Web应用防火墙（WAF）

产品文档



腾讯云TCE

版权所有：亿算云平台

文档目录

产品简介
- 产品概述
- 产品优势
- 产品分类
- 应用场景

快速入门
- 新手常见问题
- 快速入门

操作指南
- 租户端功能清单
- 负载均衡WAF域名接入
- 规则引擎
- CC防护设置
- 自定义策略
- 网页防篡改
- 防信息泄露
- 防信息泄露
- 地域封禁
- 攻击日志
- IP管理
- 常见操作
  - 场景1 创建实例
  - 场景2：添加clb-waf型防护域名
  - 场景3：添加saas-waf型防护域名
  - 场景4：删除防护域名
  - 场景5：删除实例
  - 场景6：添加自定义规则
  - 场景7：添加CC防护规则
  - 场景5：检查域名是否处于被防护状态
  - 场景6：应急预案

最佳实践
- 搭建负载均衡型WAF测试环境
- 搭建SaaS型WAF源站

常见问题
- 常见问题

版权所有：亿算云平台

产品简介
产品概述

最近更新时间: 2024-12-19 17:12:00

什么是 Web 应用防火墙

Web 应用防火墙（Web Application Firewall，WAF）是一款基于 AI 的一站式 Web 业务运营风险防护方案。通过 AI+规则双引擎识别恶意流量，保护网站安全，提高 Web 站点的安全性和可靠性。

WAF 提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF，两种 WAF 提供的安全防护能力基本相同，接入方式不同。

- SaaS 型 WAF 通过 DNS 解析，将域名解析到 WAF 集群提供的 CNAME 地址上，通过 WAF 配置源站服务器 IP，实现域名恶意流量清洗和过滤，将正常流量回源到源站，保护网站安全。
- 负载均衡型 WAF 通过和负载均衡集群进行联动，将负载均衡的 HTTP/HTTPS 流量镜像到 WAF 集群，WAF 进行旁路威胁检测和清洗，将用户请求的可信状态同步到负载均衡集群进行威胁拦截或放行，实现网站安全防护。

WAF 可以有效防御 SQL 注入、XSS 跨站脚本、木马上传、非授权访问等 OWASP 攻击。此外还可以有效过滤 CC 攻击、DNS 链路劫持检测、提供 0day 漏洞补丁、防止网页篡改等，通过多种手段全方位保护网站的系统以及业务安全。

主要功能

功能	简介
AI + Web 应用防火墙	基于 AI + 规则的 Web 攻击识别，防绕过、低漏报、低误报、精准有效防御常见 Web 攻击，如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造，Webshell 木马上传等 OWASP 定义的十大 Web 安全威胁攻击
0day 漏洞虚拟补丁	安全团队 7 * 24 小时监测，主动发现并响应，24 小时内下发高危 Web 漏洞，0day 漏洞防护虚拟补丁，受护用户无需任何操作即可获取紧急漏洞，0day 漏洞攻击防护能力，大大缩短漏洞响应周期
网页防篡改	用户可设置将核心网页内容缓存云端，并对外发布缓存中的网页内容，实现网页替身效果，防止网页篡改给组织带来负面影响

功能	简介
数据防泄漏	通过事前服务器应用隐藏，事中入侵防护及事后敏感数据替换隐藏策略，防止后台数据库被黑客窃取
CC 攻击防护	智能CC防护，综合源站异常响应情况（超时、响应延迟）和网站行为大数据分析，智能决策生成防御策略。多维度自定义精准访问控制、配合人机识别和频率控制等对抗手段，高效过滤垃圾访问及缓解 CC 攻击问题

计费方式

购买须知

按量付费是一种先使用后付费的计费方式。开通按量付费实例后，您可以按需使用资源，无需提前购买。系统会根据您的实际用量，在每个结算周期生成账单并从账户中扣除相应费用。

操作步骤

访问Web应用防火墙实例购买页。0元开通实例，接入流量后，按照运营平台的定价，第T+1天输出前一天（第T天）的账单。

为何需要 Web 应用防火墙

在以下场景中，使用 WAF 均可有效防御以及预防，保障企业网站的系统以及业务安全。

- **数据泄露（核心信息资产泄露）** Web 站点作为很多企业信息资产的入口，黑客可以通过 Web 入侵进行企业信息资产的盗取，对企业造成不可估量的损失。
- **恶意访问和数据抓取（无法正常服务，被对手利用数据）** 黑客控制肉鸡对 Web 站点发动 CC 攻击，资源耗尽而不能提供正常服务。恶意用户通过网络爬虫抓取网站的核心内容（文学博客、招聘网站、论坛网站、电商内的评论）电商网站被竞争对手刻意爬取商品详情进行研究。羊毛党们试图搜寻低价商品信息或在营销大促前提前获取情报寻找套利的可能。
- **网站被挂马被篡改（影响公信力和形象）** 攻击者在获取 Web 站点或者服务器权限后，通过插入恶意代码来让用户执行恶意程序、赚取流量、盗取账号、炫技等；植入“黄、赌、非”链接；篡改网页图片和文字；对网站运行造成很大影响，损坏网站运营者的形象。对外公信力和形象蒙受损失。
- **框架漏洞（补丁修复时段被攻击）** 很多 Web 系统基于常见的开源框架如 Structs2、Spring、WordPress 等，这些框架常常爆出安全漏洞，但等待安装补丁的维护时段，则是一段艰难和危险的过程，很多攻击会漏洞公布之后一天内就遍地开花。

产品优势

最近更新时间: 2024-12-19 17:12:00

多种接入防护方式

- 开通 WAF 后，无需进行业务变更即可完成防护接入，一键绑定亿算云平台负载均衡实现网站旁路检测和威胁清洗，同时提供一键 bypass 功能，实现业务转发和安全防护分离，稳定可靠。
- 通过 CNAME 接入 WAF，隐藏用户真实源站，将可信流量回源，覆盖亿算云平台和非亿算云平台上用户。
- 防护集群资源多地部署、动态扩展，按需使用，避免冗余及单点故障。

AI+规则双引擎防护

- 在安全规则引擎进行 OWASP Top 10防御（如SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造、命令行注入等）的基础上，引入 AI 防御能力，通过交叉验证持续学习，精准有效捕捉各类常规 Web 攻击、0day 攻击及其它新型未知攻击。
- 通过不断学习海量业务数据特征，生成基于业务的个性化防护策略，避免误报，用户可基于 AI 引擎实现自助误报和漏报处理，提升运营效率。

及时的补丁修复保障

- 可提供在 12h 内更新高危漏洞补丁，在 24h 内更新常见通用型漏洞补丁。
- 云端自动升级，全球秒级同步下发策略，帮助企业无忧 Web 漏洞隐患。

智能 CC 防护

- 可自定义 session，通过 session 维度进行 CC 防护，更加精确防护 CC 攻击，减少误报。
- 可实时查看 CC 封堵状态 IP，根据需要快速调整防护策略。
- 一键抗 DDoS联动，轻松应对敏感大流量 DDoS 攻击问题，无惧突发风险。

稳定的高可用业务保障

- 产品无需安装维护软硬件，提供用户便捷的接入。稳定的低延时高性能 VIP 专线服务，在隐藏保护源站 IP 的同时，优质加速线路可保障毫秒级业务延时与配置响应速度。

IPv6 安全防护

- 可使用云上 NAT64 实例，实现网站 IPv6 防护接入，无需对 IPv4 站点进行改造即可支持 IPv6 访问和防护。
- 通过和负载均衡进行联动，无缝处理 IPv4 和 IPv6 访问流量，使其具备同等安全防护能力，简单快捷。

产品分类

最近更新时间: 2024-12-19 17:12:00

类型概述

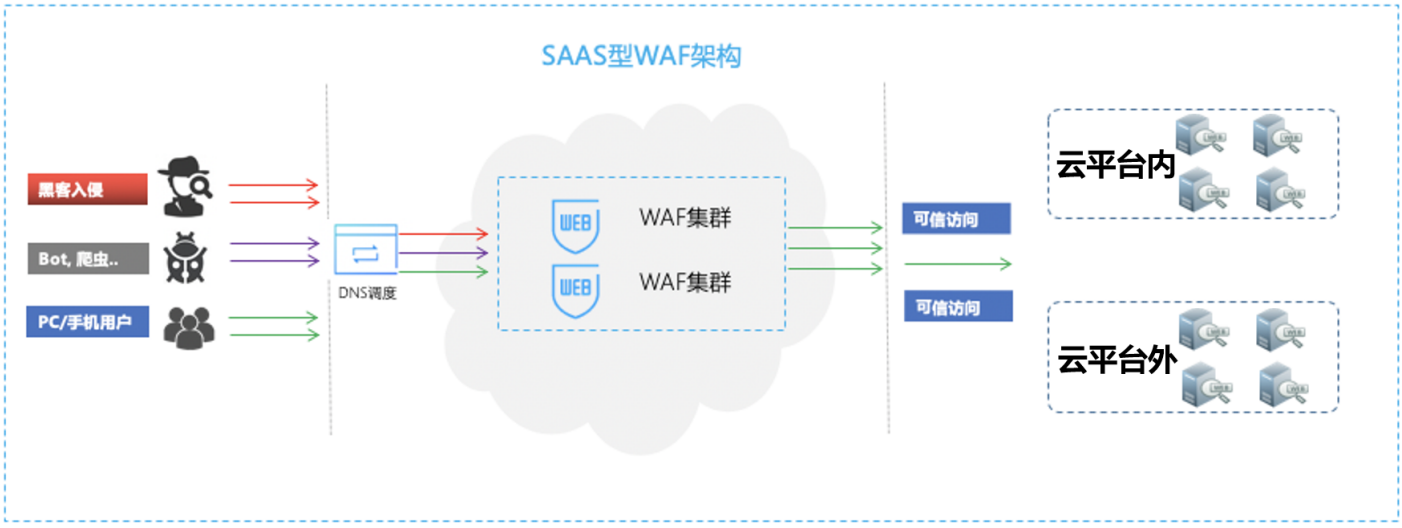
亿算云平台提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF。两种 WAF 的安全防护能力基本相同，但接入方式不同，适用场景不同，您可以根据实际部署需求选择不同类型的 WAF。

类别	SAAS型	负载均衡型
适用场景	适合所有用户（云上用户或本地 IDC 用户），通过 DNS 解析调度实现域名接入。	亿算云平台上已使用或计划使用七层负载均衡的用户。
核心优势	· 适用范围广阔，广泛覆盖亿算云平台上和非亿算云平台上用户。 · 支持源站隐藏，减少风险暴漏面	· 无感知接入，毫秒级延迟，WAF 接入不需要调整现有的网络架构。 · 网站业务转发和安全防护分离，一键 bypass，保障网站业务安全、稳定可靠。 · 支持多地域接入。
如何选择	若用户在亿算云平台上和本地均有网站需要防护需求，或亿算云平台上未使用七层负载均衡，推荐使用 SAAS 型 WAF。	亿算云平台上已使用或计划使用七层负载均衡的用户，且有 Web 安全防护、等保合规保护、网站安全运营需求，推荐使用负载均衡型 WAF。

> **说明：**
>
> 负载均衡型 WAF，当前灰度开放中，如需使用请提交申请，我们将尽快为您核实开通。

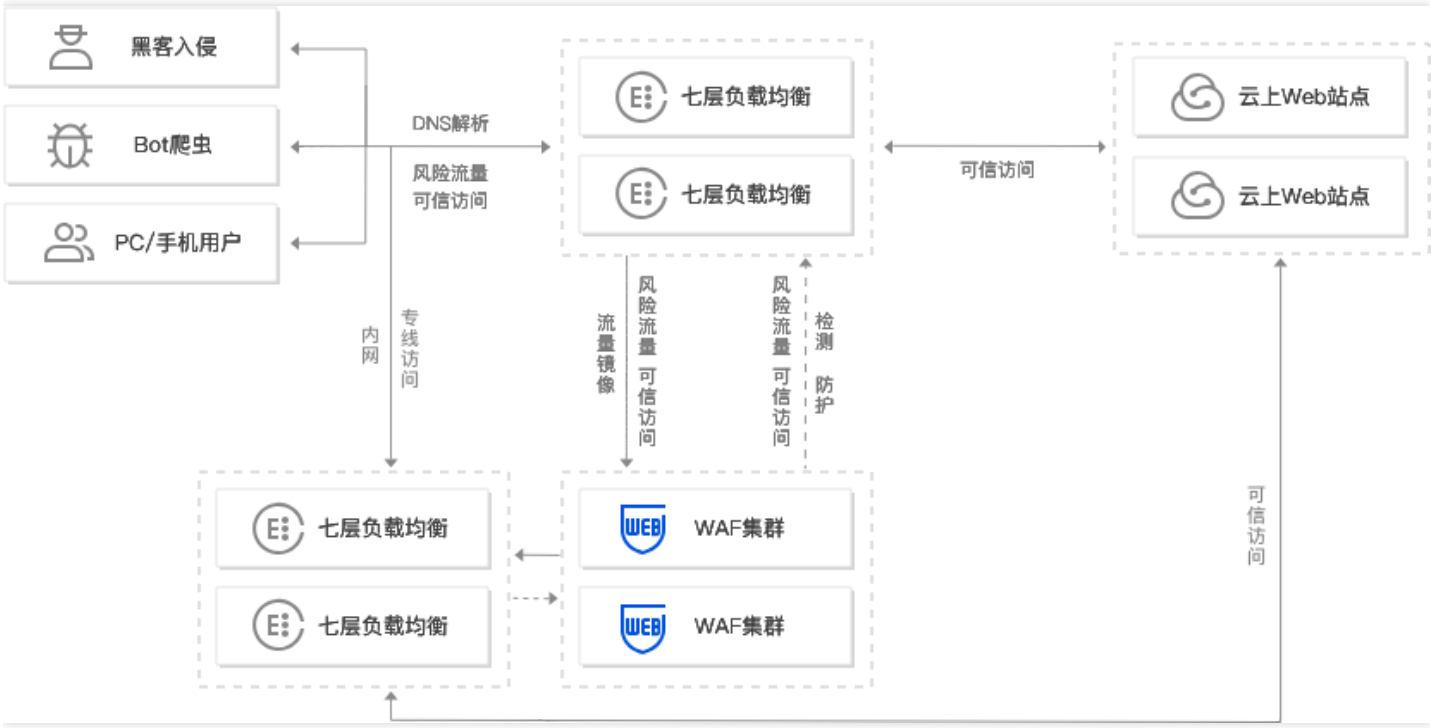
SaaS型WAF

Web 应用防火墙采用 SaaS 化模式交付，通过修改 DNS 引流设置，用户侧无需部署任何硬件设备，即可分钟级获取 Web 防护能力。WAF 集群对防护域名进行恶意流量检测和防护后，将正常流量回源到源站，保护网站安全。



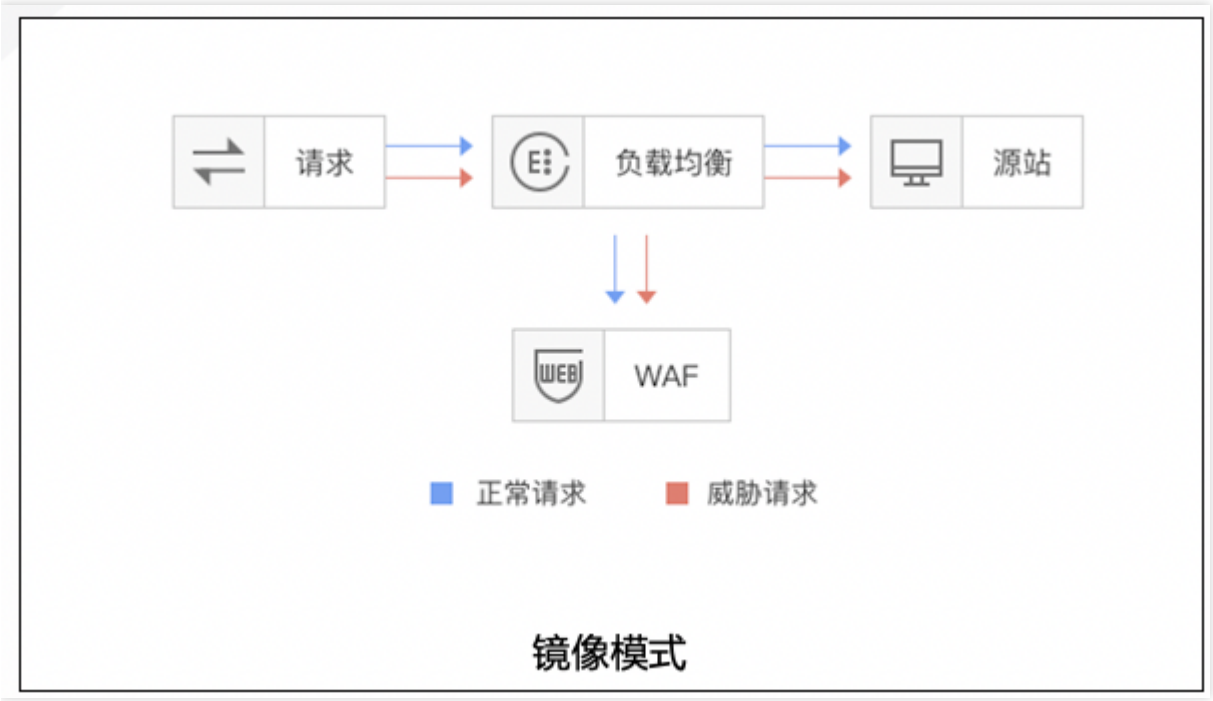
负载均衡型WAF

WAF 通过配置域名和亿算云平台各种网络环境下的七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP/HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离，最大限度减少安全防护对网站业务的影响，保护网站稳定运行。

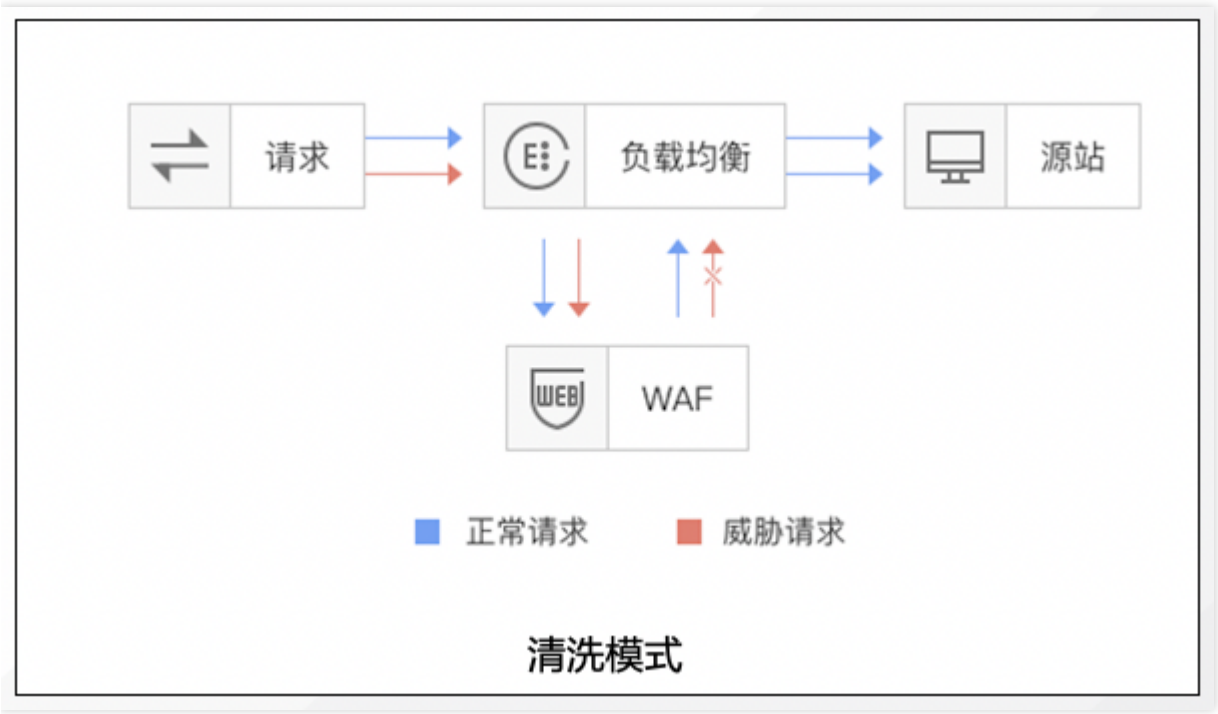


负载均衡型 WAF 提供两种流量处理模式：

- **镜像模式**：通过域名进行关联，CLB 镜像流量到 WAF 集群，WAF 进行旁路检测和告警，不返回请求可信状态。



- **清洗模式**：通过域名进行关联，CLB 镜像流量到 WAF 集群，WAF 进行旁路检测和告警，同步请求可信状态，CLB 集群根据状态对请求进行拦截或放行处理。


请求
负载均衡
源站
WAF
正常请求
威胁请求
清洗模式

应用场景

最近更新时间: 2024-12-19 17:12:00

金融网站防护

- 一键接入防护，可跟大流量 DDoS 防御有机结合，同时具备 Web 安全防护。
- 有效监测 DNS 链路劫持，防止网站流量被恶意指向。
- 可有效检测撞库等异常访问，保护用户信息不外泄。
- 云端资源优势，自动伸缩，轻松应对业务突发，大流量 CC 攻击。

政务网站防护

- 一键接入防御，轻松配置，隐藏并保护源站，保证网站内容不会被黑客入侵、篡改。保障网站信息正确，政府服务正常可用，民众访问满意畅通。

电商网站防护

- 持续优化防护规则、精准拦截 Web 攻击，全面抵御 OWASP Top 10 Web 应用风险。
- 在高并发抢购场景下，可智能过滤恶意攻击及垃圾访问，保障正常访问业务流畅。

防数据泄密

- 避免因黑客的注入入侵攻击，导致网站核心数据被拖库泄露。
- 防 CC 攻击：防恶意 CC（http get flood），通过在四层和七层阻断海量的恶意请求，保障网站可用性。

版权所有：亿算云平台

快速入门
新手常见问题

最近更新时间: 2024-12-19 17:12:00

WAF接入方式？

WAF分为两种类型，SaaS 型 WAF 和负载均衡型 WAF，两种类型 WAF 域名接入方式不同，请根据实际情况完成接入。

WAF 是否支持 HTTPS 防护？

WAF 全面支持 HTTPS 业务。用户只需根据提示将 SSL 证书及私钥上传，WAF 即可防护 HTTPS 业务流量。

WAF 一个防护域名可以设置多少个回源 IP？

WAF 一个防护域名最多可以设置50个回源 IP。

WAF 是否支持健康检查？

WAF 默认启用健康检查。WAF 会对所有源站 IP 进行接入状态检测，如果某个源站 IP 没有响应，WAF 将不再将请求转发到该源站 IP ，直到接入状态恢复正常。

在 WAF 的控制台中，更改配置后大约需要多少时间生效？

一般情况下，更改后的配置在10s内即可生效。

SaaS 型和负载均衡型 WAF 是否支持 国密证书认证？

SaaS 型 WAF 暂不支持国密证书认证，负载均衡型 WAF 支持国密证书认证。

快速入门

最近更新时间: 2024-12-19 17:12:00

WAF分为两种类型，SaaS 型 WAF 和负载均衡型 WAF，两种类型 WAF 域名接入方式不同，请根据实际情况完成接入。

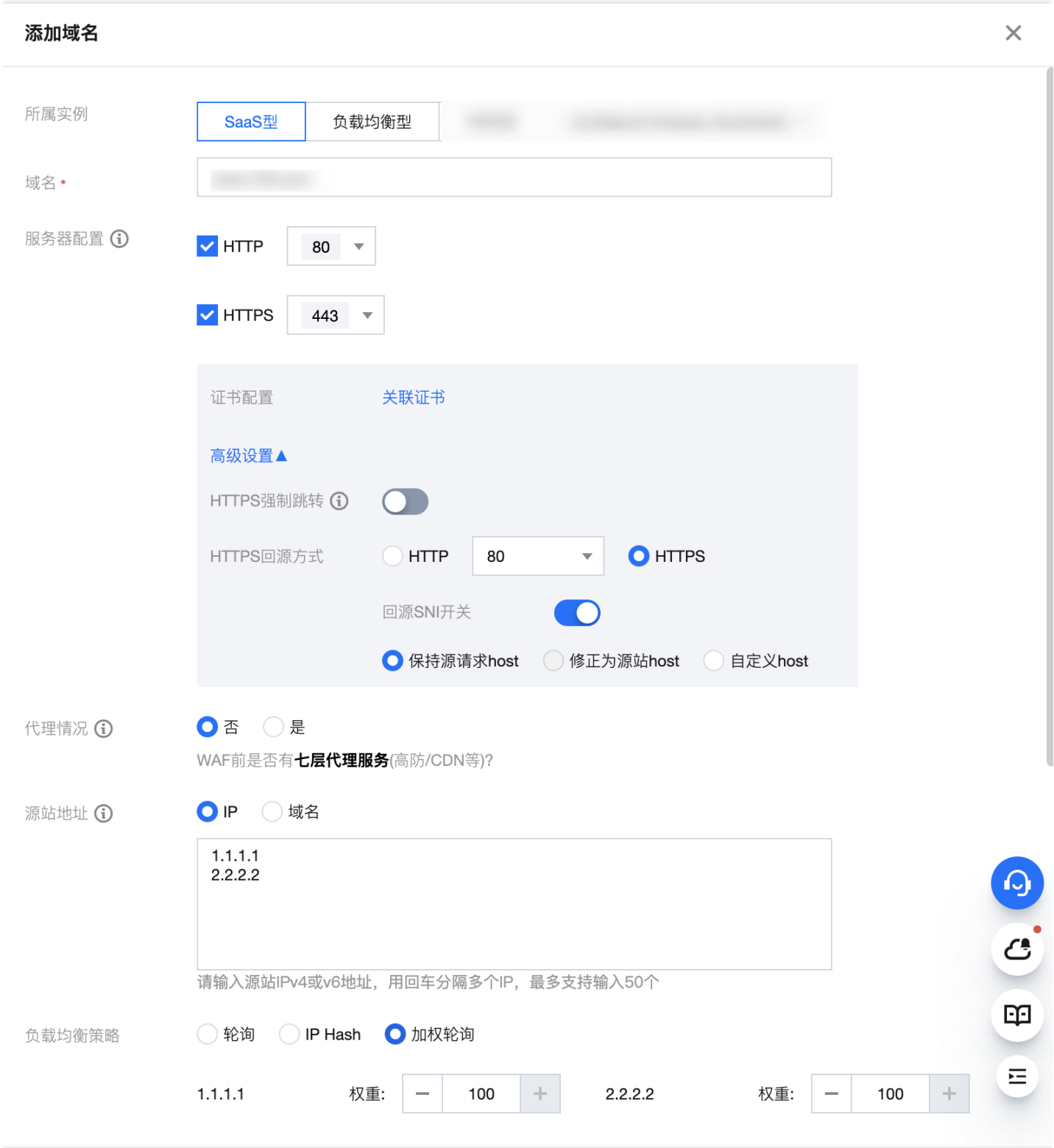
SaaS型WAF接入配置

SaaS 型 WAF 通过为防护域名分配 CNAME，修改网站的 DNS 解析记录，将网站收到的 Web 请求转发给 WAF ，从而对网站进行安全防护。配合安全组使用，可以避免攻击者绕过 WAF 直接攻击网站源站。为了实现上述功能，您需要完成以下步骤：

步骤1：域名添加

为了使 Web 应用防火墙识别出需要防护的域名，需要先在 Web 应用防火墙中添加域名。下面以防护 waf.qcloudwaf.com 为例，说明配置步骤。

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** > **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**，进入添加域名页面选择“SAAS型”。
3. 在添加域名页面，配置相关基础参数



