边缘安全加速平台 EO

安全防护

产品文档

腾讯云

文档目录

安全防护
概述

最近更新时间：2023-12-06 15:41:40

安全防护为接入 EdgeOne 的应用提供安全策略配置、安全事件告警选项，帮助您在边缘校验流量和请求，避免外部攻击和安全风险对您的业务和敏感数据造成影响。

接入 EdgeOne 安全加速服务并订阅相关安全防护服务后，您可以配置下列安全策略：

说明：

DDoS 防护为网络层 DDoS 防护，适用于四层代理应用（TCP/UDP 应用），DDoS 防护相关配置仅开通 独立 DDoS 防护 用户可配置。

如果您需要通过 Web 防护配置 Referer 黑白名单、UA 黑白名单、IP 黑白名单或区域封禁，请使用 **Web 防护 > 自定义规则 > 基础访问管控**。详情参考 Web 防护-自定义规则。

可配置的规则和执行方式选项可能根据您订阅的 EdgeOne 套餐有所不同。套餐规格请参考 套餐选型对比。

分类	功能	使用场景	默认配置
DDoS 防护（网络层 DDoS 防护）	DDoS 防护等级	自动防护清洗针对四层业务（TCP/UDP 应用）的 DDoS 攻击。 例如： 日常防护：使用 `适中` 防护等级丢弃具有明显 DDoS 攻击特征的流量。 攻击透传时应急恢复：使用 `严格` 防护等级丢弃所有疑似 DDoS 攻击的流量。	防护等级：**适中**
	IP 黑白名单	丢弃或放行指定 IP 的流量。 例如： 内部调用放行：放行内部服务 IP `11.11.11.11`，允许服务间高频访问。	无
	区域封禁	禁止指定地区客户端访问。 例如： 境外封禁：丢弃源 IP 位于中国大陆以外地区的流量。	无
	端口过滤	丢弃或放行指定源端口/目的端口流量。 例如： 高危反射端口丢弃：丢弃 `源端口匹配 UDP 53` 的流量，禁止访问私有 UDP 协议应用。	无

	特征过滤	丢弃包含指定数据或参数的流量。 例如： 丢弃异常长度 UDP 包：丢弃长度超过 500 的 UDP 流量。	无
	协议封禁	丢弃指定 IP 协议的流量。 例如： 禁止外部 PING 指令：配置封禁 ICMP 协议流量。	无
	连接类攻击防护	拦截高频建连，高频异常连接等异常 TCP 行为。	无
Web 防护	CC 攻击防护	缓解 HTTP/HTTPS DDoS 攻击，包括高频访问和慢速请求攻击。	**高频访问请求限制** 限制等级：自适应 - 宽松 处置方式：JavaScript 挑战 **慢速攻击防护** 未启用 **智能客户端过滤** 处置方式：JavaScript 挑战
	托管规则	拦截针对 Web 应用的漏洞攻击（SQL 注入、跨站点脚本执行、远程命令执行等）。 例如： 拦截 Apache log4j 漏洞：将开源组件漏洞中 log4j 相关规则启用为拦截。	全部规则启用为观察模式
	自定义规则	根据头部内容和 IP 处置请求。 例如： 防盗链：按 Referer 头部匹配请求进行拦截。 区域封禁：按区域匹配请求客户端 IP 进行拦截。 IP 黑名单：按指定 IP 或者 IP 分组拦截。	无
	速率限制	拦截访问超过预设速率的客户端。 例如： 拦截造成源站短时间内大量错误的客户端：设定每个 IP 允许造成源站错误的速率，超过阈值后拦截 IP 访问。	无

		拦截访问特定 API 频率过高的账户 ID：设定每个账户（指定账户 ID 所在参数位置）允许访问指定 API 的频率，超过阈值后拦截账号访问。 拦截访问频率过高的客户端指纹（JA3 指纹）：设定每个 JA3 指纹（即 TLS 指纹）的访问速率，超过阈值后拦截相同指纹访问。	
	防护例外规则 - 跳过防护模块	按模块跳过 Web 防护中的防护规则。 例如： 放行内部服务：设定内部服务 IP 列表和指定 API 路径，允许列表内客户端不受限制访问该路径。	无
	防护例外规则 - 跳过指定托管规则	跳过指定托管规则。 例如： 放行用户内容上传：请求中包含用户撰写内容的参数时，配置业务路径和误报规则，放行请求。	无
Bot 管理	Bot 智能分析	按风险等级拦截 Bot 请求。（适合快速启用 Bot 管理策略，并建立 Bot 访问画像） 例如： 拦截 CDN 资源滥用（盗刷）：拦截来自恶意 Bot 请求。	无
	Bot 基础管理	处置搜索引擎、开源开发工具和商业用途的爬虫。 例如： 允许 Google 搜索引擎爬虫访问：使用搜索引擎特征规则库，将 Google 搜索引擎爬虫配置为放行。 拦截 cURL 工具访问：使用 UA 特征库，拦截 Web 开发工具访问。	无
	客户端画像分析	根据 IP 威胁情报，对有恶意行为历史或高危特征的客户端请求进行处置。 例如： 拦截 VPN / 代理 请求：拦截识别为恶意代理、秒拨 IP、代理 IP 池的客户端请求。	无
	主动特征识别	拦截浏览器运行环境和访问行为异常的请求。	无

		例如： Cookie 挑战：启用 Cookie 校验，拦截不支持 Cookie 的客户端。 拦截自动工具访问：启用客户端行为校验，识别JavaScript 运行环境异常和访问行为异常的自动化工具。	
	自定义 Bot 规则	根据请求的 Bot 访问特征、头部和客户端 IP，对抗 Bot 工具。功能提供了更多处置方式选项用于 Bot 对抗。 例如： 对抗访问敏感业务的高危Bot：按访问路径和客户端画像进行匹配，按一定权重配置观察、静默和等待后响应。	无
	Bot 管理例外规则	跳过 Bot 管理的各类防护规则。 例如： 放行内部爬虫工具：允许来自内部服务 IP 的爬虫工具访问指定 API。	无

DDoS 防护
DDoS 防护概述

最近更新时间：2023-08-17 14:22:30

什么是 DDoS 攻击

分布式拒绝服务攻击（Distributed Denial of Service，DDoS）是指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

DDoS 攻击的危害

如果遭受 DDoS 攻击导致业务中断或受损，将会带来巨大的商业损失。
重大经济损失：在遭受 DDoS 攻击后，源站服务器可能无法提供服务，导致用户无法访问您的业务，从而造成巨大的经济损失和品牌损失。
数据泄露：黑客在对您的服务器进行 DDoS 攻击时，可能会趁机窃取您业务的核心数据。
恶意竞争：部分行业存在恶性竞争，竞争对手可能会通过 DDoS 攻击恶意攻击您的服务，从而在行业竞争中获取优势。

DDoS 防护使用场景

游戏：游戏行业是 DDoS 攻击的重灾区，DDoS 防护能有效保证游戏的可用性和持续性，保障游戏玩家流畅体验，同时为活动、新游戏发布或节假日游戏收入旺季时段保驾护航，确保游戏业务正常。
互联网：保证互联网网页的流畅访问，业务正常不中断，对电商大促等重大活动时段，提供安全护航。
金融：满足金融行业的合规性要求，保证线上交易的实时性及安全稳定性。
政府：满足国家政务云建设标准的安全需求，为重大会议、活动、敏感时期提供安全保障，保障民生服务正常可用，维护政府公信力。
企业：保障企业站点服务持续可用，避免 DDoS 攻击带来的经济及企业品牌形象损失问题，零硬件零维护，节省安全成本。

EdgeOne 默认 DDoS 防护介绍

DDoS 防护是腾讯云 EdgeOne 提供的针对 L3/L4 流量型 DDoS 攻击的防护服务。EdgeOne 可提供基础 DDoS 防护能力，满足日常安全运营需求，平台级基础 DDoS 防护默认开启，实时监控网络流量，发现流量型 DDoS 攻击立即清洗，为 EdgeOne 秒级开启防护。DDoS 防护默认提供基础安全策略，策略基于攻击画像、行为模式分析、AI 智能识别等防护算法，有效应对常见 DDoS 攻击行为。

防护分类	描述
畸形报文过滤	过滤 frag flood，smurf，stream flood，land flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包。
网络层 DDoS 攻击防护	过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接。
DNS DDoS 攻击	DNS DDoS 攻击主要包括 DNS Request Flood、DNS Response Flood、虚假源+真实源 DNS Query Flood、权威服务器攻击和 Local 服务器攻击等。
连接型 DDoS 攻击	连接型 DDoS 攻击主要是指TCP慢速连接攻击、连接耗尽攻击、Loic、Hoic、Slowloris、Pyloris、Xoic 等慢速攻击。

EdgeOne 独立 DDoS 防护介绍

适用场景

独立 DDoS 防护是 EdgeOne 推出的一项增强 DDoS 防护的付费功能，提供独享清洗中心接入能力。当平台默认防护无法满足您的业务正常运行诉求时，您可以通过使用独立 DDoS 防护，来帮助您保护您的业务正常运行。独立 DDoS 防护开启后，将为您的业务提供独立高防 IP 来进行流量清洗，可根据您选购的保底防护容量和弹性防护容量，提供承诺的防护带宽值。

说明：

独立 DDoS 防护仅 EdgeOne 企业版套餐可订阅。

能力介绍

1. 默认接入节点使用清洗中心，提供更大的 DDoS 防护能力，最高可达 T 级。
2. 可承诺防护容量，可根据业务部署情况灵活选择全球可用区（不含中国大陆）、中国大陆可用区、全球可用区的防护规格。
3. 除了自动清洗与识别机制，EdgeOne DDoS 防护可针对您的业务防护需求，提供多样化、灵活的 DDoS 自定义防护策略，您可根据特殊业务特点灵活设置，应对不断变化的攻击手法。对于四层代理实例，支持以下自定义规则能力配置：

说明：

当请求同时匹配多个规则时，按照如下规则顺序处理

防护模块	功能说明

IP 黑白名单	在 DDoS 攻击中通过匹配 IP 黑白名单的方式来限制对 EdgeOne 站点的访问。
端口过滤	在 DDoS 攻击中通过自定义端口规则，限制指定端口范围访问 EdgeOne 站点。
协议封禁	可配置仅允许用户通过指定协议访问 EdgeOne 站点。
连接类攻击防护	支持对连接型攻击进行防护，对连接行为异常的客户端自动封禁。
特征过滤	在 DDoS 攻击中支持针对 IP、TCP 及 UDP 报文头或载荷中的特征自定义拦截策略。
区域封禁	在 DDoS 攻击中通过匹配区域的方式来限制对 EdgeOne 站点的访问。

使用独立 DDoS 防护

最近更新时间：2023-10-11 10:30:37

背景介绍

如果您的业务对接入服务有如下要求:
1. 需要承诺防护容量的 DDoS 防护服务。如：金融业务、游戏平台服务等。
2. 在遭受大规模 DDoS 攻击时，平台默认防护下的业务可能会由于业务调度而改变解析 IP，从而影响到业务正常运行。您有需要持续保持会话状态业务，包括保持 DNS 解析 IP 不变、维持 TCP 长连接和 HTTP 长会话状态。如：多人在线游戏服务、语音服务等。
3. 需要定制网络层 DDoS 防护策略或网络层管控策略。如：需要丢弃来自指定地区的客户端流量。

建议您选购独立 DDoS 防护服务。独立 DDoS 防护服务在平台默认防护基础上，进一步提供：
1. 常态接入清洗中心，持续检测清洗并过滤恶意流量。
2. 承诺的防护容量，防护过程中保持会话状态稳定。
3. 可定制的 DDoS 防护策略，包括基于 IP 和客户端区域的管控选项。
帮助您缓解 DDoS 攻击风险，保障业务稳定。

使用指引

独立 DDoS 防护可应用于七层业务以及四层业务中，您可以参照以下不同的场景来了解如何为您的站点开启独立 DDoS 防护。
说明：
独立 DDoS 防护仅支持 2023 年 07 月 01 日后接入的企业版套餐使用。如您在此日期之前接入了 EdgeOne企业版并希望使用独立 DDoS 防护，请联系售后或技术支持。

场景一：为七层站点开启独立 DDoS 防护

场景示例

您通过站点域名 `onelogin.example.com` 提供了 HTTPS 统一登录服务（SSO，Single-Sign-On），主要服务于中国大陆地区用户，由于经常被 DDoS 攻击会导致用户无法正常登录，预计日常攻击量级为 30Gbps，高峰期可能达到 50Gbps，需要接入独立 DDoS 防护以确保提供稳定可用服务。

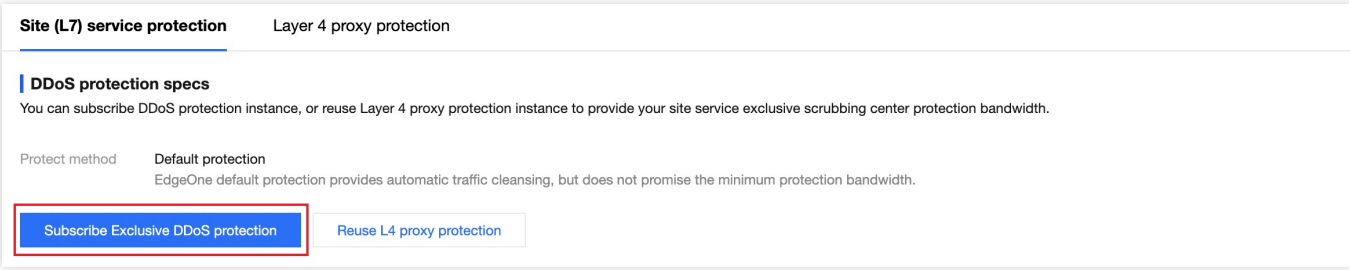
注意事项

七层站点内的独立 DDoS 防护创建后，暂不支持在控制台内退订，如需退订请联系腾讯云商务。

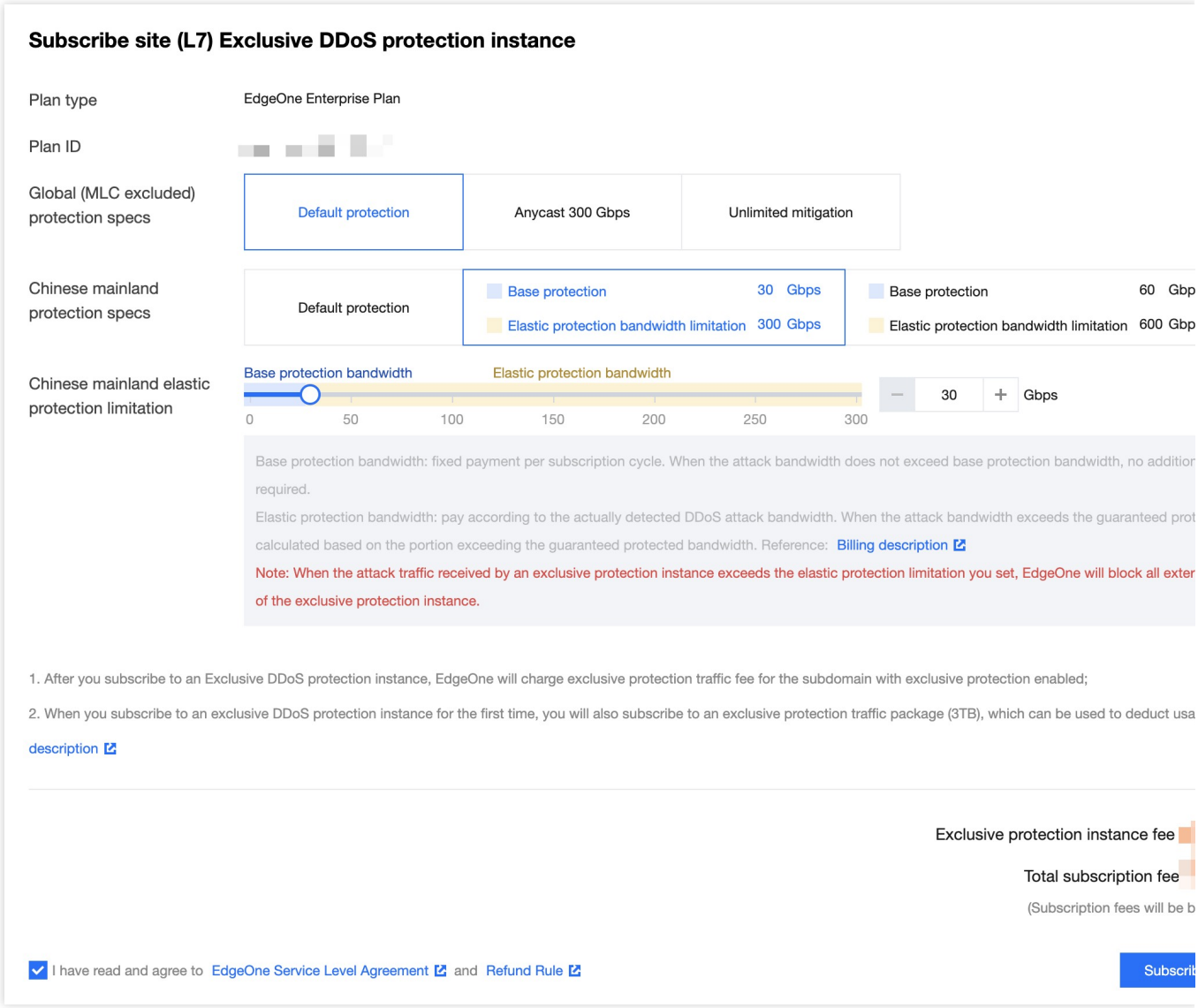
开启或关闭 DDoS 防护过程中，会对业务造成影响（连接重置等），影响时长预估为启用或关闭一般 2-3 分钟左右生效，如有本地或运营商 DNS 缓存时，切换可能更晚生效，具体时效时长取决于客户端所使用的 DNS 记录的 TTL 配置。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **DDoS 防护**。
3. 在站点（七层）服务防护页签，单击**订阅独立 DDoS 防护**。



4. 在订阅独立 DDoS 防护实例页面，选择需要订阅的防护区域以及防护规格。以本场景为例，根据服务区域及历史攻击量级，可选择订阅中国大陆可用区保底 30Gbps，弹性容量防护峰值为 50Gbps。



5. 确认相关费用信息后，勾选同意相关用户协议，并单击**立即订阅**，将开始为您自动下发独立 DDoS 防护实例配置。

6. 实例下发完成后，您可以在防护配置页面内，为所有域名开启独立 DDoS 防护，或者选择该场景内的 `onelogin.example.com`，为该域名开启独立 DDoS 防护。

7. 如果对单域名启用独立 DDoS 防护，将弹出部署确认窗，单击**确认**后开始部署，等待部署完成后即可生效。

场景二：为四层代理实例开启独立 DDoS 防护

场景示例

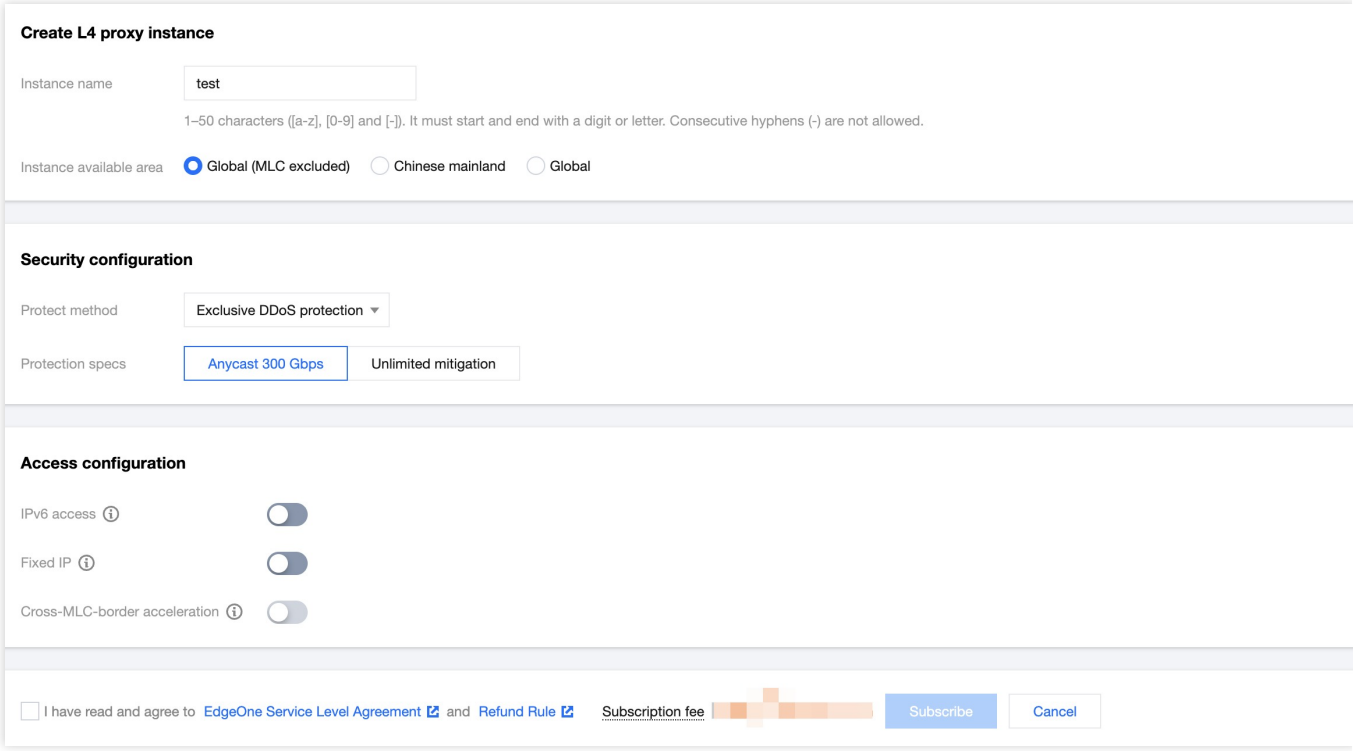
您有一款即将发布上线的游戏，需借助四层代理加速来优化玩家登录体验，通过 80 端口转发 TCP 流量数据，该游戏主要在海外发行， 预计在上线期间可能遭遇大流量 DDoS 攻击（不超过300 Gbps），可通过接入独立 DDoS 防护以确保在发布和运营期间的登录接口服务稳定，避免玩家流失。

注意事项

当前仅允许在新建四层代理实例时选用独立 DDoS 防护，创建后不可修改、不可变更；
四层代理的独立 DDoS 防护创建后，暂不支持动态开启/关闭。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**四层代理。**
3. 在四层代理管理实例页面，单击**新建四层代理**。
4. 新建四层代理实例时，在安全防护配置中，可选择对应的防护方式，切换为独立 DDoS 防护，以当前场景为例，可选择 Anycast 联防 300Gbps。



5. 确认相关用户协议以及价格信息后，点击订阅，完成四层代理实例创建。创建后，平台会自动为该实例下发独立 DDoS 防护配置；
6. 下发配置完成后，您可以点击**配置**，进入该实例配置界面，添加需要加速的端口信息以及源站地址，点击**保存**，即可开启四层代理加速。

场景三：七层站点复用四层代理实例 DDoS 防护资源

场景示例

假设您当前的邮箱 Exchange 服务同时通过 HTTPS 协议和多个 TCP/UDP 协议在内的多种协议提供服务，近期遭受了超过 200Gbps DDoS 攻击。由于其业务架构特点同时具有 HTTPS 和 TCP/UDP 服务，黑客可以同时通过 HTTPS 或者 TCP/UDP 发起 DDoS 攻击。因此，需要同时为七层站点和四层代理提供安全防护。

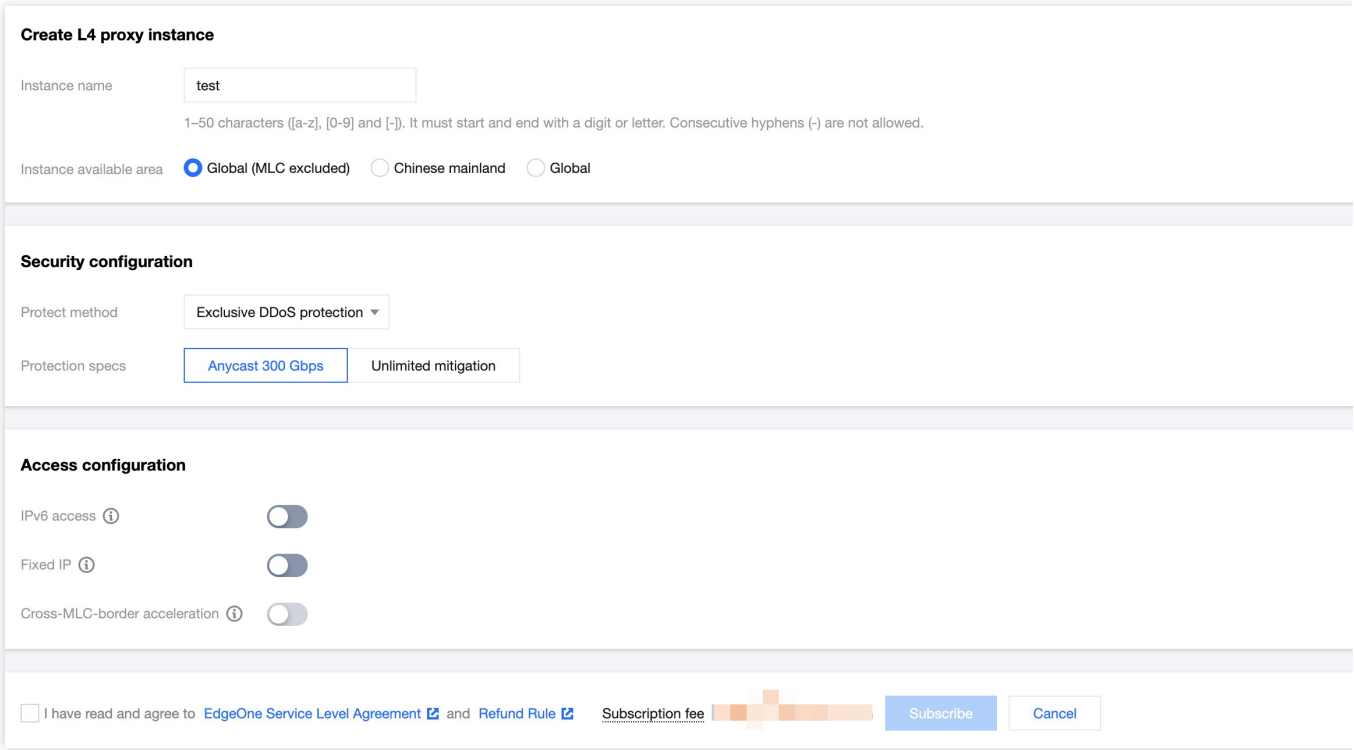
注意事项

七层站点复用四层代理的独立 DDoS 防护时，需要在独立 DDoS 防护内配置端口过滤，放行七层流量访问时使用的端口，避免七层流量被拦截。
当前功能仍在内测中，如有需要，您可联系腾讯云商务开通。

操作步骤

步骤1：新建四层代理实例并开启防护

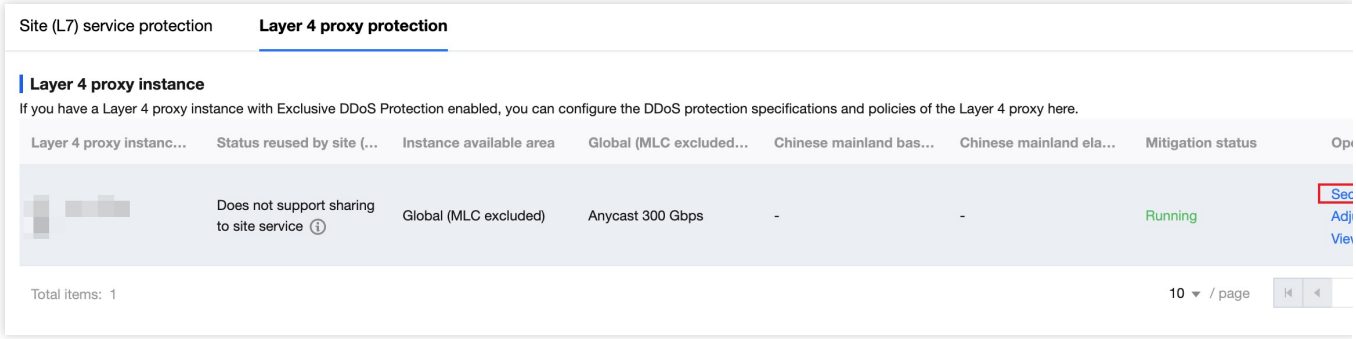
1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击站点列表，在站点列表内单击需配置的站点，进入站点详情页面。
2. 在站点详情页面，单击**四层代理**，在四层代理管理实例界面内，点击**新建四层代理**。
3. 新建四层代理实例时，在安全防护配置中，可选择对应的防护方式，切换为独立 DDoS 防护，以当前场景为例，可选择 Anycast 联防 300Gbps。



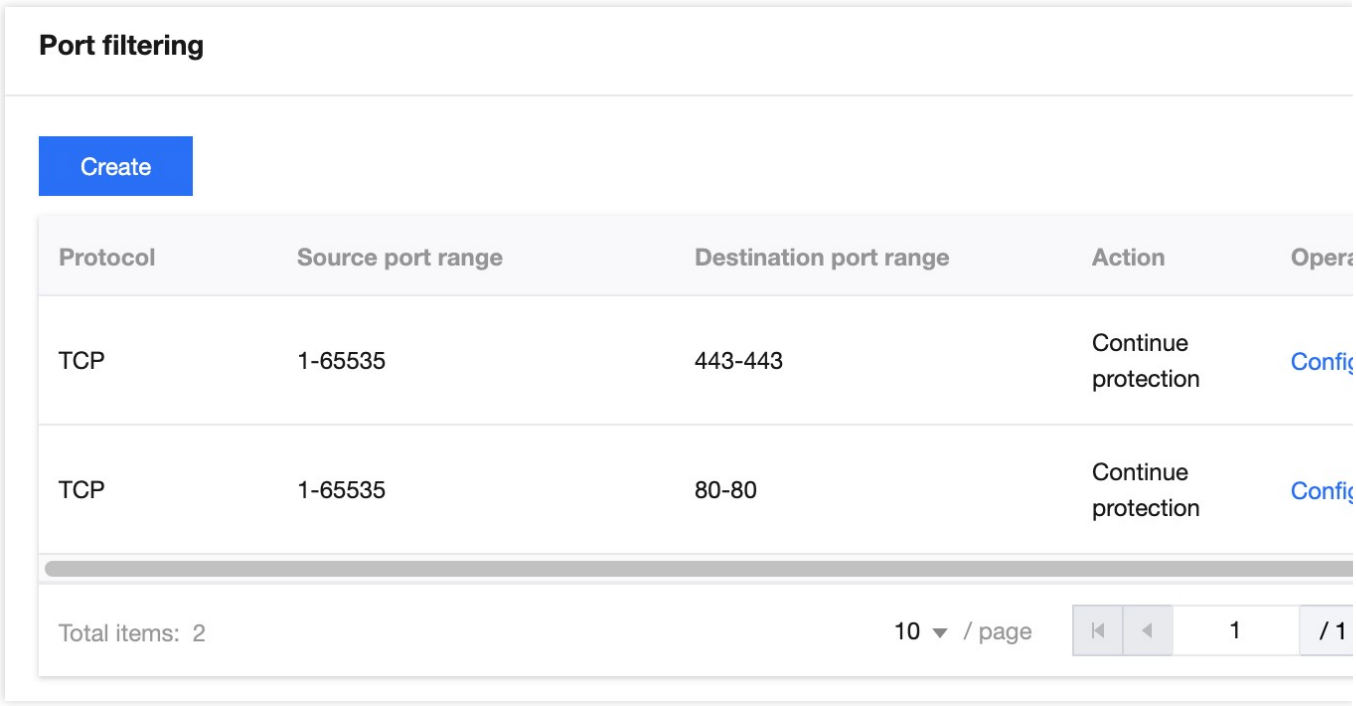
4. 确认相关用户协议以及价格信息后，点击订阅，完成四层代理实例创建。创建后，平台会自动为该实例下发独立 DDoS 防护配置；
5. 下发配置完成后，您可以点击**配置**，进入该实例配置界面，添加需要加速的端口信息以及源站地址，点击**保存**，即可开启四层代理加速。

步骤2：在四层代理安全防护实例中，放行七层访问流量

1. 四层代理配置完成后，您可以通过菜单 安全防护 > DDoS 防护，在四层代理防护内，选择步骤1所创建的四层代理实例，点击防护配置；

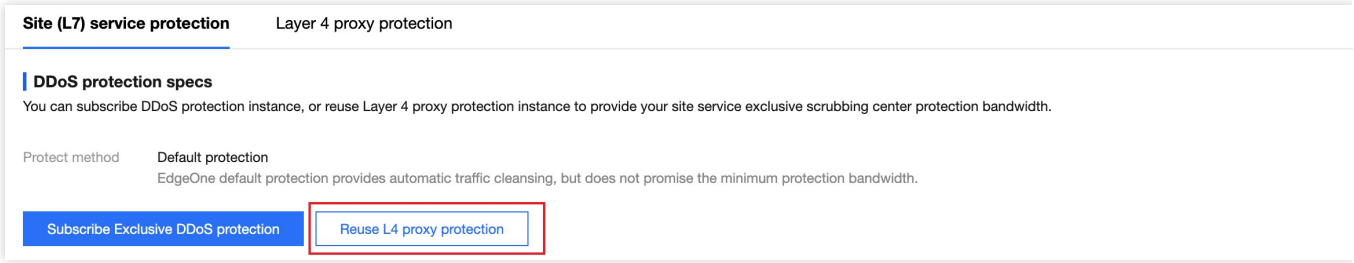


2. 在防护配置中，找到端口过滤卡片，点击**设置**进入配置界面；点击**新建**，配置放行源端口范围为1-65535，目的端口范围443的规则，动作选择为继续防护，放行对应的七层流量，点击**保存**即可生效。通过同样的步骤再添加一条规则放行80端口。完整配置规则如下：

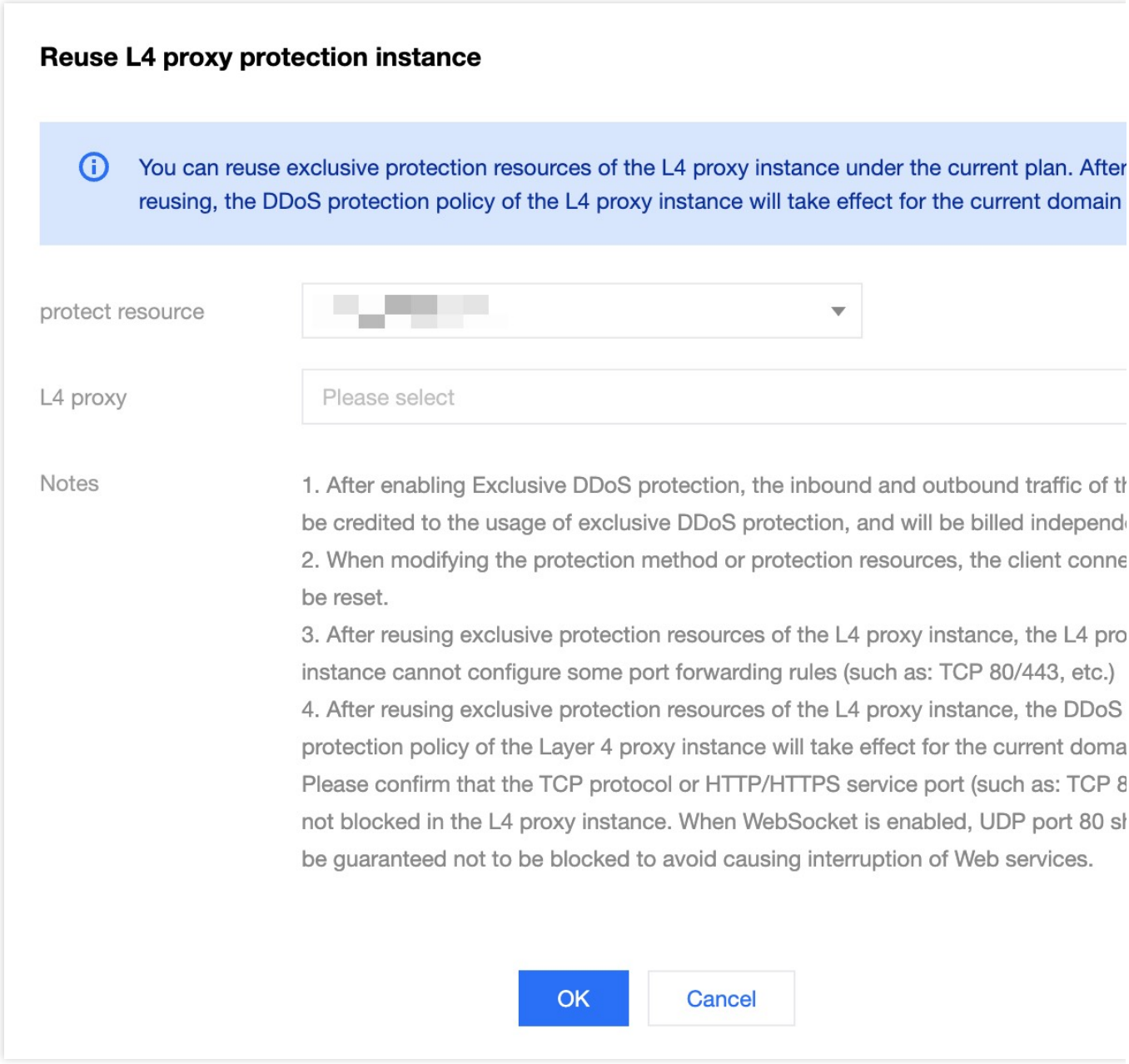


步骤3：复用四层代理防护实例，为七层站点域名提供防护

1. 完成步骤2后，点击 安全防护 > DDoS 防护，在站点（七层）服务防护中，点击复用四层代理防护；



2. 选择需要复用的四层代理防护资源后，点击确定，将开启自动下发独立 DDoS 实例配置；



3. 实例下发完成后，您可以在防护配置界面内，为所有域名开启独立 DDoS 防护，或者选择该场景内的 `exchange.example.com`，为该域名开启独立 DDoS 防护。

相关参考

工作原理

开启独立 DDoS 防护后，将按下列流程处理流量：

1. 客户端解析服务 DNS 记录时，将获得清洗中心地址。
2. 客户端访问服务时，清洗中心首先对流量进行清洗，自动识别并过滤其中的网络层 DDoS 攻击流量。如果当前业务已接入四层代理，过滤后流量由四层代理服务转发加速。

如果您的站点包含七层站点加速，流量将继续按照如下步骤转发：

3. 经过 SSL 认证后，HTTPS 协议请求继续经过 Web 防护、Bot 管理安全策略进行防护；
4. 通过安全模块校验的请求将继续进行站点缓存、站点加速、回源服务等功能模块。

配置独立 DDoS 防护策略
调整 DDoS 防护等级

最近更新时间：2023-10-12 17:13:54

DDoS 防护等级是 EdgeOne DDoS 防护为您提供的默认防护策略模版，DDoS 防护将根据防护等级，自动拦截符合特征的流量攻击，以下是各个防护等级的防护策略说明：

