奇墨科技（ITQM）
WAF 应用防火墙
产品使用手册

创建时间：2024 年 3 月 14 日

修改时间：2024 年 4 月 22 日

文件修订记录

版本号	变化状态	简要说明	变更人	变更日期	备注
V0.1	C	创建文档		2024/3/14	
V1.0	A	补充功能说明		2024/3/22	

变化状态：C-创建，A-增加，M-修改，D-删除

目录

1　WAF 接入操作

1.1　接入步骤概览：

步骤 1：整理接入信息

步骤 1：域名添加

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 5：验证测试

步骤 6：业务测试

1.2　步骤 1：整理接入信息

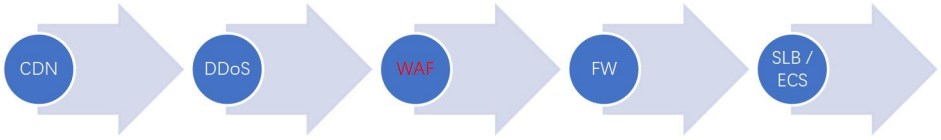
1. 确认接入域名使用的协议（http、https、websocket）、端口、证书等信息；

   a) 若使用 https，请准备证书；

   b) 若使用了 websocket，请在 WAF 域名接入高级配置中启用 websocket 支持；

   c) 若使用非 http 非标准端口号，请查阅《WAF 支持端口列表》确认端口在支持范围内。

2. 确认 WAF 接入后的流量路径，是否有高防、CDN 等设备在 WAF 前端。



   a) 若配有 CDN 或 DDoS 高防，请在 WAF 域名接入中启用代理；

   b) 若配有 CDN 或 DDoS 高防，请按上图把对应设备的配置的回源地址指向下一节点的 cname 或 IP，FW 为透明设备；

   c) 若配有 DDoS 高防，请把 DDoS 高防 IP 配置到 WAF 白名单。

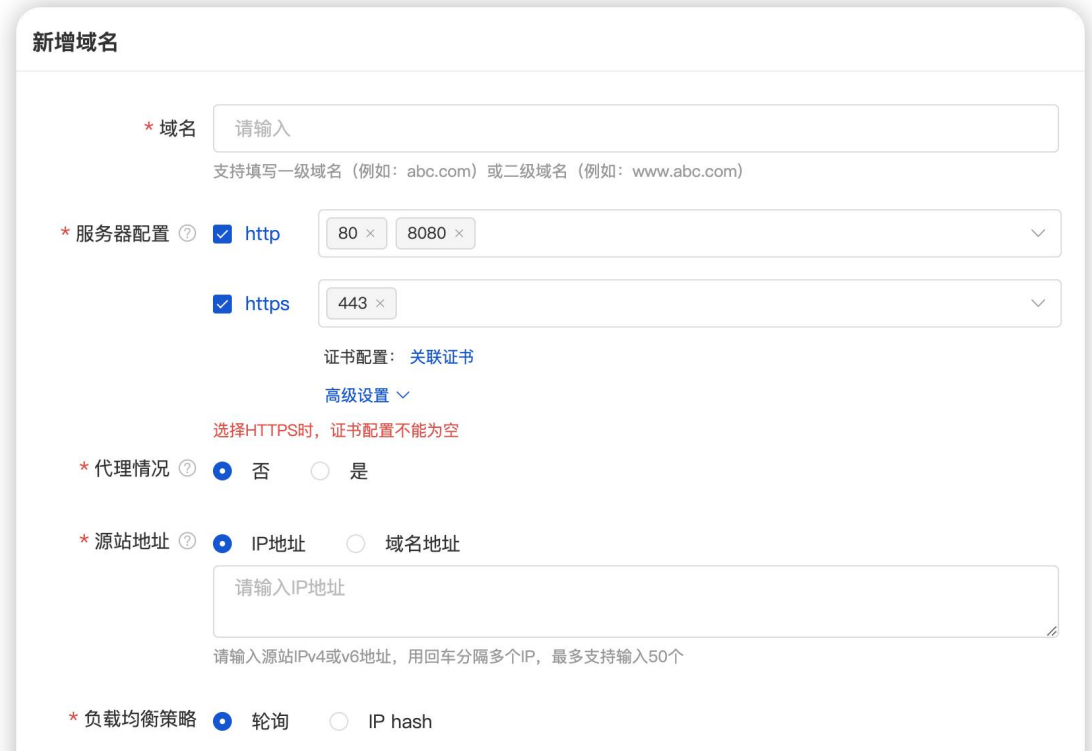
1.3 步骤 2：域名添加

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 WAF 中接入域名。

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 > 接入管理，进入域名接入页面。

2. 在域名接入页面，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

域名：在域名输入框中添加需要防护的域名 yyyyy.xxxxxxx.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/导入证书。

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 协议时可以指定配置回源端口；选择 HTTPS 暂不支持指定配置回源端口，端口和对外开放端口一致。

选择 HTTPS 协议时支持开启回源 SNI 开关，并选择保持源请求 host、修正为源站 host 或自定义 host。

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。

选择否：表示 WAF 收到的业务请求来自发起请求的客户端。WAF 直接获取与 WAF 建立连接的 IP 地址作为客户端 IP。

选择是：表示 WAF 收到的业务请求来自其他七层代理服务转发，而非直接来自发起请求的客户端。为了保证 WAF 可以获取真实的客户端 IP，进行安全分析和防护，您需要进一步设置客户端 IP 判断方法。

读取请求 Header 字段 X-Forwarded-For（XFF）中的第一个 IP 地址作为客户端 IP。

获取网络层的 remote_ip 作为客户端的源 IP，防止 XFF 伪造。

获取指定 header 字段的 IP 地址。

说明：

推荐您在业务使用自定义 Header 存放客户端 IP，并在 WAF 中配置对应 Header 字段。该方式可以避免攻击者伪造 XFF 字段，屏蔽 WAF 的防护规则，有效提高业务的安全性。

源站地址：根据实际需求选择 IP 或域名。

IP：请输入源站 IPv4 或 IPv6 地址，用回车分隔多个 IP，最多支持输入 50 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，并设置不同的权重。

负载均衡策略：默认为轮询方式，可根据实际需求选择轮询、 IP Hash 或加权轮询方式。

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 也将降级为 1.1。

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

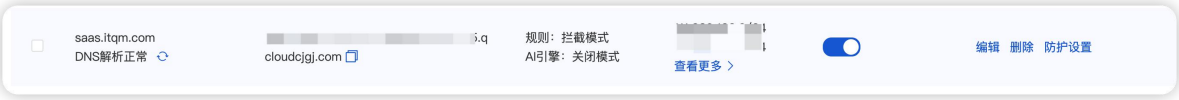
开启健康检查：企业版以及以上版本，支持开启基于回源 IP 的四层健康检查机制。

开启 XFF 重置：支持清空 X-Forwarded-For 字段值，请确认 WAF 前无七层代理服务后开启。

5. 完成配置后，可在域名接入页面看到新添加的域名。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。

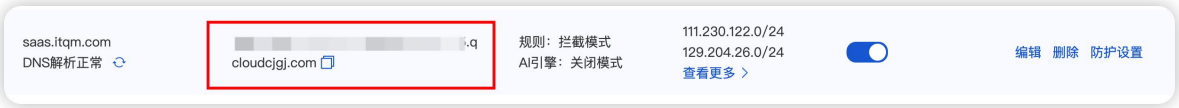


1.4 步骤 3：本地测试

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。

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。

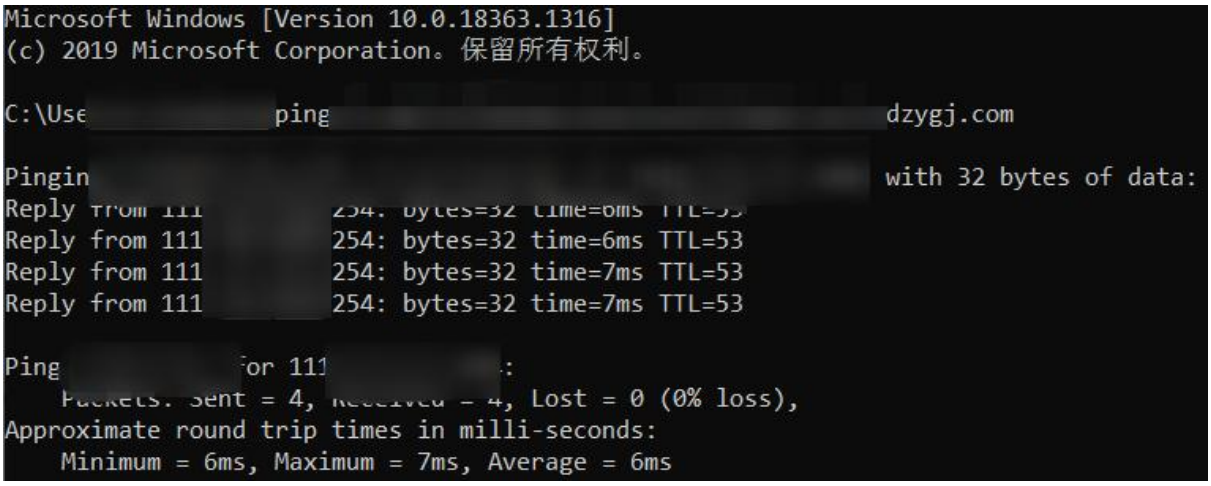
1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择资产中心 > 接入管理，在域名列表中查看接入域名的 CNAME 地址。



