Web 应用防火墙

操作指南

产品文档

腾讯云

文档目录

操作指南

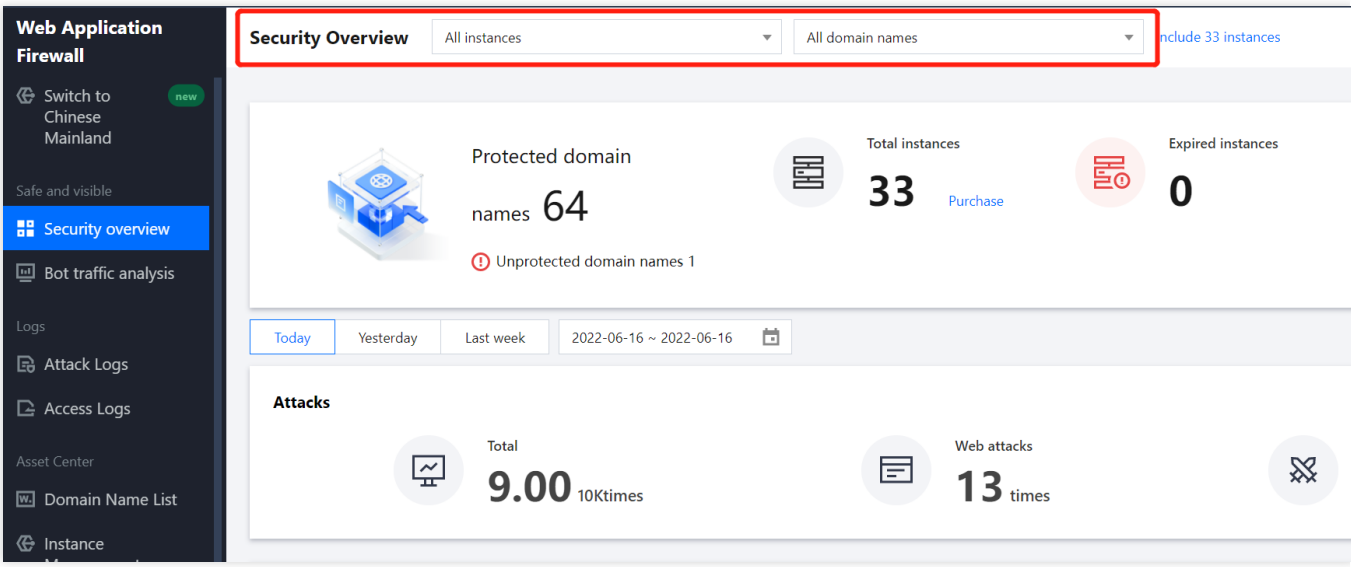
概览

最近更新时间：2023-12-29 11:38:15

概览页面可浏览当前账户下 WAF 实例信息，攻击概览，安全分析等模块。

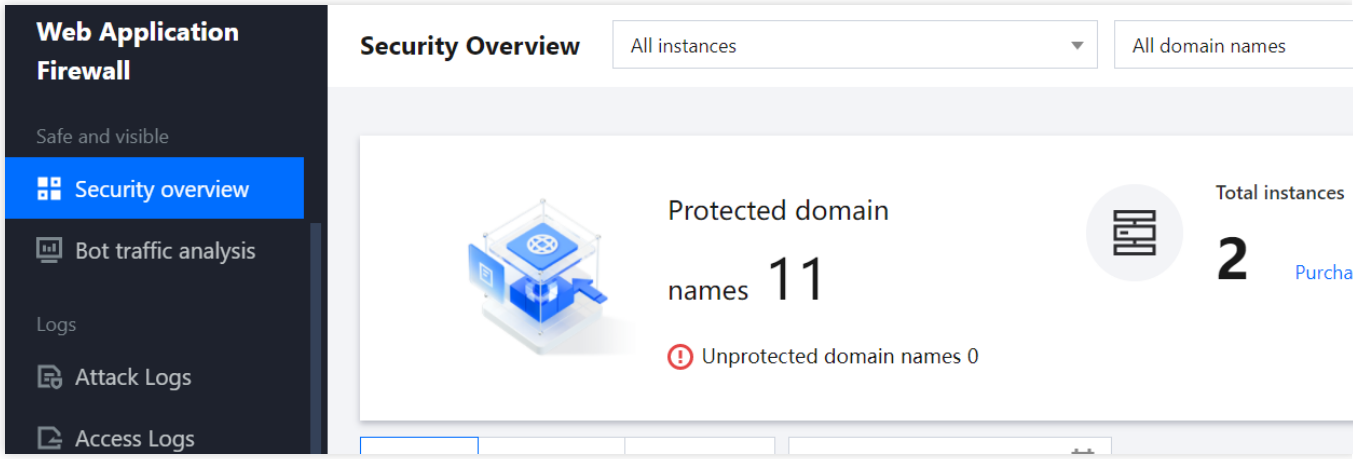
安全概览

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**概览**，进入概览页面。
2. 在概览页面，左上角选择对应域名，即可查看该域名的概览信息。



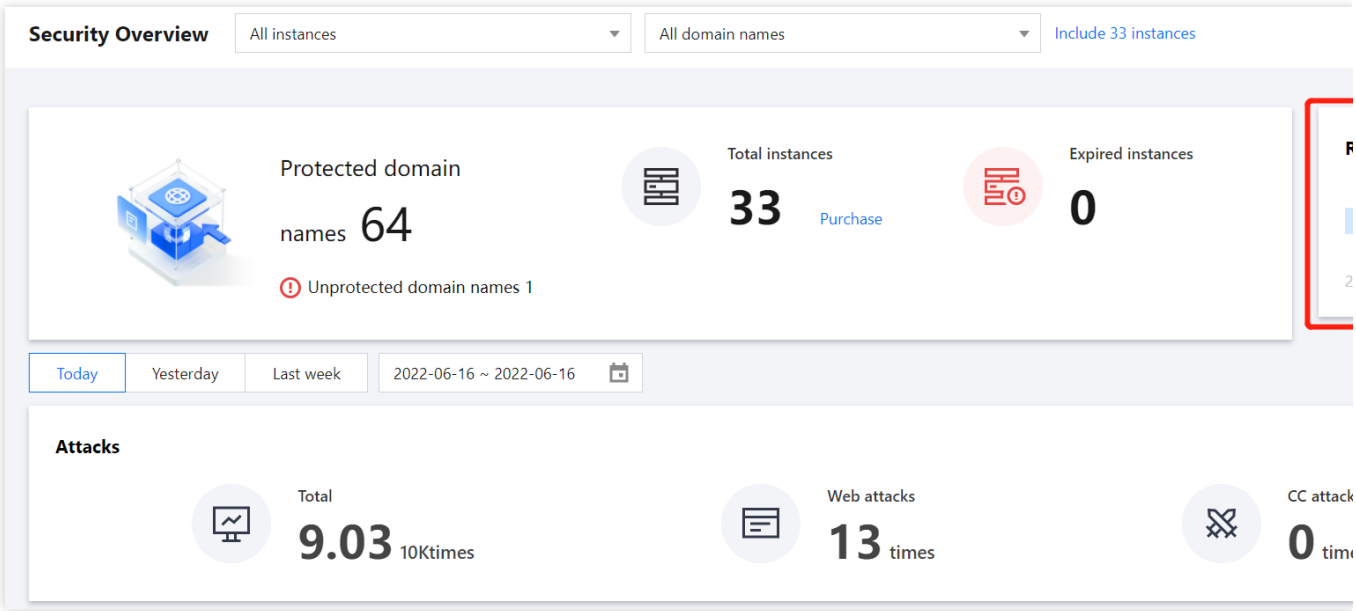
实例概览

在概览页面，左上角选择对应域名，单击**包含x个实例**，即可查看当前账户下已购实例过期信息。



规则更新动态

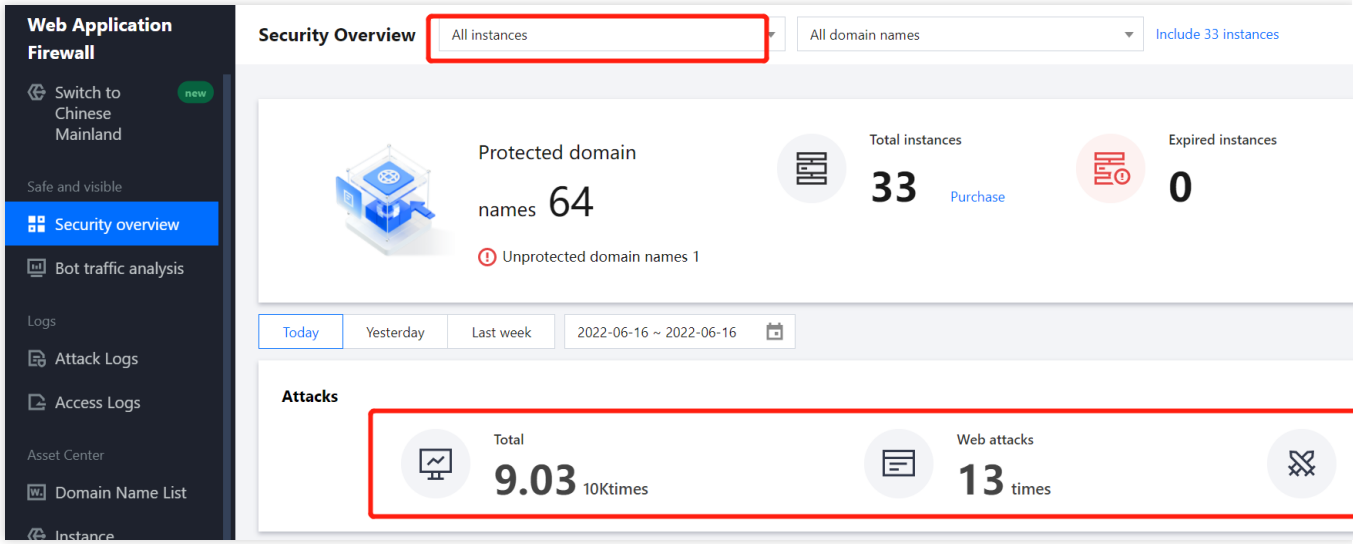
在概览页面的规则更新动态模块，单击右上角的**查看更多**，即可查看当前 WAF 支持的 Web 规则库。



攻击总览

全部域名

1. 当安全概览为全部域名时，攻击总览统计数据为全局攻击数，统计周期可以通过筛选显示。



2. 同时，在页面下方可以查看域名 Web 攻击次数 TOP5(次)、攻击来源 IP TOP5(次) 、域名 CC 攻击次数 TOP5(次)等信息。

字段说明：

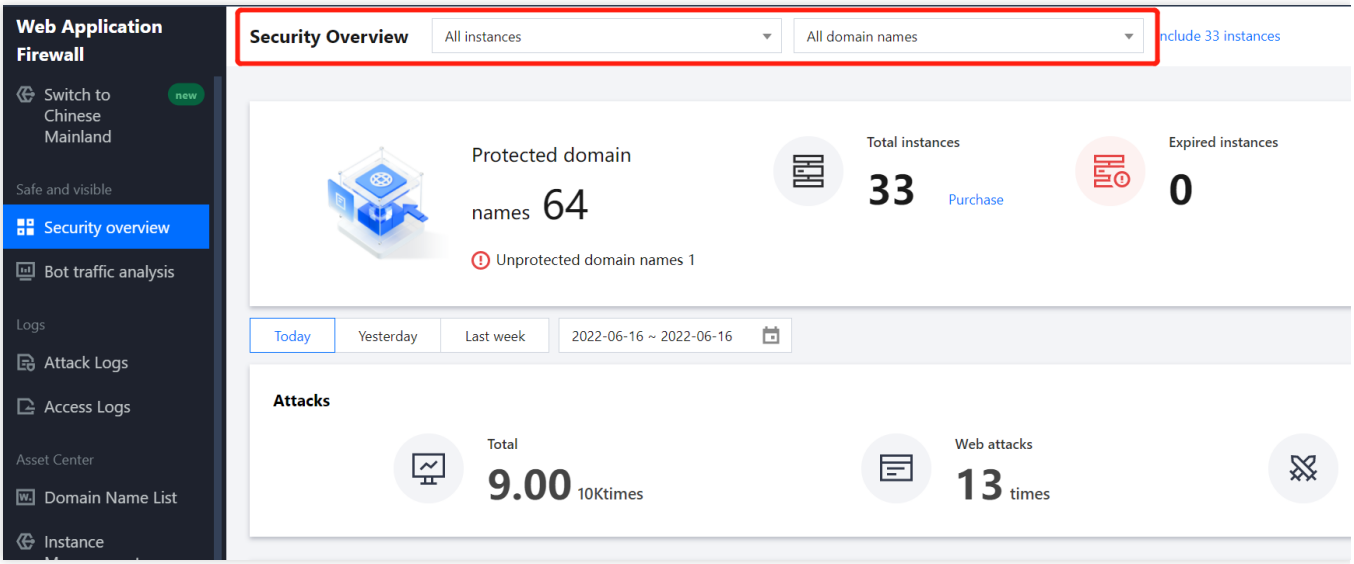
域名 Web 攻击次数 TOP5(次)：展示全部实例中受到攻击最多的5个域名。

攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的5个 IP。

域名 CC 攻击次数 TOP5(次) ：展示全部实例中受到攻击最多的5个域名。
请求来源 IP TOP5(次) ：展示全部实例中访问最多的5个 IP。
攻击来源区域分布(次)：展示全部实例中攻击来源分布的地区。
攻击类型占比：展示全部实例中攻击类型的分布。
浏览器类型占比：展示全部实例中浏览器类型的分布。

单个域名

1. 当安全概览为单个域名时，攻击总览统计数据为单个域名收到攻击数，统计周期可以通过筛选显示。



2. 同时，在页面下方可以查看攻击来源 IP TOP5(次)、请求来源 IP TOP5(次) 、攻击来源区域分布(次)等信息。

字段说明：

攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的5个 IP。

请求来源 IP TOP5(次) ：展示全部实例中访问最多的5个 IP。

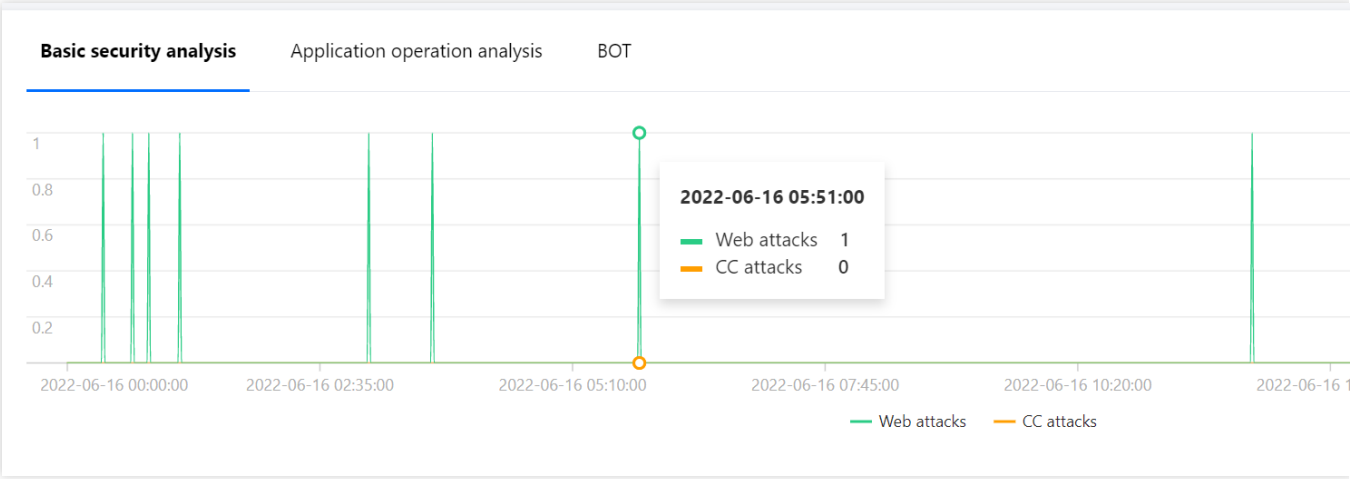
攻击来源区域分布(次)：展示全部实例中攻击来源分布的地区。

攻击类型占比：展示全部实例中攻击类型的分布。

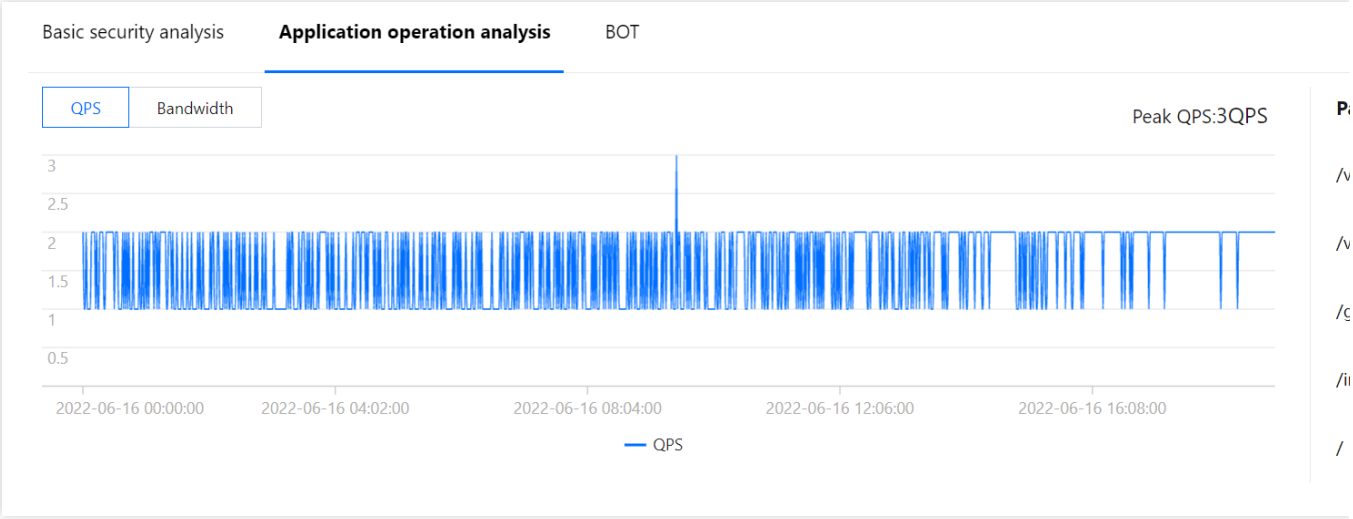
浏览器类型占比：展示全部实例中浏览器类型的分布。

概览安全分析

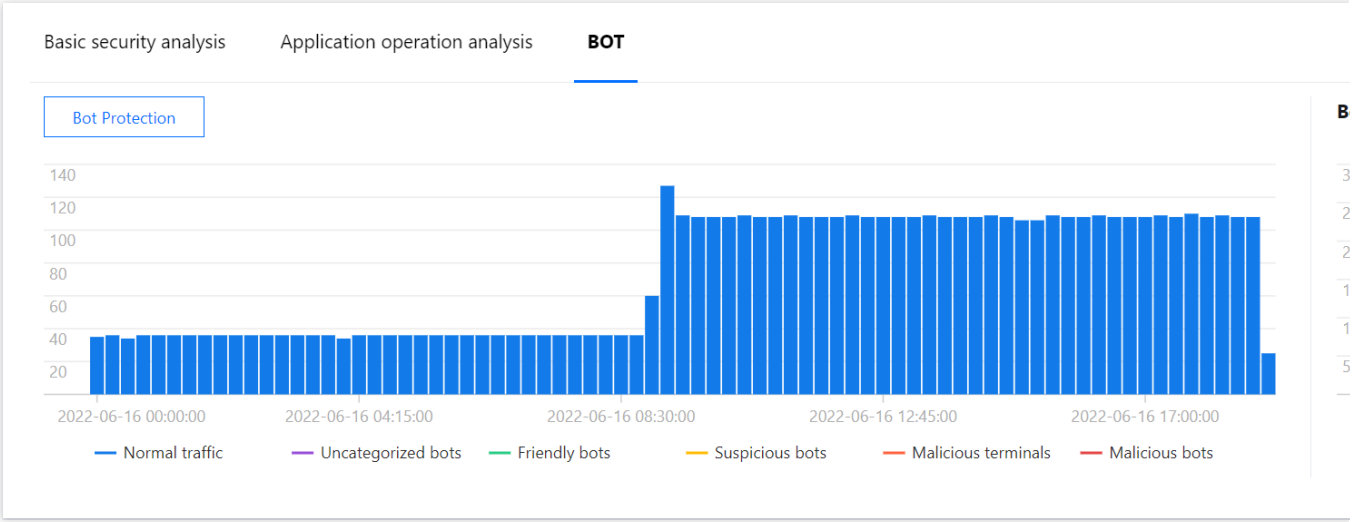
基础安全：分析描述了当前选择的域名在统计周期内所受到的 Web 攻击次数。



业务运营：分析描述了当前选择的域名在统计周期内的 QPS 及带宽详情，右侧统计了该域名统计周期内的响应及访问次数的 Top 值。



BOT 与业务安全：描述了当前域名在统计周期内的 BOT 信息，单击前往 BOT流量分析 即可查看 BOT 与业务安全的流量信息。


Basic security analysis
Application operation analysis
BOT
Bot Protection
140
120
100
80
60
40
20
2022-06-16 00:00:00
2022-06-16 04:15:00
2022-06-16 08:30:00
2022-06-16 12:45:00
2022-06-16 17:00:00
Normal traffic
Uncategorized bots
Friendly bots
Suspicious bots
Malicious terminals
Malicious bots

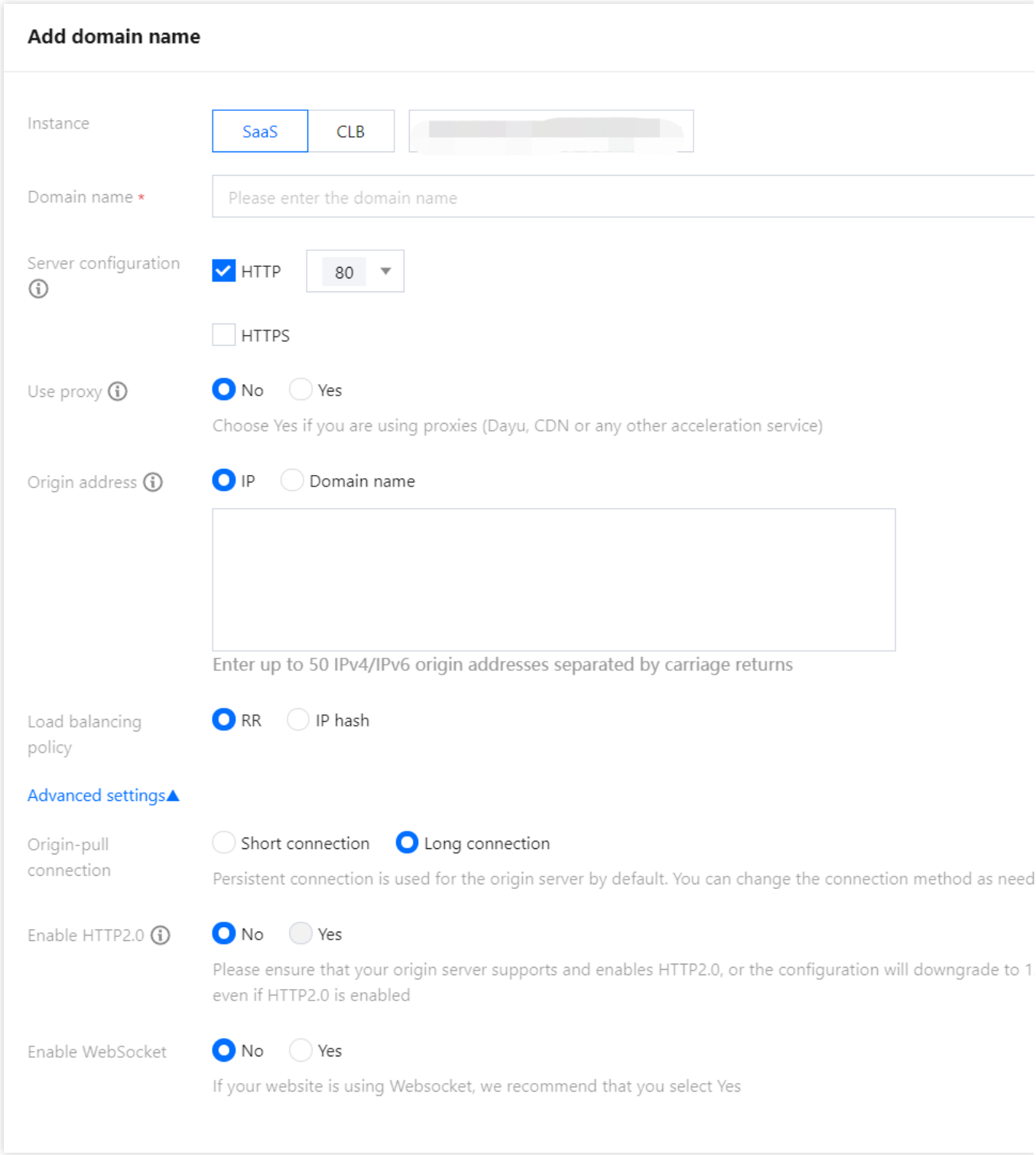
接入 SaaS 型 WAF
步骤 1：域名添加

最近更新时间：2023-12-29 14:22:46

使用 Web 应用防火墙（WAF）防护您的 Web 业务前，需要先将防护的网站接入到 Web 应用防火墙。未完成接入前，您的 Web 应用防火墙防护将无法生效。本文档将指导您如何在 SaaS 型 WAF 中接入域名。

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**资产中心** > **域名列表**，进入域名列表页面。
2. 在域名列表页面，单击**添加域名**，进入添加域名页面。
3. 在添加域名页面，配置相关基础参数。



字段说明

所属实例：选择 SaaS 型，在右侧选择所需实例。

域名：在域名输入框中添加需要防护的域名 `saas.technicalsupport.cn` 。

服务器配置：协议和端口可按实际情况选择。更多端口添加请参见 接入相关端口。

选择 **HTTP** 协议，输入端口。

选择 **HTTPS** 协议，输入端口后需要配置关联证书、HTTPS 强制跳转和 HTTPS 回源方式。

关联证书：单击**关联证书**，根据需求选择腾讯云托管证书或自有证书。

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

HTTPS 回源方式：HTTP 或 HTTPS。

说明：

选择 HTTP 时可以指定回源端口。选择 HTTPS 暂不支持指定回源端口，端口和对外开放端口一致。

代理情况：根据实际情况选择是否已使用了高防、CDN、云加速等代理。

说明：

选择“是”，WAF 将通过 XFF 字段获取客户真实 IP 地址作为源地址，勾选可能存在源 IP 被伪造的风险。

源站地址：根据实际需求选择 IP 或域名。

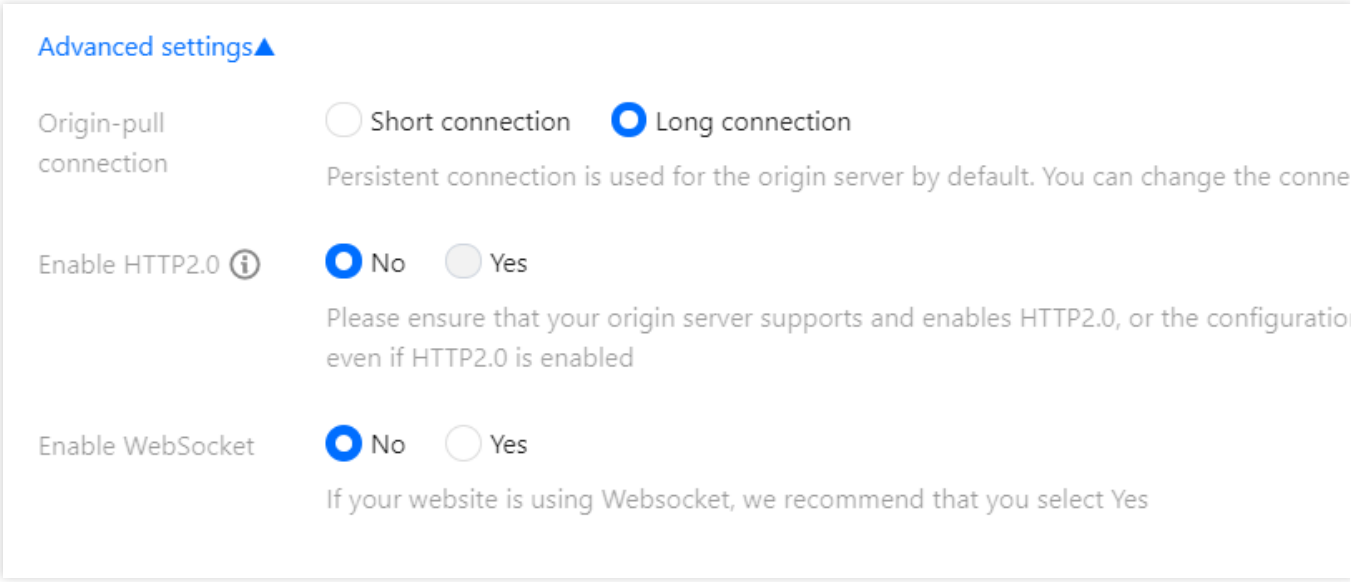
IP:请输入源站IPv4或v6地址，用回车分隔多个IP，最多支持输入20个。

域名：请输入源站域名，注意：源站域名不能和防护域名相同。

加权回源：当源站地址设置多 IP 回源时。可以选择加权回源方式。

负载均衡策略： 默认为轮询方式，可根据实际需求选择轮询或 IP Hash。

4. 配置完基础参数后，可根据需求配置高级参数，单击**确定**保存。



字段说明

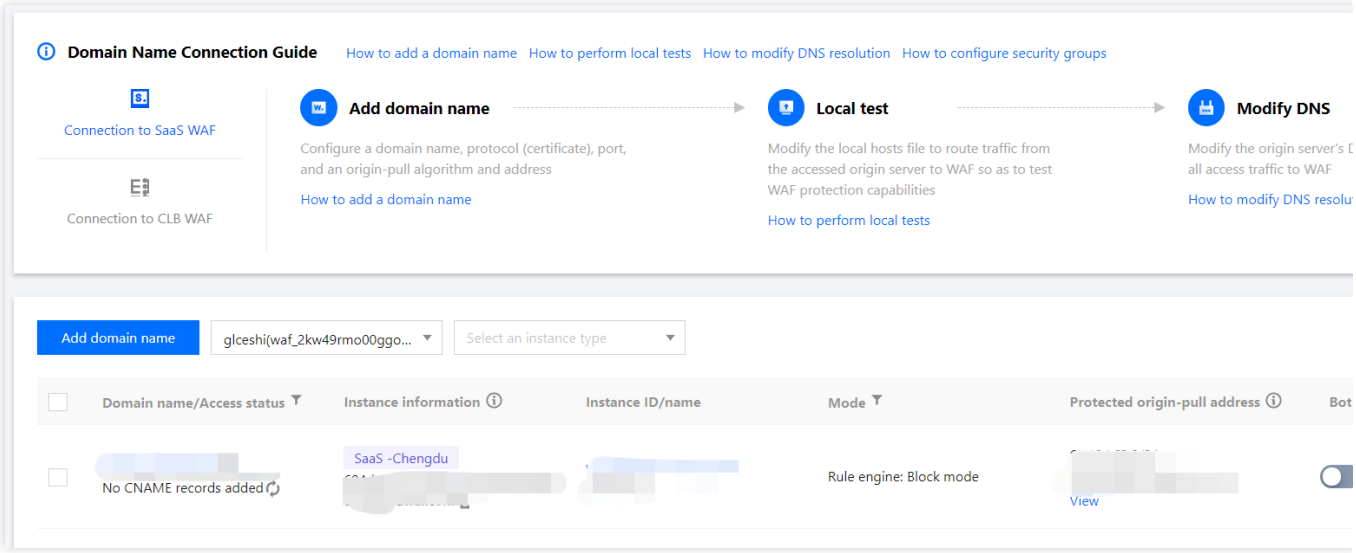
回源连接方式：默认使用长连接回源，请确认源站是否支持长连接，若不支持，即使设置长连接，也会使用短连接。

开启 HTTP2.0：请确保您的源站支持并开启了 HTTP2.0，否则，即使配置开启2.0也将降级1.1。

开启 Websocket：如果您的网站使用了 Websocket，建议您选择是。

开启健康检查：企业版以及以上版本，支持开启基于回源IP的四层健康检查机制。

5. 完成配置后，可在域名列表看到刚刚添加的域名。当前界面显示未配置 CNAME 记录，需要 本地验证测试 后，再 修改 DNS 解析。



说明：

Web 应用防火墙将会为每个添加到 Web 应用防火墙的域名（不区分一级域名和二级域名）分配一个唯一的 CNAME。

后续步骤

当您添加完域名后，可执行如下步骤：

步骤 2：本地测试

步骤 3：修改 DNS 解析

步骤 4：设置安全组

步骤 2：本地测试

最近更新时间：2023-12-29 14:23:01

本文档将指导您如何在修改 DNS 解析前进行本地测试，防止直接接入时导致生产业务中断。

操作步骤

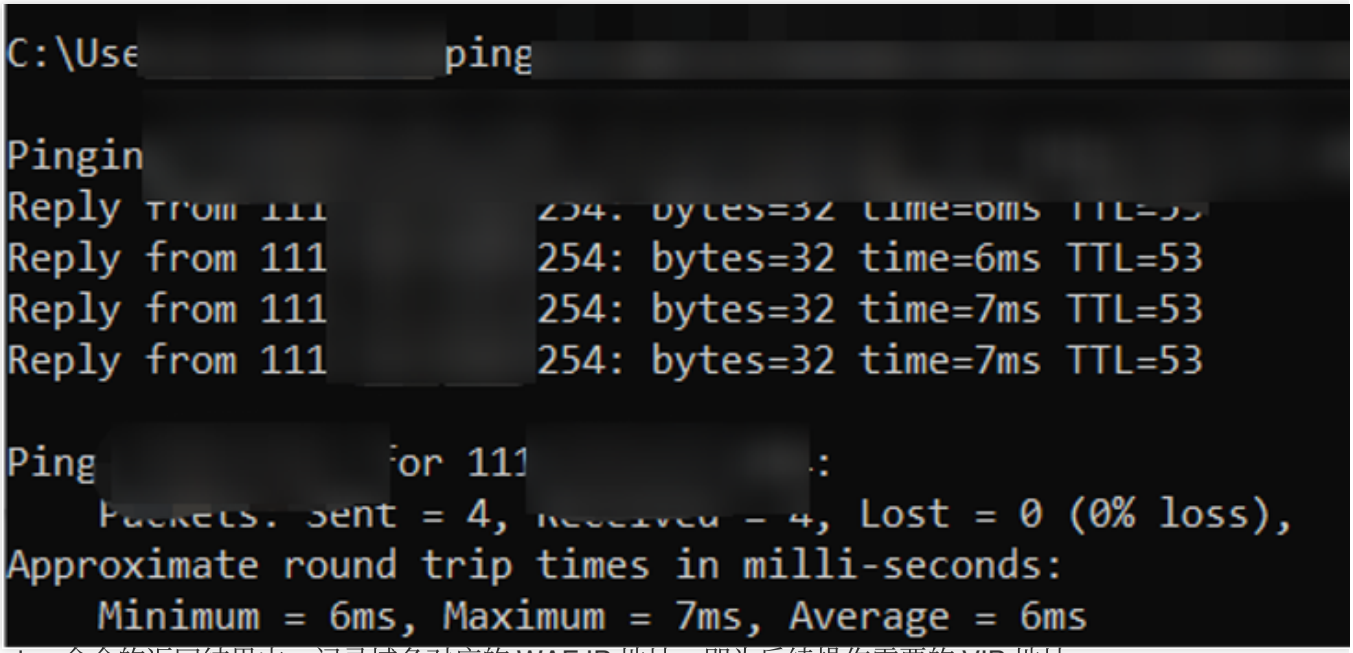
本地机器访问网站需要做 DNS 解析，在这之前会优先从本地 hosts 文件中获取目标域名对应的 IP 地址。所以可以用修改 hosts 文件的方式把本地的访问流量导向 Web 应用防火墙，从而测试经过 Web 应用防火墙访问 Web 站点的线路连通性，避免直接修改 DNS 解析记录，影响到公网用户对站点的访问。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心 > 域名列表**，在域名列表中查看 `saas.technicalsupport.cn` 的 CNAME 地址。

如需要获取对应域名的 VIP 地址，可通过 ping 该 CNAME 地址获取。

1.1 在 Windows 操作系统中，打开 cmd 命令行工具。

1.2 执行以下命令：`ping <已复制的 WAF CNAME 地址>`。



1.3 在 ping 命令的返回结果中，记录域名对应的 WAF IP 地址，即为后续操作需要的 VIP 地址。

2. 修改 hosts 文件。

在 Windows 下修改 `C:\\Windows\\System32\\drivers\\etc\\hosts`，增加条目。

格式：VIP 地址+接入 Web 应用防火墙的域名。

说明：

本文中的1.1.1.1为测试地址，实际使用中此处应为 VIP 地址。

```
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted]
#

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

1.1.1.1  saas.technicalsupport.cn
```

在 Linux 下 修改/etc/hosts，增加条目。

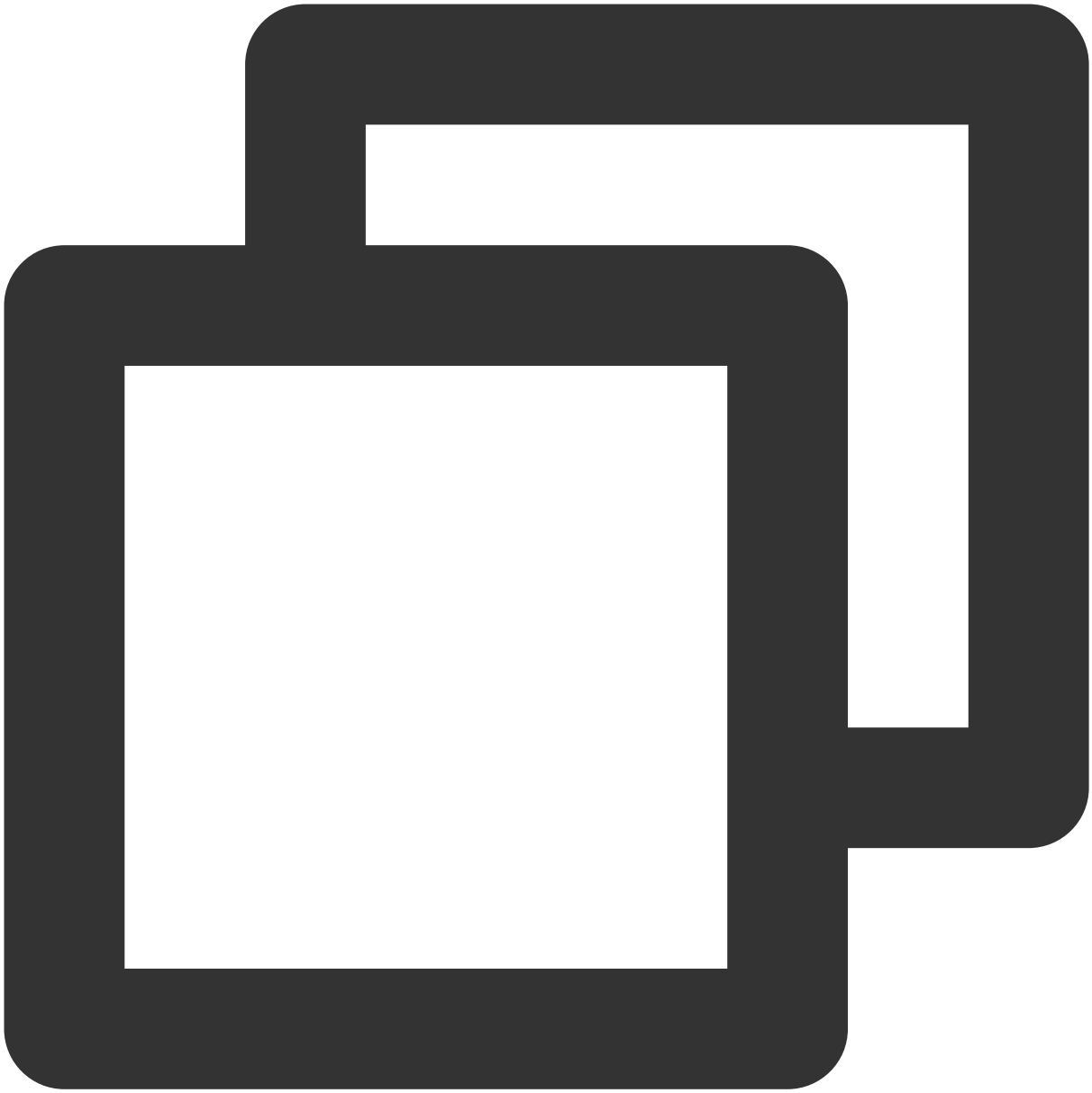
格式：VIP 地址+接入 Web 应用防火墙的域名。

```
[root@centos73 ~]# cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

[redacted]190 waf.qcloudwaf.com

[root@centos73 ~]#
```

3. 访问测试

在本地电脑上访问 Web 站点，若站点能够正常打开，说明 Web 应用防火墙访问 Web 源站的线路连通性正常。

3.1 在浏览器中输入下面的网址并访问。

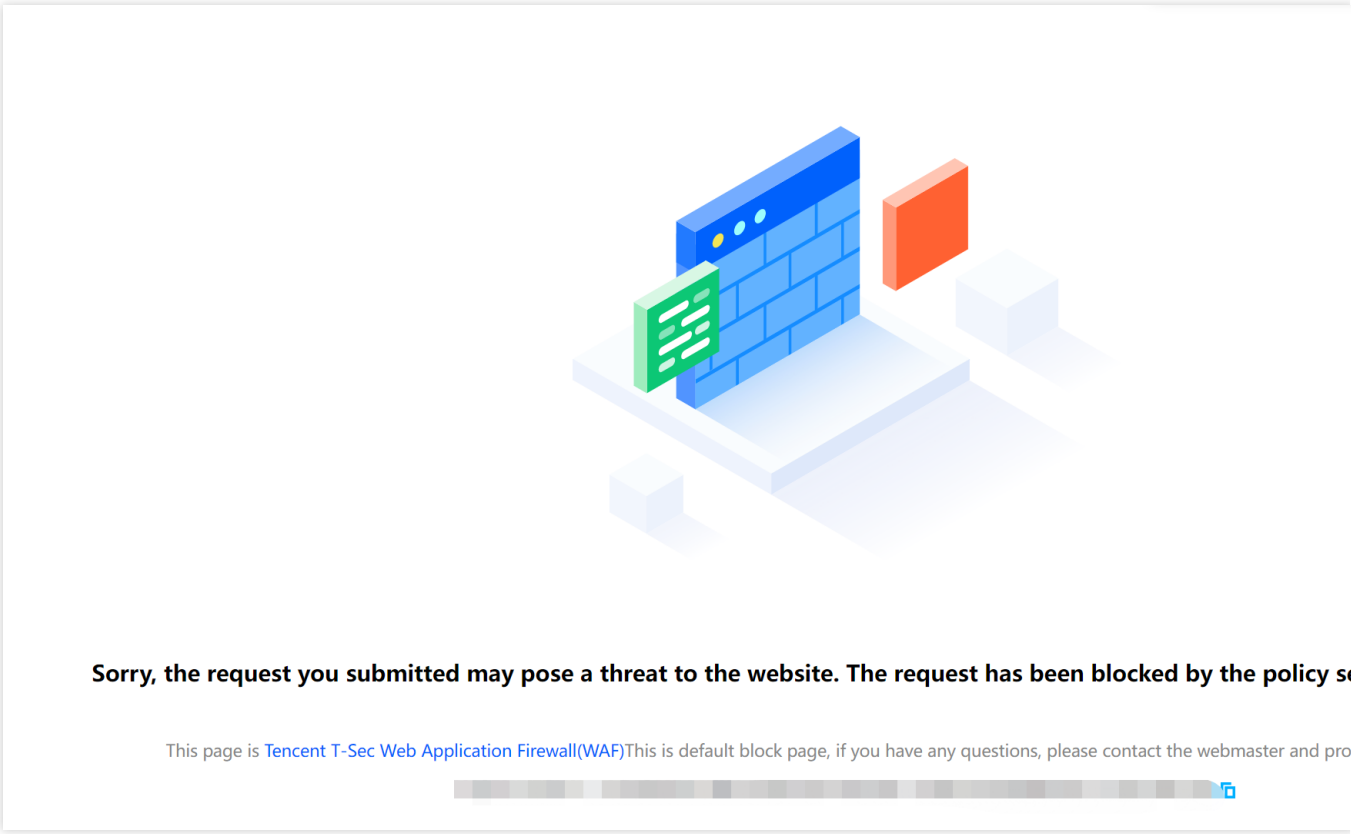


```
http:// saas.technicalsupport.cn/?test=alert(123)
```

3.2 浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。

说明：

该拦截页面，可以通过访问： Web应用防火墙(WAF)默认提示页面 获取。



后续步骤

当您完成本地测试后，可执行如下步骤：

步骤 3：修改 DNS 解析

步骤 4：设置安全组

步骤 3：修改DNS解析

最近更新时间：2023-12-29 14:23:17

本文档将指导您如何修改 DNS 的解析记录，使公网用户访问网站的流量经过 Web 应用防火墙的防护。

操作步骤

为了使公网用户访问网站的流量经过 Web 应用防火墙的防护，需要修改 DNS 的解析记录。下面以在腾讯云 DNS 解析 DNSPod 上修改测试站点 `waf.qcloudwaf.com` 的 DNS 解析为例，说明配置步骤。

1. 登录 DNS 解析 DNSPod 控制台，在左侧导航栏中，单击**我的域名**，找到需要接入 Web 应用防火墙的域名 `.technicalsupport.cn`，单击**解析**进入解析配置界面。
2. 单击**添加记录**。
3. 在当前配置页面中填写相应信息。

主机记录填写对应网站的主机记录，本例中需要防护的是 `saas.technicalsupport.cn`，即填写 saas 。

记录类型选择 CNAME。

记录值填写 Web 应用防火墙分配的 CNAME 域名，分配的 CNAME 域名样式为： `xxxx.qcloudcjgj.com` 。

填写完毕后， 单击**保存**。

4. 修改完成之后，待 DNS 记录生效，Web 应用防火墙即可对访问网站的流量进行防护了。同时，Web 应用防火墙检测到被防护域名解析正常之后，Web 应用防火墙控制台 上将提示 “正常防护”。

说明：

DNS 记录生效需要10分钟左右时间。

后续步骤

当您修改完成 DNS 的解析记录后，可执行 步骤 4：设置安全组。

步骤 4：设置安全组

最近更新时间：2023-12-29 14:23:43

本文档将指导您如何设置安全组，使仅允许来自 Web 应用防火墙的流量访问网站。

操作步骤

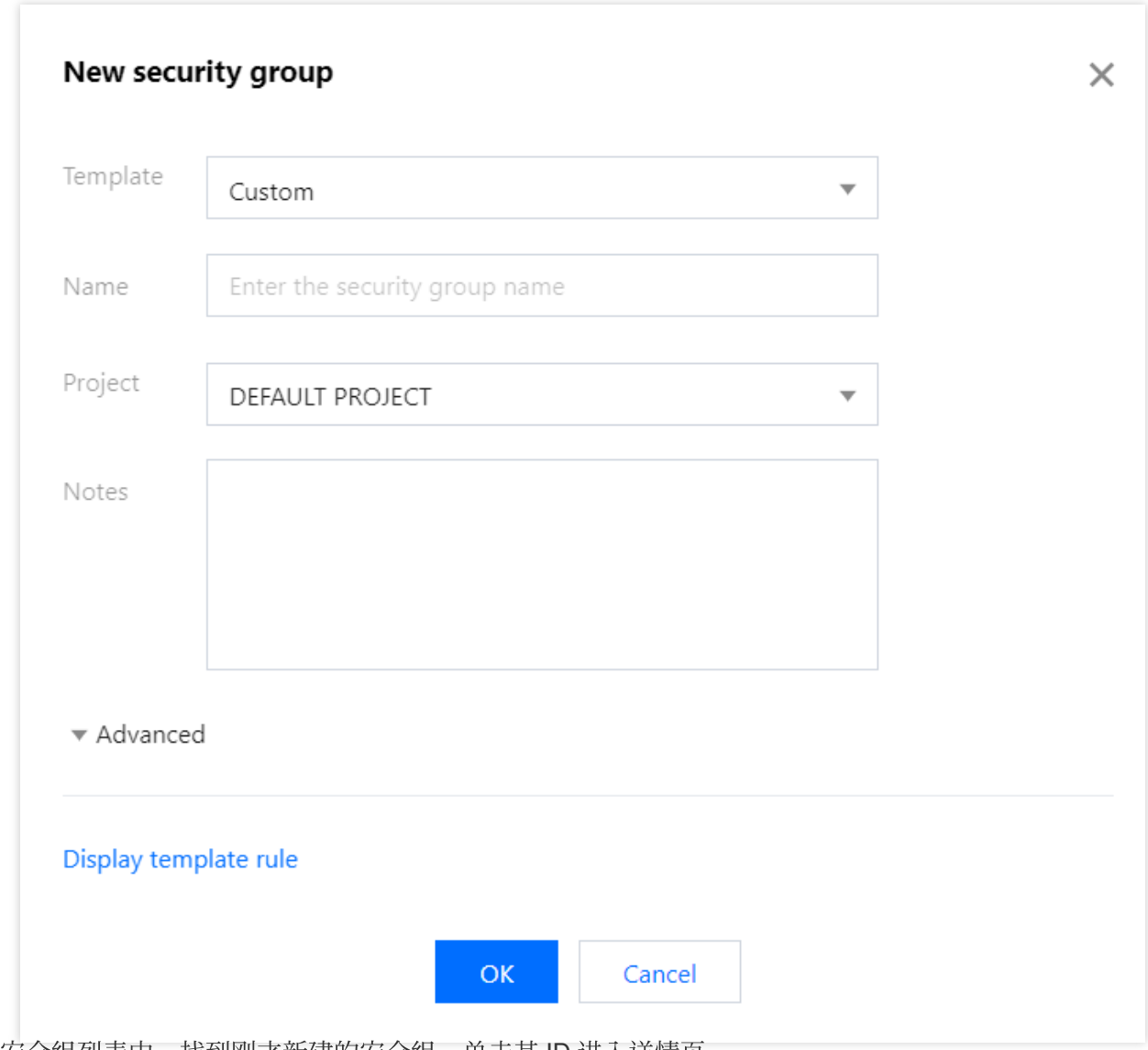
安全组是腾讯云提供的实例级别防火墙，可对任意云服务器进行入或出流量控制。在安全组中设置仅允许来自 Web 应用防火墙的流量访问网站，可避免攻击者绕过 Web 应用防火墙直接攻击网站源站。

下面以在安全组中放行 Web 应用防火墙的回源 IP 111.230.27.90 为例，说明配置过程。

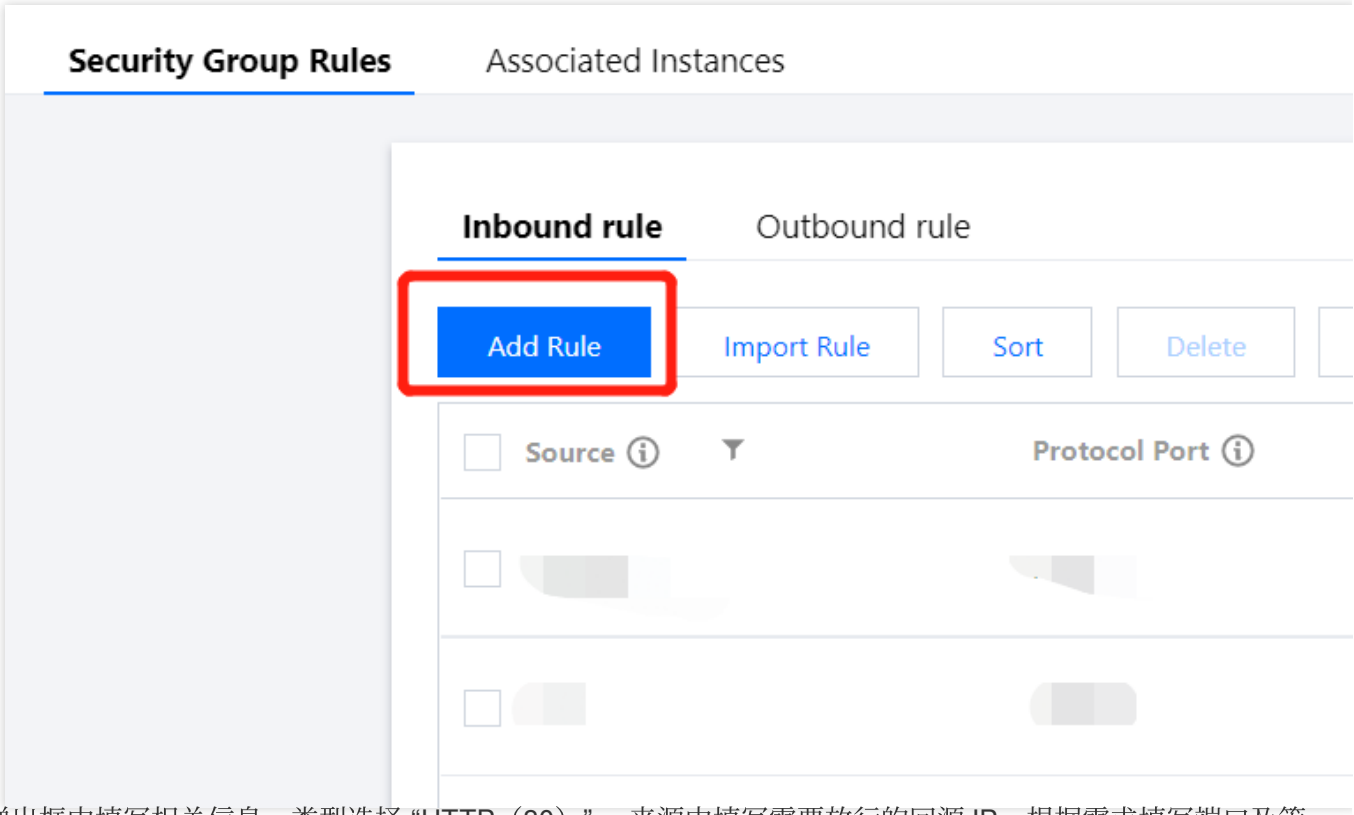
注意：

回源 IP 可在 Web 应用防火墙控制台的 域名列表 中查看。

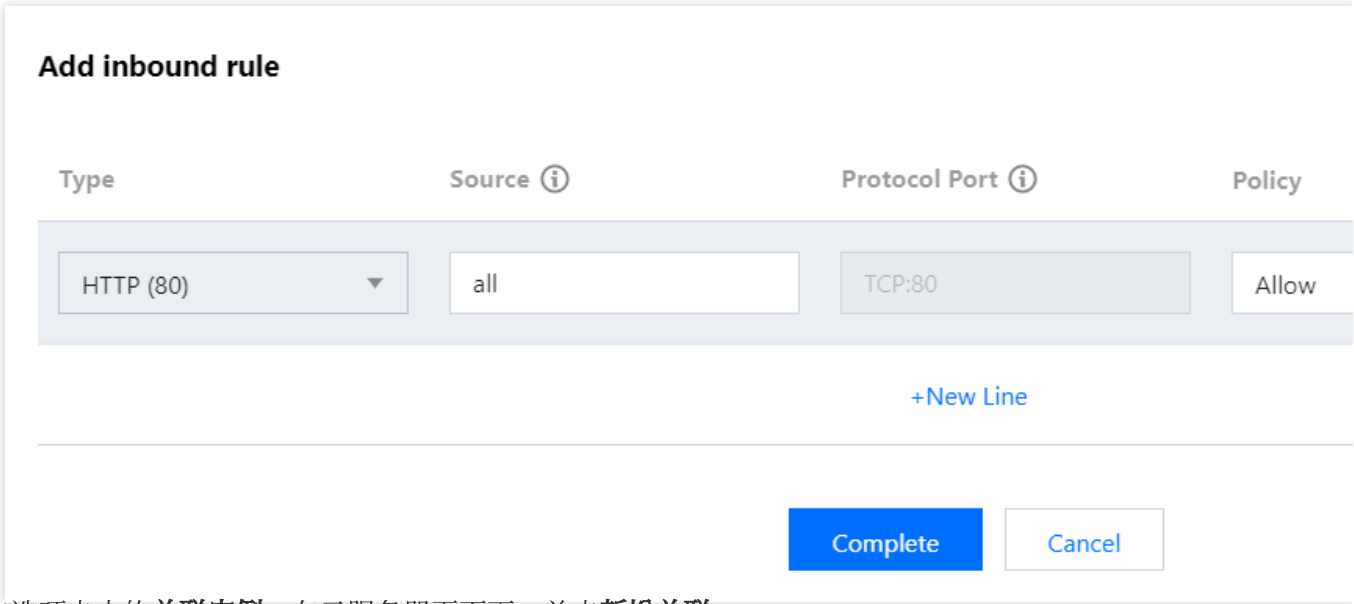
1. 登录 云服务器控制台，在左侧目录中，单击**安全组**。
2. 进入安全组页面，单击**新建**，根据要求填写信息，模板选择**自定义**，输入安全组的名称（例如 my-security-group），填写相关备注，填写完成后，单击**确定**。



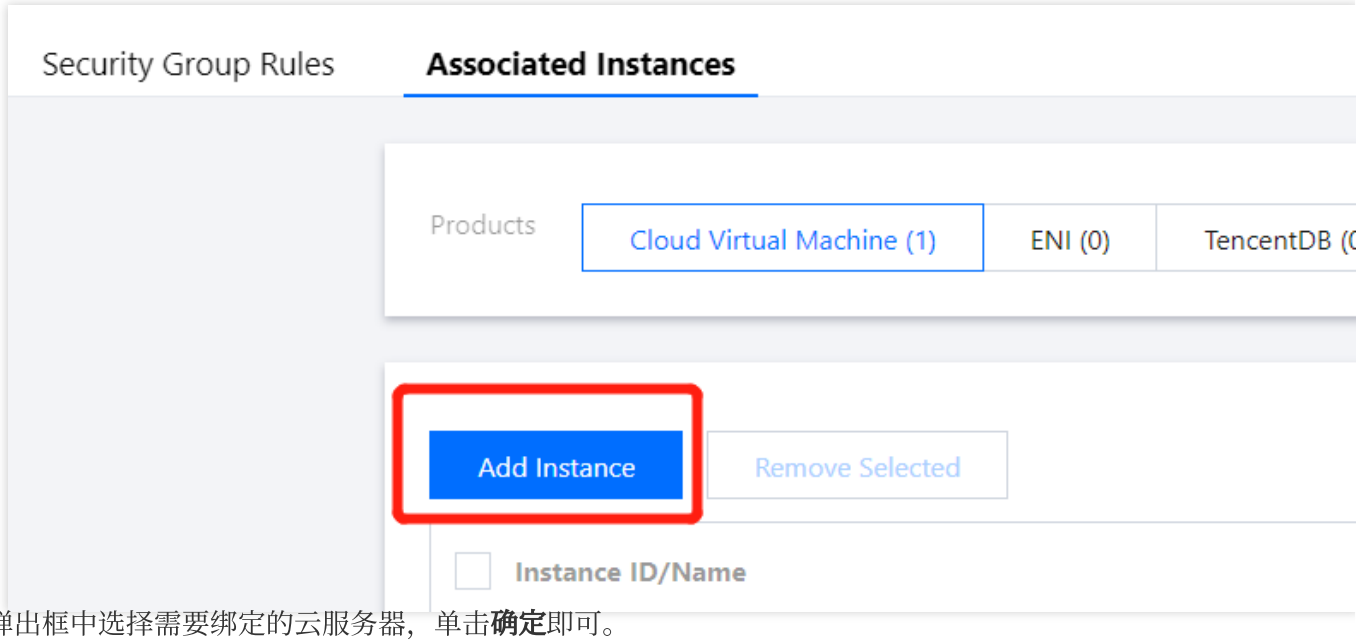
3. 在安全组列表中，找到刚才新建的安全组，单击其 ID 进入详情页。
4. 在入站规则页面中，单击**添加规则**。



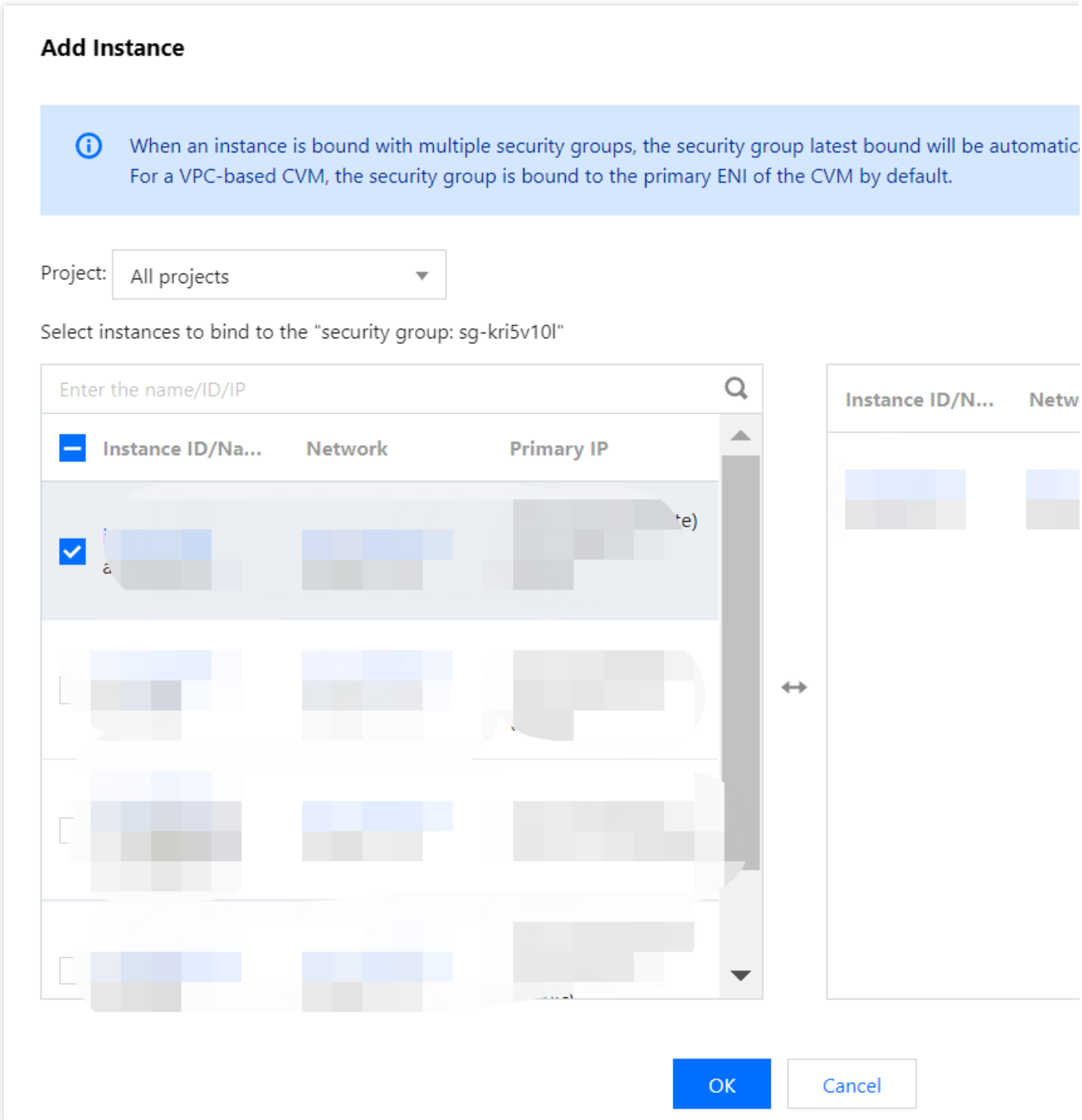
5. 在弹出框中填写相关信息，类型选择“HTTP（80）”，来源中填写需要放行的回源 IP，根据需求填写端口及策略，填写完毕后，单击**完成**。



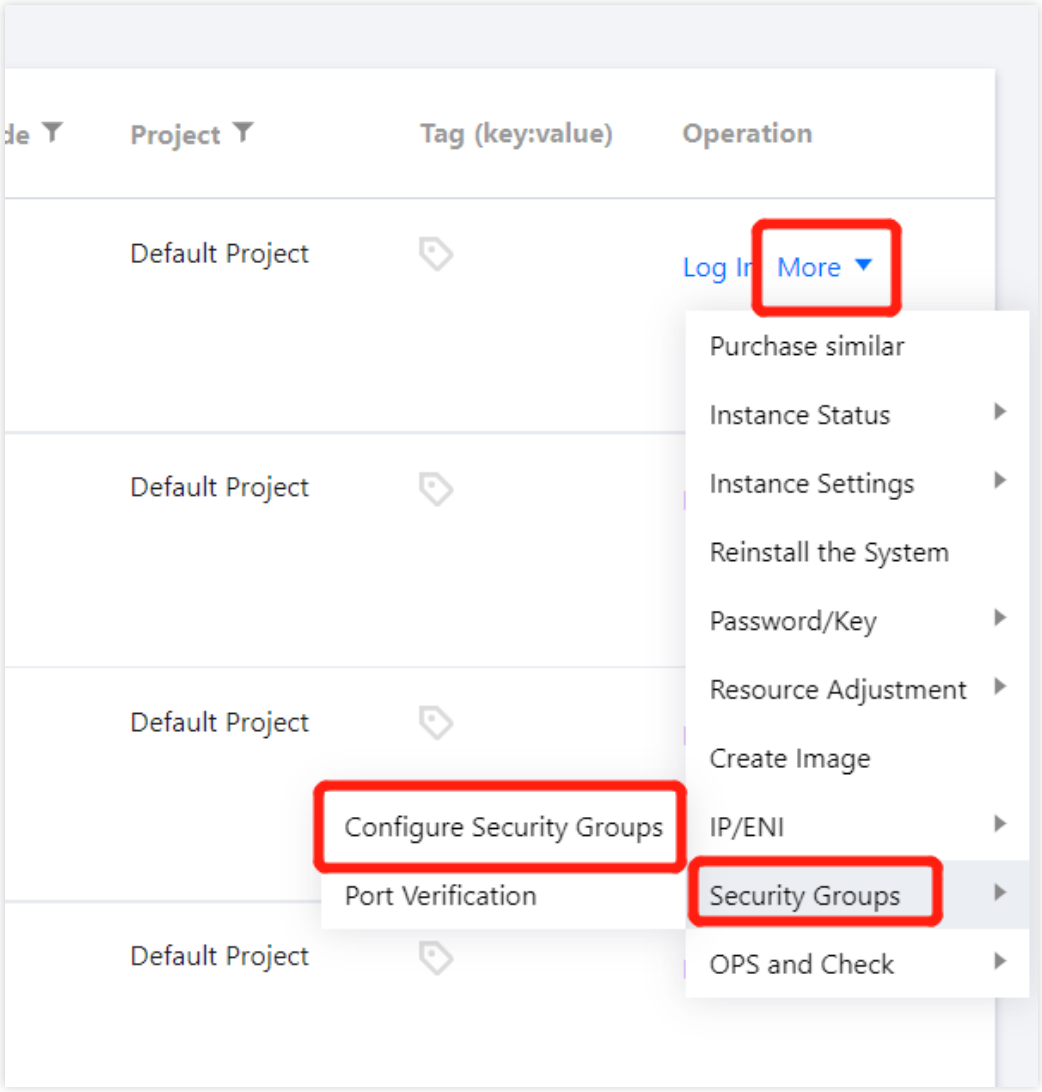
6. 单击选项卡中的**关联实例**，在云服务器页面下，单击**新增关联**。



7. 在弹出框中选择需要绑定的云服务器，单击**确定**即可。



或者您还可以进入 云服务器列表页，查看或修改某云服务器已绑定的安全组，在列表页选择需要调整安全组的云服务器 ID，在右侧操作栏，选择**更多** > **安全组** > **配置安全组**，选择安全组进行绑定。


Project
Tag (key:value)
Operation
Default Project
Log In
More
Purchase similar
Instance Status
Instance Settings
Reinstall the System
Password/Key
Resource Adjustment
Create Image
IP/ENI
Security Groups
OPS and Check
Default Project
Default Project
Default Project
Configure Security Groups
Port Verification
Default Project

步骤5：验证测试

最近更新时间：2023-12-29 14:24:56

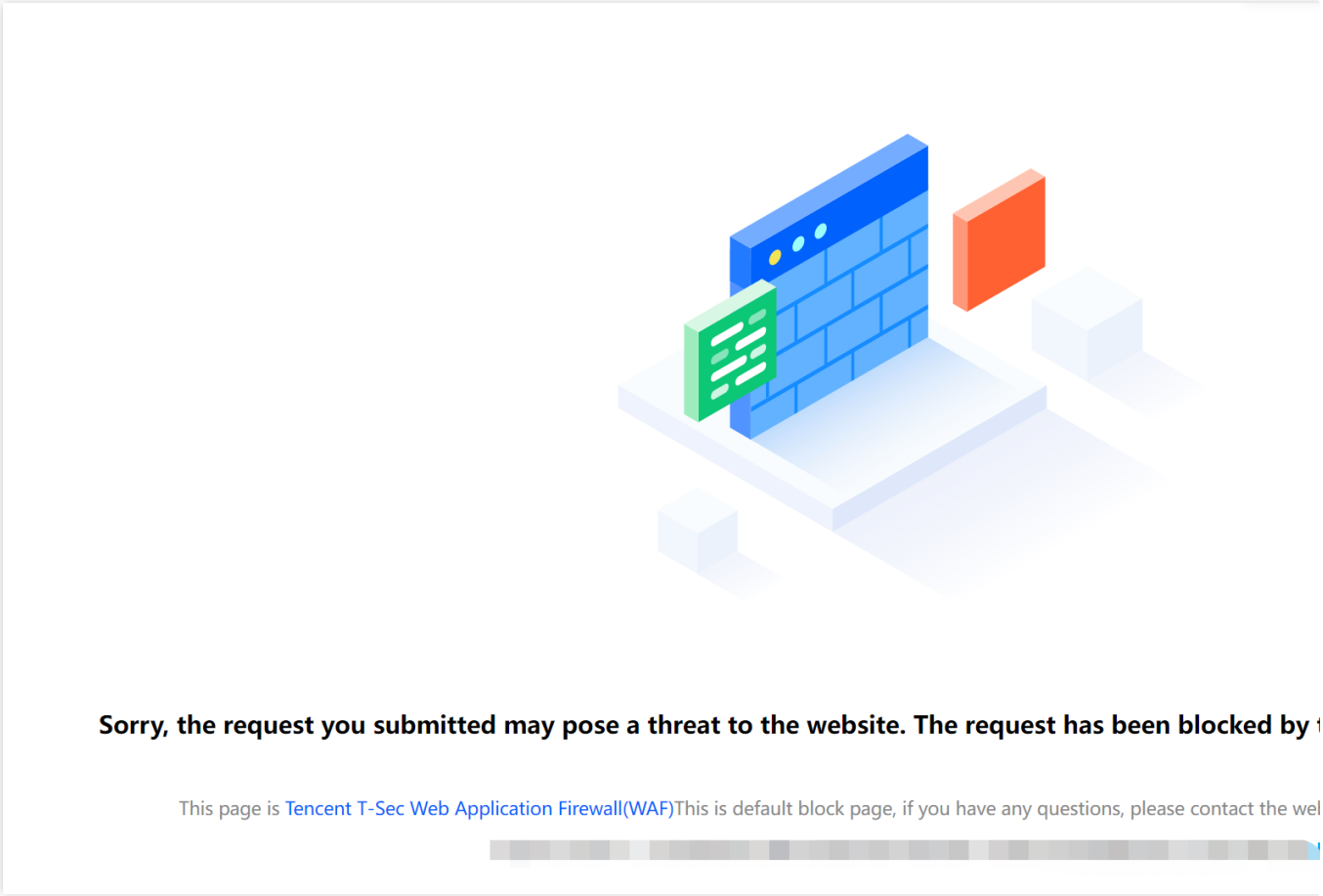
本文档将指导您如何验证SaaS 型 WAF 是否生效。

操作步骤

1. WAF 通过域名和源站进行绑定，对流量进行防护。验证SaaS型 WAF 是否生效，请先确保本地电脑可以正常访问在 SaaS不同实例下添加的域名。
2. 在浏览器中输入网址 `http:// saas.technicalsupport.cn/?test=alert(123)` 并访问，浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。

注意：

`saas.technicalsupport.cn` 为本案例中域名，此处需要将域名替换为实际添加的域名。



接入负载均衡型 WAF
步骤1：确认负载均衡配置

最近更新时间：2023-12-29 14:25:39

本文档将指导您如何在接入负载均衡型 WAF 前，确认负载均衡配置。

操作步骤

负载均衡型 WAF 通过添加域名的方式与负载均衡监听器进行绑定，实现对经过负载均衡监听器的 HTTP 或 HTTPS 流量进行检测和拦截。在接入负载均衡型 WAF 前，请确保网站业务已在腾讯云上，并且使用了腾讯云负载均衡（原应用型负载均衡，网络类型为公网类型）。

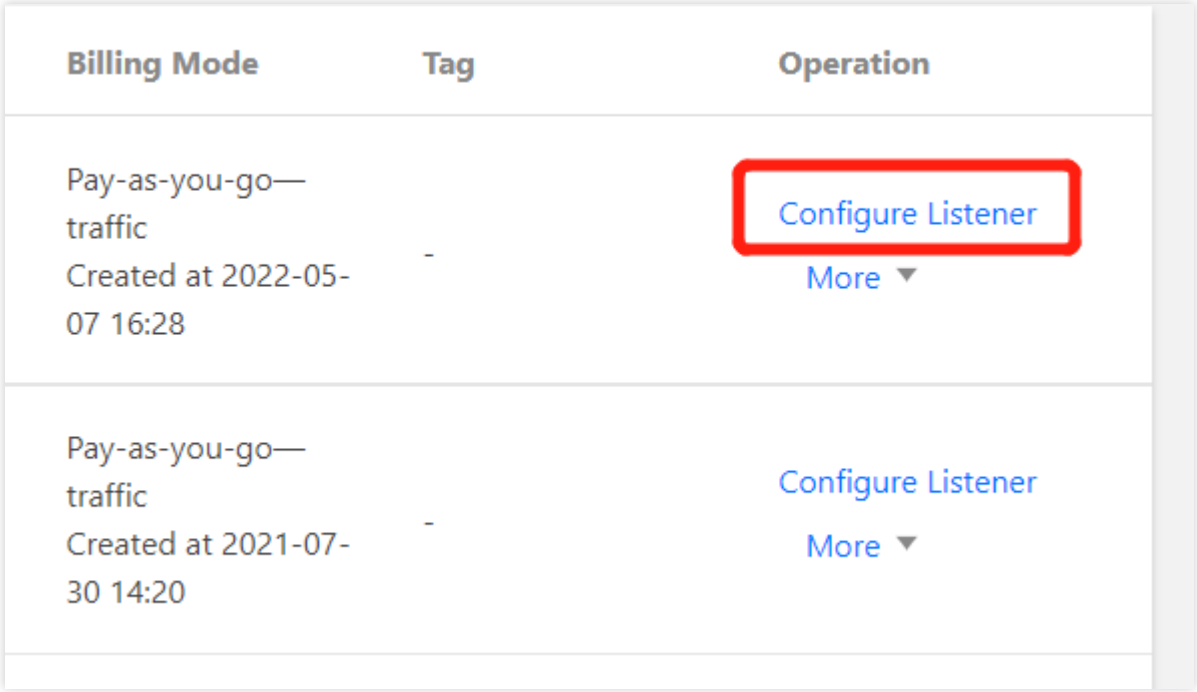
说明：

若您的网站业务不在腾讯云上，建议您使用 SaaS 型 WAF 接入防护。

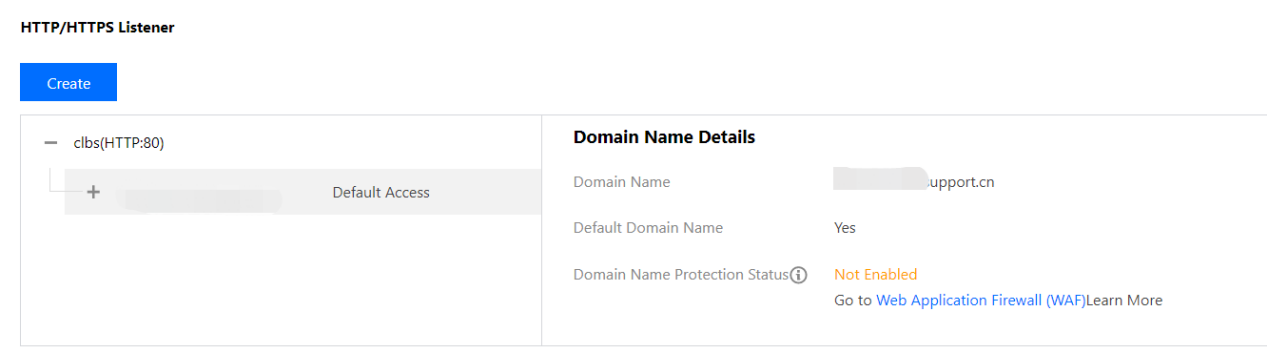
为了使负载均衡型 WAF 能够识别出需要防护的域名，需要配置负载均衡并且在监听器配置相应域名，实现业务正常转发。详情请参见 配置 HTTP 监听器 和 配置 HTTPS 监听。

本文以防护 `clb.technicalsupport.cn` 为例，查看已配置完成的负载均衡监听器的配置信息。

1. 登录腾讯云 负载均衡控制台，在左侧导航栏中，单击**实例管理**，进入实例管理页面。
2. 选择**地区** > **负载均衡**，查看已经创建好的负载均衡，在右侧操作栏，单击**配置监听器**，进行配置查看。



3. 在监听器配置页面，单击**监听器管理**，查看监听器域名配置信息。监听器的名称为 waftest，监听器转发规则监听的域名为 `clb.technicalsupport.cn` ，域名防护状态为未启用。