说明：

该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置。

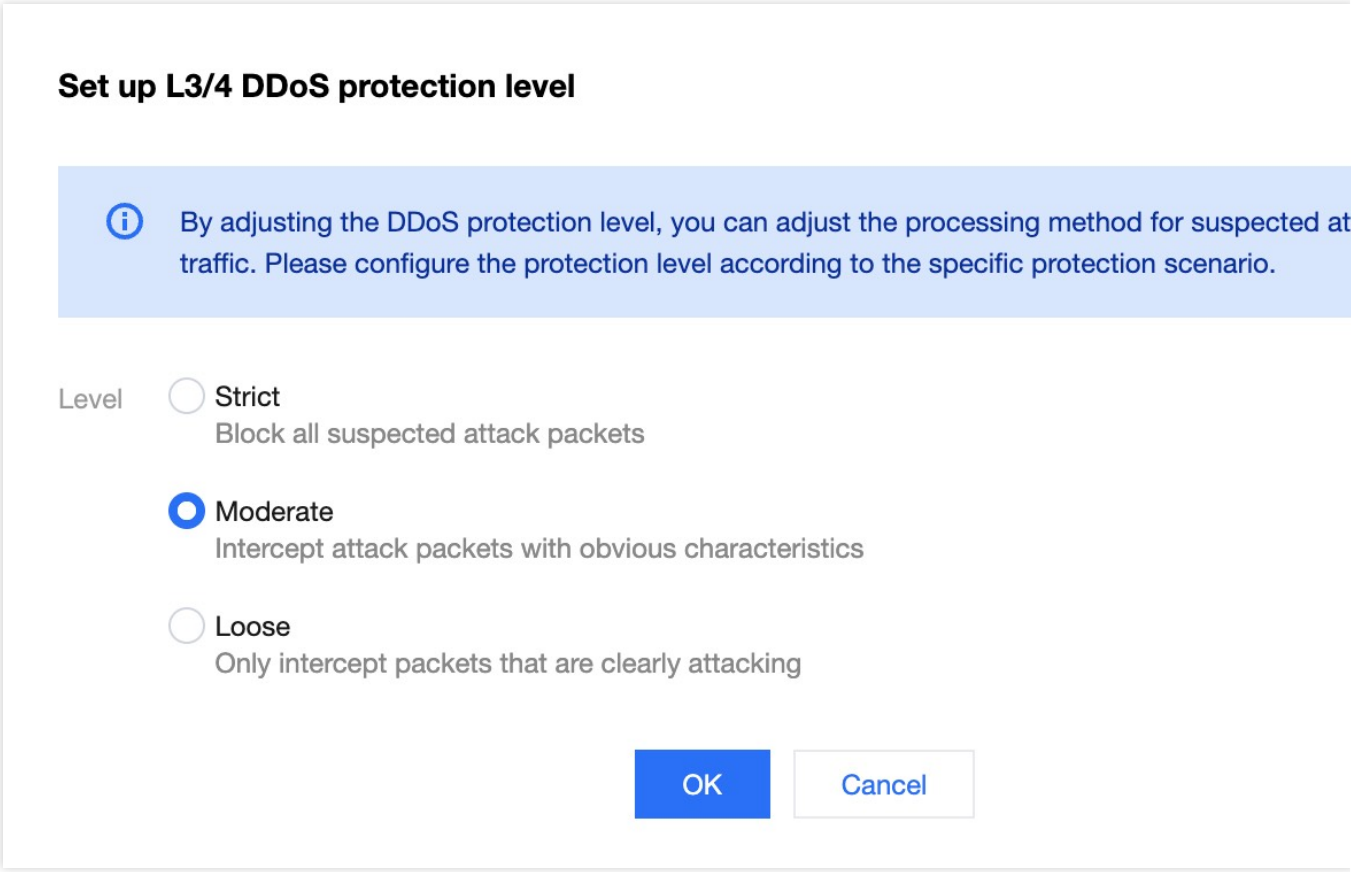
各个防护等级防护策略

对比项		**宽松** 清洗策略相对宽松，仅对具有明确攻击特征的攻击包进行防护。建议在怀疑有误拦截时启用，遇到复杂攻击时可能会有攻击透传。	**适中（默认）** 清洗策略适配绝大多数业务，可有效防护常见攻击。DDoS防护默认为适中模式。	**严格** 清洗策略相对严格，建议在正常模式出现攻击透传时使用。
具有明确攻击特征的数据包	SYN数据包	过滤	过滤	过滤
	ACK数据包	过滤	过滤	过滤
	UDP数据包	过滤	过滤	过滤
不符合协议规范的数据包	TCP数据包	过滤	过滤	过滤
	UDP数据包	过滤	过滤	过滤
	ICMP数据包	过滤	过滤	过滤
基于威胁情报攻击数据包		不过滤	过滤	过滤
对部分访问源 IP 进行主		不过滤	过滤	过滤

动验证			
ICMP攻击包	不过滤	不过滤	过滤

调整防护等级

如果您的业务存在以下两种情况，建议您调整防护等级：
当前业务运行过程中，查看安全日志分析中，存在误拦截时，为了保障业务的可用性，您可以调整降低防护策略等级为宽松；
当前业务运行过程中，在适中防护等级下仍发现有攻击透传至源站，建议您调高防护等级为严格。
您可以参照以下步骤调整：
1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 找到 L3/4 DDoS 防护等级卡片，点击设置，调整防护等级；



独立 DDoS 攻击流量告警

最近更新时间：2023-10-13 14:15:46

DDoS 攻击流量告警功能允许用户为 DDoS 防护实例设置自定义攻击流量速率告警阈值。当检测到的攻击流量速率超过设定阈值时，系统会发送告警通知，帮助用户及时了解并应对潜在的 DDoS 攻击。收到攻击流量速率告警后，用户应关注业务运行情况，参考连接数、访客量、正常会话数等正常业务指标，结合在线用户数等业务指标，对业务健康度进行评估，判断是否受到了 DDoS 攻击影响。

说明：

此功能仅适用于单独订阅了独立 DDoS 防护实例用户，且告警仅针对 L3/L4（网络层）的攻击流量速率。

场景：为四层代理的独立 DDoS 防护实例配置告警阈值

示例场景

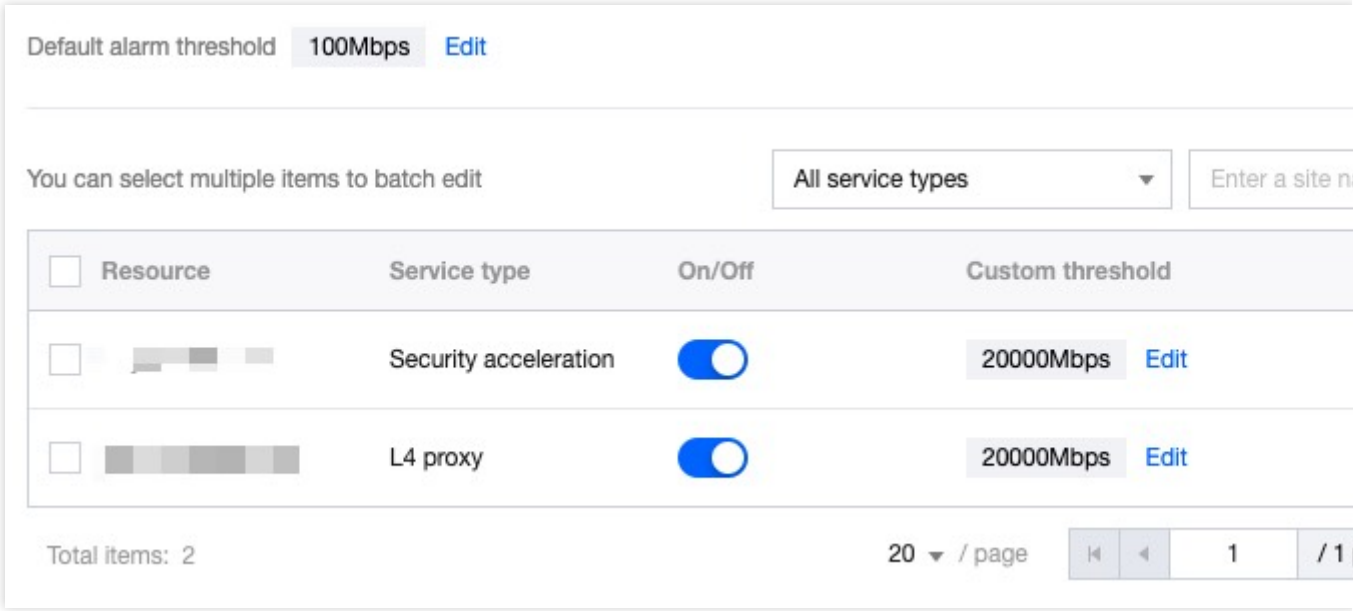
某游戏客户的业务当前已为四层代理服务购买的独立 DDoS 防护能力，保底防护量为30,000Mbps，当遇到 DDoS 攻击流量超过20,000Mbps 时，需要提前重点知晓并关注以便客户及时采取措施升级防护能力，以免影响业务的正常访问。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **告警通知推送**，进入告警通知推送详情页面。
3. 在 DDoS 攻击流量告警卡片中，单击**设置**。
4. 在告警配置页面中，以当前场景为例，可选择需要配置的四层代理实例，在开启自定义阈值开关后，单击**编辑**，修改告警阈值为20000Mbps ，单击**保存**，即可生效。

说明：

默认告警域名为针对所有业务类型生效，如果您需要自定义告警阈值，需要开启自定义阈值开关。



相关参考

监控范围

DDoS 攻击流量告警功能监控范围是对应到 IP。在实际运营中，多个域名的服务可能使用同一个防护实例 IP，因此告警针对的是防护实例，而不是具体域名。

设置的告警阈值仅针对检测到的攻击流量速率，而非全量业务流量速率。

触发方式

注意：

攻击流量速率告警基于瞬时峰值，而控制台上的攻击流量速率趋势图是基于分钟维度的平均值，因此两者对比时可能存在差异。

DDoS 攻击流量告警功能统计方式为攻击流量速率瞬时峰值，单位为 Mbps。告警功能会监控防护实例的流量情况，当攻击流量速率达到或超过用户设定的阈值时，发送告警通知。

配置 IP 黑白名单

最近更新时间：2023-10-11 10:31:40

功能说明

EdgeOne DDoS 防护服务支持通过配置 IP 黑名单和白名单的方式，控制客户端源 IP 封禁或者放行访问请求，从而限制访问您业务资源的用户。配置 IP 黑白名单针对源 IP 设置过滤或放行规则，当白名单中的 IP 访问时，将被直接放行，不经过 DDoS 防护内其他防护策略过滤（不影响其他模块的防护策略），当黑名单中的 IP 访问时，将会被直接阻断。

说明：

1. 该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置；
2. IP 黑白名单规则保存后，将在5-10秒内生效。
3. IP 黑白名单最多可以配置8个 IP 分组，每个分组最多填写2000个 IP。

使用场景

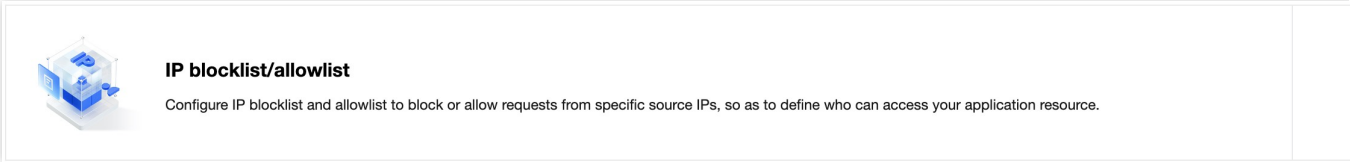
攻击时仅允许白名单内 IP 访问：在遭受 DDoS 攻击时，仅允许受白名单信任的用户访问该站点，可以大幅度降低网站的安全风险，但是可能会影响不在白名单内的正常 IP 访问请求。

黑名单直接拦截攻击源 IP：对已确定为攻击源 IP 添加为黑名单，阻断来自该 IP 的所有访问请求，降低 DDoS 清洗流量，减少攻击透传。

场景一：通过 IP 白名单，添加受信任 IP 放行请求

针对站点 `example.com` 下的所有业务域名，IP 地址段 `1.1.1.1/24` 是该站点信任的访问 IP，为了避免受信任 IP 被误拦截，可将该 IP 添加至白名单内，不经过 DDoS 防护模块清洗。操作步骤如下：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在 IP 黑白名单卡片中，单击**设置**，进入 IP 黑白名单配置页面。

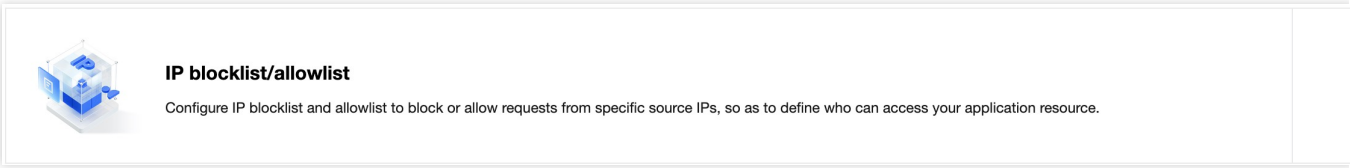


5. 在 IP 黑白名单页面中，单击**新建**，以当前场景为例，输入 IP 段 `1.1.1.1/24`，类型选择为白名单，单击**保存，即可生效。**

场景二：通过 IP 黑名单，永久阻断攻击源 IP 访问请求

针对站点 `example.com` 下的所有业务域名，IP 地址 `1.1.1.1` 已被确认为攻击源 IP，可直接将该 IP 添加至黑名单内，阻断所有来源该 IP 的访问请求。操作步骤如下：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在 IP 黑白名单卡片中，单击**设置**，进入 IP 黑白名单配置页面。



5. 在 IP 黑白名单页面中，单击**新建**，以当前场景为例，输入 IP `1.1.1.1`，类型选择为黑名单，单击**保存，即可生效。**

配置区域封禁

最近更新时间：2023-10-11 10:32:05

功能说明

如果您发现您的所有攻击都来源于特定地区，或者您的业务仅允许特定地区访问，不信任其他地区来源的访问。EdgeOne 支持通过指定区域列表的方式，按照源 IP 地理区域在清洗机房进行一键封禁，帮助您自定义阻断来自指定地区的源 IP 的访问请求。开启区域封禁后，由封禁地区到 EdgeOne 站点的流量将被丢弃。支持多地区、国家进行流量封禁。

说明：

1. 该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置；
2. 在配置了区域封禁后，该区域的攻击流量依然会被平台统计和记录，但不会流入业务源站。

适用场景

排除受信任区域外的所有攻击行为：当前业务的仅适用于特定地区访问，通过区域封禁可以在 DDoS 清洗中一键封禁其他区域的访问客户端，以避免其他区域的攻击来源透传至源站。

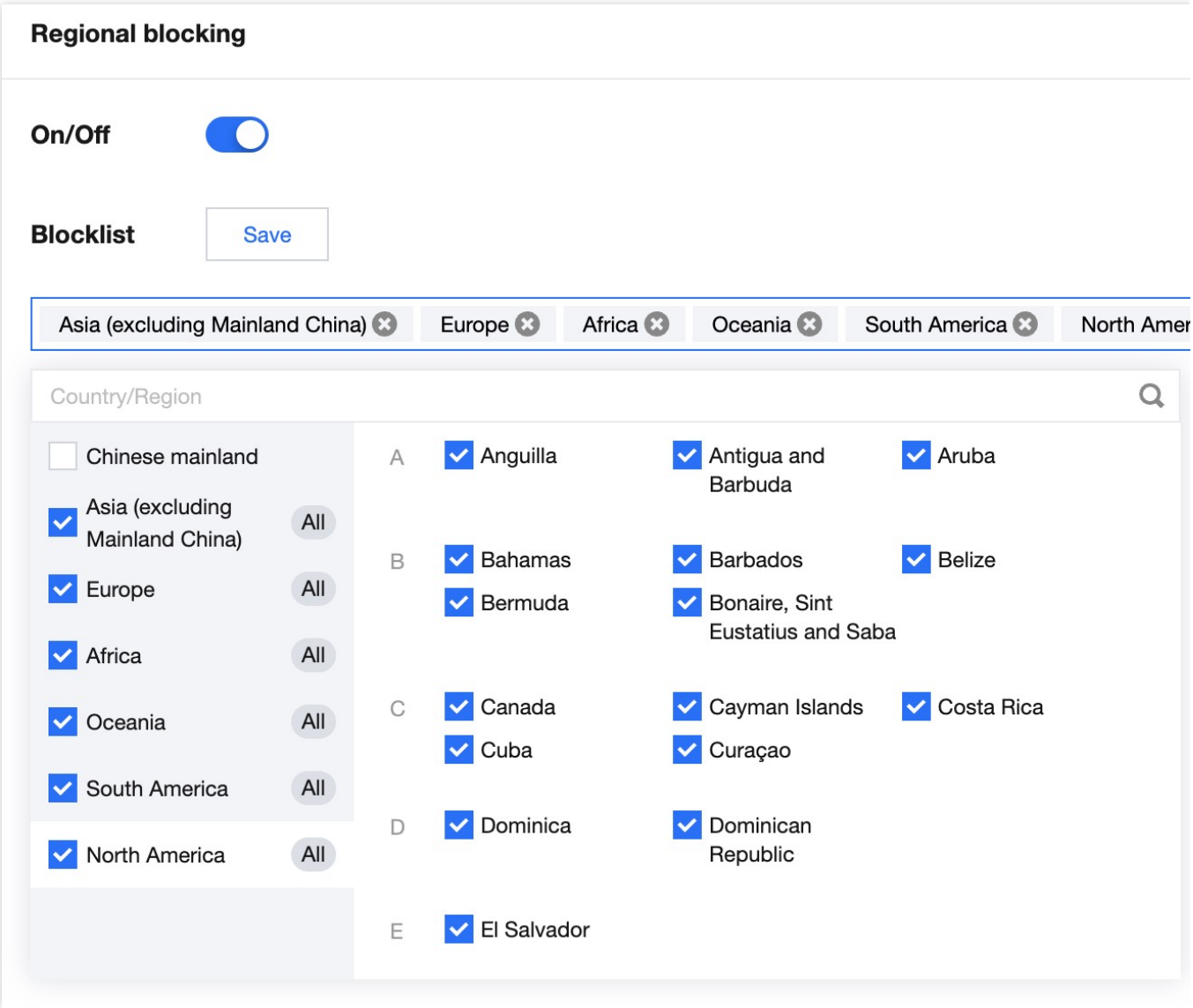
一键封禁区域集中的攻击行为：如果当前站点的攻击来源主要为特定地区，您可以通过区域封禁，在 DDoS 清洗中一键封禁来自该区域的所有访问请求，能更有效地防止该区域攻击透传。

操作步骤

例如：当前站点用户都在中国，只允许中国用户访问该站点，不信任其他地区来源的访问请求，为杜绝其他区域可能的攻击行为，在产生 DDoS 攻击时，其他区域请求全部封禁。操作步骤如下：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在区域封禁卡片中，单击**设置**，进入区域封禁页面。

5. 在区域封禁配置页面，点击封禁列表右侧**编辑**按钮，选择封禁区域，以当前场景为例，全选除中国大陆以外的所有区域。



6. 单击**保存**，完成区域封禁配置即可。

配置端口过滤

最近更新时间：2023-10-11 10:32:30

功能说明

端口过滤用于通过指定端口和协议的方式精准制定防护策略，管控客户端可访问 EdgeOne 的端口和协议。开启端口过滤后，可以根据需求自定义协议类型、源端口范围、目的端口范围的组合，并对匹配中的规则进行设置拦截、放行、继续防护的策略动作。

说明：

该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置；

适用场景

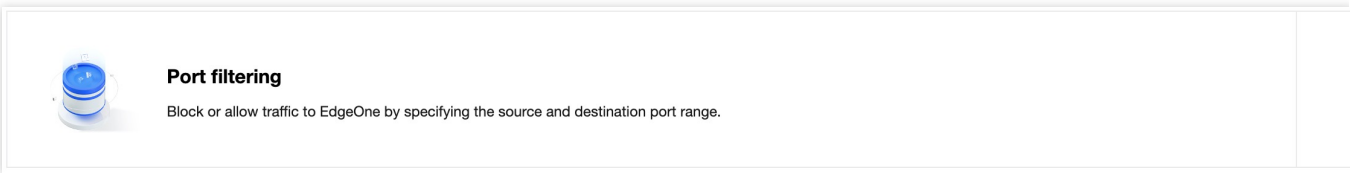
源站存在 UDP 业务，通过端口过滤 UDP 反射攻击：如果当前您的源站业务存在 UDP 连接，无法直接封禁 UDP 协议访问，您可以通过在端口过滤中，配置在 DDoS 清洗需拦截的 UDP 访问端口，防止 UDP 反射攻击透传。常见的 UDP 反射攻击端口包括：1-52、54-161、389、1900、11211。

清洗非允许的端口访问来源：当您的源站仅开放指定端口访问时，可以通过端口过滤，配置在 DDoS 清洗后仅允许访问的端口，直接丢弃所有来自其余端口的访问连接，减少攻击透传。

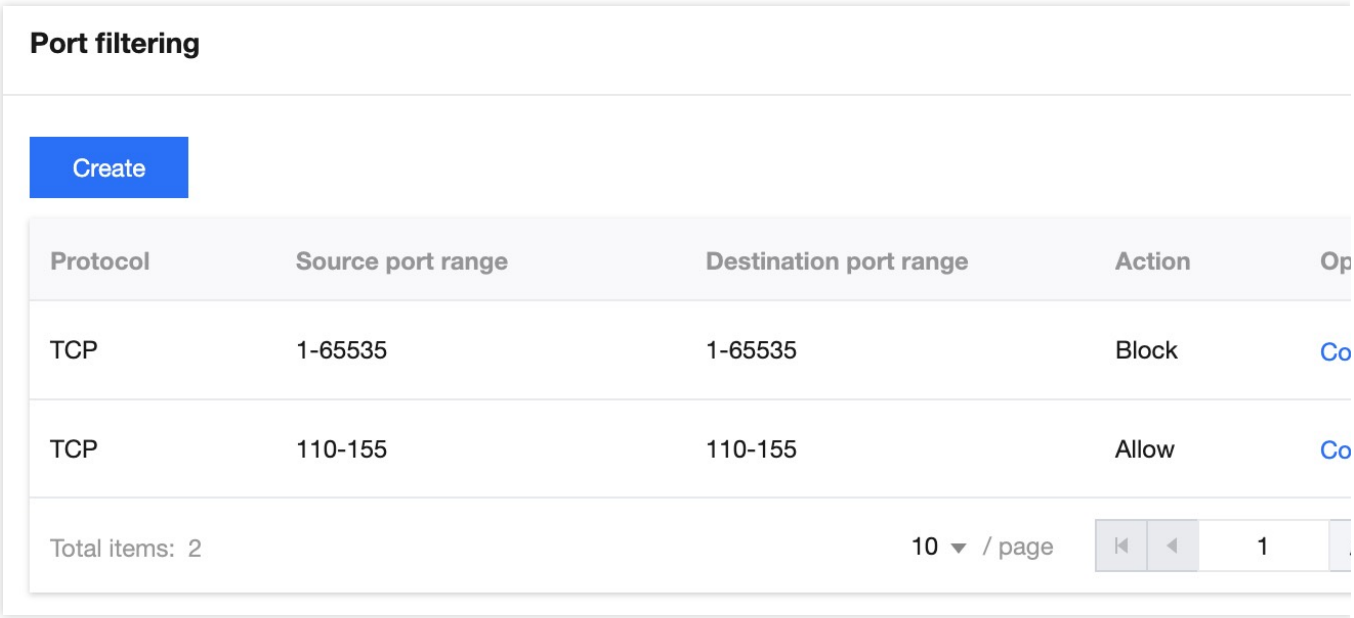
操作步骤

例如针对站点 `example.com` 下的所有业务域名，业务仅对外开放了 TCP 协议的 110-155 号端口，其余端口不允许访问。操作步骤如下：

1. 登录边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在端口过滤卡片中，单击**设置**，进入端口过滤页面。



5. 在端口过滤页面中，单击**新建**，创建端口过滤规则，以当前场景为例，新建两条规则，拦截所有协议选择为 TCP 协议，源端口范围填写 1-65535，目的端口范围填写为 10-155 端口，选择不同防护动作并填写相关字段，单击**保存**。



字段	说明
协议	可选全部、TCP或UDP协议
源端口范围	指客户端发起访问的端口信息，支持填写范围：1-65535
目的端口范围	指客户端访问的目的端口信息，支持填写范围：1-65535
动作	拦截：阻断该请求； 放行：放行该请求，并不再匹配剩余的防护策略。 继续防护：放行当前请求，继续匹配其余的防护策略。

配置特征过滤

最近更新时间：2023-10-11 10:32:58

功能说明

特征过滤可以精准制定针对业务报文特征或攻击报文特征的防护策略来防止畸形报文攻击透传。EdgeOne 支持针对 IP、TCP 及 UDP 报文头或载荷中的特征自定义拦截策略。开启特征过滤后，您可以将源端口、目的端口、报文长度、IP 报文头或荷载的匹配条件进行组合，并对命中条件的请求设置丢弃、放行、丢弃并拉黑、继续防护等策略动作。

说明：

该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置。

适用场景

站点业务接入 EdgeOne 后，如果您需要针对性地管理具有固定特征的访问请求，则您可以为该站点开启特征过滤并设置精确访问控制规则。特征过滤访问控制规则由匹配条件与匹配动作构成。

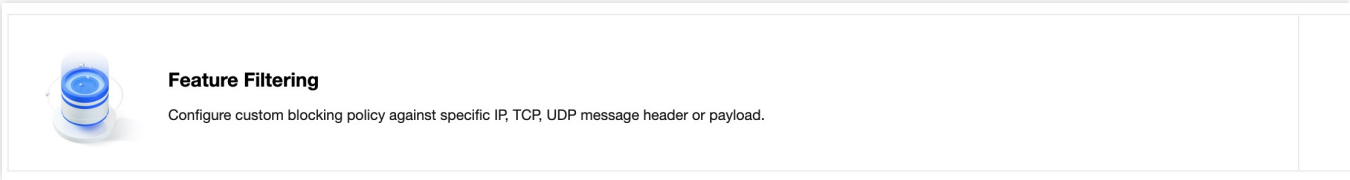
匹配条件定义了要识别的请求特征，具体指访问请求中TCP/UDP协议字段的属性特征。

匹配动作定义了访问请求命中匹配条件时，对访问请求执行的动作，具体包括拦截、放行、丢弃并拉黑、继续防护。

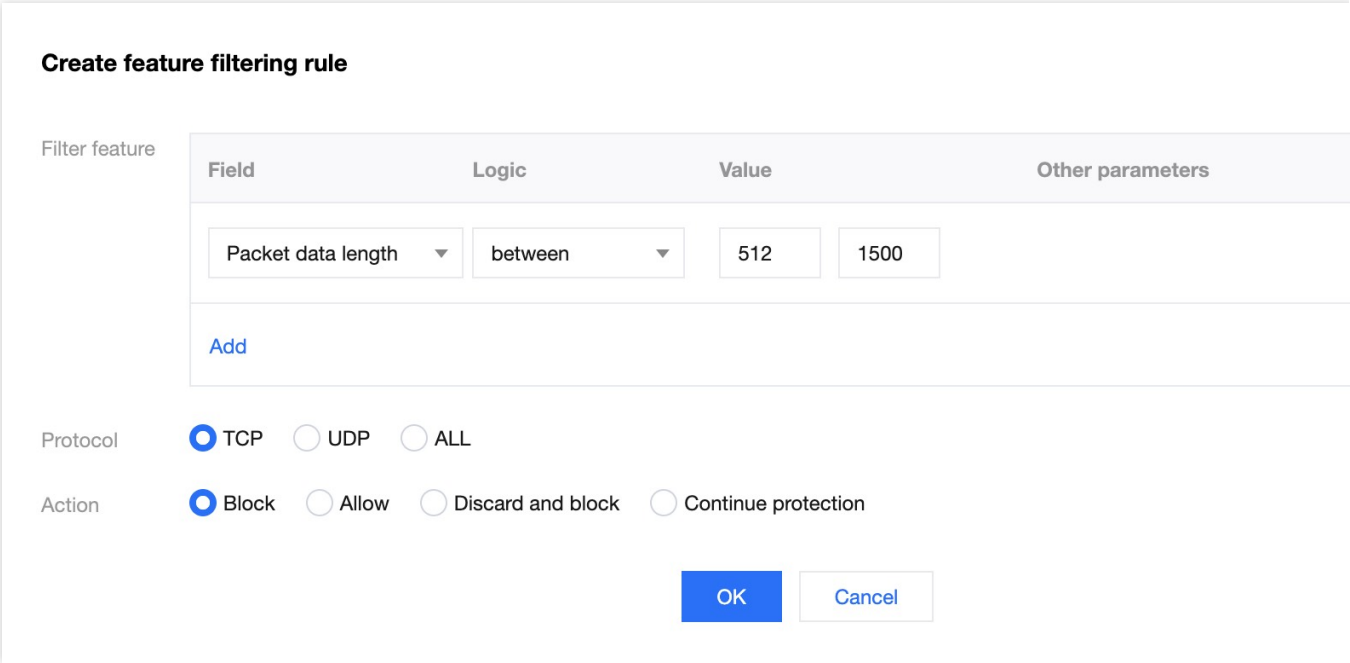
操作步骤

例如：针对站点 `example.com` 下的所有业务域名，对外仅开放的 TCP 业务包长度要求均不大于 512 字节，对不符合该特征的请求全部拦截。操作步骤如下：

1. 登录边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在特征过滤卡片中，单击**设置**，进入特征过滤页面。



5. 在特征过滤页面中，单击**新建**。
6. 在新建特征过滤对话框中，创建特征过滤规则，根据需求，选择不同防护动作并填写相关字段，单击**确定**。



各个特征字段说明如下：

过滤特征	说明	其他参数
源端口	指访问来源端口 支持输入1-65535范围的端口号 支持逻辑等于或介于	/
目标端口	指访问目标端口 支持输入1-65535范围的端口号 支持逻辑等于或介于	
包长度	指访问报文的数据包长度 支持输入1-1500范围数字 支持逻辑等于或介于	
IP 首部开始检测	支持正则匹配或关键词匹配，其中关键词通过偏移量及检查深度匹配	**偏移量**：UDP或TCP头部后数据体（payload）的偏移量，可选范围：0~1500，单位：Byte。

TCP/UDP 首部开始检测	支持正则匹配或关键词匹配，其中关键词通过偏移量及检查深度匹配	偏移量为0时，从数据体的第一字节开始匹配。 **检查深度：**要匹配的数据体（payload）内容，需要输入以0x开头的十六进制字符串
载荷开始检测	指跳过IP首部和TCP/UDP首部，从报文所携带的载荷开始检测 支持正则匹配或关键词匹配，其中关键词通过偏移量及检查深度匹配	

配置协议封禁

最近更新时间：2023-10-11 10:33:21

功能说明

EdgeOne 支持对访问站点的源流量按照协议类型一键封禁。您可配置 ICMP 协议封禁、TCP 协议封禁、UDP 协议封禁和其他协议封禁，配置完成后，当检测到攻击流量有相关访问请求会被直接截断。

说明：

该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置；

适用场景

当您的网站不存在指定的访问协议时，可通过对指定协议一键封禁，在流量清洗时直接过滤对应协议的访问请求，防止相应请求透传至源站。

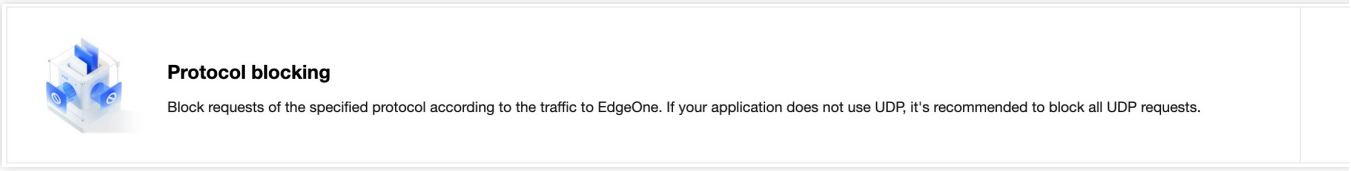
说明：

由于 UDP 协议无连接的特点（不像 TCP 具有三次握手过程）具有天然的安全性缺陷。若您没有 UDP 业务，建议封禁 UDP 协议。

操作步骤

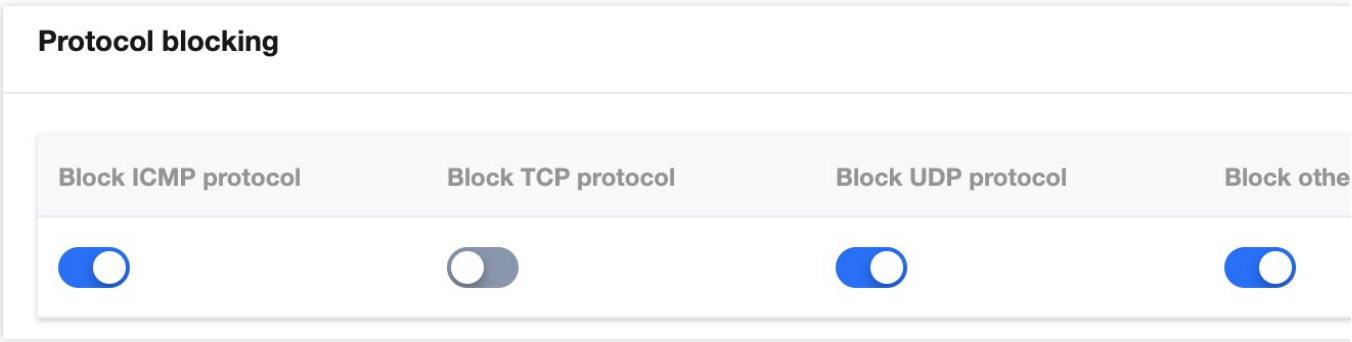
例如：针对站点 `example.com` 下的所有业务域名，对外仅开放 TCP 协议连接，封禁其他协议请求。操作步骤如下：

1. 登录边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在协议封禁卡片中，单击**设置**，进入协议封禁页面。



5. 在协议封禁页面，单击封禁所需协议开关

，以当前场景为例，打开 ICMP 协议、UDP 协议封禁、其他协议封禁开关，开启后，规则将立即生效，对应的协议请求将被阻断。



配置连接类攻击防护

最近更新时间：2023-10-11 10:33:44

功能说明

EdgeOne 支持对连接型攻击进行防护，对连接行为异常的客户端自动封禁。在源 IP 最大异常连接数开启防护后，当边缘安全加速平台检测到同一个源 IP 短时间内频繁发起大量异常连接状态的报文时，会将该源 IP 纳入黑名单中进行封禁惩罚，封禁时间为15分钟，等封禁解除后可恢复访问。

说明：

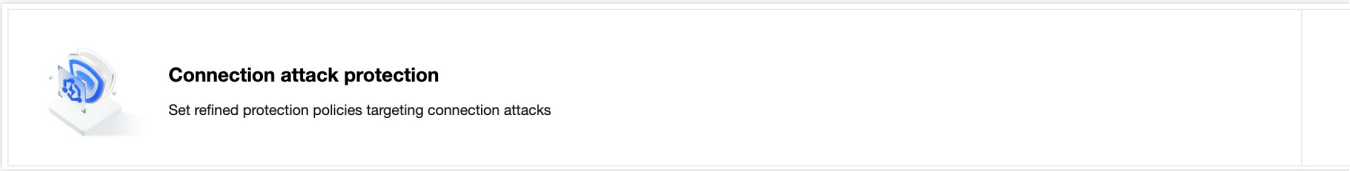
该功能仅在四层代理开启独立 DDoS 防护时支持，默认平台防护以及七层站点独立 DDoS 防护均不支持配置；

适用场景

为了防住大量连接耗尽源站的 TCP 连接资源或者网络资源，您可以通过配置连接类攻击防护保护源站。

操作步骤

1. 登录边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护> DDoS 防护**，进入 DDoS 防护详情页。
3. 在四层代理防护选项卡内，选择需要配置的四层代理防护实例，点击**防护配置**。
4. 在连接类攻击防护卡片中，单击**设置**，进入连接类攻击防护页面。



5. 在连接类攻击防护页面中，单击连接规则右侧的**编辑**，各连接规则说明及处置方式请参考相关参考。
6. 在配置规则对话框中，修改配置后，单击**确定**，即可完成下发规则。

相关参考

支持的连接规则

（单个源 IP）新建连接限制：通过限制单位时间内允许单个源 IP 发起的新建连接数量，避免攻击方通过大量空连接耗尽 TCP 连接资源。
（单个源 IP）并发连接限制：通过限制同一时间单个源 IP 开放状态的连接数量，避免攻击方通过大量并发连接耗尽 TCP 连接资源。
（单个源 IP）异常连接限制：通过限制同一时间单个源 IP 连接至 EdgeOne 的异常连接数量，避免有大量异常连接状态的高危客户端连接至源站，产生安全风险。异常连接可以自定义通过SYN报文占比、SYN报文数量、连接超时、异常空连接等不同维度规则组合判断。
全局新建连接限制：通过限制单位时间内允许通过 EdgeOne 对源站站点新建连接数量，避免攻击方通过大量空连接耗尽 TCP 连接资源。
全局并发连接限制：通过限制同一时间通过 EdgeOne 对源站站点开放状态的连接数量，避免攻击方通过大量并发连接耗尽 TCP 连接资源。
全局数据速率限制：通过限制同一时间通过 EdgeOne 转发至源站应用的数据速率，避免攻击方通过大量伪造请求消耗源站网络和计算资源。
全局包速率限制：通过限制同一时间通过 EdgeOne 转发至源站应用的包速率，避免攻击方通过大量伪造请求消耗源站网络和计算资源。

处置方式

限制新建连接：单个源 IP 规则下时，拒绝该 IP 新增的连接请求，全局策略下，拒绝所有新增的 TCP 连接请求。
断开连接并惩罚：断开该 IP 连接并封禁该 IP 15分钟。
丢弃超额数据：丢弃超出数据传输速率或者连接包速率的请求内容。

相关参考
处置方式

最近更新时间：2023-08-17 15:23:47

DDoS 防护模块提供多种处置方式。不同处置方式的处理规则如下：

处置方式	处置方式描述	后续动作
拦截（Deny）	直接丢弃请求数据包，并且不继续匹配其他策略	无
放行（Allow）	直接通过改请求数据包的访问，不再继续匹配其他策略	无
丢弃并拉黑	直接丢弃改请求数据包，并且将改IP拉入后台黑名单	无
继续防护	继续执行匹配其他策略	继续按顺序匹配其他策略

相关概念介绍

最近更新时间：2023-08-17 15:26:17

DDoS 攻击介绍

分布式拒绝服务攻击（Distributed Denial of Service，DDoS）是指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

网络层 DDoS 攻击

网络层 DDoS 攻击主要是指攻击者利用大流量攻击拥塞目标服务器的网络带宽，消耗服务器系统层资源，导致目标服务器无法正常响应客户访问的攻击方式。
常见攻击类型包括 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 以及 DNS/NTP/SSDP/memcached 反射型攻击。

传输层 DDoS 攻击

主要包括 Syn Flood、Ack Flood、UDP Flood、ICMP Flood。以 Syn Flood 攻击为例，它利用了 TCP 协议的三次握手机制，当服务端接收到一个 Syn 请求时，服务端必须使用一个监听队列将该连接保存一定时间。因此，它向服务端不停发送 Syn 请求，但不响应 Syn+Ack 报文，从而消耗服务端的资源。当服务端监听队列被占满时，服务端将无法响应正常用户的请求，达到拒绝服务攻击的目的。

应用层 DDoS 攻击

主要包括 DNS DDoS 攻击和 Web 应用 DDoS 攻击。DNS DDoS 攻击主要包括 DNS Request Flood、DNS Response Flood、虚假源+真实源DNS Query Flood。Web 应用 DDoS 攻击主要指 HTTP Get Flood、HTTP Post Flood 等。HTTP Get Flood 通常指黑客从 Web 服务或界面找出一些资源消耗较大的事务和页面，并对这些事务和页面不停地发送 HTTP Get 请求，从而导致 Web 应用服务器资源耗尽，无法提供正常服务，或导致数据中心入口网络带宽被占满，整个数据中心无法正常对外提供服务。

CC 攻击

CC 攻击主要是指通过恶意占用目标服务器应用层资源，消耗处理性能，导致其无法正常提供服务的攻击方式。常见的攻击类型包括基于 HTTP/HTTPS 的 GET/POST Flood、四层 CC 以及 Connection Flood 等攻击方式。

防护能力

防护能力指抵御 DDoS 攻击的能力， DDoS 防护承诺根据当前地域腾讯云最大 DDoS 防护能力提供全力防护。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云 DDoS 防护系统将自动对该 IP 的公网入向流量进行清洗。通过 BGP 路由协议将流量从原始网络路径中重定向到腾讯云 DDoS 清洗设备上，通过清洗设备对该 IP 的流量进行识别，丢弃攻击流量，将正常流量转发至目标 IP。通常情况下，清洗不会影响正常访问，仅在特殊场景或清洗策略配置有误时，可能会对正常访问造成影响。当流量持续一定时间（根据攻击情况动态判断）没有异常时，清洗系统会判定攻击结束，停止清洗。