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>。

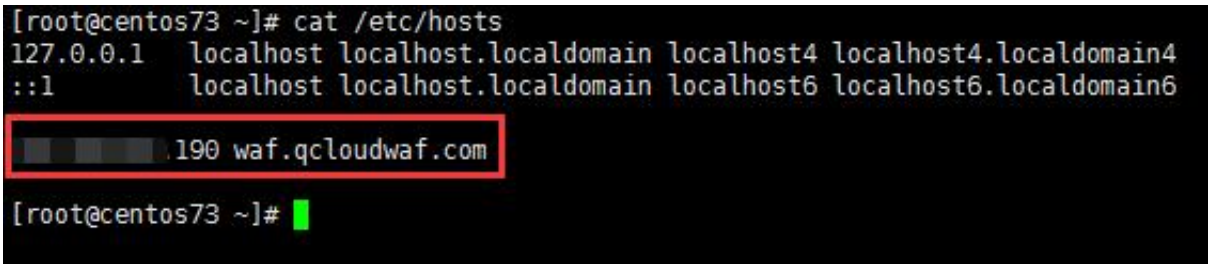


1.3 在 ping 命令的返回结果中,记录域名对应的 WAF IP 地址,即为后续操作需要的 VIP 地址。

2. 修改 hosts 文件。

在 Windows 下修改 C:\Windows\System32\drivers\etc\hosts，增加条目。 格式：<WAF VIP 地址> + 空格 +<接入 WAF 中被防护域名>

在 Linux 下 修改 /etc/hosts，增加条目。 格式：<WAF VIP 地址> + 空格 +<接入 WAF 中被防护域名>



在 MAC 下修改 /etc/hosts，打开访达，单击前往 > 前往文件夹， 修改 /etc/hosts，在弹框中输入 /etc，进入 /ect 目录且修改下面的 hosts 文件。