后续步骤

当您确认完成负载均衡配置后，可执行如下步骤：

步骤2：域名添加绑定负载均衡

步骤3：验证测试

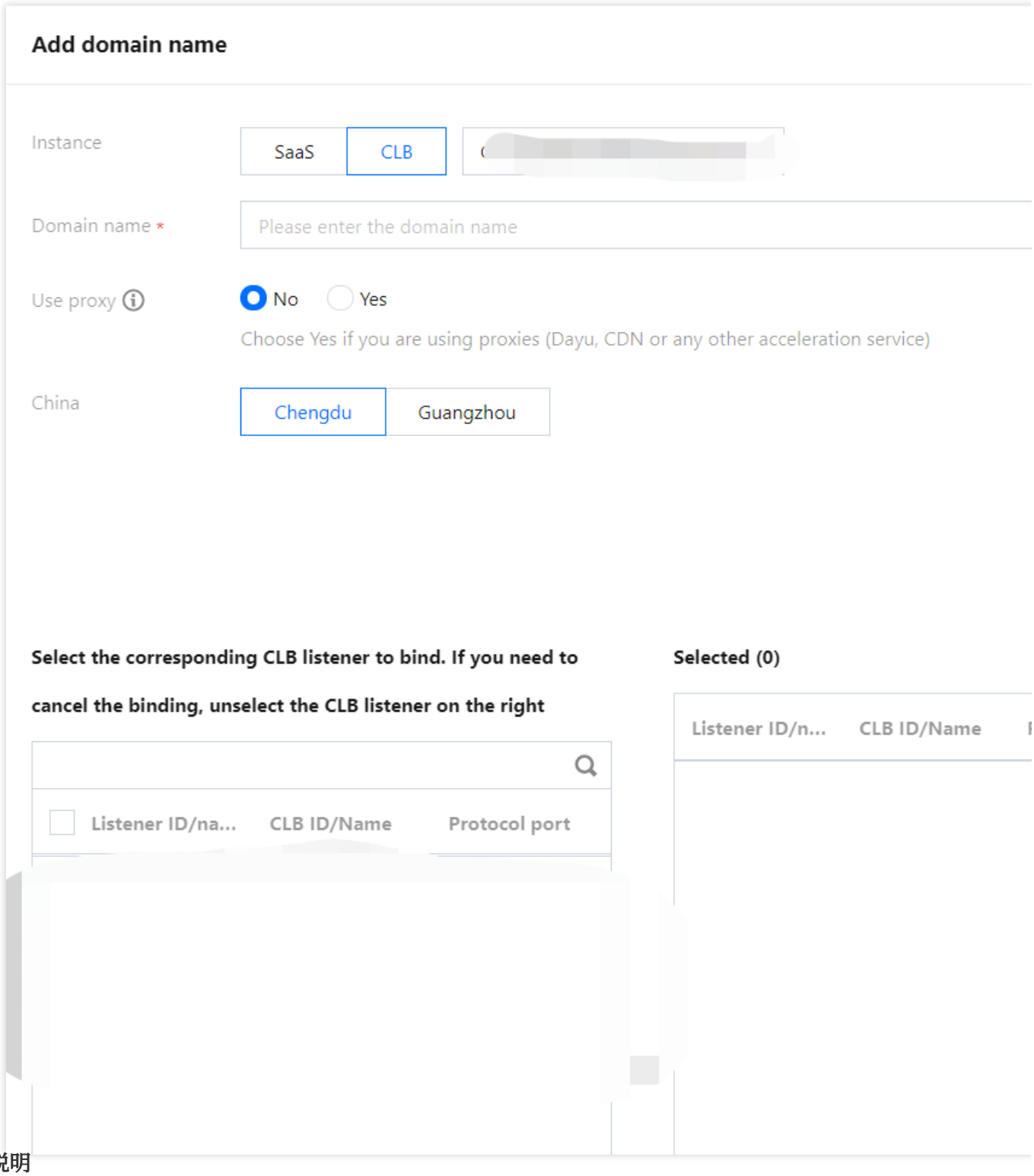
步骤 2：添加域名并绑定负载均衡

最近更新时间：2023-12-29 14:25:54

本文档将指导您如何在 Web 应用防火墙控制台中，进行域名添加绑定负载均衡。

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**资产中心 > 域名列表**，进入域名列表页面。
2. 在域名列表页面，单击**添加域名**，配置相关参数，单击**确定**即可。



字段说明

所属实例：选择负载均衡型和实例名称。

域名： 在域名输入框中添加需要防护的域名`clb.technicalsupport.cn`。

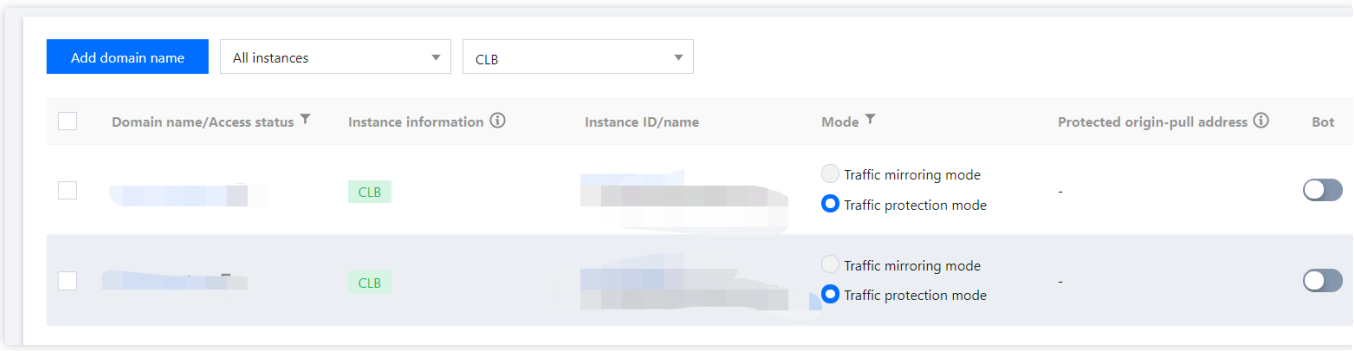
代理情况：根据情时间情况选择是否已使用了高防、CDN、云加速等代理。

说明：

选择“是”，WAF 将通过 XFF 字段获取客户真实 IP 地址作为源地址，勾选可能存在源 IP 被伪造的风险。

国内地域：根据实际需求选择。

国外地域：根据实际需求选择。
选择域名对应的负载均衡监听器：根据实际需求选择。
3. 单击**确定**，即可返回域名列表。在域名列表可以查看到防护域名 `clb.technicalsupport.cn` 和负载均衡的负载均衡 ID、名称、VIP 和监听器信息等。



后续步骤

当您完成域名添加绑定负载均衡后，可执行 步骤3：验证测试。

步骤3：验证测试

最近更新时间：2023-12-29 14:26:12

本文档将指导您如何验证负载均衡型 WAF 是否生效。

操作步骤

1. WAF 通过域名和 CLB 对应监听器进行绑定，对经过 CLB 监听器的域名流量进行防护。验证负载均衡型 WAF 是否生效，请先确保本地电脑可以正常访问在负载均衡不同实例下添加的域名。

说明：

验证添加在负载均衡中域名型访问是否正常，IPv4 域名请求，请参见负载均衡快速入门的 验证负载均衡服务，IPv6 域名请求，请参见 IPv6 负载均衡快速入门的 步骤4：测试 IPv6 负载均衡。

2. 在浏览器中输入网址 `http://wow.qcloudwaf.com/?test=alert(123)` 并访问，浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。

注意：

`wow.qcloudwaf.com` 为本案例中域名，此处需要将域名替换为实际添加的域名。

Sorry, the request you submitted may pose a threat to the website. The request has been blocked by t

This page is Tencent T-Sec Web Application Firewall(WAF)This is default block page, if you have any questions, please contact the wel

资产中心
实例管理

最近更新时间：2023-12-29 14:26:26

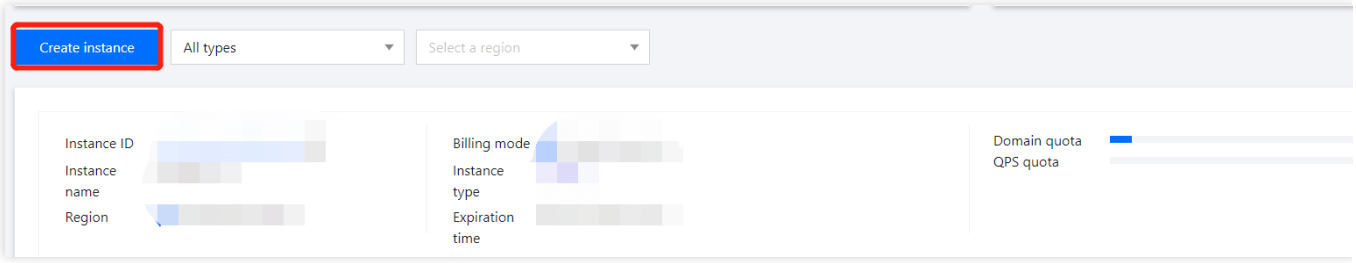
操作场景

本文档将为您介绍 Web 应用防火墙（WAF）资产中心的实例管理模块，可以查看实例详情和购买新实例，并对实例的套餐和扩展包进行续费和购买管理。

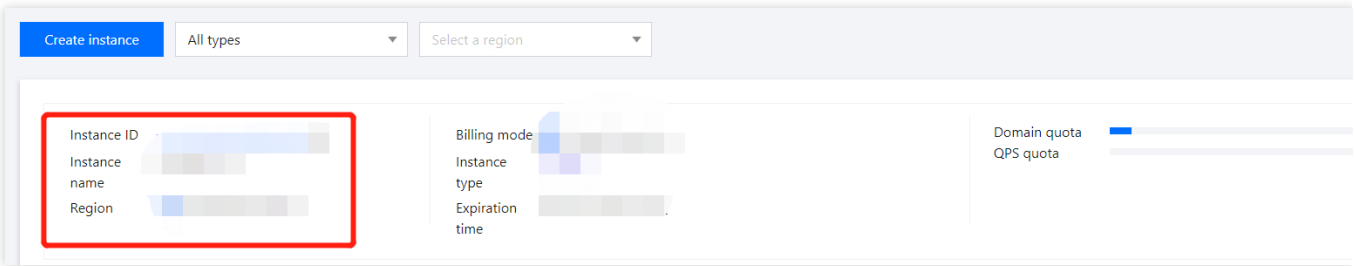
操作步骤

新建与查看实例

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心 > 实例管理**，进入实例管理页面。
2. 在实例管理页面，单击**新建实例**，跳转至购买页，按需购买即可。更多购买详情，请参见 购买指南。

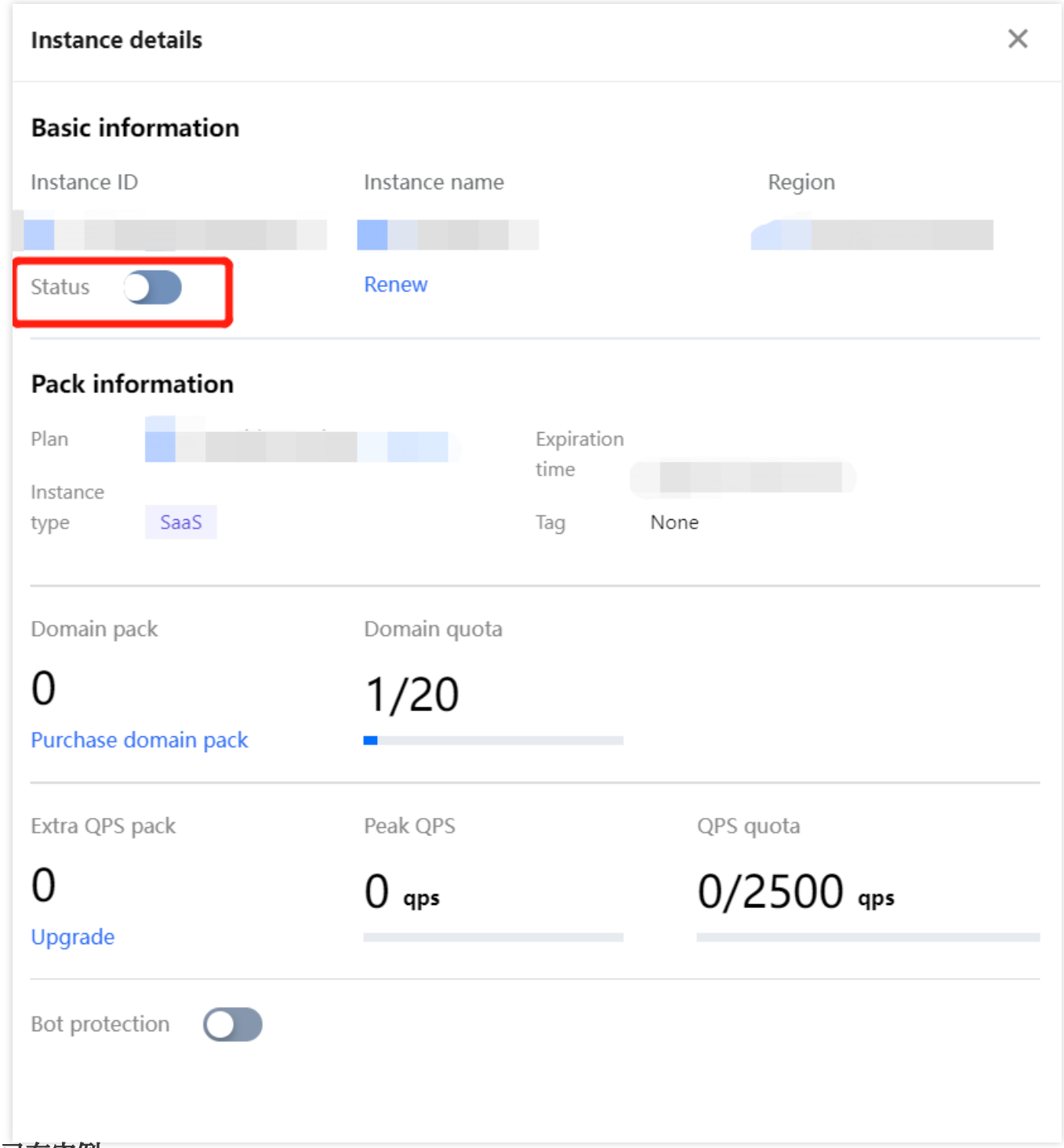


3. 在实例管理页面，单击“实例 ID”，右侧弹出实例详情页面。



4. 在实例管理页面，可以查看该实例的基本信息和套餐信息，单击

，可以关闭套餐续费。

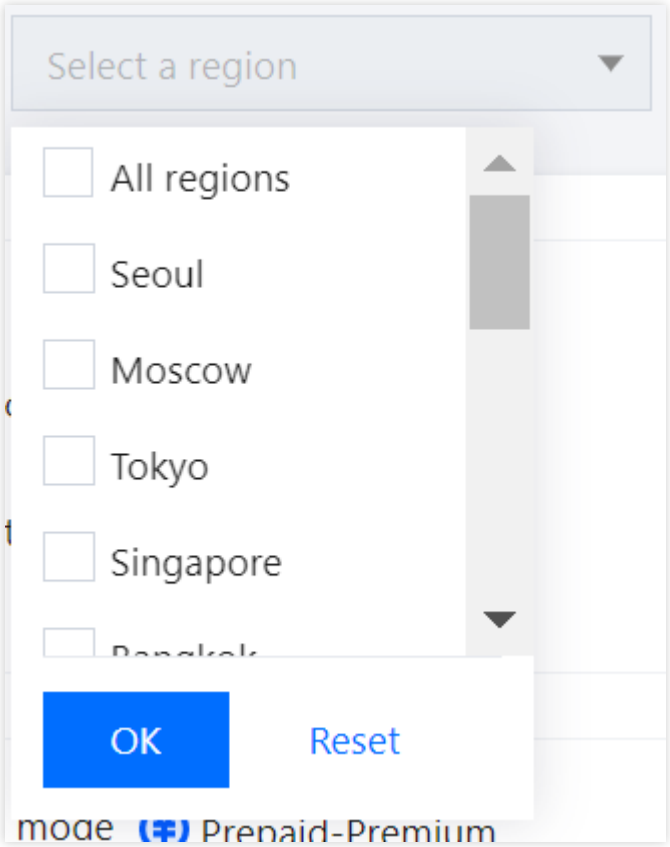


搜索已有实例

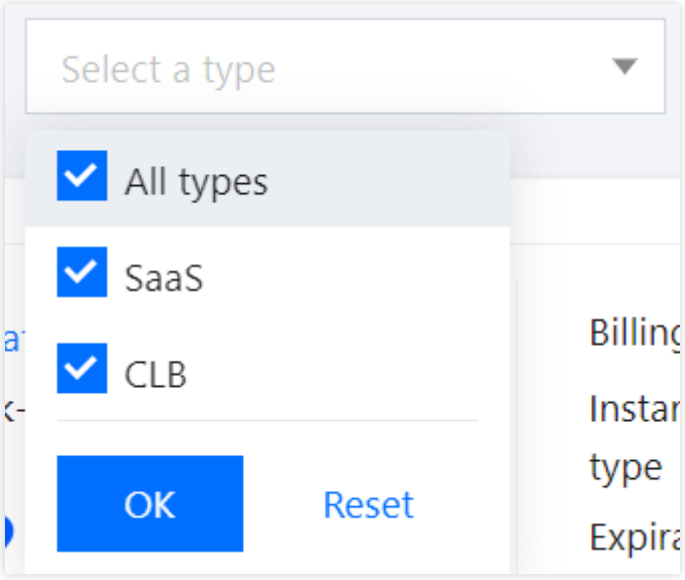
如果购买了多个实例，需要检索或搜索，则可使用本功能，已有实例支持按地域和类型检索和按关键字搜索。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心 > 实例管理**，进入实例管理页面。
2. 在实例管理页面，可按类型、地域对已有实例进行筛选，或搜索框通过“实例 ID、实例名称和计费方式”关键字对已有实例查找。

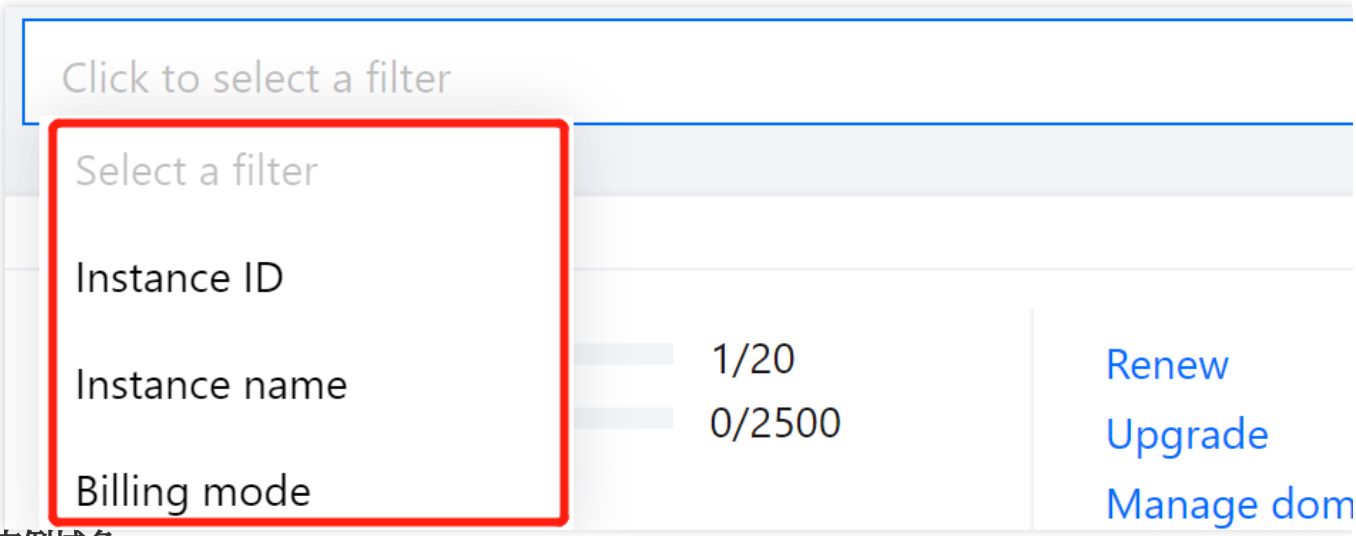
单击左上角的类型下拉框，按Web 应用防火墙类型对已有实例进行筛选。



单击左上角的地域下拉框，按地域对已有实例进行筛选。



单击搜索框，可通过“实例 ID、实例名称和计费方式”关键字对已有实例进行查询。



管理实例域名

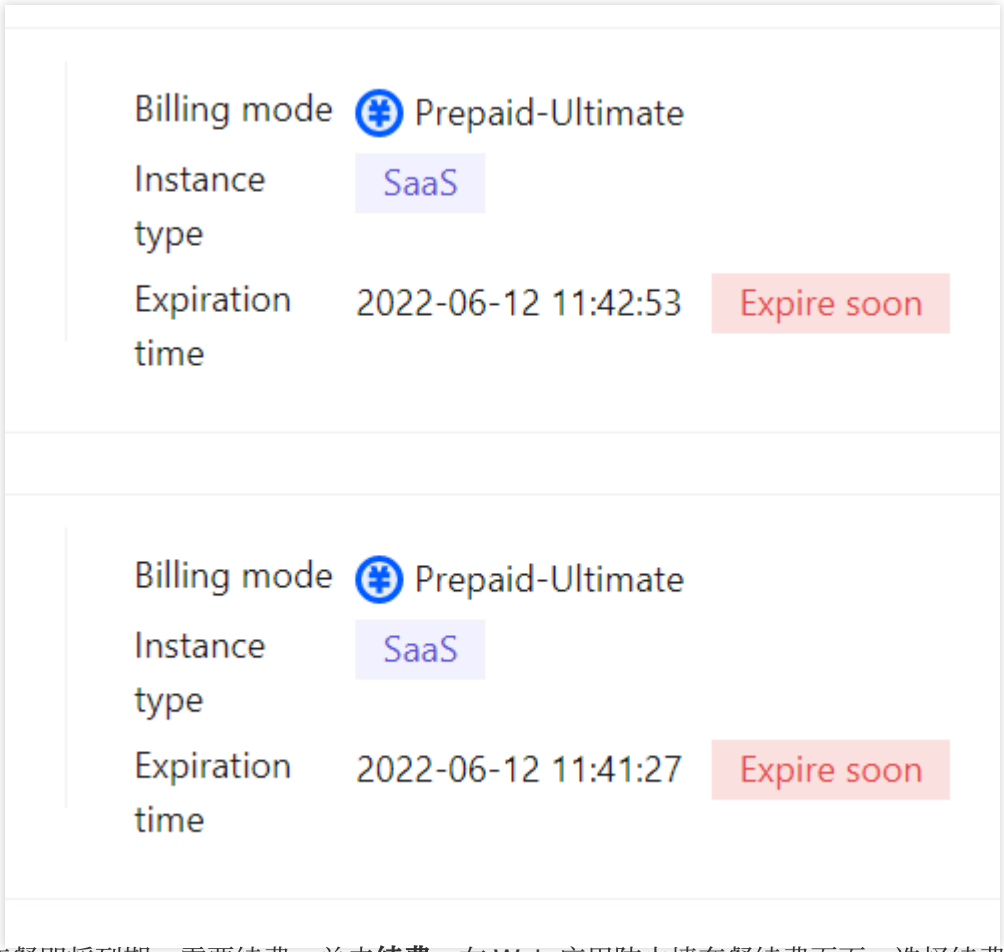
搜索到所需实例并查看后，需要配置实例的域名。

1. 在 实例管理页面，单击**管理域名**，跳转至域名列表页面。

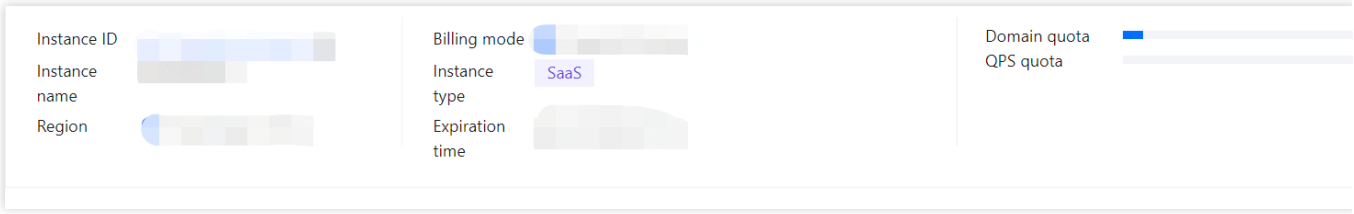
2. 在 域名列表页面，可以进行新建域名、编辑域名和删除域名等操作，详情请参见 域名列表。

实例续费与扩展包购买

搜索到所需实例并查看后，在 实例管理页面 的展板上可以查看您购买的产品套餐的到期时间和扩展包的使用剩余情况。



1. 若套餐即将到期，需要续费，单击**续费**，在 Web 应用防火墙套餐续费页面，选择续费时长，单击**立即续费**，可对当前套餐进行续费。

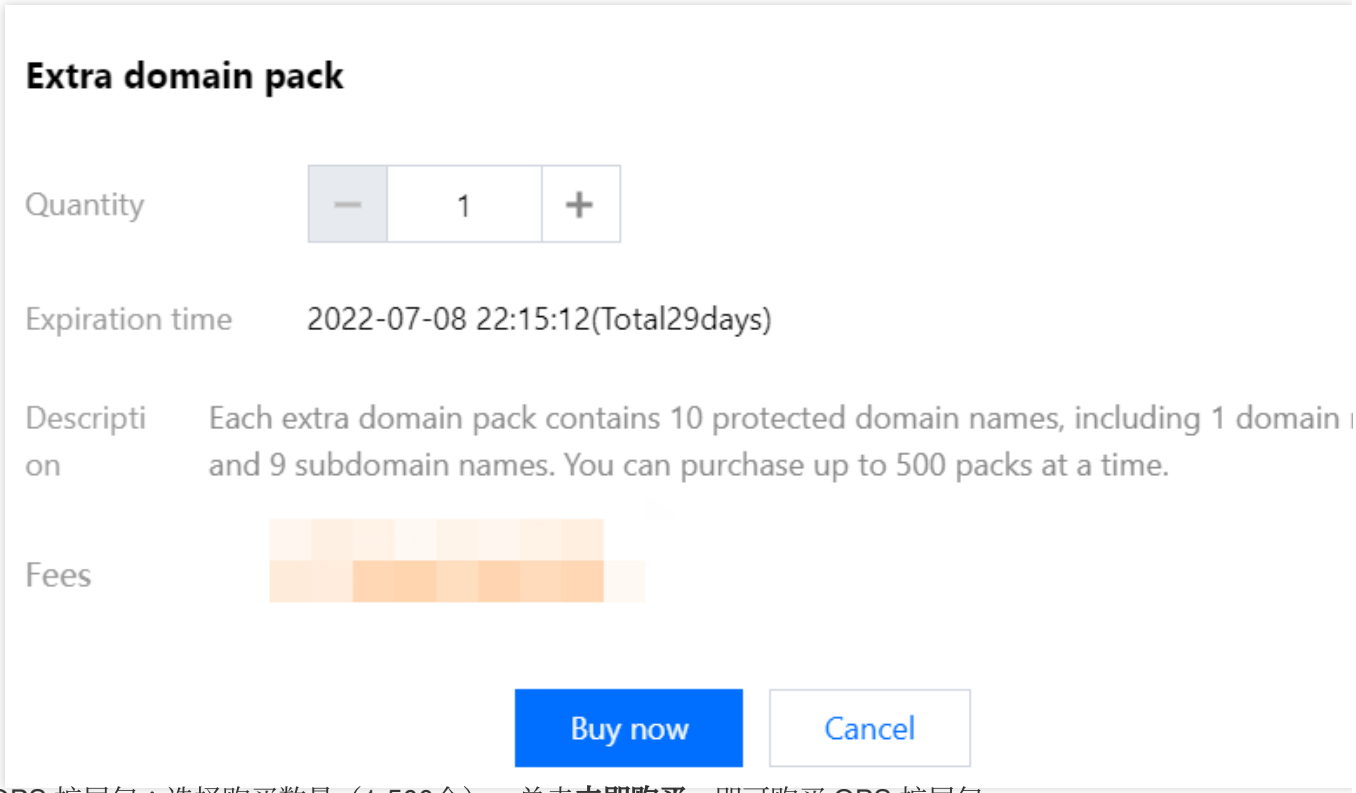


2. 如果展板显示域名数量包或 QPS 规格将满，单击**更多**，选择**购买域名包**、**购买 QPS 扩展包**或 **BOT与业务安全**，即可进行域名包、QPS 扩展包或 BOT与业务安全的购买。

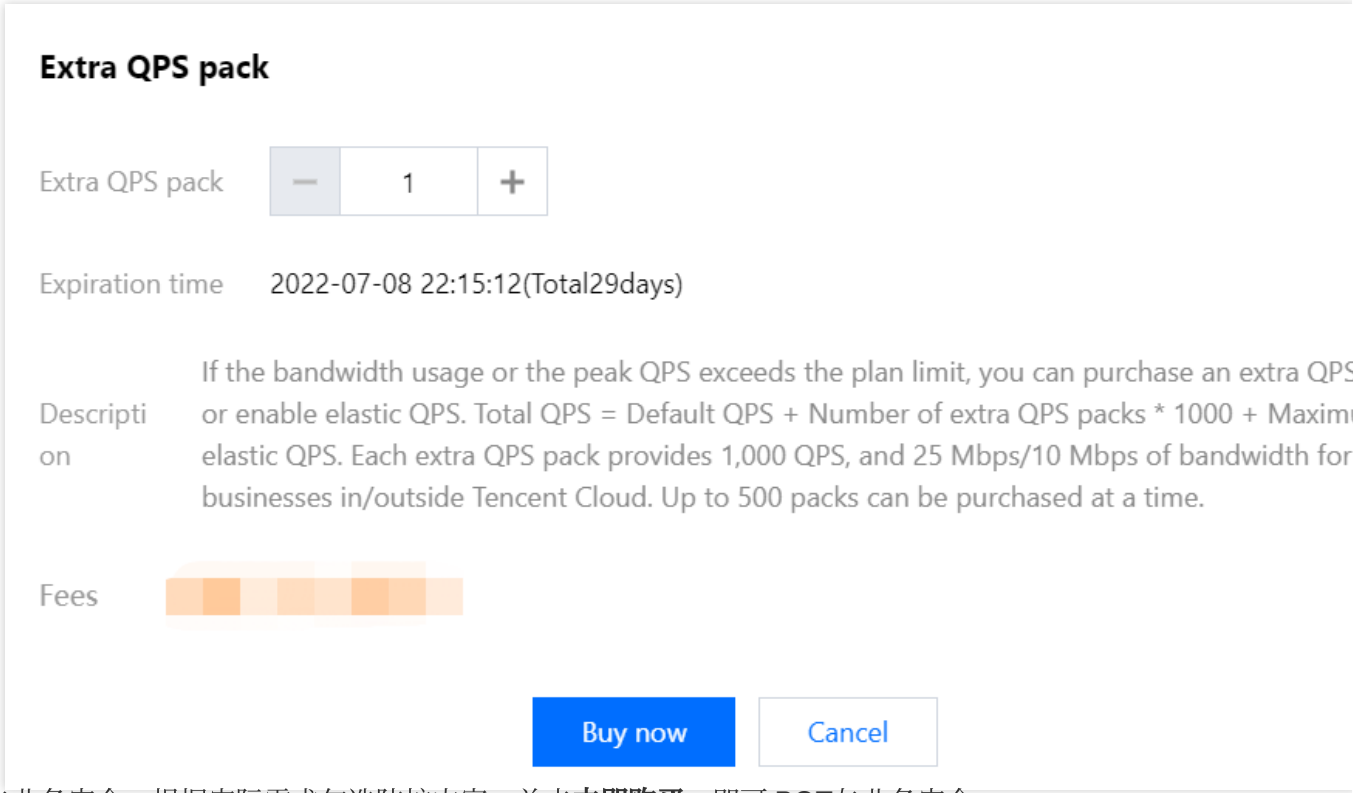
说明：

如果当前实例或域名包已经过期，请先续费，再购买。

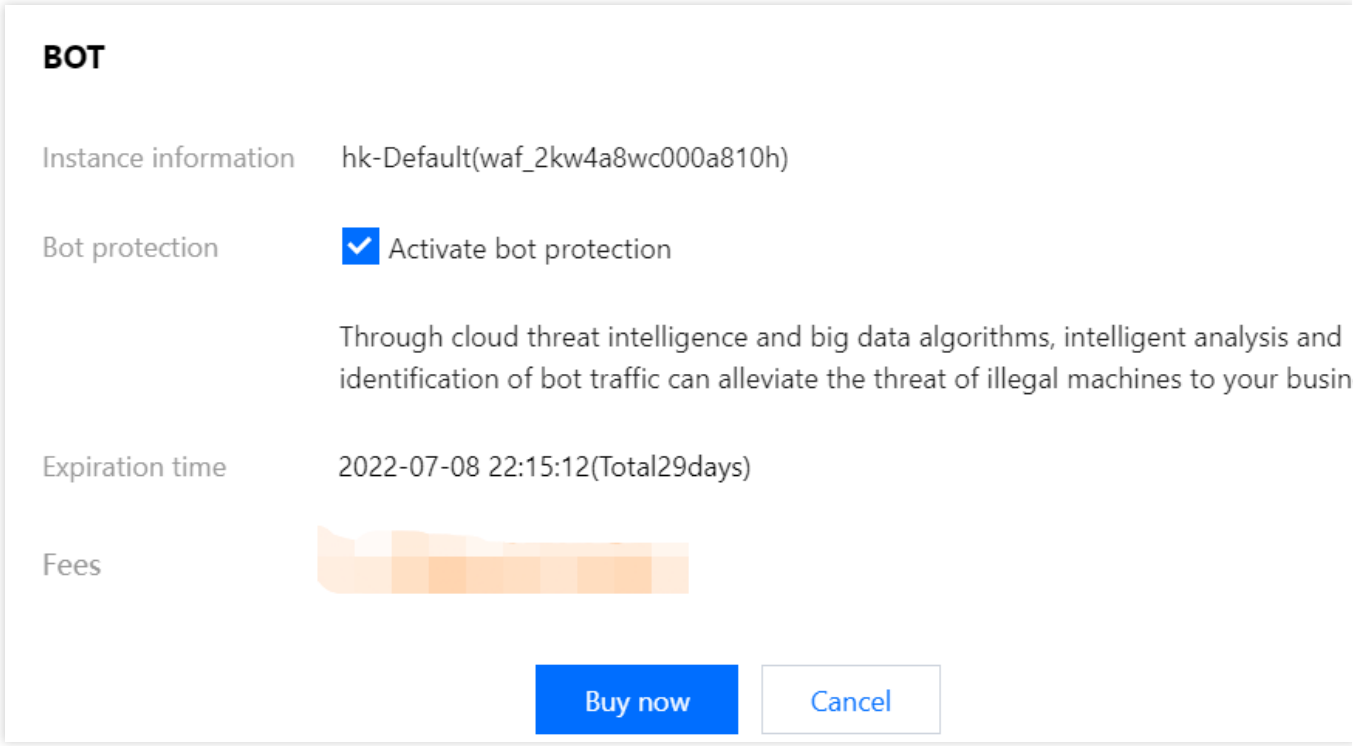
购买域名包：选择购买数量（1-500个），单击**立即购买**，即可购买域名包。



购买 QPS 扩展包：选择购买数量（1-500个），单击**立即购买**，即可购买 QPS 扩展包。



BOT与业务安全：根据实际需求勾选防护内容，单击**立即购买**，即可 BOT与业务安全。


BOT
Instance information
hk-Default(waf_2kw4a8wc000a810h)
Bot protection
Activate bot protection
Through cloud threat intelligence and big data algorithms, intelligent analysis and identification of bot traffic can alleviate the threat of illegal machines to your busin
Expiration time
2022-07-08 22:15:12(Total29days)
Fees
Buy now
Cancel

域名管理

最近更新时间：2023-12-29 14:26:38

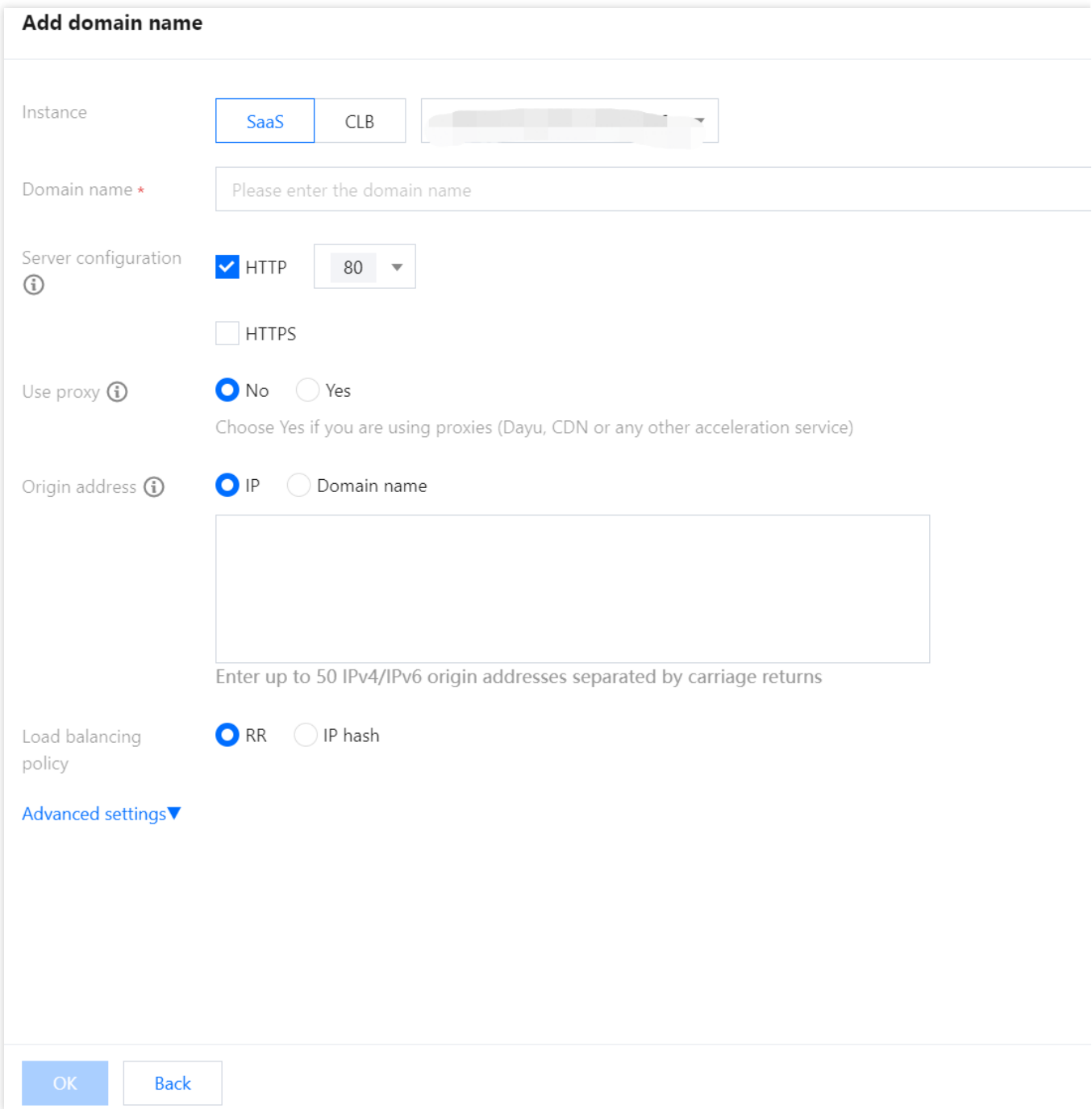
操作场景

本文档将为您介绍 Web 应用防火墙（WAF）资产中心的域名列表模块，可以查看域名详情，进行新建域名、编辑域名、删除域名等操作。

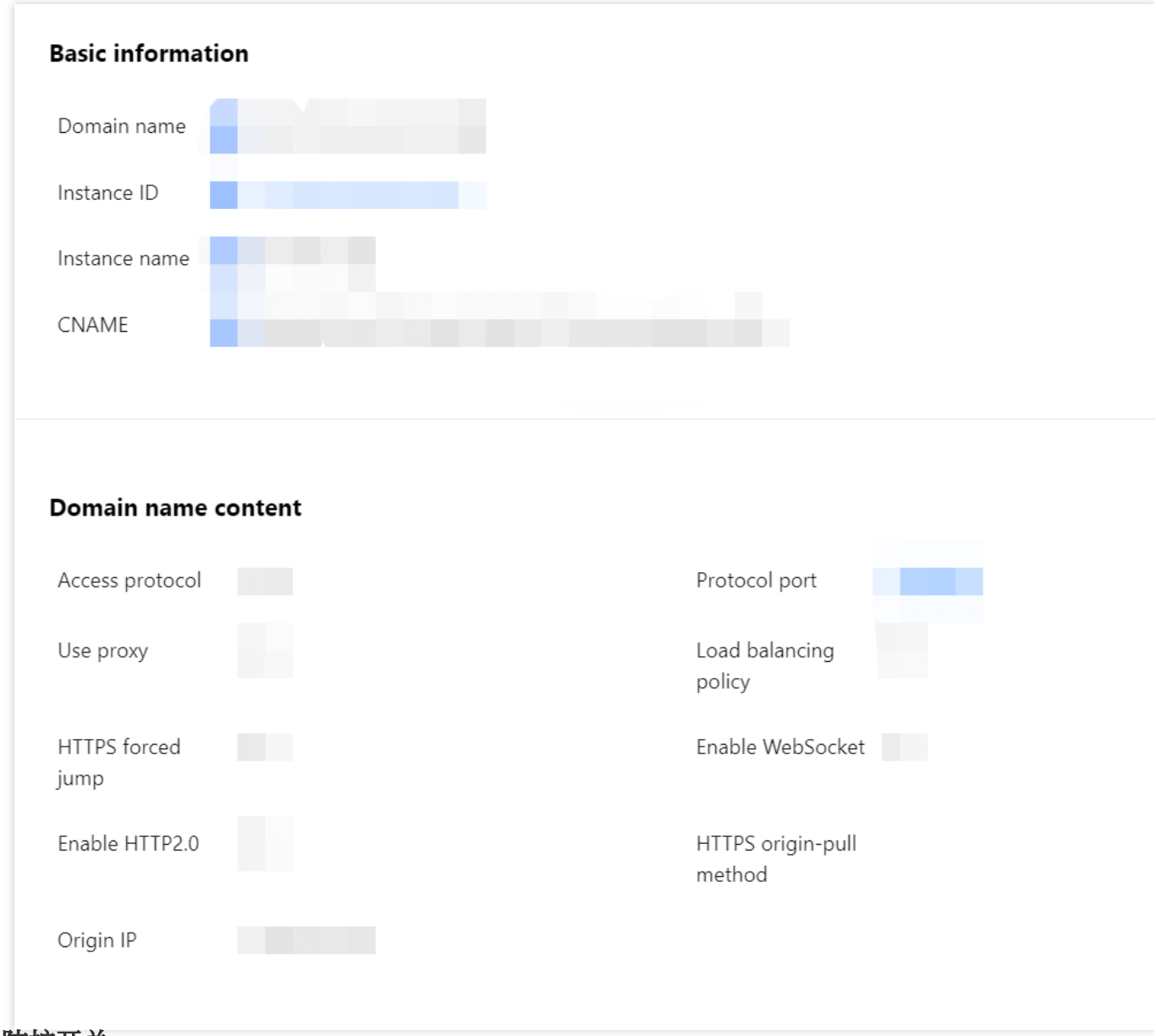
操作步骤

添加和查看域名

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心 > 域名列表**，进入域名列表页面。
2. 在域名列表页面，单击**添加域名**，右侧弹出添加域名页面。
3. 在添加域名页面，根据页面提示配置相关信息，单击**确定**，即可完成添加域名。



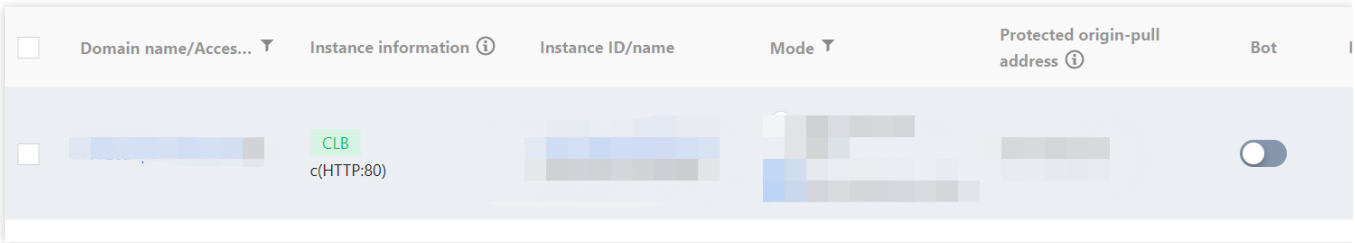
4. 在域名列表页面， 单击“域名”，进入域名详情页，可以查看域名的基本信息和域名内容。



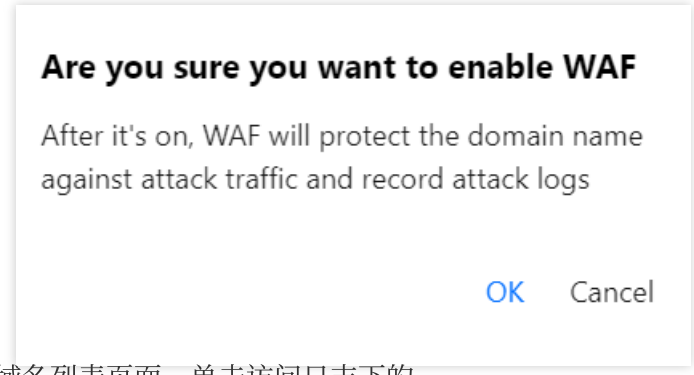
开启防护开关

1. 在域名列表页面，单击 WAF 开关下的

，弹出“确认开启”弹窗。

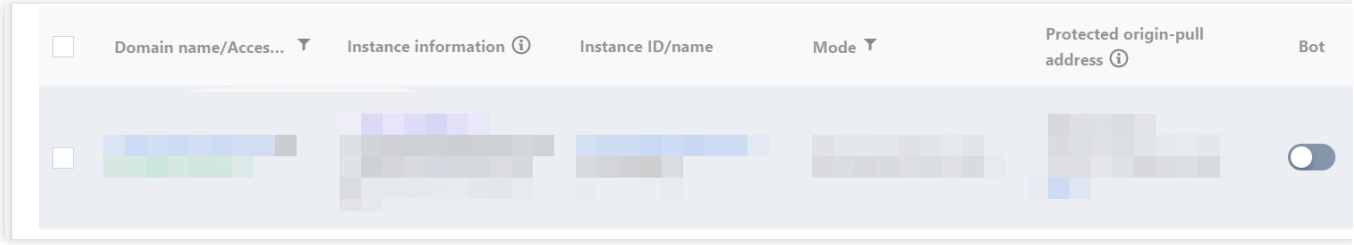


2. 在“确认开启”弹窗中，单击**确定**，开启 WAF 开关后，系统会自动根据您的自定义策略和各种攻击设置进行 WAF 防护。



3. 在域名列表页面，单击访问日志下的

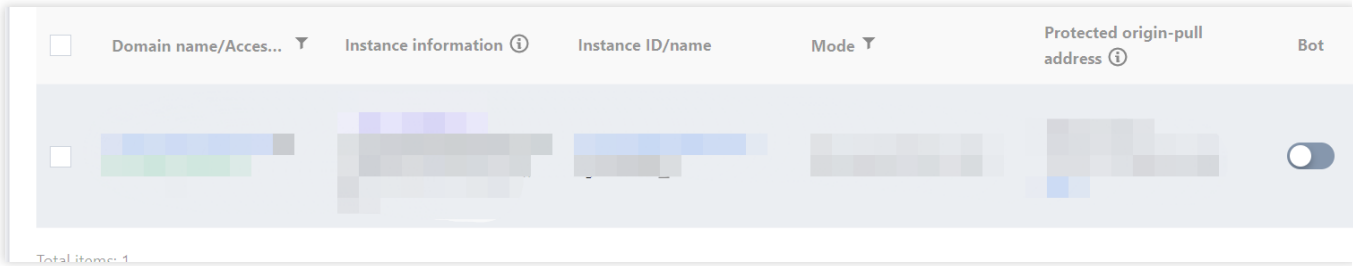
，弹出“确认开启”弹窗。



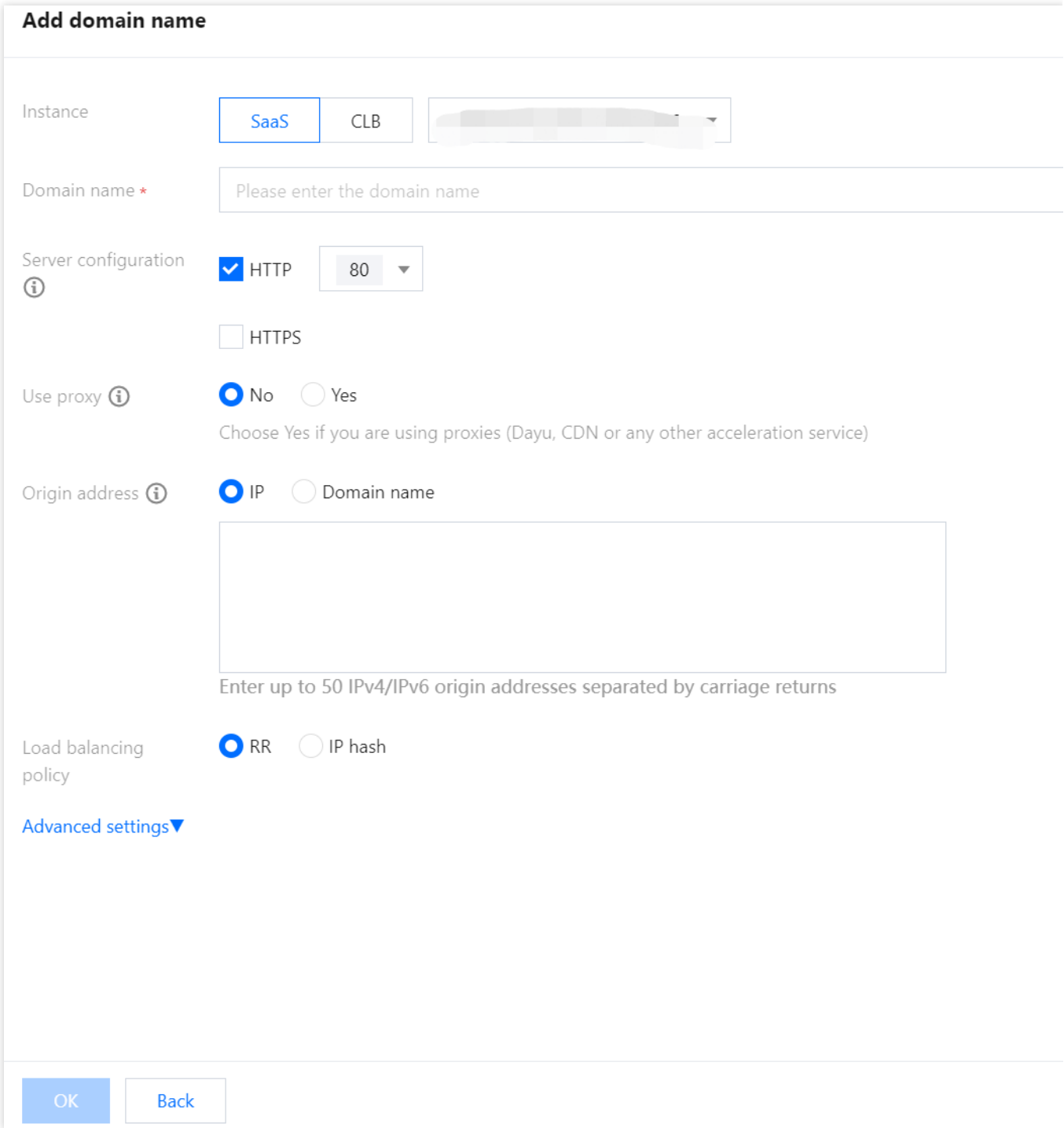
4. 在“确认开启”弹窗中，单击**确定**，开启访问日志开关后，WAF 将会记录该域名的访问流量。

编辑域名

1. 在域名列表页面，单击**编辑**，进入编辑域名页面。

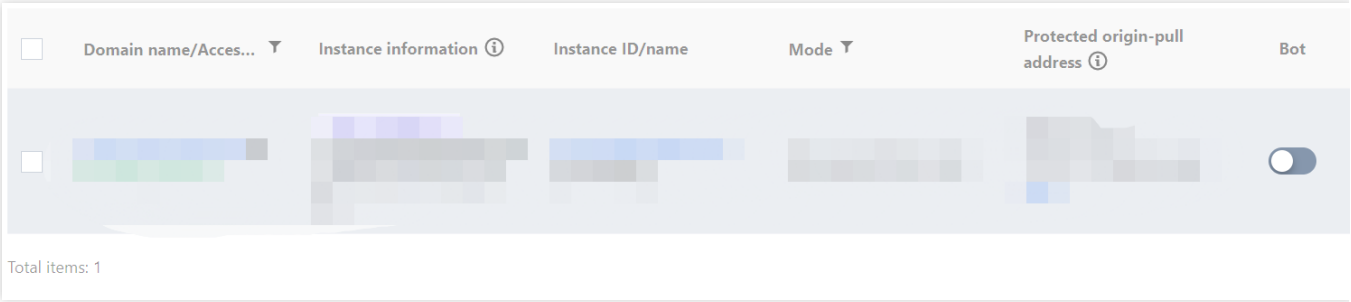


2. 在编辑域名页面，可修改服务器配置、代理情况和源站地址等信息，单击**确定**，即可保存修改。

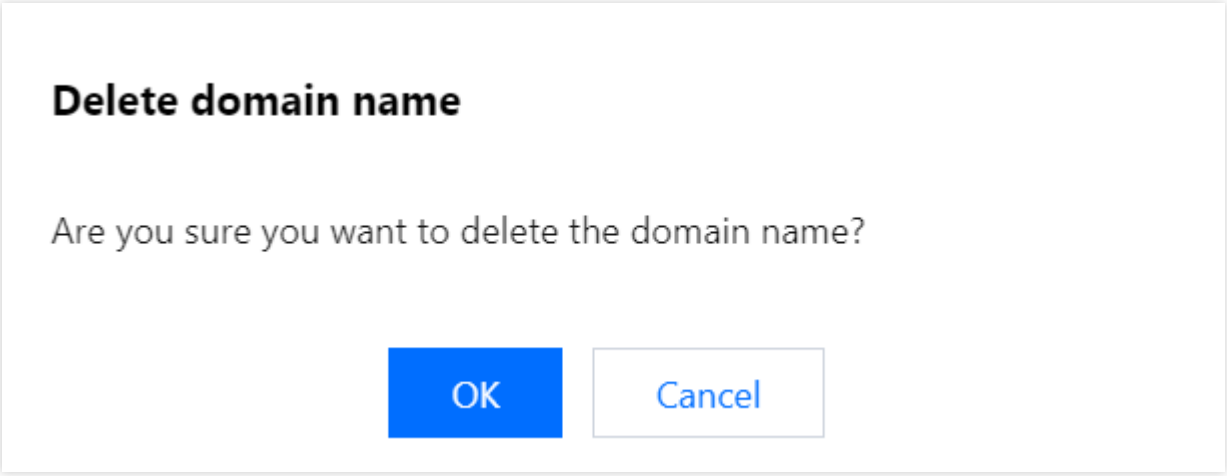


删除域名

1. 在域名列表页面，单击**删除**，弹窗“确认删除”弹窗。



2. 在“确认删除”弹窗中，单击**确定**，即可删除该域名。



域名管理高级功能

最近更新时间：2023-12-29 14:26:57

本文档主要介绍在接入域名后，如何配置流量标记、远端地址传递功能，以及访问日志记录等基于域名级的配置能力，助力客户满足等保合规合法诉求。

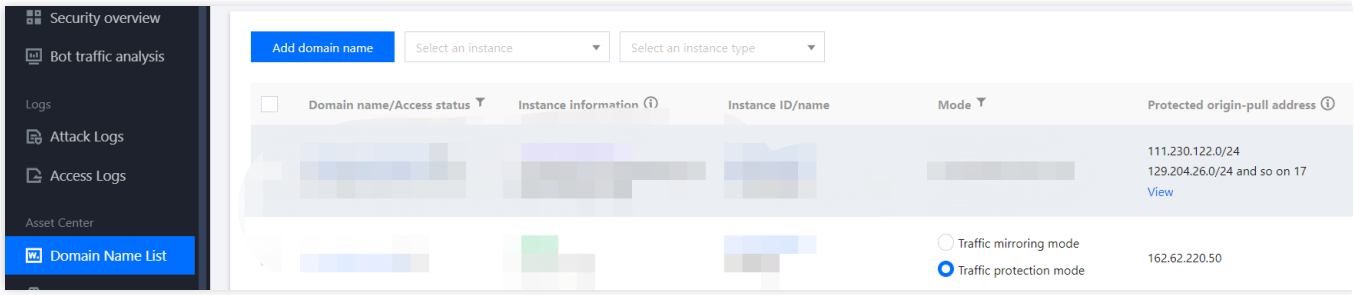
说明：

仅支持企业版、旗舰版、独享版用户使用该功能。

启用流量标记

流量标记表示 WAF 在转发客户端请求到源站服务器时，在请求头中添加或修改由您指定的自定义字段，用于标记该请求经过 WAF 转发。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**资产中心 > 域名列表**，进入域名列表页面。
2. 在域名列表页面，选择所需域名，单击操作列的**更多 > 流量标记**，弹出高级设置弹窗。



3. 在高级设置弹窗中，单击启用流量标记处的

，填写相关参数，单击**保存**。

字段说明：

流量标记字段名称：自定义 header 头标记名称。

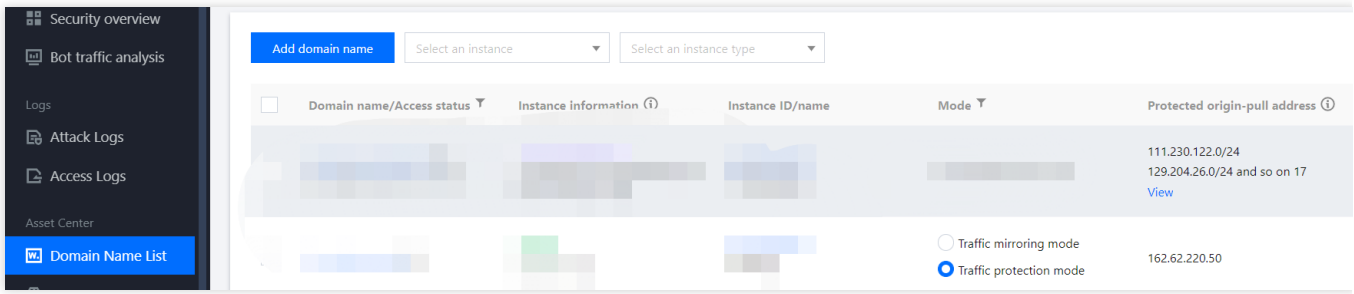
流量标记字段：自定义 header 头标记值。

4. 配置完成后，可单击**返回**，返回域名列表页面。

启用远端地址传递

远端地址传递表示 WAF 在转发客户端请求到源站服务器时，上一跳的 IP 和端口信息。

1. 在 域名列表页面，选择所需域名，单击操作列的**更多 > 请求源配置**，弹出高级设置弹窗。



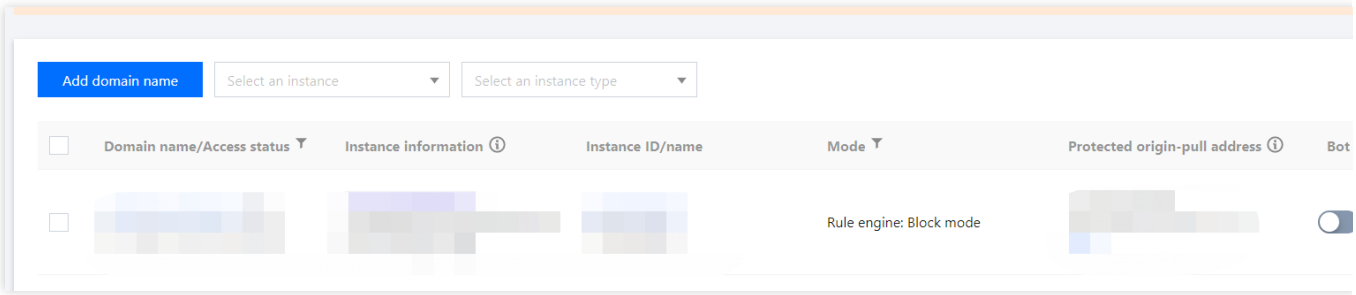
2. 在高级设置弹窗中，单击启用客户端远端地址传递处的

，开启后将记录客户端的真实 IP 及相关信息。

启用日志服务

在 域名列表页面，选择所需域名，单击访问日志处的

，开启后将自动记录访问日志，用于日常快速检索和溯源分析。



API 资产管理

最近更新时间：2023-12-29 14:27:13

功能简介

API 流量分析功能支持自动发现并梳理已接入 Web 应用防火墙（WAF）防护的业务中开放的 API 、API 参数资产，并提供相关攻击防护指引及相关异常业务调查方案，通过对异常的 API 事件及流量分析，提供详细的风险处理建议和 API 生命周期管理参考数据，帮助您实现 API 安全防护。

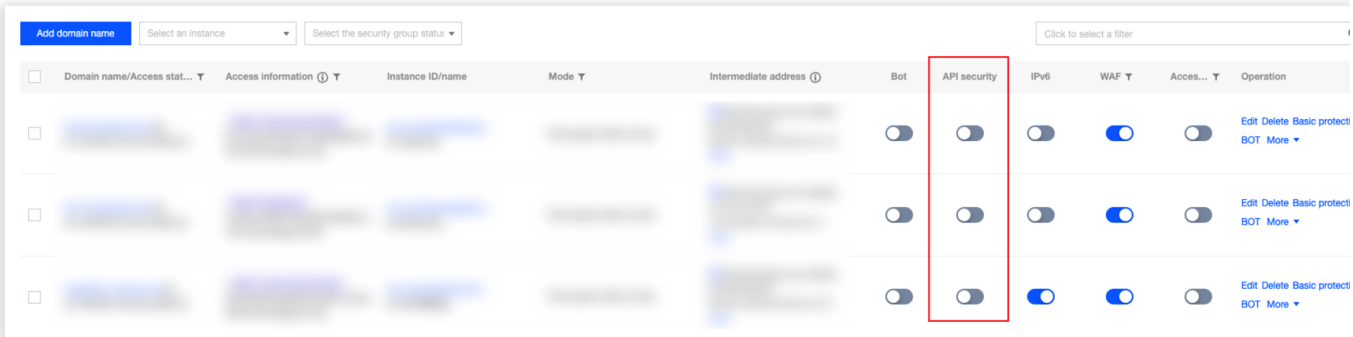
前提条件

已开通中国大陆版的 WAF 包年包月实例，并购买 API 安全实例。

开启 API 流量分析

1. 登录 Web 应用防火墙控制台，支持通过如下两种方式开启 API 流量分析功能。
在 域名列表页面，支持查看当前有哪些域名开启了 API 分析功能，并且可以在对应的 WAF 开关列中单击

，经二次确认后，即可开启 API 分析开关。

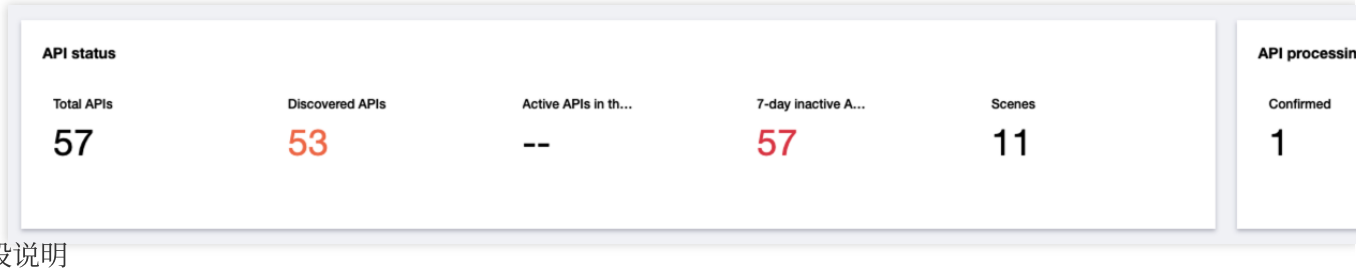


2. 开启对应域名的 API 流量分析开关后，即可对当前域名进行 API 流量的分析。

查看 API 资产列表数据

自开启所选域名的 API 流量分析功能后，API 安全会发现并捕获相关的流量数据，自动对当前业务项进行相关的分析及梳理，并展示在 API 资产列表页面。

在 **API 概览模块**中，展示当前域名下的全部的 API 数量、过去7天内活跃/不活跃的 API 数量以及涉敏的 API 数量。并可以直观的了解到对比上一个7日中的环比数量的增减，清晰的了解到当前线上的 API 的现状。



字段说明

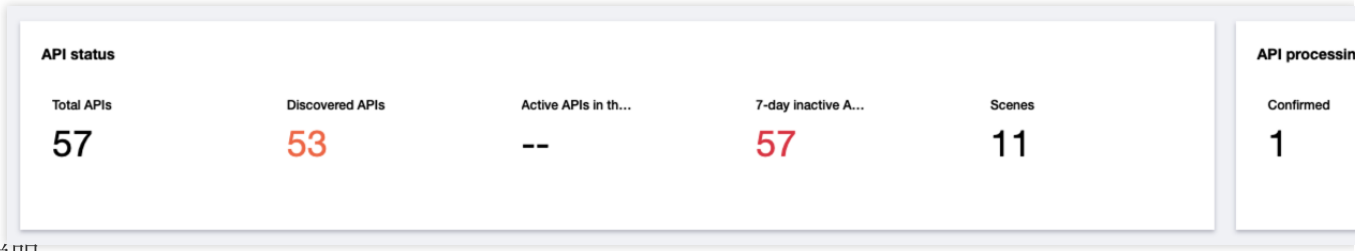
API 总数： API 管控所识别的 API 资产总数。

过去7日活跃 API：过去7日有活跃流量的 API 数。

过去 7 日不活跃 API：过去7日没有活跃流量的 API 数，有潜在变为僵尸 API 的风险。

涉敏 API：API 管控识别的包含涉敏字段的 API 数量。

在 **API 防护概况模块**中，展示当前域名的防护场景数量，并且可以获取对应的防护建议，以及当前 API 分析的内容。

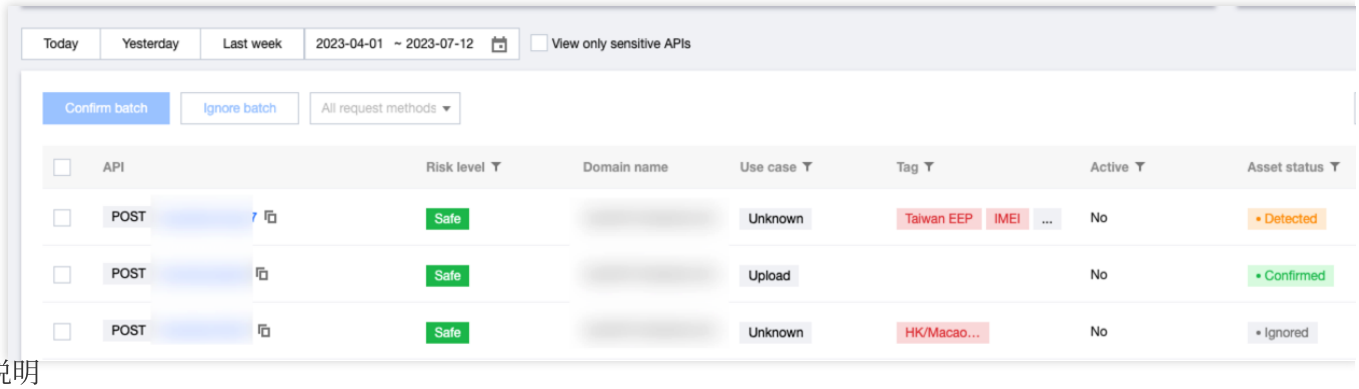


字段说明

覆盖场景：指当前 API 管控中，识别出来当前 API 所覆盖的场景类型的数量，该场景数量会随着识别出来的 API 场景增多而增加。

防护建议：指在当前的 API 管控中，识别出来对应场景的防护建议。

在 **API 列表**中，展示了 API、请求方式，对应域名、覆盖功能场景、是否包含敏感字段、是否活跃，是否存在相关防护建议、以及 API 发现时间、API 参数最近变更时间等。并支持通过单击对应 API 的**查看详情**，获悉该 API 的相关 API 详情。

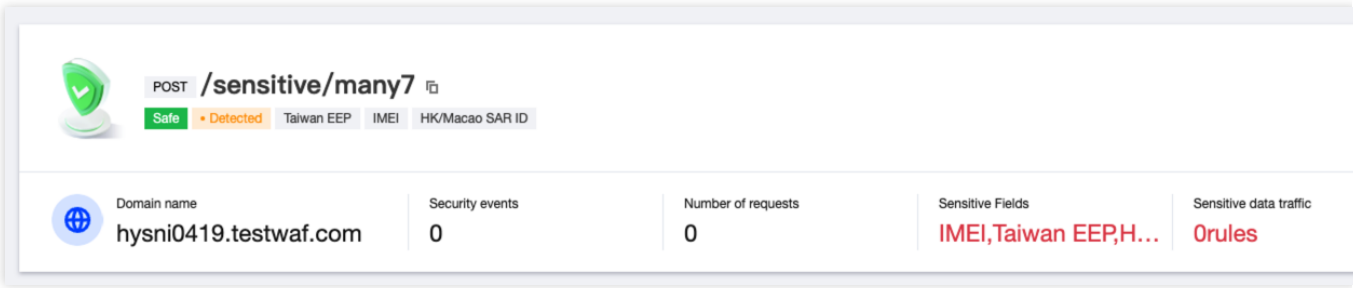


字段说明

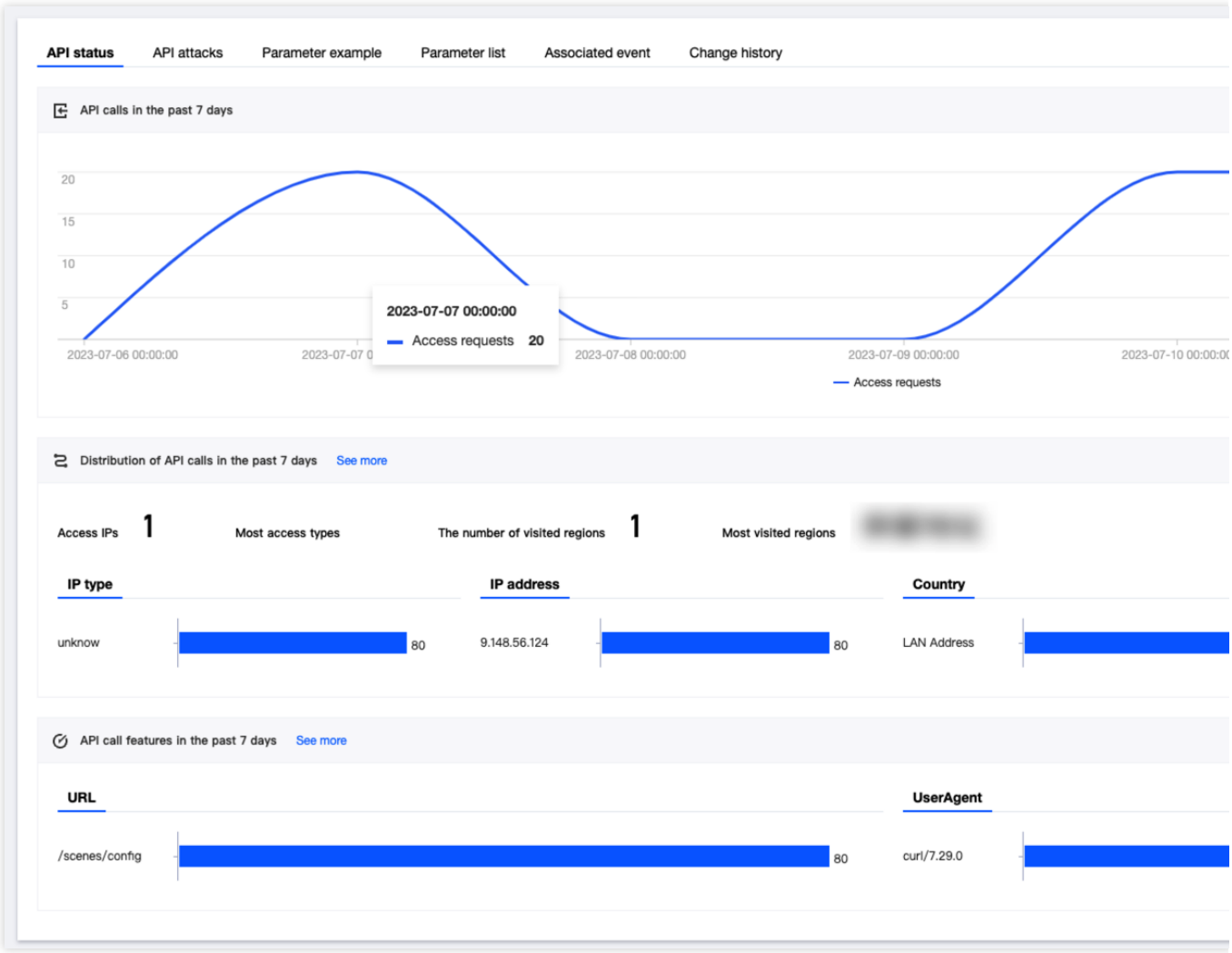
API：指经过 API 管控分析后，识别出来的经过数据归一化折叠后的 API 信息，展示当前 API 的经过数据归一化后的 API 的样式，用户 id 、信息 id 等信息过于分散导致 API 的散列度过大，造成当前 API 观测过难的问题。
请求方法：HTTP 请求方法。
所属域名：当前 API 的归属域名。
功能场景：由 API 管控识别出来的相关业务的功能场景、如验证码、回调等，如果识别出的数据不准确，可以在 API 详情 中进行相关修正。
涉敏字段：由 API 管控识别出来的传输参数上存在敏感字段的字段内容，包括但不限于银行卡号、身份证号等数据字段，如果识别出来的数据类型不准确，可以在 API 详情 中进行相关修正。
过去7天是否活跃：过去7天内是否为活跃流量。
最近更新时间：最新的更新时间，用于检测当前 API 的相关数据字段是否发生新增等情况。
发现时间：api 首次被 API 分析模块发现的时间。
查看详情：进入对应 API 的详情页面。

API 详情

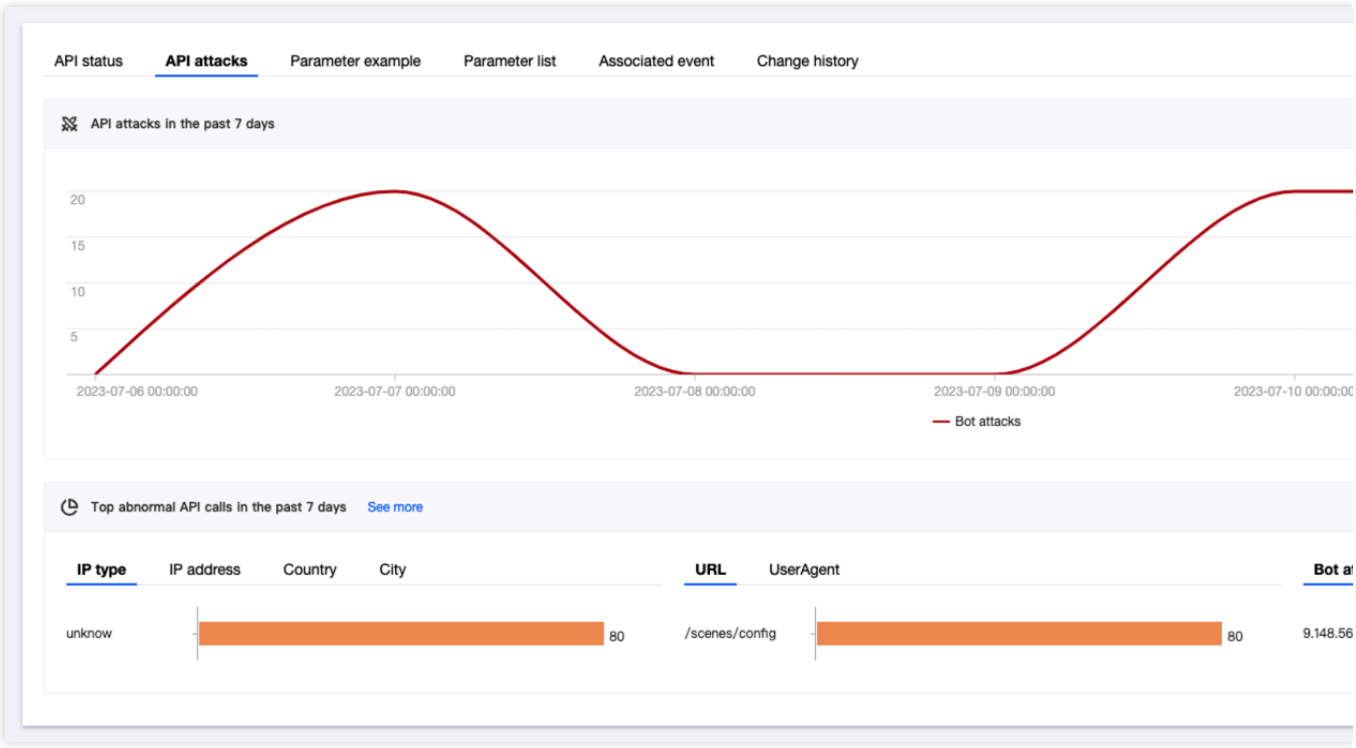
在 API 列表中，单击目标 API **操作列**的**查看详情**，可以进入 API 详情页面，该页面展示了经过 API 管控分析之后的单一 API 的相关详情，包括如下5个部分内容：
API 概要：展示该 API 所属域名、请求方法、相关功能标签、是否存在敏感字段、是否活跃以及进行数据归一化后的 API 内容。



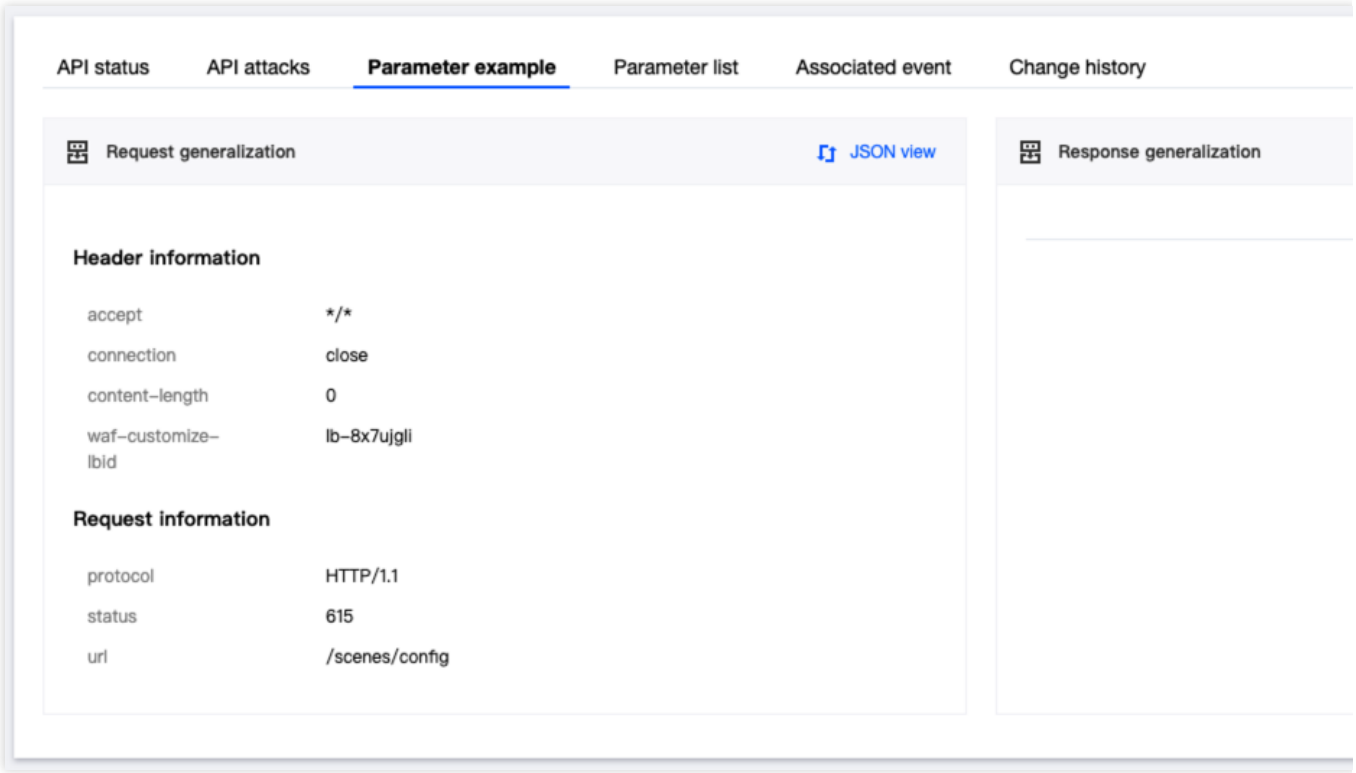
API 概览：展示最近7天内，对应 API 的总请求量及请求趋势，访问的来源分布、访问最多的 URL 及 UA 类型。