Web 防护

概述

最近更新时间：2024-04-16 16:30:16

Web 防护功能提供对 HTTP/HTTPS 协议的应用层防护，您可以使用 EdgeOne 预设的安全策略，或者自己定义安全策略，识别并处置有风险的请求，保护您站点的敏感数据，并确保服务稳定运行。

说明：

EdgeOne 对被安全策略拦截的请求不会计费。

使用场景

Web 防护可对多种风险进行管控和缓解，典型场景包括：

漏洞攻击防护：对于涉及客户数据或敏感业务数据的站点，可以通过开启托管规则，拦截注入攻击、跨站点脚本攻击、远程代码运行攻击、第三方组件漏洞等恶意攻击请求。

访问管控：区分合法和未授权请求，避免敏感业务暴露到未授权的访客。包括外部站点链接管控、合作方访问管控、攻击客户端过滤等。

缓解资源占用：限制每个访客的访问频率，避免过度占用资源，导致服务可用性下降。EdgeOne 提供的 CC 攻击防护和速率限制可以有效缓解站点资源耗尽，以保障服务可用稳定。

缓解服务滥用：限制会话或者业务维度滥用，包括批量注册、批量登陆、过度使用 API 等恶意使用场景。并强化单一会话（如用户、订阅实例等）的用量限制，确保用户在合理限度内使用服务资源。

API 参数校验：校验 API 参数，确保请求合法性，控制接口暴露风险。

Web 防护功能

Web 防护提供下列功能，建议根据业务类型和业务预期的访问客户端类型进行配置：

说明：

不同的防护模块处置顺序优先级以及模块内相同优先级策略的处置动作执行优先级，详情请参见 Web 防护请求处理顺序。

防护模块	功能介绍
托管规则	识别请求头部或正文中的攻击特征（包括 SQL 注入、XSS 攻击、开源组件漏洞等多种攻击特征类别），并进行处置。规则由 EdgeOne 定义并自动更新。
CC 攻击防护	识别 CC 攻击（七层 DDoS 攻击），并进行处置。
自定义规则	按指定方式处置匹配条件的请求。

速率限制	统计一段时间内匹配条件的请求数量，当超过指定阈值时规则生效，处置匹配条件的请求。请求数量低于阈值后，处置动作维持生效一段时间，然后不再生效，直到再次触发。
Bot 管理	识别非人类访问行为（Bot 客户端），根据 Bot 客户端类型或行为特征进行处置。
防护例外规则	匹配条件的请求跳过指定安全模块扫描，不会命中对应模块中的规则。对于托管规则，可以配置更精细的例外，跳过指定托管规则扫描。

托管规则

最近更新时间：2024-04-16 16:30:16

概述

暴露的站点漏洞可能导致源站被入侵、敏感数据丢失，并可能进一步严重伤害您和用户的关系。托管规则为您的网站提供全面且实时的漏洞攻击防护，涵盖OWASP TOP 10 注1常见漏洞和攻击类型，如 SQL 注入、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）等。通过持续更新，这套规则库能有效应对新兴安全威胁，确保您的站点运行环境和敏感数据受到可靠保护。

说明：

注1：
OWASP TOP 10 列出了网络应用中常见和严重安全风险。这些风险代表了当前网络安全威胁的主要部分，因此覆盖这些场景对于保护网络应用的安全性至关重要。EdgeOne 提供的漏洞攻击防护规则集覆盖了全部 OWASP Top 10 风险场景，并针对 0-day 漏洞自动更新规则列表。
注2：托管规则默认仅扫描请求正文中前 10KB 内容。如果您订阅了企业版套餐，并且需要扫描更多请求正文数据，请联系您的商务进行扩展。
注3：不同套餐可支持的托管规则集不一致，详情请参考：套餐选型对比。

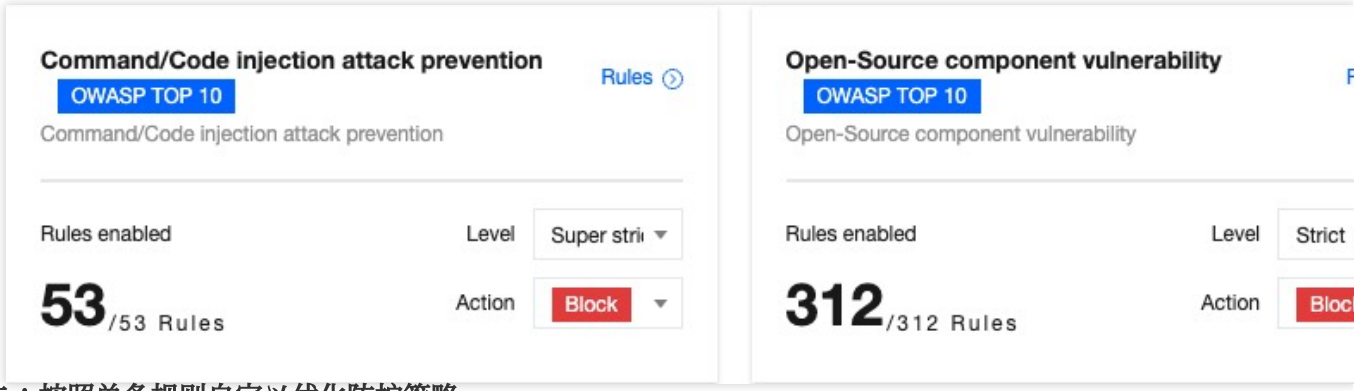
优化托管规则策略

如果您需要根据自身的实际业务情况和防护要求，自定义配置防护规则策略，您可以通过以下方式配置：

场景一：按规则类型配置全局防护等级策略

根据托管规则划分的规则类型，可针对该类型包含的所有规则，根据防护等级启用拦截。例如：当前站点域名 `www.example.com` 经常爆出开源组件漏洞，可以将开源组件漏洞内的所有规则，拦截严格及以下防护等级的所有规则。

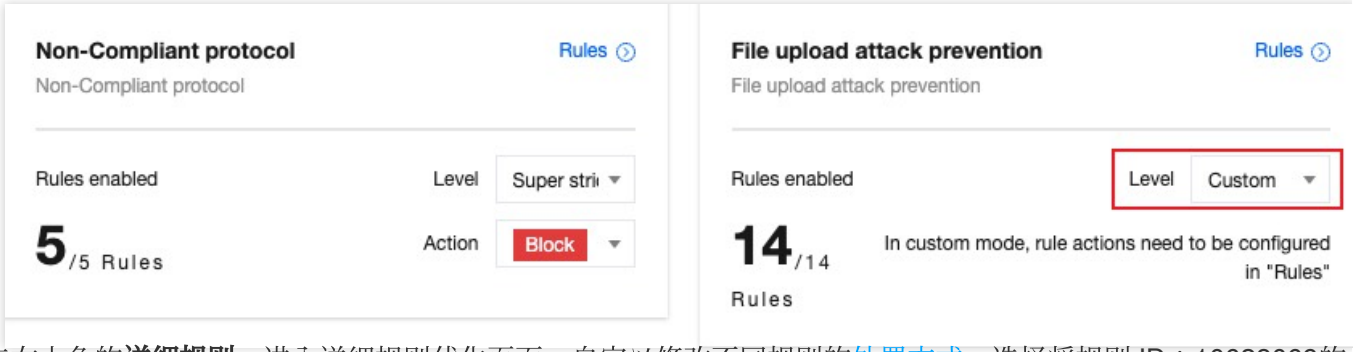
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Web 防护**。
3. 在 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。
4. 找到托管规则卡片，单击**设置**。
5. 在托管规则页面，找到开源组件漏洞规则卡片，单独配置 防护等级及 处置方式，调整防护等级为**严格**，处置方式为**拦截**，即可完成规则配置。



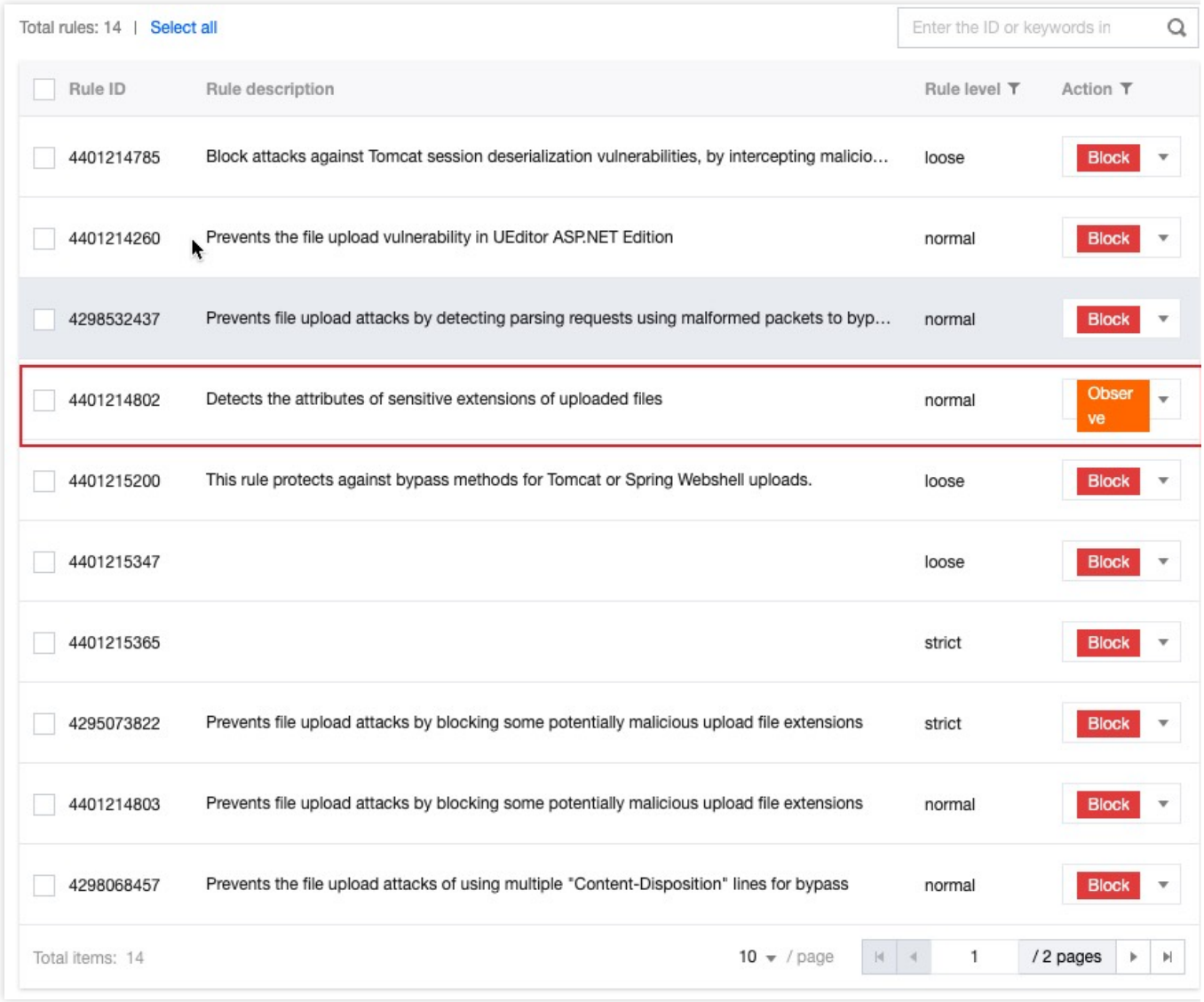
场景二：按照单条规则自定义优化防护策略

如果您需要自定义针对单条规则灵活配置防护策略，可以自定义进行规则优化。例如：当前站点域名 `www.example.com` 存在文件上传场景，当前对文件上传攻击防护策略希望为严格拦截策略，但是正常的文件上传时因为名称存在 `.exe` 后缀会被拦截，希望针对该规则单独配置为观察，仅记录日志即可。

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > Web 防护。**
3. 在 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。
4. 找到托管规则卡片，单击**设置**。
5. 在托管规则页面，以示例场景为例，找到文件上传攻击防护规则模块，修改防护等级为**自定义**。



6. 单击右上角的**详细规则**，进入详细规则优化页面，自定义修改不同规则的处置方式，选择将规则 ID：10628069的处置方式为**观察**，即可完成配置。



使用深度分析自动识别未知漏洞

深度分析采用先进的语义分析技术，深入理解 SQ L和 XSS 语句的意图。不仅能有效应对已知攻击手法，还具备对未知攻击的防护能力。这种方法超越了传统基于模式匹配的检测方式，提高了对复杂和新型攻击的识别准确性。借助深度分析，您将获得更高级别的安全防护，降低误报和漏报风险，确保网站免受恶意攻击和数据泄露的威胁。

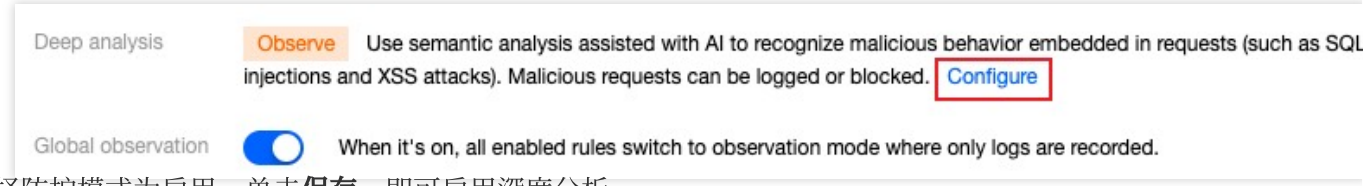
说明：

深度分析功能仅标准版和企业版套餐支持。

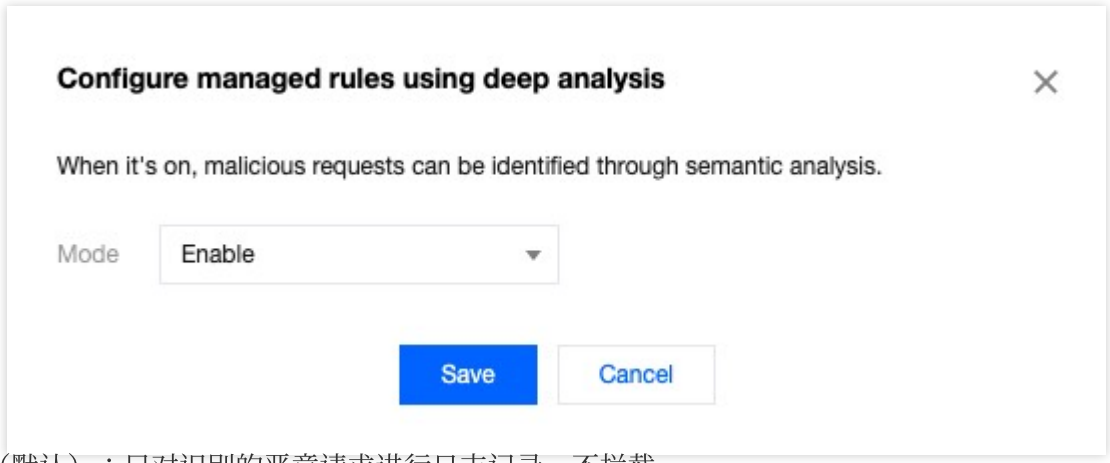
启用深度分析

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Web 防护**。
3. 在 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。
4. 找到托管规则卡片，单击**设置**。

5. 在托管规则页面，单击深度分析的**配置**。



6. 选择防护模式为启用，单击**保存**，即可启用深度分析。



观察（默认）：只对识别的恶意请求进行日志记录，不拦截。

启用：对识别的恶意请求进行拦截。

关闭：关闭深度分析。

相关参考

防护等级说明

托管规则为不同攻击和漏洞类型提供多重防护等级，包括宽松、正常、严格和超严格。选择某一防护等级时，将启用对应等级及其以下等级的规则。例如，选择严格防护等级将启用宽松、正常和严格等级的规则，实现分层保护。

建议根据业务场景启用对应防护等级：

宽松：满足最基础防护需要，并尽量避免误报。建议所有对外 HTTP 服务至少启用该等级全部规则。

正常（推荐）：防护较为全面，适用大多数场景。建议涉及客户数据的服务启用该等级。该等级规则可能会在特定场景产生误报，可通过观察模式调试优化。

严格：全力防护，适用较严格的防护场景，确保无攻击绕过。建议涉及金融数据（如：网上银行）的服务使用该等级。该防护等级下，规则可能产生一定误报，建议结合观察模式和自定义规则调试优化。

超严格：适用于严格控制环境下的访问场景。该等级规则可能造成较多误报，请根据具体防护需要开启，并结合防护例外规则、观察和自定义规则调试部署。

如需更精细的控制，您还可以使用**自定义防护等级**，按业务特定需要，自定义不同规则的处置方式。

CC 攻击防护

最近更新时间：2024-04-16 16:30:24

概述

CC（Collapse Challenge）攻击，即 HTTP/HTTPS DDoS 攻击。攻击者通过占用 Web 服务的连接和会话资源，导致服务无法正常响应用户请求，拒绝服务。为避免 CC 攻击，EdgeOne 提供了预设的 CC 攻击防护策略，并默认开启，确保您的站点稳定在线。

说明：

CC 攻击防护旨在保障业务可用性。对于不会造成源站错误或者站点可用性下降的安全场景，例如：盗刷资源、批量登录、购物车自动下单等场景，请使用 速率限制 和 Bot 管理 进一步加固安全策略。

EdgeOne 使用“干净流量”计费模式，即对于安全防护功能拦截的请求不进行计费，仅对通过安全防护功能处理后的流量和请求用量计费。对“干净流量”计费模式的定义请参考：关于“干净流量”计费说明。

使用 CC 攻击防护

CC 攻击防护通过速率基线学习、头部特征统计分析和客户端IP情报等方式识别 CC 攻击，并进行处置。EdgeOne 提供了预设的三种 CC 攻击防护策略：

高频访问请求限制：用于应对通过高频和大量并发的连接请求占用服务器资源的 CC 攻击行为，可基于单 IP 源限制访问频次限制。

慢速攻击防护：用于应对通过大量慢速连接请求占用服务器资源的 CC 攻击行为，可基于单会话限制访问连接最低速率，淘汰慢速连接客户端。

智能客户端过滤：融合了速率基线学习、头部特征统计分析和客户端 IP 情报，实时动态生成防护规则。针对来自高危客户端、或者携带高危头部特征的请求进行人机验证。智能客户端过滤默认开启且对符合规则的客户端执行 JavaScript 挑战。

配置高频访问请求限制

高频访问请求限制规则根据配置的限制等级，统计当前域名的请求速率，基于最近7天请求建立速率基线（速率基线每 24 小时更新），结合配置的限制等级，限制单个客户端访问该域名的请求速率。

注意：

高频访问请求限制适用于 Web 类业务。当站点同时提供 API 接口服务时，为了防止频率较高的正常请求被拦截。建议为需要支持高频访问的 API 接口配置 防护例外规则，跳过 CC 攻击防护模块，同时通过配置 速率限制 精准限制 API 接口暴露面，避免使用适中、攻击紧急、严格限制等级。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。

3. 找到 CC 攻击防护卡片，单击**设置**。进入CC 攻击防护配置页面，单击高频访问请求限制右侧的**编辑**。
4. 配置高频访问请求限制的限制等级和处置方式，各限制等级说明如下：

限制类型	限制等级	适用场景	速率上限	初始速率限制
自适应	宽松（默认配置，推荐）	适用于大部分 Web 业务场景。	无上限 至少7000 次/分	2000 次/ 5 秒
	适中	适用于页面内容较为简单，动态数据或动态加载内容较少的业务场景。	1200-2400 次/分	200 次/ 10 秒
	攻击紧急	当攻击发生时，或者其他限制等级防护有防护透传造成业务影响时，可选择该限制等级进行紧急防护。由于该等级的速率限制较为严格，可能存在误杀风险，不建议长期使用。	60-1200 次/分	40 次/ 10 秒

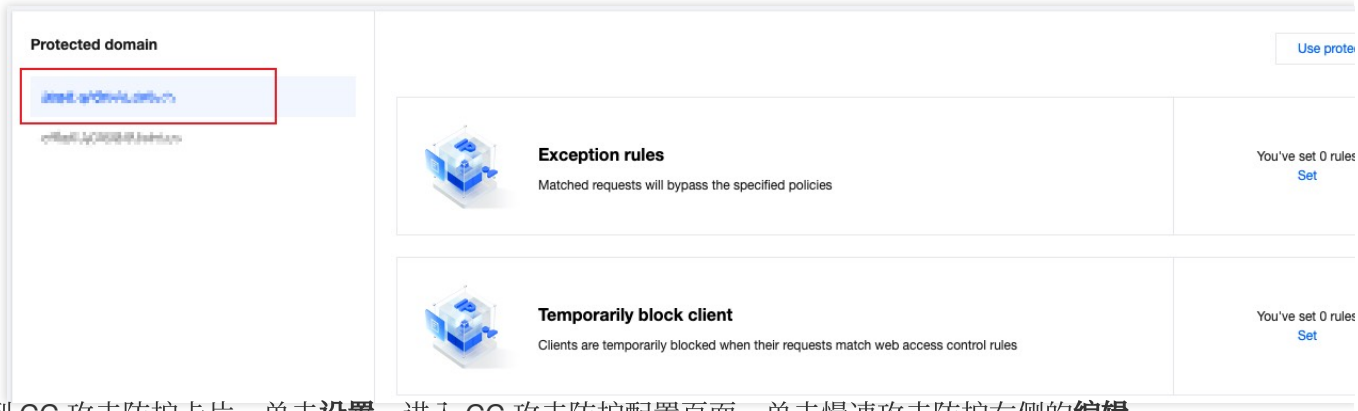
说明：
处置方式支持**观察**和 **JavaScript 挑战**两种方式，不同的处置方式说明详见：处置方式。
5. 单击**保存**，完成规则配置。

配置慢速攻击防护

通过限制最小请求速率和设置超时，缓解慢速传输等攻击场景对站点资源的消耗，避免服务可用性下降。EdgeOne 慢速攻击防护支持**正文传输超时**和**正文传输最小速率**选项，当正文传输速率缓慢，或长时间无数据传输时，对客户端进行处置。

操作步骤

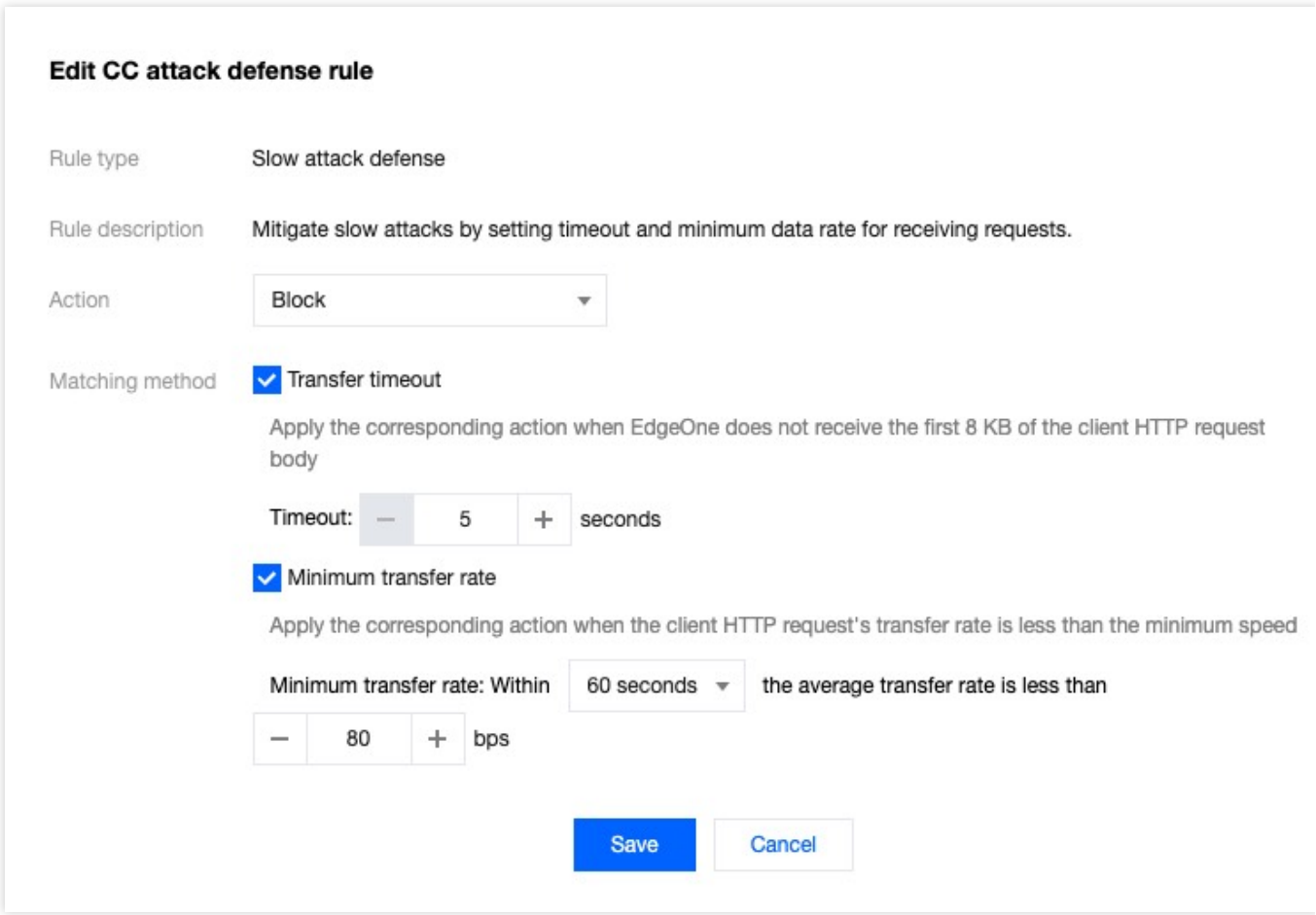
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到 CC 攻击防护卡片，单击**设置**。进入 CC 攻击防护配置页面，单击慢速攻击防护右侧的**编辑**。
4. 配置慢速攻击防护规则的匹配方式，可选以下限制：

正文传输时长：缓解通过占用连接但不传输正文数据的慢速攻击方式。指定正文传输**超时时长**，超过配置时间未完成前 8KB 正文数据传输的客户端，将按指定方式处置；支持配置5-120秒。

正文传输最小速率：缓解通过极慢速传输正文占用连接和会话资源的攻击。可指定最低传输速率，在统计时间窗口内传输的请求正文小于配置速率时，按指定方式处置，传输速率配置最小支持 1 bps，最大 100 Kbps。



说明：

配置处置方式，支持**拦截**、**观察**两种方式，不同的处置方式说明详情请参见 处置方式。

5. 单击**保存**，完成规则配置。

智能 CC 防护

融合了速率基线学习、头部特征统计分析和客户端 IP 情报，实时动态生成防护规则。针对来自高危客户端、或者携带高危头部特征的请求进行人机识别。智能客户端过滤默认开启且对符合规则的客户端执行 JavaScript 挑战。

注意：

智能客户端过滤使用业务速率基线作为参考之一，业务重大变更（接入、切量、新增业务、活动上新）时，业务基线可能造成误拦截，可将处置方式暂时修改为观察，待业务平稳后开启。

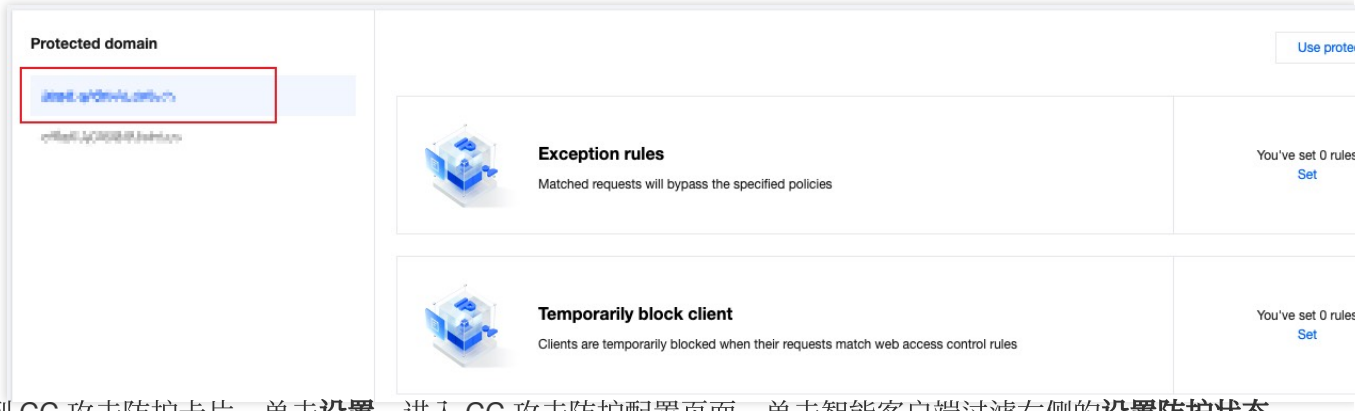
智能客户端过滤仅标准版及企业版套餐支持。

修改智能 CC 攻击防护处置方式

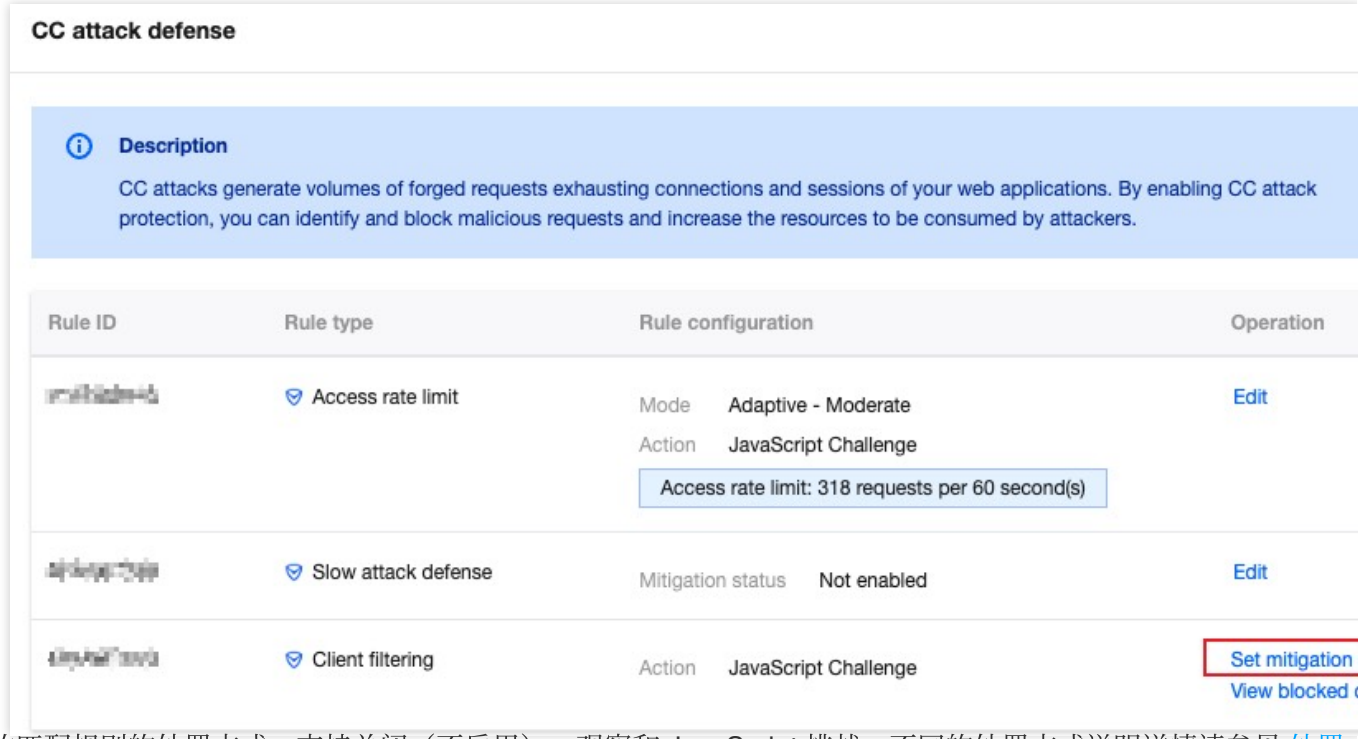
如果您需要修改触发智能客户端过滤后的处置方式，您可以参照以下操作步骤：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

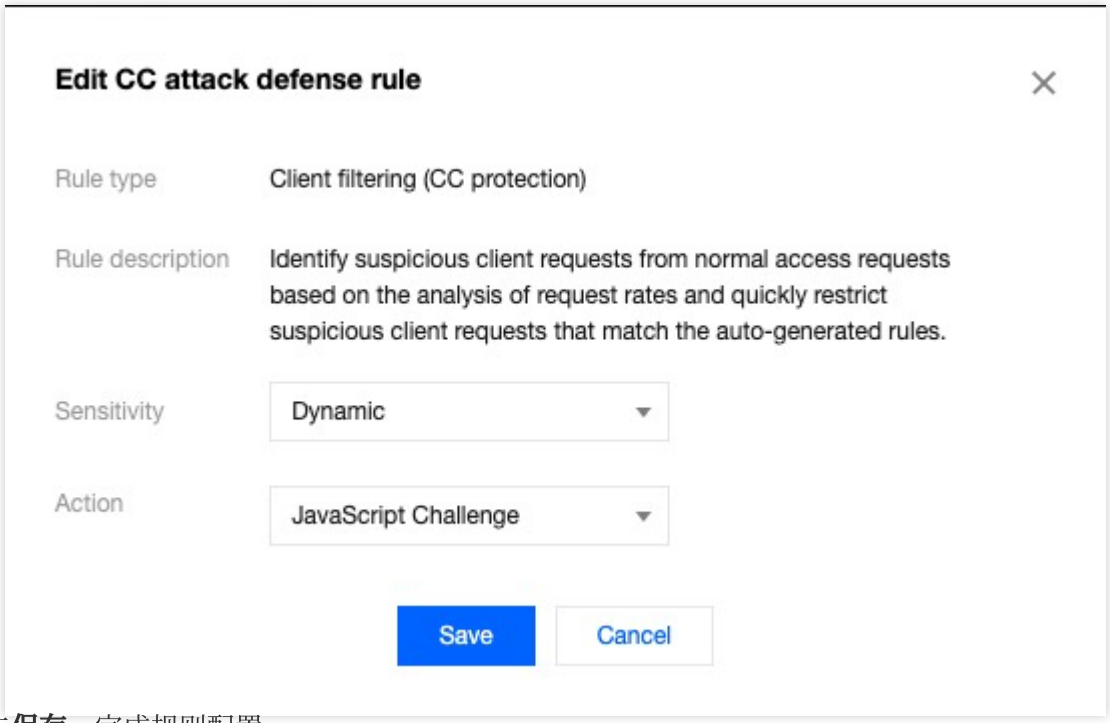
2. 在站点详情页面，单击**安全防护** > **Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到 CC 攻击防护卡片，单击**设置**。进入 CC 攻击防护配置页面，单击智能客户端过滤右侧的**设置防护状态**。



4. 修改匹配规则的处置方式，支持关闭（不启用）、观察和 JavaScript 挑战，不同的处置方式说明详情请参见 处置方式。



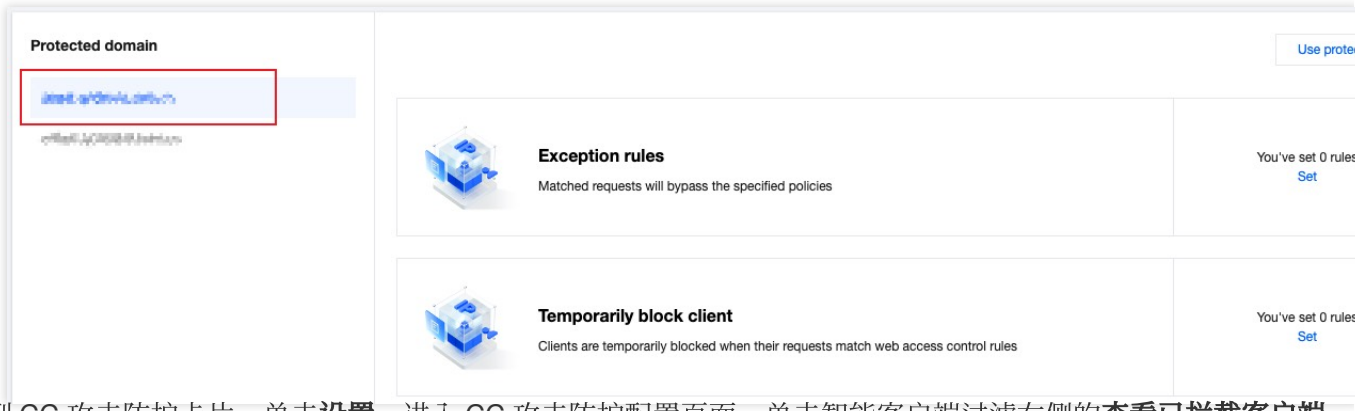
5. 单击**保存**，完成规则配置。

查看或放行已拦截的客户端列表

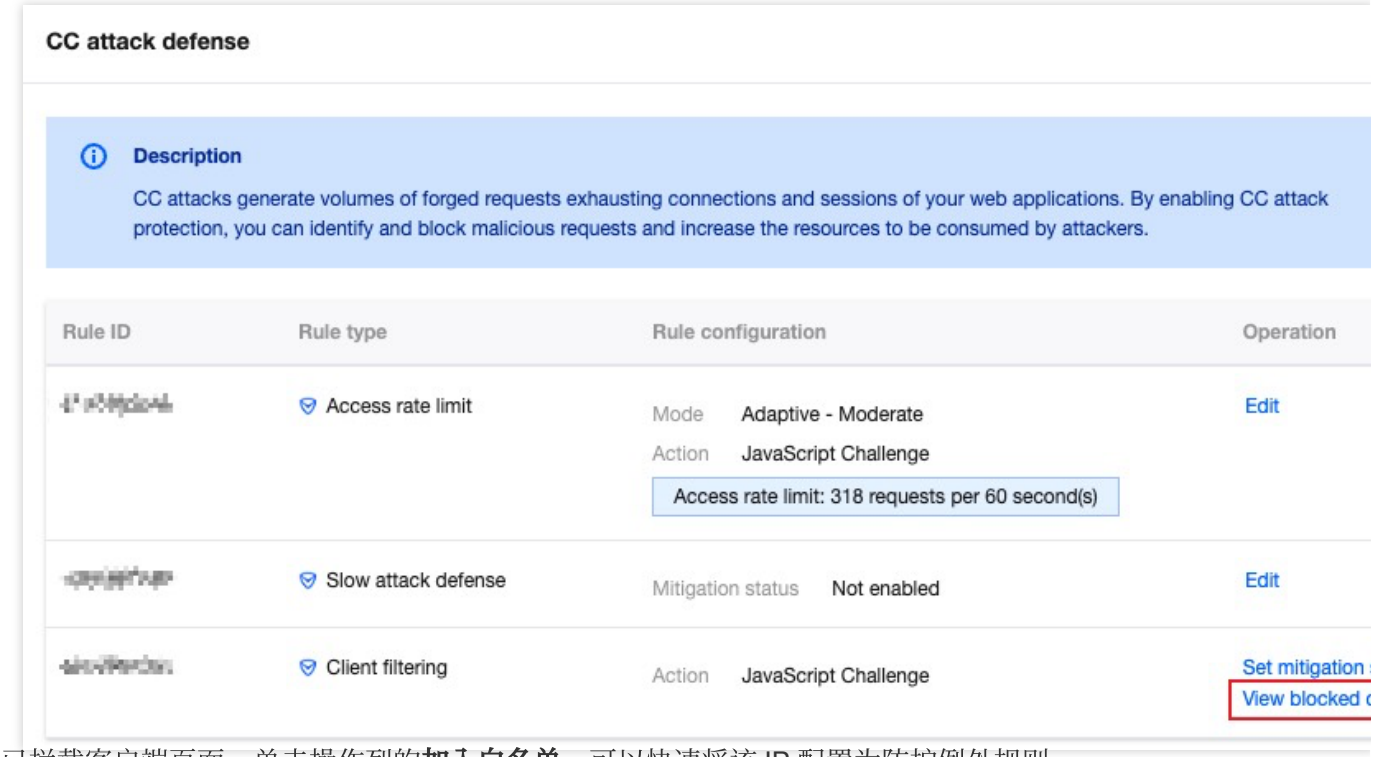
如果您需要查看被智能客户端过滤拦截的客户端列表，您可以参照以下操作步骤：

1. 登录边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，单击**安全防护** > **Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到 CC 攻击防护卡片，单击**设置**。进入 CC 攻击防护配置页面，单击智能客户端过滤右侧的**查看已拦截客户端**。