格式：<WAF VIP 地址> + 空格 +<接入 WAF 中被防护域名>

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


[redacted] www.qcloud.com
```

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。

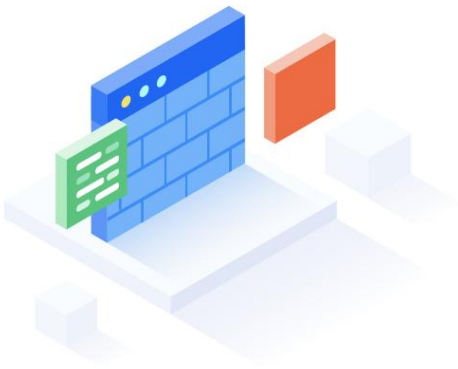
3.1 在浏览器中输入下面的网址并访问。

http://接入域名/?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。



很抱歉，您提交的请求可能对网站造成威胁，请求已被管理员设置的策略阻断

本页面为腾讯T-Sec Web应用防火墙(WAF)默认提示页面，如有疑问请联系网站管理员并提供UUID信息

您的请求UUID为 [redacted]

1.5 步骤 4：修改 DNS 解析

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。

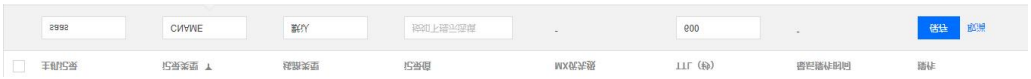
为了使公网用户访问网站的流量经过 Web 应用防火墙的防护，需要修改 DNS 的解析记录。下面以在腾讯云 DNS 解析 DNSPod 上修改测试站点 waf.qcloudwaf.com 的 DNS 解析为例，说明配置步骤。

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。

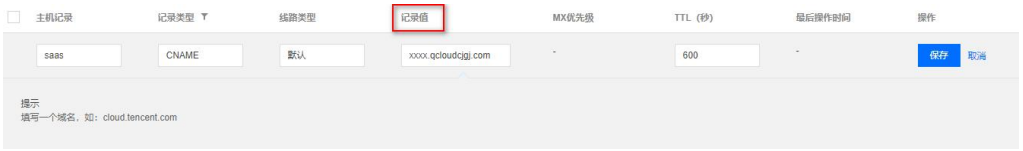
3. 在当前配置页面中填写相应信息。

3.1 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。



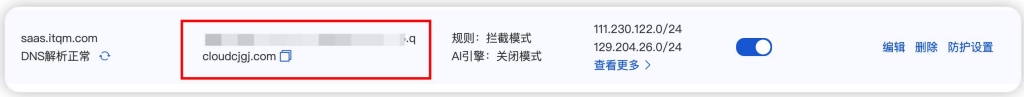
3.2 记录类型选择 CNAME。

3.3 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。



说明：

CNAME 域名可以前往 接入管理 > 域名接入页面，选择目标域名，在接入信息列获取。



3.4 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。

1.6 步骤 5：设置安全组

本文档将指导您如何设置安全组，SAAS-WAF 中需要用户在各产品安全组（如：CLB、防火墙等安全设备）中放通 WAF 回源 IP，仅允许来自 Web 应用防火墙的流量访问网站。

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。

1.7 步骤 6：验证测试

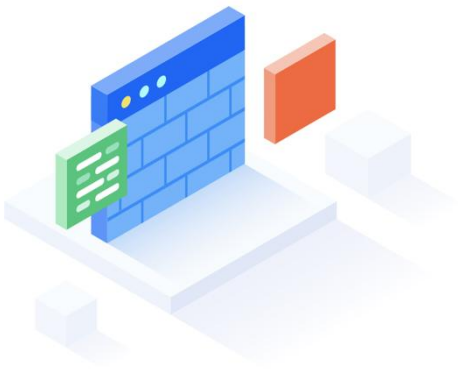
本文档将指导您如何验证 SaaS 型 WAF 是否生效。

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。



1.8 步骤 7：业务测试

本文档将指导您如何验证 SaaS 型 WAF 接入后确保业务访问不被拦截。

对接入的业务系统的关键业务流程进行验证，确保攻击日志中不存在拦截的记录。

2 WAF 维护操作

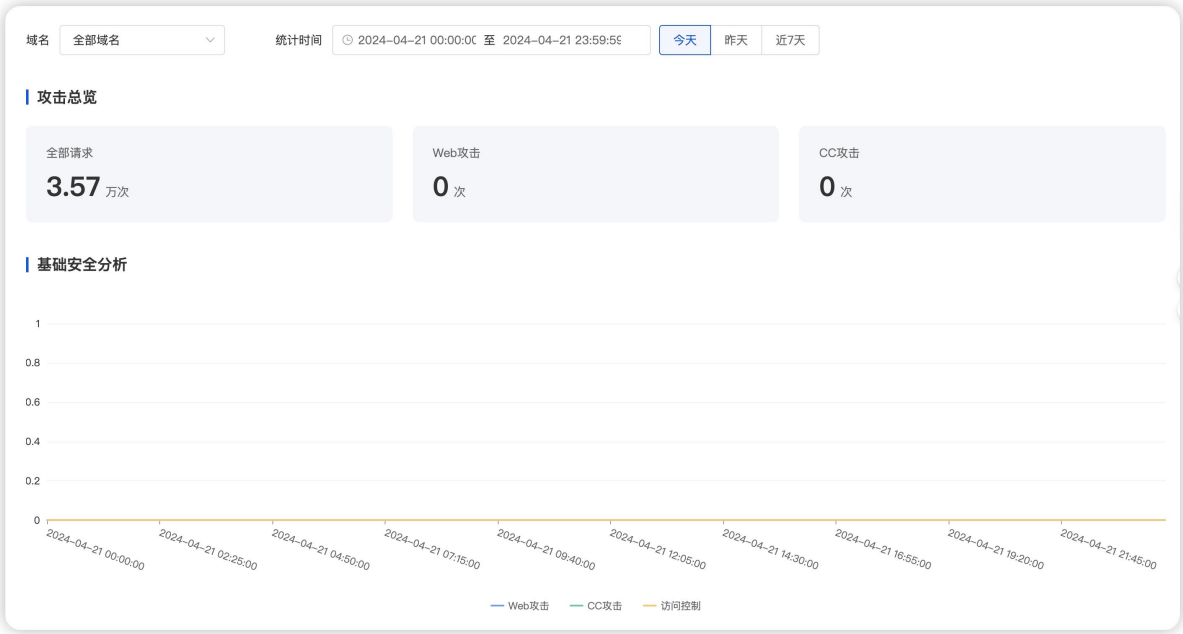
2.1 安全概览

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，左上角选择对应实例或域名，即可查看该实例或域名的概览信息。

