Web 应用防火墙

最佳实践

产品文档

腾讯云

文档目录

最佳实践
WAF 等保测评解读

最近更新时间：2023-12-29 14:52:25

腾讯云 Web 应用防火墙（Web Application Firewall，WAF）符合等级保护2.0标准体系主要标准。根据《网络安全等级保护基本要求》（GB/T 22239-2019 ），腾讯云 Web 应用防火墙满足第三级安全要求。

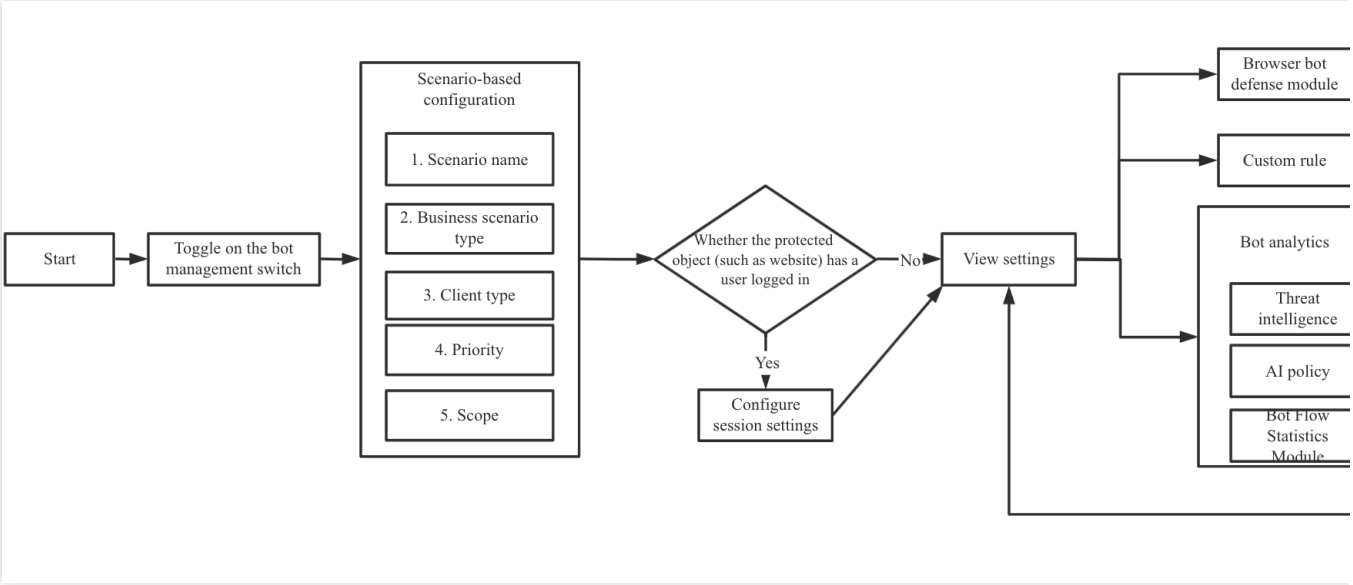
序号	等保标准章节	等保标准序号	等保标准内容	对应功能描述
1	访问控制	8.1.3.2 e）	应对进出网络的数据流实现基于应用协议和应用内容的访问控制	配置应用层的访问控制策略，对进出网络的数据流实现基于应用协议和应用内容的访问控制
2	入侵防范	8.1.3.3 a）	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为	边界区域部署 WAF，能对各种攻击和扫描行为进行检测和报警
3	入侵防范	8.1.3.3 c）	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析	WAF 支持对 Web 流量进行实时检测和阻断，支持 AI+ 规则双引擎防护，可阻断 0day 攻击和其他新型未知攻击
4	入侵防范	8.1.3.3 d）	当检测到攻击行为时，记录攻击源 IP，攻击类型、攻击目的、攻击事件，在发生严重入侵事件时应提供报警	WAF 支持 HTTP 和 HTTPS 流量攻击检测和防御，记录攻击类型、攻击 URL、攻击内容、攻击源 IP、命中规则名称和 ID、风险等级、攻击时间、目的 host、执行动作等信息
5	恶意代码防范	8.1.3.4 a）	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新	WAF 基础安全和规则引擎模块可以实现该功能
6	安全审计	8.1.3.5 a）	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计	在边界处对入侵事件进行审计
7	安全审计	8.1.3.5 c）	应对审计纪录进行保护，定期备份，避免受到为未预期的删除、修改或覆盖等	日志存储至少6个月，租户不能删除、篡改

BOT管理相关
BOT 场景化最佳实践

最近更新时间：2023-12-29 14:52:44

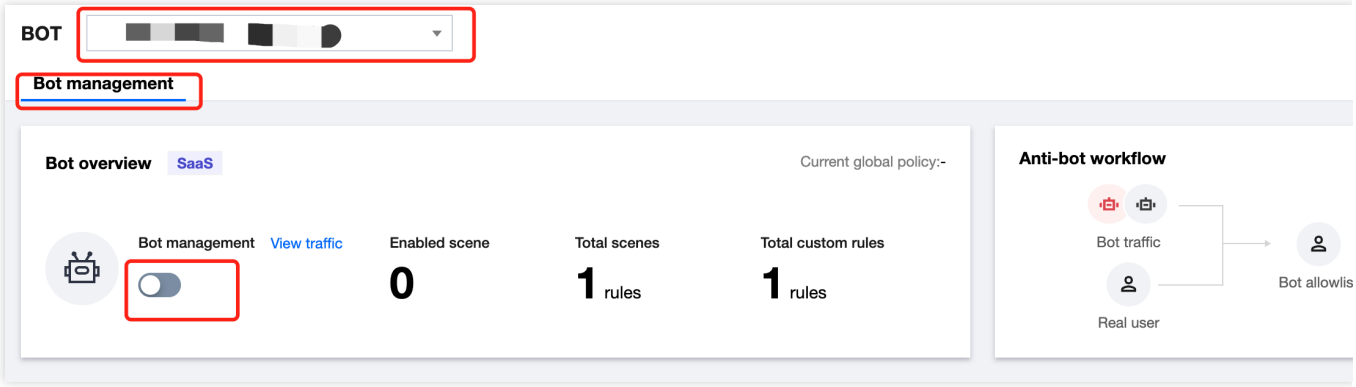
功能介绍

通过 BOT 与业务安全，用户可以在 BOT 管理中开启并配置对应模块内容，并结合 BOT 流量分析与访问日志进行观察和分析。根据流量分析提供的会话状态信息进行精细化策略设置，保护网站核心接口和业务免受 BOT 侵害。
BOT 管理设置支持配置 BOT 场景类型、客户端风险识别（前端对抗）、威胁情报、AI 评估、智能统计、动作分数、自定义规则、Token 配置、合法爬虫模块，通过配置这些模块，实现对 BOT 的精细化管理。BOT 最佳实践流程图如下所示：



前提条件

BOT 流量管理需要购买 WAF 对应实例的扩展包。
已在 BOT 与业务安全页面，选择需要防护的域名，并开启 BOT 流量开关。



BOT 场景化配置

该功能依托腾讯多年 BOT 治理的专家经验，针对 BOT 中常见的秒杀、爬价格/爬内容和登录等场景，从客户端风险识别（前端对抗）、威胁情报、AI 策略、智能分析、动作得分、会话管理、合法爬虫和自定义规则等维度基于专家经验进行设置，解决客户配置难的问题，简单易用，轻松上手。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。
3. 在 BOT 管理页面，单击**新建场景**。
4. 在新建场景弹窗中，配置相关参数，单击**立即创建**。

注意：

选中秒杀、登录和爬文案/爬内容 中的任意一个场景与自定义场景互斥。

参数说明：

场景名称：描述场景的名称，不可超过50个字符

业务场景类型：支持多选，可选择秒杀、登录、爬文案/爬内容和自定义场景。

客户端类型：访问防护目标的客户端类型。

优先级：该场景的执行优先级，输入范围为1-100的整数，数字越小，优先级越高；

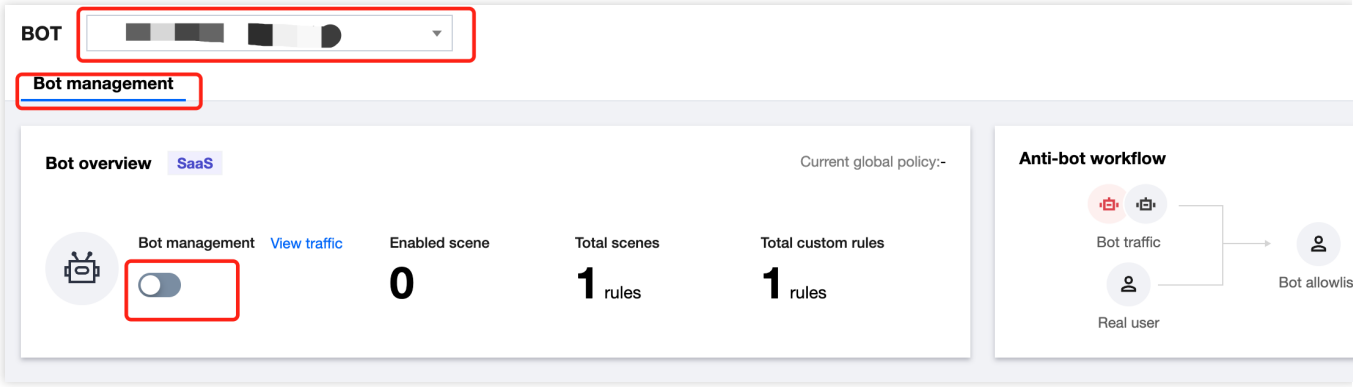
生效范围：该场景在该域名下的生效范围，支持全部范围和自定义范围

5. 场景化管理列表中，将出现创建完成的场景卡片数据，即可进一步对其进行配置。

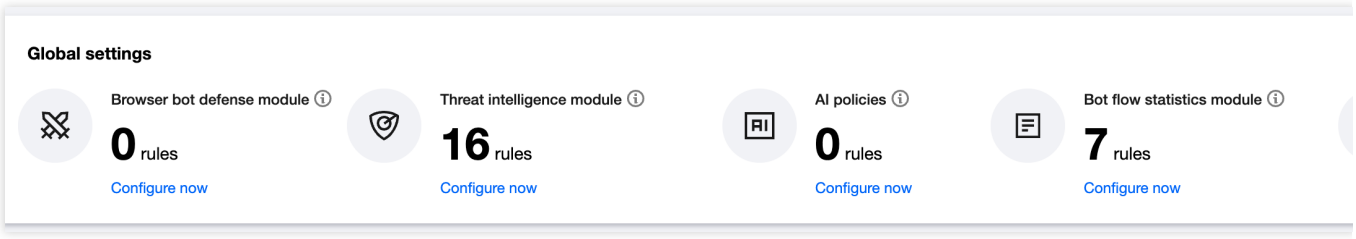
会话管理

用户可通过配置该功能，配置会话 Token 所在的位置，实现在同一 IP 下区分识别不同用户的访问行为，实现不影响其他用户的情况下，精准处置存在异常访问行为的用户。

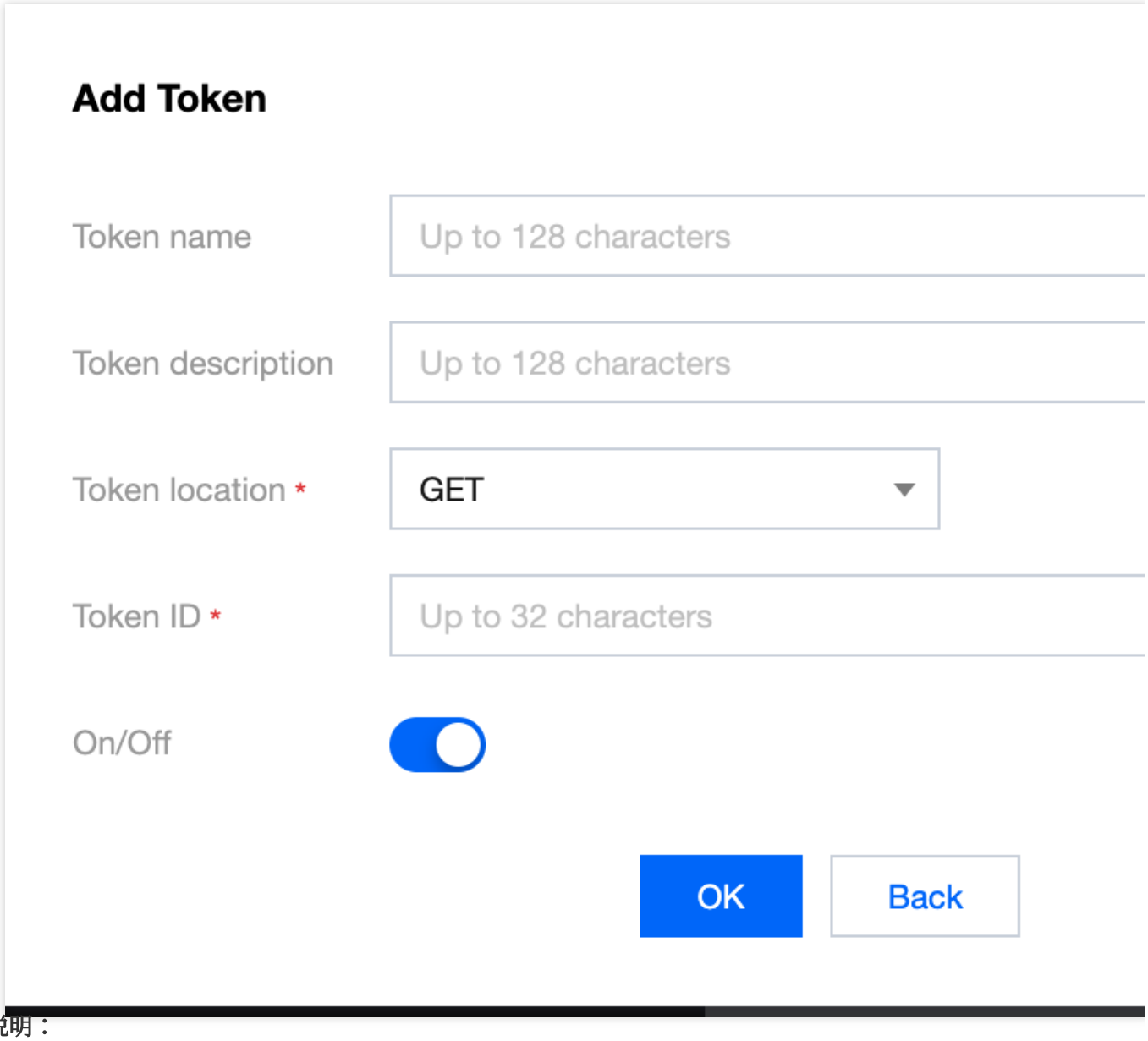
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在 BOT 管理页面，在全局设置中，单击会话管理模块的**前往配置**。



4. 在会话管理页面，单击**添加配置**，配置相关参数，单击**确定**。



参数说明：

Token 名称：自定义名称，最多128个字符。

Token 描述：自定义描述，最多128个字符。

Token 位置：可选择 HEADER、COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。

Token 标识：取值标识。

客户端风险识别（前端对抗）

客户端风险识别功能通过客户端动态安全验证技术，对业务请求的每个客户端生成唯一 ID，检测客户端对 Web 或 H5页面访问中可能存在机器人和恶意爬虫行为，保护网站业务安全。

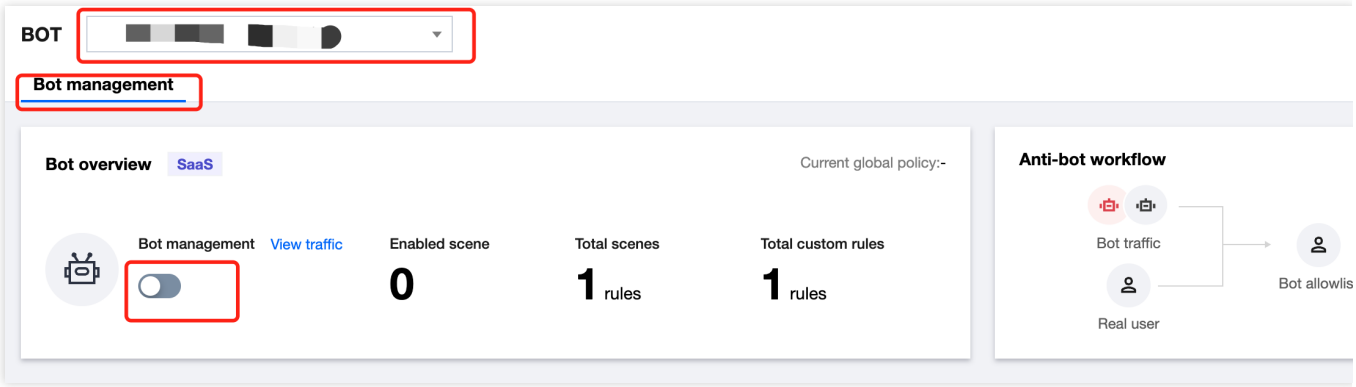
说明：

本功能**不支持 CLB-WAF，泛域名，以及 App**，只适用与 Web 或 H5页面，如果有非动态认证，自动化接口脚本需要优先加入白名单。

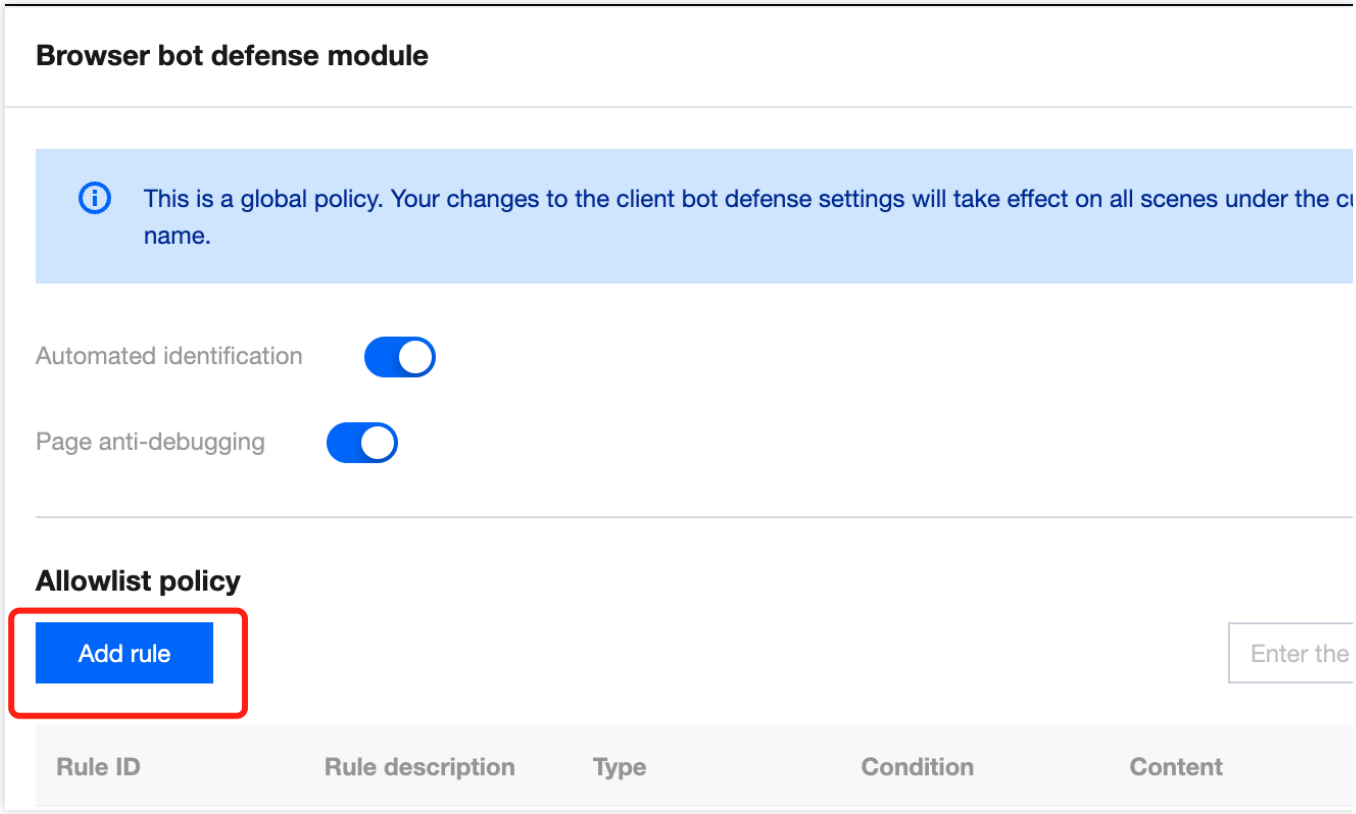
添加白名单

添加白名单主要用于对不需要进行设置的接口放行处理。

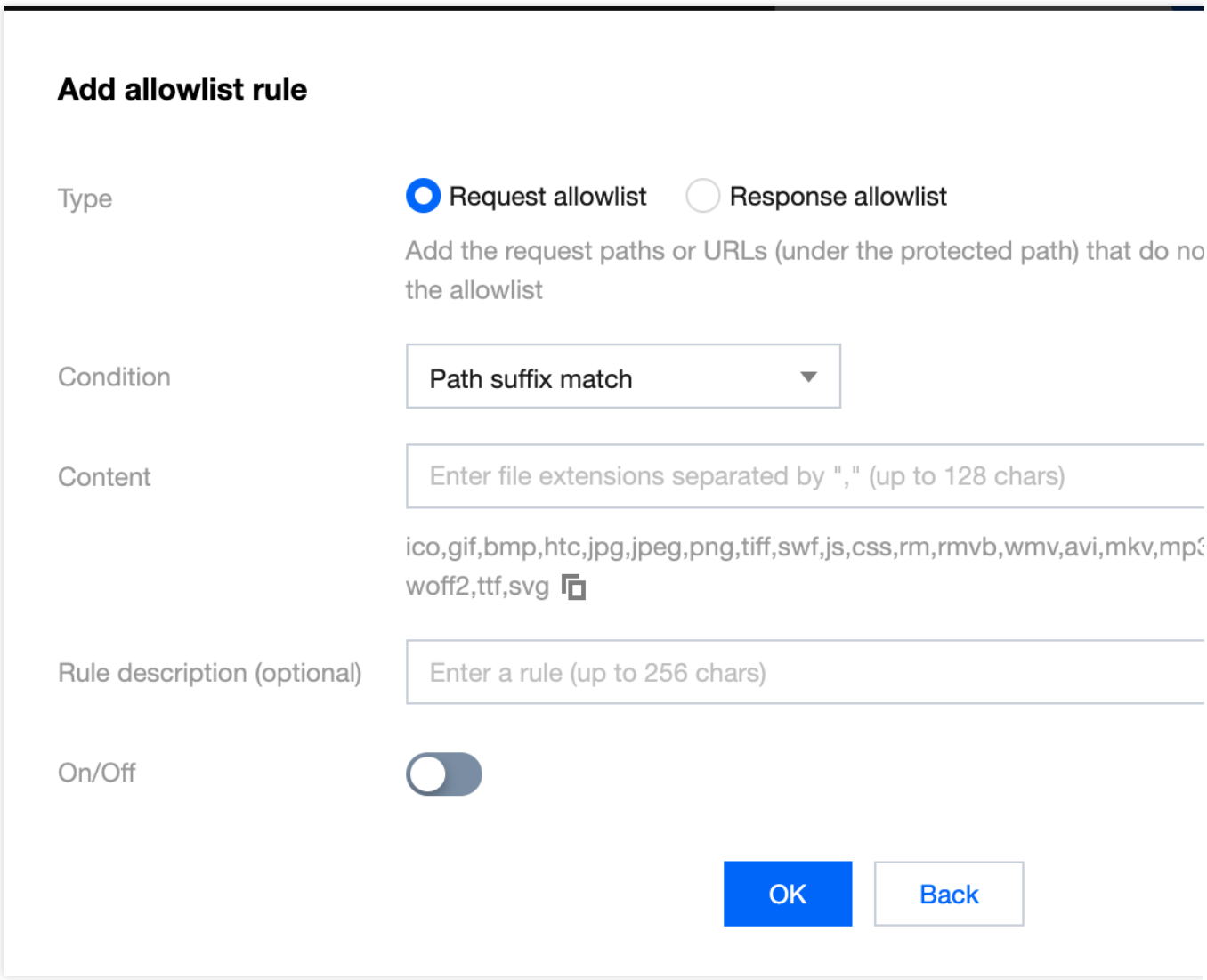
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在 BOT 管理页面，在全局设置中，单击前端对抗模块的**前往配置**。
4. 在前端对抗页面，单击**添加规则**，弹出添加白名单规则窗口。



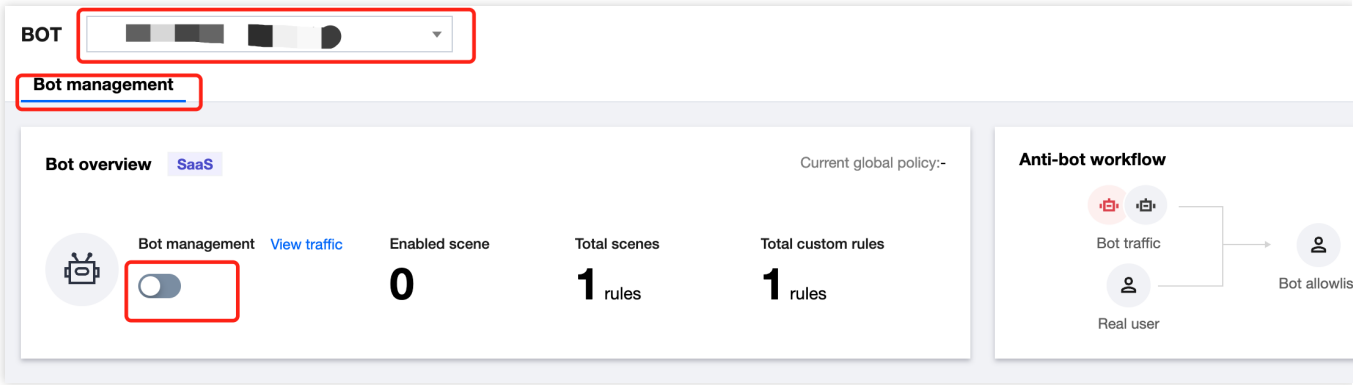
5. 在添加白名单规则窗口中，配置相关参数，单击**确定**即可。



案例一：大量机器自动化脚本请求服务

有大量机器自动化脚本请求服务，禁止类似 CURL，SOAPUI、JMETER、POSTMAN 访问请求。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。

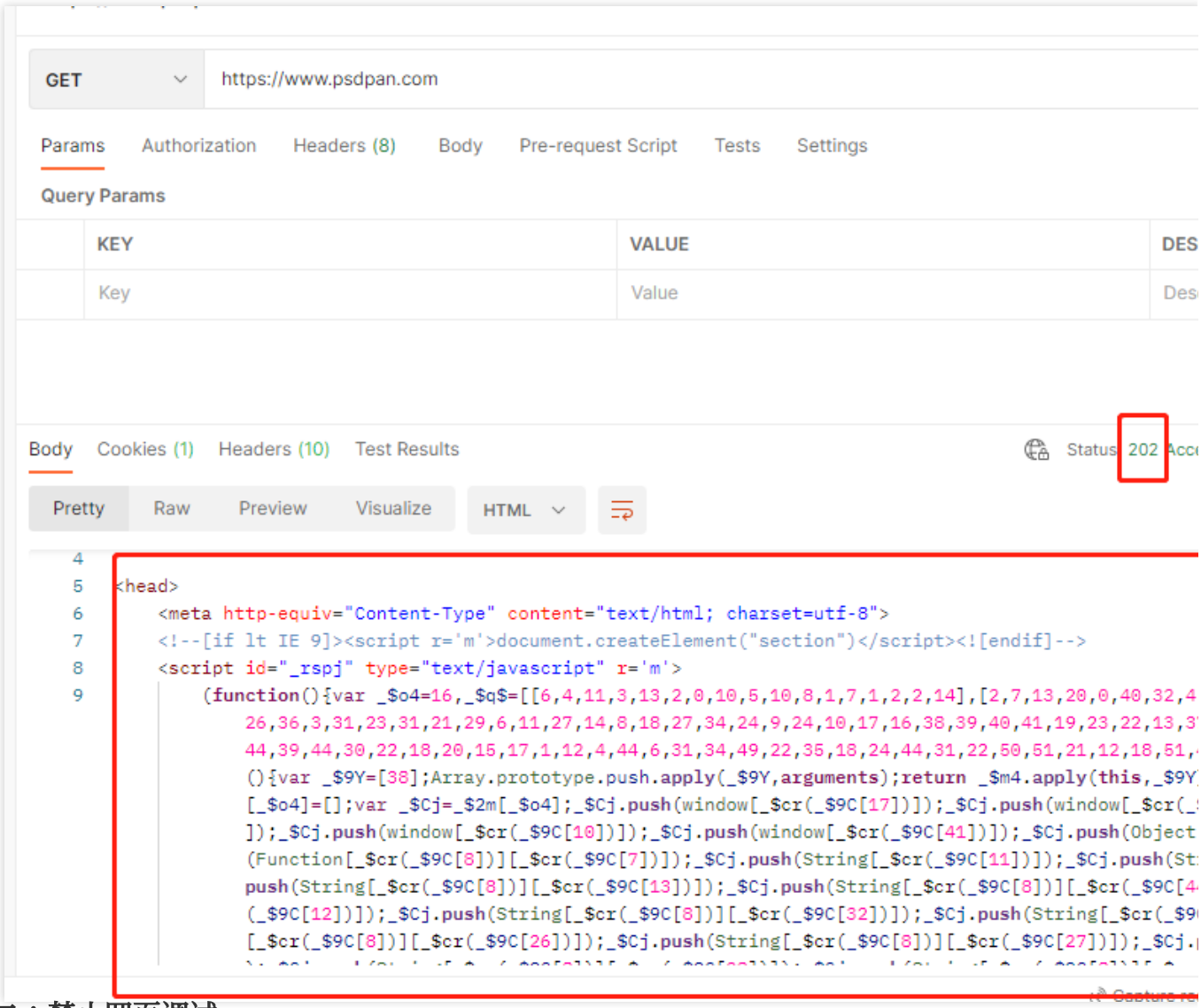


3. 在 BOT 管理页面，在全局设置中，单击前端对抗模块的**前往配置**。
4. 单击自动化工具识别的

，确认白名单。
5. 单击某场景配置页，单击**前端对抗**，单击该场景下前端对抗模块的

，防护模式选择**拦截**，开启该前端对抗功能。
6. 使用 CURL、SELENIUM、POSTMAN 请求结果分别如下所示：

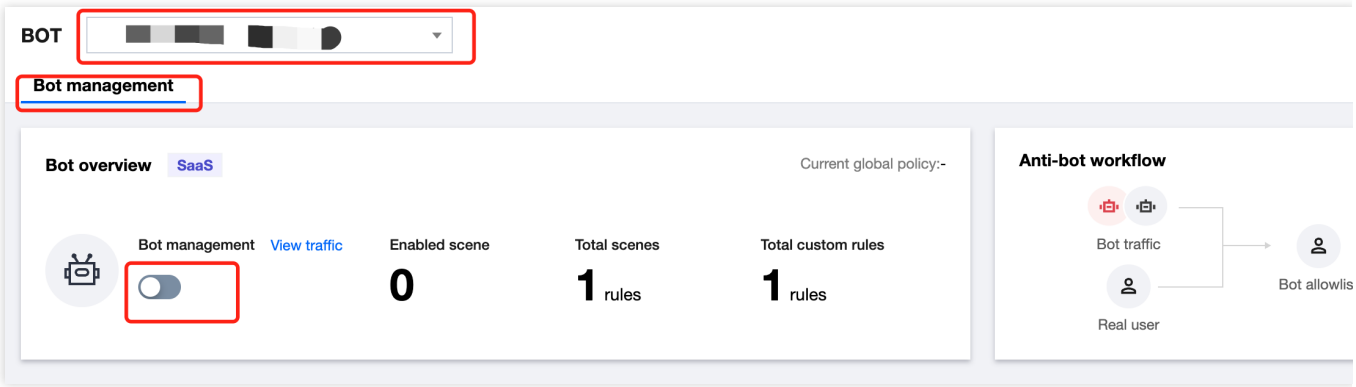
```
$1f.length;_$uD++){_$1f[_$uD]^=_$2_[Math.abs(_$uD)%16];}}return;}}}else if(_$WA*122>1
WA*122<3416){if(150===126+_$WA){_$hL+=7;}else if(92*_$WA===2300){_$hL+=-13;}else if(-
OxmJnUWnNuL");}else{var _$wr=_$mt[19];}}else if(_$WA*79>1501&&24-_$WA>0){if(131===111
===42){_$12=_$2_[_$8B(_$mt[5])];}else if(16===_$WA-6){_$12=_$vc&&_$vc[_$8B(_$mt[3])];
_$mt[0]));}}else if(15-_$WA<0&&20>_$WA){if(43===27+_$WA){_$vc[_$8B(_$mt[3])][_$8B(_$m
7){return;}else if(-63===_$WA-81){_$uD.push(4);}else{_$y2();}}else{if(91===63+_$WA){_
=_$lt[_$8B(_$mt[4])];}else if(-73===_$WA-103){_$hL+=13;}else{_$lt[_$8B(_$mt[6])](_$8B
}}else if(16>_$WA){if(-55<_$WA-62&&_$WA*124<1488){if(41===33+_$WA){_$uD.push("{qqqr0
8nQ.UPWqqr7Dccebc0qqr4r0qqr0c22qq.CB.7K7RYGXUTYmj9XtdgeOmTyesaZg_0qSWhVgawzuE|)YCaXKu
2bWDEEql0G1qflJhlQzcHTRdpfCCuWWBV44bufWBL4gCuHMzar5pkcMJLaN16Qh_90_Ok8MJZM4SuJiZZaak6
VnCKpRxxfvD4jMWzB2CIJ3wRPPDFmMHL1auBDHz9GOk1KlQlwarciRdNy6OsMJwSvZob.xH9u4pDZoMZAZC8r
7DDIDRzP_PIPqtEcBDtbEy9_zaqqqqqqr0QQSplxlW7APrrh9L71n2ct0EXAP2hqqVHiGJ6GOIcJ0J6GuVkwZ
7rGzuBJM5xzec66wHRzzCdNMIlzZosuM3SBTD6ihQT0nD6gIENB0b6lUtWqqh7QQHsrGZiGac64qqr0HQNywd
iGJkEOxVPeGt4c64qql4096qqqhQAM3Ma8MO_wkRbQqqk162HmCGbKcppEmgBVn3qqt1083179040lrrL.");
iP;}else if(-21===_$WA-31){_$uD.push("7V00OtRWGFA");}else{if( !_$12)_$hL+=1;}}else if
_$WA){_$2_.id=_$1f;}else if(118*_$WA===590){_$2_[_$8B(_$mt[35])]=_$eV;}else if(-117==
3])](_$8B(_$mt[24]));}else{_$uD.push(4);}}else if(4>_$WA){if(101===101+_$WA){_$lt[_$8
se if(52*_$WA===52){if( !_$12)_$hL+=2;}else if(-69===_$WA-71){_$uD.push("Vk_yxby7sIG"
==122+_$WA){_$2_[_$8B(_$mt[34])]=_$mt[33];}else if(74*_$WA===962){_$2_.src=_$13;}else
][_$8B(_$mt[2])](_$2_);}else{_$uD.push("R.ldTebdfga");}}}else{if(-17<_$WA-64&&_$WA*22
se if(51*_$WA===2499){return Math.abs(arguments[1]) % 16;}else if(36===_$WA-14){retur
}}}function _$rY(_$vs){var _$wr,_$uD,_$KD=_$vs,_$vc=_$Fb[2];while(1){_$uD=_$vc[_$KD++
_$2_[_$8B(_$mt[5])]==_$8B(_$mt[15])||_$2_[_$8B(_$mt[5])]==_$8B(_$mt[42]);}else if(120
_$uD===140){_$2_[_$8B(_$mt[46])]=null;}else{if( !_$wr)_$KD+=2;}}else{return;}}}}})()<
<body>
<input type="hidden" id="__onload__" name="cDLJ.6zflivja8RAGWSNtmGchMfTmH_nrcvrZ2rWMS
XBKK8HwG" value="g.bsDjQpVCmzPMoeR.dbDA">

</body>
</html>
psdpan@psdpandeMacBook-Pro ~ % curl http://www.psdpan.com -I
HTTP/1.1 202 Accepted
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Set-Cookie: Cc2838679FS=5ffyjNUVxUtd.BOCnqlHHKmk7AhiBH.OtxKdMrzQg1gG.T8yHY8c.A2gLxFTi
expires=Tue, 02 Mar 2032 09:11:53 GMT; HttpOnly
Expires: Sat, 05 Mar 2022 09:11:53 GMT
Date: Sat, 05 Mar 2022 09:11:53 GMT
Server: ******
Cache-Control: no-store
Pragma: no-cache
```



案例二：禁止网页调试

禁止用户打开网页调试，避免针对性爬虫编写。

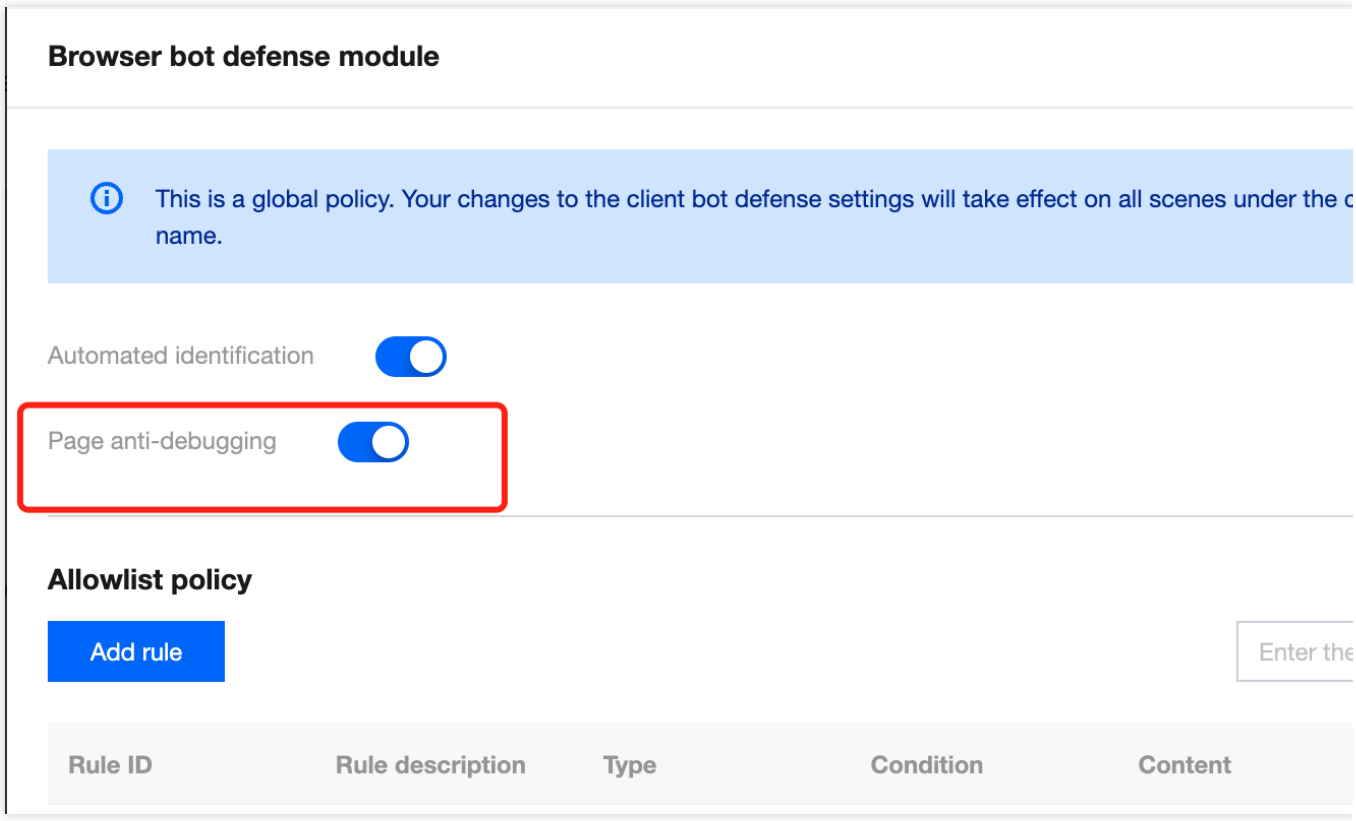
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在 BOT 管理页面，在全局设置中，单击前端对抗模块的**前往配置**。

4. 单击页面防调试的

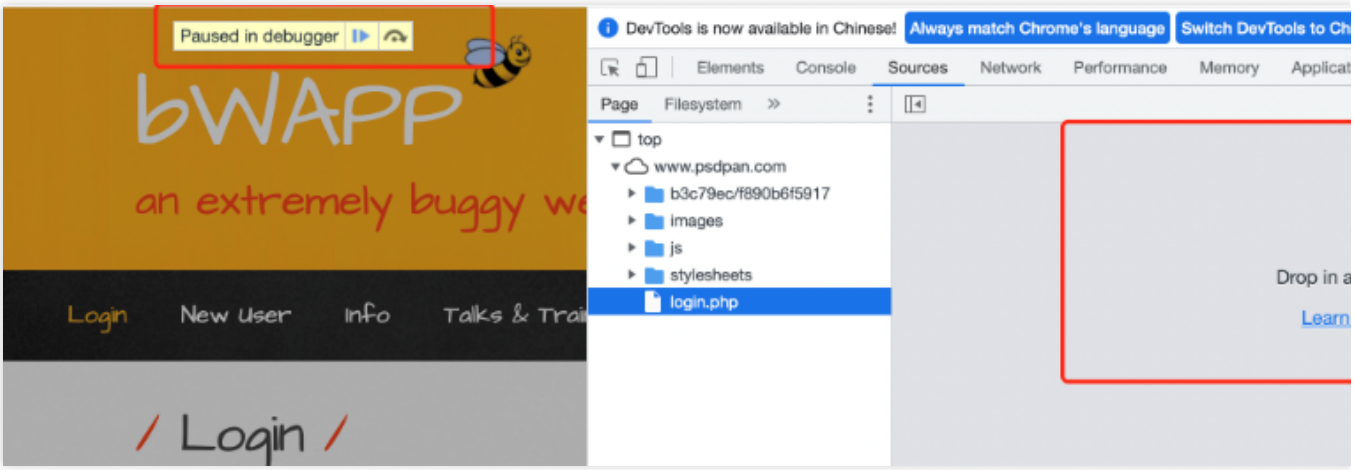
，确认白名单。



5. 单击某场景配置页，单击**前端对抗**，单击该场景下前端对抗模块的

，防护模式选择**拦截**，开启该前端对抗功能。

6. 使用 Chrome 请求结果如下所示：



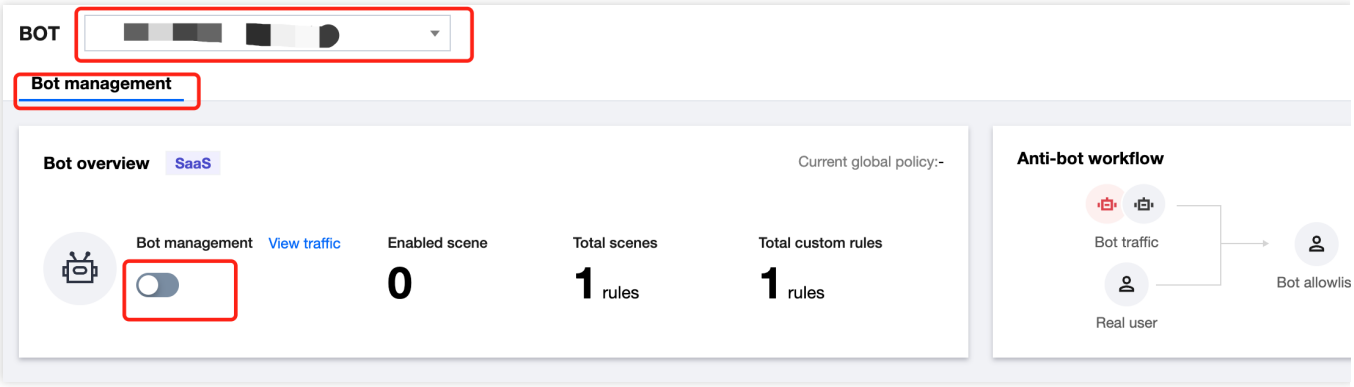
威胁情报

威胁情报功能依托腾讯近二十年的网络安全经验和大数据情报，将通过实时判定 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、IDC 的访问，同时智能识别恶意爬虫特征，解决来自恶意爬虫、分布式爬虫、代理、撞库、薅羊毛等风险访问。