- **域名配置**

1. 在域名输入框中添加需要防护的域名 waf.qcloudwaf.com 。
2. 协议和端口可按实际情况选择。例如：勾选 HTTP，选择80端口；勾选 HTTPS，选择443端口。
3. HTTPS 回源方式可选：HTTP 或 HTTPS。

4. 证书来源可选：托管证书，自有证书。
5. 在源站 IP 输入框内输入需要防护网站的真实 IP 源站地址，即源站的公网 IP 地址。

- **其他配置**

1. 在 Web 应用防火墙前，是否接入了其他中间代理设备，若有，请选择【是】且支持自定义获取展示源IP的方式，若无，请选择【否】。
2. 单击【保存】，完成配置后，可在域名列表看到刚刚添加的域名和为站点分配的 CNAME地址。

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。

步骤2：本地测试

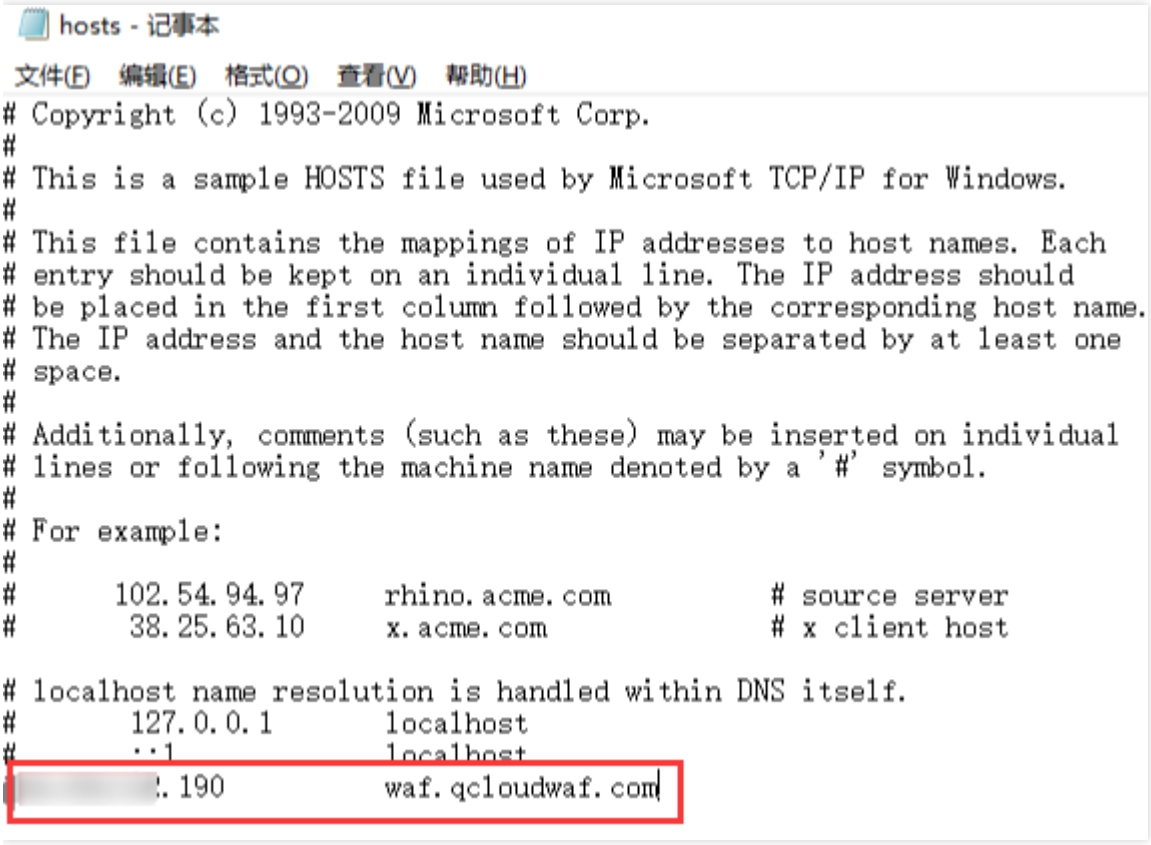
本地机器访问网站需要做 DNS 解析，在这之前会优先从本地 hosts 文件中获取目标域名对应的 IP 地址。所以可以用修改 hosts 文件的方式把本地的访问流量导向 Web 应用防火墙，从而测试经过 Web 应用防火墙访问 Web 站点的线路连通性，避免直接修改 DNS 解析记录，影响到公网用户对站点的访问。

1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择【Web 应用防火墙】>【防护设置】，在域名列表中查看 `waf.qcloudwaf.com` 的 VIP 地址。



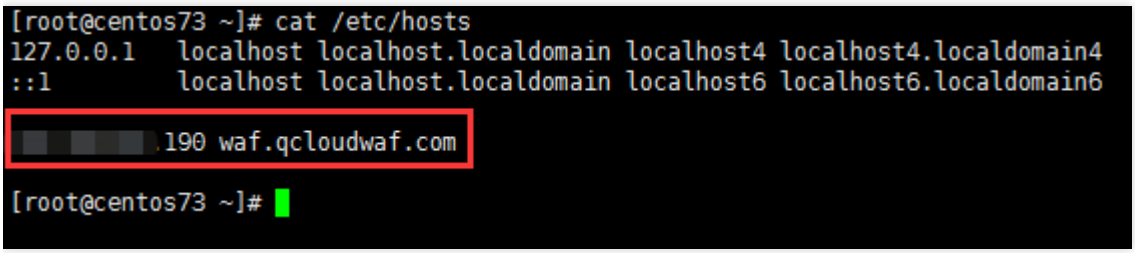
2. 修改 hosts 文件

- 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。



- 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。



3. 访问测试

(1) 在本地电脑上访问 Web 站点，若站点能够正常打开，说明网站管家访问 Web 源站的线路连通性正常。

(2) 在浏览器中输入下面的网址并访问。

```
http://waf.qcloudwaf.com/?test=alert(123)
```

(3) 浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。

步骤3：修改 DNS 解析

当您想通过Web应用防火墙WAF防护公网用户访问网站的流量时，需要修改 DNS 的解析记录，相关DNS CNAME记录修改使用DNS标准修改流程即可。

步骤4：设置安全组

安全组是云平台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。

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】。



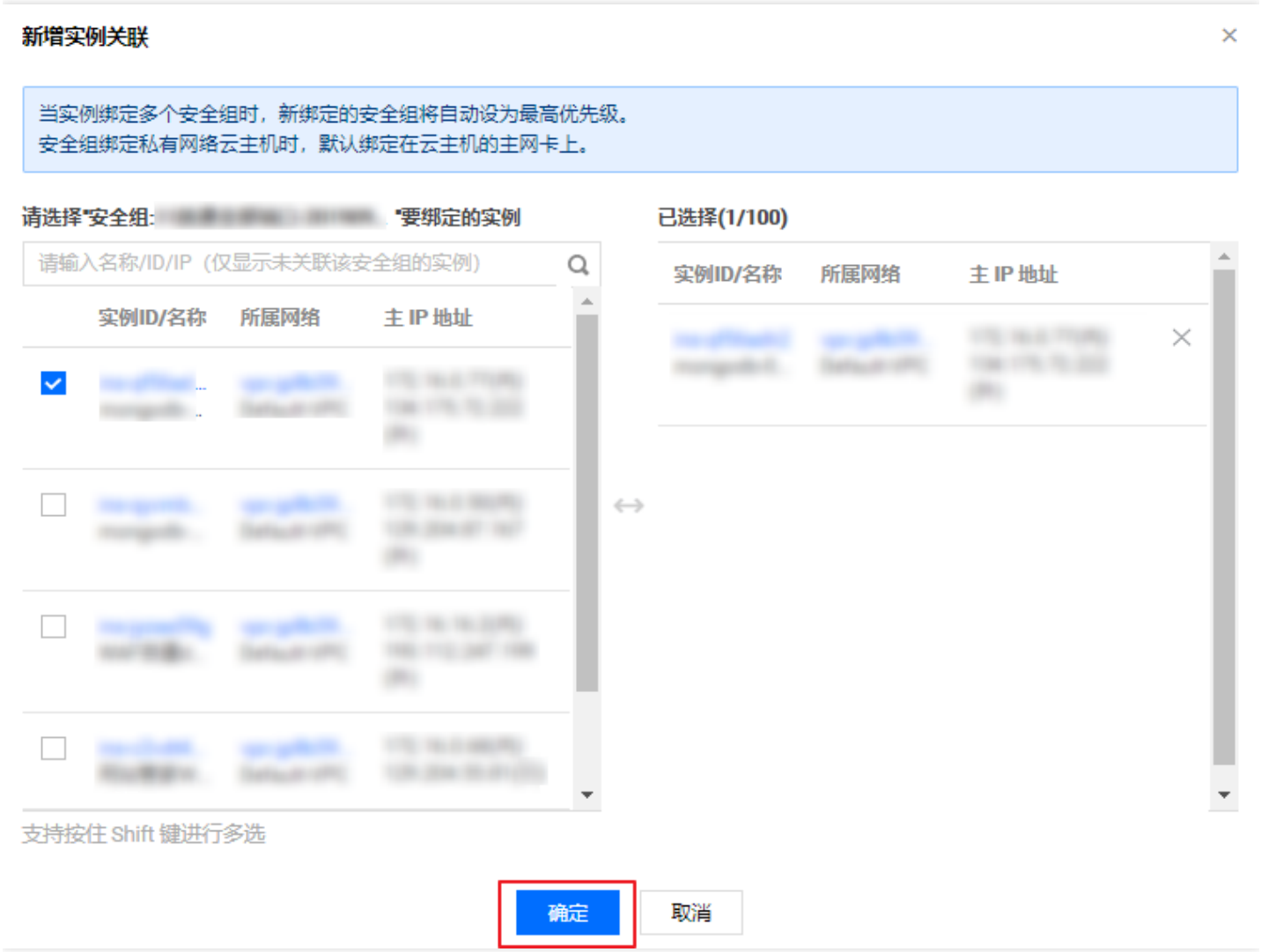
5. 在弹出框中填写相关信息，类型选择“HTTP（80）”，来源中填写需要放行的回源 IP，根据需求填写端口及策略，填写完毕后，单击【完成】。



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。



负载均衡型WAF

负载均衡型 WAF 通过配置域名和七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP 或 HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离。为了实现联动防护，您需要完成以下步骤：

步骤1：确认负载均衡配置

负载均衡型WAF通过添加域名和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，请确保网站业务已经在云平台上，并且使用了负载均衡（原应用型负载均衡，网络类型为公网类型）。若您的网站业务不在云平台上，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wow.qcloudwaf.com为例，查看负载均衡监听器配置信息。

1. 登录云控制台，单击【云产品】>【云计算与网络】>【负载均衡】，进入负载均衡控制台。
2. 在"LB 实例列表"中，找到已创建的负载均衡实例，单击实例 ID，进入负载均衡详情页。



3. 在负载均衡详情页面，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，协议 HTTP，端口80。



4. 创建转发规则，监听器转发规则监听的域名为 wow.qcloudwaf.com ，URL路径填"/"，选择是否进行监控检查，以及会话保持，点击【提交】，完成域名添加。此时域名防护状态为未启用。

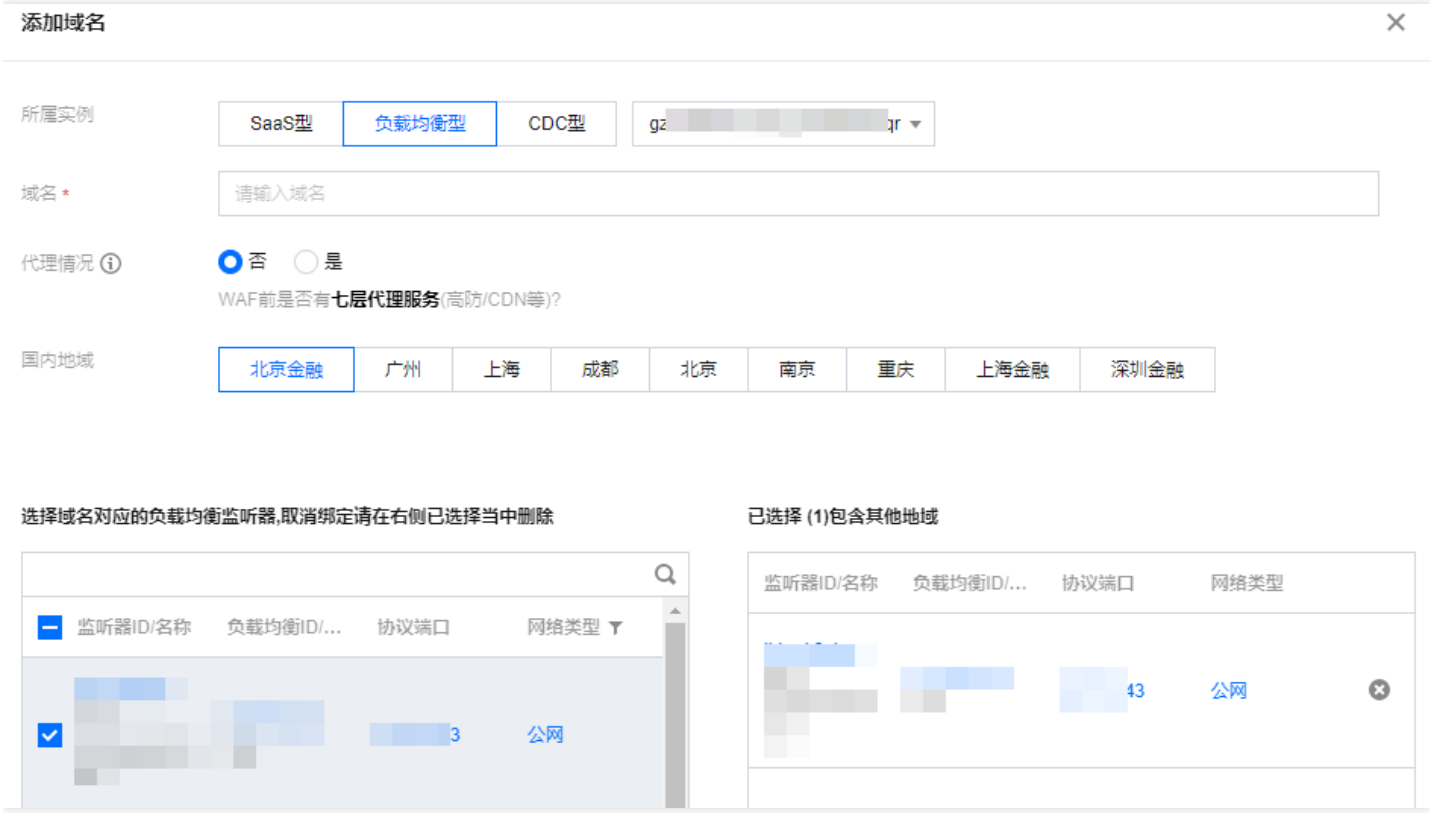




步骤2：域名添加绑定负载均衡

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** > **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**，进入添加域名页面选择"负载均衡型"。
3. 在添加域名页面，填写需要防护域名，根据域名所在地域选择监听器信息，配置代理情况后确认完成接入。



> **注意：**
>
> 填写的域名需要和负载均衡监听器中添加的域名保持一致。

步骤3：验证测试

1. 确保本地电脑可以正常访问 Web 站点。
2. 在浏览器中输入网址http://wow.qcloudwaf.com/?test=alert(123) 并访问。

> **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。

3. 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】，进入攻击日志查询页面，进行日志查询。

4. 选择添加防护的域名，单击【查询】。若看到攻击类型为“XSS 攻击”，说明 WAF 配置已经生效。



> **说明：**
>
> 如果域名未配置 DNS，可参见 SaaS 型 WAF 快速入门的步骤2：本地测试进行接入有效性验证。

操作指南
租户端功能清单

最近更新时间: 2024-12-19 17:12:00

安全可视	概览	安全概览展示
		攻击总览展示
		基础安全分析展示
		业务运营分析展示
		域名Web攻击次数 TOP5(次)展示
		域名CC攻击次数 TOP5(次)展示
		攻击来源IP TOP5(次)展示
		攻击类型占比展示
		攻击来源区域分布(次)展示
日志服务	攻击日志	日志服务-原始数据展示
		日志检索
		日志下载
资产中心	接入管理	添加域名
		删除域名
		编辑域名
		域名列表展示
		WAF开关
	实例管理	新建实例
		删除实例
		管理域名
配置中心	基础安全	自定义返回拦截页面功能

		防护模式选择功能
		防护等级选择功能
		恶意文件检测
		IP封禁设置，包括Web攻击次数、检测时长、封禁时间
		tiga规则列表
		tiga规则检索功能
		单条tiga规则开关
		添加tiga规则白名单
		地域封禁功能
		访问控制规则功能
		CC防护功能
		网页防篡改功能
		信息防泄漏功能
	黑白名单	IP黑名单
		IP白名单
		精准白名单
		规则白名单
服务管理	web规则库	防护规则列表
	审计日志	在控制台调用waf接口日志列表

|目录|页面|功能项| |

负载均衡WAF域名接入

最近更新时间: 2024-12-19 17:12:00

负载均衡型 WAF 通过配置域名和七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP 或 HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离。为了实现联动防护，您需要完成以下步骤：

步骤1：确认负载均衡配置

负载均衡型WAF通过添加域名和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，请确保网站业务已经在该租户的VPC中，并且使用负载均衡（原应用型负载均衡，网络类型为公网类型）。

若您的网站业务未使用负载均衡，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wow.qcloudwaf.com为例，查看负载均衡监听器配置信息。

1. 登录云租户控制台，单击【云产品】>【云计算与网络】>【负载均衡】，进入负载均衡控制台。
2. 在“LB 实例列表”中，找到已创建的负载均衡实例 clb-test，单击实例 ID，进入负载均衡详情页。
3. 在负载均衡详情页面，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，协议 HTTP，端口80。



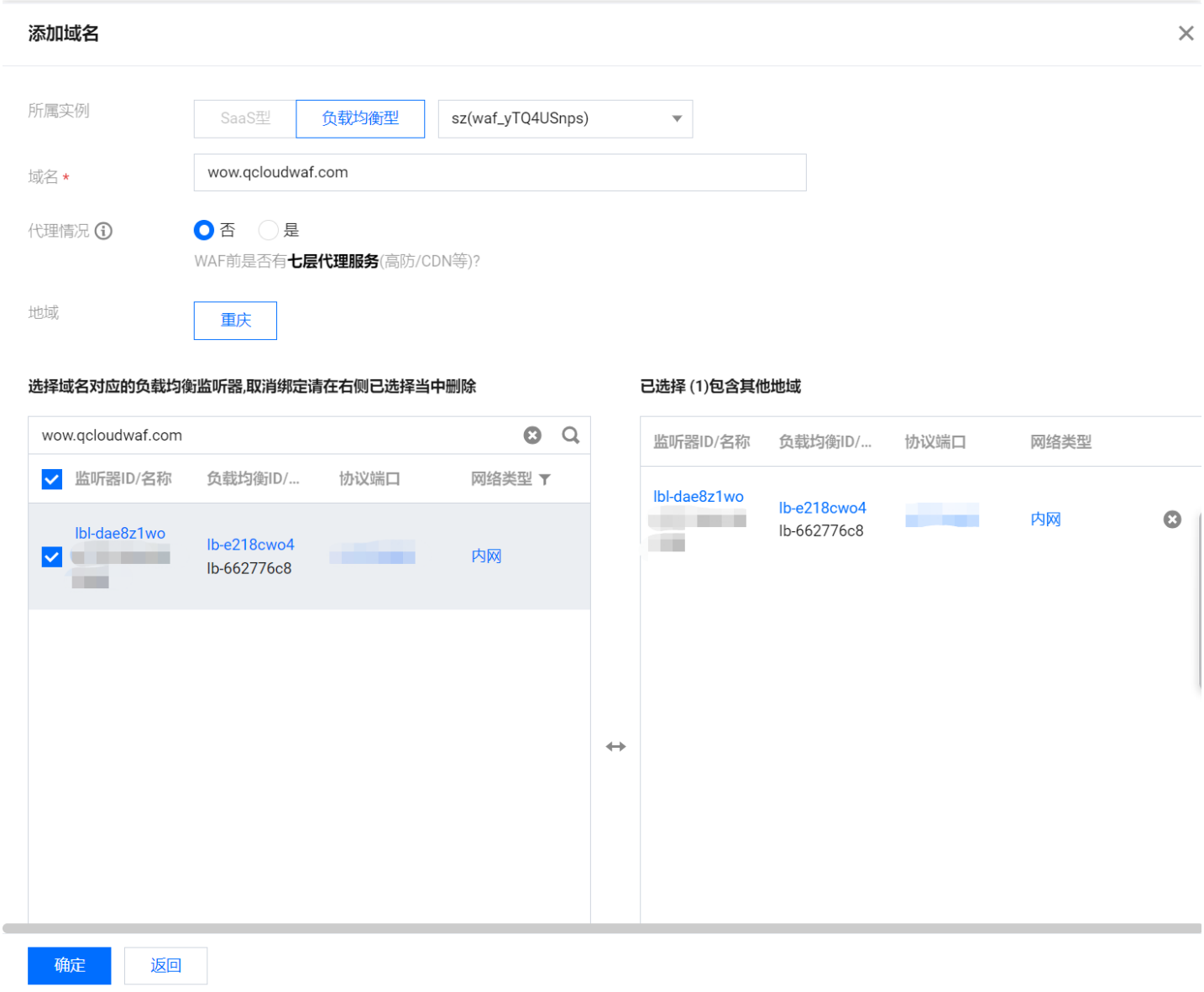
4. 创建转发规则，监听器转发规则监听的域名为 wow.qcloudwaf.com ，URL路径填“/”，选择是否进行监控检查，以及会话保持，点击【提交】，完成域名添加。此时域名防护状态为未启用。


创建HTTP/HTTPS转发规则
1 基本配置
2 健康检查
3 会话保持
域名
wow.qcloudwaf.com
默认域名
当客户端请求没有匹配本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名，详情
URL路径
/
均衡方式
按权重轮询
当后端CVM的权重都设置为同一个值时，权重属性将不生效，将按照简单的轮询策略分发请求
获取客户端IP
已启用
Gzip压缩
已启用
下一步：健康检查
取消



步骤2：域名添加绑定负载均衡

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**，进入添加域名页面选择“负载均衡型”。
3. 在添加域名页面，填写需要防护域名，根据域名所在地域选择监听器信息，配置代理情况后确认完成接入。



注意：

填写的域名需要和负载均衡监听器中添加的域名保持一致。

4. 绑定完成后，在页面下方，单击【完成】即可返回域名列表。在域名列表可以查看到防护域名wow.qcloudwaf.com和负载均衡的负载均衡 ID、名称、VIP 和监听器信息等。

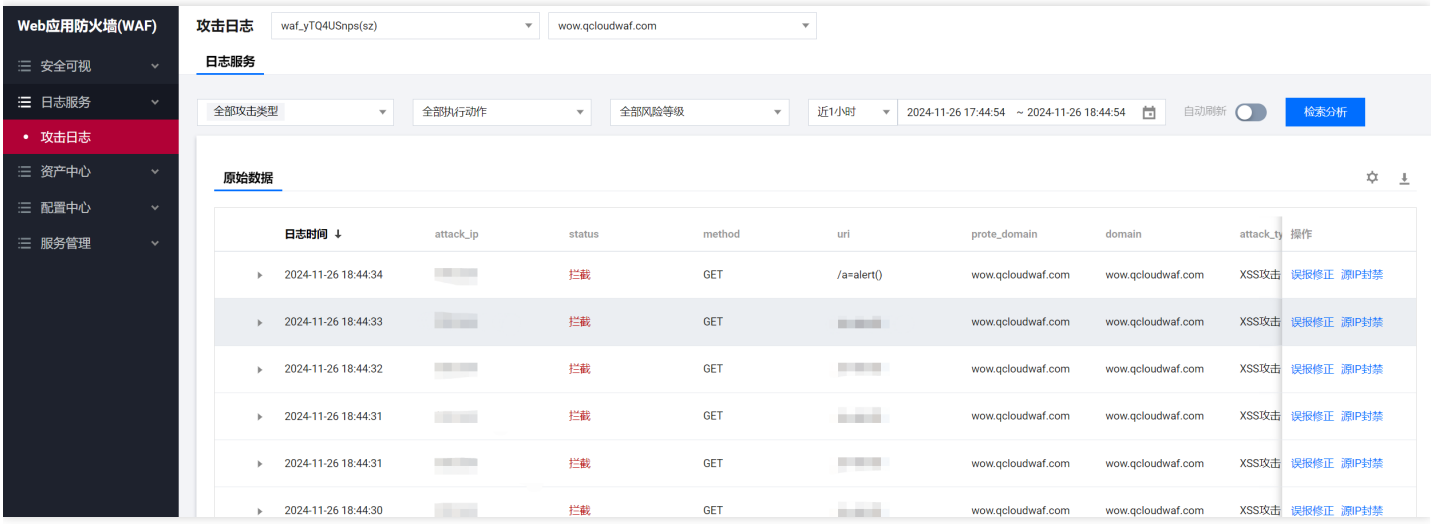


步骤3：验证测试

1. 确保本地电脑可以正常访问 Web 站点。
2. 在浏览器中输入网址 http://wow.qcloudwaf.com/?test=alert(123) 并访问。

> **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。

3. 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】，进入攻击日志查询页面，进行日志查询。
4. 选择添加防护的域名，单击【查询】。若看到攻击类型为 “XSS 攻击”，说明 WAF 配置已经生效。



> **说明：**

> 如果域名未配置 DNS，可参见 SaaS 型 WAF 快速入门的步骤2：本地测试进行接入有效性验证。

规则引擎

最近更新时间: 2024-12-19 17:12:00

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

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。

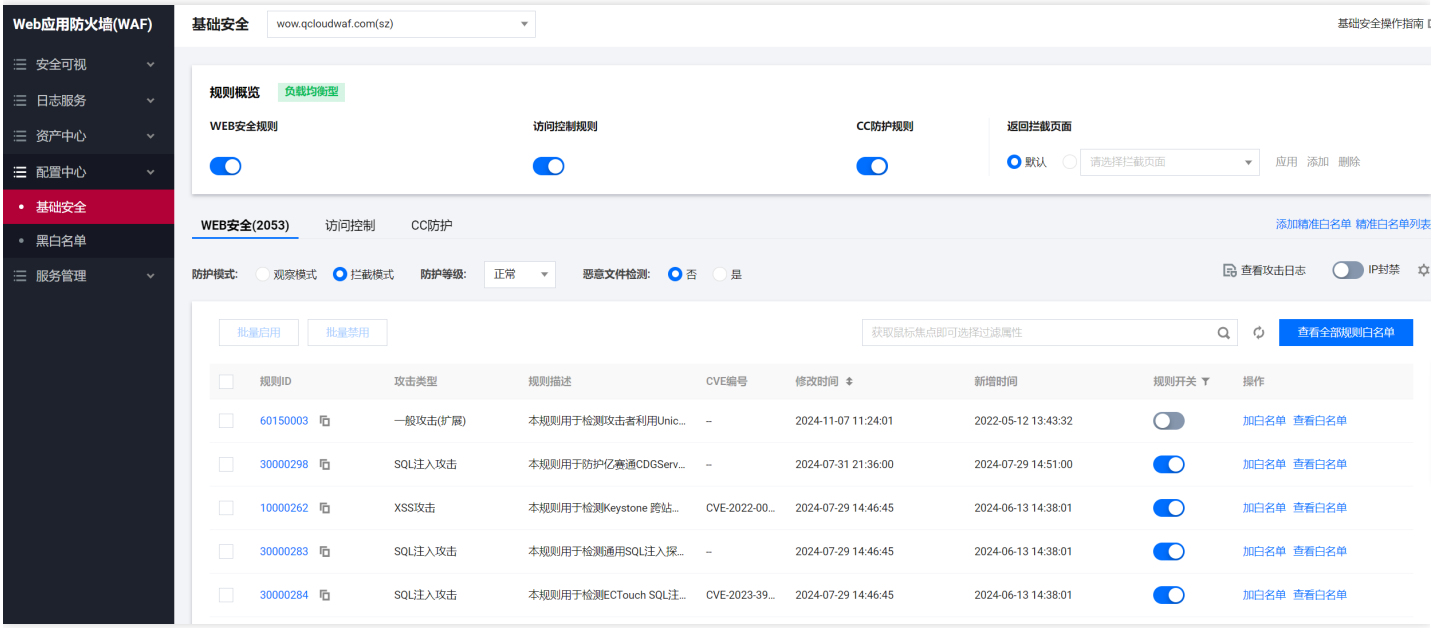
WAF 规则防护引擎，提供基于安全 Web 威胁和情报积累的专家规则集，自动防护 OWASP TOP10 攻击。目前防护 Web 攻击包括： SQL 注入、XSS 攻击、恶意扫描、命令注入攻击、Web 应用漏洞、Webshell 上传、不合规协议、木马后门等12类通用的 Web 攻击。

