

操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“网页防篡改”区域，添加规则，完成相关设置。具体操作请参见**配置网页防篡改规则**。

- **防敏感信息泄露**：帮助您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。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“防敏感信息泄露”区域，添加规则，完成相关设置。具体操作请参见**配置防敏感信息泄露规则**。

- **网站反爬虫**：
  - **特征反爬虫**：帮助您为网站放行合法爬虫（例如Googlebot、Baiduspider）的访问请求，或者拦截大多数脚本和自动化程序的爬虫攻击。
  - **JS脚本反爬虫**：开启JS脚本反爬虫后，帮助您完成JS脚本的的检测，您也可以自定义JS脚本反爬虫的防护策略。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“网站反爬虫”区域，添加规则，完成相关设置。具体操作请参见**配置网站反爬虫防护规则**。

- **威胁情报访问控制**：提供IDC机房IP库平台（例如鹏博士、谷歌公司、腾讯、美团网等其他平台），当目标IP库平台内的来源IP向网站下任意路径发起访问请求时，将触发控制规则，即拦截、放行或者仅记录请求。

  操作导航：在“防护策略”页面，单击策略名称，进入“防护配置”页面，选择“威胁情报访问控制”区域，添加规则，完成相关设置。具体操作请参见**配置威胁情报访问控制**。

4 Web 漏洞防护最佳实践

4.1 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 **购买WAF**。

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

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

图 4-1 Web 基础防护页面

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

4.2 Apache Dubbo 反序列化漏洞

2020年02月10日，华为云安全团队监测到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，华为云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，可以使用华为云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 **购买WAF**。

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

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

----结束

4.3 开源组件 Fastjson 拒绝服务漏洞

2019年09月03日，华为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，华为云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 **购买WAF**。

步骤2 将网站域名添加到WAF中并完成域名接入，详细的操作请参见**添加防护域名**。

步骤3 将Web基础防护的状态设置为“拦截”模式，具体方法请参见**配置Web基础防护规则**。

----结束

4.4 开源组件 Fastjson 远程代码执行漏洞

2019年07月12日，华为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

华为云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 **购买WAF**。

步骤2 将网站域名添加到WAF中并完成域名接入，详细的操作请参见**添加防护域名**。

步骤3 将Web基础防护的状态设置为“拦截”模式，具体方法请参见**配置Web基础防护规则**。

----结束

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

2019年04月17日，华为云应急响应中心检测到国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）发布的Oracle WebLogic wls9-async组件安全公告。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4-2**和**图4-3**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。精准访问防护规则的具体配置方法请参见**配置精准访问防护规则**。

图 4-2 async 配置

图 4-3 wls-wsat 配置

5 防护策略配置

5.1 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 单击管理控制台左上角的，选择区域或项目。

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

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

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

步骤6 在“Web基础防护”配置框中，查看Web应用攻击防护的防护状态。

图 5-1 Web 基础防护配置框

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7 进入“Web基础防护”界面。

图 5-2 Web 基础防护

- “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 5-1 防护等级说明

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

防护等级	说明
严格	防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求。 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，如图5-4所示。

图 5-3 SQL 攻击拦截

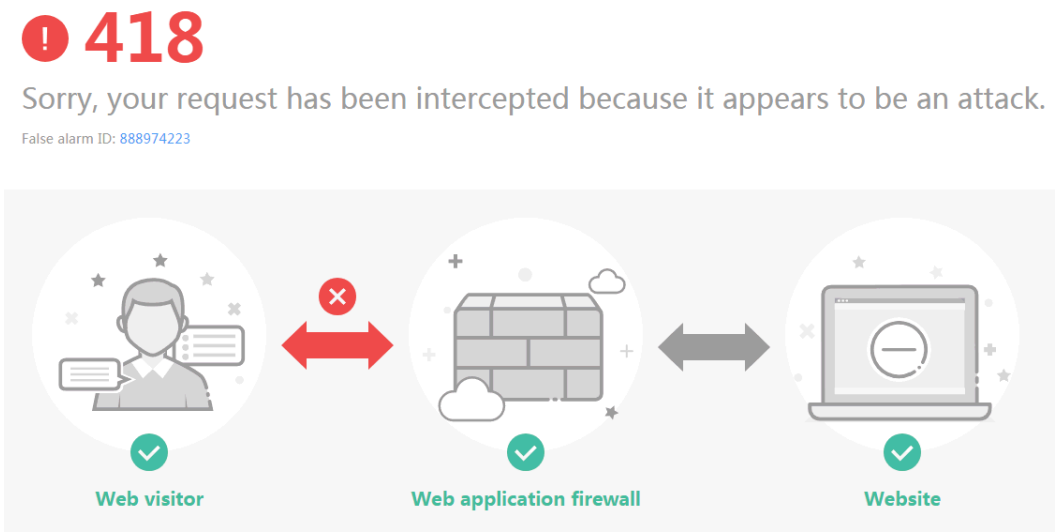
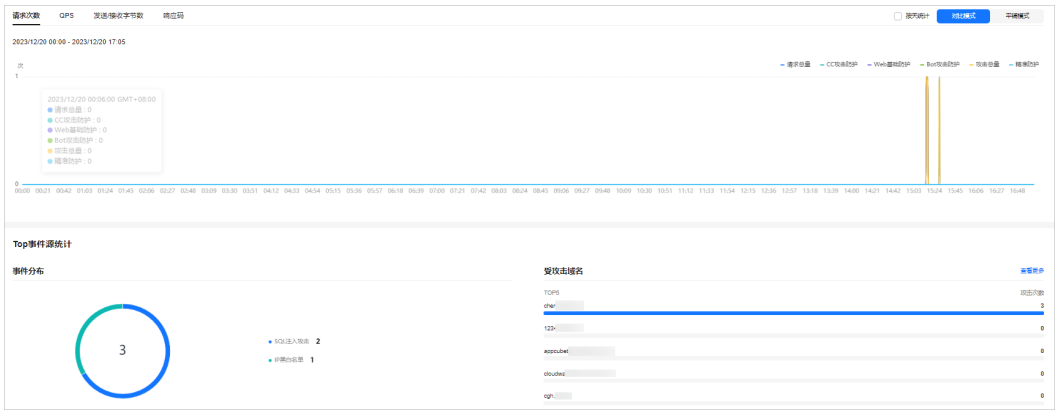


图 5-4 安全统计



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。同时，在攻击事件的“操作”列，单击“详情”，可以查看具体的攻击信息。

5.2 CC 攻击防御最佳实践

5.2.1 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。

如何判断网站是否遭受 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。

5.2.2 CC 攻击常见场景防护配置

本文介绍了基于Web应用防火墙的相关功能给出具体的CC攻击场景的防护策略，帮助您有针对性的防御CC攻击。

概述

您可以从以下不同的CC攻击防护场景中选择贴近您自身实际需求的场景，了解相关的防护设置：

- **大流量高频CC攻击**
- **攻击源来自海外或IDC机房IP**

- 请求特征畸形或不合理

大流量高频 CC 攻击

在大规模CC攻击中，单台傀儡机发包的速率往往远超过正常用户的请求频率。针对这种场景，直接对请求源IP设置限速规则是最有效的办法。建议您使用CC攻击的基于IP限速的模式，具体请参见**基于IP限速的配置**。

配置示例：您可以配置以下CC规则，当一个IP在30秒内访问当前域名下任意路径的次数超过1000次，则封禁该IP的请求10个小时。该规则可以作为一般中小型站点的预防性配置。

在实际场景中，您需要根据自身业务需求调整限速模式和触发防护的限速频率，并选择合适的防护动作，以达到更有针对性、更精细化的防护效果。例如，为了预防登录接口受到恶意高频撞库攻击的影响，您可以配置路径（示例：使用“前缀为”逻辑符，将匹配内容设置为/login.php）。

说明

- “域名聚合统计”：开启后，泛域名对应的所有子域名的请求次数合并限速(不区分访问IP)。例如，配置的泛域名为“*.a.com”，会将所有子域名（b.a.com，c.a.com等）的请求一起聚合统计。
- “全局计数”：仅云模式支持配置该参数。默认为每WAF节点单独计数，开启后本区域所有节点合并计数。

攻击源来自海外或 IDC 机房 IP

CC攻击中很大比例的攻击来源于海外IP和IDC机房IP的情形。

对于面向中国用户的网站，在遭受攻击时可以通过封禁海外访问来缓解攻击压力。推荐您使用WAF的地理位置访问控制功能，封禁中国境外IP地址的访问，具体操作请参见**配置地理位置访问控制规则**。

如果您已经开启了WAF的**威胁情报访问控制**规则，可以封禁常见IDC库的爬虫IP，例如华为、腾讯。详细操作请参见**配置威胁情报访问控制**。

须知

威胁情报访问控制功能现处于公测阶段，如需使用请**提交工单**申请开通。

请求特征畸形或不合理

由于很多CC攻击请求是攻击者随意构造的，仔细观察日志后，往往会发现这些请求有很多与正常请求不相符的畸形报文特征。常见的畸形报文特征及防护策略：

以下的防护配置是通过WAF的**精准访问防护**规则实现的，具体的操作请参见**配置精准访问防护规则**。

- User-agent异常或畸形：例如，包含Python等自动化工具特征、明显格式错乱的UA（例如Mozilla///）、明显不合理的UA（例如www.example.com）。如果存在该请求特征，可以直接封禁请求。

  配置示例：拦截User-agent包含Mozilla///的内容

- User-agent不合理：例如，对于微信推广的H5页面，正常用户都应该通过微信发起访问，如果UA来自于Windows桌面浏览器（例如MSIE 6.0），则明显是不合理的。如果存在该请求特征，可以直接封禁请求。

  配置示例：拦截User-agent包含MSIE 6.0的内容

- Referer异常：例如，不带Referer或Referer固定且来自于非法站点，则可以封禁这种请求（访问网站首页或第一次访问页面的情形除外）。针对只能通过某个站内地址跳转访问的URL，您可以从Referer角度分析行为异常，决定是否封禁。

  配置示例：拦截不带Referer的请求

- Cookie异常：正常用户往往会在请求中带上属于网站本身业务集的一些cookie（第一次访问页面的情形除外）。很多情况下，CC攻击的报文不会携带任何cookie。您可以从这个角度出发，封禁不带cookie的访问请求。

  配置示例：拦截不带Cookie的请求

- 缺少某些HTTP Header：例如，针对一些业务中需要的认证头等，正常用户的请求会携带，而攻击报文则不会。

  配置示例：拦截Header不带authorization头的请求。

- 不正确的请求方法：例如，只有POST请求的接口被大量GET请求攻击，则可以直接封禁GET请求。

配置示例：拦截GET请求。

5.2.3 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。关于域名接入的具体操作请参见**添加防护域名**。
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” 。

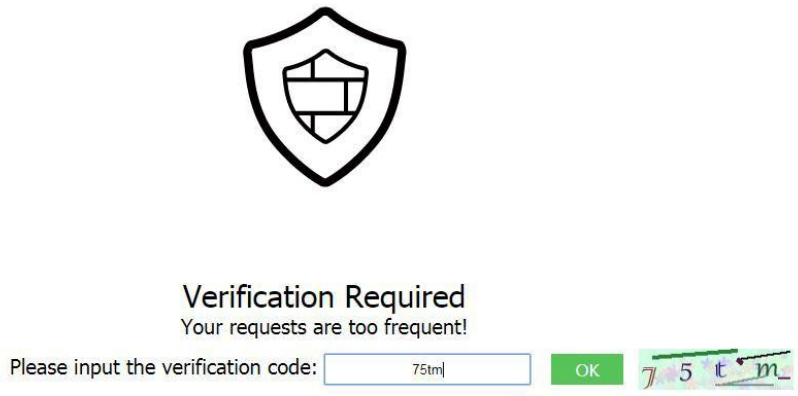
图 5-5 CC 防护规则配置框

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5-6**所示。

图 5-6 IP 限速

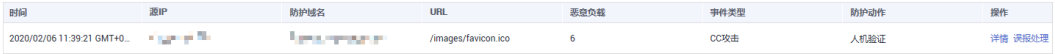
- 限速模式：选择“源限速”、“IP限速”，根据IP区分单个Web访问者。
- 限速频率：单个Web访问者在限速周期内可以正常访问的次数，如果超过该访问次数，Web应用防火墙服务将暂停该Web访问者的访问。
- 防护动作：防止误拦截正常用户，选择“人机验证”。
  - 人机验证：表示在指定时间内访问超过次数限制后弹出验证码，进行人机验证，完成验证后，请求将不受访问限制。
  - 阻断：表示在指定时间内访问超过次数限制将直接阻断。
  - 仅记录：表示在指定时间内访问超过次数限制将只记录不阻断。