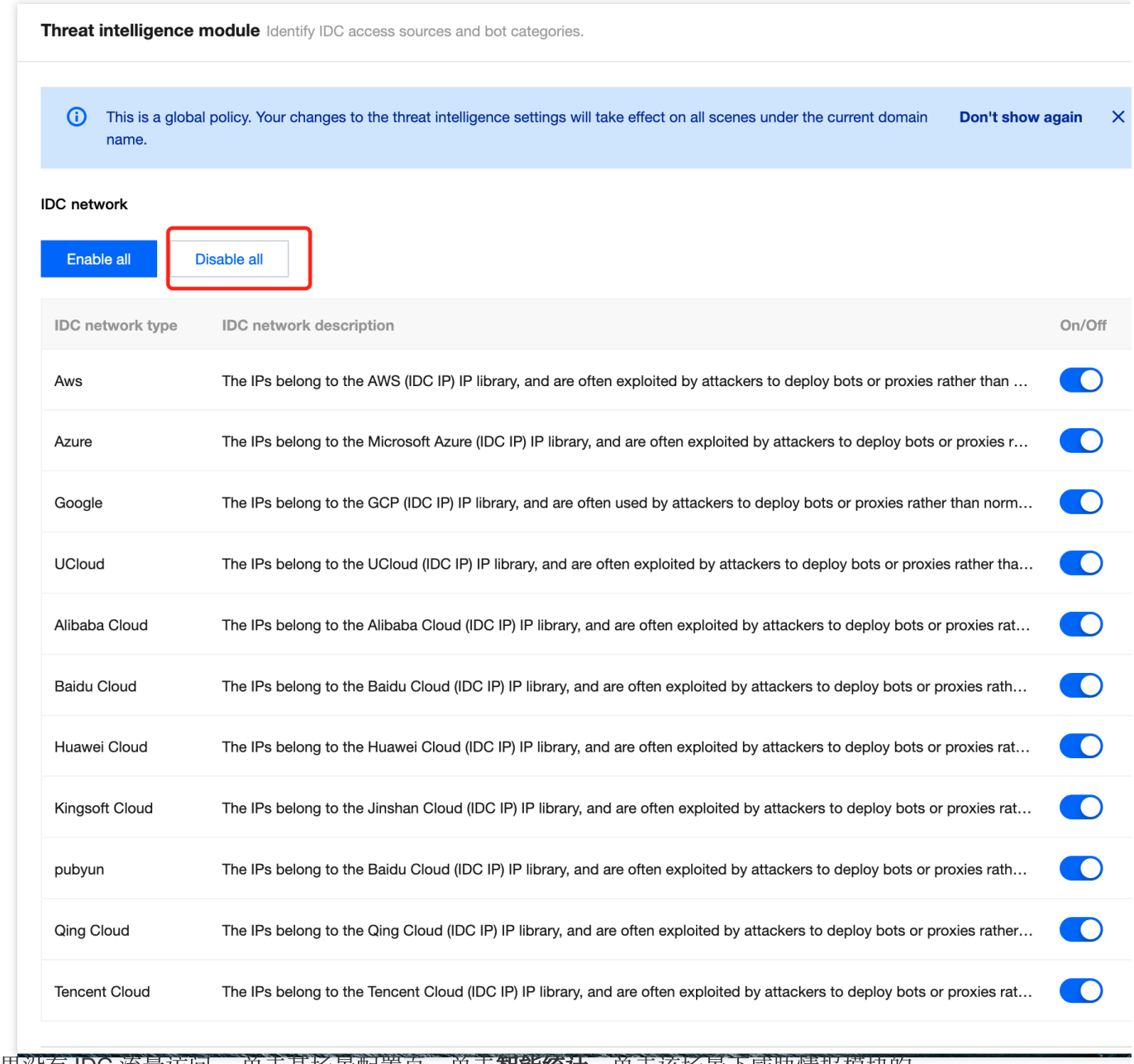
说明：

开启威胁情报功能时需要确认业务是否有 IDC 侧的用户访问，确认业务有 IDC 流量访问时，需要先关闭 ID 后，再开启威胁情报功能。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。

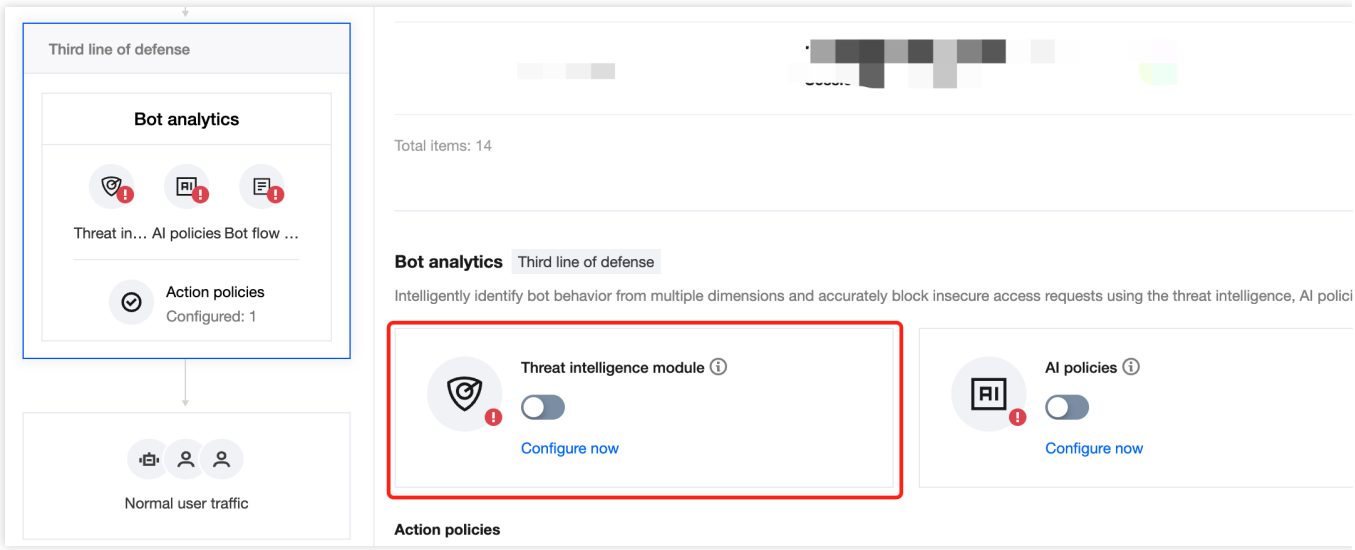


3. 在 BOT 管理页面，在全局设置中，单击威胁情报模块的**前往配置**。
4. 在威胁情报页面，如果有 IDC 流量访问，单击 IDC 网络的**一键关闭**，关闭功能。



5. 如果没有 IDC 流量访问，单击某场景配置页，单击**智能统计**，单击该场景下威胁情报模块的

，直接开启威胁情报功能即可。



AI 评估

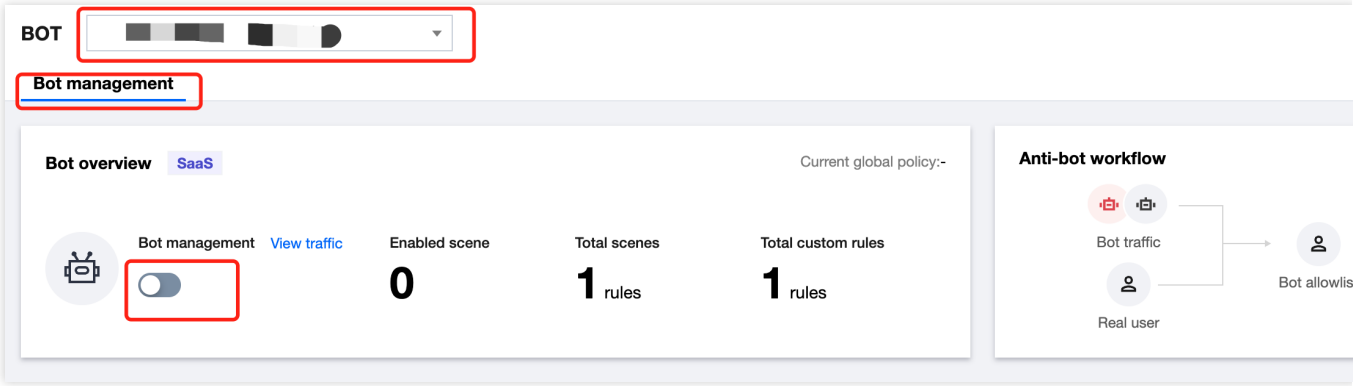
AI 评估功能基于人工智能技术和腾讯风控实战沉淀，将风控特征和黑灰产对抗经验转化为 AI 评估模型，通过访问流量进行大数据分析与 AI 建模，实现快速识别恶意访问者、深层次恶意访问者，解决来自高级持续性威胁 BOT、隐蔽性威胁 BOT 的风险访问行为。

说明：

AI 评估是根据 AI 建模自动学习，可直接开启；如果有误评估，将对相应 URL 加白即可。

开启 AI 评估

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。

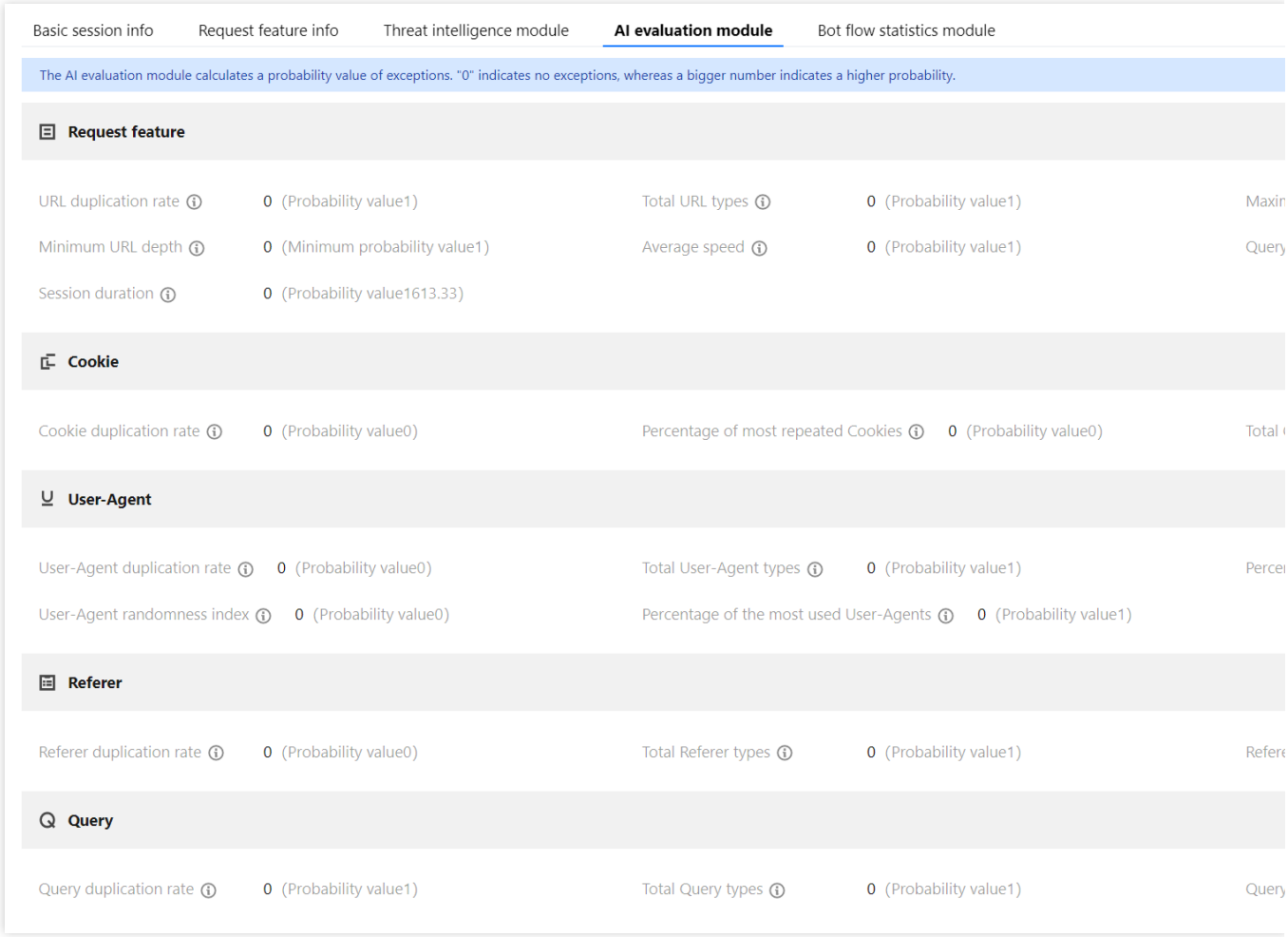


3. 在 BOT 管理页面，在全局设置中，单击AI策略模块的**前往配置**。

添加白名单

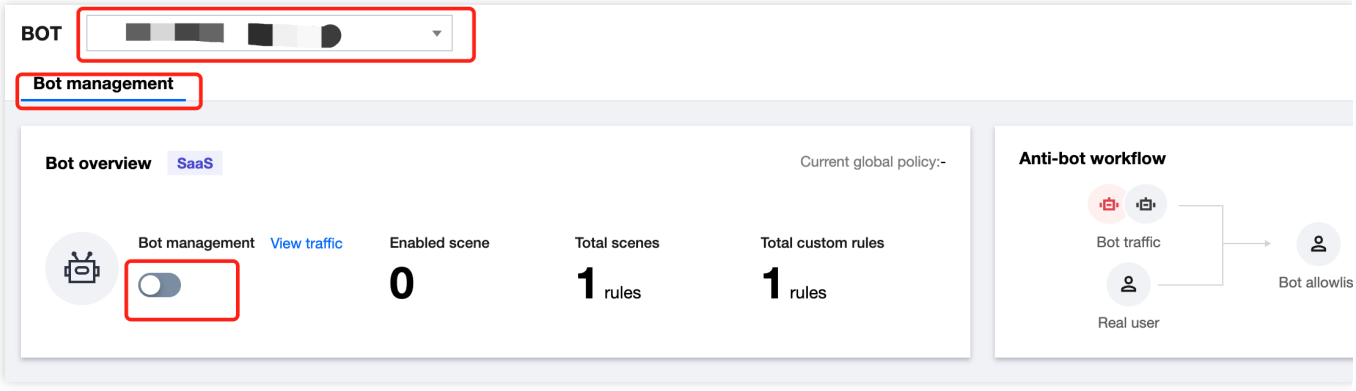
背景信息

在 AI 评估页面，该请求为正常请求，但是被 AI 误报。



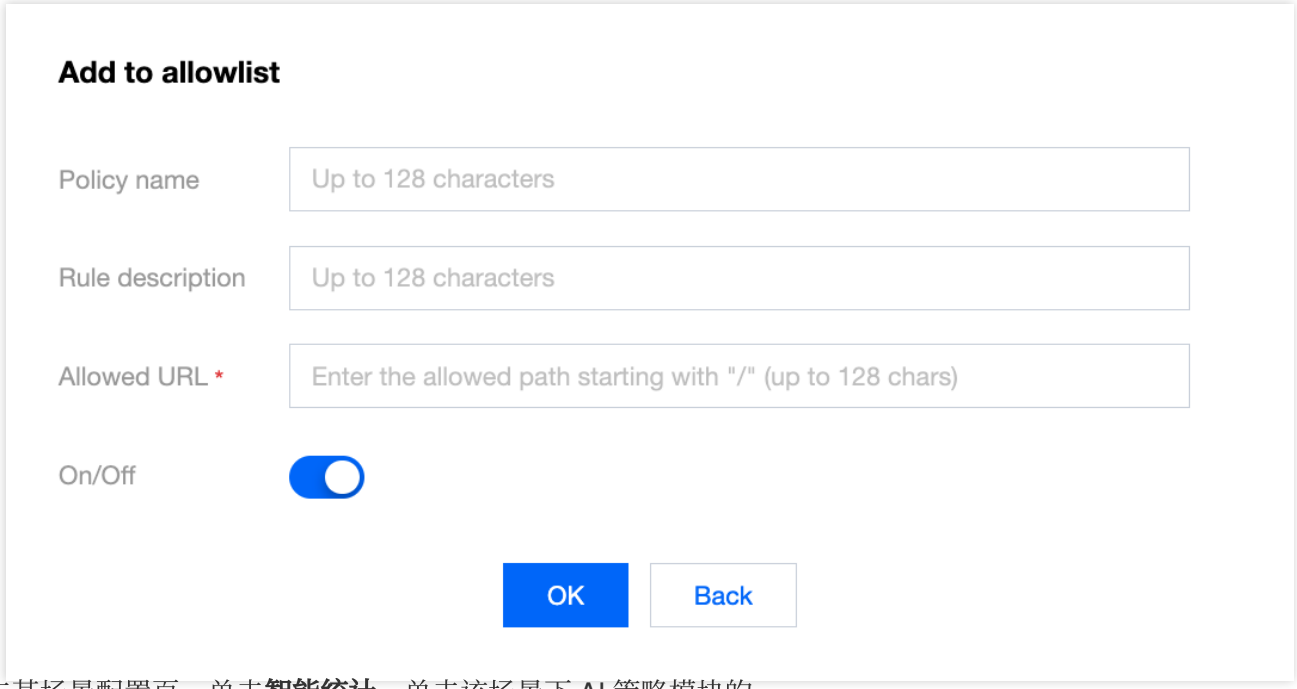
操作步骤

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在 BOT 管理页面，在全局设置中，单击 AI 评估模块的**前往配置**。

4. 在 AI 评估页面，单击**添加白名单**，输入名称、描述和加白 URL，单击**确定**。



5. 单击某场景配置页，单击**智能统计**，单击该场景下 AI 策略模块的

，直接开启 AI 策略功能即可。

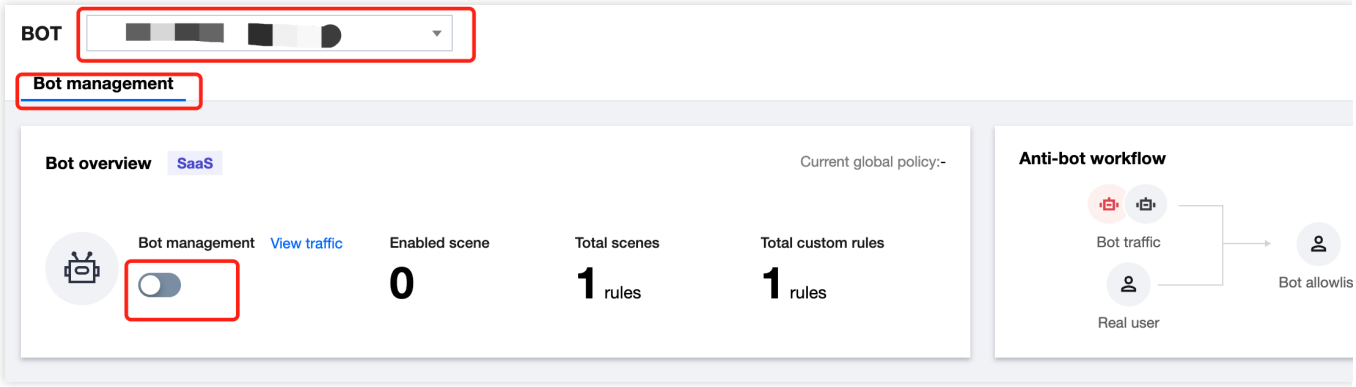
智能统计

智能统计功能基于大数据分析统计，根据用户群体的流量特征自动分类，自动识别存在异常的恶意流量，通过大数据分析，自动调整恶意流量阈值，解决来自常规 BOT、高频 BOT 的风险访问，并通过自动调整统计模型，解决大部分的 BOT 行为绕过问题。

说明：

可直接开启智能统计，推荐使用智能模式。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在 BOT 管理页面，在全局设置中，单击 AI 评估模块的**前往配置**。

动作策略

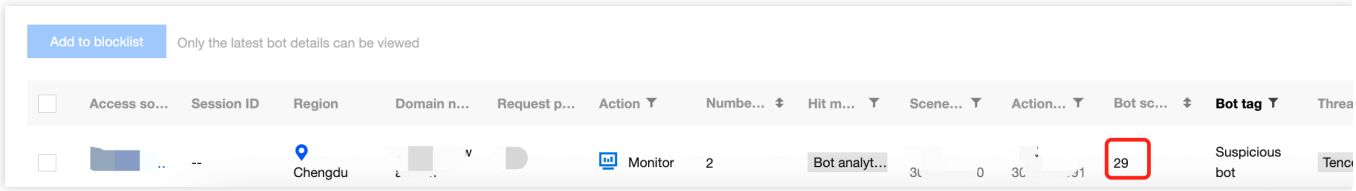
动作设置功能通过威胁情报、AI 评估、智能统计对网站的访问请求进行综合性打分。打分范围在0-100分范围内，分数越高 BOT 的可能性越高、其访问对网站产生的危害/压力则越大。通过分数智能识别访问行为的风险程度，用户可配置不同动作策略和每个动作策略相应的生效范围和不同分数段的动作实现风险访问的精准拦截。

背景信息

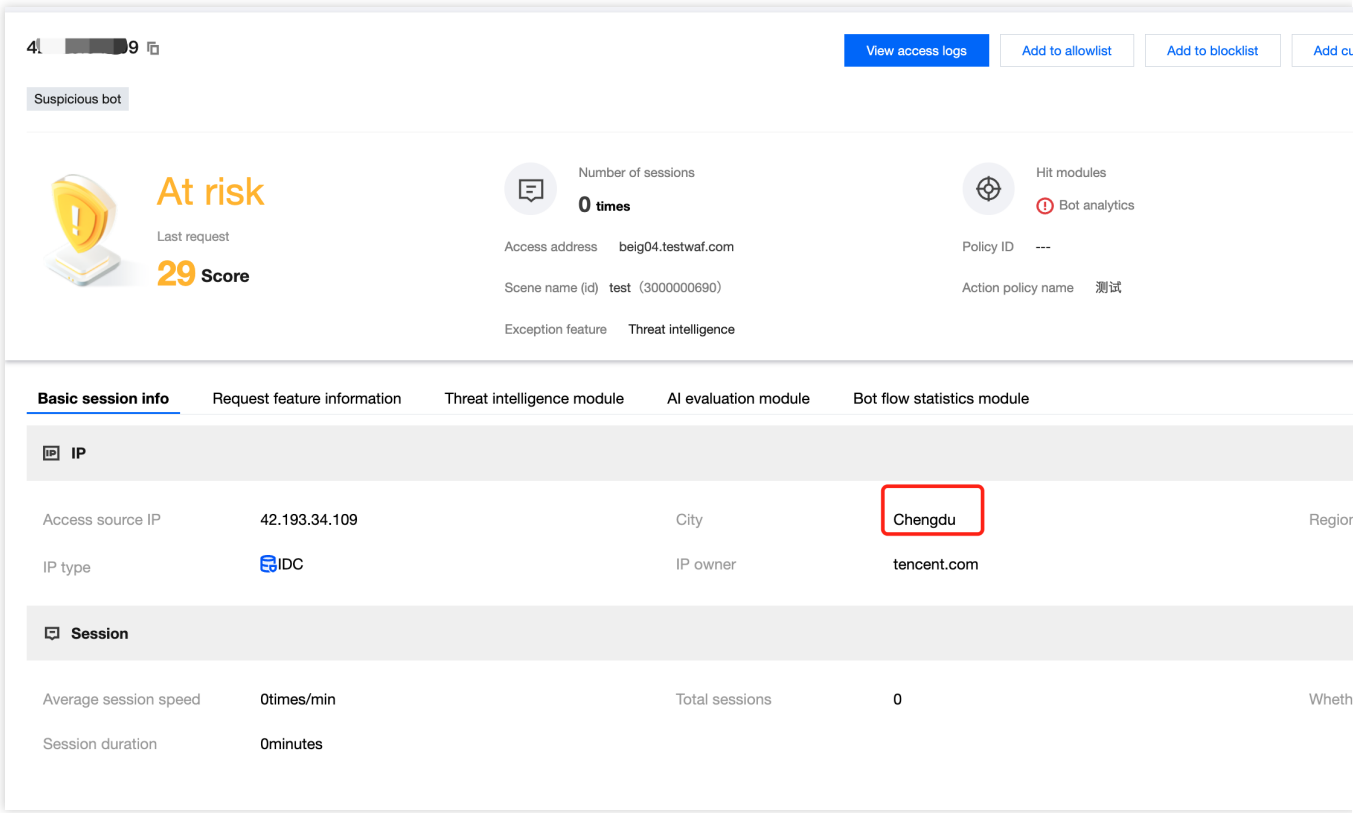
当威胁情报，AI 评估以及智能统计标记出了大量流量，默认配置无法做到更加详细的拦截，需要自定义动作如何分析配置。

操作步骤

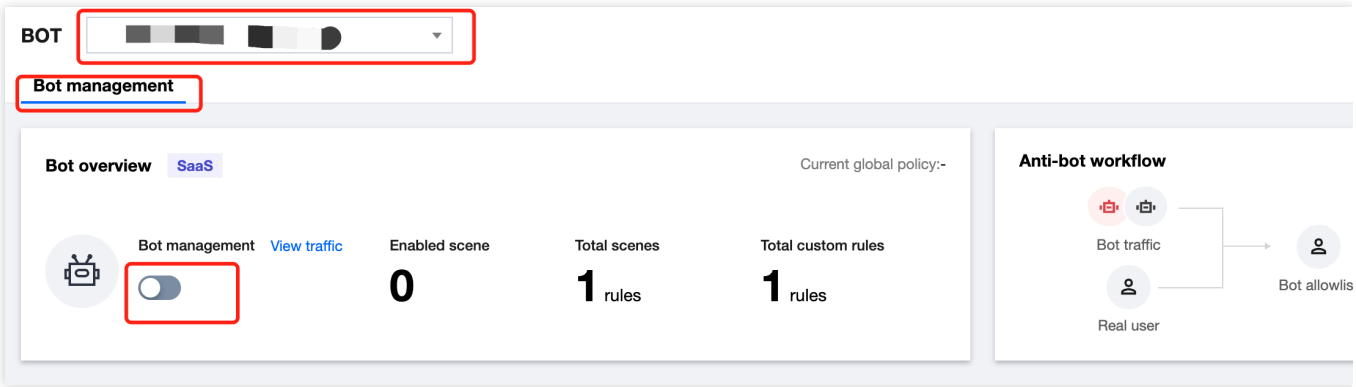
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择 **BOT 流量分析**。
2. 在 BOT流量分析页面，左上角选择需要防护的域名，选择所需访问源，单击**查看详情**。



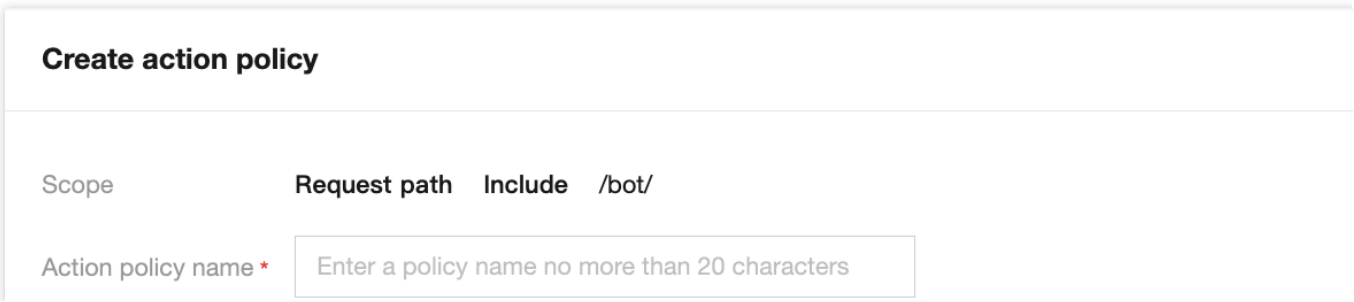
3. 在 BOT 流量详情页面的基础会话信息模块，查看城市和 IP 地区。

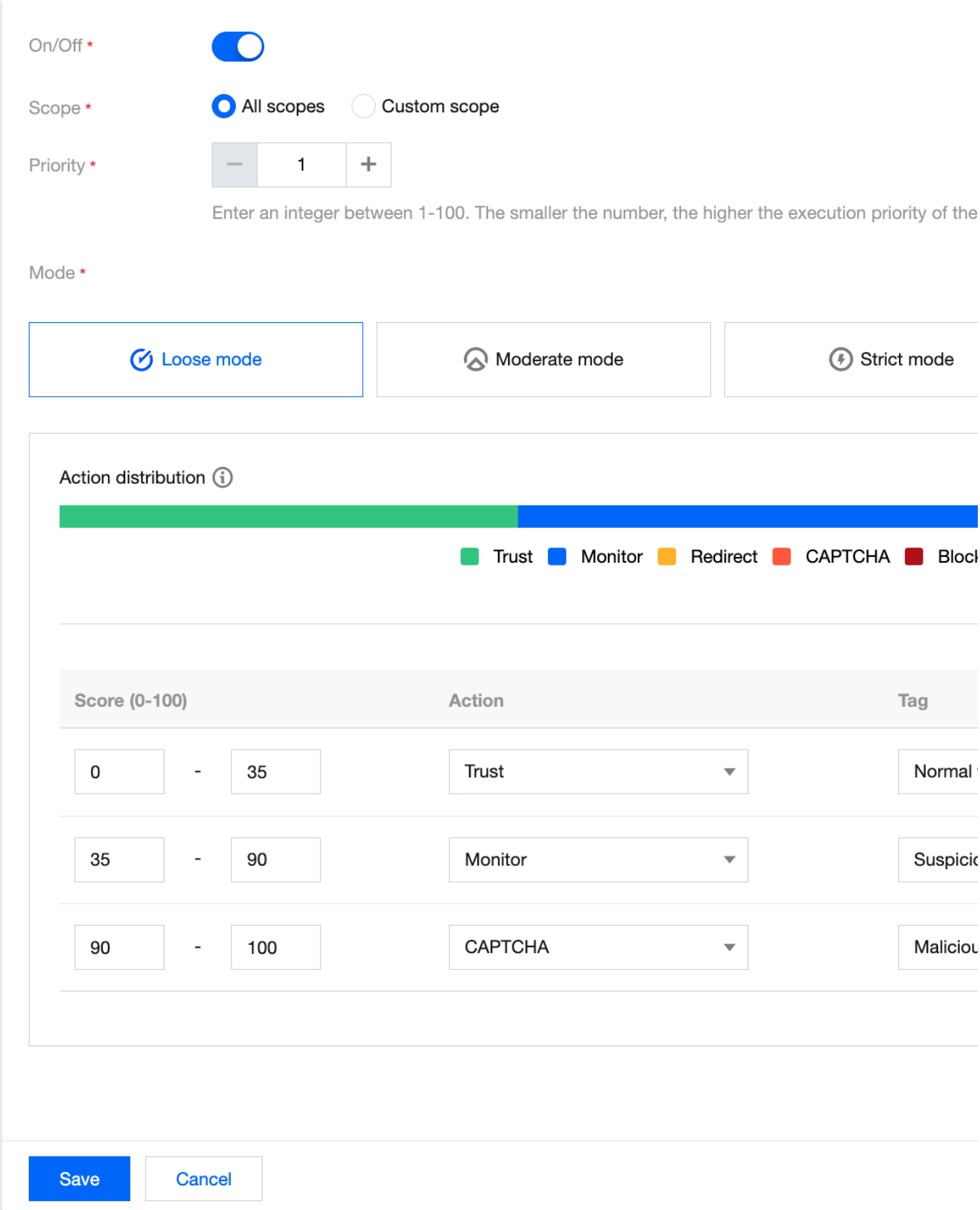


4. 当业务没有该地区的流量时，则表明此处评分为异常，可以自定义动作设置，进行一个更加细化的设置。
5. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



6. 点击某场景配置页，单击**智能统计**，单击该场景下动作策略模块的**新增动作策略**。
7. 在动作策略页面，配置相关参数，单击**立即发布**。





参数说明：

策略名称：填写动作策略名称

生效开关：当前动作策略是否生效

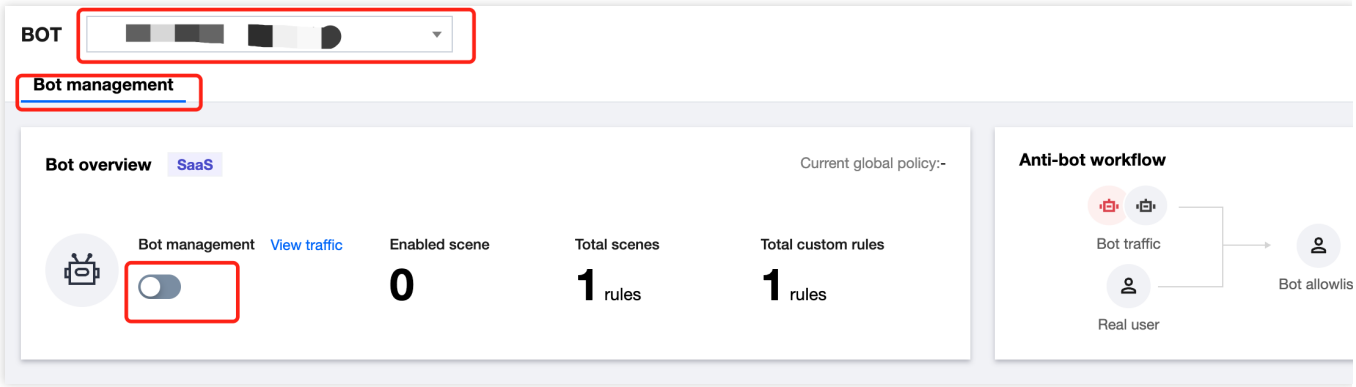
生效范围：当前动作策略的生效范围

优先级：当前动作策略的执行优先级，请输入1-100的整数，数字越小，代表这条策略的执行优先级越高；

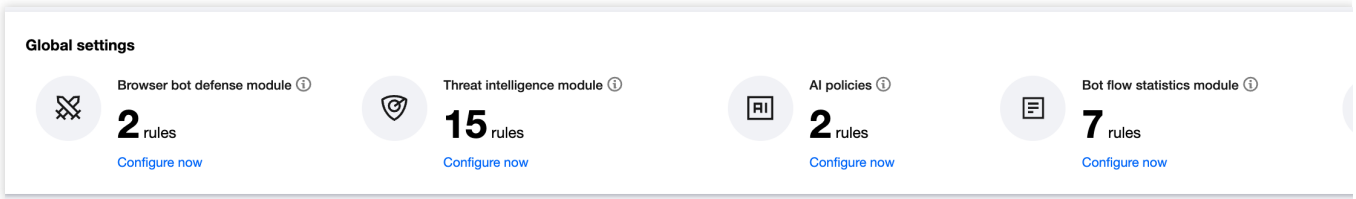
模式设置：提供宽松模式、中等模式、严格模式、自定义模式这四种默认处置模式，宽松、中等、严格这三种模式为预设模式，分别代表 BOT 流量管理针对不同危害程度的 BOT 的推荐分类及处置策略。这三种预设模式可进行修改，修改后为自定义模式。
分数段设置：分数段区间总分数为 0-100 分，每个分数段总共可以添加10条，配置的分数区间范围左闭右开，分数段不可重合，分数区间可设置为空，设置为空时，空的分数段不处置动作。
动作设置：可设置为信任、监控、重定向（重定向至特定网站 URL）、人机识别（验证码）或拦截。
标签设置：可设置为友好 BOT、恶意 BOT、正常流量或疑似 BOT。
友好 BOT：为默认对网站友好/合法的 BOT。
疑似 BOT：为识别出该访问源流量疑似 BOT，但无法判断其对网站的是否有害。
正常流量：为认为访问的流量为正常人类。
恶意 BOT：为对网站产生恶意流量/访问请求不友好的 BOT。

合法爬虫

通过配置合法爬虫（如：搜索引擎、订阅机器人）可以正常获取网站数据，使网站可以正常被索引。
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。

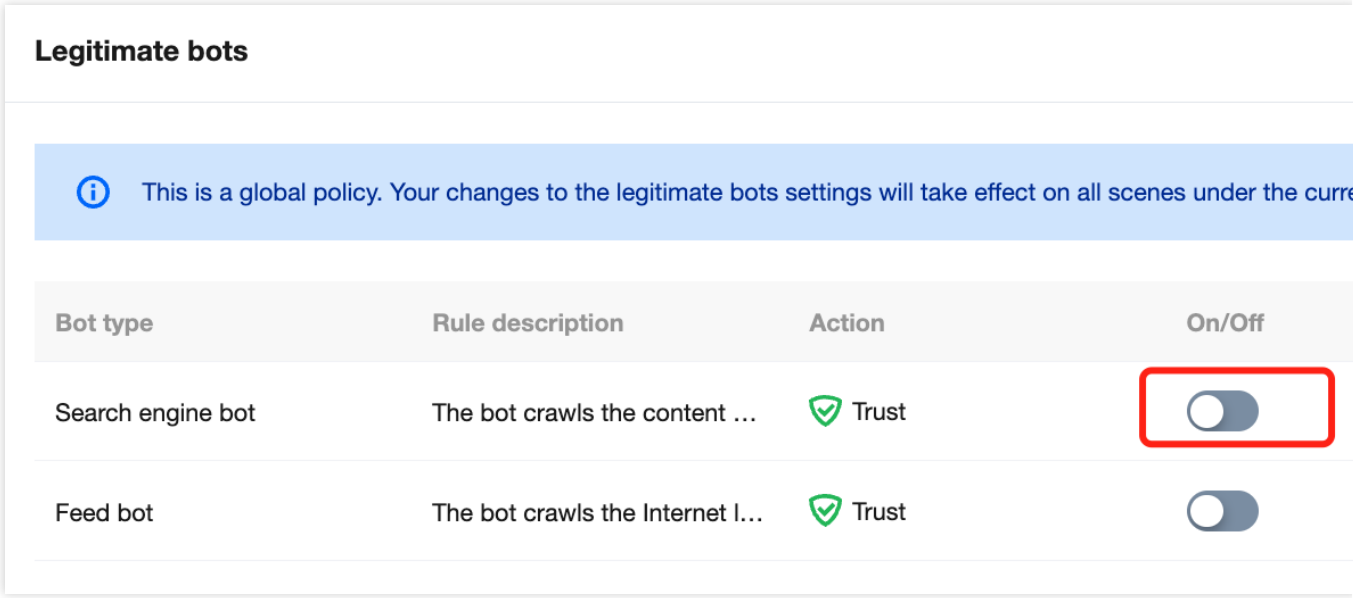


3. 在 BOT 管理页面，在全局设置中，单击合法爬虫模块的**前往配置**。



4. 在合法爬虫页面，可单击

，开启对应功能。



自定义规则

通过配置自定义规则功能，可精准处置符合行为配置的爬虫，精准处置对应特征的访问特征请求。

注意：

目前在创建 BOT 场景化时，已经根据场景类型内置相应场景的自定义规则集。

本功能主要分析数据来源于 BOT 流量分析。

该内容**只做使用分析参考，不能当做业务标准配置**，网络爬虫分为很多种，基本都是随着业务类型而变。

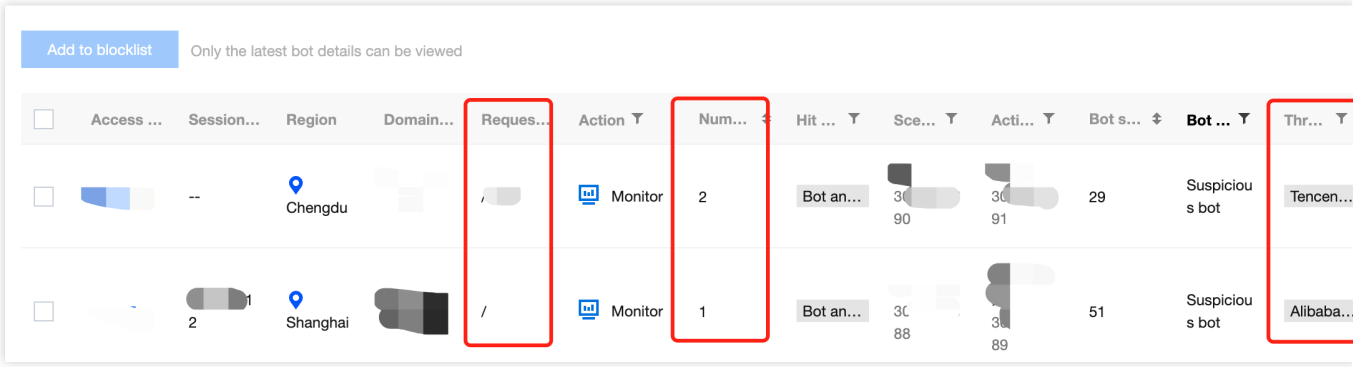
案例详情

目前已经无法通过动作得分进行拦截，需要对异常行为特征进行设置，在 BOT 流量分析进行查看出大概异常后，单击**详情**，可查看异常数据指标，并结合实际业务情况进行对比。