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

域名规则防护引擎设置

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】>【基础安全】>【WEB安全】。
2. 在防护设置页面的对 Web 基础防护进行防护模式、防护等级、以及恶意文件检测方式进行配置，同时支持开启和设置防扫描的IP封禁能力。



字段说明：

- 规则引擎开关：默认开启。开关关闭后，经过WAF的域名请求将不进行规则引擎威胁处理。
- 防护模式：规则引擎工作模式，默认为拦截。 观察：不阻断攻击请求，进行预计，产生观察日志。 拦截：直接阻断 Web 攻击请求，产生拦截日志。
- 防护等级：规则引擎防护等级，默认为正常。 严格：检测常见 Web 应用攻击。用户发现默认等级下存在较多误拦截，或者业务存在较多不可控的用户输入时（含有富文本编辑器的网站），建议您选择该模式。 严格：严格检测 SQL 注入、XSS 攻击、命令执行等 Web 应用攻击，默认模式。
- 规则管理：通过规则管理，用户可查看规则引擎信息并对规则引擎进行设置，包括查看攻击分类、查看规则等级包含的规则内容、规则集更新动态，同时可对单条规则进行开关设置，添加基于域名 URL 和规则 ID 的白名单。
- 支持的解码类型：当前规则引擎默认支持以下解码类型，暂不支持手动设置。 URL 解码（多重解码）、javascript Unicode 解码、注释处理、空格压缩、UTF-7 解码、HTML 实体解码、Multipart 解析、JSON 解析、XML 解析、Form 解析。

查看规则分类

1. 进入规则引擎设置页面。

- 方式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】，进入域名列表管理页面，选择任意域名，点击操作列的【防护配置】按钮，进入域名的web安全防护配置页面，查看规则详情。
- 方式2： a.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】。 b.在域名列表中，单击需要防护的域名，进入【web安全】设置页面，进入规则引擎页面。

2. 进入规则库管理页面

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】，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。



当前 WAF 支持防护的攻击分类如下：

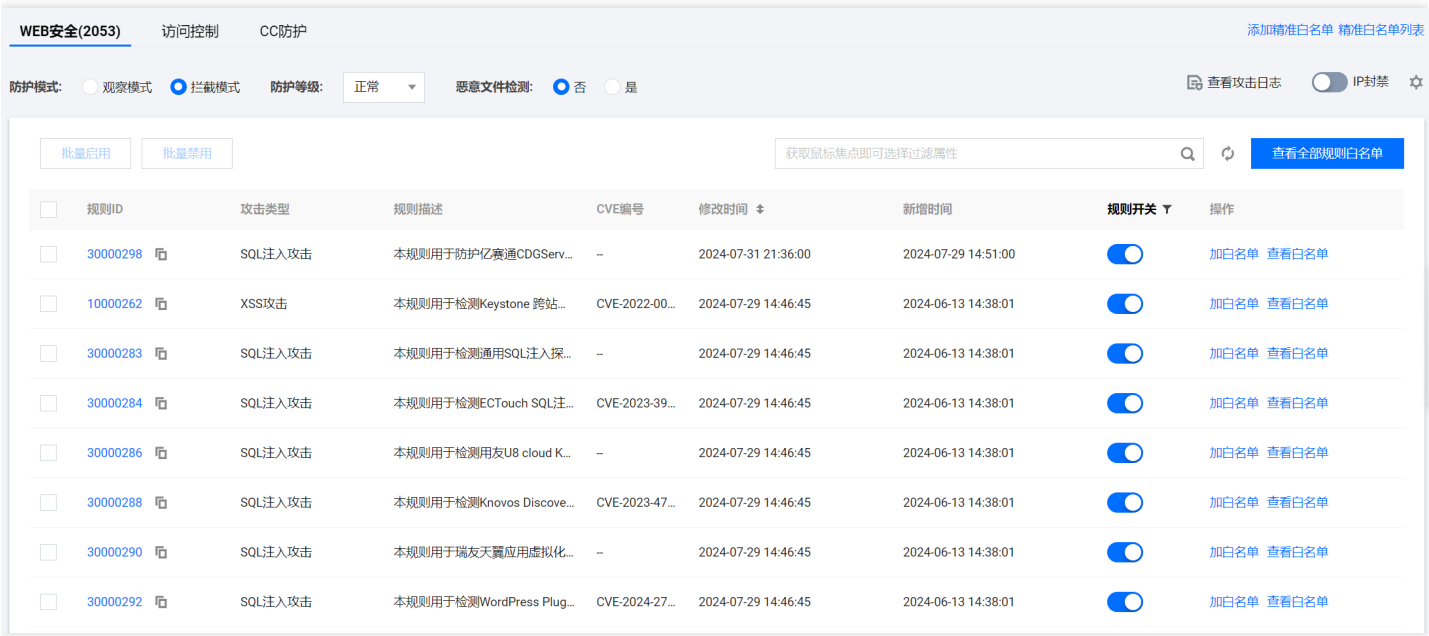
攻击分类	攻击描述
XSS攻击	跨站脚本 (XSS) 攻击是一种注入，其中恶意脚本被注入到其他受信任的网站中。 当攻击者使用 Web 应用程序将恶意代码（通常以浏览器端脚本的形式）发送给不同的最终用户时，就会发生 XSS 攻击。 允许这些攻击成功的缺陷非常普遍，并且发生在 Web 应用程序在其生成的输出中使用来自用户的输入而不对其进行验证或编码的任何地方。 攻击者可以使用 XSS 向毫无戒心的用户发送恶意脚本。 最终用户的浏览器无法知道该脚本不应受信任，并且会执行该脚本。 由于它认为脚本来自可信来源，因此恶意脚本可以访问浏览器保留并与该站点一起使用的任何 cookie、会话令牌或其他敏感信息。 这些脚本甚至可以重写 HTML 页面的内容。
XSS攻击(扩展)	跨站脚本攻击的扩展规则集，相比于标准规则集检测范围更广，检测内容更宽，检测能力更强，但是需要容忍一定的规则误报。

攻击分类	攻击描述
SQL注入攻击	SQL 注入攻击包括通过从客户端到应用程序的输入数据插入或"注入"SQL 查询。 成功的 SQL 注入漏洞可以从数据库中读取敏感数据、修改数据库数据（插入/更新/删除）、对数据库执行管理操作（例如关闭 DBMS）、恢复 DBMS 文件中存在的给定文件的内容 系统并在某些情况下向操作系统发出命令。SQL 注入攻击是一种注入攻击，其中 SQL 命令被注入到数据平面输入中，以影响预定义 SQL 命令的执行。
SQL注入攻击(扩展)	SQL注入攻击的扩展规则集，相比于标准规则集检测范围更广，检测内容更宽，检测能力更强，但是需要容忍一定的规则误报。
一般攻击	通用攻击包含操作系统命令注入攻击、Coldfusion 注入、LDAP 注入和更多其他通用攻击。
一般攻击(扩展)	通用攻击的扩展规则集，相比于标准规则集检测范围更广，检测内容更宽，检测能力更强，但是需要容忍一定的规则误报。
已知弱点	已知弱点主要用来检测各种应用、web服务器、中间件等出现的远程任意代码执行漏洞、远程任意命令执行漏洞、路径遍历漏洞、开放重定向漏洞、未授权访问漏洞等。
恶意机器人	恶意机器人检测主要用来检测Web扫描器，脚本批量获取工具等恶意工具。

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】，选择需要管理的域名后，进入WEB安全页面。
2. 在WEB安全管理页面，支持规则开启，关闭和只观察管理，以及添加对应的白名单规则能力。

备注：所有规则默认为开启拦截模式。



3. 用户可以通过“规则等级”、“攻击分类”、“CVEID”或输入“规则 ID”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严格规则。

CC防护设置

最近更新时间: 2024-12-19 17:12:00

功能简介

CC 防护对网站特定的 URL 进行访问保护。

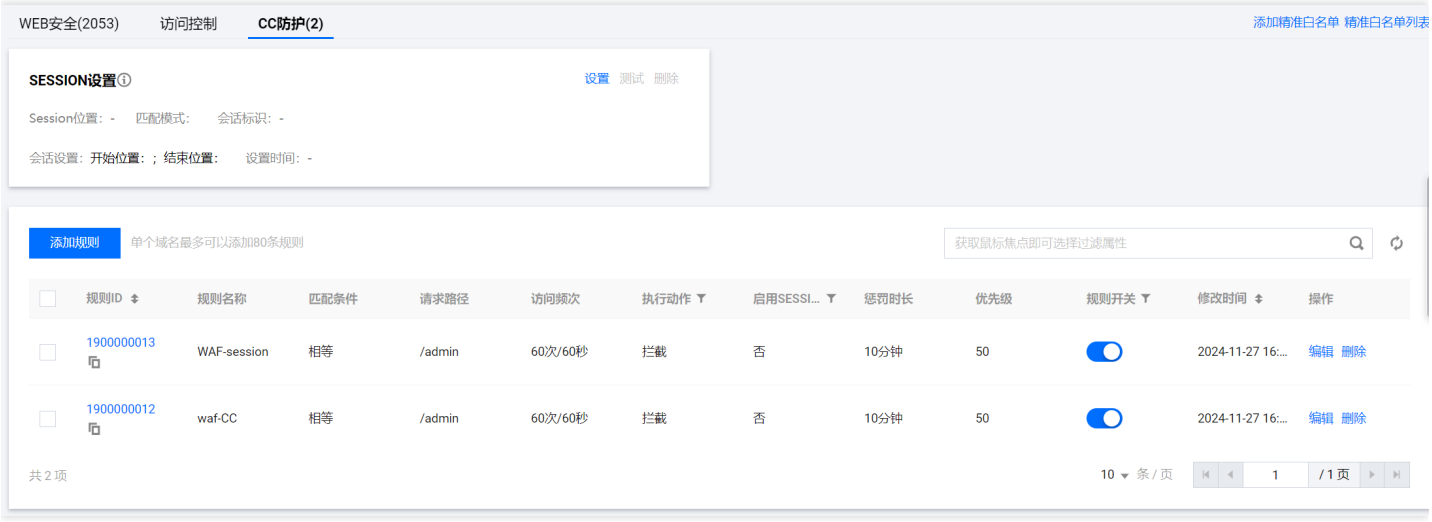
- 使用基于 SESSION 的 CC 防护策略，需要先进行 SESSION 设置，才能设置基于 SESSION 的 CC 防护策略。

配置步骤

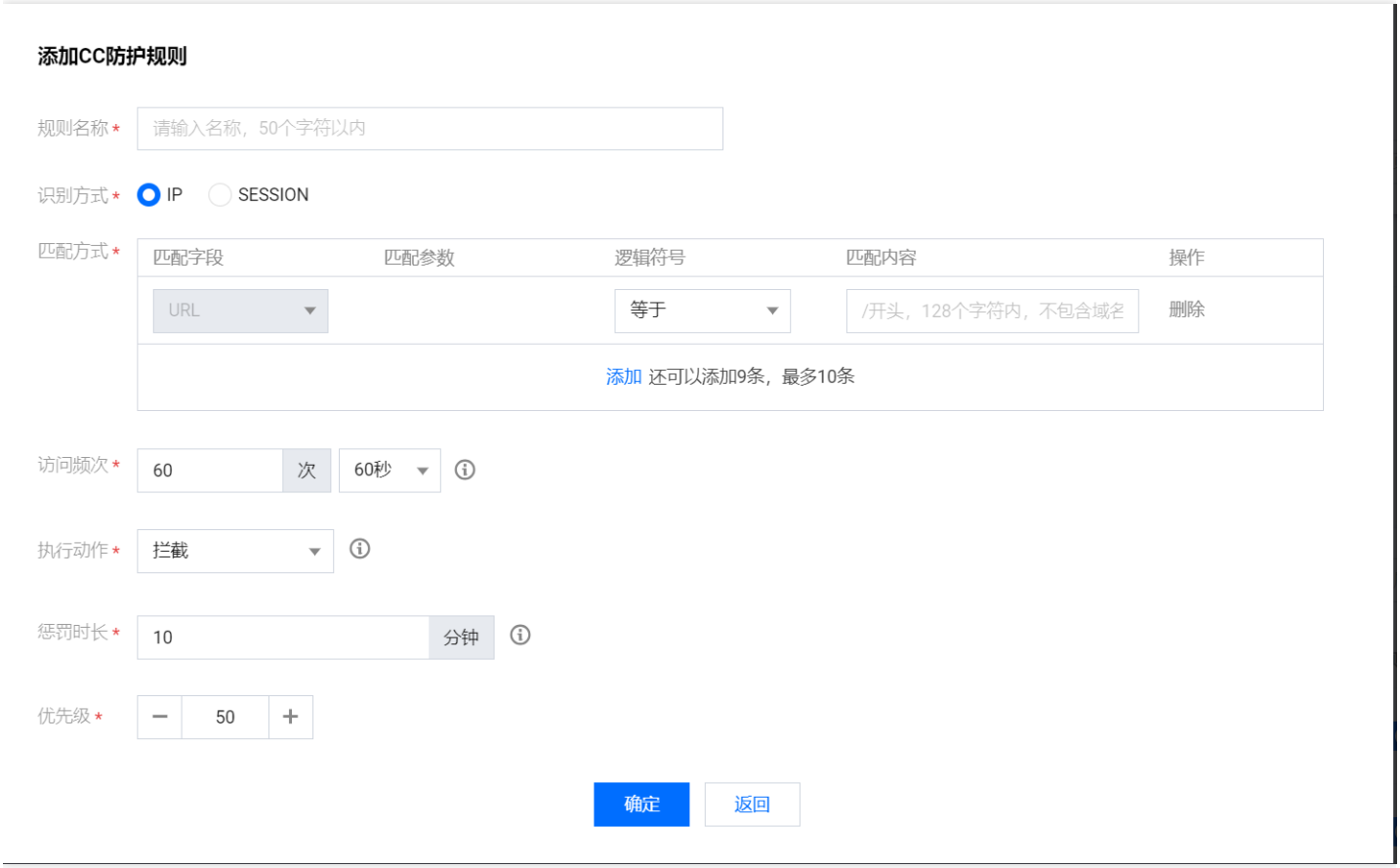
示例一： 基于访问源 IP 的 CC 防护设置

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【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名，单击选择【CC防护】进入配置页面。



2. 点击【添加规则】支持用户自定义添加 CC 防护规则页面，填写相应信息。



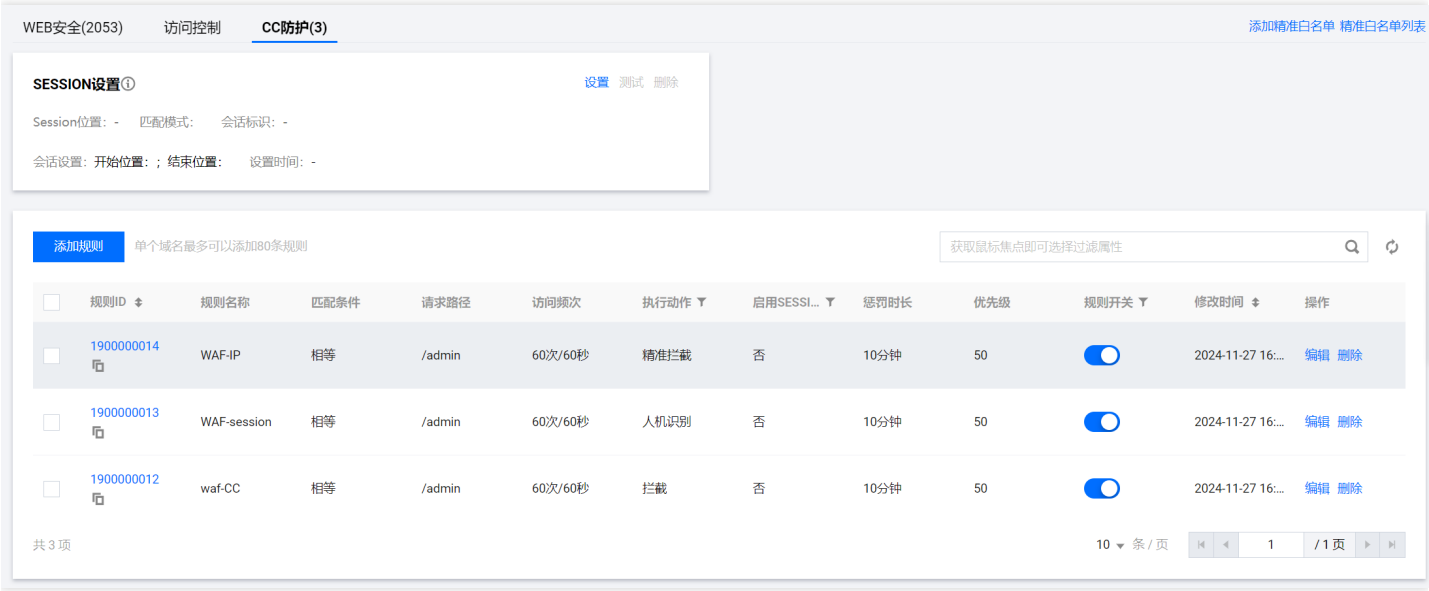
配置项说明：

- **识别模式：** IP、SESSION。
- **匹配条件：** 包括相等、前缀匹配和包含。

高级匹配：

- **匹配方式：**参考自定义规则的全部匹配字段设置。
- **访问频次：**根据业务情况设置访问频次。建议输入正常访问速度的3 - 10倍，例如网站人平均访问20次/分钟，可配置为60 - 200/分钟，可依据被攻击严重程度调整。
- **执行动作：**观察、人机识别和阻断。
- **惩罚时长：**最短为1分钟，最长为一周。
- **优先级：**请输入1 - 100的整数，数字越小，代表这条规则的执行优先级越高，相同优先级下，创建时间越晚，优先级越高。

1. 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。



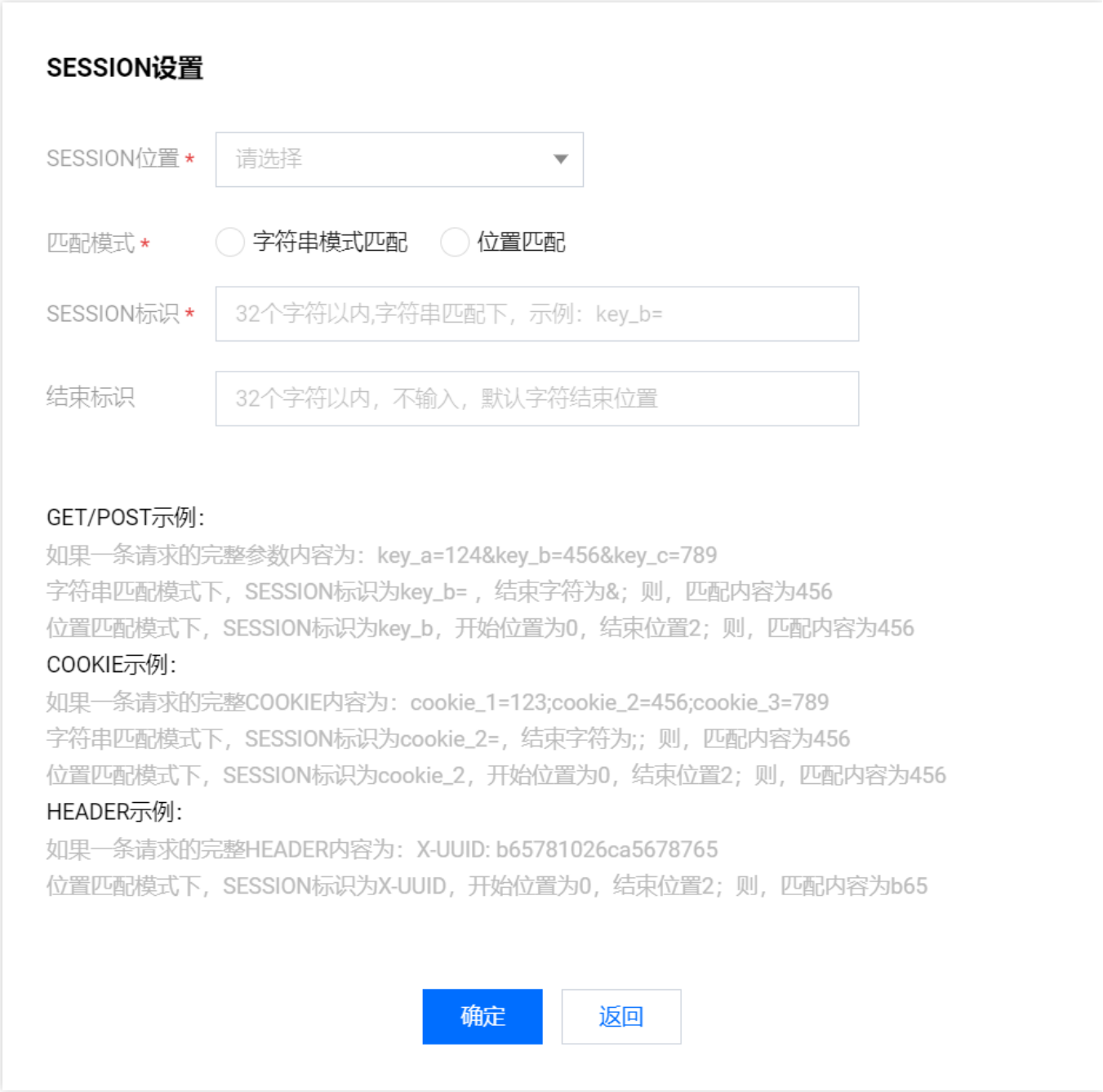
2. 根据规则设置，触发 CC 攻击行为，看到WAF返回的拦截页面。
3. 查看 IP 实时阻断信息。在左侧导航栏，选择【IP 管理】>【IP 封堵状态】 ，可以查看实时阻断的 IP 信息 ,并对 IP 进行加白或者加黑处理。

示例二： 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. 进入 Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名，单击选择【CC防护】进入配置页面。

2. 单击CC 防护设置中【新增】，支持自定义SESSION字段设置。



3. 进入 SESSION 设置页面，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【设置】。

配置项说明：

- **SESSION 位置 ：**可选择 COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。
- **匹配说明 ：**位置匹配或者字符串匹配。
- **SESSION 标识 ：**取值标识。

- **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。

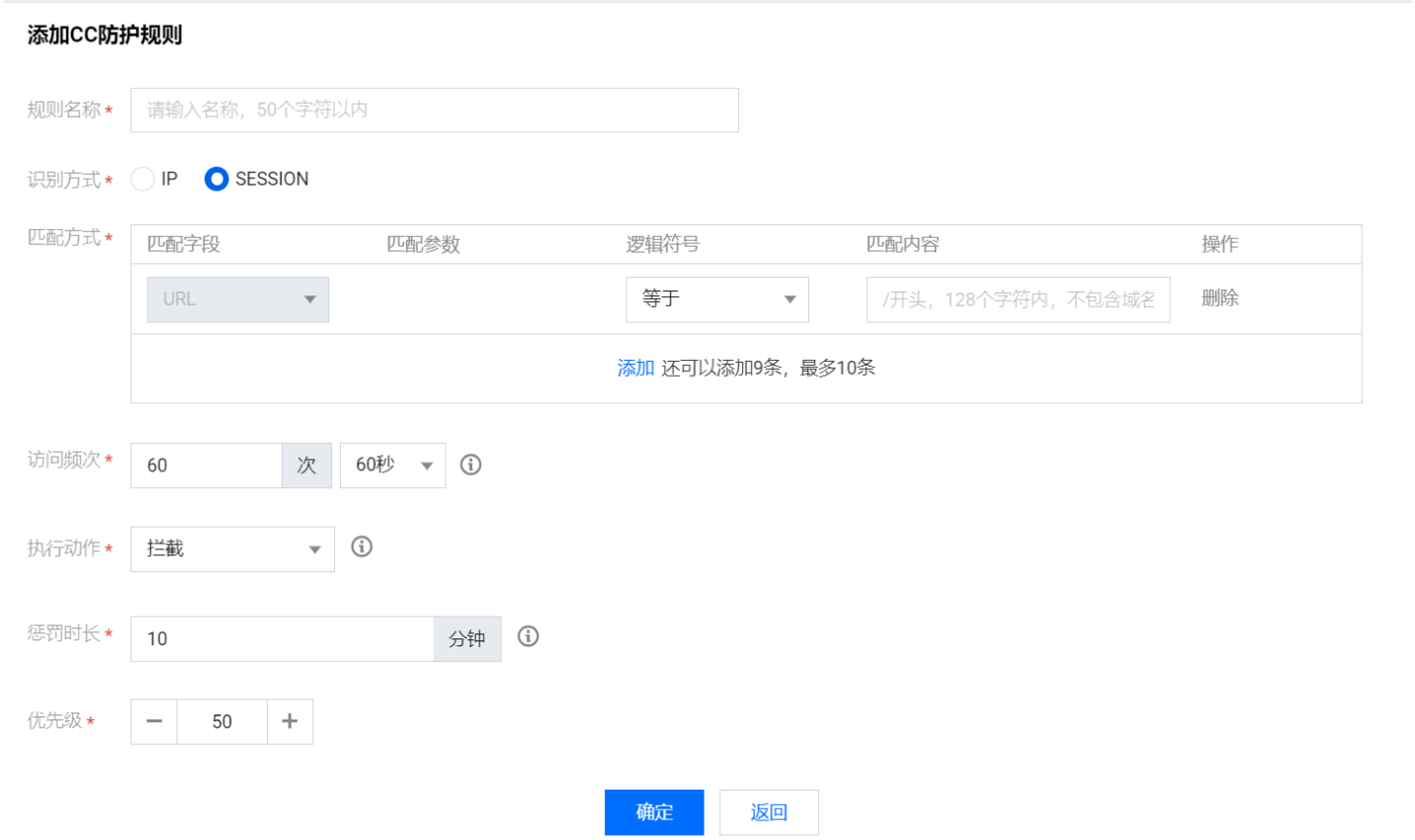
COOKIE 示例 ： 如果一条请求的完整 COOKIE 内容为：cookie_1 = 123;cookie_2 = 456;cookie_3 = 789。

- 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。

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



2. 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。



3. 配置完成，基于 SESSION 的 CC 防护策略生效。 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。

自定义策略

最近更新时间: 2024-12-19 17:12:00

功能简介

自定义策略支持从 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，用户可以利用自定义策略灵活应对，组合出有针对性的规则来阻断各类攻击行为。