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。

图 5-7 查看 CC 攻击事件日志



5.2.4 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。关于域名接入的具体操作请参见**添加防护域名**。
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”  。

   图 5-8 CC 防护规则配置框

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。

图 5-9 添加 CC 防护规则

- 限速模式：选择“源限速”、“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。
- “全局计数”：根据不同的限速模式，将已经标识的请求在一个或多个WAF节点上的计数聚合。默认为每WAF节点单独计数，开启后本区域所有节点合并计数。“IP限速”不能满足针对某个用户进行限速，需要选择“用户限速”或“其他”的Referer限速，此时标识的请求可能会访问到不同的WAF节点，开启全局计数后，将请求访问的一个或多个WAF节点访问量聚合，达到全局统计的目的。
- 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”。

5.2.5 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。

- 云模式添加域名的方法：**添加防护域名（云模式）**。
- 独享模式添加域名的方法：**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。

图 5-10 CC 防护规则配置框

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5-11**进行配置。

根据实际情况配置以下参数。

图 5-11 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。

- 云模式添加域名的方法：**添加防护域名（云模式）**。
- 独享模式添加域名的方法：**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”  。

图 5-12 CC 防护规则配置框

图 5-13 CC 防护规则配置框

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5-14**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 5-14 HWWAFSESID 配置

步骤6 单击“确认”，完成配置。

----结束

5.3 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“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“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 。

图 5-15 Web 基础防护配置框

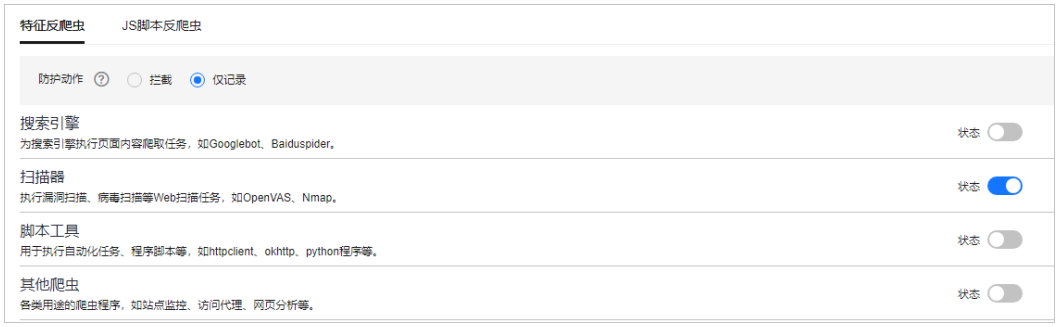
步骤7 在“防护配置”页面，开启“常规检测”和“Webshell检测”开关。

步骤8 选择“网站反爬虫”配置框，开启网站反爬虫。

- ：开启状态。
- ：关闭状态。

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。

图 5-16 特征反爬虫防护



----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“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在目标域名所在行的“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 选择“网站反爬虫”配置框，开启网站反爬虫。

- ：开启状态。
- ：关闭状态。

步骤7 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。

防护动作：拦截、仅记录、人机验证。

说明

人机验证：JavaScript挑战失败，弹出验证码提示，输入正确的验证码，请求将不受访问限制

须知

- JS脚本反爬虫依赖浏览器的Cookie机制、JavaScript解析能力，如果客户端浏览器不支持Cookie，此功能无法使用，开启后会造成永远无法访问源站。
- 如果您的业务接入了CDN服务，请谨慎使用JS脚本反爬虫。
  由于CDN缓存机制的影响，JS脚本反爬虫特性将无法达到预期效果，并且有可能造成页面访问异常。

步骤8 根据业务配置JS脚本反爬虫规则，相关参数说明如表5-2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。

- 除了指定请求规则以外，防护其他所有请求
  “防护模式”选择“防护所有请求”，单击“添加排除请求规则”，配置排除请求规则后，单击“确认”。

图 5-17 添加排除防护请求

- 只防护指定请求时

  “防护模式”选择“防护指定请求”，单击“添加请求规则”，配置请求规则后，单击“确认”。

图 5-18 添加请求规则

表 5-2 JS 脚本反爬虫参数说明

参数	参数说明	示例
规则名称	自定义规则名称。	waf
规则描述	可选参数，设置该规则的备注信息。	-
生效时间	立即生效。	立即生效

参数	参数说明	示例
条件列表	条件设置参数说明如下： • 字段：在下拉列表中选择需要防护的字段，当前仅支持“路径”、“User Agent”。 • 子字段 • 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”、“不包含任意一个”、“等于任意一个”、“不等于任意一个”、“前缀为任意一个”、“前缀不为任意一个”、“后缀为任意一个”或者“后缀不为任意一个”时，需要选择引用表。 • 内容：输入或者选择条件匹配的内容。 • 区分大小写：“字段”选择“路径”时，可配置该参数。开启后，系统在检测配置的路径时，将区分大小写。	“路径”包含“/admin/”
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优先级依次进行匹配，优先级较小的规则优先匹配。	5

----结束

开启该防护后，非浏览器的访问将不能获取业务页面。

```
</body>
</html>
[root@VM_0_9_centos ~]# curl http://cloudsecuritylab.tech/ --user-agent 'xpymep.exe'
<html>
<head>
<meta http-equiv="Server" content="HuaweiCloudWAF">
</head>
<body>
<noscript>
<h1><strong>Please Enable JavaScript and Cookie.</strong></h1>
</noscript>
<h1> <span id = "open_cookie"/> </h1>
<script type="text/javascript">
(function(t,a,c){"function"===typeof window.define&&window.define.amd?window.define(c):"undefined"!=
=typeof module&&module.exports?module.exports=c():a.exports?a.exports=c():a[t]=c()})("fe",this,funct
ion(){var t=function(a){if(!(this instanceof t))return new t(a);this.options=this.extend(a,{swfConta
inerId:"fingerprintjs2",swfPath:"flash/compiled/FontList.swf",detectScreenOrientation:!0,sortPlugins
For:[/palemoon/i],userDefinedFonts:[]});this.nativeForEach=Array.prototype.forEach;this.nativeMap=Ar
ray.prototype.map};
t.prototype={extend:function(a,c){if(null==a)return c;for(var b in a)null!=a[b]&&c[b]!==a[b]&&(c[b]=
a[b]);return c},get:function(a){var c=this,b={data:[],addPreprocessedComponent:function(a){var b=a.v
alue;"function"===typeof c.options.preprocessor&&(b=c.options.preprocessor(a.key,b));this.data.push(
{key:a.key,value:b})}},b=this.userAgentKey(b),b=this.languageKey(b),b=this.colorDepthKey(b),b=this.d
eviceMemoryKey(b),b=this.pixelRatioKey(b),b=this.hardwareConcurrencyKey(b),b=this.screenResolutionKe
y(b),
b=this.availableScreenResolutionKey(b),b=this.timezoneOffsetKey(b),b=this.platformKey(b),b=this.plug
```


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“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

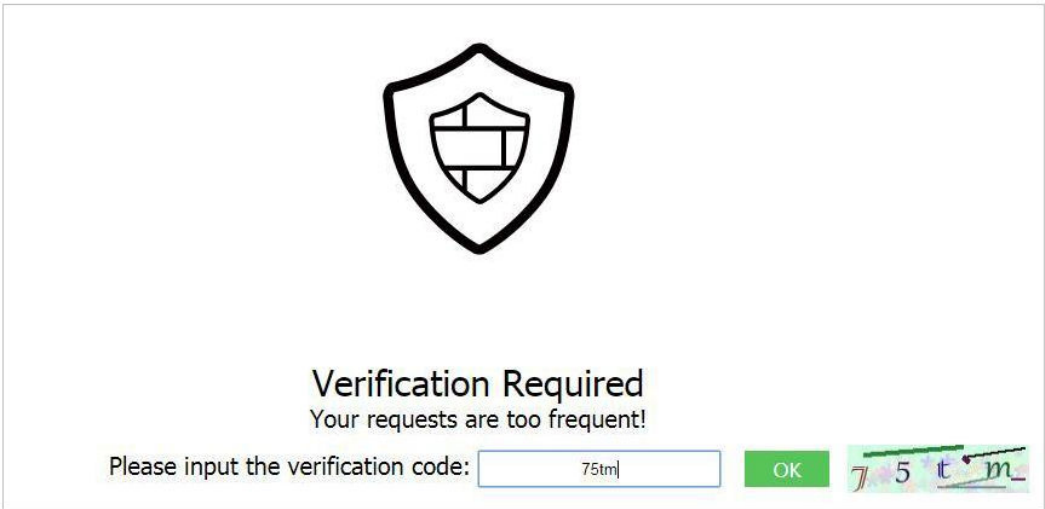
步骤5 在目标域名所在行的“防护策略”栏中，单击“已开启N项防护”，进入“防护策略”页面，确认“CC攻击防护”的“状态”为“开启”。

图 5-19 CC 防护规则配置框

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5-20所示。

图 5-20 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

5.4 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，您在华为云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。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域或项目。

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

步骤4 在左侧导航树中，选择“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。

图 5-21 防护事件列表

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 5-22 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“误报处理”。

步骤8 在弹出的对话框中，添加误报处理策略。

图 5-23 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。

相关操作

- **下载防护事件数据**

  您可以在“防护事件”的“下载”页面，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，在次日凌晨生成到防护事件数据csv文件。

- **配置全局白名单（原误报屏蔽）规则**

  针对某些规则ID或者事件类别进行忽略设置。例如，某URL不进行XSS的检查，可通过配置全局白名单规则，屏蔽XSS检查。

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5-3**所示。

表 5-3 检测项说明

检测项	说明
常规检测	防护SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等攻击。其中，SQL注入攻击主要基于语义进行检测。 **说明** 开启“常规检测”后，WAF将根据内置规则对常规检测项进行检测。
Webshell检测	防护通过上传接口植入网页木马。 **说明** 开启“Webshell检测”后，WAF将对通过上传接口植入的网页木马进行检测。
深度检测	防护同形字符混淆、通配符变形的命令注入、UTF7、Data URI Scheme等深度反逃逸。 **说明** 开启“深度检测”后，WAF将对深度反逃逸进行检测防护。
header全检测	默认关闭。关闭状态下WAF会检测常规存在注入点的header字段，包含User-Agent、Content-type、Accept-Language和Cookie。 **说明** 开启“header全检测”后，WAF将对请求里header中所有字段进行攻击检测。
Shiro解密检测	默认关闭。开启后，WAF会对Cookie中的rememberMe内容做AES，Base64解密后再检测。Web应用防火墙检测机制覆盖了几百种已知泄露密钥。 **说明** 如果您的网站使用的是Shiro 1.2.4及之前的版本，或者升级到了Shiro 1.2.5及以上版本但是未配置AES密钥，强烈建议您开启“Shiro解密检测”，以防攻击者利用已泄露的密钥构造攻击。

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5-4所示。

表 5-4 防护等级说明

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

防护等级	说明
严格	防护粒度最精细，可以拦截具有复杂的绕过特征的攻击请求。 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。