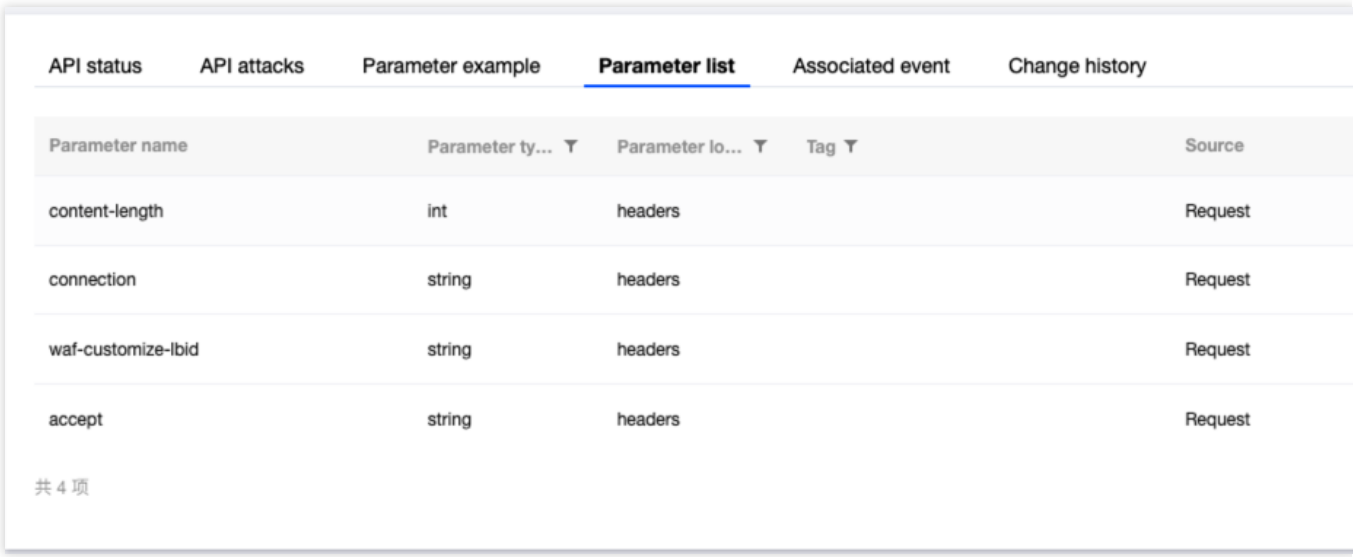
API 攻击概览：展示最近7天内，该 API 的攻击趋势，以及攻击分布，包括 IP 类型、IP 来源、URL、UA、攻击类型分类。



请求参数样例：展示该 API 经过数据抽象化后，展示的数据内容信息。



参数列表：展示该 API 传输的各个参数字段的内容信息、位置信息，并可以对其进行手动打标。


API status
API attacks
Parameter example
Parameter list
Associated event
Change history
Parameter name
Parameter ty...
Parameter lo...
Tag
Source
content-length
int
headers
Request
connection
string
headers
Request
waf-customize-lbid
string
headers
Request
accept
string
headers
Request
共 4 项

基础安全配置
规则引擎

最近更新时间：2023-12-29 14:27:35

本文档将为您介绍如何通过 Web 应用防火墙（WAF）进行规则防护设置，以防护 Web 攻击。

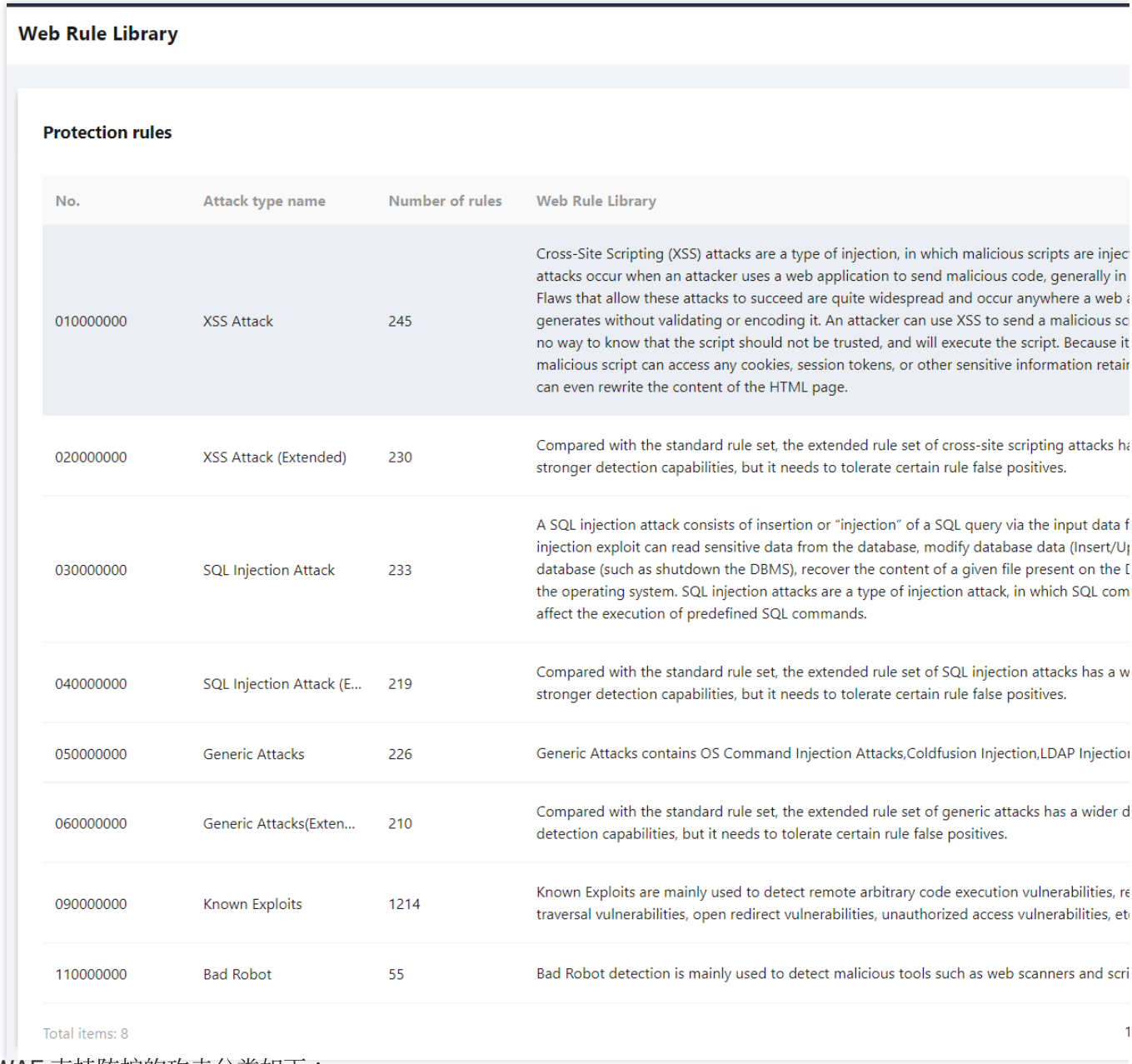
背景信息

腾讯云 Web 应用防火墙（WAF）使用基于正则的规则防护引擎和基于机器学习的 AI 防护引擎，进行 Web 漏洞和未知威胁防护。
腾讯云 WAF 规则防护引擎，提供基于腾讯安全 Web 威胁和情报积累的专家规则集，自动防护 OWASP TOP10 攻击。目前防护 Web 攻击包括：SQL 注入、XSS 攻击、恶意扫描、命令注入攻击、Web 应用漏洞、Webshell 上传、不合规协议、木马后门等17类通用的 Web 攻击。
WAF 规则防护引擎，支持规则等级划分，用户可根据实际业务需要进行规则防护等级设置，并支持对规则集规则或单条规则进行开关设置，可以对 WAF 预设的规则进行禁用操作，同时提供基于指定域名 URL 和规则 ID 白名单处置策略，进行误报处理。

操作步骤

查看规则分类

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择服务管理 > Web 规则库，进入 Web 规则库页面。
2. 在 Web 规则库页面的“防护规则”标签内，可查看当前 WAF 支持防护的攻击分类描述和规则更新动态信息。



Web Rule Library

Protection rules

No.	Attack type name	Number of rules	Web Rule Library
010000000	XSS Attack	245	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injec attacks occur when an attacker uses a web application to send malicious code, generally in Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web generates without validating or encoding it. An attacker can use XSS to send a malicious sc no way to know that the script should not be trusted, and will execute the script. Because it malicious script can access any cookies, session tokens, or other sensitive information retai can even rewrite the content of the HTML page.
020000000	XSS Attack (Extended)	230	Compared with the standard rule set, the extended rule set of cross-site scripting attacks h stronger detection capabilities, but it needs to tolerate certain rule false positives.
030000000	SQL Injection Attack	233	A SQL injection attack consists of insertion or "injection" of a SQL query via the input data f injection exploit can read sensitive data from the database, modify database data (Insert/U database (such as shutdown the DBMS), recover the content of a given file present on the D the operating system. SQL injection attacks are a type of injection attack, in which SQL com affect the execution of predefined SQL commands.
040000000	SQL Injection Attack (E...	219	Compared with the standard rule set, the extended rule set of SQL injection attacks has a w stronger detection capabilities, but it needs to tolerate certain rule false positives.
050000000	Generic Attacks	226	Generic Attacks contains OS Command Injection Attacks,Coldfusion Injection,LDAP Injectio
060000000	Generic Attacks(Exten...	210	Compared with the standard rule set, the extended rule set of generic attacks has a wider d detection capabilities, but it needs to tolerate certain rule false positives.
090000000	Known Exploits	1214	Known Exploits are mainly used to detect remote arbitrary code execution vulnerabilities, re traversal vulnerabilities, open redirect vulnerabilities, unauthorized access vulnerabilities, et
110000000	Bad Robot	55	Bad Robot detection is mainly used to detect malicious tools such as web scanners and scri

Total items: 8

当前 WAF 支持防护的攻击分类如下：

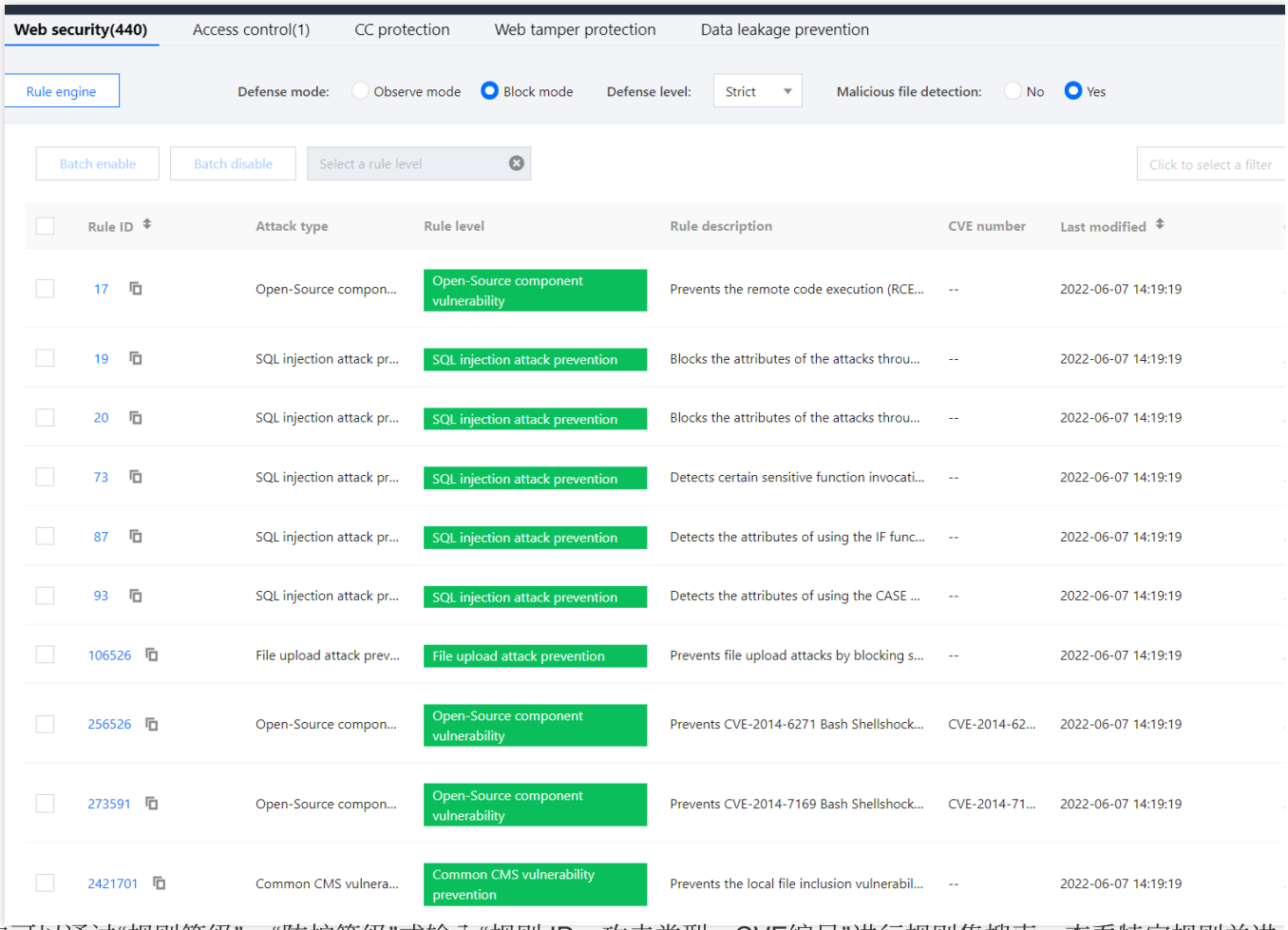
攻击分类	攻击描述
SQL 注入攻击	在网站实现上，对于输入参数过滤不严，导致 SQL 数据库的内容被非法获取。
XSS 攻击	当应用程序的新网页中包含不受信任的、未经恰当验证或转义的数据，或者使用可以创建 HTML 或 JavaScript 的浏览器 API 更新现有的网页时，会出现 XSS 缺陷。XSS 让攻击者能够在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。
恶意扫描	检测网站是否被恶意扫描。
核心文件非法访问	检测某些配置文件、数据库文件及参数数据，是否被随意下载。
开源组件漏洞攻击	常见 Web 开源组件漏洞产生的攻击行为。

命令注入攻击	注入攻击的一种，包含 shell 命令注入，PHP 代码注入，Java 代码注入等，若被攻击者成功利用，可导致网站执行攻击者注入的代码。
WEB 应用漏洞攻击	Web 应用程序的安全性（在 Web 服务器上运行的 Java、 ActiveX、PHP、ASP 代码的安全）。
XXE 攻击	由于 XML 处理器在 XML 文件中存在外部实体引用。攻击者可利用外部实体窃取使用 URI 文件处理器的内部文件和共享文件、监听内部扫描端口、执行远程代码和实施拒绝服务攻击。
木马后门攻击	检测木马传播过程或木马上传后与控制端通信行为。
文件上传攻击	当上传文件伪装成正常后缀的恶意脚本时，攻击者可借助本地文件包含漏洞执行该文件。
其他漏洞攻击	由于Web 服务器本身安全和其他软件配置安全或漏洞引起的攻击。
不合规协议	HTTP 协议参数，头部请求参数异常。

3. 通过“防护规则”标签右侧的规则更新动态，可查看规则更新信息，更多安全公告信息可在 安全公告 中查看。

规则管理

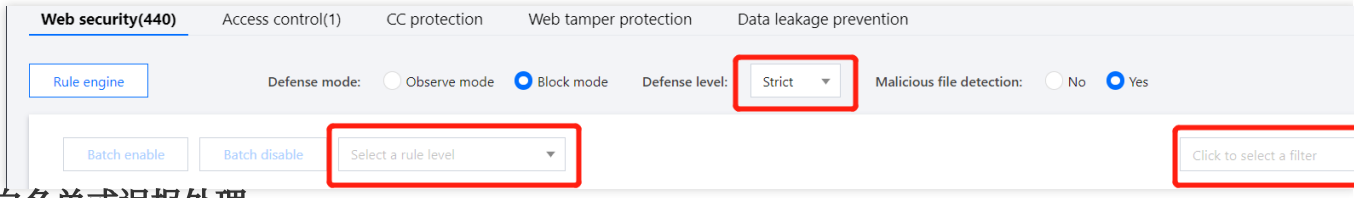
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > 基础安全**，进入基础安全页面。
2. 在基础安全页面，单击 WEB 安全，在“规则引擎”页签内，可基于域名实现对单条规则的开通设置，决定在规则引擎中是否启用该规则，所有规则默认为开启。



3. 用户可以通过“规则等级”、“防护等级”或输入“规则 ID、攻击类型、CVE编号”进行规则集搜索，查看特定规则并进行操作。

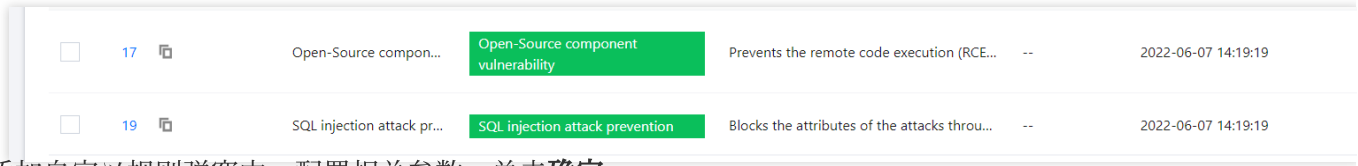
说明：

严格规则等级包含正常和宽松规则，正常规则等级包含宽松规则。

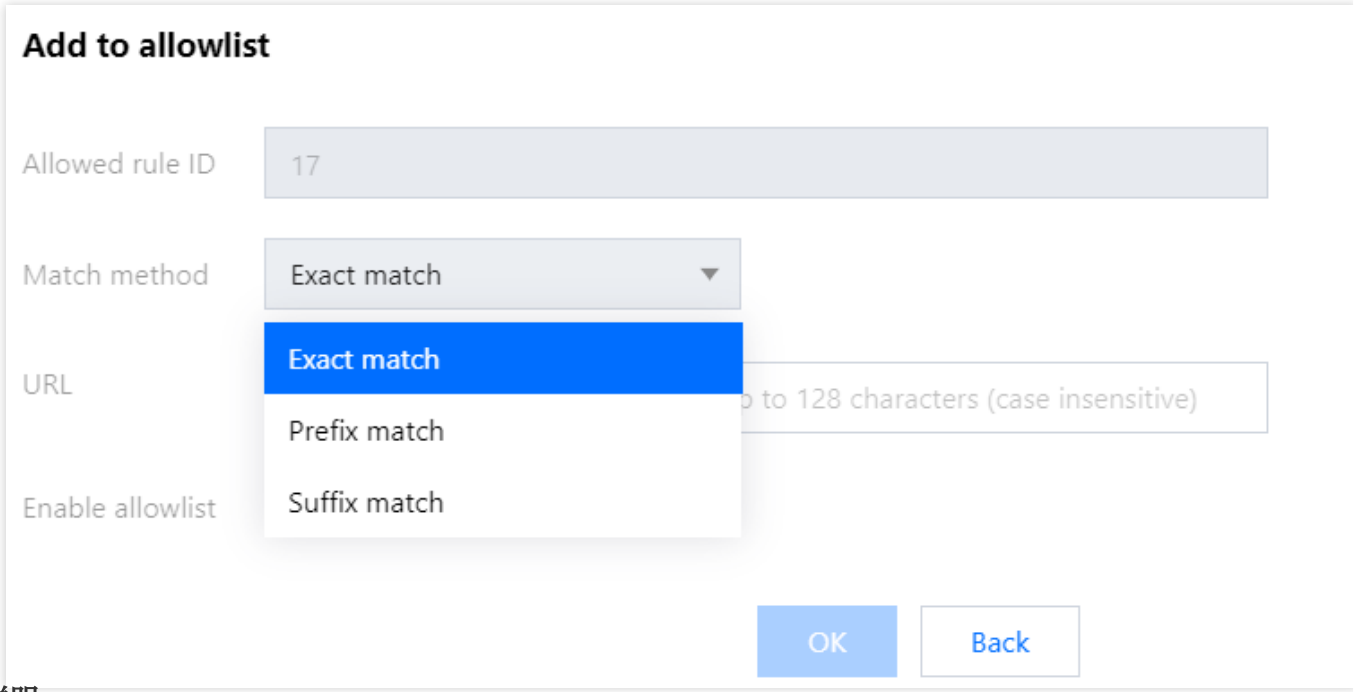


规则白名单或误报处理

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 > 基础安全**，进入基础安全页面。
2. 在基础安全页面，单击 **WEB 安全**，在“规则引擎”页签内，可以实现基于域名 URL 和规则 ID 的加白名单及误报处理。
3. 在“规则引擎”页签，选择所需规则，单击加白名单，弹出添加自定义规则弹窗。



4. 在添加自定义规则弹窗中，配置相关参数，单击**确定**。



字段说明

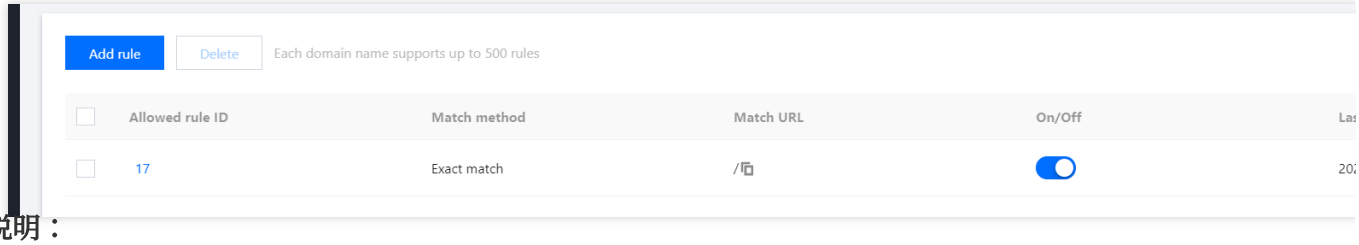
添加规则 ID：填写需要加白的规则 ID，一条策略可添加1个规则 ID。

匹配方式：加白 URL 路径的匹配方式，支持完全匹配（默认）、前缀匹配和后缀匹配。

URL 路径：需要加白的 URL 路径，同一个域名下 URL 不可重复添加。

白名单开关：白名单策略生效开关，默认为开启。

5. 白名单添加完成后，单击**查看白名单**，查看该白名单规则，并进行相关操作。



字段说明：

加白规则 ID：所设置的加白规则 ID，可以通过攻击日志或规则管理获取。

匹配方式：加白 URL 路径的匹配方式，支持完全匹配（默认）、前缀匹配和后缀匹配。

匹配路径：需要加白的 URI 路径，同一个域名下 URI 不可重复添加。

白名单开关：白名单策略生效开关。

修改时间：最近一次创建或修改策略的时间。

操作：对策略进行编辑或删除操作。

单击**编辑**，修改相关参数，单击**确认**，即可以对规则参数进行修改。]

单击**删除**，经过二次确认后，可删除该策略。

IP 封禁

最近更新时间：2023-12-29 14:30:30

本文档将为您介绍 Web 应用防火墙（WAF）攻击 IP 惩罚功能，可以快速拦截恶意 Web 攻击 IP，快速反应应对恶意扫描及代理、Web 攻击威胁等行为，可提升攻防对抗效率。

背景信息

攻击 IP 惩罚指的是自动阻断在短时间内发起多次 Web 攻击（规则引擎触发）的客户端 IP，一段时间内阻止所有请求，阻断日志可以在 攻击日志 中查看。

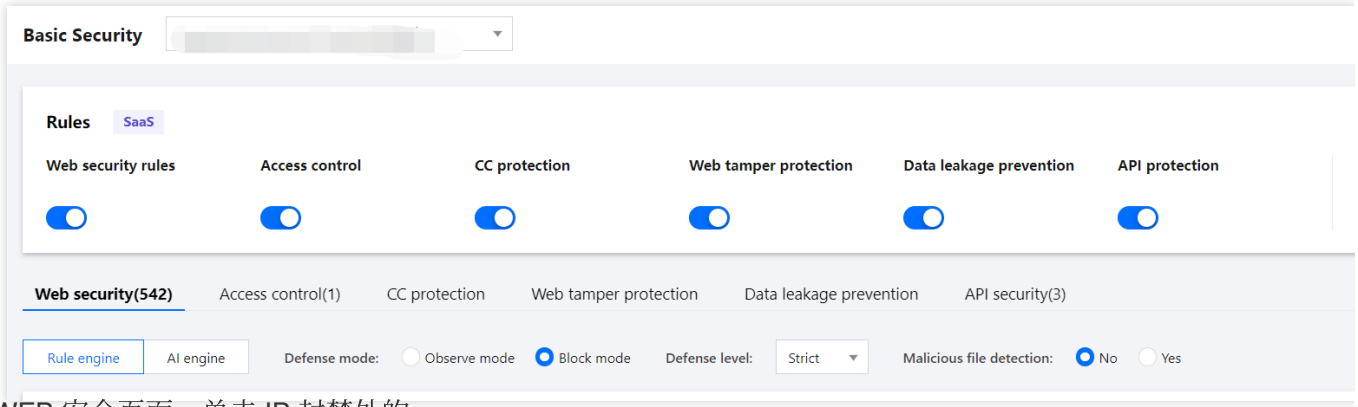
前提条件

已 购买 Web 应用防火墙套餐。
完成防护域名添加，域名处于正常防护状态。操作详情请参见 快速入门。
当前 IP 封禁支持域名级区分封禁，不同域名检测时长不同，封禁时间也单独计算。

操作步骤

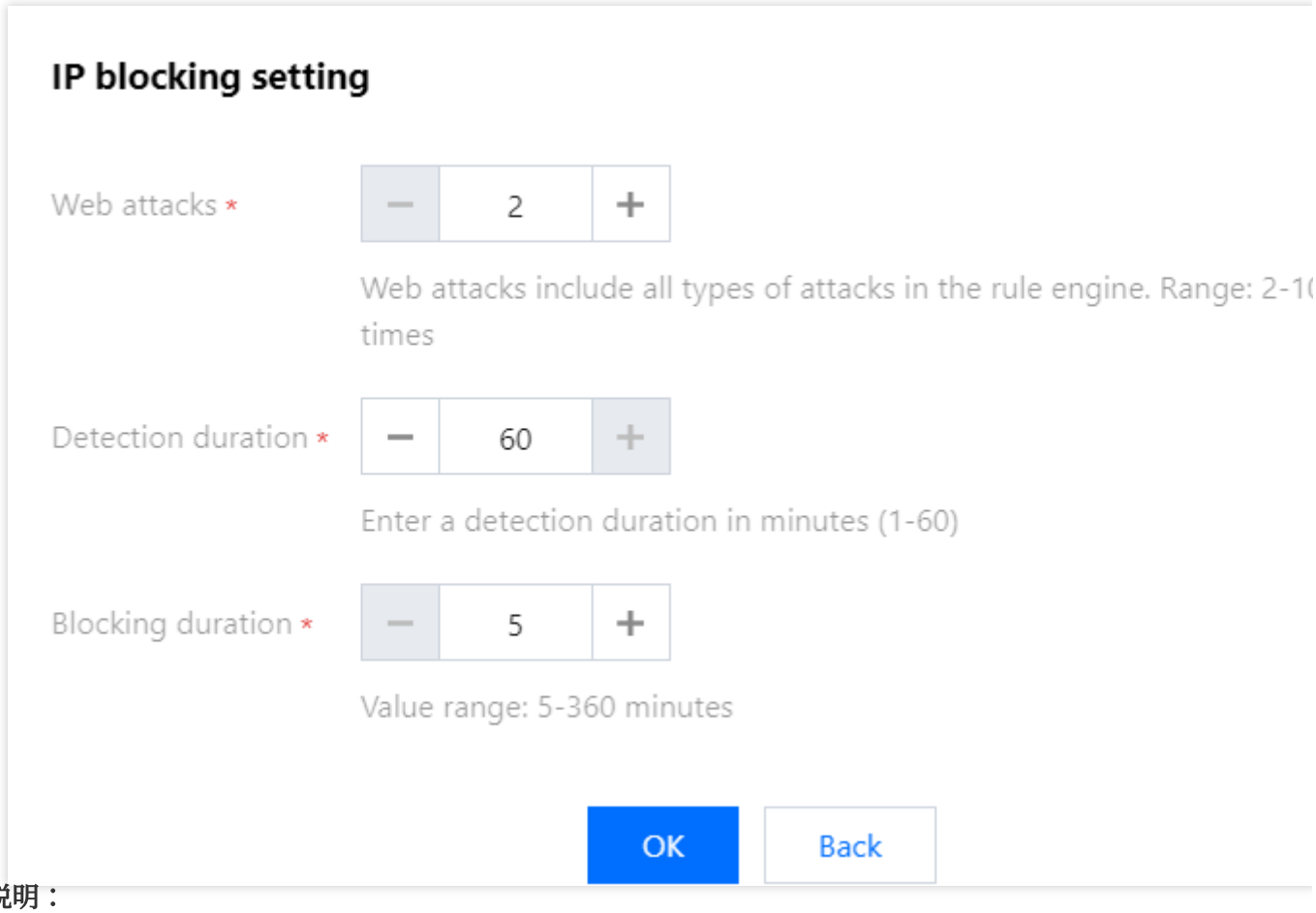
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > 基础安全 > WEB 安全**，进入 WEB 安全页面。
2. 在 WEB 安全页面，左上角选择需要防护的域名，单击 IP 封禁处的

，开启 IP 封禁。



3. 在 WEB 安全页面，单击 IP 封禁处的

，对 IP 封禁的默认参数进行修改，单击**确定**即可根据业务情况设置阈值。



字段说明：

Web 攻击次数：统计攻击源 IP 在指定时间内触发 Web 攻击（规则引擎触发，不包括 AI 引擎、自定义策略、CC 攻击等模块）的次数。

检测时长：指定统计攻击源 IP 检测时长。

封禁时间：封禁该 IP 的请求时长。

访问控制

最近更新时间：2023-12-29 14:36:41

功能简介

访问控制策略支持从 HTTP 报文的请求路径、GET 参数、 POST 参数、 Referer 和 User-Agent 等多个特征进行组合，通过特征匹配来对公网用户的访问进行管控。面对来自互联网上的各种攻击行为，腾讯云用户可以利用访问控制策略灵活应对，组合出有针对性的规则来阻断各类攻击行为。

说明：

每个访问控制策略最多可以设置5个条件进行特征控制。

每个访问控制策略中的多个条件之间是“与”的关系，即所有条件全部匹配，策略才可生效。

每个访问控制策略匹配之后可以配置四种处理动作：拦截、人机识别、观察、重定向。

拦截：WAF 对命中该策略的访问进行拦截操作；

人机识别：WAF 对命中该策略的访问进行人机识别操作，图片验证码。

观察：WAF 对命中该策略的访问进行观察操作。

重定向：WAF 对命中该策略的访问进行重定向页面。

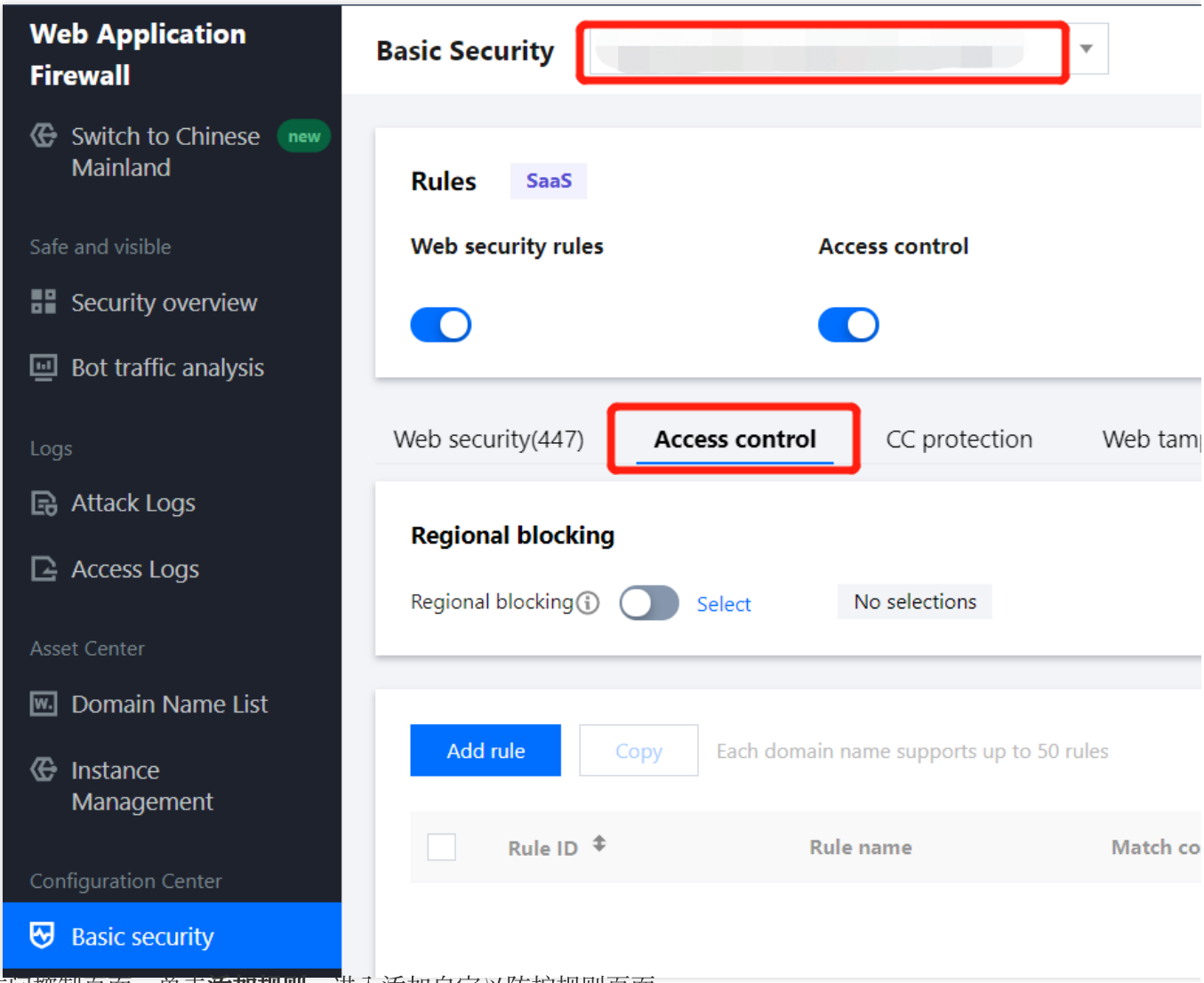
优先级：优先级数值越小则优先级越高，即1优先级最高，100优先级最低。

配置案例

示例一：禁止特定 IP 地址访问指定站点

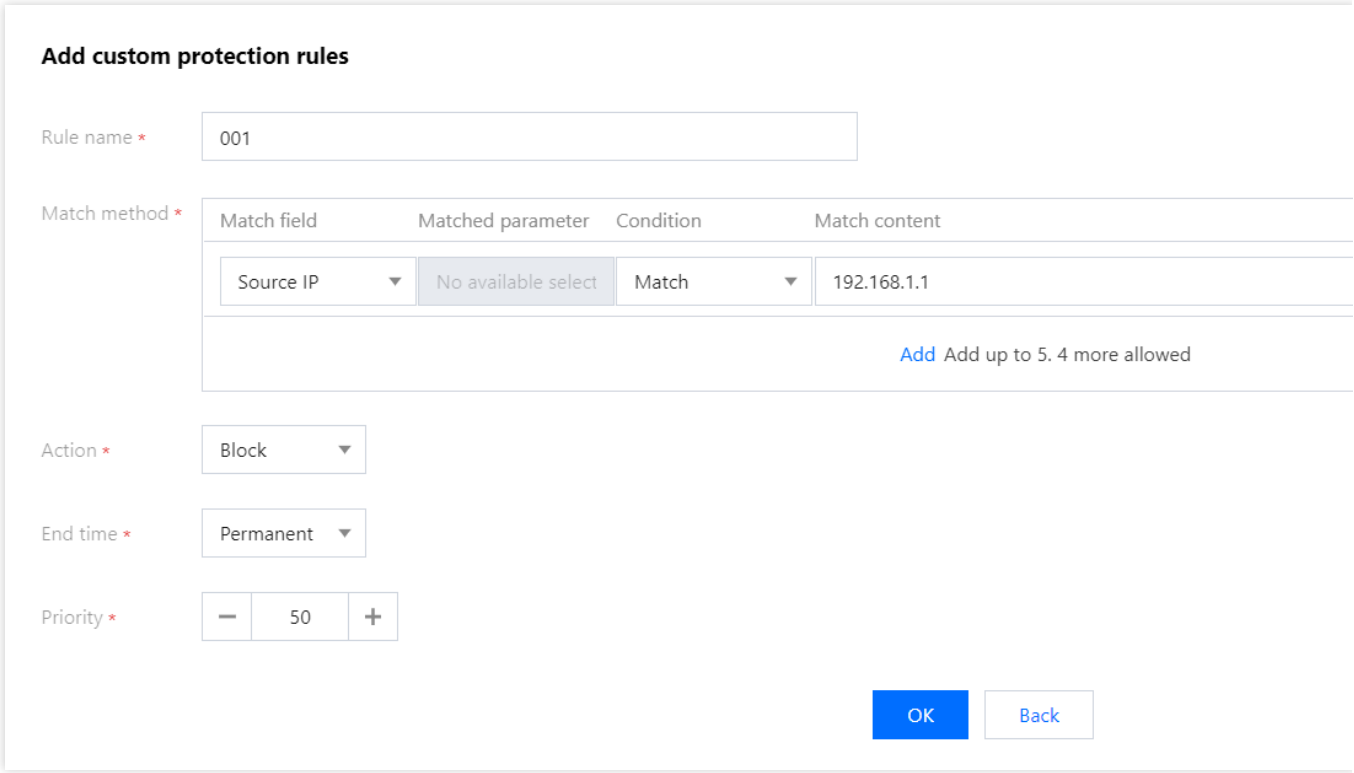
当网站管理员需要禁止特定 IP 地址访问指定站点时，可以通过以下方法进行配置：

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心 > 基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击**访问控制**，进入访问控制页面。



3. 在访问控制页面，单击**添加规则**，进入添加自定义防护规则页面。

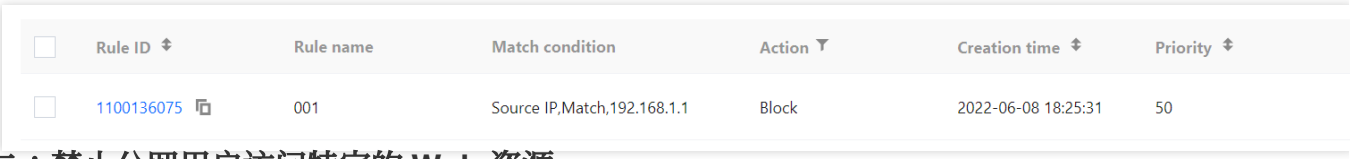
4. 在添加自定义防护规则页面，输入规则名称（如001），在匹配字段中选择一个字段（如来源 IP），逻辑符号选择匹配，匹配内容填入需要禁止访问的来源 IP（如192.168.1.1），选择执行动作（如阻断），填写完成后，单击**确定**，保存规则。



说明：

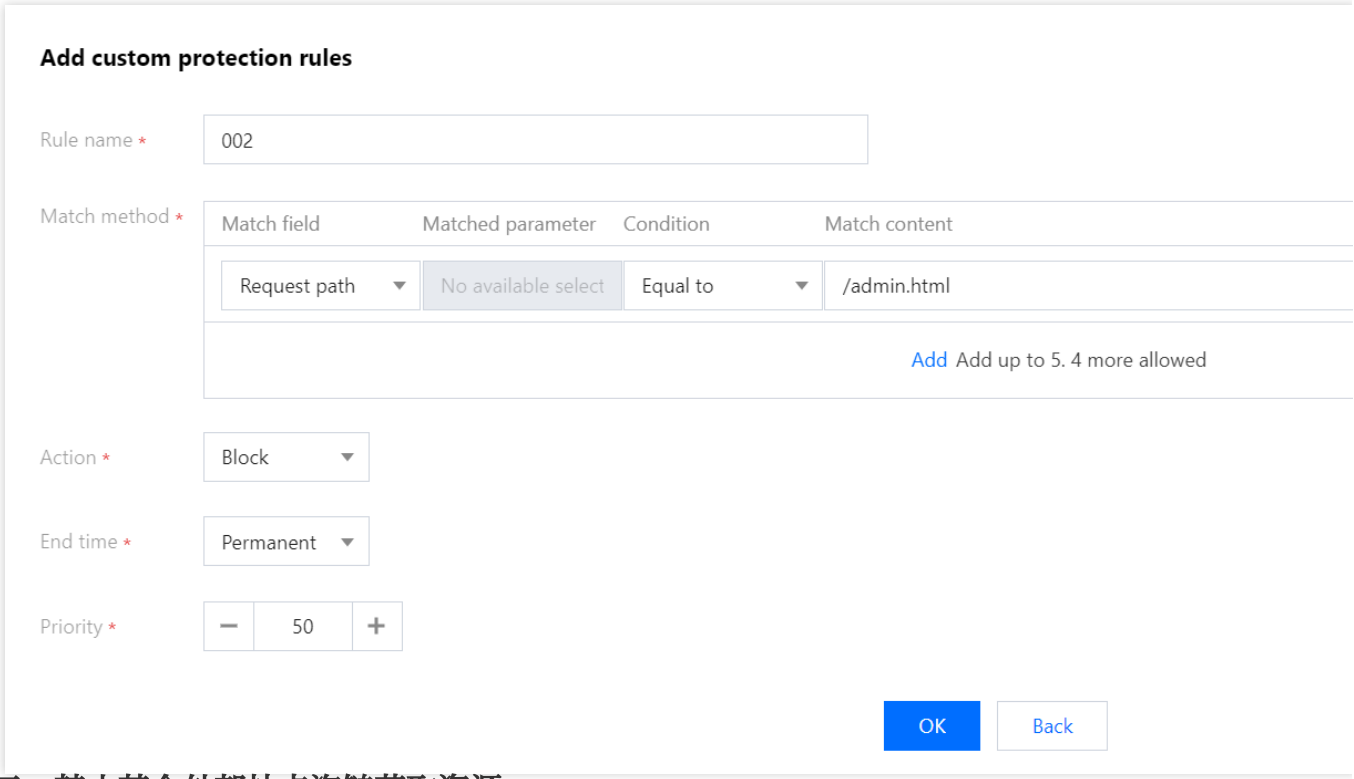
Web 应用防火墙的访问控制策略支持使用掩码来控制某一网段的源 IP 的访问请求。我们可以在匹配内容中输入特定网段（如10.10.10.10/24 ）。

5. 此时规则将会生效，来自特定源 IP 的 HTTP 访问请求将会全部阻断。



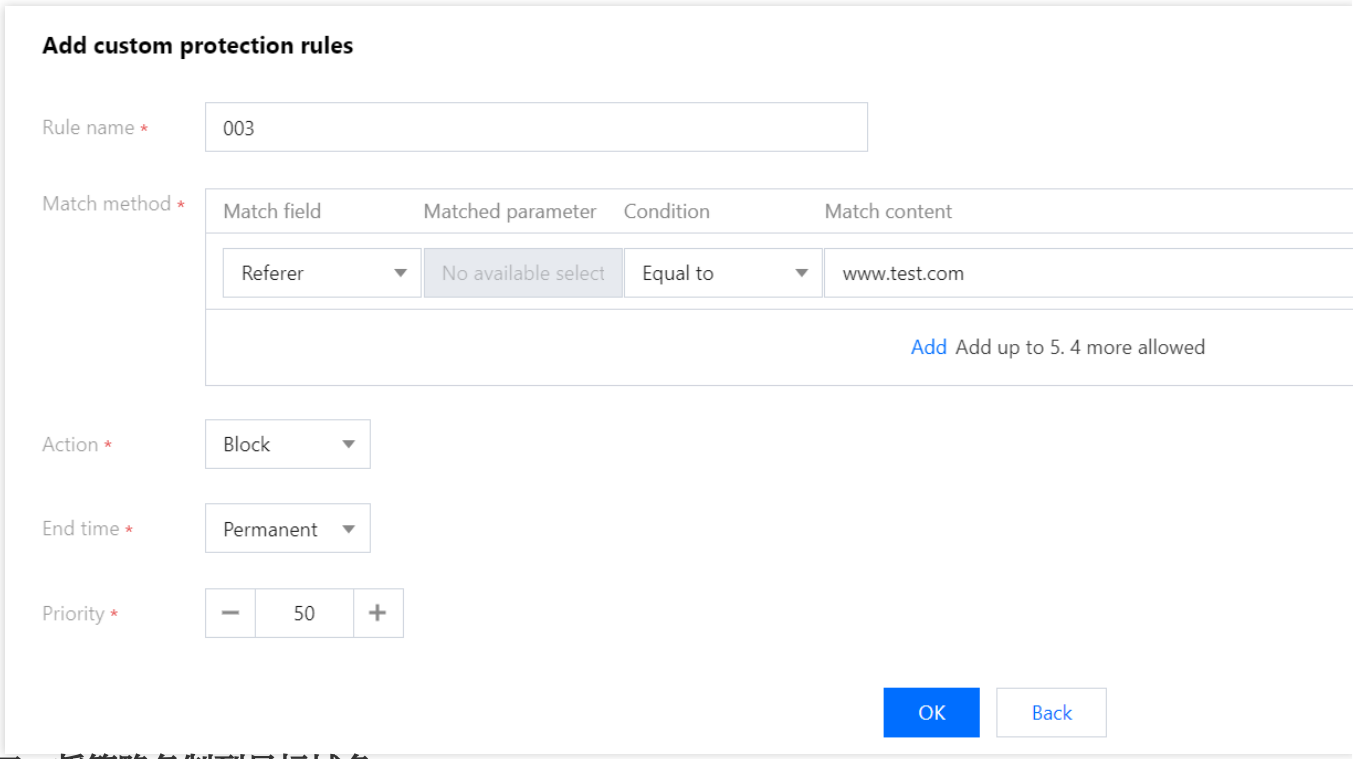
示例二：禁止公网用户访问特定的 Web 资源

当网站管理员不希望公网用户访问某些特定的 Web 资源时（如管理后台 `/admin.html` ），可以进行以下配置：匹配字段选择“请求路径”，逻辑符号选择“等于”，匹配内容输入 `/admin.html` ，执行动作选择“阻断”，配置完成后单击**确定**即可。



示例三：禁止某个外部站点盗链获取资源

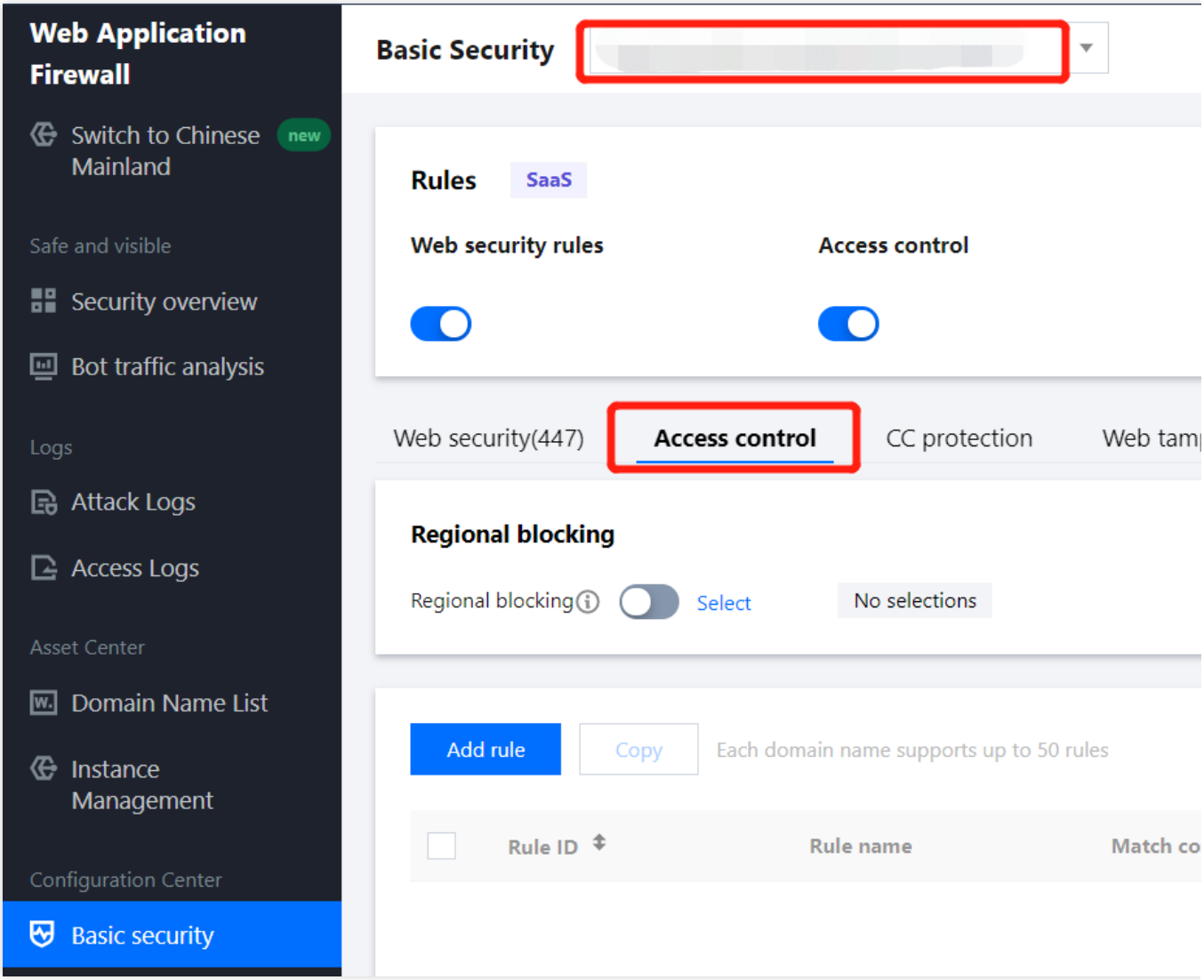
当网站管理员需要阻断外部站点（如 `www.test.com` ）的盗链行为时，可以利用访问控制策略对盗链请求的 Referer 特征进行捕获和阻断，配置如下：匹配字段选择 “Referer”，逻辑符号选择“包含”，匹配内容输入 `www.test.com` ，执行动作选择“阻断”，配置完成后单击**确定**即可。



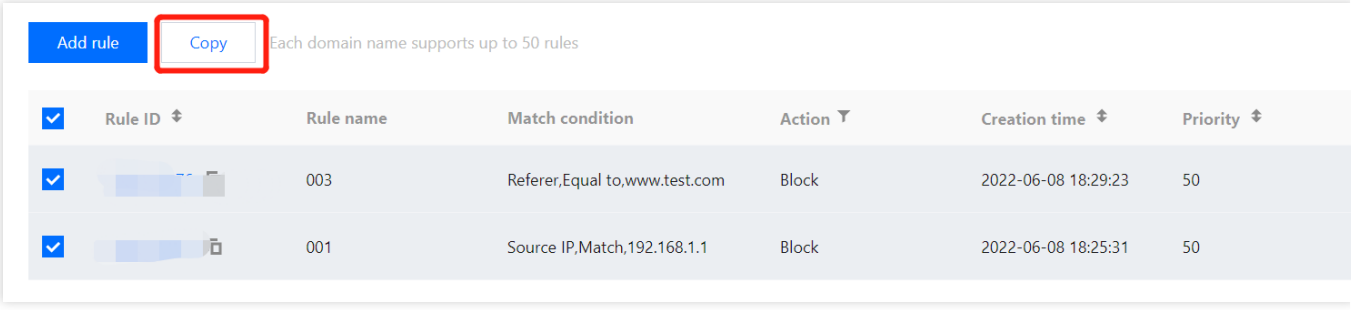
示例四：将策略复制到目标域名

当配置好某个策略时，若希望将此策略同时应用到其他域名，则可以通过复制策略来实现。

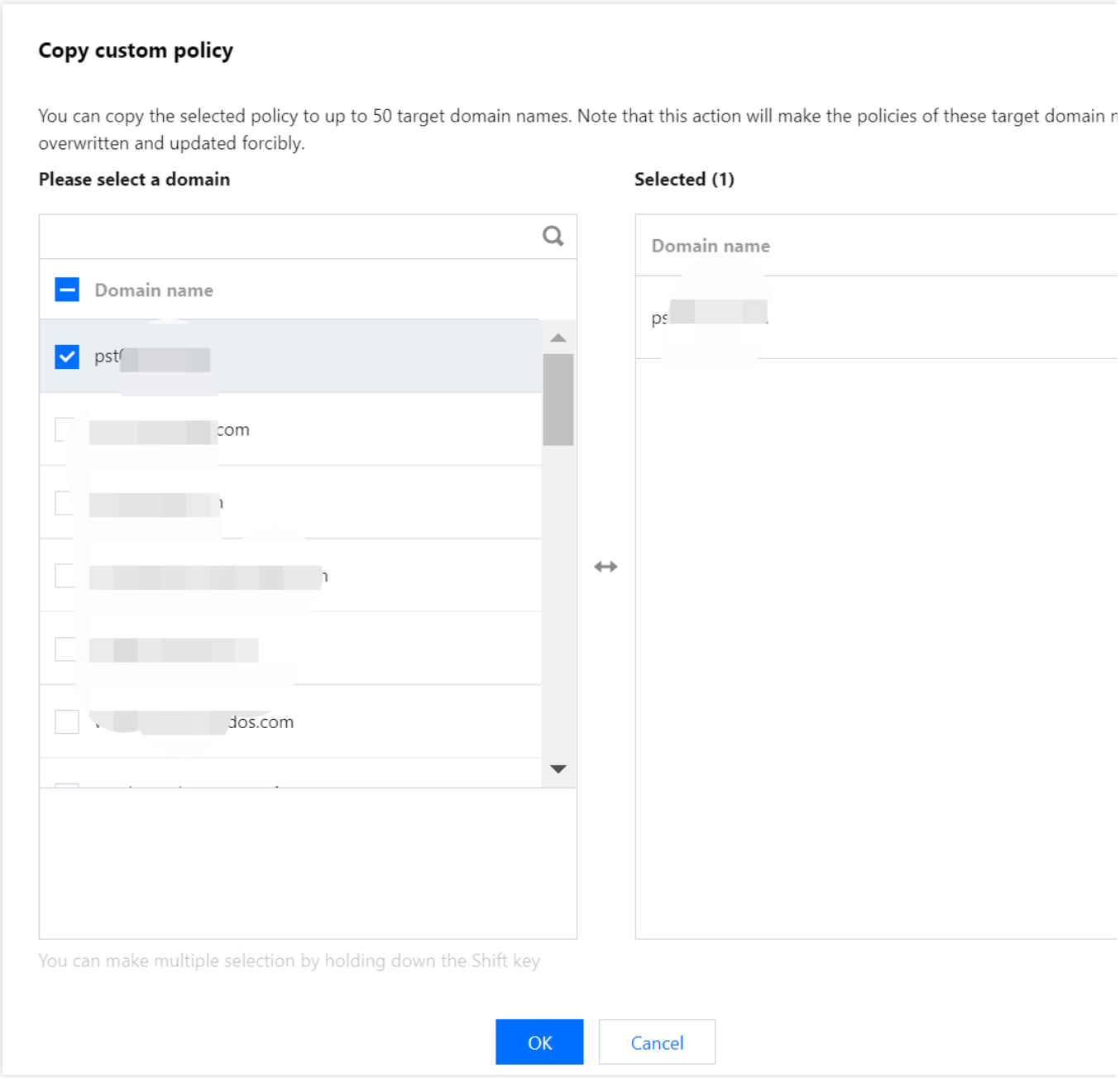
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心** > **基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击**访问控制**，进入访问控制页面。



3. 在访问控制页面，选中所需策略并单击**复制**，弹出复制自定义策略弹窗。



4. 在复制自定义策略弹窗，选择需要的域名，单击**确定**，即可将策略复制到目标域名。


Copy custom policy
You can copy the selected policy to up to 50 target domain names. Note that this action will make the policies of these target domain n
overwritten and updated forcibly.
Please select a domain
Selected (1)
Domain name
Domain name
com
dos.com
You can make multiple selection by holding down the Shift key
OK
Cancel

地域封禁

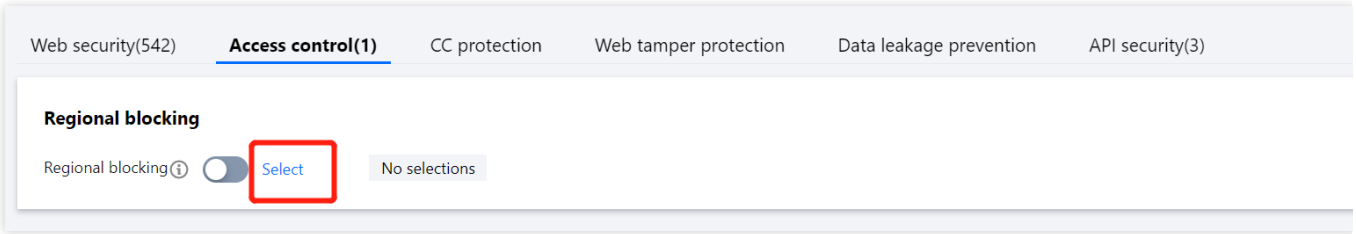
最近更新时间：2023-12-29 14:36:50

功能简介

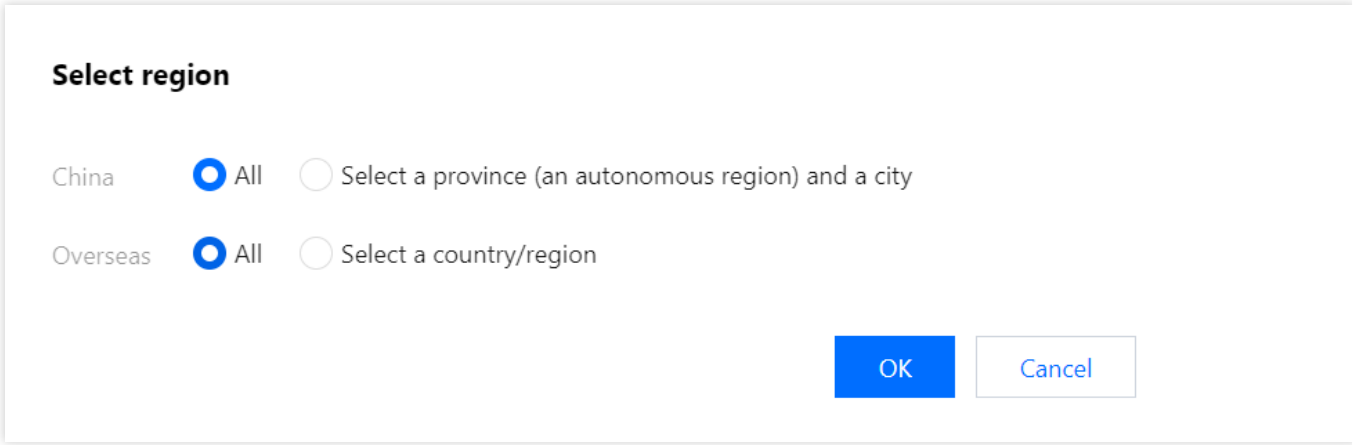
地域封禁功能可以对境外国家和地区以及中国各大省份和地区进行黑名单封禁，阻断该区域的所有访问来源。

操作步骤

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择**配置中心 > 基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击**访问控制**，进入访问控制页面。
3. 在访问控制页面，单击地域封禁处的**编辑**，弹出选择封禁地区弹窗。

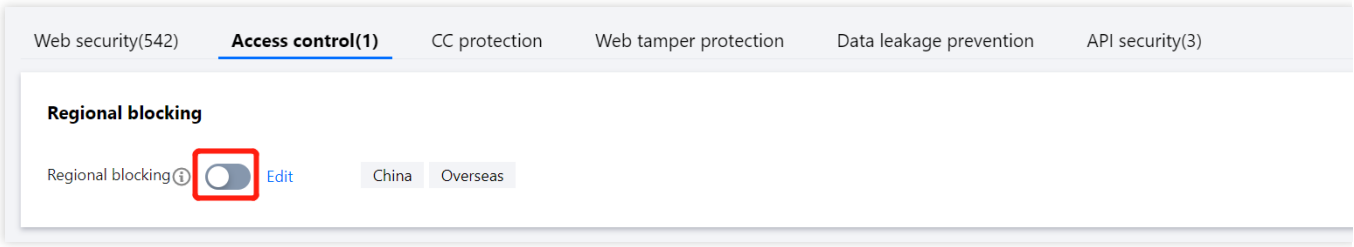


4. 在编辑封禁地区弹窗中，选择封禁的地域，单击**确定**。

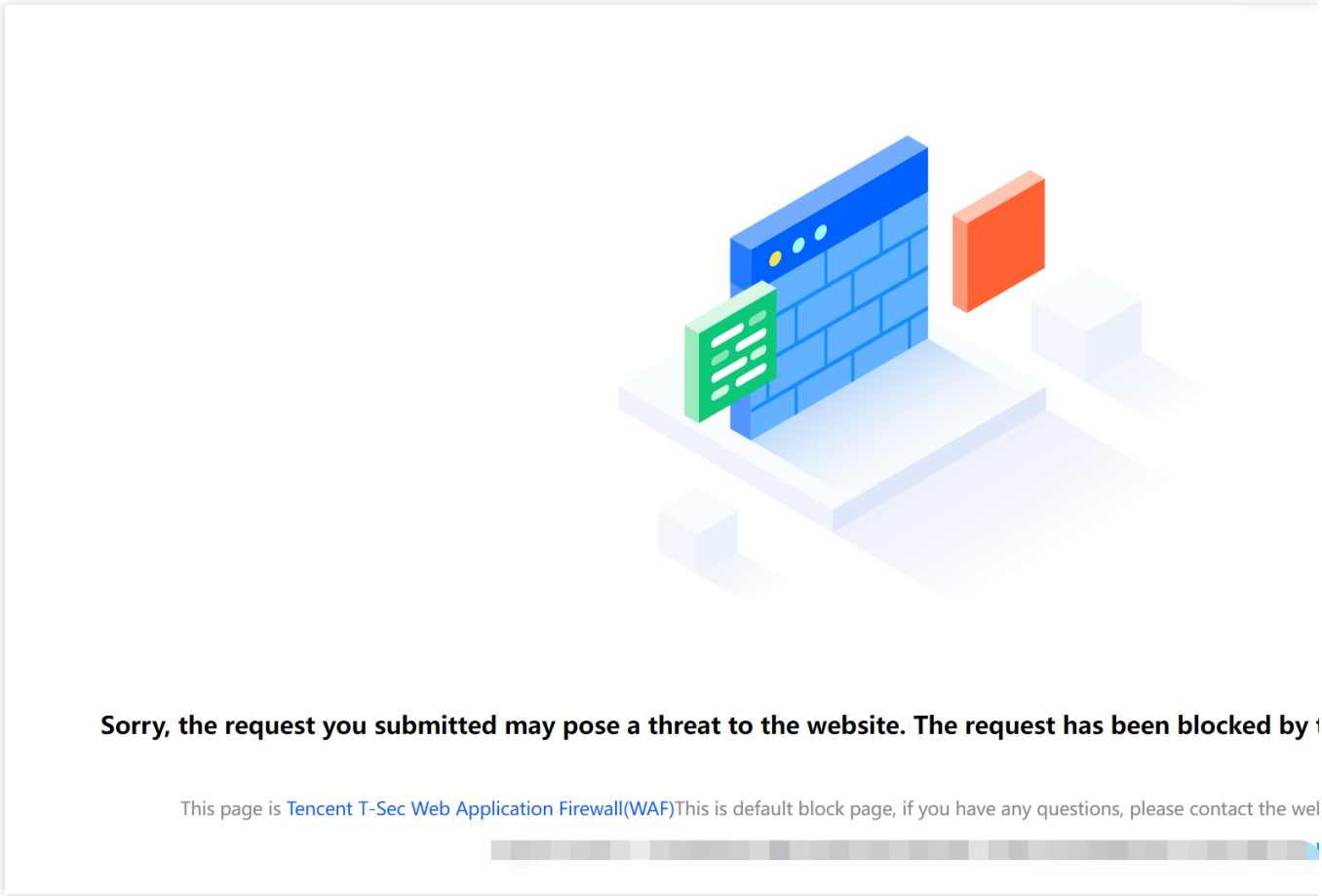


5. 保存完成后，单击地域封禁处的

，开启地域封禁状态。



6. 此时您选择封禁的地区，将无法访问您的网站。本文将国外全部地区列入封禁地域后，以境外 IP 地址访问防护网站，Web 应用防火墙会提示您已被腾讯云 Web 应用防火墙拦截。



支持地区

地域封禁功能所支持的封禁地区如下所示：

中国地区

区域	省市自治区
华东地区	山东、江苏、安徽、浙江、福建、江西、上海。

华南地区	广东、广西、海南。
华中地区	湖北、湖南、河南。
华北地区	北京、天津、河北、山西、内蒙古。
西北地区	宁夏、新疆、青海、陕西、甘肃。
西南地区	四川、云南、贵州、西藏、重庆。
东北地区	辽宁、吉林、黑龙江。
港澳台地区	台湾、香港、澳门。

其他国家和地区

大洲	国家/地区
亚洲	阿塞拜疆、亚美尼亚、阿富汗、孟加拉、巴林、文莱、不丹、塞浦路斯、柬埔寨、东帝汶、格鲁吉亚、根西岛、印度、印度尼西亚、伊朗、以色列、伊拉克、日本、约旦、哈萨克斯坦、科威特、吉尔吉斯斯坦、黎巴嫩、老挝、摩洛哥、蒙古、缅甸、马尔代夫、阿曼、尼泊尔、巴勒斯坦、巴基斯坦、菲律宾、韩国、卡塔尔、斯里兰卡、叙利亚、沙特阿拉伯、新加坡、泰国、土耳其、塔吉克斯坦、土库曼斯坦、阿联酋、乌兹别克斯坦、越南、也门、朝鲜。
欧洲	奥地利、阿尔巴尼亚、安道尔、比利时、保加利亚、白俄罗斯、波斯尼亚和黑塞哥维那、捷克、克罗地亚、丹麦、爱沙尼亚、法国、芬兰、法罗群岛、德国、希腊、直布罗陀、匈牙利、意大利、爱尔兰、冰岛、马恩岛、泽西岛、立陶宛、拉脱维亚、卢森堡、列支敦士登、摩尔多瓦、马其顿、马其他、黑山、摩纳哥、荷兰、挪威、葡萄牙、波兰、瑞士、瑞典、西班牙、罗马尼亚、俄罗斯、塞尔维亚、斯洛文尼亚、斯洛伐克、圣马力诺、英国、乌克兰、梵提冈。
非洲	阿尔及利亚、安哥拉、布基纳法索、贝宁、博茨瓦纳、布隆迪、科特迪瓦、喀麦隆、刚果(金)、刚果(布)、佛得角、乍得、中非、科摩罗、吉布提、埃及、厄瓜多尔、埃塞俄比亚、赤道几内亚、加纳、加蓬、冈比亚、几内亚、几内亚比绍、肯尼亚、利比亚、莱索托、利比里亚、摩洛哥、毛里求斯、马拉维、莫桑比克、马达加斯加、马里、毛里塔尼亚、尼日尔、纳米比亚、尼日利亚、南非、卢旺达、留尼汪、苏丹、塞舌尔、索马里、斯威士兰、塞拉利昂、塞内加尔、圣多美和普林西比、南苏丹、突尼斯、坦桑尼亚、多哥、乌干达、赞比亚、津巴布韦。
大洋洲	澳大利亚、美属萨摩亚、库克群岛、斐济群岛、法属波利尼西亚、关岛、密克罗尼西亚联邦、新西兰、瑙鲁、马里亚纳群岛、新喀里多尼亚、巴布亚新几内亚、帕劳、圣卢西亚、萨摩亚、所罗门群岛、汤加、图瓦卢、瓦努阿图。
北美洲	安提瓜和巴布达、安圭拉、巴巴多斯、伯利兹、巴哈马、百慕大、加拿大、哥斯达黎加、古巴、开曼群岛、荷兰加勒比区、多米尼加、萨尔瓦多、危地马拉、格陵兰、瓜德罗普、格林纳达、洪都拉斯、海地、牙买加、墨西哥、马提尼克、尼加拉瓜、波多黎各、巴拿马、荷属圣马丁、圣文森特和格林纳丁斯、法属圣马丁、圣基茨和尼维斯、特立尼达和多巴哥、塔吉克斯坦、英文属维尔京群岛、多米尼克、特克斯和凯科斯群岛、美国、美属维尔京群岛。

南美洲	阿根廷、阿鲁巴、巴西、玻利维亚、哥伦比亚、智利、库拉索、法属圭亚那、圭亚那、巴拉圭、秘鲁、苏里南、乌拉圭、委内瑞拉。

设置 CC 防护规则

最近更新时间：2023-12-29 14:41:13

功能简介

CC 防护对网站特定的 URL 进行访问保护，CC 防护2.0全新改版，支持紧急模式 CC 防护和自定义 CC 防护策略。紧急模式 CC 防护，综合源站异常响应情况（超时、响应延迟）和网站历史访问大数据分析，紧急模式决策生成防御策略，实时拦截高频访问请求。自定义 CC 防护可以根据用户访问源 IP 或者 SESSION 频率制定防护规则，对访问进行处置，处置措施包括告警、人机识别和阻断。

Caution

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。
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。
慢速攻击防护：Web 应用防火墙在进行流量转发时会聚合清洗慢速请求，具备一定慢速攻击防护能力。

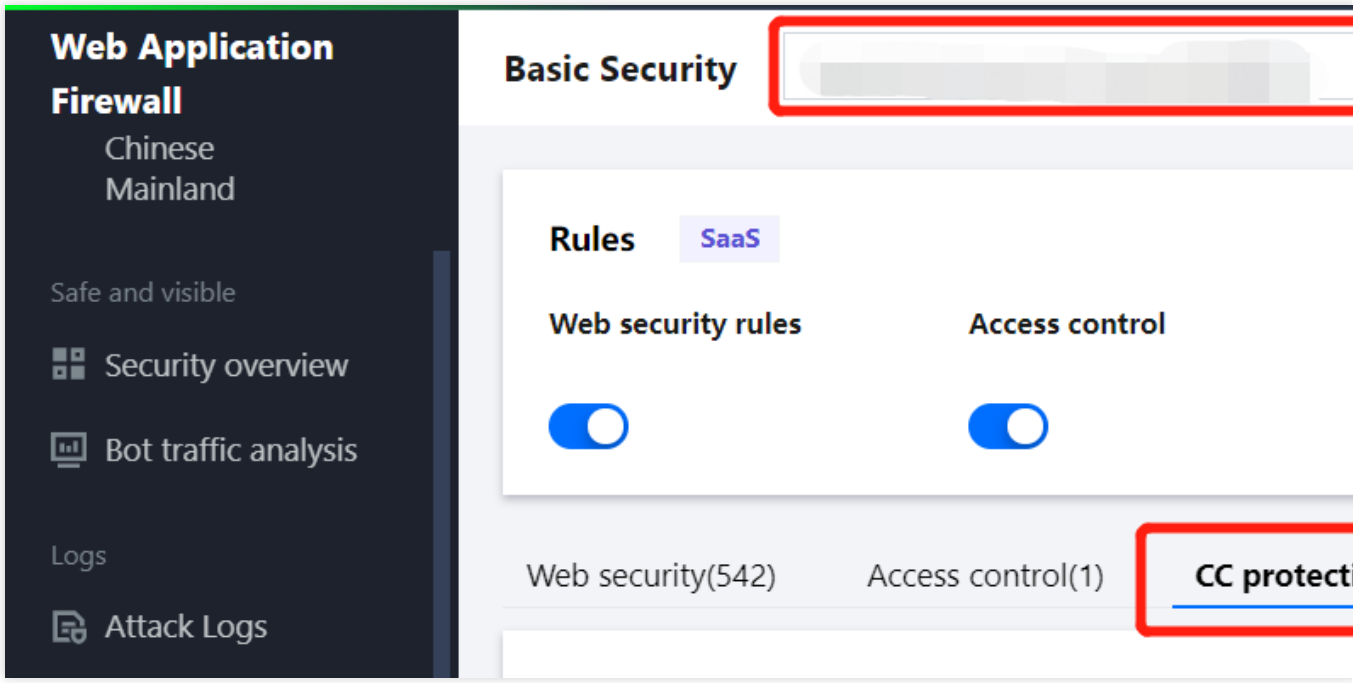
慢速攻击防护

Slowloris、RUDY 等慢速攻击是一种拖慢服务器响应速度的攻击手法，通常通过发送大量慢速请求或者不完整的请求来消耗服务器资源，从而导致正常用户无法访问 Web 应用。
1. Web 应用防火墙在进行流量转发时，默认会聚合清洗慢速请求，具备慢速攻击防护能力，可以清洗类似 Slowloris 类型的慢速攻击。
2. Web 应用防火墙清洗慢速请求时，HTTP 协议类型请求会返回状态码400，TCP 协议类型请求会返回 TCP RST。

操作步骤

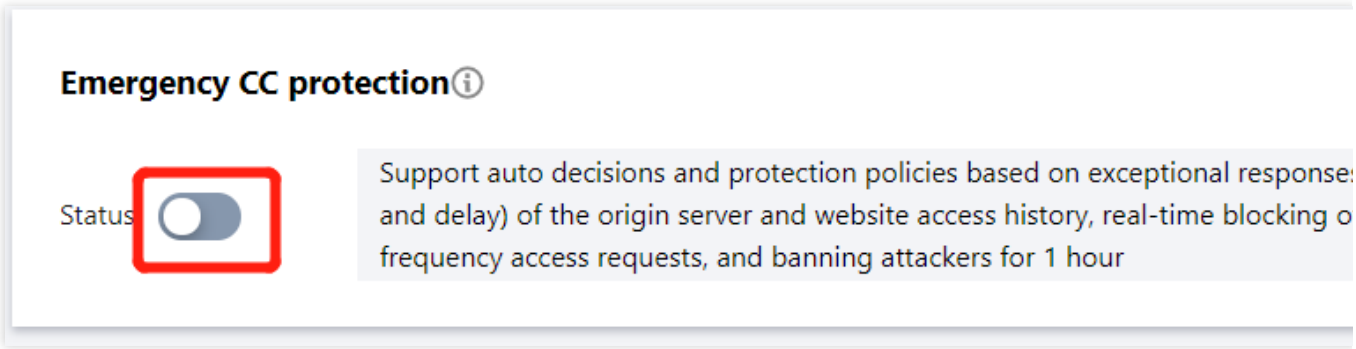
示例一：紧急模式 CC 防护配置

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**配置中心 > 基础安全**，进入基础安全页面。
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. 单击紧急模式 CC 防护模块的

，经过二次确认后，即可进行紧急模式 CC 防护配置。



配置项说明：

状态开关： 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 IP 查询，查看拦截 IP 信息，并及时处理。