- 每个自定义策略最多可以设置5个条件进行特征控制。
- 每个自定义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。
- 每个自定义策略匹配之后可以配置两种处理动作：阻断和放行。

配置案例

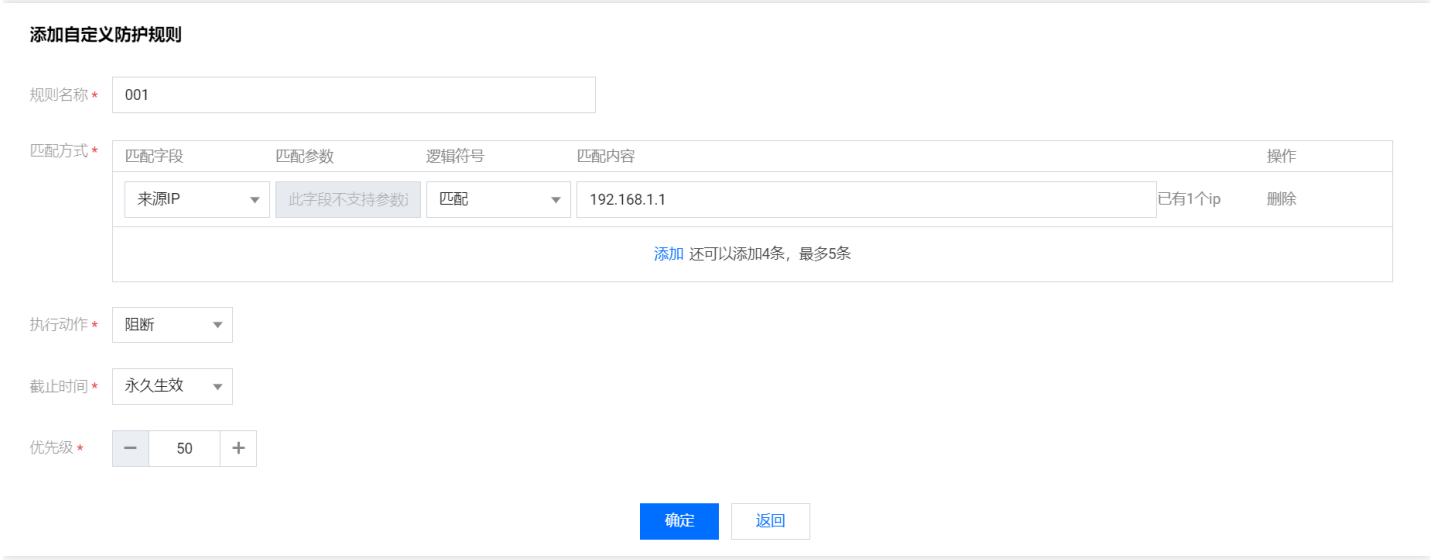
案例一：禁止特定 IP 地址访问指定站点

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，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【访问控制】进入配置页面。



2. 在添加规则页面内，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 【添加】 保存规则。



Web 应用防火墙的自定义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` ）。

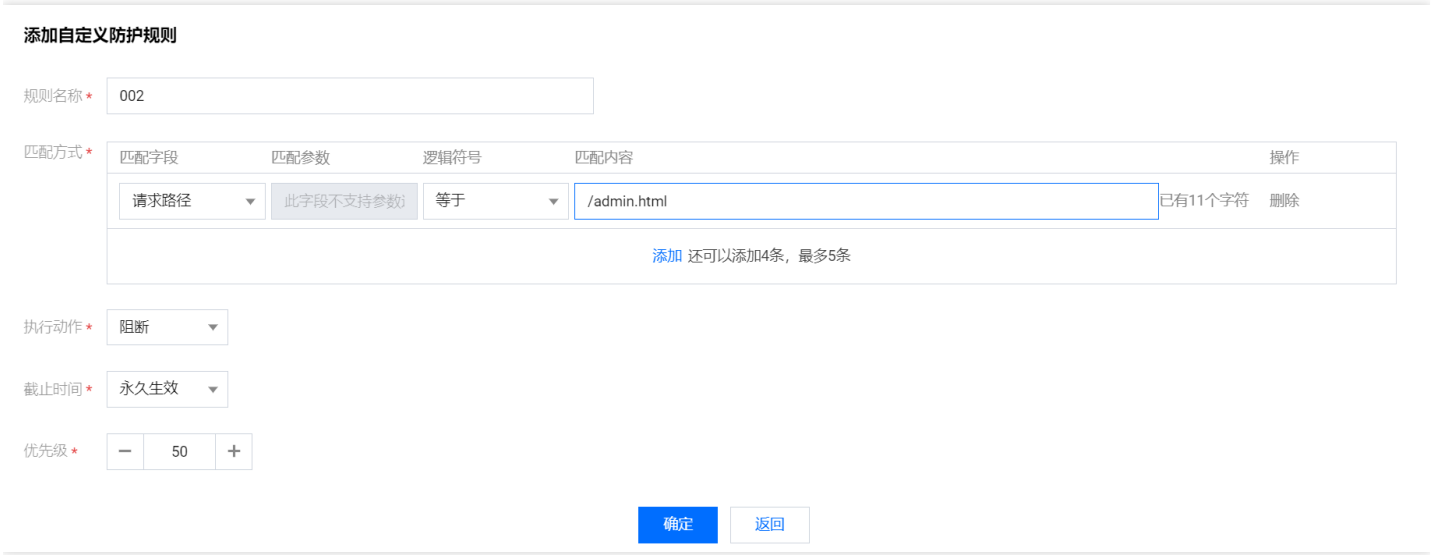
3. 此时规则将会生效，来自特定源 IP 的 HTTP 访问请求将会全部阻断。



规则ID	规则名称	匹配条件	执行动作	创建时间	优先级	过期时间	规则开关	操作
1100000026	001	来源IP匹配,192.168.1.1	阻断	2024-11-27 16:37:35	50	永不过期		编辑 删除
1100000025	WAF-自定义	来源IP匹配,1.1.1.1	阻断	2024-11-27 16:35:19	50	2024-12-28 23:59:59		编辑 删除

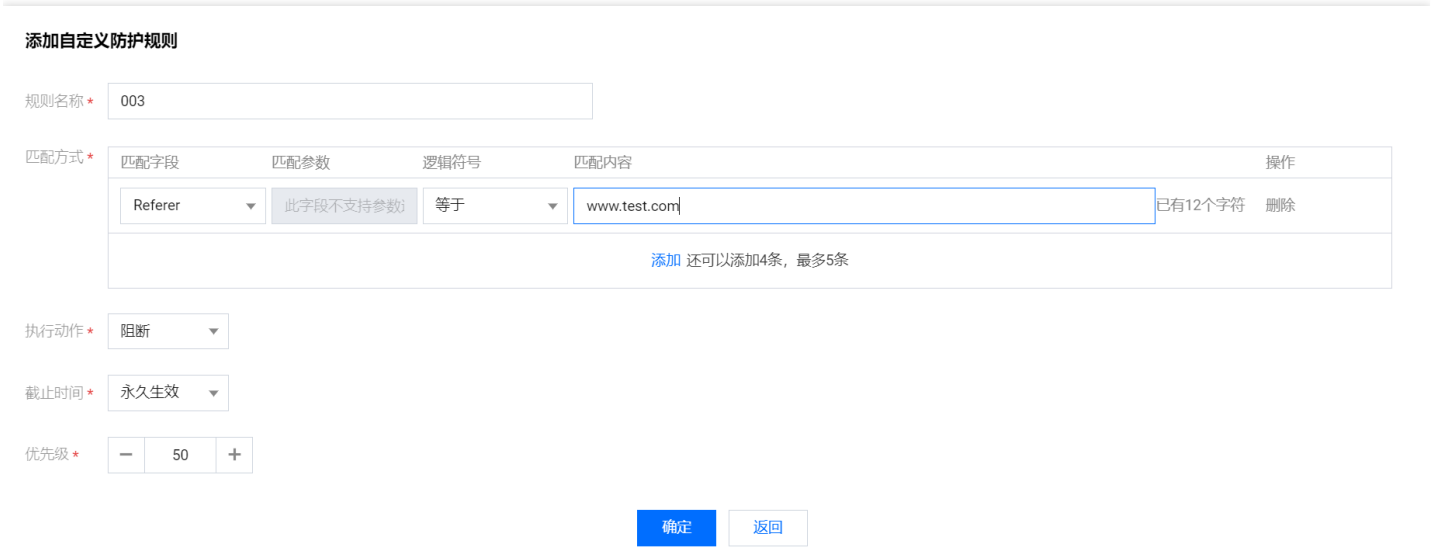
案例二：禁止公网用户访问特定的 Web 资源

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【添加】即可。



案例三：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，可以利用自定义策略对盗链请求的 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【添加】即可。



网页防篡改

最近更新时间: 2024-12-19 17:12:00

功能简介

防篡改功能可用于防止发生指定页面被篡改而显示异常的问题。

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

备注：负载均衡型WAF实例暂不支持

配置示例

保护网站主页不被篡改

1. 登录Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【防篡改】进入配置页面。



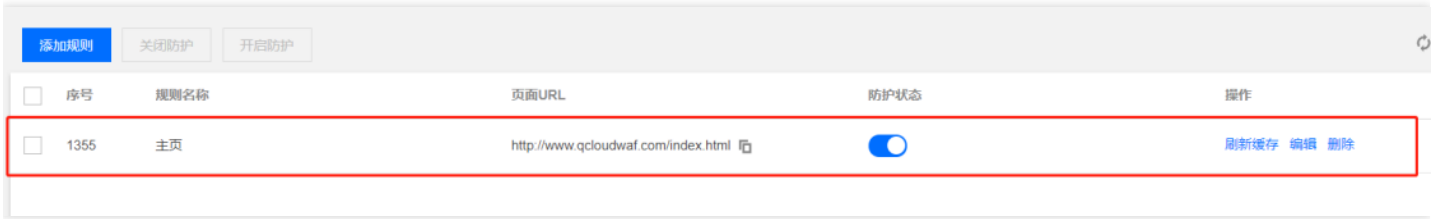
2. 进入防护设置页面，如果有需要可以在上方更换需要防护的站点域名，单击【防篡改】，进入防篡改配置界面，单击 【添加规则】。



3. 在添加防篡改规则弹窗内，输入规则名称（如主页），输入规则（如主页）完整的 URL 路径（如 `http://www.qcloudwaf.com/index.html` ），输入完成后单击【添加】，保存规则。



4. 此时规则将会生效，如果规则更新，在右侧操作栏，单击【刷新缓存】，可更新缓存内容。



防信息泄露

最近更新时间: 2024-12-19 17:12:00

1. 功能简介

防信息泄露功能支持将您网页中返回的敏感信息进行替换，如手机号码、身份证号等。

备注：负载均衡型WAF实例暂不支持

2. 配置示例

1. 登录Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【防信息泄漏】进入配置页面。选择【防信息泄露】>【添加规则】。

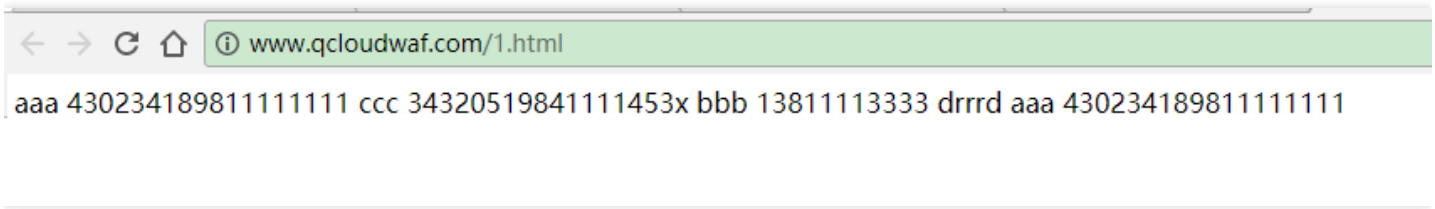


在添加规则页面，输入规则名称、选择匹配条件（匹配字段为敏感信息，匹配条件为包含，匹配内容为身份证或手机号）和执行动作（替换或观察），设置完成后，单击 【确定】 保存。



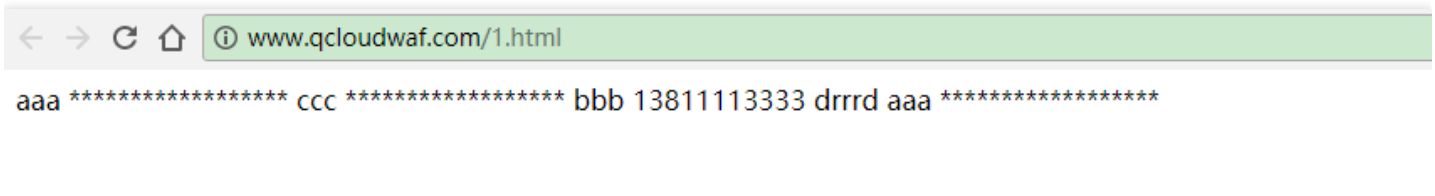
2. 规则生效，会对您网页中返回的敏感信息进行防护，防护效果如下（敏感内容为虚构）：

- **开启防护前：**



开启防护前

- **开启防护后：**



开启防护后

防信息泄露

最近更新时间: 2024-12-19 17:12:00

1. 功能简介

防信息泄露功能支持将您网页中返回的敏感信息进行替换，如手机号码、身份证号等。

备注：负载均衡型WAF实例暂不支持

2. 配置示例

1. 登录Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【防信息泄漏】进入配置页面。选择【防信息泄露】>【添加规则】。

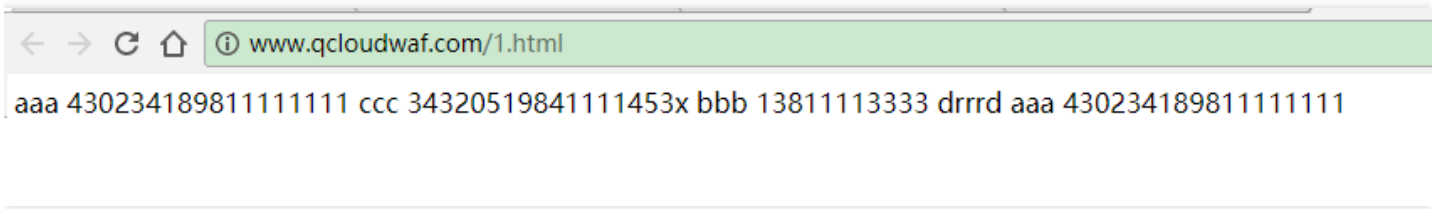


在添加规则页面，输入规则名称、选择匹配条件（匹配字段为敏感信息，匹配条件为包含，匹配内容为身份证或手机号）和执行动作（替换或观察），设置完成后，单击 【确定】 保存。



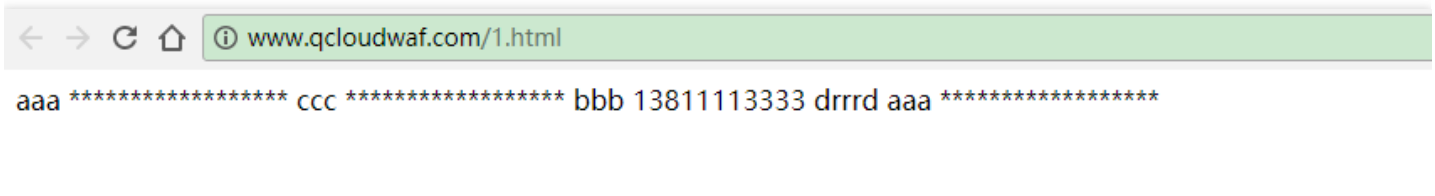
2. 规则生效，会对您网页中返回的敏感信息进行防护，防护效果如下（敏感内容为虚构）：

- **开启防护前：**



开启防护前

- **开启防护后：**



开启防护后

地域封禁

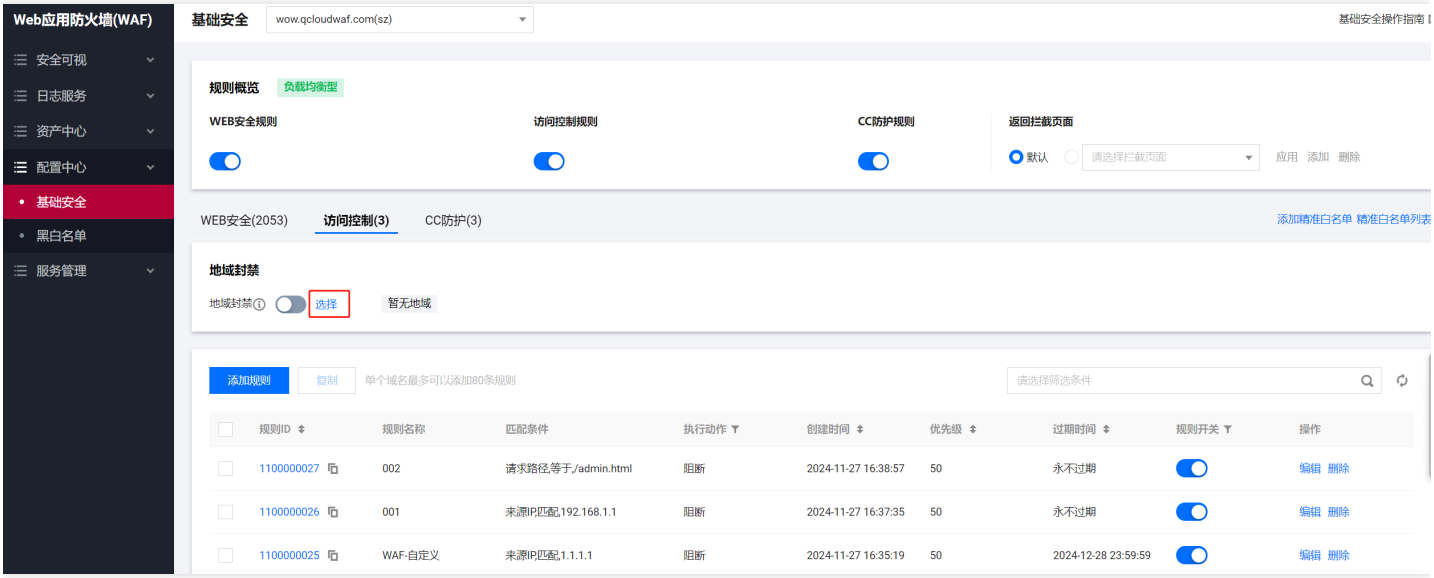
最近更新时间: 2024-12-19 17:12:00

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。

配置说明

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【访问控制】进入配置页面，选在地域封禁配置。



2. 在访问控制设置页面，单击【选择】地域封禁配置，进入地域封禁配置页面。



3. 在封禁地域设置页面，勾选需要封禁的国内地区，国外地区支持搜索或单击下拉列表进行选择，选择完成后单击【确定】。



4. 编辑完成后，开启地域封禁状态。

5. 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，使用境外 IP 地址访问防护网站，Web 应用防火墙会提示您已被拦截。

攻击日志

最近更新时间: 2024-12-19 17:12:00

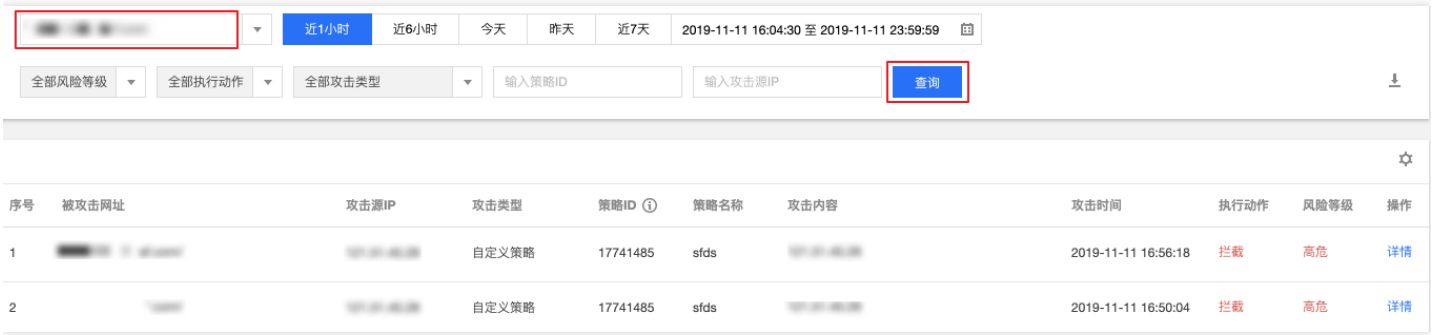
1. 功能简介

Web 应用防火墙默认记录 Web 攻击日志信息，包括攻击产生的时间、攻击源 IP、攻击类型、攻击详情等信息。您可以根据需要按照过滤条件进行日志查询，并下载查询结果。

2. 使用说明

2.1 查询攻击日志

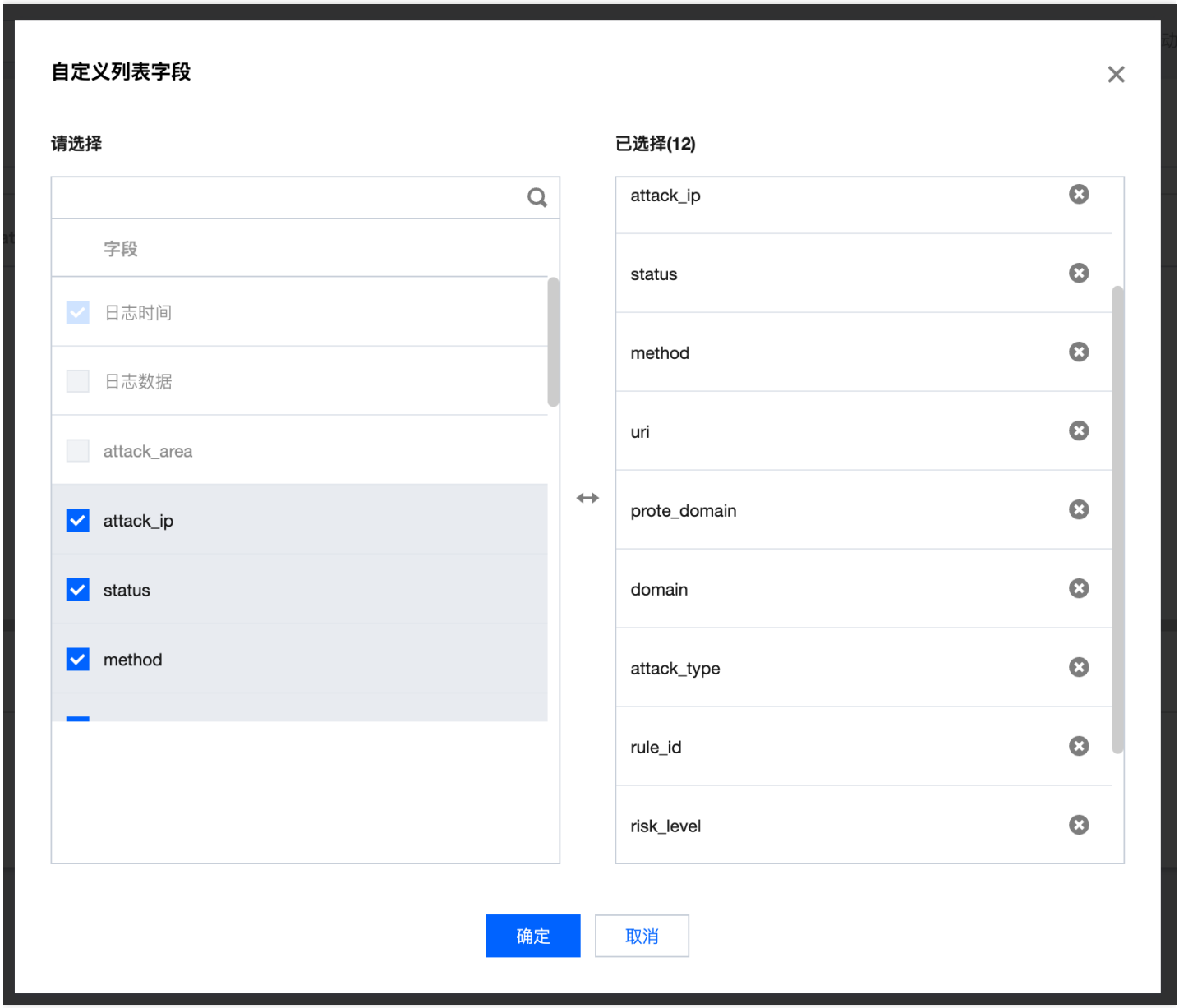
1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择【日志服务】>【攻击日志】。进入攻击日志查询页面，单击【日志查询】，在上方下拉搜索列表中选择域名，根据需要设置查询条件，单击【查询】，查看对应的攻击日志信息。



查询条件说明：

- 域名：在域名下拉搜索列表中，选择需要查询的域名。
- 时间条件：默认为1个小时，最长可查询30天的攻击日志信息。
- 风险等级：默认为全部，可选择高危、中危、低危。
- 执行动作：默认为全部，可选观察和拦截。
- 策略 ID：输入您需要查询的策略 ID（策略 ID 可以在日志条目中查看）。
- 攻击源 IP：输入您要查询的攻击源 IP，进行查询。

2. 单击攻击日志右上角的设置按钮 ，在弹出的“自定义列表字段”弹窗中，选择需要显示的列表详细信息。如下图所示：



3. 查看攻击详情。选择您需要查看日志条目，在右侧操作栏，单击【详情】，查看攻击详情信息。

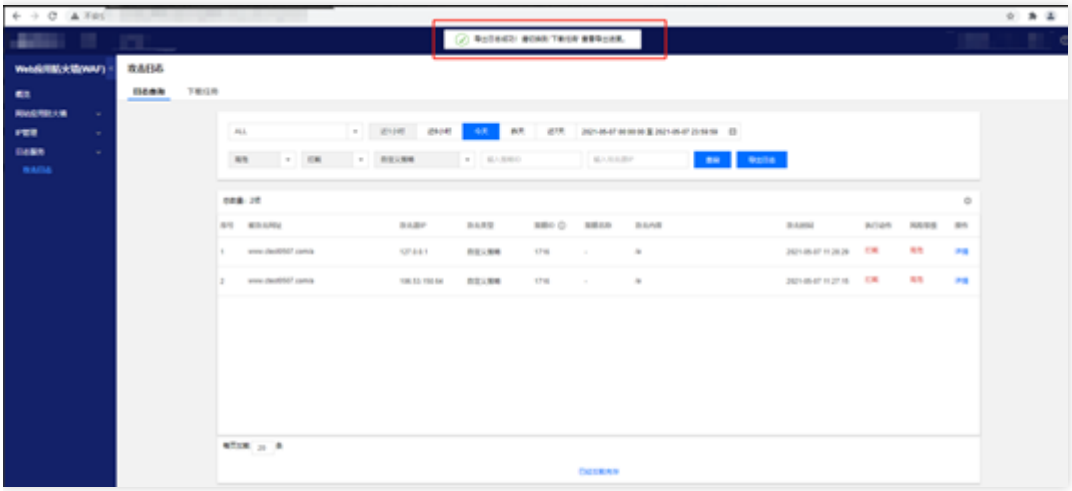


4. 进入日志详情页面，查看对应字段。



2.2 导出攻击日志

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】。进入攻击日志查询页面，单击【日志查询】，在上方下拉搜索列表中选择域名，根据需要设置查询条件，单击【查询】，查看对应的攻击日志信息。单击【导出日志】，导出对应的攻击日志信息。