2.2 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)、攻击类型占比等信息。

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。

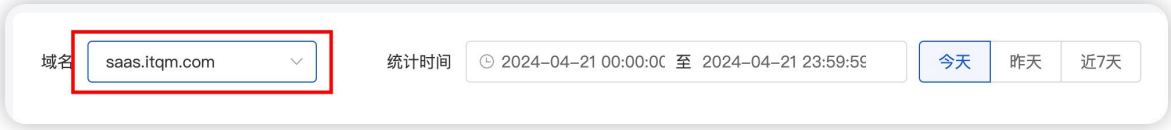
攻击来源 IP TOP5(次) ：展示全部实例中受到攻击最多的 5 个 IP。

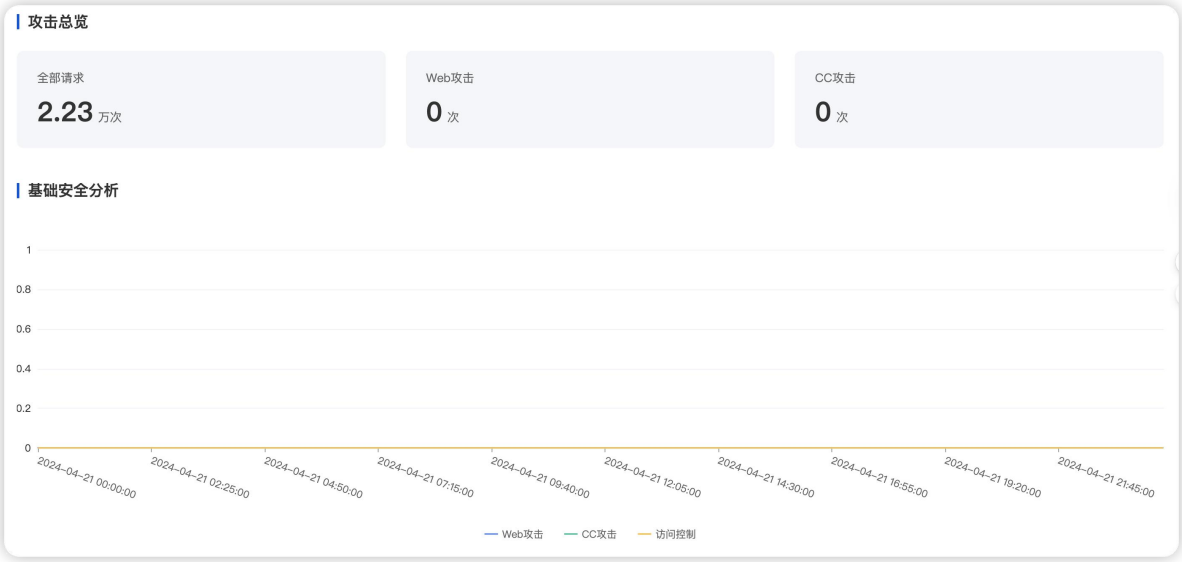
域名 CC 攻击次数 TOP5(次) ：展示全部实例中受到攻击最多的 5 个域名。

攻击类型占比：展示全部实例中攻击类型的分布。

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受到攻击数，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)、攻击类型占比等信息。

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。

攻击类型占比：展示全部实例中攻击类型的分布。

2.3 黑白名单配置

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。

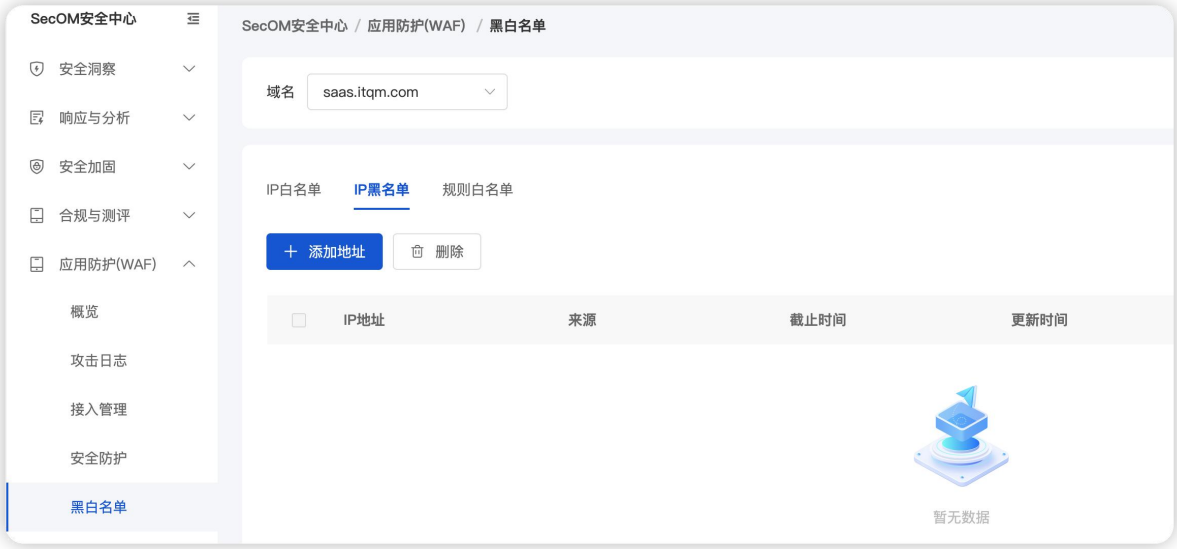
同时，可以添加基于域名的黑白名单或基于全局的黑白名单，生效优先级说明如下所示：

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。

添加 IP 黑名单

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 > 黑白名单。
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。



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：

选择域名为全局时，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分别为：1000 条/域名、5000 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。

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。

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。

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

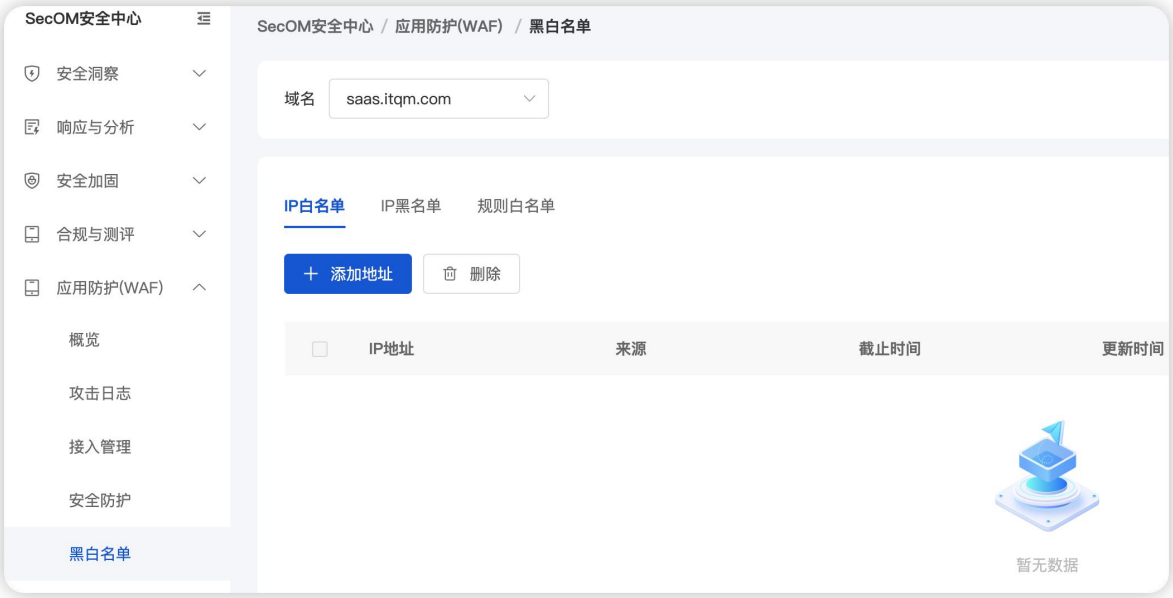
此操作将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

3. 在“确认删除”弹窗中，单击确定，即可删除地址。

添加 IP 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 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。

参数说明

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

选择域名为全局时，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分别为：1000 条/域名、5000 条/域名，每个 IP 地址或者 IP 段占用一条额度。