5.5 使用 Postman 工具模拟业务验证全局白名单规则

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

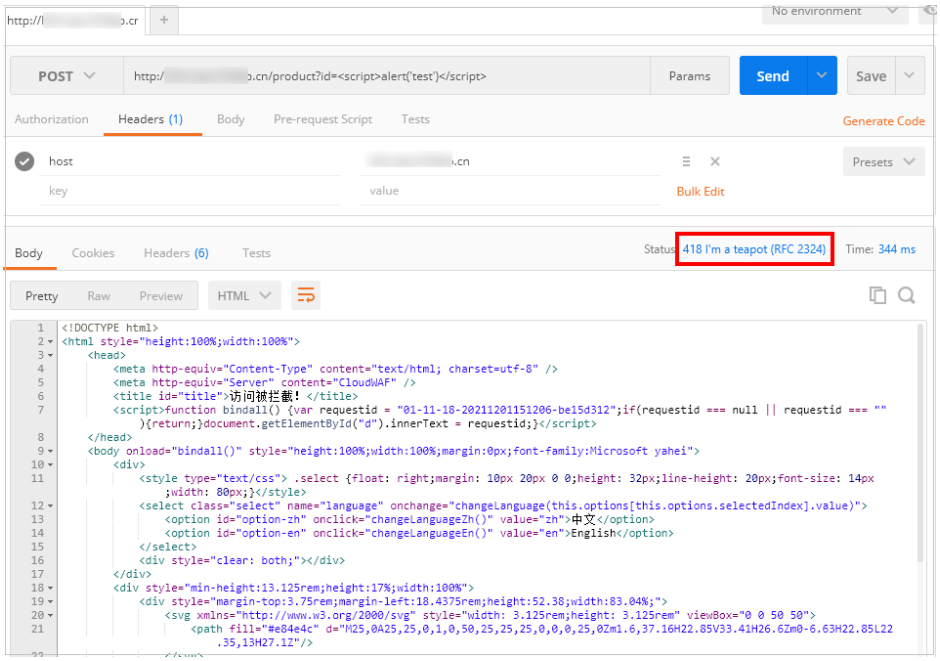
- 防护网站已成功接入WAF。
- 已开启“Web基础防护”，且防护模式为“拦截”。同时，“常规检测”已开启。

  有关配置Web基础防护的详细操作，请参见**配置Web基础防护规则**。

操作步骤

步骤1 **下载**并安装Postman。

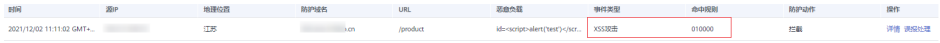
步骤2 在Postman上设置请求路径为“/product”，参数ID为普通测试脚本，防护网站的访问请求被拦截。



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“安全与合规 > Web应用防火墙 WAF”。
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。

   图 5-24 查看防护事件

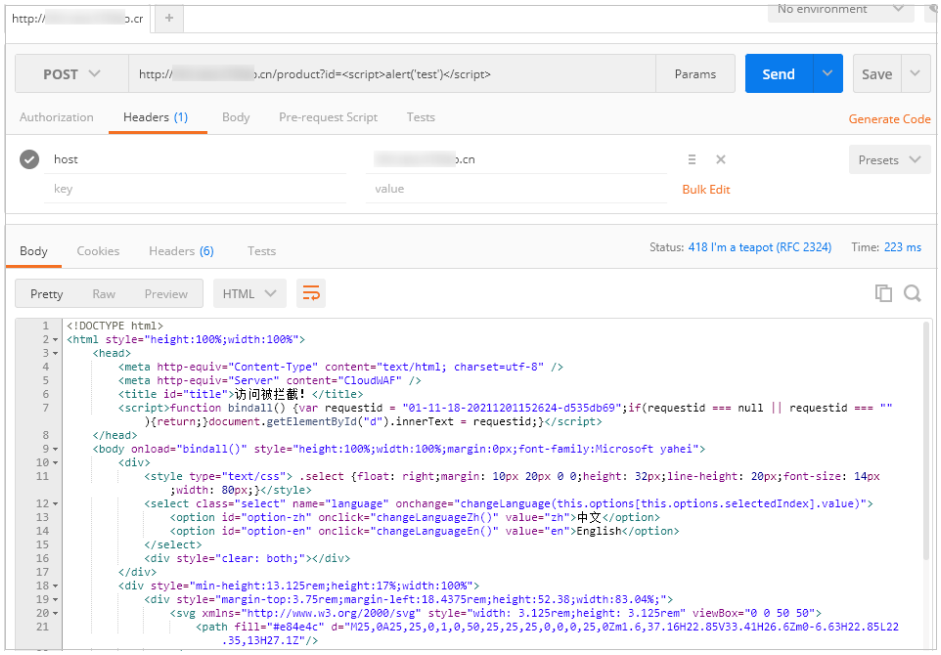
   

6. 在该防护事件所在行的“操作”列中，单击“误报处理”。
7. 在弹出的“误报处理”对话框中，添加如**图5-25**所示全局白名单规则。

图 5-25 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。

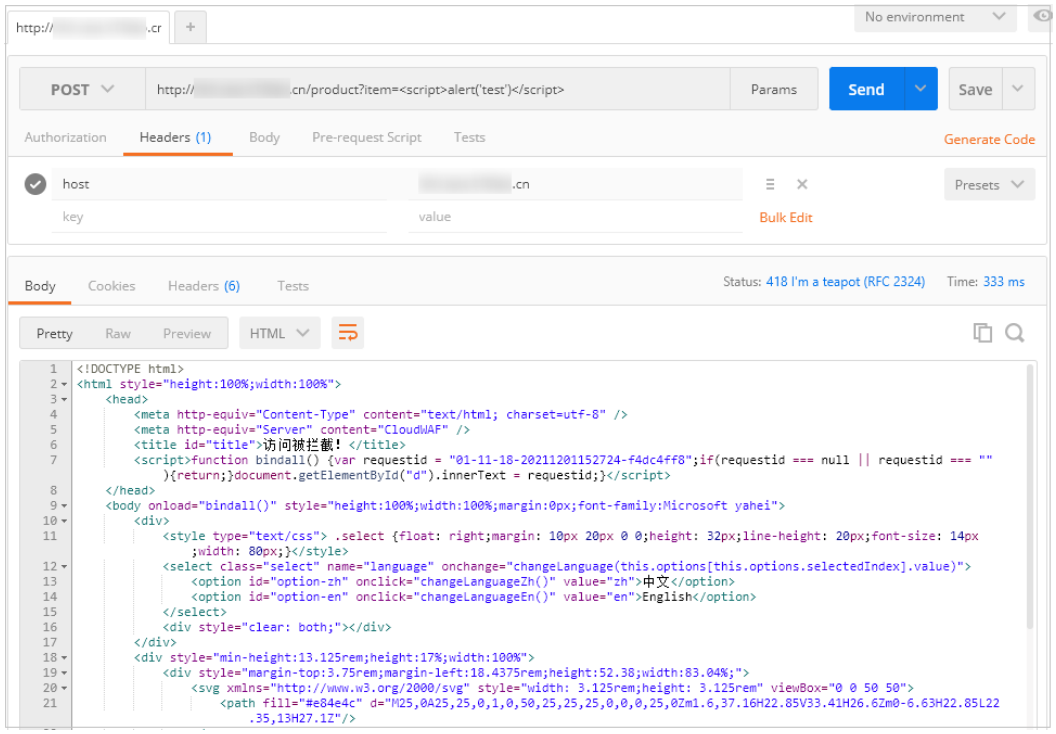


步骤5 参照**步骤3**，查看防护事件，处理命中“XSS攻击”的“110053”规则的误报防护事件。

图 5-26 查看防护事件

图 5-27 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 5-28 查看防护事件

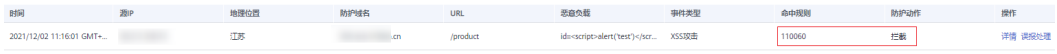
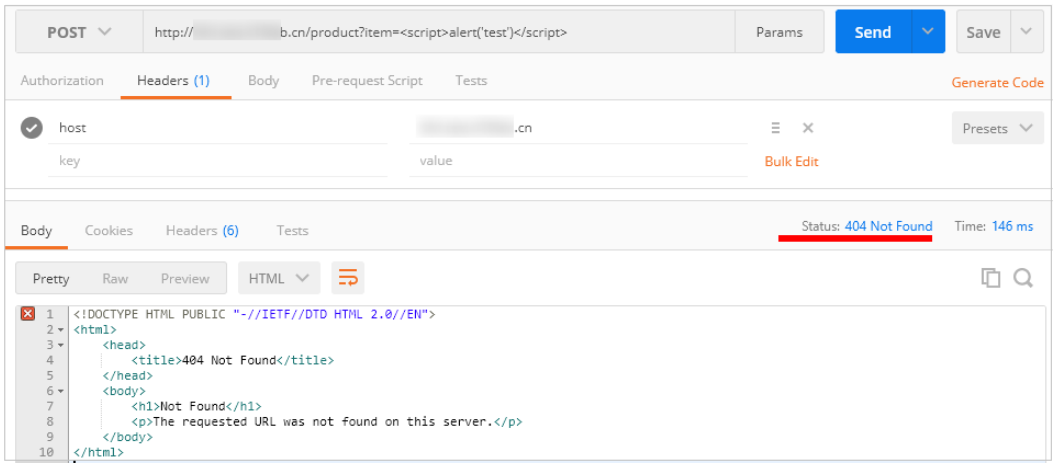


图 5-29 添加全局白名单规则

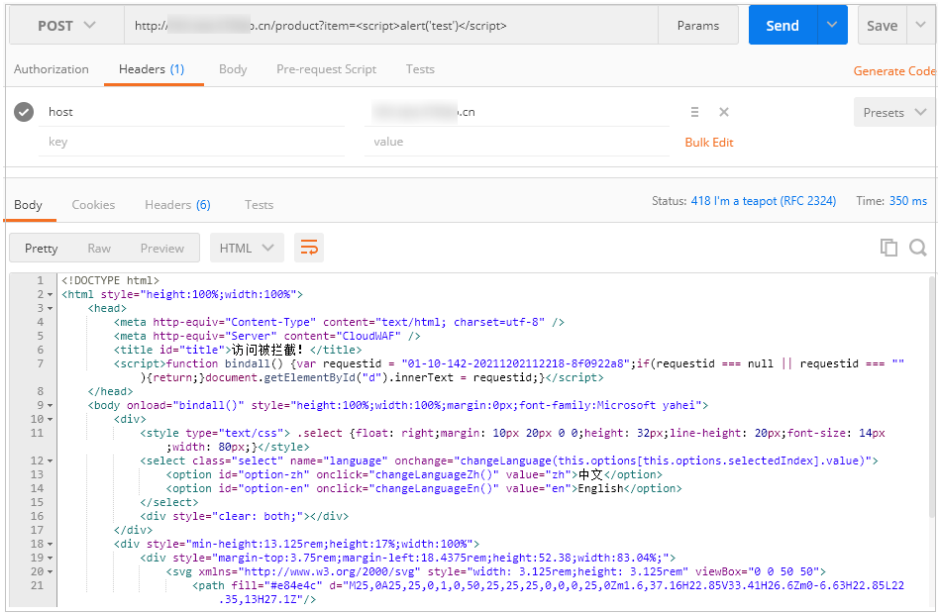
步骤8 在Postman上第四次设置请求路径为“/product”，参数ID为普通测试脚本。此时，防护网站的访问请求不再被拦截，说明所有全局白名单规则都已生效。