导出条件说明：

- 域名：在域名下拉搜索列表中，选择需要查询的域名。
- 时间条件：默认为1个小时，最长可查询30天的攻击日志信息。
- 风险等级：默认为全部，可选择高危、中危、低危。
- 执行动作：默认为全部，可选观察和拦截。
- 策略 ID：输入您需要查询的策略 ID（策略 ID 可以在日志条目中查看）。
- 攻击源 IP：输入您要查询的攻击源 IP，进行查询。

- 日志表格内容不可为空。

2. 选择【日志服务】>【攻击日志】>【下载任务】。进入下载任务查询页面。如下图所示：



3. 单击【下载】，提示"日志文件下地址复制成功，请新建浏览器窗口打开"将链接复制到浏览器中打开，成功下载出日志压缩包。



日志详情字段说明：

- **基础信息**

字段名称	字段说明
域名	客户端访问的域名
攻击类型	当前 Web 应用防火墙支持的攻击类型信息，默认为全部。
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。
攻击源 IP	客户端攻击的源 IP。
命中规则 ID	触发防护策略的规则 ID，其中 AI 引擎检出的攻击，规则 ID 为0。
命中规则名称	触发防护策略的策略名称，其中规则引擎和 AI 引擎的策略名称为空。

字段名称	字段说明
请求方法	客户端攻击请求方法。
风险等级	客户端攻击触发的风险等级。
攻击时间	客户端攻击触发的时间。
匹配来源	客户端攻击匹配来源信息，如来源 IP。
执行动作	客户端攻击触发的动作。
请求 URI	请求 URI 的内容。
攻击内容	客户端触发攻击的内容。

- **攻击 IP 详情**

字段名称	字段说明
地区	购买源 IP 国家英文缩写。
IP 所有者	购买源 IP 所有者信息。
国家	攻击源 IP 所属的国家名称。
省份	攻击源 IP 所属的省份信息。
城市	攻击源 IP 所属的城市信息。
运营商	攻击源 IP 所属的运营商信息。
经度	攻击源 IP 的经度信息。
纬度	攻击源 IP 的纬度信息。

- **详情信息**

字段名称	字段说明
协议版本	攻击源 IP 的 HTTP 协议版本信息。
User-Agent	攻击源 IP 向服务器用来表明自己的浏览器类型和操作系统标识等信息。

IP管理

最近更新时间: 2024-12-19 17:12:00

功能简介

Web 应用防火墙 IP 管理功能，对经过 Web 应用防火墙防护域名的访问源 IP 进行状态查询和黑白名单设置，主要功能包括：IP 查询，IP 黑白名单设置和 IP 封堵状态查询。

- IP 查询，查询输入 IP 在防御域名中状态信息，包括是否在黑白名单中，是否处于封堵状态。
- 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。
- IP 封堵状态，实时查看 CC 攻击、自定义策略人机识别等源 IP 封堵状态信息。

配置步骤

示例一 IP 查询

1. 进入 Web 应用防火墙控制台，选择【IP 管理】>【IP 查询】输入需要查询的 IP 地址查看该 IP 状态。



2. 查询出的 IP 地址，可手动添加黑白名单。

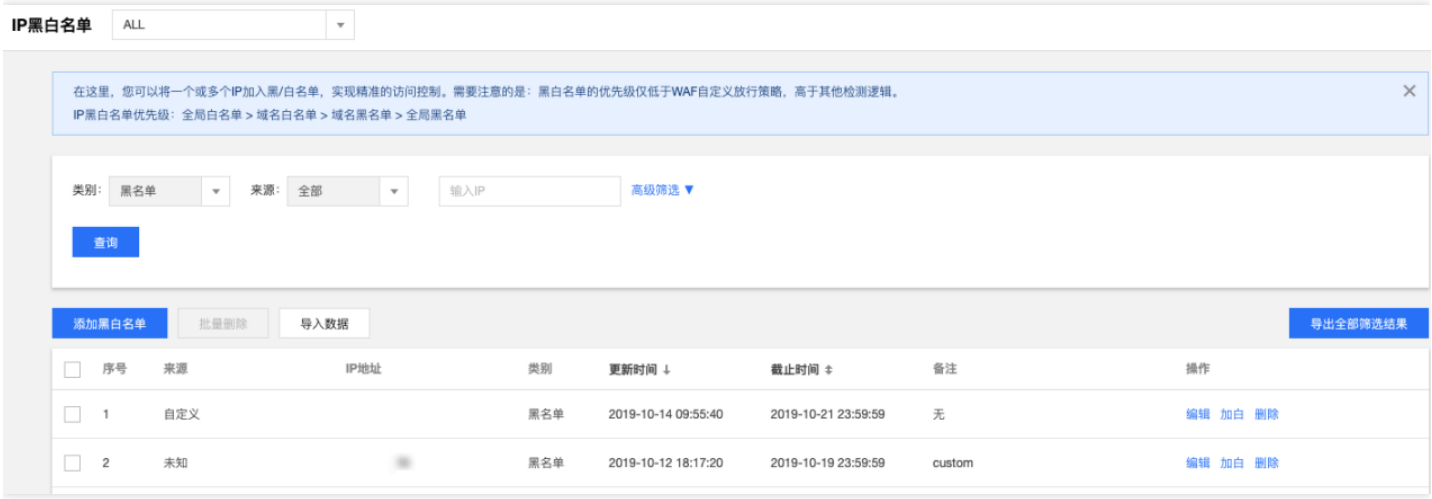


示例二 添加 IP 黑名单

1. 进入 Web 应用防火墙控制台，选择【IP 管理】>【IP 黑白名单】进入配置页面。

IP 黑名单名单模块，可以添加基于域名的黑白名单或基于全局的黑白名单，生效优先级说明说如下：

- 黑白名单的优先级仅低于 Web 应用防火墙自定义放行策略，高于其他检测逻辑。
- IP黑白名单优先级从高到低顺序：全局白名单>域名白名单>域名黑名单>全局黑名单。



配置项说明：

- 类别：黑名单、白名单。
- 来源：CC 防护、自定义规则。
- 高级筛选：利用创建时间和有效截止时间进行 IP 信息筛选。

2. 添加黑白名单。左上角选择需要添加防护的域名，单击【添加黑白名单】，选择黑名单添加需要加黑的 IP 地址。



选择域名为 ALL 时，添加的 IP 黑白名单为全局的黑白名单。

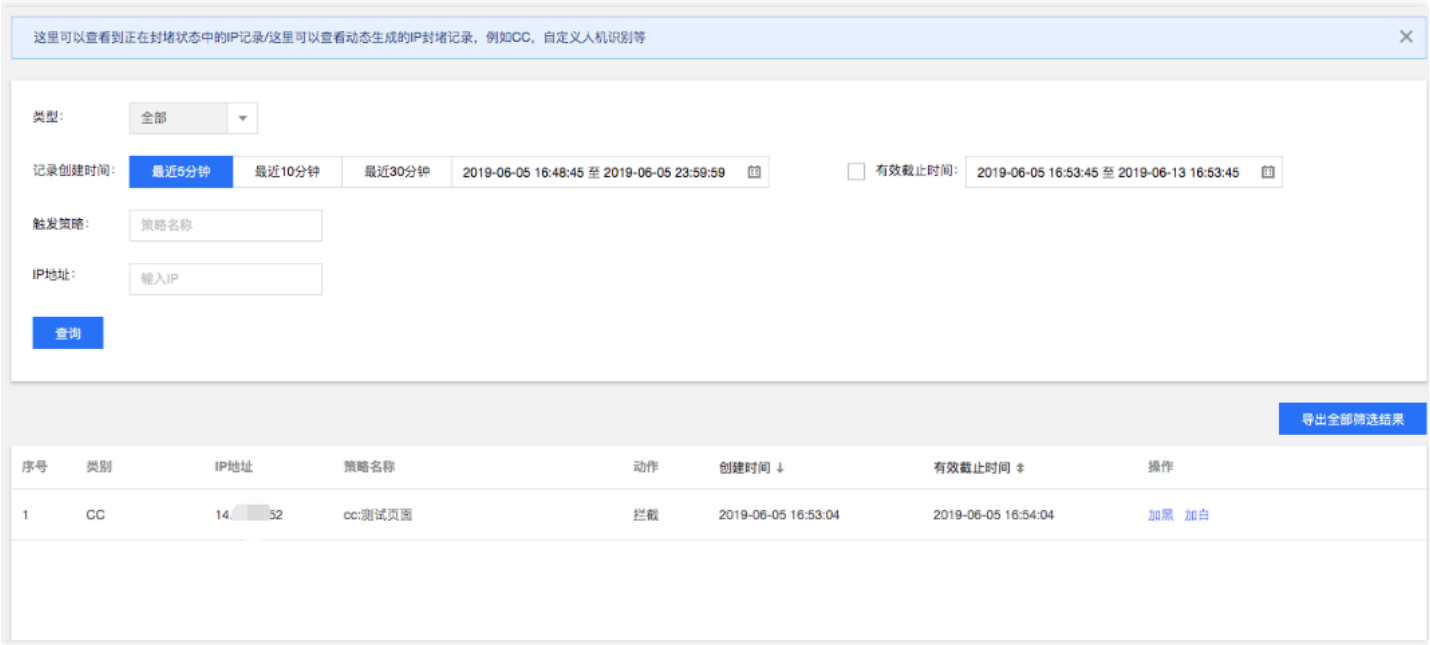
3. 黑白名单支持导入和筛选结果导出，导入 IP 信息时，请参考导出格式。



4. 添加完成后，可以在 IP 查询中输入添加的源 IP，查询状态信息。

示例三 IP 封堵状态查询

进入Web 应用防火墙控制台，选择【IP 管理】>【IP 封堵状态】进入查询页面，可以查询自定义规则、CC 防护模块拦截的 IP 信息。可对查询结果进行导出，对单个 IP 进行加黑加白操作。


这里可以查看到正在封堵状态中的IP记录/这里可以查看动态生成的IP封堵记录，例如CC，自定义人机识别等
类型：
全部
记录创建时间：
最近5分钟
最近10分钟
最近30分钟
2019-06-05 16:48:45 至 2019-06-05 23:59:59
有效截止时间：
2019-06-05 16:53:45 至 2019-06-13 16:53:45
触发策略：
策略名称
IP地址：
输入IP
查询
导出全部筛选结果
序号
类别
IP地址
策略名称
动作
创建时间
有效截止时间
操作
1
CC
14.52
cc:测试页面
拦截
2019-06-05 16:53:04
2019-06-05 16:54:04
加黑
加白

常见操作
场景1 创建实例

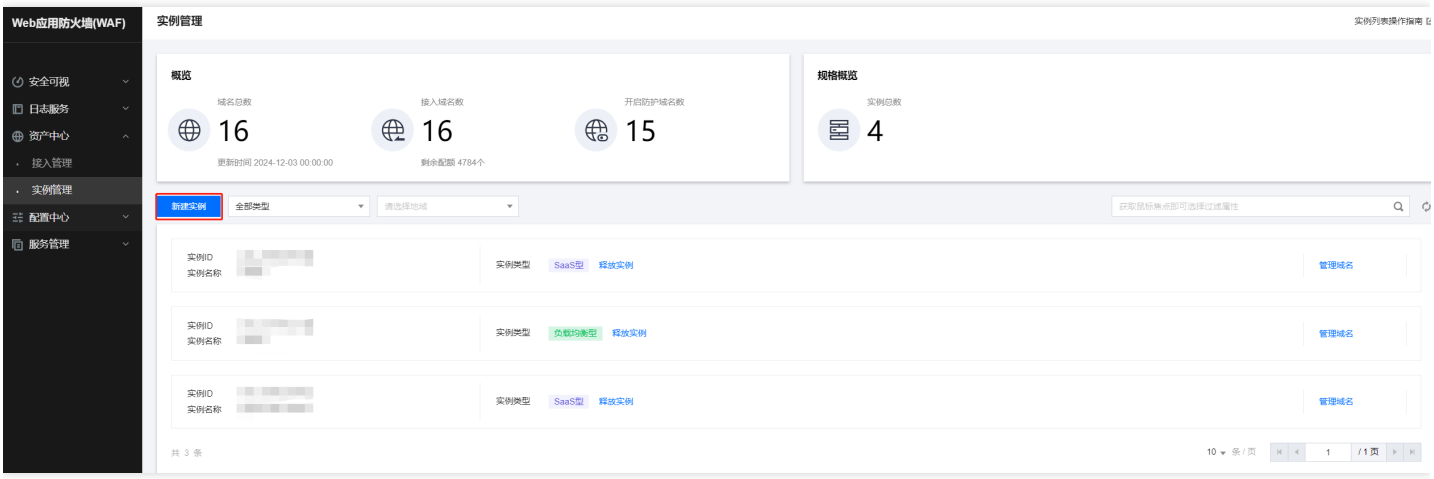
最近更新时间: 2024-12-19 17:12:00

实例是WAF计量的最小单位，支持创建多个实例；1个实例支持管理20个域名。

以下操作以cloud为例，创建实例。

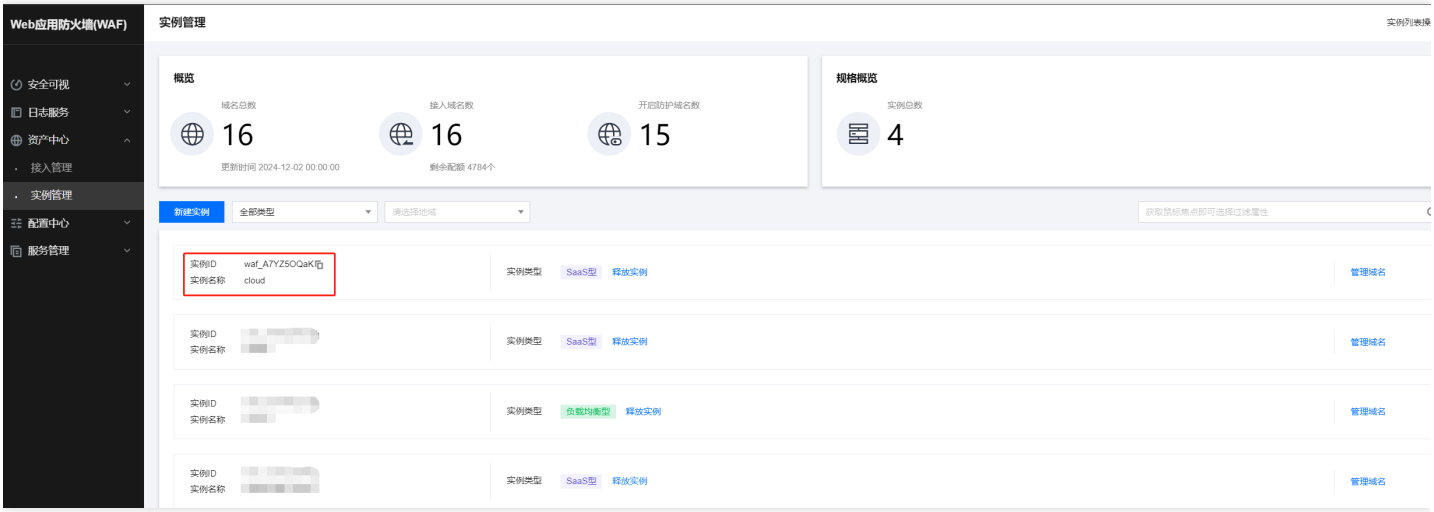
创建SaaS型实例

1.登录租户端WAF-资产中心-实例管理页面，点击新建实例；



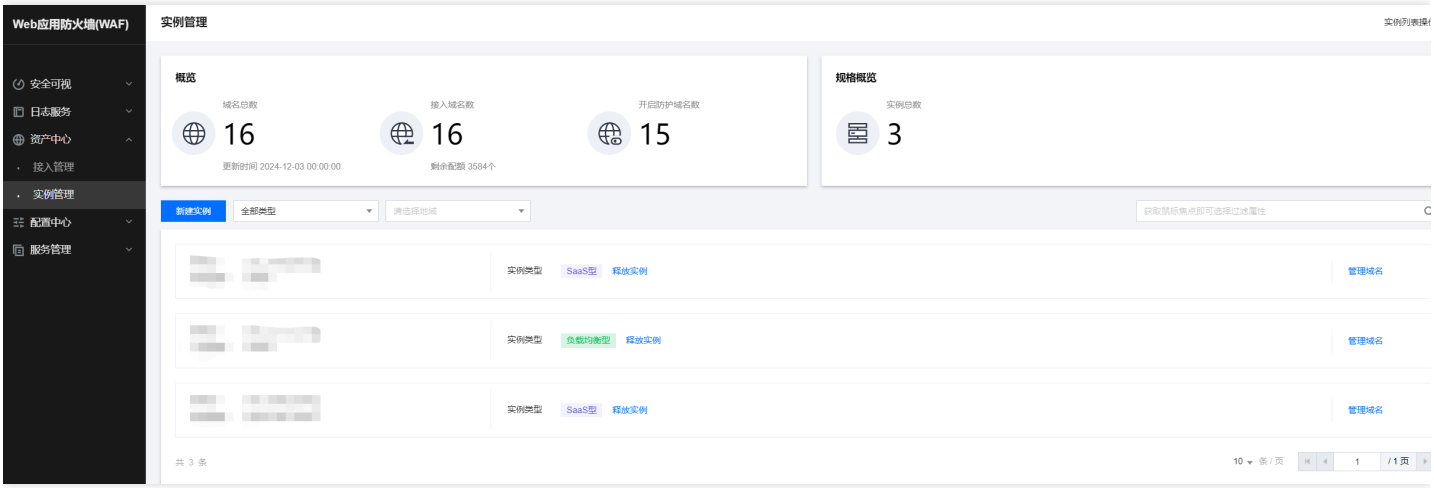
2.在购买页，实例类型选择“SaaS型”，实例名称填“cloud”，最后点击“立即购买”；



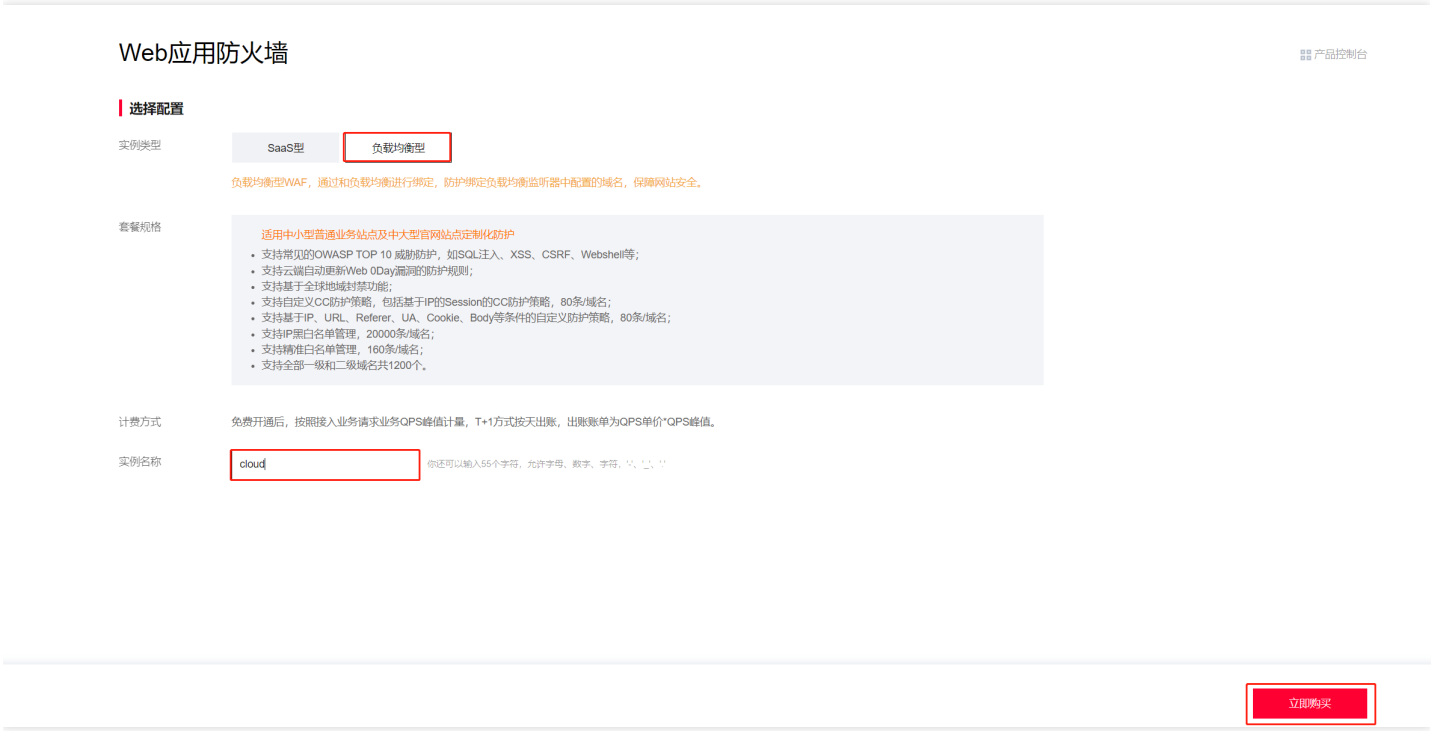


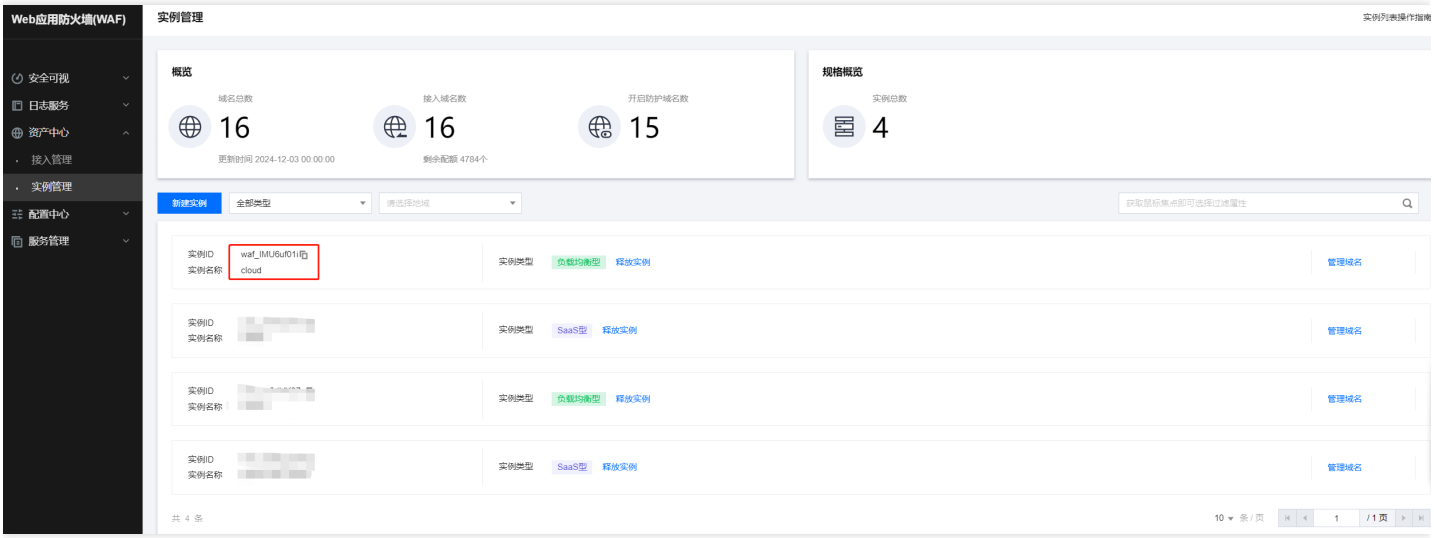
创建负载均衡型实例

1.登录租户端WAF-资产中心-实例管理页面，点击新建实例；



2.在购买页，实例类型选择“负载均衡型实例”，实例名称填“cloud”，最后点击“立即购买”；



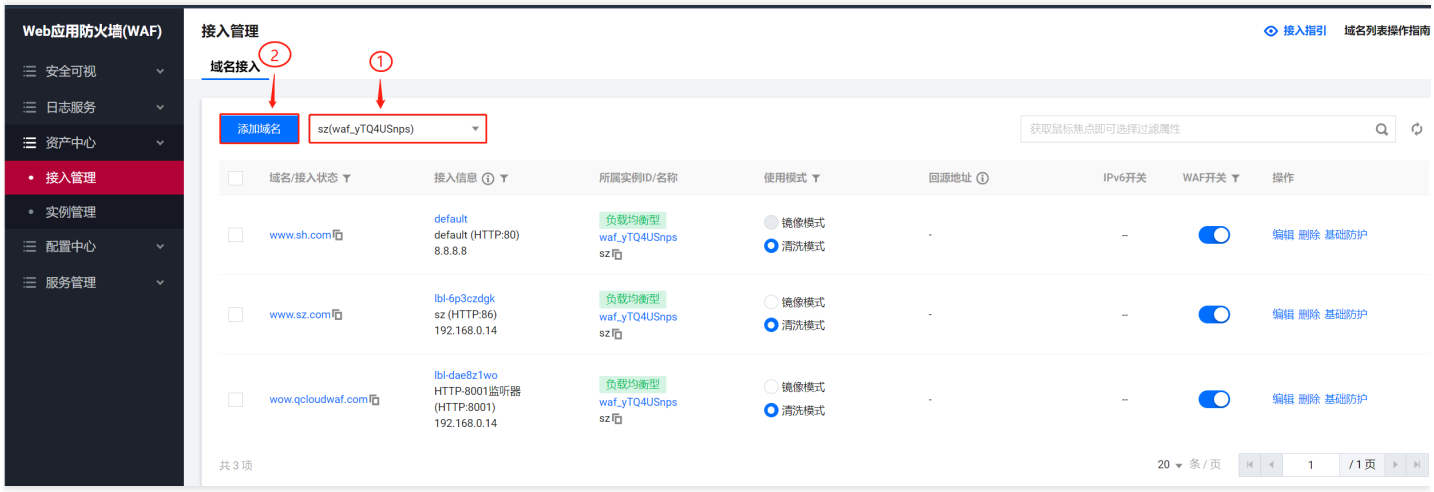

Web应用防火墙(WAF)
实例管理
实例列表操作指南
安全可视
日志服务
资产中心
接入管理
实例管理
配置中心
服务管理
概览
域名总数
16
更新时间 2024-12-03 00:00:00
接入域名数
16
剩余配额 4784个
开启防护域名数
15
规格概览
实例总数
4
新建实例
全部类型
请选择地域
获取鼠标焦点即可选择过滤属性
实例ID
实例名称
waf_IMU6uf01i
cloud
实例类型
负载均衡型
释放实例
管理域名
SaaS型
共 4 条
10 条 / 页
1
/ 1 页