4. 在已拦截客户端页面，单击操作列的**加入白名单**，可以快速将该 IP 配置为防护例外规则。

自定义规则

最近更新时间：2023-10-11 10:35:07

概述

如果您的站点需要自定义控制用户的访问策略，例如禁止指定地区用户访问、允许指定外部站点链接到本站内容、仅允许指定用户访问某些资源等。自定义规则支持根据单一规则匹配条件或者多个匹配条件进行组合匹配客户端请求，通过允许、拦截、重定向、返回自定义页面等方式来控制匹配的请求策略，可以帮助您的站点更加灵活地限制用户可访问的内容。

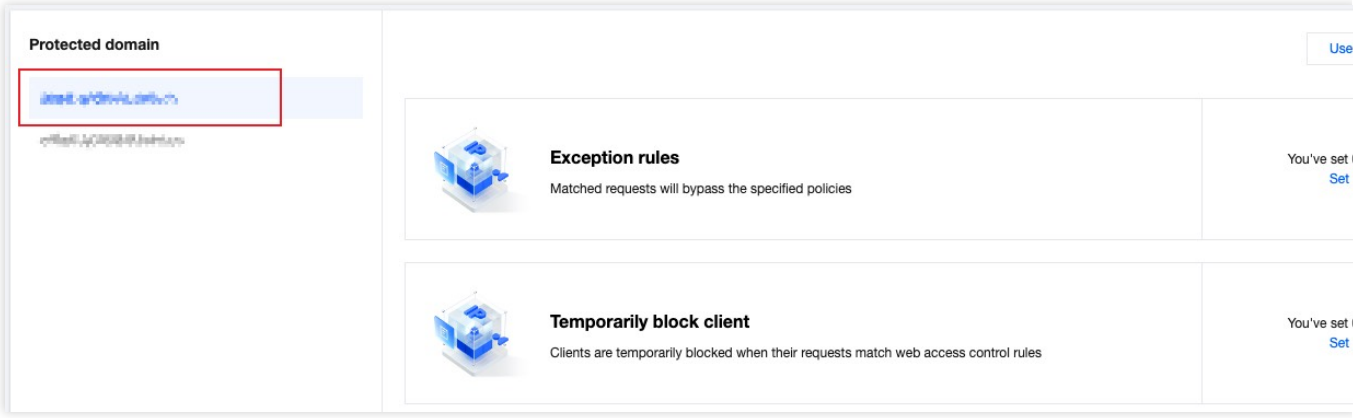
典型场景与使用方式

您可以根据不同场景选择适当的规则类型来保护您的站点。自定义规则分为下列类型：
基础访问管控：支持单一条件匹配请求，对命中的请求进行处置或观察，适用于简单场景下的防护处置，例如：配置访问 IP 黑白名单、Referer 黑名单、UA 黑白名单或地域限制。
精准匹配规则：支持多个条件组合匹配请求，对命中的请求进行处置或观察，适用于复杂场景下的防护配置，例如：指定路径下文件仅允许指定用户访问。
托管定制策略：由腾讯安全专家定制的策略，不支持控制台调整策略。详情请见：托管定制规则。
说明：
当存在多条相同类型规则时，规则生效优先级如下：
1. 基础访问管控内的规则，当请求匹配多条规则时，此时将按照处置方式顺序执行：观察 > 拦截。
2. 精准匹配规则将按优先级自高到低（优先级数值从小到大）执行；
3. 自定义规则与其他 Web 防护能力之间的规则优先级顺序详见：Web 防护请求处理顺序。

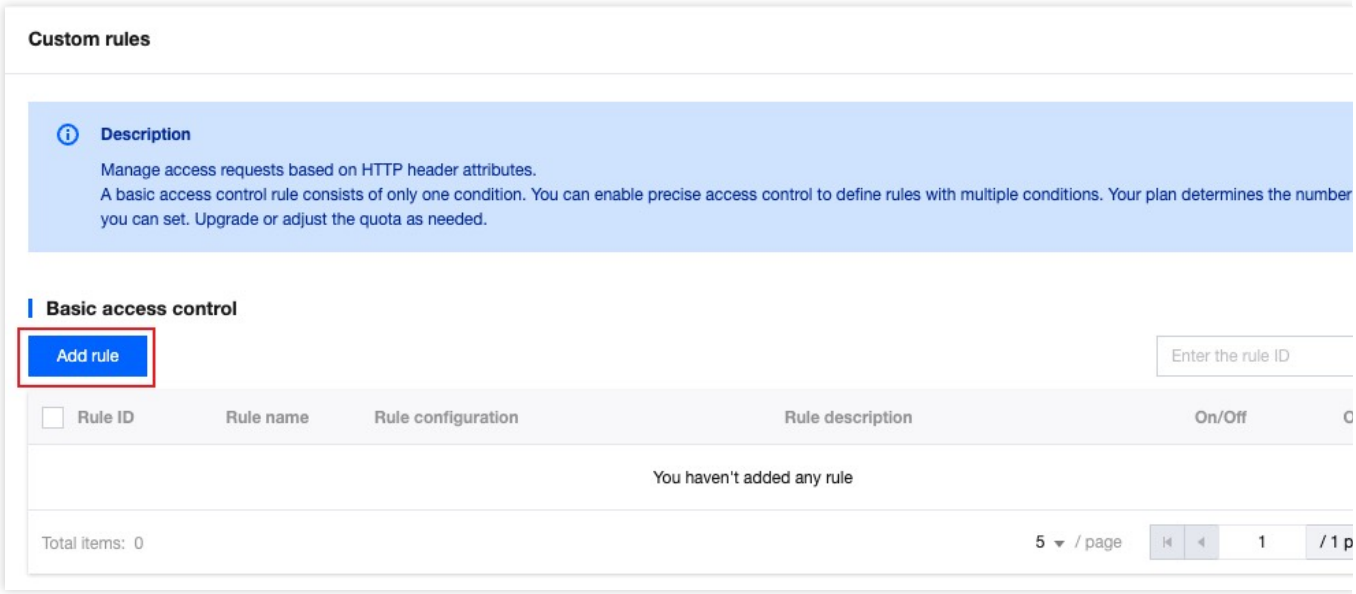
基础访问管控

示例场景一：仅允许特点国家/地区访问

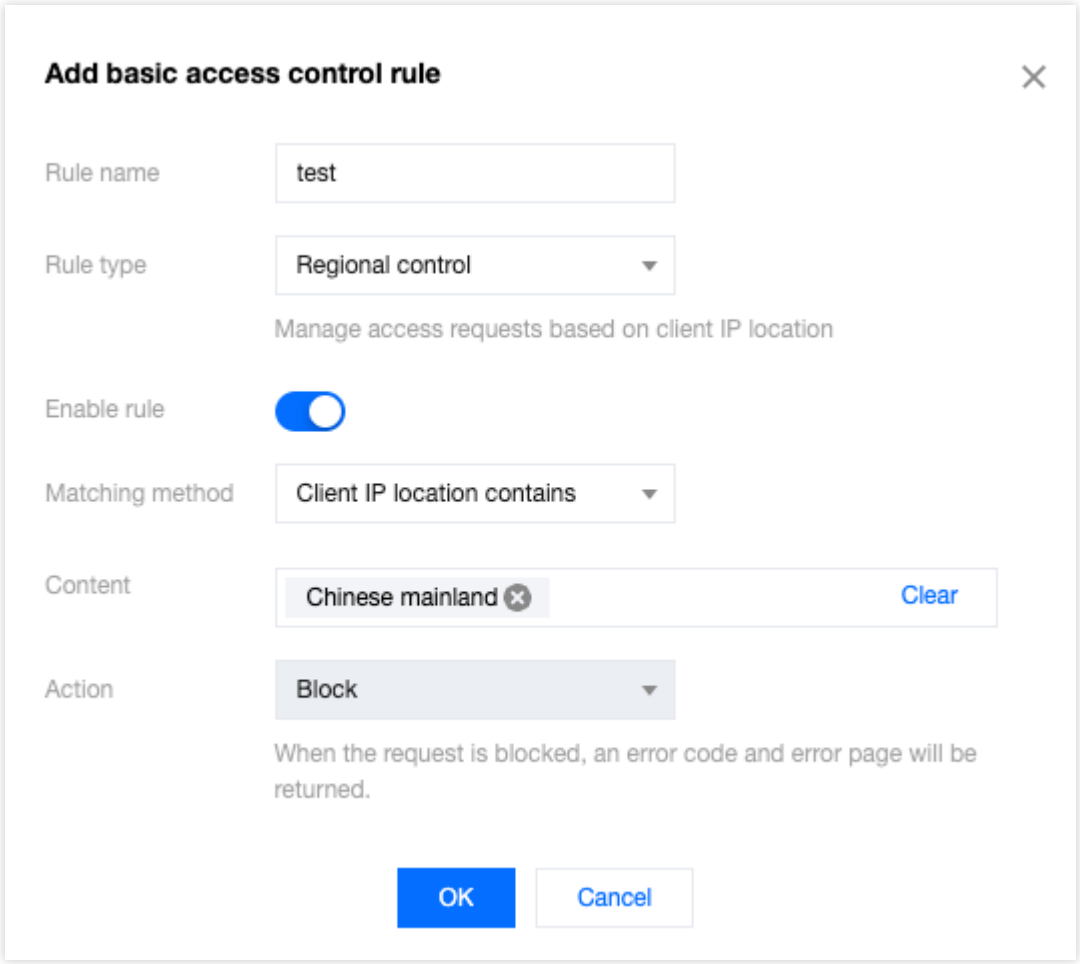
为遵守指定业务地区的法规要求，如果当前业务仅允许来自**非中国大陆地区**的访问，您可能需要限制访客来源区域。对于这类场景，您可以通过基础访问管控中的区域管控规则来实现，操作步骤如下：
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到**自定义规则**卡片，单击**设置**。进入自定义规则页面，单击基础访问管控中的**添加规则**。



4. 在新建基础管控规则界面内，填写规则名称后，以配置规则类型、匹配方式及匹配内容。规则类型即匹配条件，匹配该规则类型的请求将按照该规则配置的处置方式进行处理。
以当前场景为例，可选择规则类型为区域管控，匹配方式选择为客户端 IP 区域包含，匹配内容选择中国大陆（全部），处置方式为拦截。



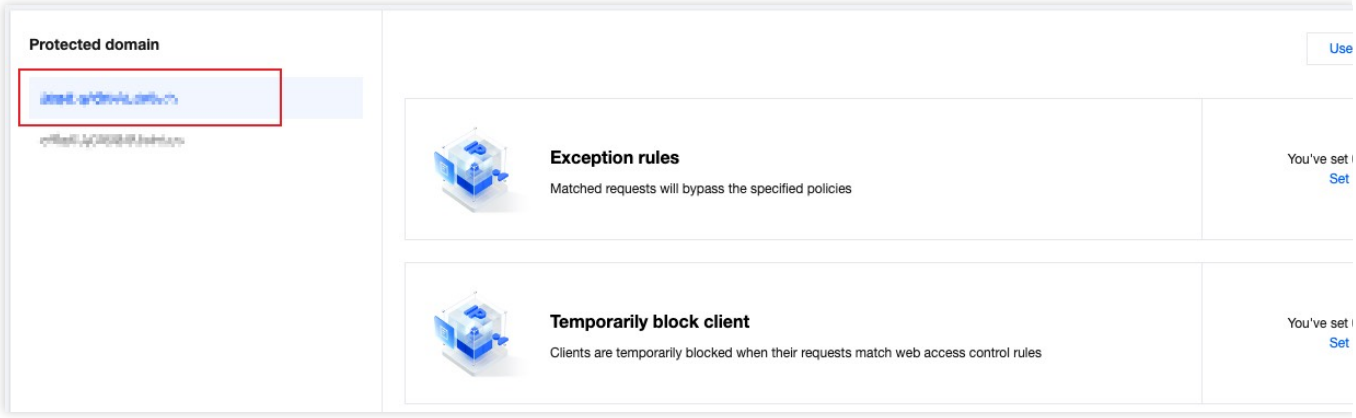
5. 单击**确定**后，规则将部署生效。此时，客户端访问 IP 如果是中国大陆用户，则不允许访问该网站。

示例场景二：配置 Referer 控制外部站点访问

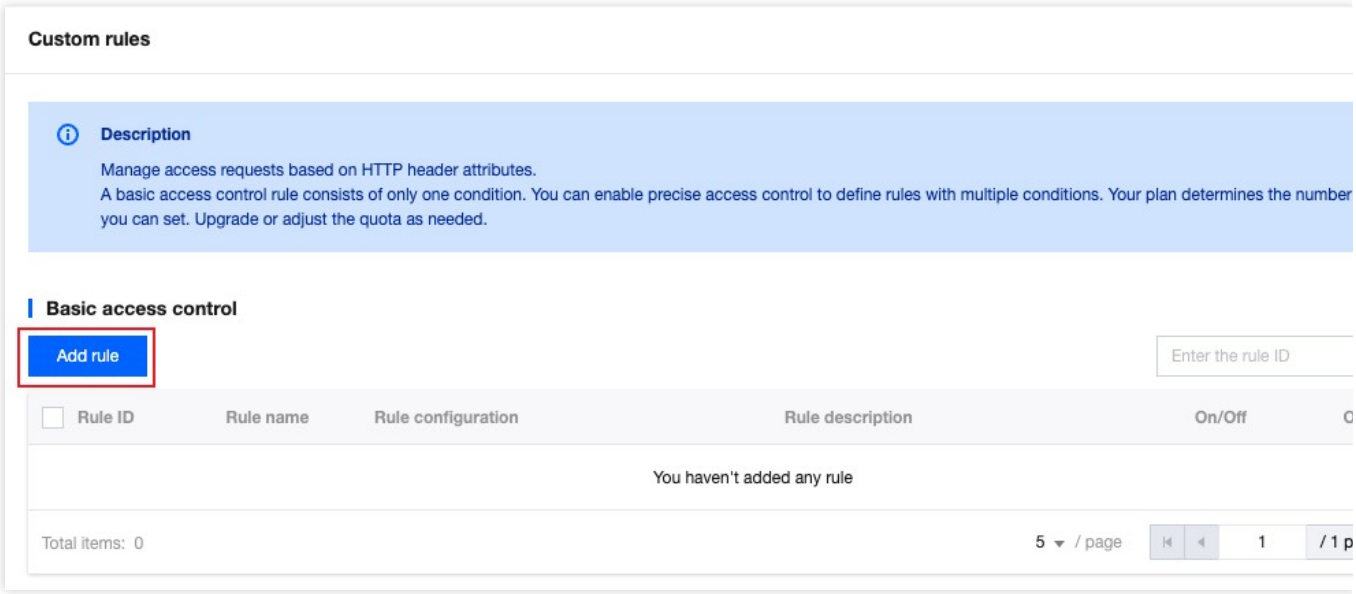
为了防止未授权站点方式访问盗链，您可以使用基础访问管控中的 Referer 管控规则来阻止携带未授权 Referer 头部的访问请求。例如：站点域名 `www.myexample.com` 需要放行通过广告合作方 `ads.example.com` 的链接访问的请求，同时拒绝通过其他站点链接访问内容。操作步骤如下：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

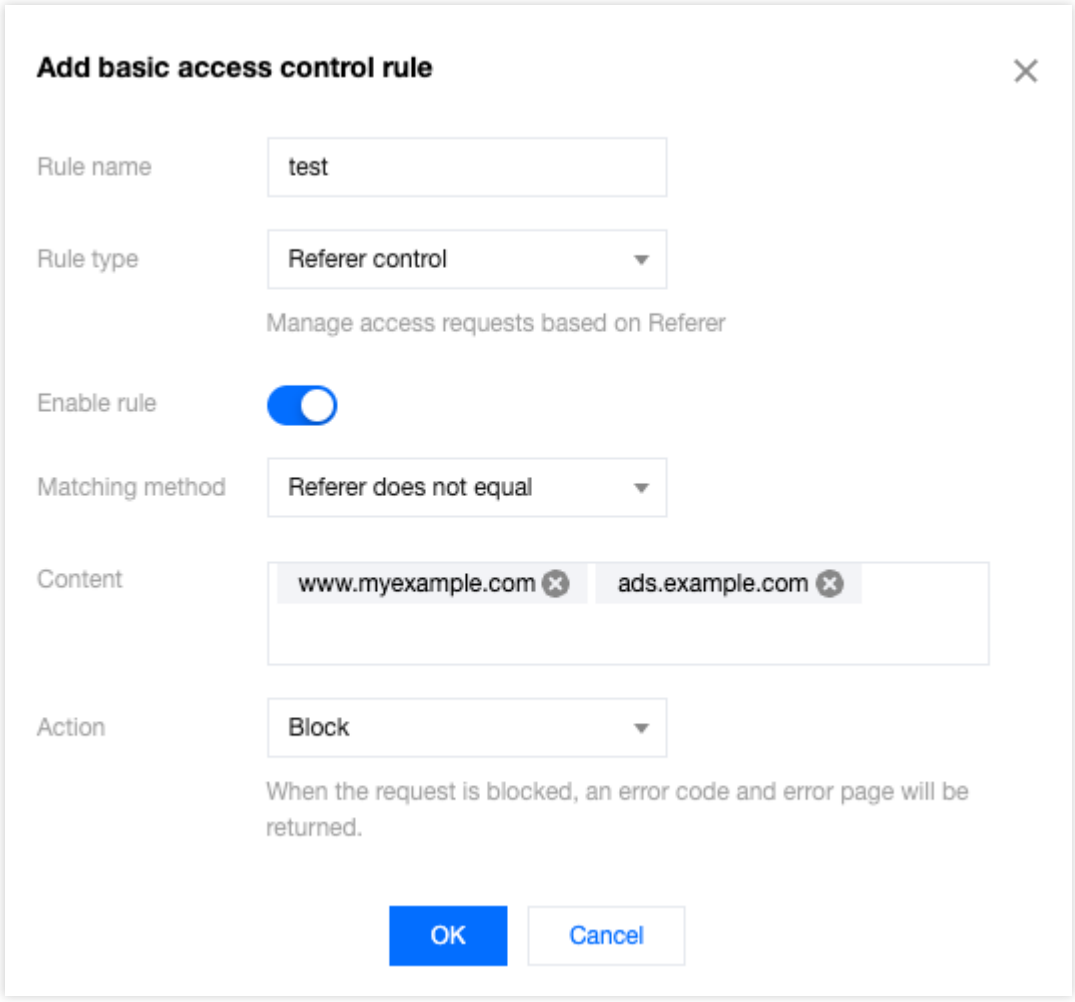
2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到**自定义规则**卡片，单击**设置**。进入自定义规则页面，单击基础访问管控中的**添加规则**。



4. 在新建基础管控规则界面内，填写规则名称后，配置规则类型、匹配方式及匹配内容。规则类型即匹配条件，匹配该规则类型的请求将按照该规则配置的处置方式进行处理。
以当前场景为例，可选择规则类型为 **Referer 管控**，当请求 Referer 不等于包括：`www.myexample.com` 、 `ads.example.com` 时，处置方式为拦截。



5. 单击**确定**后，规则将部署生效。

精确匹配规则

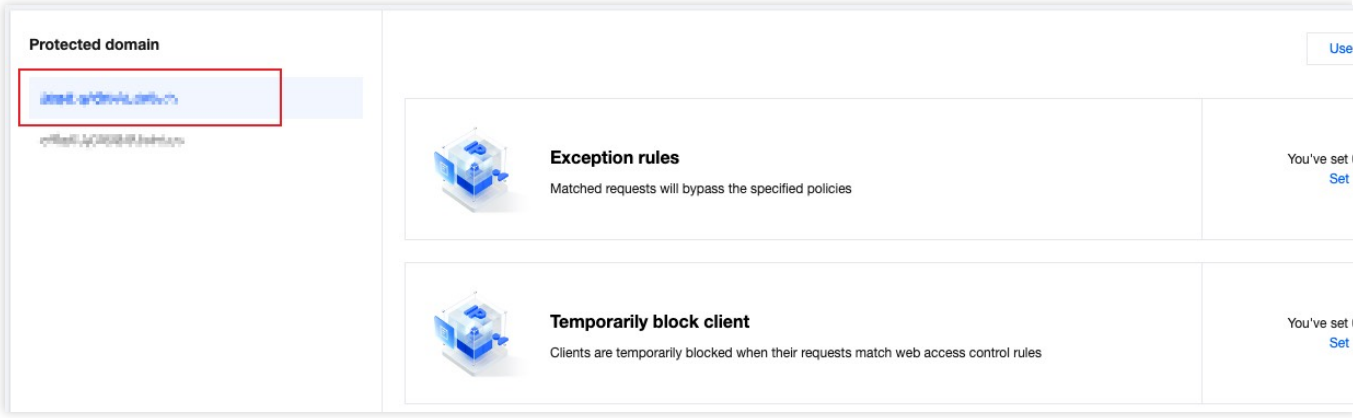
示例场景：精准控制站点敏感资源暴露面

如果您需要控制站点敏感资源（例如：后台管理页面）暴露面，仅允许特定客户端或指定网络访问。您可以使用**精准匹配规则**中的**客户端 IP** 匹配和**请求 URL** 匹配组合来实现。

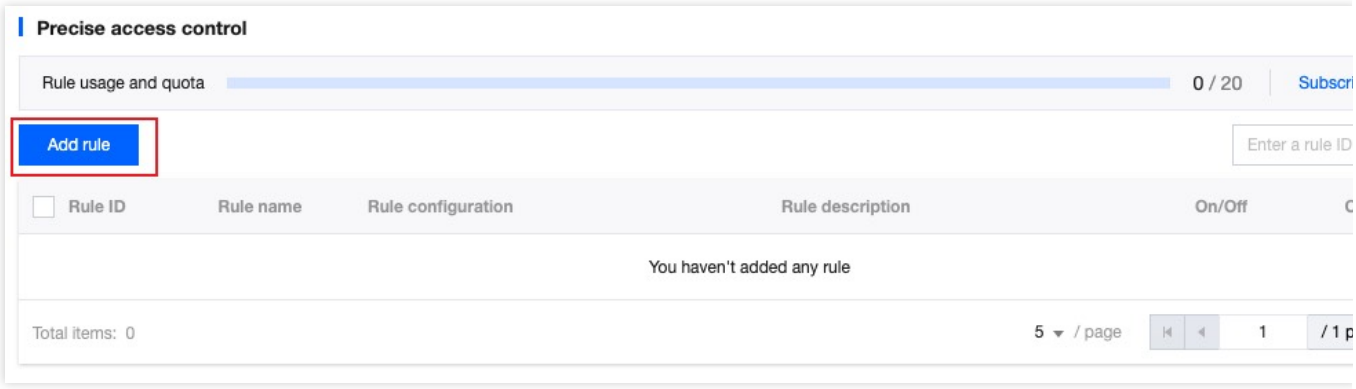
例如：当前站点域名 `www.example.com` 的管理后台登录地址路径为 `/adminconfig/login`，该后台仅允许指定的客户端 IP 用户 `1.1.1.1` 登陆。操作步骤如下：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到**自定义规则**卡片，单击**设置**。进入自定义规则页面，单击精准匹配策略中的**添加规则**。

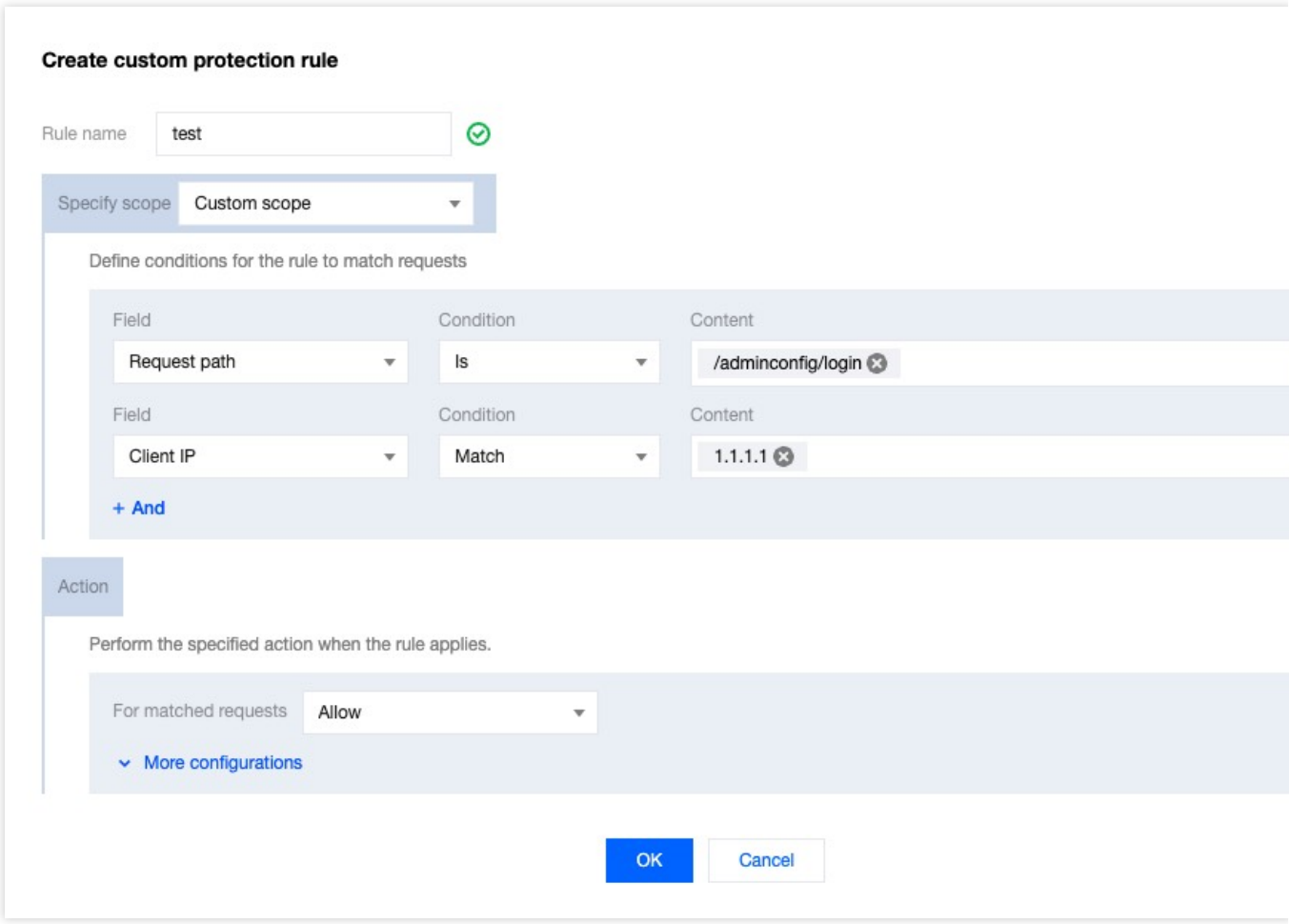


4. 在新建自定义防护规则界面内，填写规则名称后，配置匹配字段以及执行动作。

以当前场景为例，可配置匹配字段为请求路径（Path）等于 `/adminconfig/login` 且客户端 IP 匹配 `1.1.1.1` 的用户，执行动作为放行。

说明：

单击**更多配置**，可修改该规则的优先级，数值越低，优先级越高。



5. 单击**确定**后，规则将部署生效。

相关参考

支持的匹配条件范围

自定义规则可以使用匹配条件来控制规则的适用范围。以下是不同的自定义规则类型支持的匹配条件：

基础访问管控

规则类型	说明
客户端 IP 管控	根据客户端 IP 管控访问请求
区域管控	根据客户端 IP 归属地区管控访问请求
Referer 管控	根据请求的 Referer 头部内容管控访问请求
User-Agent 管控	根据请求的 User-Agent 管控访问请求
ASN 管控	根据客户端 IP 归属 ASN 管控访问请求

URL 管控	根据请求的 URL 管控访问请求，支持以通配符匹配

精准匹配规则

精准匹配规则支持以下匹配条件，且不同 EdgeOne 套餐支持程度也不一致。

说明：

支持的匹配条件的说明及套餐限制请参考：匹配条件。

请求客户端 IP

请求客户端 IP（优先匹配 XFF 头部）

自定义请求头部

请求 URL

请求 Referer 头部

请求 User-Agent 头部

请求路径（Path）

请求方式（Method）

请求 Cookie

XFF 扩展头部

网络层协议

应用层协议

支持的处置方式

不同的自定义防护规则支持的处置方式如下，不同的处置方式说明请参见 处置方式。

防护规则类型	支持的处置方式
基础访问管控	观察 拦截
精准匹配规则	放行 拦截 观察 IP 封禁 重定向 返回自定义页面注 JavaScript 挑战

说明：

注：

如您想自定义响应请求的页面和状态码，自定义规则支持下列配置方式：

使用**返回自定义页面**处置方式：您可以为单条自定义规则（仅支持精准匹配规则）配置**返回自定义页面**处置方式。响应匹配该条规则的请求时，EdgeOne 将返回您指定的页面和状态吗。

使用**自定义页面**：您可以使用**自定义页面**配置，指定全部自定义规则在**拦截请求**时使用的页面和状态码。

速率限制

最近更新时间：2023-12-18 15:31:19

概述

在站点运营中，经常会出现恶意占用资源、业务滥用和暴力破解等问题。这些问题如果被忽视，将会导致服务质量下降、产生高额成本账单，甚至可能会导致敏感数据泄露。为了有效管理这些风险，客户端访问频率是一个重要的指标。恶意客户端通常会以更高的频率进行访问，以便快速达到破解登录、占用资源和爬取内容的目的。使用合适的阈值限制客户端访问频率，可以有效区分正常客户端和恶意客户端，从而缓解资源占用和滥用的风险。

注意：

在管理和对抗爬虫时，仅使用速率限制策略效果有限，请结合 Bot管理 功能，制定完整的爬虫管理策略。

典型场景与配置方式

速率限制常用于区分正常客户访问与恶意访问，通过选择合适的统计方式、限制阈值和处置方式，速率限制可以帮助您缓解安全风险。速率限制配置分为下列类型：

精准匹配规则：用户定义的访问频率控制策略。支持多个条件组合匹配请求，限制每个请求来源请求速率，适用于绝大部分场景下用于区分正常用户访问和恶意的高频访问。

托管定制策略：由腾讯安全专家定制的策略，不支持控制台调整策略。详情请参见 托管定制规则。

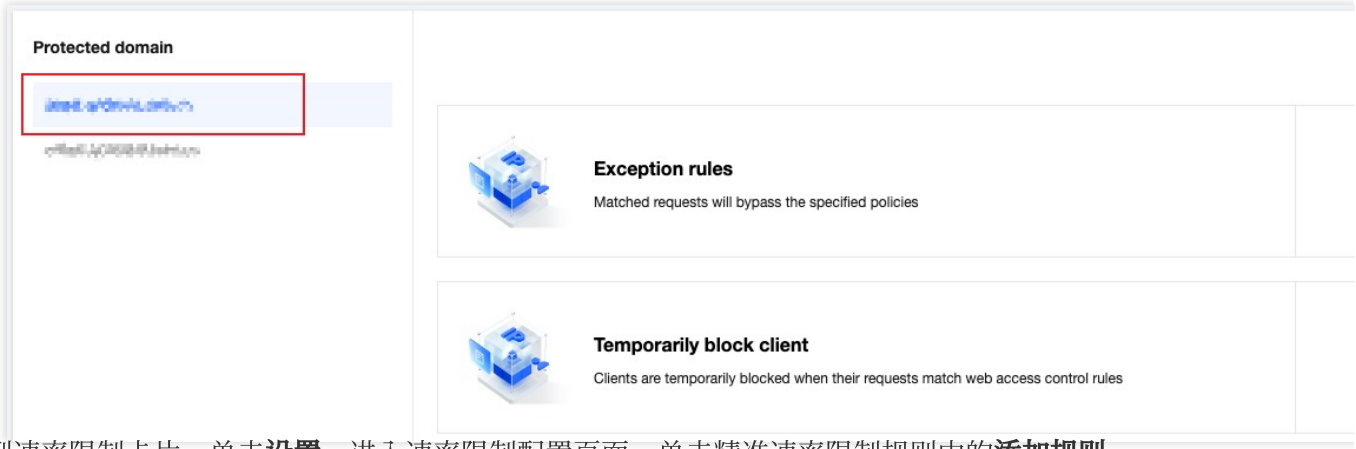
精准匹配规则

示例场景一：限制登陆 API 接口访问频率，缓解撞库和暴力破解攻击

在面临撞库和暴力破解攻击的场景中，攻击者通常会频繁地使用访问登陆 API 接口尝试获取或破解信息。通过限制对登陆接口的请求频率，我们可以大幅缓解攻击者的破解尝试，从而有效抵御这类攻击，保护敏感信息不被泄露。

例如：站点域名 `www.example.com` 提供了对外接口为 `/api/UpdateConfig` ，该接口允许的访问调用频次为100次/分钟，当超过频次限制后，将封禁该 IP 10分钟。操作步骤如下：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到速率限制卡片，单击**设置**。进入速率限制配置页面，单击精准速率限制规则中的**添加规则**。

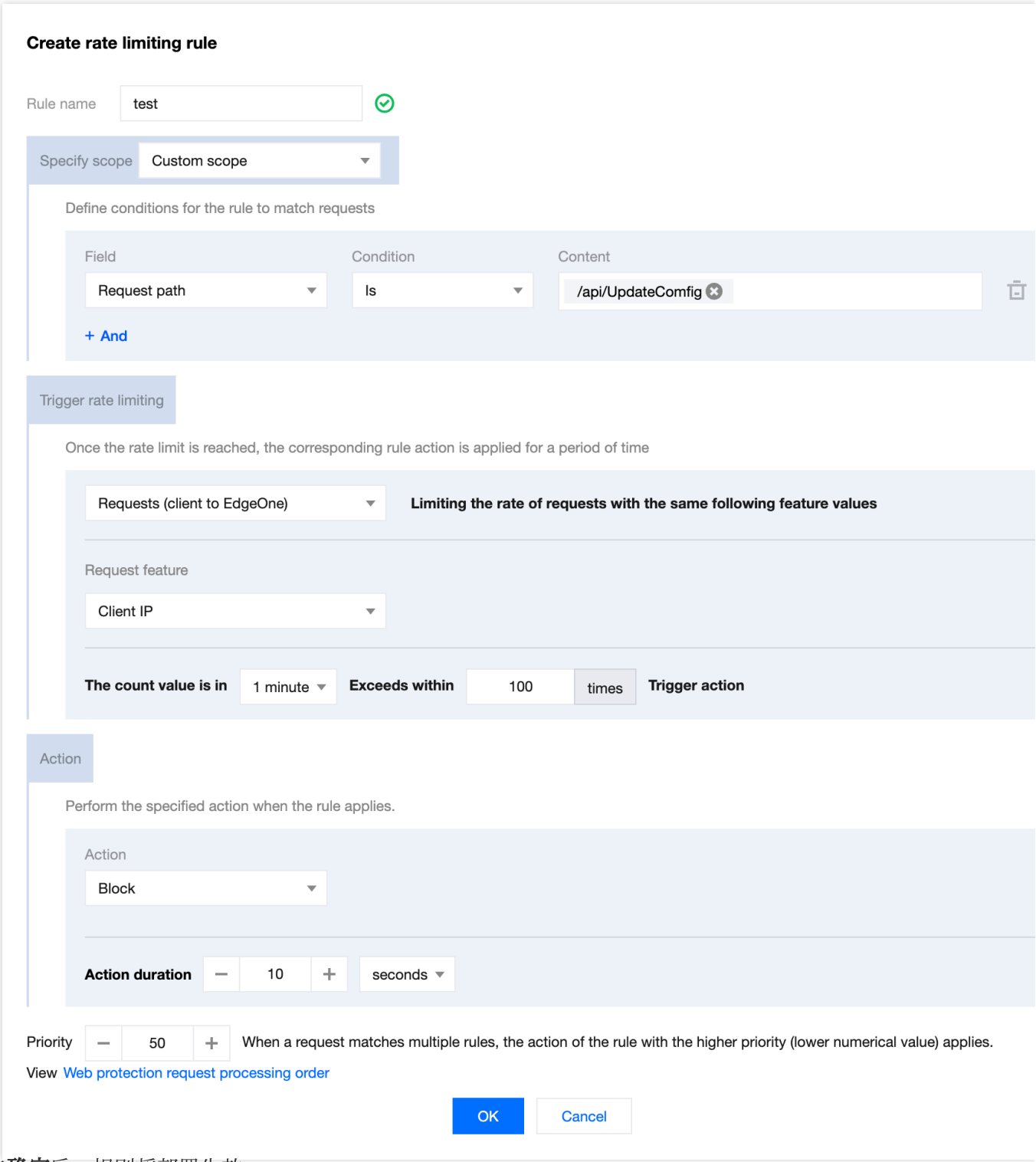
4. 在弹出的规则页面内，按照如下步骤配置：

4.1. 填写规则名称，匹配对象选择为**自定义防护对象**。

4.2. 在匹配条件列表选项，配置规则的匹配条件，以当前场景为例，匹配字段选择**请求路径（Path）**等于 `/api/UpdateConfig` 。

4.3. 配置该规则的触发方式，以当前场景为例，配置计数周期1分钟内，计数超过100次时触发，统计方式为单个客户端 IP 请求到 EdgeOne 节点时触发，触发后，保持该触发状态10分钟。

4.4. 执行动作选择为拦截。完整的规则配置如下：



5. 单击**确定**后，规则将部署生效。

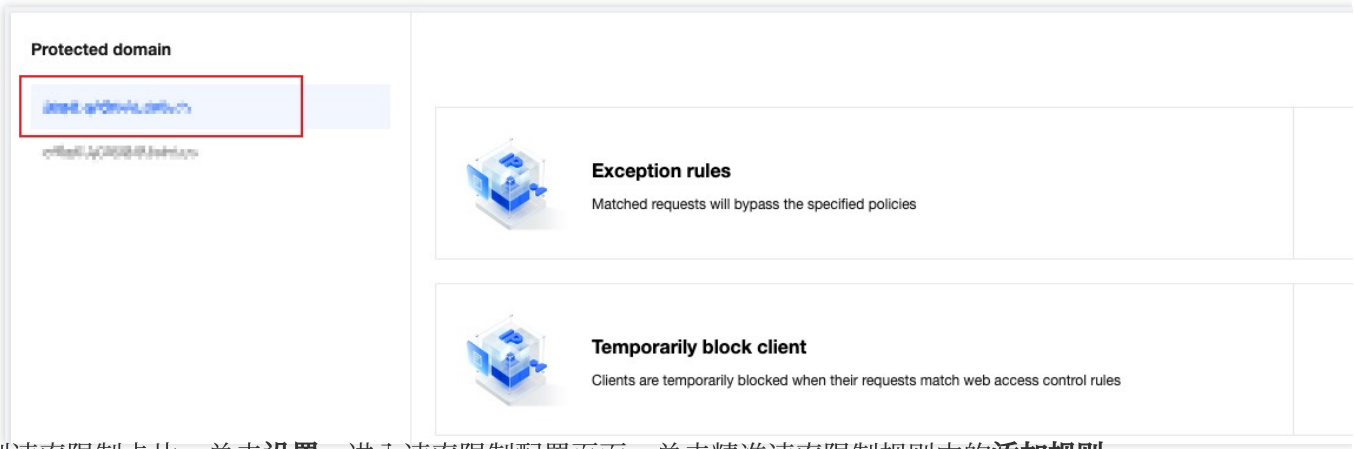
示例场景二：限制导致404状态码的请求速率，缓解资源随机扫描

在恶意客户端随机扫描站点图片资源，尝试爬取内容时，常常会因为访问路径不存在导致源站响应 `404` 错误。通过限制导致源站 `404` 状态码的请求频率，EdgeOne 能够避免恶意攻击者大规模地扫描和请求静态资源，从而减少源站的错误响应，缓解服务器压力，提升静态资源站点的安全性和稳定性。例如：针对站点域名