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。

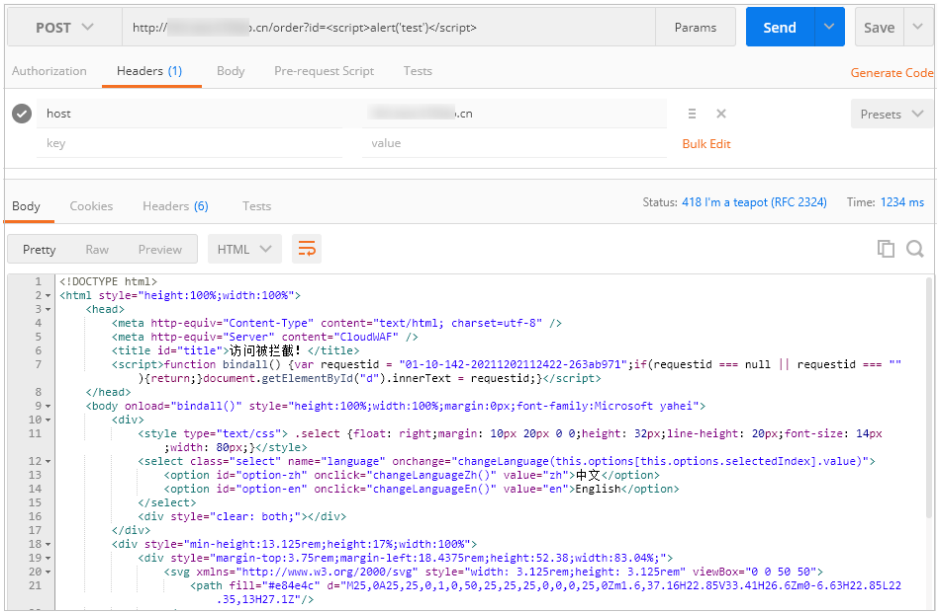


2. 查看“防护事件”页面，WAF拦截参数item的XSS攻击事件。

图 5-30 查看防护事件

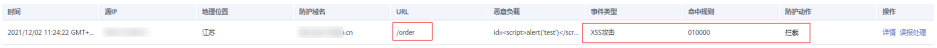
步骤10 在Postman上模拟攻击，验证设置的全局白名单规则不会影响WAF拦截其他路径的XSS攻击事件。

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。

图 5-31 查看防护事件



----结束

6 源站安全配置

6.1 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**域名接入WAF**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。

支持配置的最低 TLS 版本说明

WAF默认配置的最低TLS版本为“TLS v1.0”，为了确保网站安全，建议您根据业务实际需求进行配置，支持配置的最低TLS版本如**表6-1**所示。

表 6-1 支持配置的最低 TLS 版本说明

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

支持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。

表 6-2 加密套件说明

加密套件名称	支持的加密算法	不支持的加密算法	说明
默认加密套件 **说明** WAF默认给网站配置的是“加密套件1”，但是如果请求信息不携带sni信息，WAF就会选择缺省的“默认加密套件”。	• 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	支持的加密算法	不支持的加密算法	说明
加密套件1	• ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH	• MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • 3DES • DSS • EXP • CAMELLIA	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多种算法。

加密套件名称	支持的加密算法	不支持的加密算法	说明
加密套件4	• 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5	• AES128-SHA:AES256-SHA • AES128-SHA256:AES256-SHA256 • HIGH	• MEDIUM • LOW • aNULL • eNULL • EXPORT • DES • MD5 • PSK • RC4 • DHE	仅支持RSA-AES-CBC算法。

加密套件名称	支持的加密算法	不支持的加密算法	说明
加密套件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	×	×	×	×	×

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
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

以下介绍如何配置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“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

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

步骤6 在“TLS配置”所在行，单击。

图 6-1 修改 TLS 配置

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”。

图 6-2 “TLS 配置”对话框

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的接入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“安全与合规 > Web应用防火墙 WAF”。
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。

图 6-3 复制 CNAME

步骤2 获取WAF的接入IP。

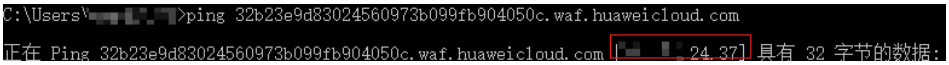
- 云模式

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

  ping *CNAME值*

  在界面回显信息中获取WAF接入IP，如**图6-4**所示。

  图 6-4 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。

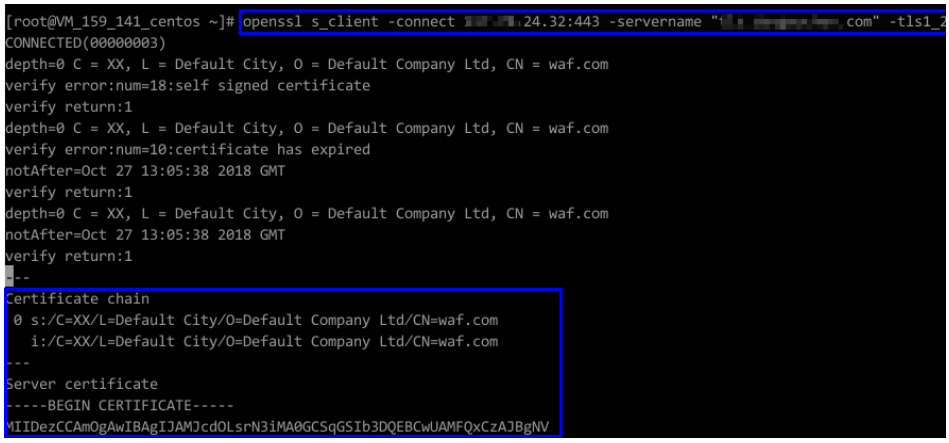
  b. 在独享引擎列表的“IP地址”栏，获取所有创建的独享引擎对应的子网IP地址，即独享引擎实例对应的接入IP。

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接入IP* **-servername** "*防护域名*" **-tls1_2**

界面返回证书相关信息，如**图6-5**所示，说明“TLS v1.2”协议可以访问目标网站。

图 6-5 验证 TLS v1.2

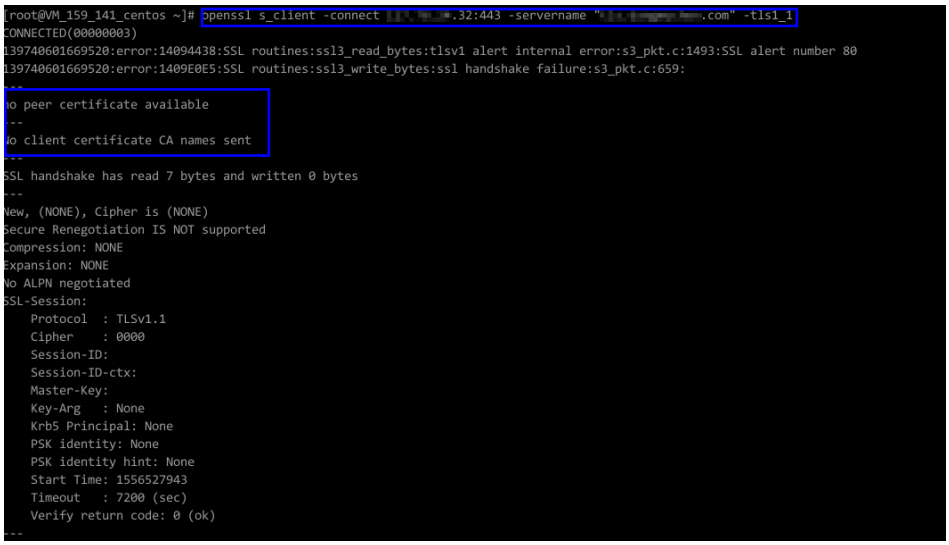


步骤4 执行以下命令，验证“TLS v1.1”协议不能访问目标网站。

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

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

图 6-6 验证 TLS v1.1



----结束

6.2 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华为云弹性云服务器（以下简称ECS）时或华为云弹性负载均衡（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

您可以在非华为云环境直接使用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。

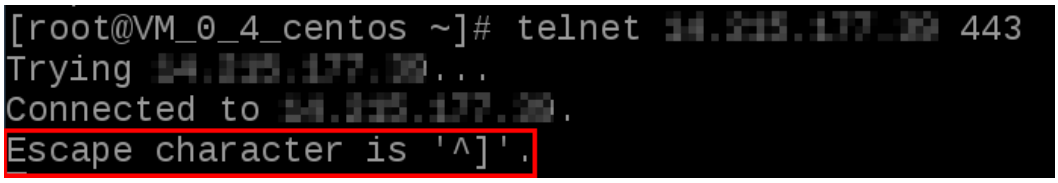
- 如果可以连通

  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6-7**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 6-7 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。有关回源IP地址的详细介绍，请参见**如何放行回源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“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

步骤5 在网站列表右侧上方，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。

图 6-8 Web 应用防火墙的回源 IP 网段

----结束

设置 ECS 入方向规则

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

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6-4所示。

图 6-9 添加入方向规则

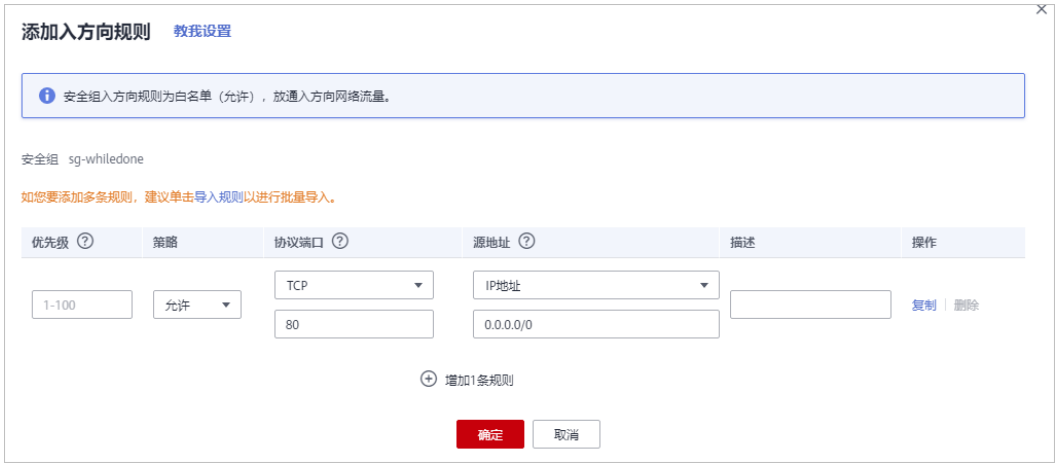


表 6-4 入方向规则参数配置说明

参数	配置说明
协议端口	安全组规则作用的协议和端口。选择“自定义TCP”后，在TCP框下方输入源站的端口。
源地址	逐一添加步骤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华为云ELB上，请参考以下操作步骤设置访问控制（白名单）策略，只放行WAF回源IP段。

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

步骤3 单击页面左上方的，选择“网络 > 弹性负载均衡 ELB”。

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

步骤5 在目标监听器所在行的“访问控制”列，单击“设置”。

图 6-10 监听器列表

步骤6 在弹出的对话框中，“访问控制”选择“白名单”。

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

步骤7 单击“确定”，白名单访问控制策略添加完成。

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

7 通过 LTS 分析 WAF 日志

7.1 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”），如**图7-1**所示，进入“日志流”页面。