场景2：添加clb-waf型防护域名

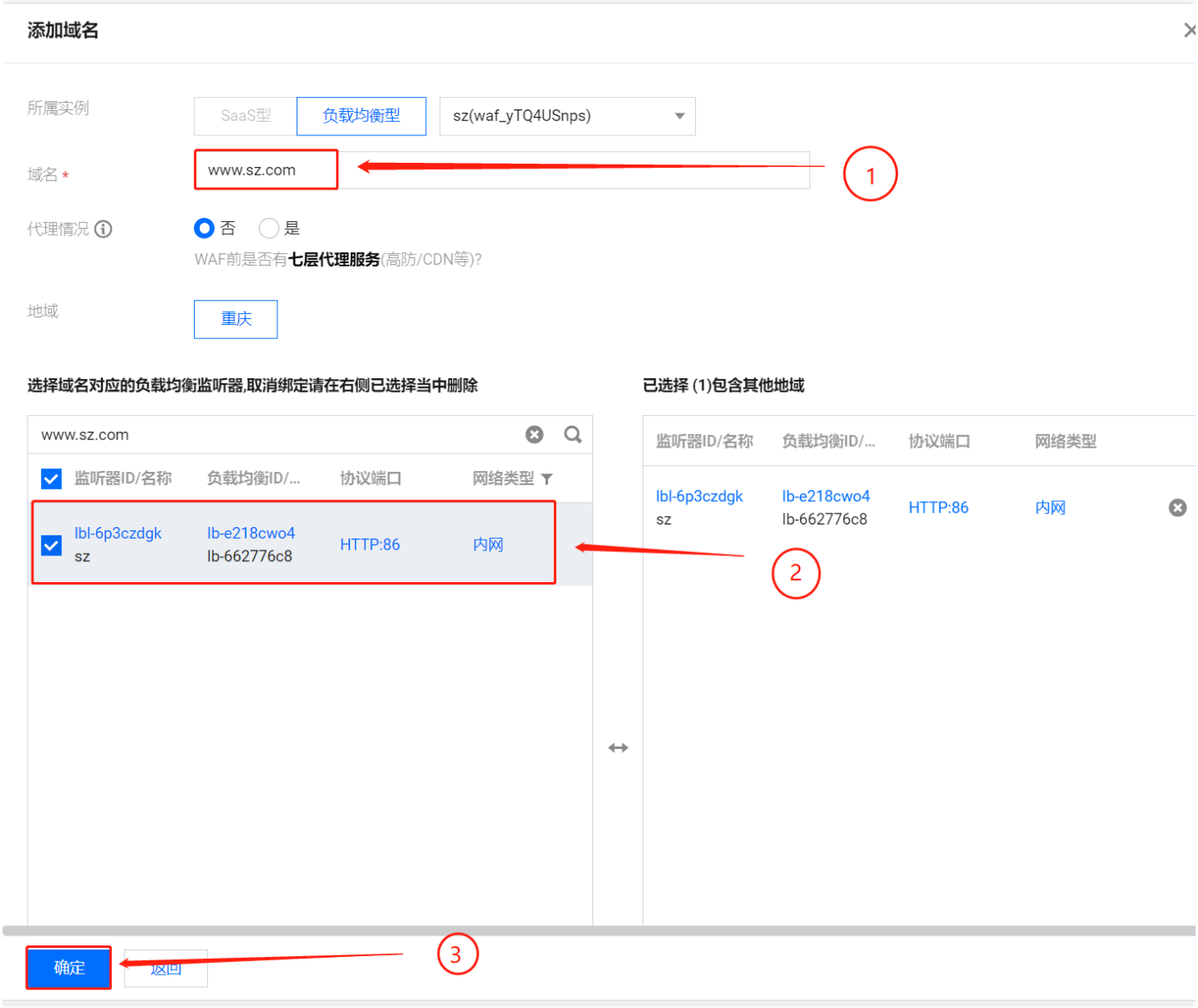
最近更新时间: 2024-12-19 17:12:00

如下操作是以“www.sz.com”为例，“www.sz.com” 域名绑定在该租户的CLB中。

1. 登录租户端WAF-资产中心-接入管理页面，先选择实例，然后点击添加域名。



2. 进入添加域名界面，先输入域名，勾选域名对应的负载均衡监听器，最后点击确定。





3. 进入接入管理界面，核实域名防护状态。

- 检查域名/接入状态，确认添加的域名为预期域名；

- 检查接入信息中的ip为clb实例中的vip；
- 检查所属实例ID/名称为预期创建的实例ID；
- 检查使用模式为清洗模式：清洗模式可检测流量、可拦截恶意流量，镜像模式不能拦截流量、可检测流量；
- 检查WAF开关为蓝色开启状态。



场景3：添加saas-waf型防护域名

最近更新时间: 2024-12-19 17:12:00

如下操作是以“www.cloud.com”为例。

1. 在租户端WAF-资产中心-接入管理页面，选择"cloud"实例，点击“添加域名”按钮；

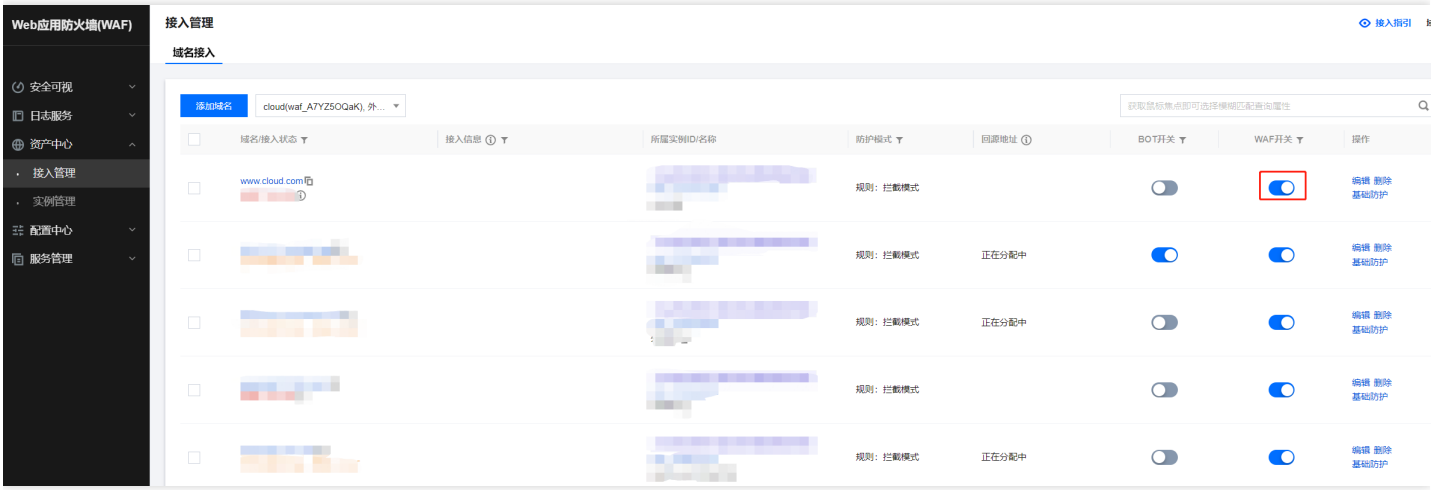


2. 在添加域名界面，选择Saas型，确认实例为预期的实例，填写实例域名，选择实际的站点端口，写入实际的源站地址，最后点击“确定”按钮；





3. 域名接入成功后，在租户端WAF-资产中心-接入管理页面，检查域名接入状态正常，检查WAF开关正常开启。



场景4：删除防护域名

最近更新时间: 2024-12-19 17:12:00

如下操作是以“www.sz.com”为例

1. 登录租户端WAF-资产中心-接入管理，找到对应域名，删除对应域名。

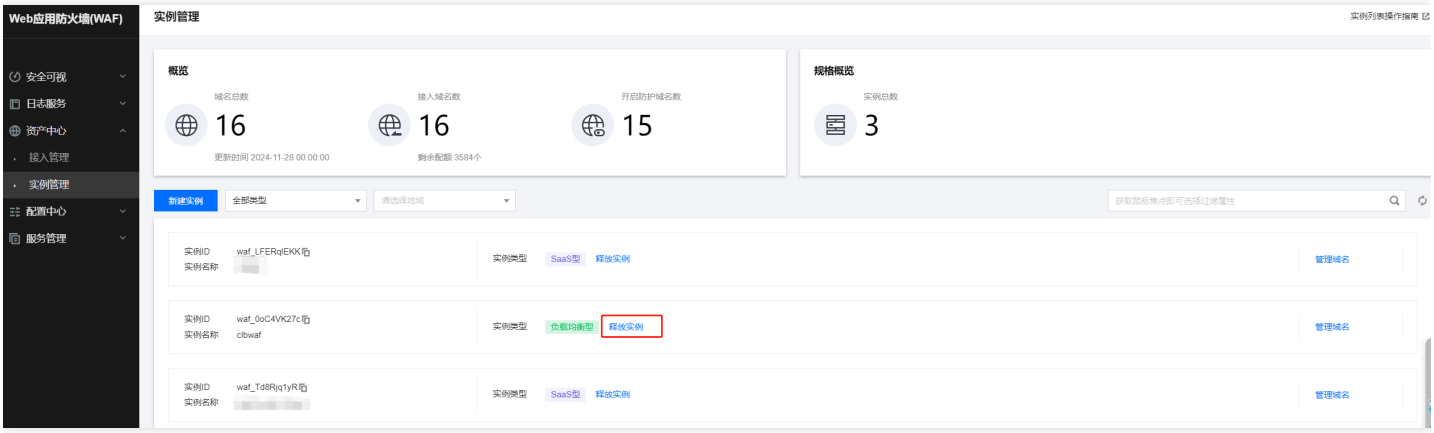


场景5：删除实例

最近更新时间: 2024-12-19 17:12:00

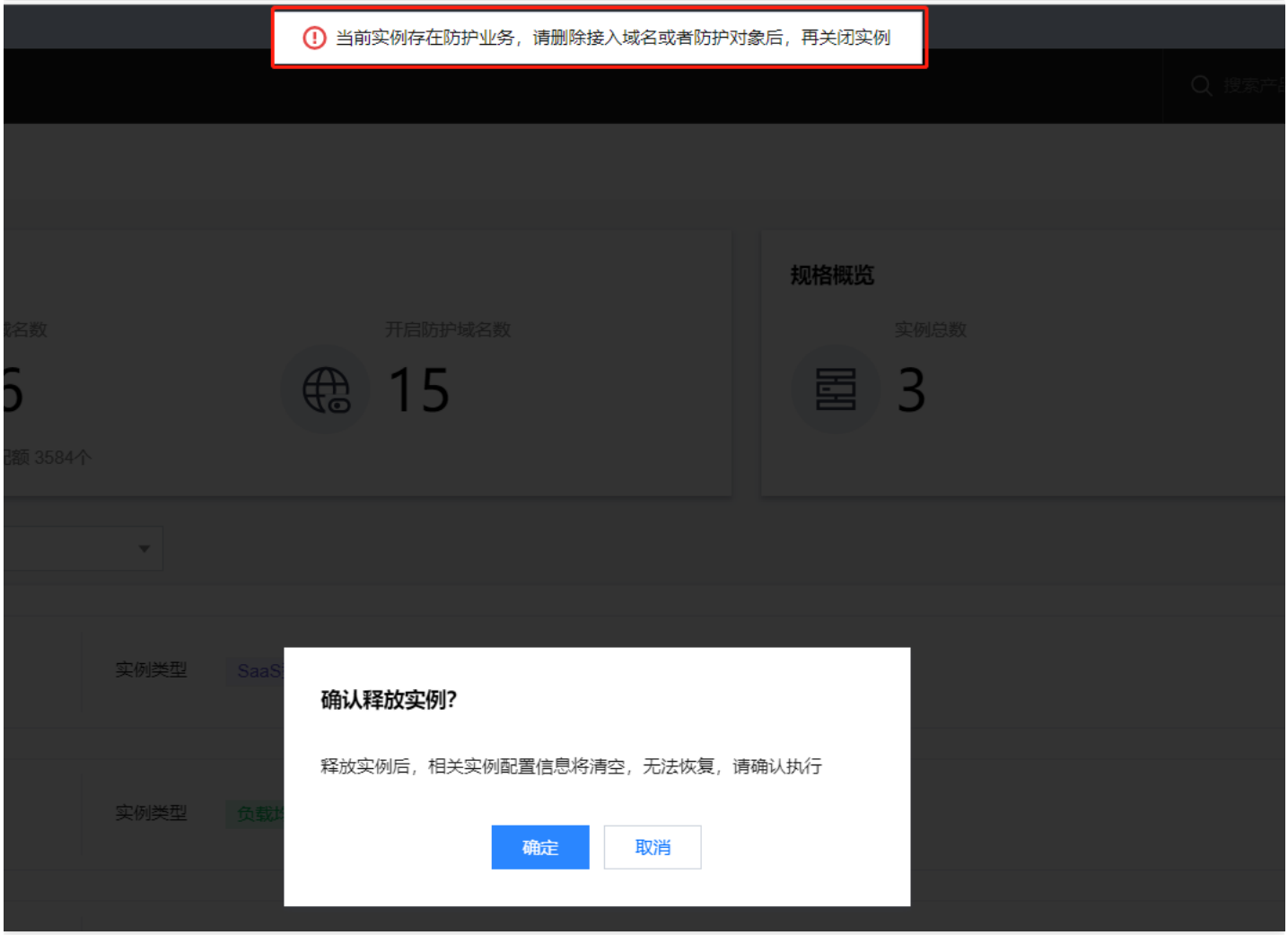
如下操作是以“clbwaf”为例，前提条件是实例内无域名：

1. 登录租户端WAF-资产中心-实例管理，找到对应实例，点击释放实例按钮，然后点击确定。





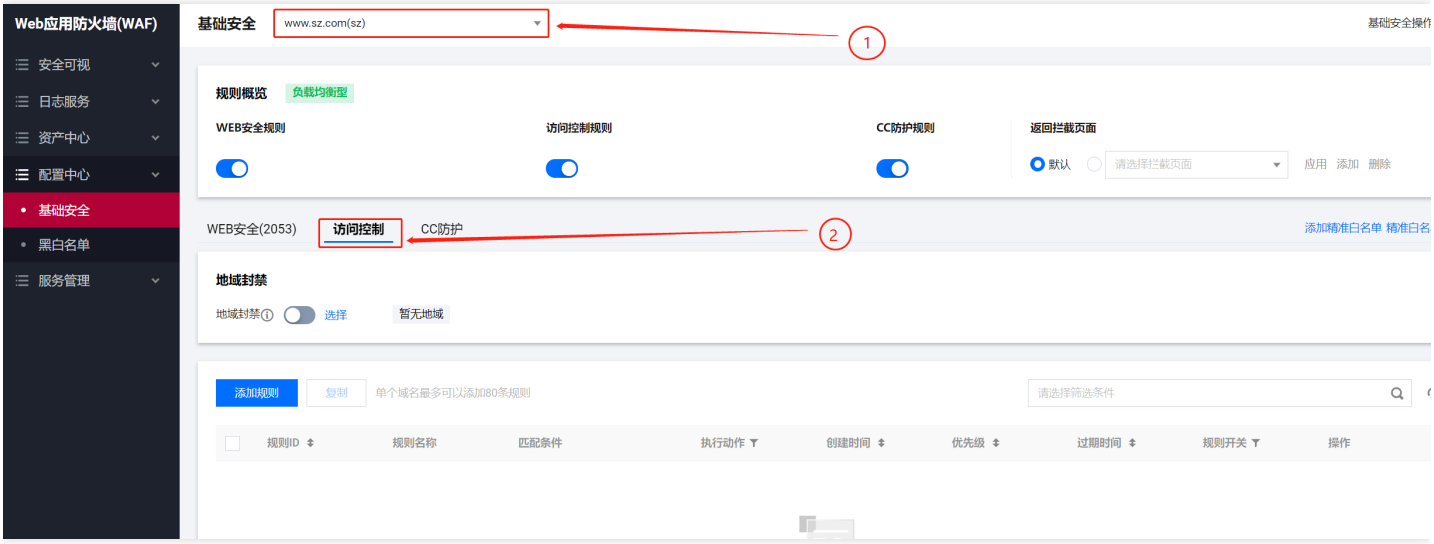
2. 如果实例中存在域名，则会释放实例失败。


当前实例存在防护业务，请删除接入域名或者防护对象后，再关闭实例
规格概览
开启防护域名数
15
实例总数
3
实例类型
确认释放实例?
释放实例后，相关实例配置信息将清空，无法恢复，请确认执行
确定
取消

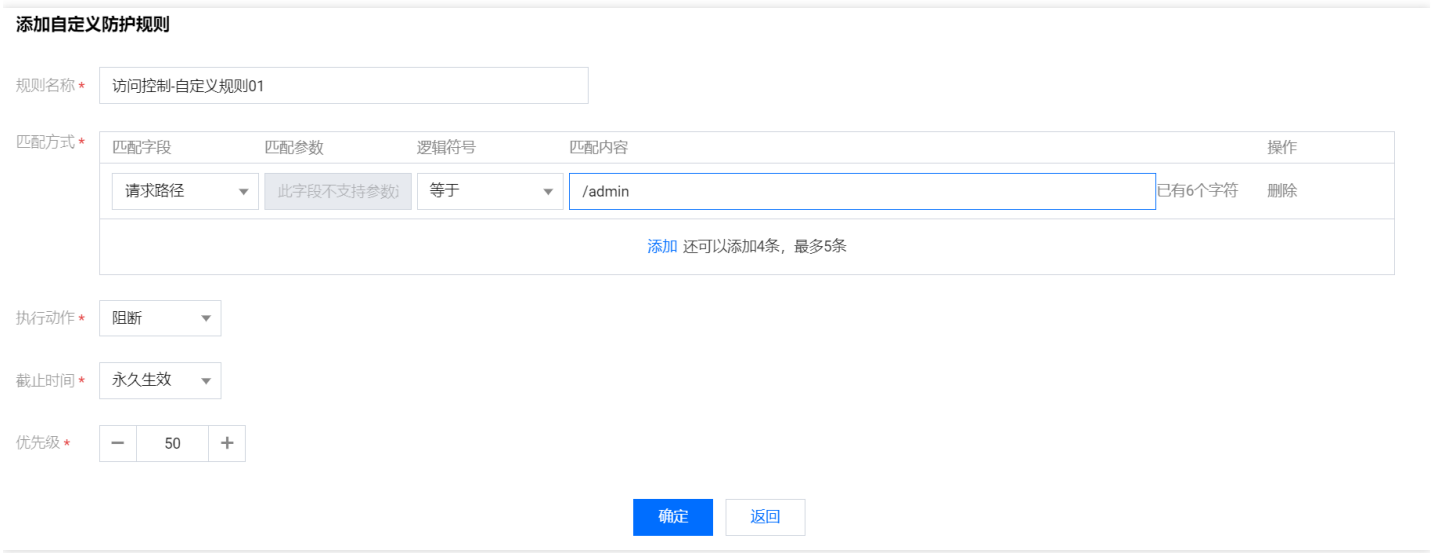
场景6：添加自定义规则

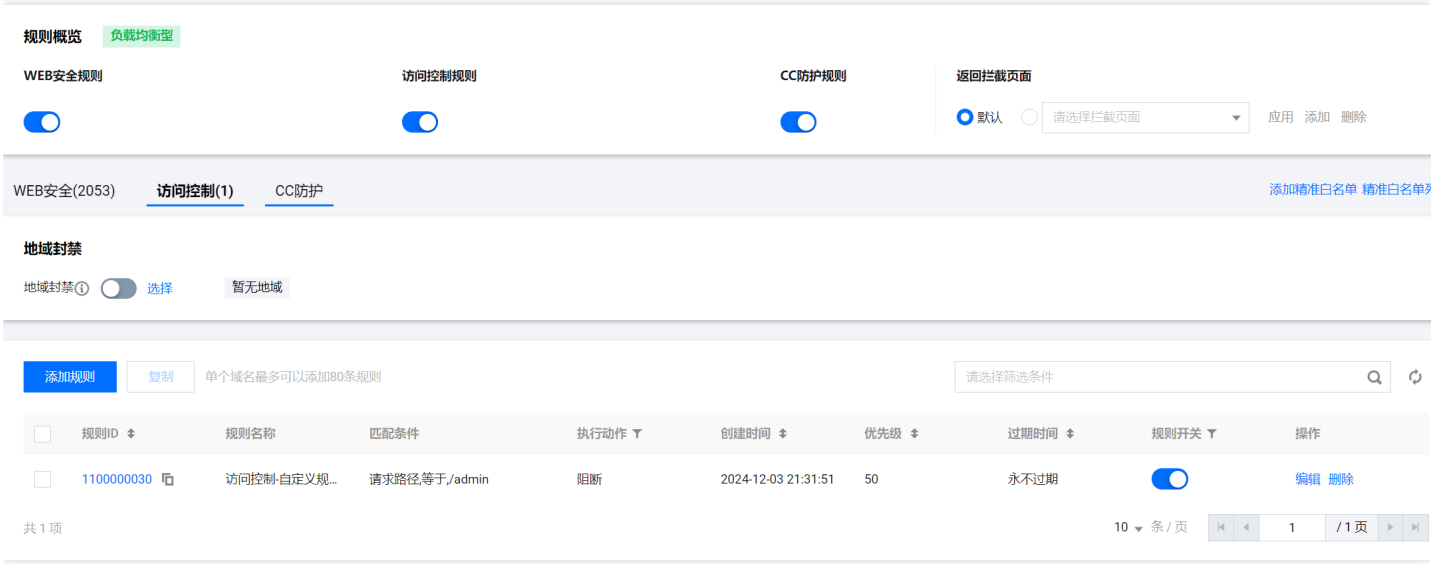
最近更新时间: 2024-12-19 17:12:00

1.登录租户端WAF控制台-基础安全界面，选择需要的域名，点击“访问控制”。



2.点击添加规则，添加一条自定义策略，匹配字段为‘请求路径’，逻辑符号选择‘包含’匹配内容为‘/admin’,执行阻断操作,最后点击确定。

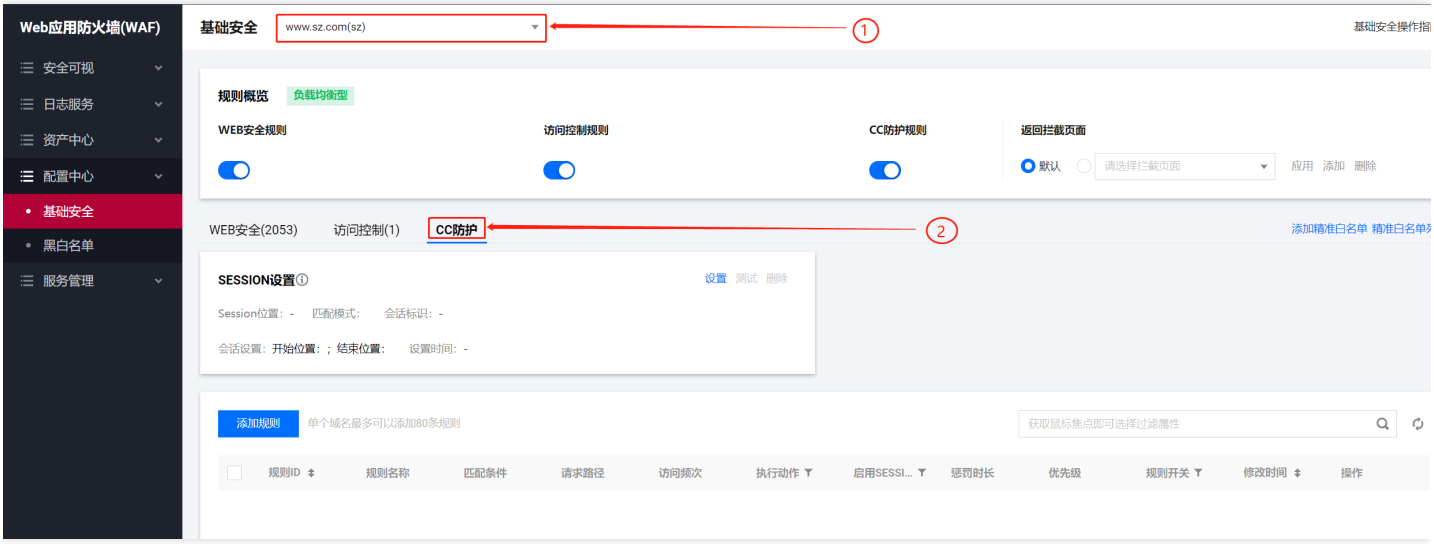



规则概览
负载均衡型
WEB安全规则
访问控制规则
CC防护规则
返回拦截页面
默认
请选择拦截页面
应用
添加
删除
WEB安全(2053)
访问控制(1)
CC防护
添加精准白名单
精准白名单列
地域封禁
地域封禁
选择
暂无地域
添加规则
复制
单个域名最多可以添加80条规则
请选择筛选条件
规则ID
规则名称
匹配条件
执行动作
创建时间
优先级
过期时间
规则开关
操作
1100000030
访问控制-自定义规...
请求路径,等于,/admin
阻断
2024-12-03 21:31:51
50
永不过期
编辑
删除
共 1 项
10
条 / 页
1
/ 1 页

场景7：添加CC防护规则

最近更新时间: 2024-12-19 17:12:00

1.登录租户端WAF控制台-基础安全界面，选择需要的域名，点击“CC防护”。



2.点击添加规则，添加一条CC防护设置，输入规则名称，URI输入为‘/test.html’,访问频次为3次/10秒，执行‘拦截’动作，惩罚时间设为2分钟,最后点击确定。

添加CC防护规则

规则名称 * CC

识别方式 * IP SESSION

匹配方式 *

匹配字段	匹配参数	逻辑符号	匹配内容	操作
URL		等于	/test.html	删除

添加 还可以添加9条，最多10条

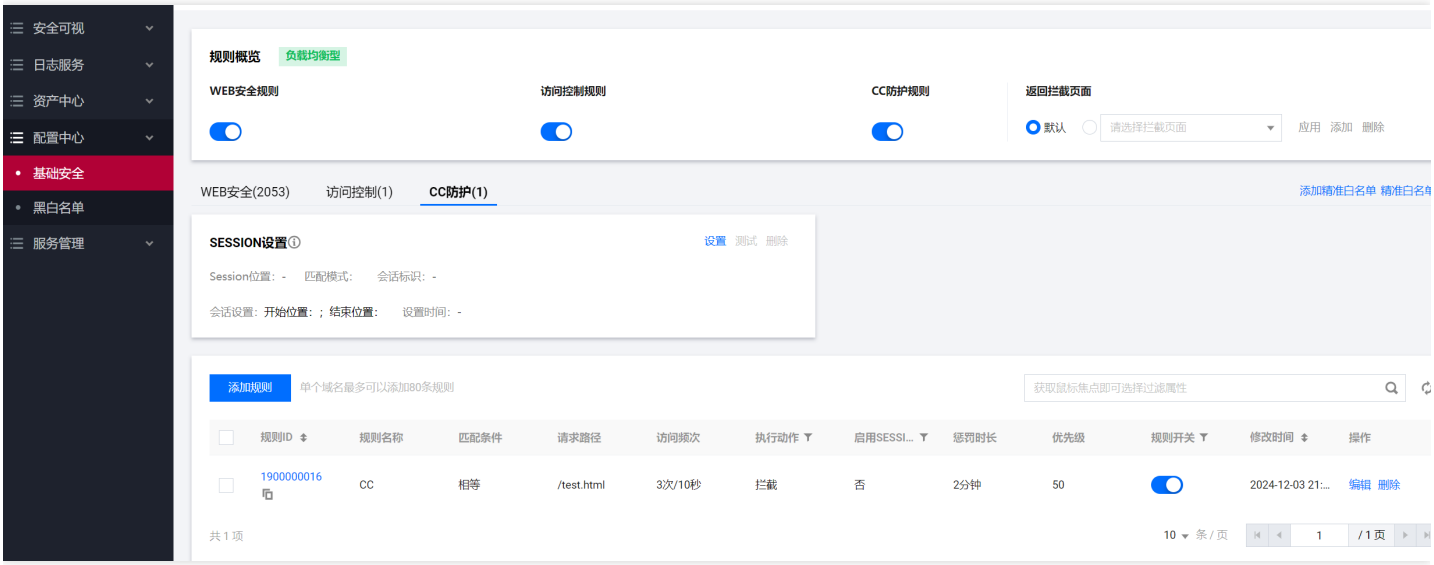
访问频次 * 3 次 10秒

执行动作 * 拦截

惩罚时长 * 2 分钟

优先级 * 50

确定 返回



场景5：检查域名是否处于被防护状态

最近更新时间: 2024-12-19 17:12:00

租户端域名是否开启防护的巡检方案

操作人：租户端运维人员

步骤一：查看WAF配置防护的域名数量和具体域名

登录租户端WAF-资产中心-接入管理界面，查看WAF防护域名的数量和具体域名。



步骤二：查看域名防护状态，如下4种场景域名防护状态为关闭状态

监听器为空白或者"defalut"