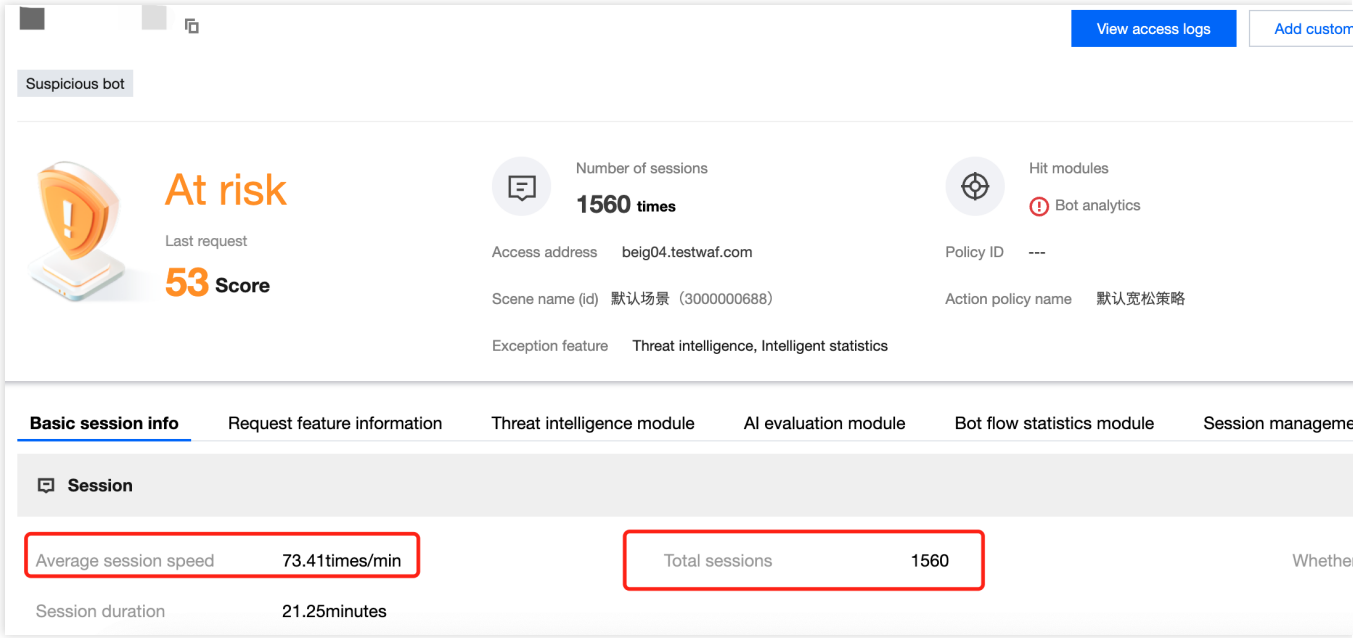
例如：URL 重复性是1，会话次数100次分钟，UA 滥用等，就需要结合业务是否有访问相同的请求或者是代理等业务，如果没有就说明有人恶意攻击。那么就可以根据以下方式查看并配置拦截策略。

分析案例

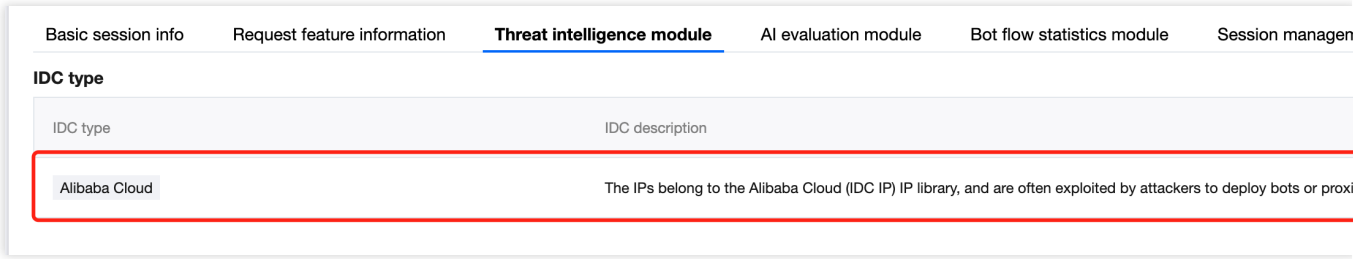
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**BOT 流量分析**。
2. 在 BOT流量分析页面，左上角选择需要防护的域名，选择所需访问源，目前根据展示，能看到该 IP 请求速度很快，URL 单一，并且是 IDC 类。



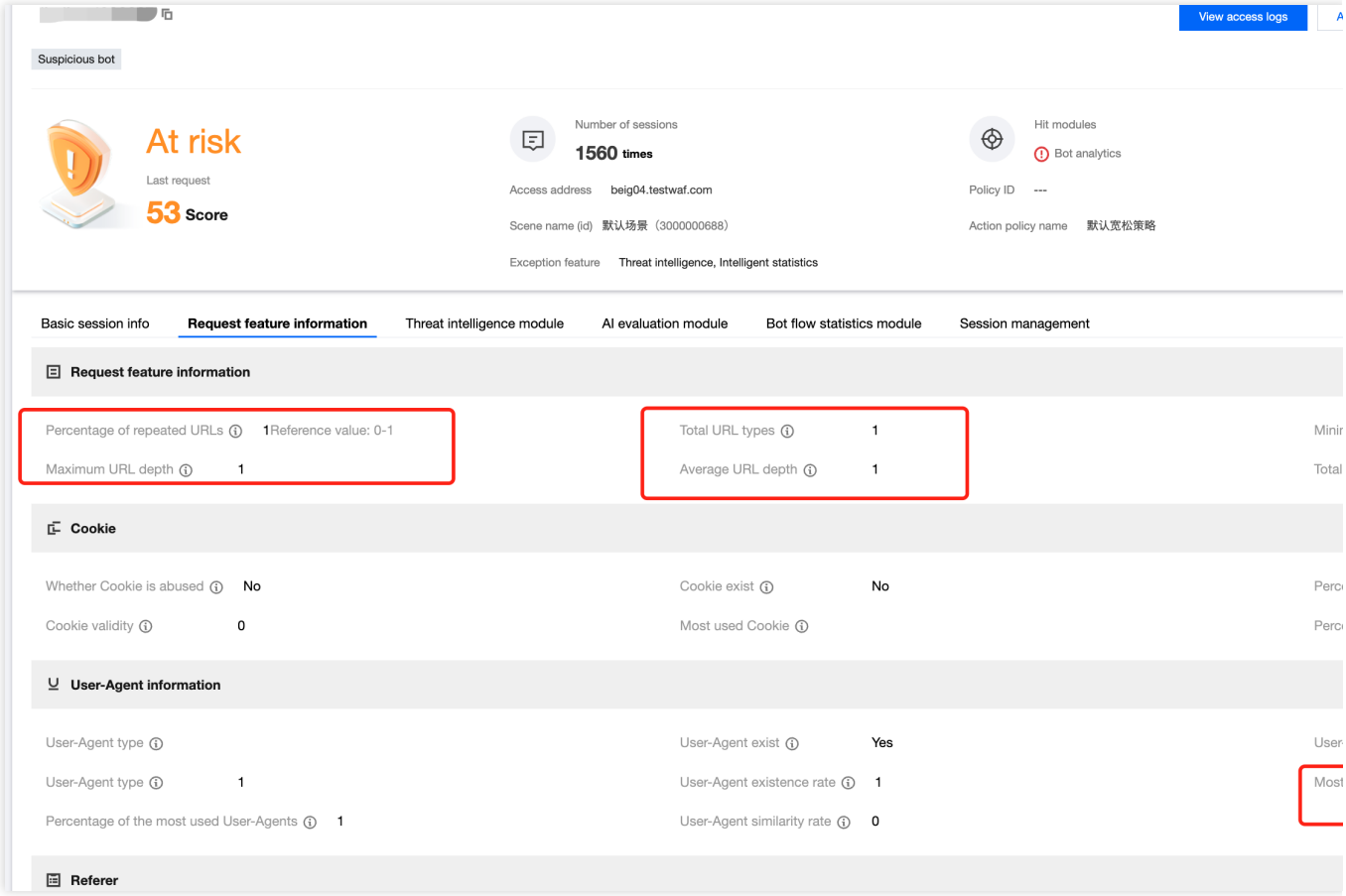
3. 单击**查看详情**，通过基础会话信息可以看出，会话速度平均次数，总次数。也可以直接根据该条件进行设置。



4. 在威胁情报页面，可以根据情报数据判断该 IP 是否有正常用户使用过。

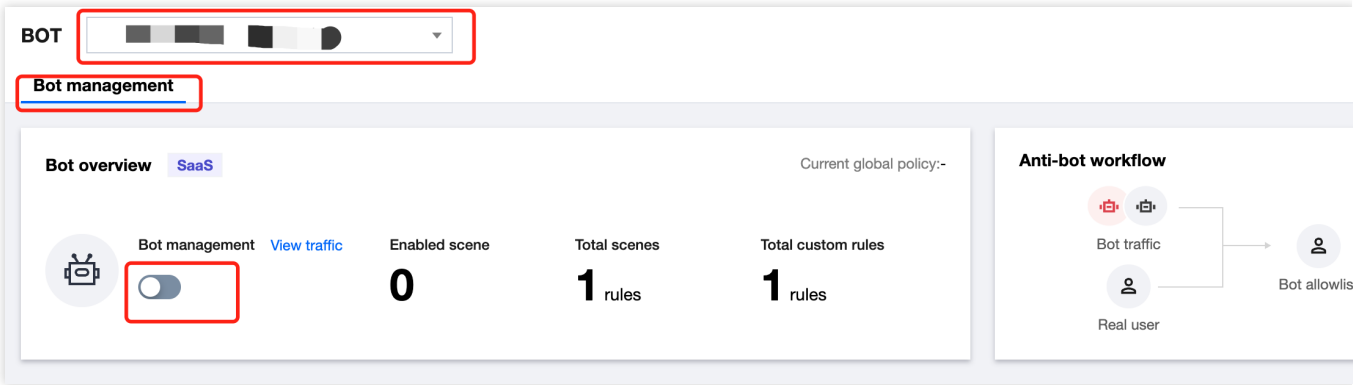


5. 在请求特征信息页面，可以查看请求详情。

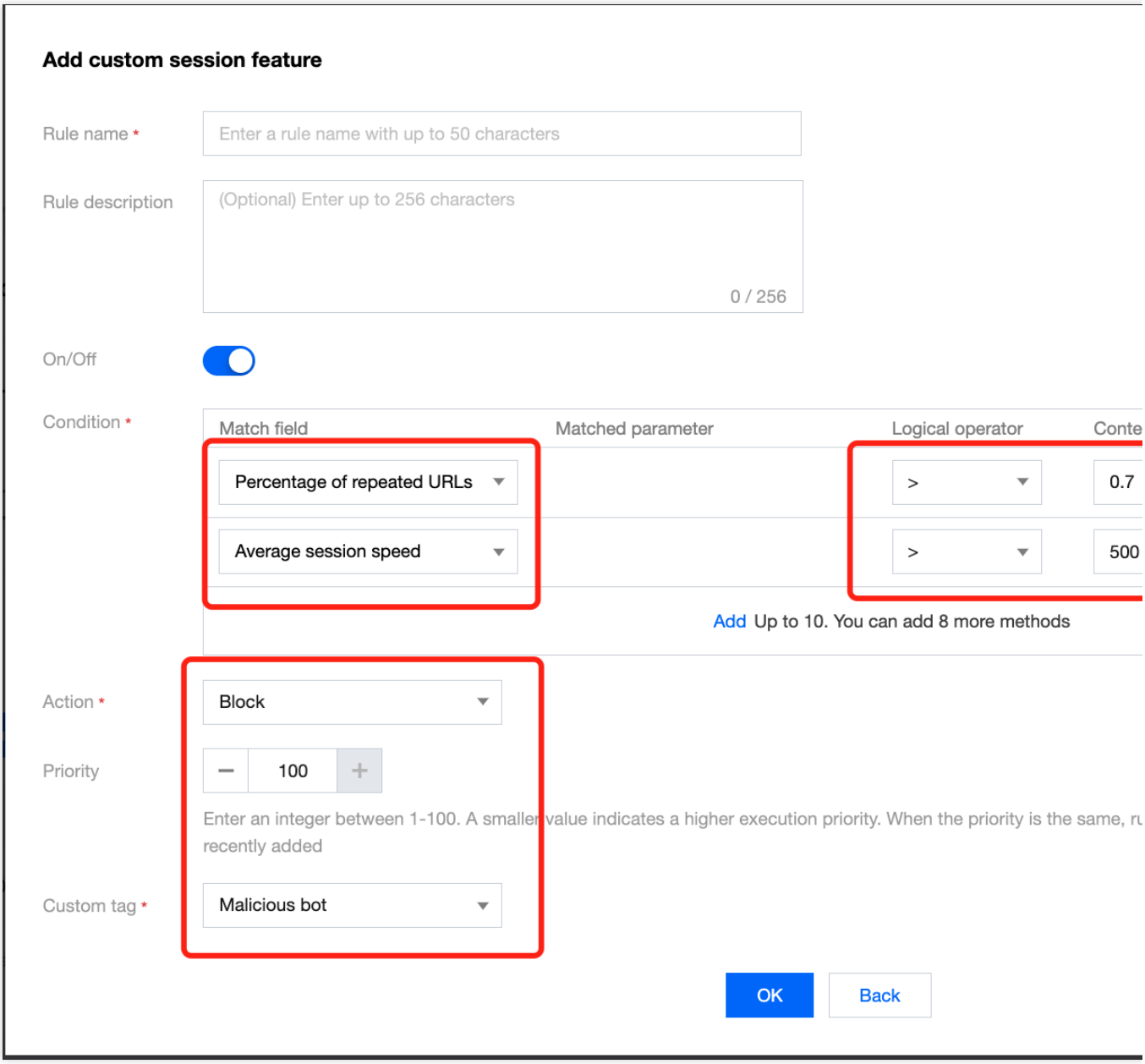


策略配置

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 单击某场景配置页，单击**自定义规则**。
4. 在自定义规则页面，单击**添加配置**，根据上述分析，将设置 URL 重复比大于0.7（70%在这过程中，除该数据外没有大于70%的），将会话速度设置为大于500次分钟，单击**确定**。



注意：

目前在创建 BOT 场景化时，已经根据场景类型内置相应场景的自定义规则集。

API安全相关
WAF 结合 API 网关提供安全防护

最近更新时间：2023-12-29 14:52:59

本文档将介绍如何配置 Web 应用防火墙（WAF），为 API 网关上的 API 提供安全防护。

前提条件

已开通 Web 应用防火墙。
已在 API 网关上发布了 API，详情请参见 快速入门。

操作步骤

步骤1：在 API 网关控制台绑定自定义域名

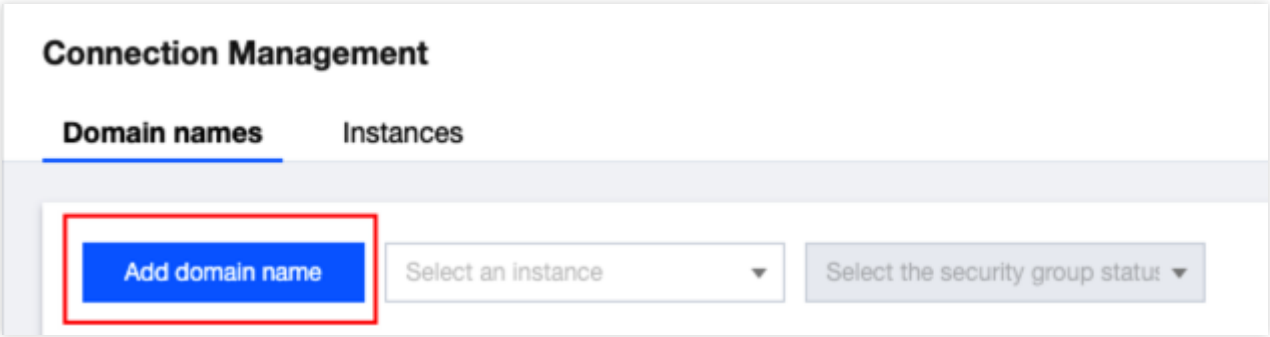
参考 配置自定义域名 文档，在 API 网关控制台绑定自定义域名。

注意

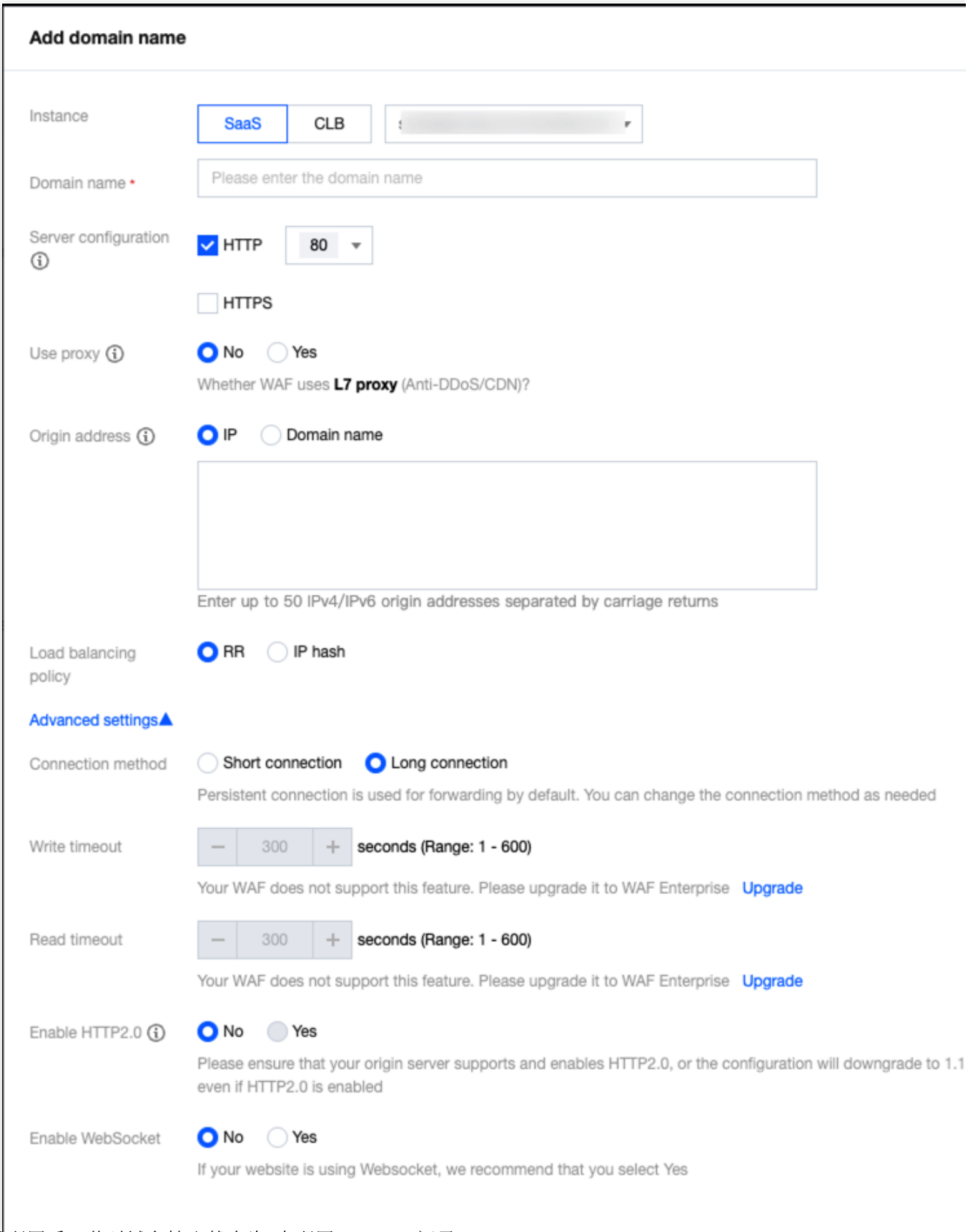
API 网关绑定自定义域名时，会校验自定义域名是否解析（通过 CNAME）到该服务的子域名。因此，您必须先将自定义域名解析（通过 CNAME）到 API 网关服务的子域名并配置绑定成功，再修改 DNS 记录，将自定义域名指向 WAF 的 CNAME 域名。

步骤2：配置 WAF

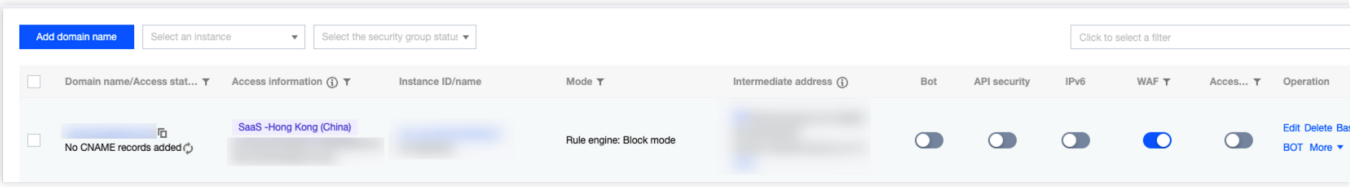
1. 登录 Web 应用防火墙控制台，在左侧导航中，选择**接入管理**。
2. 在域名接入页面，单击**添加域名**。



3. 在添加域名页面，配置相关参数，单击**确定**。



4. 完成配置后，此时域名接入状态为“未配置 CNAME 记录”。



步骤3：修改 CNAME 记录

1. 在 DNS 提供商中修改 CNAME 记录，将自定义域名指向 WAF 的 CNAME 域名。
2. 登录 Web 应用防火墙控制台，选择**接入管理**，进入域名接入页面，即可看到正常防护的界面。

API 容量保护

最近更新时间：2023-12-29 14:53:12

为什么要对 API 进行容量保护？

由于 API 是面向程序自动化调度所设计的，因此容易受到自动化调度引发的网络攻击。
攻击者会试图重放并自动填充不同认证凭据的业务流量攻击，导致相关业务敏感数据的泄露造成业务损失。
利用自动化工具发起 Layer-7 的 DOS 攻击，通过不断地发起相关业务请求，通过高频次的调度占满服务器的带宽及上下游的计算、存储资源，造成业务平台不稳定。
攻击者通过利用自动化模糊测试的工具，对业务进行定向攻击绕过测试，用于绕过定向的安全防护。
攻击者通过编写自动化编程工具，将有资源额度的相关 API 进行资源耗尽攻击。

可以分为如下四个模块，对 API 进行业务防护。
API 容量防护
API 安全防护
API 资产管理
API 生命周期管理
本文将从 API 容量保护角度进行梳理。在开发的生命周期内，API 的开发运营人员在进行 API 开发及维护时，可以通过使用**缓存、降级、限流**措施用来保护及提高 API 系统容量的稳定性。
缓存
降级
限流
提升系统访问速度和增大系统处理容量。
当服务出现问题或者影响到核心流程时，需要暂时屏蔽掉 API 的访问，待高峰或者问题解决后再打开。
通过对并发访问/请求进行限速，或者对一个时间窗口内的请求进行限速来保护系统，一旦达到限制速率则可以拒绝服务、排队或等待、降级等处理。
上述三种有效的防护手段措施可以在开发、运营部署的过程中进行实现，但是会消耗大量的人力资源成本及开发成本。并且在整个 API 安全的生命周期中，需要对所有的 API 资产进行对应的 API 容量保护。
因此需要对每一个 API 接口进行特定的业务改造，这个时候工程量就会呈指数级上涨。可以采用如下方式来对业务 API 进行快速的容量保护。

如何对 API 进行容量保护？

对 API 进行容量保护时，除了上述部分中描述的**缓存、降级、限流**可以通过自己开发运维外，还可以通过 Web 应用防火墙中的相关模块进行定向的 API 容量保护，本文将会以如下9种可在 Web 应用防火墙中保护的方法进行定向

API 的快速容量保护。

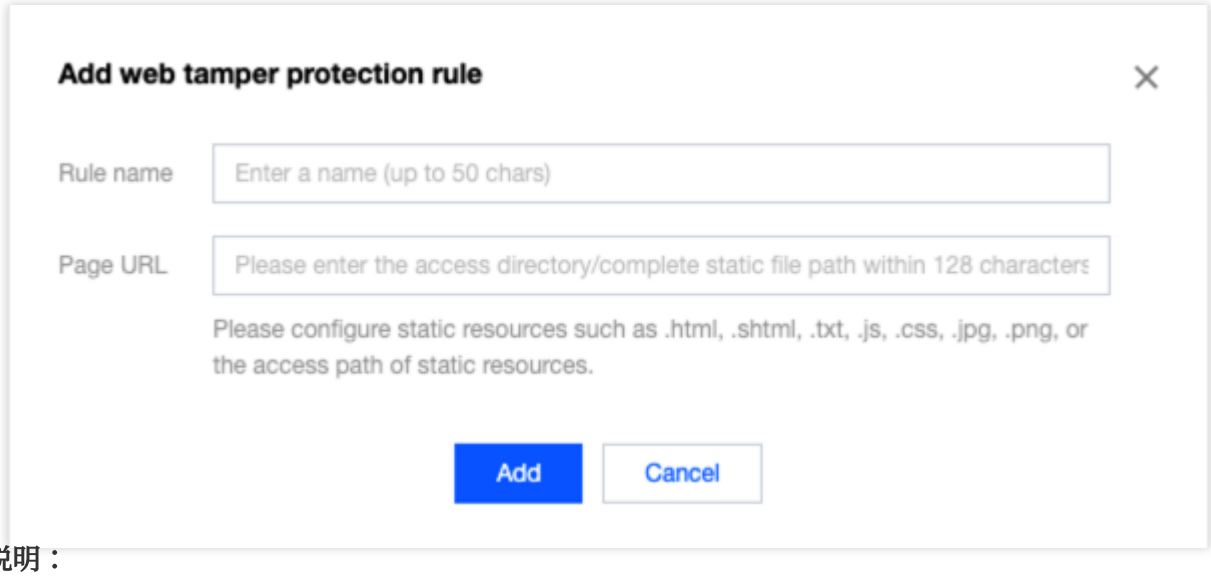
防护细项	防护实践内容
API 内容缓存	静态 API 资源缓存
API 访问降级	阻断 API 的异常流量保护业务系统稳定
API 限流	限制 API 整体访问请求流速
API 客户端调度访问限速	限制客户端调度 API 的访问速度
API 敏感调用保护	保护敏感 API 接口调度不被滥用，保证业务数据不被外泄
API 资源调用保护	保护 API 强资源消耗接口调度不超限额
关键 API 调用保护	在调度关键 API 的时候进行2fa/mfa/人机识别
API 验签保护	验证客户端是否为真实客户端进行访问
API 异常访问源调度保护	保护 API 不被异常的访问资源访问

API 内容缓存

由于公共 API 的返回接口内容较为频繁，消耗资源较大，如果 API 返回内容在一段时间内都不会持续的更新，那么就可以对 API 的相关内容进行缓存，减少 API 服务端的计算资源、带宽资源的损耗。

此处可以使用 Web 应用防火墙中的 基础安全 > **网页防篡改**模块对 API 内容进行快速缓存，对业务 API 进行特定的数据缓存，帮助业务系统快速内容缓存。

1. 在网页防篡改页面，单击**添加规则**，弹出添加防篡改规则弹窗。
2. 在添加防篡改规则对话框中，填写相关字段，设置完成后，单击**添加**。



字段说明：

规则名称：防篡改规则名称，最长50个字符，可以在攻击日志中按照规则名称进行搜索。

页面路径：防篡改路径，需要进行防篡改保护的 URL，需要指定详细 URL，不支持路径配置。

说明

指定页面仅限于.html、.shtml、.txt、.js、.css、.jpg、.png 等静态资源。

添加规则后，用户第一次访问该页面，WAF 将会对页面进行缓存，后继访问的请求为 WAF 缓存页面。

3. 完成的防篡改规则后，规则默认启用。

API 流速限制

对 API 的流速限制分为两个部分：

对服务端 API 整体的流速限制

如果对服务端进行整体的 API 限速限流，容易导致部分客户端无法访问到业务信息。由于恶意流量在攻击时，流量数据会比较大，如果通过 API 后端服务限速，大多数访问流量信息基本都为异常访问用户，正常访问用户很少，容易造成大量正常用户的客诉。因此，建议对**客户端的调用进行流速限制，可以通过对客户端的限频或限速，来实现对 API 流速的限制**。

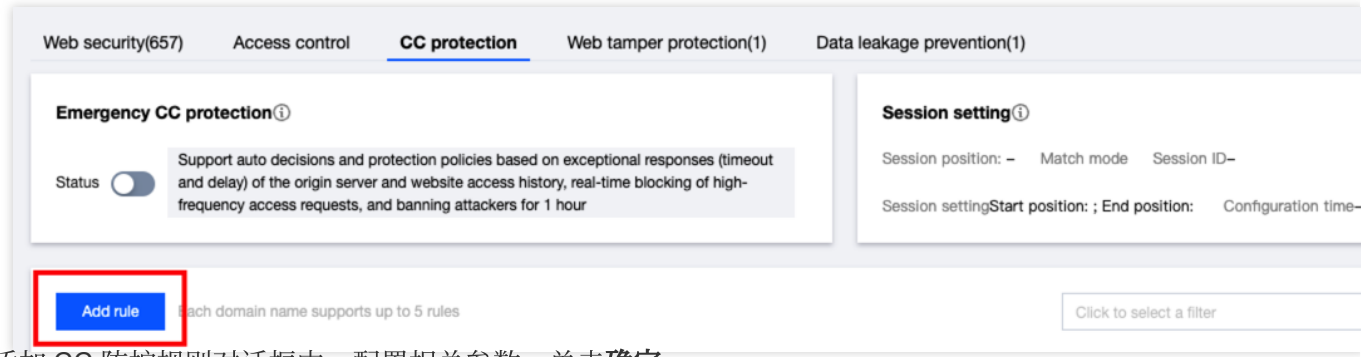
对客户端调用的流速限制

在 Web 应用防火墙中的，可以通过 CC 防护设置、BOT 管理进行对客户端的限流。

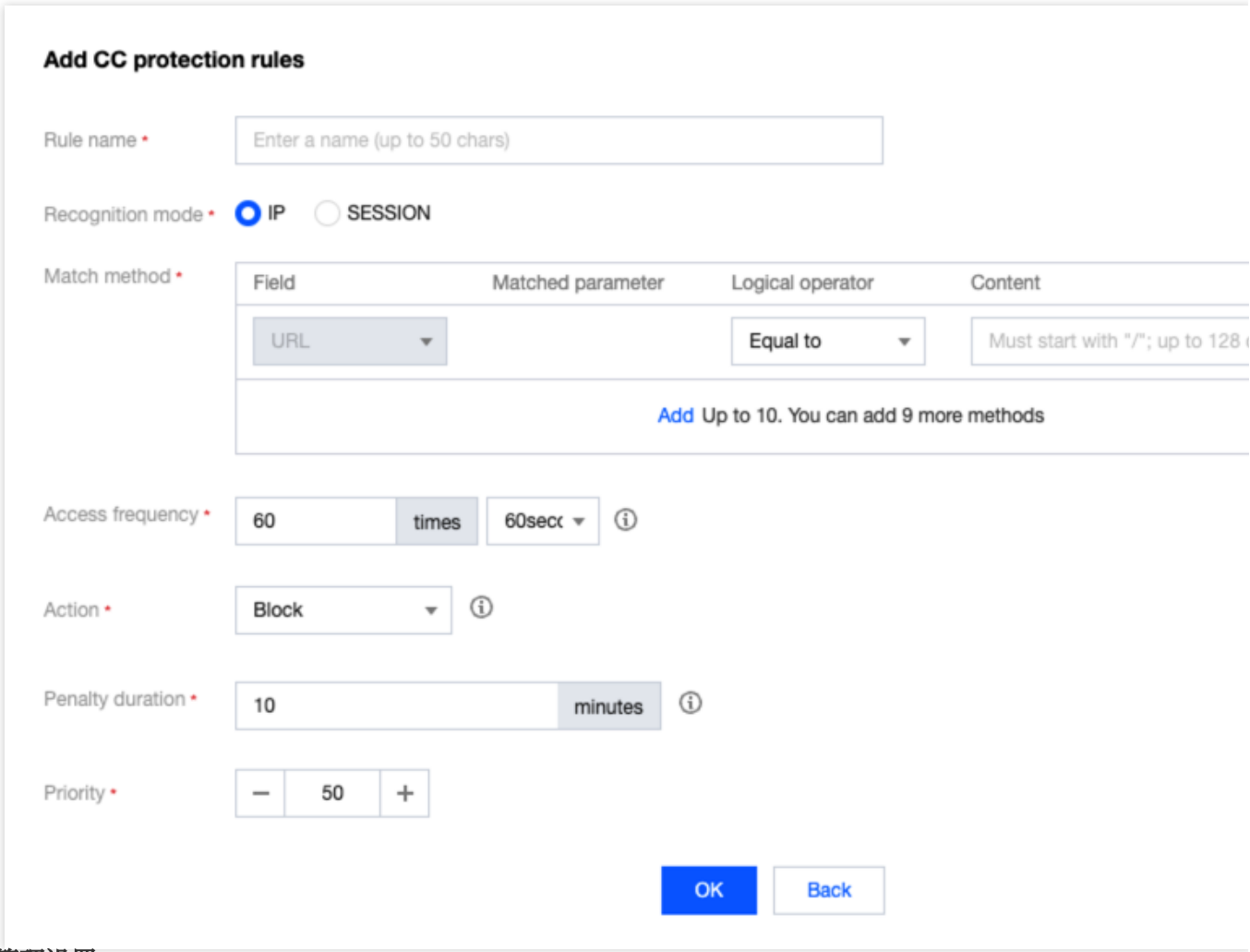
CC 防护设置

CC 防护功能可配置每个客户端的整体的访问频次，一旦客户端的访问频次超出限制的预期，则对其进行相关处置。

1. 在 CC 防护页面，单击**添加规则**。



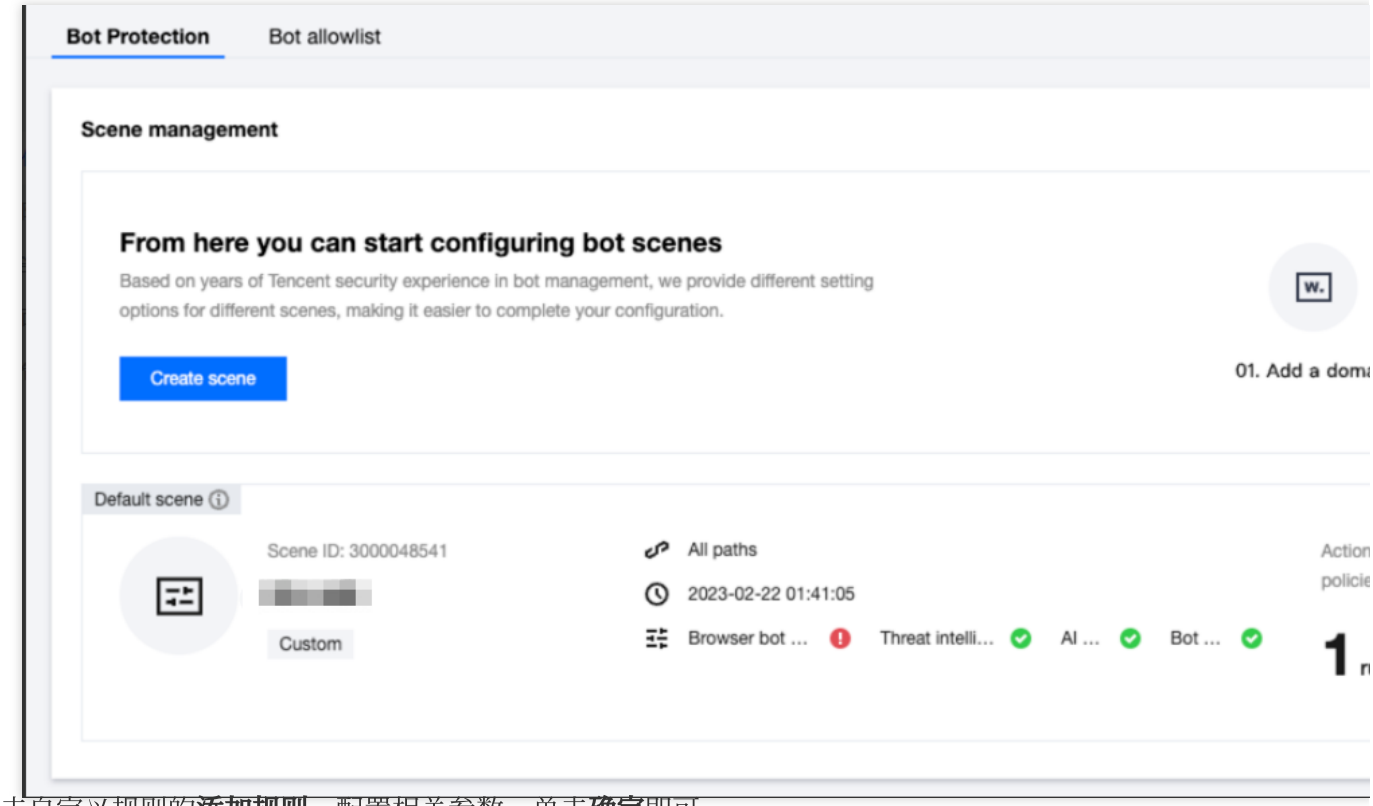
2. 在添加 CC 防护规则对话框中，配置相关参数，单击**确定**。



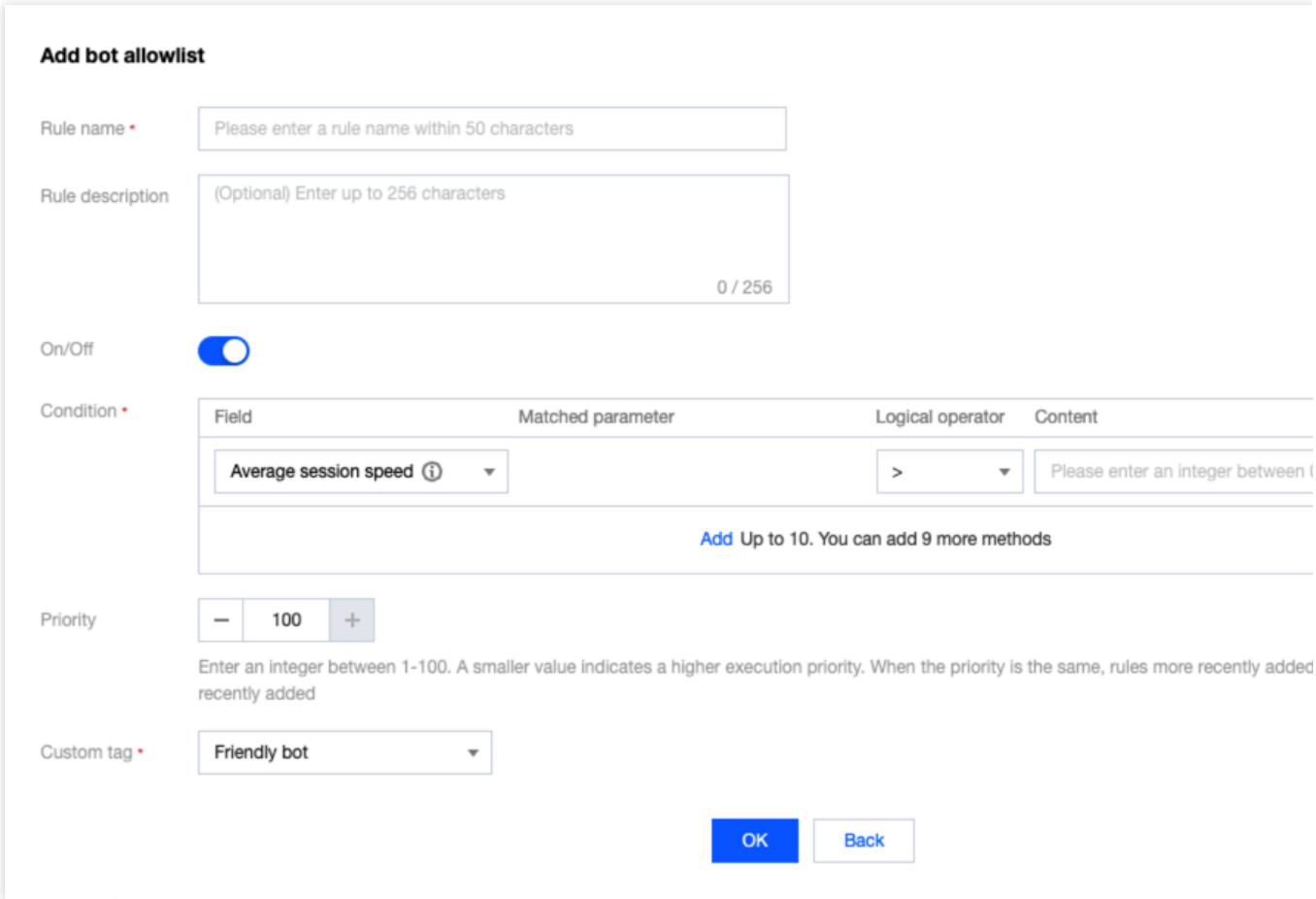
BOT 管理设置

通过配置 BOT 管理 > **BOT 防护**页面的会话平均速度条件，可以控制每个客户端的会话持续访问速度。

1. 在 BOT 防护页面的场景化管理模块，单击目标场景的**查看配置**。



2. 单击自定义规则的**添加规则**，配置相关参数，单击**确定**即可。



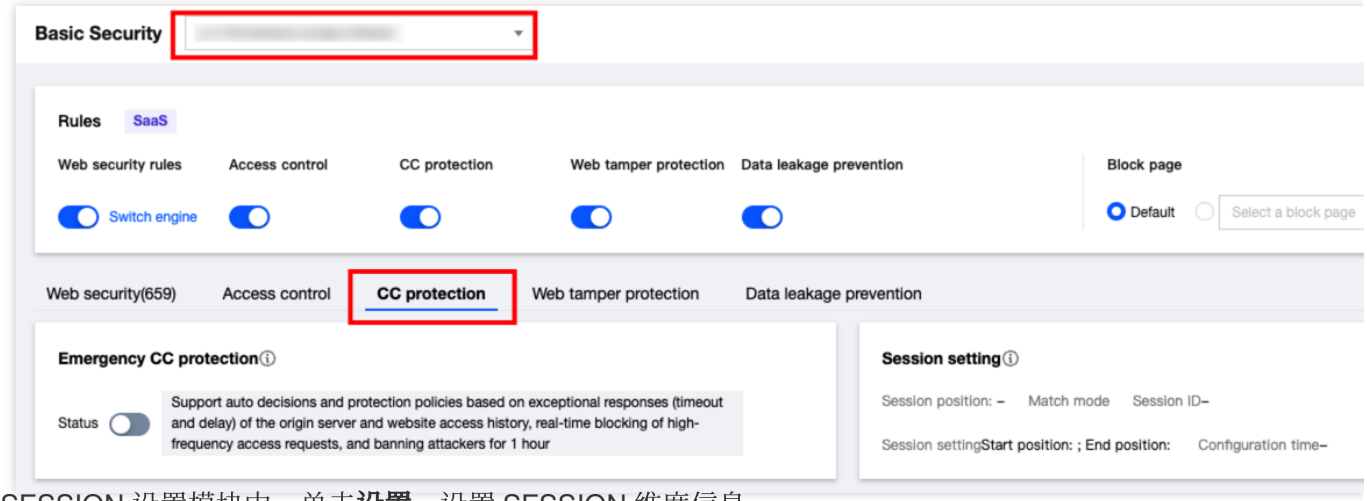
Session 设置/会话设置

由于在现网环境下，IPv4 的 IP 数量越发紧张，目前很多 IP 运营商都会将客户端放置在 NAT IP 下，即一个 IP 下面有多个业务客户端。如果单纯对业务进行 IP 的限速，在面对 NAT IP 的情况下，容易触碰到业务配置的 IP 限频策略，导致误拦截的现象。如果业务配置限频过于宽松，又会使相关业务的限频拦截无法起到限流的效果。