图 7-1 进入访问日志流页面

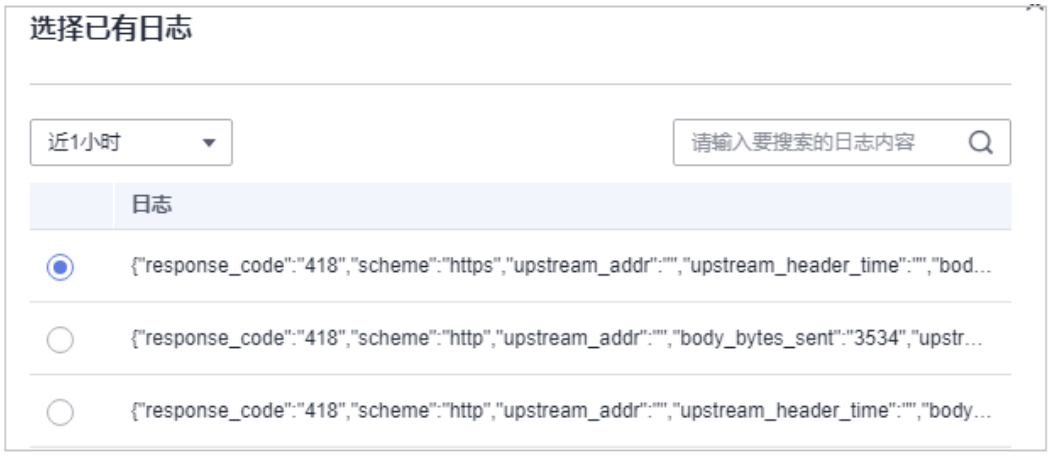
步骤6 在日志流详情页面，单击右上角 ，在弹出页面中，选择“云端结构化解析”页签，进入日志结构化配置页面。

步骤7 选择“JSON”日志结构化方式，如图7-2所示。

图 7-2 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”。

图 7-3 选择已有日志



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”），如图7-4所示。

“remote_ip”：访问请求的客户端IP地址。

图 7-4 选择快速分析日志字段

步骤10 单击“保存”，LTS将对周期内的日志进行快速分析、统计，如图7-5所示。

图 7-5 快速分析访问日志

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%'**

有关SQL查询语法的详细介绍，请参见**SQL查询语法**。

----结束

7.2 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。

图 7-6 单击攻击日志流名称

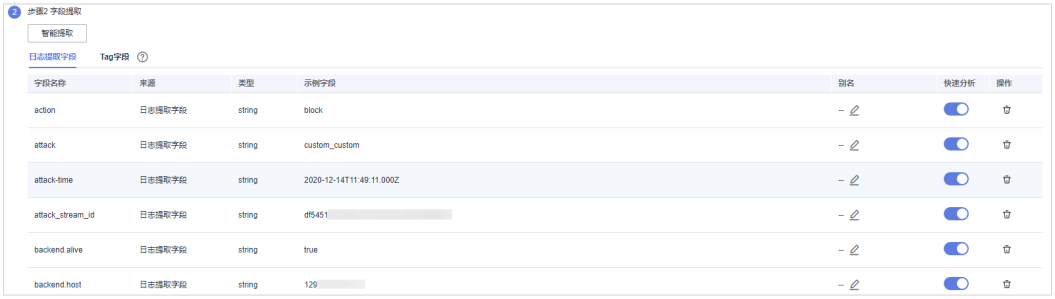
步骤4 在日志组列表中，展开waf日志组，选择日志流“attack”。

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。

图 7-7 日志提取字段



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',)

有关SQL查询语法的详细介绍，请参见**SQL查询语法**。

说明

- XX代表Spring core RCE漏洞的规则ID，请提前获取。
- 可视化查询功能当前只针对“北京4”白名单用户可用。

图 7-8 可视化查询

----结束

7.3 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**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。

图 7-9 单击攻击日志流名称

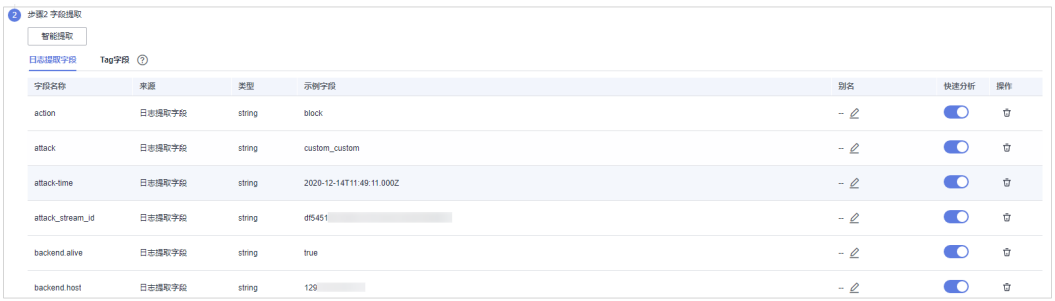
步骤4 在日志组列表中，展开waf日志组，选择日志流“attack”。

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。

图 7-10 日志提取字段



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

有关SQL查询语法的详细介绍，请参见**SQL查询语法**。

说明

可视化查询功能当前只针对“北京4”白名单用户可用。

----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，如**图7-11**所示，参数说明如**表7-1**所示。

图 7-11 配置告警规则

表 7-1 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。 单击“查看主题”创建新主题的操作步骤如下： 1. 参见创建主题创建一个主题。 2. 配置接收告警通知的手机号码、邮件地址、函数、平台应用的终端、DMS或HTTP(S)终端，即为创建的主题添加一个或多个订阅，具体操作请参见添加订阅。 3. 确认订阅。添加订阅后，完成订阅确认。 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

8 联动防护配置

8.1 “DDoS 高防+WAF”联动，提升网站全面防护能力

防护原理

- **DDoS高防**通过高防IP代理源IP对外提供服务，将所有的公网流量都引流至高防IP，进而隐藏源站，避免源站（用户业务）遭受大流量DDoS攻击。

  DDoS高防支持防护的对象：域名，华为云、非华为云或云下的Web业务

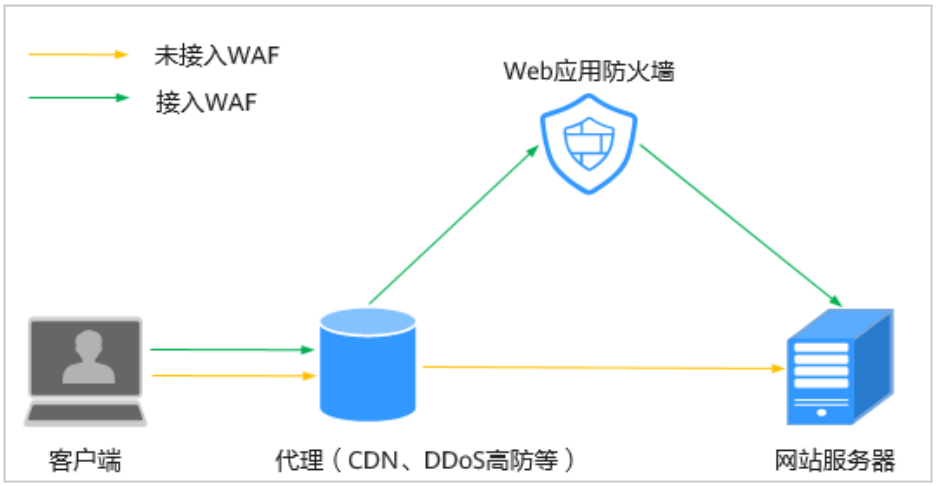
- Web应用防火墙通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

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

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

DDoS高防+WAF可以对华为云、非华为云或云下的域名进行联动防护，可以同时防御DDoS攻击（NTP Flood攻击、SYN Flood攻击、ACK Flood攻击、ICMP Flood攻击、HTTP Get Flood攻击等），以及Web应用攻击（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），确保业务持续可靠运行，配置原理图如**图8-1**所示。

图 8-1 使用代理配置原理图



DDoS高防+WAF配置后，流量被DDoS高防转发到WAF，WAF再将流量转到源站，实现网站流量检测和攻击拦截。

相关配置说明如下：

- 云模式-CNAME接入

  先将域名解析到DDoS高防，再修改DDoS高防域名信息，将源站域名修改为WAF的“CNAME”。同时，为了防止其他用户提前将您的域名配置到WAF上，从而对您的域名防护造成干扰，建议您到DNS服务商处添加一条WAF的子域名和TXT记录。
- 云模式-ELB接入

  先将域名解析到DDoS高防，再修改DDoS高防域名信息，将源站IP修改为**添加到ELB模式**中选择的ELB对应的弹性公网IP。
- 独享模式

  先将域名解析到DDoS高防，再修改DDoS高防域名信息，将源站IP修改为WAF独享引擎实例配置弹性负载均衡绑定的弹性公网IP。

约束条件

- “DDoS高防+WAF”联动仅支持域名防护。
- 如果WAF前使用了高防、CDN（Content Delivery Network，内容分发网络）、云加速等代理，配置CC防护规则时，建议“限速模式”选择“用户限速”，并勾选“全局计数”。

前提条件

已**购买DDoS高防实例**并已完成DDoS高防**网站类业务接入**，且已完成如**表8-1**所示配置操作。

表 8-1 WAF 各模式配置说明

部署模式	配置说明
云模式-CNAME接入	1. 已**购买WAF云模式**。 2. 已将域名信息（源站服务器的IP、端口等信息）**添加到WAF云模式**。 **说明** 当源站存在IPv6地址，默认开启IPv6防护。WAF为了防止客户IPv6的业务中断，禁止关闭IPv6的开关，如果确定不需要IPv6防护，需要先修改服务器配置，在源站删除IPv6的配置，具体的操作方法请参见**修改服务器配置信息**。 3. 在域名的DNS服务商处有添加域名的权限。 4. （可选）放行WAF回源段IP。源站服务器上已启用非华为云安全软件（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**。
云模式-ELB接入	1. 已**购买WAF云模式**。 2. 已将域名信息**添加到ELB模式**。
独享模式	1. 已**购买WAF独享模式**。 2. 已将域名信息（源站服务器的IP、端口等信息）**添加到WAF独享模式**。 3. 已为WAF独享模式实例**配置负载均衡**。 4. 已**为弹性负载均衡绑定弹性公网IP**。 5. **放行独享引擎回源IP**。

WAF 云模式-CNAME 接入配置策略

以下操作以华为云DDoS高防为例介绍配置域名解析的方法。如果您使用的是华为云DDoS高防，您可以直接参照以下步骤进行操作；若您使用华为云以外的DDoS高防，请参考以下步骤在其他DDoS高防上进行类似配置。

步骤1 获取“CNAME”、“子域名”和“TXT记录”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. 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。
4. 在目标域名所在行的“网站设置”列中，单击目标域名，进入域名基本信息页面。

图 8-2 基本信息页面

5. 确认“是否已使用代理”是否为“四层代理”或“七层代理”。

   说明

   如果您使用的是四层代理转发的DDoS高防，请选择“四层代理”，反之则选择“七层代理”。

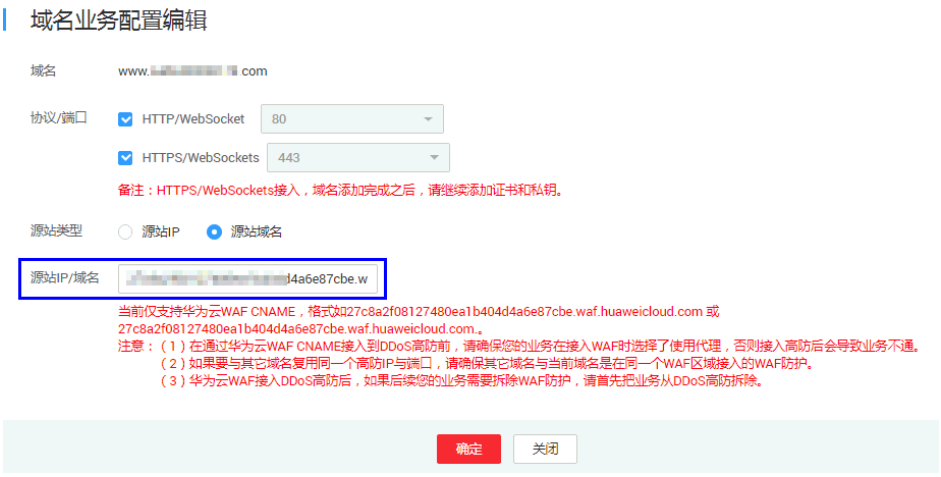
   - 否。单击“是否已使用代理”后的，在弹出的“是否已使用代理”界面，选择“四层代理”或“七层代理”，单击“确认”。然后执行**步骤1.6**。
   - 是。直接执行**步骤1.6**。