说明：

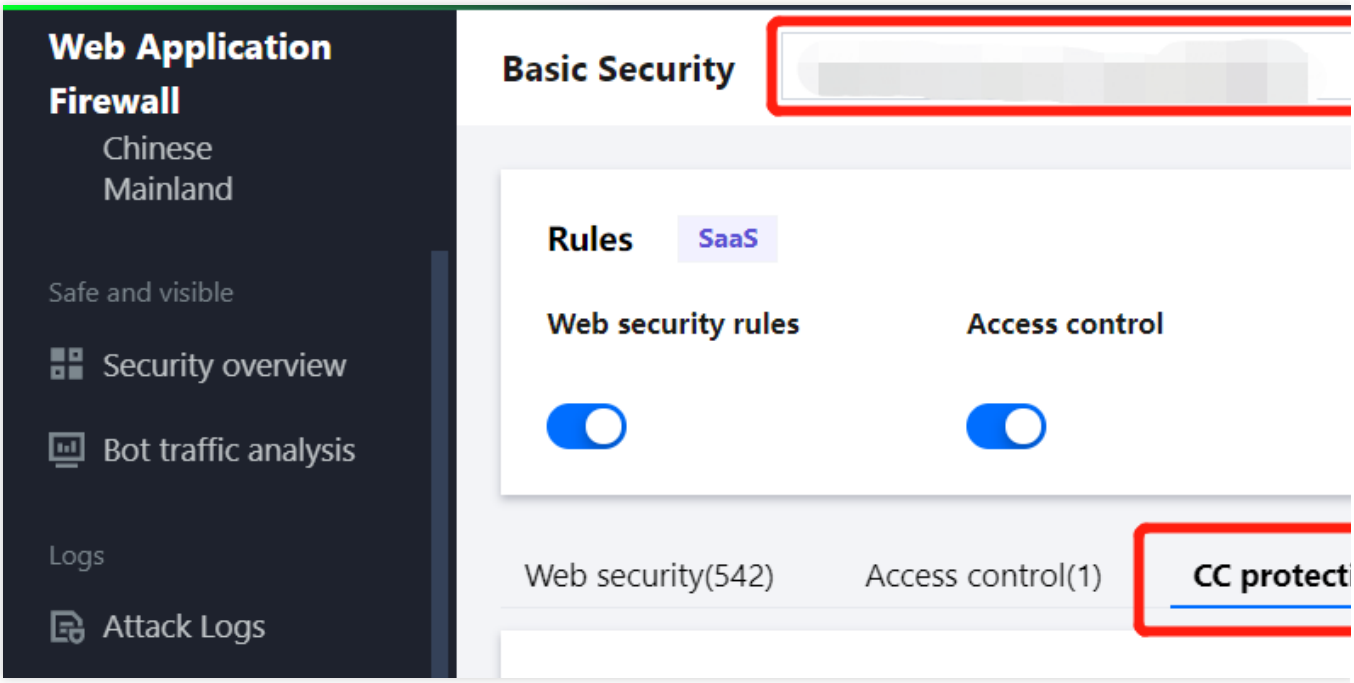
如果知晓明确的防护路径，建议使用自定义 CC 规则进行防护。

CLBWAF 暂不支持紧急模式，请直接使用自定义 CC 进行防护。

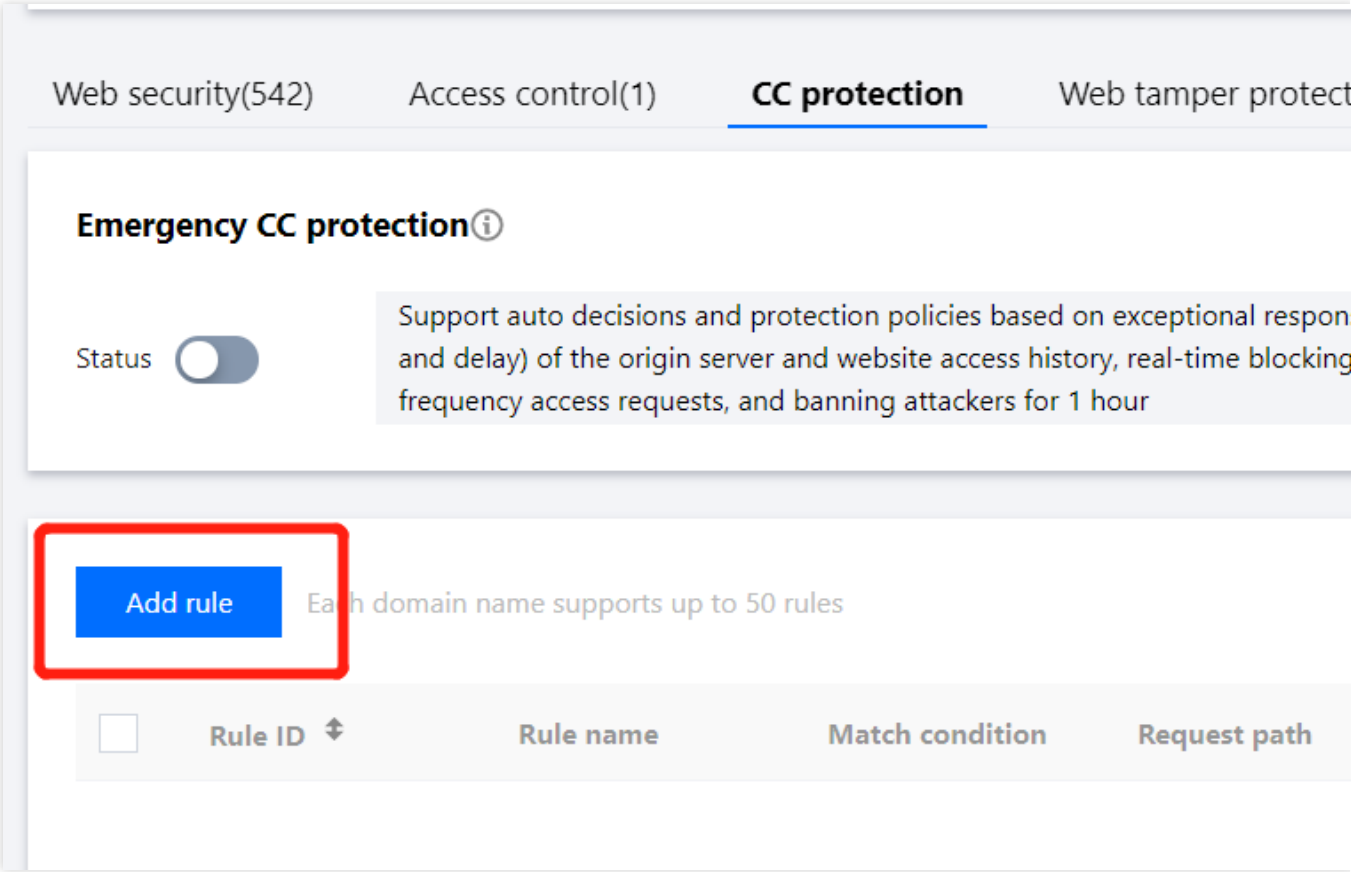
示例二： 基于访问源 IP 的 CC 防护设置

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。

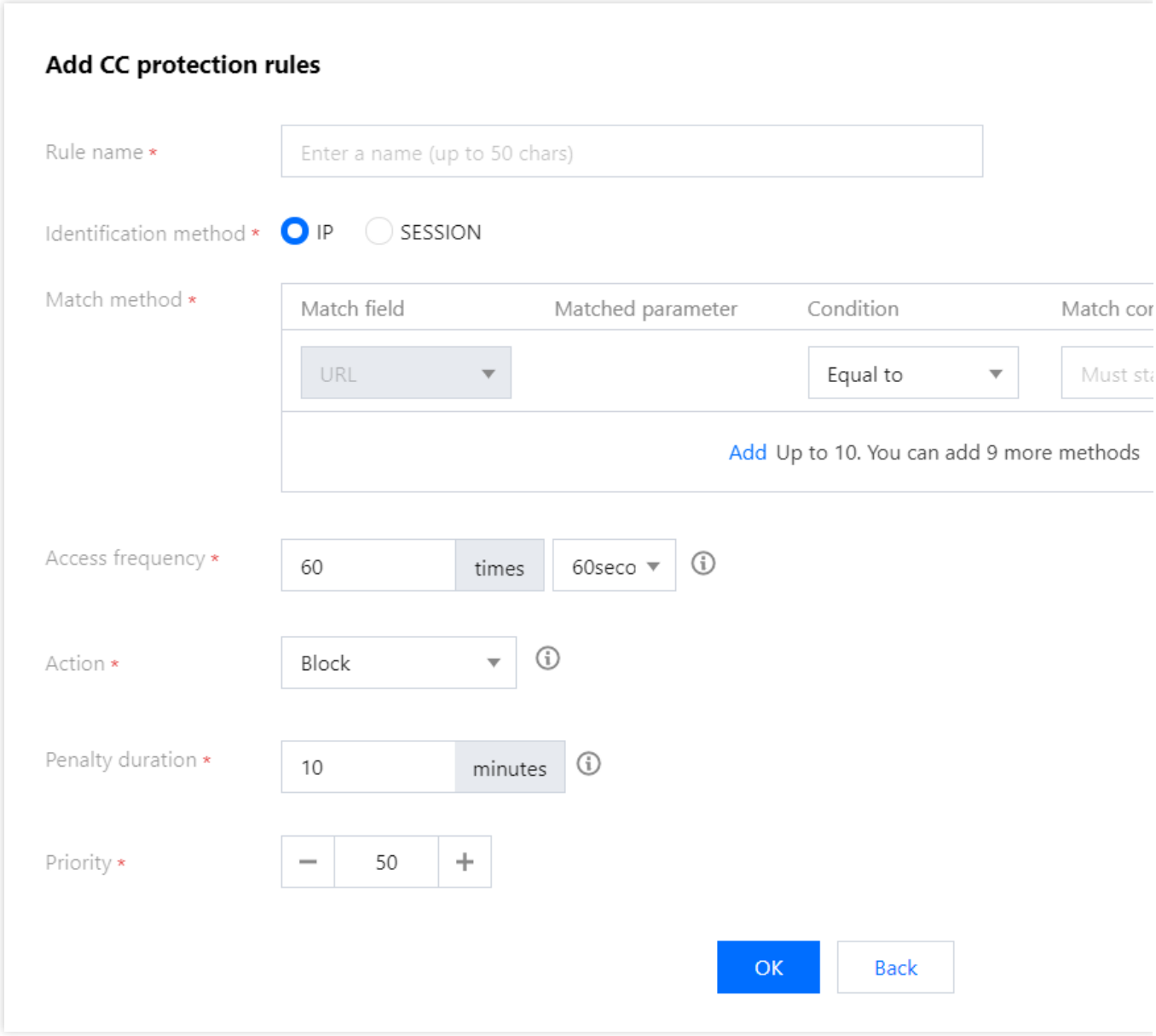
1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择**配置中心 > 基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **CC 防护**，进入 CC 防护页面。



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，填写相应参数，单击**确定**。



字段说明：

规则名称：CC 防护规则名称，50个字符以内。

识别方式：支持 IP 和 SESSION 识别模式，默认为 IP，SESSION 模式需要提前设置 SESSION 位置信息。

匹配方式：CC 防护规则频率控制匹配条件，默认为 URL。支持设置多个匹配条件，同一规则的多个条件是“与”关系，同时满足才会执行动作，且最多配置10个，需要至少配置URL，详细字段说明如下：

匹配字段	匹配参数	逻辑符号	匹配内容说明
URL	无	等于 包含 前缀匹配	必填字段，以/开头，支持目录和具体路径，128字符以内 。
Method	无	等于	支持 HEAD、GET、

		包含 不等于	POST、PUT、OPTIONS、TRACE、DELETE、PATCH、CONNECT，每次支持输入一个值 。
Query	Query 参数中 key 值	等于	Query 需要填写 key-value 组合，填写具体 value 值，512字符以内，可配置多次。
Referer	无	等于 包含 前缀匹配	填写 value 值，512字符以内。
Cookie	Cookie 参数中 key 值	等于 包含 不等于	Cookie 需要填写 key-value 组合，填写具体 value 值，512字符以内。
User-Agent	无	等于 包含 不等于	填写 value 值，512字符以内。
自定义请求头	填写请求头 key 值，如：Accept、Accept-Language，Accept-Encoding，Connectiton 等	等于 包含 不等 内容为空 不存在	填写具体 value 值，512字符以内，可配置多次；内容为空或者不存在时，无匹配内容输入框，填写匹配参数即可。

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：默认为拦截，可根据需要进行设置，各个动作详细说明如下：

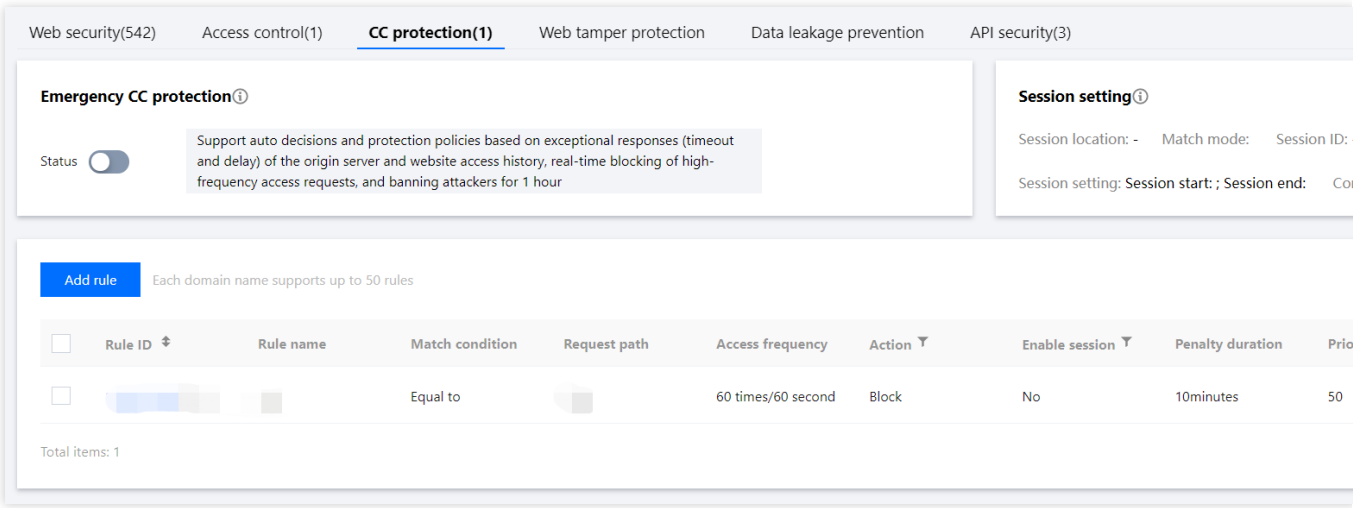
动作类型	说明
观察	符合匹配条件的会话请求将会被监控记录日志，观察结果可在 攻击日志 中查看。
人机识别	仅用于浏览器访问场景，符合匹配条件的会话请求将进行验证码挑战，若挑战失败，执行拦截动作。若挑战成功，惩罚时长内正常访问。验证码记录日志为观察。
精准拦截	符合频率控制条件的请求将执行精准拦截，将会拦截该IP对防护 URL 的访问，区别于对整个域名的拦截，可设置惩罚时长，取值为：5分钟 - 10080分钟（7天），拦截结果可在 攻击日志 中查看。

拦截	符合频率控制条件的请求将执行拦截，将会拦截该IP对网站所有 URL 的访问，可设置惩罚时长，取值为：5分钟 - 10080分钟（7天），拦截结果可在 攻击日志 中查看，拦截 IP 的实时信息可在 IP 查询 中查看。

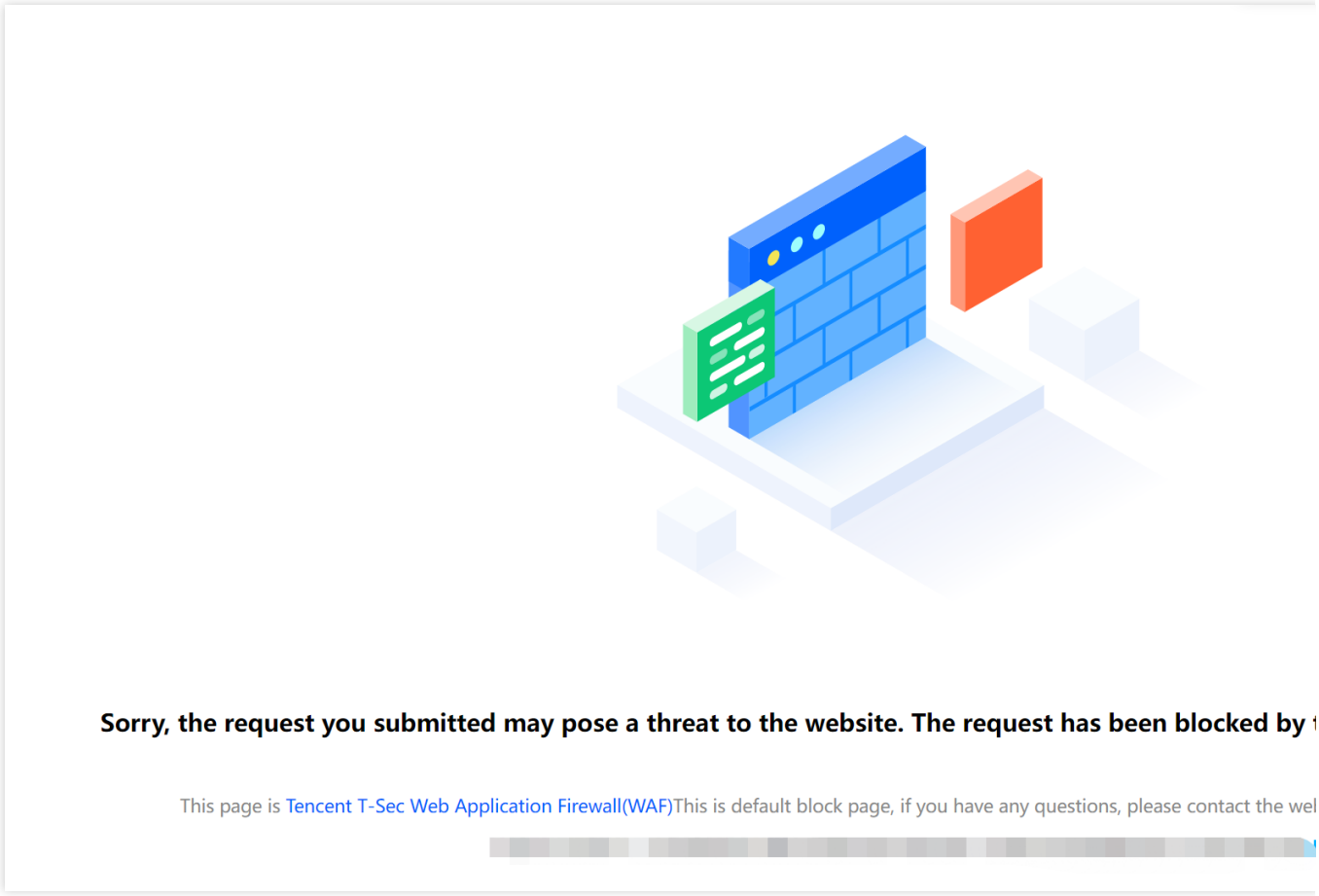
惩罚时长：默认为10分钟，最短为1分钟，最长为一周。

优先级：默认为50，可输入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。

5. 规则操作，选择已经创建的规则，可以对规则进行关闭、修改和删除。



6. 根据规则设置，触发 CC 攻击行为。

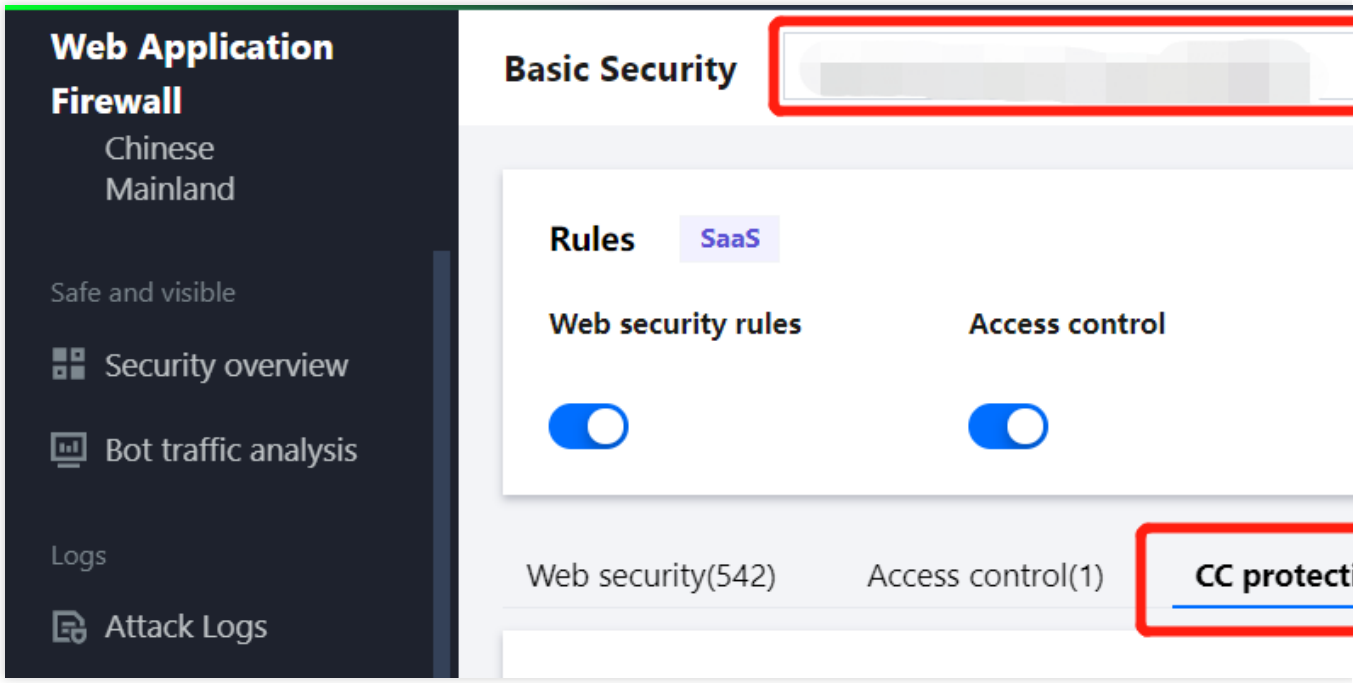


7. 可在 黑白名单页面，对 IP 进行加白或者加黑处理，在 IP 查询页面 可以查看阻断信息。

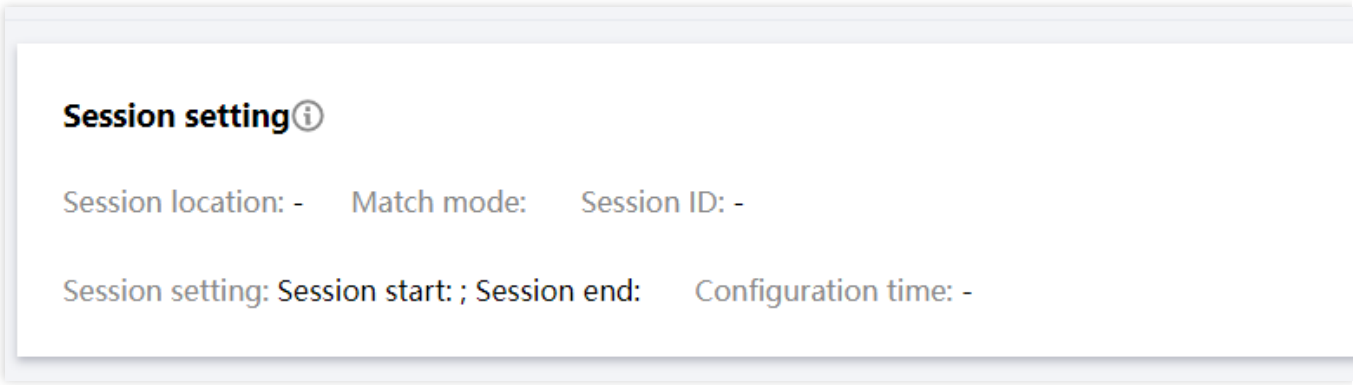
示例三： 基于 SESSION 的 CC 防护设置

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 WIFI 场合，用户因使用相同 IP 出口而导致的误拦截问题。

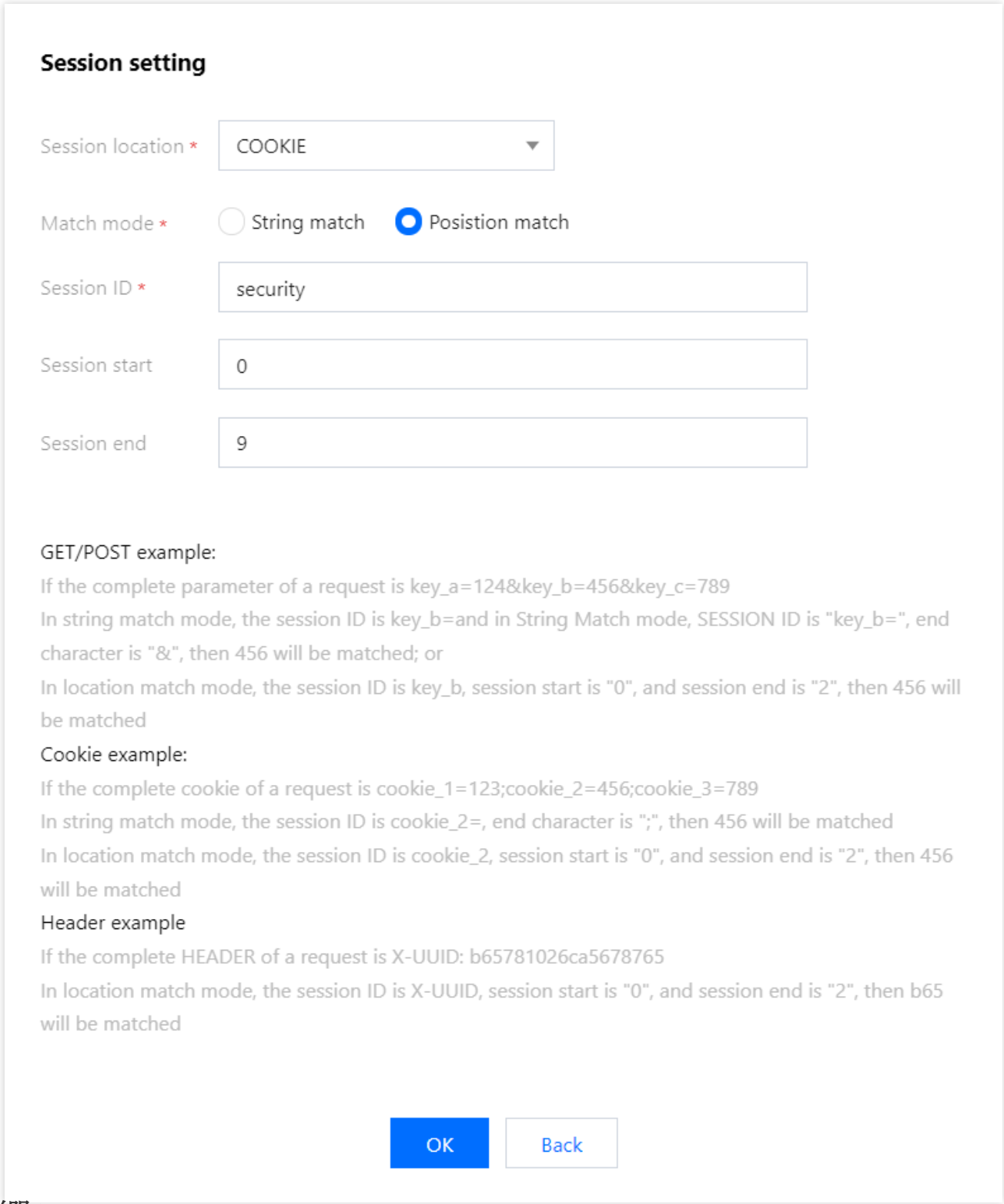
1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择**配置中心 > 基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **CC 防护**，进入 CC 防护页面。



3. 单击 SESSION 设置处的**设置**，弹出 SESSION 设置弹窗。



4. 在 SESSION 设置弹窗中，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**。



字段说明：

SESSION 位置 ：可选择 COOKIE、GET 、HEADER 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。

开始位置：字符串或者位置匹配的开始位置。

结束位置：字符串或位置匹配的结束位置。

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。

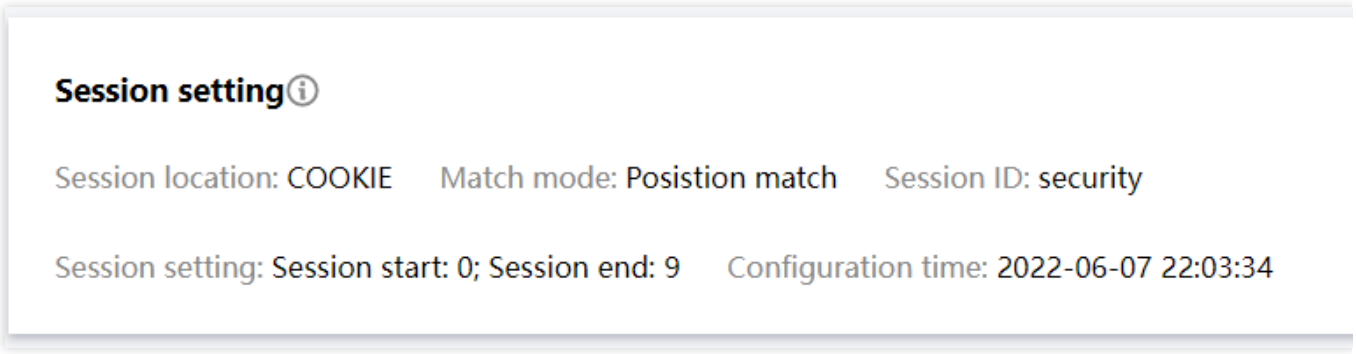
位置匹配模式下，SESSION 标识为 cookie_2，开始位置为0，结束位置2，则匹配内容为456。

HEADER 示例 ：

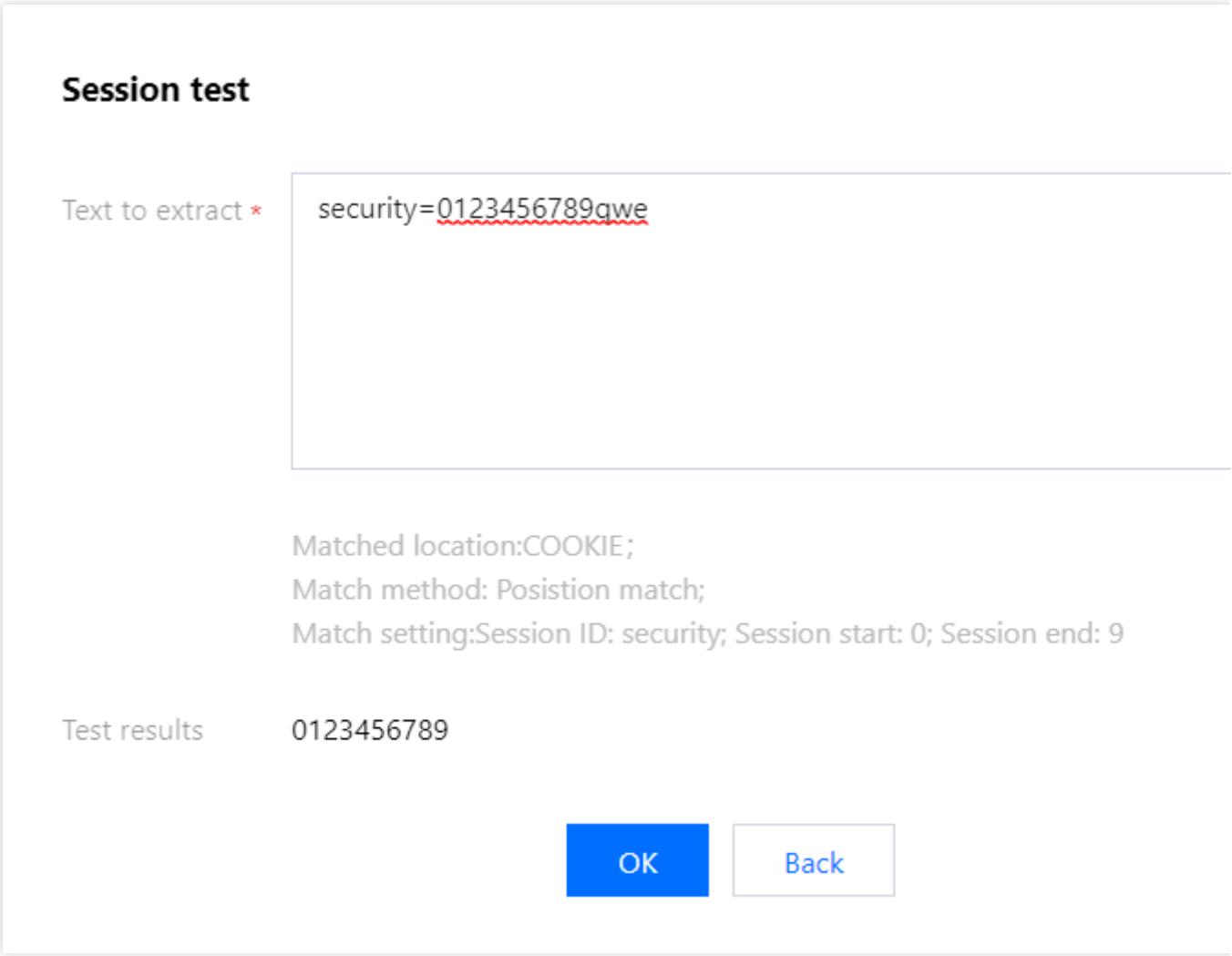
如果一条请求的完整 HEADER 内容为：X-UUID: b65781026ca5678765。

位置匹配模式下，SESSION 标识为X-UUID，开始位置为0，结束位置2；则，匹配内容为 b65。

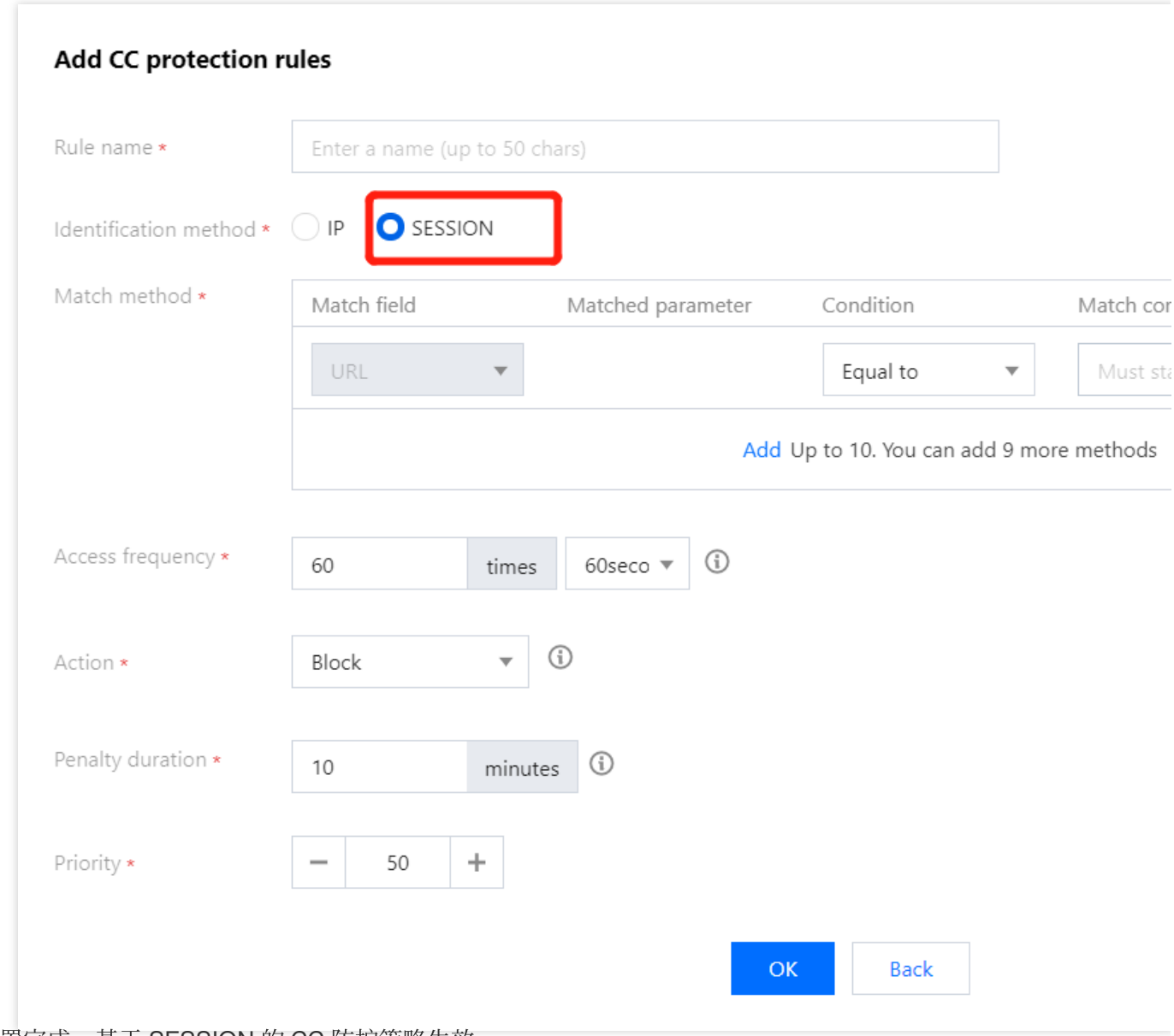
5. SESSION 维度信息测试。添加完成后，单击**测试**将填写内容后，单击**确定**进行测试。



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，配置过程和示例一保持一致，识别模式选择 SESSION 即可。



8. 配置完成，基于 SESSION 的 CC 防护策略生效。

Caution

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。

网页防篡改

最近更新时间：2023-12-29 14:41:35

本文档将为您介绍 Web 应用防火墙（WAF）的防篡改功能。防篡改功能用于保护网站核心静态页面，通过缓存页面和锁定访问请求，保护网站因为源站页面被恶意篡改带来的负面影响，同时您可以根据需要配置防篡改规则。

背景信息

通过防篡改功能，您可以添加防护规则，根据实际需要对网站核心页面进行防篡改保护。您可以对防篡改页面进行刷新，刷新时 WAF 将更新防篡改页面，确保防篡改页面和源站保持一致，同时您可以选择是否记录防篡改规则命中日志，对您的命中情况进行分析。

说明：

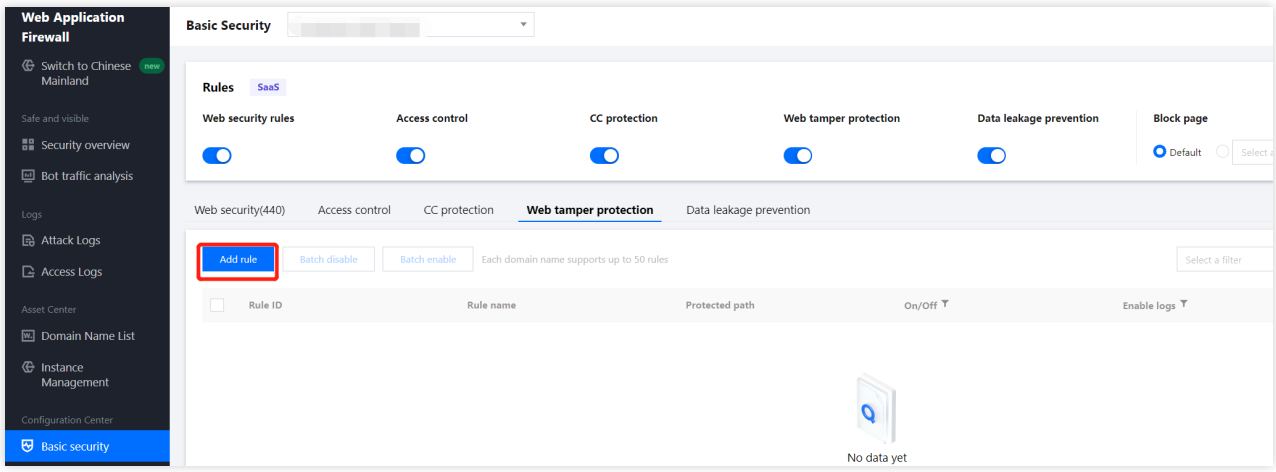
CLB WAF 不支持防信息防篡改功能，详细规格信息请参见 计费概述。

前提条件

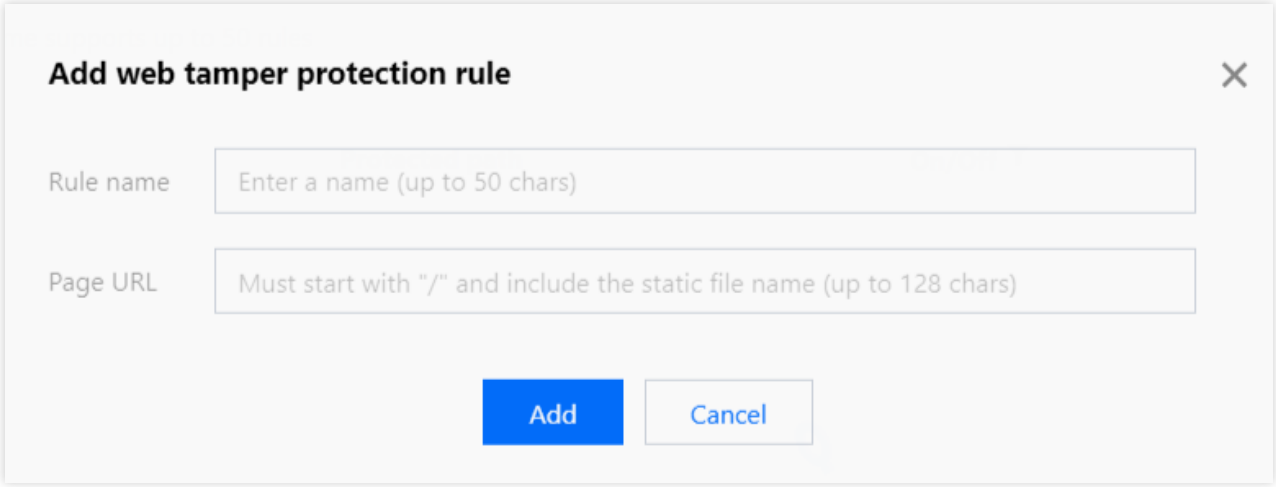
您已经在 WAF（SaaS 版本）中 添加防护域名，且域名处于正常防护状态。

添加规则

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择**配置中心 > 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**网页防篡改**，进入网页防篡改页面。
3. 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。



4. 在添加防篡改规则弹窗中，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：

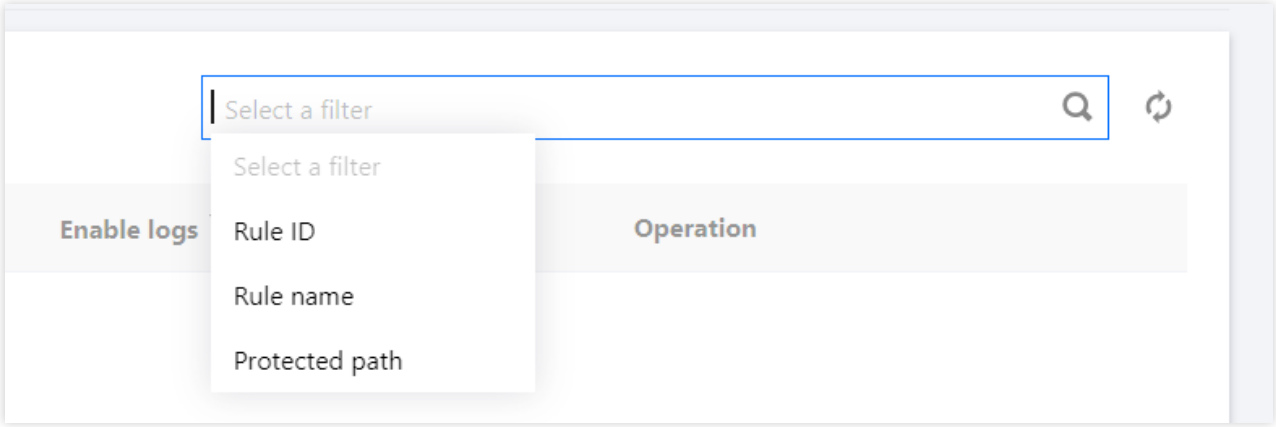
指定页面仅限于.html、.shtml、.txt、.js、.css、.jpg、.png 等静态资源。

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。

5. 完成的防篡改规则后，规则默认启用。

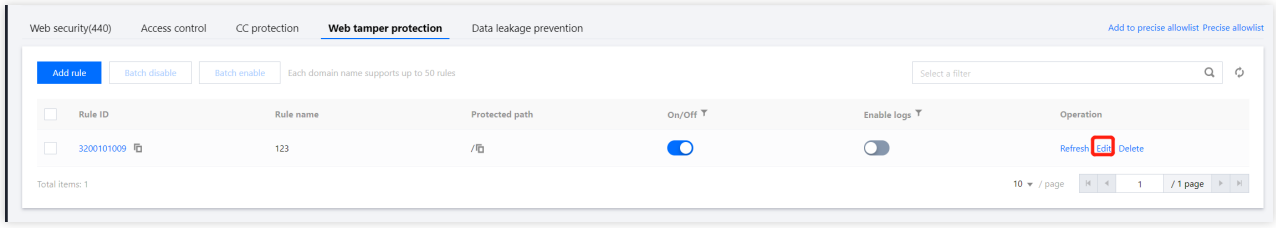
检索规则

1. 在 基础安全页面，左上角选择需要防护的域名，单击**网页防篡改**，进入网页防篡改页面。
2. 在网页防篡改页面，单击搜索框通过“规则 ID、规则名称、防御路径”关键词对规则进行查询。

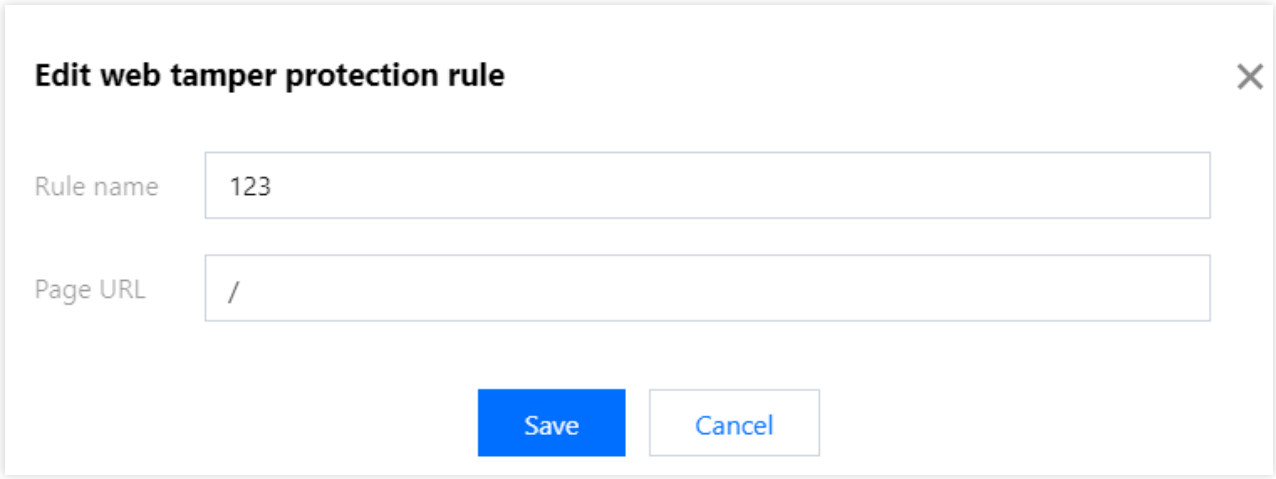


编辑规则

1. 在 基础安全页面，左上角选择需要防护的域名，单击**网页防篡改**，进入网页防篡改页面。
2. 在网页防篡改页面，选择所需规则，单击操作列的**编辑**，弹出网页防篡改弹窗。



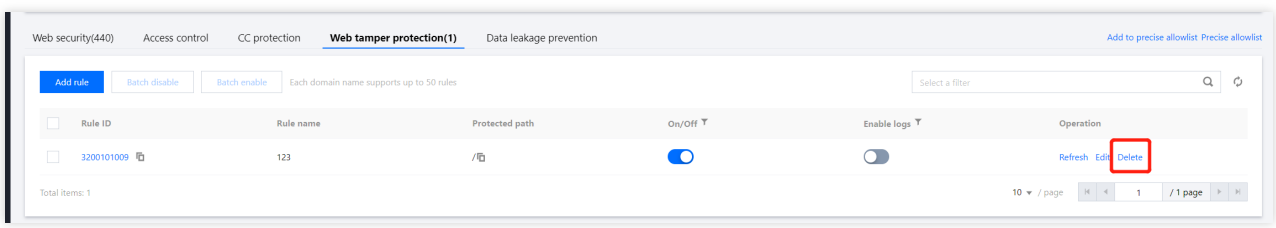
3. 在编辑防篡改规则弹窗中，修改相关参数，单击**保存**即可。



4. 防护页面更新后，单击**刷新缓存**，将更新后的界面缓存至 WAF 进行更新。

删除规则

1. 在 基础安全页面，左上角选择需要防护的域名，单击**网页防篡改**，进入网页防篡改页面。
2. 在网页防篡改页面，选择所需规则，单击操作列的**删除**，弹出确认删除弹窗。



3. 在确认删除弹窗中，单击**删除**，即可删除该规则。

说明：

删除后将无法恢复，重新添加才能生效。

信息防泄漏

最近更新时间：2023-12-29 14:41:50

本文档将为您介绍 Web 应用防火墙的防信息泄露功能。防信息泄露功能支持对网站返回的内容进行过滤（支持替换、脱敏展示和拦截），过滤内容包括敏感信息（如身份证、手机号和银行卡）、关键字和响应码。您可以根据实际需要设置防敏感信息泄露的规则，满足数据安全保护和等保合规需求。

背景信息

通过防信息泄露功能，您可以添加防护规则，根据实际需要对网站返回的内容进行过滤。过滤内容包括但不限于身份证、手机号和银行卡等，您也可以自定义关键字（支持正则）对订单号、地址信息等进行过滤、部分替换或者全部替换。针对网站返回的状态码，您可以对非200的状态码进行阻断或者告警，满足合规要求。

说明：

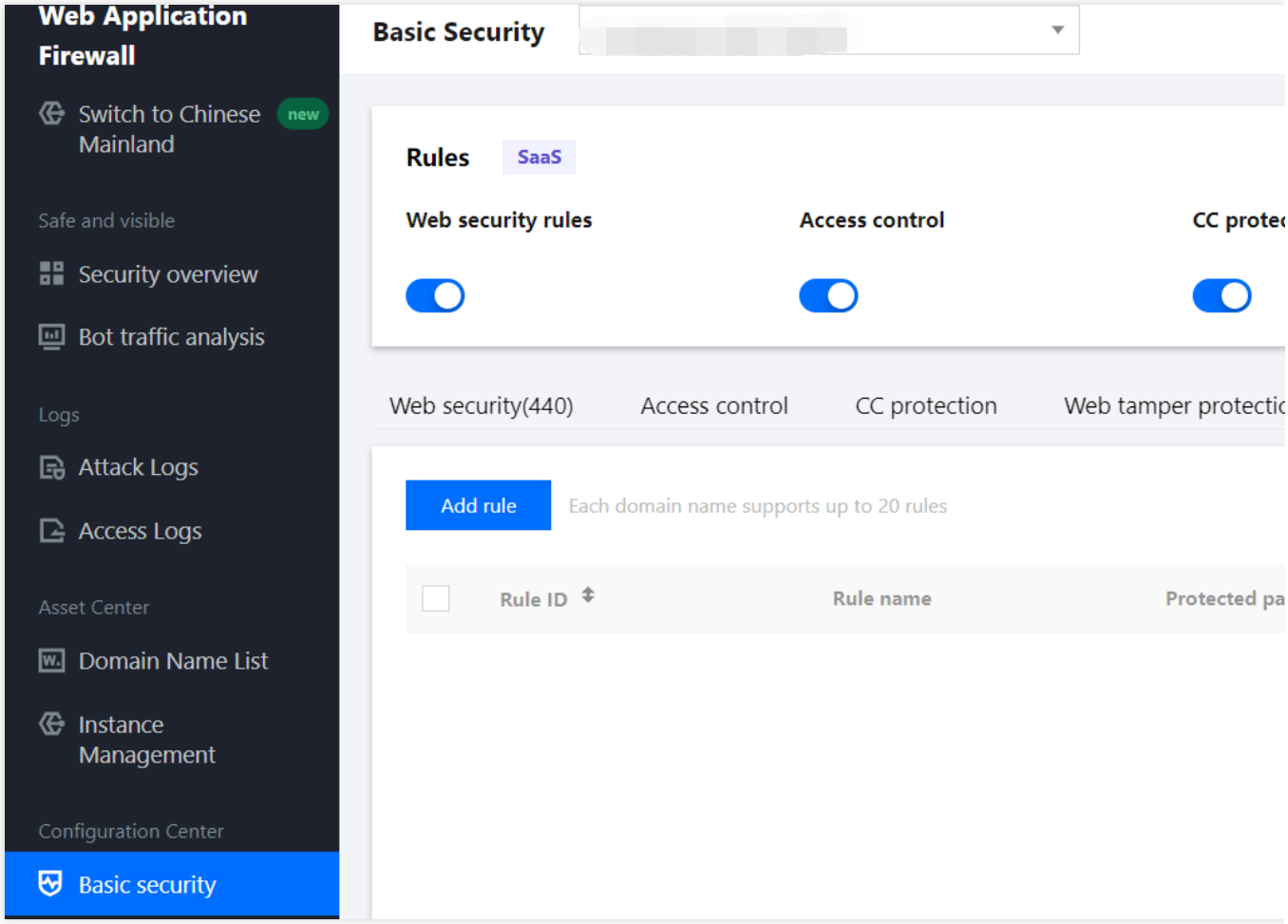
负载均衡型 WAF 不支持防信息泄露功能，详细规格信息请参见 计费概述。

前提条件

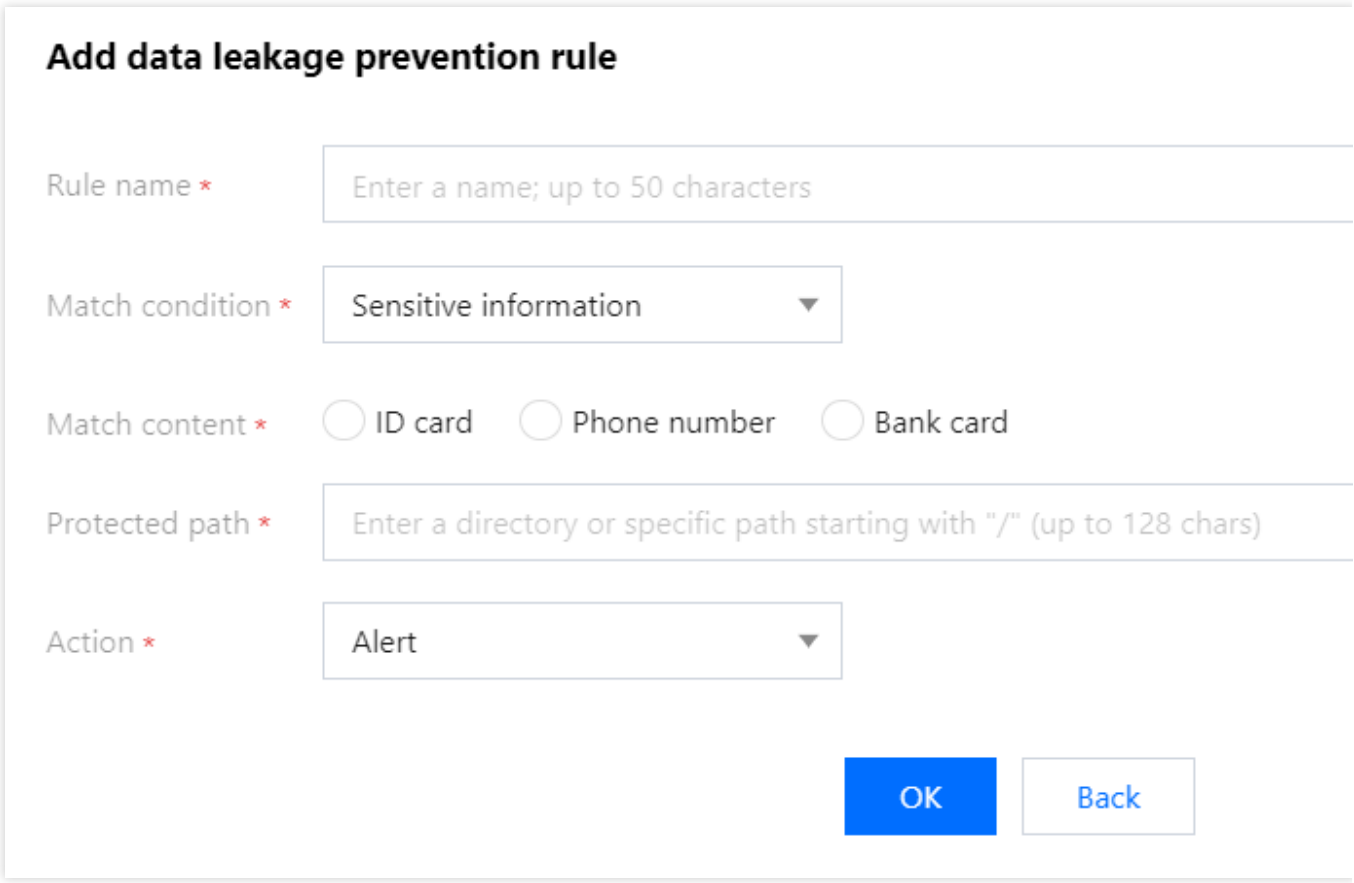
您已经在 Web 应用防火墙（SaaS 版本）添加防护域名，且域名处于正常防护状态。

添加规则

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择**配置中心** > **基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击**信息防泄漏**，进入信息防泄漏页面。
3. 在信息防泄漏页面，单击**添加规则**，弹出添加防信息泄露规则弹窗。



4. 在添加防信息泄露规则弹窗中，填写相关字段，设置完成后，单击**确定**。



字段说明：

规则名称：防信息泄露规则名称，最长50个字符，可以在攻击日志中按照规则名称进行搜索。

匹配条件：防泄漏信息匹配条件，支持敏感信息、关键字和响应码，不同类型对应不同的匹配内容和动作类型，关系如下：

匹配条件	匹配内容	匹配动作
敏感信息	身份证、手机号、银行卡	告警、全部替换、仅显示后四位、仅显示前四位、阻断
关键字	支持关键字，支持正则	告警、全部替换、阻断
响应码	400、403、404、其他4xx、500、501、502、504、其他5xx	告警 、阻断

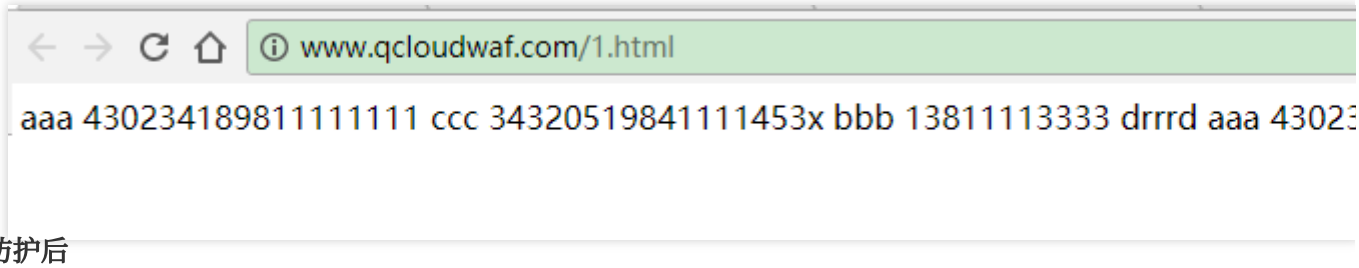
匹配内容：匹配内容因匹配条件不同有差异。

防御路径：需要进行防泄露的路径，支持目录和局路径，根据实际需要填写。

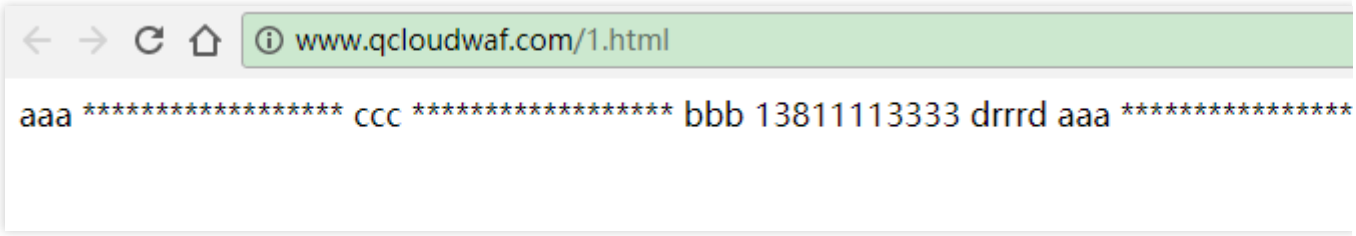
执行动作：命中防泄漏匹配条件的执行动作，相关命中信息可在攻击日志中查询。

5. 规则生效，会对您网页中返回的敏感信息进行防护，例如执行动作为：替换，则防护效果如下（敏感内容为虚构）：

开启防护前

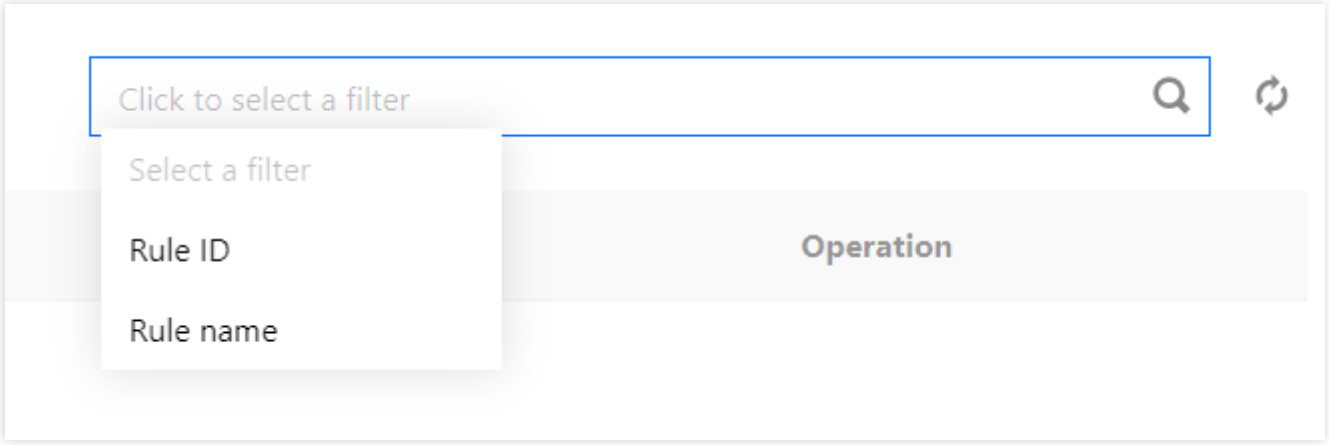


开启防护后



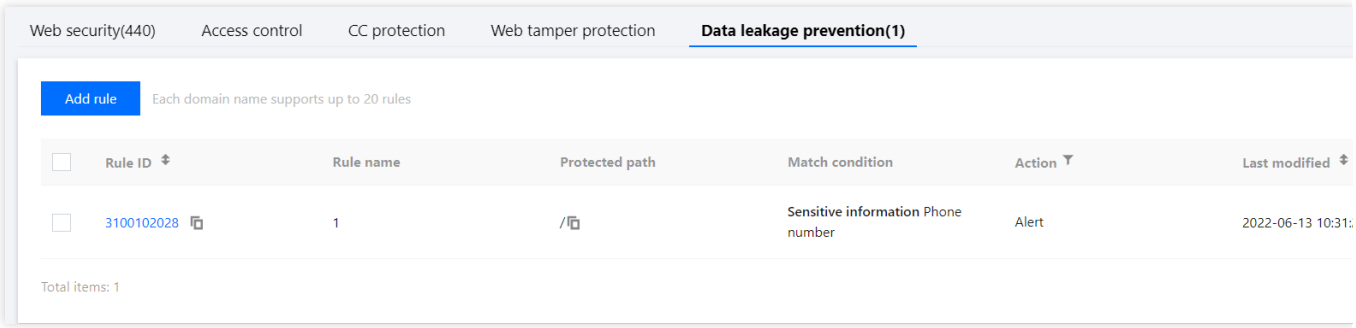
检索规则

1. 在 基础安全页面，左上角选择需要防护的域名，单击**信息防泄漏**，进入信息防泄漏页面。
2. 在信息防泄漏页面，单击搜索框通过“规则 ID、规则名称、防御路径”关键词对规则进行查询。

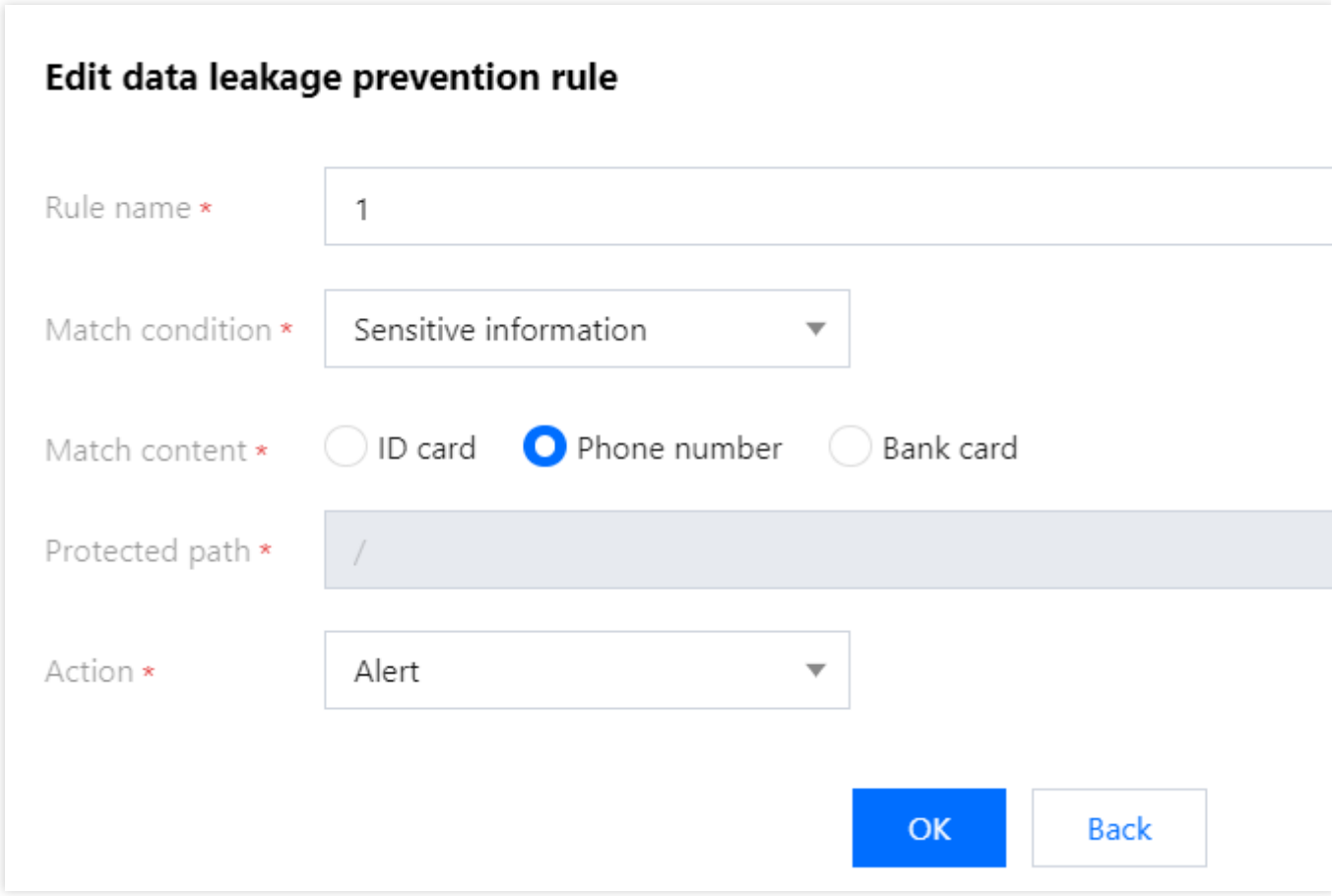


编辑规则

1. 在 基础安全页面，左上角选择需要防护的域名，单击**信息防泄漏**，进入信息防泄漏页面。
2. 在信息防泄漏页面，选择所需规则，单击操作列的**编辑**，弹出编辑防信息泄露规则弹窗。

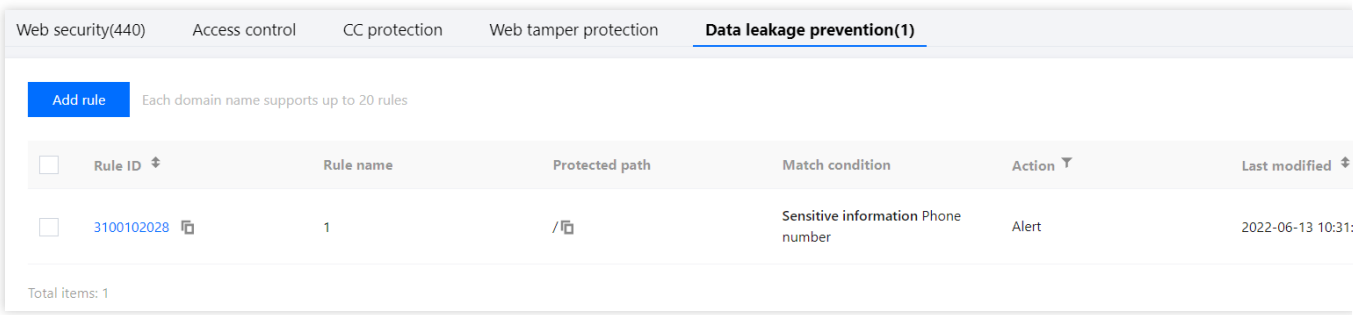


3. 在编辑防信息泄露规则弹窗中，修改相关参数，单击**确定**即可。



删除规则

1. 在 基础安全页面，左上角选择需要防护的域名，单击**信息防泄漏**，进入信息防泄漏页面。
2. 在信息防泄漏页面，选择所需规则，单击操作列的**删除**，弹出确认删除弹窗。



3. 在确认删除弹窗中，单击**确定**，即可删除该规则。

API 安全

最近更新时间：2023-12-29 14:42:06

本文档将为您介绍如何通过 API 安全功能，添加 API 接口或 API 规则文件，从而进一步保护 API 接口安全。

背景信息

通过 API 安全功能，您可以添加 API 接口或 API 规则文件，WAF 将对 API 请求进行安全检查，只有符合定义规范的 API 才能被执行。同时 API 安全防护模块将和 AI 引擎 及 BOT 流量管理 进行联动，进行 API 接口保护。

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** > **基础安全**，进入基础安全页面。
2. 在基础安全页面，左上角选择需要防护的域名，单击 **API 安全**，进入 API 安全页面。
3. 在 API 安全页面，添加 API 防护规则，目前支持通过 导入 API 和 添加 API 两种方式进行增加 API 规则。

说明：

导入 API（推荐）：根据获取的 API 文档，直接导入文件进行解析。

添加 API：用户根据网站的路径接口，手动添加需要防护的 API 路径。

导入 API（推荐）

1. 在 **基础安全** > **API 安全**页面，单击**导入 API**，弹出导入API 接口弹窗。
2. 在导入 API 接口弹窗中，选择上传文件类型，单击**点击上传**，传入 API 文件即可。

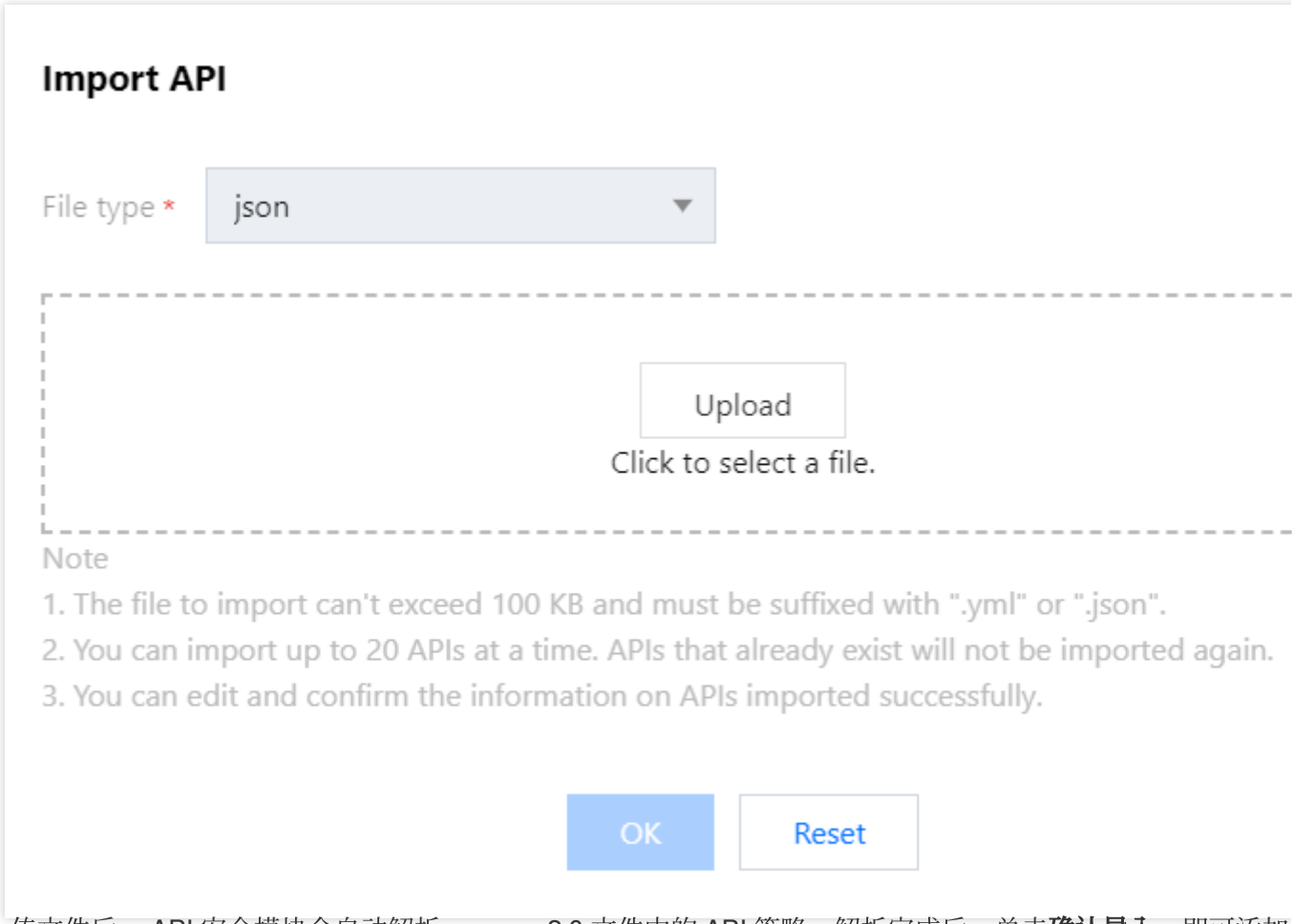
说明：

目前 WAF 支持两种 swagger2.0 文件的解析，分别是： yml 文件和 json 文件。导入规则说明：

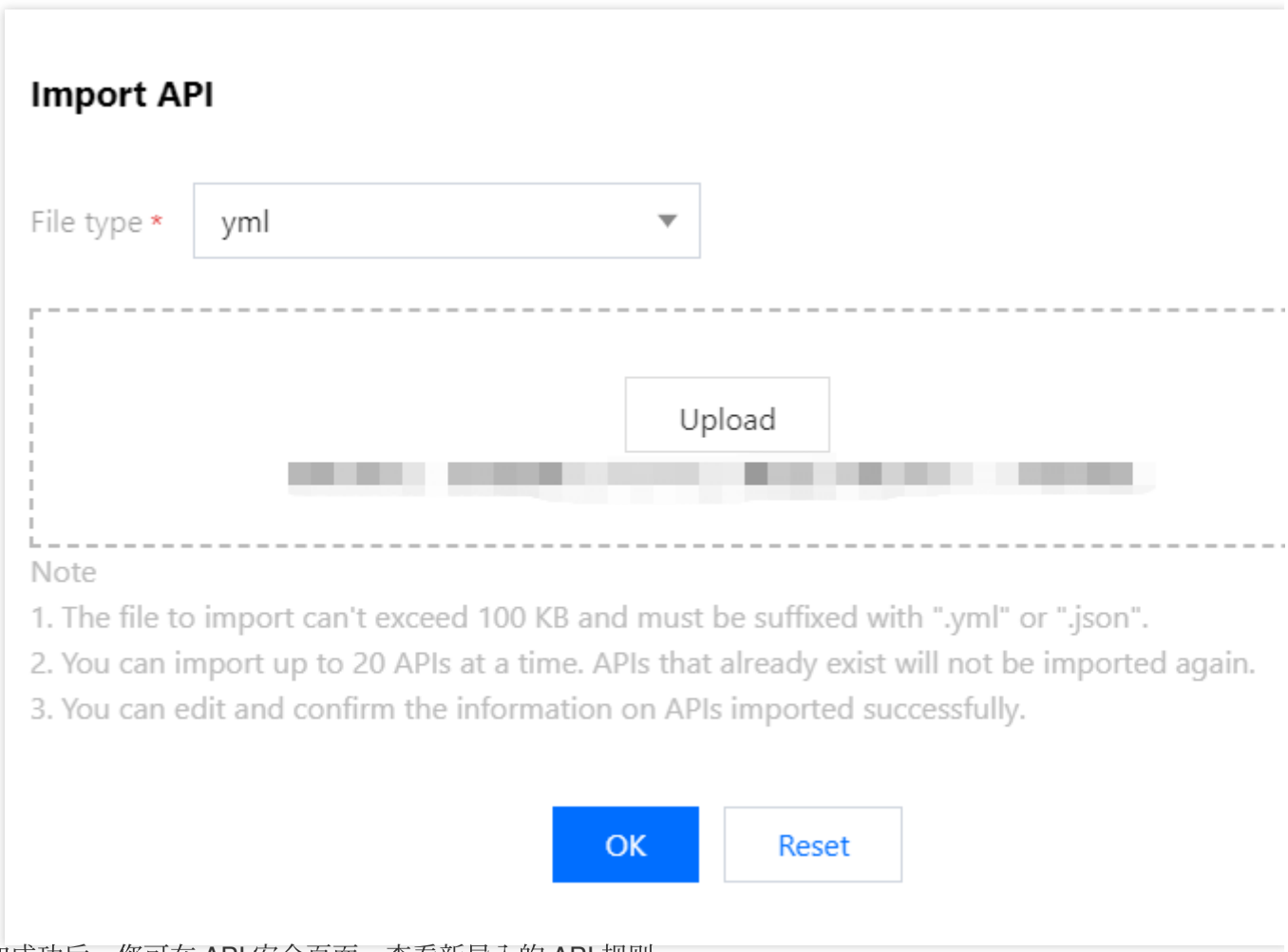
格式：导入 API 描述文件，文件后缀名必须为 .yml 或 .json，单次上传的 API 描述文件不超过100KB。

数量：每次最多可上传创建20条 API，导入已经存在的 API 会默认跳过。

导入创建成功的 API ，可进行编辑，请根据实际情况进行接口确认。



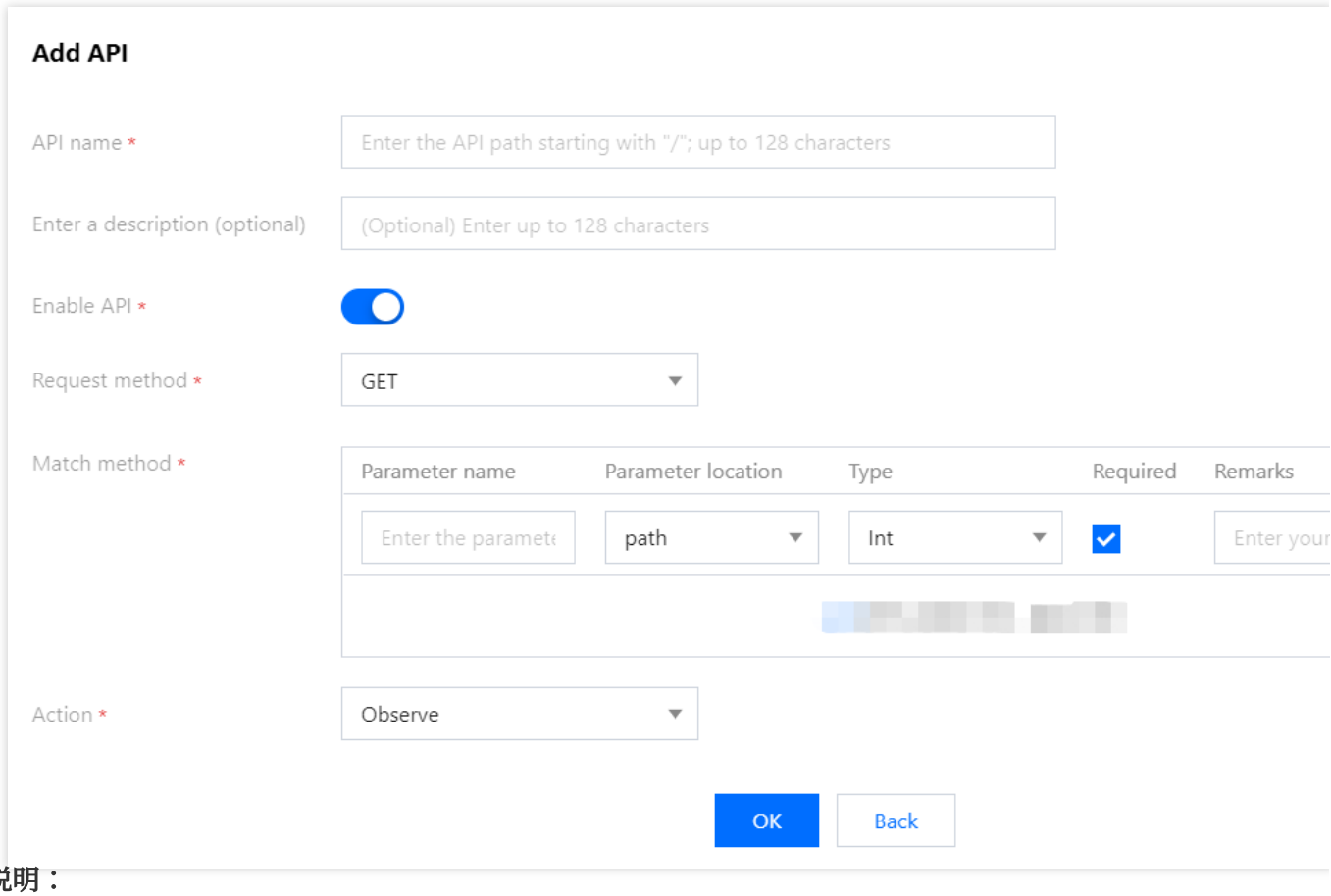
3. 您上传文件后， API 安全模块会自动解析 swagger2.0 文件中的 API 策略，解析完成后，单击**确认导入**，即可添加成功。



4. 添加成功后，您可在 API 安全页面，查看新导入的 API 规则。

添加 API

1. 在 **基础安全** > **API 安全**页面，单击**添加规则**，弹出添加 API 接口弹窗。
2. 在添加 API 接口弹窗中，您可根据网站的 API 策略，添加对应的 API 安全规则，添加完成后，单击**添加**。