登录租户端WAF-资产中心-接入管理界面查看域名接入信息，如果接入信息为空白或者default,即域名防护不正常；





域名防护开关为“关闭”

登录租户端WAF-资产中心-接入管理界面查看WAF开关，如果WAF开关为“灰色”，则流量不会转给WAF，既域名防护不生效；

备注：WAF开关 开启为 “蓝色”；WAF开关关闭为“灰色”。



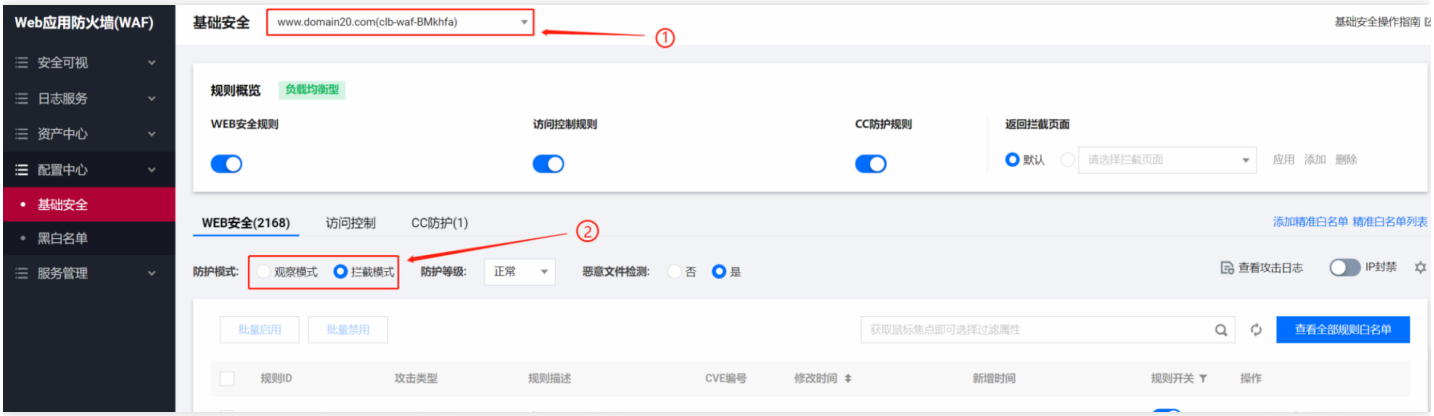
域名流量模式为“镜像模式”

登录租户端WAF-资产中心-接入管理界面查看域名使用模式，如果是镜像模式，只记录攻击日志不拦截，即域名防护拦截不生效；



域名规则模式为“观察模式”

登录租户端WAF-配置中心-基础安全界面，选择域名，查看域名防护模式，如果是观察模式，则域名规则拦截功能不生效。



场景6：应急预案

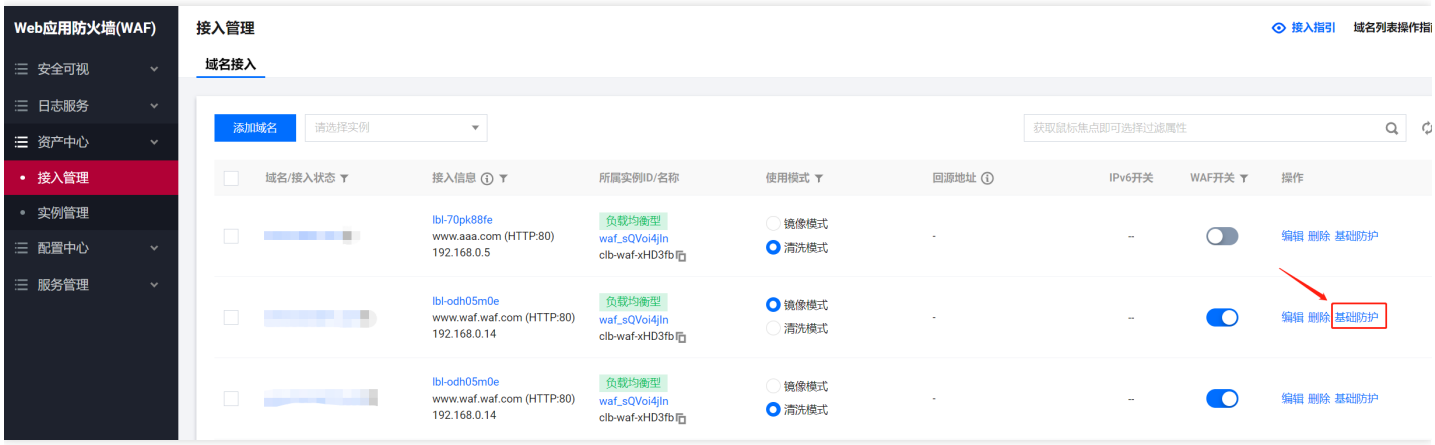
最近更新时间: 2024-12-19 17:12:00

防护域名出现误拦截客户业务应急预案

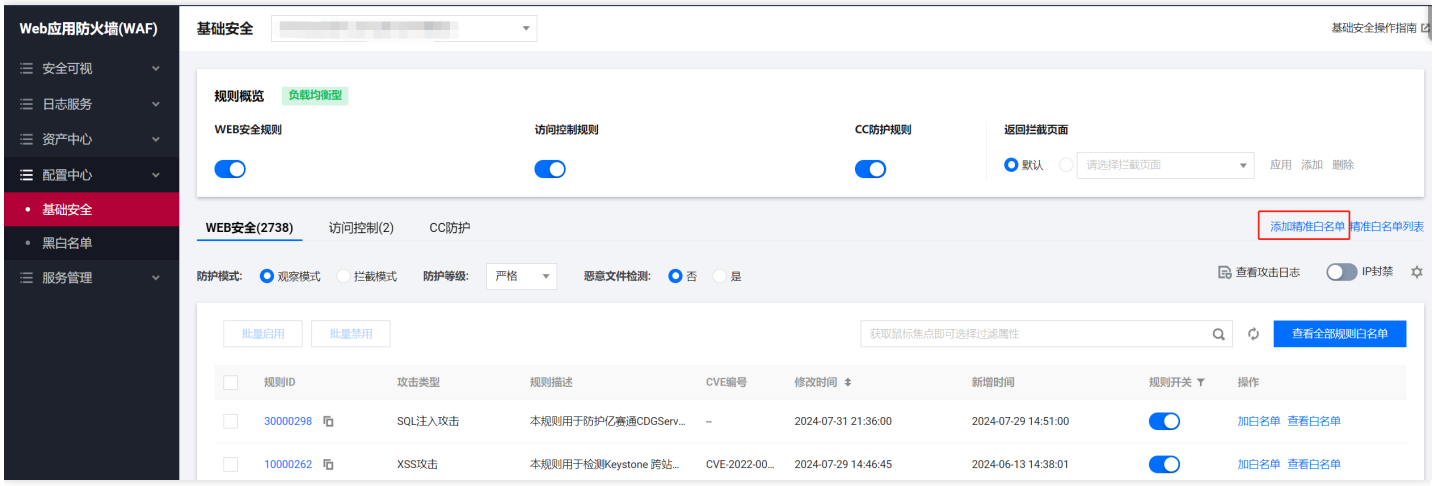
防护域名接入waf后，部分url出现正常访问被拦截情况，按照业务的影响面评估，推荐依次使用手动三 -> 手动二 -> 手动一；

应急手段一：添加白名单(特定白名单放行，其他访问命中规则则拦截)

在控制台页面上添加放行的规则；



选择 "精准白名单"



根据告警的路径配置规则；



如果上述配置后不符合预期，则执行手段二；

应急手段二：将流量模式改为镜像模式(只告警不拦截)

在控制台页面上将waf工作模式改为镜像模式。

点击-接入管理-配置镜像模式；



如果配置后仍然不符合预期，执行手段三。

应急手段三：关闭域名的防护能力(不告警也不拦截)

在控制台页面上关闭waf开关,此时整个域名不拦截任何攻击；



最佳实践
搭建负载均衡型WAF测试环境

最近更新时间: 2024-12-19 17:12:00

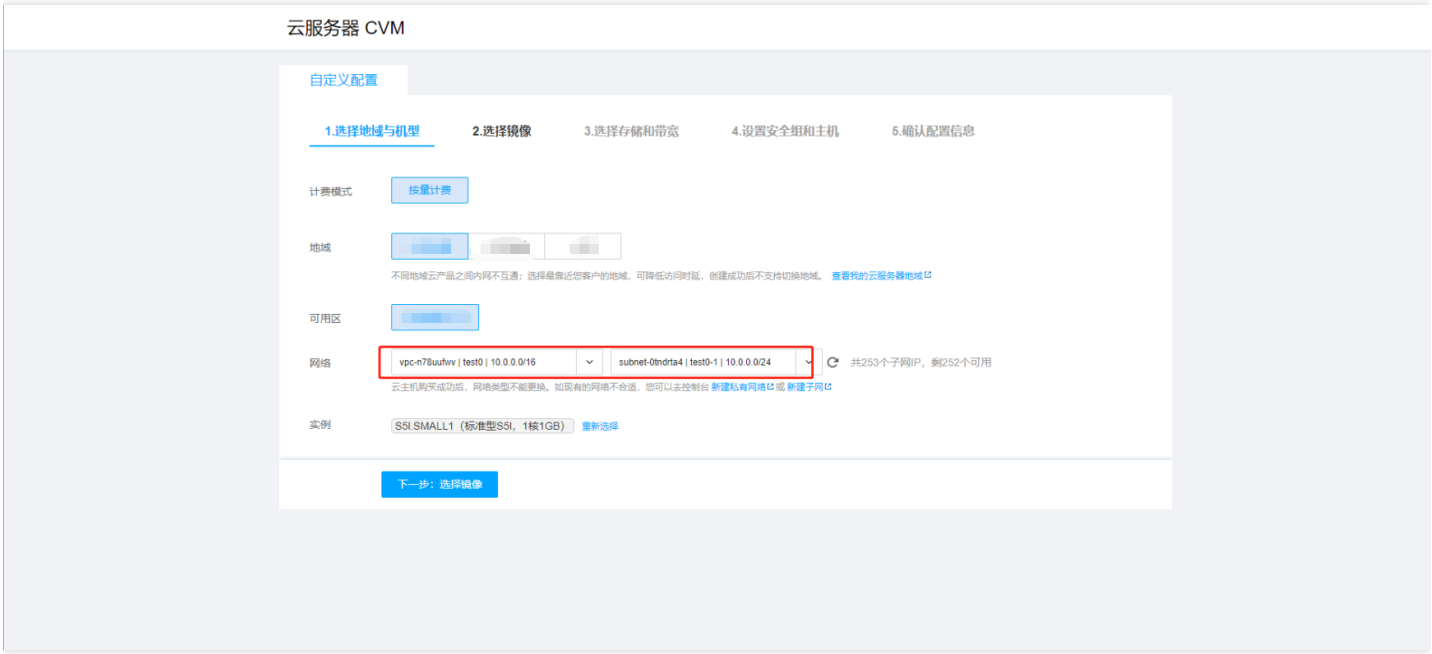
搭建负载均衡型WAF测试环境

购买cvm

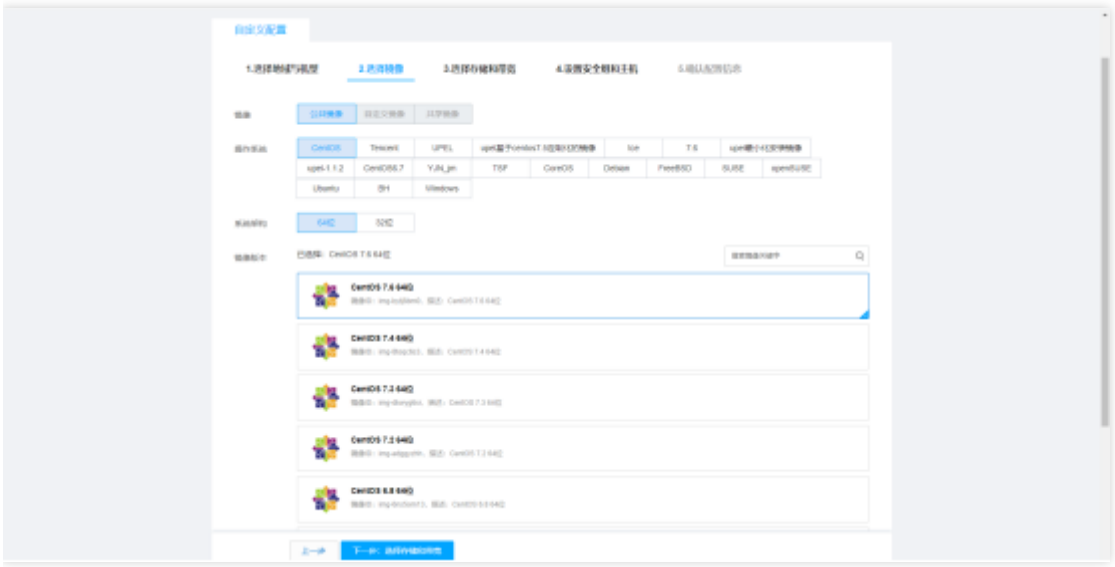
1. 登录租户端，进入到CVM页面，选择对应的地域，点击【新建】；



2. 所选网络需要与CLB网络一致，其余选项按照实际情况选择，点击【下一步：选择镜像】；



3. 按照实际情况选择镜像后，点击【下一步：选择存储和带宽】；



4. 按照实际情况选择存储和带宽后，点击【下一步：设置安全组和主机】；



5. 按照实际情况选择安全组合主机后，输入主机密码，点击【下一步：确认配置信息】；





6. 查看到刚才所选的信息，确认无误后，点击【开通】；



申请弹性公网ip地址，绑定CVM

1. CVM菜单下，点击【弹性公网IP】，选择与CVM相同的地域后，点击【申请】，按照实际情况选择各项；



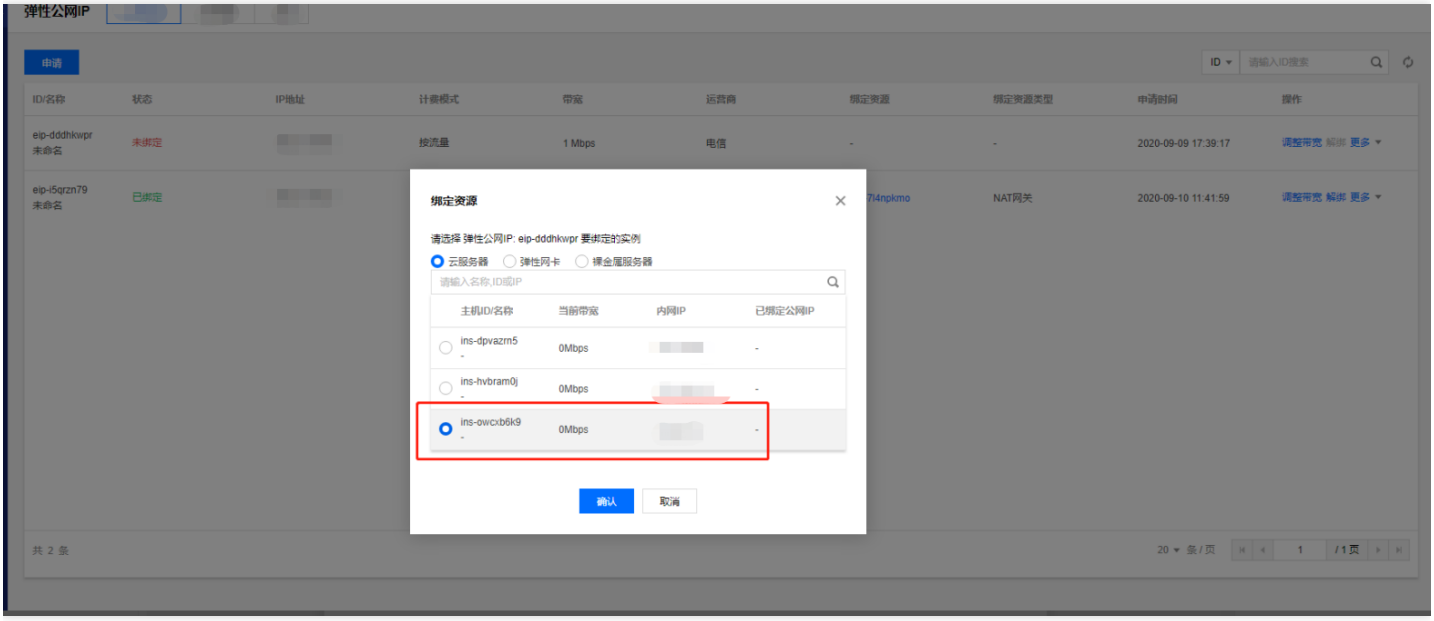
2. 点击【确认】，返回到弹性公网IP列表页面，可以查看到新建的弹性公网IP显示未绑定状态；



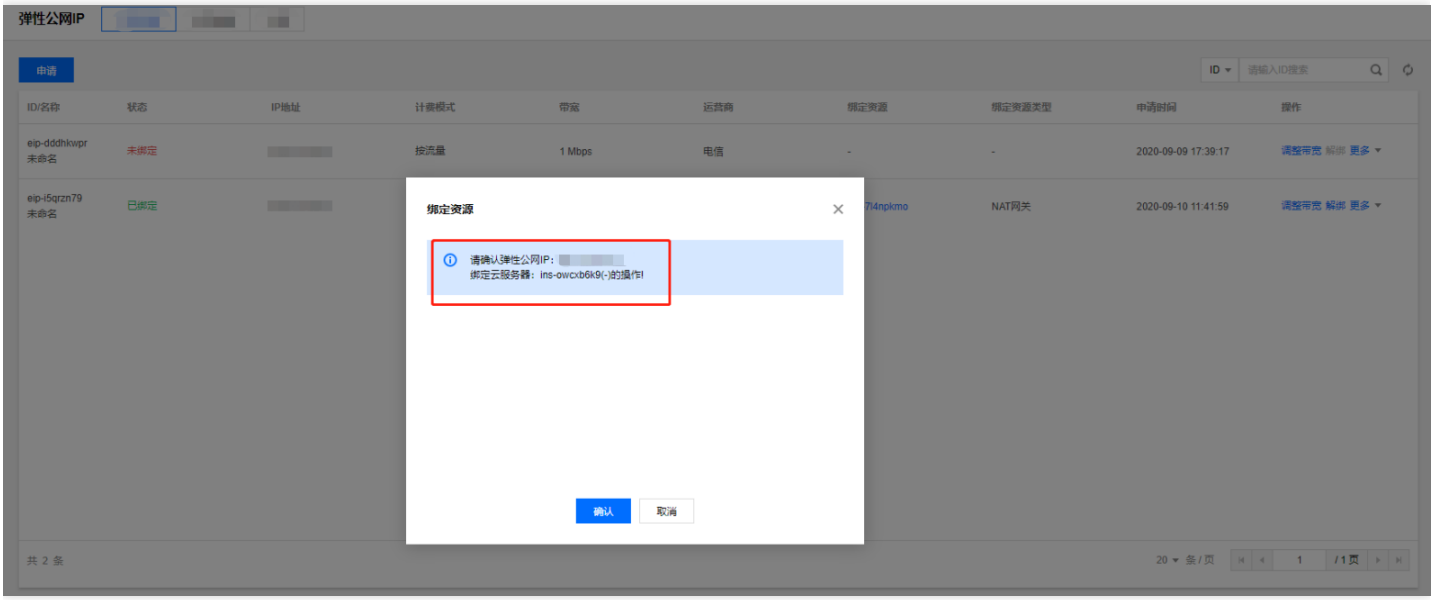
3. 点击弹性公网IP的"操作"栏，点击【更多】，选择【绑定】；



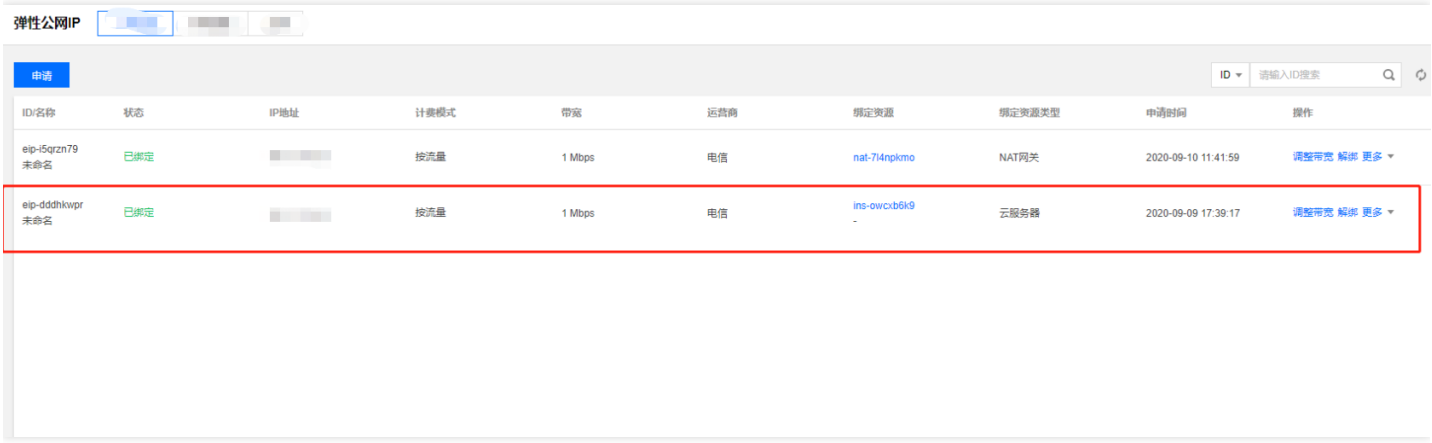
4. 选择要绑定的CVM，点击【确认】；



5. 查看需要确认的信息，确认无误后点击【确认】；

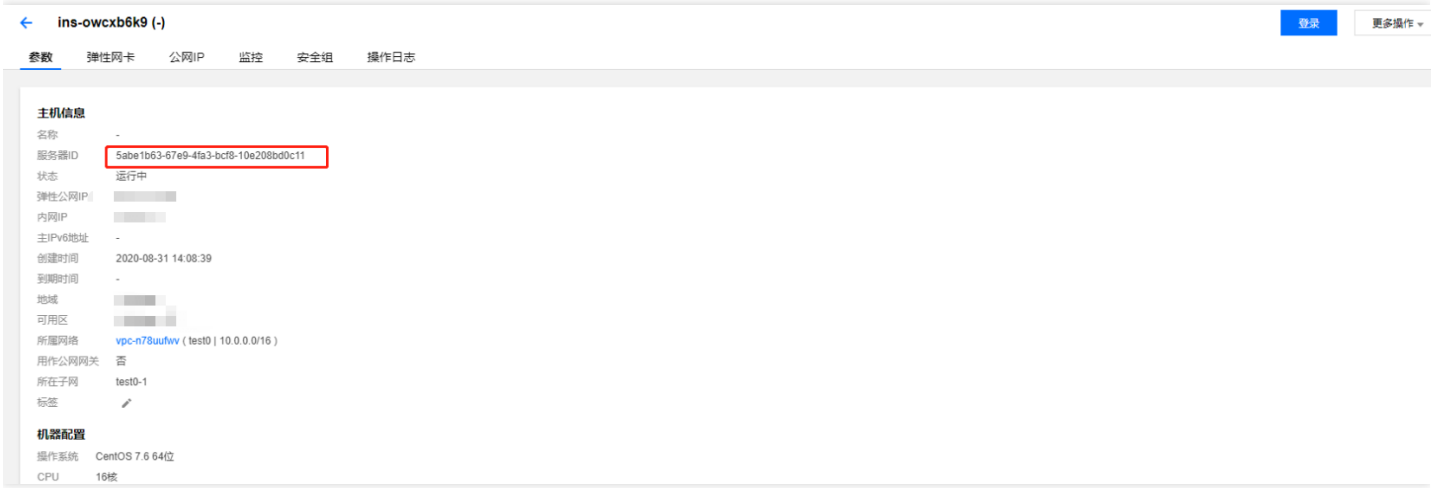


6. 返回到弹性公网IP列表页面，显示“已绑定”状态；

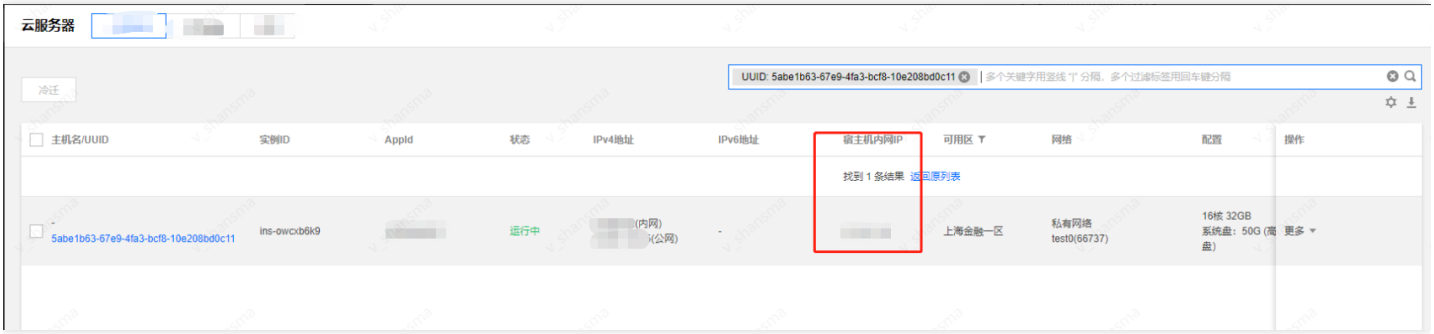


安装nginx，启用80端口

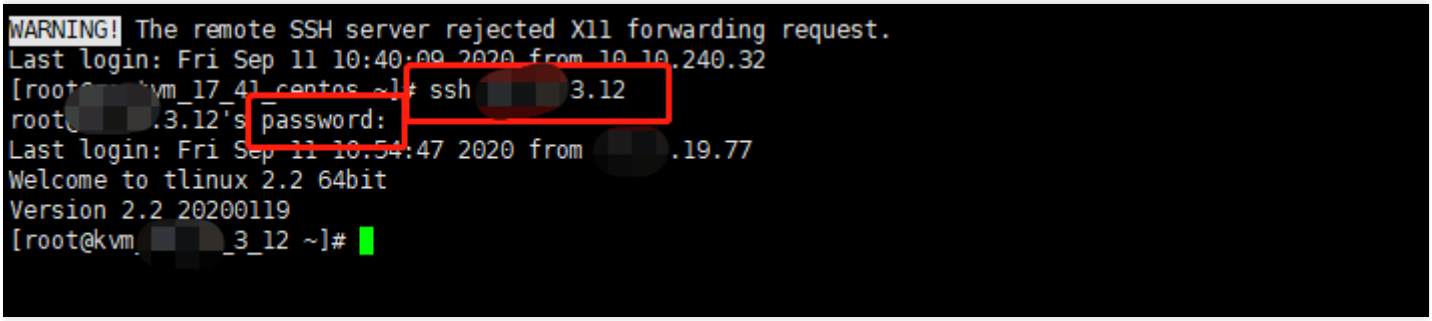
1. 点击CVM的ID，进入到CVM参数页面，复制CVM的服务器ID；



2. 在运营端中CVM-云主机（租户资源）下，搜索框中选择UUID，粘贴刚才复制的服务器ID，可以查询到宿主机内网IP；

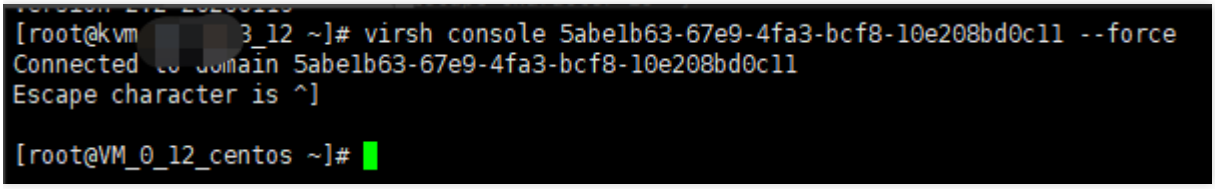


3. 登录到宿主机内网IP，输入命令：ssh 宿主机内网IP，密码为开通CVM时填入的密码；





4. 输入命令 `virsh console UUID --force` ，如virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force，进入到CVM中；