6. 单击CNAME所在行的，复制“CNAME”。在页面顶部，单击“未接入”旁边的，在弹出的对话框中，复制“子域名”和“TXT记录”。

步骤2 DDoS高防回源IP地址修改。

1. 单击页面上方的，选择“安全与合规 > DDoS防护”，在左侧导航树中，选择“DDoS高防 > 域名接入”，进入域名配置页面。
2. 在使用的DDoS高防代理类服务的域名所在行的“操作”列，单击“编辑”，进入“域名业务配置编辑”页面，将“源站IP/域名”的内容修改为复制的WAF的CNAME值，如**图8-3**所示。

图 8-3 域名业务配置编辑



3. 单击“确定”，DDoS高防回源地址修改完成。

步骤3 （可选）在DNS服务商添加一条WAF的子域名和TXT记录。

说明

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，建议您完成此操作。

1. 进入云解析页面的入口，如图8-4所示。

图 8-4 云解析页面入口

2. 在页面的右上角，单击“添加记录集”，进入“添加记录集”页面，配置模式如图8-5所示。
   - “主机记录”：步骤1.6中复制的TXT记录。
   - “类型”：选择“TXT-设置文本记录”。
   - “别名”：选择“否”。
   - “线路类型”：全网默认。
   - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
   - “值”：将步骤1.6中复制的TXT记录加上引号后粘贴在对应的文本框，例如，"**TXT记录**"。
   - 其他的设置保持不变。

图 8-5 添加记录集

3. 单击“确定”，完成子域名配置。

步骤4 （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

WAF 独享模式/ELB 接入配置策略

请参考以下步骤在华为云DDoS高防上进行配置操作。

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“安全与合规 > DDoS防护”，进入DDoS防护页面。

步骤4 在左侧导航树中，选择“DDoS高防 > 域名接入”，进入域名接入页面。

步骤5 在目标域名所在行的“操作”列中，单击“编辑”。

步骤6 在弹出“域名业务配置编辑”对话框中，修改源站IP，如图8-6所示。

图 8-6 修改源站 IP

须知

- 如果您的业务使用了WAF独享模式，“源站IP/域名”文本框中输入**为弹性负载均衡绑定弹性公网IP**。
- 如果您的业务使用了WAF云模式-ELB接入，“源站IP/域名”文本框中输入**添加到ELB模式**中选择的ELB对应的弹性公网IP。

步骤7 单击“确定”，完成源站IP配置。

----结束

生效条件

当“接入状态”为“已接入”，表示域名/IP接入成功。

须知

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

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。

8.2 “CDN+WAF”联动，提升网站防护能力和访问速度

防护原理

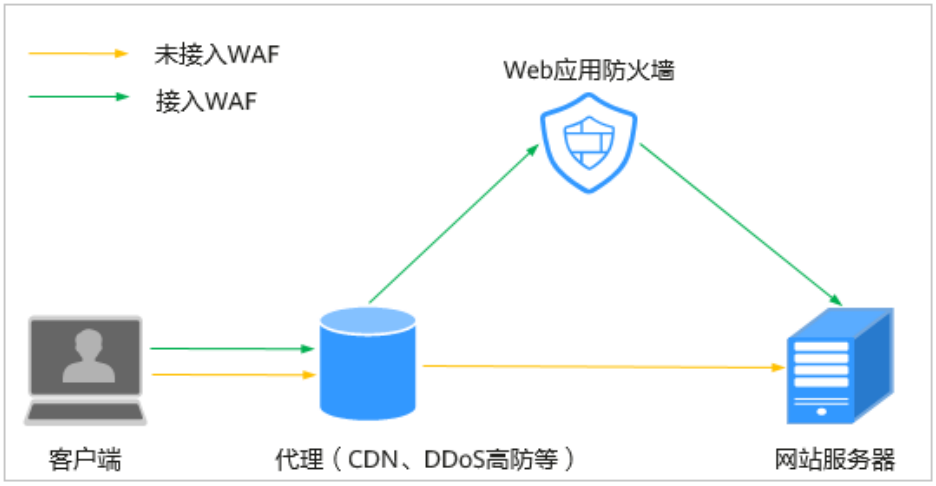
- 当用户访问使用CDN服务的网站时，本地DNS服务器通过CNAME方式将最终域名请求重定向到CDN服务。**CDN**通过一组预先定义好的策略（如内容类型、地理区域、网络负载状况等），将当时能够最快响应用户的CDN节点IP地址提供给用户，使用户可以以最快的速度获得网站内容。

  CDN支持的对象：域名，华为云、非华为云或云下的Web业务
- Web应用防火墙通过对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。

  WAF支持云模式-CNAME接入、云模式-ELB接入和独享模式三种部署模式，各部署模式支持防护的对象说明如下：
  - 云模式-CNAME接入：域名，华为云、非华为云或云下的Web业务
  - 云模式-ELB接入：域名或IP，华为云的Web业务
  - 独享模式：域名或IP，华为云的Web业务

CDN+WAF可以对华为云、非华为云或云下的域名进行联动防护，同时提升网站的响应速度和网站防护能力，配置原理图如**图8-7**所示。

图 8-7 使用代理配置原理图



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

相关配置说明如下：

- 云模式-CNAME接入

  先将域名解析到CDN，再修改CDN源站信息，将源站域名修改为WAF的“CNAME”，同时，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服务商处添加一条WAF的子域名和TXT记录。

- 云模式-ELB接入

  先将域名解析到CDN，再修改CDN源站信息，将源站IP修改为ELB模式实例所绑定ELB的弹性公网IP。

- 独享模式

  先将域名解析到CDN，再修改CDN源站信息，将源站IP修改为WAF独享引擎实例配置弹性负载均衡绑定的弹性公网IP。

约束条件

如果您选择的是云模式-CNAME接入方式，且WAF前使用了高防、CDN（Content Delivery Network，内容分发网络）、云加速等代理，配置CC防护规则时，建议“限速模式”选择“用户限速”，并勾选“全局计数”。

前提条件

域名或IP已**接入CDN**，且已完成如**表8-2**所示配置操作。

表 8-2 WAF 各模式配置说明

部署模式	配置说明
云模式-CNAME接入	1. 已**购买WAF云模式**。 2. 已将域名信息（源站服务器的IP、端口等信息）**添加到WAF云模式**。 **说明** 当源站存在IPv6地址，默认开启IPv6防护。WAF为了防止客户IPv6的业务中断，禁止关闭IPv6的开关，如果确定不需要IPv6防护，需要先修改服务器配置，在源站删除IPv6的配置，具体的操作方法请参见**修改服务器配置信息**。 3. 在域名的DNS服务商处有添加域名的权限。 4. （可选）放行WAF回源段IP。源站服务器上已启用非华为云安全软件（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**。 **须知** 为了保证WAF的安全策略能够针对真实源IP生效，请确保域名“是否已使用代理”已配置为“七层代理”，详细操作请参见**查看基本信息**。
云模式-ELB接入	1. 已**购买WAF云模式**。 2. 已将域名信息**添加到ELB模式**。

部署模式	配置说明
独享模式	1. 已**购买WAF独享模式**。 2. 已将域名信息（源站服务器的IP、端口等信息）**添加到WAF独享模式**。 3. 已为WAF独享模式实例**配置负载均衡**。 4. 已**为弹性负载均衡绑定弹性公网IP**。 5. **放行独享引擎回源IP**。

WAF 云模式配置策略

以下操作以华为云CDN为例介绍配置域名解析的方法。如果您使用的是华为云CDN，您可以直接参照以下步骤进行操作；若您使用华为云以外的CDN，请参考以下步骤在其他CDN上进行类似配置。

步骤1 获取“CNAME”、“子域名”和“TXT记录”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. 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。
4. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
5. 在目标域名所在行中，单击域名名称，进入域名基本信息页面。
6. 在域名基本信息页面，单击CNAME所在行的，复制“CNAME”。在页面顶部，单击“未接入”旁边的，在弹出的对话框中，复制“子域名”和“TXT记录”。

步骤2 **将CDN的主源站的源站域名修改为WAF的CNAME**。

步骤3 （可选）在DNS服务商添加一条WAF的子域名和TXT记录。

说明

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，建议您完成此操作。

1. 进入云解析页面的入口，如**图8-8**所示。

图 8-8 云解析页面入口

2. 在页面的右上角，单击“添加记录集”，进入“添加记录集”页面，配置模式如图8-9所示。
   - “主机记录”：步骤1.6中复制的TXT记录。
   - “类型”：选择“TXT-设置文本记录”。
   - “别名”：选择“否”。
   - “线路类型”：全网默认。
   - “TTL(秒)”：一般建议设置为5分钟，TTL值越大，则DNS记录的同步和更新越慢。
   - “值”：将步骤1.6中复制的TXT记录加上引号后粘贴在对应的文本框，例如，"**TXT记录**"。
   - 其他的设置保持不变。

图 8-9 添加记录集

3. 单击“确定”，完成子域名配置。

步骤4 （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

WAF 独享模式/ELB 接入配置策略

请参考以下步骤在华为云CDN上进行配置操作。

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“CDN与智能边缘 > 内容分发网络 CDN”，进入CDN页面。

步骤4 在左侧导航树中，选择“域名管理”。

步骤5 在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面。

步骤6 选择“基本配置”页签，在源站配置模块，单击“编辑”。

- 如果您的业务使用了WAF独享模式，“源站地址”文本框中输入**为弹性负载均衡绑定弹性公网IP**。
- 如果您的业务使用了WAF云模式-ELB接入，“源站地址”文本框中输入**添加到ELB模式**中选择的ELB对应的弹性公网IP。

步骤7 单击“保存”，完成源站配置。

----结束

生效条件

当“接入状态”为“已接入”，表示域名/IP接入成功。

须知

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

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。

8.3 CDN 回源 OBS 桶场景下串接 WAF

当您的网站域名开启了华为云CDN加速，且回源到华为云对象存储 OBS（Object Storage Service，OBS）时，如果该网站存在一定的Web攻击风险，我们推荐您组合使用CDN、OBS和Web 应用防火墙 WAF（Web Application Firewall），将开启CDN加速的域名接入WAF，实现OBS的安全防护。本文介绍如何为业务同时部署CDN、OBS、WAF。

前提条件

- 已将域名添加到CDN用于内容加速，并将请求回源到OBS桶。更多信息，请参见**添加CDN加速域名**。

  此时，域名DNS解析指向CDN的CNAME地址，源站为OBS域名。

- 已**购买WAF云模式**。

约束条件

- 仅WAF云模式的CNAME接入支持该场景。
- 该场景下，WAF只能防护网站动态内容、较小的静态资源文件。因此，如果OBS存储的资源为大文件(100M以上)，不建议使用云WAF进行防护。

方案架构

华为云CDN可以有效加速网站，WAF可以拦截网站恶意流量，而OBS桶提供海量文件存储。将数据存放在OBS桶中然后通过配置CDN加速，WAF过滤恶意请求，这样构造的业务系统可以在降低成本的同时，提高OBS数据的安全防护。

步骤一：在 OBS 中绑定 CDN 加速域名

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“存储 > 对象存储服务 OBS”。
4. 在左侧导航树中，选择“桶列表”，单击目标桶名称，进入“对象”页面。
5. 在左侧导航树中，选择“域名管理”，进入“域名管理”界面。
6. 单击“配置加速域名”，在“源站信息”所在行，复制桶域名。