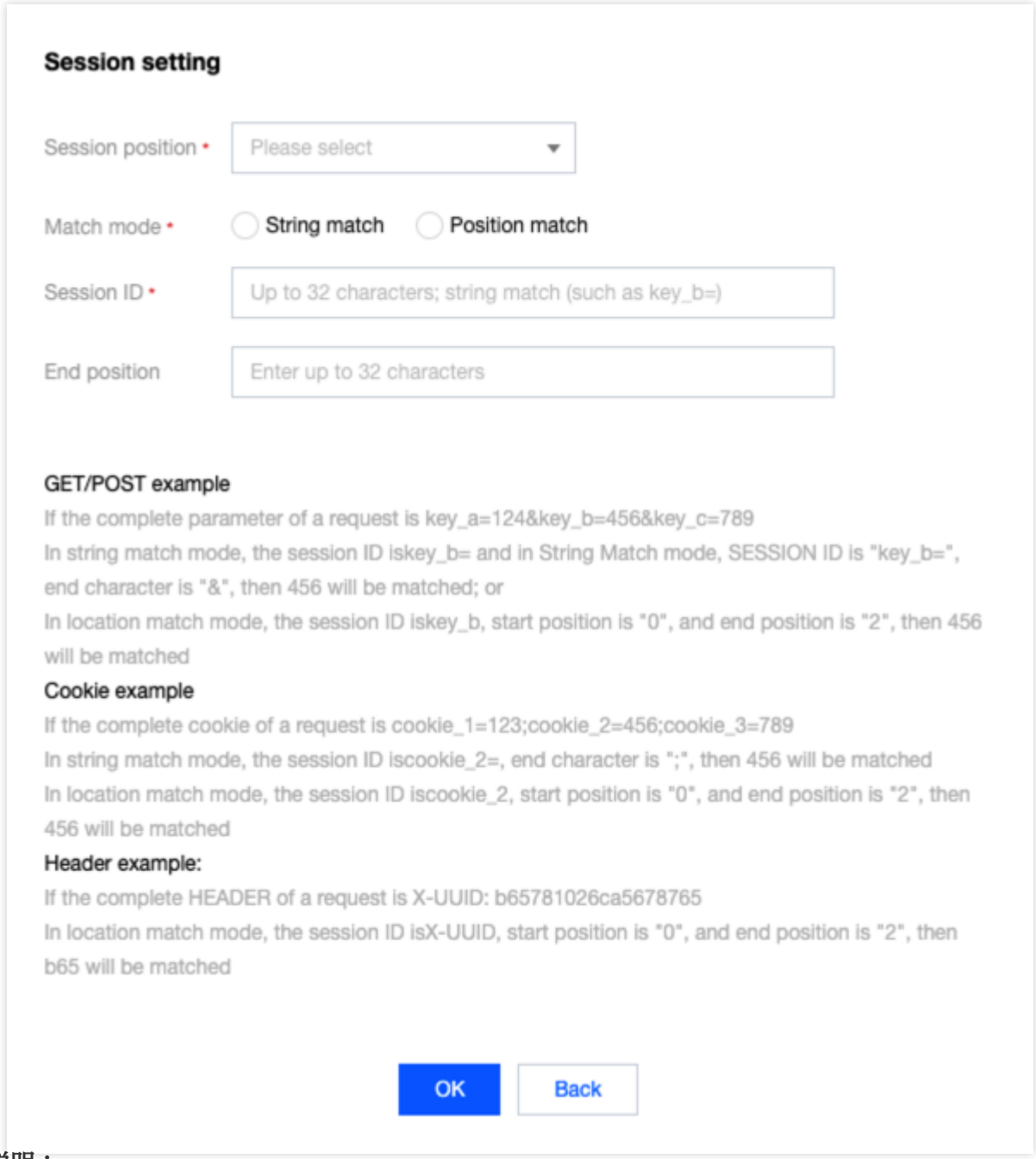
因此，可以在 Web 应用防火墙中配置 Session 设置/会话设置，既可做到**自动分辨同一 IP 下的不同客户端，实现对单一客户端的业务限频**。

Session 设置

1. 登录 Web 应用防火墙控制台，在左侧导航栏选择**基础安全**。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **CC 防护**，进入 CC 防护页面。



3. 在 SESSION 设置模块中，单击**设置**，设置 SESSION 维度信息。
4. 在 SESSION 设置对话框，配置相关参数，单击**确定**。



参数说明：

SESSION 位置：可选择　HEADER、COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。

匹配模式：除　　HEADER 模式（仅支持位置匹配）外，均支持选择字符串模式匹配或位置匹配。

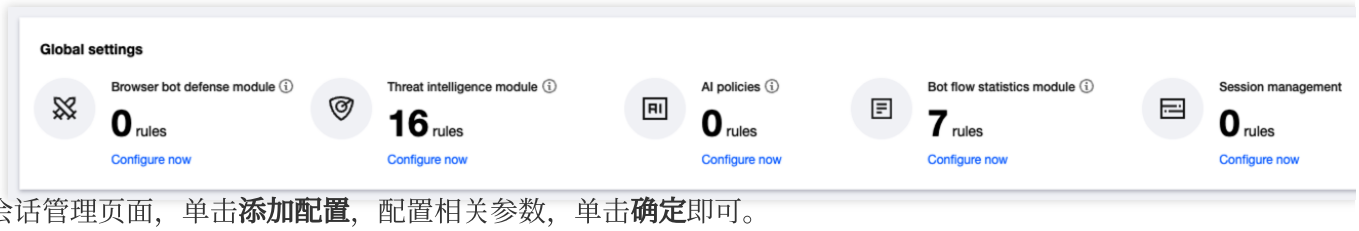
SESSION 标识：取值标识，32个字符以内。

开始位置：字符串或位置匹配的开始位置，1-2048以内的整数，并且最多只能提取128个字符。

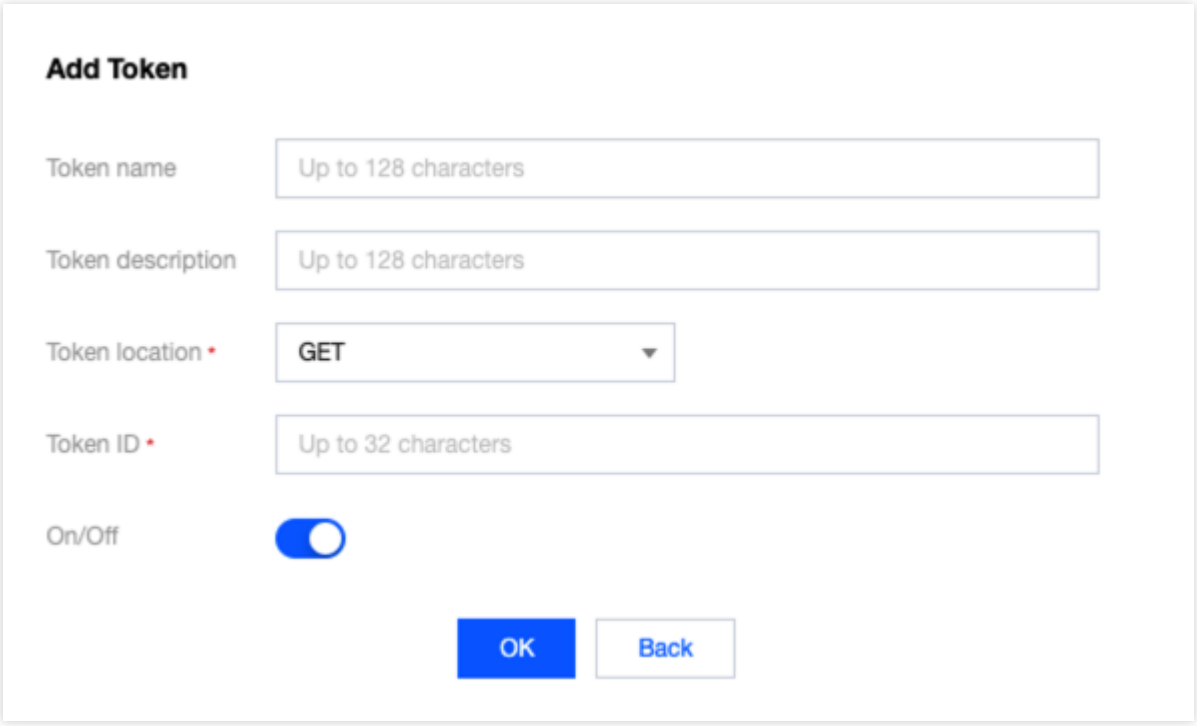
结束位置：字符串或位置匹配的结束位置，1-2048以内的整数，并且最多只能提取128个字符。

会话设置

1. 在 BOT 管理 > **高级设置**模块，单击会话管理的**前往配置**。



2. 在会话管理页面，单击**添加配置**，配置相关参数，单击**确定**即可。



说明

会话管理应为可持续性跟踪 tokenid ， 例如登录后的 set-cookies 的值。

参数说明：

Token 位置： 可选择 HEADER、COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。

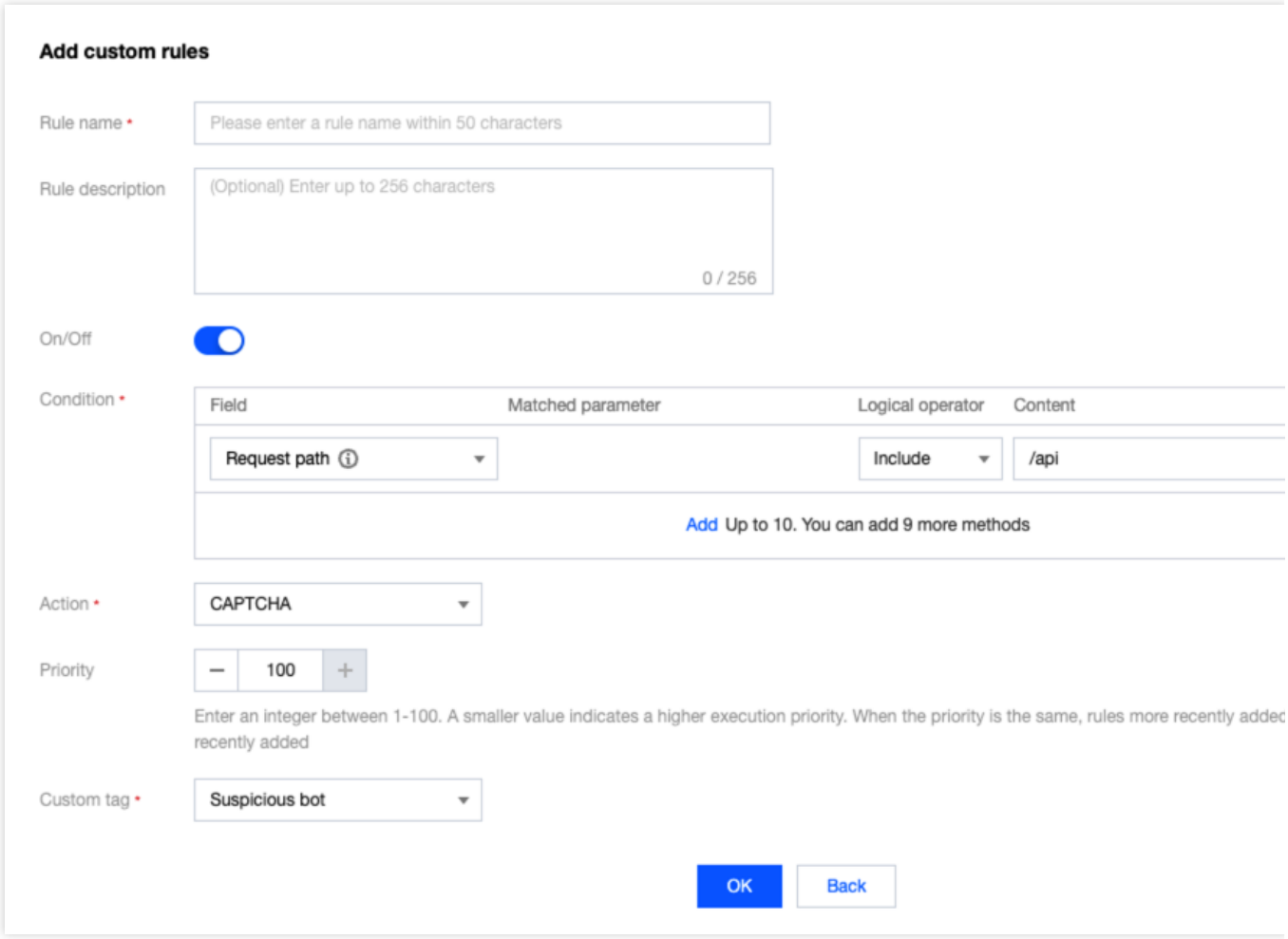
Token 标识：取值标识。

控制客户端的 API 调用

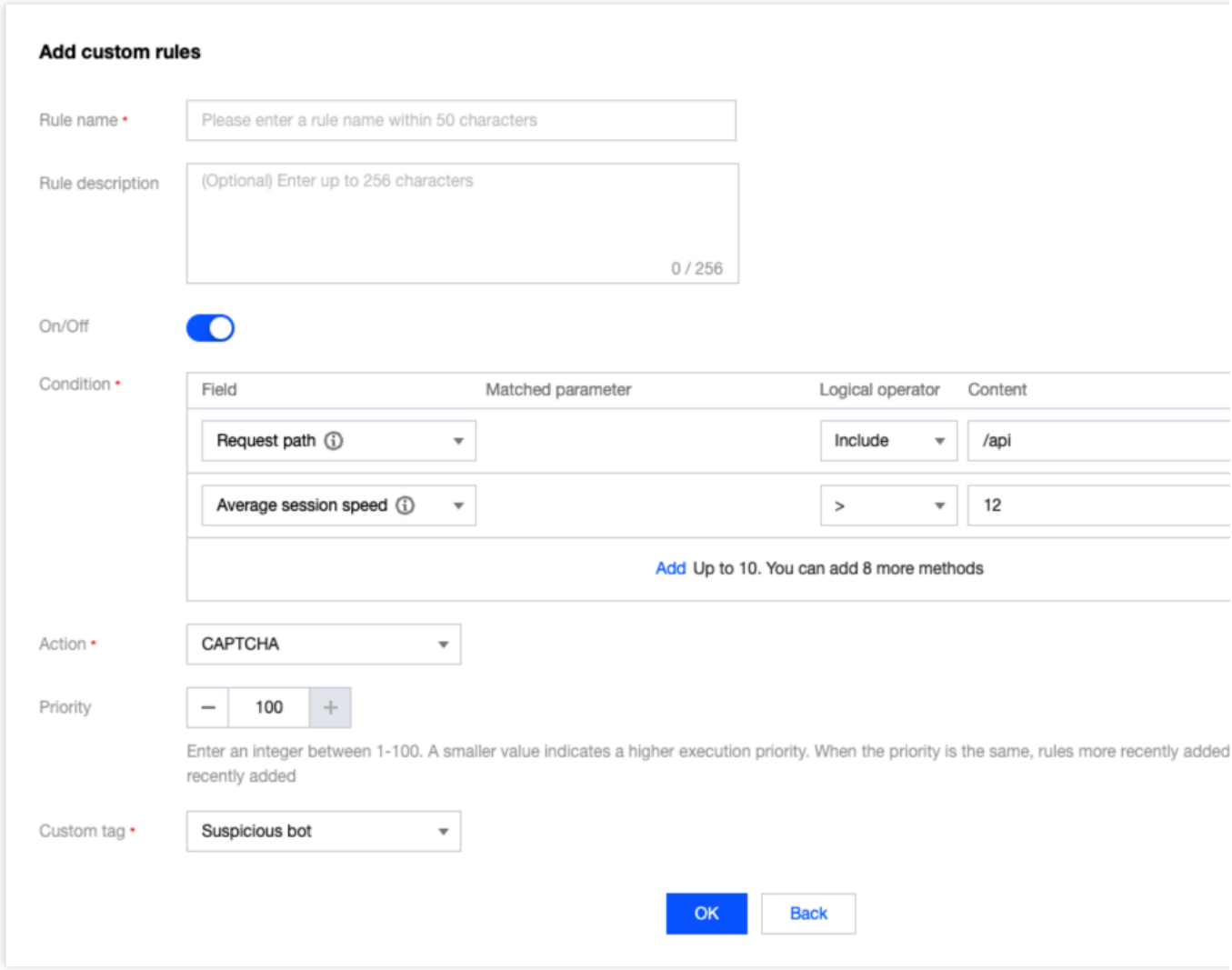
每一个敏感的 API 都有应该存在调用次数限制，例如：在短信 API 服务中，如果不对其进行相关限制，攻击者会滥用 API 接口，消耗短信资源包，造成超额的计费账单。如果敏感 API 接口在客户端调用前，进行 2fa/mfa 或人机识别等验证，可以有效减少异常 API 调度。

在 Web 应用防火墙的 BOT 管理 > **BOT 防护**页面，通过简单的配置，实现对 API、客户端的次数调用，敏感 API 调用前，对其进行敏感操作保护。

敏感 API 调度前进行人机识别



限制客户端在单一会话时间内的 API 调度总次数



如何进行客户端的 API 访问进行验签？

客户端的验签可以有很多种方式，包括但不限于：

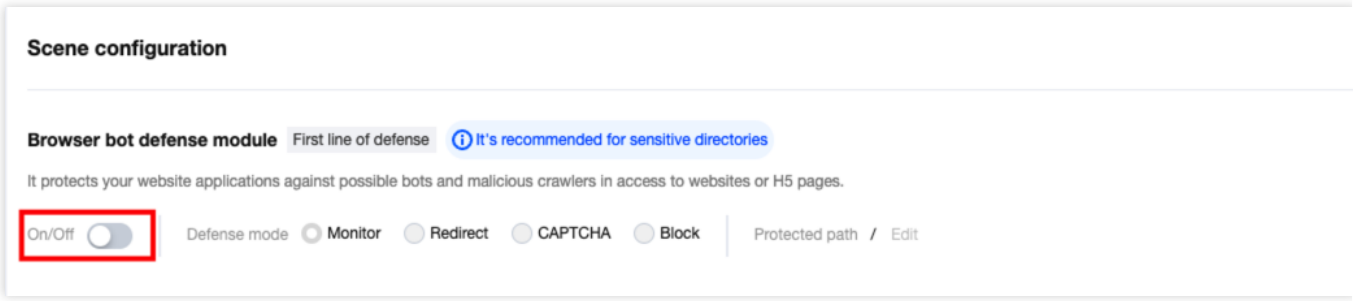
mtls。

客户端签名验证。

客户端数据挑战。

用户可以通过配置 mtls、客户端数据签名挑战等方式进行数据的加强验签。

在 Web 应用防火墙中，通过开启前端对抗功能，对客户端的 API 数据进行验签，并进行定向防重放功能。对抗 API 滥用有良好的效果，详细可以参见 客户端风险识别。


Scene configuration
Browser bot defense module
First line of defense
It's recommended for sensitive directories
It protects your website applications against possible bots and malicious crawlers in access to websites or H5 pages.
On/Off
Defense mode
Monitor
Redirect
CAPTCHA
Block
Protected path
/
Edit

API 数据防护与加固

最近更新时间：2023-12-29 14:53:24

API（Application Programming Interface）应用程序接口，可以应用于所有计算机平台和操作系统，以不同的格式连接数据调用数据，用户可以跟踪电商平台购买的货物位置，就是电商平台与物流公司之间使用了 API 位置实时调用产生的效果。

许多组织更关注于快速的 API 和应用程序交付，而忽视了 API 安全保护，这也是近几年来 API 攻击和数据泄露的主要原因。

API 的调用场景可分为如下三种类型：

API 类型	API 描述	安全现状
公开 API	支持任何人从任何地方访问服务，被暴露在互联网中，调用方可根据相关接口，提供相关字段的数据，即可完成相关数据、流程的调度。公开 API 对安全性、使用性的监控、处置程度最高。	网络限制少，可能存在相关认证等授权的限制，但是相关业务鉴权逻辑漏洞也更为频发，攻击者更加偏爱对此类 API 通过自动化模糊测试、定向安全测试等方式进行定向攻击及绕过。
内部 API	通常在数据中心或私有云网络环境中部署和运行，以运营管理、内部服务支撑为主。通常用于用户的内部之间的快速调度及使用，通常不暴露在外网	网络限制较大，可能存在相关鉴权等操作，通常校验力度较低，安全防护力度较低，攻击者如果发现并嗅探到了此类内部 API 接口，就会针对此类 API 接口进行定向攻击。在多起数据泄露事件中， 对内部 API 的攻击、是导致泄露的罪魁祸首。
渠道 API	通常在数据中心或私有云网络环境中部署和运行，向特定的外部合作伙伴、供应商提供对内部 API 的有限制的访问。 通常用于特定合作伙伴的定向数据拉取及管控，对数据拉取的敏感度低，但对数据外泄的敏感程度较高。	访问程度控制权位于内部和外部 API 之间，安全管控层级也是一样，主流手段是通过 API 网关管控，但缺少安全方面的考虑。很少对此类 API 进行相关越权方面的业务管控。如果上下游供应链上的合作伙伴被入侵进而调度相关的 API 进行数据滥用，在渠道 API 上通常会缺少滥用的监控监管机制，因此多起数据泄漏事件就因为没有对渠道 API 进行滥用管控造成的。

为什么要做 API 敏感数据发现

据《Salt Labs State of API Security Report, Q1 2022》报告，在受访者最关心的 API 安全问题中，僵尸 API 以43%占比高居第一；远超过以22%的占比位居第二的账户接管/滥用；还有83%的受访者对组织 API 资产清单是否完整没有信心。

为何企业对 API 资产有如此大的担忧？安全隐患往往藏于“未知”，未知的僵尸 API、未知的影子 API、未知的敏感数据暴露等，根源都在于企业对 API 资产全貌的未知。安全的管理与防护始于“已知”和“可见”，人们难以掌控那些被遗忘的、看不见摸不着的资产安全状况。然而正是这些被人遗忘、不可管控的 API，往往会有相关敏感数据在上面运行，如果没有办法及时的发现这些敏感的 API 接口则会导致相关 API 数据被拖取或意外暴露的情况，攻击者很有可能就会通过此类 API 接口对业务敏感数据进行定向发现及攻击，紧接着进行相关敏感数据拖取，更有甚者会进一步的扩大 API 攻击的利用权限，对服务器、数据库的权限进行进一步获取。从而导致页数受损。

即便是企业已经开始重视并着手治理僵尸 API 问题，也仍有一处容易被忽略的巨大风险——僵尸参数。不同于那些被彻底遗忘的僵尸 API，这些僵尸参数有可能还存在于当前仍在服务且持续维护的 API 接口中。常见的僵尸参数，例如在开发测试周期内设置的调试参数、系统属性参数，它们在接口正式上线后未对外暴露给用户，但仍能被暗处的攻击者恶意调用。攻击者基于僵尸参数，能够利用批量分配等漏洞获得越权的响应。一旦这些未知的 API 脆弱点被恶意利用，背后的核心业务数据、平台用户数据等海量敏感数据在黑客面前就变成了内部 API 调用，没有任何安全管制，再无秘密可言。

操作步骤

步骤1：发现 API 资产

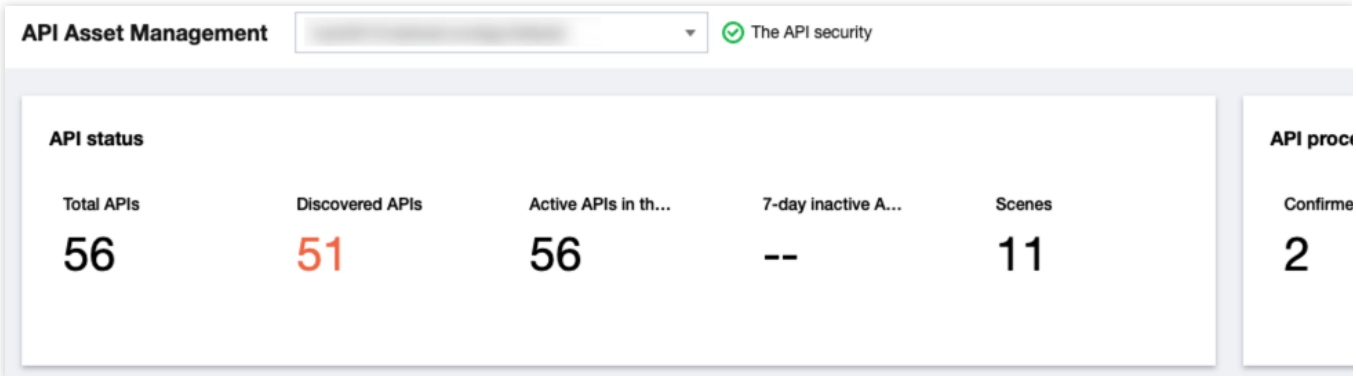
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择 **API 流量分析**。

说明

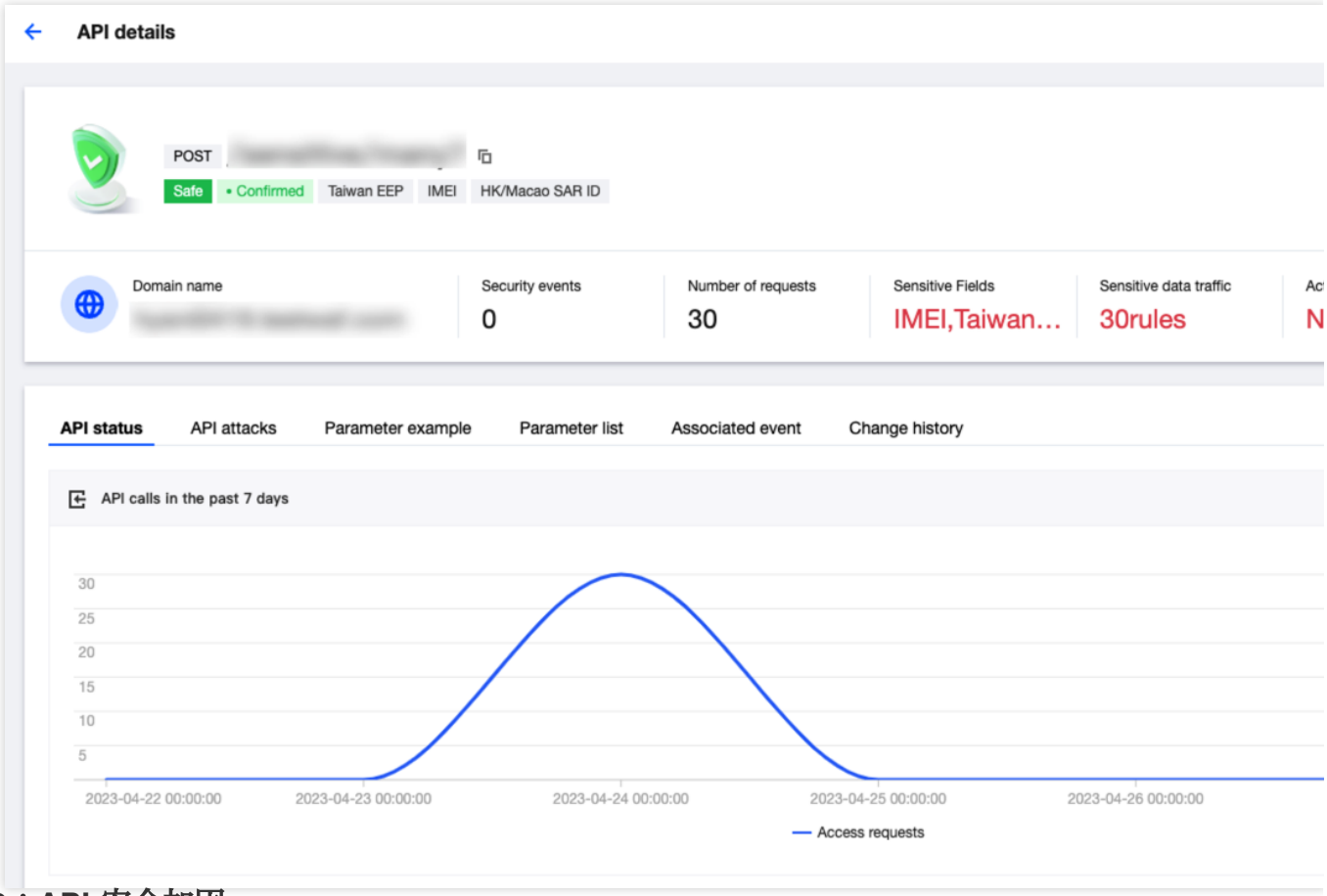
API 流量分析功能当前处于公测中，支持 提交工单 或联系商务经理申请试用该功能，公测期间仅支持开启3个域名。