字段说明：

接口名称：添加 API 路径，以'/'开头，注意接口名称+请求方式不能重复，如：`/guanjia/waf/config`。

描述：选填项，API 策略的相关描述。

接口开关：API 安全策略开关，默认为关。当开启开关后，才能对相应 API 策略进行解析，执行后续的观察和拦截动作。

请求方式：目前 API 安全支持四种请求方式：GET、POST、PUT 及 DELETE 方式。

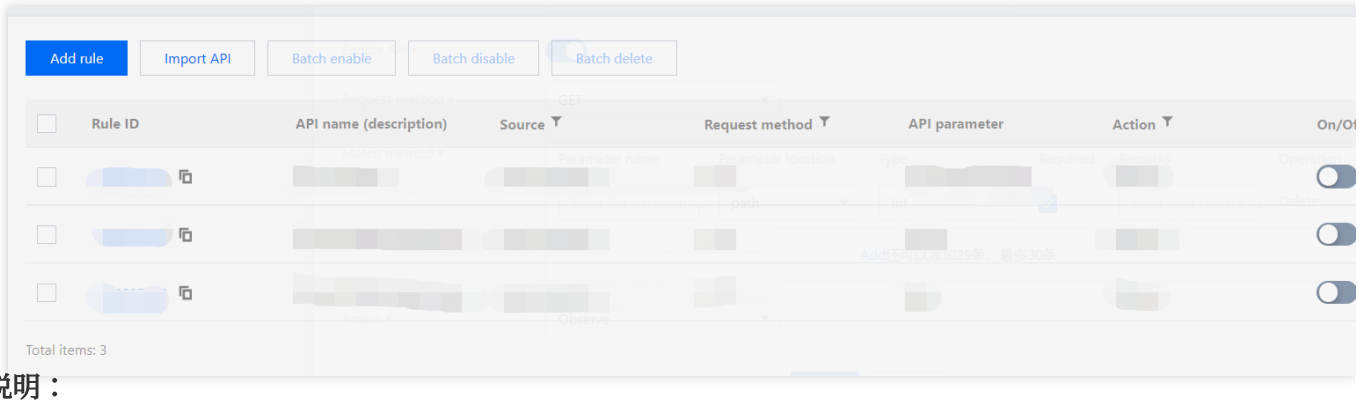
匹配条件：需要您添加5个参数，分别为参数名称、参数位置、参数类型、是否必填（若勾选必填，WAF 会检查请求中，是否含有该参数，若有，则请求正常通过，若没有就会被拦截。）以及备注（可填项），参数位置目前支持 body、query 及 path 三种类型（可根据您业务实际参数所在位置进行选择）。

执行动作：目前支持两种动作，观察和拦截模式。

说明：

建议您开启 API 安全功能时，先开观察模式，查看攻击日志是否存在误拦截，确认无误后，再开启拦截模式。

3. 添加完后，即可将 API 接口添加至 API 安全防护配置列表中。



字段说明：

规则 ID：添加成功一条 API 规则后，会自动生成一个对应的规则 ID，该 ID 在 API 安全模块具有唯一性，您可根据此 ID 在 攻击日志 中，查找对应的日志。

接口名称/描述：显示配置的 API 名称和描述，API 名称为 API 的实际路径，请按照实际防御域名的路径填写。

来源：来源分为两种，文件解析和手动添加。如果是导入的 API，则显示为文件解析，如果是手动添加的 API，则显示为手动添加。

请求方法：您配置的请求方法，分为 GET、POST、PUT 及 DELETE 四种。

API 参数：配置的 API 具体的参数列表，最多支持30个。

动作：分为观察和拦截两种。

开关：API 规则的启用状态，若关闭开关，则表示不启用。如需同时开启或关闭多个开关，可选择多个 API 规则，在列表上方，单击**批量启用**或**批量禁用**，进行批量操作。

修改时间：API 防护规则最新更新的时间。

操作：对指定的防护 API 操作说明，包括编辑及删除规则两种操作。如需批量删除规则，可选择多个 API 规则，在列表上方，单击**批量删除**，即可进行批量操作。

BOT 与业务安全
BOT 设置
BOT 管理
概述

最近更新时间：2023-12-29 14:42:24

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 场景化

该功能依托腾讯云多年 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。

客户端风险识别（前端对抗）

该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 HTML5 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。

威胁情报

该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。

AI 评估

该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。

智能统计

该功能基于大数据分析统计，根据客户的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。

动作设置

该功能通过威胁情报、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，用户可根据配置不同分数段的动作，实现风险访问的精准拦截。
同时，支持通过配置**生效范围**，对符合该生效范围的请求数据，进行相应的精准处置。

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。

合法爬虫

用户可以通过配置该功能，使合法爬虫（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。

自定义规则

用户可以通过该功能，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。
同时，支持通过配置**生效范围**，对符合该生效范围的请求数据，进行相应的精准处置。

BOT 白名单

BOT 白名单，支持从 HTTP 报文的会话特征、请求特征、COOKIE、HTTP 头部、生效范围、IP 特征、UserAgent、Referer、会话设置等多个特征进行组合，通过特征匹配来对特定公网用户的访问进行加白。
优先级从高到低顺序：BOT 白名单 > 场景1（优先级1） > 场景2（优先级2）> …… > 场景 n（优先级 m）。

BOT 管理概览

最近更新时间：2023-12-29 14:42:37

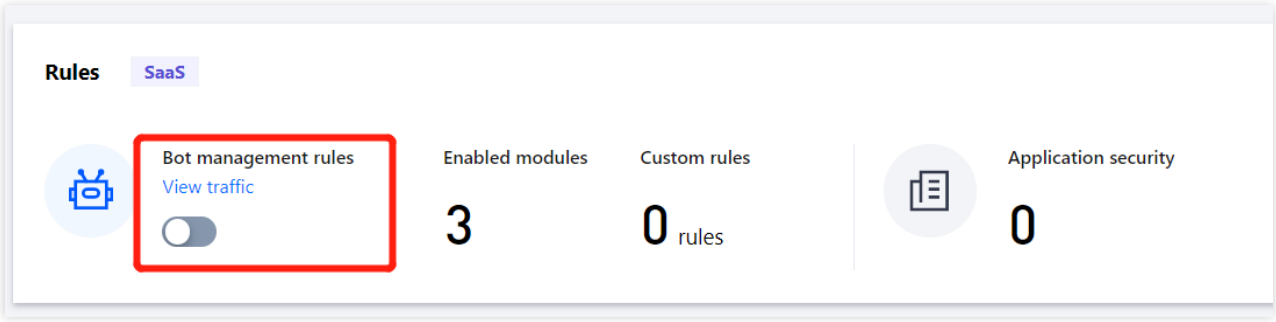
前提条件

BOT 流量管理需要购买 WAF 对应实例的增值服务。

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**，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 管理规则的

，即可开启 BOT 流量分析。



字段说明

BOT 管理规则开关：默认关闭，可根据需要开启。

说明：

当且仅当域名 WAF 开关开启时，BOT 流量分析功能生效。

生效场景：展示当前域名下，开启了多少个 BOT 分析的场景模块，BOT场景中包含：前端对抗、威胁情报、AI 模型、智能统计等。

场景总数：展示当前域名下，存在多少个 BOT 分析的场景模块。

当前全局场景：展示当前域名下，生效的全局场景名称

自定义总数规则：展示当前开启了多少个 BOT 的自定义规则。

高级设置

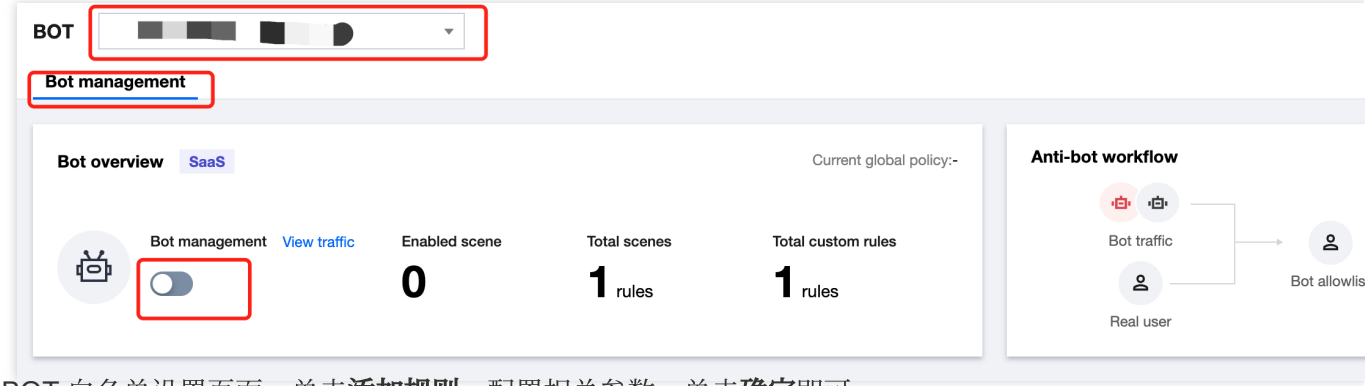
最近更新时间：2023-12-29 14:43:56

前提条件

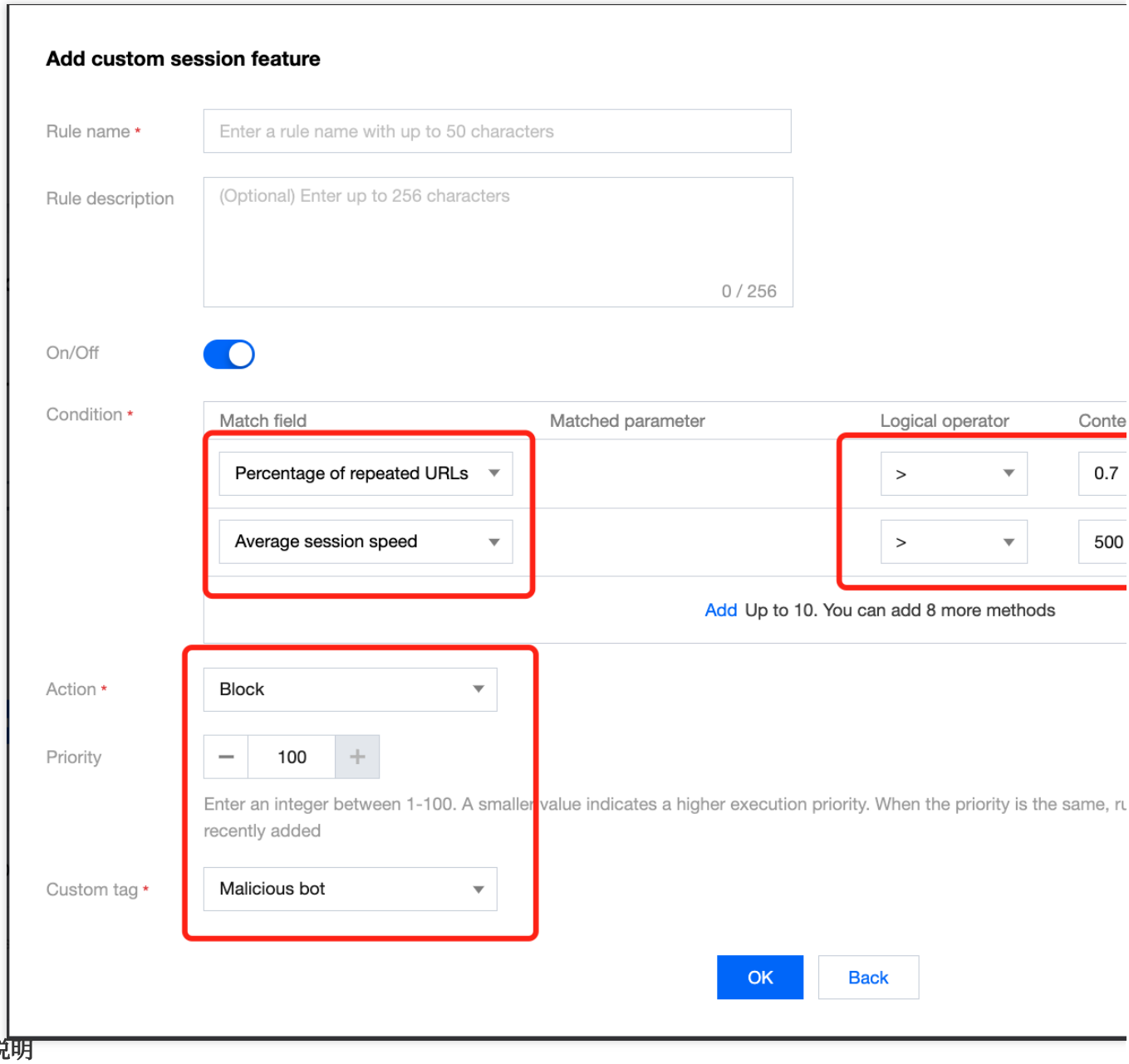
购买 Web 应用防火墙及 BOT 流量管理拓展包，并且打开已接入 WAF 域名 BOT 分析开关。

BOT 白名单

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 > BOT 白名单**。



3. 在 BOT 白名单设置页面，单击**添加规则**，配置相关参数，单击**确定**即可。



字段说明

策略名称： 策略名称字段。

策略描述：策略描述字段。

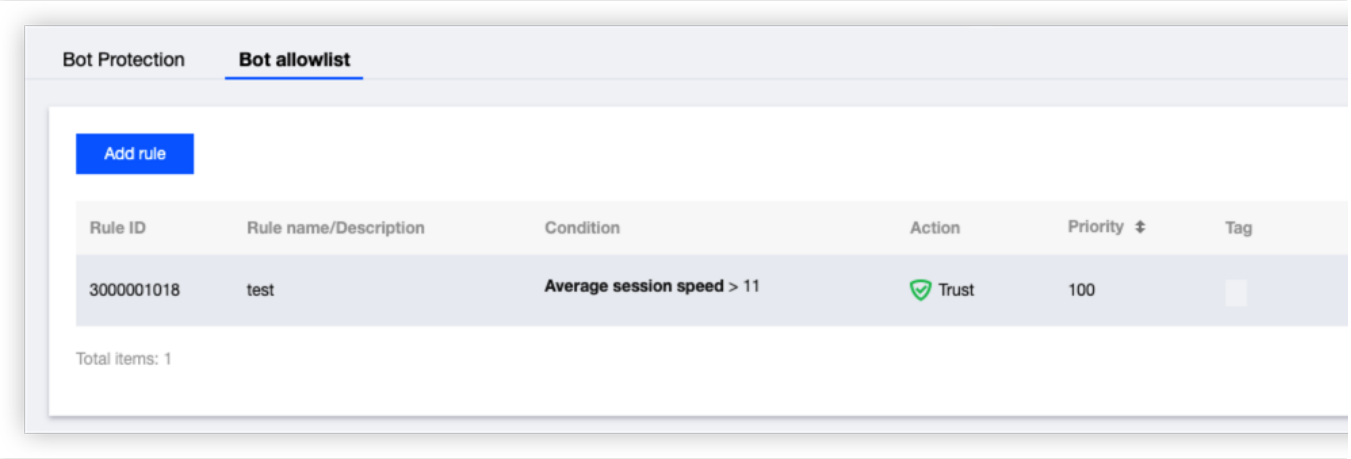
规则开关：策略开关状态，默认开启。

匹配条件：设置 BOT 策略的匹配条件，最多可以设置10个匹配条件，各个条件之间是“与”的关系。鼠标悬停具体的匹配条件时，可以查看相应的条件说明。

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。

自定义标签： 可设置为友好 BOT、正常流量。

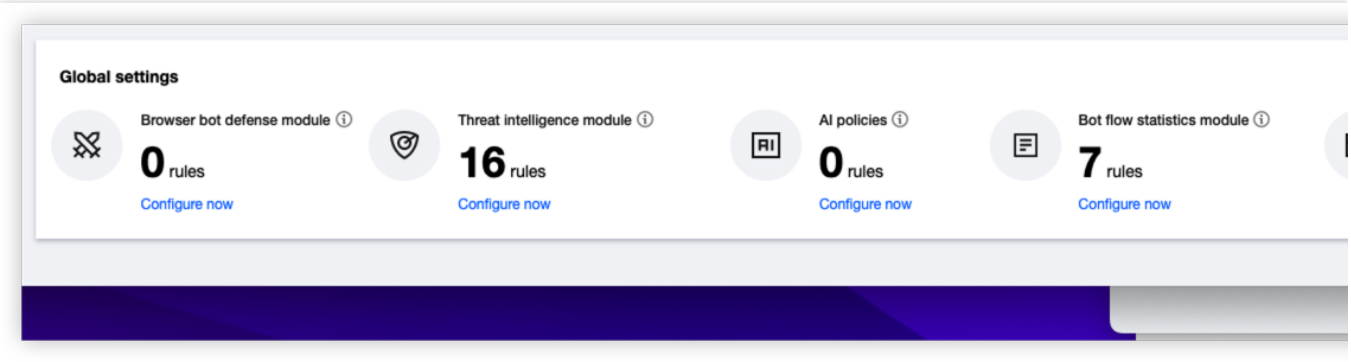
4. 完成添加后，可在策略列表中查看刚刚创建的规则，单击**编辑**或**删除**，可对该规则进行编辑或删除。



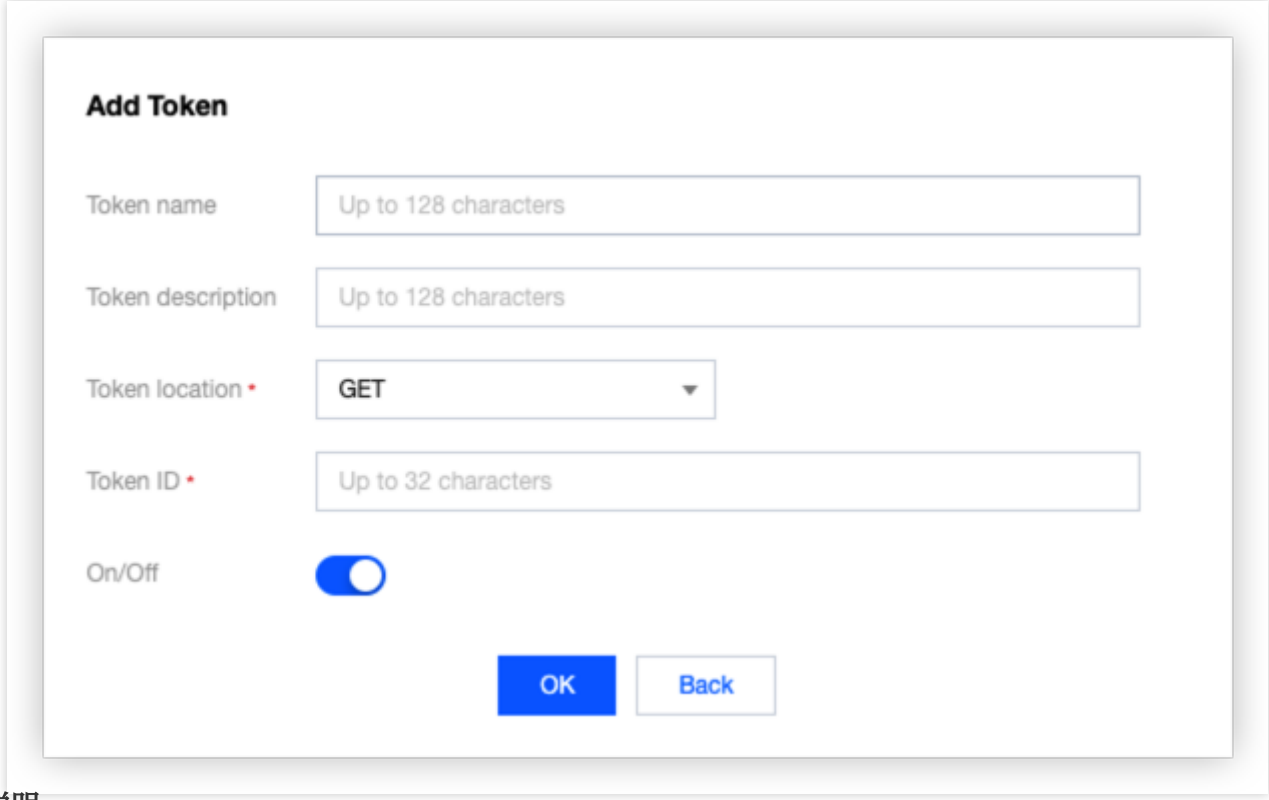
5. 优先级从高到低顺序：BOT 白名单 > 场景1（优先级1）> 场景2（优先级2）> ..... > 场景 n（优先级 m）。

会话管理

该功能和 CC 防护 中的 Session 设置类似，通过不同的 Token 标识配置，用于区分在同一个 IP 下不同访问者的访问，分别统计不同访问者的访问行为特征。
同时，可以根据不同的 Token 标识配置，连续跟踪不同访问者的访问行为，解决来自住宅 IP/公共出口 IP 下无法精准处置 BOT 访问行为，以及快速变换代理 IP 中无法统计会话特征的问题。
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 > BOT 防护**。
3. 在 BOT 防护页面，单击会话管理的**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**。
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。



字段说明

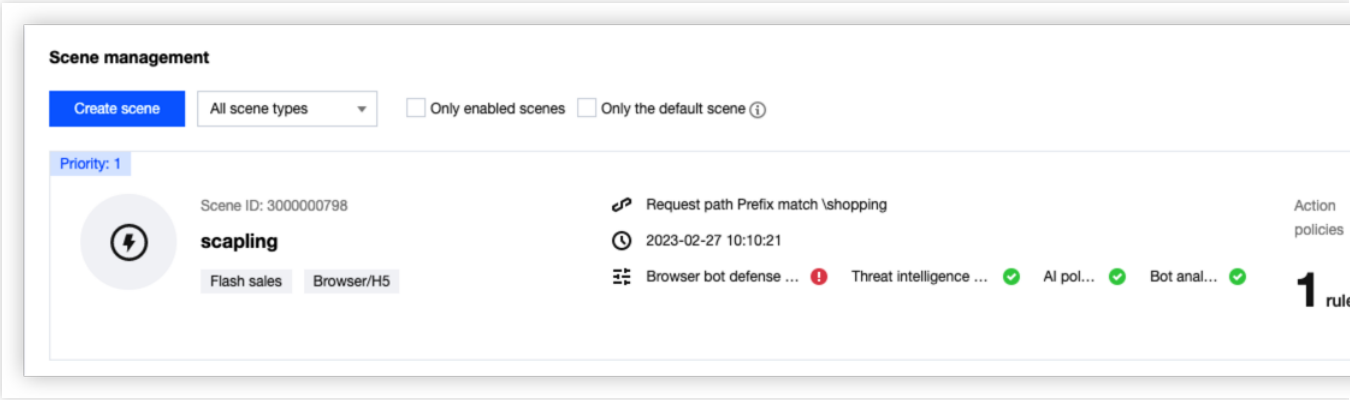
Token 位置： 可选择 HEADER、COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。

Token 标识：取值标识。

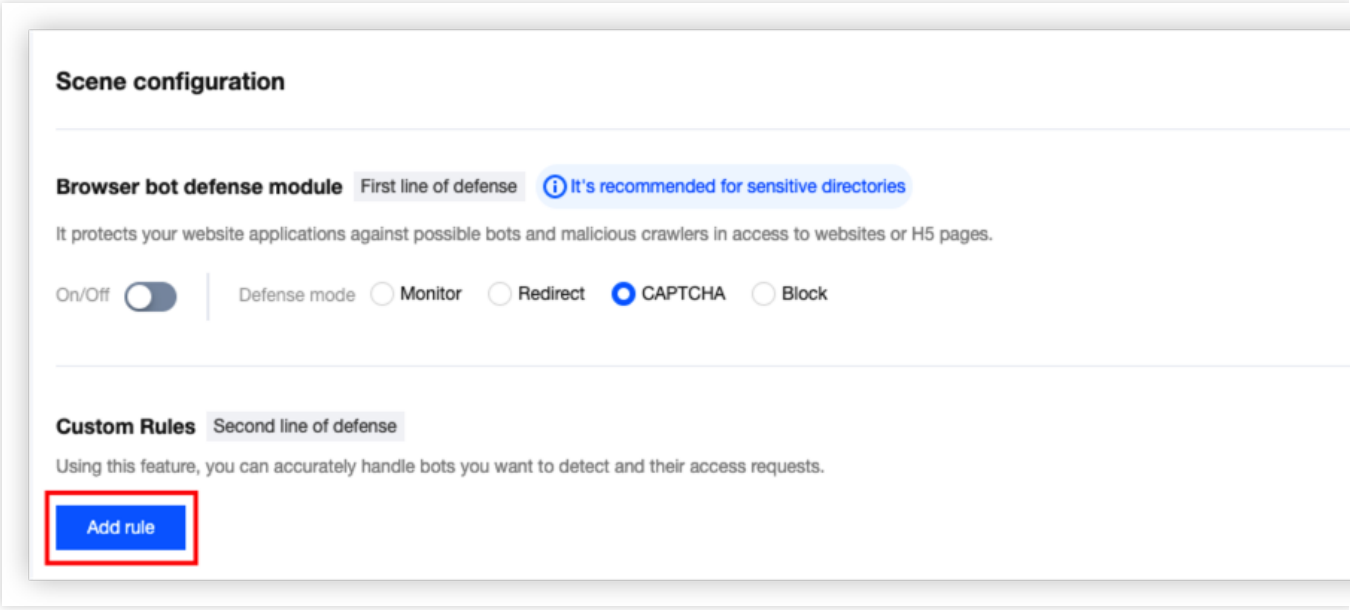
5. 配置完成后即可自动生效，BOT 流量分析将开始根据会话特征特征所在字段，进行流量分析。

设置自定义规则

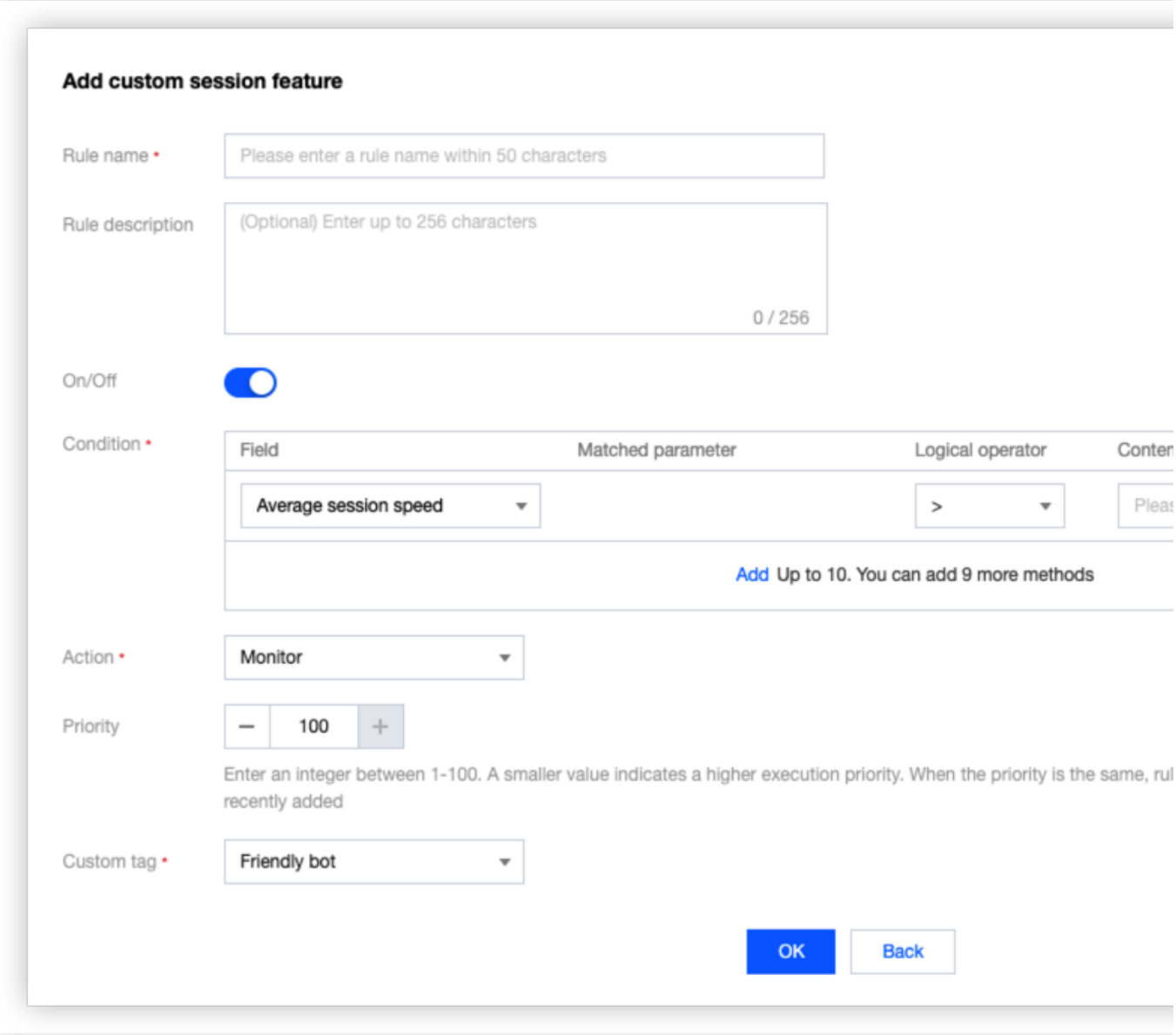
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理 > BOT 防护**。
3. 在场景化管理中，选择目标场景，单击右侧的**查看配置**。



4. 在场景详情页面，单击自定义规则的**添加规则**。



5. 在添加自定义会话特征窗口中，配置相关参数，单击**确定**。



字段说明

策略名称：策略名称字段。

策略描述：策略描述字段。

策略开关：策略开关状态，默认开启。

匹配条件：设置 BOT 策略的匹配条件，最多可以设置10个匹配条件，各个条件之间是“与”的关系。鼠标悬停具体的匹配条件时，可以查看相应的条件说明。

执行动作：设置执行动作，具体说明如下。

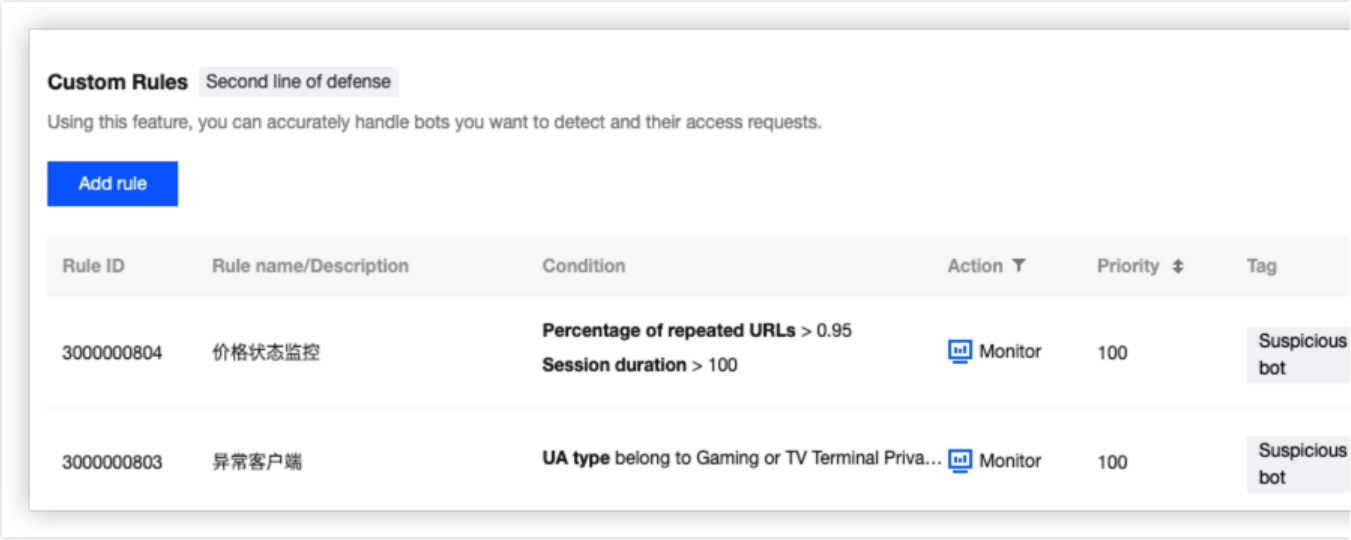
动作类型	说明
信任	符合匹配条件的会话请求将被放行，放行不记录日志。
监控	符合匹配条件的会话请求将会被监控记录日志，可在 BOT 详情的自定义类型中查看监控的会话信息。

人机识别	仅用于浏览器访问场景，符合匹配条件的会话请求将进行验证码挑战，若挑战失败，执行拦截动作。若挑战成功，正常访问。
重定向	符合匹配条件的会话请求执行重定向，将请求重定向到指定 URL，但只支持重定向到当前域名下的 URL。
拦截	符合匹配条件的会话请求将执行拦截，拦截结果可在 攻击日志 中查看，拦截 IP 的实时信息可在 IP 封堵状态 中查看。

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。

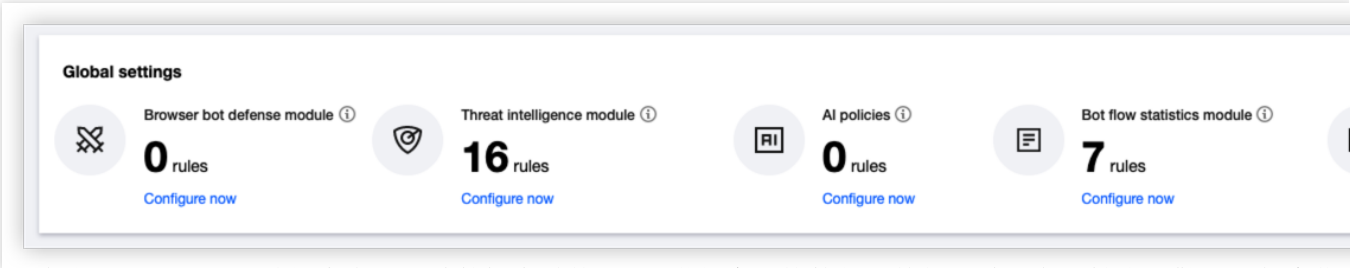
自定义标签： 可设置为友好 BOT、恶意 BOT、正常流量或疑似 BOT。

6. 完成添加后，可在策略列表中查看刚刚创建的规则，单击**编辑**或**删除**，可对该规则进行编辑或删除。

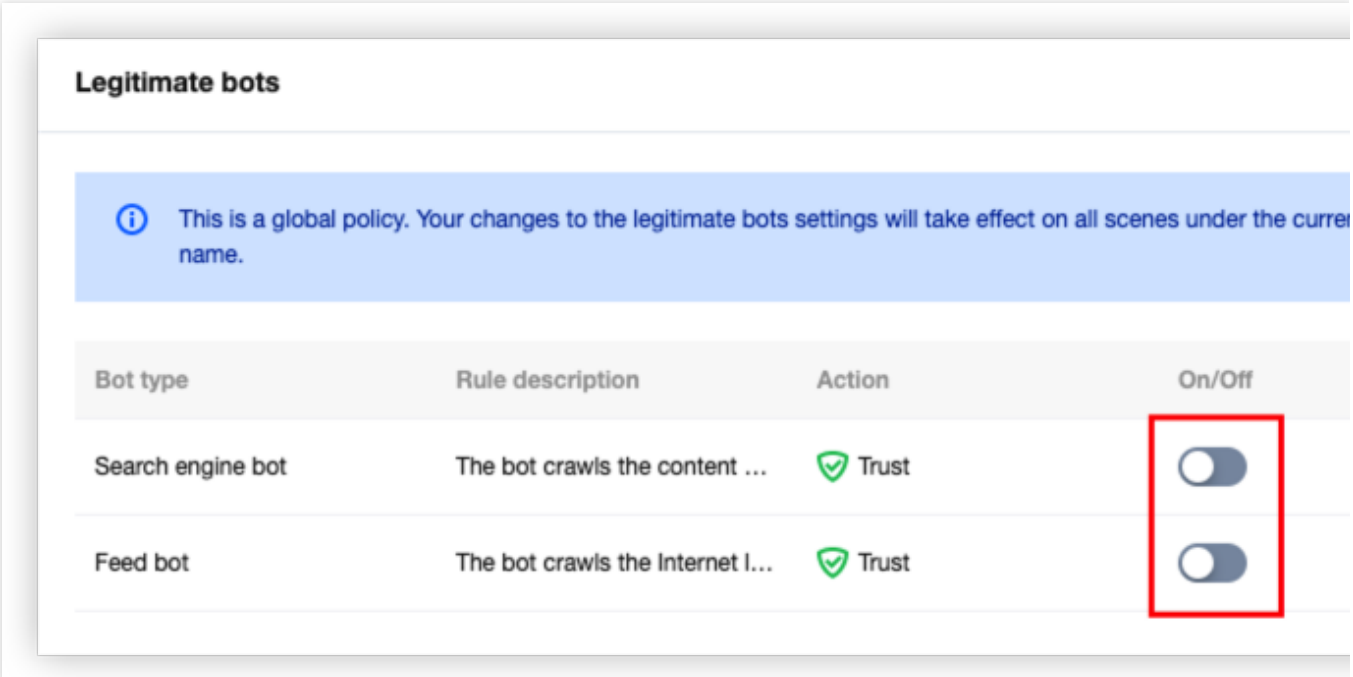


合法爬虫

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 > BOT 防护**。
3. 在 BOT 防护页面，单击合法爬虫的**前往配置**。



4. 在合法爬虫页面，通过开关将来自对网站数据有益的 BOT 进行合理的放行，使得网站上在对搜索引擎、外部合作爬虫进行。



客户端风险识别

最近更新时间：2023-12-29 14:42:49

本文为您介绍客户端风险识别中的前端对抗功能。该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 HTML5 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。

背景信息

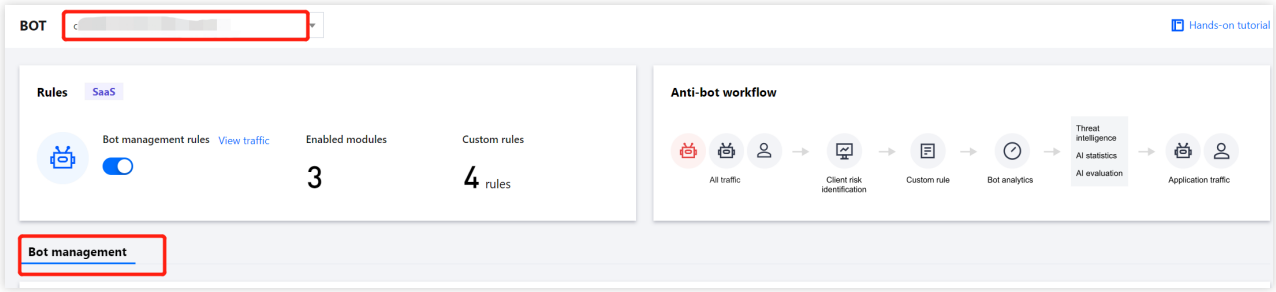
兼容性说明：前端对抗适用于网页或 HTML5 业务防护，通过前端对抗技术，动态生成客户端 ID 和 Token，通过检测客户端 ID 和动态 Token，完成恶意和爬虫请求识别。在特定情况下，POST 请求可能存在兼容性问题（响应体 content-type 内容不为：text/html，且响应体中未包含有 `<html>` 标签），导致前端动态检测异常，此时可以对请求路径或者响应请求进行加白处理。
有感前端对抗：对符合条件的客户请求通过弹出验证码（滑块、拼图、字符比较等方式）的方式进行验证识别，区别人和工具（BOT）的访问行为，对验证失败达到一定次数的请求进行拦截处理；适用于保护网站核心接口（如购物车、支付、短信接口等）。该能力已经在 WAF 的各个模块动作处理（观察、人机识别、重定向和拦截等）中集成，您可以根据实际需要进行配置使用。
无感前端对抗：在对用户体验无影响的情况完成客户端行为检测，适合对用户体验要求较高的场景。无感前端对抗通过动态安全技术，对请求客户端生成客户端唯一 ID，检测客户端对 Web 或 HTML5 页面访问中可能存在刷量和恶意爬虫行为，您可以根据实际需要对恶意访问行为进行动作处理。
注意：
前端对抗技术仅适用于 Web 或 HTML5 环境，移动端和小程序暂不支持。

前提条件

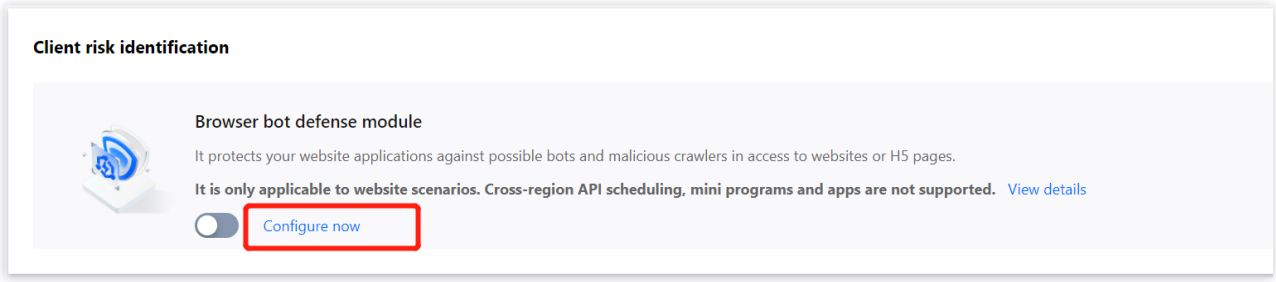
已购买 Web 应用防火墙，并购买 BOT 流量管理扩展包。
完成防护域名的添加及正常接入，当前域名处于正常防护，且开启 BOT 管理规则总开关，详情请参见 快速入门。
说明：
在 CLB-WAF 实例添加的域名，暂时不支持开通前端对抗。
在 SaaS-WAF 实例添加的泛域名，暂时不支持开通前端对抗。

防护配置

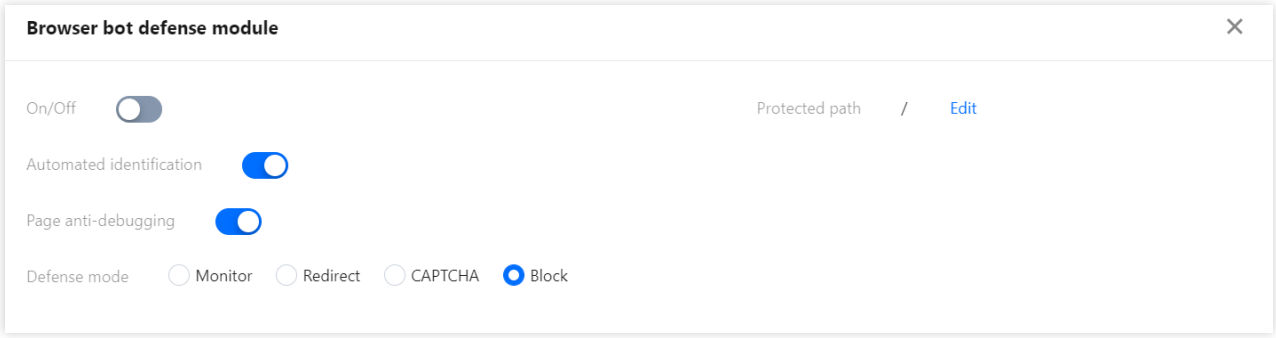
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在全局设置中，单击前端对抗模块的**前往配置**，进入前端对抗配置页。
4. 单击设置前端对抗自动化识别攻击、页面防调试和白名单策略等维度的配置。



5. 在前端对抗页面，可以配置页面防调试、自动化工具识别等功能开关。



6. 单击某场景配置页，单击前端对抗，配置该场景下前端对抗的功能开启/关闭，并选择防护模式。

字段说明

开关：默认关闭。开启后， WAF 将对域名下该场景的生效范围的页面，进行前端对抗安全防护，识别客户端请求中可能存在爬虫行为，可以对识别为爬虫行为的请求采取不同处置动作。APP 和小程序暂不适用该策略。

自动化工具识别：默认开启，自动化工具识别能力，开启后辅助进行动态威胁检测。

页面防调试：默认开启，为了防止用户查看页面逻辑，页面防调试功能在用户调用浏览器的开发者工具页面时，阻止用户跟踪页面逻辑。

注意：

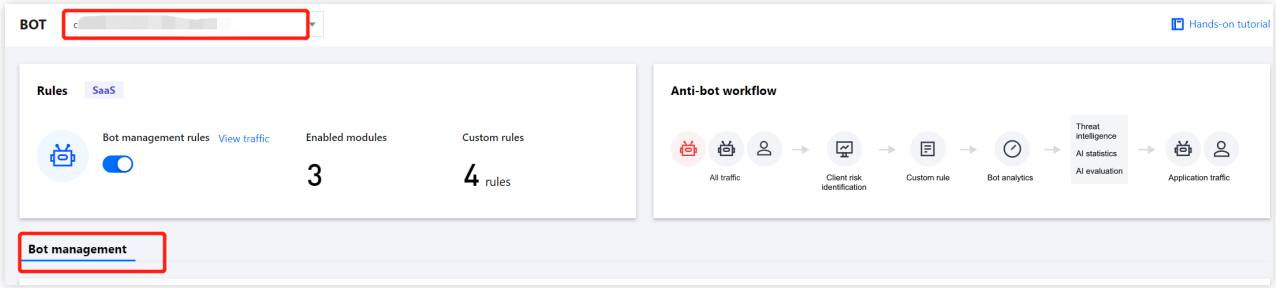
建议在需要进行防护的敏感目录下开启此防护功能。

防护模式：默认为监控状态，开启开关后，您可以设置对前端对抗模块检出的爬虫行为进行动作处理，动作类型包括：监控、人机识别、重定向和拦截。

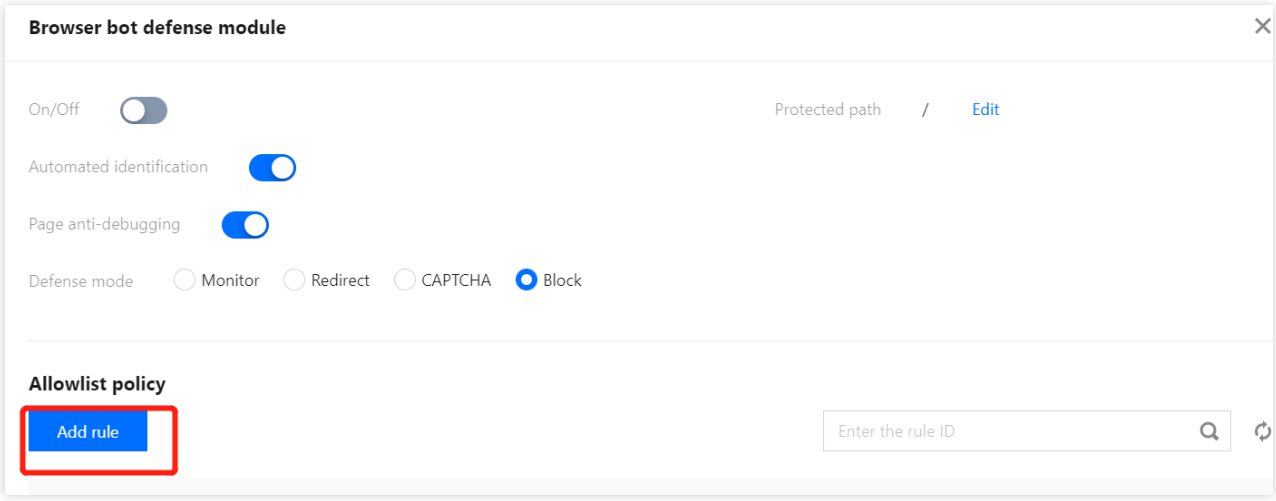
配置白名单策略

添加规则

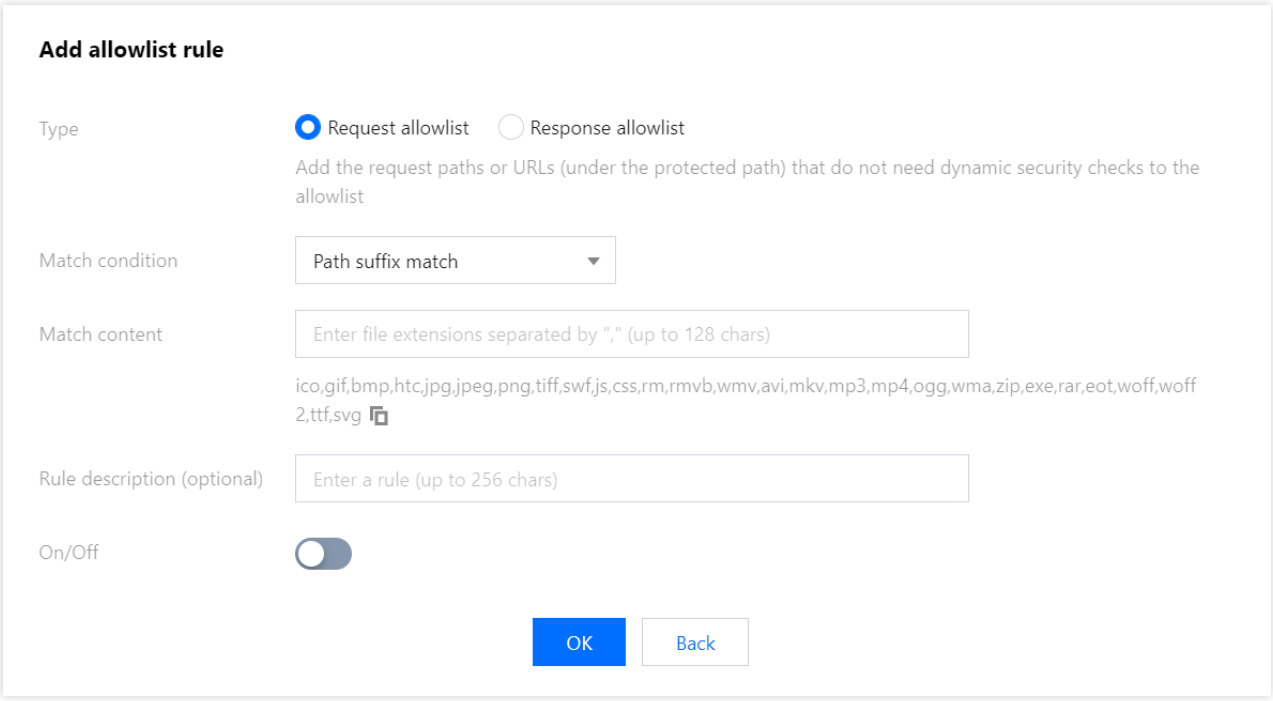
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，在全局设置中，单击前端对抗模块的**前往配置**。



3. 在前端对抗页面，单击**添加规则**，弹出添加白名单规则窗口。



4. 在添加白名单规则窗口中，配置相关参数，单击**确定**即可。



字段说明

类型

请求白名单：加白网站 URL 页面不需要进行动态安全检测。

响应白名单：默认 WAF 会根据业务情况对响应页面插入 JS，可指定页面不插入 JS，提高网站兼容性。

匹配条件：支持路径后缀匹配、前缀匹配、相等和包含，默认为：路径后缀匹配。

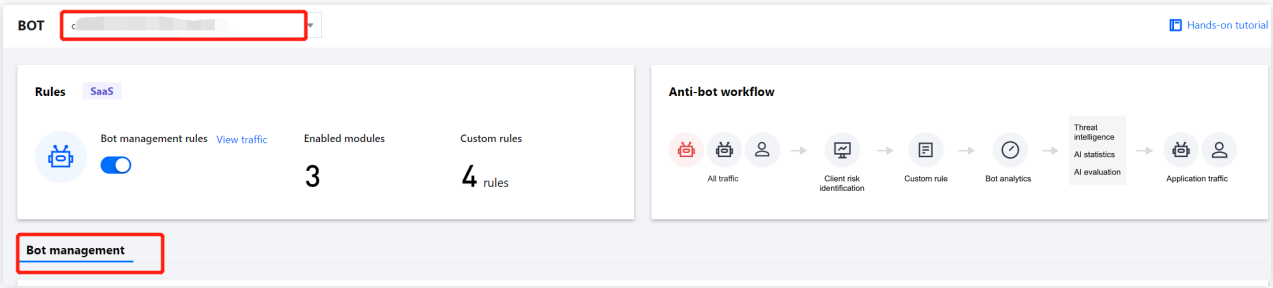
匹配内容：当匹配条件为**路径后缀匹配**，默认给出需要加白的文件后缀名称，包括：ico、gif、bmp、htc、jpg、jpeg、png、tiff、swf、js、css、rm、rmvb、wmv、avi、mkv、mp3、mp4、ogg、wma、zip、exe、rar、eot、woff、woff2、ttf、svg。您可以根据实际情况进行修改。 输入其他匹配条件，请按照实际情况输入白名单路径。

规则描述（选填）：输入规则描述信息。

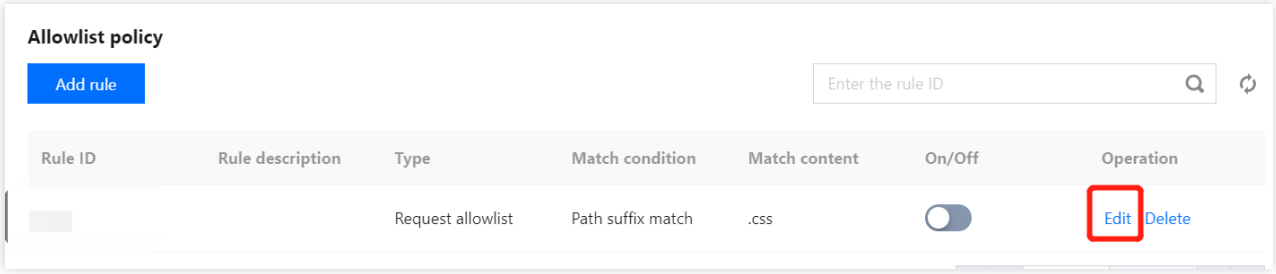
规则开关：默认关闭，您可根据实际情况调整。

编辑规则

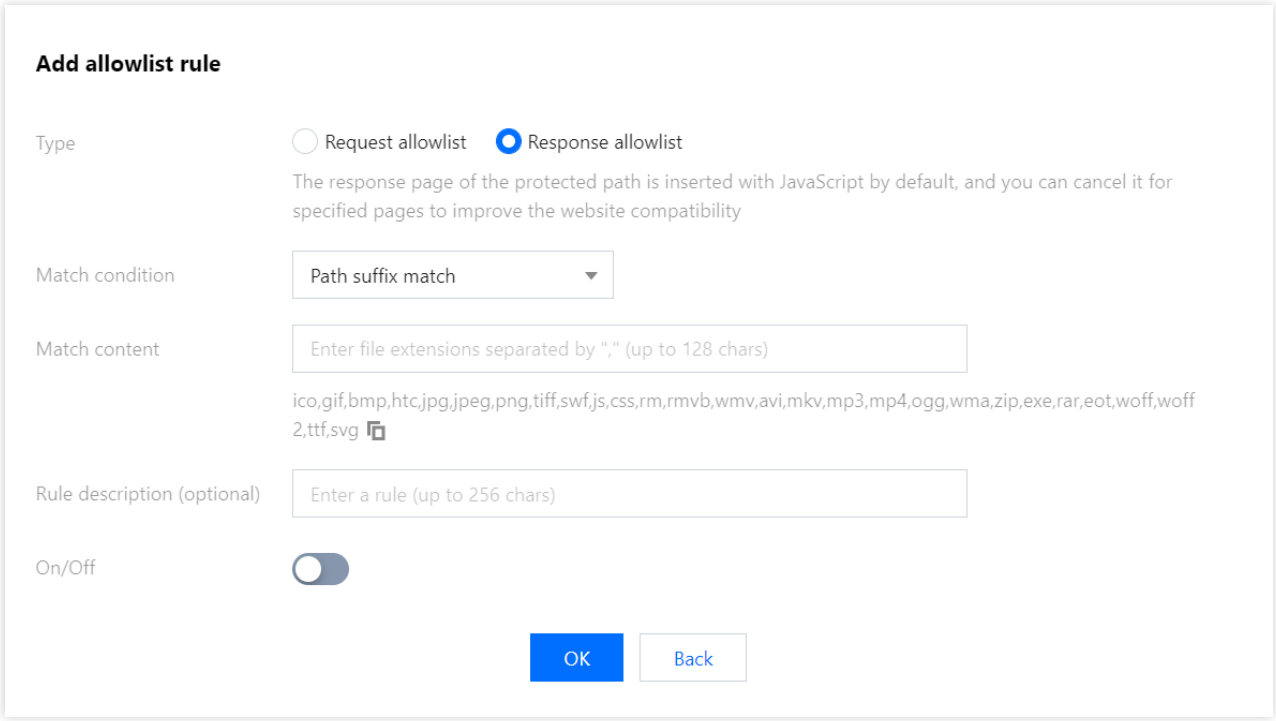
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，在全局设置中，单击前端对抗模块的**前往配置**。



3. 在前端对抗页面，选择所需规则，单击**编辑**，弹出编辑白名单规则窗口。

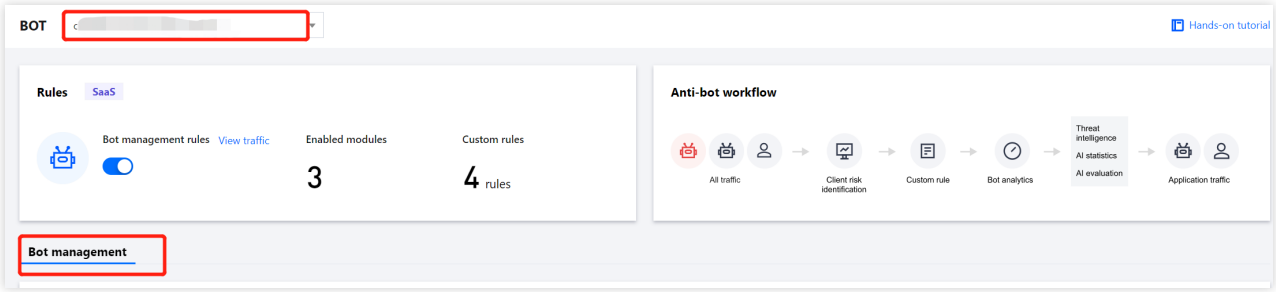


4. 在编辑白名单规则窗口中，修改相关参数，单击**确定**即可。

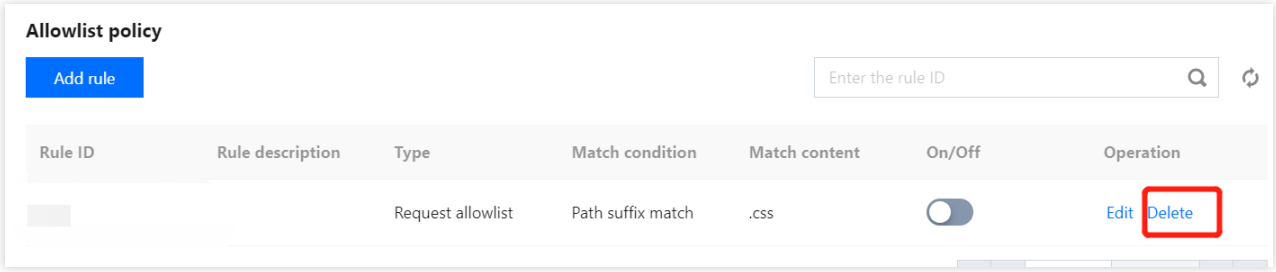


删除规则

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，在全局设置中，单击前端对抗模块的**前往配置**。



3. 在前端对抗页面，选择所需规则，单击**删除**，弹出“确认删除”弹窗中。



4. 在“确认删除”弹窗中，单击**确定**，即可删除该规则。

智能分析
AI 策略

最近更新时间：2023-12-29 14:43:03

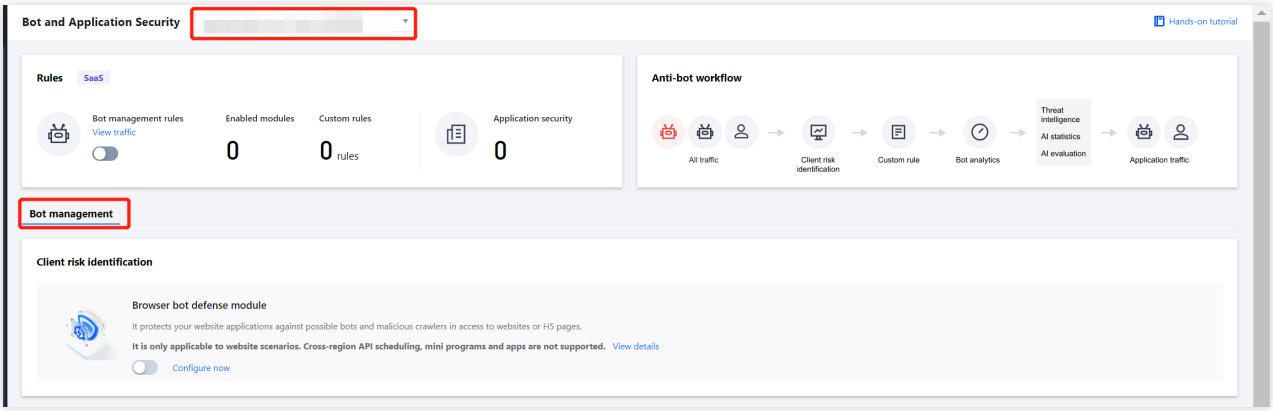
本文为您介绍 BOT 流量管理的 AI 策略模块。该功能依托腾讯近二十年的网络安全经验和 BOT 对抗经验，基于人工智能技术和腾讯风控实战沉淀，将风控特征和黑灰产对抗经验转化为 AI 策略模型，快速识别恶意访问者。快速识别并处置来自 BOT 对抗经验积累的 BOT、高级持续威胁 BOT、分布式 BOT。

前提条件

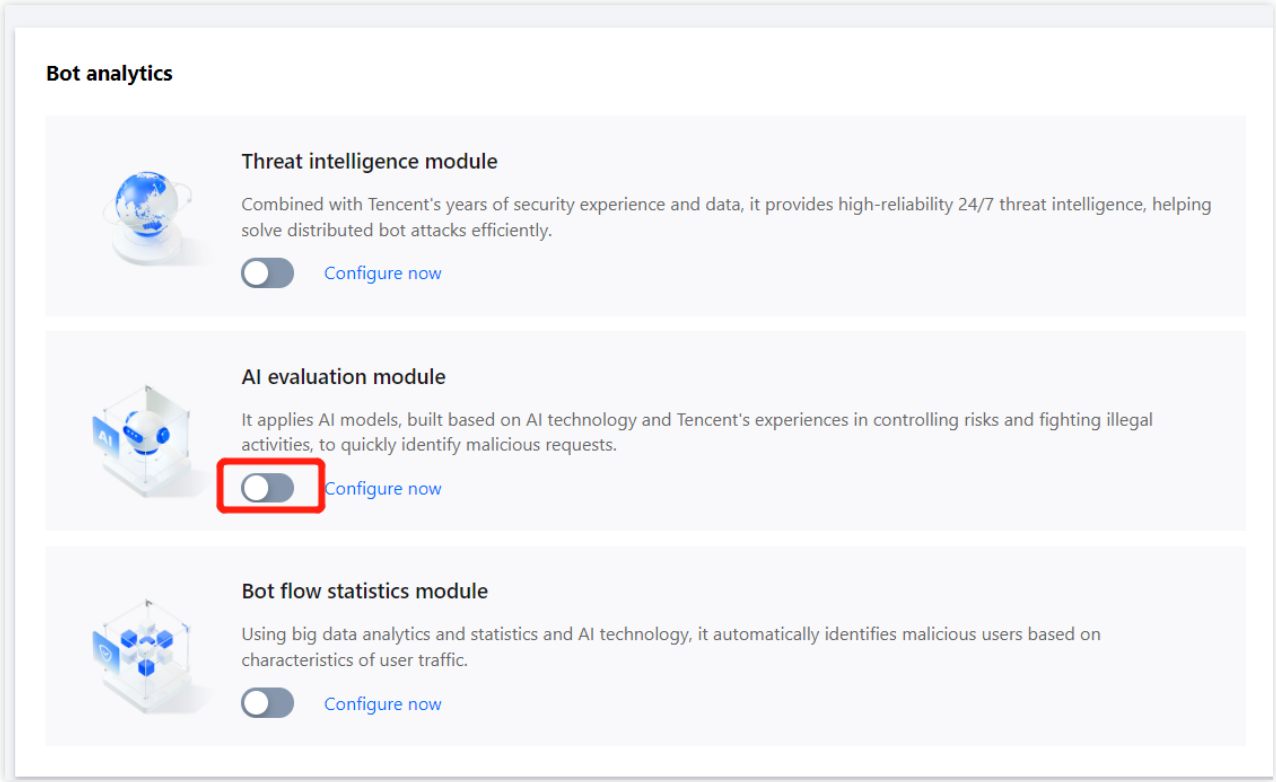
购买 Web 应用防火墙及 BOT 流量管理拓展包，并且打开已接入 WAF 域名 BOT 规则管理开关。

防护配置

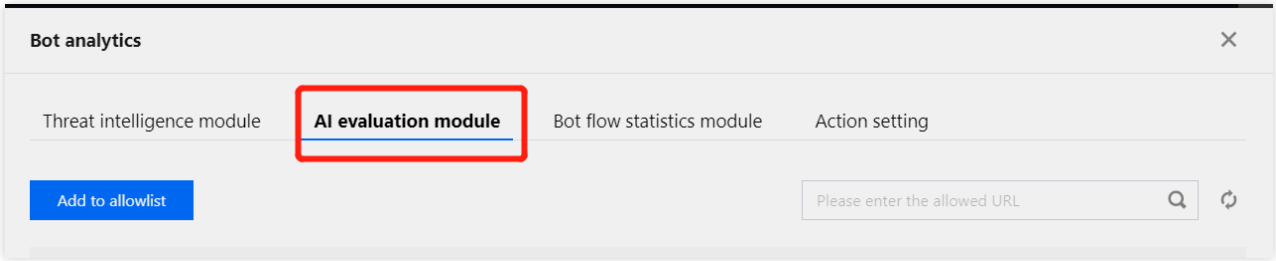
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击**BOT 管理**。



3. 在全局设置中，单击前端对抗模块的**前往配置**。



4. 在发现 AI 检出误报时，可以单击**添加白名单**定向加白特定的 URL 检出，减少误报。



5. 在 AI 策略页面中，可加白相关 URL 白名单，避免核心业务/回调业务的访问频次过多造成核心业务异常拦截，可增加对应 URL 的 AI 策略白名单，避免误拦截。

说明：

此处 AI 策略白名单仅影响 AI 策略模块，不影响其他模块的正常检出。

参数说明：

策略名称：策略的名称。

规则描述：策略的描述。

加白 URL：AI 策略的加白路径，影响 AI 策略的得分结果。

规则开关：AI 策略白名单的开关，开启状态时，当前 AI 策略白名单生效，在 URL 命中 AI 策略白名单时，AI 策略将不增加其分数，其 BOT 评估分值由威胁情报、智能统计进行提供。

6. 配置完成AI策略相关配置之后，单击某场景配置页，单击 AI 策略模块的

。即可针对该场景开启 AI 策略模块。

AI 策略最佳实践

AI 策略基于 BOT 对抗历史经验以及 BOT 攻防实验室运营经验，可快速发现通用 BOT 以及高级持续威胁 BOT， 因此建议在任何情况下开启 AI 策略，并且 AI 策略白名单中加白来自业务回调接口。

威胁情报

最近更新时间：2023-12-29 14:43:16

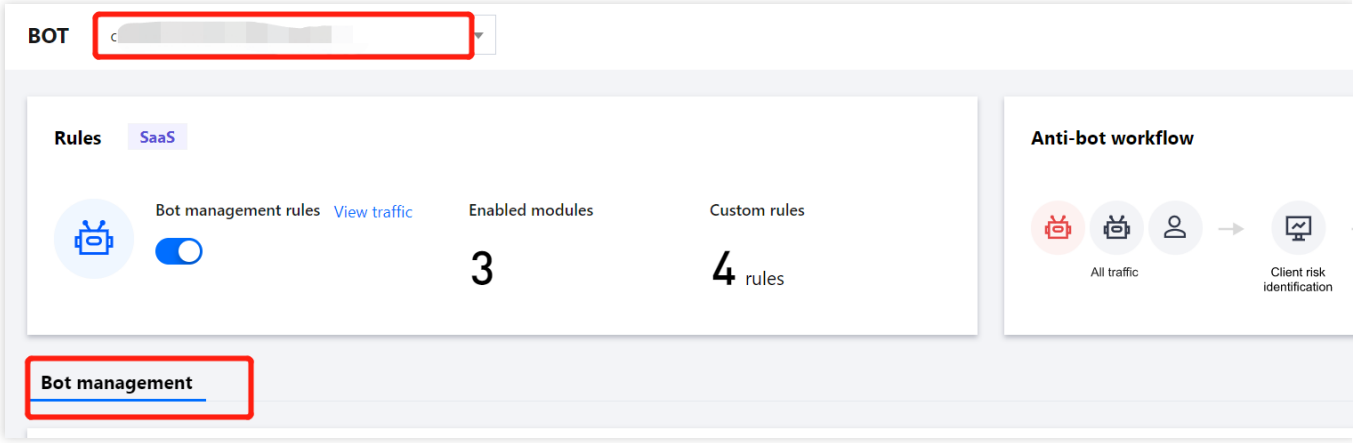
本文为您介绍 BOT 流量管理的智能分析中威胁情报模块。该功能依托腾讯近二十年的网络安全经验和大数据情报，将通过实时判定 IP 状态，采取打分机制、量化风险值、精准识别来自恶意动态 IP、IDC 的访问，同时智能识别恶意爬虫特征，解决来自恶意爬虫、分布式爬虫、代理、撞库、薅羊毛等风险访问。

前提条件

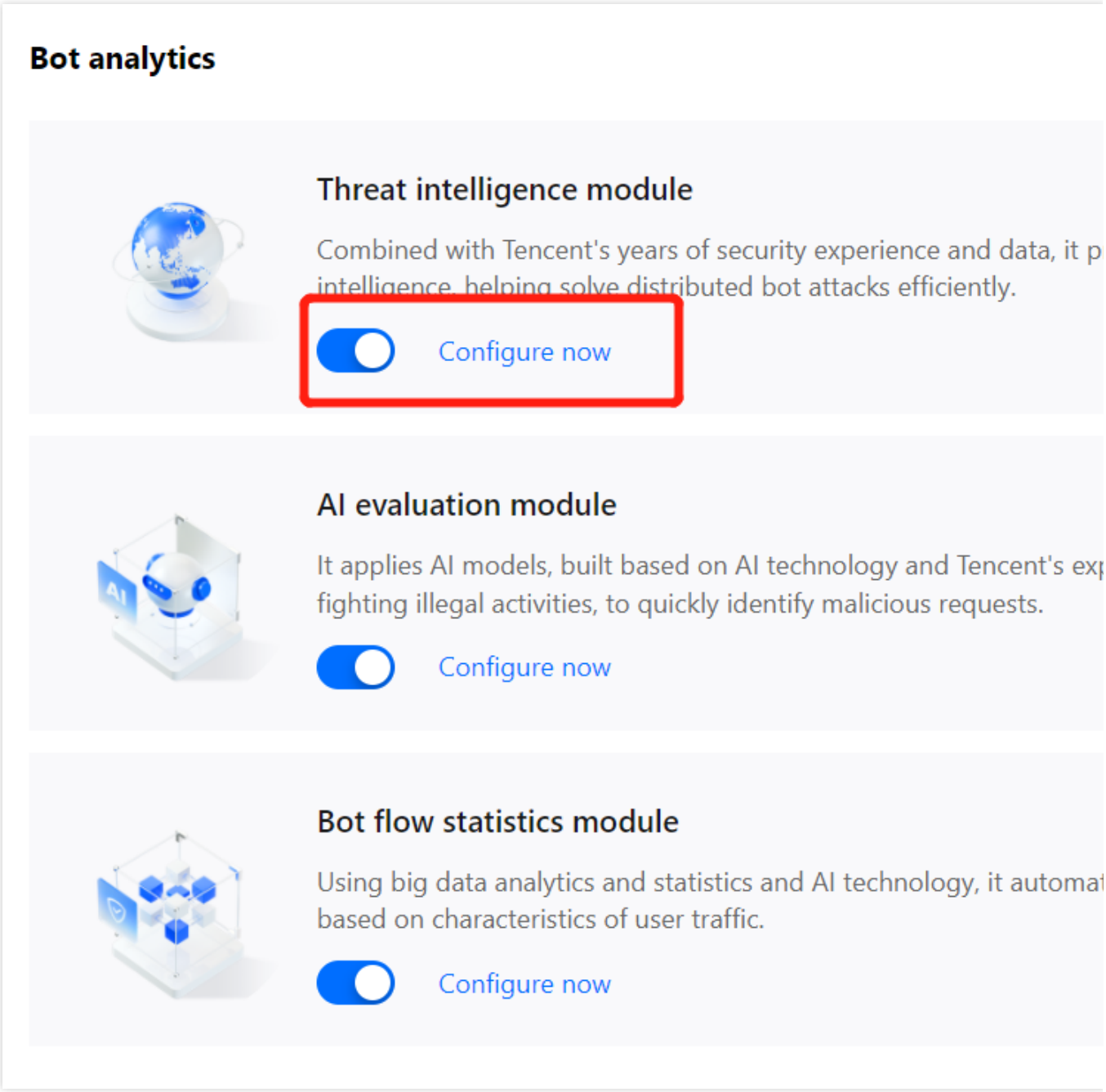
购买 Web 应用防火墙及 BOT 流量管理拓展包，并且打开已接入 WAF 域名 BOT 分析开关。

防护配置

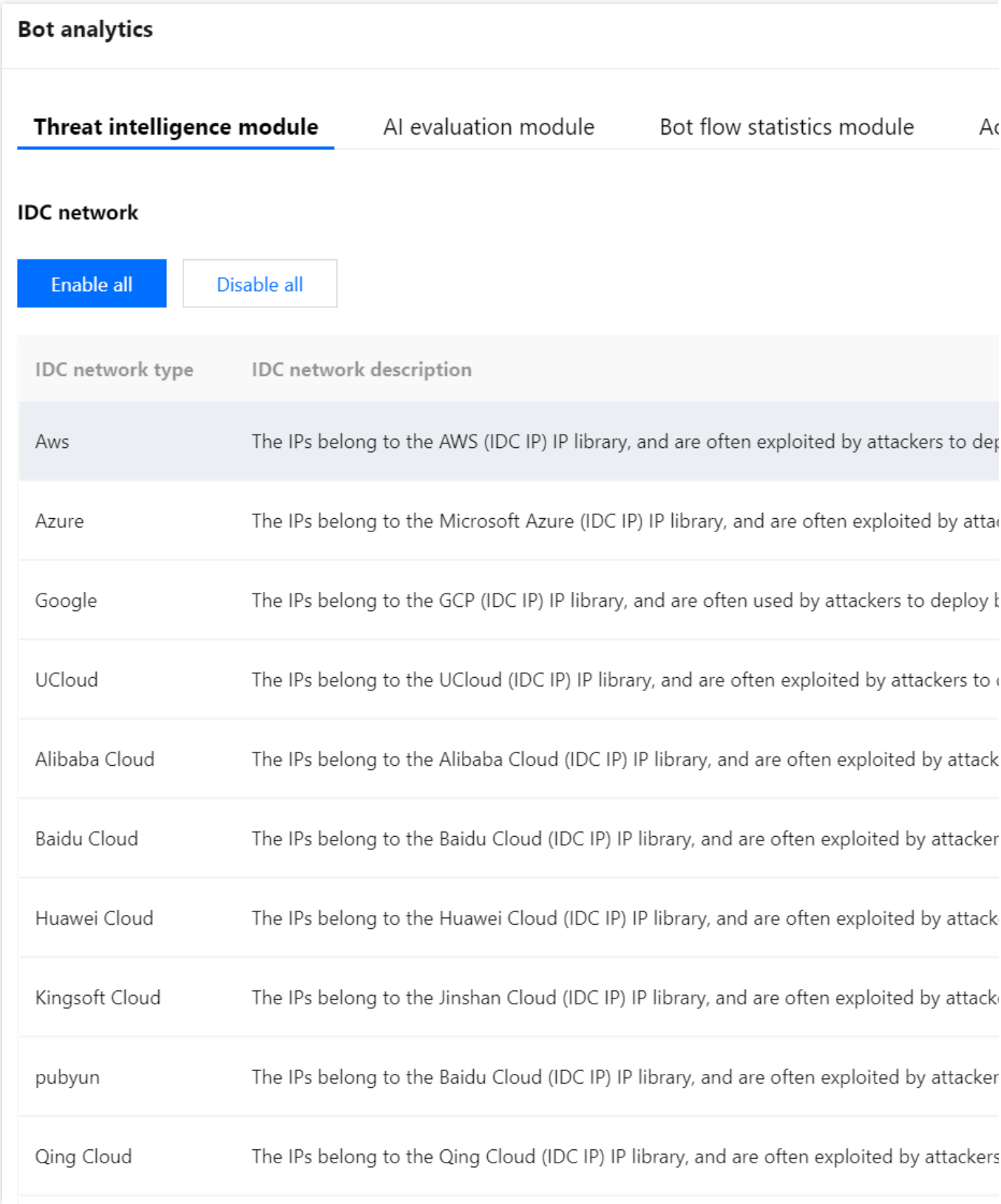
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击 **BOT 管理**。



3. 在全局设置中，单击威胁情报模块的**前往配置**，进入威胁情报配置页面，



4. 在威胁情报配置页面，可以配置识别项开关，也可以一键开启/关闭识别项的开关。



参数说明：

一键开启/关闭：一键开启/关闭当前类别下的规则开关。

IDC 类型：IP 归属于对应类型的 IP 库，这些 IP 段经常被爬虫用于部署爬虫程序或用作代理，而不会被正常用户使用。开启此识别项后，威胁情报模块将识别来自此 IDC 的访问源。

威胁情报库：

BOT 机器人：基于腾讯安全威胁情报提供的威胁情报，结合 WAF 实时检测出的爬虫 IP 源 IP 进行结合分析，得出的 IP 情报库，不会被正常用户使用。开启此识别项后，威胁情报模块将识别来自腾讯安全威胁情报中 BOT 机器人的访问源。

网络攻击：基于腾讯安全威胁情报提供的入站威胁情报 IP，这些 IP 在威胁情报存活有效期内发起大量攻击，存在大量恶意扫描行为，不会被正常用户使用。开启此识别项后，威胁情报模块将识别来自腾讯安全威胁情报中网络攻击的访问源。

网络代理：基于腾讯安全威胁情报提供的代理威胁情报，这些 IP 被爬虫/灰黑产利用，不会被正常用户使用。开启此识别项后，威胁情报模块将识别来自腾讯安全威胁情报中 BOT 机器人的访问源。

扫描器：腾讯安全威胁情报实时统计提供的全网恶意扫描行为攻击源 IP 情报库。开启此识别项后，威胁情报模块将识别来自腾讯安全威胁情报中网络代理的访问源。

账号接管：拥有该情报标签的 IP 过去一段时间内曾发起在线身份盗窃，账户爆破，撞库等攻击。开启此识别项后，威胁情报模块将识别来自腾讯安全威胁情报中账号接管攻击的访问源。

5. 配置完威胁情报模块之后，单击某场景配置页，单击威胁情报模块的

，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。

ToC 业务网站威胁情报配置最佳实践

概述

ToC 业务特性：2C 面对大量用户层，用户业务主要从住宅 IP/基站 IP 中发起。

注意：

部分业务存在回调接口，回调接口会从 IDC 侧发起访问。由于回调接口的量级为多个用户的集合。

业务相关调度接口可能从指定 IP/IDC 发起访问。

部分企业出口的用户会从 IDC 发起访问。

配置流程

1. 开启威胁情报开关。
2. 自定义会话策略配置从人机识别来自代理/ IDC 的访问。
3. 自定义会话策略配置回调接口地址/业务 IDC 地址进行信任操作，在确保网站安全的情况下，避免业务的 API 接口误拦截，影响业务。
4. APP /站点按情况接入，人机识别。