截止时间：长期生效或限定日期。

备注：自定义，50 个字符以内。

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。

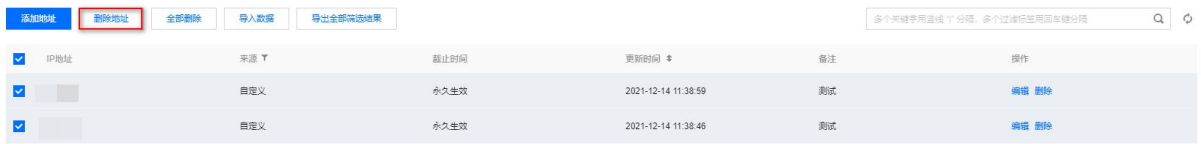
说明

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

此操作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。

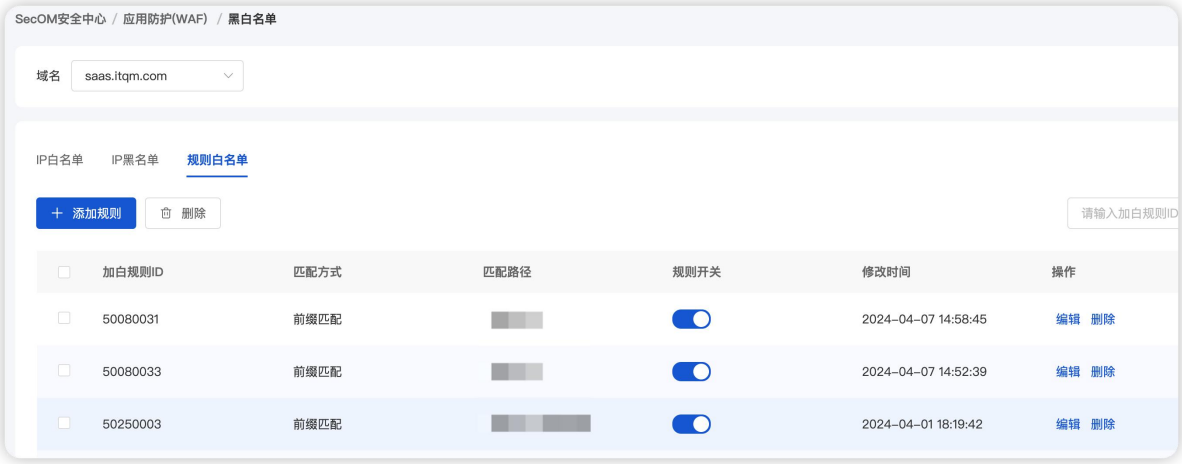
2.4 规则白名单

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，加白该规则后就不会被拦截。

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。

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。

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：

白名单规则 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。获取方法如下所示：

在安全防护页面，选择所需规则 ID，复制。

在日志页面，选择所需数据，复制该数据的 rule_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。

2.5 攻击日志

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。

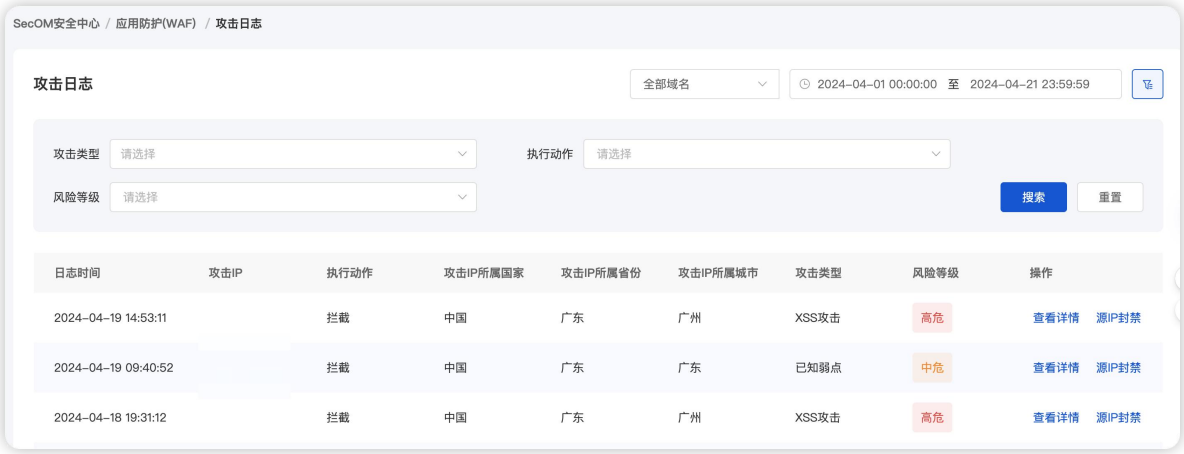
背景信息

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，选择攻击日志。

2. 在日志服务页面，您可以根据需要，选择域名、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
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、重定向、人机识别、拦截四种类型。
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。

3. 设置完成检索条件，单击检索，即可查看检索结果。

日志时间	攻击IP	执行动作	攻击IP所属国家	攻击IP所属省份	攻击IP所属城市	攻击类型	风险等级	操作
2024-04-19 14:53:11		拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁
2024-04-19 09:40:52		拦截	中国	广东	广东	已知弱点	中危	查看详情 源IP封禁
2024-04-18 19:31:12		拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁
2024-04-18 18:56:35		拦截	中国	湖南	长沙	一般攻击	高危	查看详情 源IP封禁
2024-04-18 18:55:50		拦截	中国	湖南	长沙	一般攻击	高危	查看详情 源IP封禁
2024-04-18 18:55:14		拦截	中国	广东	广州	XSS攻击	高危	查看详情 源IP封禁

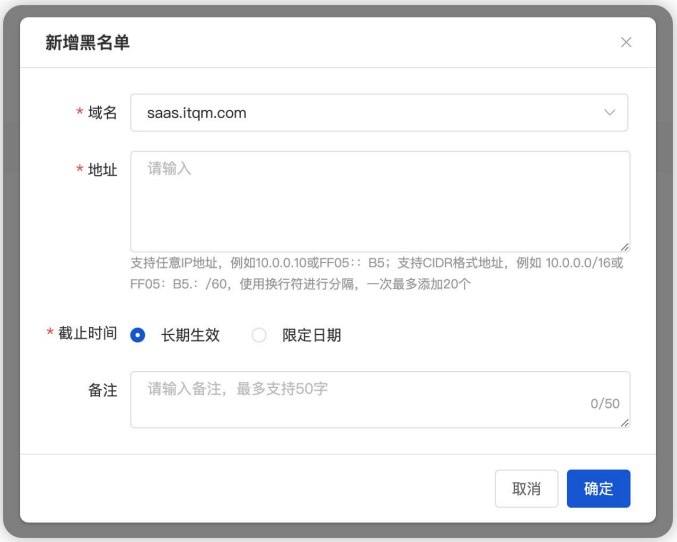
分析攻击日志

1. 在攻击日志数据列表右方，单击查看详情，即可查看日志详情。