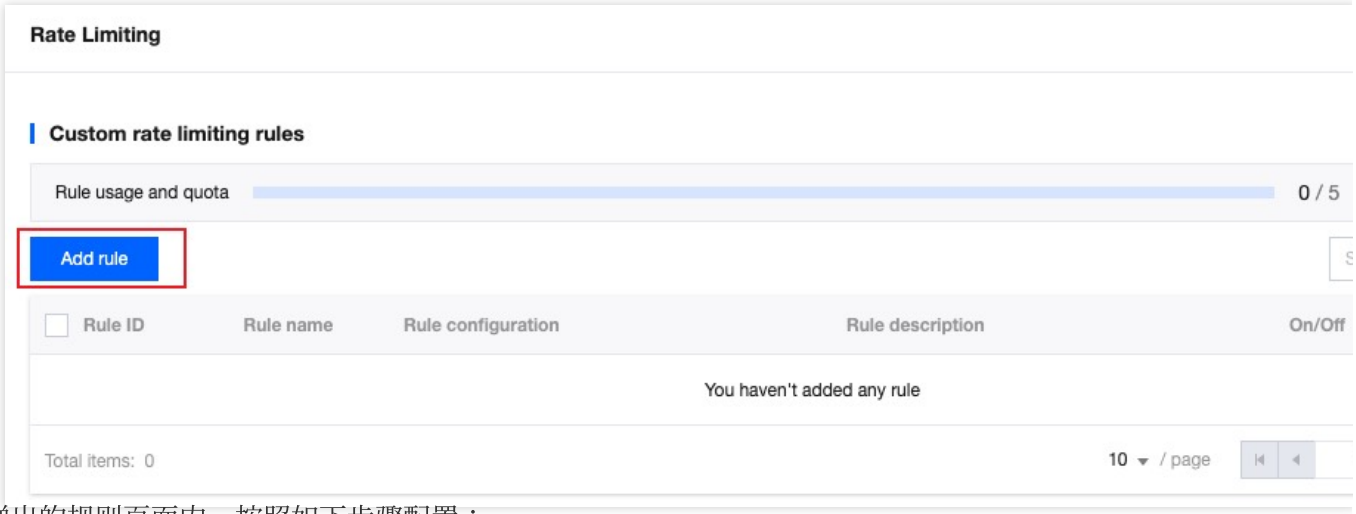
`www.example.com` 的图片静态资源 `.jpg` `.jpeg` `.webp` `.png` `.svg`，当资源不存在响应 404 时，访问在 10 秒内超过 200 次时，则直接拦截对应的客户端 IP 请求 60 秒。操作步骤如下：

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，单击**安全防护> Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到速率限制卡片，单击**设置**。进入速率限制配置页面，单击精准速率限制规则中的**添加规则**。



4. 在弹出的规则页面内，按照如下步骤配置：

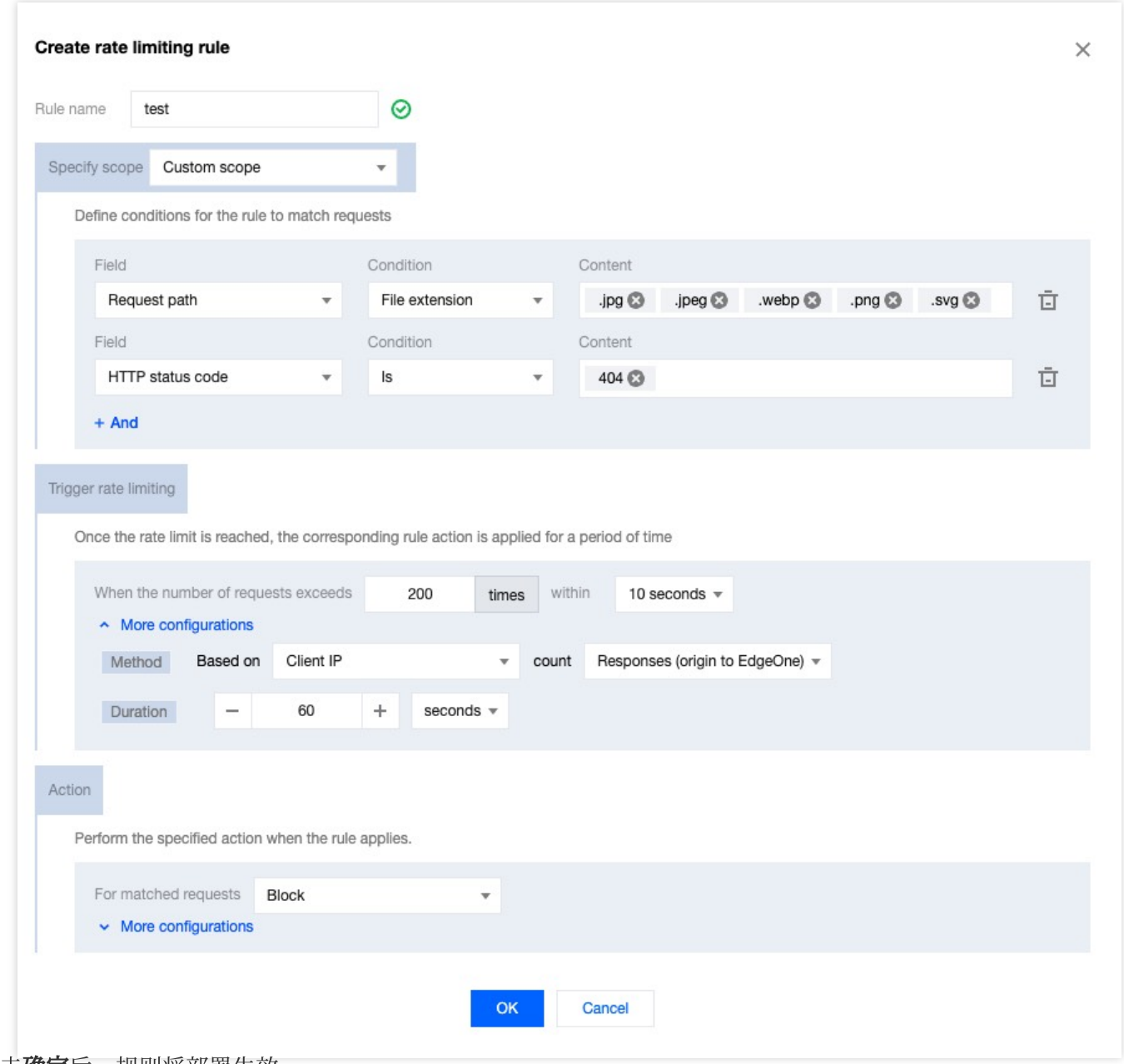
4.1. 填写规则名称，匹配对象选择为**自定义防护对象。**

4.2. 在匹配条件列表选项，配置规则的匹配条件，以当前场景为例，匹配字段选择**请求路径（Path）**的**文件后缀匹配**内容包括 `.jpg` `.jpeg` `.webp` `.png` `.svg` 图片类静态资源类型。

4.3. 单击 **+And**，添加新的匹配条件，在新增的匹配条件中，匹配字段选择 HTTP 状态码（需使用企业版套餐支持）等于404的请求。

4.4. 配置该规则的触发方式，以当前场景为例，配置计数周期10秒内，计数超过200次时触发，统计方式为单个客户端 IP 维度，由源站响应至 EdgeOne 节点时，触发后，持续处置60秒。

4.5.执行动作选择为拦截。完整的配置规则如下：



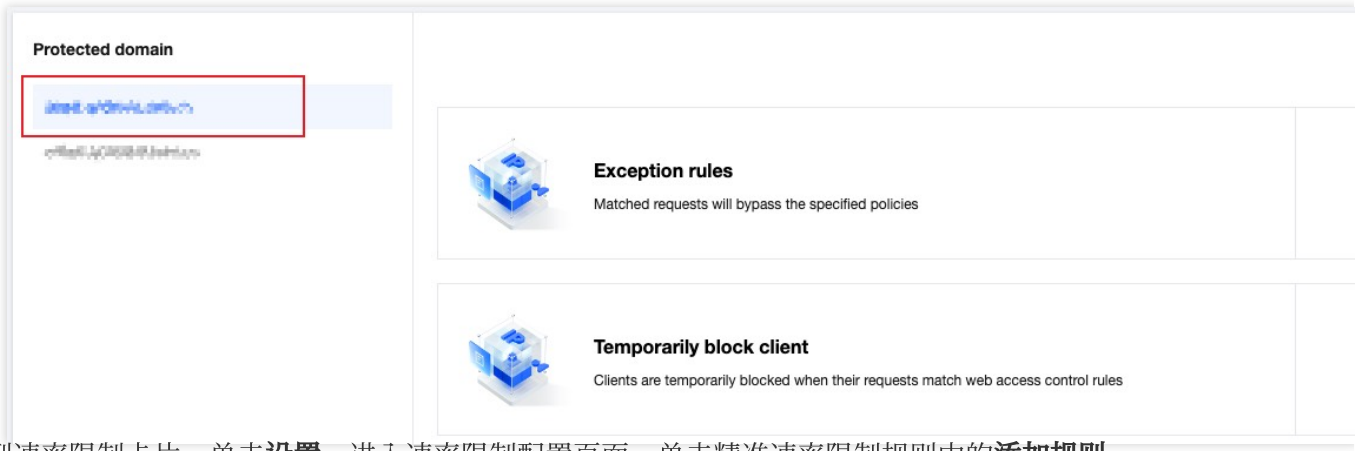
5. 单击**确定**后，规则将部署生效。

示例场景三：限制高并发的搜索引擎爬虫访问 Web 站点，缓解对正常业务的影响

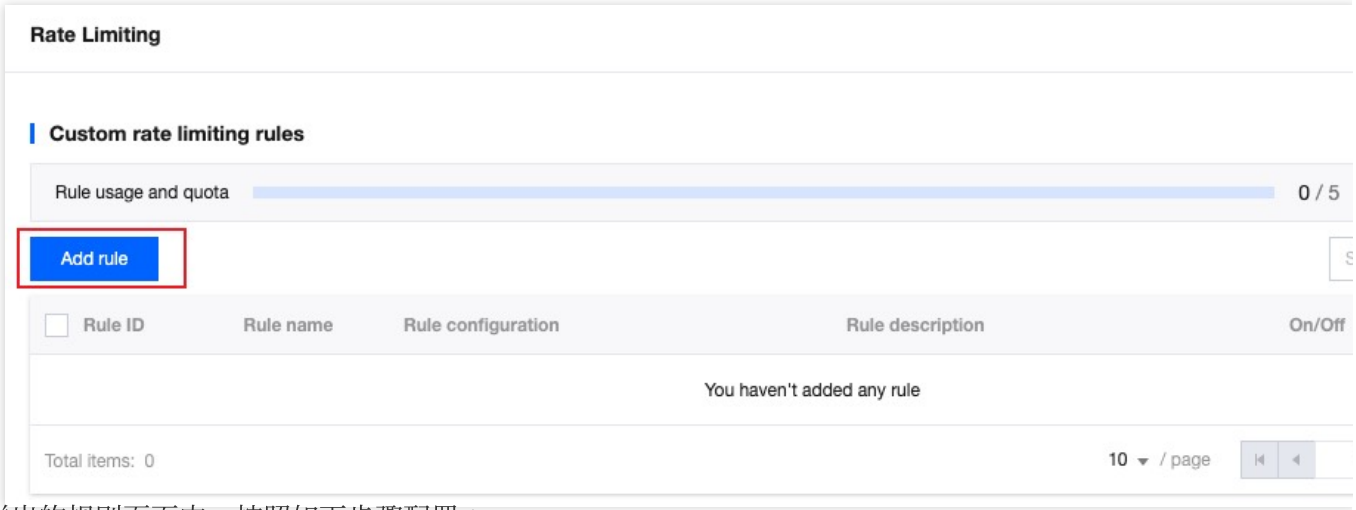
某 Y 搜索引擎供应商使用了大规模分布式的爬虫架构，对访问行为缺少限制，导致其爬虫行为较激进，短时间内产生较大访问量，对正常业务可能造成影响，并消耗大量资源。因此通过速率限制识别并限制该类爬虫访问，缓解其影响。例如：站点 `www.example.com` 由于 Y 搜索引擎爬虫高频访问影响正常业务。通过 Web 安全分析 分析，Y 搜索引擎的爬虫使用的分布式架构在 `JA3 指纹` 和 `User-Agent` 特征聚集，因此配置速率限制规则，当相同 JA3 指纹 和 User-Agent 的访问请求在 30 秒统计窗口超过 60 次时，对该 JA3 指纹和 User-Agent 特征相同的请求进行拦截，持续拦截10分钟。操作步骤如下：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，单击**安全防护> Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名，例如：`www.example.com`。



3. 找到速率限制卡片，单击**设置**。进入速率限制配置页面，单击精准速率限制规则中的**添加规则**。



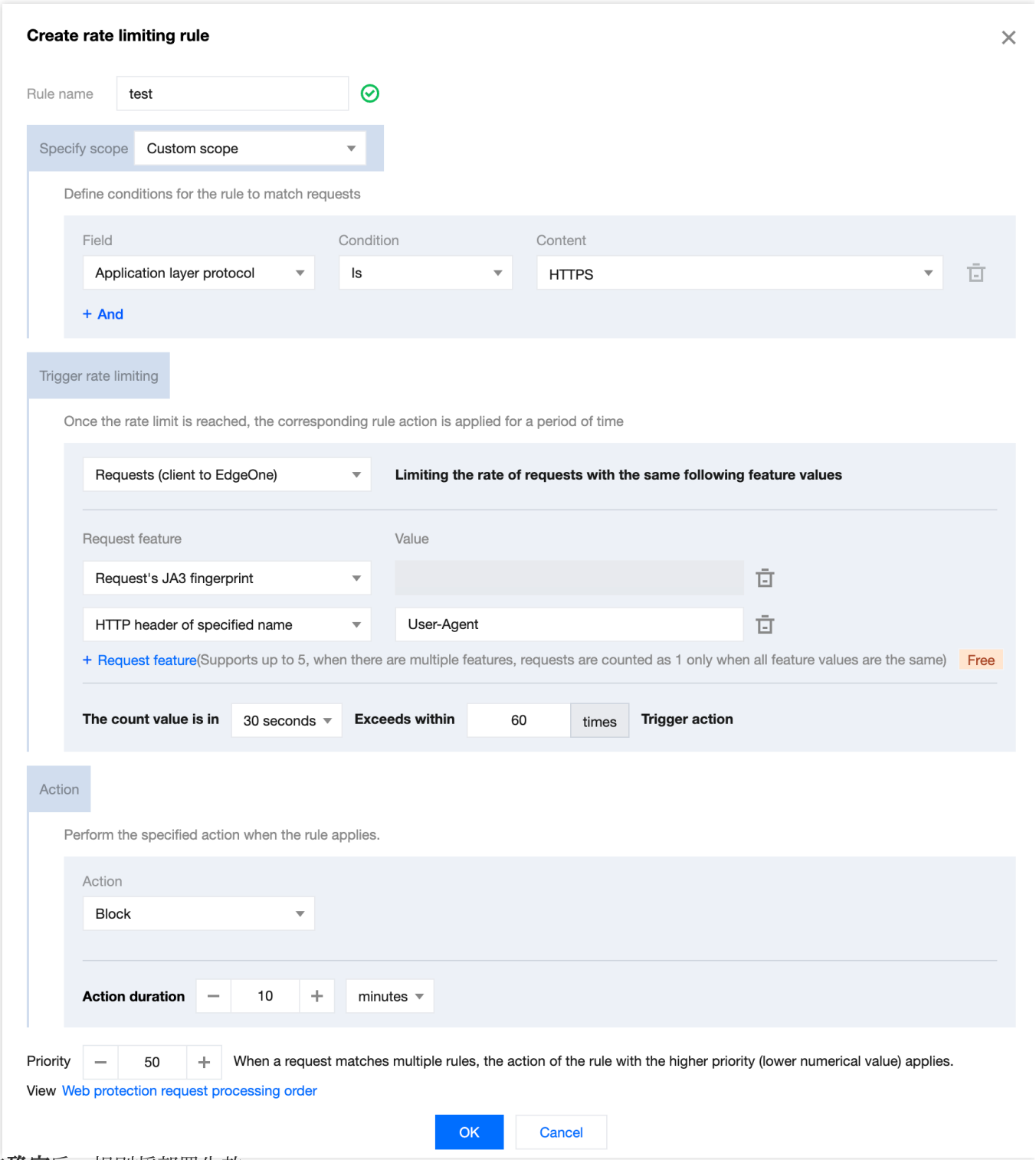
4. 在弹出的规则页面内，按照如下步骤配置：

4.1. 填写规则名称，匹配对象选择为**自定义防护对象**。

4.2. 在匹配条件列表选项，配置规则的匹配条件，以当前场景为例，匹配字段选择应用层协议等于 HTTPS。

4.3. 配置该规则的触发方式，以当前场景为例，配置请求为客户端至 EdgeOne，请求特征中 JA3 指纹和 HTTP 头部中的 User-Agent 特征相同的客户端，配置计数周期30秒内，计数超过60次时触发。

4.5.执行动作选择为拦截。完整的配置规则如下：



5. 单击**确定**后，规则将部署生效。

相关参考

创建速率限制规则时，需配置规则匹配对象、触发方式以及处置方式，各配置项说明如下：

注意：

如果您当前的速率规则，需要基于某个已知的确定值的 HTTP 头部进行匹配时，可通过配置匹配对象，指定匹配条件等于 HTTP 指定头部参数值进行匹配。
如果您当前的速率规则，需要基于一类可能存在相同值的 HTTP 头部进行匹配时，可通过配置统计维度，使用指定名称的 HTTP 头部进行匹配。

匹配对象

根据请求来源、头部特征、响应状态码等设定匹配条件组合[1]，速率限制规则仅对匹配条件的业务进行管控。匹配条件说明及不同套餐的支持程度详情请参见 匹配条件。

触发方式

说明：
未达到速率限制阈值时，请求不会进行处置，也不会记录日志。
规则将根据触发方式内配置的统计规则进行计数统计，在计数周期内累计请求次数超过阈值时，规则触发并执行对应限制动作[2]。统计基于技术周期和统计方式，对指定特征维度（如：客户端 IP）下不同特征值的请求次数计数[1]。
您可以定义触发方式的下列参数：
计数周期：用于计数时，滚动时间窗口的长度。支持最短 1 秒，最长 1 小时。
统计方式：区分请求来源的方式，速率限制为每个请求来源限制请求速率。详见统计维度。
速率阈值：计数周期内，每个来源（如客户端 IP）允许请求的次数。
触发状态保持时长：当规则触发后，对该来源匹配条件的请求持续限制[3]的时长。支持最短 1 秒，最长 30 天。

统计维度

支持基于一个或多个请求特征进行统计，当统计维度内的请求特征达到触发方式内设置的速率阈值时，则触发速率限制规则。您可以指定下列统计维度[1]：
客户端 IP：来自相同源 IP 的请求将计入同一个计数器，超过阈值时触发规则的处置动作。
客户端 IP（优先匹配 XFF 头部）：来自相同客户端 IP 的请求将计入同一个计数器，超过阈值时触发规则的处置动作。当X-Forwarded-For 头部存在且包含合法 IP 列表时，将优先使用X-Forwarded-For 头部中第一个 IP 进行统计。
指定名称的 Cookie：提取请求头部中指定名称的 Cookie 值，相同 Cookie 值的请求计入同一个计数器，超过阈值时触发规则的处置动作。
例如：当站点使用名为 `user-session` 的 Cookie 标记访问会话时，您可以配置指定名称为 `user-session` 的 Cookie 值作为统计维度，对每个会话的请求速率进行统计。当单个会话中的请求速率超过阈值时，触发规则配置的处置动作。
指定名称的 HTTP 头部：提取请求头部中指定名称的头部值，相同头部值的请求计入同一个计数器，超过阈值时触发规则的处置动作。例如：您可以指定 Origin 头部，以限制来自每个外部域的访问频率，当某个外部域访问频率超过阈值时，触发规则配置的处置动作。
指定名称的 URL 查询参数：提取请求 URL 查询参数中指定名称的参数值，相同查询参数值的请求计入同一个计数器，超过阈值时触发规则的处置动作。

例如：当站点使用名为 `user-session` 的查询参数标记访问会话时，您可以配置指定名称为 `user-session` 的查询参数作为统计维度，对每个会话的请求速率进行统计。当单个会话中的请求速率超过阈值时，触发规则配置的处置动作。

请求的 JA3 指纹[4]：计算每个请求的 JA3 指纹，讲 JA3 指纹相同的请求计数统计，超过阈值时触发规则的处置动作。每个请求对应了唯一的 JA3 指纹值，不存在键值模型，因此无需输入指定参数。考虑到 JA3 的特性，建议您将其与 User-Agent 头部统计维度同时配置，以较好地区分客户端。

说明：

注 1：根据您订阅的套餐，支持配置的匹配条件、统计维度和处置方式选项可能会有所不同。详情请参考 套餐选项对比。

注 2：如果存在多条速率限制规则，一个请求可同时匹配多条规则内容，会同时根据不同规则的统计方式来决定是否触发该规则。当统计触发其中一个规则并被拦截后，其余规则将不会再被触发。当多条规则同时被触发时，按照已触发规则的优先级顺序执行，优先级数值小的规则优先匹配。详见 Web 防护请求处理顺序。

注 3：规则触发后，仅对匹配当前规则的请求生效。

注 4：JA3 指纹是基于客户端的 TLS 信息形成的识别信息，可以有效区分来自不同 Bot 网络的请求。当请求基于非 SSL 的 HTTP 协议发起时，请求的 JA3 指纹为空。如果需要使用 JA3 指纹，请确保您当前域名已开启 Bot 管理功能。

注 5：如果您需要通过多种统计维度组合，对请求特征相同的请求进行统计，需订阅 EdgeOne 企业版套餐。

处置方式

当请求超过限制阈值时，采取相应的限制动作。支持拦截、观察、JavaScript 挑战、重定向至 URL 和响应自定义页面[1]，详细处置方式说明，请参见 处置方式。

防护例外规则

最近更新时间：2024-01-02 10:48:07

概述

防护例外规则提供了集中的访问白名单配置选项，可快速配置放行合法请求，避免被其他模块拦截。除此之外，当 EdgeOne 内置的预设防护策略（如 CC 攻击防护、托管规则等）未准确识别区分合法请求时，防护例外规则可以为您提供精细化调优配置，精准指定需要放行的请求或请求参数。

说明：

防护例外规则中，**部分请求字段跳过规则扫码**功能仅 EdgeOne 企业版套餐支持。

典型场景与配置方式

防护例外规则可在已有防护策略基础上，指定符合特征的正常请求跳过指定模块或指定规则的扫描。

说明：

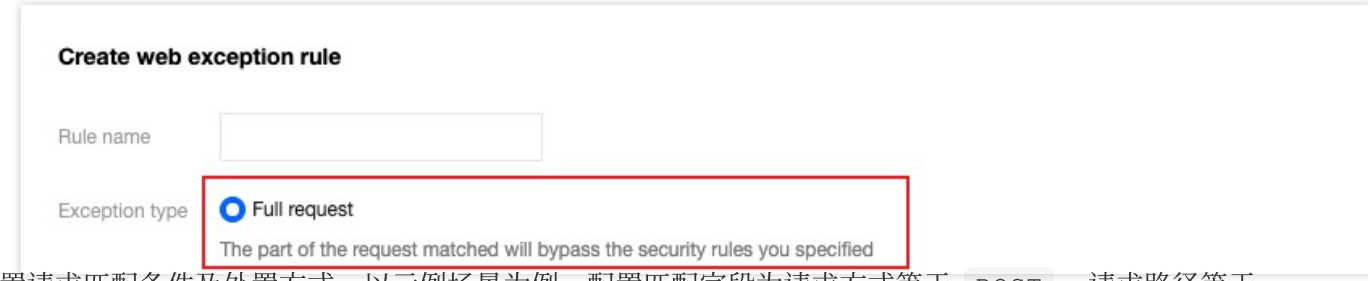
1. 支持跳过**自定义规则、速率限制、CC 攻击防护、托管规则**防护模块。
2. 如需跳过Bot 管理模块，请使用 **Bot 管理 > 防护例外规则**或**自定义 Bot 规则**进行配置。

示例场景一：指定高频 API 接口请求跳过 CC 攻击防护扫描

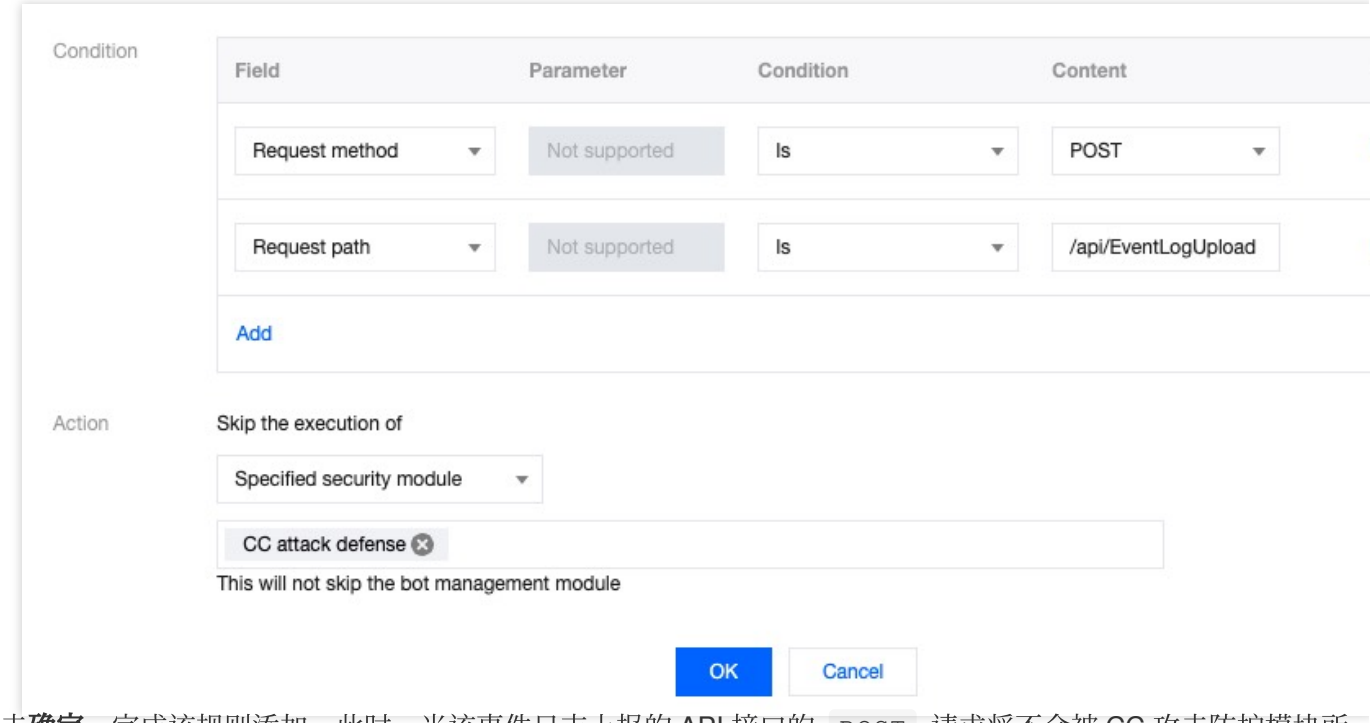
当前站点域名 `api.example.com` ，用于事件上报的 API 接口为 `/api/EventLogUpload` ，在业务突增时，可能出现突发高频访问的场景。这样的访问模式极容易被 CC 攻击防护识别为攻击并进行拦截。对于该接口，可通过配置防护例外规则跳过 CC 攻击防护模块，避免误拦截。操作步骤如下：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名，例如： `api.example.com` 。
3. 找到防护例外规则卡片，单击**设置**。进入 Web 防护例外规则列表，单击**添加规则**。

4. 在新建 Web 防护例外规则弹窗中，填写规则名称，例外类型选择为**完整请求跳过规则**。



5. 配置请求匹配条件及处置方式，以示例场景为例，配置匹配字段为请求方式等于 `POST`，请求路径等于 `/api/EventLogUpload` 时，处置方式选择为指定安全防护模块中的 CC 攻击防护。匹配字段可配置多个，多条同时存在为“且”的匹配关系。详细匹配条件介绍可参考：匹配条件。



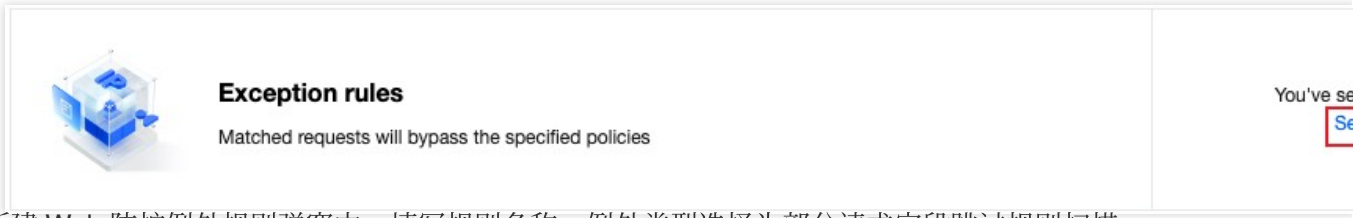
6. 单击**确定**，完成该规则添加。此时，当该事件日志上报的 API 接口的 `POST` 请求将不会被 CC 攻击防护模块所拦截，避免了高频日志上报产生误拦截的可能，同时其他接口可正常接受检测防护。

示例场景二：避免个人博客内容被漏洞防护误拦截

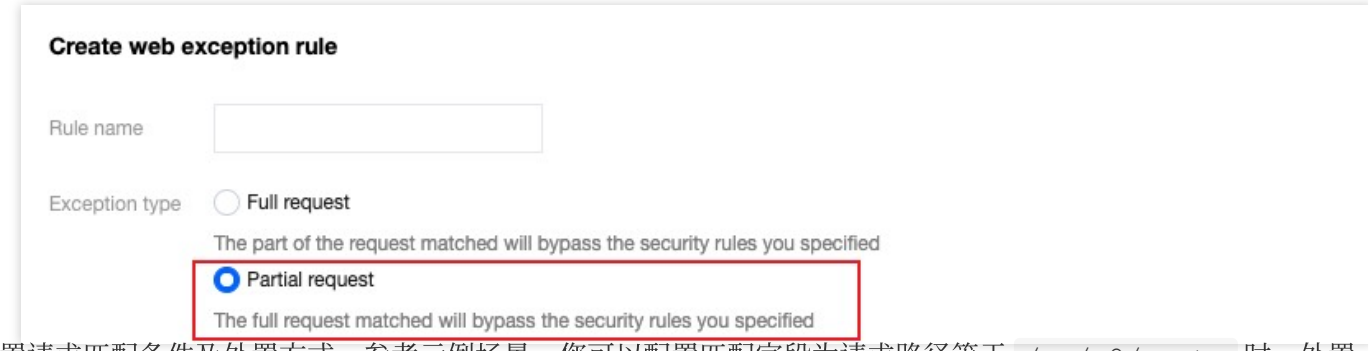
当前站点下域名 `blog.example.com` 用于博客内容分享，该博客基于 WordPress 搭建。其中博客内容可能分享的技术内容相关文本（例如：SQL 和 Shell 命令示例），发布博客时会因为博客内容文本匹配 SQL 注入攻击特征而触发防护规则。通过防护例外规则，可配置请求参数白名单，匹配博客发布 API 接口路径 `/wp/v2/posts`，指定对发布内容请求中的文本参数 `Content` 不参与 SQL 注入攻击规则扫描，避免对博客内容的误报和拦截。操作步骤如下：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

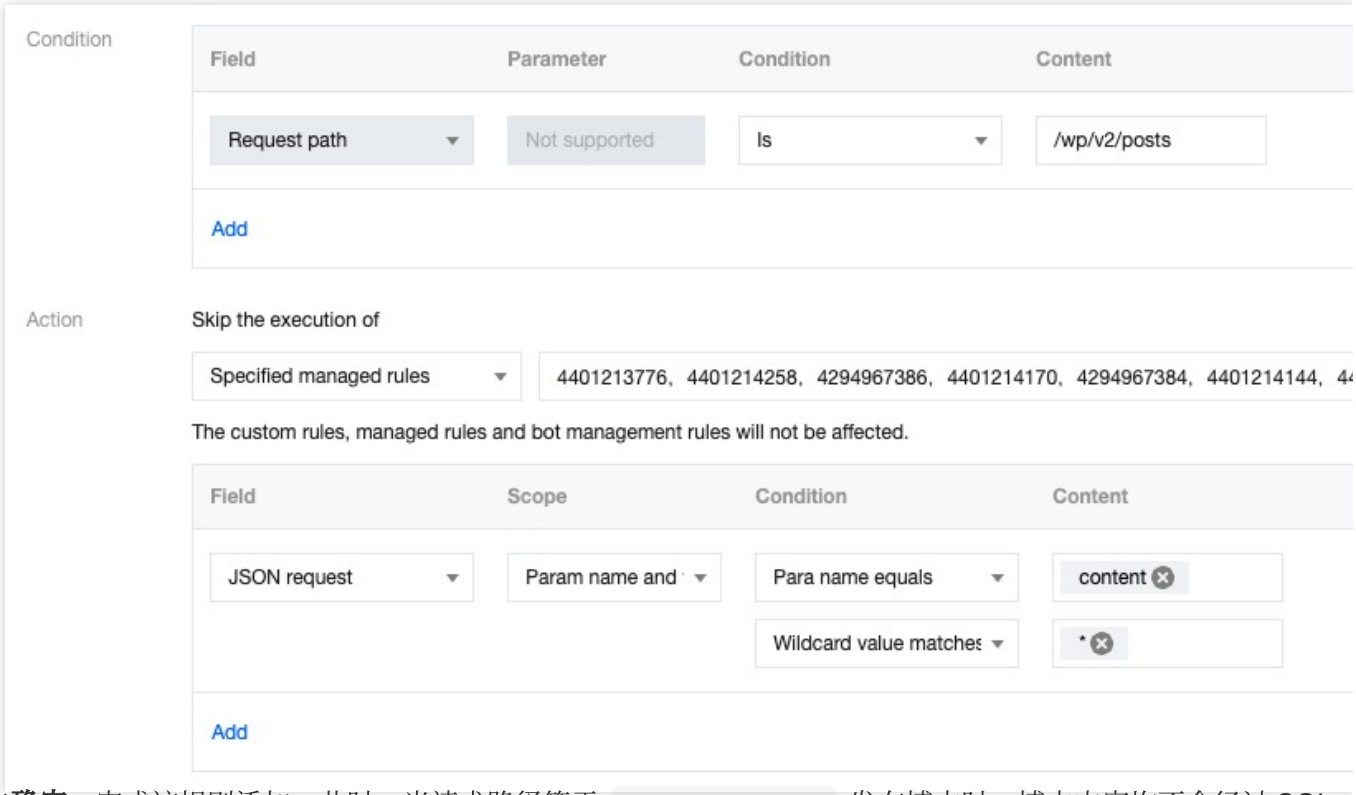
2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名，例如：`api.example.com`。
3. 找到防护例外规则卡片，单击**设置。**进入 Web 防护例外规则列表，单击**添加规则**。



4. 在新建 Web 防护例外规则弹窗中，填写规则名称，例外类型选择为部分请求字段跳过规则扫描。



5. 配置请求匹配条件及处置方式，参考示例场景，您可以配置匹配字段为请求路径等于 `/wp/v2/posts` 时，处置方式为指定托管规则包括所有 SQL 注入攻击防护规则，不扫描 JSON 请求内容中指定参数名称等于 `content`，且参数值通配符匹配为 `*` 的参数内容。详细匹配条件介绍可参考：匹配条件。



6. 单击**确定**，完成该规则添加。此时，当请求路径等于 `/wp/v2/posts` 发布博文时，博文内容均不会经过 SQL 注入攻击防护规则校验，可以避免正常文本内容被误扫描为攻击行为。

相关参考

部分请求字段跳过规则扫描时支持的例外字段类型说明如下：

类别	选项
JSON 请求内容	全部参数 匹配指定名称的参数 匹配条件的参数
Cookie 头部	全部参数 匹配指定名称的参数 匹配条件的参数
HTTP 头部参数	全部参数 匹配指定名称的参数 匹配条件的参数
URL 编码内容或查询参数	全部参数 匹配指定名称的参数 匹配条件的参数

请求路径 URI	查询参数部分 路径部分 完整路径
请求正文内容	完整请求正文 分段文件名

说明：

匹配条件的参数通过同时指定参数名称和参数值的匹配条件完成，参数名称和值都支持完整匹配和通配符匹配。

托管定制规则

最近更新时间：2024-05-08 21:44:08

当您使用 EdgeOne 提供的安全专家服务时（包括活动保障、应急攻防、安全托管和策略定制服务），腾讯安全专家将根据业务场景和攻击手法为您的业务定制安全策略。托管定制策略仅提供规则展示，不支持控制台调整匹配条件或处置方式。如您的业务有变更，或您有特殊安全防护诉求，请联系 腾讯云技术支持。

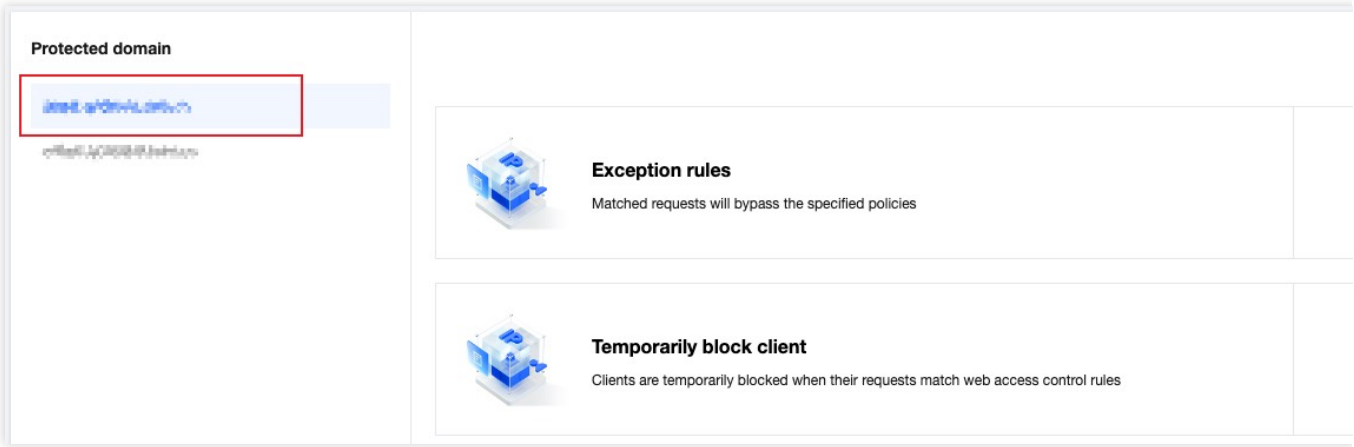
说明：

自定义规则、速率限制支持托管定制规则。

定制的规则将在托管定制策略列表中展示，如您当前已定制有托管规则，可以按照如下步骤查看：

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，单击**安全防护 > Web 防护**，进入 Web 防护详情页左侧的防护域名列表中，选择需开启防护的域名。