ToB 业务网站威胁情报配置最佳实践

ToB 业务特性：2B 面对大量业务，客户业务主要从 IDC/企业出口中发起。少数访问源为住宅 IP/基站 IP。

注意：

部分业务存在回调接口，回调接口会从IDC侧 发起访问。由于回调接口的量级为多个用户的集合。

业务相关调度接口从指定 IP/IDC 发起访问。

部分企业出口的用户会从住宅发起访问。

配置流程

1. 开启威胁情报开关，并将业务预期 IDC 的开关设置为关闭。
2. 自定义会话策略配置从人机识别来自住宅 IP 的访问。
3. 自定义会话策略配置回调接口地址/业务 IDC 地址进行信任操作，在确保网站安全的情况下，避免业务的 API 接口误拦截，影响业务。
4. A /站点按情况接入，人机识别。

智能统计

最近更新时间：2023-12-29 14:43:31

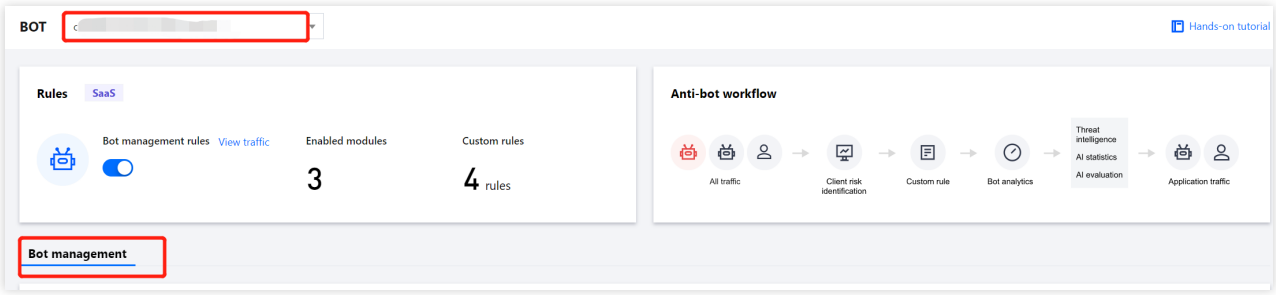
本文为您介绍 BOT 流量管理的智能分析中智能统计模块的功能设置。基于大数据分析统计和人工智能技术，根据客户用户群体的流量特征自动分类，区分正常用户和恶意用户。

前提条件

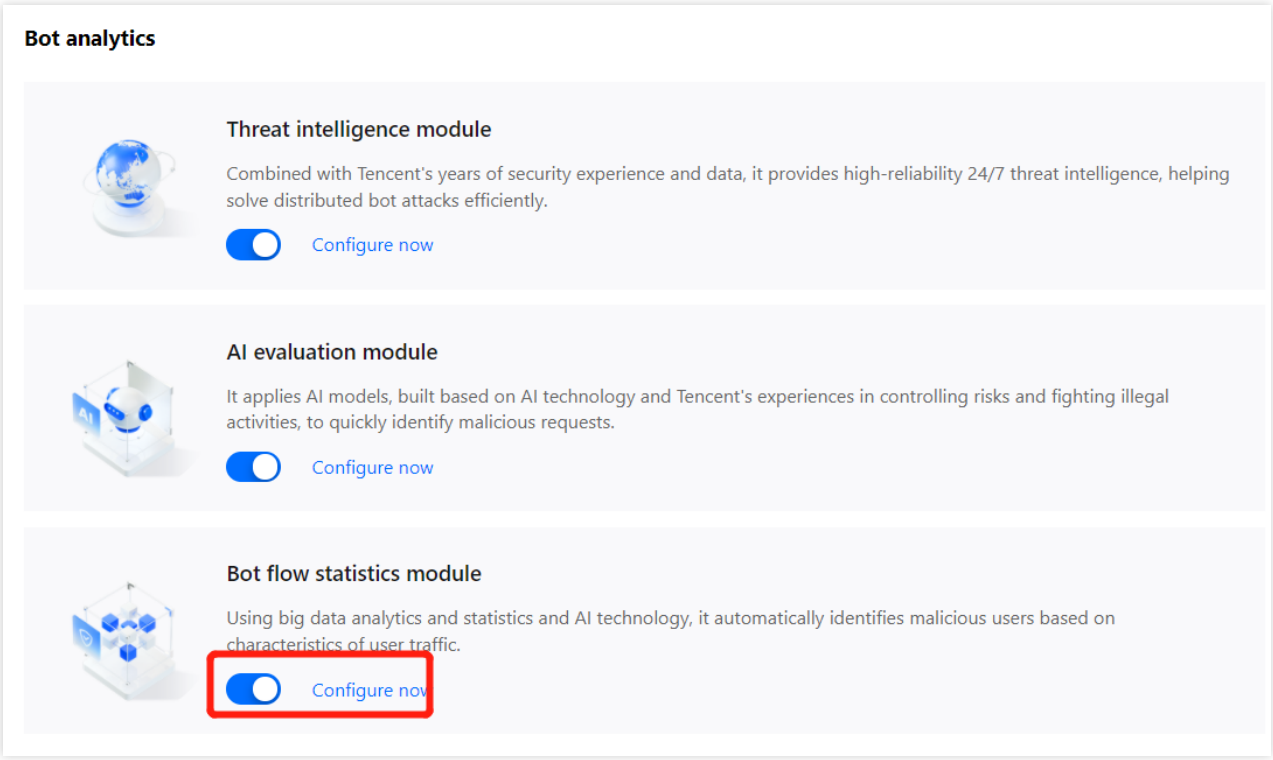
购买 Web 应用防火墙及 BOT 流量管理拓展包，并且打开已接入 WAF 域名 BOT 分析开关。

防护配置

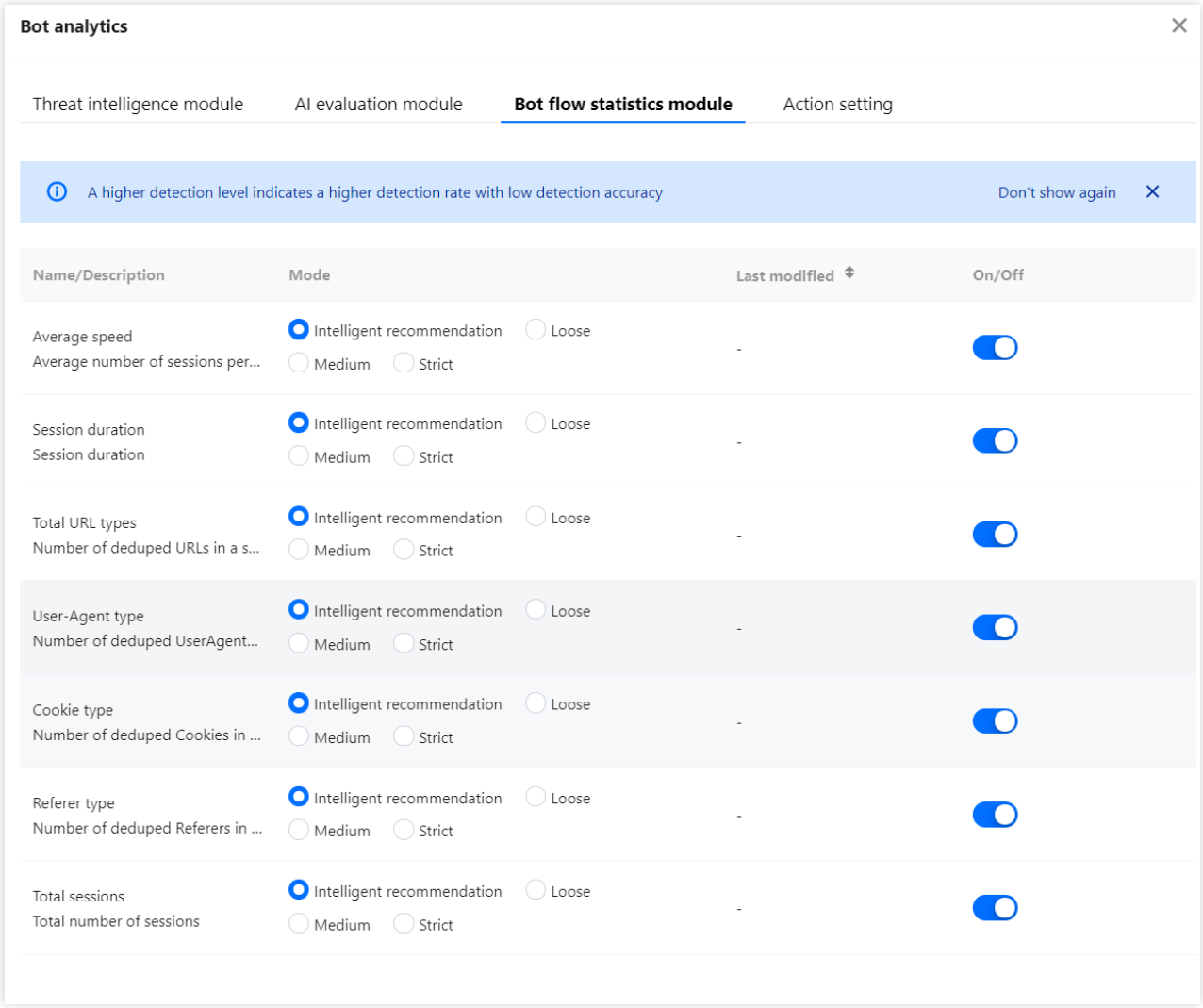
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**配置中心 > BOT 与业务安全**。
2. 在 BOT 与业务安全页面，左上角选择需要防护的域名，单击开启 **BOT 管理**。



3. 在全局设置中，单击智能统计模块的**前往配置**，进入前端对抗配置页。



4. 在智能统计页面中，可以配置不同特征的检出等级。



参数说明：

名称/描述：

Referer 种类：通过检出会话请求中 Referer 去重后的数目，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求。

URL种类：检出会话请求中 URL 去重后条目数，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求。

UserAgent 种类：检出会话请求中 UserAgent 去重后的数目，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求。

Cookie种类：检出会话请求中 Cookie 去重后的数目，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求。

会话总次数：检出会话发生的总访问次数，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求。

会话平均速度：检出会话平均访问速度，单位为：次/分钟，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求

会话持续时间：检出会话持续时间，通过不同等级的检出阈值，检出超出对应等级阈值的访问请求。

模式：不同检出等级代表不同的阈值，阈值随网站的访问水位浮动。

检出等级越高，检出率越高，检出精度有所下降。
检出等级越低，检出精度高，检出率会有所降低。
智能推荐等级为腾讯安全 BOT 流量管理通过自动化学习网站历史流量自动化生成推荐检出等级，该检出等级在宽松/中等之间随当前网站的 BOT 态势自动选择。
规则开关：可开启或关闭当前选项的检出类型。关闭检出项后，该检出项不贡献 BOT 分数值。
5. 配置完成智能统计相关配置之后，单击某场景配置页，单击智能统计模块的

，即可针对该场景开启智能统计模块。

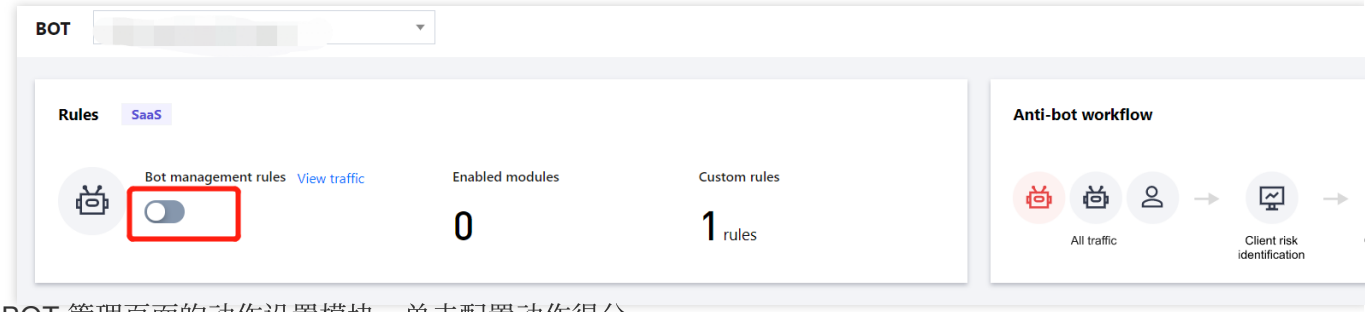
智能统计最佳实践

由于智能统计通过 BOT 对抗历史经验积累以及 BOT 攻防实验室相互积累运营，可快速发现异常的访问行为，因此建议在任何情况下开启智能统计，并将规则等级设置为智能推荐。

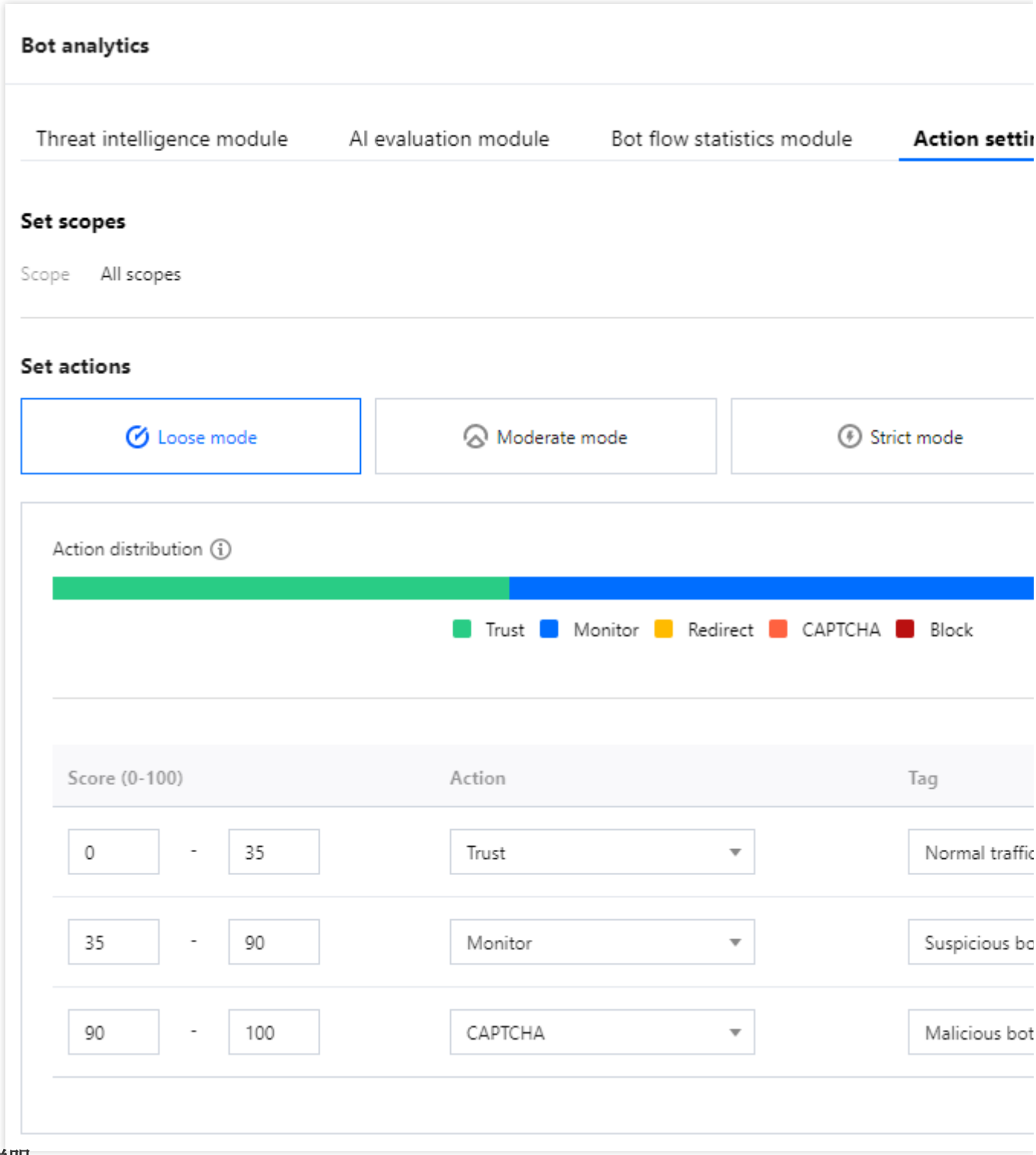
动作设置

最近更新时间：2023-12-29 14:43:44

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 管理页面的动作设置模块，单击配置动作得分。
4. 在动作设置页面，用户可通过配置不同动作策略、每个动作策略相应的生效范围和不同分数段的动作，来实现风险访问的精准拦截。



使用说明

动作策略：目前支持一个 BOT 场景下，支持多套动作策略。

生效范围：提供**全部范围**和**自定义范围**两个模式，命中生效范围的流量，再进一步根据配置的不同分数段的动作，精准拦截风险访问。

模式设置： 提供宽松模式、中等模式、严格模式、自定义模式四种默认处置模式，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：默认对网站友好/合法的 BOT。

疑似 BOT：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：识别访问流量为正常人类。

恶意 BOT：对网站产生恶意流量/访问请求不友好的 BOT。

5. 设置完成后，单击界面左下方的**立即发布**，即可生效。

BOT 流量分析

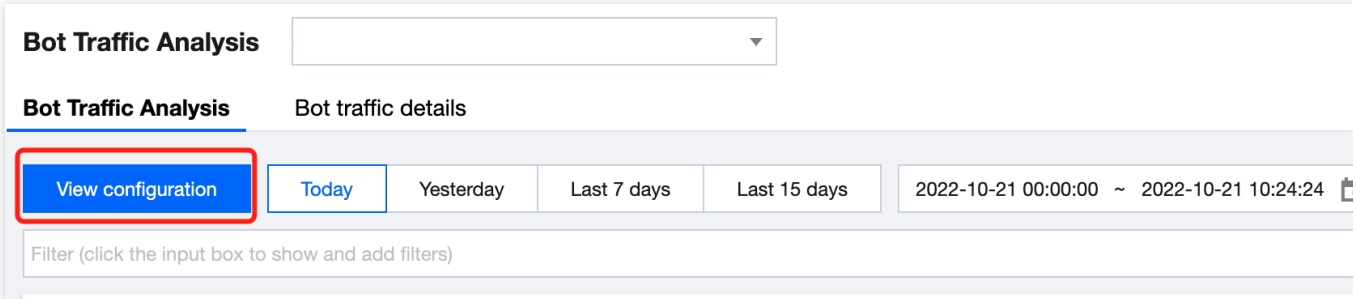
最近更新时间：2023-12-29 14:44:09

背景信息

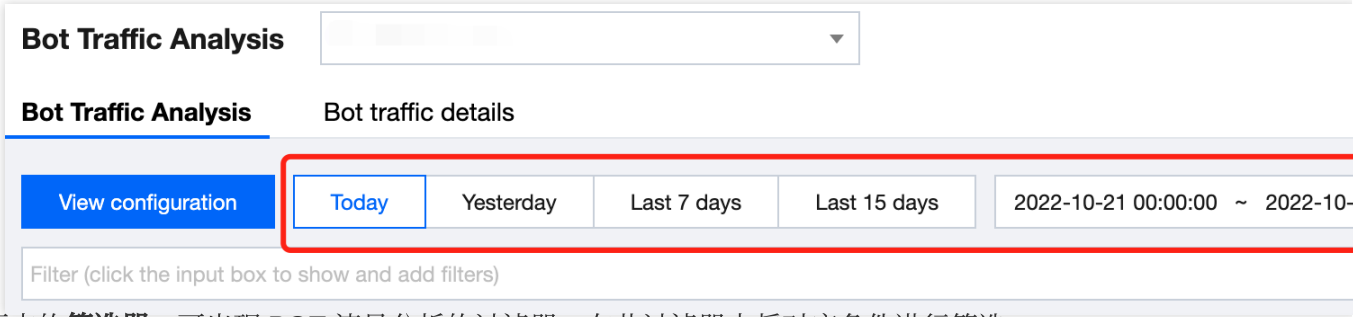
BOT 流量管理功能能够对友好及恶意机器人程序进行甄别分类，并采取针对性的流量管理策略。例如：放通搜索引擎类机器人流量；对恶意爬取商品信息流量采取不响应；减缓响应或差异化响应策略；应对恶意机器人程序爬取带来的资源消耗、信息泄露及无效营销问题，同时也保障友好机器人程序（如搜索引擎，广告程序）的正常运行。
BOT 流量分析通过采集 BOT 流量管理中的数据，可以快速了解选中，并开启了 BOT 流量分析的域名受 BOT 影响的情况，快速得知当前域名的 BOT 分类趋势、处置趋势、BOT 得分分布、请求量 TOP 统计以及 URL 易受侵害的资产 URL 列表。

操作步骤

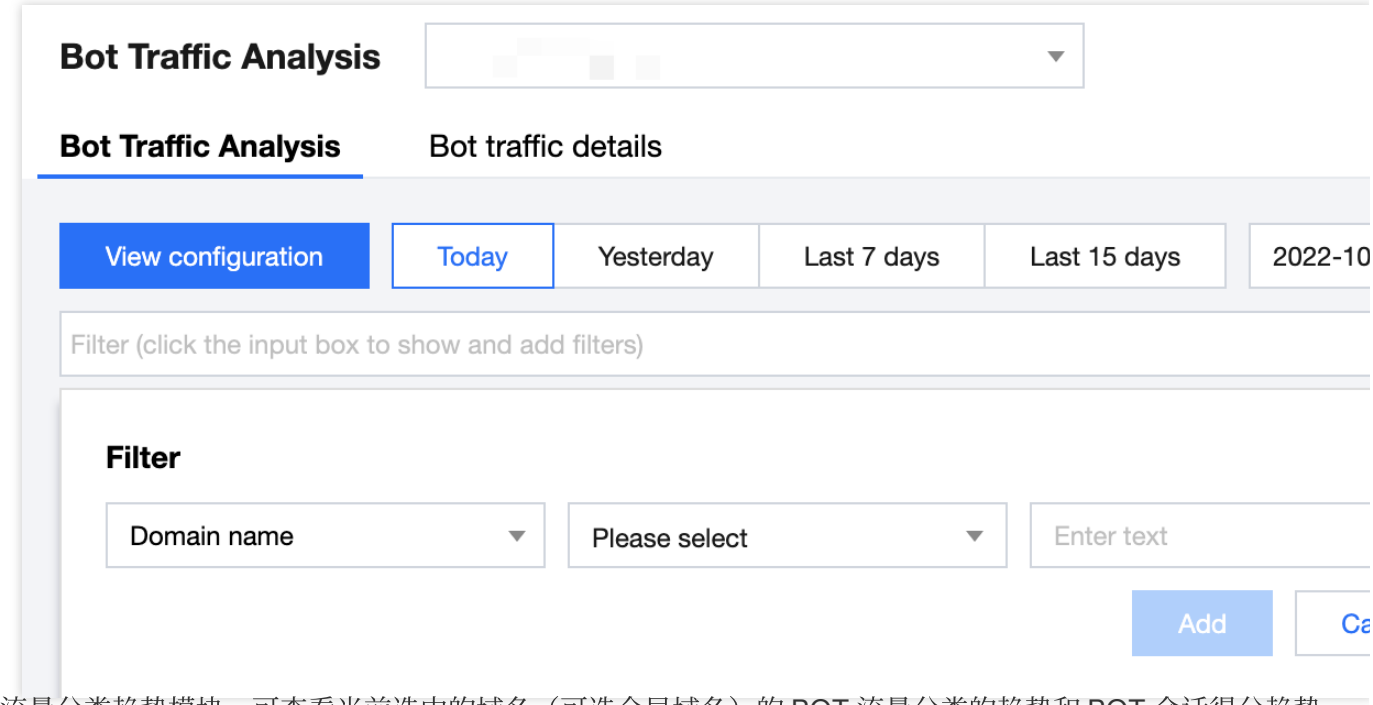
1. 登录 Web 应用防火墙控制台，在左侧导航栏中选择 **BOT 流量分析**。
2. 在 BOT 流量分析页面，单击左上角“全部域名”下拉框，选择要查看的域名。
3. 在选中非全部域名的情况下，单击左上角**查看配置**，会跳转至对应域名的 BOT 与业务安全页面。



4. 在 BOT 流量分析页面，可以通过时间或筛选器，搜索某个域名的防护数据。
通过指定的时间范围，搜索某个域名在查询时间范围内的 BOT 防护效果数据。

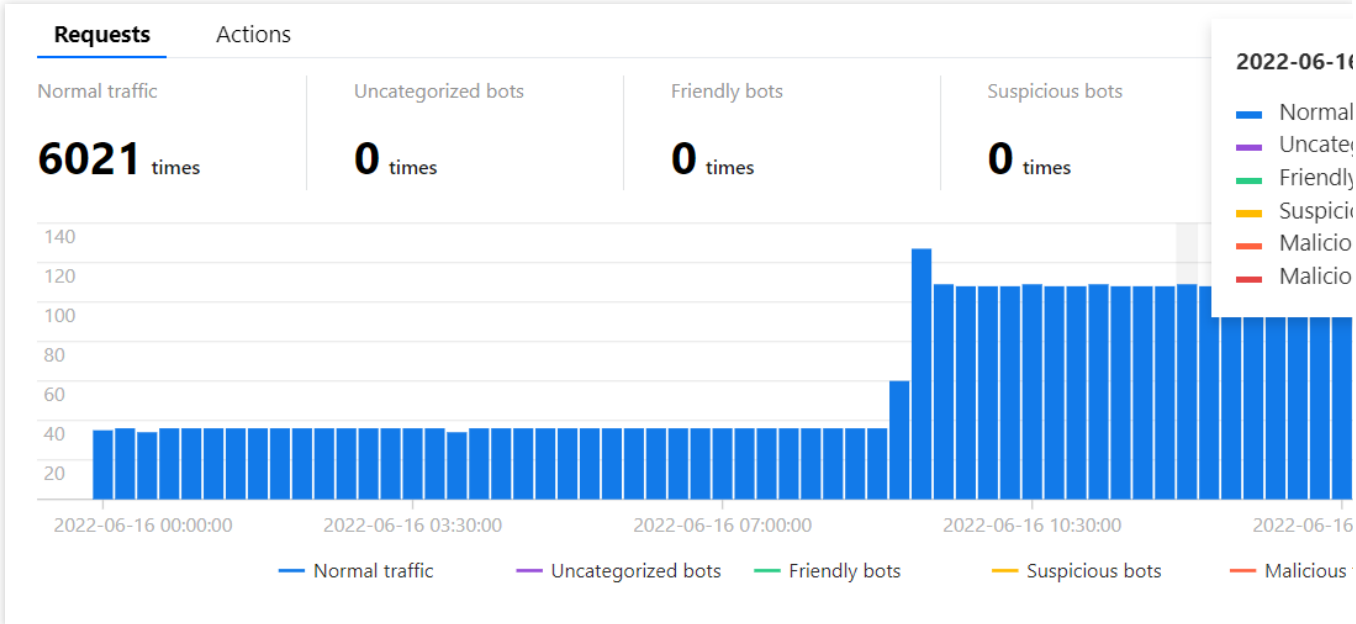


单击下方的**筛选器**，可出现 BOT 流量分析的过滤器，在此过滤器中将对应条件进行筛选。

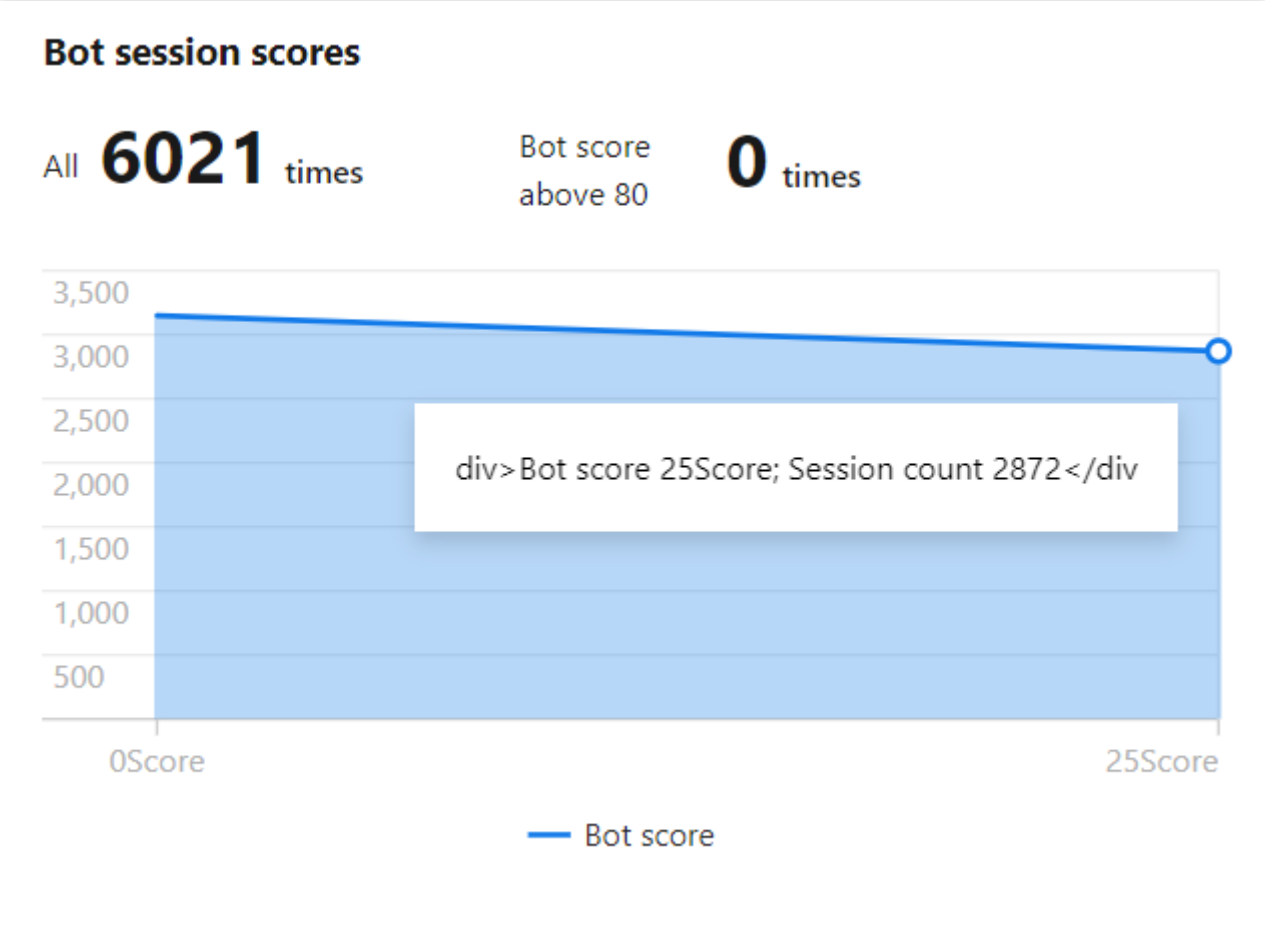


5. 在流量分类趋势模块，可查看当前选中的域名（可选全局域名）的 BOT 流量分类的趋势和 BOT 会话得分趋势。

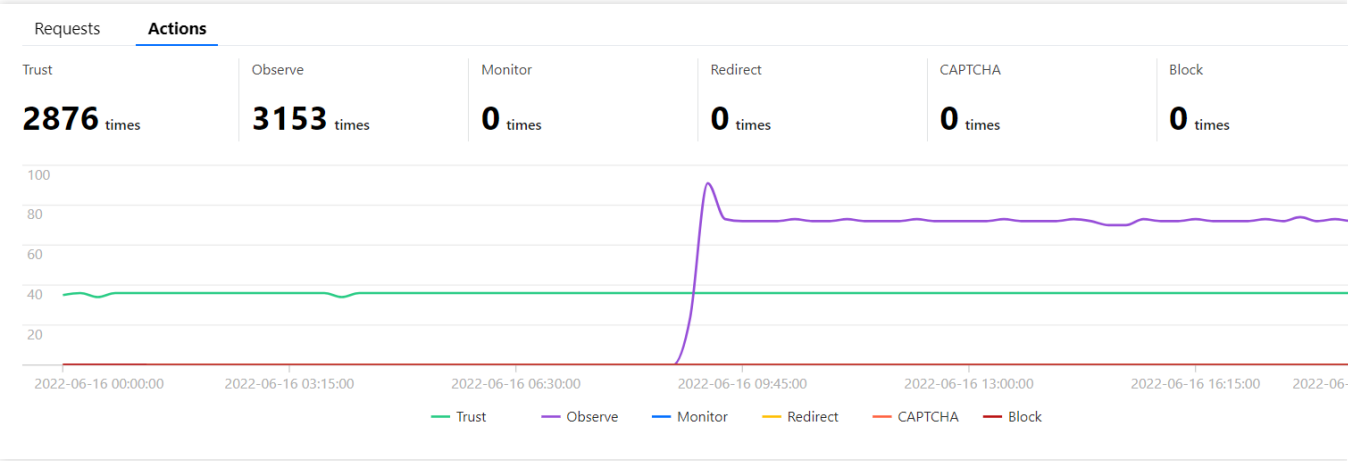
BOT 流量分类趋势：按照动作配置中相关动作的标签 BOT 得分进行不同分数段的分类，对每一个访问网站的流量请求进行打分并标记，展示到流量分类趋势图中。



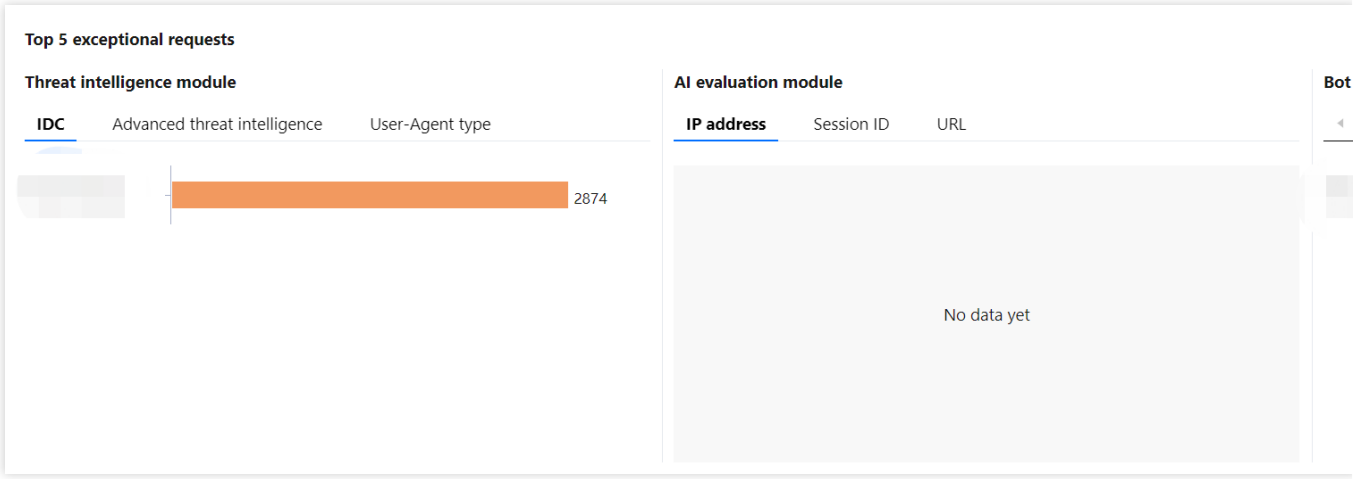
BOT 会话得分趋势：展示当前用户对应域名下的 BOT 流量风险分布图，用于展示用户当前的访问流量的趋势分布，用户可以根据趋势分布，在"BOT 分数"的动作设置中进行对应的处置。聚集的分数越高，受有害 BOT 影响越大。



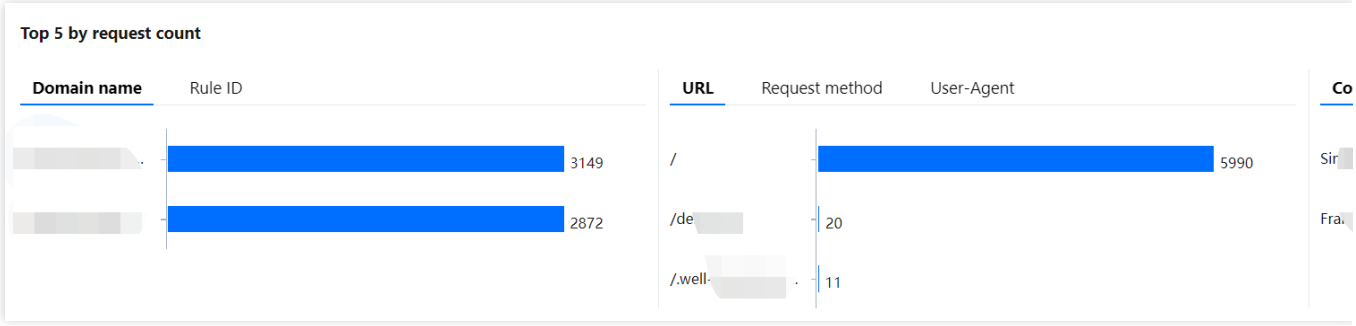
6. 单击**流量处置趋势**，可查看当前选中的域名（可选全局域名）在不同时间中 BOT 流量管理对流量的相关处置情况，以及整体的 BOT 对所有请求流量的处置动作占比。



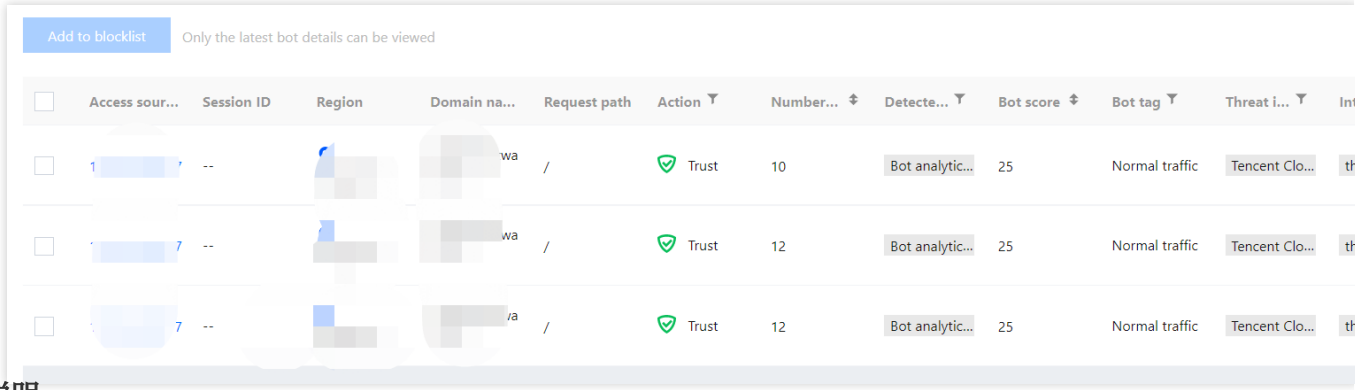
7. 在异常请求量 TOP5 统计模块，展示对应时间段内 BOT 的发现异常相关特征所统计出的 TOP5 键值及其数量。统计图受筛选器影响，受流量趋势对比图框选时间影响。单击对应的“柱状图”，会展示对应提示框，该提示框包含该键值的信息。单击**筛选**或**排除**，可以快速添加相关的过滤器。



8. 在请求量 TOP5 统计模块，展示对应时间段内 BOT 的相关特征，所统计出的 TOP5 键值及其数量。统计图受筛选器影响，受流量趋势对比图框选时间影响。单击对应的“柱状图”，会展示对应提示框，该提示框包含该键值的信息。单击**筛选**或**排除**，可以快速添加相关的过滤器。



9. 在受侵害资产统计列表，展示受到 BOT 影响最多的 URL 资产，以及 BOT 流量管理对其访问进行的处置，该聚合条目以5分钟聚合一次。



字段说明

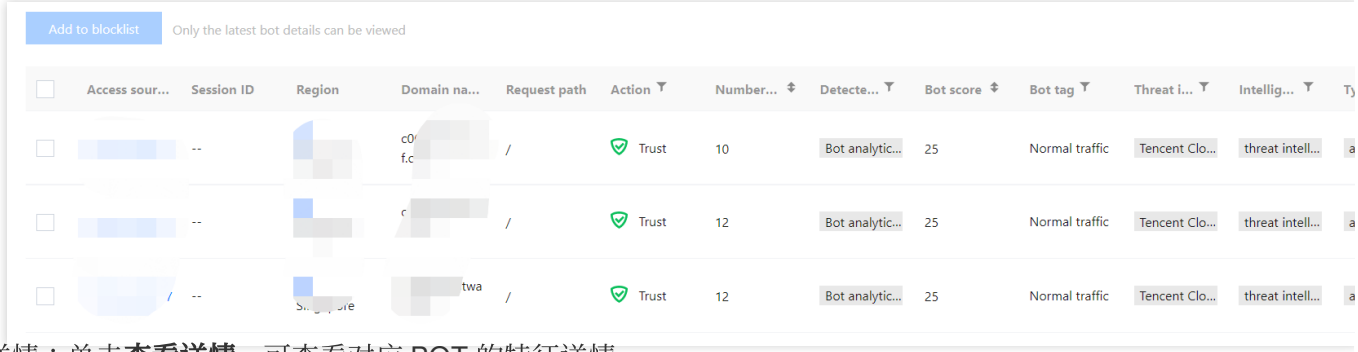
访问源：访问者来源。

会话：单次建联会话。

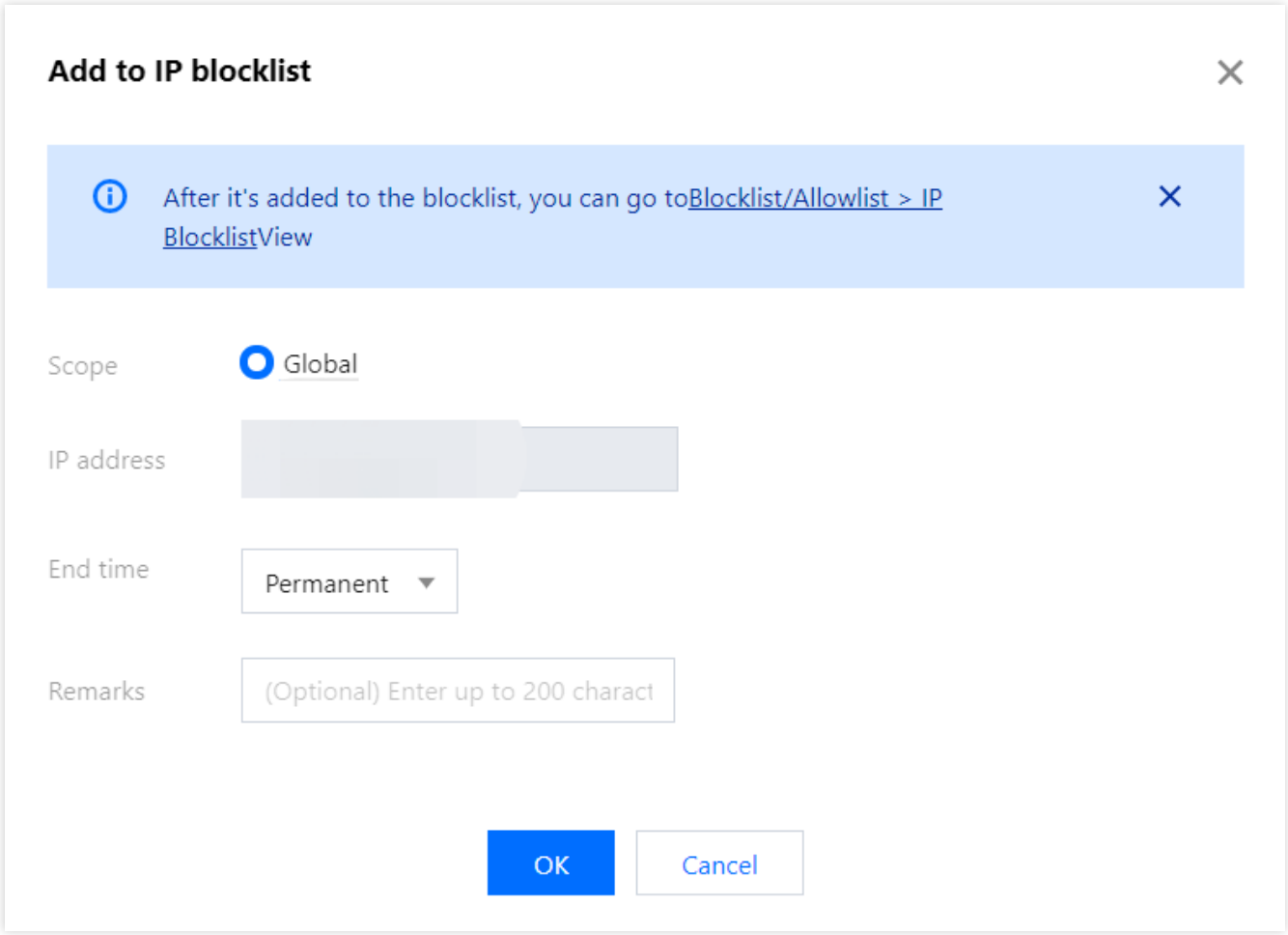
地区：访问者地理位置。

域名：访问的域名。

请求路径：访问请求的 URI。
处理动作：BOT 流量管理处置的动作。
访问次数：会话次数。
检出模块：命中了哪些模块。
BOT 得分：展示在该聚合维度下，当前访问请求的 BOT 得分信息。
BOT 标签：展示在该聚合维度下，当前访问请求命中的 BOT 标签。
威胁情报：当前 BOT 命中威胁情报中的匹配标签。
智能分析异常：展示在该聚合维度下，当前访问请求命中智能分析模块的异常。
统计特征异常：展示在该聚合维度想，智能统计发现特征的异常情况。
聚合时间：发现 BOT 访问的时间。
操作：
查看日志：单击**查看日志**，可查看对应 BOT 的访问日志。
说明：
需已 购买访问日志。



查看详情：单击**查看详情**，可查看对应 BOT 的特征详情。
加黑名单：单击**加黑名单**，配置相关参数单击**确定**，即可将对应访问源的 IP 加入黑名单。


Add to IP blocklist
After it's added to the blocklist, you can go toBlocklist/Allowlist > IP BlocklistView
Scope
Global
IP address
End time
Permanent
Remarks
(Optional) Enter up to 200 charact
OK
Cancel

BOT 流量详情

最近更新时间：2023-12-29 14:44:47

背景信息

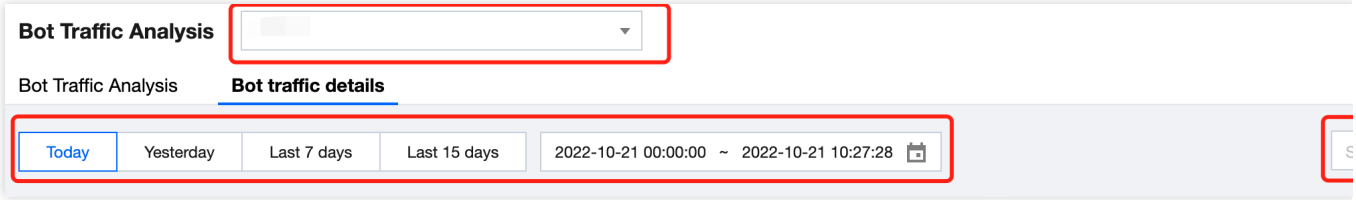
BOT 流量分析通过采集 BOT 流量管理中的数据，可以快速了解选中并开启了 BOT 流量分析的域名受 BOT 影响的情况，快速得知当前域名的 BOT 分类趋势、处置趋势、BOT 得分分布、请求量 TOP 统计以及 url 易受侵害的资产 url 列表，并可以通过单击**查看详情**，查看对应访问源的 BOT 详情，发现对应访问源的访问特征，以及访问源 BOT 异常的情况。
在 BOT 流量详情中，可以快速发现已开启 BOT 流量分析功能中，流量 TOP10的访问源，如果配置了会话设置，还可以查看到访问流量TOP10 的会话访问信息，快速查看选中访问源的详情与日志。同时，可以通过定向检索对应的访问源/IP 的信息。

前提条件

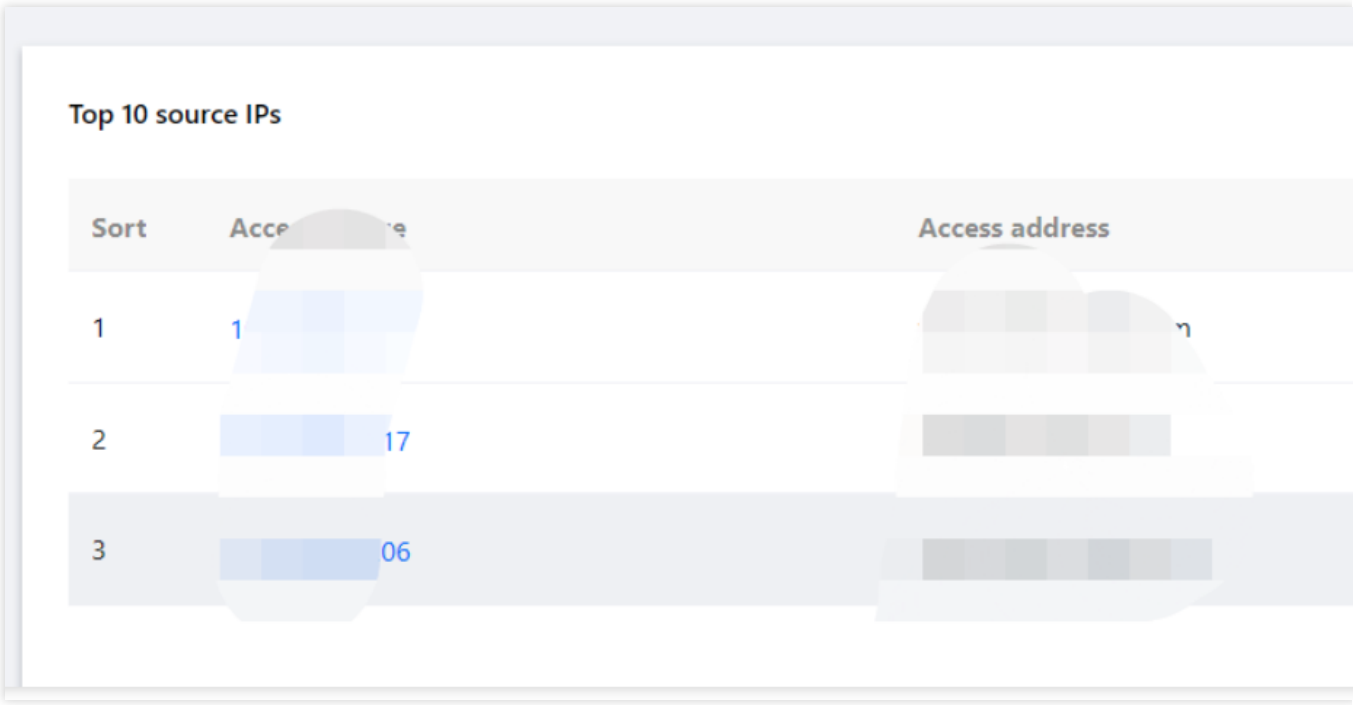
购买 WAF 并购买 BOT 流量管理扩展包 后，开启 BOT 流量分析。

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 > BOT 流量详情**。
2. 在 BOT 流量详情页面，单击左上角“全部域名”下拉框，选择要查看的域名。
3. 在 BOT 流量详情页面，可以通过时间或筛选器，搜索全部域名或某个域名的 TOP10流量信息，并可以快速进入相关的日志中。

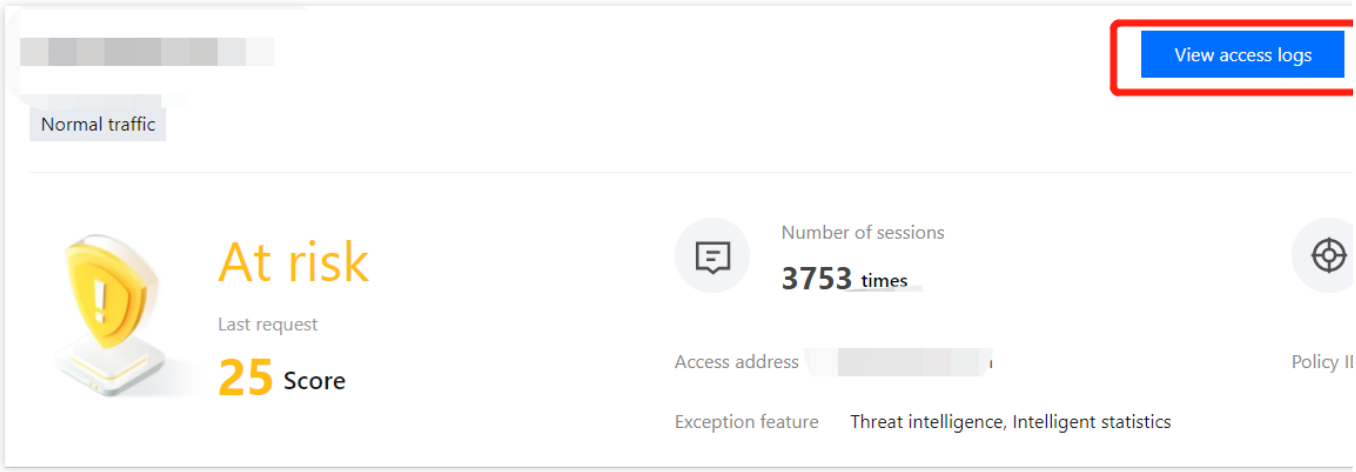


4. 在BOT 流量详情页面，选择所需访问源，单击**查看详情**，即可进入该访问源的详情页面。



查看概览

在详情页面的概览模块中，展示访问源风险值与命中策略信息，并可以通过查看访问日志、加白名单、加黑名单、加自定义规则，对该访问源进行快速定向处置。



字段说明：

IP 地址与标签：访问源的 IP 基础信息及命中的标签信息。

最后一次请求得分：该访问源最近一次访问时，BOT 识别出来的访问分数以及当前访问风险的情况。

会话次数：展示最近的一次连续会话中，该访问源访问网站的总次数，该总次数统计与右侧 BOT 动作统计数会有不同，此处展示当前访问源在最近一次访问会话的会话次数。

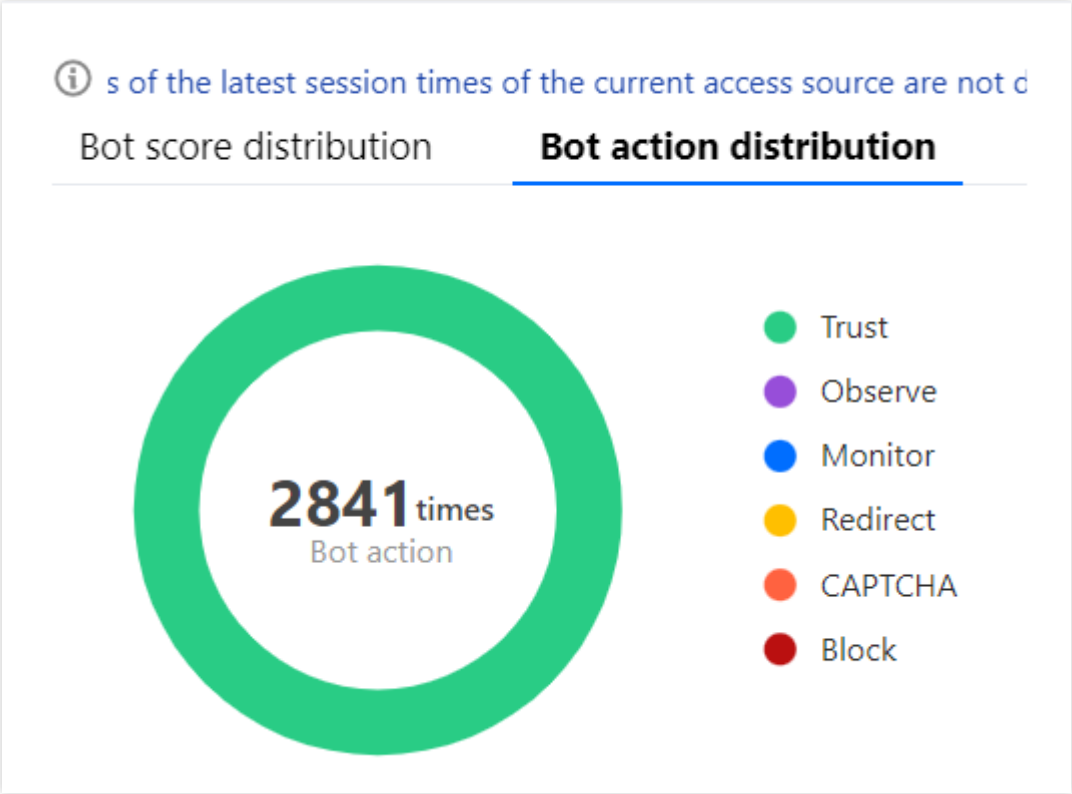
访问目的：展示该访问源的访问域名。

异常特征：展示该访问源出现异常特征的模块。

命中模块：最近一次产生处置动作时，产生动作的模块。
策略 ID：展示该访问源命中的策略 ID。
查看访问日志：可跳转至访问日志页面，查看该访问源的访问详情。
加白名单：可将该访问源加入白名单。
加黑名单：可将该访问源加入黑名单。
添加自定义规则：可添加该访问源的自定义规则。

查看 BOT 得分与占比

在详情页面的 BOT 得分与占比模块中，展示在已选中的访问时间段内，访问源的 BOT 动作占比与 BOT 的得分分布。通过 BOT 得分分布可以快速发现当前访问源整体的威胁程度。

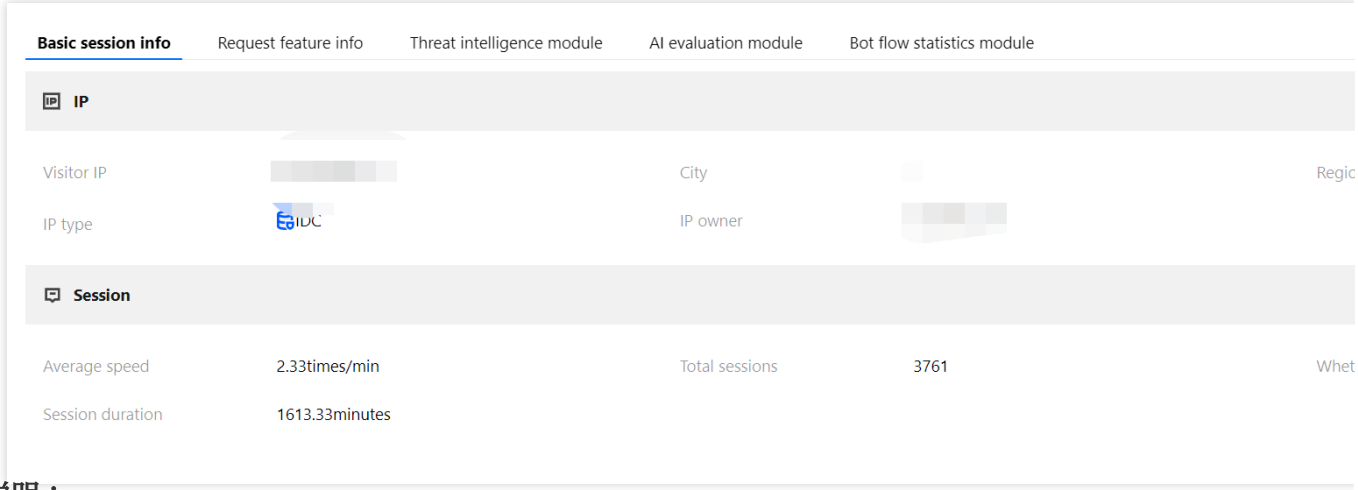


查看 BOT 信息

在详情页面的 BOT 信息模块中，展示了访问源 BOT 的基础特征信息、请求特征信息、威胁情报信息、AI 评估信息、智能统计、会话等特征信息。通过这些特征信息，可以快速发现当前访问请求存在异常，发现不同访问源中的不同的地方，快速定向处置此类 BOT。

基础会话信息

在基础会话信息页签，展示当前访问源的 IP 基础信息以及基础会话信息，当展示的维度为会话 ID 维度时，不展示 IP 基础信息。



字段说明：

IP 基础信息

访问源 IP：当前访问源的 IP 地址。

城市：当前访问源的归属城市。

IP 地区：当前访问源归属的国家。

IP 类型：当前访问源的 IP 类型。

IP 所有者：当前访问源的 IP 所有者。

会话基础信息

会话平均速度：当前访问源在最新的一次会话中的会话平均速度，为会话请求总次数/会话持续时间，单位为：次/分钟。

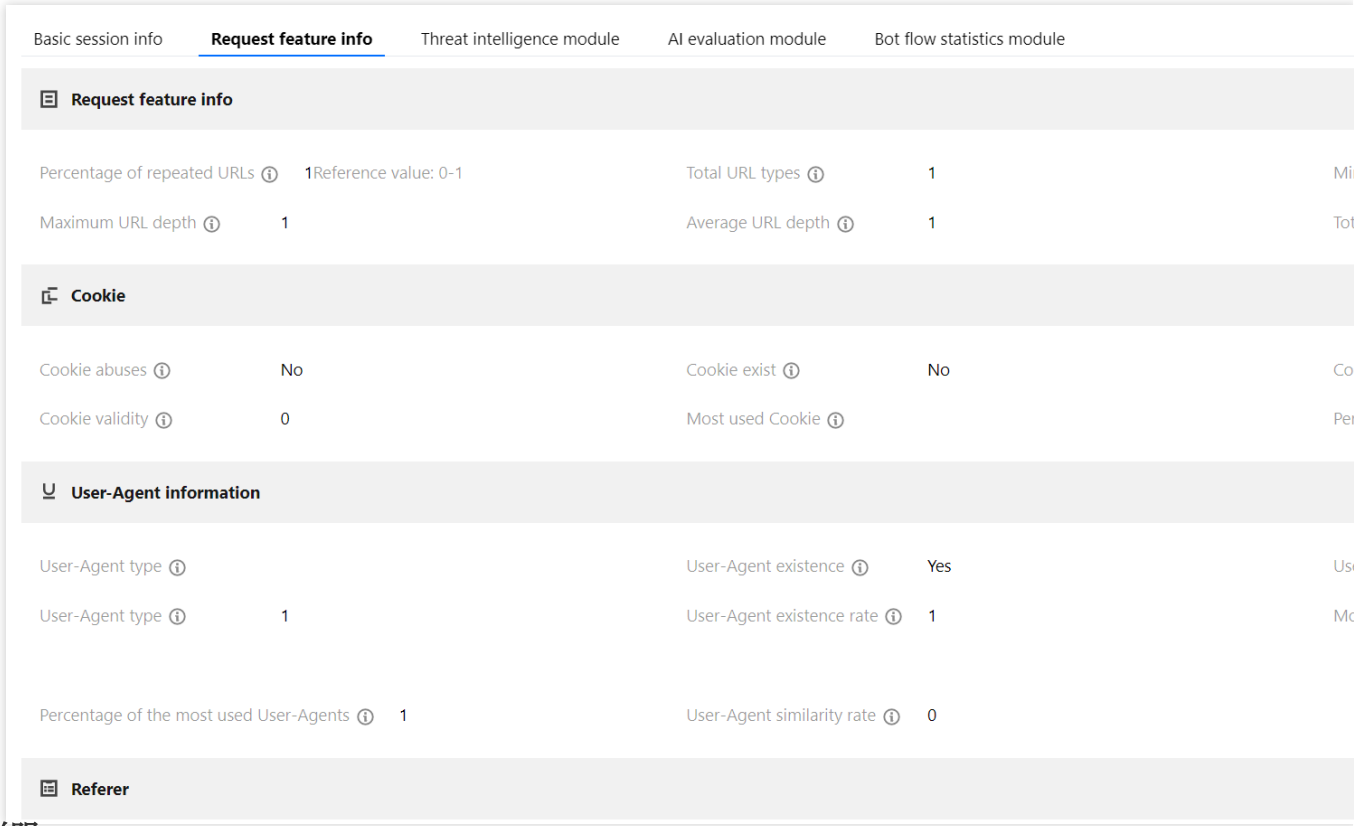
会话总次数：当前访问源在最新的一次会话中的会话总次数。

是否存在 Robots.txt：当前访问源在最新的一次会话中，当前访问源是否访问过 Robots.txt 文件，通常访问此文件的会话均为爬虫机器人的会话。

会话持续时间：当前访问源在最新的一次会话中，最近一次会话的访问持续时长。

请求特征信息

在请求特征信息页签，展示当前会话请求中请求特征信息、Cookie 信息、User-Agent 信息、Referer 信息、Query 信息。



字段说明：

信息类型	信息名称	信息详情
请求特征信息	URL 重复比	会话请求中 URL 重复比例，取值范围0 - 1，根据实际业务情况，进行参数配置，过高或过低为疑似异常（根据实际情况进行判断）。
	URL 种类	会话请求中 URL 去重后条目数。会话请求中 URL 去重后条目数。
	URL 最小深度	会话请求中 URL 的最小层级。会话请求中 URL 最小的栏目层级。
	URL 最大深度	会话请求中 URL 的最大层级数。会话请求中 URL 最大的栏目层级。
	URL 平均深度	会话请求中 URL 的平均层级数。会话请求中 URL 平均的栏目层级。
	URL 数量	会话请求中的访问的 URL 总数（未去重）。
Cookie 信息	Cookie 是否滥用	多种不同的 UA 使用相同的 COOKIE。
	Cookie 存在性	会话请求中 COOKIE 是否存在。
	Cookie 重复性	会话请求中 COOKIE 的重复比例，取值范围0 - 1。

	Cookie 有效率	会话请求中 COOKIE 能正常解析的比例。
	出现最多的 Cookie	会话请求中出现最多的 COOKIE。
	出现最多的 Cookie 比例	会话请求中出现最多的 COOKIE 占比。
User-Agent 信息	User-Agent 类型	会话请求中访问用户的 User-Agent 类型。
	User-Agent 存在性	会话请求中，判断 HTTP 头部字段是否存在 User-Agent。
	User-Agent 随机性指数	会话请求中 UA 的随机分布情况，取值范围0 -1，指数越高越异常。参考值阈值：超过0.6疑似异常，指数超过0.92基本确定为异常。
	User-Agent 种类	会话请求中 UA 去重后的数目，过多疑似异常（根据实际情况进行判断），对非代理 IP 有效。
	User-Agent 有效比	会话请求中 UA 的存在比例，取值范围0 - 1，过低疑似异常（根据实际情况进行判断）。
	出现最多的 User-Agent	会话请求中，HTTP User-Agent 字段出现最多的值。
	出现最多的 User-Agent 占比	会话请求中，HTTP User-Agent 字段出现最多的值在总体流量中所占的比例。
	User-Agent 相似性比例	会话请求中，HTTP User-Agent 字段出现最多的值与其余访问请求的相似度。
Referer 信息	Referer 重复比	会话请求中 Referer 的重复比例，取值范围0 - 1，对浏览器访问有效，过高疑似异常（根据实际情况进行判断）。
	Referer 存在比	会话请求中 Referer 存在比例，取值范围0 - 1，对浏览器访问有效，过低疑似异常（根据实际情况进行判断）。
	Referer 有效比	会话请求中 Referer 有效比例，取值范围0 - 1，对浏览器访问有效，过低疑似异常（根据实际情况进行判断）。
	Referer 是否滥用	在同一会话请求内多种不同的 UA 使用相同的 Referer。
	出现最多的 Referer	会话请求中，HTTP Referer字段出现最多的值。
	出现最多的 Referer 的比例	会话请求中，HTTP Referer 字段出现最多的值在请求中的占比。

Query 信息	请求参数比	会话请求中 GET 请求参数（Query 内容）或 POST 请求参数（Body 内容）重复比例，取值范围0 - 1，根据实际业务情况，进行参数配置，过高或过低疑似异常（根据实际情况进行判断）。
	请求参数种类	会话请求出现最多的参数，包括 GET 请求参数（Query 内容）或 POST 请求参数（Body 内容）。

威胁情报

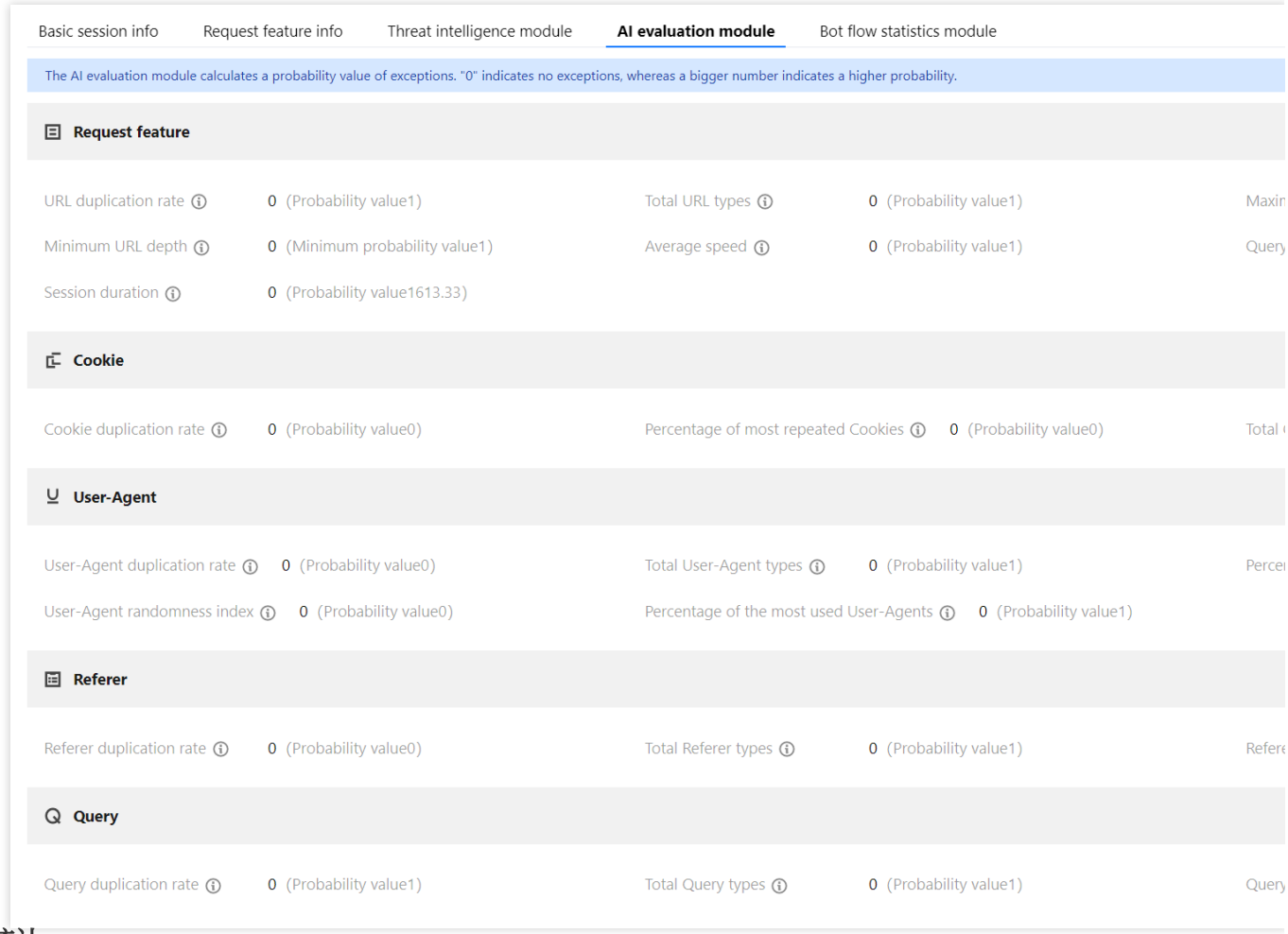
在威胁情报页签，如果当前访问源 IP/会话 ID 命中了威胁情报的相关信息，将会展示访问源的 IDC 详情以及命中的威胁情报信息。

IDC 详情：如果访问源的信息中包含 IDC 的，会展示当前的 IDC 信息。

威胁情报：如果访问源的 IP 信息中包含威胁情报信息的，会展示当前访问源的威胁情报命中的标签以及命中的标签对应的释义。

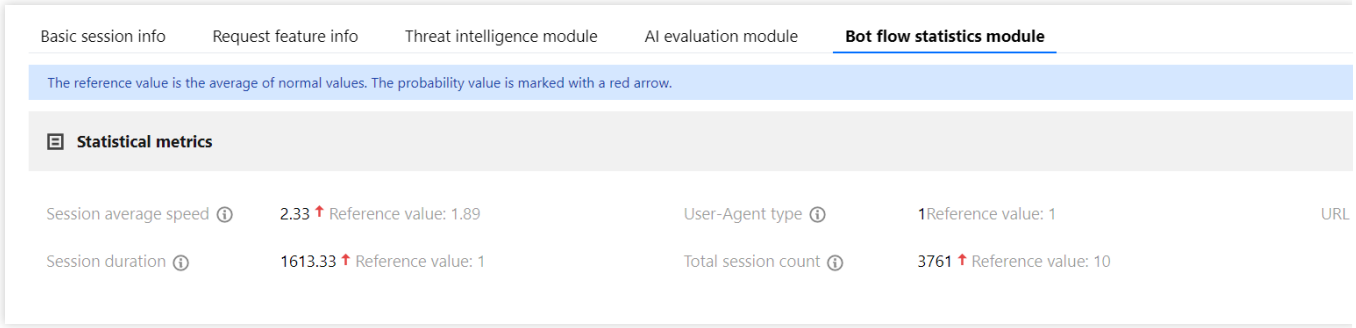
AI 评估

在 AI 评估页签，会展示当前会话请求中，各个维度的异常特征信息异常度以及对应指标特征值，展示内容请求包含请求特征异常信息、Cookie 异常信息、User-Agent 异常信息、Referer 异常信息、Query 异常信息。在 AI 评估中 AI 得出的异常度大于0，即为 AI 评估发现异常的特征参数。



智能统计

在智能统计页签，会展示当前会话请求中，最新一次智能统计出来的各个维度的异常特征信息以及对应特征的当前的特征值，以及正常的客户端的特征阈值为多少。



字段说明：

信息名称	信息详情
会话平均速度异常	当前会话的平均速率特征值出现异常。若会话平均速率异常则会展示当前会话的异常值数量，并且会展示当前域名中，异常访问会话该特征的临界值。
User-Agent种类异常	当前会话的 User-Agent 种类特征值出现异常。若会话 User-Agent 种类异常则会展示

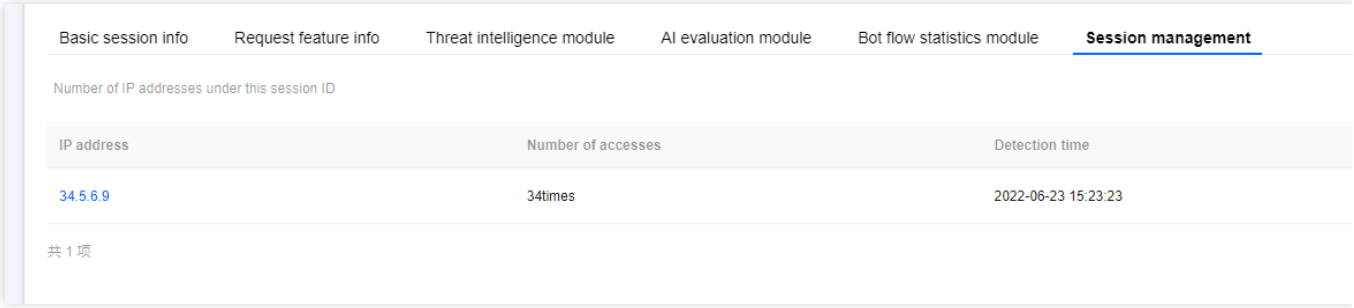
	当前会话的 User-Agent 种类异常值数量，并且会展示当前大盘中，异常访问会话该特征的临界值。
URL种类异常	当前会话的 URL 种类特征值出现异常。若会话 URL 种类异常则会展示当前会话的 URL 种类异常值数量，并且会展示当前大盘中，异常访问会话该特征的临界值。
会话持续时间异常	当前会话的持续时间特征值出现异常。若会话持续时间异常则会展示当前会话的异常持续时间，并且会展示当前大盘中，异常访问会话该特征的临界值。
会话总次数异常	当前会话的总次数特征值出现异常。若会话总次数异常则会展示当前会话的异常访问总次数的数量，并且会展示当前域名中，异常访问会话该特征的临界值。

会话管理

在会话管理页签，会展示当前会话访问的 IP 地址，以及在每个 IP 地址中的访问次数，并可通过当前的访问信息，查看当前的会话 ID 的历史访问 IP 的访问日志。

说明：

当配置了会话设置，并且流量中包含会话设置的内容的情况下，会展示会话管理选项。



黑白名单防护设置
功能简介

最近更新时间：2023-12-29 14:45:06

腾讯云 Web 应用防火墙的黑白名单功能，指的是对经过 Web 应用防火墙防护域名的访问源 IP 进行黑白名单设置，以及对多个 HTTP 特征进行精准白名单设置，主要功能包括： IP 黑白名单设置和精准白名单设置。

IP 黑白名单设置，支持设置基于域名或全局的 IP 黑白名单规则，支持网段设置。

精准白名单设置，支持从 HTTP 报文的请求路径、GET 参数、 POST 参数、 Referer 和 User-Agent 等多个特征进行组合，通过特征匹配来对特定公网用户的访问进行加白。