2. 在 API 流量分析页面，左上角选择需要防护的域名，并单击开启是否开启分析的

。

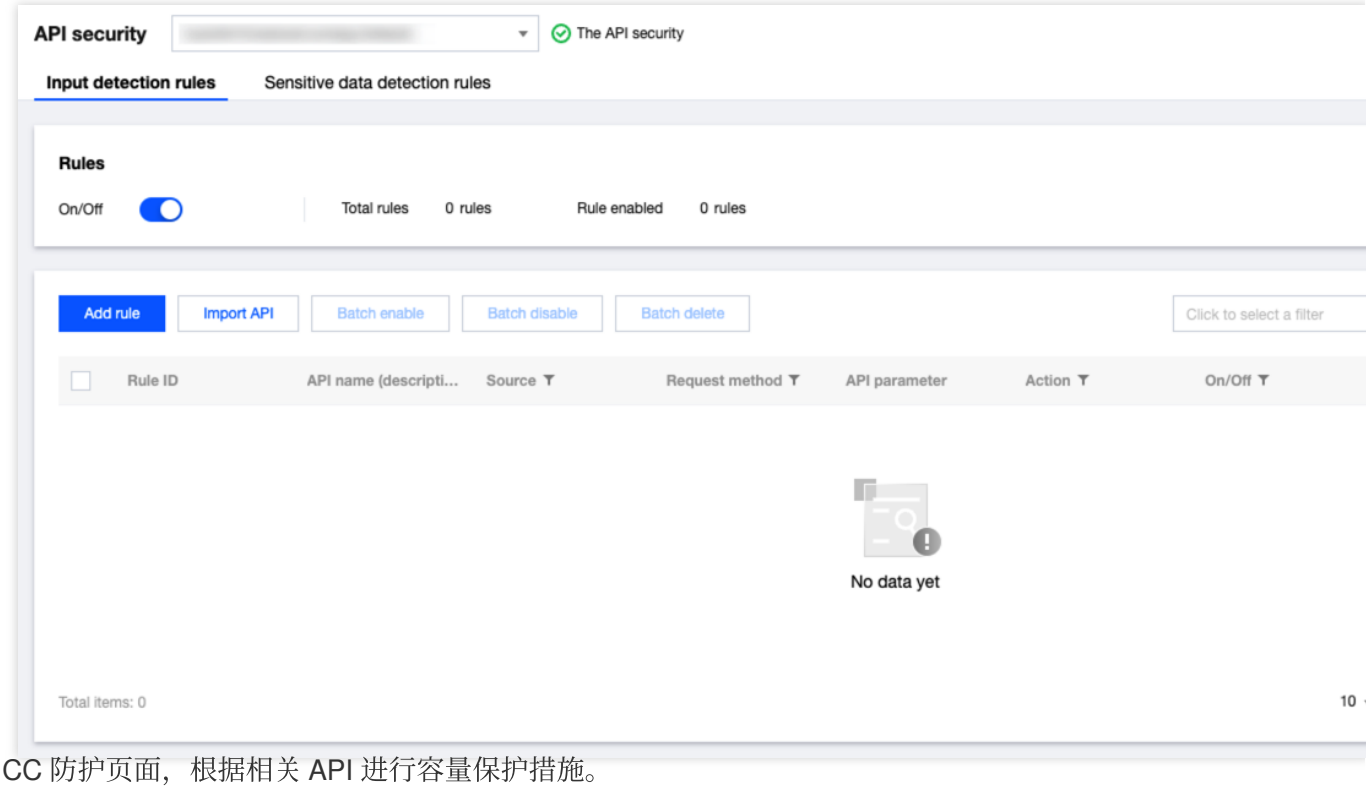


3. 开启开关后，即可在相关 API 详情页查看对应 API 的相关详情信息。

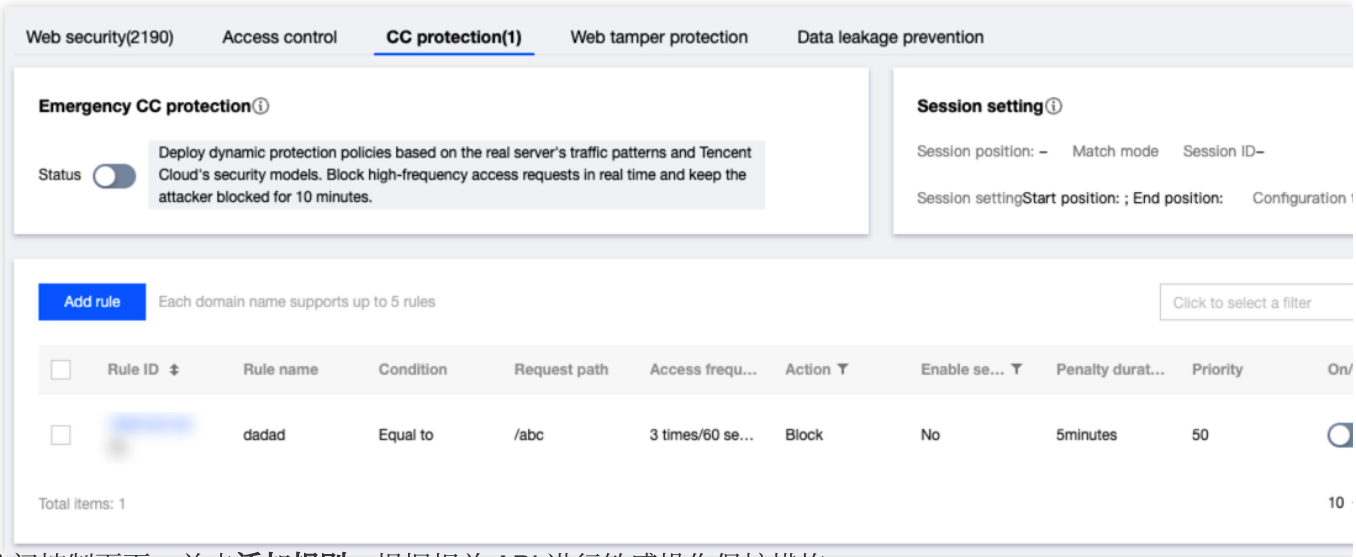


步骤2：API 安全加固

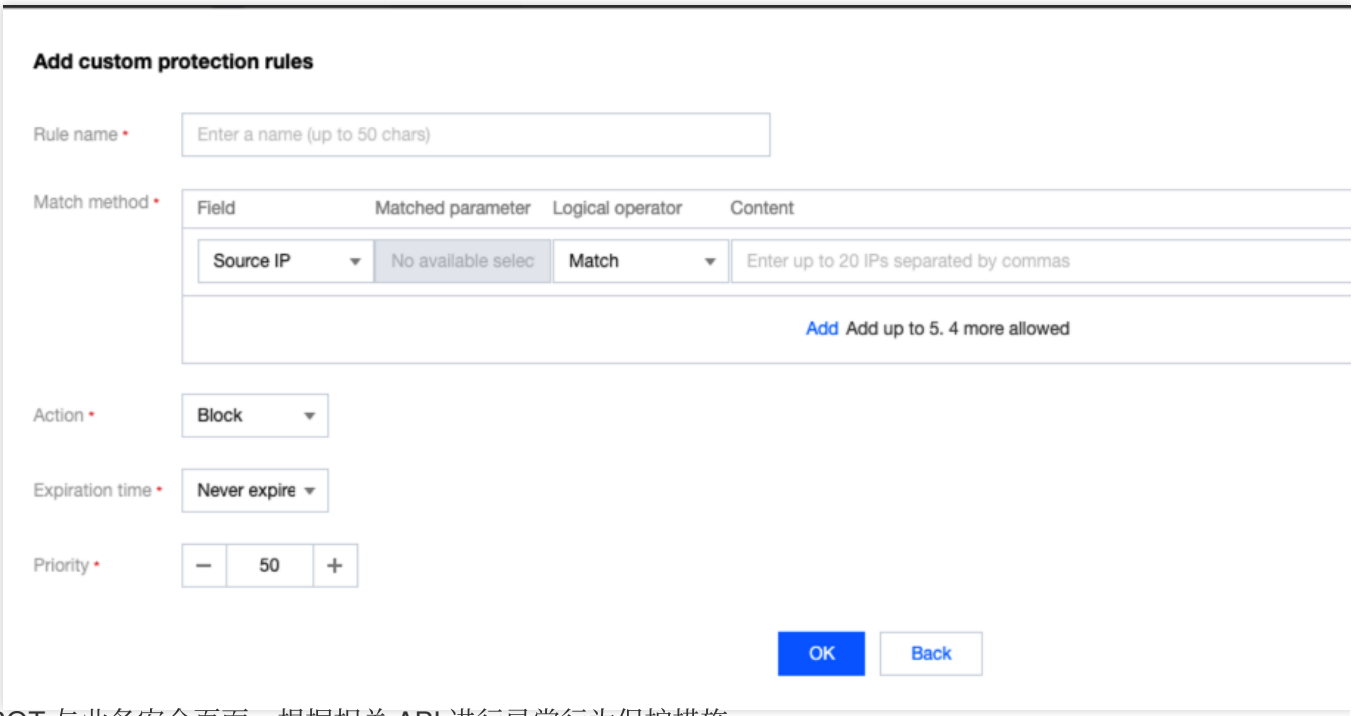
1. 在 API 安全页面，根据相关 API 进行 API 合法性加固。



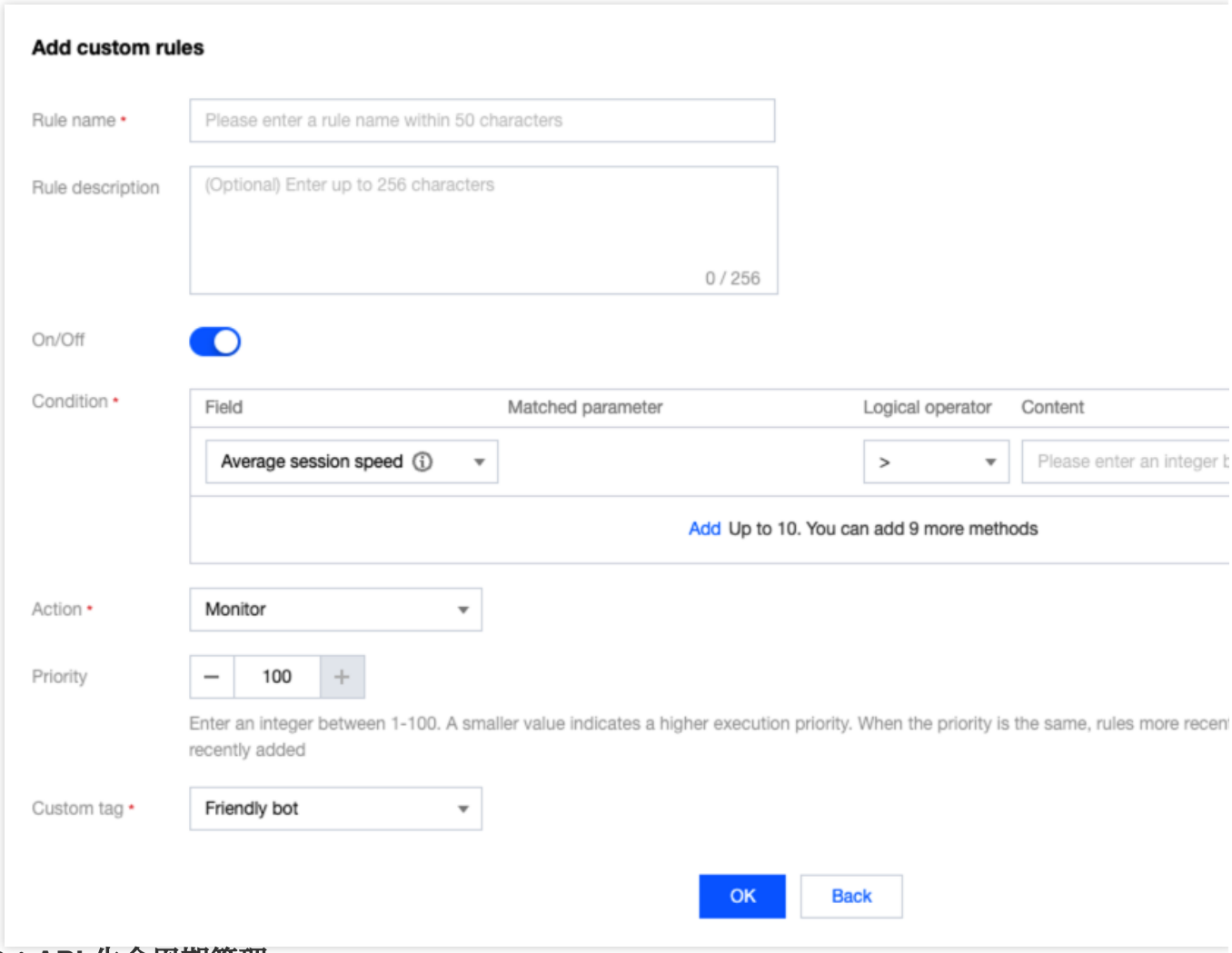
2. 在 CC 防护页面，根据相关 API 进行容量保护措施。



3. 在访问控制页面，单击**添加规则**，根据相关 API 进行敏感操作保护措施。

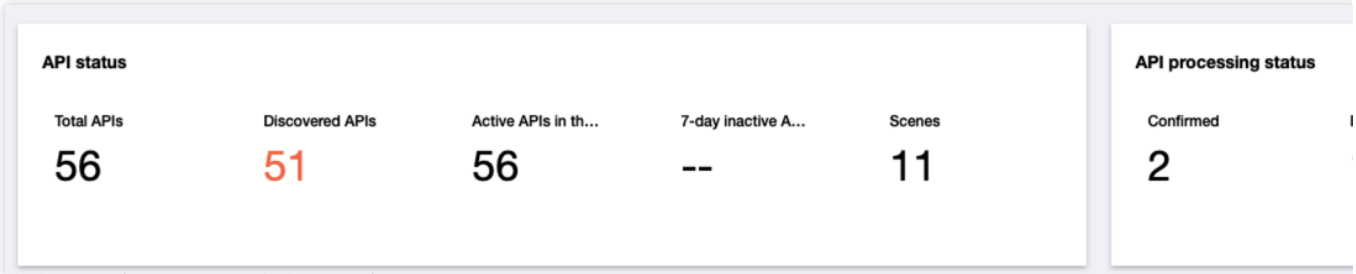


4. 在 BOT 与业务安全页面，根据相关 API 进行异常行为保护措施。

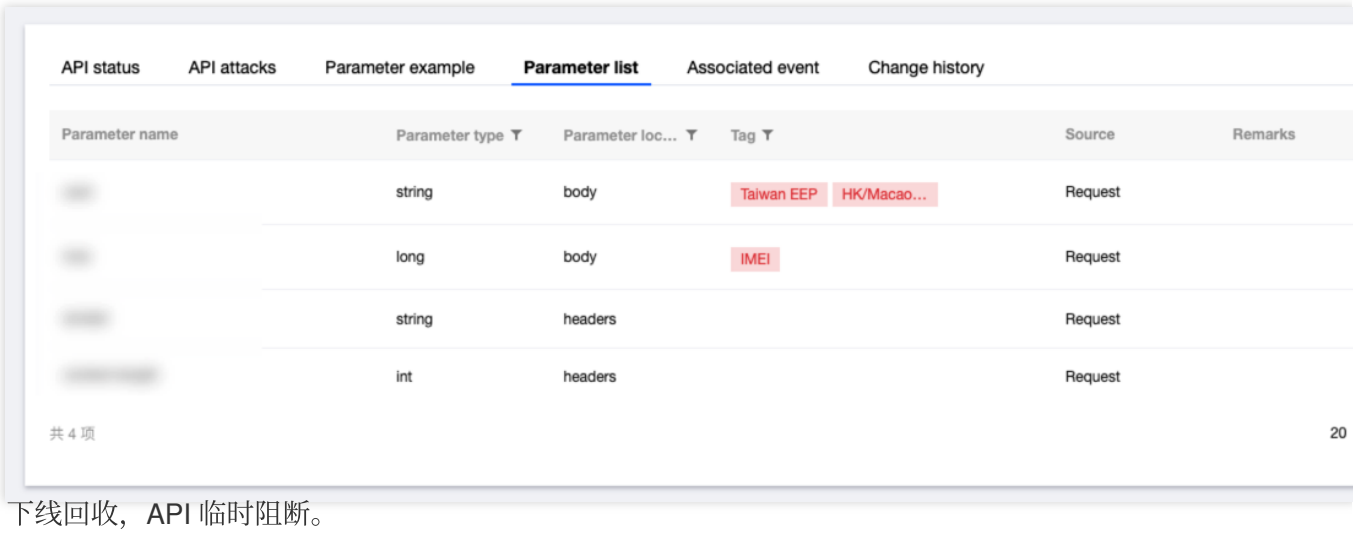


步骤3：API 生命周期管理

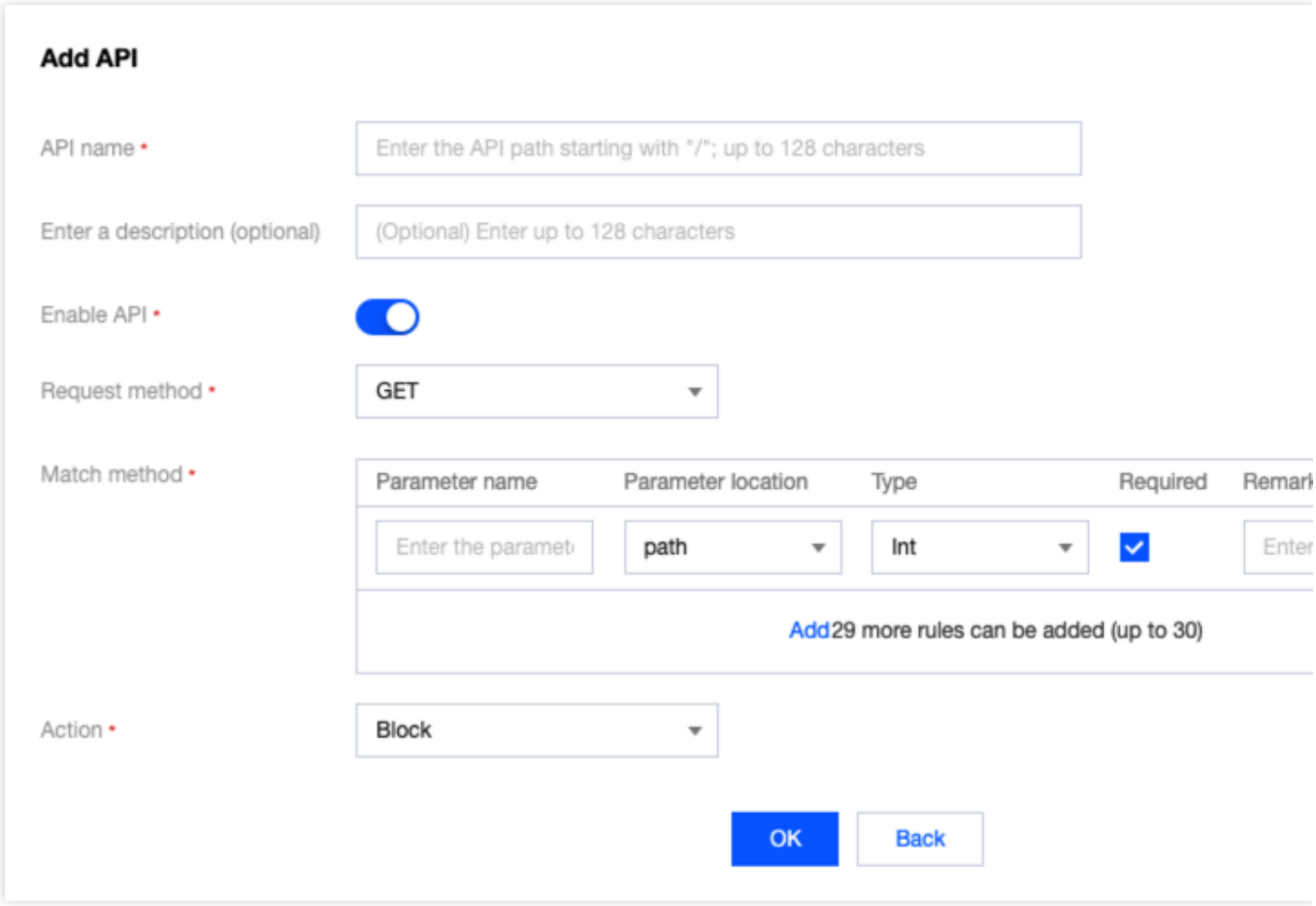
1. API 上线监测。



2. API 参数新增检测，API 参数新增检测。



3. API 下线回收，API 临时阻断。



API 暴露面管理

最近更新时间：2023-12-29 14:53:37

背景信息

API 为当今大多数数字体验提供了动力，API 安全性仍然是大多数 CISO 最关心的问题。随着各个行业的数字化转型，针对 API 的恶意威胁行为与日俱增。当前 API 的安全状态与组织的需要存在很大差距，组织经常受困于难以理解的攻击面，缺乏正确的策略来构建防御。
API 处于数字化体验的中心，移动应用、Web 网站和应用程序的核心功能、微服务架构、监管机构的要求等等，均离不开 API 的支持，根据 Akamai 的一项统计，API 请求已占所有应用请求的83%，预计2024年 API 请求命中数将达到42万亿次。与此同时，针对 API 的攻击成为了恶意攻击者的首选，相对于传统 Web 窗体，API 的性能更高、攻击的成本更低，Gartner 预测，到2022年 API 滥用将是最常见的攻击方式。之所以 API 安全问题如此严重，主要是因为 API 安全面临着如下挑战：

应用和逻辑迁移上云，暴露更多攻击面

随着云计算技术的广泛应用，越来越多的 SaaS 被迁移上云，在为更多的用户提供服务的同时，也将 API 暴露到云中，相对于传统数据中心的单点调用，东西向和南北向都可能成为 API 的攻击面。

创新强调速度和灵活，忽略构建 API 安全

敏捷开发模式是当今主流开发模式，敏捷开发强调个体和互动、工作的软件、客户合作、响应变化，虽然提升了创新速度和灵活性，但是对于如何构建 API 安全性却缺少合适的方法，导致在软件构建过程中难以顾及 API 安全。

API 接口对外不可见，引发多种攻击隐患

由于 API 是由程序员书写，除了编写代码的程序员，很少有人意识到这些 API 的存在，缺少维护的 API 经常容易被忽略，然而恶意攻击者却可以利用网络流量、逆向代码、安全漏洞等各种手段找到不设防 API 并实施攻击。

组织经常低估 API 风险，造成安全措施遗漏

人们通常会假设程序会按照想象中的过程运行，从而导致 API 被攻击的可能性以及影响被严重低估，因此不去采取充分的防护措施。此外，第三方合作伙伴系统的 API，也容易被组织所忽视。
那么要治理 API，首先就需要治理 API 资产，对 API 进行暴露面攻击面的管理。

什么是API 暴露面？

API 暴露面主要分为两个大的部分：

分类	详情

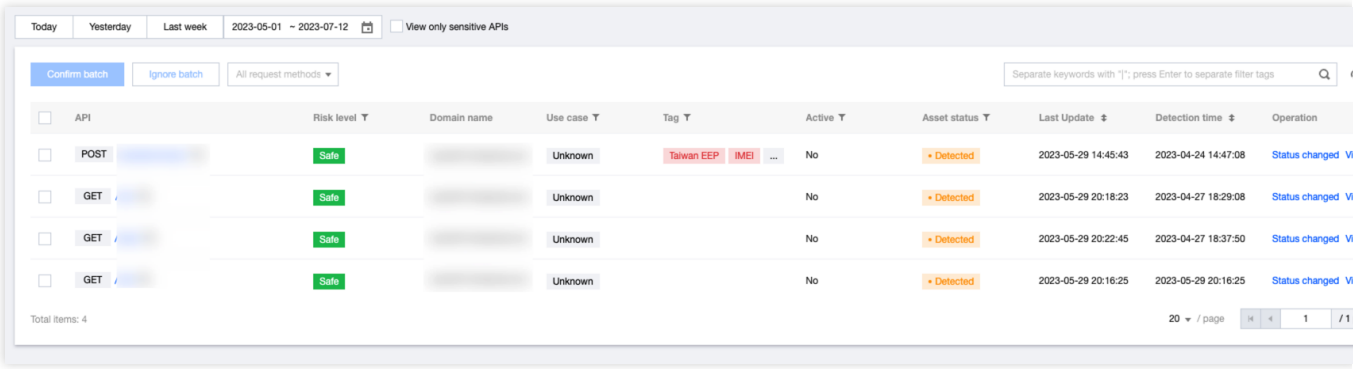
API 外部的暴露面	内部 API 暴露信息
	合作伙伴 API 暴露信息
	僵尸 API 暴露信息
	外部 API 暴露信息
	测试 API 暴露信息
API 参数的暴露面	API 敏感参数暴露
	API 后台参数暴露

其中 API 的暴露会造成内部 API、合作伙伴 API 意外暴露给攻击者，攻击者可以通过利用这些弱校验的 API 进行对应攻击，造成意外的数据泄露、API 滥用、权限外泄等意外的安全事件。
同时，在开放的 API 中，如果存在敏感、后台的 API 参数被攻击者嗅探或识别出来，攻击者可以通过这些敏感的参数信息，对业务进行定向的数据获取及 API 滥用，造成越权、数据外泄的等安全事件场景。

如何发现异常暴露面？

1. 通过自动化识别业务 API 调用关系，全面、持续清点 API 接口，包括影子 API 和僵尸 API、老版本和功能重复的 API，缩小风险暴露面。
2. 持续监测敏感数据流动，对各种敏感数据进行识别，并对敏感数据进行自定义检测，减少数据暴露面。
3. 持续动态梳理系统访问账号，多维度记录账号访问和操作行为，主动识别风险操作。

那么在异常暴露面发现的基石就是 API 的资产发现，API 的资产发现在 Web 应用防火墙中，可以通过 API 流量分析 进行对流量内的 API 进行发现及管控。要进行暴露面监测，及时了解当前网站中包含的 API 及相关敏感资产信息及其资产标签与风险、活跃状态。


Today
Yesterday
Last week
2023-05-01 ~ 2023-07-12
View only sensitive APIs
Confirm batch
Ignore batch
All request methods
Separate keywords with "|"; press Enter to separate filter tags
API
Risk level
Domain name
Use case
Tag
Active
Asset status
Last Update
Detection time
Operation
POST
GET
GET
GET
Safe
Unknown
Taiwan EEP
IMEI
No
Detected
2023-05-29 14:45:43
2023-04-24 14:47:08
2023-05-29 20:18:23
2023-04-27 18:29:08
2023-05-29 20:22:45
2023-04-27 18:37:50
2023-05-29 20:16:25
2023-05-29 20:16:25
Status changed
Total items: 4
20 / page
1
/ 1

API 行为管控

最近更新时间：2023-12-29 14:53:49

什么是 API 异常访问行为？

在“万物皆可 API”的时代，通过 API 快速构建产品和服务、迅速响应客户需求已是数字化企业的必备技能。但同时，API 承载着越来越复杂的应用程序逻辑和大量敏感数据，也使得 API 成为黑产的重点攻击目标。
近年来，不少国际知名企业都因 API 安全疏忽而遭受了巨大的打击。不仅如此，据研究部门 Salt Labs 发布的《2022年第一季度 API 安全状况报告》显示，在过去12个月中，恶意 API 流量增加了681%，95%的组织都经历了 API 安全事件。然而，大多数组织并没有准备好应对这些挑战，超过三分之一（34%）的企业没有 API 安全策略。
在 API 访问中会传输大量的数据，数据的传输分为正常访问和数据窃取等方式，对于正常的数据访问，可以在数据分级分类的情况下，在 WAF 上实现对数据的脱敏和混淆等功能；对于数据窃取的情况下，需要识别异常的数据泄露，并阻断异常访问和连接。

API 的异常访问行为有哪些？

无明显特征的攻击行为。
针对业务的异常访问。
大量的数据传输。
异常的访问对象。
被攻击利用的过期 API 或者是僵尸 API。
过度暴露的数据。

API 异常访问行为挖掘最佳实践

发现 API 的异常访问行为、调查 API 的访问的异常行为，是在日常安全运营中发现并修补安全/运营漏洞的最佳手段。那么在 Web 应用防火墙控制台，可以通过 API 流量分析、BOT 流量分析等相关安全视图，进行快速的 API 异常访问行为的发现及挖掘，实现快速的安全运营闭环。
说明
API 流量分析功能当前处于公测中，支持 提交工单 或联系商务经理申请试用该功能，公测期间仅支持开启3个域名。
API 的异常访问行为发掘调查主要分为以下几个步骤：
1. 发现异常访问请求。
在 攻击日志页面，发现异常的访问行为日志，并对其进行跟踪。
在 API 流量分析功能 中，发现异常的 API 概览信息，确认相关异常 API 日志，并对其进行跟踪。

在 BOT 流量分析页面，发现分数异常的 API 访问请求，并对其进行跟踪。

2. 确认异常访问请求中的唯一 UUID，根据 UUID 确认事件爆炸范围。

开启访问日志后，每一条访问日志存在唯一的 uuid，可以根据唯一 uuid 进行相关用户、API 访问日志、BOT 行为信息的分析及跟踪。

3. 考虑用户典型行为背景下的异常。

在不同的业务场景下，不同用户的 API 访问行为并非一致，如在登录 API 的场景下，如果频繁访问登录接口则异常的可能性极大。

4. 以影响访问因素为指导，确认是否异常。

确认当前访问源是否为异常访问源、登录地是否异常、调用方是否非业务访问源用户。

5. 已返回报表内容信息为指导，确认是否异常。

确认访问的 body size 等参数是否远超异常。

确认返回内容是否超出预期。

6. 确认相关 API 及用户信息、进行安全闭环。

确认异常访问行为、用户信息、以及相关 API 信息，对其进行处置后，及时进行安全修复。

接入相关
WAF 与 DDoS 高防包结合应用

最近更新时间：2023-12-29 14:54:03

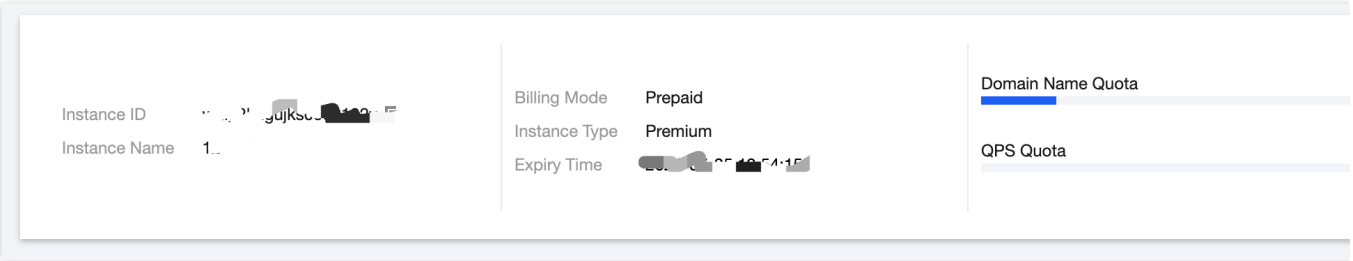
应用场景

Web 应用防火墙（WAF）具备 CC 防护能力，针对非 HTTP 请求，Web 应用防火墙支持和 DDoS 高防包联动，为用户提供全方位的安全防护。
DDoS 高防包可以提供上百 Gbps 的 DDoS 防护能力，轻松应对 DDoS 攻击，保障业务稳定运行。
Web 应用防火墙提供实时防护能力，可有效拦截 Web 攻击，保障用户业务的数据和信息安全。

操作步骤

步骤1：配置 Web 应用防火墙

1. 登录 Web 应用防火墙控制台，在左侧导航中，选择选择**实例管理** > **实例列表**，进入实例列表页面。
2. 在实例列表页面，选择需要添加域名的实例，在右侧单击所属实例的**域名接入**。



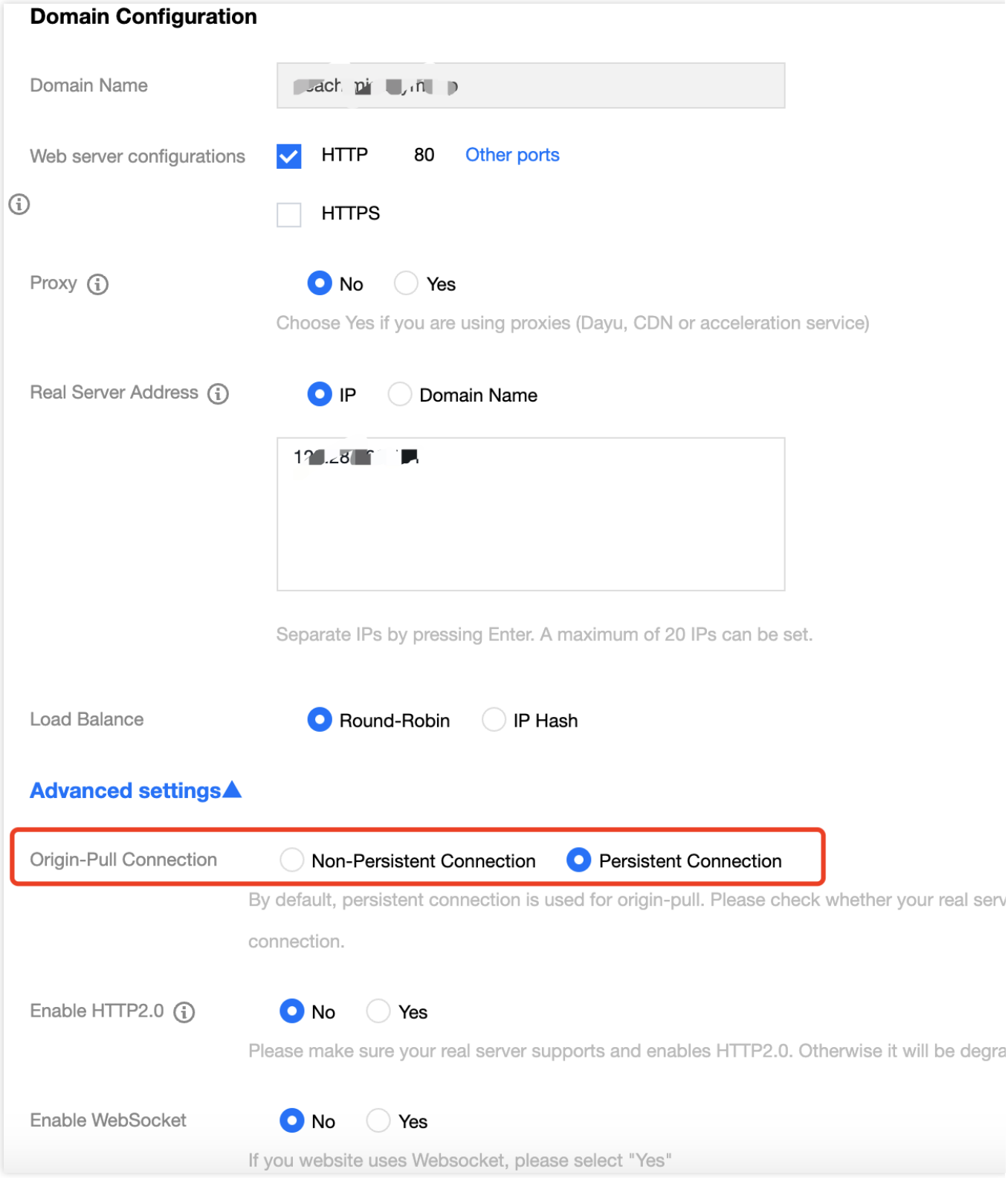
3. 在域名接入页面，单击**添加域名**，并根据实际情况设置以下参数。

域名配置

域名：输入需要防护的域名。
服务器配置：按实际情况选择协议类型及端口。
开启 HTTP2.0：按实际情况选择。
服务器端口：按实际情况选择。
源站地址：输入需要防护网站的真实 IP 源站地址，即源站的公网 IP 地址。

其他配置

代理情况：请选择**否**（如果 WAF 和高防 IP 结合，需要选择**是**）。
开启 WebSocket、负载均衡策略：按实际情况选择。



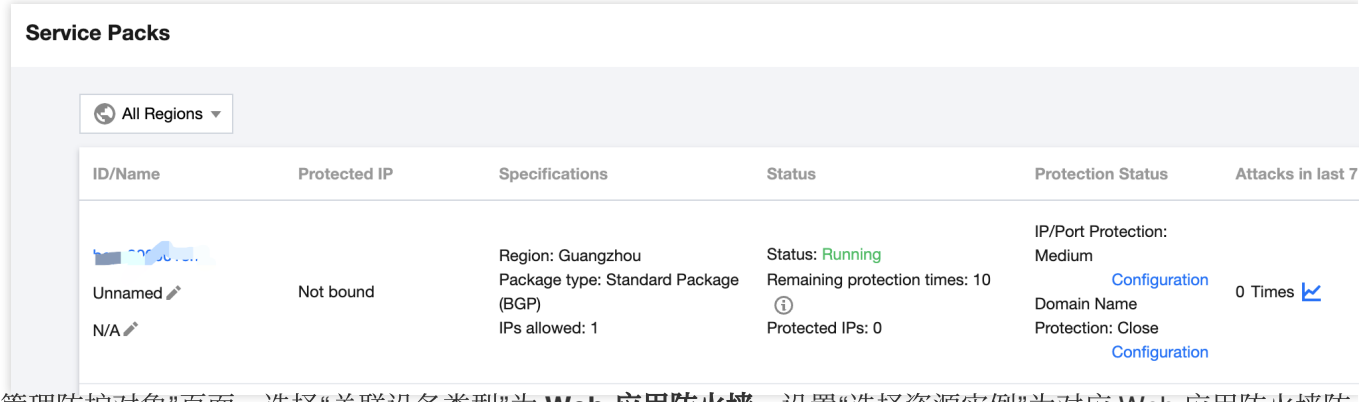
说明：

如果源站有多个回源 IP 可以根据实际需要选择回源负载均衡策略，当前策略支持按照客户请求进行轮询（同一个访问源 IP 的请求按照顺序转发到不同的源站服务器）或 IP Hash（同一个访问源 IP 的请求回源到一个台源站服务器），默认为轮询。

4. 设置完成后，单击**保存**即可。

步骤2：配置 DDoS 高防包

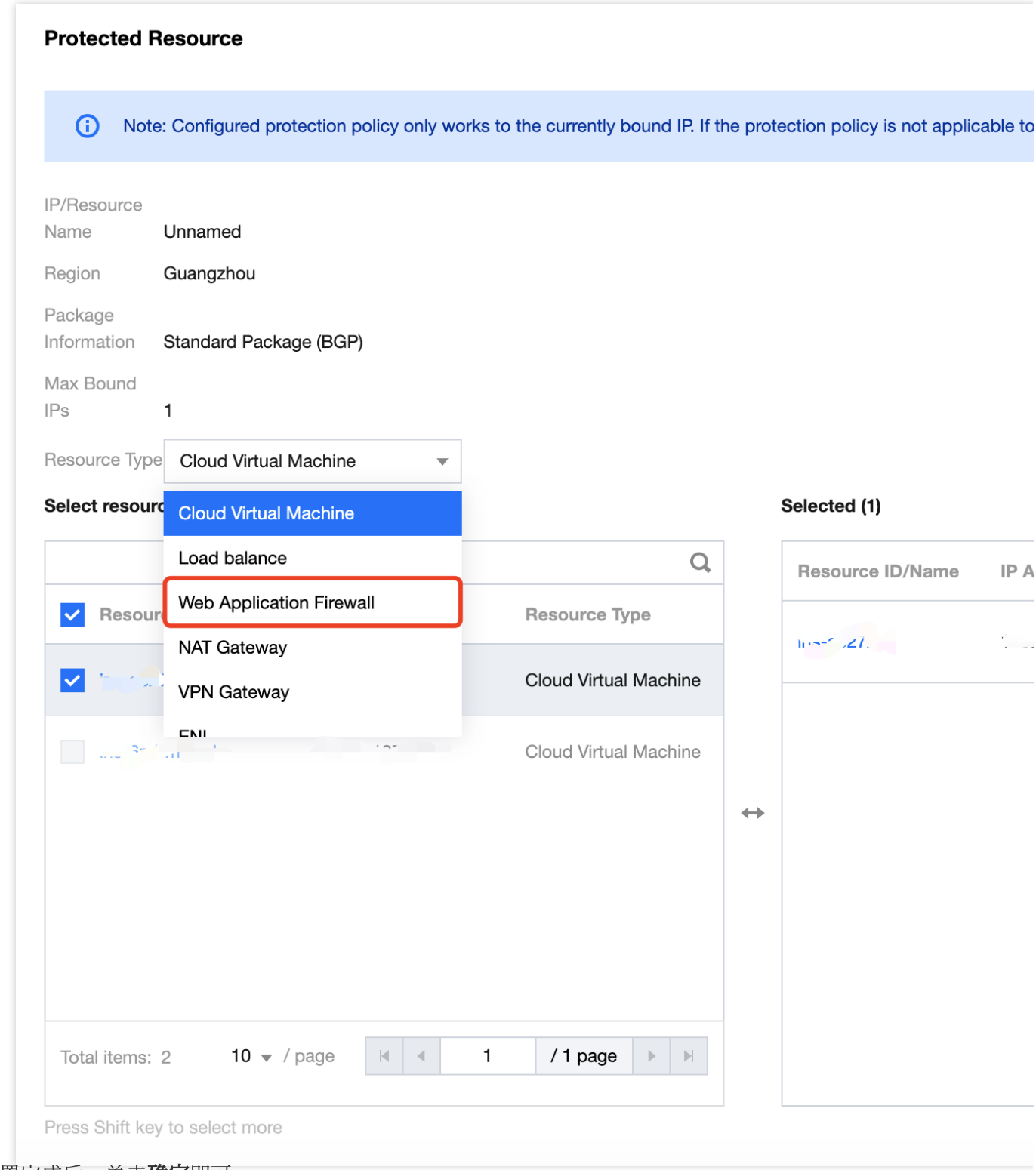
1. 登录 DDoS 防护管理控制台，在左侧导航中，选择 **DDoS 高防包 > 高防包**。
2. 选择目的高防包实例所在地域，并在目的高防包实例所在行的右侧操作栏，单击**管理防护对象。**



3. 在“管理防护对象”页面，选择“关联设备类型”为 **Web 应用防火墙**，设置“选择资源实例”为对应 Web 应用防火墙防护的 IP 地址。

说明：

若是负载均衡型 WAF，在绑定界面选择“关联设备类型”为负载均衡，设置“选择关联机器”为对应负载均衡的公网 IP 地址。



4. 设置完成后，单击**确定**即可。

HTTPS 免费证书申请和应用

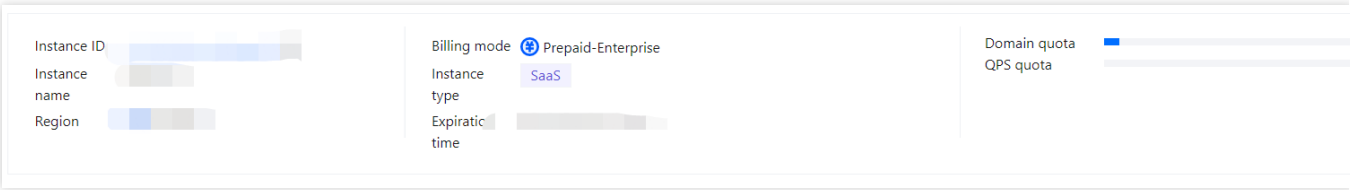
最近更新时间：2023-12-29 14:54:14

前提条件

Web 应用防火墙提供域名 HTTPS 接入配置和防护能力，若您的网站未进行 HTTPS 改造，您可以在 腾讯云 SSL 证书控制台 申请免费的域名证书。证书申请后，在 Web 应用防火墙控制台关联证书，Web 应用防火墙将帮助您在不改造源站的情况下，一键实现全站 HTTPS 访问，客户端使用 HTTPS 连接网站。

HTTPS 证书关联操作步骤

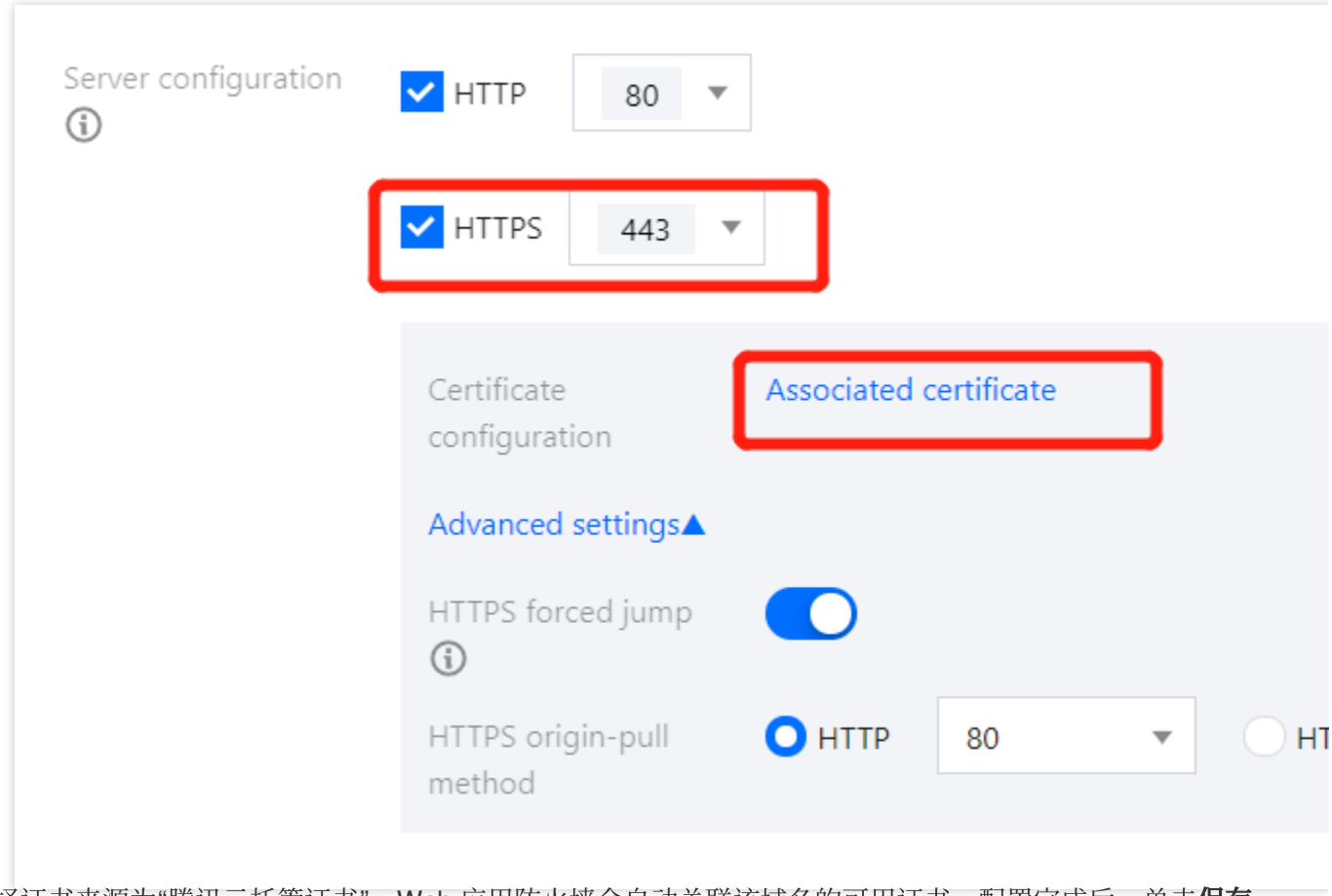
1. 登录 Web 应用防火墙控制台，在左侧导航中，选择选择**实例管理** > **实例列表**，进入实例列表页面。
2. 在实例列表页面，选择需要添加域名的实例，在右侧单击所属实例的**域名接入**。



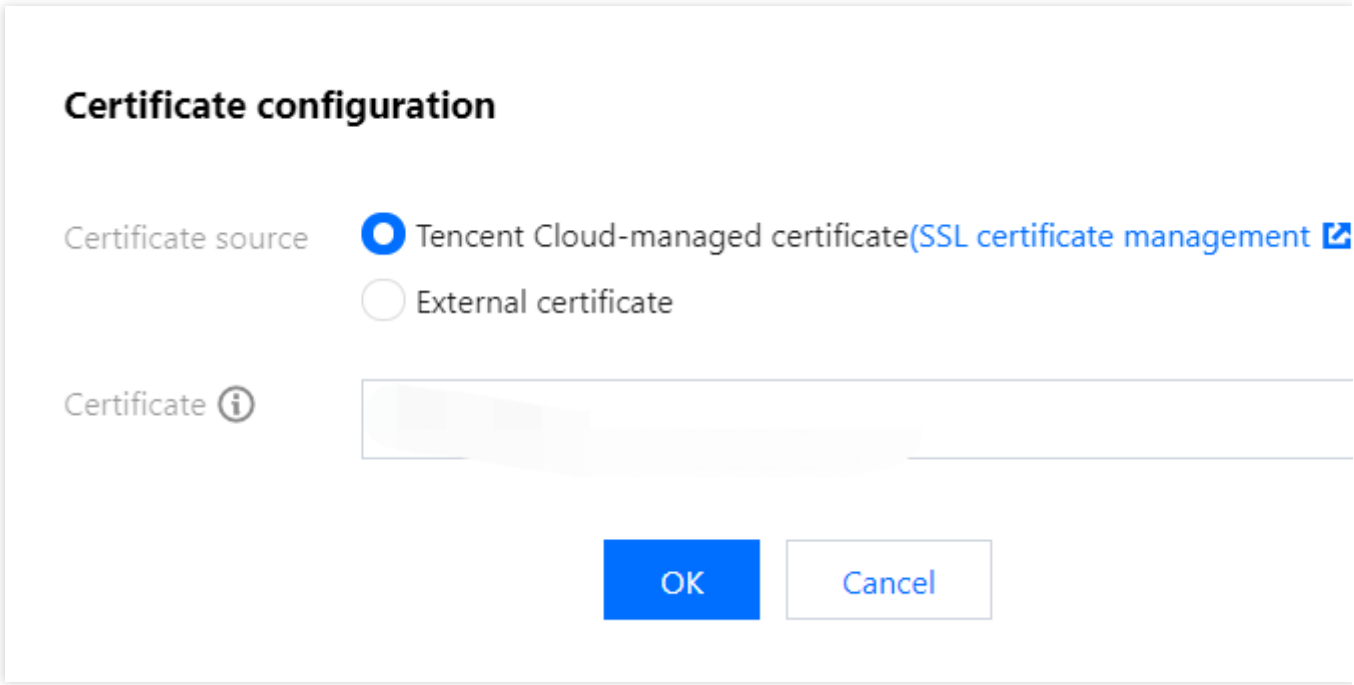
3. 在域名接入页面，单击**添加域名**，进入添加域名页面。
4. 在域名配置的服务器配置中，勾选 **HTTPS**，在证书配置中，单击**关联证书**。

说明：

证书格式为 PEM 格式，内容为文本类型。



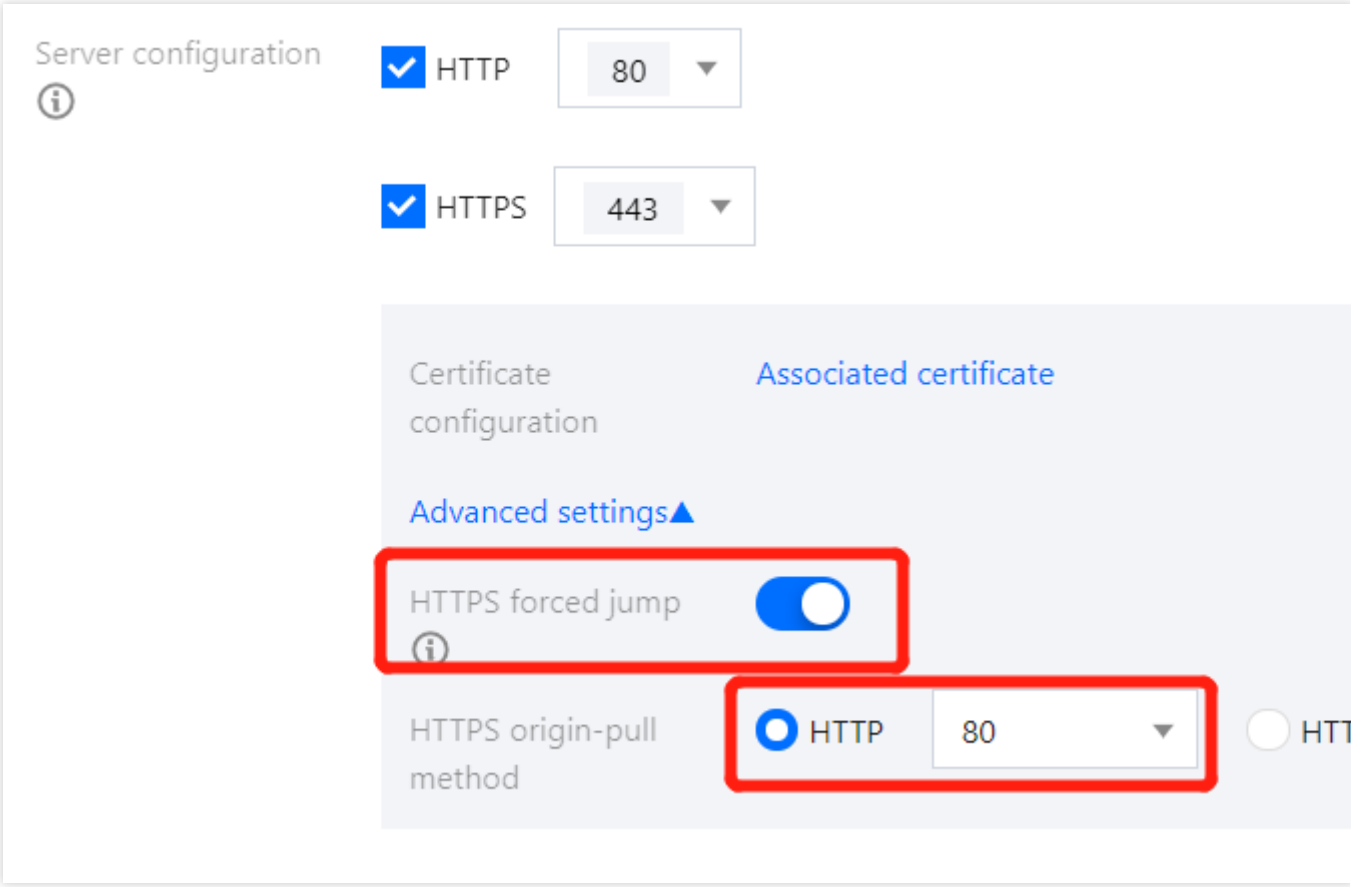
5. 选择证书来源为“腾讯云托管证书”，Web 应用防火墙会自动关联该域名的可用证书，配置完成后，单击**保存**。



6. 开启 HTTPS 强制跳转开关，并在上方勾选 **HTTP** 访问协议，同时选择 “HTTPS 回源方式”选择 HTTP，其他参数根据实际情况填写完成后，您的网站将支持 HTTPS 访问。

注意：

如需开启 HTTPS 强制跳转开关，需同时勾选 HTTP 和 HTTPS 访问协议。



如何获取客户端真实 IP

最近更新时间：2023-12-29 14:54:26

WAF 获取客户端真实 IP 说明

WAF 通过反向代理的方式实现网站安全防护，用户访问 WAF 防护的域名时，会在 HTTP 头部字段中添加一条 X-Forwarded-For 记录，用于记录用户真实 IP，其记录格式为 `X-Forwarded-For:用户 IP` 。如果用户访问域名存在多级代理，WAF 将记录靠近 WAF 上一条的代理服务器 IP。例如：

场景一：用户＞WAF＞源站，X-Forwarded-For 记录为： `X-Forwarded-For:用户真实 IP`

场景二：用户＞CDN＞WAF＞源站，X-Forwarded-For 记录为： `X-Forwarded-For:用户真实 IP,X-Forwarded-For:CDN 回源地址` 。

说明：

场景二中，需要在 WAF 添加域名 时，选择代理情况为“是”，选择代理接入后，可能存在客户端 IP 被伪造的风险。如果您使用腾讯云 CDN，不存在客户端 IP 被伪造的风险，腾讯云 CDN 会对 X-Forwarded-For 信息进重置，只填写 CDN 获取的客户端 IP。（如果使用代理接入，攻击者需要在能直接对 WAF VIP 地址进行请求的情况下才会产生影响，代理接入时用户无法探测到 WAF VIP 地址，请避免代理接入时 WAF VIP 地址泄露）。