3. 找到自定义规则或者速率限制卡片，单击**设置**，即可看到托管定制规则。

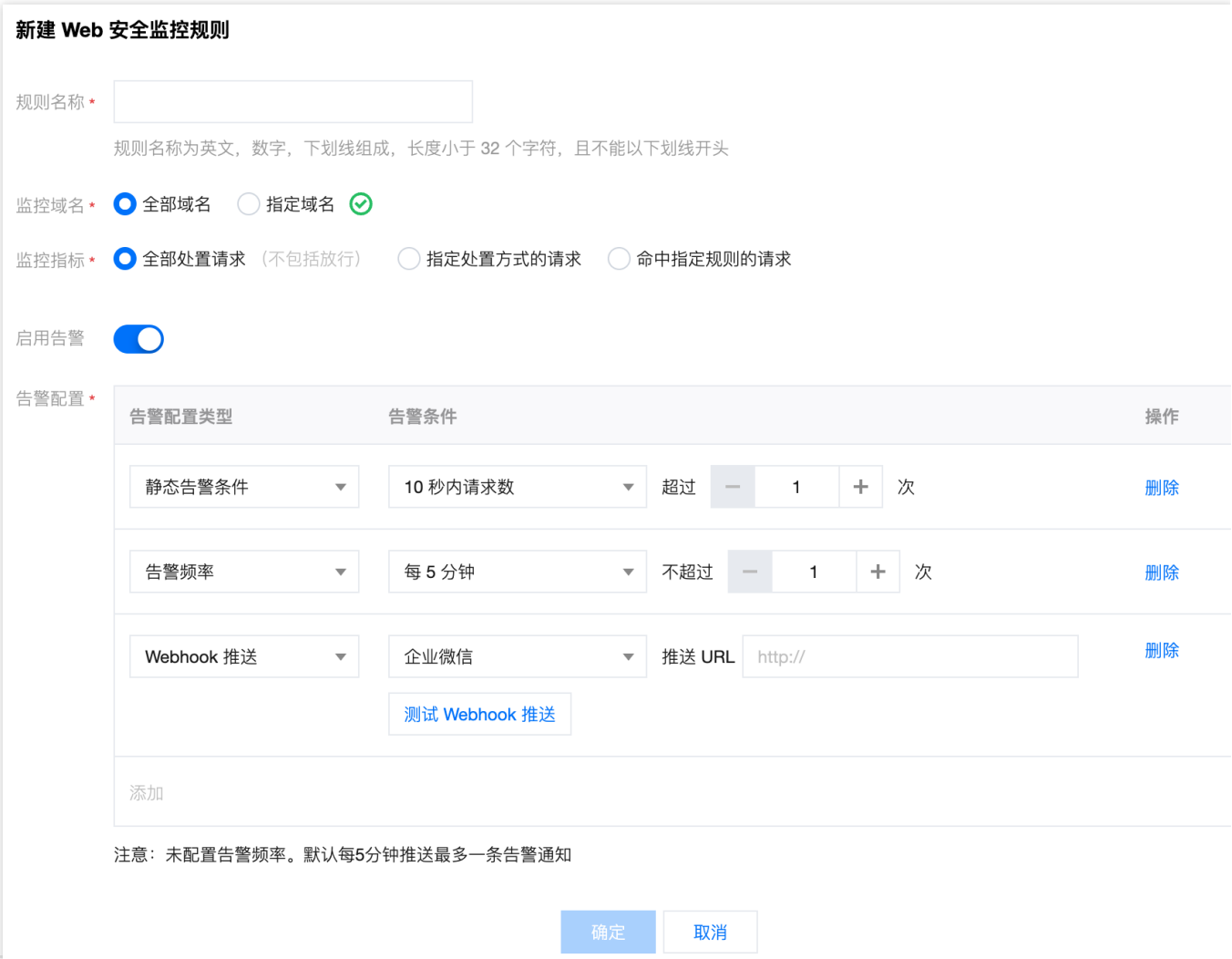
Web 安全监控告警

最近更新时间：2024-04-16 16:49:55

功能简介

Web 安全监控规则可为您提供实时、定制化的安全事件通知，并支持 Webhook 推送，使告警与常用企业通讯工具无缝对接，提高安全运维效率，帮助您快速发现并应对潜在风险。您可以根据业务需求和风险评估，灵活配置监控范围、阈值和告警频率。

配置项说明



配置项	说明
规则名称（必填）	需满足以下要求：

		英文、数字和下划线组合； 长度小于32个字符； 不可使用下划线开头。
监控域名（必选）		**全部域名：**包含本站点下全部域名，也包括后续添加的域名。 **指定域名：**仅监控本站点下特定域名。 **说明** 阈值统计仅针对单个域名独立生效，不会合并统计多个域名内的请求数。
监控指标（必选）		支持按处置方式或者按规则选择统计请求范围。 **全部处置请求：**所有命中安全模块规则，并被处置的请求（不包括放行），计入监控规则的统计计数。 **仅统计指定处置方式的请求：**命中 Web 防护或 Bot 管理规则，并最终按选择的方式处置的请求，计入监控规则的统计计数。 **仅统计命中指定规则的请求：**命中指定 Web 防护或 Bot 管理规则的请求。 **说明** 放行方式不会记录日志，因此不会加入监控统计。
告警开关		控制本条 Web 安全监控规则是否生效。 开启后，将通过消息中心提供的消息推送渠道（站内信/邮件/短信/微信/语音/企业微信服务号）进行告警，具体消息推送渠道可在 消息中心控制台 进行配置。 关闭后，本条 Web 安全监控规则将不再告警，包括消息中心相关渠道和 Webhook 推送。 **说明** EdgeOne Web 安全监控告警消息对应消息中心的「安全事件通知」类型消息。
告警配置	静态告警条件（必选）	支持配置按照指定时间窗口内请求达到的阈值数量，当达到指定阈值时，即触发告警。
	告警频率（可选）	配置推送告警的频率。当未进行自定义配置时，默认每条规则每 5 分钟最多推送 1 条告警通知。
	Webhook 推送（可选）	在 消息中心 提供的消息推送渠道之外，额外提供 Webhook 接口回调方式。 目前支持的渠道包括：企业微信、飞书、钉钉、自定义接口回调。当您填写对应渠道的 Webhook 地址后，可单击**测试 Webhook 推送**，EdgeOne 将向您填写的地址推送一条测试消息以验证连通性。 消息内容模板以 Go text/template 语法定义，支持通过 `{{.通知变量}}` 引用与 Web 安全监控相关的变量。具体可参考消息内容模板与通知变量。

场景一：监控站点遭遇 CC 攻击事件并在 5 分钟内告警

某金融业务站点为满足监管合规要求，当业务域名 `www.example.com` 被 CC 攻击时需要在 5 分钟内快速响应。因此对站点的 CC 攻击事件进行监控。当站点遭受超过 5000 QPS CC 攻击时，5 分钟内推送告警至其安全运维团队处理。

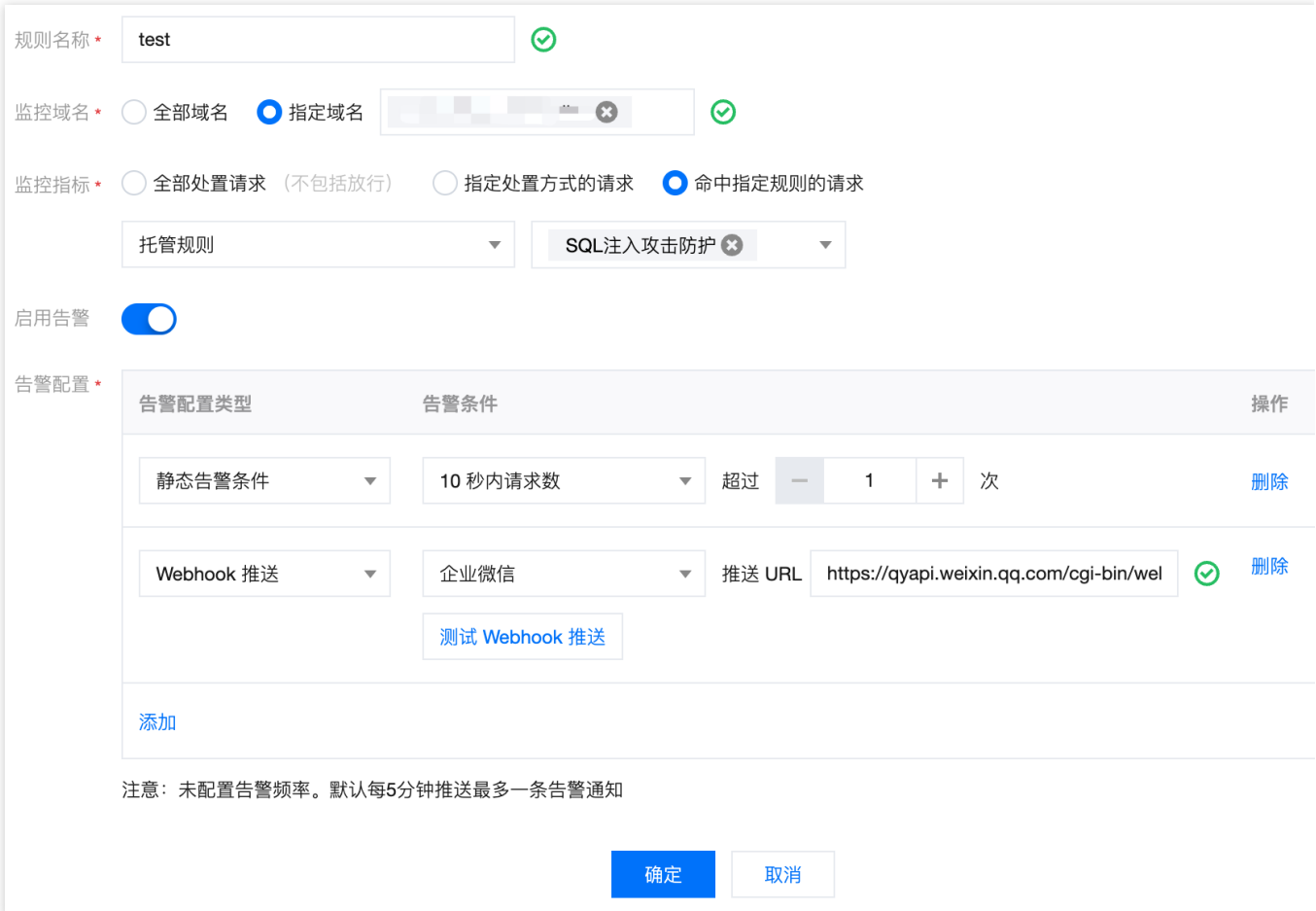
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **告警通知推送**，进入告警通知推送详情页面。
3. 在 Web 安全监控规则卡片中，单击**设置**，进入规则管理页面。
4. 单**击添加规则**，配置对应的告警规则。以当前场景为例，输入规则名称后，选择监控域名为 `www.example.com`，监控指标为 CC 攻击防护中高频访问请求限制、智能客户端过滤和慢速攻击防护事件，当 10 秒内超出 50000 次 CC 攻击时，则立即触发告警并通过您在 消息中心控制台 配置的通知渠道发送告警消息。

5. 单击**确定**完成配置。

场景二：监控命中托管规则的疑似漏洞攻击请求，并推送 Webhook 告警

某企业官网已接入的站点域名为 `www.example.com`，站点包含客户敏感信息，需时刻关注 SQL 注入类型漏洞攻击情况。当有任何请求命中了 SQL 注入攻击类别的 Web 托管规则时，需要立即触发告警并通过 Webhook 推送至企业微信机器人中，进行进一步分析。

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > 告警通知推送**，进入告警通知推送详情页面。
3. 在 Web 安全监控规则卡片中，单击**设置**，进入规则管理页面。
4. 单击**添加规则**，配置对应的告警规则。以当前场景为例，输入规则名称后，选择监控域名为 `www.example.com`，监控指标为请求命中托管规则为 SQL 注入攻击防护的规则，在 10 秒内超出 1 次，则立即触发告警并通过您在 消息中心控制台 配置的通知渠道发送告警消息，同时通过 Webhook 推送至指定的 URL 地址中。

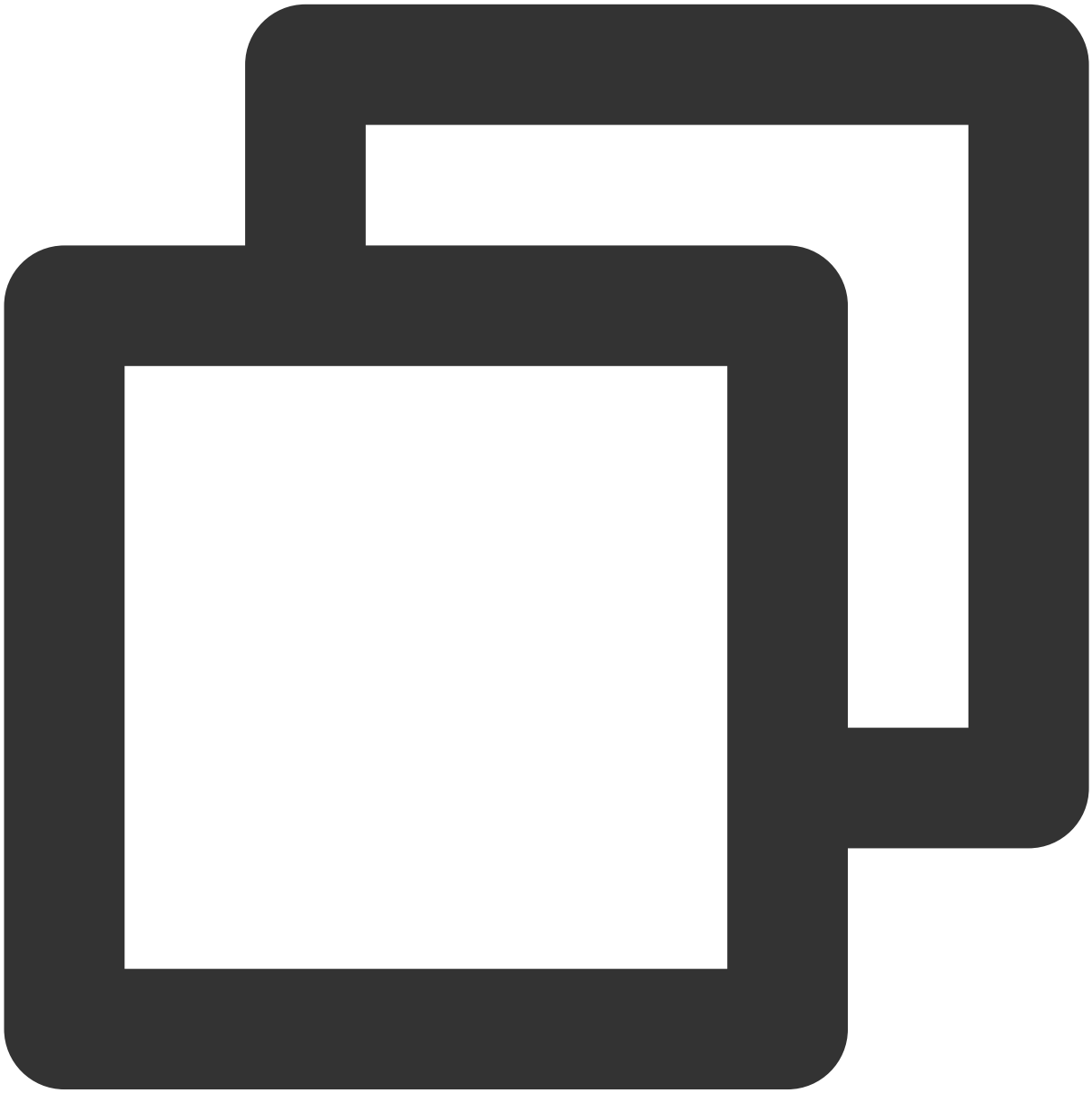


5. 单击**确定**完成配置。

相关参考

Webhook 消息内容模板

消息内容模板以 Go text/template 语法定义，支持通过 `{{.通知变量}}` 引用与 Web 安全监控相关的变量。默认消息内容模板如下：



```
通知类型：站点安全监控通知

账号ID: {{.UIN}}
昵称: {{.AccountName}}
```

```
站点名称：{{.Zone}}
监控对象：{{.Object}}
监控规则名称：{{.AlertRule}}
告警时间：{{.StartTime}} (GMT +8:00)
告警条件：{{.Condition.TimeSpan}}秒内超过{{.Condition.Threshold}}个请求
监控项指标：{{.Condition.TimeSpan}}秒内{{.MetricValue}}个请求
```

通知变量名称	数据类型	变量含义
UIN	String	腾讯云账号 ID
AccountName	String	腾讯云账号昵称
Zone	String	EdgeOne 站点名称
AlertRule	String	告警策略名称
Object	Array of String	告警对象（用户配置的监控域名）
Condition	JSON object	告警触发条件（用户配置的静态告警条件）
StartTime	String	告警触发时间，默认时区为东八区，示例值：2024-01-08 18:00:40
MetricValue	Integer	告警触发时告警指标值

说明

目前控制台不支持自助修改消息内容模板，若您有相关需求，请联系 售后支持。

Condition 对象结构

告警触发条件，即用户配置的静态告警条件。

key 名称	value 含义
TimeSpan	用户配置的告警时间窗口
Threshold	用户配置的请求数静态阈值

相关参考

Web 防护请求处理顺序

最近更新时间：2023-07-28 14:35:46

当 Web 防护收到请求时，会先按照下列顺序经过各个安全模块处理，只有通过安全模块扫描后的请求才会继续由其他功能模块处理。

模块处理顺序	请求处理方式
防护例外规则	请求匹配多条规则时，所有匹配的规则均生效。
自定义规则	请求匹配多条规则时，按优先级自高到低（优先级数值从小到大）执行[注1]。
速率限制	请求命中的规则均进行计数，满足速率条件的规则独立生效[注2]。 满足速率条件的规则按优先级自高到低（优先级数值从小到大）执行[注2]。
CC 攻击防护	请求命中多条规则时，所有匹配的规则均生效。
Bot 管理	详情请见 Bot 管理。

说明：

注1：
请求匹配多条自定义规则时，如优先级较高的规则处置了请求（观察除外），请求不再继续匹配优先级较低的规则。优先级相同时，按处置方式顺序执行：观察 > 放行 > 托管挑战 > JavaScript 挑战 > 重定向 > 返回指定页面 > 封禁 IP > 拦截。

注2：
命中已生效的速率限制规则不影响其他速率限制规则统计计数。同一请求命中多条速率限制规则时，按已生效的速率限制规则优先级顺序进行匹配并处置。同时有多条相同优先级的速率限制规则生效，并被请求同时匹配时，按处置方式顺序执行：观察 > 放行 > 托管挑战 > JavaScript 挑战 > 重定向 > 返回指定页面 > 封禁 IP > 拦截。

处置方式

最近更新时间：2023-11-24 16:49:06

Web 防护模块提供多种处置方式。不同功能模块支持使用的处置方式有所不同，请参考具体功能模块文档。

处置方式	用途	处置方式描述	后续动作
拦截	用于阻断请求访问站点（包括缓存或非缓存内容）。	响应拦截页面和拦截状态码。	不再匹配其他策略
放行	用于跳过当前安全模块其余规则。	当前模块中，其余规则不再匹配该请求。	继续匹配其他生效的规则
观察	用于评估或灰度安全策略。	仅记录日志，不进行处置。	继续匹配其他规则
重定向	用于提供备用资源，改进被拦截时的用户访问体验。	重定向至指定 URL。	不再匹配其他策略
返回自定义页面	用于提供体验更好的拦截页面。 用于兼容 API 格式，响应 API 可以解析的错误信息。 用于业务监控，通过指定状态码监控被拦截的请求。	返回自定义错误页面和状态码。支持引用 自定义错误页面 功能中定义的页面内容。	不再匹配其他策略
IP 封禁	用于惩罚恶意客户端。	当有请求命中匹配条件时，丢弃一段时间内来自该客户端 IP 的请求。	不再匹配其他策略
JavaScript 挑战	用于识别不支持 JavaScript 的工具客户端，常见于 DDoS 攻击源。	响应重定向（HTTP 302）页面，页面携带 JavaScript 代码验证客户端浏览器行为，仅通过校验的访客可以继续访问。	通过挑战的请求继续匹配其他规则
托管挑战	用于 Bot 对抗， 首先进行 JavaScript 挑战校验，对通过校验的请求再进行 CAPTCHA 人机校验。	首先进行 JavaScript 挑战；对通过校验的客户端，响应重定向（HTTP 302）页面，携带验证码校验，用户通过交互操作完成校验。两次校验都通过的访客才可以继续访问。	通过挑战的请求继续匹配其他规则

匹配条件

最近更新时间：2023-07-28 14:35:47

概述

Web 防护功能通过匹配请求的不同条件来实现访问管控。以下详细介绍了各种匹配条件选项、匹配条件说明以及相关配置方式和限制。

使用匹配条件

您可以使用规则的匹配条件指定规则的生效范围，控制防护例外规则、自定义规则、速率限制、自定义 Bot 规则的生效范围。

说明：

当配置了多个匹配条件时，规则仅在全部匹配条件都满足时生效。

匹配条件选项及说明

说明：

支持配置的匹配条件，根据规则类型和您订阅的 EdgeOne 套餐有些区别。具体支持情况请参考对应的功能介绍文档。

匹配条件选项	匹配条件说明	标准版套餐	企业版套餐
请求客户端 IP	匹配请求的来源IP地址。支持基于地域、ASN、IP 和 CIDR 网段进行匹配。 当使用 IP 和 CIDR 网段匹配时，可以引用 IP 分组。 单个匹配条件最多可配置8个 IP 分组。	支持	支持
请求客户端 IP（优先匹配 XFF 头部）	当请求携带合法 XFF（X-Forwarded-For）头部时，匹配 XFF 头部第一个 IP；否则，匹配来源 IP 地址。	不支持	支持
自定义请求头部	匹配请求的指定头部，提供额外参数选项匹配特定名称的头部值。 忽略大小写。 支持等于、不等于、包含、不包含、通配符匹配、通配符不匹配、长度大于、长度小于、内容为空、不存在、正则匹配。 最多支持128个匹配值。	不支持	支持

请求 URL	匹配请求的 URL。 忽略大小写。 支持等于、不等于、包含、不包含、通配符匹配、通配符不匹配、长度大于、长度小于、内容为空、不存在、正则匹配。 最多支持128个匹配值。	匹配条件不支持正则匹配	支持
请求来源（Referer 头部）	匹配请求的 Referer 头部。 忽略大小写。 支持等于、不等于、包含、不包含、通配符匹配、通配符不匹配、长度大于、长度小于、内容为空、不存在、正则匹配。 最多支持128个匹配值。	匹配条件不支持正则匹配	支持
请求内容类型（Accept 头部）	匹配请求的 Accept 头部。 忽略大小写。 支持等于、不等于、包含、不包含、通配符匹配、通配符不匹配、长度大于、长度小于、内容为空、不存在、正则匹配。 最多支持128个匹配值。	不支持	支持
请求路径（Path）	匹配请求 URL 的路径部分（不包含查询参数）。 忽略大小写。	不支持	支持
请求方式（Method）	匹配请求的方法。 忽略大小写。 支持多项选择：GET、POST、HEAD、PUT、DELETE、TRACE、OPTIONS、CONNECT。	匹配条件不支持正则匹配	支持
请求 Cookie	匹配指定请求 Cookie 头部参数值。需指定 Cookie 参数名称。 忽略大小写。 支持等于、不等于、包含、不包含、通配符匹配、通配符不匹配、长度大于、长度小于、内容为空、不存在、正则匹配。 最多支持128个匹配值。	不支持	支持
XFF 扩展头部	匹配请求的 XFF（X-Forwarded-For）头部。 忽略大小写。 支持等于、不等于、包含、不包含、通配符匹配、通配符不匹配、长度大于、长度小于、内容为空、不存在、正则匹配。 最多支持128个匹配值。	不支持	支持
网络层协议	匹配请求使用的 IP 协议类型。 支持多项选择：IPv4、IPv6。	不支持	支持

应用层协议	匹配请求使用的应用层协议。 支持多项选择：HTTP、HTTPS。	不支持	支持
响应状态码	匹配响应的 HTTP 状态码。 仅支持速率限制，选择基于响应统计时支持配置。 最多支持同时匹配20个状态码。	不支持	支持

Bot 管理

概述

最近更新时间：2023-09-21 10:45:19

Bot 管理是一项维护您网站流量质量的服务。在您的网站访客中，可能有一部分并非真实用户发起的访问，而是由自动化程序操控的访问请求，我们通常称之为 Bot。虽然一些 Bot（例如：搜索引擎的爬虫）对网站有所助益，但同时也可能会引发以下问题：

1. **网站流量异常或性能下降**：大量的 Bot 访问可能会消耗大量服务器资源，从而影响真实用户的访问体验。此时，Bot 管理有助于识别和控制这些 Bot，优化网站性能和提升用户体验。
2. **数据统计出现异常，例如访问量、点击率等**：这可能是由于 Bot 模拟用户行为造成的。Bot 管理能更准确地区分真实用户和 Bot 的行为，让您获得更真实的数据。
3. **网站内容或用户信息被泄露或滥用**：Bot 可能会尝试爬取和复制网站内容，或者获取用户个人信息。Bot 管理能有效阻止这类无授权的访问，保护网站内容和用户信息的安全。

如果您在运营网站的过程中遇到了上述的问题，那么 Bot 管理正是您需要的工具。

功能概述

Bot 管理主要包括以下功能，将按照如下顺序处理请求。

说明：

Bot 管理功能仅当站点域名开启 Bot 管理能力后支持，开启后，Bot 管理的计费标准详见：增值服务用量单元费用（后付费）

模块	功能说明
例外规则	放行特定请求，使其不经过 Bot 管理模块处理。例如：来自合作伙伴指定 IP 的流量，或携带特定 User-Agent 的测试流量。
自定义 Bot 规则	可定制的灵活 Bot 管理规则，支持多种识别机制并提供灵活的处置选项。例如：延迟响应一半的自动购物车爬虫，并静默处置另一半。
Bot 基础访问管控	通过请求中 User-Agent 头部和客户端 IP 结合搜索引擎和工具的对应特征，识别 Bot 工具并进行管控。 例如：允许搜索引擎的 Bot 访问网站资源。
客户端画像分析	通过客户端 IP 结合 IP 威胁情报库，识别恶意 Bot 并提供管控。 例如：拦截使用秒拨 IP 等代理设备池进行恶意访问的 Bot 行为。
Bot 智能分析	快速部署 Bot 识别机制，综合多种 Bot 特征识别机制，快速部署，识别并分析网站流量模式的情况。它通过自动化分析和分类流量，提供了用户和机器人访问者的清晰视图，并允许针对不同类型的流量做出相应的处置决策。

主动特征识别	通过 Cookie 和 JavaScript 校验客户端运行环境和访问行为，识别人类浏览器客户端（不适用于非 H5 的原生移动端 APP）。

Bot 智能分析

最近更新时间：2023-10-11 10:37:27

功能概述

Bot 智能分析适用于需要快速部署，识别并分析网站流量模式的情况。Bot 智能分析基于聚类分析算法和大数据模型的智能引擎，旨在帮助您从多种角度综合判断请求风险，更便捷地使用 Bot 管理快速识别和处理已知或未知 Bot，避免固定单一的策略被绕过。Bot 智能分析将通过对多个因素进行综合分析，将请求分类为正常请求、正常Bot请求、疑似Bot请求以及恶意Bot请求，并支持对不同类型的请求进行相应的处置方式配置。

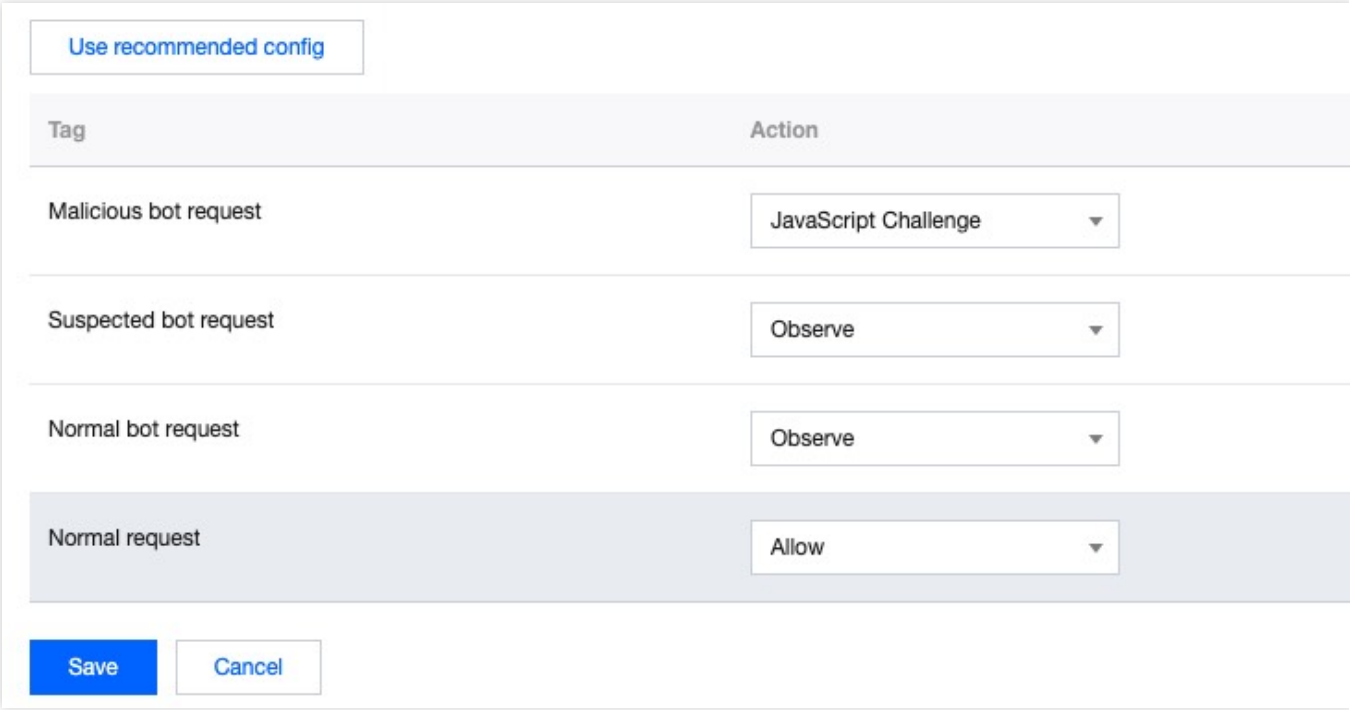
说明：

Bot 智能分析综合了 Bot 基础管理和客户端画像分析功能中的请求特点，并结合动态聚类分析，形成请求风险标签。Bot 智能分析可以帮助您了解整体访客情况并快速部署Bot管理策略。如您对于请求特征有非常明确的策略要求（例如：放行特定搜索引擎请求、拦截Web开发工具请求等），您可以进一步使用 Bot 基础管理、客户端画像分析和自定义 Bot 规则进行策略调整。

操作步骤

例如：电商站点 `shop.example.com` 发现商品展示页面访问用量突增，判断可能遭受了大量的 Bot 访问，因此通过 Bot 智能分析策略可快速启用 Bot 管理功能对 Bot 工具进行拦截。您可以参照以下步骤操作：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页。
3. 在 Bot 智能分析卡片中，点击**设置**，进入配置页面。以当前场景为例，可配置恶意 Bot 请求的处置方式为 JavaScript 挑战，疑似 Bot 请求和正常 Bot 请求保持为观察即可。



4. 点击**保存**，完成配置。

相关参考

请求的 Bot 标签

Bot 智能分析根据分析结果，将请求分类成下列类型：

恶意 Bot 请求：来自 Bot 的请求，风险较高，建议配置为拦截或者挑战处置动作。

疑似 Bot 请求：来自 Bot 客户端的请求，有一定风险，建议至少配置为观察或者挑战处置动作。

正常 Bot 请求：合法爬虫请求，包括来自搜索引擎爬虫的请求。

正常请求：客户端不具备明显 Bot 特征的请求，仅支持放行处置方式。

影响 Bot 智能分析判定的相关因素

Bot智能分析引擎将根据以下几个主要因素对请求进行综合评估：

1. **请求速率**：请求速率会影响 Bot 的识别结果，过高的请求速率可能存在恶意 Bot 行为。
2. **IP 情报库**：引擎将参考我们的 IP 情报库，识别是否有恶意行为记录或黑名单信息。
3. **搜索引擎特征**：根据源IP是否匹配合法搜索引擎爬虫，例如谷歌、百度等。
4. **访问 URL 序列**：分析访问 URL 的顺序和规律，以评估请求是否类似于正常用户行为或正常 Bot 行为。
5. **JA3 指纹**注1：利用 JA3 指纹技术识别客户端 TLS 连接的特征，以识别 Python 工具等非浏览器客户端。
6. **BotnetID 指纹**注2：通过分析 BotnetID 指纹，对比已知恶意 BotnetID，识别来自僵尸网络的恶意爬虫行为。

说明：

注1：

JA3是一种针对TLS客户端握手过程中的特征进行指纹生成的方法。通过收集客户端在TLS握手过程中提供的信息（如支持的加密套件、扩展等），生成一个唯一的哈希值作为指纹。JA3指纹可以帮助我们识别出使用特定工具或库发起请求的客户端，例如使用Python库发起的请求。通过对比客户端的JA3指纹与已知的恶意工具或库的指纹，我们可以更准确地识别潜在的恶意Bot行为。

注2：

BotnetID是一种基于Bot网络行为特征的识别方法。Bot网络（Botnet）通常由多个被控制的恶意设备组成，它们可能用于发起攻击或执行其他恶意活动。通过分析客户端行为特征及其与已知Bot网络的相似性，可以生成一个BotnetID。通过对比客户端的BotnetID与已知的恶意Bot网络ID，我们可以更准确地识别潜在的恶意Bot行为。

Bot 基础管理

最近更新时间：2023-10-11 10:37:50

功能概述

许多公开或商业化程序，包括搜索引擎爬虫，具备固定或默认的 User-Agent 头部特征，且有明确的用途。Bot 基础管理规则收录了大部分公开的 Bot 类型特征，您可以对符合这些特征的 Bot 工具直接管理，可以帮助您：
1）允许搜索引擎爬虫访问，避免误拦截；
2）识别特定用途的商业化工具，限制其访问。

EdgeOne 会定期更新自动化工具的特征，确保您的策略持续覆盖管控场景。

使用场景

默认情况下，Bot 基础管理策略为未启用状态。当您有以下场景诉求的时候，可以开启并按需调整 Bot 基础管理防护策略：

管控来源于 IDC（数据中心）的请求

大部分 To C 应用的访问来源均来自移动网络、宽带供应商、或教育网等网络，正常请求不会来源于数据中心（IDC）。因此，来自云供应商或者数据中心的请求，多来自于代理或者爬虫。您可以选择管控来源于数据中心（IDC）的请求，对其进行拦截或者 JavaScript 挑战，以缓解恶意访问的风险。

管控合法的具有搜索引擎特征的 Bot 请求

搜索引擎的爬虫是目前少数合法的 Bot 类型之一。为了站点能够区分来源于搜索引擎的合法爬虫，大部分搜索引擎供应商提供了其爬虫引擎使用的网段和 UA 特征。EdgeOne 的搜索引擎特征规则集合了搜索引擎公开的 IP 特征、User-Agent 头部特征、rDNS 解析特征等多种匹配方式。您可以针对搜索引擎特征的 Bot 请求配置为放行，以避免被 Bot 管理策略拦截。

管控来自于商用或开源工具的请求

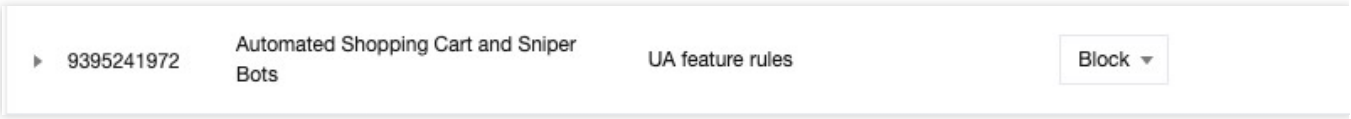
商业化工具软件或开源工具往往携带了特定的 User-Agent 特征，EdgeOne 根据使用用途对这些自动化工具进行了分类，并定期更新对应的 User-Agent 库。如果您不允许来自这些商业或者开源工具的 Bot 请求，您可以对其进行拦截。

调整基础管理防护策略

例如：当前您的站点 `shop.example.com` 是一个电商网站，为了避免被用户通过工具的方式来进行下单抢购，需要禁用自动购物车类的 Bot。您可以参照以下步骤操作：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页。
3. 在 Bot 基础管理设置卡片中，点击**设置**，进入配置页面。

4. 以选择 UA 特征规则，点击右上角**详细规则。**
5. 在详细规则页中，您可以单独针对指定的规则 ID 修改处置方式；如果您需要批量配置，也可以点击**批量配置**，批量勾选需要配置的规则 ID后，选择处置方式并应用。
以当前场景为例，您可以对自动购物车机器人，修改处置方式为**拦截**。



6. 点击确定，即可完成修改。

客户端画像分析

最近更新时间：2024-04-28 11:10:24

概述

恶意 Bot 通常会通过代理池、僵尸设备网络（botnet）或者特定设备发起请求。EdgeOne 的客户端画像分析通过使用腾讯近二十年的网络安全经验和大数据情报积累，实时判定 IP 状态，采取打分机制、量化风险值、精准识别来自恶意动态 IP 的访问，准确识别高危客户端，每 24 小时更新最新威胁情报并提供不同 IP 地址的威胁置信度报告，按照不同类型攻击的客户端提供5种 风险分类 和 置信度，您可以通过自定义每个威胁置信度的防护策略，来帮助您管控多种类别（网络攻击源、被利用的网络代理设备、漏洞扫描工具、破解登录客户端等）高危客户端访问，减少业务风险，有效拦截这类恶意行为。

示例场景

您在 Web 安全分析模块内，观察到 `api.example.com` 站点下，登录接口 `/api/login` 有高频访问，且在短时间内有大量失败访问请求，但是由于访问 IP 较多，主要来自宽带运营商网络，单个 IP 请求仅为 1-2 次。从访问特征判断，疑似使用秒拨 IP 进行暴力破解登录尝试。为加固安全策略，我们建议拦截较高置信度的网络代理客户端，并对中等置信度客户端设置为观察。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页面。
3. 在客户端画像分析卡片中，单击**设置**，进入配置页面。
4. 客户端画像分为网络攻击、网络代理、扫描器、账号接管攻击、恶意 BOT，您可以针对不同类型的客户端，自定义根据客户端画像置信度来选择相对应的处置方式。

以当前场景为例，秒拨 IP 属于典型的网络代理类型客户端，在观察到站点收到较高的分散 IP 高频访问时，您可以拦截较高置信度的网络代理客户端，并对中等置信度客户端设置为**观察**。

5. 单击**确定**，完成配置。

相关参考

风险分类

客户端画像分析基于实时的威胁情报库，能够有效识别具有以下5类恶意行为历史的客户端：

网络攻击：近期有攻击行为（如：DDoS，高频恶意请求、站点攻击等）的客户端。例如：Mirai 僵尸网络发起的攻击可以归入此类别。

网络代理：近期开放可疑代理端口，并且被用作网络代理的客户端，包括秒拨 IP 的代理池和用于发起恶意请求的 IoT 代理网络。

扫描器：近期有攻击已知漏洞的扫描器行为的客户端。例如：针对 Web 应用程序的漏洞扫描工具。

账号接管攻击：近期有恶意破解登录，发起账号接管攻击的客户端。例如：撞库等暴力破解用户登录凭据的攻击者。

恶意 Bot：近期有恶意爬虫、刷量和暴力破解行为的客户端。例如：采集网站内容的非法爬虫。

置信度

对于各个类别的客户端画像规则，每个置信度对应了一个客户端地址列表，置信度反应了该列表内的客户端地址近期进行该类别恶意行为的频率和一致性：

较高置信度：该客户端地址近期稳定、高频率进行该类别的恶意行为。建议对此类客户端进行拦截。

中等置信度：该客户端地址近期有过显著频率进行该类别的恶意行为。建议对此类客户端配置为 JavaScript 挑战或观察。

一般置信度：该客户端地址近期有过稳定进行该类别的恶意行为记录。建议对此类客户端配置为观察，后续可根据分析结果调整为 JavaScript 挑战或托管挑战。

主动特征识别

最近更新时间：2023-10-11 10:38:40

概述

除了对收到的客户端请求进行分析，识别头部和客户端 IP 中的特征，EdgeOne 也提供了主动特征识别的 Bot 识别方式。主动特征识别可以对客户端进行 Cookie 校验和会话跟踪，以及客户端行为校验来进行交互，进一步通过客户端的交互反馈来识别当前访问者是否为工具。主动特征识别具有以下优势：
对于能够模拟浏览器行为的工具（如：Headless Chrome 等）具有较强的识别效果。
相比其它前端校验方式（如：CAPTCHA 人机校验），主动特征识别的集成的方式对业务侵入性较小，用户几乎不会感知，可以为您带来更好的 Bot 识别效果和集成体验。