   “加速域名”：配置为在CDN中配置的加速域名。

   其他参数的详细配置请参见**配置加速域名**。

完成域名绑定后，您可以在浏览器输入域名和OBS桶中任意文件名称（例如，<被防护域名>/test.png，test.png为上传到OBS桶中的图片名称），如果网站能正常访问，表示域名添加成功。

步骤二：将域名接入 WAF，源站地址为 OBS 域名

为了实现WAF对OBS桶的防护，您需要将开启CDN加速且绑定OBS桶的域名接入WAF，并将源站修改为OBS域名。

1. 单击页面左上方的，选择“安全与合规 > Web应用防火墙 WAF”。
2. 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。
3. 在网站列表左上角，单击“添加防护网站”。
4. 选择“云模式-CNAME接入”并单击“确定”。
5. 在添加防护网站页面，关键参数配置如**表8-3**。

   其他参数的配置请参见**添加防护域名（云模式-CNAME接入）**。

表 8-3 配置信息

配置项	配置说明
防护域名	填写**步骤一：在OBS中绑定CDN加速域名**中，绑定到OBS中的域名。
防护域名端口	填写需要防护的域名对应的业务端口。
服务器配置	• 对外协议：客户端请求访问服务器的协议类型。包括HTTP、HTTPS两种协议类型。 • 源站协议：Web应用防火墙转发客户端请求的协议类型。包括HTTP、HTTPS两种协议类型。 • 源站地址：填写网站对应的源站服务器的公网IP地址或源站域名，用于接收WAF转发回源的正常业务请求（回源请求），此处填写**OBS桶域名**。 **说明** 在OBS“概览”页的“域名信息”栏，也可复制OBS桶域名。 • 源站端口：WAF转发客户端请求到服务器的业务端口。

6. 单击“确认”，按照接入向导完成“放行WAF回源IP”和“本地验证”，在“修改DNS解析”页面，复制CNAME值。

图 8-10 复制 CNAME 截图

步骤三：修改 CDN 源站为 WAF 提供的 CNAME 地址

步骤1 单击页面左上方的 ☰，选择“CDN与智能边缘 > 内容分发网络 CDN”，进入CDN页面。

步骤2 在左侧导航树中，选择“域名管理”。

步骤3 在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面。

步骤4 选择“基本配置”页签，在源站配置模块，单击“编辑”。

“源站地址”文本框中输入6中复制的WAF CNAME值。

----结束

效果验证

完成配置后，您可以再次在浏览器输入已添加的域名和OBS桶中任意文件名称（例如，<被防护域名>/test.png），test.png为上传到OBS中的图片名称），如果网站能正常访问，表示域名添加成功。

您也可以在浏览器输入已添加的域名和Web攻击代码（例如，SQL注入：**curl -kv <被防护域名>?name='1%20or%201=1'**），如果返回418拦截提示页面，表示攻击被拦截，WAF防护成功。

后续操作

完成上述配置后，WAF会默认为域名开启Web基础防护规则，通过对访问域名的请求特征进行识别和检测，将正常的访问请求转发给OBS私有桶，实现安全防护。您也可以根据实际情况，开启更多的防护策略，详见**防护策略配置**。

8.4 “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**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

- 已购买七层独享型负载均衡。有关ELB类型的详细介绍，请参见**共享型弹性负载均衡与独享型负载均衡的功能区别**。

  说明

  2023年4月之前的独享引擎版本，不支持与独享ELB网络型配合使用。因此，如果您使用了独享ELB网络型（TCP/UDP）负载均衡，在目标独享引擎实例列表中的“版本”列查看WAF实例版本，确认已升级到最新版本（2023年4月及之后的版本）。

- 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。

  有关添加安全组规则的详细操作，请参见**添加安全组规则**。

操作步骤

步骤1 **购买WAF独享实例**。

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“七层代理”，其他参数的配置参见**添加防护网站（独享模式）**。

图 8-11 添加防护域名

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”。

图 8-12 配置监听器信息

6. 单击“下一步：配置后端分配策略”，配置后端服务器组。

图 8-13 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。
- 有关ELB流量分配策略的详细介绍，请参见**流量分配策略**。

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“安全与合规 > Web应用防火墙”，进入“安全总览”页面。
4. 在左侧导航树中，选择“系统管理 > 独享引擎”，进入“独享引擎”页面。

图 8-14 独享引擎列表

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”。

图 8-15 添加到 ELB

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。

图 8-16 配置业务端口

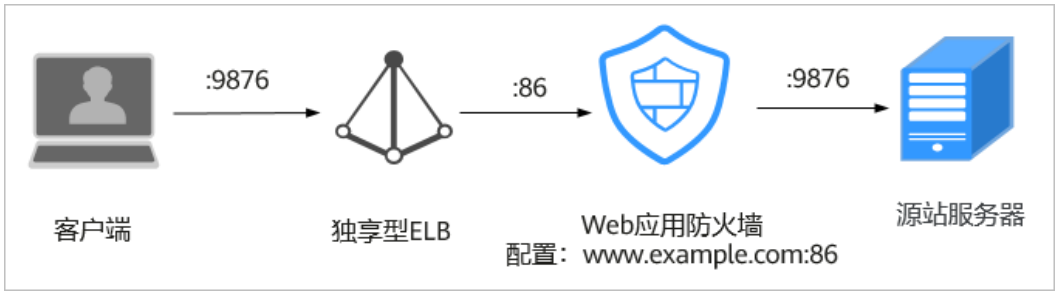
8. 单击“确认”，配置完成。

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



8.5 “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；发表反动言论，从而造成不良社会影响，损害企业品牌形象；对政府、高校、企事业单位等有影响力的单位来说，页面被恶意篡改将无意间成为传播危害社会安全等信息的帮凶，无形中错误引导大众，造成难以挽回的损失。

HSS 和 WAF 的网页防篡改的区别

表 8-4 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

说明

- WAF云模式的入门版和ELB模式不支持该功能。
- 关于WAF网页防篡改的更多信息，请参见**配置网页防篡改规则**。

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域或项目。

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

步骤4 在左侧导航树中，选择“防护策略”，进入“防护策略”页面。

步骤5 单击目标策略名称，进入目标策略的防护配置页面。

步骤6 选择“网页防篡改”配置框，用户可根据自己的需要开启或关闭网页防篡改策略。

-  ：开启状态。
-  ：关闭状态。

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8-5所示。

图 8-17 添加网页防篡改规则

表 8-5 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 登录管理控制台。

步骤2 在页面左上角选择“区域”，单击，选择“安全合规 > 主机安全服务”，进入主机安全服务界面。

步骤3 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”。

图 8-18 添加防护服务器

步骤4 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5 开启“网页防篡改”防护服务后，请在控制台上查看主机安全服务的开启状态。

“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。
- 选择“资产管理 > 主机管理 > 云服务器”，目标主机所在行的“防护状态”为“防护中”，且“版本/到期时间”为“网页防篡改版”，则表示网页防篡改赠送的旗舰版已开启。

----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。

9 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，建议您至少购买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**购买WAF独享模式**购买一个新的独享引擎实例。

- 新购买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。
- 确保新购买的实例，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404/502/504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“安全与合规 > Web应用防火墙”，进入“安全总览”页面。
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 参见**修改后端云服务器权重**，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 参见**修改后端云服务器权重**，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404/502/504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 参见**修改后端云服务器权重**，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

10 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。

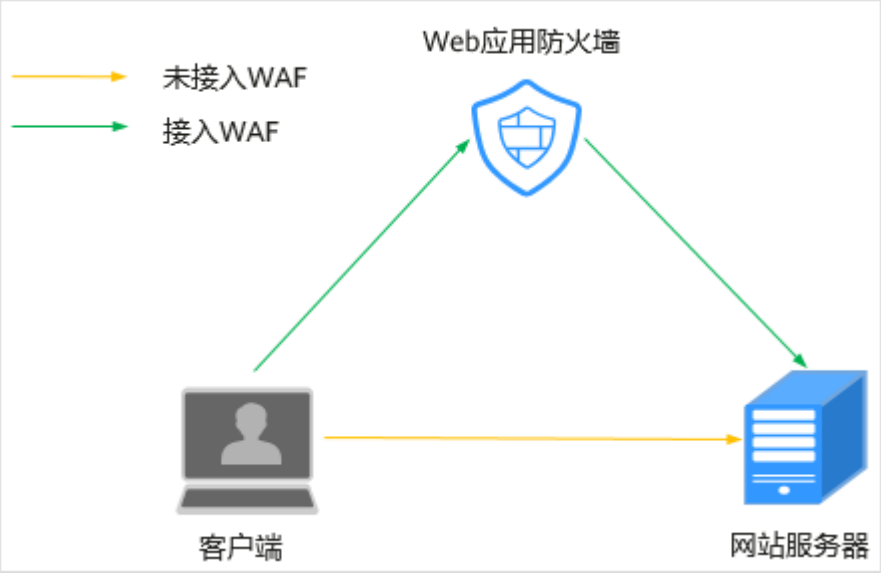
当您的网站已接入Web应用防火墙（Web Application Firewall，简称WAF）进行安全防护后，WAF作为一个反向代理存在于客户端和服务器之间，服务器的真实IP被隐藏起来，Web访问者只能看到WAF的IP地址。此时，您可直接通过WAF获取客户端的真实IP，也可以通过配置网站服务器获取客户端的真实IP。

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10-1所示。

图 10-1 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“七层代理”，其他情况，“是否已使用代理”选择“无代理”。
- 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。WAF获取真实IP原则请参见**WAF获取真实IP是从报文中哪个字段获取到的?**。