负载均衡型 WAF 接入，请参见负载均衡中 如何获取客户端真实 IP。

下文将对常见的应用服务器 X-Forwarded-For 配置方案进行介绍：

IIS 7 配置方案

Apache 配置方案

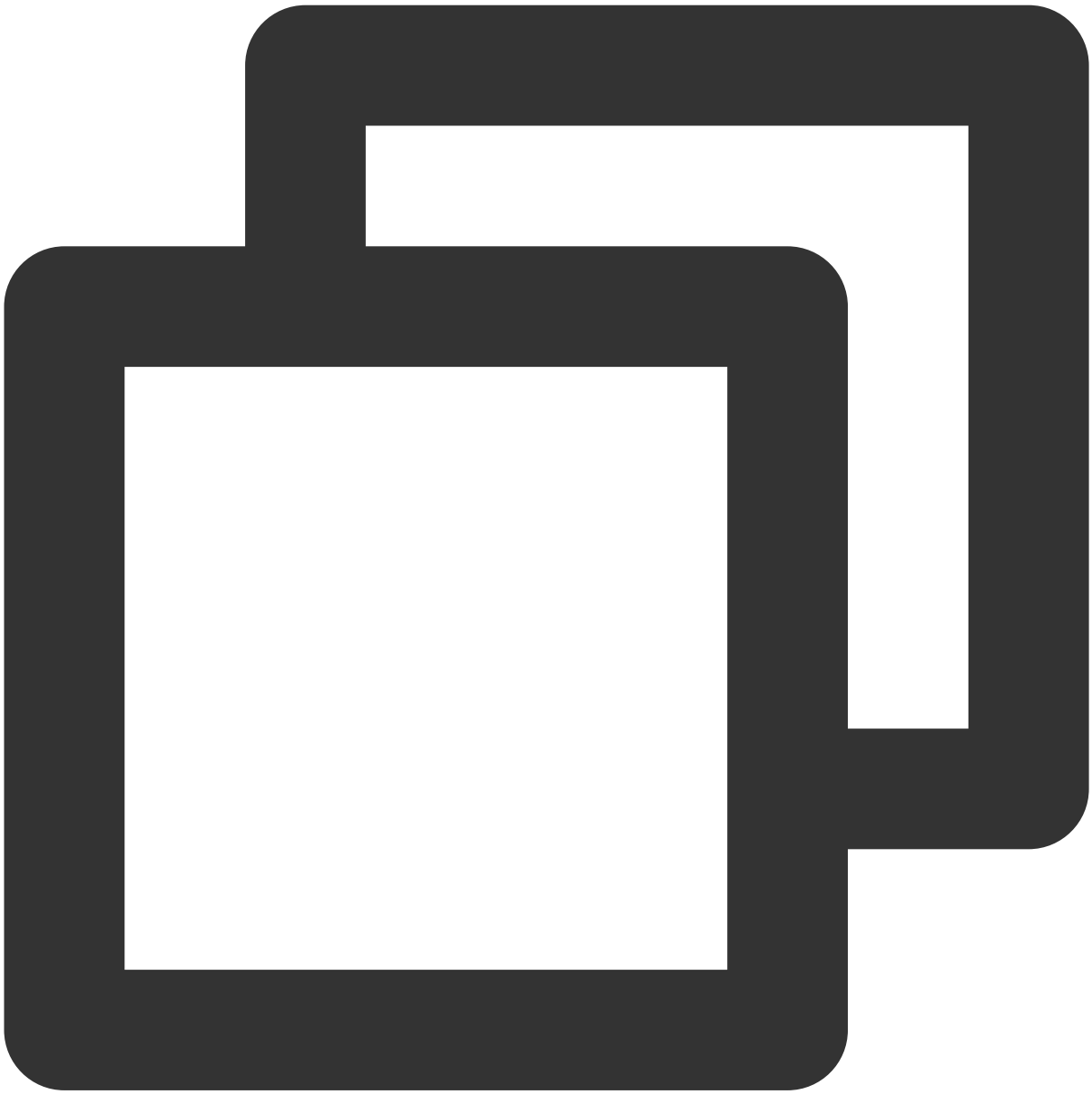
Nginx 配置方案

IIS 7 配置方案

1. 下载与安装插件 F5XForwardedFor 模块，根据自己的服务器操作系统版本将 `x86\\Release` 或者 `x64\\Release` 目录下的 `F5XFFHttpModule.dll` 和 `F5XFFHttpModule.ini` 拷贝到某个目录，这里假设为 `C:\\F5XForwardedFor` ，确保 IIS 进程对该目录有读取权限。
2. 选择【IIS 服务器】，双击【模块】功能。
3. 单击【配置本机模块】。
4. 在弹出框中单击【注册】。
5. 添加下载的 DLL 文件。
6. 添加完成后，勾选并单击【确定】。
7. 在 IIS 服务器的 “ISAPI 和 CGI 限制”中，添加如上两个 DLL ，并将限制设置为允许。
8. 重启 IIS 服务器，等待配置生效。

Apache 配置方案

1. 安装 Apache 第三方模块“mod_rpaf”，需执行如下命令：



```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

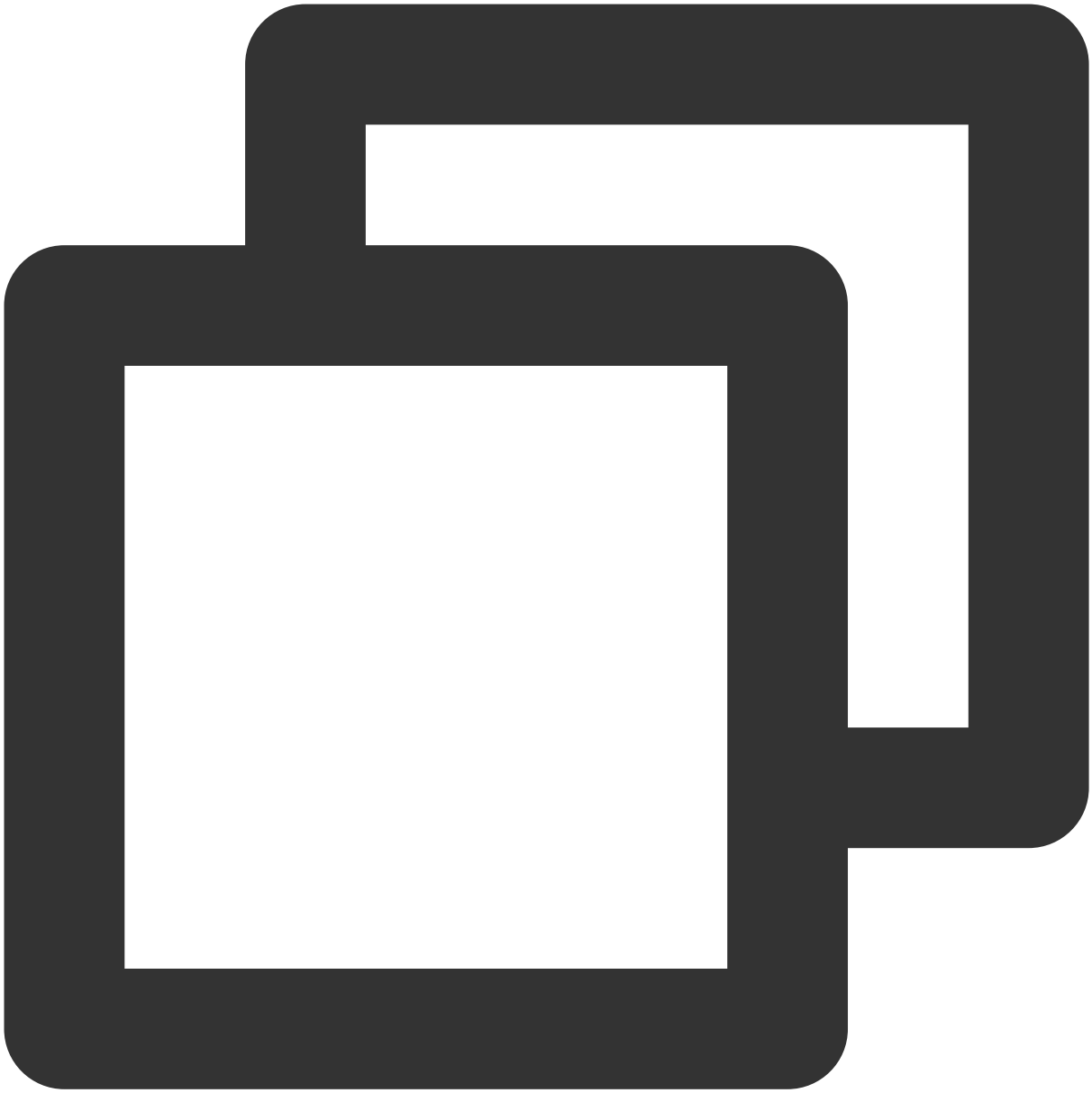
2. 修改 Apache 配置 `/etc/httpd/conf/httpd.conf`，需在最末尾添加：

<pre>
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On

RPAFproxy_ips IP地址 //IP 地址为 WAF 防护域名的回源 IP 地址，可以在 Web应用防火墙控制台，防护配置域名列表中的回源 IP 地址中查看，也可以在服务器后台的日志中查看，只需要将所有需要查看的 IP 都填写上即可。
RPAFheader X-Forwarded-For

</pr>

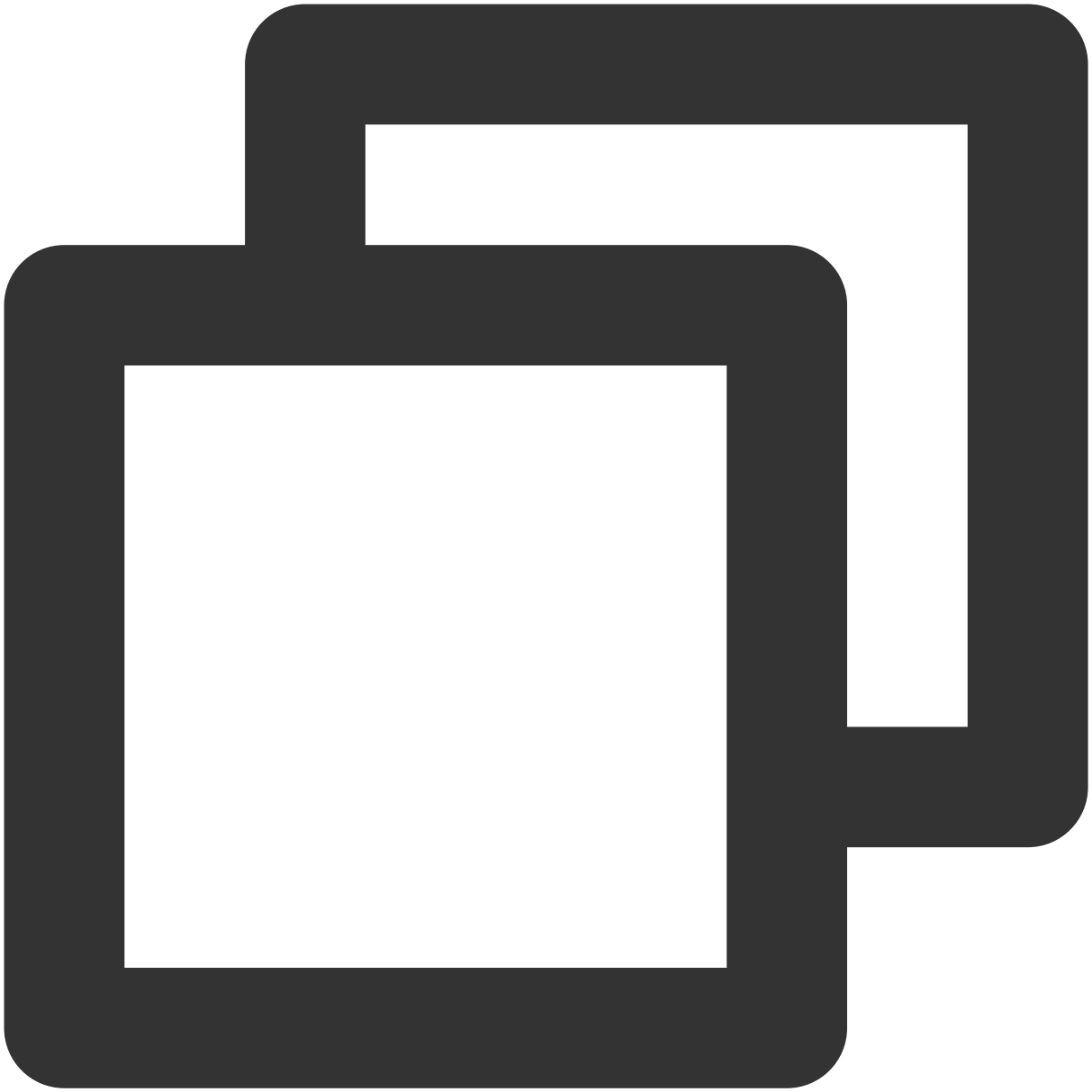
3. 添加完成后，重启 Apache。



```
/usr/sbin/apachectl restart
```

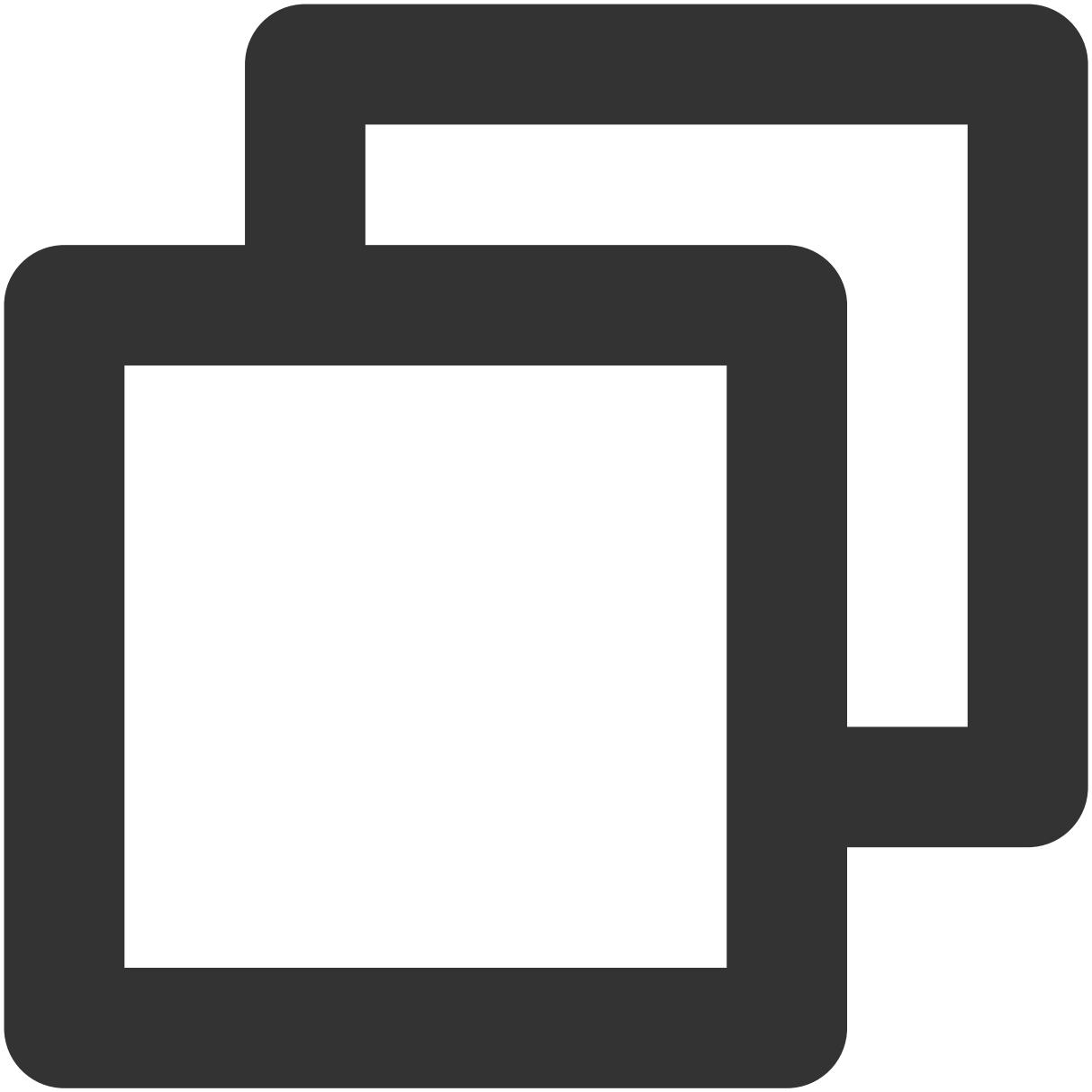
Nginx 配置方案

1. 当 Nginx 作为服务器时，获取客户端真实 IP，需使用 http_realip_module 模块，默认安装的 Nginx 是没有编译 http_realip_module 模块的，需要重新编译 Nginx，在configure 增加 --with-http_realip_module 选项， 确保 http_realip_module 模块编译进 nginx 中 。编译代码如下：



```
wget  http://nginx.org/download/nginx-1.14.0.tar.gz
tar  zxvf nginx-1.14.0.tar.gz
cd nginx-1.14.0
./configure --user=www --group=www --with-http_stub_status_module --without-http-ca
make
make install
```

2. 修改 nginx.conf。