攻击处置

1. 在攻击日志数据列表中，支持单击操作列中的源 IP 封禁，快速添加处置规则。

源 IP 封禁：支持一键添加 IP 黑名单，拦截对应 IP 的访问，完成修改后，单击确定。



3 功能说明

3.1 WAF 支持端口列表

WAF 套餐端口支持情况，可以在控制台进行查看并配置。

1. 登录 Web 应用防火墙控制台 ，在左侧导航中，选择 Web 安全防护 > 防护设置，进入防护设置页面。

2. 在防护设置页面，单击添加域名，进入添加域名页面。

3. 在添加域名页面的“服务器配置”中，选择对应的协议查看并配置端口，一个域名最多可配置 5 个端口。

WAF 高级版默认支持 HTTP（80/8080）和 HTTPS（443/8443）标准端口防护，不支持非标端口。

WAF 企业版和旗舰版套餐中除了默认支持 HTTP（80/8080）和 HTTPS（443/8443）标准端口防护外，还支持非标端口。 企业版和旗舰版支持的所有端口详情如下：

协议名称	端口

HTTP 协议	80、81、82、83、84、85、86、87、88、89、97、800、805、808、1000、1090、2020、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7007、7008、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7040、7070、7081、7082、7083、7088、7097、7510、7621、7777、7800、8000、8002、8003、8004、8005、8006、8007、8008、8009、8010、8011、8012、8020、8021 、8022、8060、8025、8026、8060、8077、8078、8080、8081、8082、8083、8086、8087、8088、8089、8090、8106、8181、8182、8184、8210、8215、8334、8336、8445、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9182、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、10000、10001、10080、10083、12601、20080、20083、25060、28080、28080、33702、48800、52301
HTTPS 协议	443、4443、5100、5200、5443、6443、7443、8084、8085、8091、8442、8443、8553、8663、9443、9550、9553、9663、10803、18980

3.2 日志详情字段说明

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。

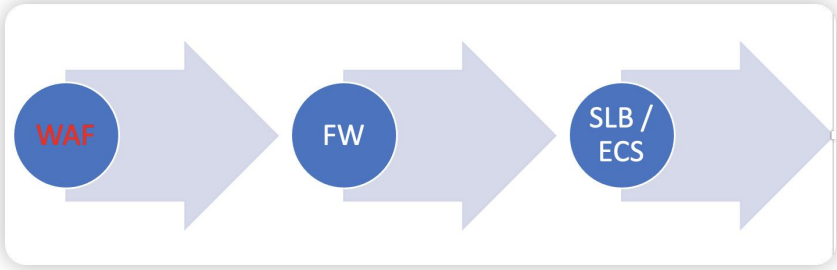
字段名称	字段说明
scene_id	场景 ID：触发防护策略的场景 ID。
scene_module	场景模块：触发防护策略的场景模块，包括前端对抗（jsinject）、自定义规则（ucb）、智能分析（autoanalyze）。
method	请求方法：客户端攻击请求方法。
user_agent	User-Agent：攻击源 IP 向服务器表明的浏览器类型和操作系统标识等信息。
risk_level	风险等级：客户端攻击触发的风险等级，包括高危（1）、中危（2）、低危（3）三种风险等级。
status	执行状态：攻击请求的处置结果，包括观察（0）、拦截（1）、人机识别（2）、重定向（3）四种处理结果。