同时，可以添加基于域名的黑白名单或基于全局的黑白名单，生效优先级说明如下所示：

黑白名单的优先级仅低于 Web 应用防火墙精准白名单策略，高于其他检测逻辑。

黑白名单优先级从高到低顺序：精准白名单策略 > 全局白名单 > 域名白名单 > 域名黑名单 > 全局黑名单 > WAF 其他模块。

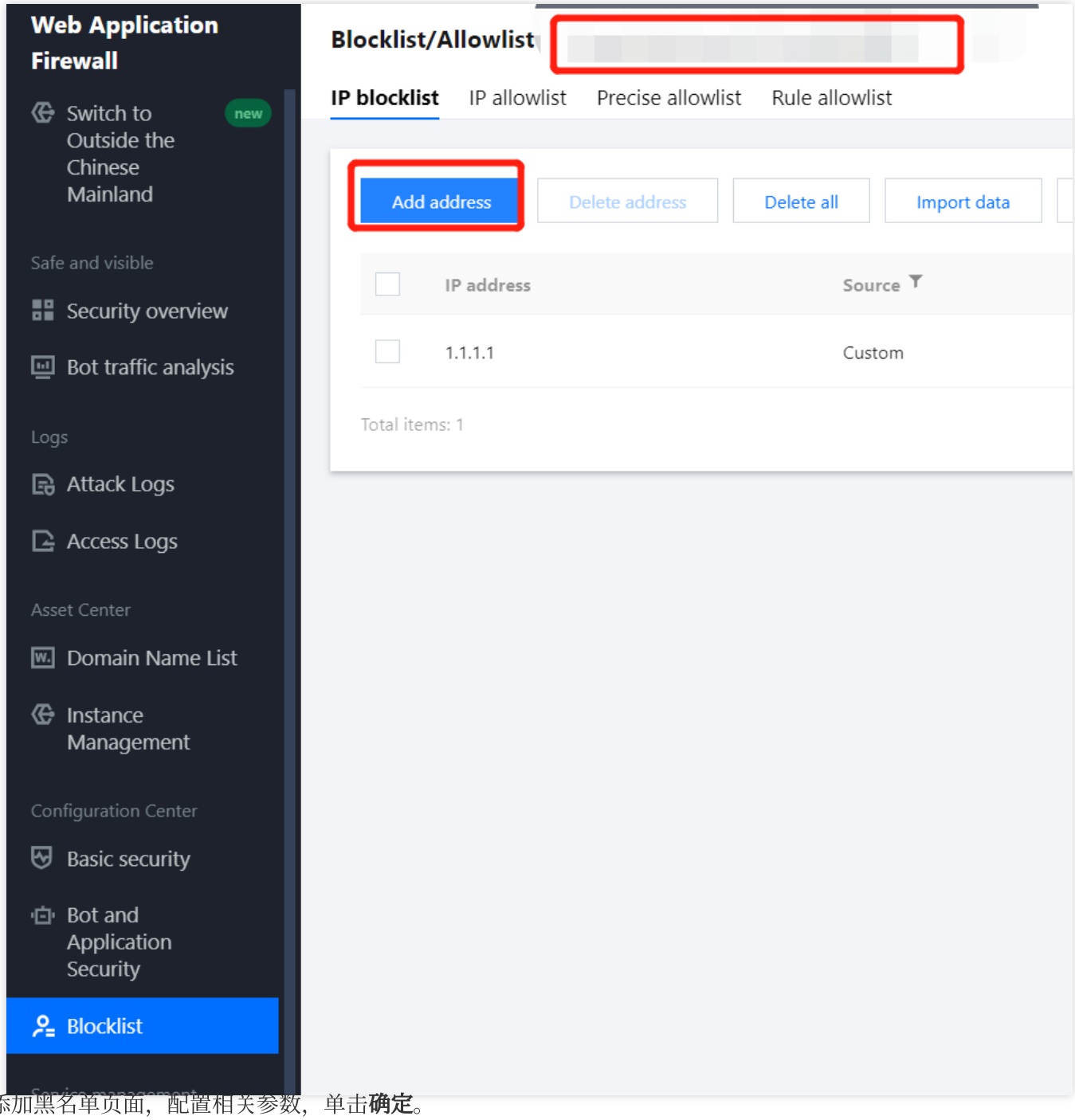
IP 黑名单

最近更新时间：2023-12-29 14:45:20

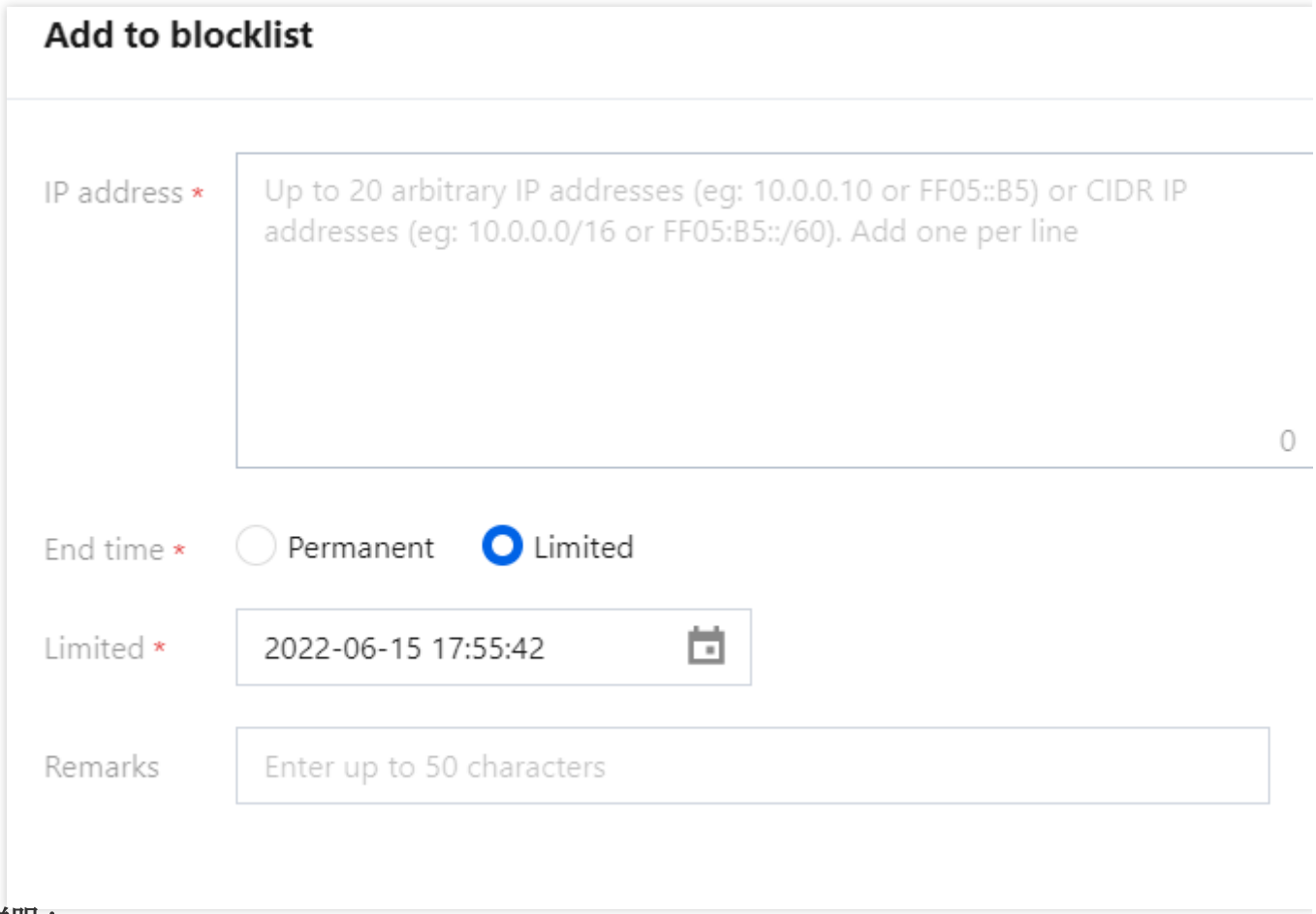
添加 IP 黑名单

手动添加

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心 > 黑白名单**，进入黑白名单页面。
2. 在黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**，进入 IP 黑名单页面。
3. 在 IP 黑名单页面，单击**添加地址**，进入添加黑名单页面。



4. 在添加黑名单页面，配置相关参数，单击**确定**。



字段说明：

IP 地址：支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或 FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。

说明：

选择域名为 ALL 时，添加的 IP 地址或 IP 段为全局的黑白名单。

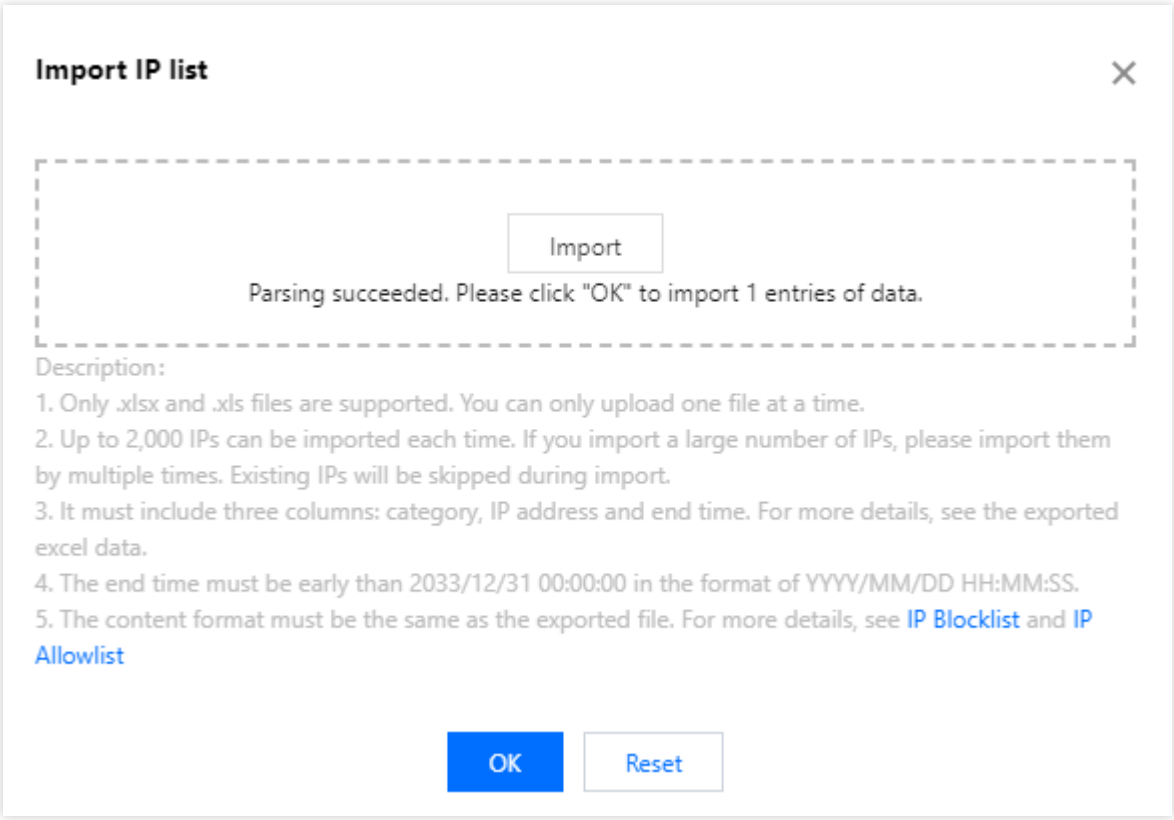
各个版本每个域名规格限制为：高级版1000条/域名、企业版5000条/域名、旗舰版:20000条/域名，每个 IP 地址或者 IP 段占用一条额度。

截止时间：永久生效或限定日期。

备注：自定义，50个字符以内。

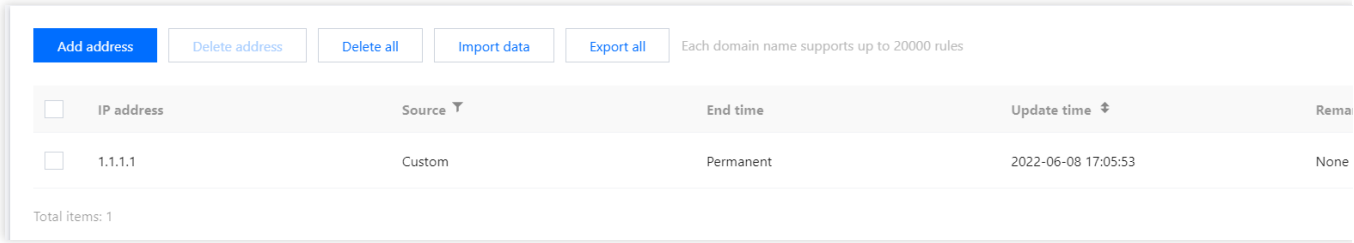
导入数据

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**，进入 IP 黑名单页面。
2. 在 IP 黑名单页面，单击**导入数据** > **导入**，解析成功后，单击**确认导入**即可。



编辑 IP 黑名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**，进入 IP 黑名单页面。
2. 在 IP 黑名单页面，选择所需 IP 地址，单击操作列的**编辑**，修改截止时间和备注，单击**确定**保存。



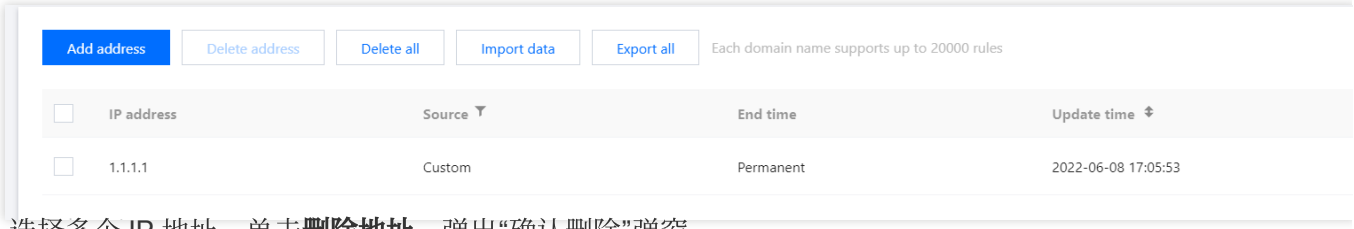
删除 IP 黑名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**，进入 IP 黑名单页面。
2. 在 IP 黑名单页面，支持删除单个、部分、全部地址，具体操作如下：

单个：选择单个 IP 地址，单击**删除地址**或操作列的**删除**，弹出“确认删除”弹窗。

说明：

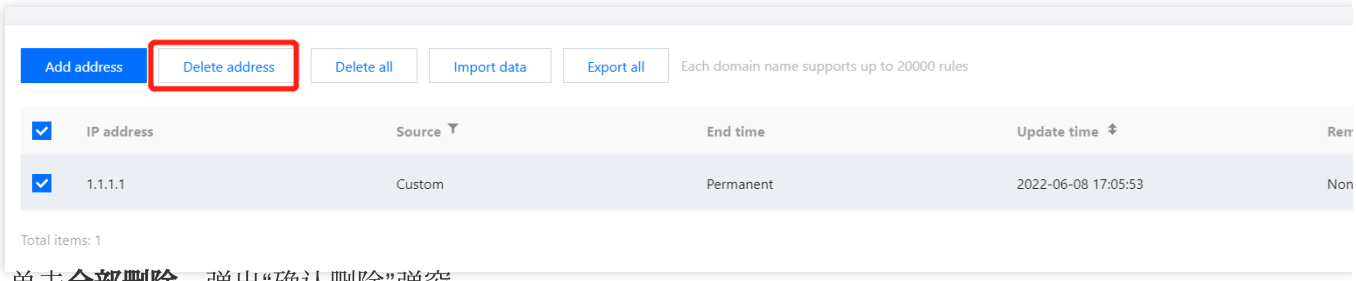
删除后将无法恢复，重新添加才能生效。



部分：选择多个 IP 地址，单击**删除地址**，弹出“确认删除”弹窗。

说明：

删除后将无法恢复，重新添加才能生效。



全部：单击**全部删除**，弹出“确认删除”弹窗。

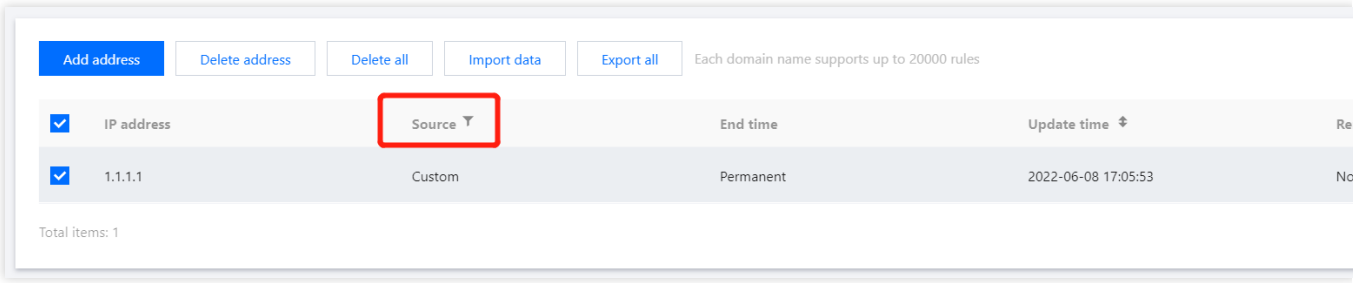
注意：

将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

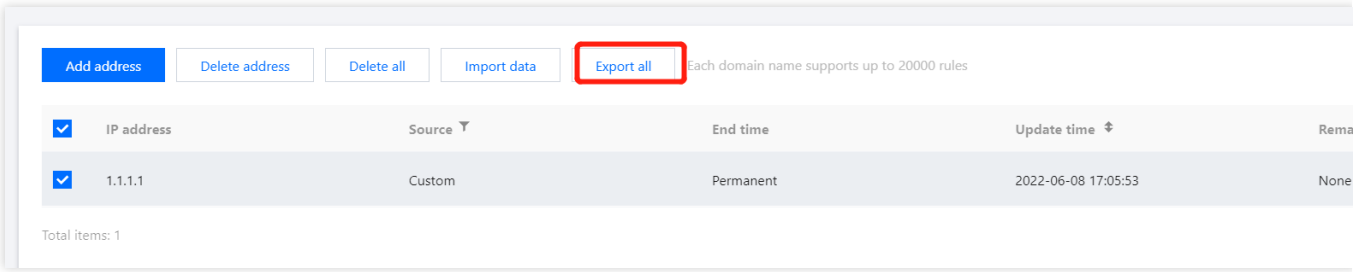
3. 在“确认删除”弹窗中，单击**确定**，即可删除地址。

导出全部筛选结果

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 黑名单**，进入 IP 黑名单页面。
2. 在 IP 黑名单页面，单击搜索框通过 **IP 地址**对 IP 进行筛选，或单击**来源**根据来源分类对 IP 进行筛选。



3. 筛选完所需 IP 后，单击**导出全部筛选结果**，即可导出所需的 IP 筛选结果。


Add address
Delete address
Delete all
Import data
Export all
Each domain name supports up to 20000 rules
IP address
Source
End time
Update time
Rema
1.1.1.1
Custom
Permanent
2022-06-08 17:05:53
None
Total items: 1

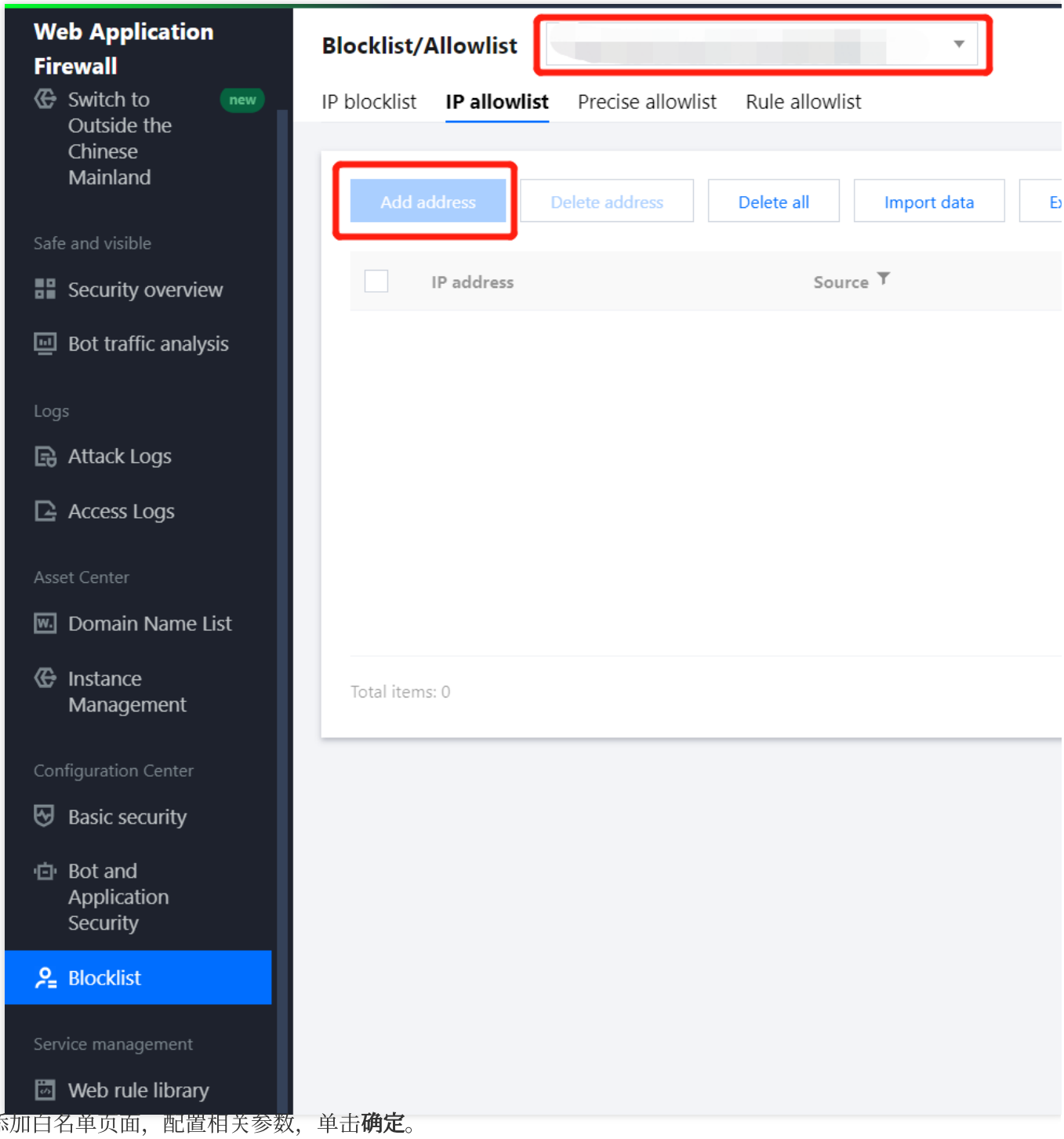
IP 白名单

最近更新时间：2023-12-29 14:45:34

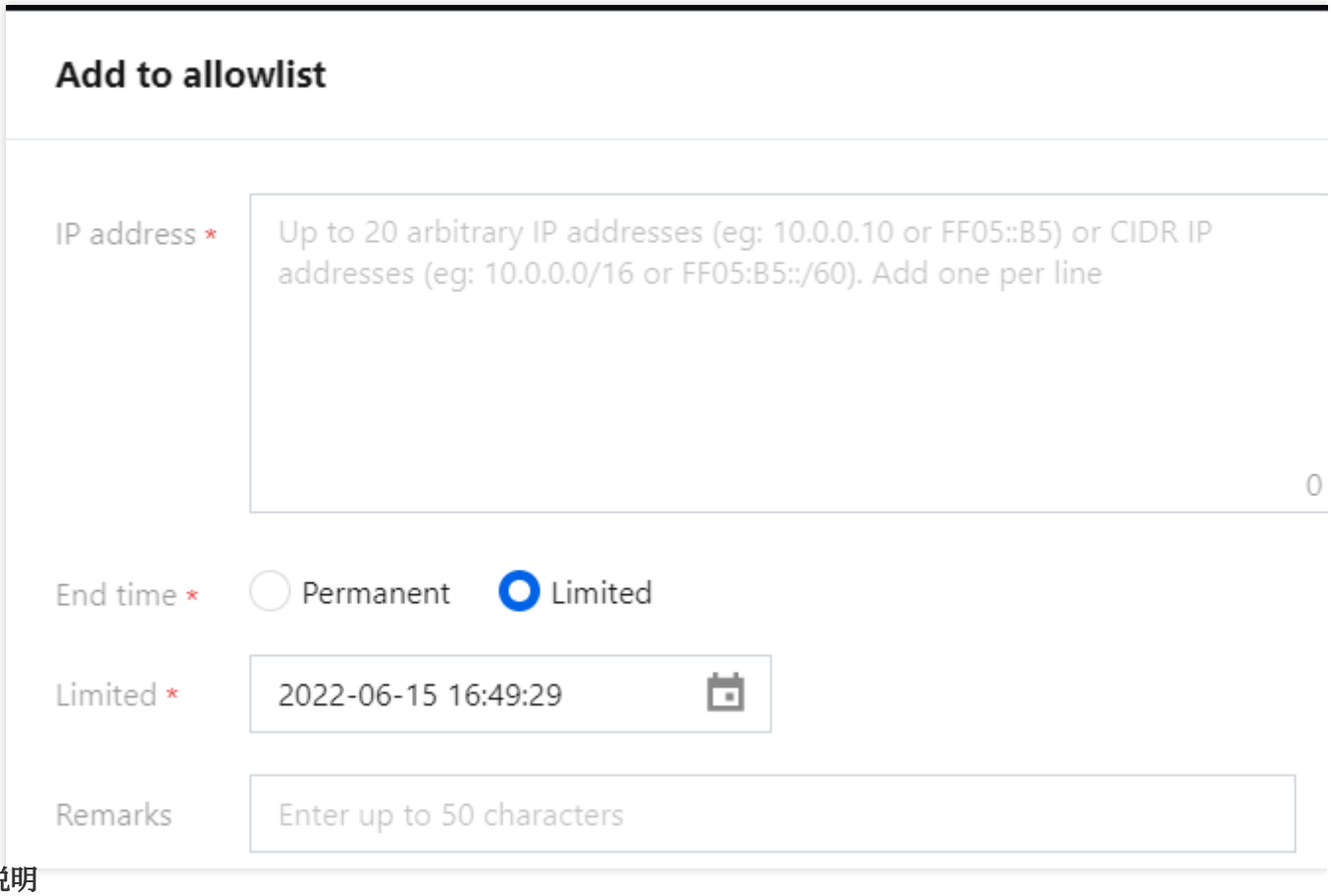
添加 IP 白名单

手动添加

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心 > 黑白名单**，进入黑白名单页面。
2. 在黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。
3. 在 IP 白名单页面，单击**添加地址**，进入添加白名单页面。



4. 在添加白名单页面，配置相关参数，单击**确定**。



字段说明

IP 地址：支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或 FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。

说明：

选择域名为 ALL 时，添加的 IP 地址或 IP 段为全局的白名单。

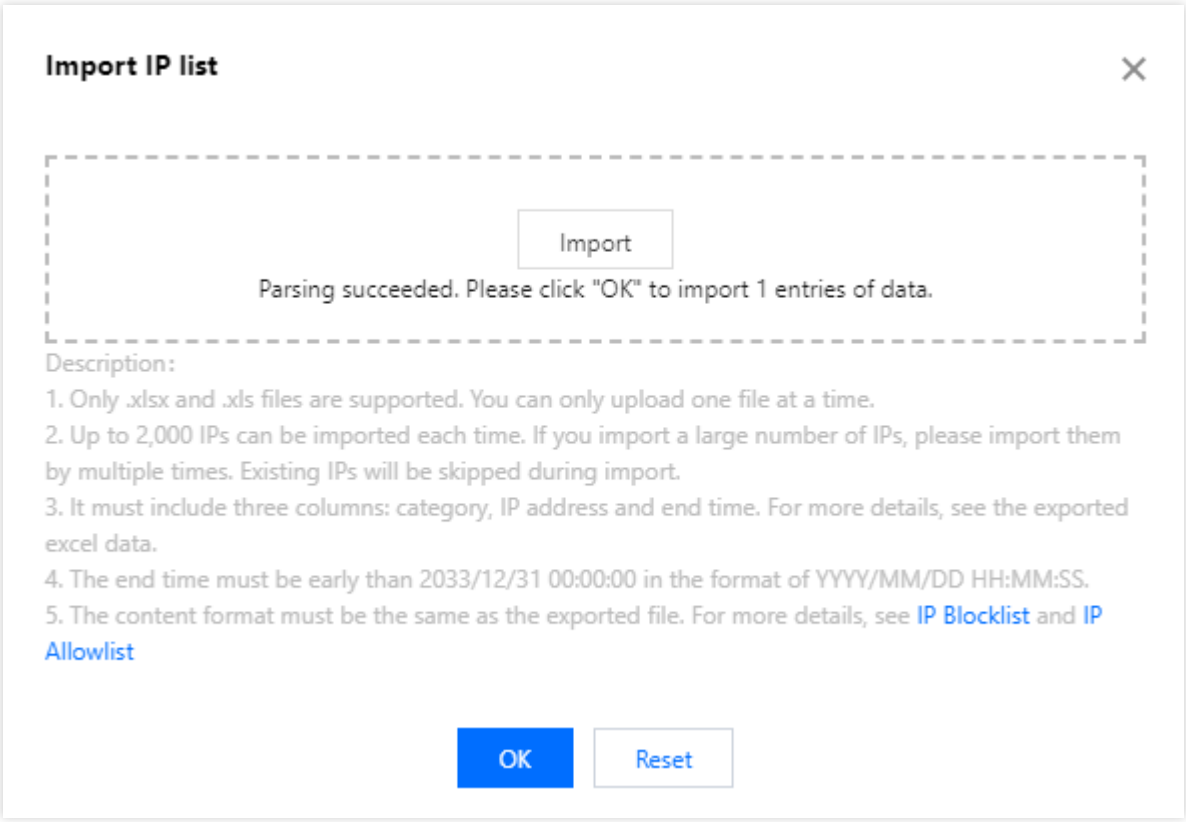
各个版本每个域名规格限制为：高级版1000条/域名、企业版5000条/域名、旗舰版:20000条/域名，每个 IP 地址或者 IP 段占用一条额度。

截止时间：永久生效或限定日期。

备注：自定义，50个字符以内。

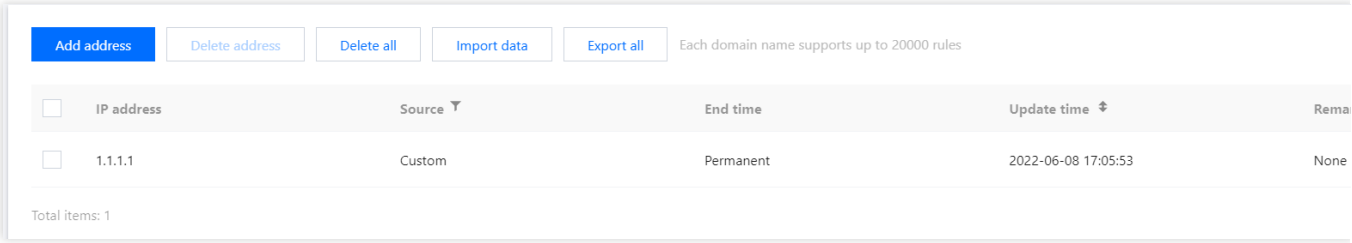
导入数据

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。
2. 在 IP 白名单页面，单击**导入数据** > **导入**，解析成功后，单击**确认导入**即可。



编辑 IP 白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。
2. 在 IP 白名单页面，选择所需 IP 地址，单击操作列的**编辑**，修改截止时间和备注，单击**确定**保存。



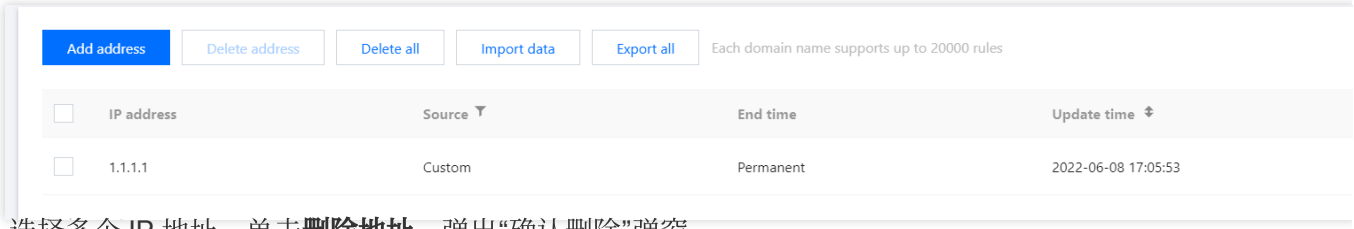
删除 IP 白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。
2. 在 IP 白名单页面，支持删除单个、部分、全部地址，具体操作如下：

单个：选择单个 IP 地址，单击**删除地址**或操作列的**删除**，弹出“确认删除”弹窗。

说明：

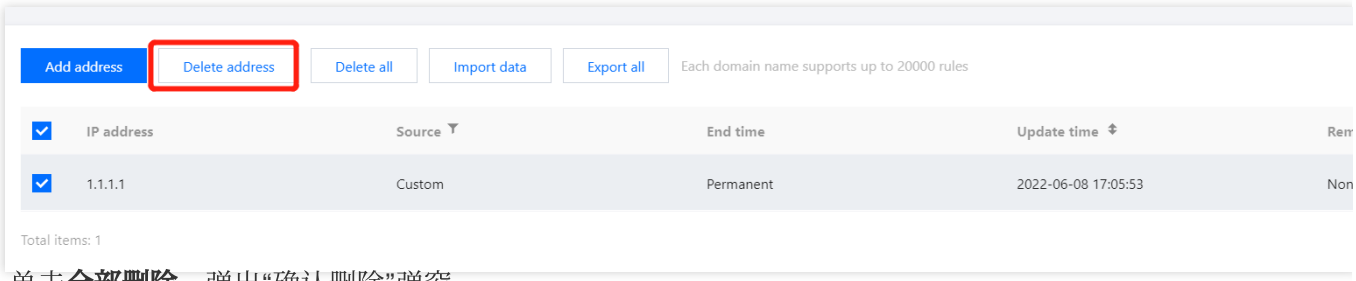
删除后将无法恢复，重新添加才能生效。



部分：选择多个 IP 地址，单击**删除地址**，弹出“确认删除”弹窗。

说明：

删除后将无法恢复，重新添加才能生效。



全部：单击**全部删除**，弹出“确认删除”弹窗。

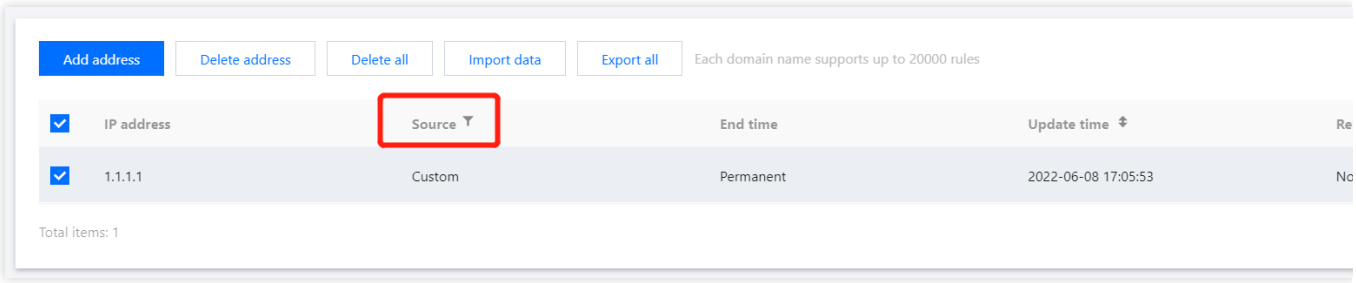
注意：

将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

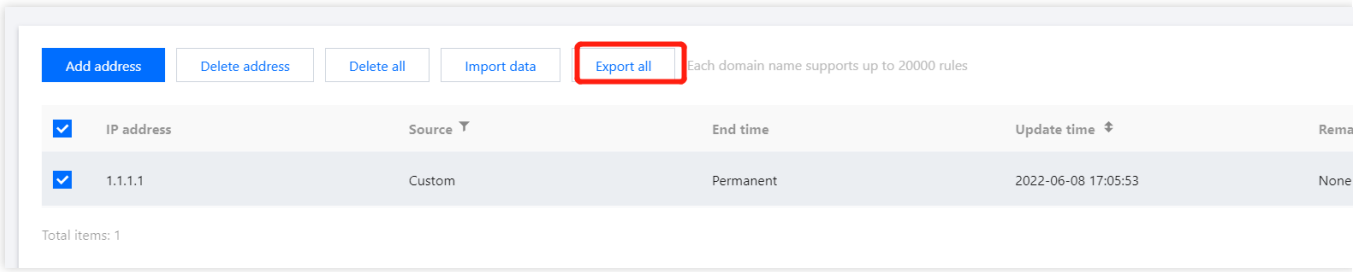
3. 在“确认删除”弹窗中，单击**确定**，即可删除地址。

导出全部筛选结果

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **IP 白名单**，进入 IP 白名单页面。
2. 在 IP 白名单页面，单击搜索框通过 **IP 地址**对 IP 进行筛选，或单击**来源**根据来源分类对 IP 进行筛选。



3. 筛选完所需 IP 后，单击**导出全部筛选结果**，即可导出所需的 IP 筛选结果。


Add address
Delete address
Delete all
Import data
Export all
Each domain name supports up to 20000 rules
IP address
Source
End time
Update time
Rema
1.1.1.1
Custom
Permanent
2022-06-08 17:05:53
None
Total items: 1

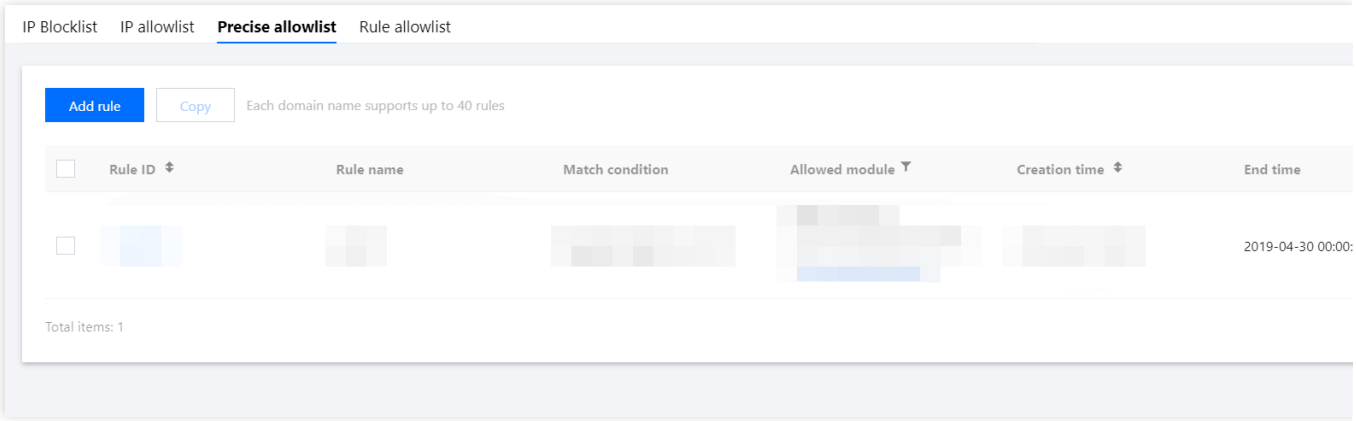
精准白名单管理

最近更新时间：2023-12-29 14:45:51

当网站管理员需要根据用户的访问请求特征来放行公网用户访问指定站点时，可以通过添加精准白名单的方法进行配置。

添加精准白名单

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心 > 黑白名单**，进入黑白名单页面。
2. 在黑白名单页面，左上角选择需要防护的域名，单击 **精准白名单**，进入精准白名单页面。
3. 在精准白名单页面，单击**添加地址**，弹出添加精准白名单弹窗。



4. 在添加精准白名单弹窗中，配置相关参数，单击**确定**。

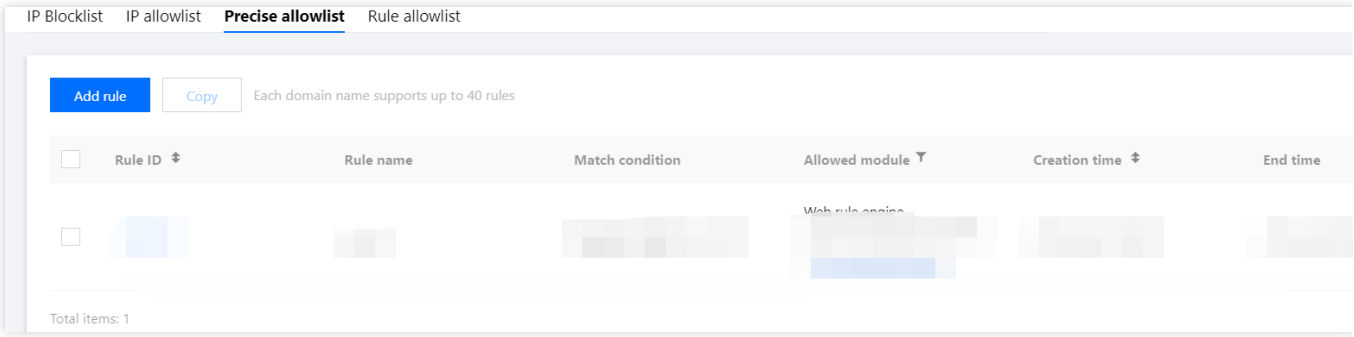
说明：

Web 应用防火墙的精准白名单支持使用掩码来放行某一网段的源 IP 的访问请求。我们可以在匹配内容中输入特定网段（如10.10.10.0/24）。

5. 此时规则将会生效，来自特定源 IP 的 HTTP 访问请求将会全部放行。

编辑精准白名单

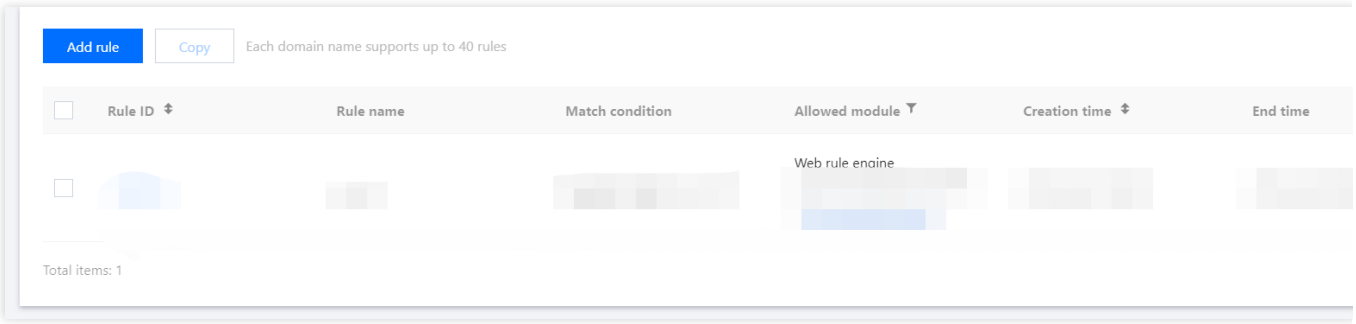
1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **精准白名单**，进入精准白名单页面。
2. 在精准白名单页面，选择所需规则，单击**编辑**，弹出编辑精准白名单弹窗。



3. 在编辑精准白名单弹窗中，修改相关参数，单击**确定**保存。

删除精准白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 **精准白名单**，进入精准白名单页面。
2. 在精准白名单页面，选择所需规则，单击**删除**，弹出确认删除弹窗。



3. 在确认删除弹窗中，单击**确定**，即可删除该规则。

说明：

删除后将无法恢复，重新添加才能生效。

规则白名单

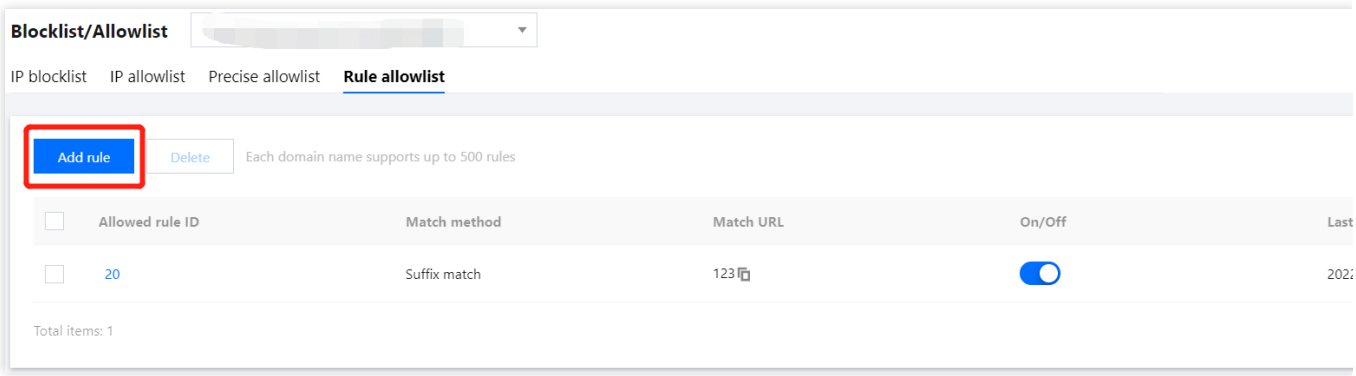
最近更新时间：2023-12-29 14:46:05

操作场景

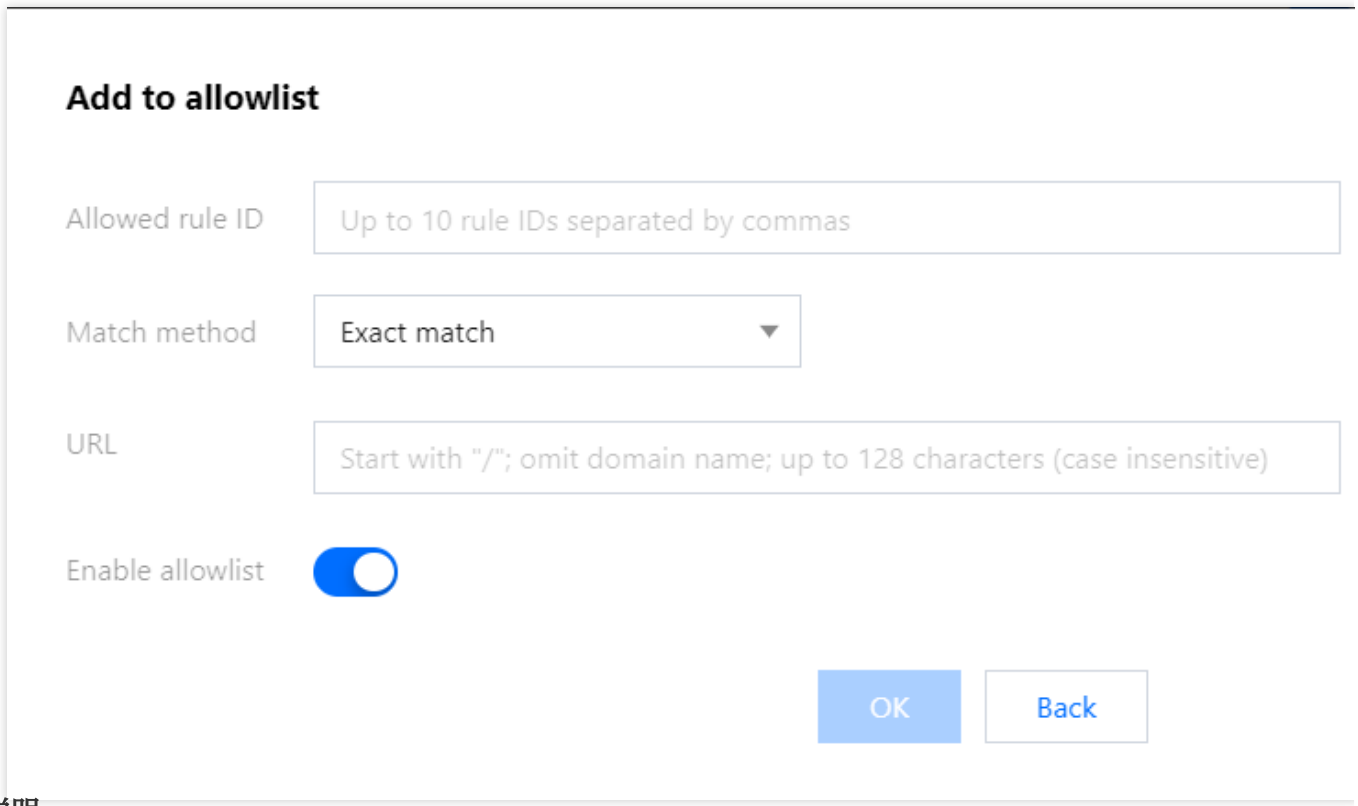
在生产环境中如出现正常访问流量被 WAF 规则引擎拦截时，可以通过黑白名单中的**规则白名单**进行加白相应规则，加白该规则后则不会被拦截。

操作步骤

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击**配置中心 > 黑白名单**，进入黑白名单页面。
2. 在黑白名单页面，左上角选择需要防护的域名，单击**规则白名单**，进入规则白名单页面。
3. 在规则白名单页面，单击**添加规则**，弹出添加白名单弹窗。



4. 在添加规则弹窗中，配置相关参数，单击**确定**。



字段说明:

加白规则 ID：填写需要加白的规则 ID，一条策略可添加最多10个规则 ID。

匹配方式：加白 URL 路径的匹配方式，支持完全匹配（默认）、前缀匹配和后缀匹配。

URL 路径：需要加白的 URL 路径，同一个域名下 URL 不可重复添加。

白名单开关：白名单策略生效开关，默认为开启。

流量体检

最近更新时间：2024-06-18 14:45:53

功能简介

流量体检功能能够对当前接入防护的业务进行流量风险分析，帮助您快速梳理接入资产、检测业务流量风险、梳理当前 WAF 配置情况，并生成详细流量体检报告，助力提升网站防护效果，保障业务稳定运行。

体检说明：

免费开放：流量体检当前为公测功能，购买 Web 应用防火墙后即可使用。

日志记录：开始体检后，将对体检域名的 Web 风险、BOT 风险、API 资产风险等进行检测。**如有相关风险将记录攻击日志及访问日志，执行动作均为观察（仅监控不拦截），不会影响/拦截业务访问。**

数据来源：体检展示数据来源于您当前正在使用的 Web 应用防火墙产品，如部分增值功能未开启时，统计数据可能与实际访问情况稍有偏差，建议您购买并开启该功能后再次体检。

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**流量体检**。
2. 在流量体检页面，您可以根据发起体检、查看重点关注的问题 TOP5、下载历史体检报告。

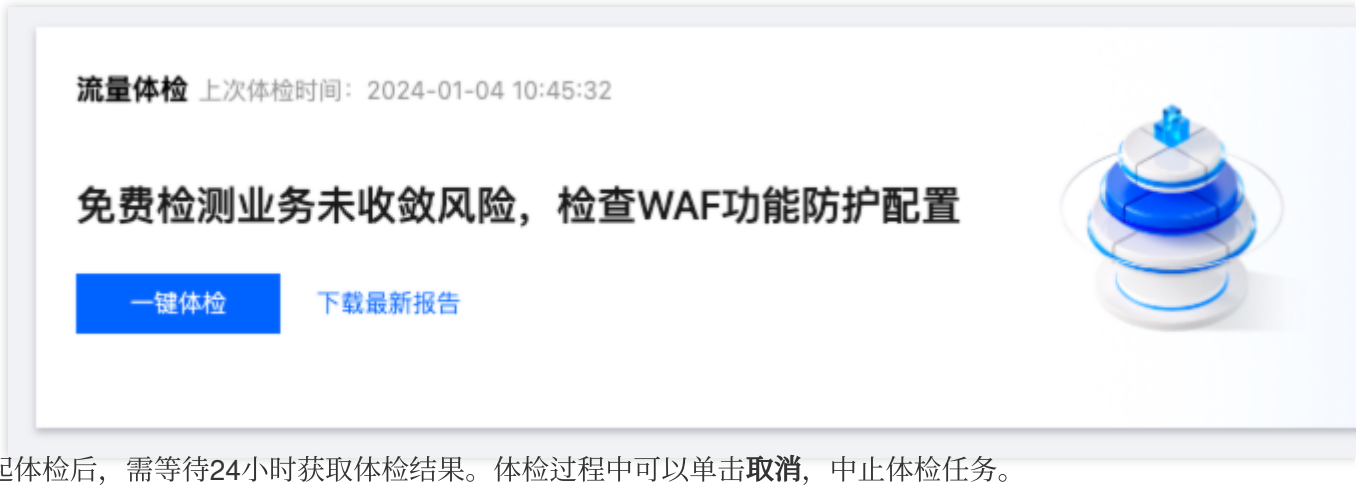
发起流量体检

1. 在流量体检卡片，单击**一键体检**，即可发起体检任务。

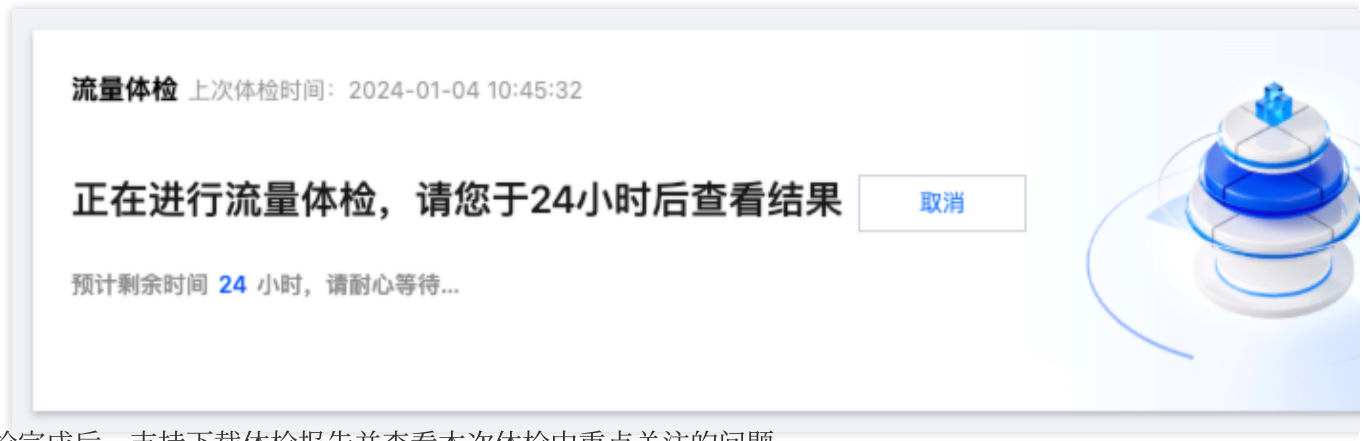
体检范围：支持检测2万 QPS 内最多100个域名，超出则随机抽取部分域名检测。

体检周期：每7天仅支持体检一次。

体检时长：每次体检周期预计为24小时，发起体检后仅检测近24小时异常流量，体检结束生成体检报告及重点问题。



2. 发起体检后，需等待24小时获取体检结果。体检过程中可以单击**取消**，中止体检任务。



3. 体检完成后，支持下载体检报告并查看本次体检中重点关注的问题。

查看重点关注问题

体检完成后支持在页面下方查看重点关注的问题TOP5，并对重点风险进行处置。

优先级：风险处置的优先级，分为高、中、低三级，根据风险程度及影响面评估。

统计数据：统计体检周期内风险数据，并展示较上次体检结果的风险增减变化。

下载报告

体检完成后支持下载详尽流量体检报告，体检报告**仅保存30天**。

说明：

由于报告篇幅有限，每个检测项详情列表仅展示前五项，完整明细请参考报告引导在控制台对应页面查看。

在报告下载卡片，单击**预览**，在线预览体检报告内容。

在报告下载卡片，单击**下载**，支持下载 PDF 格式体检报告。

流量体检检测项说明

检测模块	检测项	检测内容
接入资产梳理	域名资产梳理	梳理当前域名总数、接入 WAF 域名总数、开启 WAF 防护总数，并展示未接入 WAF 防护域名列表。
	API 资产梳理	梳理当前接入域名中发现的 API 资产总数、涉及业务场景，并展示昨日 API QPS峰值 TOP5、活跃 API 较多的域名列表。
流量风险梳理	业务访问趋势	分析业务访问趋势及是否有超量风险。
	攻击流量趋势	分析当前接入业务体检周期内的攻击类型分布。
	BOT 攻击风险	分析访问流量中是否有 BOT 风险，如有，进一步分析相关 BOT 的类型/目的、恶意程度及访问趋势。
	API 风险梳理	分析访问流量中发现的 API 资产是否存在风险，如有，进一步分析相关资产的涉敏情况、风险事件及资产的访问总数、QPS、业务场景。
WAF 配置梳理	WAF 配置梳理	检测产品关键功能的配置情况，包括资产的接入情况、防护开关开启情况、防护配置情况、日志存储配置情况等。

统计与日志
攻击日志

最近更新时间：2023-12-29 14:46:18

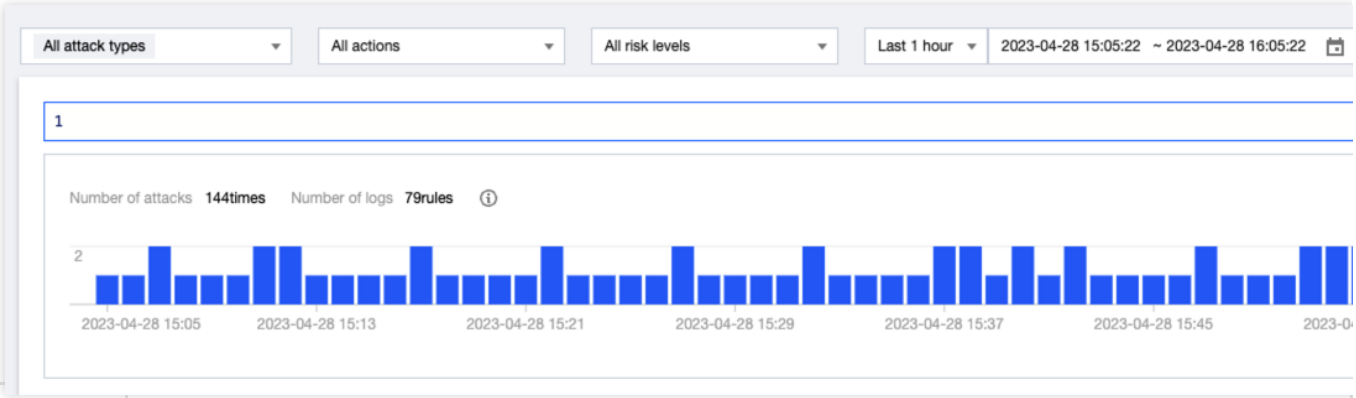
本文为您介绍如何使用攻击日志进行攻击日志索引、快速分析和查询。

背景信息

Web 应用防火墙默认提供攻击日志功能，详细记录攻击产生的时间、攻击源IP、攻击类型及攻击详情等信息。攻击日志仅支持查询或导出最近30天日志。攻击日志支持全文检索、模糊搜索和组合条件搜索等检索方式，同时支持根据检索条件下载日志，支持百万级日志下载。

检索攻击日志

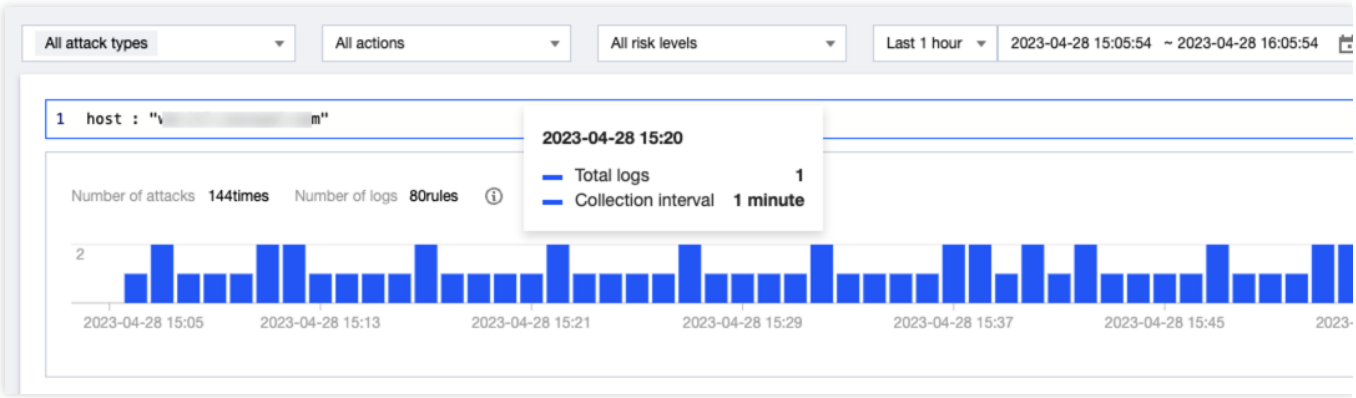
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**日志服务 > 攻击日志 > 日志服务**。
2. 在日志查询页签，您可以根据需要，选择实例、域名、攻击类型、执行动作、风险等级及时间维度等信息，筛选查看攻击日志。



字段名称	字段说明
实例	支持多选，默认显示全部实例。
域名	支持多选，默认显示全部域名。
攻击类型	支持多选，默认为全部攻击类型，攻击类型包括各个安全模块产生的观察和拦截日志。
执行动作	单选，默认为全部执行动作，包括观察和拦截两种类型。
风险等级	单选，默认为全部风险等级，包括高危、中危和低危三种类型。

时间范围	默认为近一小时，支持筛选最近时间及相对时间。
自动刷新	定时自动刷新当前页面，默认为关闭；若开启开关，您可选择按照时间范围刷新当前页面，获取最新攻击日志数据。

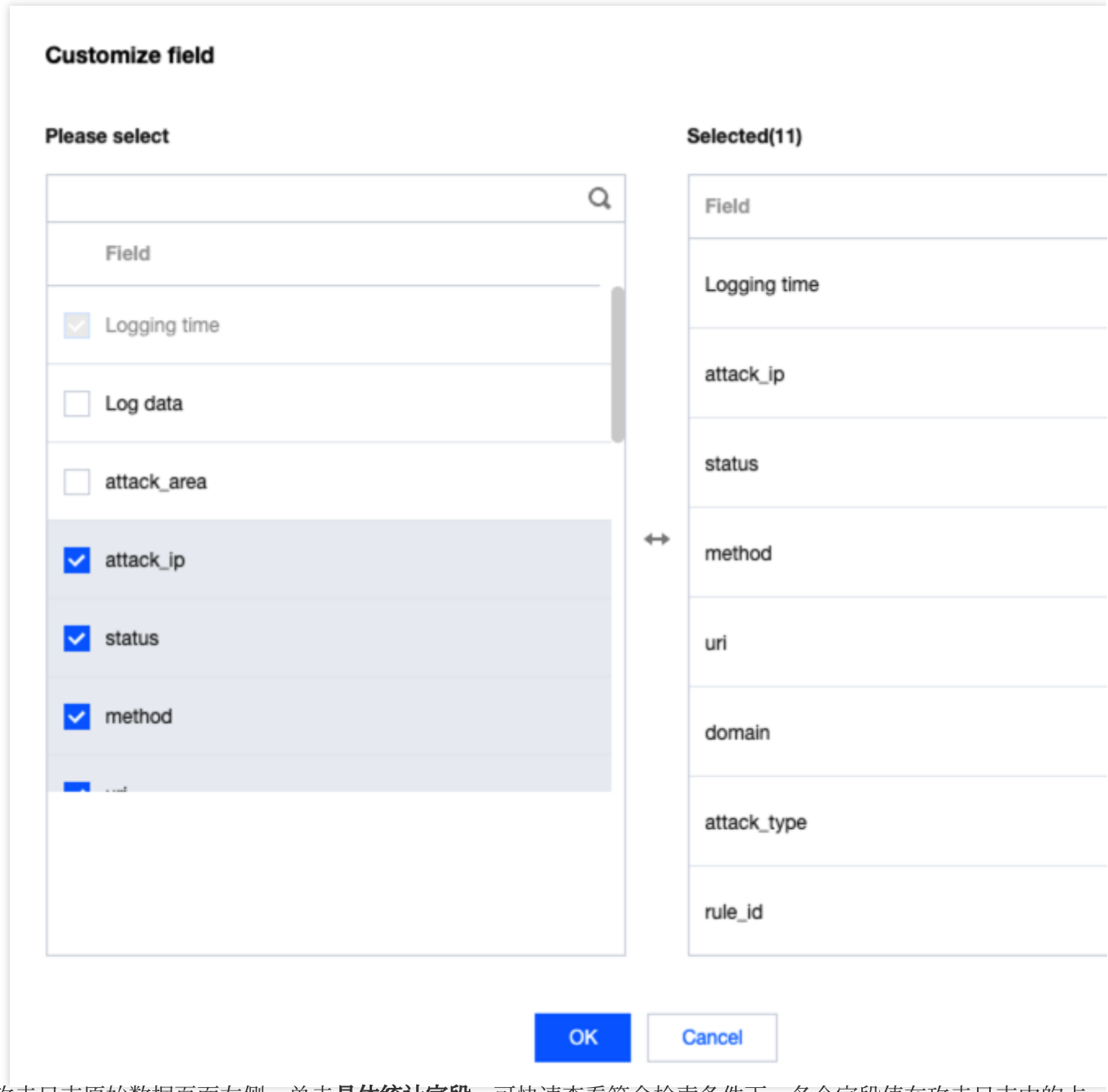
3. 设置完成检索条件，单击**检索分析**，即可查看检索分析结果。



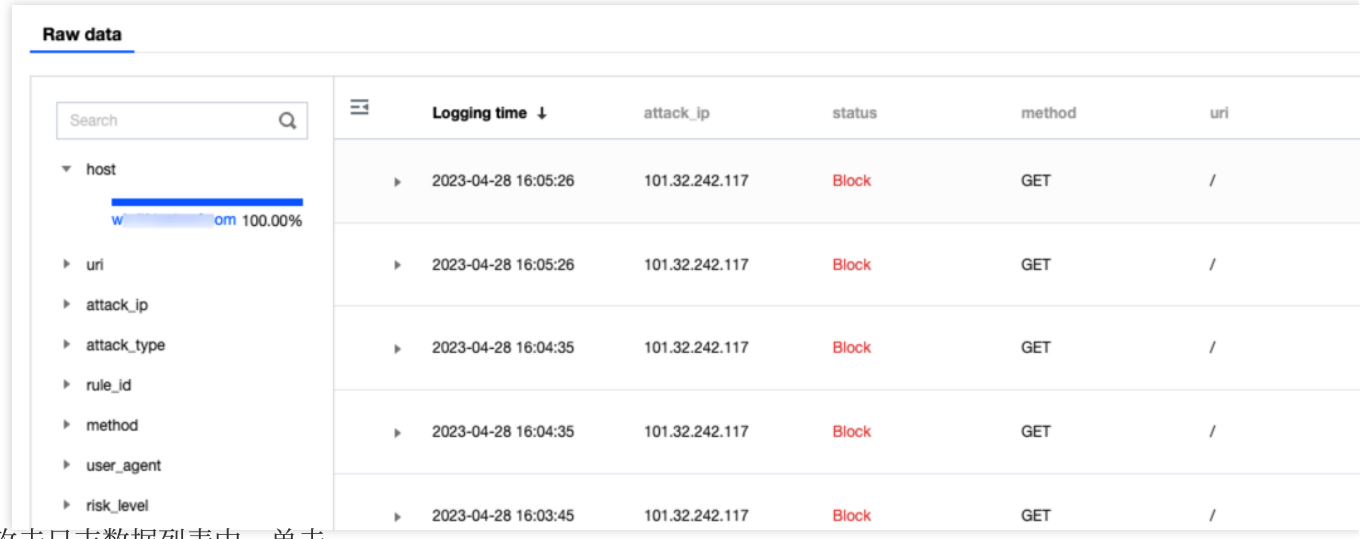
分析攻击日志

1. 在攻击日志数据列表右上方，单击

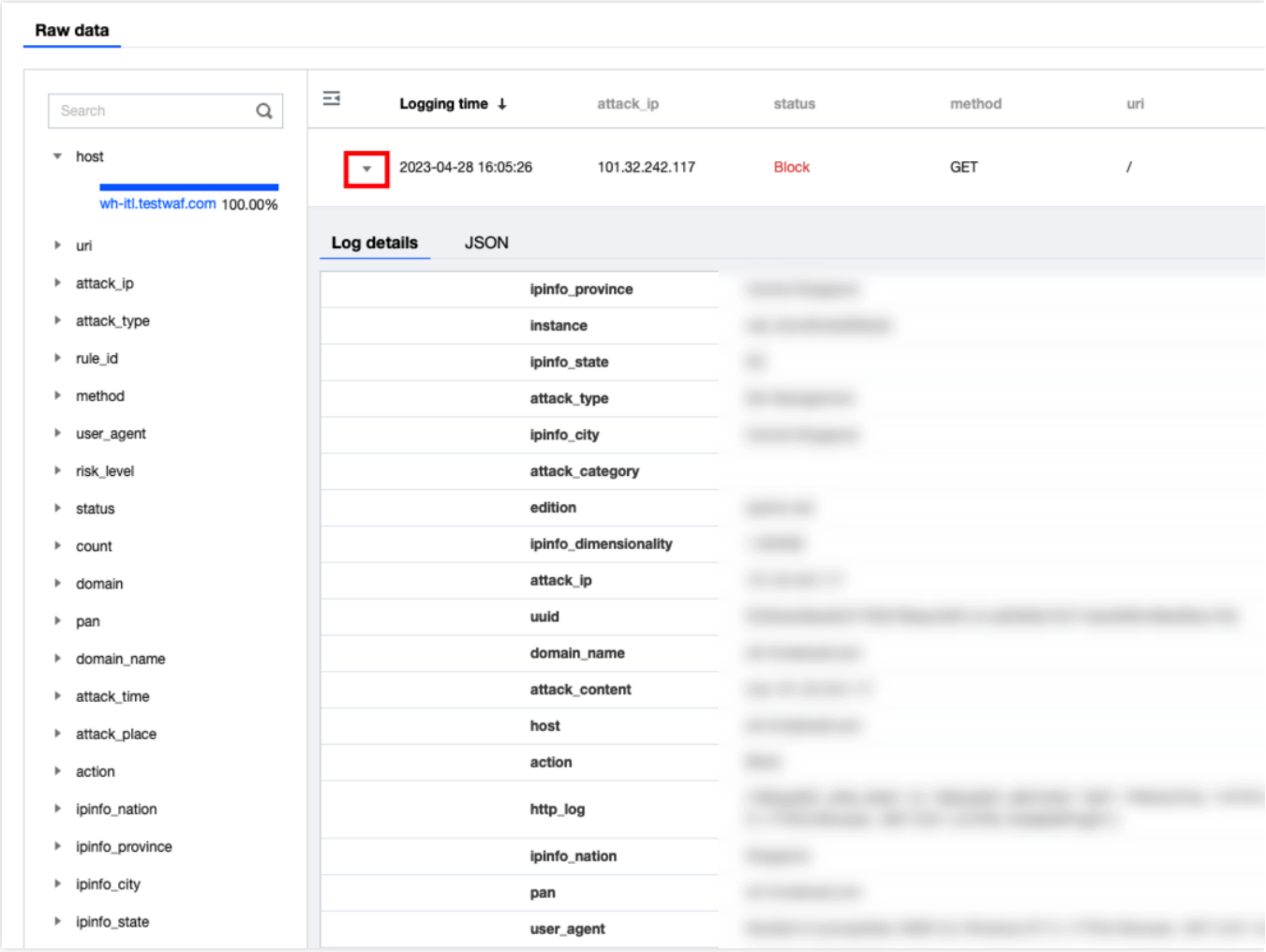
，可设置列表展示字段；选择完成后，单击**确定**，即可设置成功。各字段说明，请参见 日志详情字段说明。



2. 在攻击日志原始数据页面左侧，单击**具体统计字段**，可快速查看符合检索条件下，各个字段值在攻击日志中的占比。单击**字段值**，可快速筛选包含该字段值的所有攻击日志。



3. 在攻击日志数据列表中，单击 ▶ 可展开单条日志详情。单击日志详情中的**字段值**，可快速筛选包含该字段值的所有攻击日志。单击 **JSON**，可查看对应 JSON 格式展示样式。



下载攻击日志

1. 在攻击日志数据列表右上方，单击

，侧边栏展开下载任务页面。

说明

默认下载当前检索的日志范围。

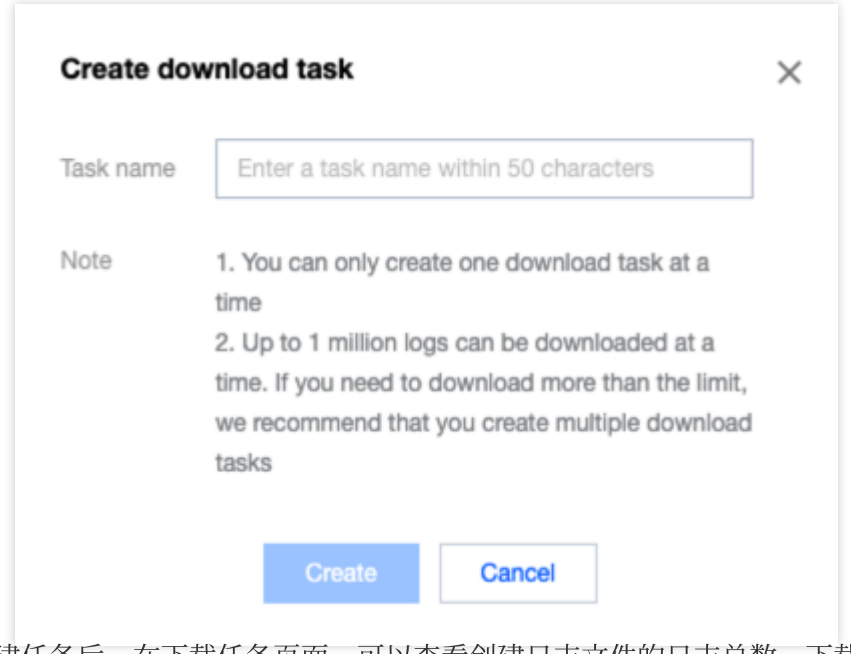
同一时间段内只允许创建一个下载任务，请耐心等待。

单次最多支持下载100万条日志，如果您需要下载的日志超过100万条，建议您分多次任务进行下载，或 联系我们 为您提供支持服务。

当选择泛域名（如 `*.abc.com` ）时，所有关联子域名（如以 `.abc.com` 结尾）的日志也将会被下载。

2. 在下载任务页面，单击**创建任务**。

3. 在创建下载任务弹窗内输入任意任务名称，单击**创建**后即可下载。



4. 创建任务后，在下载任务页面，可以查看创建日志文件的日志总数、下载进度、创建时间、过期时间和下载状态信息。单击**下载**，即可下载 csv 格式的日志文件。

说明

创建成功的日志下载任务，保留3天，超过3天之后日志文件将会删除，请及时下载。

附录

日志详情字段说明

基本信息

字段名称	字段说明

host	客户端访问的域名信息。
uri	请求 URI ：用于标识请求资源的字符串。
attack_ip	攻击源 IP：客户端攻击的源 IP。
attack_type	攻击类型：攻击具体命中的攻击类型。
rule_id	规则ID：触发防护策略的规则 ID，其中 AI 引擎检出的攻击详情的规则 ID 为0。
method	请求方法：客户端攻击请求方法。
user_agent	User-Agent：攻击源 IP 向服务器表明的浏览器类型和操作系统标识等信息。
risk_level	风险等级：客户端攻击触发的风险等级。
status	执行状态：攻击请求的处置结果，包括观察（0）、拦截（1）两种处理结果。
count	聚合攻击次数，相同攻击源 IP 和攻击类型，汇总每10秒产生的攻击次数。
domain	客户端攻击的域名信息。
pan	客户端访问的域名信息。
domain_name	客户端访问的域名信息。
attack_time	攻击时间，客户端攻击触发的时间。
attack_place	攻击位置，攻击方式在 HTTP 请求中的位置。
action	执行动作，客户端攻击触发的处置动作，包括观察（0）、拦截（1）两种处理结果。
ipinfo_nation	攻击 IP 所属国家名称。
ipinfo_province	攻击 IP 所属省份信息。
ipinfo_city	攻击 IP 所属城市。
ipinfo_state	攻击 IP 所属国家信息，国家英文缩写。
ipinfo_dimensionality	攻击 IP 所属纬度信息。
instance	域名接入的 Web 应用防火墙实例名称。
attack_category	攻击一级分类，暂未提供。
edition	域名接入的 Web 应用防火墙实例类型：分为 sparta-waf（SaaS 型 WAF）和 clb-waf（负载均衡型 WAF）。
uuid	日志唯一标识。

attack_content	攻击内容：客户端触发攻击的内容。
http_log	记录 HTTP 请求和响应信息的日志文件：包含此次 http 请求的所有 http 信息。
headers	协议头部信息：包括自定义头部信息。
rule_name	规则名称，暂未提供。
count	攻击聚合次数，相同攻击源 IP 和攻击类型，每10秒产生的攻击次数汇总。
args_name	参数名称：HTTP 请求中的参数名
ipinfo_isp	攻击 IP 运营信息。
appid	用户腾讯云账号的 APPID。
ipinfo_longitude	攻击 IP 的经度信息。

访问日志

最近更新时间：2023-12-29 14:46:32

功能简介

访问日志功能用于记录 Web 应用防火墙防护域名的访问日志信息，提供防御域名最近30天访问日志查询和下载功能，及不少于180天的访问日志存储服务。启用访问日志功能后，您可以根据需要查询和下载访问日志，满足安全合规、安全运维等需求。

注意：

使用访问日志功能，需要先 购买安全日志服务包，并且根据 操作步骤 启用访问日志开关。只有开启访问日志开关的域名，Web 应用防火墙才会记录该域名的访问日志。

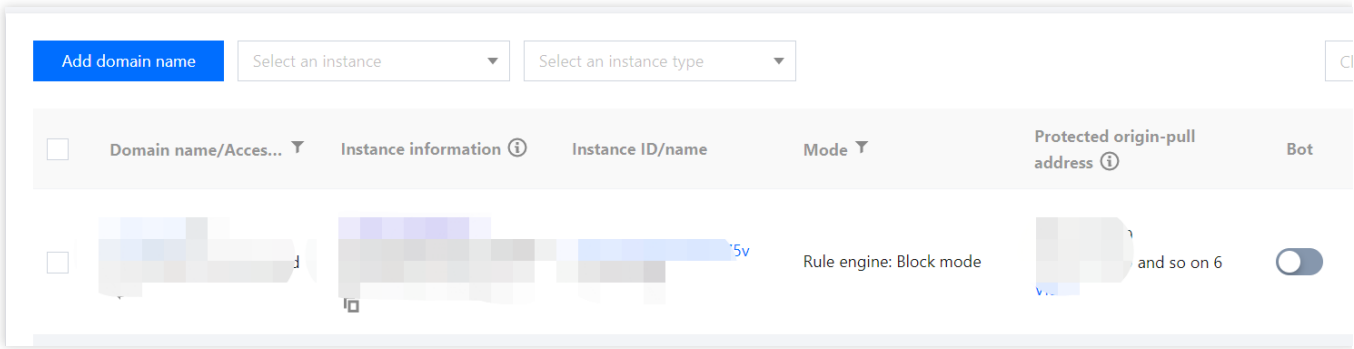
关闭日志服务：如需关闭访问日志功能，可以在 续费管理 中，找到相应计费项取消。取消后，系统2个小时内停止新的访问日志写入，并于24小时内清空历史访问日志，请谨慎操作。

升级日志服务容量：当存储的日志容量超过购买容量后，系统将自动停止新的访问日志写入，历史的访问日志不受影响，直到到达存储周期后开始自动删除。为了避免超量导致丢失访问日志，建议关注日志使用量，提前扩容避免超量导致访问日志丢失。

操作步骤

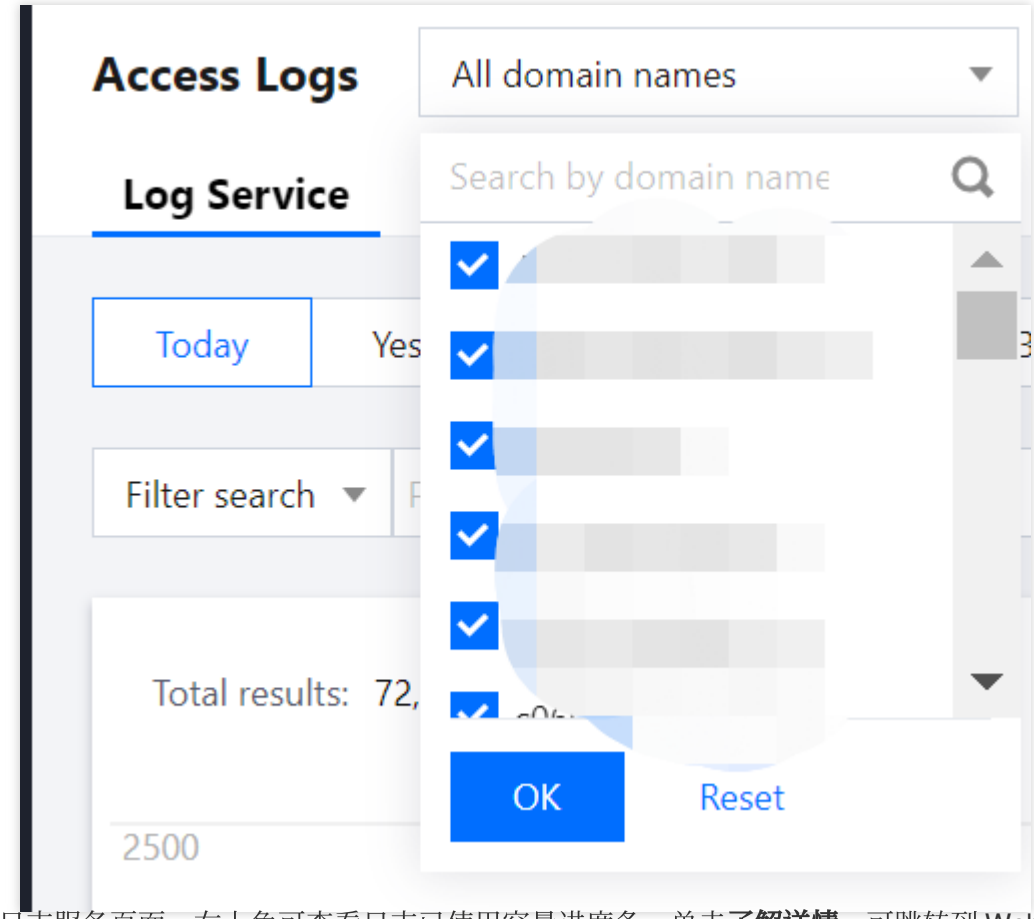
启用访问日志

登录 Web 应用防火墙控制台，在左侧导航栏中，选择**实例管理** > **域名接入**，进入域名接入页面，在域名列表中选择域名，单击开启访问日志开关。



查看日志

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**日志服务** > **日志服务**，进入日志服务页面。
2. 在日志服务页面，单击左上角的域名下拉框，选择所需域名后，单击**确定**，即可该域名的访问日志。