```
vi /etc/nginx/nginx.conf
```

修改如下红色部分：

<pre>

fastcgi connect_timeout 300;

fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;

set_real_ip_from IP地址; //IP 地址为 WAF 防护域名的回源 IP 地址，可以在 Web应用防火墙控制台，域名接入列表中的回源 IP 地址中查看。
real_ip_header X-Forwarded-For;

</pre>

3. 重启 Nginx。
<pre>
service nginx restart
</pre>

如何更换证书

最近更新时间：2023-12-29 14:54:37

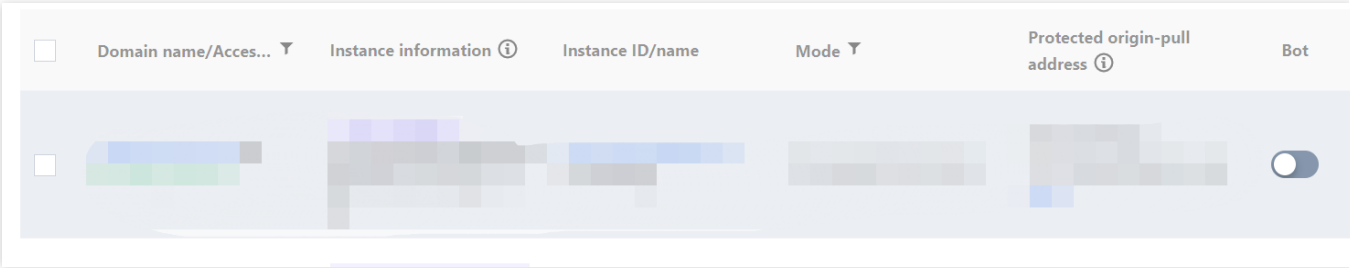
操作场景

如果证书已过期，用户在浏览网站的时候会显示证书不可信；如果客户该域名有使用 API 调用，在调用过程中将会报错。为了避免证书过期对业务造成影响，请在腾讯云控制台上及时更新证书。

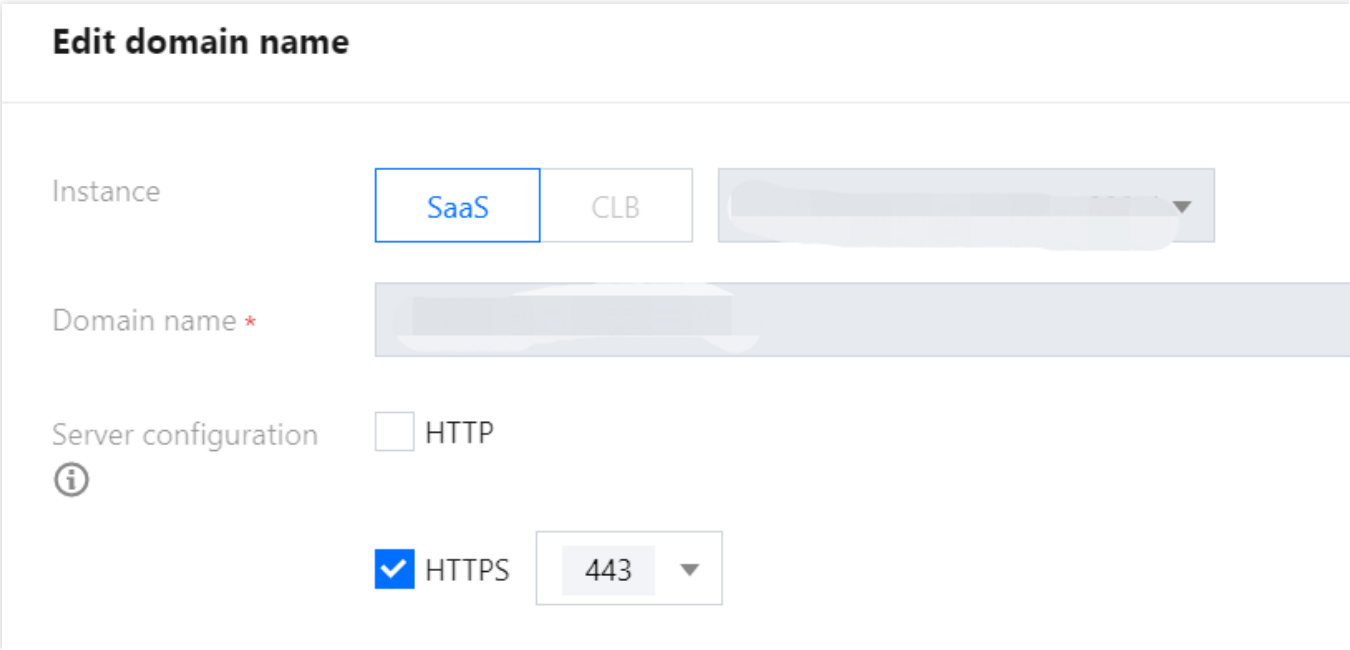
操作步骤

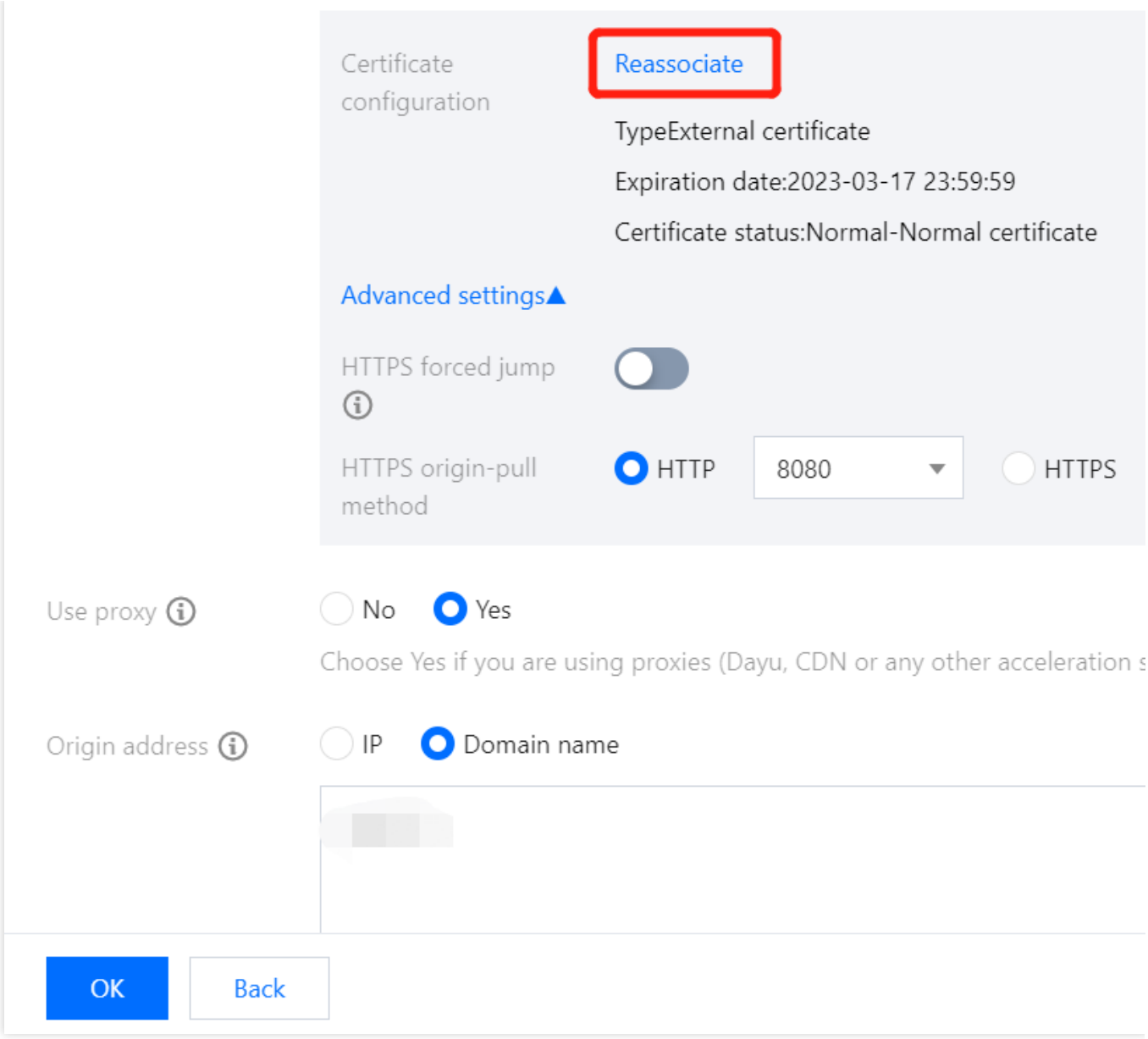
示例1：更换自有证书

1. 登录 Web 应用防火墙控制台，在左侧导航中，选择选择**资产中心 > 域名列表**。
2. 在域名列表页面，选中所需域名，单击**编辑**，进入编辑域名页面。

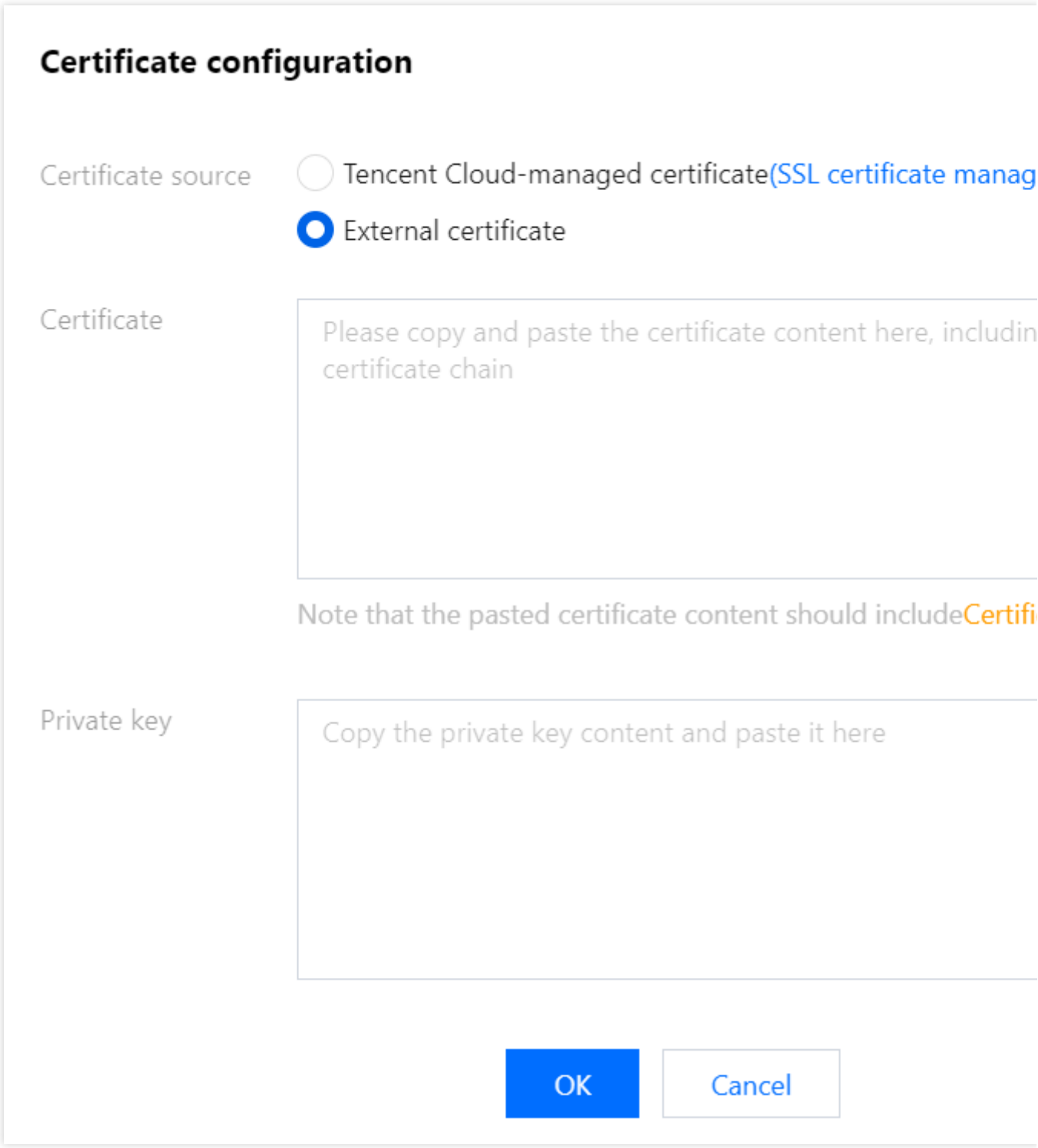


3. 在编辑域名页面，单击服务器配置中的**重新关联**，弹窗证书配置窗口。



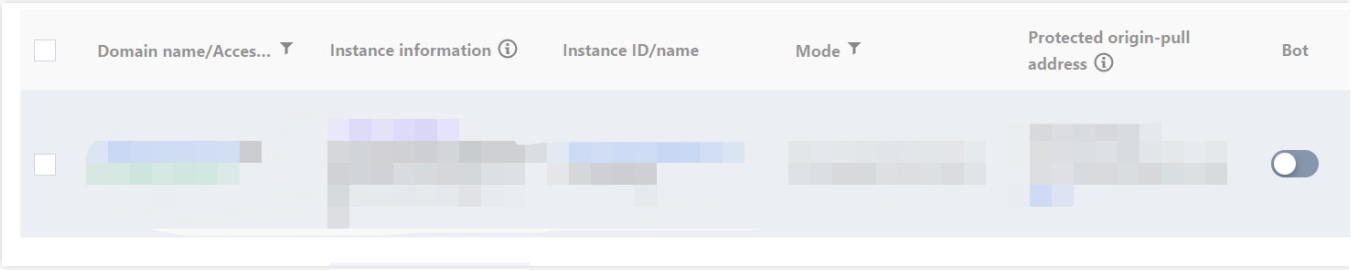


4. 在证书配置窗口，证书来源选择自有证书，并输入相关的证书和私钥，单击**确认**，即可更换自有证书。

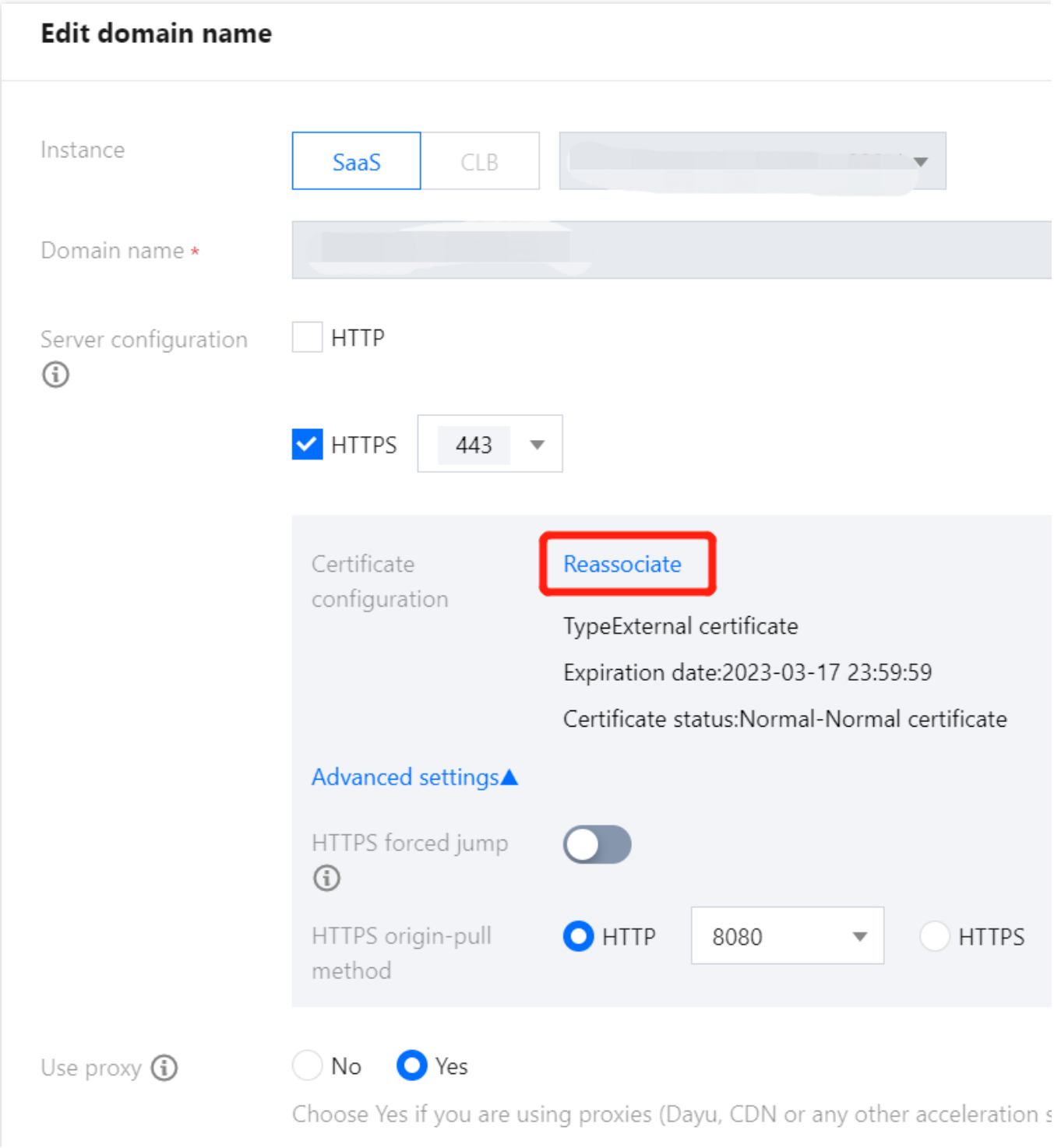


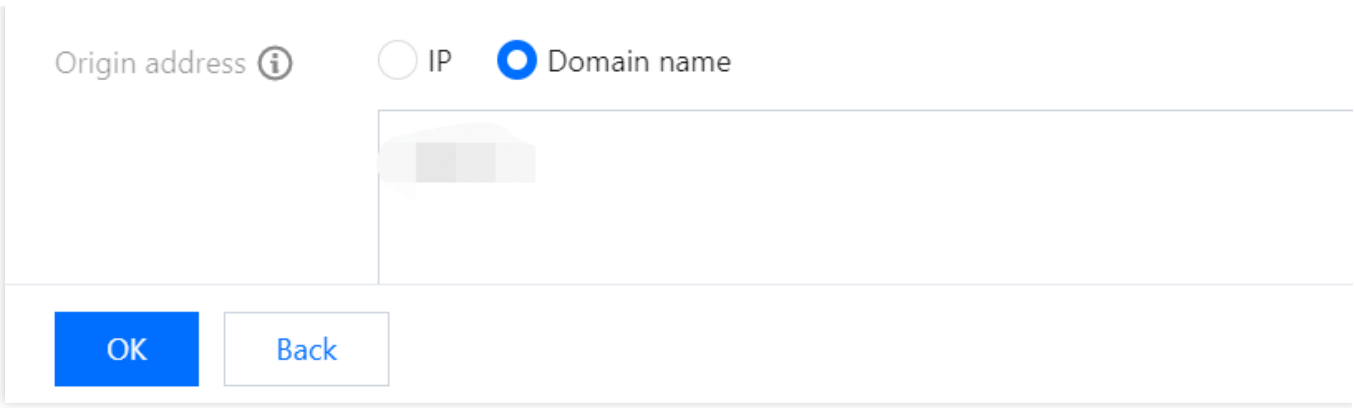
示例2：腾讯云托管证书

1. 在 域名列表 页面，选中所需域名，单击**编辑**，进入编辑域名页面。



2. 在编辑域名页面，单击服务器配置中的**重新关联**，弹窗证书配置窗口。

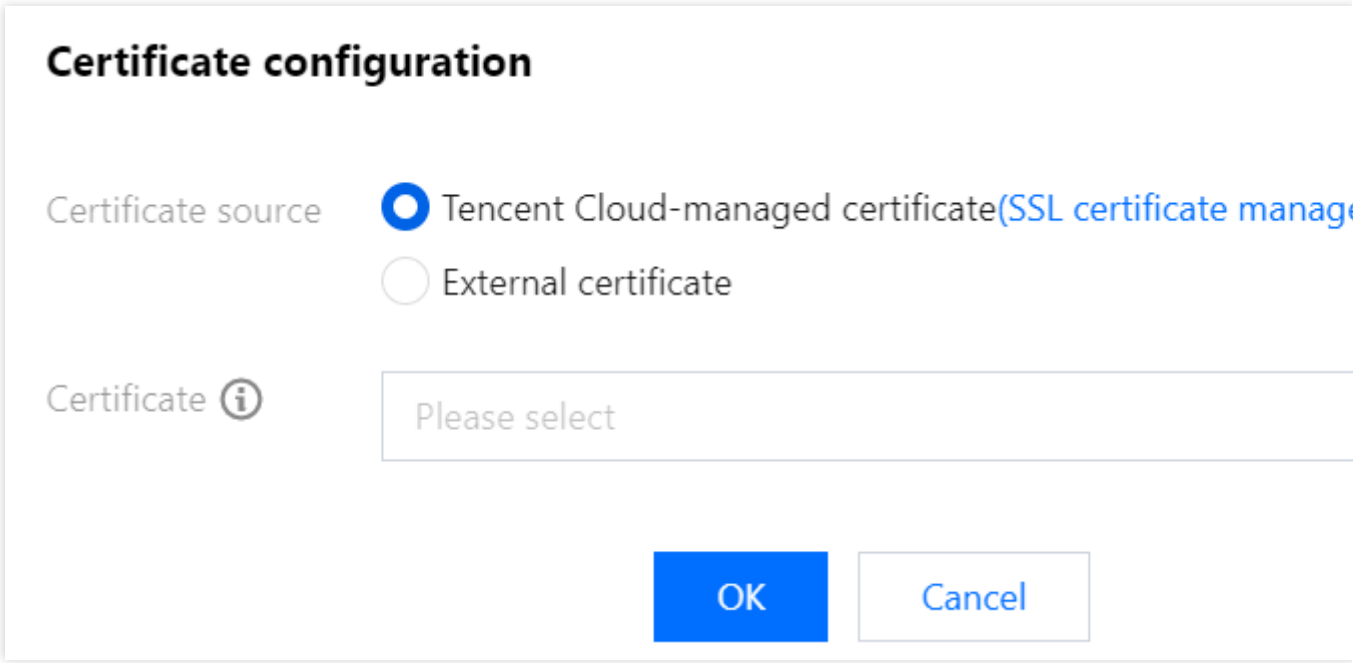




3. 在证书配置窗口，证书来源选择腾讯云托管证书，并选择新证书，单击**确定**，即可更换 SSL 证书。

说明：

此方法只适用于证书已经上传到 SSL 证书管理。



检验是否生效

通过浏览器访问相关域名，可以查看证书的生效时间和到期时间。如果更换证书始终不生效，请 联系我们 获得帮助。

防护与配置相关
如何设置 CC 防护

最近更新时间：2023-12-29 14:54:52

本文将为您介绍如何在 Web 应用防火墙控制台设置 CC 防护。

背景信息

CC 防护可以对网站特定的 URL 进行访问保护，CC 防护支持紧急模式 CC 防护和自定义 CC 防护策略。

注意：

紧急模式 CC 防护策略和自定义 CC 规则防护策略，不能同时开启。

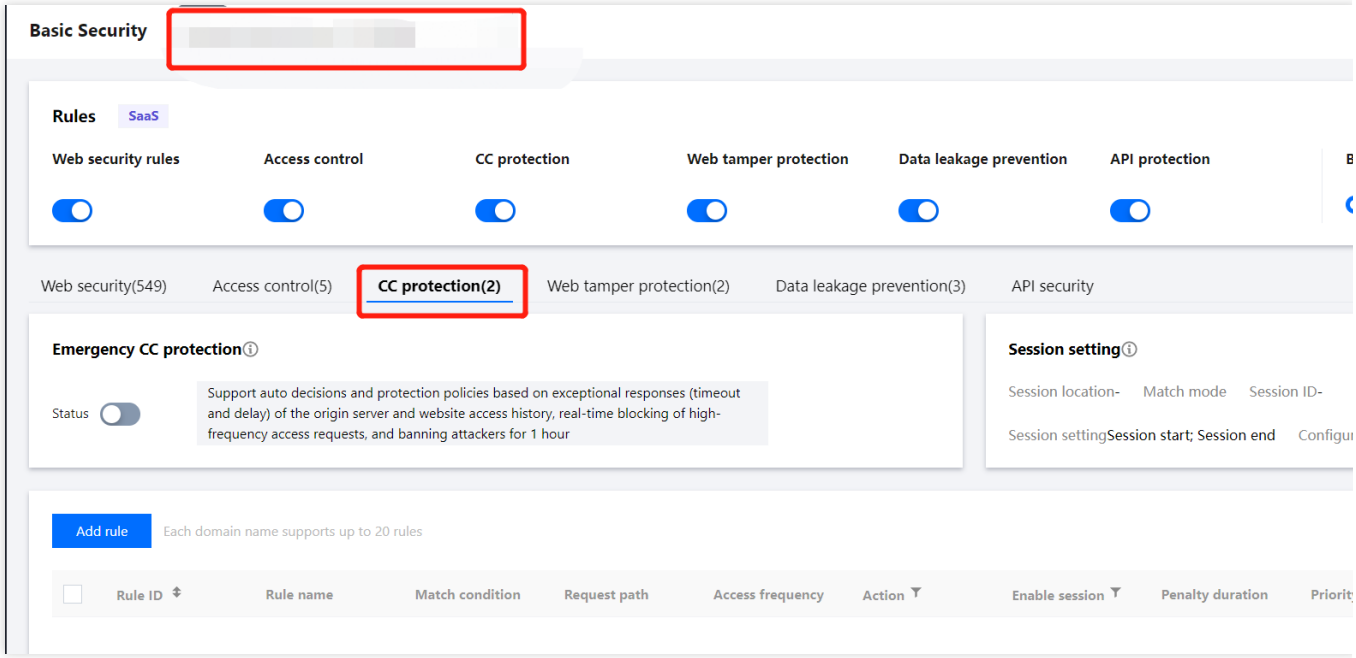
操作步骤

示例一：紧急模式 CC 防护配置

注意：

紧急模式 CC 防护默认关闭，开启前请确认自定义 CC 防护规则处于未启用状态。

1. 登录 Web 应用防火墙控制台，在左侧导航栏选择**基础安全**。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **CC 防护**，进入 CC 防护页面。



3. 在紧急模式 CC 防护模块中，单击状态右侧的

，经过二次确认后，开启紧急模式 CC 防护。

说明：

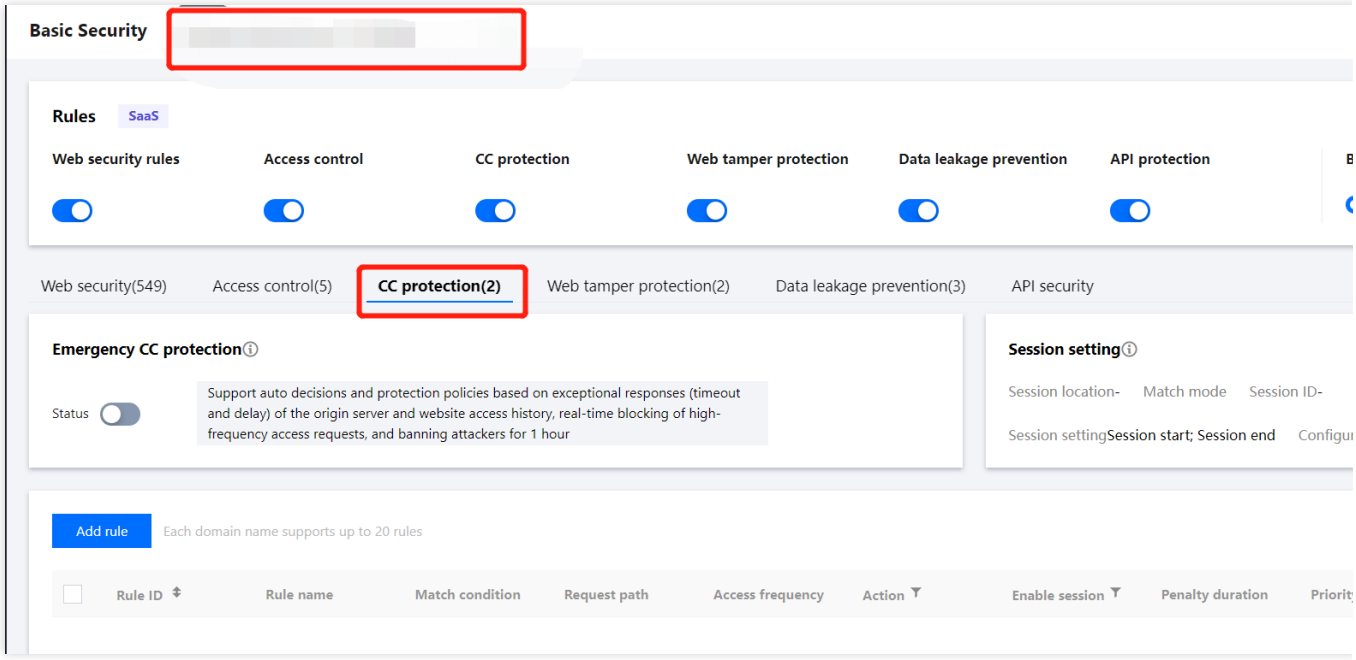
当开启紧急模式 CC 防护时，若网站遭大流量 CC 攻击会自动触发防护（网站 QPS 不低于1000QPS），无需人工参与。若无明确的防护路径，建议启用紧急模式 CC 防护，可能会存在一定误报。可以在控制台进入黑白名单，对拦截 IP 信息，进行加白处理。

如果知晓明确的防护路径，建议使用自定义 CC 规则进行防护。

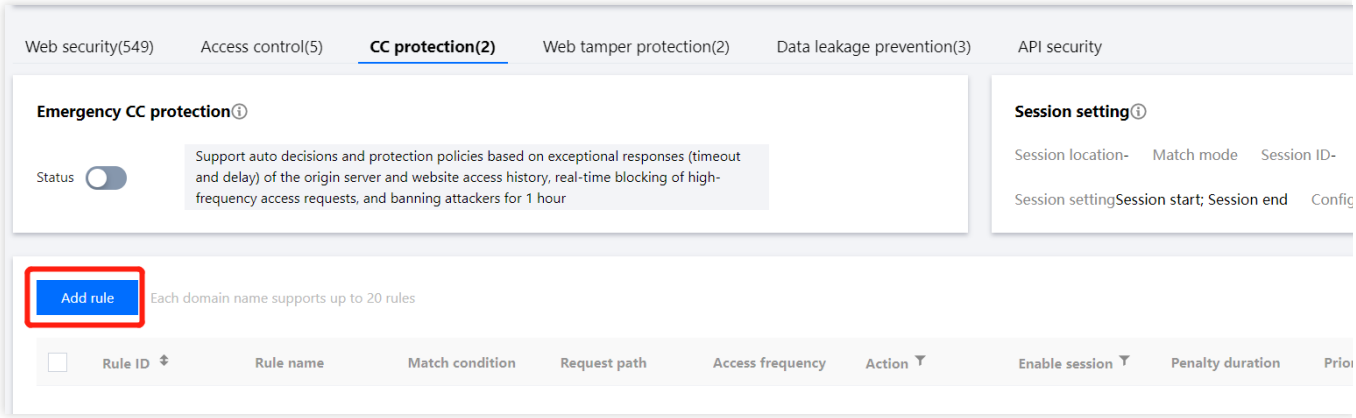
示例二： 基于访问源 IP 的 CC 防护设置

基于 IP 的 CC 防护策略，不需要对 SESSION 维度进行设置，直接配置即可。

1. 登录 Web 应用防火墙控制台，在左侧导航栏选择**基础安全**。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **CC 防护**，进入 CC 防护页面。



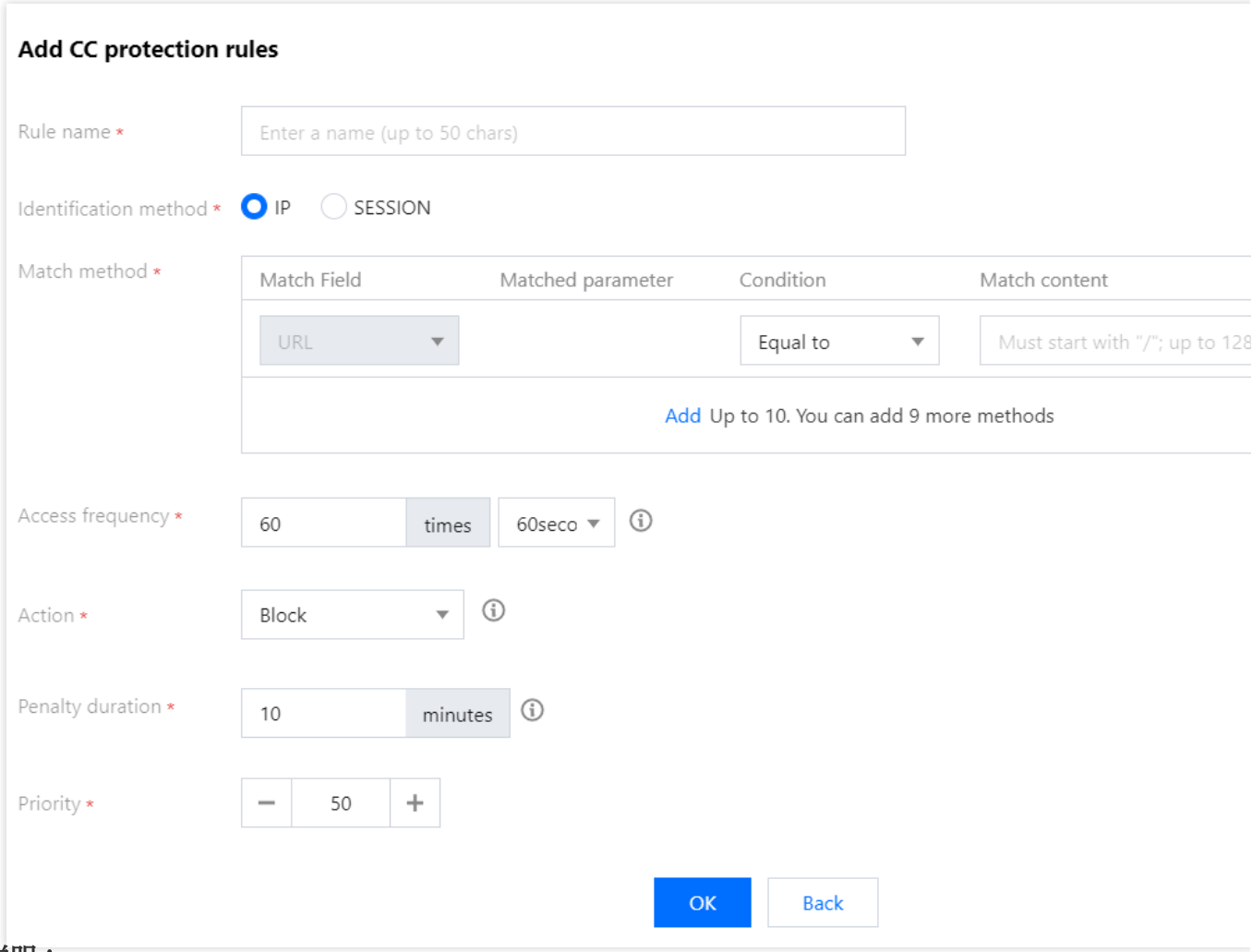
3. 在 CC 防护页面，单击**添加规则**，弹出添加 CC 防护规则弹窗。



4. 在添加 CC 防护规则弹窗中，填写相应信息。

注意：

IP 为识别方式时，规则被触发拦截时会全站封锁（该 IP 访问其他 URL 也拦截），SESSION 则不会全站拦截。



参数说明：

规则名称：自定义名称，50个字符以内。

识别方式： IP、SESSION。

匹配方式：包括相等、前缀匹配和包含。

高级匹配：通过进行 GET 表单和 POST 表单参数过滤，支持更加精细化频率控制，提高命中率。
匹配字段：指定请求方法，支持 GET 或 POST。
参数名：请求字段中的参数名，最多512字符。
参数值：请求字段中的参数值，最多512字符。
示例说明：如下三条 GET 请求测试数据：a=1&b=11、a=2&b=12、 a=&b=13。
如果 GET 配置参数名为 a，参数值为1，则1命中。
如果 GET 配置参数名为 a，参数值为*，则1、2、3均命中。
访问频次：根据业务情况设置访问频次。建议输入正常访问次数的3倍 - 10倍，例如，网站人平均访问20次/分钟，可配置为60次/分钟 - 200次/分钟，可依据被攻击严重程度调整。
执行动作：观察、人机识别和阻断。
惩罚时长：最短为1分钟，最长为一周。
优先级：请输入1 - 100的整数，数字越小，代表这条规则的执行优先级越高，相同优先级下，创建时间越晚，优先级越高。

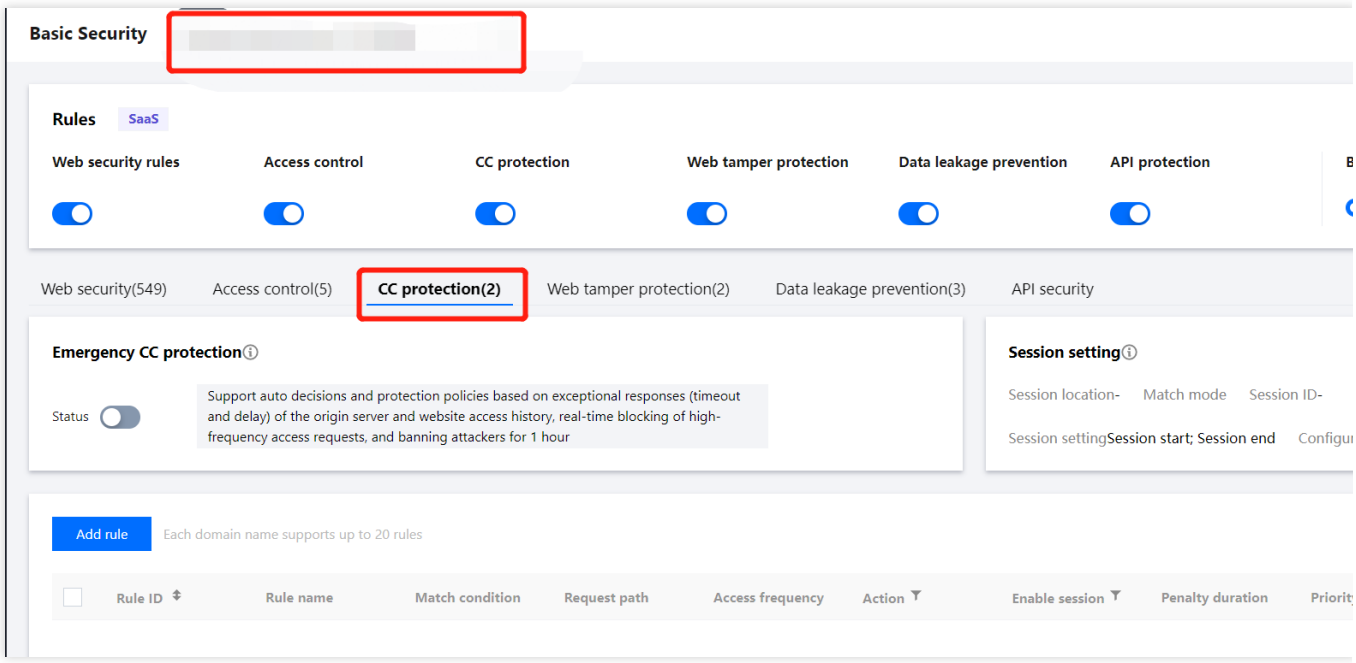
示例三： 基于 SESSION 的 CC 防护设置

基于 SESSION 访问速率的 CC 防护，能够有效解决在办公网、商超和公共 Wi-Fi 场合，用户因使用相同 IP 出口而导致的误拦截问题。

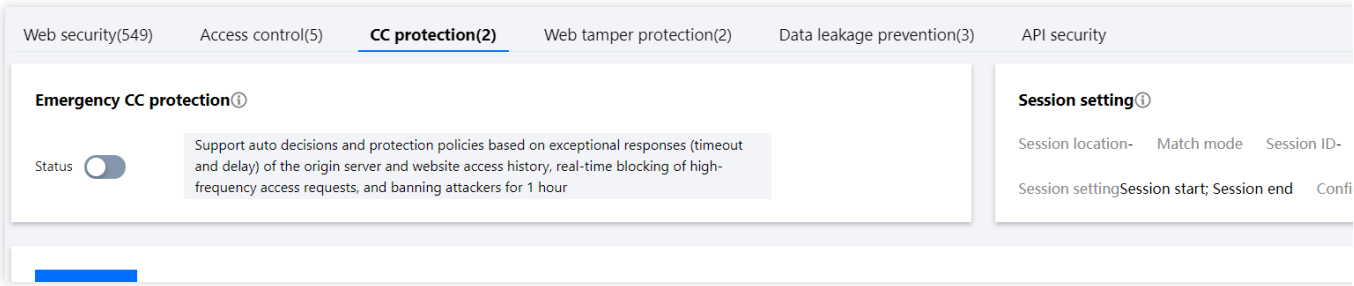
注意：

使用基于 SESSION 的 CC 防护策略，需要先进行 SESSION 设置，才能设置基于 SESSION 的 CC 防护策略，下文步骤1 - 步骤4为 SESSION 设置操作。

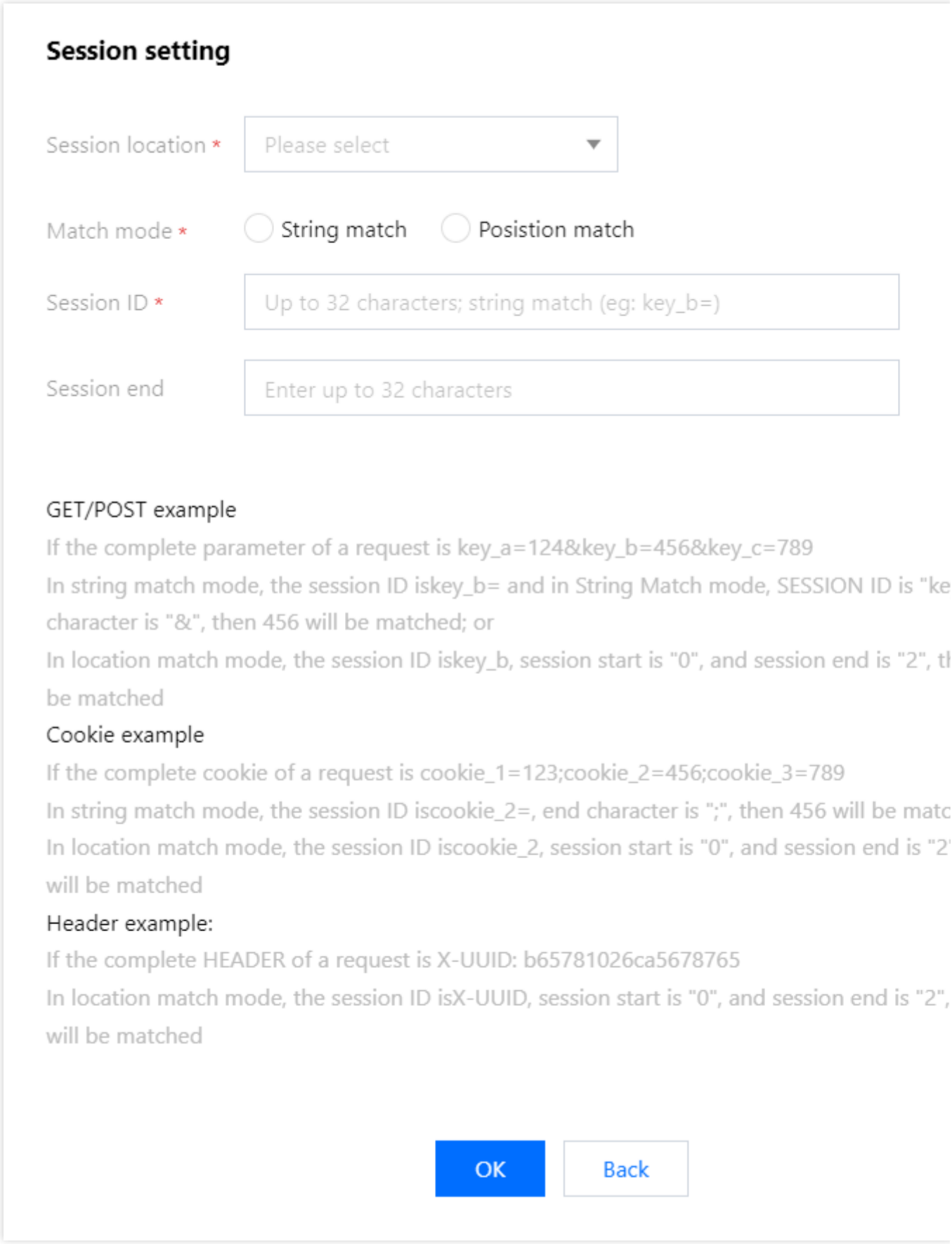
1. 登录 Web 应用防火墙控制台，在左侧导航栏选择**基础安全**。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **CC 防护**，进入 CC 防护页面。



3. 在 SESSION 设置模块中，单击**设置**，设置 SESSION 维度信息。



4. 在 SESSION 设置弹窗，此示例选择 COOKIE 作为测试内容，标识为 security，开始位置为0，结束位置为9，配置完成后单击**确定**即可。


Session setting
Session location *
Please select
Match mode *
String match
Posistion match
Session ID *
Up to 32 characters; string match (eg: key_b=)
Session end
Enter up to 32 characters
GET/POST example
If the complete parameter of a request is key_a=124&key_b=456&key_c=789
In string match mode, the session ID iskey_b= and in String Match mode, SESSION ID is "ke
character is "&", then 456 will be matched; or
In location match mode, the session ID iskey_b, session start is "0", and session end is "2", tl
be matched
Cookie example
If the complete cookie of a request is cookie_1=123;cookie_2=456;cookie_3=789
In string match mode, the session ID iscookie_2=, end character is ";", then 456 will be matc
In location match mode, the session ID iscookie_2, session start is "0", and session end is "2
will be matched
Header example:
If the complete HEADER of a request is X-UUID: b65781026ca5678765
In location match mode, the session ID isX-UUID, session start is "0", and session end is "2",
will be matched
OK
Back

参数说明：

SESSION 位置 ：可选择 COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。

匹配说明 ：位置匹配或者字符串匹配。

SESSION 标识 ：取值标识，32个字符以内。

开始位置：字符串或者位置匹配的开始位置，0-2048以内的整数。

结束位置：字符串或位置匹配的结束位置，1-2048以内的整数，并且最多大只能提取128个字符。

GET/POST 示例 ：如果一条请求的完整参数内容为：key_a = 124&key_b = 456&key_c = 789。

字符串匹配模式下，SESSION 标识为 key_b = ，结束字符为&，则匹配内容为456。

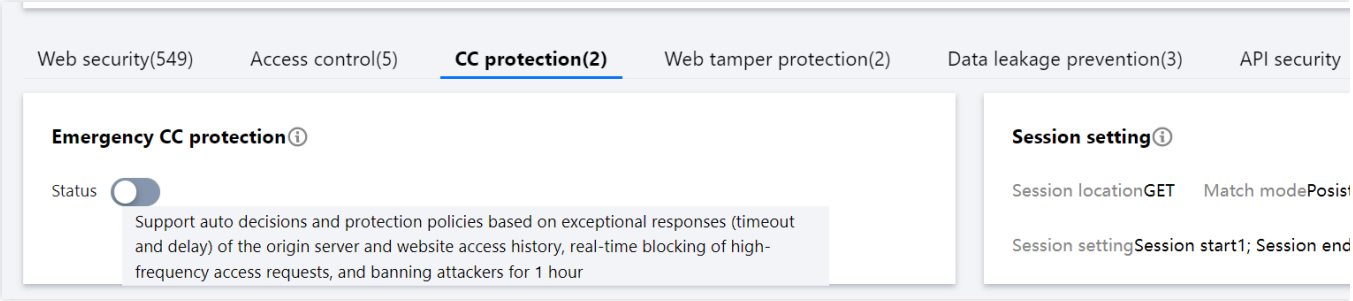
位置匹配模式下，SESSION 标识为 key_b，开始位置为0，结束位置2，则匹配内容为456。

COOKIE 示例 ：如果一条请求的完整 COOKIE 内容为：cookie_1 = 123;cookie_2 = 456;cookie_3 = 789。

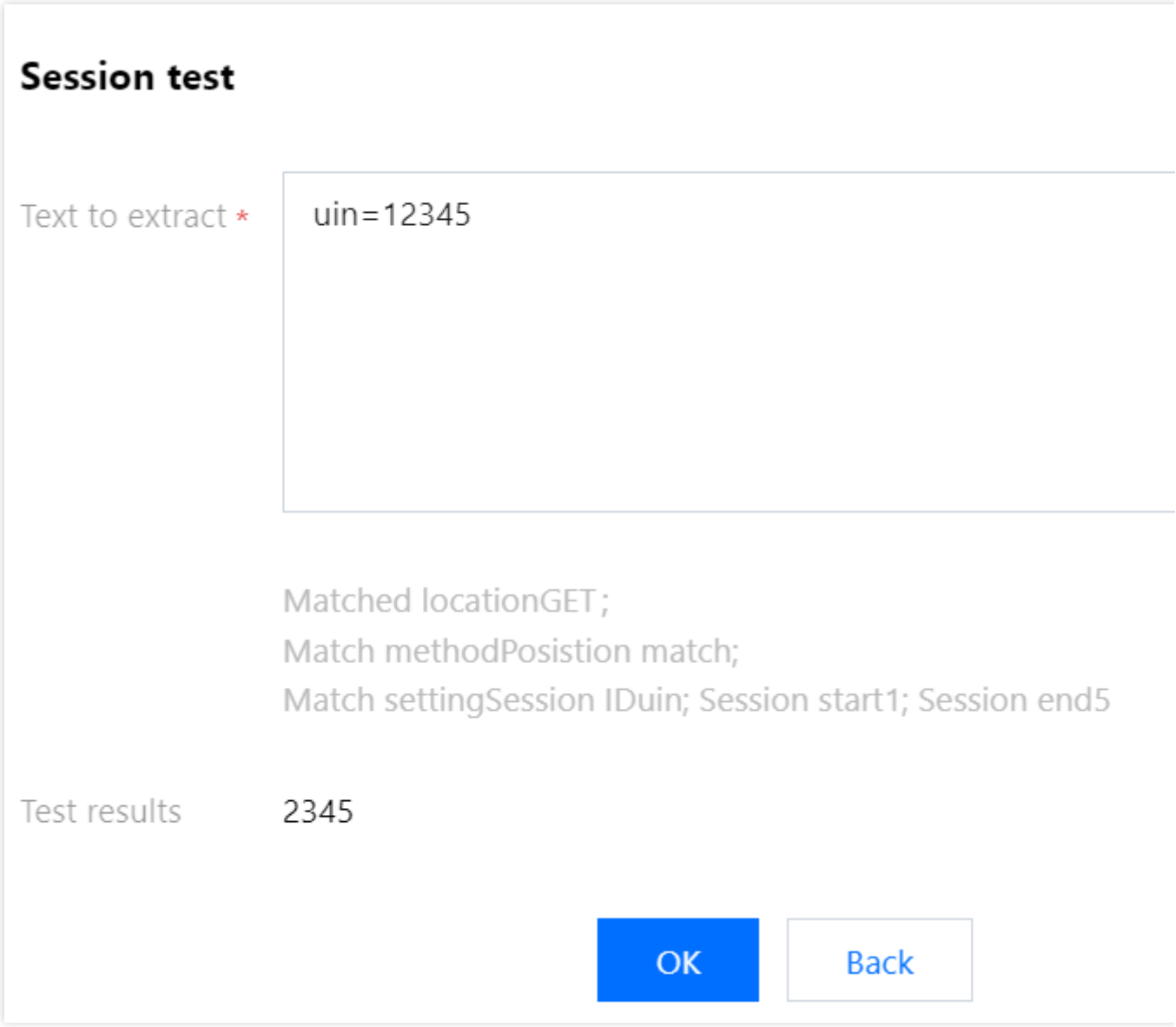
字符串匹配模式下，SESSION 标识为 cookie_2 =，结束字符为“;”，则匹配内容为456。

位置匹配模式下，SESSION 标识为 cookie_2，开始位置为0，结束位置2，则匹配内容为456。

5. SESSION 维度信息测试。添加完成后，单击**测试**将填写内容进行测试。



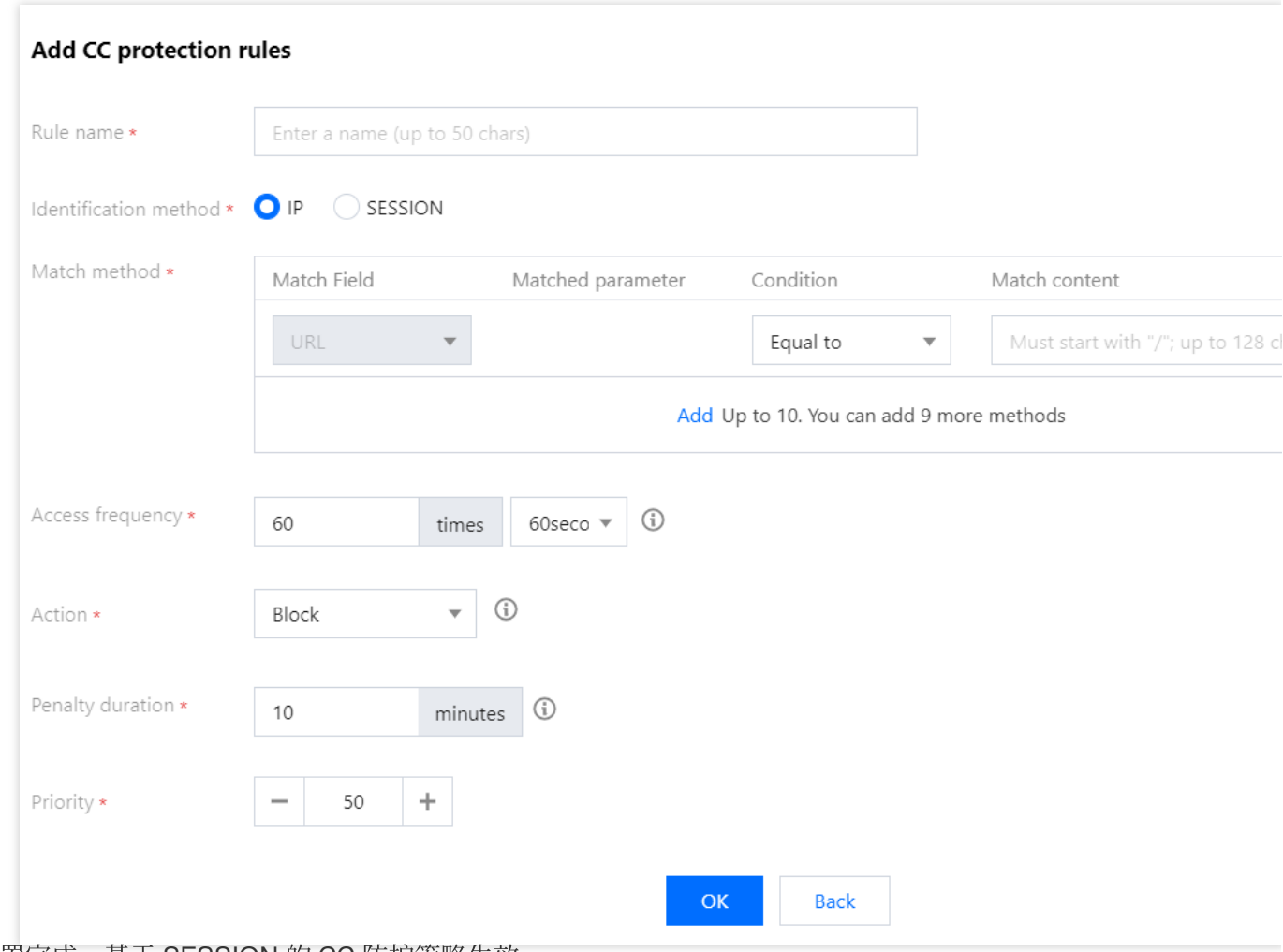
6. 进入 SESSION 设置页面，设置内容为 security = 0123456789……，后继 Web 应用防火墙将把 security 后面10位字符串作为 SESSION 标识，SESSION 信息也可以删除重新配置。



7. 设置基于 SESSION 的 CC 防护策略，配置过程和 示例二 保持一致，识别模式选择 SESSION 即可。

说明：

以 GET 位置为 SESSION 标识设置 CC 规则，当 CC 规则启用后，会把相同的 SESSION 标识作为维度拦截，而不是将 IP 作为维度。



8. 配置完成，基于 SESSION 的 CC 防护策略生效。

注意：

使用基于 SESSION 的 CC 防护机制，无法在 IP 封堵状态中查看封堵信息。

前后端分离站点接入 WAF 验证码

最近更新时间：2023-12-29 14:55:07

在前后端分离或 App 站点中接入 WAF 验证码，可以实现在前后端分离站点或 App 站点动态下发验证码。
前后端分离站点接入 WAF 验证码流程，适用于利用 WAF 进行 前后端分离站点动态进行人机验证的场景（如命中自定义规则、CC 攻击、BOT 流量管理等），App（iOS 和 Android） 皆使用 Web 前端 H5 方式进行接入。

前提条件

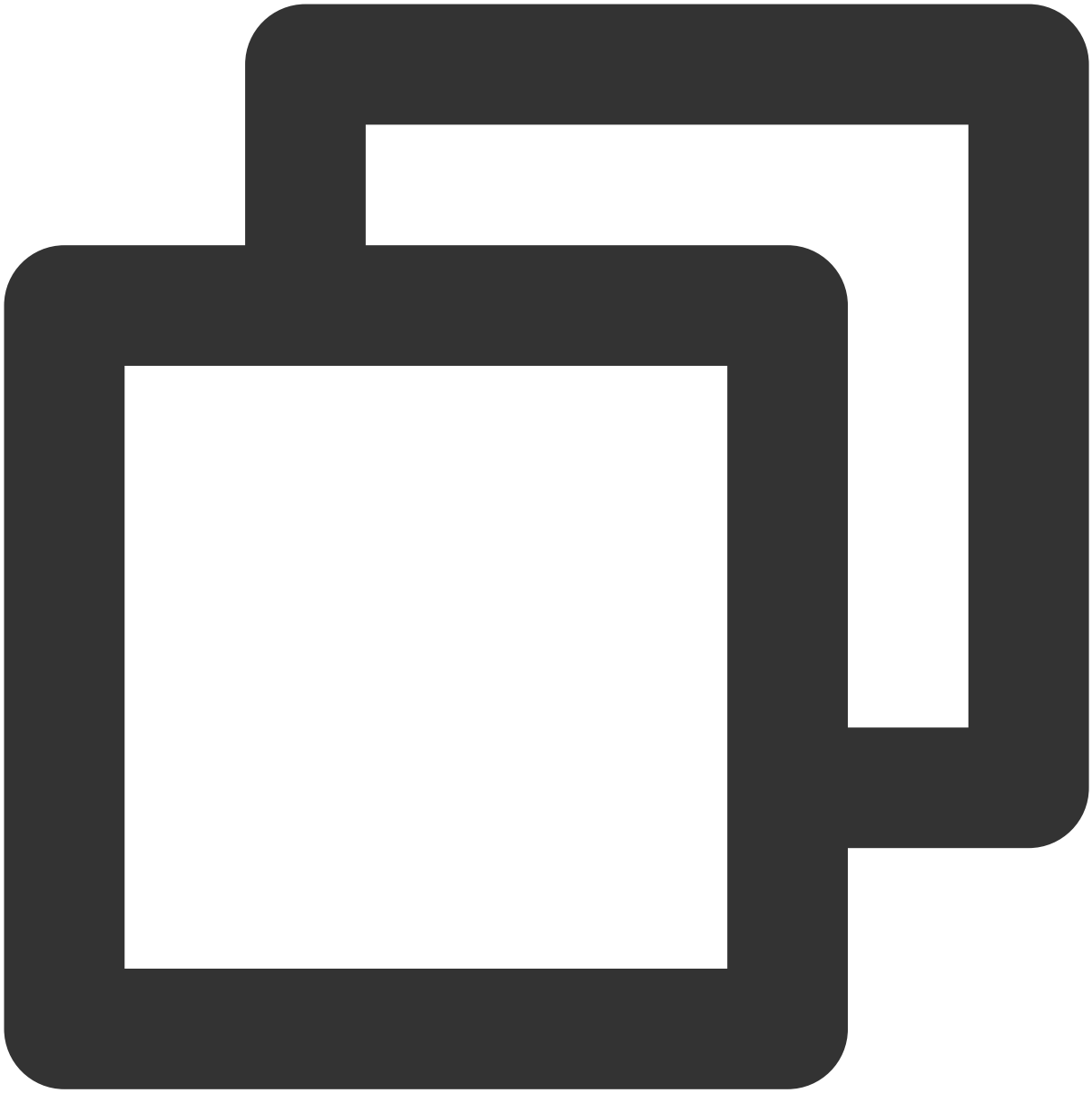
已购买 Web 应用防火墙（高级版及以上），并完成 接入 WAF。

检出原理

通过动态识别服务端返回包中是否包含 WAF 下发的验证码的相关字段，如果包含 WAF 下发的验证码的相关信息时，在顶部浮层渲染验证码，实现前后端分离站点或 App 进行 WAF 站点验证码接入。

操作步骤

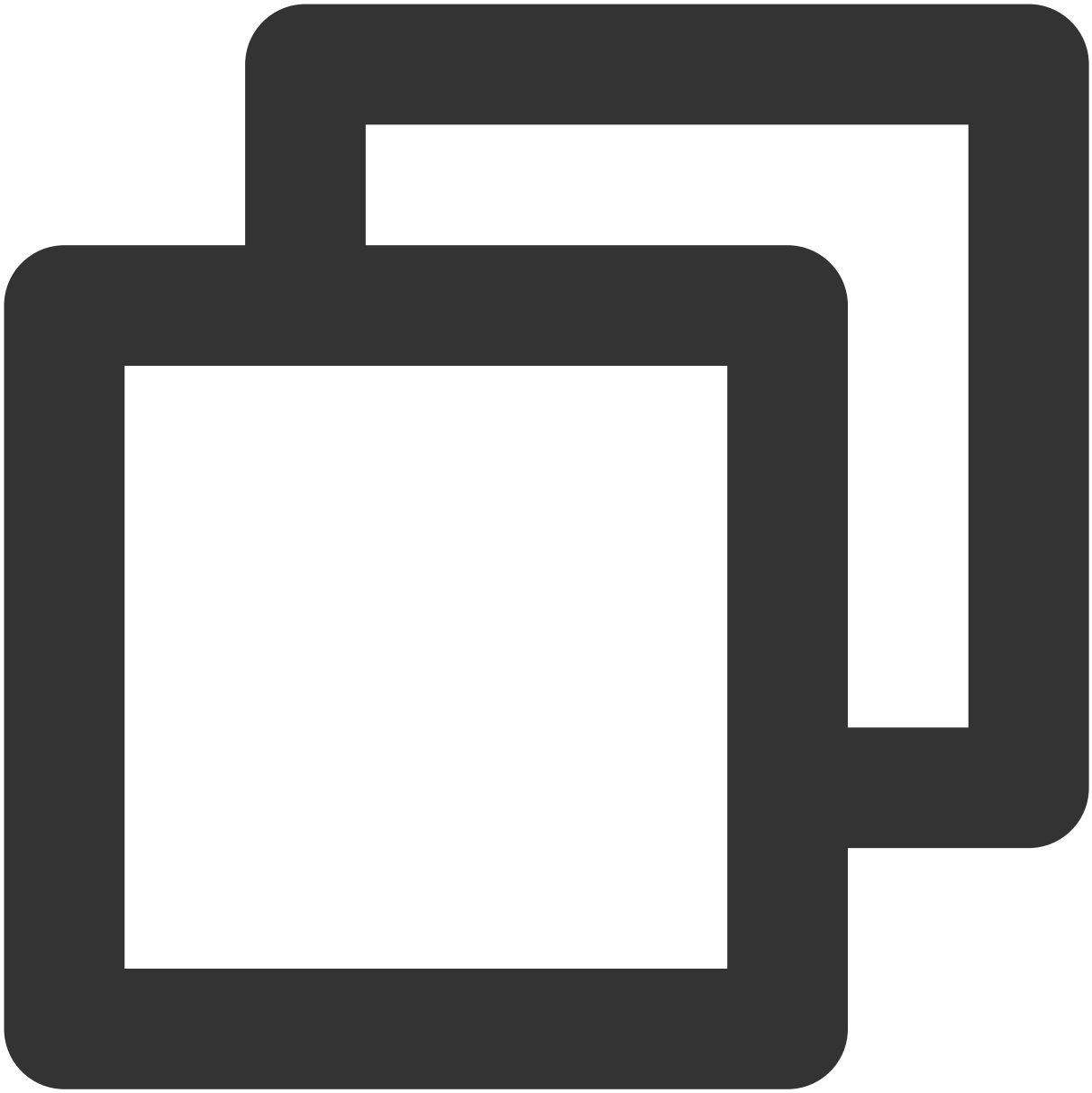
以下代码为接入WAF 验证码示例代码（以 axios 为例），根据应用场景，以此作为参考完成前后端分离站点的接入 WAF 验证码。
1. Axios Response 增加 interceptors。



```
 //WAF 验证码seqid相关正则
const sig_data = /seqid\\s=\\s"(\\w+)"/g
const waf_id_data = /TencentCaptcha\\((\\'\\d+\\')/g

const service = axios.create({
baseURL: '/api',
timeout: 10000,
withCredentials: true
});

service.interceptors.response.use((response)=>{
```

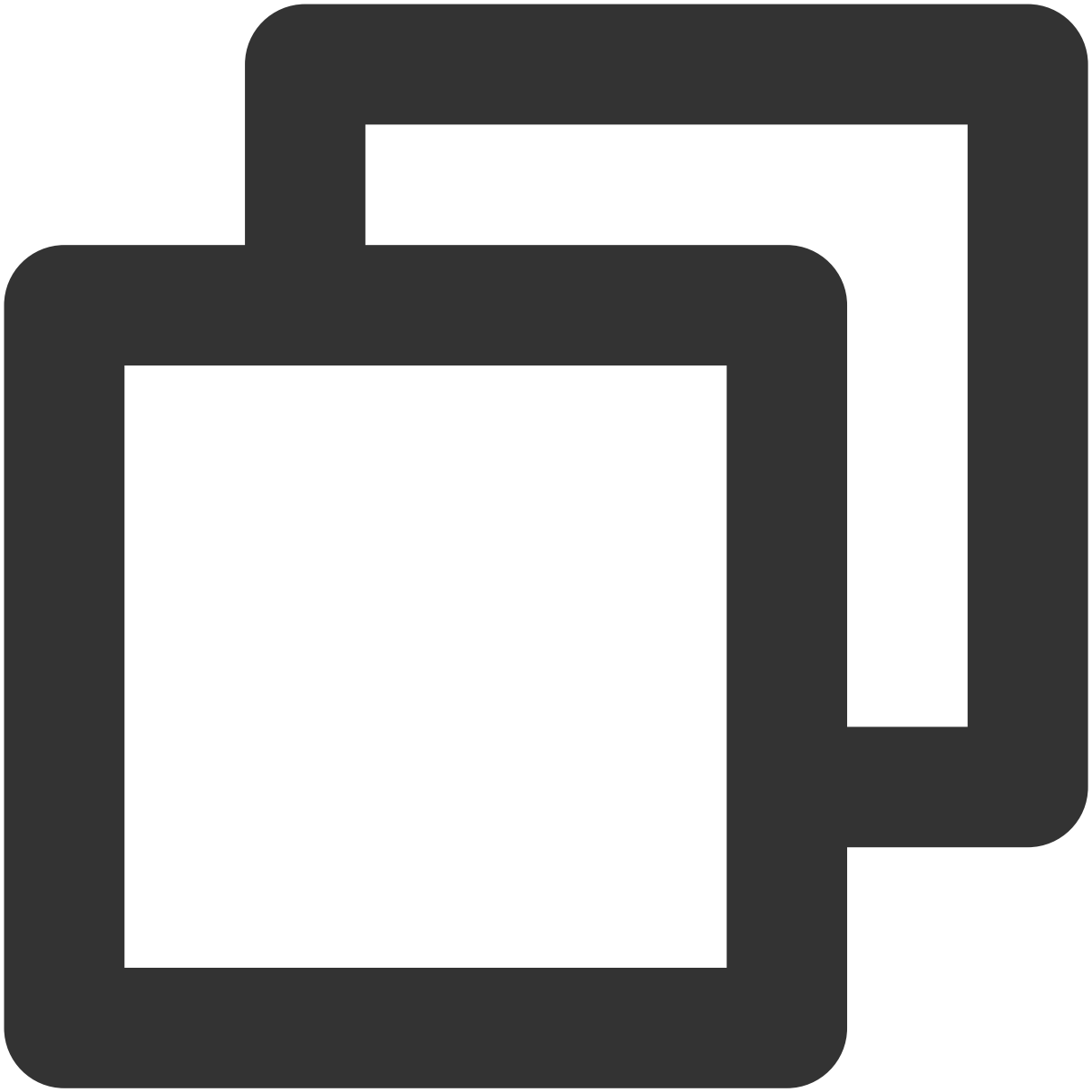
```
const res = response.data;
if(res.code === 0){
  return res;
}else{
  //捕捉错误及渲染验证码
  const matches = sig_data.exec(res);
  if(matches){
    //展示验证码
    let seqid = matches[1];
      const wid_matches = waf_id_data.exec(res);
    let wid = wid_matches[1]
    var captcha = new TencentCaptcha(wid, function(res){
      var captchaResult = []
      captchaResult.push(res.ret)
      if(res.ret === 0){
          captchaResult.push(res.ticket)
          captchaResult.push(res.randstr)
          captchaResult.push(seqid)
      }
      var content = captchaResult.join('\\n')
      axios.post(
        "/WafCaptcha",content
      ).then().catch();
    });
    captcha.show()
  }else{
    return res;
  }
}
},()=>{});
export default service;