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
     ```
     有关获取WAF回源IP段的详细介绍，请参见**如何放行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
  ```

  有关获取WAF回源IP段的详细介绍，请参见**如何放行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。

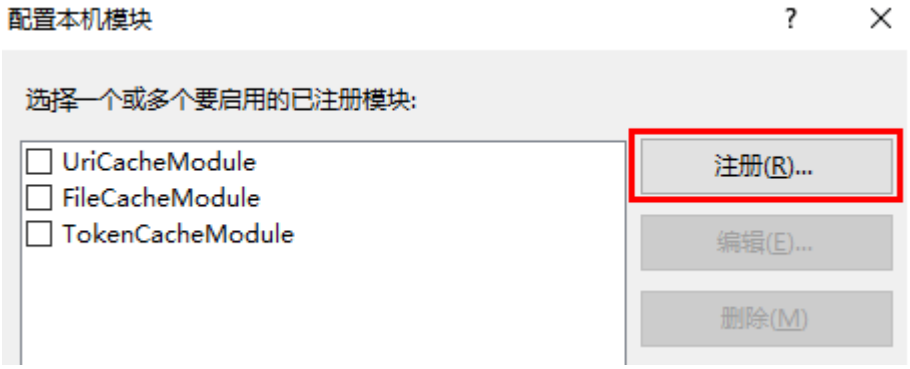
步骤1 下载**F5XForwardedFor**模块。

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”。

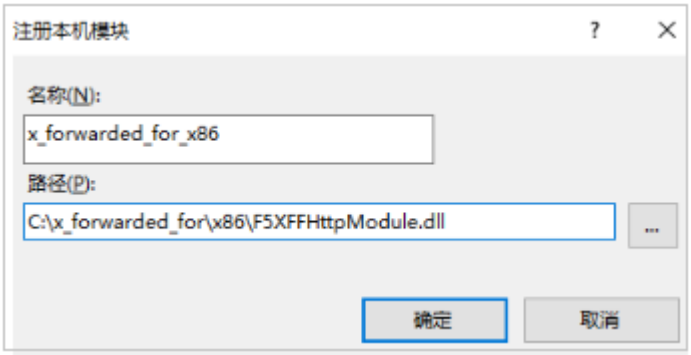
图 10-2 注册模块



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”。

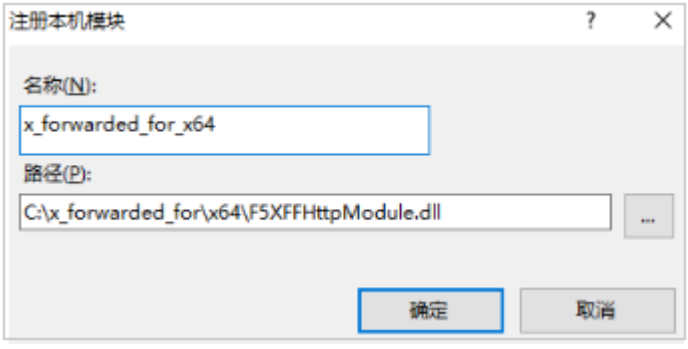
- x86操作系统：注册模块“x_forwarded_for_x86”
  - 名称：x_forwarded_for_x86
  - 路径：“C:\x_forwarded_for\x86\F5XFFHttpModule.dll”

图 10-3 x86 操作系统注册模块



- 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”

图 10-4 x64 操作系统注册模块



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

11 配置 Accept-Encoding 字段转发关闭响应报文压缩

客户端在请求头“Accept-Encoding”声明支持响应压缩，如 "Accept-Encoding: gzip"；当响应经过WAF后，WAF 认为符合压缩标准，对其进行压缩。但事实上客户端在收到响应之后，客户端并不能自动解压响应报文，那么就会存在响应获取异常的问题。

建议在WAF控制台对该域名重写“Accept-Encoding”头，这样WAF就不会对响应进行任何压缩操作。

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“安全与合规 > Web应用防火墙 WAF”。

步骤4 在左侧导航树中，选择“网站设置”，进入“网站设置”页面。

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

步骤6 在“字段转发”列，单击，在弹出的“字段转发”弹框中，输入Key/Value值，并单击“添加”。

Key值配置为“Accept-Encoding”；Value值配置为“identity”，如图11-1所示。

图 11-1 字段转发

步骤7 单击“确认”。

----结束

A 修订记录

发布日期	修改说明
2024-05-09	第七十一次正式发布。 增加： **CDN回源OBS桶场景下串接WAF**
2024-03-30	第七十次正式发布。 修改： • **“DDoS高防+WAF”联动，提升网站全面防护能力** • **配置Accept-Encoding字段转发关闭响应报文压缩** • **使用Postman工具模拟业务验证全局白名单规则** • **源站安全配置**
2024-02-01	第六十九次正式发布。 修改： • **“DDoS高防+WAF”联动，提升网站全面防护能力** • **基于IP限速的配置** • **基于Cookie字段的配置** • **通过配置反爬虫防护策略阻止爬虫攻击** • **Web基础防护功能最佳实践** • **“CDN+WAF”联动，提升网站防护能力和访问速度** • **“独享WAF+7层ELB”联动，实现防护任意非标端口** • **配置Accept-Encoding字段转发关闭响应报文压缩**
2024-01-05	第六十八次正式发布。 修改： • **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**

发布日期	修改说明
2023-11-30	第六十七次正式发布。 ● 架构调整 ● 新增： – 网站防护最佳实践 – CC攻击常见场景防护配置 ● 修改： – “DDoS高防+WAF”联动，提升网站全面防护能力 – 基于IP限速的配置 – 基于Cookie字段的配置 – 通过配置反爬虫防护策略阻止爬虫攻击 – Web基础防护功能最佳实践 – “CDN+WAF”联动，提升网站防护能力和访问速度 – “独享WAF+7层ELB”联动，实现防护任意非标端口
2023-11-15	第六十六次正式发布。 修改通过配置TLS最低版本和加密套件提升客户端访问域名的通道安全。
2023-11-06	第六十五次正式发布。 修改“DDoS高防+WAF”联动，提升网站全面防护能力。
2023-08-11	第六十四次正式发布。 增加配置Accept-Encoding字段转发关闭响应报文压缩。
2023-06-30	第六十三次正式发布。 修改获取客户端真实IP。
2023-06-07	第六十二次正式发布。 修改独享引擎实例升级配置。
2023-06-02	第六十一次正式发布。 修改通过配置ECS/ELB访问控制策略保护源站安全。
2023-03-03	第六十次正式发布。 修改： ● “CDN+WAF”联动，提升网站防护能力和访问速度 ● “DDoS高防+WAF”联动，提升网站全面防护能力
2023-01-31	第五十九次正式发布。 修改独享引擎实例升级配置。

发布日期	修改说明
2022-12-26	第五十八次正式发布。 新增： **Solution as Code一键式部署类最佳实践**
2022-10-25	第五十七次正式发布。 修改如下章节： **独享引擎实例升级配置**
2022-09-30	第五十六次正式发布。 增加**“独享WAF+7层ELB”联动，实现防护任意非标端口**。
2022-09-06	第五十五次正式发布。 修改如下章节： • **“CDN+WAF”联动，提升网站防护能力和访问速度** • **“DDoS高防+WAF”联动，提升网站全面防护能力**
2022-08-11	第五十四次正式发布。 增加以下最佳实践： • **通过业务Cookie和HWWAFSESID联合配置限制恶意抢购、下载**
2022-07-26	第五十三次正式发布。 修改**“WAF+HSS”联动，提升网页防篡改能力**章节。
2022-07-06	第五十二次正式发布。 全局计数功能上线，修改如下章节： • **CC攻击防御最佳实践** • **“CDN+WAF”联动，提升网站防护能力和访问速度** • **“DDoS高防+WAF”联动，提升网站全面防护能力**
2022-07-04	第五十一次正式发布。 全局白名单功能上线，修改如下章节： • **通过误报处理提升Web基础防护效果** • **使用Postman工具模拟业务验证全局白名单规则**
2022-06-06	第五十次正式发布。 修改如下章节： • **获取客户端真实IP** • **“DDoS高防+WAF”联动，提升网站全面防护能力**
2022-05-23	第四十九次正式发布。 • 增加**“WAF+HSS”联动，提升网页防篡改能力**。 • 修改**获取客户端真实IP**章节。

发布日期	修改说明
2022-05-17	第四十八次正式发布。 修改“DDoS高防+WAF”联动，提升网站全面防护能力章节。
2022-05-05	第四十七次正式发布。 修改获取客户端真实IP，增加了约束条件。
2022-04-19	第四十六次正式发布。 增加如下两个最佳实践： • 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
2022-04-01	第四十五次正式发布。 增加Java Spring框架远程代码执行高危漏洞最佳实践。
2022-03-29	第四十四次正式发布。 准备阶段，增加了相关说明。
2022-02-11	第四十三次正式发布。 获取客户端真实IP，增加了Apache服务器为2.4及以上版本如何获取源站IP的方法。
2021-12-22	第四十二次正式发布。 新增通过LTS快速查询分析WAF访问日志。
2021-12-02	第四十一次正式发布。 • 新增使用Postman工具模拟业务验证全局白名单规则。 • 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，优化内容描述。
2021-10-21	第四十次正式发布。 “CDN+WAF”联动，提升网站防护能力和访问速度，优化内容描述。
2021-10-12	第三十九次正式发布。 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，优化内容描述。
2021-09-22	第三十八次正式发布。 新增独享引擎实例升级配置。
2021-08-19	第三十七次正式发布。 “CDN+WAF”联动，提升网站防护能力和访问速度，更新界面截图。

发布日期	修改说明
2021-07-29	第三十六次正式发布。 **“CDN+WAF”联动，提升网站防护能力和访问速度**、**“DDoS高防+WAF”联动，提升网站全面防护能力**，补充接入成功生效条件。
2021-07-20	第三十五次正式发布。 修改管理控制台入口。
2021-06-25	第三十四次正式发布。 **单独使用WAF配置指导**，优化内容描述。
2021-06-08	第三十三次正式发布。 • **“CDN+WAF”联动，提升网站防护能力和访问速度**，优化前提条件描述。 • **“DDoS高防+WAF”联动，提升网站全面防护能力**，优化前提条件描述。
2021-05-20	第三十二次正式发布。 **“DDoS高防+WAF”联动，提升网站全面防护能力**，补充独享模式的配置策略。
2021-05-14	第三十一次正式发布。 **“CDN+WAF”联动，提升网站防护能力和访问速度**，补充独享模式的配置策略。
2021-04-08	第三十次正式发布。 **单独使用WAF配置指导**，优化内容描述。
2021-03-19	第二十九次正式发布。 **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**，优化内容描述。
2020-11-27	第二十八次正式发布。 • **通过配置ECS/ELB访问控制策略保护源站安全**，优化内容描述。 • **通过误报处理提升Web基础防护效果**，优化内容描述。 • **获取客户端真实IP**，优化内容描述。
2020-11-20	第二十七次正式发布。 • **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**，优化内容描述。 • **通过配置反爬虫防护策略阻止爬虫攻击**，优化内容描述。
2020-08-17	第二十六次正式发布。 **获取客户端真实IP**，优化内容描述。

发布日期	修改说明
2020-05-14	第二十五次正式发布。 **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**，优化内容描述。
2020-04-16	第二十四次正式发布。 优化内容描述。
2020-04-02	第二十三次正式发布。 更新界面截图。
2020-02-27	第二十二次正式发布。 **通过误报处理提升Web基础防护效果**，更新界面截图并优化内容描述。
2020-02-14	第二十一次正式发布。 新增**Apache Dubbo反序列化漏洞**。
2020-01-03	第二十次正式发布。 **获取客户端真实IP**，修改标题。
2019-12-19	第十九次正式发布。 ● **通过误报处理提升Web基础防护效果**，增加IIS服务器获取访问者真实IP的方法。 ● **“CDN+WAF”联动，提升网站防护能力和访问速度**，优化内容描述。
2019-12-16	第十八次正式发布。 操作入口连环图更新。
2019-12-05	第十七次正式发布。 **获取客户端真实IP**，优化内容描述。
2019-10-21	第十六次正式发布。 ● **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**，优化内容描述。 ● **CC攻击防御最佳实践**，优化内容描述。 ● **通过误报处理提升Web基础防护效果**，优化内容描述。 ● **“DDoS高防+WAF”联动，提升网站全面防护能力**，优化内容描述。 ● **“CDN+WAF”联动，提升网站防护能力和访问速度**，优化内容描述。
2019-09-06	第十五次正式发布。 新增**开源组件Fastjson拒绝服务漏洞**。
2019-09-04	第十四次正式发布。 **单独使用WAF配置指导**，优化内容描述。

发布日期	修改说明
2019-08-30	第十三次正式发布。 **“CDN+WAF”联动，提升网站防护能力和访问速度**，优化内容描述。
2019-08-27	第十二次正式发布。 **通过配置反爬虫防护策略阻止爬虫攻击**，优化内容描述。
2019-08-01	第十一次正式发布。 新增**“CDN+WAF”联动，提升网站防护能力和访问速度**。
2019-07-12	第十次正式发布。 新增**开源组件Fastjson远程代码执行漏洞**。
2019-06-21	第九次正式发布。 新增**获取客户端真实IP**。
2019-06-04	第八次正式发布。 ● 新增**通过误报处理提升Web基础防护效果**。 ● 新增**WAF接入配置最佳实践**。
2019-05-16	第七次正式发布。 ● 新增**通过配置ECS/ELB访问控制策略保护源站安全**。 ● 新增**Web基础防护功能最佳实践**。
2019-05-05	第六次正式发布。 **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**，优化内容描述。
2019-04-28	第五次正式发布。 新增**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**。
2019-04-23	第四次正式发布。 ● 新增**Oracle WebLogic wls9-async反序列化远程命令执行漏洞（CNVD-C-2019-48814）**。 ● **CC攻击防御最佳实践**，优化内容描述。 ● **通过配置反爬虫防护策略阻止爬虫攻击**，优化内容描述。
2018-11-08	第三次正式发布。 短描述和关键字的设置。
2018-10-15	第二次正式发布。 根据界面变化更新了截图和描述。
2018-05-11	第一次正式发布。