如果您当前站点服务中提供了登录/注册/支付服务，并且具有较高业务价值（例如：获取账号后可以获得账号内价值、通过支付可以获得稀缺商品或服务等），建议您针对关键业务接口启用主动特征识别。
说明：
1. 由于主动特征识别的机制特点，在开启前，请确认您的业务为 **Web 浏览器客户端**，或通过匹配条件将主动特征识别规则限制在**仅允许 Web 浏览器**访问的资源，避免因兼容性问题影响移动端 App 访问。
2. 该功能当前仍在内测中，如需开启请联系我们。

支持的能力

主动特征识别支持如下两种能力配置：
Cookie 校验和会话跟踪：通过 HTTP 会话状态（Cookie 机制）为每一个访客下发动态会话令牌，并要求访客请求必须携带合法会话令牌。从而跟踪并区分来自不同访客的请求并识别其行为特征。除了验证请求中的 Cookie 的合法性之外，Cookie 校验也会识别被篡改的会话信息以及高频采集 Cookie 信息的行为，降低劫持会话造成的安全风险。
客户端行为校验：高级自动化工具（如：Headless Chrome）已经可以模拟浏览器行为。客户端行为校验将通过在 HTML 响应页面中注入 JavaScript 代码，采集客户端的 JavaScript 运行环境、设备环境和客户端交互行为，从而识别工具环境和正常请求的访客。

场景一：拦截普通 Web 工具爬虫，对媒体站点 media.example.com 的访问

示例场景

媒体站点 `media.example.com` 仅允许 H5 客户端和浏览器获取站点内容，且合法客户端均支持 `Cookie` 。因此需要拦截不支持 `Cookie` 的客户端，包括劫持了其他访客会话的爬虫。对于恶意篡改 `Cookie` 的客户端使用静默方式进行对抗，保持连接但不再响应请求。

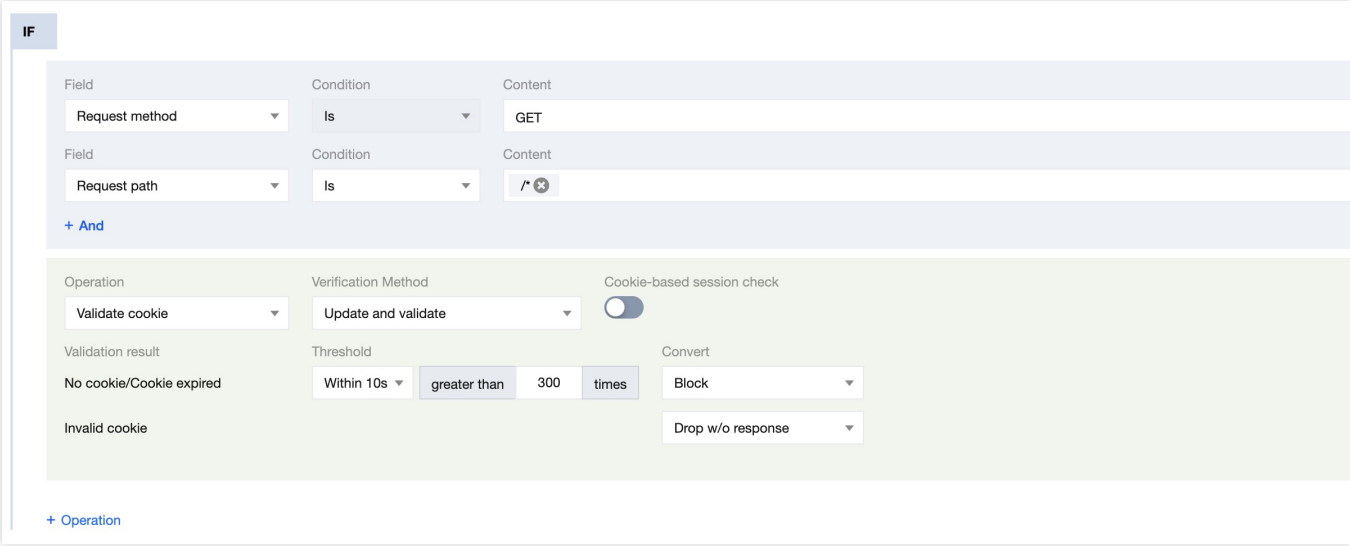
操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页面。
3. 在主动特征识别卡片中，单击**设置**，进入配置页面。
4. 单击**添加规则**，在选择匹配字段。以当前场景为例，可选择匹配字段为请求路径正则匹配 `/*` ，且请求方式等于 GET。
5. 单击**操作**，添加一个操作；选择操作为 Cookie 校验和会话跟踪，执行的处置方式可参考：处置方式。其它相关配置说明如下：

配置项	说明
校验方式	**更新 Cookie 并校验：**对于未携带合法会话信息或者会话信息过期的请求，EdgeOne 将在响应中携带 Set-Cookie 头部创建会话，并持续更新会话信息。建议使用 GET 方式访问的路径选用此校验方式。 **仅校验：**EdgeOne 仅校验请求中携带的会话信息是否合法。当请求中的会话信息过期或请求未携带合法会话信息时，不会通过更新 Cookie 创建新的会话。建议使用 POST 方式访问的接口（如：注册、登录、加购等）使用仅校验方式。
校验结果	未通过 Cookie 校验的请求，根据校验结果，可按照如下方式处理： **未携带 Cookie 或 Cookie 已过期：**Cookie 头部中携带的会话信息具有时效性，仅在一段时间内有效。若请求中未携带合法会话信息，或者会话信息过期时，需要更新会话信息才能通过 Cookie 校验。当客户端高频使用未携带会话信息的请求访问时，可能存在收割 Cookie 并劫持会话的风险。您可以选择未携带会话信息的请求到达指定速率时，处置来自该请求来源（客户端 IP），且未携带合法会话信息的请求。 **触发阈值：**您可以配置一段时间内允许的未携带 Cookie 或 Cookie 已过期可创建的会话数量上限，限制新会话的发起速率。当超过触发阈值时，将按照配置的处置方式处理。 **不合法 Cookie：**EdgeOne 下发的会话信息具备加密校验能力，随意篡改会话信息往往意味着恶意请求。您可以选项处置会话信息被篡改的请求。
会话速率和周期特征校验	通过 Cookie 校验的请求，根据预设速率特征，分为高风险、中风险和低风险三类。您可以为每个风险等级配置不同的处置方式，以便更有效地识别和防御恶意行为： **高风险：**单个会话（对应 Cookie 头部中，相同的 EO-Bot-SessionId 值）中，每 5 分钟统计窗口超过 1000 个请求。当开启客户端行为校验后，同时校验同一客户端校验票据（对应 Cookie 头部中，相同的 EO-Bot-Token 值）在 1 分钟内重复使用超过 200 次。 **中风险**：单个会话（对应 Cookie 头部中，相同的 EO-Bot-SessionId 值）中，每 5 分钟统计窗口超过 500 个请求。当开启客户端行为校验后，同时校验同一客户端校验票据（对应 Cookie 头部中，相同的 EO-Bot-Token 值）在 1 分钟内重复使用超过 100 次。 **低风险**：单个会话（对应 Cookie 头部中，相同的 EO-Bot-SessionId 值）中，每 5 分钟统计窗口超过 100 个请求。当开启客户端行为校验后，同时校验同一客户端校验票据（对应

	Cookie 头部中，相同的 EO-Bot-Token 值）在 1 分钟内重复使用超过 20 次。

以当前场景为例，您可以配置校验方式为更新 Cookie 并校验，配置当校验结果为未携带 Cookie 或 Cookie 已过期时，触发阈值为10秒内300次，则拦截请求；当有不合法 Cookie 请求时，静默处理。配置结果如下所示：



6. 单击**保存并发布**，即可完成配置。

场景二：使用客户端行为校验加固电商站点密码重置页面和 API，对抗批量重置密码的账号接管（ATO，Account Take Over）攻击

示例场景

电商站点 `shop.example.com` 的密码重置接口 `/api/password_reset` 发现有大量失败的重置请求，来自大量 IP，频率不高，且无明显 `User-Agent` 或者头部聚集性。因此使用主动特征识别功能，对密码重置接口 `/api/password_reset` 和密码重置页面 `/account/forgot_password.html` 加固 Bot 对抗策略，使用静默方式对抗自动化批量尝试重置密码工具。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页。
3. 在主动特征识别卡片中，单击**设置**，进入配置页面。
4. 单击**添加规则**，在选择匹配字段。以当前场景为例，可选择匹配字段为请求路径等于 `/account/forgot_password.html` 。

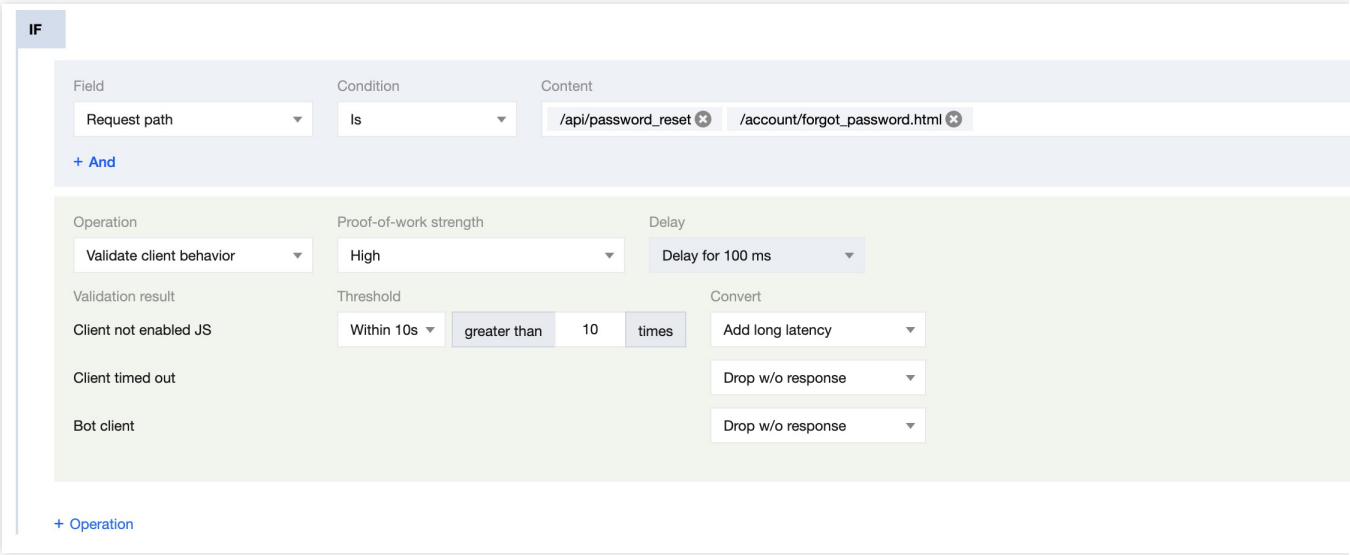
5. 在规则配置页面内，单击**操作**，添加一个操作；选择操作为客户端行为校验，执行的处置方式可参考：处置方式。相关配置说明如下：

说明：

客户端行为校验仅会在响应的 `Content-Type` 为 `text/html` 时注入 JavaScript 进行校验，其它请求会根据当前校验结果进行处置。

配置项	说明
工作量证明校验	客户端行为校验支持工作量证明校验的强度调整。通过调整强度，可以平衡客户端的计算负载和对 Bot 的识别效果。
执行方式	用于探测的 JavaScript 代码会在整个页面加载完成后运行，同时支持延迟一定时间执行 JavaScript 探测代码。这有助于避免影响正常页面渲染，确保浏览器先加载完成页面再进行校验，从而避免影响用户访问体验。
校验结果	客户端未启用 JS（未完成检测）：对于不支持 JavaScript 的客户端，或者校验未完成时发起的请求，归入此类。由于 JavaScript 校验通常需要一定时间进行，客户端在完成校验前，您可以允许一定速率的请求通过，并处置未通过校验且高频发起请求的客户端。 客户端检测超时：客户端支持 JavaScript 并已经开始校验，但是未能在 60 秒内完成校验。60 秒对于正常浏览器客户端而已足够完成客户端行为校验，而来自算力较少的 IoT 代理，则有较大概率验证超时，使用该选项可以区分处置算力较低的分布式 Bot 网络请求。 Bot 客户端：客户端成功完成了 JavaScript 校验，探测模块发现客户端运行环境异常，非正常人类通过浏览器访问。

以当前场景为例，您可以配置工作量证明为校验强度为高，执行方式为延迟 100ms 执行，在客户端未启用 JS（未完成检测）超过10次/10秒后执行（长时间）等待后响应，对客户端检测超时和 Bot 客户端保持静默方式对抗。配置结果如下所示：



6. 单击**保存并发布**，即可完成配置。

自定义 Bot 规则

最近更新时间：2024-01-02 10:41:14

概述

当您在已有的 Bot 管理策略基础上，需要针对特定 Bot 行为或特征定制精细化策略时，自定义 Bot 规则可以为您提供灵活的匹配条件（例如：客户端 IP、头部信息、请求方法、静态特征识别和客户端画像分析结果等），同时可结合按权重随机选择处置动作的处置策略，帮助您创建精确的管理策略，有效管理 Bot 访问站点带来的风险。

说明：

自定义 Bot 规则支持按权重随机配置多个处置动作。例如，您可以将 25% 的请求配置为观察，25% 的请求配置为拦截，25% 的请求配置为放行，25% 的请求配置为托管挑战。这种方式可以混淆 Bot 工具对 Bot 效果的认知，同时也有助于在灰度测试阶段减少风险。

场景一：敏感 API 接口的 Bot 请求突增时，通过静默处理规避

示例场景

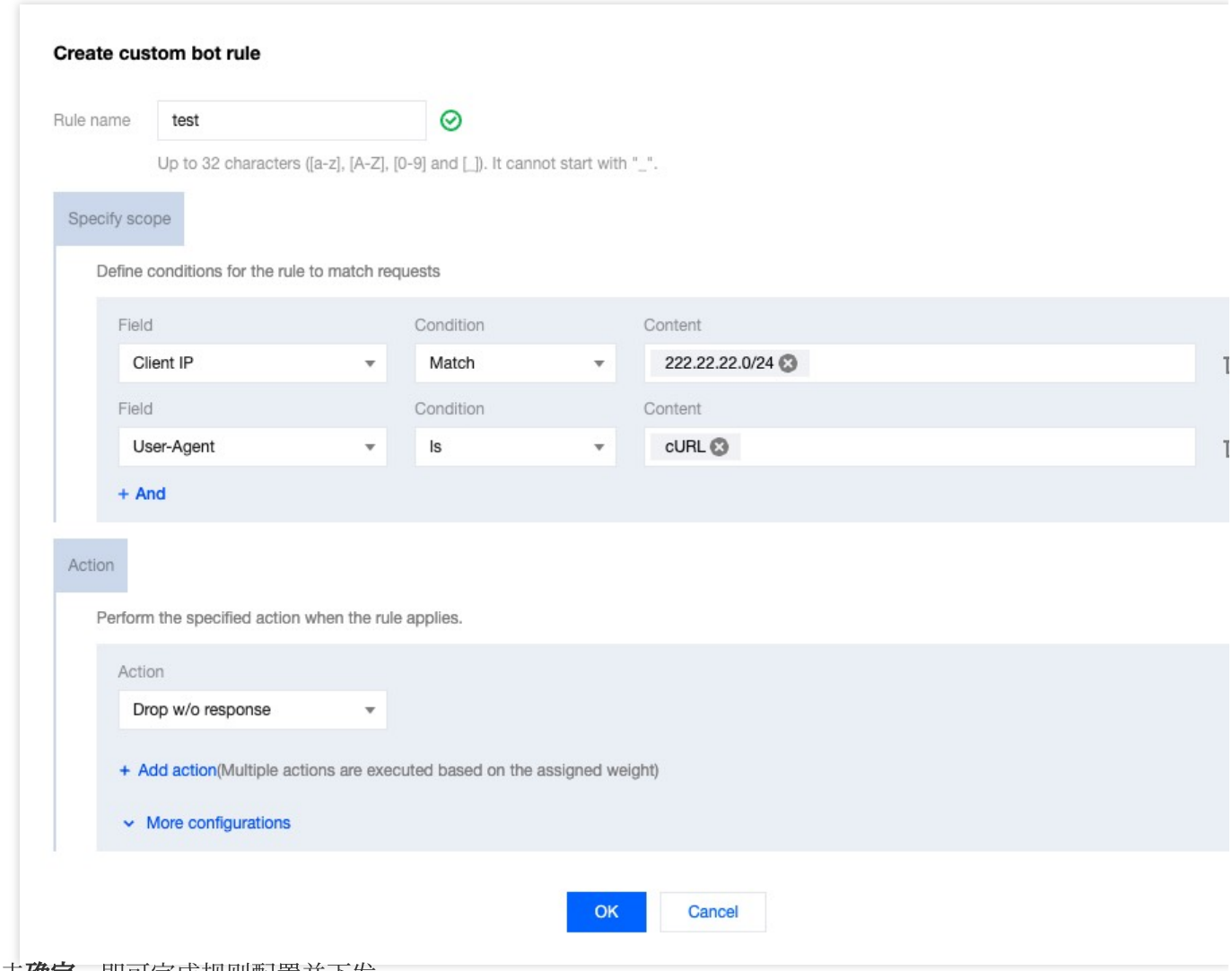
在 Web 安全分析中，发现大量突增请求访问登录接口，经过检视非正常客户端，请求主要来自 `222.22.22.0/24` 网段中多个代理客户端，大量尝试使用多种类型客户端登录账号。为了紧急规避业务风险，同时消耗恶意工具资源，可通过静默处置相关来源的请求（保持客户端 TCP 连接，但不再响应 HTTP 请求）。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页面。
3. 在自定义 Bot 规则卡片中，单击**设置**，进入配置页面。
4. 单击**添加规则**，以示例场景为例，可参照如下步骤配置：

4.1 填写规则名称后，添加匹配条件为客户端 IP 匹配 `222.22.22.0/24` 网段且 `User-Agent` 包含 `cURL`。

4.2 在执行动作中，处置方式选择为静默处理。配置后规则如下所示。



5. 单击**确定**，即可完成规则配置并下发。

场景二：对登录页面启用多种处置方式组合的 Bot 管理策略，减少账号盗用（ATO：Account-Take-Over）风险

示例场景

为了管控账号盗用风险，避免批量登录方式盗用账号，业务需针对访问登录页面进行人机校验同时尽可能保障用户体验，可针对客户端画像分析结果为 客户端画像分析（包括使用撞库等方式的账号盗用手段）的客户端进行管控处理：对一定比例登录页面访问进行人机校验，对于另一部分请求增加短时间等待，以确保工具进行批量登录尝试时，会在一定次数尝试后触发人机挑战，并且通过短时间等待避免工具进行高频尝试。

操作步骤

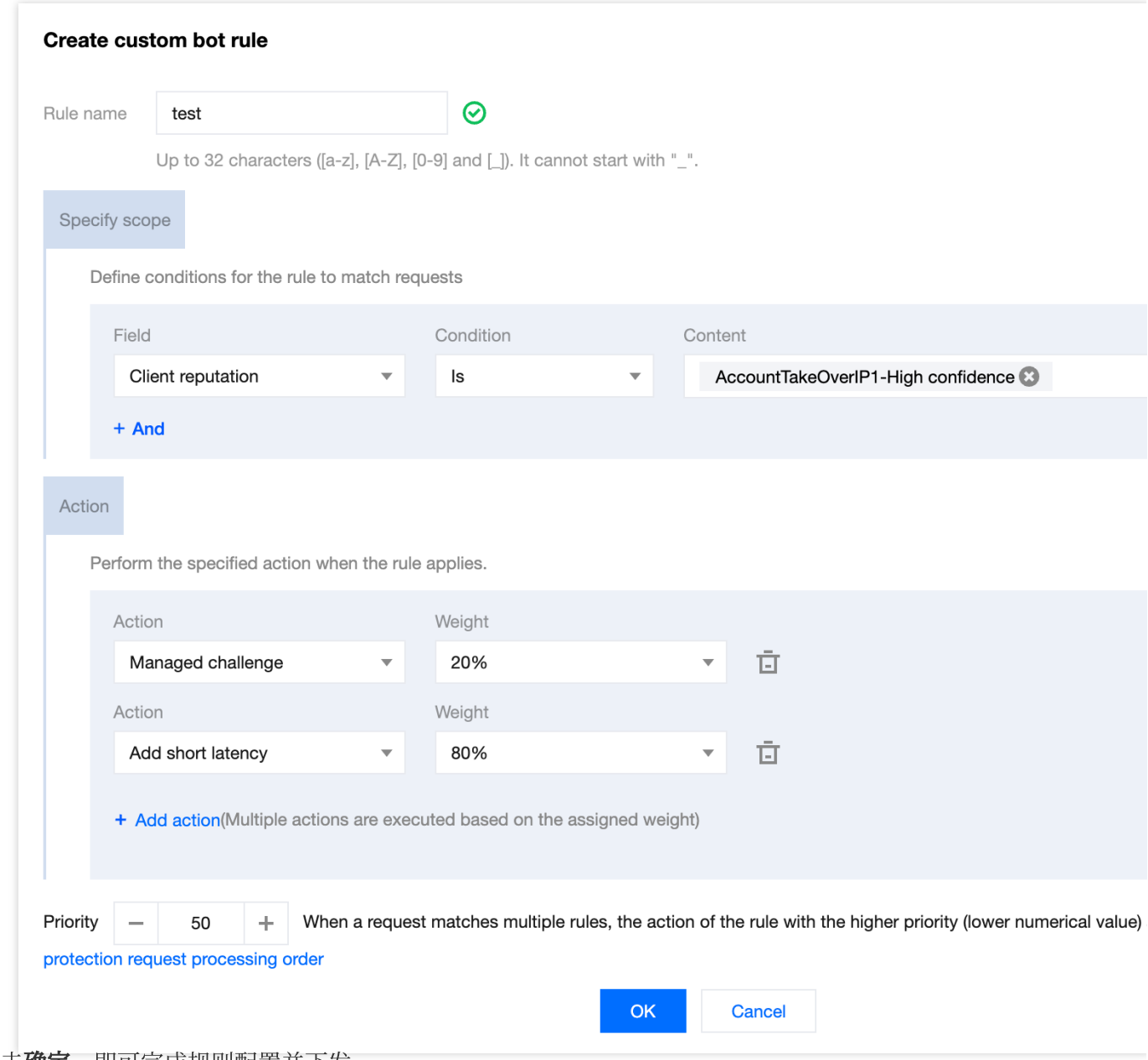
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页面。

3. 在自定义 Bot 规则卡片中，单击**设置**，进入配置页面。

4. 单击**添加规则**，以示例场景为例，可参照如下步骤配置：

4.1 填写规则名称后，添加匹配条件为**请求客户端画像**等于**账号接管攻击-较高置信度**。

4.2 在执行动作中，处置方式先选择为托管挑战，然后点击新增处置方式，添加处置方式为（短时间）等待后响应。设置托管挑战权重为20%，（短时间）等待后响应权重为80%。配置后规则如下。



5. 单击**确定**，即可完成规则配置并下发。

Bot 管理例外规则

最近更新时间：2023-10-11 10:39:27

概述

Bot 管理例外规则提供了 Bot 管理模块的访问白名单配置选项，可快速配置放行合法 Bot 访问，放行后，将跳过所有其他 Bot 规则模块，避免合法请求被其它 Bot 规则处置。

说明：

该功能仅订阅 EdgeOne 的 Bot 管理选项支持。

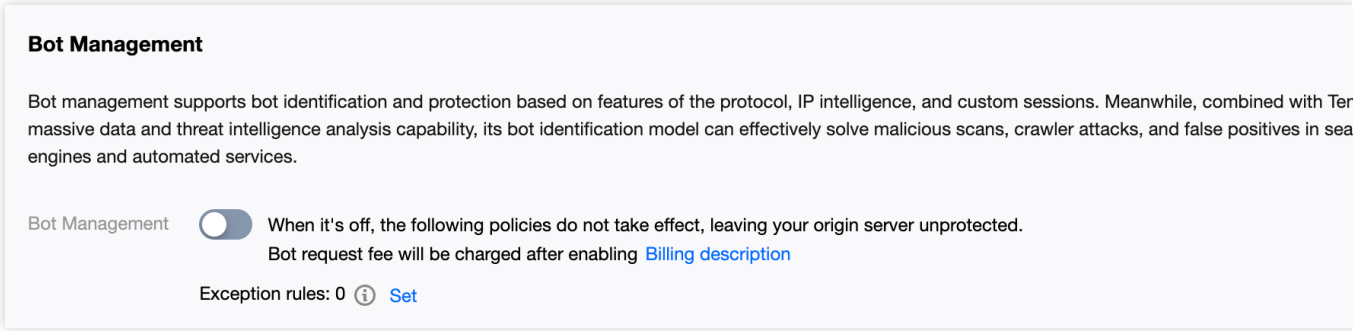
场景：放行合法的监测工具请求

示例场景

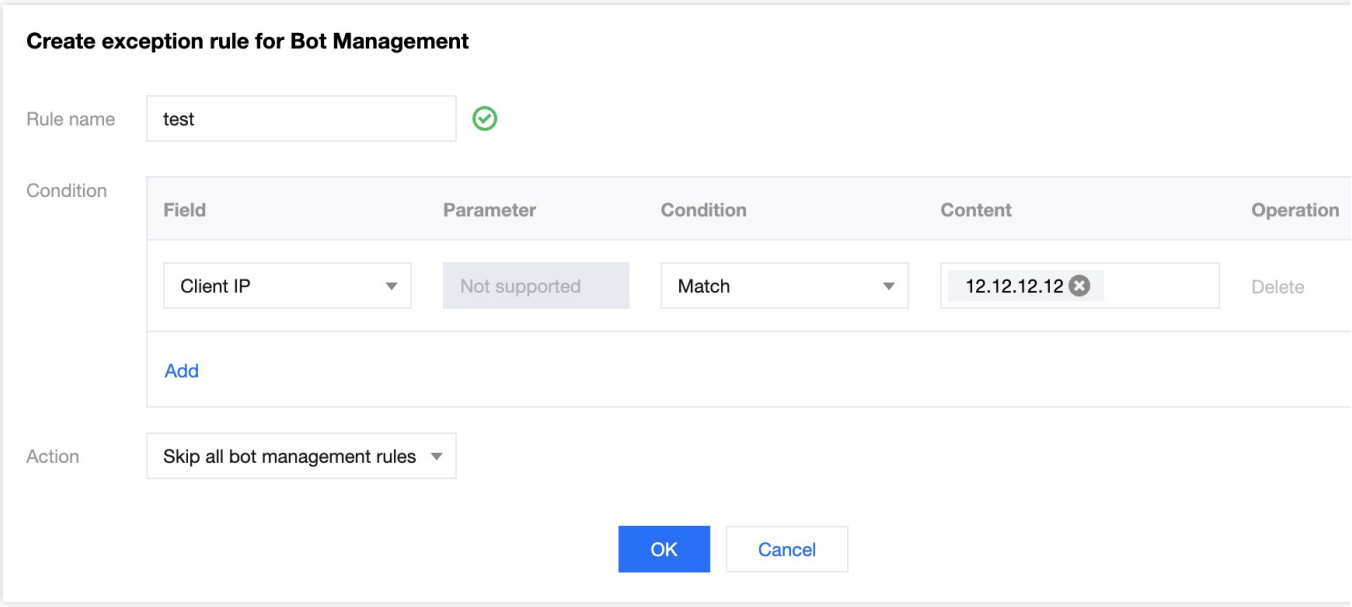
为了检测站点域名 `api.example.com` 运行情况，在客户端 IP 为 `12.12.12.12` 的设备上部署了监测工具，定期访问 API 并观测服务性能和可用性。由于监测工具不具备完整浏览器内核，主要使用 `cURL` 外部工具库进行访问，同时又具备周期性高频访问特点，为避免监测工具被误拦截，可以将其特征加入 Bot 管理例外规则。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **Bot 管理**，进入 Bot 管理详情页面。
3. 在 Bot 管理的例外规则中，单击**设置**，进去例外规则设置页面。



4. 单击**添加规则**，输入规则名称后，匹配条件选择为客户端 IP 匹配 `12.12.12.12` 的客户端，执行动作为跳过全部 Bot 管理模块规则。



5. 单击**确定**，即可下发并生效该例外规则。

相关参考
处置方式

最近更新时间：2023-09-21 09:57:31

Bot 管理模块提供多种处置方式。不同处置方式的处理规则如下：

处置方式	用途	处置方式描述	后续动作
拦截	用于阻断请求访问站点（包括缓存或非缓存内容）。	响应拦截页面和拦截状态码。	不再匹配其他策略。
放行	用于跳过当前安全模块其余规则。	当前模块中，其余规则不再匹配该请求。	继续匹配其他生效的规则。
观察	用于评估或灰度安全策略。	仅记录日志，不进行处置。	继续匹配其他规则。
JavaScript 挑战	用于识别不支持 JavaScript 的工具客户端注1，常见于 DDoS 攻击源、扫描工具等。	响应重定向（HTTP 302）页面，页面携带 JavaScript 代码验证客户端浏览器行为，仅通过校验的访客可以继续访问。	通过挑战的请求继续匹配其他规则。
托管挑战	用于 Bot 对抗， 首先进行 JavaScript 挑战校验，对通过校验的请求再进行 CAPTCHA 人机校验。	首先进行 JavaScript 挑战；对通过校验的客户端，响应重定向（HTTP 302）页面，携带验证码校验，用户通过交互操作完成校验。两次校验都通过的访客才可以继续访问。	通过挑战的请求继续匹配其他规则。
静默	属于强度较大的 Bot 对抗机制，通过消耗 Bot 网络连接数来限制 Bot 并发能力	保持 TCP 连接，但不再响应任何 HTTP 数据。	不再匹配其他策略。
（短时间）等待后响应	主要用于限制Bot 并发能力，具备混淆特点注2。	随机等待1-5秒后响应。	不再匹配其他策略。
（长时间）等待后响应	主要用于限制Bot 并发能力，具备混淆特点注2。	随机等待8-10秒后响应。	不再匹配其他策略。

说明：

注1：

支持 JavaScript 的浏览器客户端可以正常通过 JavaScript 挑战校验，而不支持 JavaScript 的客户端（如：cURL 等）则无法通过校验。

注2：
通常来说，当察觉到 Bot 被管控策略限制时，Bot 的运营者可能会调整 Bot 特性绕过 Bot 策略，从而增加 Bot 识别难度。因此，长期运营的 Bot 对抗机制通常具备混淆特点，即：Bot 运营方较难直观判断，其 Bot 是否受到 Bot 管理策略限制。具备混淆特点的对抗机制，可以在不增加 Bot 识别难度的前提下，减少 Bot 运营者的成本和难度。

支持多种处置方式随机执行

多种处置方式随机执行，可以帮助您的 Bot 管理策略达到更高的混淆强度，使 Bot 管理策略更难被 Bot 运营者察觉。自定义 Bot 规则支持使用多个方式组合处置请求，您可以配置多个处置方式和对应的权重。当规则匹配请求时，将根据权重配置，随机选取其中一种处置方式对请求进行处理。

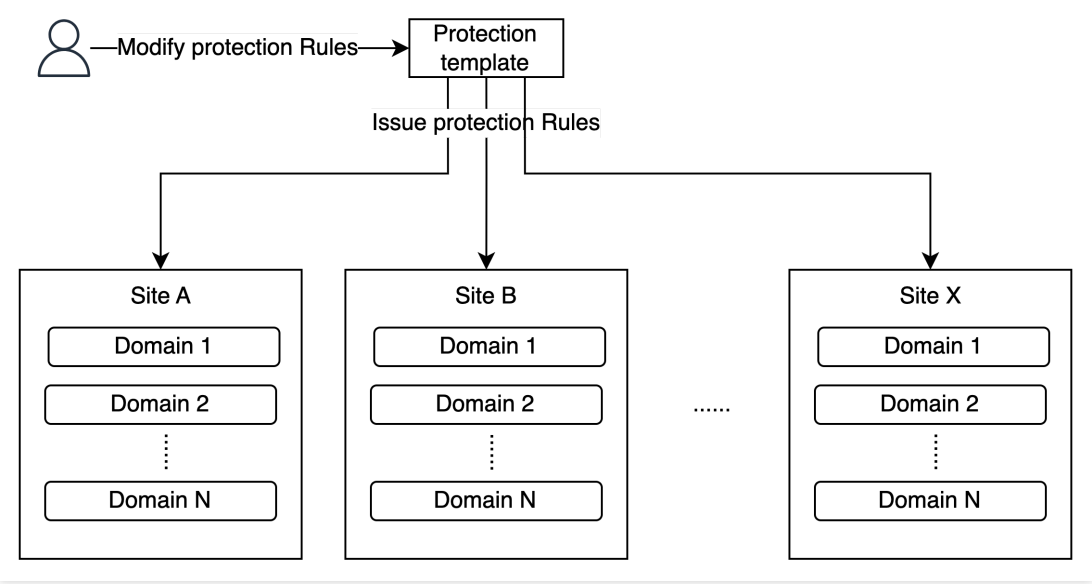
说明：
该能力仅限于 Bot 自定义规则内配置。

策略模板

最近更新时间：2023-10-11 10:39:53

概述

当您有大量域名需要同时接入 EdgeOne Web 防护时，如果域名所需使用的防护策略完全相同，当需要修改 Web 防护策略时，逐个域名修改将会带来大量的维护工作量。
EdgeOne 的安全防护内为您提供了策略模板功能，支持您将安全策略保存为模板，并将模板策略应用到指定的域名中。您可以直接在模板管理内修改对应的安全防护策略，即可在所有已应用该模板的域名上生效，极大程度上减少您的运维成本。
说明：
1. 策略模板仅支持 Web 防护策略、Bot 管理策略以及自定义页面。
2. 使用策略模板将覆盖当前域名内防护策略，当前域名内防护策略将丢失。
3. 使用策略模板后，将清空当前在智能 CC 攻击防护内临时拦截的客户端列表，应用后新增的临时拦截客户端列表将不会影响策略模板内其它域名。



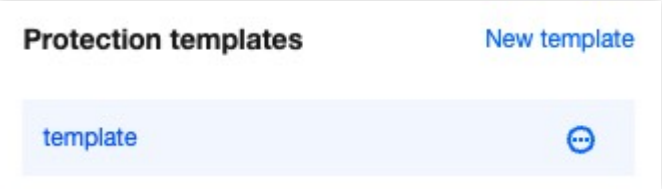
操作步骤

绑定策略模板

场景一：新建策略模板并应用到指定域名、站点内

例如：当前您需要新建一个策略模板 `template`，并将该策略模板应用到站点 `example.com` 内的所有域名。您可以参照如下步骤操作：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > 策略模板**，进入策略模板管理界面。
3. 在左侧防护策略模板中，点击**新增模板**，输入模板名称后，单击回车键确定即可新建一个模板。



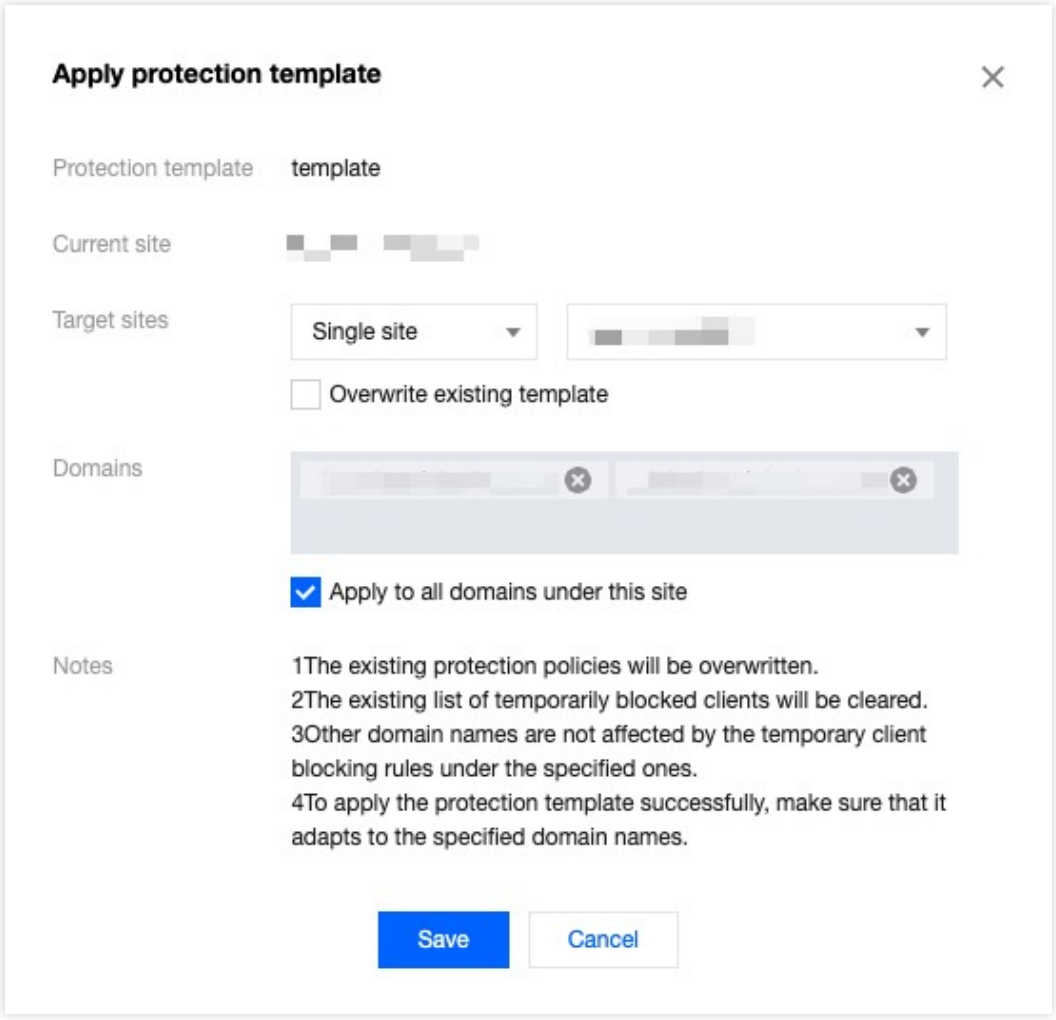
4. 新建完成后，单击步骤3新建的模板名称，即可进入该模板的编辑页面，您可以在改界面内完成相关规则的配置与修改，配置可参考：Web 防护、Bot管理。
5. 将配置好的策略模板应用到站点，支持以下三种应用方式：

应用到当前站点：将当前策略模板应用到当前站点下域名或者全部域名内；

应用到指定站点：将当前策略模板应用到其他指定的站点下域名或者全部域名内；

批量应用到站点：将当前策略模板应用到多个指定的站点下域名或者全部域名内，在批量应用到站点时，支持使用通配符表达式匹配域名。例如：

以当前场景为例，需要将该策略模板应用到 `example.com` 内的所有域名内，您可以点击模板内 **应用到域名**，选择应用方式为应用到指定站点，并选择站点为 `example.com`，勾选应用到全部域名，配置如下：