Vue.prototype.$axios = service;
```

2. 调用 API 时使用增加 interceptors 的 axios。



```
 getTopic:function(){
this.$axios.get("/api.php").then(res => {
this.topic = res
});
}
```

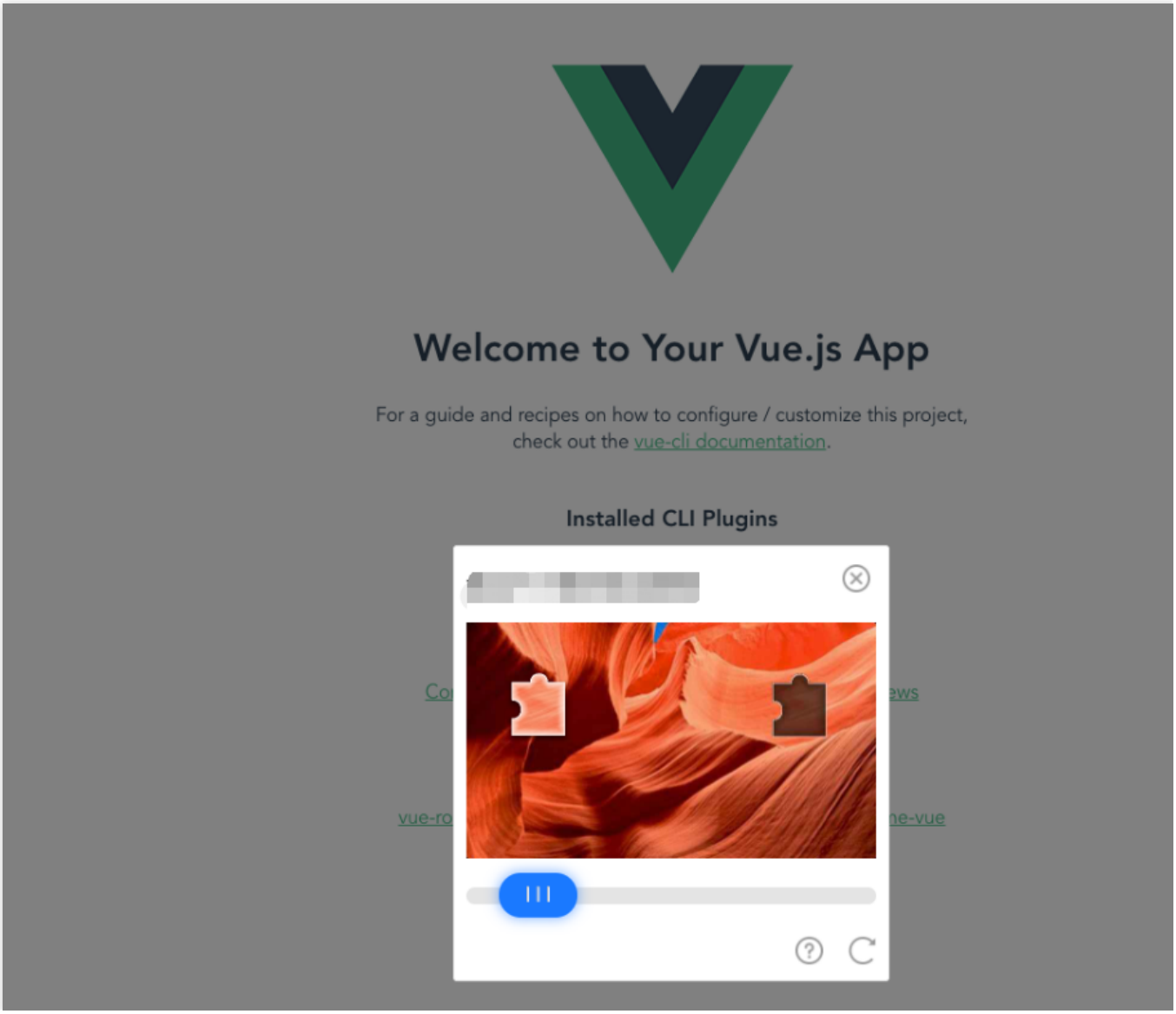
3. 全局引入验证码脚本，即在 public/index.html 引入 `<script src="https://ssl.captcha.qq.com/TCaptcha.js"></script>` 。



```
<!DOCTYPE html>
<html lang="">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width,initial-scale=1.0">
<link rel="icon" href="<%= BASE_URL %>favicon.ico">
<title><%= htmlWebpackPlugin.options.title %></title>
</head>
<body>
<noscript>
```

```
<strong>We're sorry but <%= htmlWebpackPlugin.options.title %> doesn't work properl
</noscript>
<script src="https://ssl.captcha.qq.com/TCaptcha.js"></script>
<div id="app"></div>
<!-- built files will be auto injected -->
</body>
</html>
```

4. 输入上述代码后，编译并部署至服务器上即可。
5. 在 WAF 配置自定义规则，通过异步请求，查看当前页面是否展示验证码弹窗。



BOT 流量管理接入最佳实践

最近更新时间：2023-12-29 14:55:25

本文将介绍如何接入 BOT 流量管理，以及日常运营对抗恶意流量的最佳实践。方便您快速进行相关业务接入 BOT 流量管理，快速识别并对抗恶意流量。

前提条件

BOT 流量管理需要购买 WAF 对应实例的扩展包。

说明：

WAF 企业版、旗舰版用户当前可免费试用新版本的 BOT 流量管理功能，以观察网站受 BOT 影响的情况。

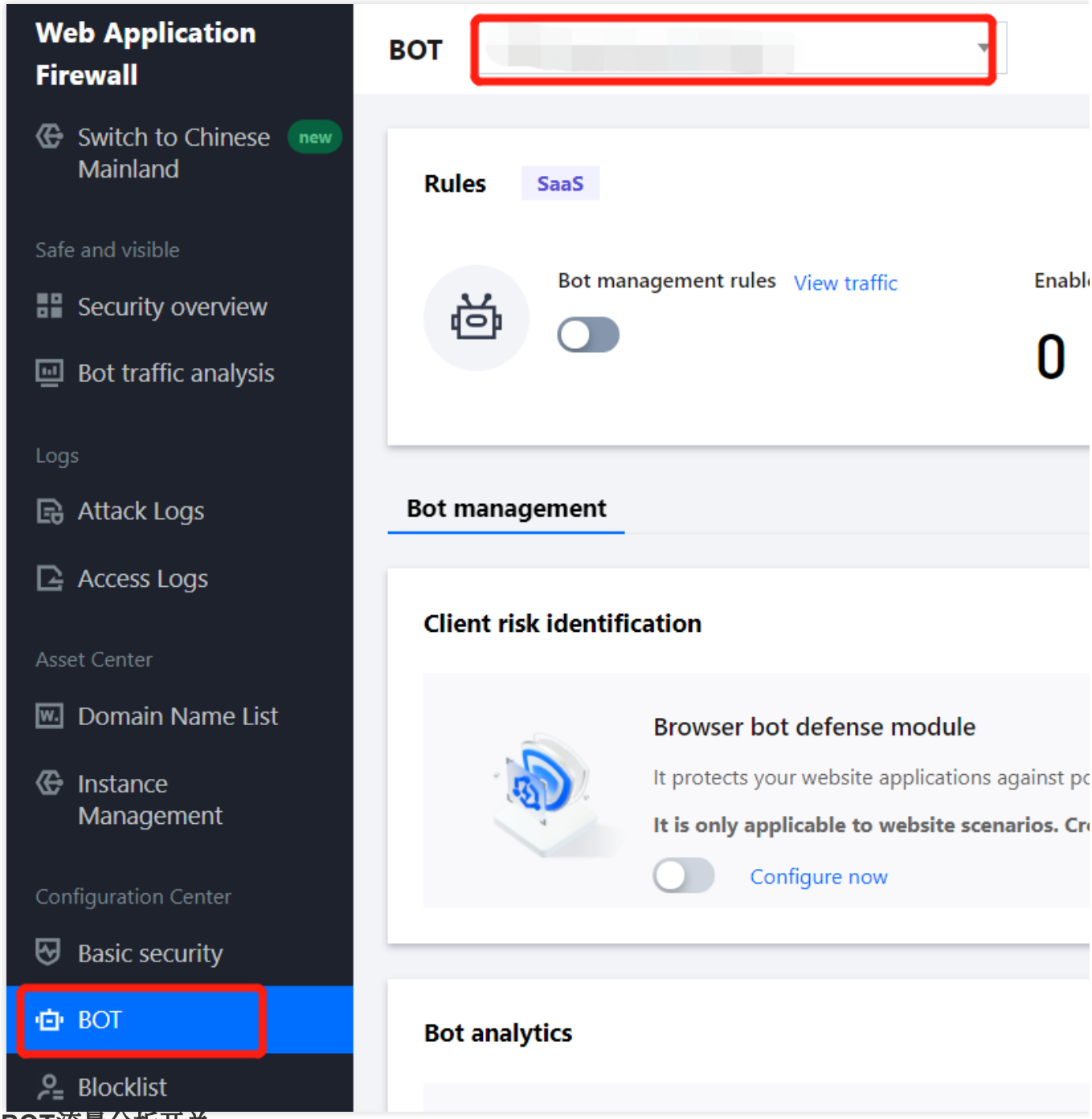
解析验证码

当客户端类型为 App、小程序、客户端以及跨域调用时，由于无法解析识别来自 WAF 下发的验证码，导致 BOT 流量管理在下发人机识别动作时，无法正常解析及弹出人机识别验证码，用户便无法正常进行人机识别交互，在触发多次验证码后，造成正常用户的访问请求被拦截，导致业务受损。

因此，在配置处置动作为人机识别时，需要对前端/客户端业务进行针对性改造，使其可以适配相关验证码，相关改造文档可参见 前后端分离站点接入 WAF 验证码。

通用业务接入业务

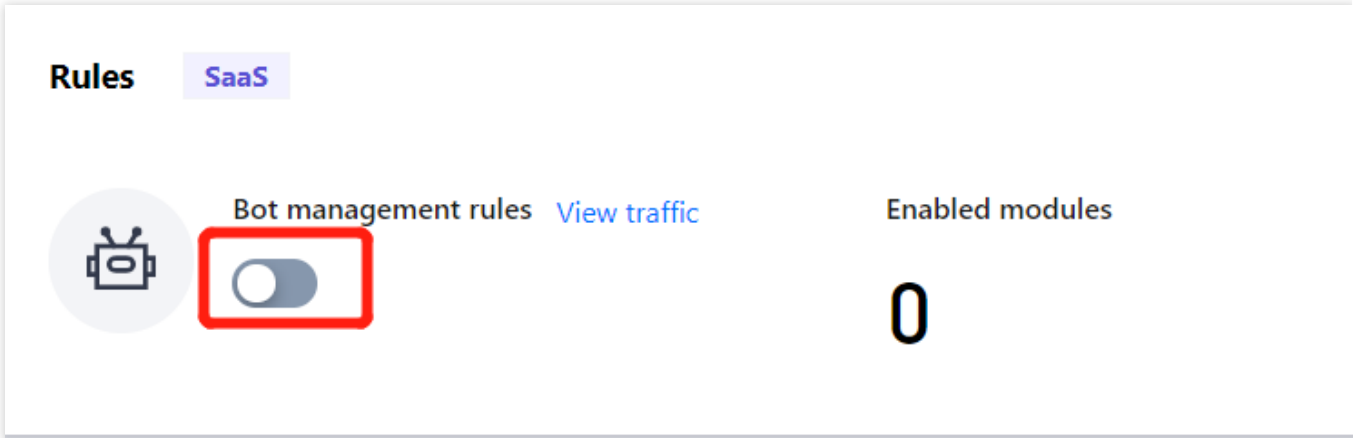
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**，进入 BOT 与业务安全页面。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



开启 BOT流量分析开关

在 BOT 管理页面，单击规则概览的

，即可开启 BOT 流量分析。



设置前端对抗

1. 在 BOT 管理页面的前端对抗模块，单击

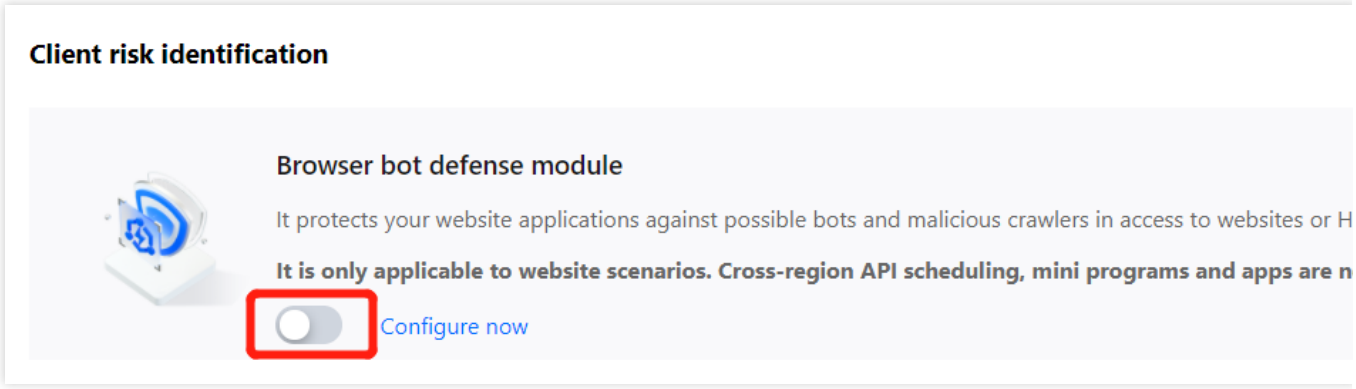
开启前端对抗分析开关。

注意：

确认当前访问客户端类型：公众号/H5、APP、小程序、客户端。

当客户端类型有且仅有浏览器/公众号/H5 并且跨域调度时，开启前端对抗，以达到最佳的防护效果。

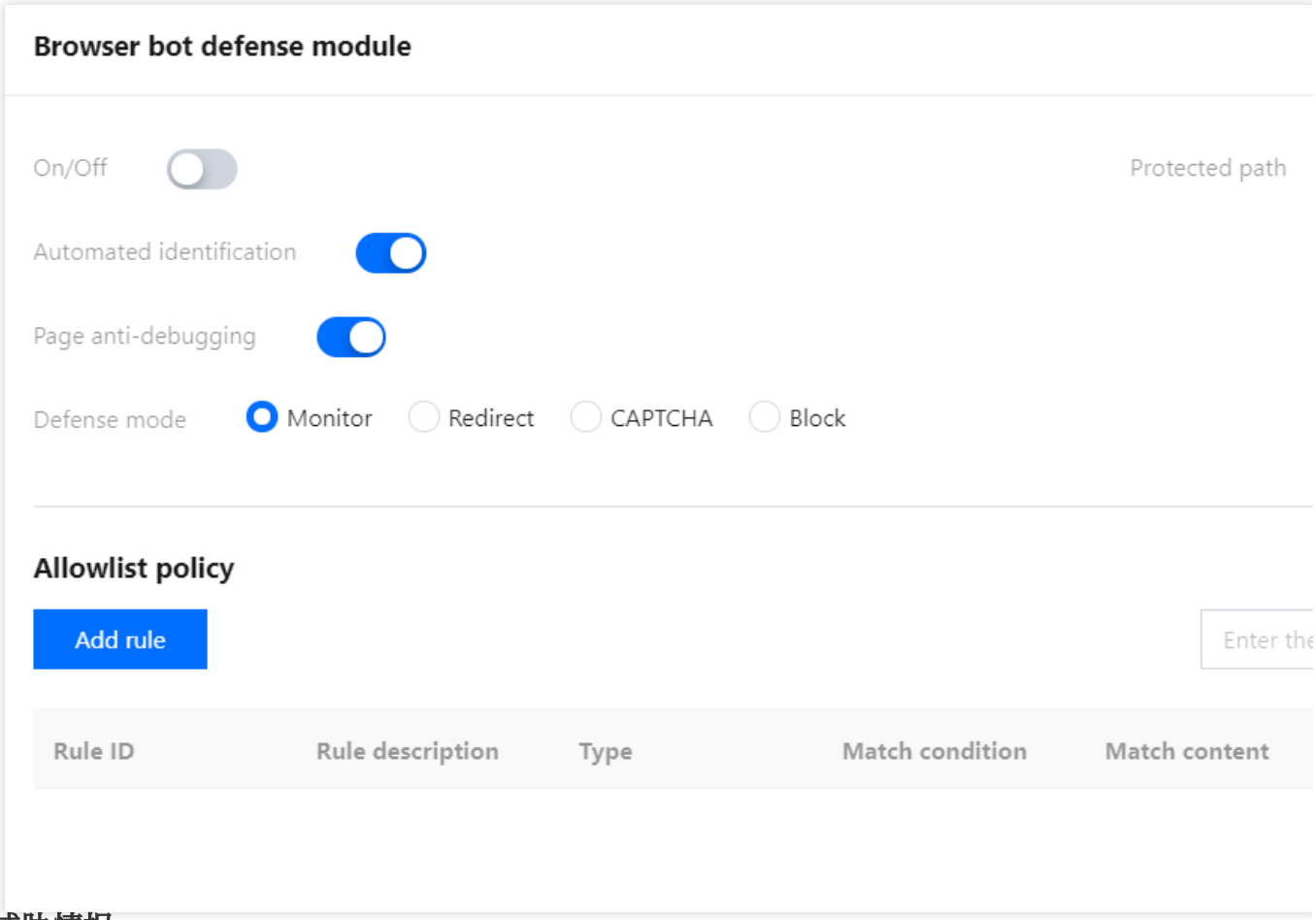
开启前端对抗后，访问前端对抗保护路径将会校验客户端是否有 JavaScripts 解析能力，会下发一段 JavaScripts 代码作为验证当前客户端是否为真实浏览器。小程序、APP、以及 API 调用由于不会主动解析 WAF上下发的质询功能，会导致客户端无法正常解析。



2. 在前端对抗模块，单击**前往设置**，对重点页面进行防护配置。

说明：

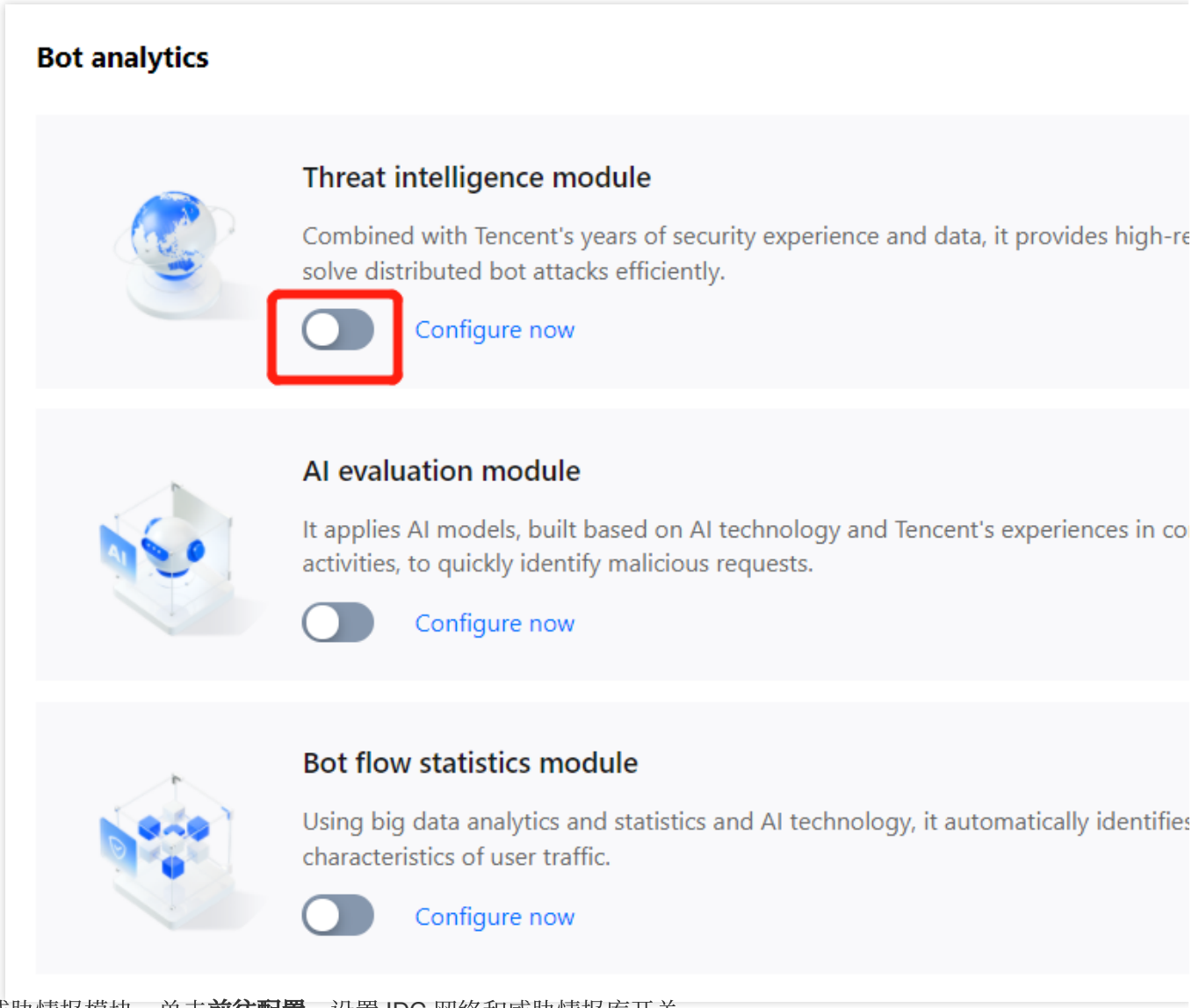
更多操作详情请参见 BOT 管理 。



设置威胁情报

1. 在 BOT 管理页面的威胁情报模块，单击

，即可开启威胁情报模块。初次开启威胁情报开关将会开启所有识别项，开启对应识别项后可识别来自威胁情报、IDC 的访问源。并提供不同的恶意程度。



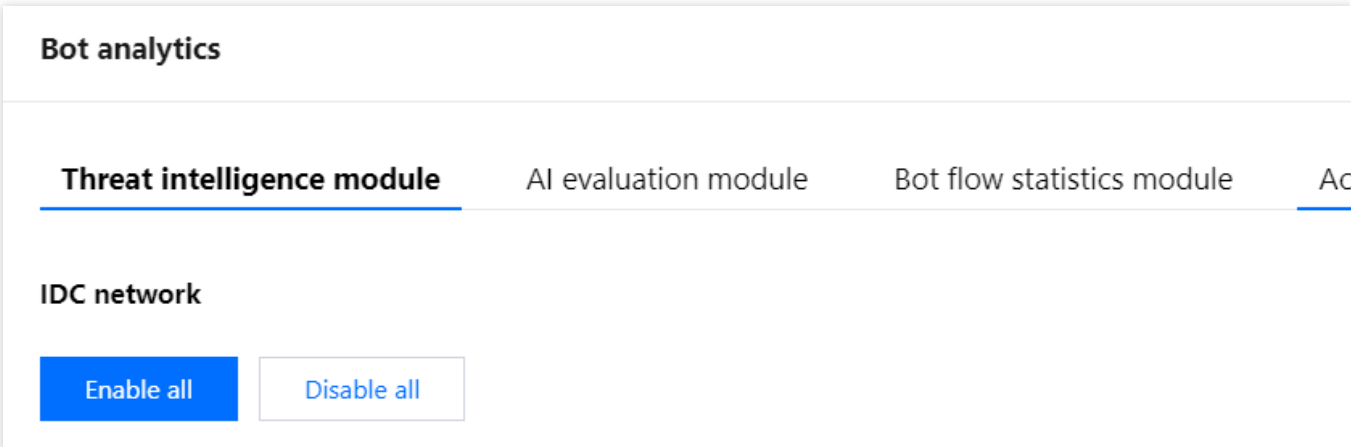
2. 在威胁情报模块，单击**前往配置**，设置 IDC 网络和威胁情报库开关。

说明：

当前业务存在业务回调接口在 IDC 域内：

如果不清楚来源 IP，请 联系我们 对 IDC 进行加白处理，即关闭对应威胁情报中对应业务 IDC 的选项。

如果清楚当前回调业务的 IP，请在 BOT-自定义规则处加白对应来源 IP，详情请参见 精准白名单管理。



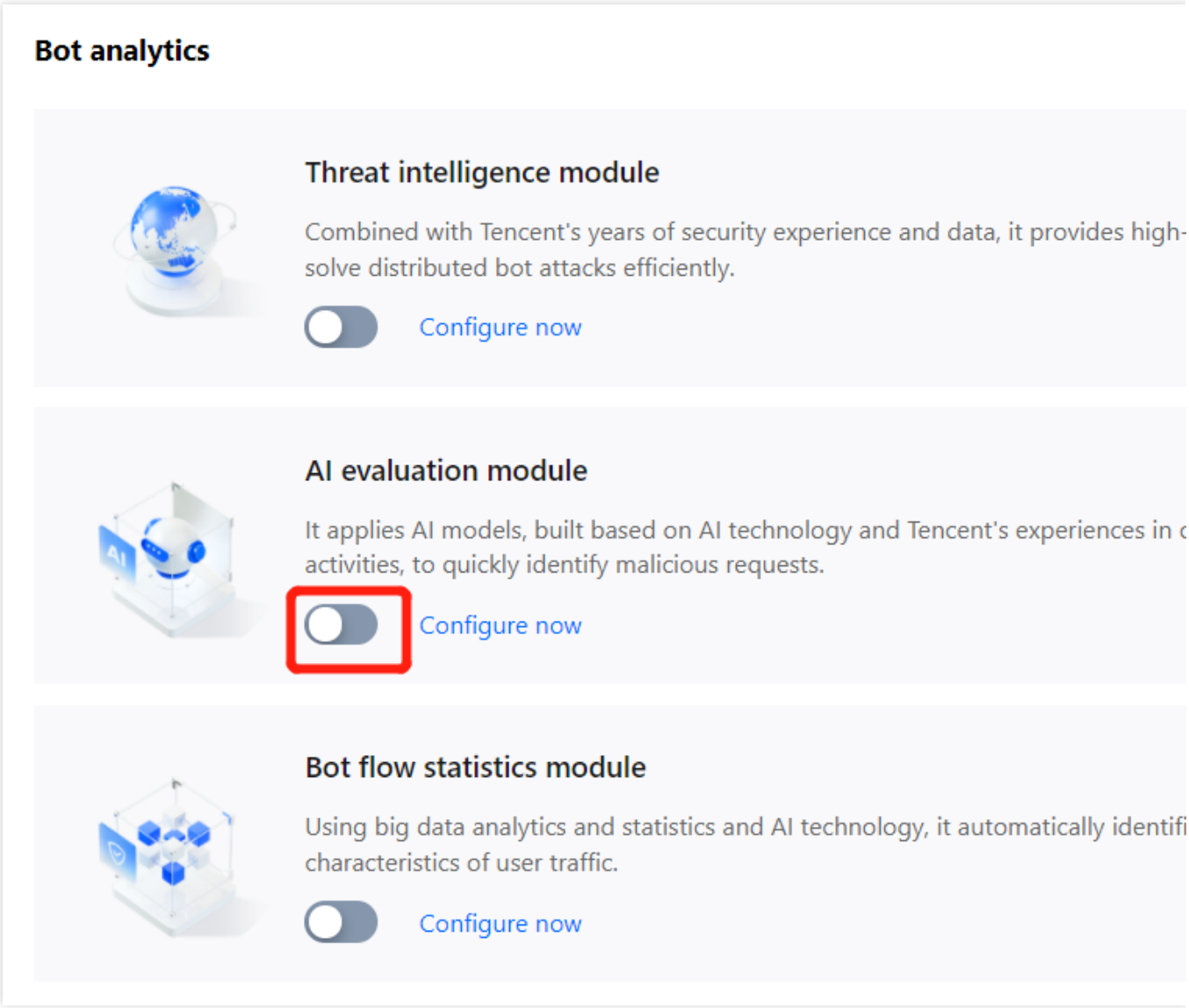
IDC network type	IDC network description
Aws	The IPs belong to the AWS (IDC IP) IP library, and are often exploited by attackers to dep
Azure	The IPs belong to the Microsoft Azure (IDC IP) IP library, and are often exploited by attac
Google	The IPs belong to the GCP (IDC IP) IP library, and are often used by attackers to deploy b
UCloud	The IPs belong to the UCloud (IDC IP) IP library, and are often exploited by attackers to c
Alibaba Cloud	The IPs belong to the Alibaba Cloud (IDC IP) IP library, and are often exploited by attacke
Baidu Cloud	The IPs belong to the Baidu Cloud (IDC IP) IP library, and are often exploited by attackers
Huawei Cloud	The IPs belong to the Huawei Cloud (IDC IP) IP library, and are often exploited by attacke
Kingsoft Cloud	The IPs belong to the Jinshan Cloud (IDC IP) IP library, and are often exploited by attacke
pubyun	The IPs belong to the Baidu Cloud (IDC IP) IP library, and are often exploited by attackers
Qing Cloud	The IPs belong to the Qing Cloud (IDC IP) IP library, and are often exploited by attackers
Tencent Cloud	The IPs belong to the Tencent Cloud (IDC IP) IP library, and are often exploited by attacke

Threat intelligence library

开启 AI 评估开关

在 BOT 管理页面的 AI 评估模块，单击

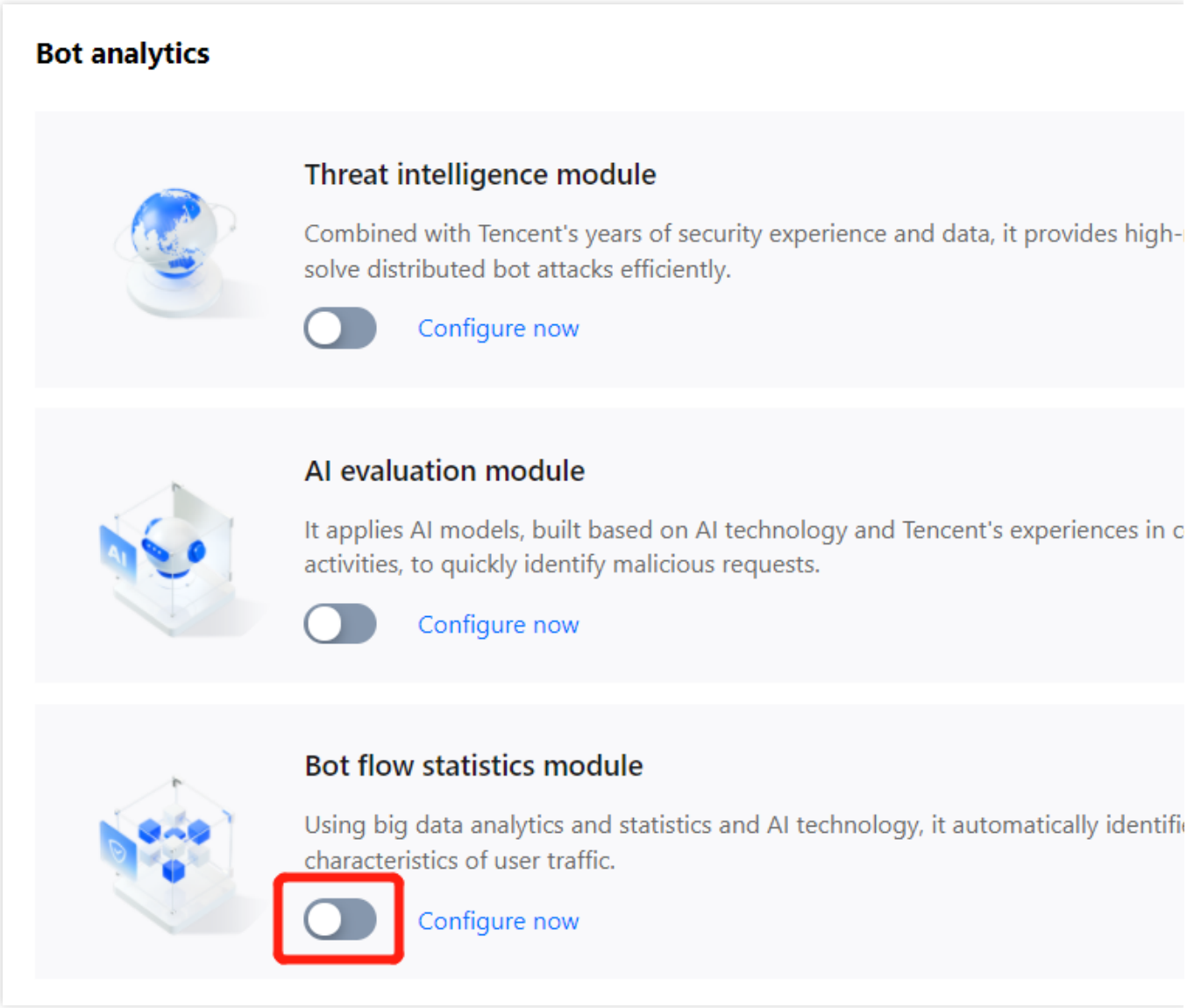
，即可开启 AI 评估模块。



开启智能统计开关

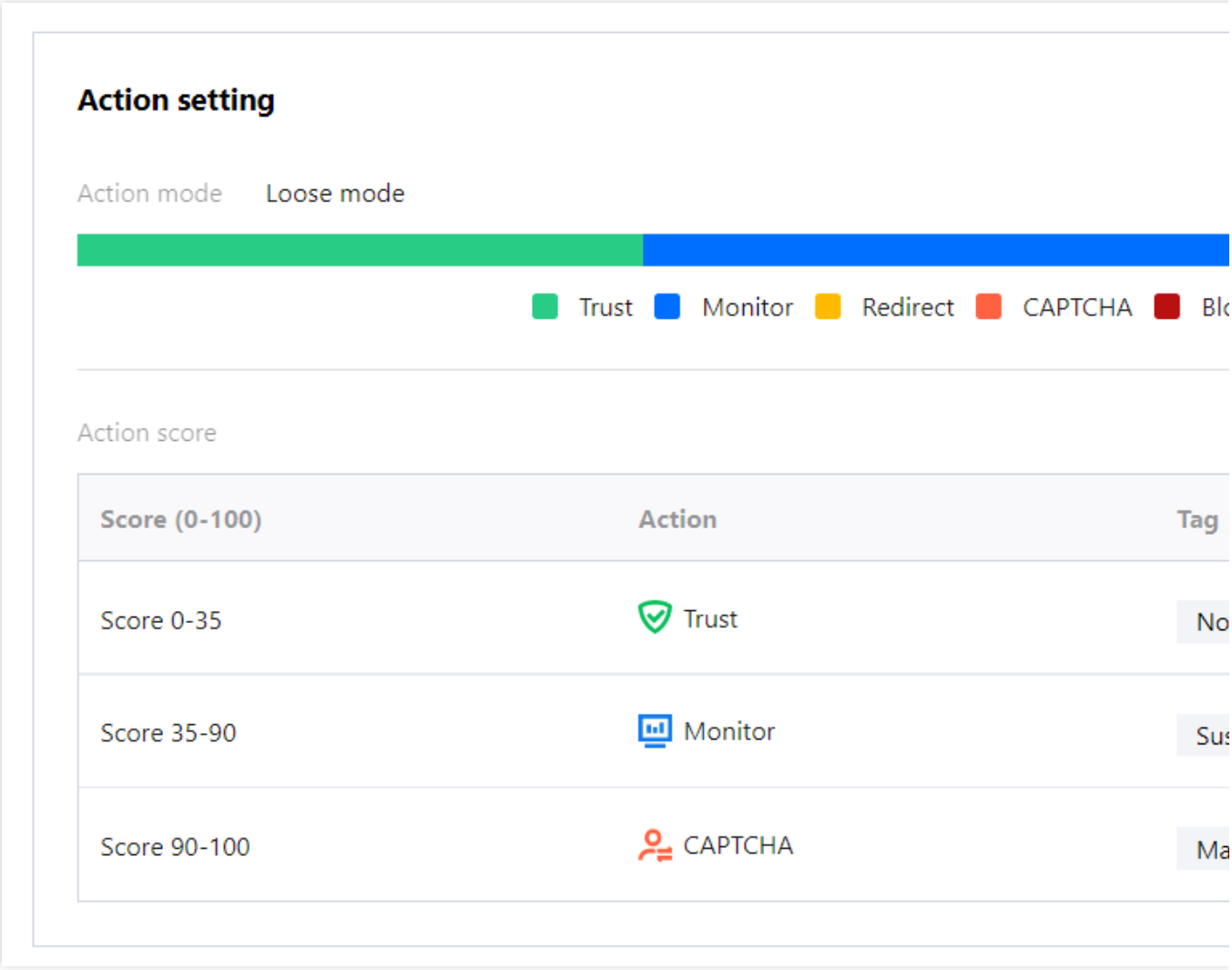
在 BOT 管理页面的智能统计模块，单击智能统计模块的

，即可开启智能统计模块。

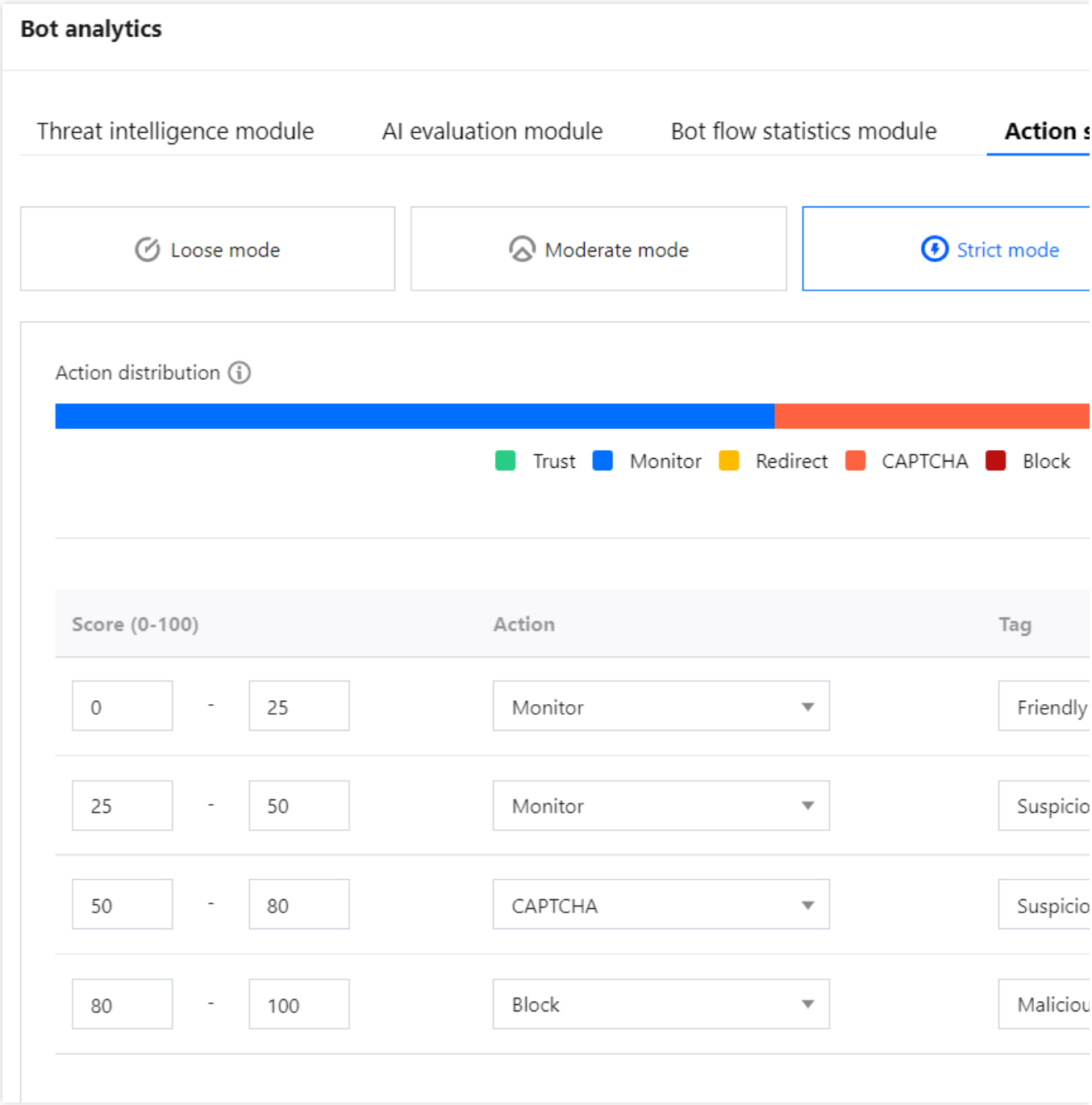


设置动作得分

1. 在 BOT 管理页面的动作设置模块，单击**配置动作得分**。



2. 在动作设置页面，用户可根据配置不同分数段的动作实现风险访问的精准拦截。



参数说明

模式设置：提供宽松模式、中等模式、严格模式、自定义模式这四种默认处置模式，宽松、中等、严格这三种模式为预设模式，分别代表 BOT行为管理针对不同危害程度的 BOT 的推荐分类及处置策略。这三种预设模式可进行修改，修改后为自定义模式。

分数段设置：分数段区间总分数为 0-100 分，每个分数段总共可以添加10条，配置的分数区间范围左闭右开，分数段不可重合，分数区间可设置为空，设置为空时，空的分数段不处置动作。

动作设置：可设置为信任、监控、重定向（重定向至特定网站 URL）、人机识别（验证码）或拦截。

标签设置：可设置为友好 BOT、恶意 BOT、正常流量或疑似 BOT。

友好 BOT：为默认对网站友好/合法的 BOT。

疑似 BOT： 为识别出该访问源流量疑似为 BOT，但无法判断其对网站的是否为有害。

正常流量：识别访问的流量为正常人类。

恶意 BOT：为对网站产生恶意流量/访问请求不友好的 BOT。

3. 设置完成后，单击界面左下方的**立即发布**，即可生效。