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	接入域名或 CLB 对象信息。
prote_domain	接入域名或 CLB 对象信息。
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。

字段名称	字段说明
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）、人机识别（2）、重定向（3）四种处理结果。
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。

字段名称	字段说明
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。
is_white	是否为情报白名单地址。
sec_chain	请求经过的安全模块及对应执行动作。

4 配置案例

4.1 接入网站架构

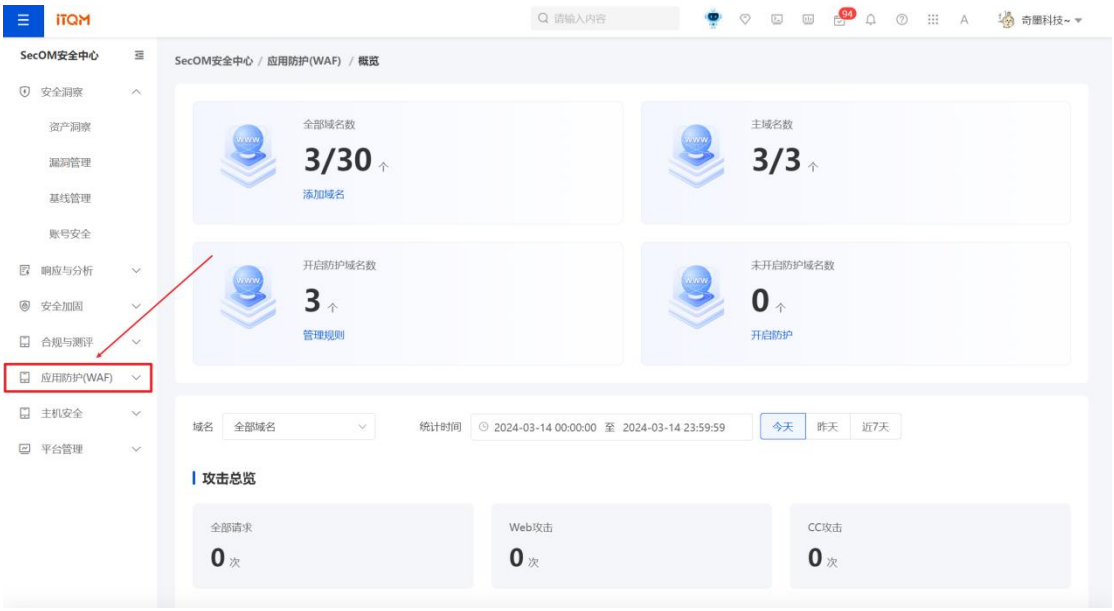


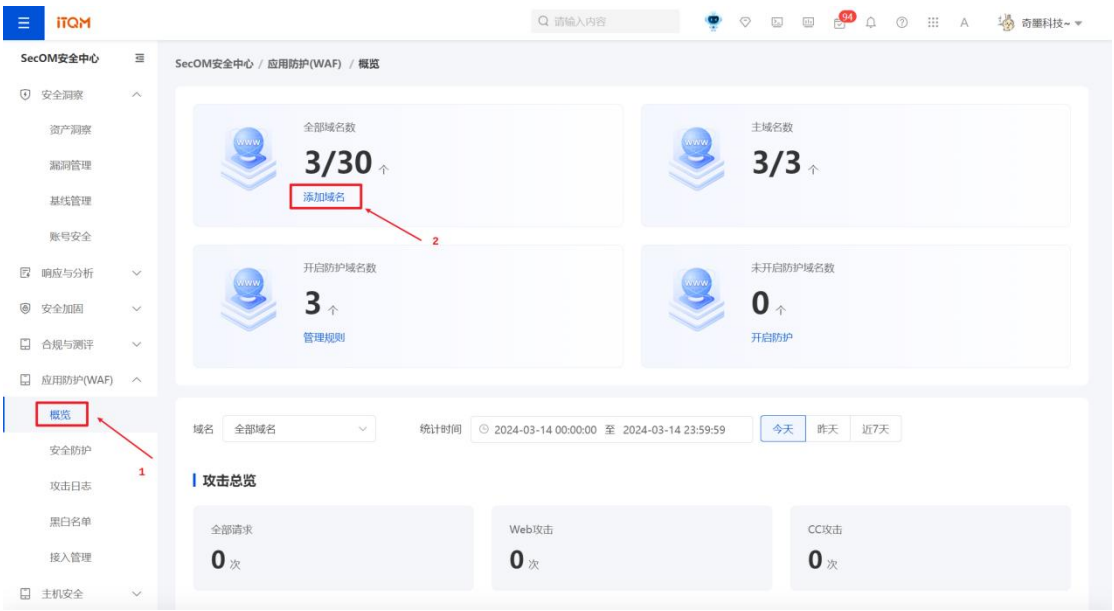
4.2 登录 ITQM 平台

访问此域名 https://saas.itqm.com，登录 ITQM 进行域名配置。

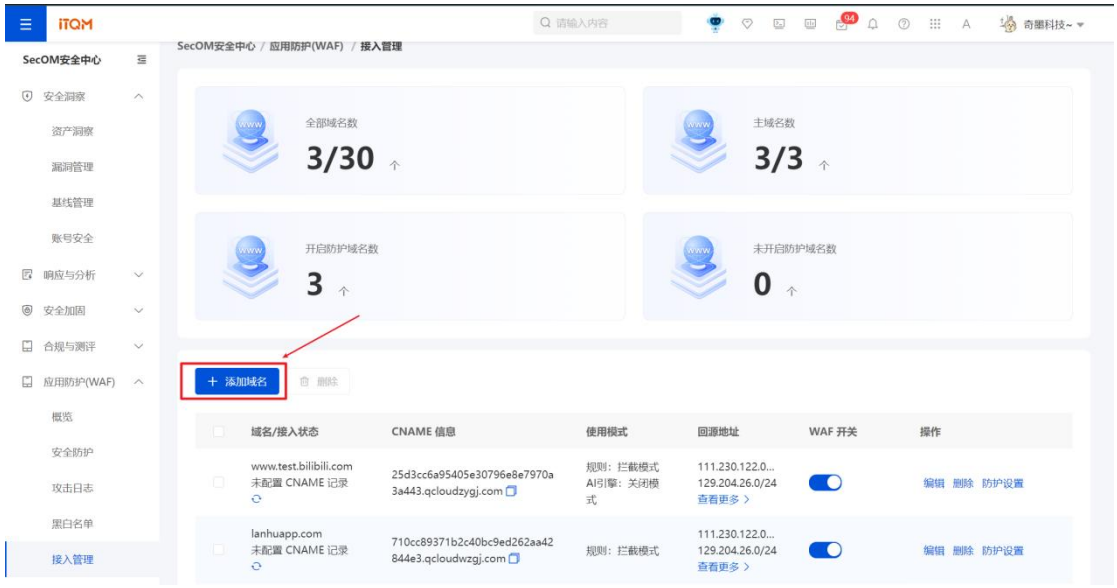
4.3 选择 SecOM 安全中心

4.4 选择应用防护（WAF）

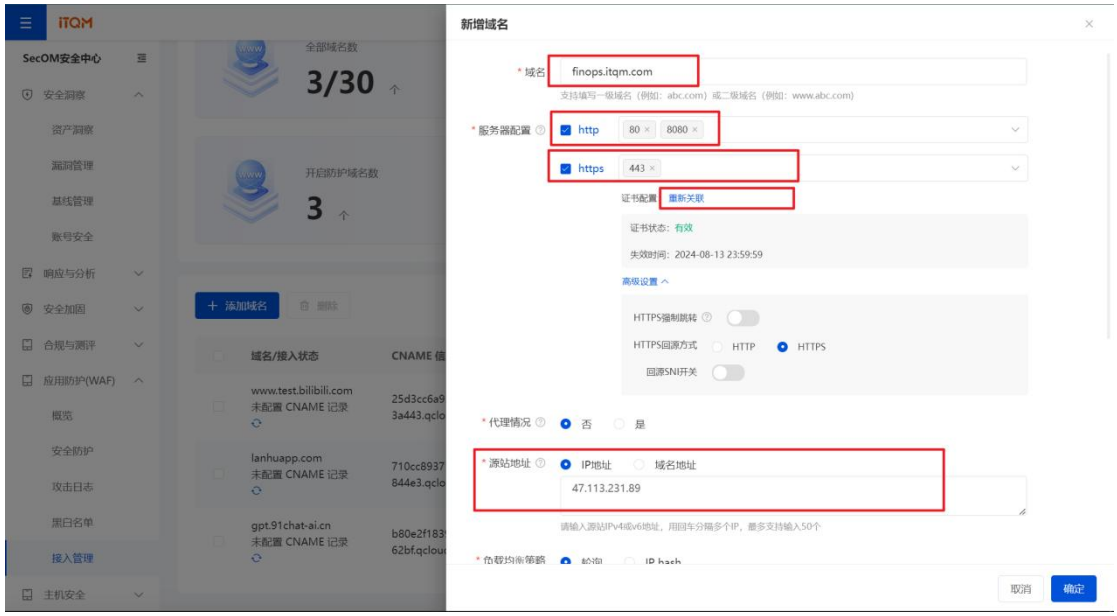




4.5 添加域名

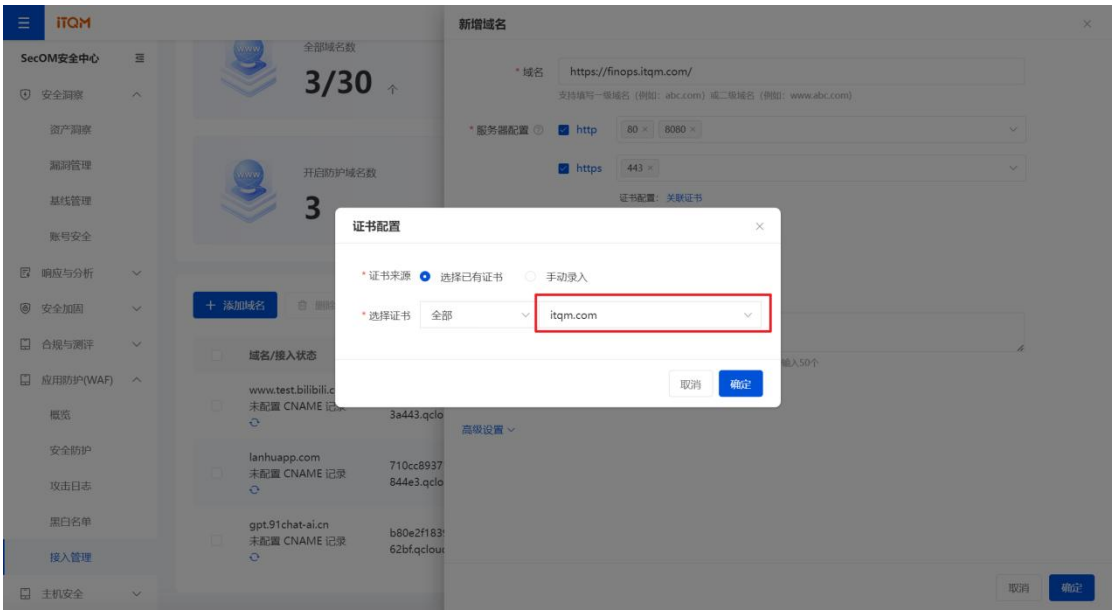


填写域名，不需要加 https://，选择【服务配置】根据现有的业务进行选择，如使用 https 则需要关联证书。

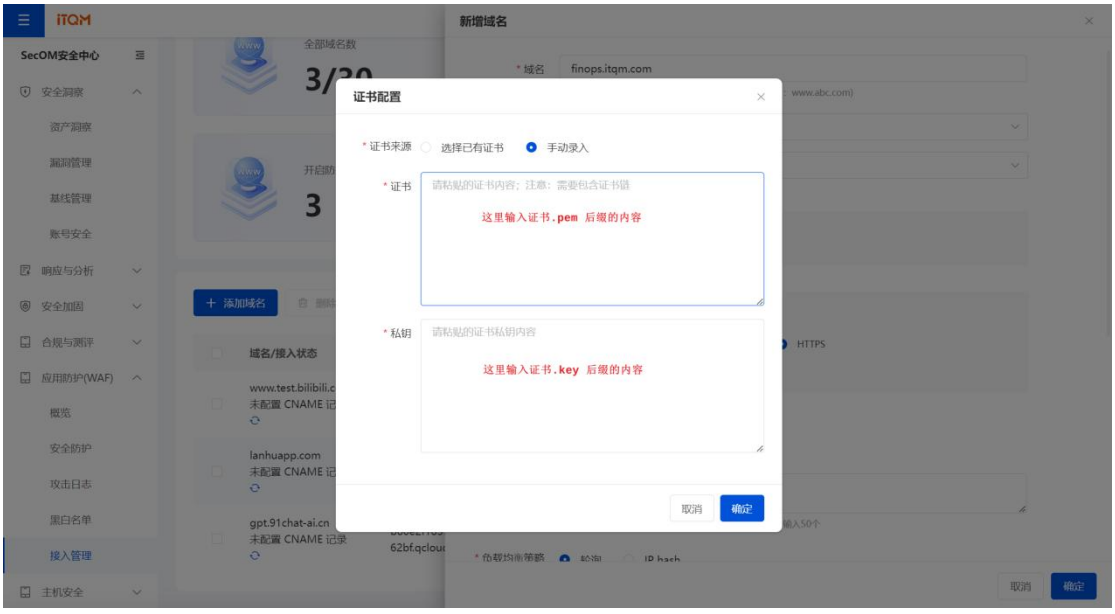


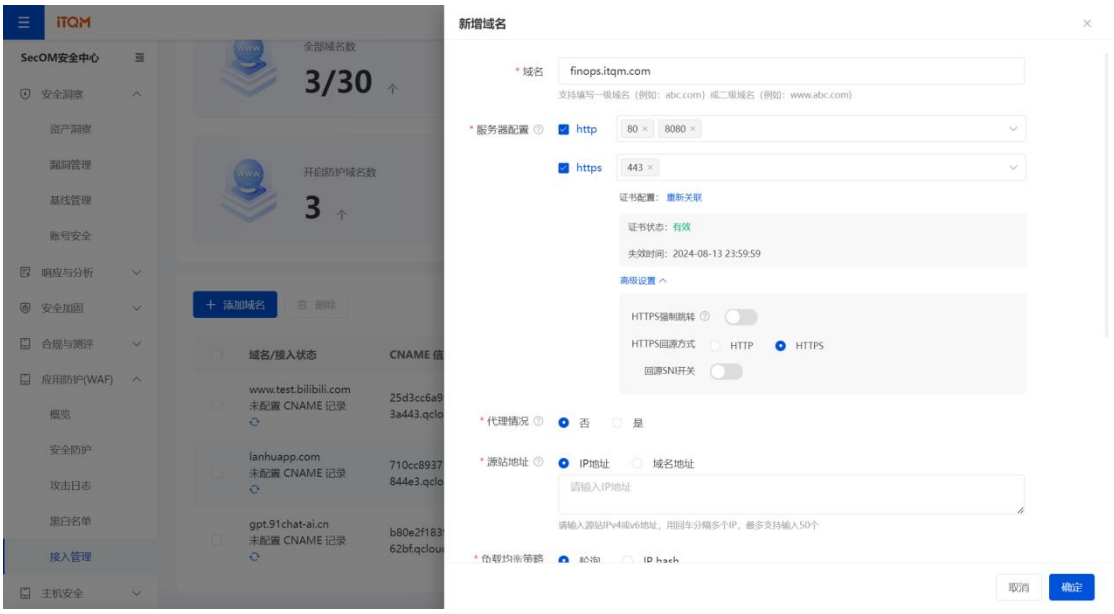
4.6 关联证书和录入证书（https）

手动录入证书，或者可选择已经导入的证书。

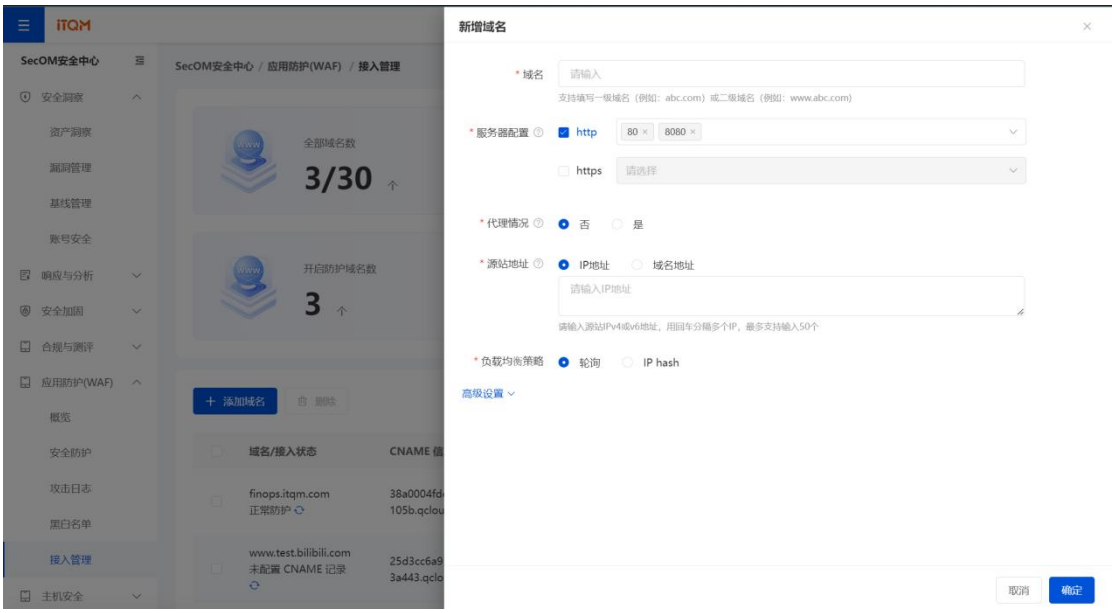


手动录入证书，证书两个文件.pem 的需要使用记事本打开将其复制进入【证书】.key 也需要使用记事本打开复制进入【私钥】当中，确认即可。使用 https 的需要关联证书，选择手动录入证书





4.7 添加域名字段说明



域名：在域名输入框中添加需要防护的域名 yyyyy.xxxxxxx.cn。

服务器配置：协议和端口可按实际情况选择。

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，根据需求选择或导入证书。

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。

源站地址：根据实际需求选择 IP 或域名。

IP：请输入源站 IPv4 或 IPv6 地址，用回车分隔多个 IP，最多支持输入 50 个。

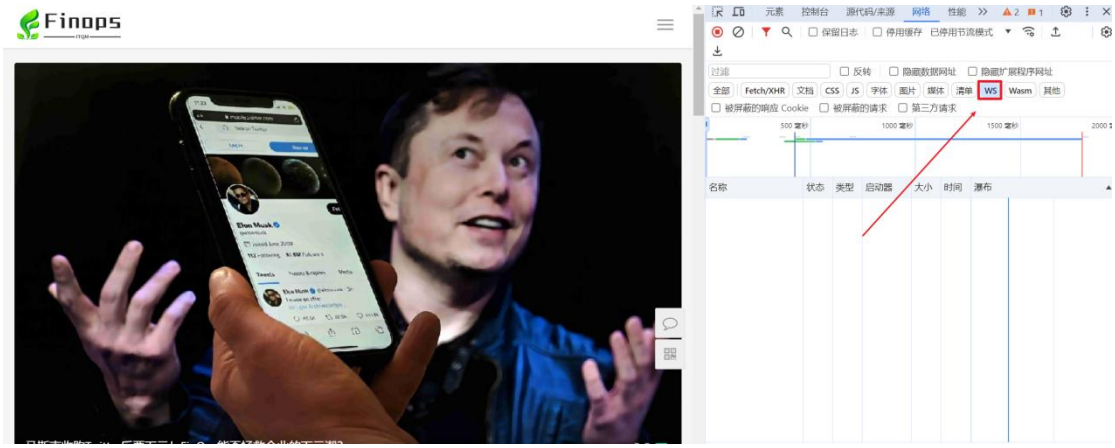
域名：请输入源站域名，注意：源站域名不能和防护域名相同。

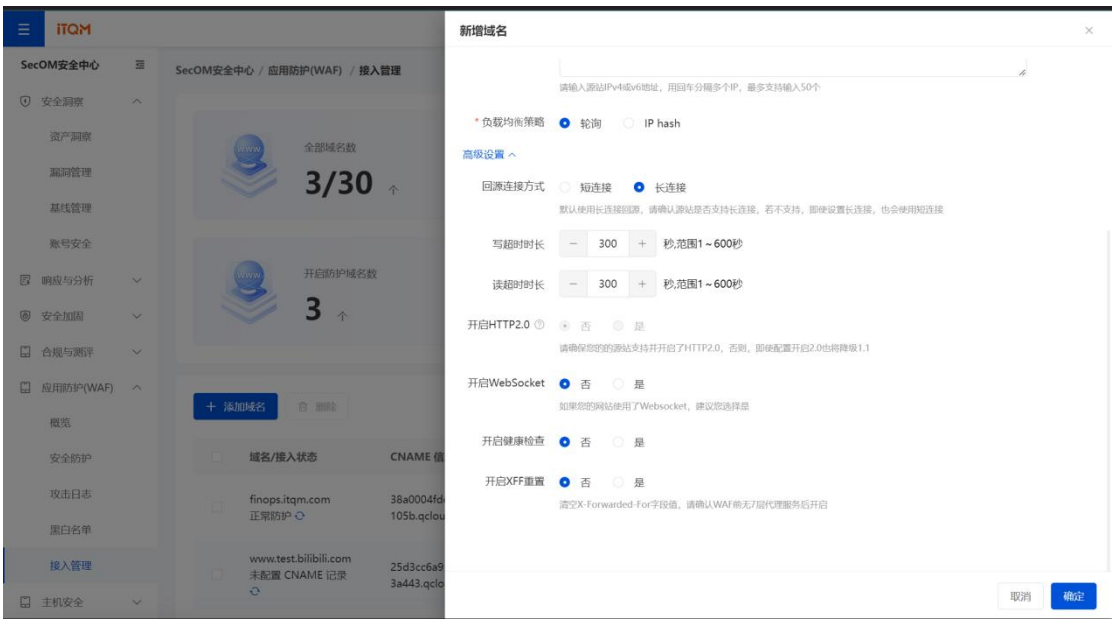
加权回源：当源站地址设置多 IP 回源时。可以选择加权回源方式，并设置不同的权重

负载均衡策略：默认为轮询方式，可根据实际需求选择轮询、 IP Hash 或加权轮询方式。

配置完基础参数后，可根据需求配置高级参数，单击确认保存。

WebSocket 检查，通过开发者模式检查是否有；ws:// 或 wss:// 开头的地址，通常这个网站是 WebSocket 会有 ws:// 或 wss:// 开头的地址。