6. 点击**保存**，即可完成策略模板应用。

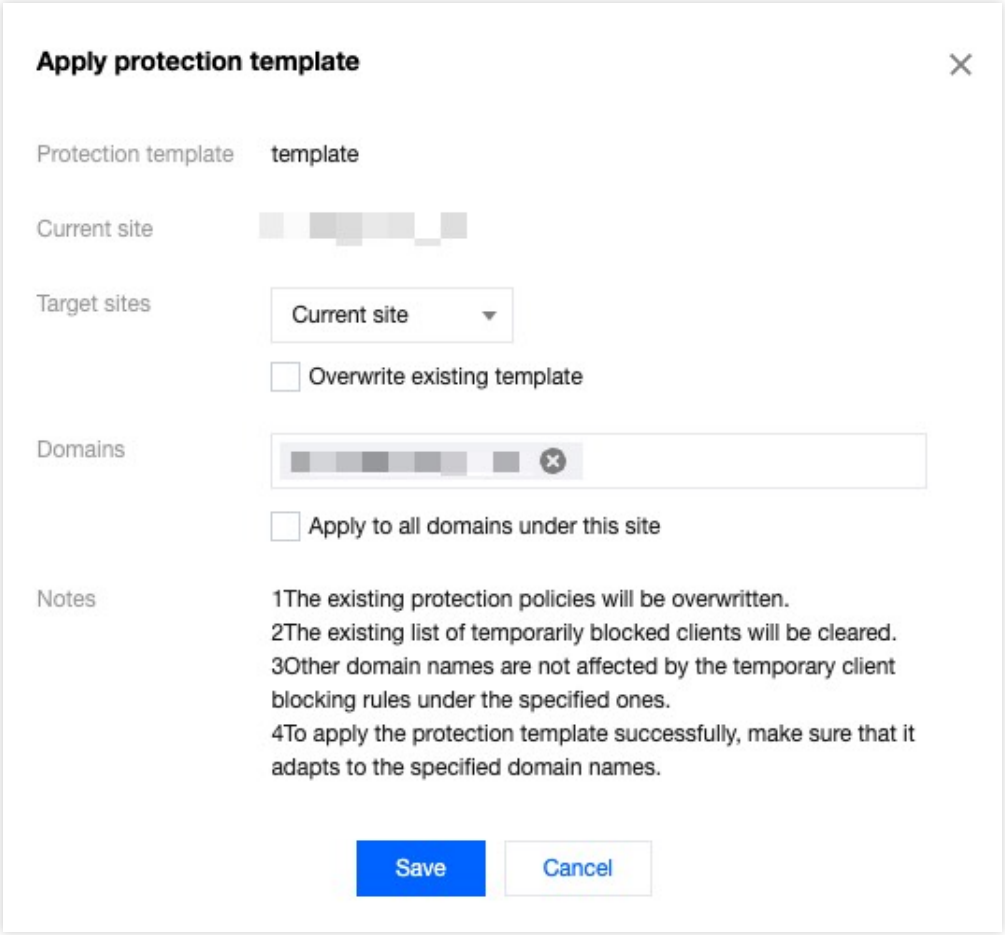
场景二：将已有模板应用到新增域名、站点内

例如：您当前在站点 `example.com` 下已配置有一个 Web 安全防护策略模板 `template`，此时在当前站点下又新增了一个域名为 `www.example.com`，该域名的 Web 防护策略与模板 `template` 完全相同，您可以通过使用模板策略，快速将当前的策略模板应用到该域名。您可以参照如下步骤操作：

方式一：在策略模板内操作

方式二：在防护配置内操作

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > 策略模板**，进入策略模板管理界面。
3. 选择对应的防护模板，例如 `template`。
4. 点击应用到域名，以当前场景为例，可选择应用方式为应用到当前站点，选择域名列表内域名为 `www.example.com`。



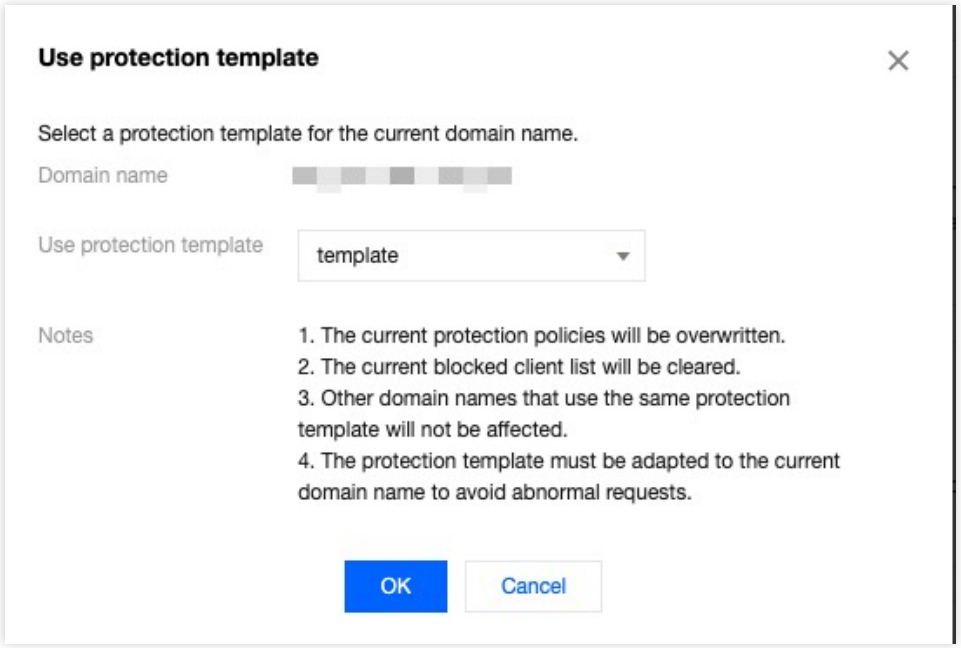
5. 点击**保存**，即可完成策略模板应用。

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，选择需要配置的防护模块，以当前场景为例，可单击**安全防护 > Web 防护**，进入 Web 防护策略配置页面。

3. 在防护域名列表内，选择需配置的域名，例如：`www.example.com`。

4. 在右上角点击使用模板策略，选择需要应用的模板策略，例如：`template`。



5. 点击确定，即可完成模板策略应用。

解绑策略模板

例如：您当前在站点 `example.com` 下域名 `www.example.com` 已绑定一个 Web 防护的策略模板 `template`，如果该域名有与其他域名不一样的个性化防护策略配置，需要在保留当前安全配置的情况下，新增自定义规则，需要解绑对应的策略模板才可以配置。您可以参照如下步骤操作：

1. 登录边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。

2. 在站点详情页面，选择需要配置的防护模块，以当前场景为例，可单击**安全防护 > Web 防护**，进入 Web 防护策略配置页面。

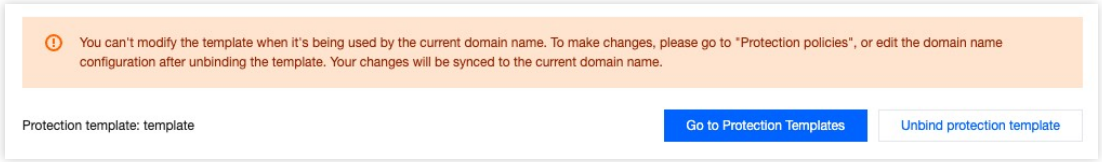
3. 在左侧防护域名列表内选择需要解绑策略模板的域名，例如：www.example.com。

4. 绑定策略模板的域名只能查看配置，不可修改，点击解除策略模板，支持两种解绑操作：

保留当前安全策略：解绑后保留当前策略模板所配置的安全防护策略内容。

使用空包安全策略：清除所有安全策略，重新配置。

以当前场景为例，可选择保留当前安全策略信息。



5. 点击**确定**，即可解绑。

IP 和网段分组

最近更新时间：2023-10-13 14:20:14

Function Description

IP/网段分组包含了 IP 或 CIDR 网段列表，您可以在 DDoS 防护、Web 防护和 Bot 管理规则中，或在跨站点的同类规则中引用该 IP/网段分组，以简化配置维护操作。

说明：

1. IP /网段分组支持跨站点使用。您可以在新建 IP/网段分组后，在其它站点内直接引用该 IP/网段分组，来保证不同站点的策略一致。
2. 同一个站点下的黑白名单最多添加 20000 个 IP/网段分组，其中 IP 分组最多添加16个。

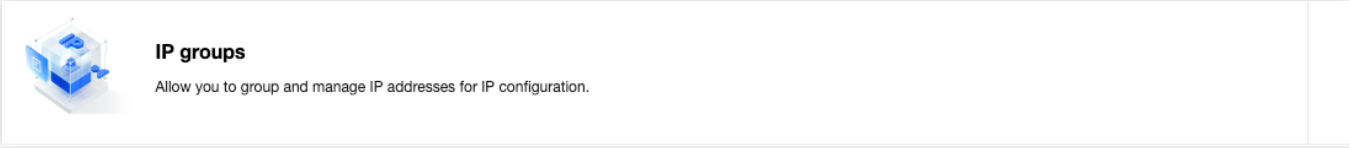
场景：分组管理具有业务威胁的 IP 信息

示例场景

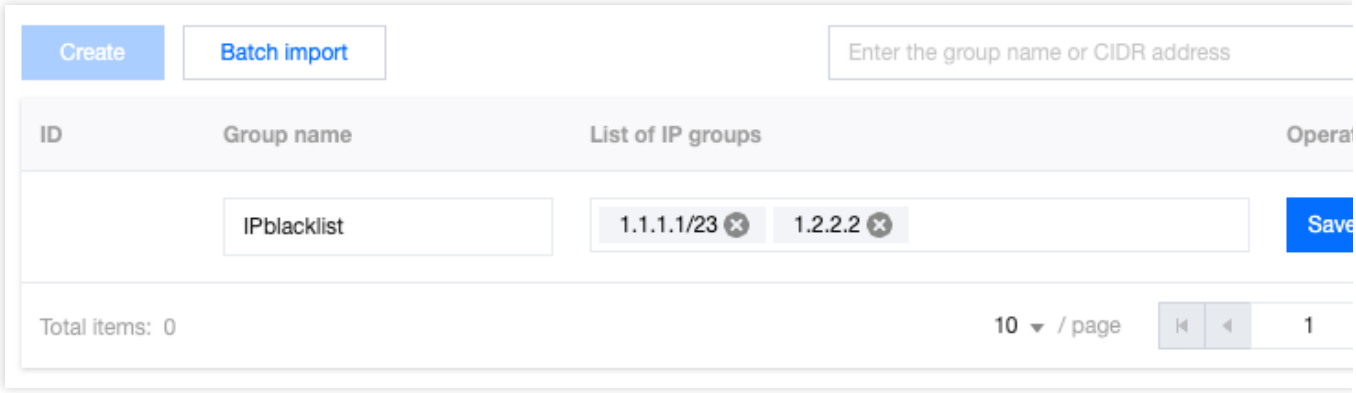
某大型游戏客户已接入站点 `example.com` 、 `site.com` 。目前，通过安全情报库以及自身业务安全，已识别出一批具有业务威胁的黑名单 IP。这些 IP 地址将会动态变化，因此需要实时更新，并应用到所有站点域名中，即时对这些 IP 进行封禁。

操作步骤

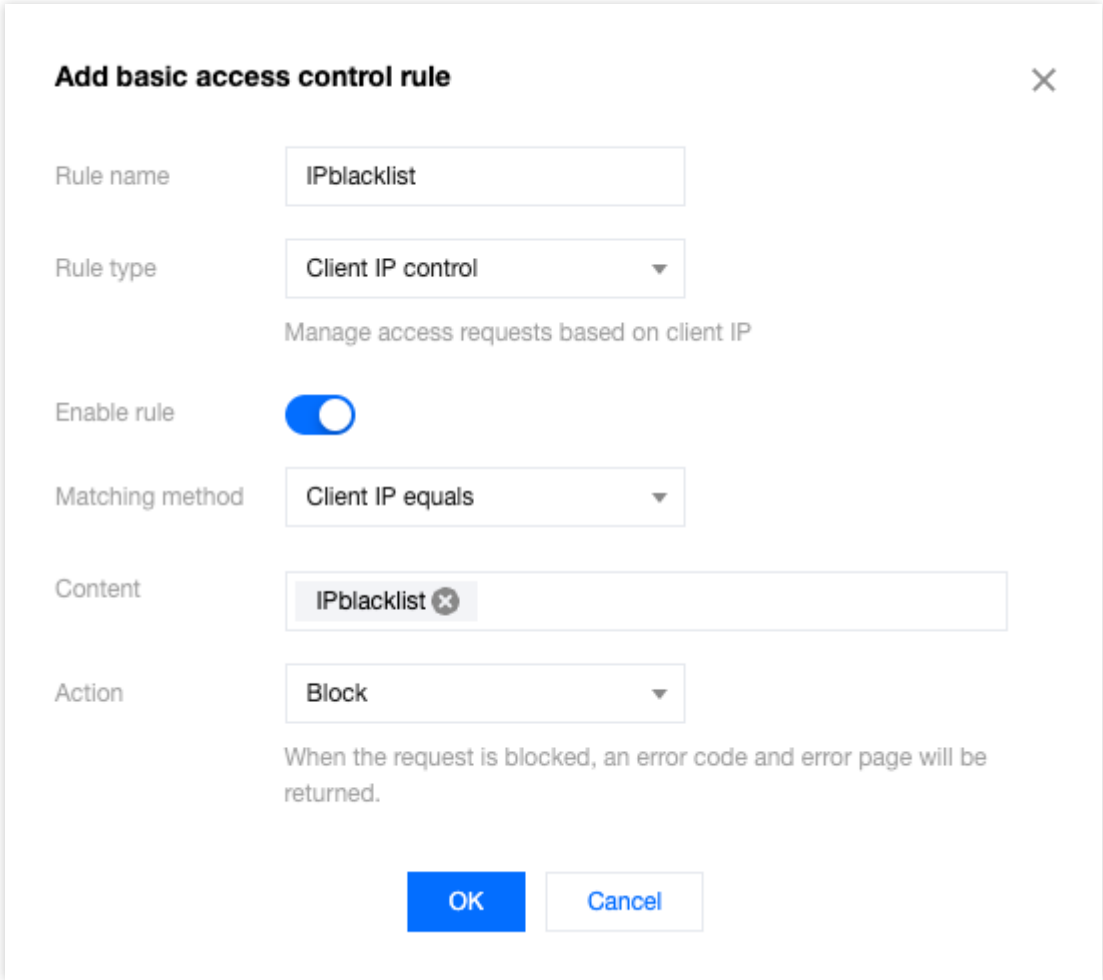
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **配置选项**，进入配置选项详情页面。
3. 在 IP 和网段分组卡片中，单击**设置**。



4. 单击**新建**，创建一个新分组，输入分组名称以及该分组包含的 IP 地址或 IP 地址段，例如： `1.1.1.1/23;1.2.2.2` 。多个地址以回车间隔。

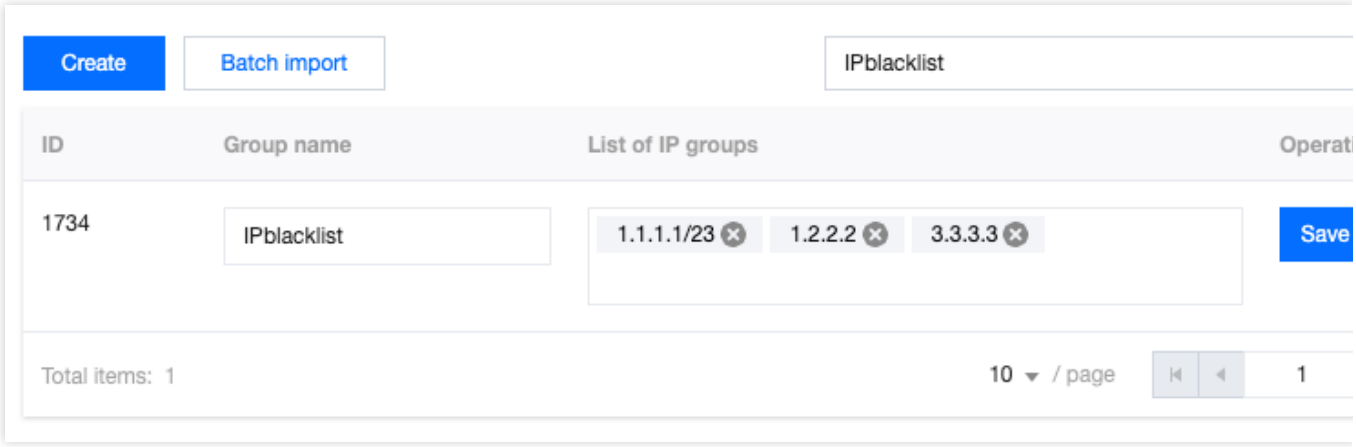


5. 单击**保存**，完成 IP 分组创建。分组创建完成后，以该场景为例，需禁用该分组内的所有 IP 访问，可分别在 `example.com` 和 `site.com` 的 **Web 防护 > 自定义规则页面**，添加基础访问管控规则。在添加规则时，选择**客户端 IP 等于**该**分组名称**时进行**拦截**，即可拦截该分组内的所有 IP 访问，并根据分组内包含 IP 进行动态更新。详细配置步骤可参考 自定义规则。



6. （可选）配置规则后，如果您识别到新的风险 IP，需要添加到该分组内并应用到所有站点，可参考步骤1~3重新进入创建该模板的站点后，单击**编辑**，输入需要新增的 IP 地址后，再单击**保存**，即可将新增的 IP 应用到所有引用该分

组的防护策略中。


Create
Batch import
IPblacklist
ID
Group name
List of IP groups
Operat
1734
IPblacklist
1.1.1.1/23
1.2.2.2
3.3.3.3
Save
Total items: 1
10 / page
1

源站防护

最近更新时间：2024-01-02 10:43:32

功能简介

获取四层代理和站点加速服务最新的回源 IP 信息，更新业务源站防火墙规则，仅允许经过固定 IP(s) 的流量回源至源站，实现源站防护。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **源站防护**。
3. 在源站防护页面，单击源站防护状态的**启用**，选择站点加速/四层代理服务，单击**确认启用**为所选资源启用源站防护。

说明

选择站点加速/四层代理服务：请绑定需要使用源站防护服务的资源。

4. 成功启用后：

您可查看到这些资源目前使用的回源 IP 列表，请将其更新至您的源站防火墙规则中。

后续如果回源 IP 列表有更新，我们将发出消息通知，直到您确认并反馈后，再为绑定的资源正式使用更新后的回源 IP 列表。

注意事项

为了您的业务能正常运行，当收到 IP 列表更新的消息，请您及时前往控制台确认并更新。

说明

如未及时更新至最新的回源 IP，则可能影响正常业务，如延时不能达到最优，高并发时可能不稳定等。

告警通知推送

最近更新时间：2023-12-18 15:03:44

功能简介

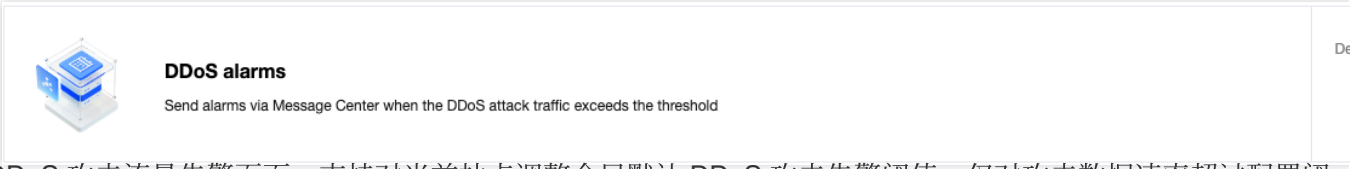
当检测到安全监控事件时，边缘安全加速平台 EO 将通过消息中心推送通知，您可在消息中心配置订阅范围：
DDoS 攻击流量告警：针对企业版 DDoS 防护（站点接入和四层代理）的 DDoS 攻击，当攻击数据速率超过配置阈值时，推送 DDoS 攻击通知。
Web 安全监控规则：针对命中 Web 防护规则和 Bot 管理规则的监控，当匹配条件的请求超过配置阈值，并符合告警条件时，推送 Web 安全监控规则告警通知。

DDoS 攻击流量告警

边缘安全加速平台 EO 持续检测外部访问流量，并识别其中的 DDoS 攻击。当检测到攻击时，无需人工介入，将自动进行流量清洗，过滤恶意攻击流量。
仅支持针对企业版 DDoS 防护（站点接入和四层代理）的 DDoS 攻击推送告警通知，其他业务暂不支持 DDoS 攻击流量告警功能。

DDos攻击流量告警设置

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护 > 告警通知推送**。



3. 在 DDoS 攻击流量告警页面，支持对当前站点调整全局默认 DDoS 攻击告警阈值，仅对攻击数据速率超过配置阈值的攻击事件推送消息中心通知。单击默认告警阈值的**编辑**，修改默认告警阈值，单击**保存**。

说明：
DDoS 攻击流量告警页面展示了全部支持 DDoS 攻击流量告警的业务，和对应的 DDoS 攻击告警阈值。对于未启用自定义阈值的业务，可通过调整**默认告警阈值**，调整对应 DDoS 攻击告警阈值。

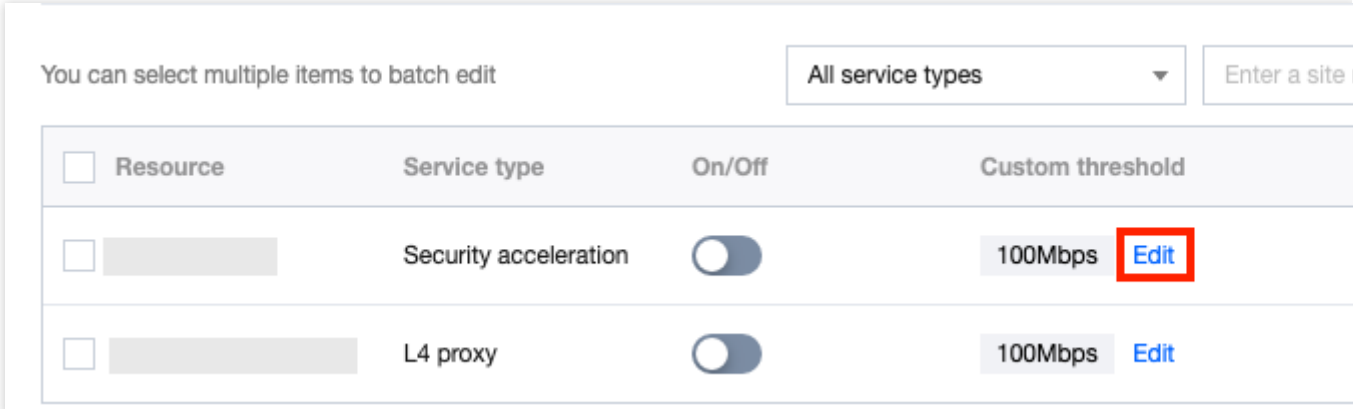
4. 在 DDoS 攻击流量告警页面，支持单独配置安全加速或四层代理业务项目的告警阈值。

说明：

建议根据被攻击频率和历史调整，默认100Mbps，最小可调节至10Mbps。

4.1 设置单个告警阈值

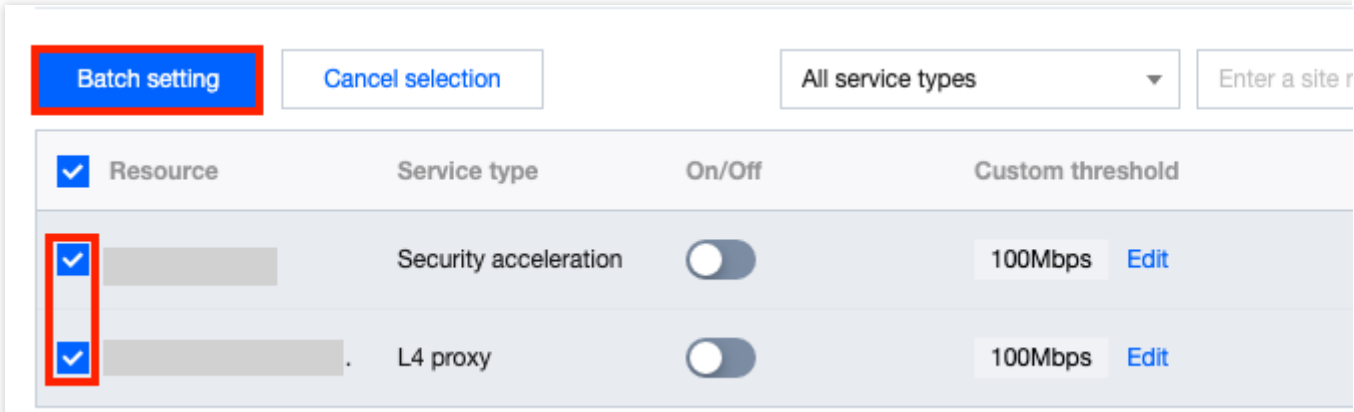
4.1.1 选择所需业务，单击对应告警阈值列的**编辑**，可调整该业务推送 DDoS 攻击通知的攻击规模范围（最小攻击速率）。



4.1.2 修改告警阈值，单击**保存**，自定义阈值自动开启。

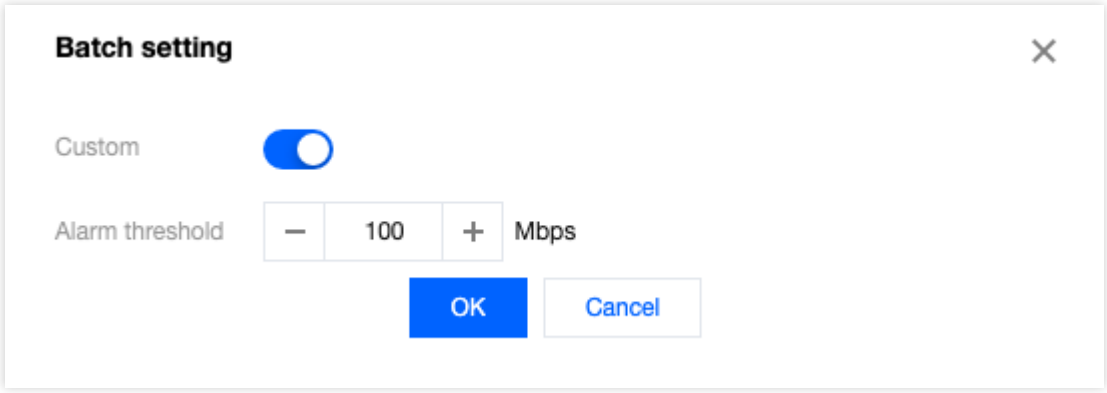
4.2 批量设置告警阈值

4.2.1 选择一个或多个业务，单击**批量设置**。



4.2.2 单击开启自定义开关

，调整预警值，单击**确定**。



Web 安全监控规则

边缘安全加速平台 EO 处理请求时，根据命中 **Web 安全**和 **Bot 管理**规则的情况（包括**策略模板**中配置的安全规则），命中规则的请求将被记录到 Web 安全日志。

说明：

命中处置方式为放行的规则，不会记录日志。

统计请求数计数时，每个域名的请求独立计数，超过告警条件阈值时告警。

Web 安全监控规则会根据监控规则的匹配条件，统计单个域名下命中规则的请求总数。当一段时间内请求总数超过阈值时，支持按告警选项推送告警。

Web 安全监控规则配置

Web 安全监控规则支持灵活的监控统计范围和告警配置，可以基于安全运维需要，配置多条监控规则，以覆盖日常监控和告警场景。

Web 安全监控规则支持下列选项：

规则名称：必填，需满足以下要求：

为英文、数字和下划线组合。

长度小于32个字符。

不能以下划线开头。

监控域名：必选

全部域名：包含本站点下全部域名，也包括后续添加的域名。

指定域名：可选择本站点下域名。

监控范围：必选，支持按处置方式或者按规则选择统计请求范围。

全部处置请求：所有命中安全模块规则，并被处置的请求（不包括放行），计入监控规则的统计计数。

仅统计**指定处置方式的请求**：命中 Web 防护或 Bot 管理规则，并最终按选择的方式处置的请求，计入监控规则的统计计数。

仅统计**命中制定规则的请求**：命中指定 Web 防护或 Bot 管理规则的请求。

告警配置：必须选择告警条件配置，可选告警频率配置。

静态告警条件：基于一个固定请求数阈值，超过阈值即满足告警推送条件，将按照该规则告警频率进行推送告警通知。

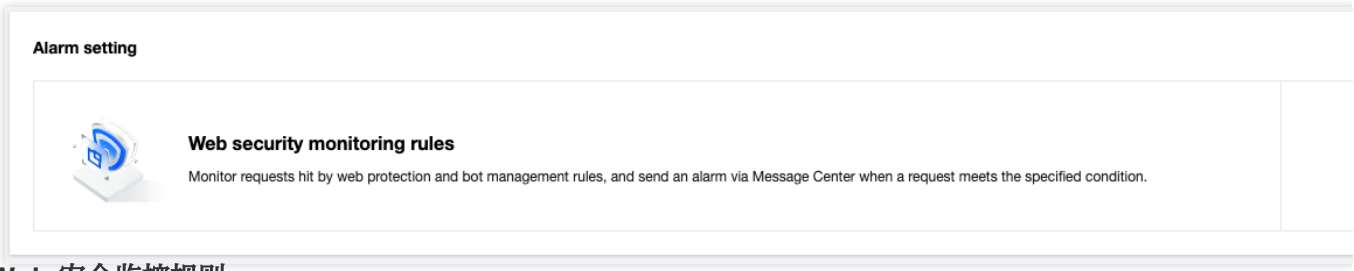
告警频率：当本规则满足告警条件时，按配置的告警频率推送告警通知。

说明：

未选择告警频率时，默认每条规则每5分钟推送最多1条告警通知。

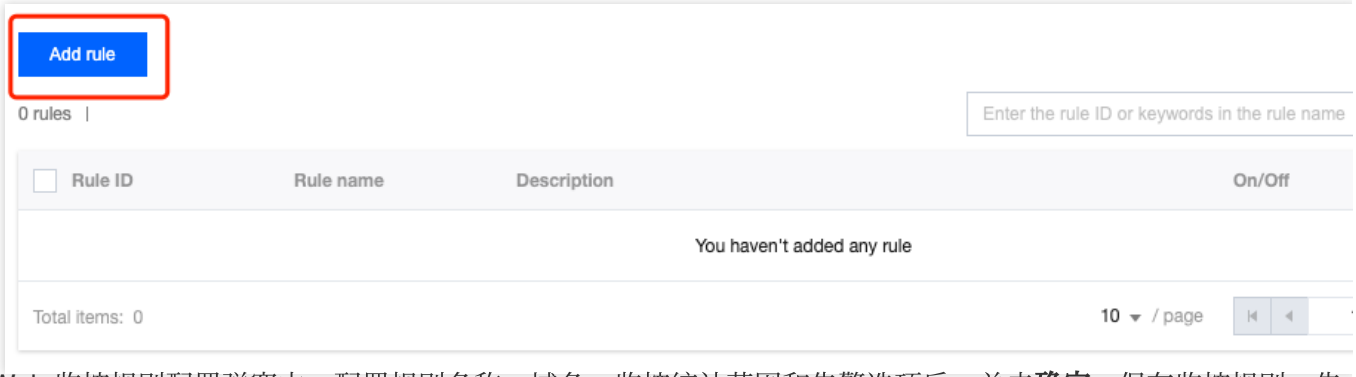
Web 安全监控规则管理

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **告警通知推送**。



添加 Web 安全监控规则

1. 在 Web 安全监控规则配置页中，单击**添加规则**新增监控规则。



2. 在 Web 监控规则配置弹窗中，配置规则名称、域名、监控统计范围和告警选项后，单击**确定**，保存监控规则，告警条件即时生效。

编辑 Web 安全监控规则

1. 在 Web 安全监控规则配置页中，找到需要编辑的 Web 安全监控规则，单击操作列中对应该规则的**编辑**。
2. 在 Web 监控规则配置弹窗中，修改规则名称、域名、监控统计范围和告警选项，单击**确定**，保存监控规则，告警条件即时生效。

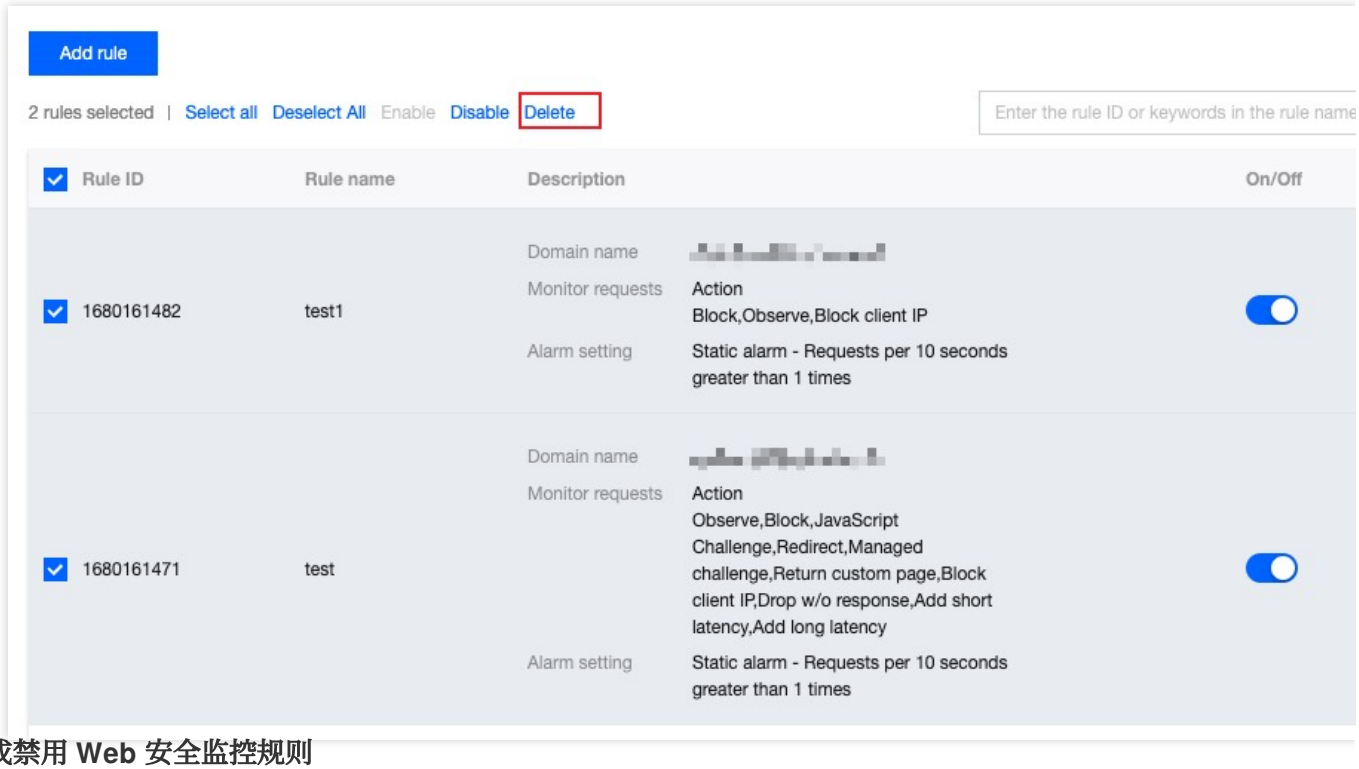
删除 Web 安全监控规则

删除单个 Web 安全监控规则

在 Web 安全监控规则配置页中，找到需要删除的 Web 安全监控规则，单击操作列中对应该规则的**删除**。

批量删除 Web 安全监控规则

在 Web 安全监控规则配置页中，选择一个或多个 Web 安全监控规则，单击**删除已选**，将同时删除全部已选中规则。

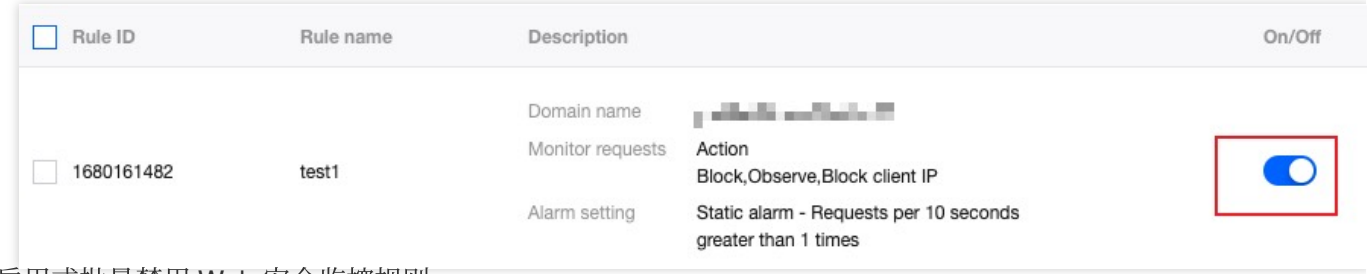


启用或禁用 Web 安全监控规则

启用或禁用单个 Web 安全监控规则

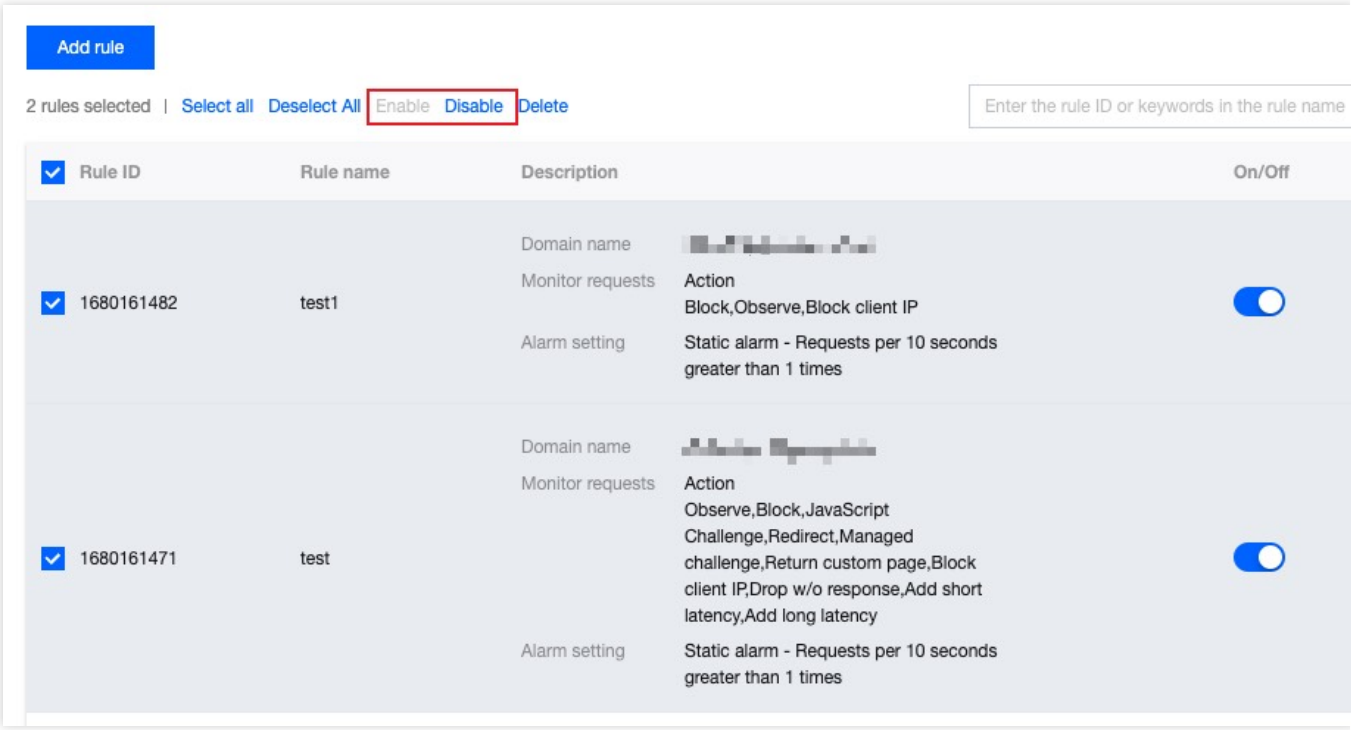
在 Web 安全监控规则配置页中，找到需要启用或禁用的 Web 安全监控规则，单击**告警开关**列中对应该规则的

。



批量启用或批量禁用 Web 安全监控规则

选择一个或多个 Web 安全监控规则，单击**启用已选**或**禁用已选**，将同时启用或禁用全部已选中规则。


Add rule
2 rules selected | Select all Deselect All Enable Disable Delete
Enter the rule ID or keywords in the rule name
Rule ID
Rule name
Description
On/Off
1680161482
test1
Domain name
Monitor requests
Action
Block,Observe,Block client IP
Alarm setting
Static alarm - Requests per 10 seconds greater than 1 times
1680161471
test
Domain name
Monitor requests
Action
Observe,Block,JavaScript Challenge,Redirect,Managed challenge,Return custom page,Block client IP,Drop w/o response,Add short latency,Add long latency
Alarm setting
Static alarm - Requests per 10 seconds greater than 1 times