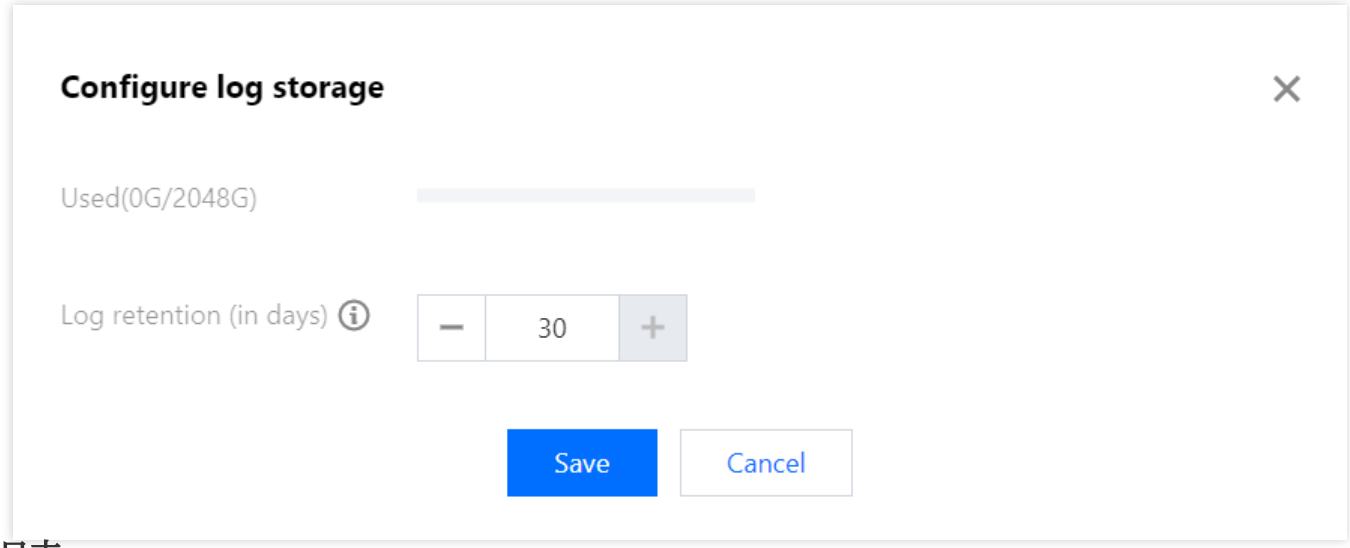


3. 在日志服务页面，右上角可查看日志已使用容量进度条，单击**了解详情**，可跳转到 Web 应用防火墙的计费详情页面。

4. 在日志服务页面，单击右上角**存储配置**，可以查看日志已使用容量进度条，和设置日志保存天数，单击**保存**，即可保存修改。

说明：

日志保存天数为1-30天。

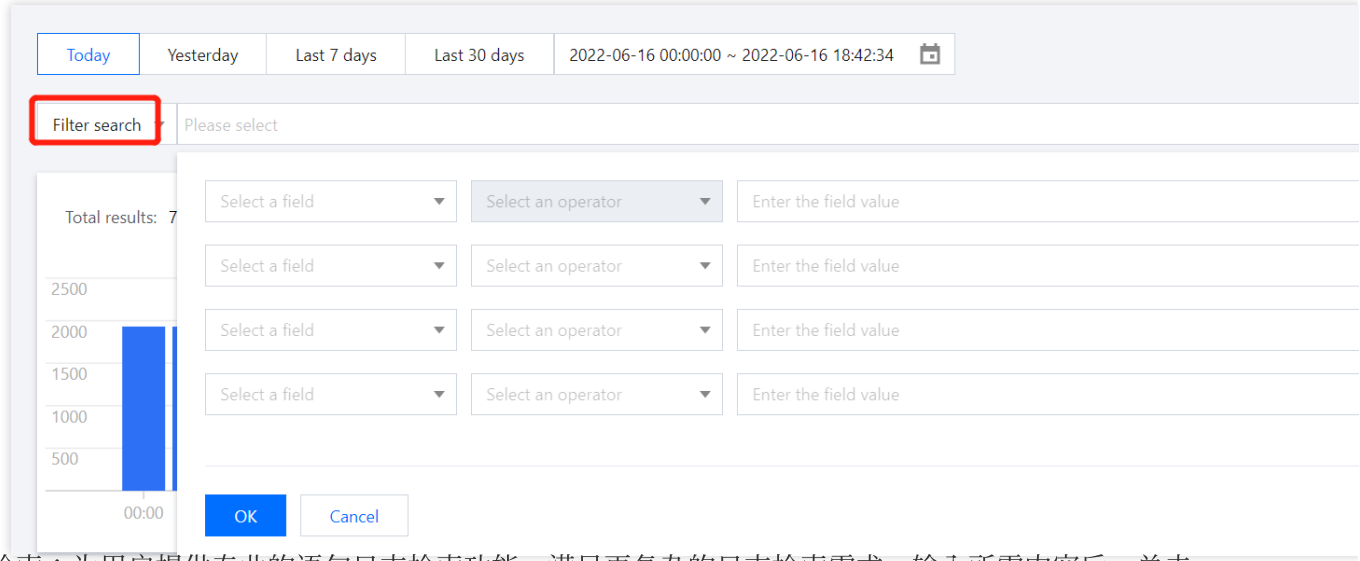


查询日志

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**日志服务 > 日志服务**，进入日志服务页面。
2. 在日志服务页面，可以用快速检索、过滤检索和语句检索查询所需日志。

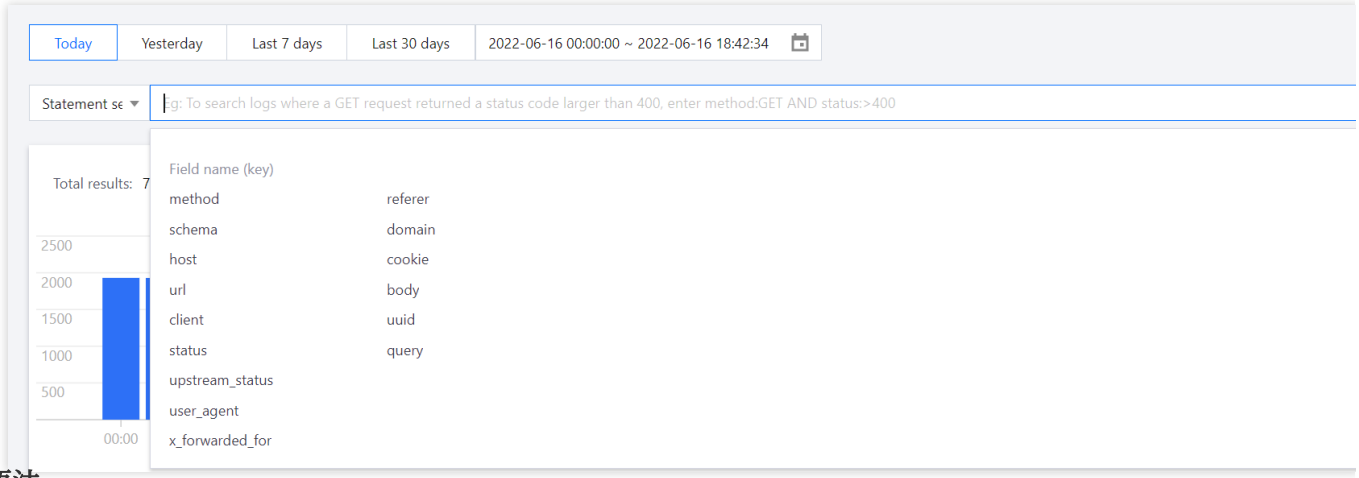
快速检索：主要是针对时间的快捷选择检索。

过滤检索：选择所需字段和操作符，输入字段值后，单击**确定**，即可针对每个字段对日志进行筛选，并支持添加多个字段限制。



语句检索：为用户提供专业的语句日志检索功能，满足更复杂的日志检索需求。输入所需内容后，单击

，即可查询。



检索语法

保留字符	说明
AND	“与”逻辑操作符，例如 level:ERROR AND pid:1234
OR	“或”逻辑操作符，例如 level:ERROR OR level:WARNING
NOT	“非”逻辑操作符，例如 level:ERROR NOT pid:1234
TO	“范围”逻辑操作符，例如 request_time:[0.1 TO 1.0]
""	双引号，引用一个短语词组（短语当作一个整体词组），例如 name:"john Smith"
：	冒号，表示作用于的 key 字段，即键值检索，例如 level:ERROR
*	通配符查询，匹配零个、单个、多个字符，例如 host:www.test*.com
?	通配符查询，匹配单个字符，例如 host:www.te?t.com
()	分组操作符，控制逻辑运算优先级，例如 (ERROR OR WARNING) AND pid:1234
>	范围操作符，表示大于某个数值，例如 status:>400
>=	范围操作符，表示大于等于某个数值，例如 status:>=400
<	范围操作符，表示小于某个数值，例如 status:<400
<=	范围操作符，表示小于等于某个数值，例如 status:<=400
[]	范围操作符，包含边界值的范围，例如 age:[20 TO 30]
{}	范围操作符，不包含边界值的范围，例如 age:{20 TO 30}

\\	转义符号，转义后的字符表示符号本身，例如 url:\\/images\\/favicon.ico，如不想使用转义符，可使用""包裹，例如url:"/images/favicon.ico"，但需注意，双引号内的词会被当作一个整体，两种查询方式的详细区别可参见 配置索引 中的查询示例
+	逻辑操作符，类似 AND，+A 表示 A 一定存在，例如 +level:ERROR +pid:1234
-	逻辑操作符，类似 NOT，-A 表示 A 不存在，例如 +level:ERROR -pid:1234
&&	与逻辑，类似 AND，例如 level:ERROR && pid:1234
!	非逻辑，类似 NOT，例如 level:ERROR !pid:1234
/	正则表达式标识符，/${regExp}/ ，例如 /[mb]oat/表示搜索包含 moat 或 boat 的结果
exists	_exists_:key，返回 key 不为空的值，例如 _exists_:userAgent 表示搜索 userAgent 字段有值的结果
~	相似搜索，例如 level:errro~，可以命中 level 为 error 关键字的结果

注意：

操作符区分大小写，例如 AND、OR 表示检索逻辑运算符，而 and、or 视为普通词组。

多个检索语句用空格连接时，视为"或"逻辑，例如 `warning error` 表示包含 `warning` 或 `error` 关键字的结果。

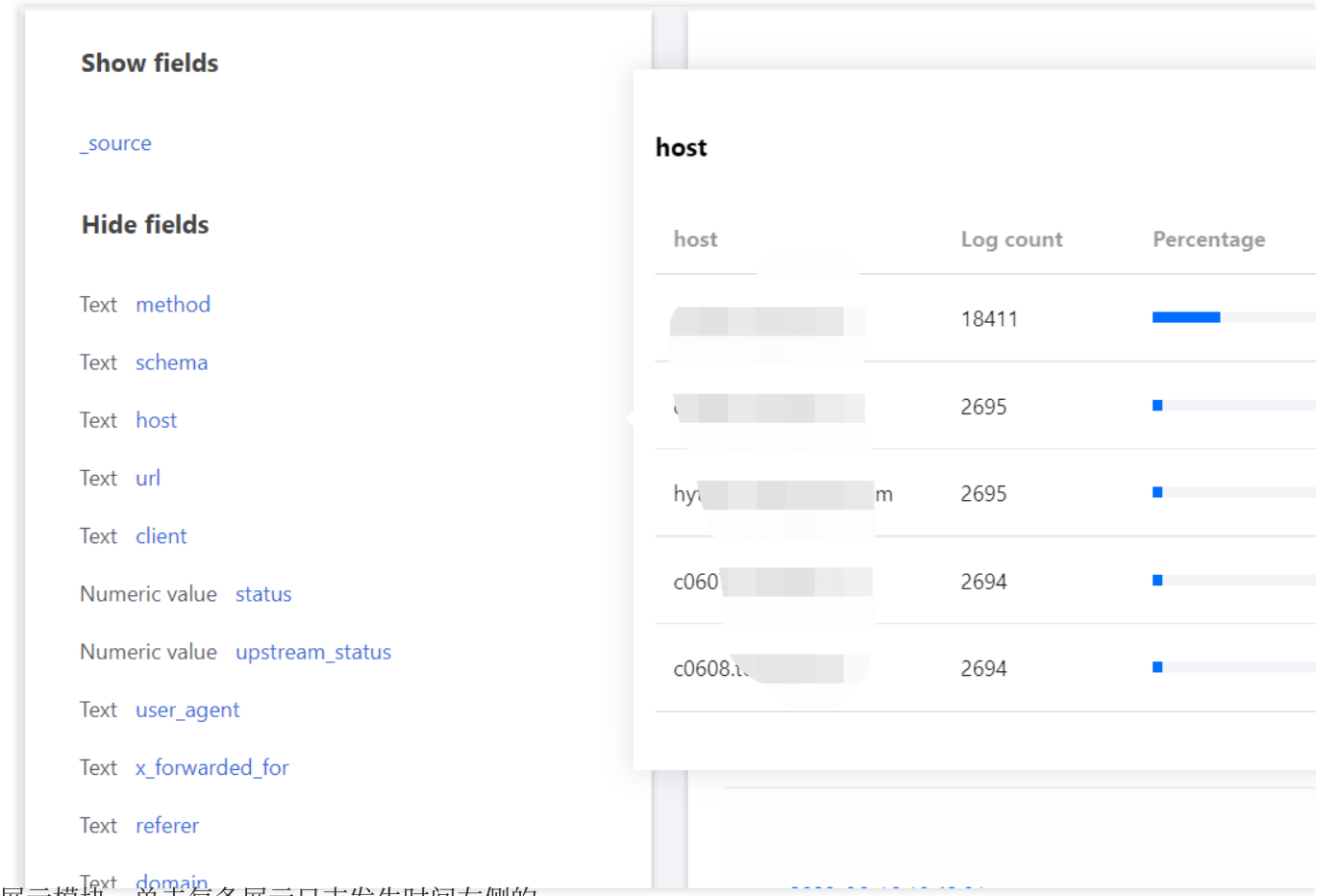
检索关键字中存在特殊字符时，需使用转义符进行转义，特殊字符包括 + - && || ! ( ) { } [ ] ^ " ~ * ? : \\。

使用键值检索时（形如 key:value），键名（key）必须在日志主题的键值索引配置项里面。

同时使用 AND 和 OR 逻辑运算符时，请使用()对检索条件进行分组，以明确逻辑优先级，例如 `(ERROR OR WARNING) AND pid:1234` 。

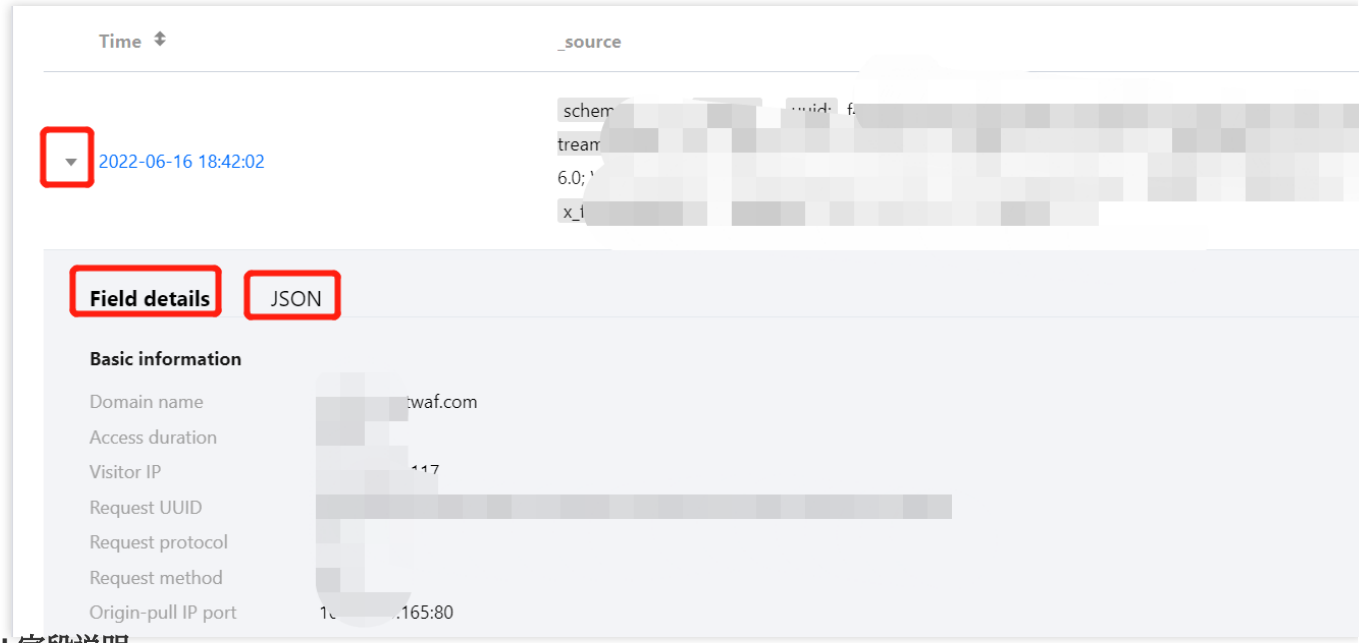
展示日志

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**日志服务 > 日志服务**，进入日志服务页面。
2. 在日志服务页面的展示模块，单击"字段名称"，会展示与本字段匹配的日志数前五的占比。



3. 在展示模块，单击每条展示日志发生时间左侧的

，可以查看字段详情；单击 **JSON**，可以查看 JSON 格式的详情。



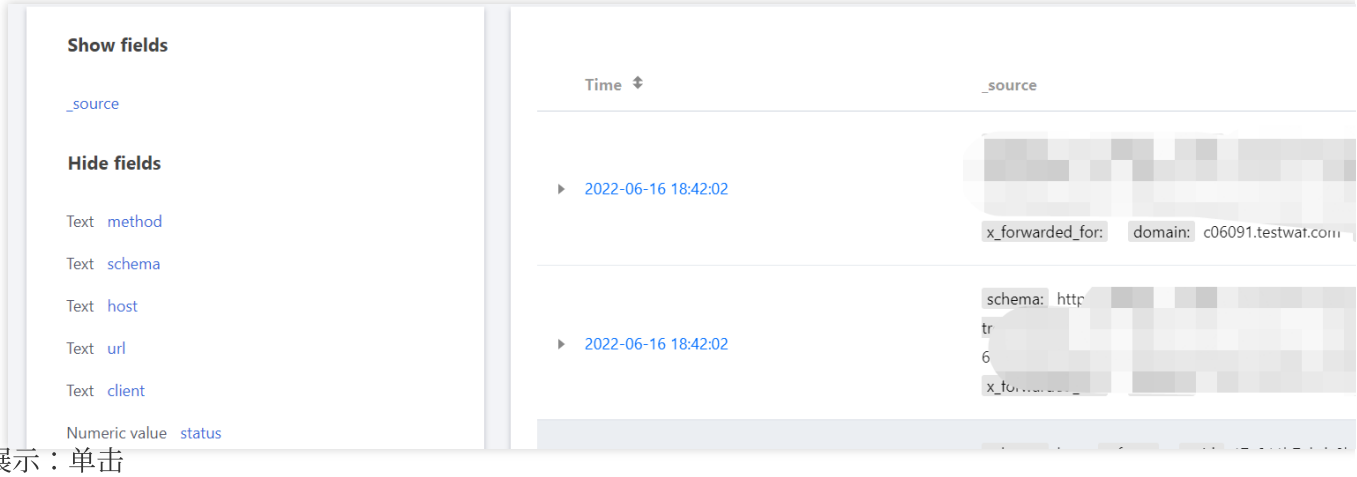
JSON 字段说明

字段名	说明

domain	所属泛域名
request_time	请求耗时，客户端请求达到 Web 应用防火墙和从 Web 应用防火墙返回需要的时间
uuid	HTTP 请求唯一标识
schema	请求协议，HTTP 或者 HTTPS
method	客户端请求方法。
url	请求的 uri，客户端完整请求路径中，域名后第一个“/”到“?”之间的内容
host	客户端请求域名
http_user_agent	请求 UA
headers	HTTP 请求的头部
upstream_status	源站返回给 Web 应用防火墙的响应状态码
status	Web 应用防火墙返回给客户端的响应状态码 CLB - WAF 状态码624为拦截，600为正常 SAAS - WAF 状态码403为拦截，200为正常
body_bytes_sent	响应体大小
upstream_response_time	客户端请求从源站返回到 Web 应用防火墙需要的时间
ip_info.country	国家
ip_info.city	城市
ip_info.province	省份
ip_info.operator	运营商
ip_info.ip_type	IP 类型
ip_info.idc	IDC 机房
ip_info.longtitude	经度
ip_info.dimensionality	纬度

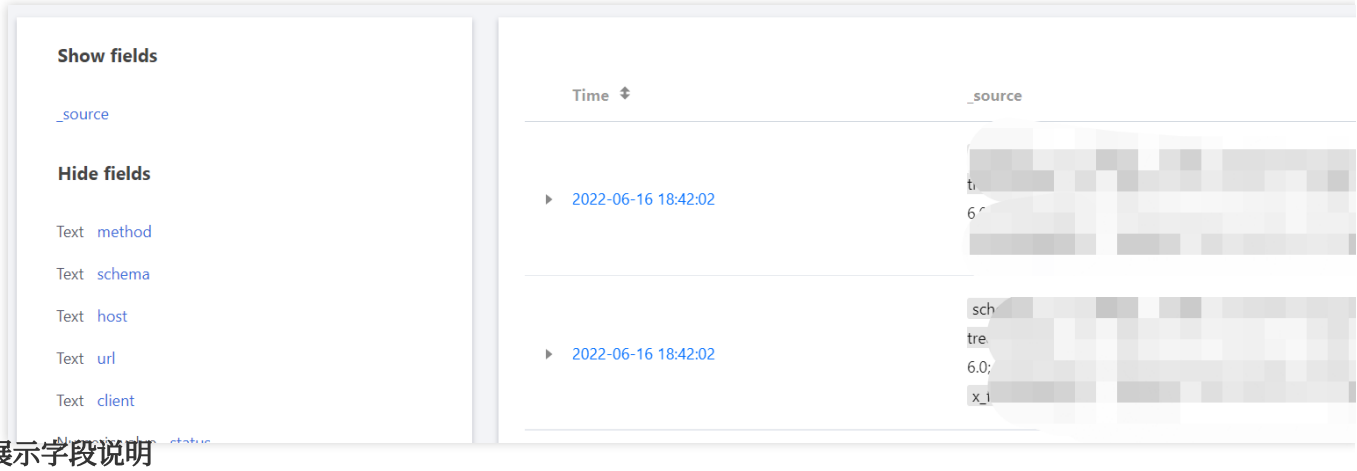
4. 在展示模块，展示已筛选出来的日志内容，目前支持列表和字段两种展示方式。

字段展示：默认展示字段模式，右上角切换图标可以操作切换。



列表展示：单击

，切换至列表模式。



列表展示字段说明

字段名	说明
msec	请求发生时候的时间戳
schema	请求协议，HTTP 或者 HTTPS
method	客户端请求方法
host	客户端请求域名
url	请求的 uri，客户端完整请求路径中，域名后第一个“/”到“?”之间的内容
query	HTTP 请求的 Query String，最大长度为 1K
body	请求的 body 数据

http_referer	源页面
http_user_agent	请求 UA
http_x_forwarded_for	出经过的所有代理
cookie	请求的 cookie 信息，最大长度为 1K
upstream_status	源站返回给 Web 应用防火墙的响应状态码
upstream_response_time	客户端请求从源站返回到 Web 应用防火墙需要的时间
upstream_addr	请求经过的上游服务器 IP
status	Web 应用防火墙返回给客户端的响应状态码
upstream_status	源站返回给 Web 应用防火墙的响应状态码
upstream_response_length	上游服务器返回的响应长度
edition	WAF 的版本，分成 sparta-waf,clb-waf,cdn-waf

下载访问日志

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**日志服务 > 日志服务**，进入日志服务页面。
2. 在日志服务页面的展示模块， 单击

，进入下载任务页面，单击**确定**，即可创建下载任务。

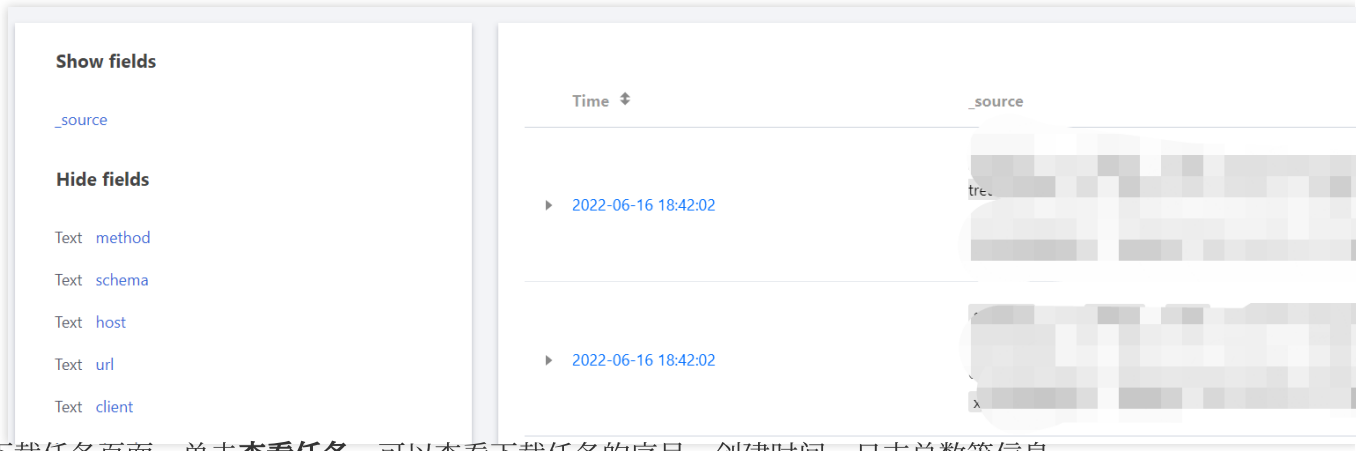
说明：

同一时间段内只允许创建一个下载任务，请耐心等待。

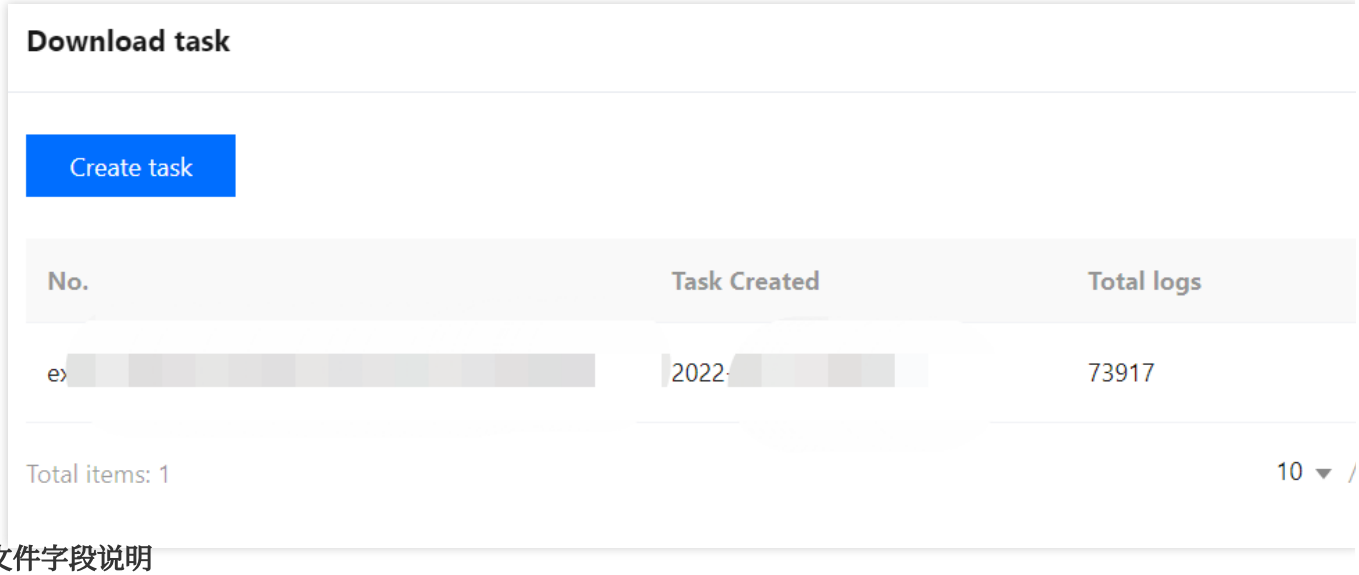
单次最多下载100万条日志，如果您需要下载的日志超过100万条，建议您分多次任务进行下载。

当选择泛域名（如：*.abc.com）时，所有关联子域名（以.abc.com结尾）的日志也将会被下载。

最多创建五条下载任务，请注意下载的任务数。



3. 在下载任务页面，单击**查看任务**，可以查看下载任务的序号、创建时间、日志总数等信息。



日志文件字段说明

字段名	说明
domain	所属泛域名
bytes_sent	响应大小，包含响应头，单位字节，下行带宽
method	客户端请求方法
request_time	请求耗时，客户端请求达到 Web 应用防火墙和从 Web 应用防火墙返回需要的时间。
http_connection	HTTP 请求的 Connection 头
upstream_connect_time	客户端请求从 Web 应用防火墙到源站需要的连接时间
uuid	HTTP 请求唯一标识
upstream_addr	请求经过的上游服务器 IP

host	客户端请求域名
upstream_response_length	上游服务器返回的响应长度
schema	请求协议，HTTP 或者 HTTPS
http_user_agent	请求 UA
headers	HTTP 请求的头部
url	请求的 uri，客户端完整请求路径中，域名后第一个“/”到“?”之间的内容
http_x_forwarded_for	出经过的所有代理
http_referer	源页面
body	请求的 body 数据
remote_addr	请求者 IP
cookie	请求的 cookie 信息，最大长度为 1K
bot_client_ip	bot 检测使用到的客户端 IP，一般和 remote_addr 一致
request_length	请求的大小，上行带宽
http_accept	HTTP 请求的 Accep t头
status	Web 应用防火墙返回给客户端的响应状态码。
protocol	HTTP 协议版本，例如：1.1、1.0 和 2.0等
msec	请求发生时候的时间戳
pipe	请求的 PIPE，nginx 的内置变量
content_type	HTTP 请求的 Content-Type 头
time_local	NGINX 的本地可读性的时间字符串
upstream_response_time	客户端请求从源站返回到 Web 应用防火墙需要的时间。
server_addr	WAF 的引擎内网 IP
edition	WAF 的版本，分成 sparta-waf,clb-waf,cdn-waf
upstream_status	源站返回给 Web 应用防火墙的响应状态码。
body_bytes_sent	响应体大小

query	HTTP 请求的 Query String，最大长度为 1K

日志投递

最近更新时间：2023-12-29 14:46:46

功能简介

日志投递功能用于将日志数据投递到 CLS（日志服务）、CKafka（消息队列），助力挖掘日志数据价值，满足用户日志运维诉求。日志投递支持当前 WAF 引擎采集到的全部访问日志字段数据，用户只需要在 WAF 控制台进行简单配置，即可完成访问日志数据准实时投递服务。如需要非标定制投递字段请 提交工单 申请。

说明

如使用日志投递时出现异常，请 联系我们 进行处理。

日志投递支持攻击日志、访问日志的 付费 投递，需分别开启。

完成投递到CLS或CKafka的配置后，还需要参考开启日志投递相关操作，开启攻击日志/访问投递设置。

使用日志投递功能和使用日志服务功能不冲突，无论是否开启日志服务都可以开启和使用日志投递功能（建议根据业务需要开启）。

日志投递至 CLS

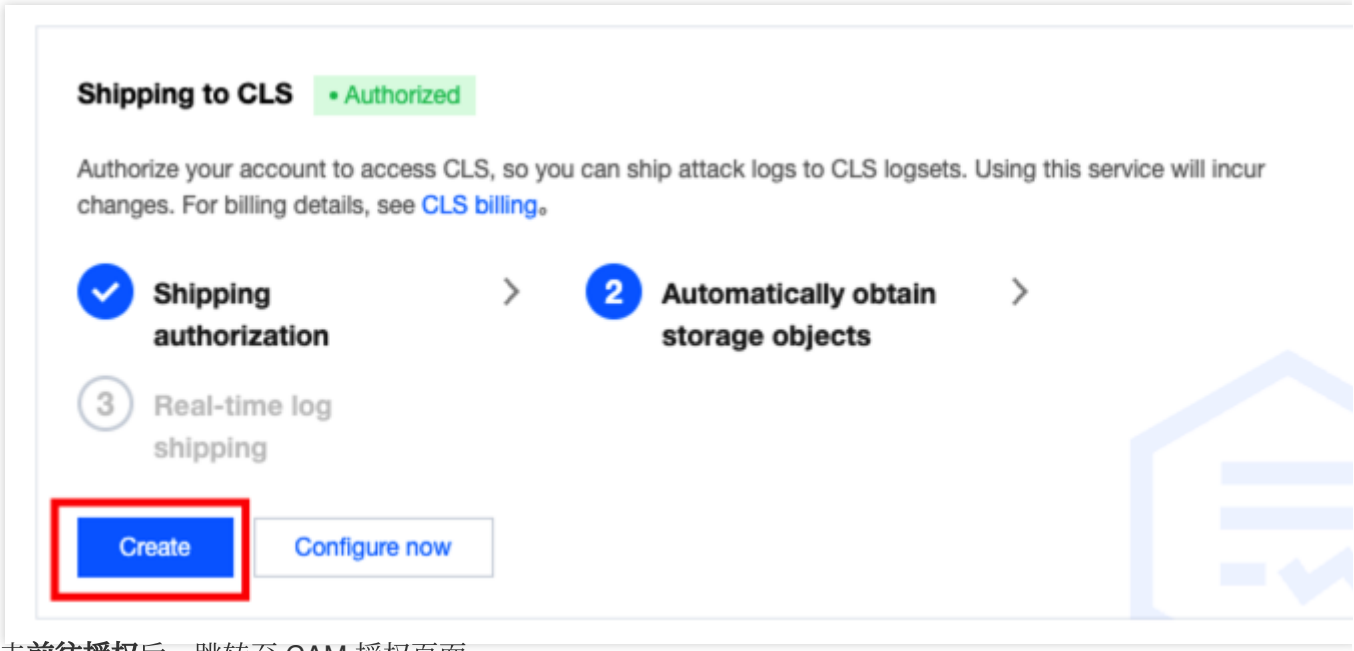
投递至 CLS 日志服务需要提前开通 CLS 日志服务并且对 Web 应用防火墙进行授权。

说明

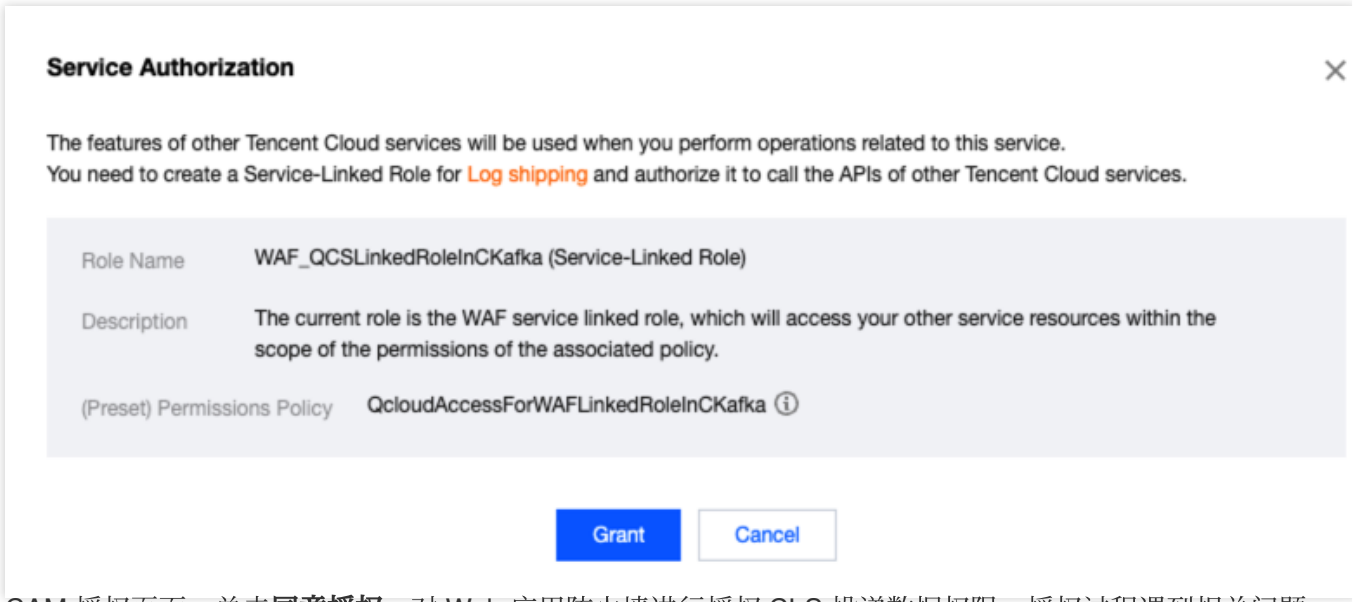
已开通 CLS 日志服务的可以直接跳转至 步骤三 授权指引界面。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，对应选择选择**访问日志 / 攻击日志 > 日志投递**。
2. 如果没有开通 CLS 服务，请单击**立即开通**，跳转到 CLS 服务开通页面进行开通，详情见 CLS 日志服务文档。
3. 授权 WAF 投递数据至 CLS 服务。

3.1 在日志投递页面的投递至 CLS 模块中，单击**立即配置**，唤起授权弹窗。

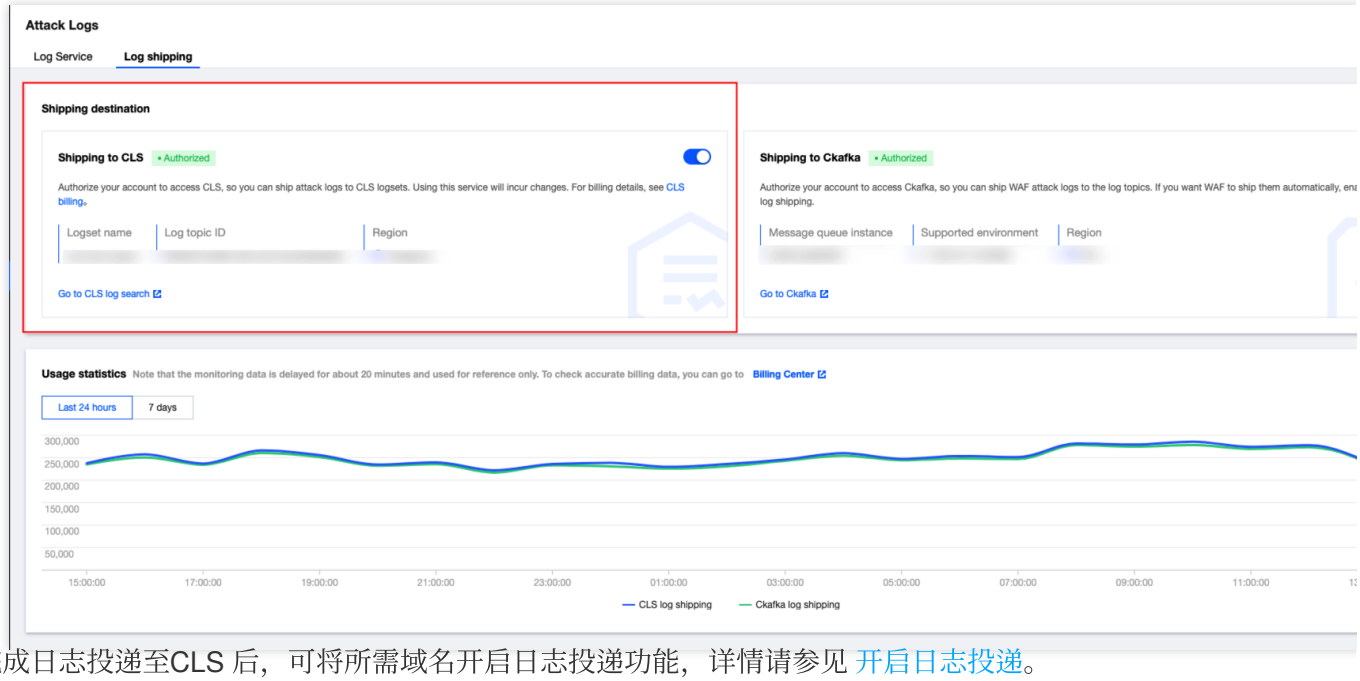


3.2 单击**前往授权**后，跳转至 CAM 授权页面。



3.3 在 CAM 授权页面，单击**同意授权**，对 Web 应用防火墙进行授权 CLS 投递数据权限。授权过程遇到相关问题，请参考 CAM 管理文档。

3.4 单击同意授权后，可以返回日志投递页面单击前往配置，选择投递地域和日志主题，单击**确认**完成配置。或单击**立即创建**，自动创建 WAF 日志集 waf_post_logset 并支持将 WAF 日志自动投递到该日志主题中。详情请参见 日志服务控制台。



3.5 完成日志投递至CLS 后，可将所需域名开启日志投递功能，详情请参见 开启日志投递。

说明

如授权状态异常可以 提交工单 联系我们对异常进行处理。

日志投递至 Ckafka

前提条件

已购买腾讯云 消息队列 Ckafka 实例，按照实际日志用量来配置 Ckafka 实例的带宽规格。

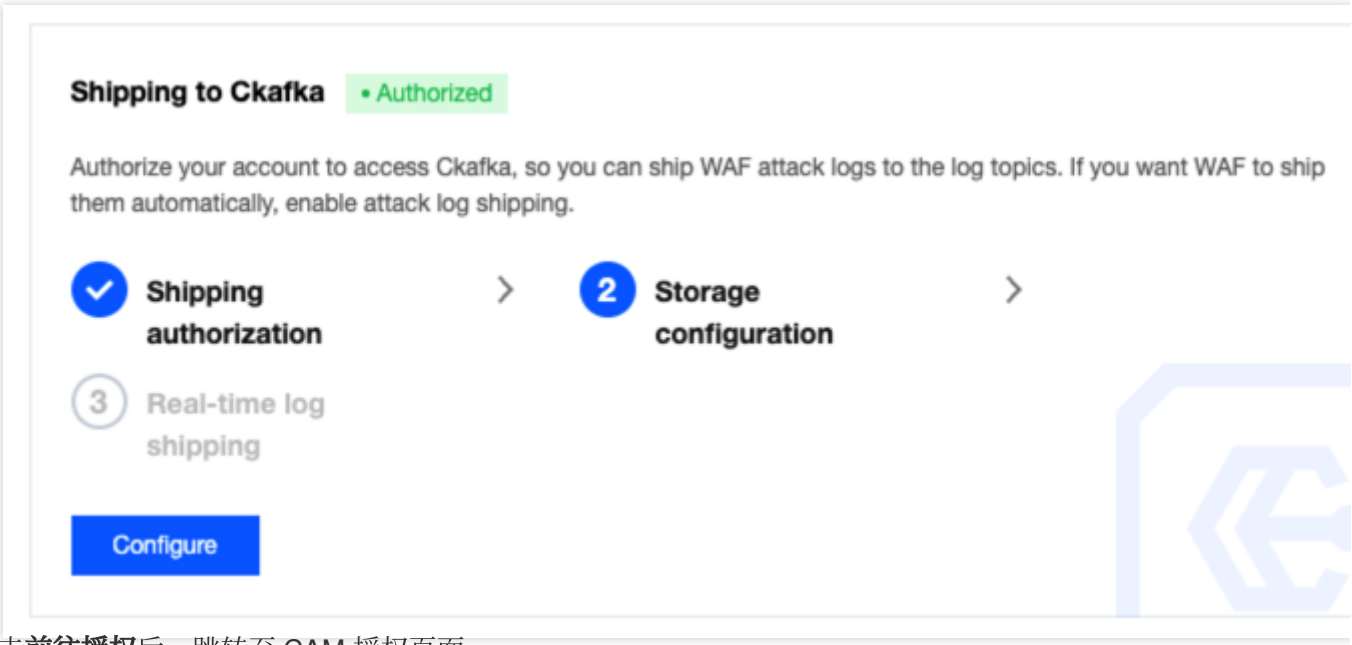
支撑环境接入 CKafka 时需 提交工单。

操作步骤

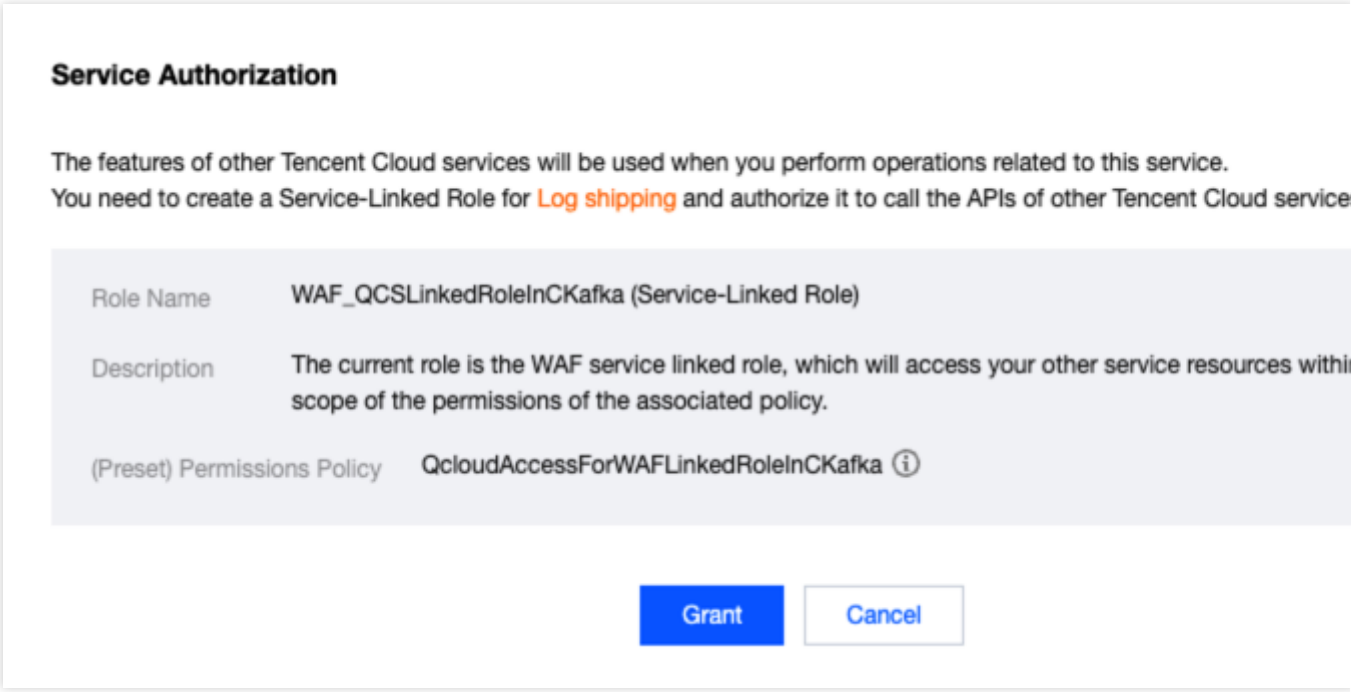
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**访问日志 > 日志投递**。

2. 授权 WAF 投递数据至 Ckafka 实例。

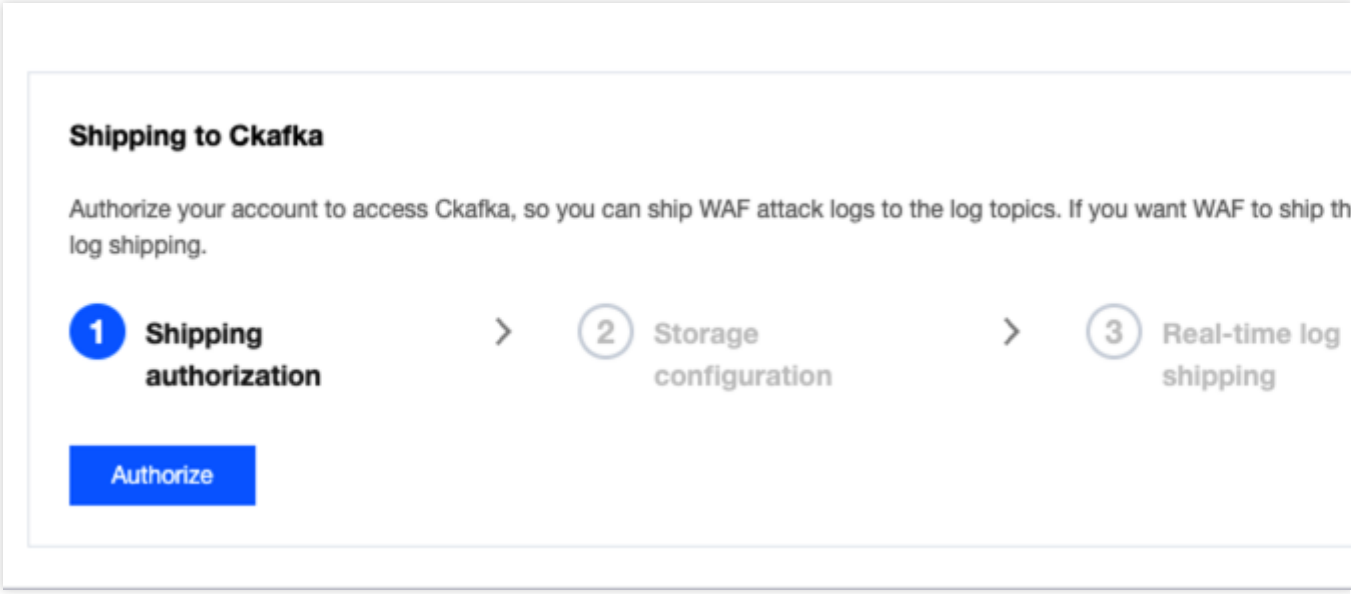
2.1 在日志投递页面的投递至 Ckafka 模块中，单击**立即配置**，唤起授权弹窗。



2.2 单击**前往授权**后，跳转至 CAM 授权页面。



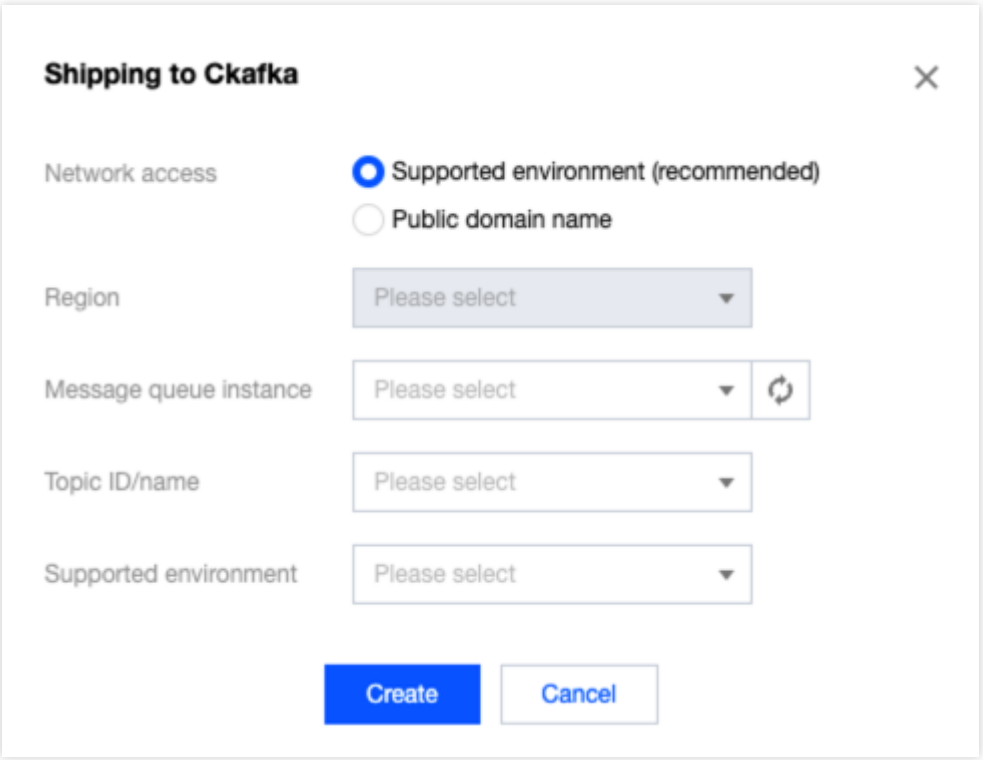
2.3 在 CAM 授权页面，单击**同意授权**，对 Web 应用防火墙进行授权 CKafka 投递数据权限。授权过程遇到相关问题，请参考 CAM 管理文档。



2.4 单击同意授权后，可以返回日志投递页面单击**立即配置**，唤起 CKafka 投递配置弹窗。

3. 在 Ckafka 投递配置弹窗中，配置相关参数，单击**确定**即可完成配置。

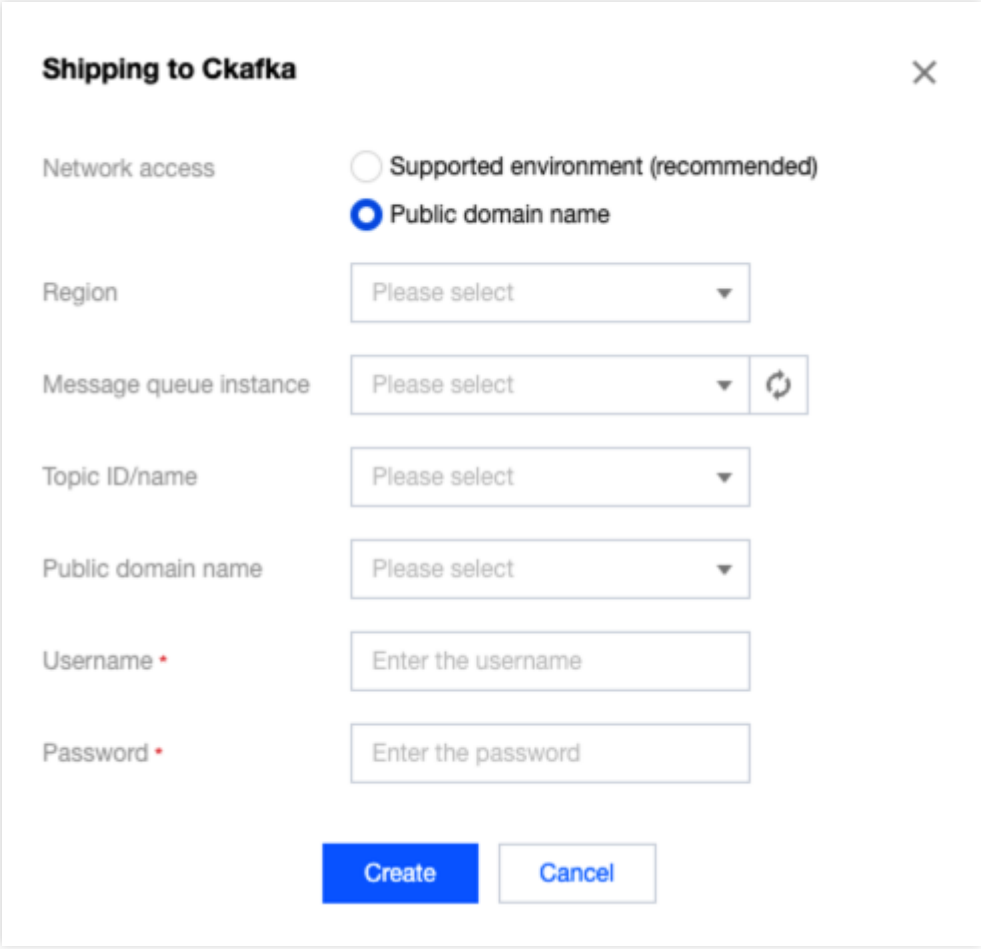
支撑环境：支撑环境接入指您在腾讯云已选购可以与 Ckafka 结合使用的产品，并选择消息队列实例和 IP 端口。



参数名称	参数说明	注意事项
地域	Ckafka 支持的地域，详情请参见 CKafka 地域和可用区。	支撑环境接入 CKafka 时需 提交工单，转 Ckafka 消息队列小助手加白名单才可以使用。

消息队列实例	当前地域下运行中的 Ckafka 实例。
Topic ID/名称	对应的 Topic ID 信息。
支撑环境接入	支撑网络的路由。

公网域名接入：选择公网域名接入，选择消息队列实例和公网域名，并输入所选消息队列实例的用户名和密码。



参数名称	参数说明
地域	Ckafka 支持的地域，详情请参见 CKafka 地域和可用区。
消息队列实例	当前地域下运行中的 Ckafka 实例。
Topic ID/名称	对应的 Topic ID 信息。
支撑环境接入	支撑网络的路由。
用户名	SASL 用户名。
密码	SASL 密码。

4. 完成日志投递至CKafka 后，可将所需域名开启日志投递功能，详情请参见 开启日志投递。

开启日志投递

当完成 日志投递至 CLS 或 日志投递至 Ckafka 后，需要将所需域名/实例开启日志投递功能。

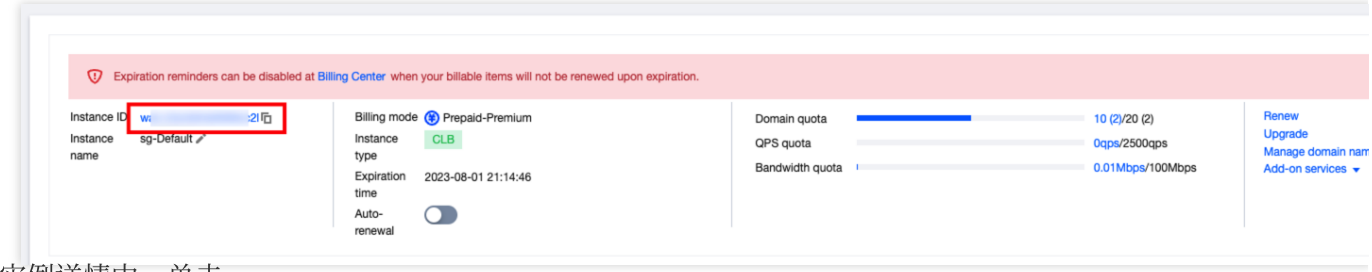
说明

攻击日志以实例维度开启投递，仅企业版及以上版本实例支持开启攻击日志投递。

访问日志以域名维度开启投递，不限实例版本，均支持配置开启访问日志投递。

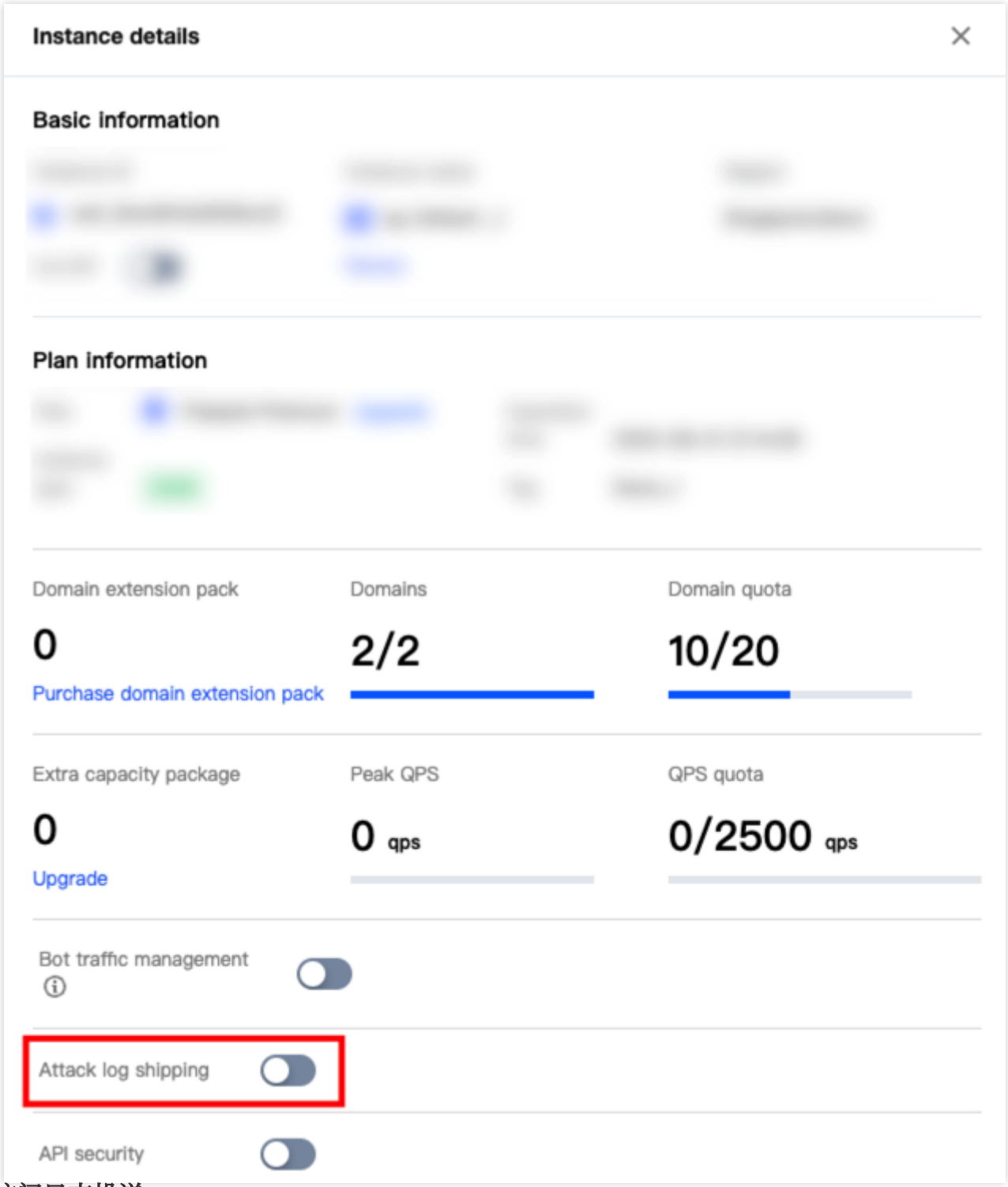
开启攻击日志投递

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**实例管理**。
2. 在实例管理页面，单击**实例名称**，唤起侧边栏。



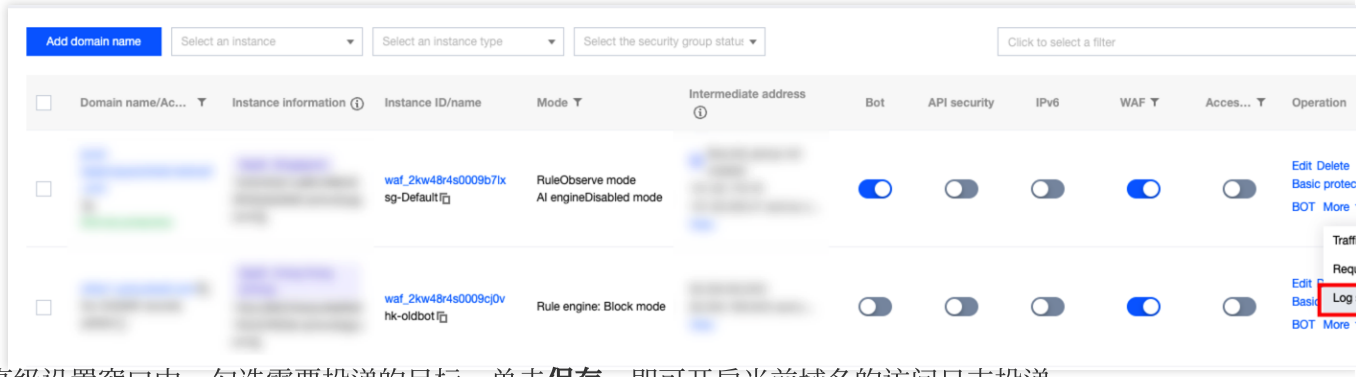
3. 在实例详情中，单击

开启攻击日志投递，即可开启当前实例的攻击日志投递。

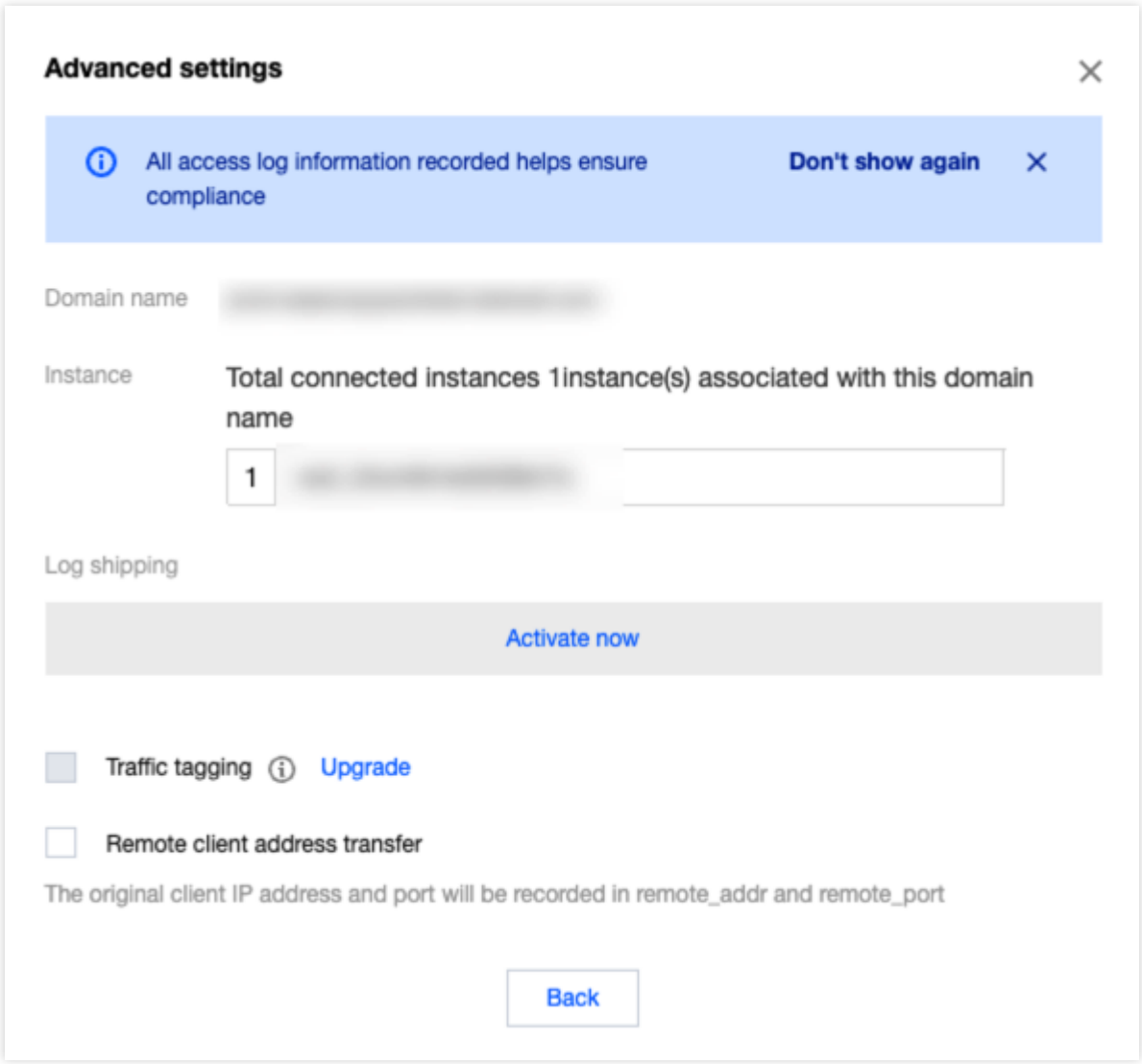


开启访问日志投递

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择**接入管理** > **域名接入**。
2. 在域名接入页面，选择所需域名，单击**更多** > **日志投递**。



3. 在高级设置窗口中，勾选需要投递的目标，单击**保存**，即可开启当前域名的访问日志投递。



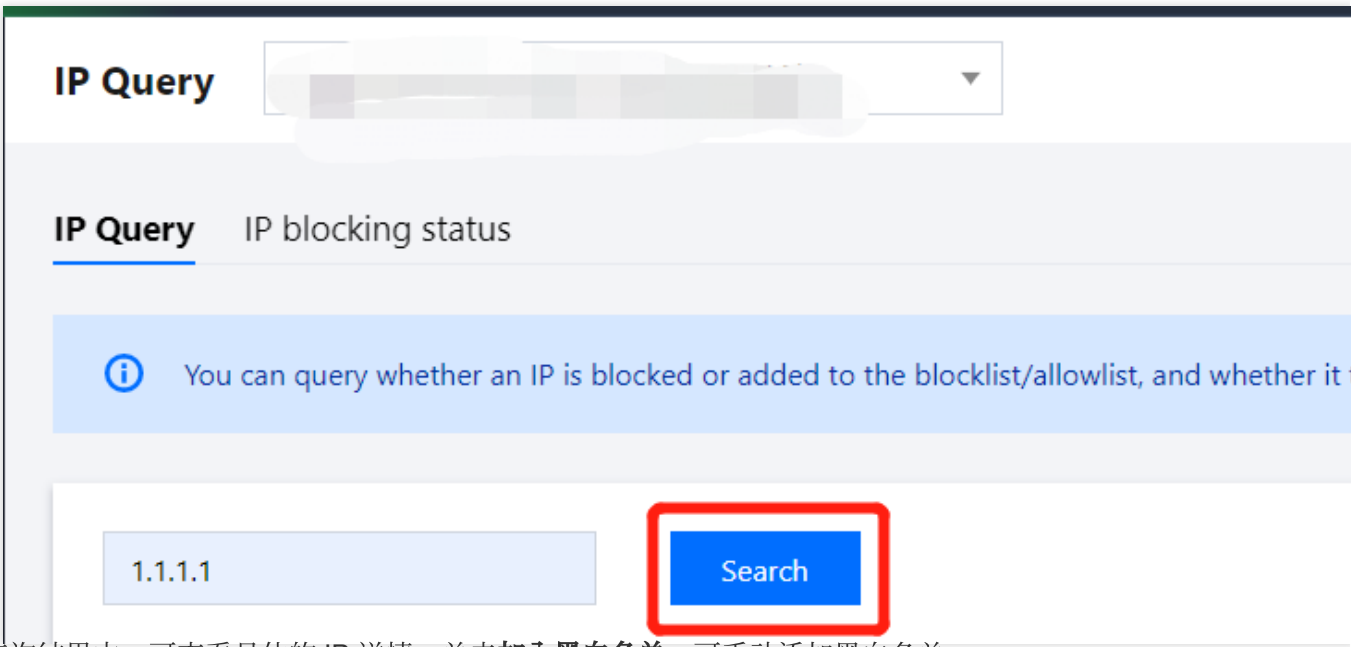
IP 查询

最近更新时间：2023-12-29 14:52:01

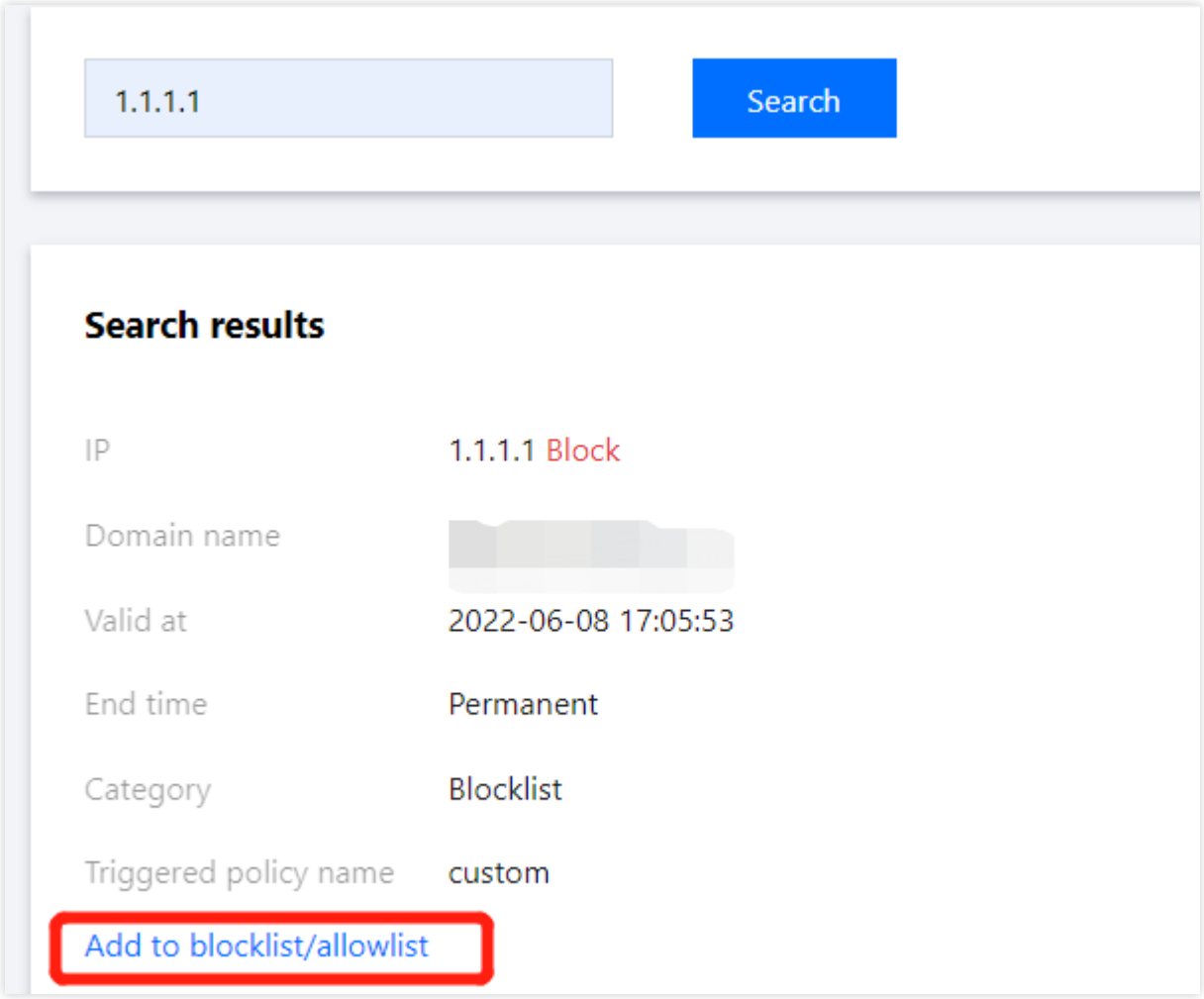
本文将介绍如何使用 IP 查询功能来查询 IP 信息和封堵状态。

IP 查询

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击 **IP 查询**。
2. 在 IP 查询页面，左上角选择需要防护的域名，输入需要查询的 IP，单击**查询**。

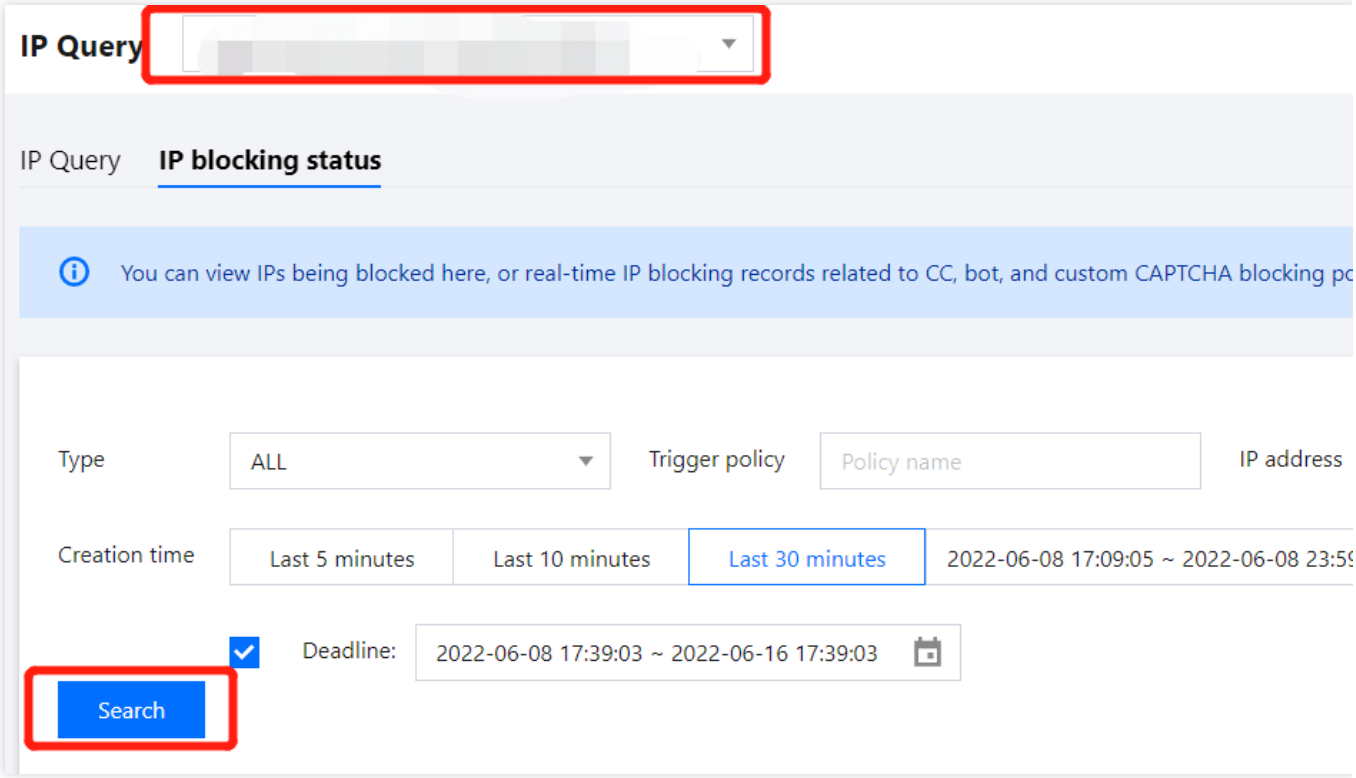


3. 在查询结果中，可查看具体的 IP 详情，单击**加入黑白名单**，可手动添加黑白名单。



IP 封堵状态

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击 **IP 查询** > **IP 封堵状态**。
2. 在 IP 封堵状态页面，可根据类型、触发策略、IP 地址、创建时间或有效截止时间，单击**查询**可筛选所需 IP 信息。



3. 单击**导出全部筛选结果**，在导出记录弹窗中，单击**导出记录**，可对查询结果进行导出。

说明：

数据量大的时候，导出可能比较慢，请耐心等待。

最多导出10000条数据。

4. 在查询结果列表中，可单击**加黑**或**加白**，对单个 IP 进行加黑或加白操作。