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 也将降级为 1.1。

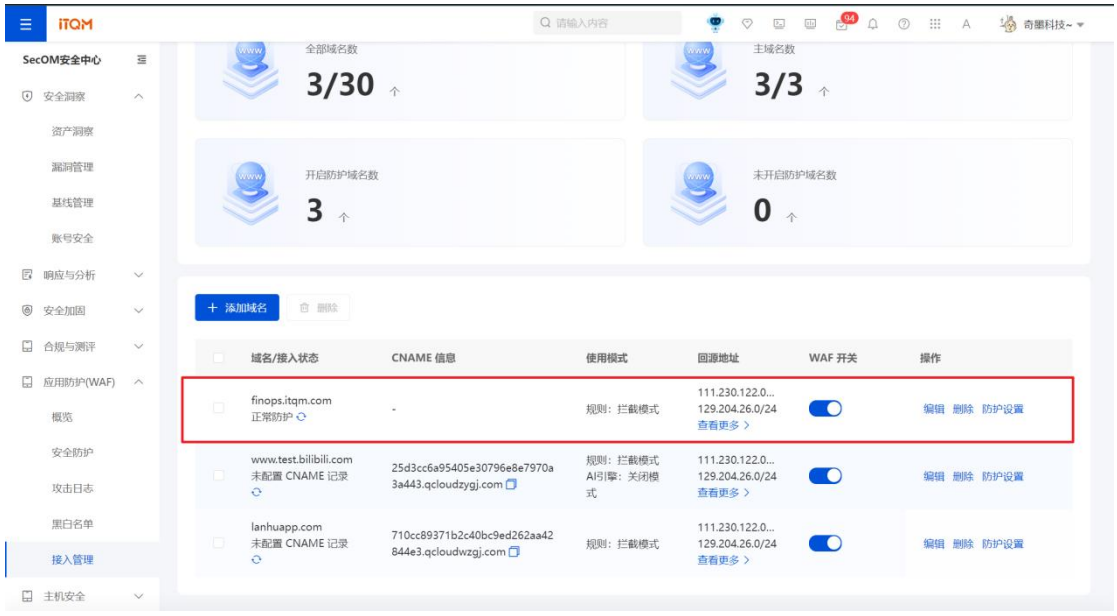
开启 Websocket：如果您的网站使用了 Websocket，建议您选择是。

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。

开启 XFF 重置：支持清空 X-Forwarded-For 字段值，请确认 WAF 前无七层代理服务后开启。

注：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。

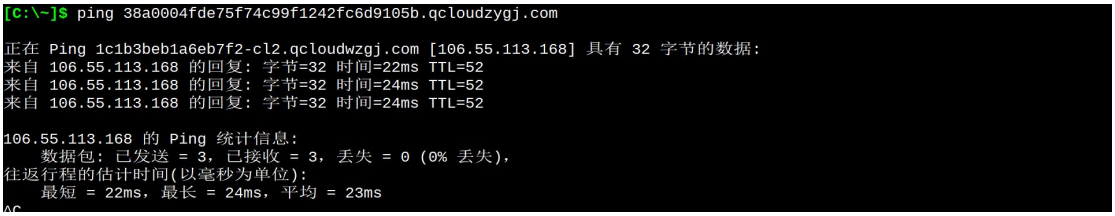
5. 完成配置后，可在域名接入页面看到新添加的域名。当前界面显示未配置 CNAME 记录，需要 本地验证测试 后，再 修改 DNS 解析。

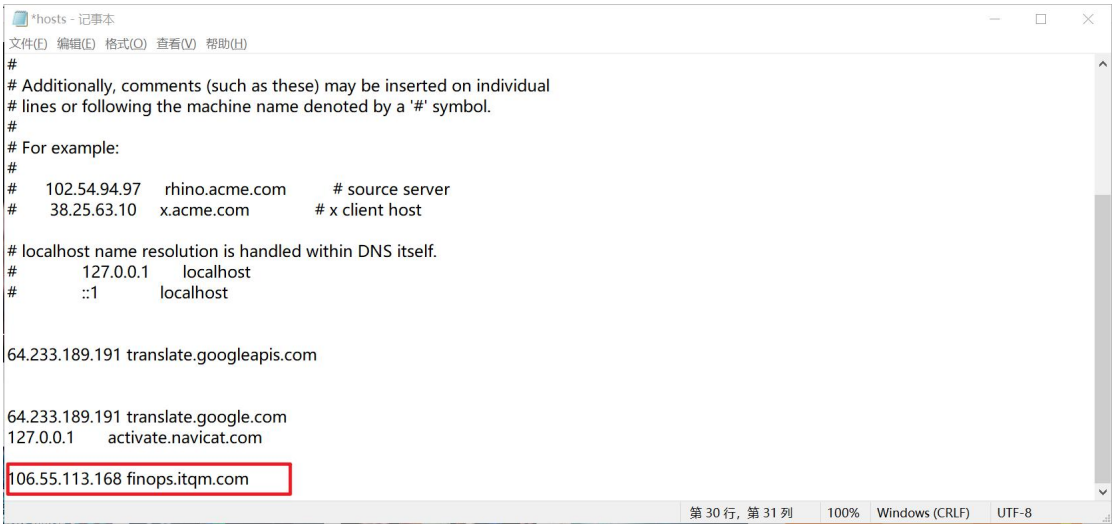


4.8 本地测试

4.8.1 修改本地 hosts

修改本地 hosts 文件进行测试，Windows10 举例以管理员的身份打开 C:\Windows\System32\drivers\etc\hosts 在末尾添加通过 ping CNAME 值得到的 IP 地址进行验证

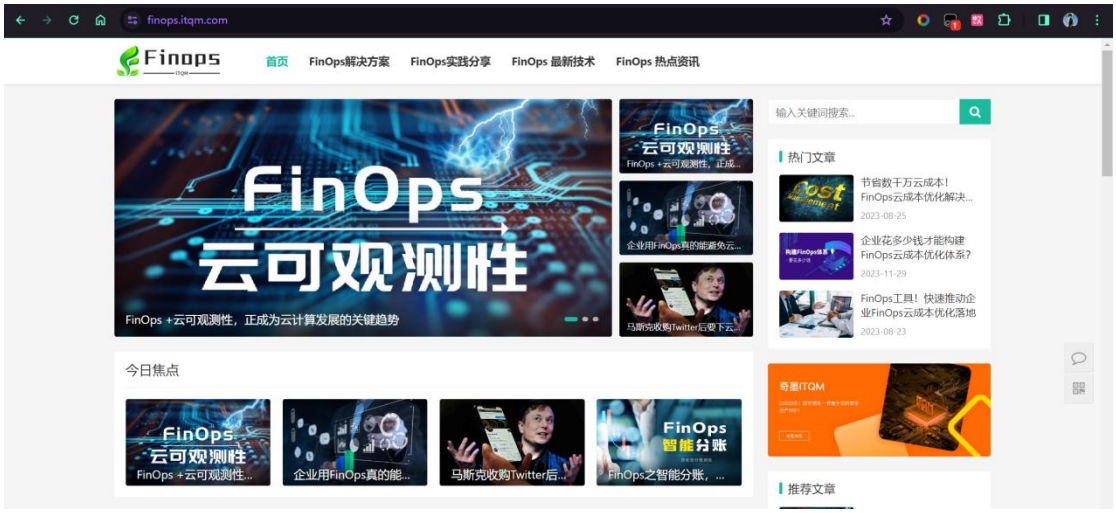




添加完成保存退出，验证 https://finops.itqm.com/（变更为实际受保域名） 站点是否正常。

4.8.2 访问验证

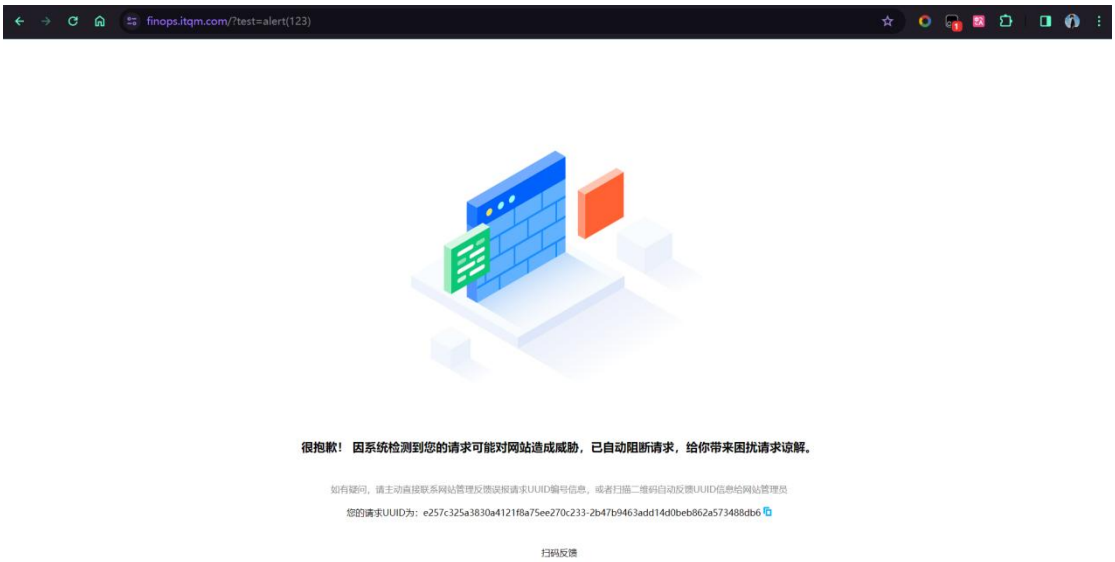
在本地电脑上访问 Web 站点，若站点能够正常打开，说明 Web 应用防火墙访问 Web 源站的线路连通性正常。



在浏览器中输入下面的网址并访问（此为例子，实际域名变更为“受保护域名”）。

https://finops.itqm.com/?test=alert(123)

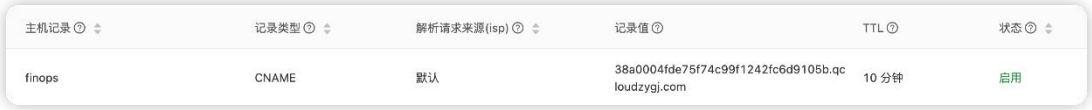
浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。



4.9 修改 DNS

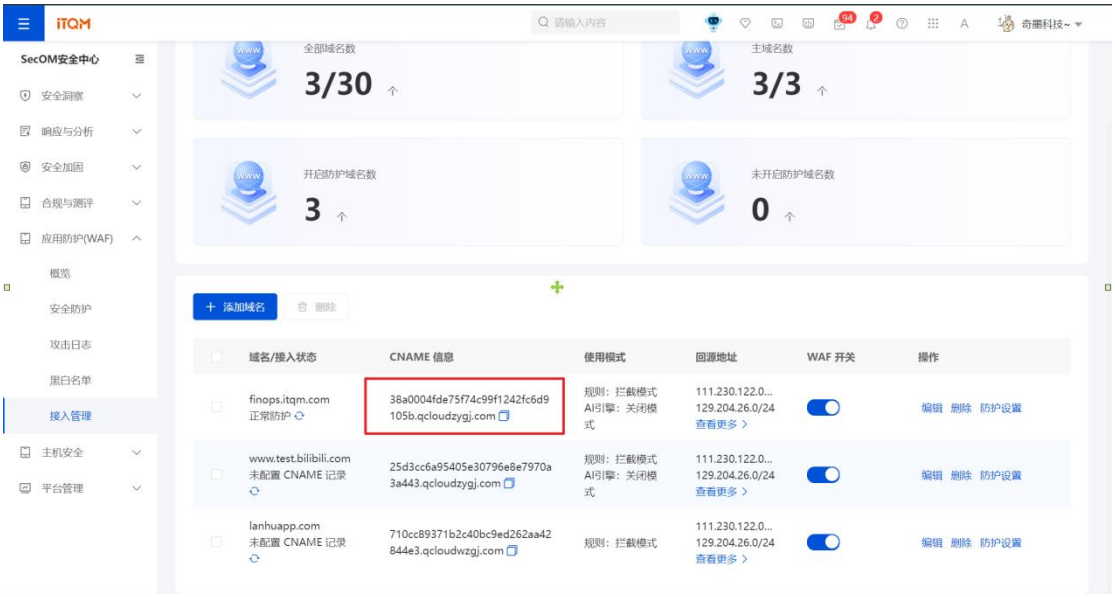
4.9.1 添加 CNAME 记录

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。需要登录 DNS 解析控制台添加 CNAME 记录



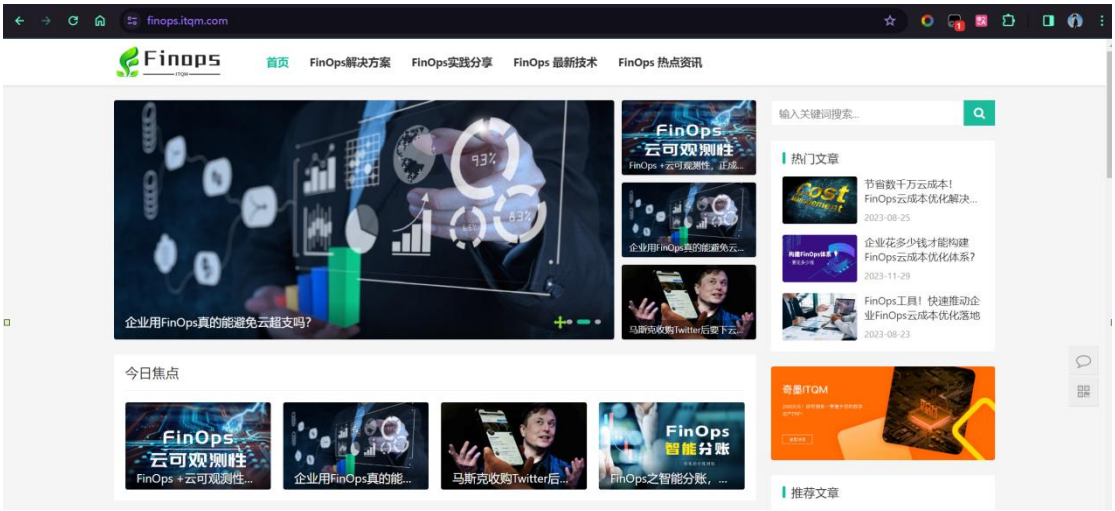
4.9.2 记录值获取

CNAME 记录值获取，登录 IQTM >［应用防护 WAF］>［CNAME 信息］中获取

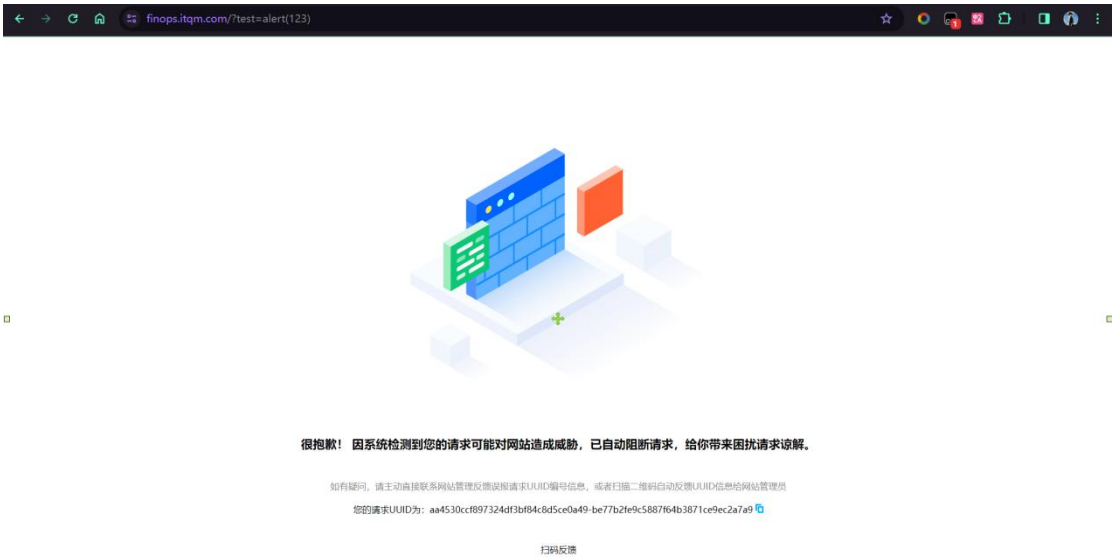


4.10 访问测试

正常访问，如下图显示成功



非法访问出现如下图，说明成功



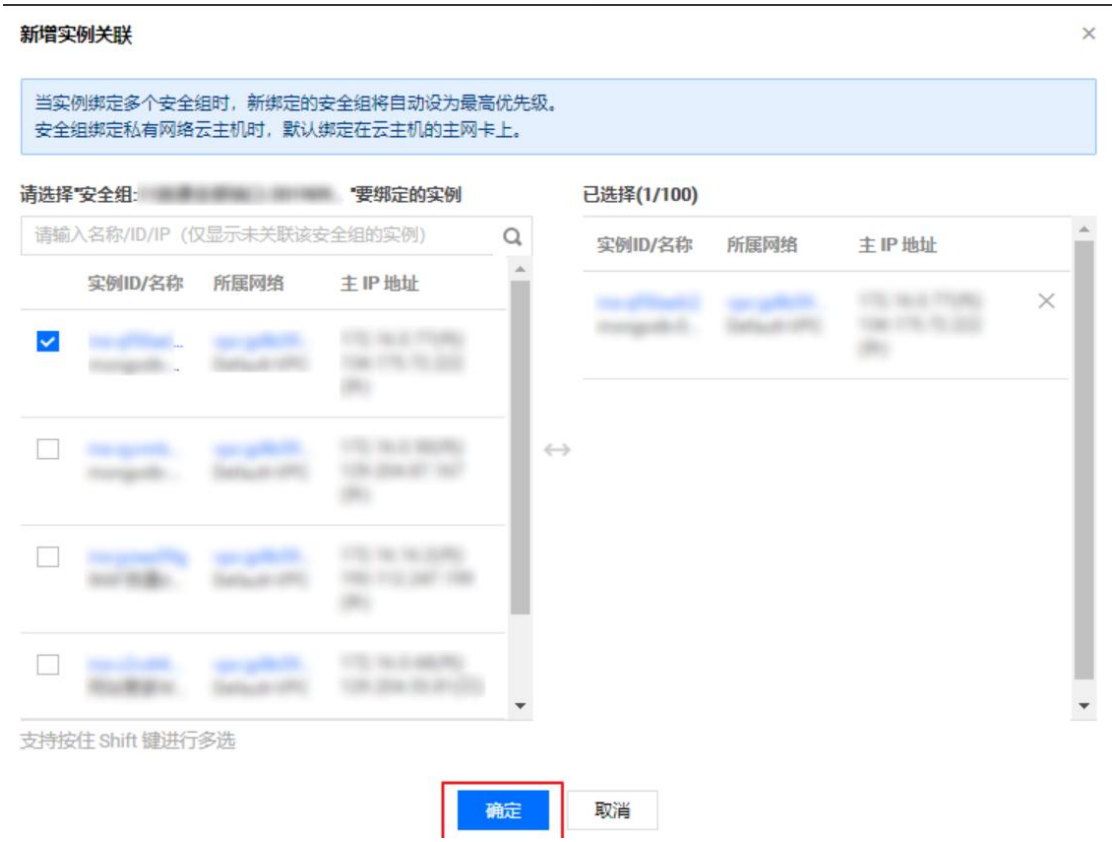
4.11 安全组开放

如访问测试无法通过需开放安全组进行测试，以腾讯云为例：

添加一个安全组规则

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。

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**



以上就是安全组开放流程。

（完）