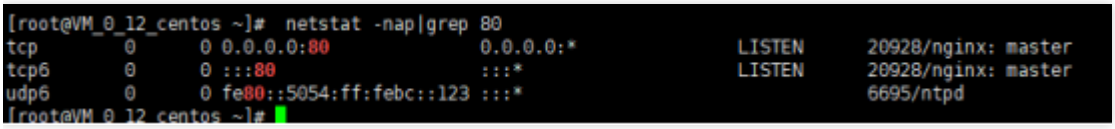


5. 进入后输入以下命令进行安装；

安装： `yum install -y nginx`

启动Nginx服务： `service nginx start`

查看80端口是否启用： `netstat -nap|grep 80`

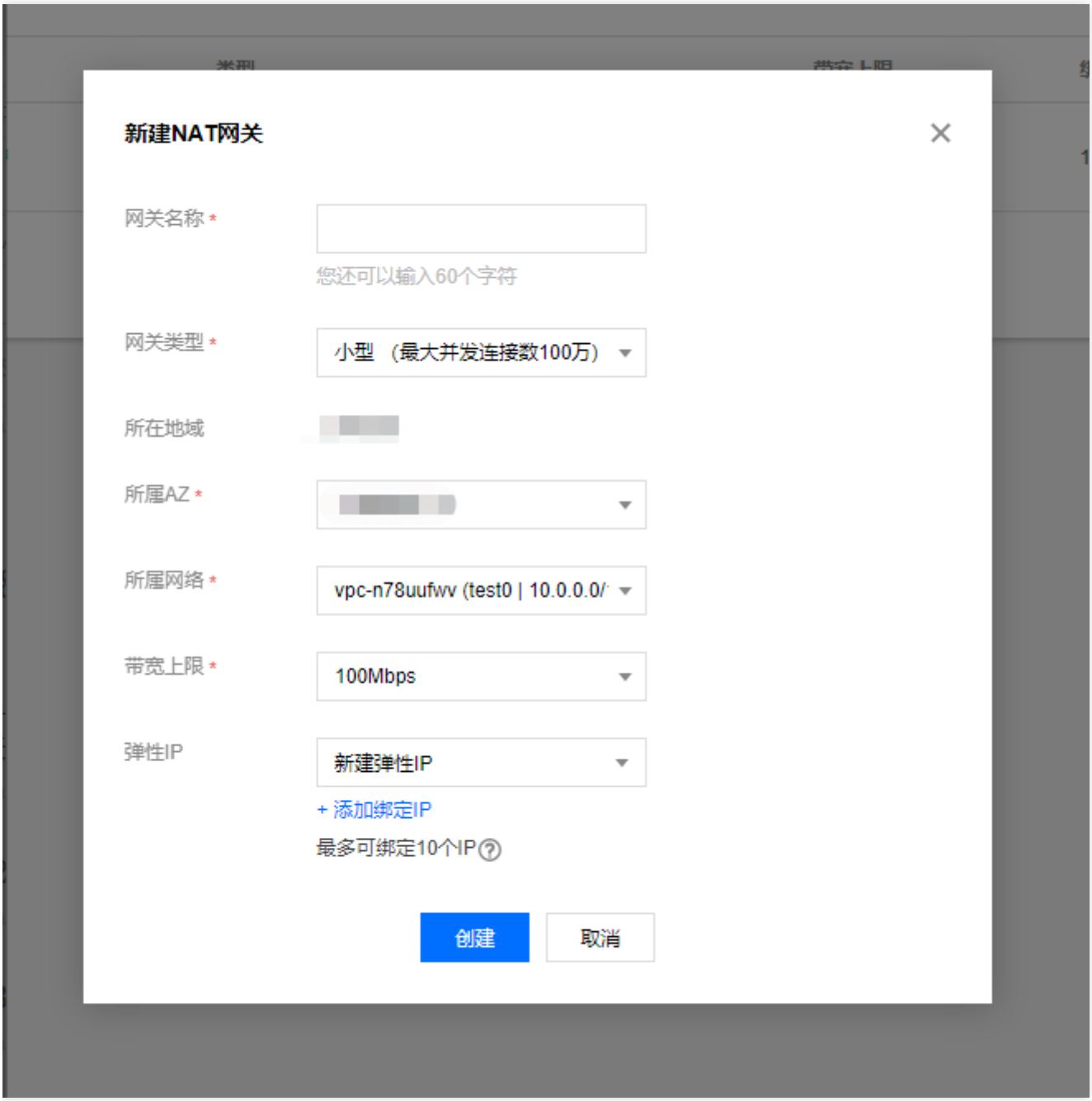


由于有些客户公网ip地址禁止对外开放端口80和443，需要通过natgw把cvm的80端口转到其他端口，例如788，并在路由表中关联此网关（如不涉及此项请忽略）；

1. 私有网络菜单下选择NAT网关，选择对应的地域后，点击【新建】，新建NAT网关；



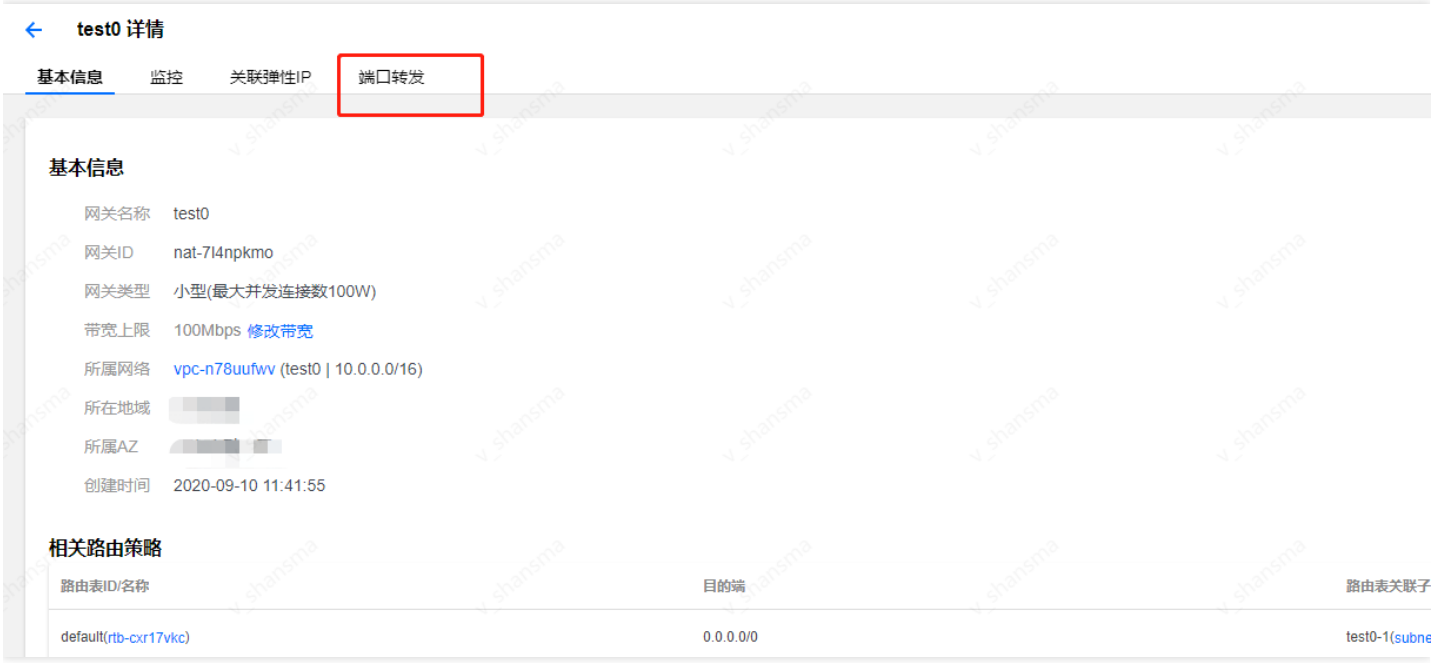
2. 按照实际情况输入各项，点击【创建】，返回到NAT网关列表页面；



3. 在新建的NAT网关中点击网关ID；



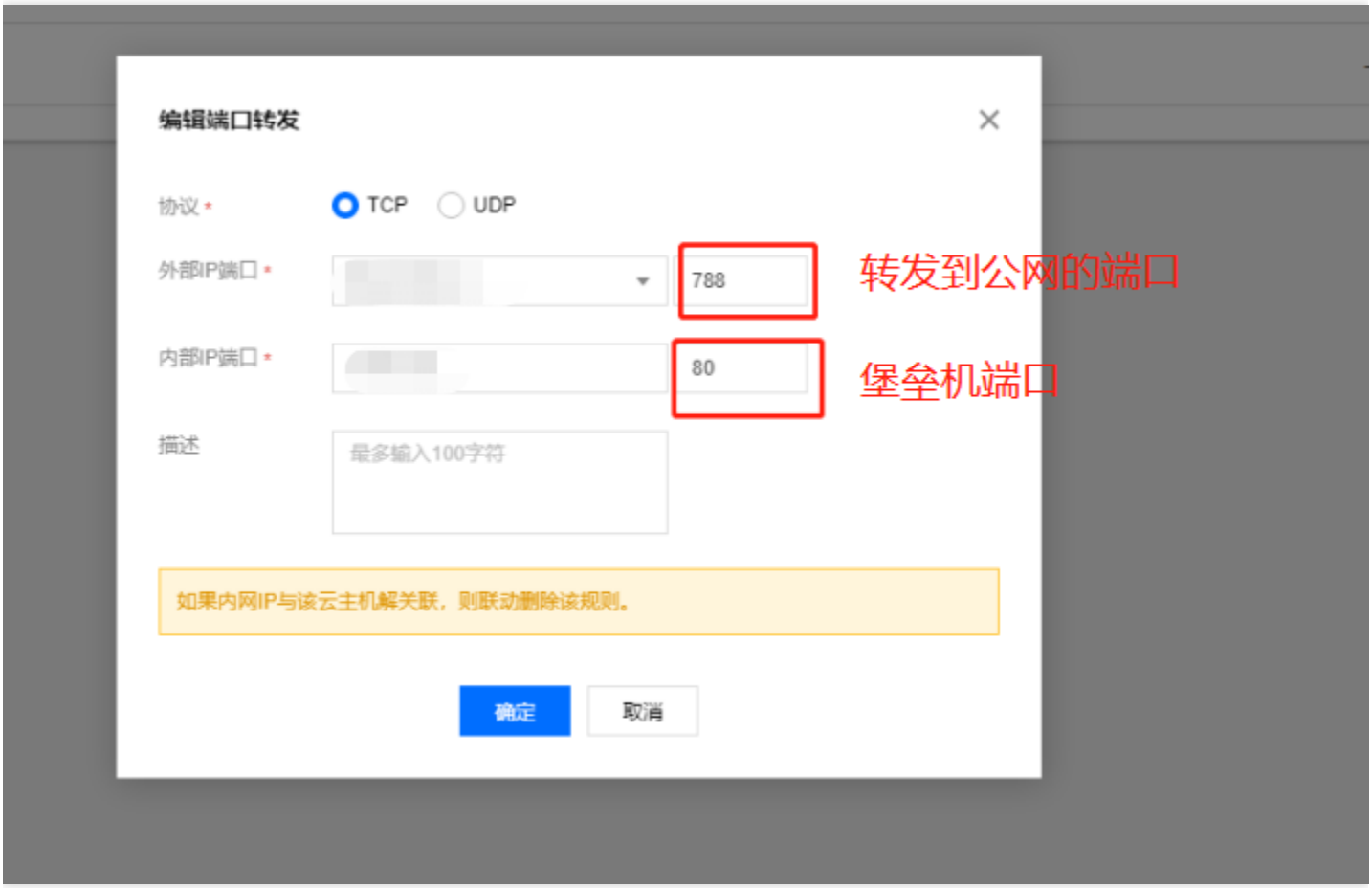
4. 点击端口转发；



5. 点击【新建】；



6. 添加转发端口；



7. 在私有网络下，选择路由表，在相应的地域下，点击【新建】，新建路由表；

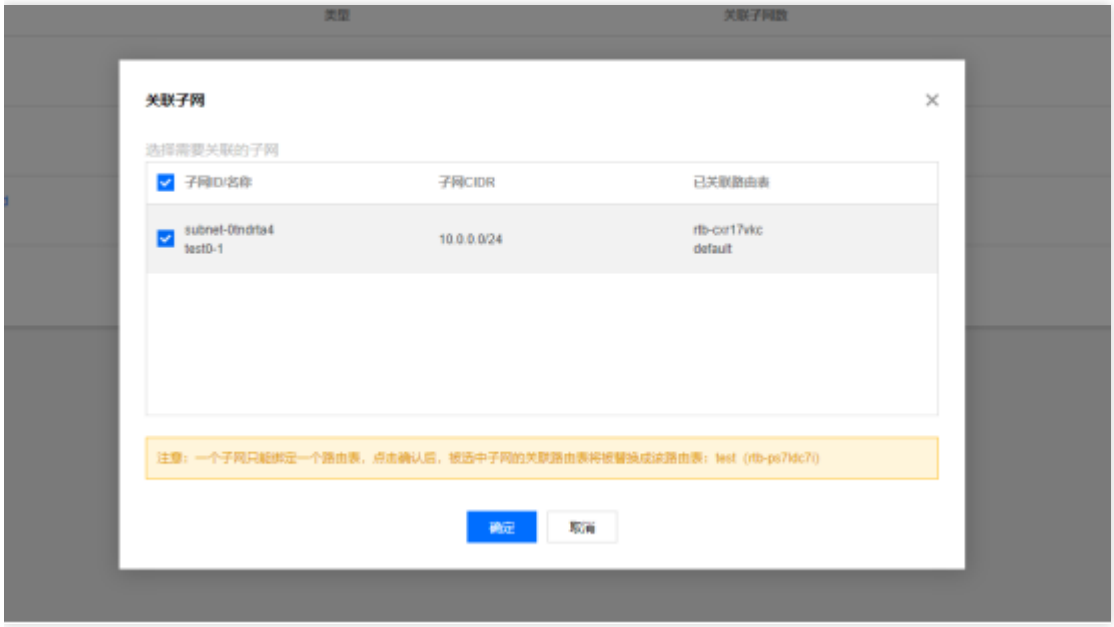




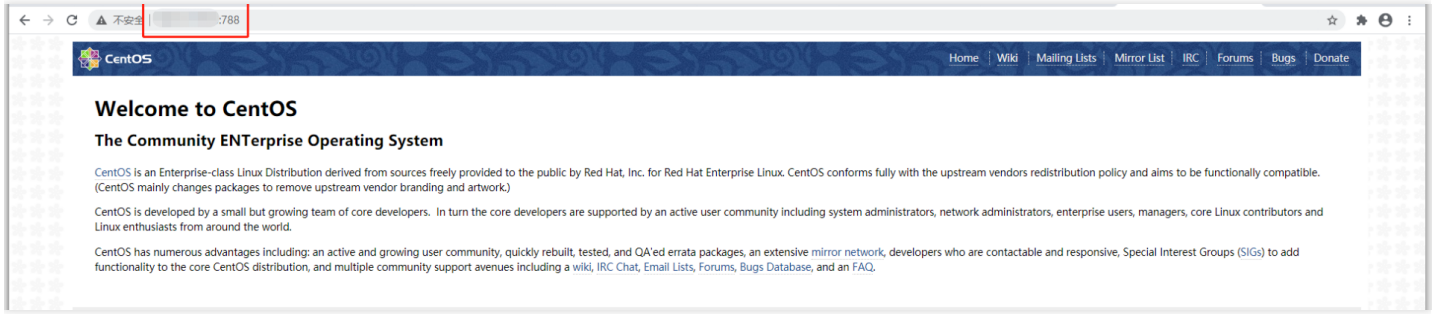
8. 输入各项后点击【创建】，策略选择已经添加的NAT网关；



9. 提示需要关联子网，选择关联的子网后，点击【确定】，返回到路由表列表页面；



访问http://公网ip:788/ 验证web网站是否正常

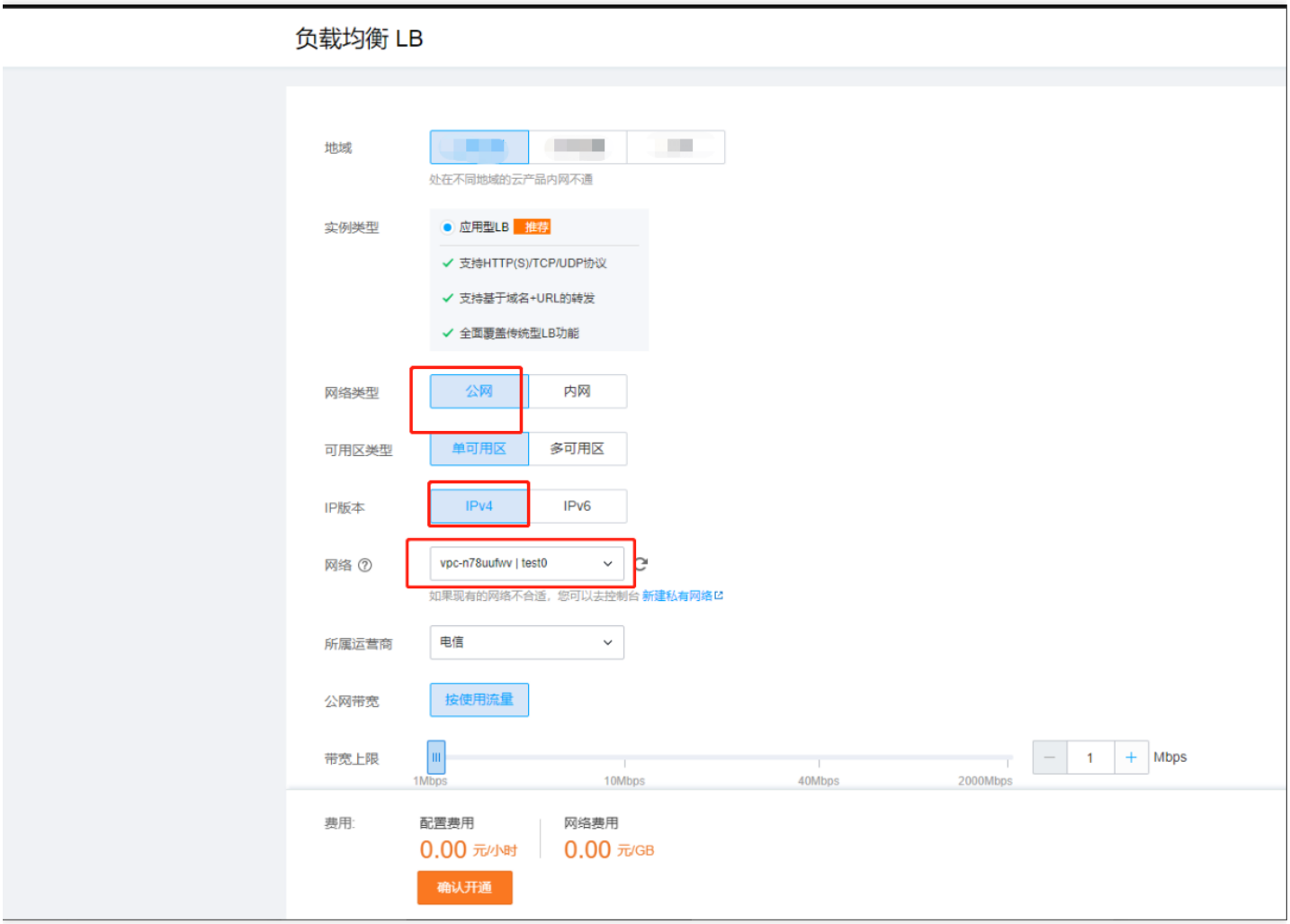


新增CLB实例及监听器；

1. 点击【负载均衡】，在LB实例列表页点击【新建】；



2. 按照实际情况输入各项，负载均衡需要与CVM网络一致。点击【确认开通】；



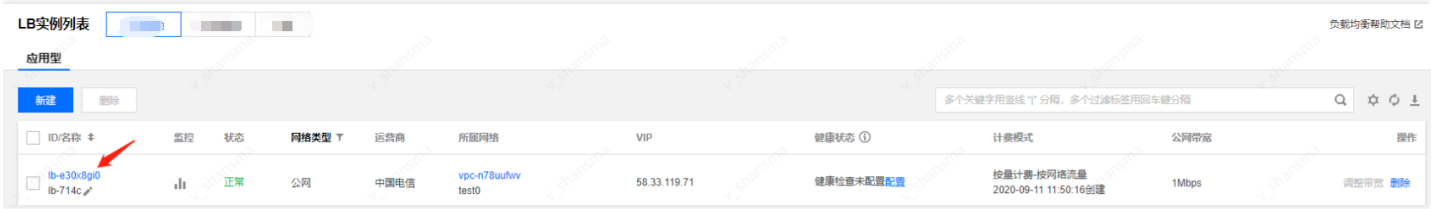
3. 在确认购买提示页点击【确认】；



4. 点击【完成】；



5. 在LB实例列表页可以查看到刚购买的实例，点击实例ID；



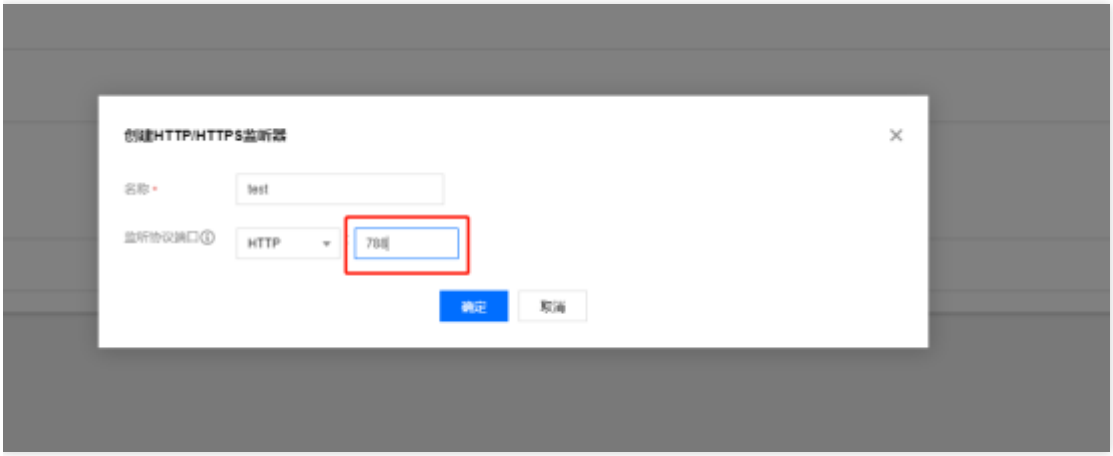
6. 点击监听器管理；



7. 点击【新建】或者【开始创建】，创建监听器；

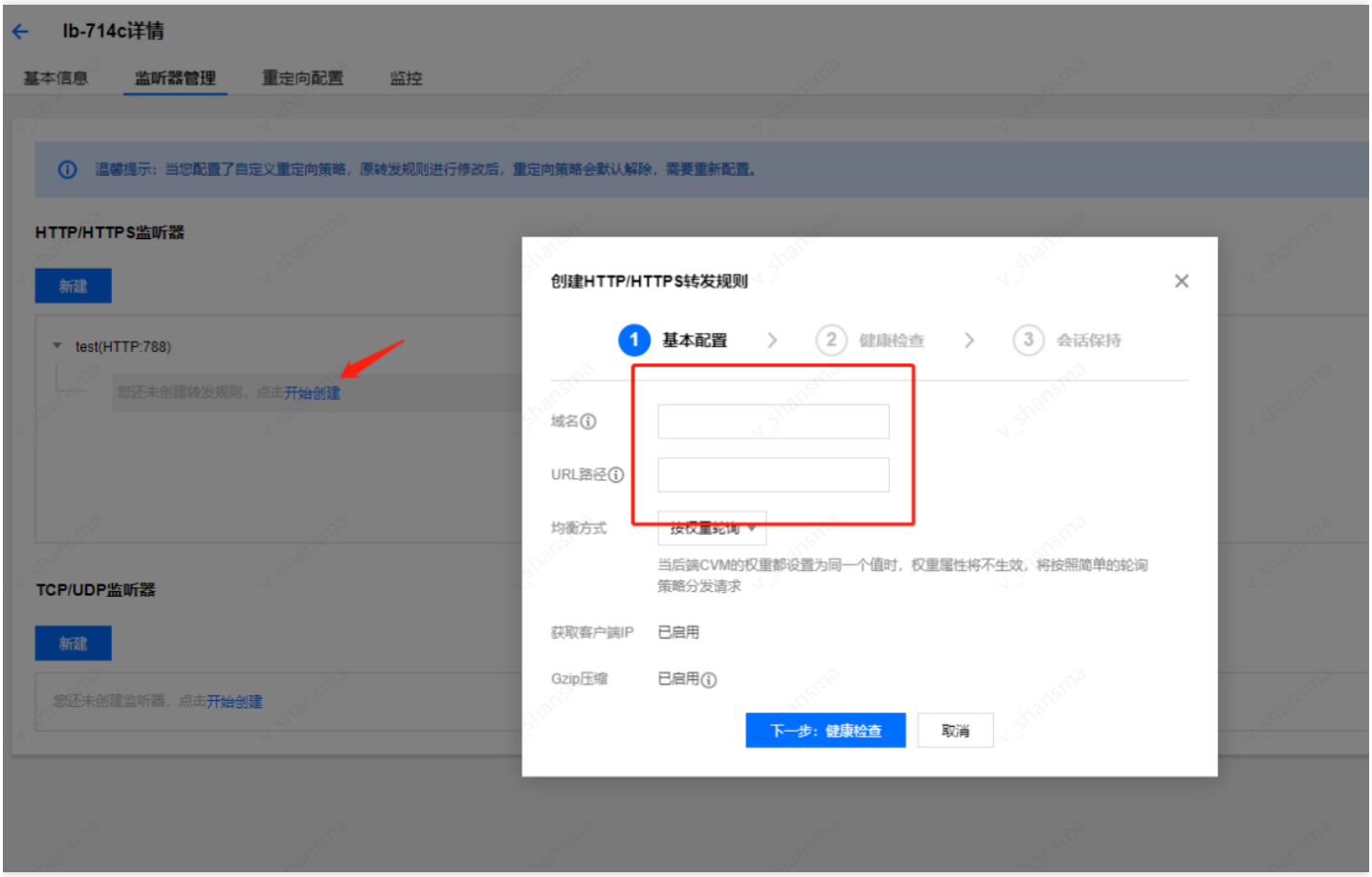


8. 输入名称、协议和端口号，端口号输入NAT网关转发的端口号，如788，点击【确定】；



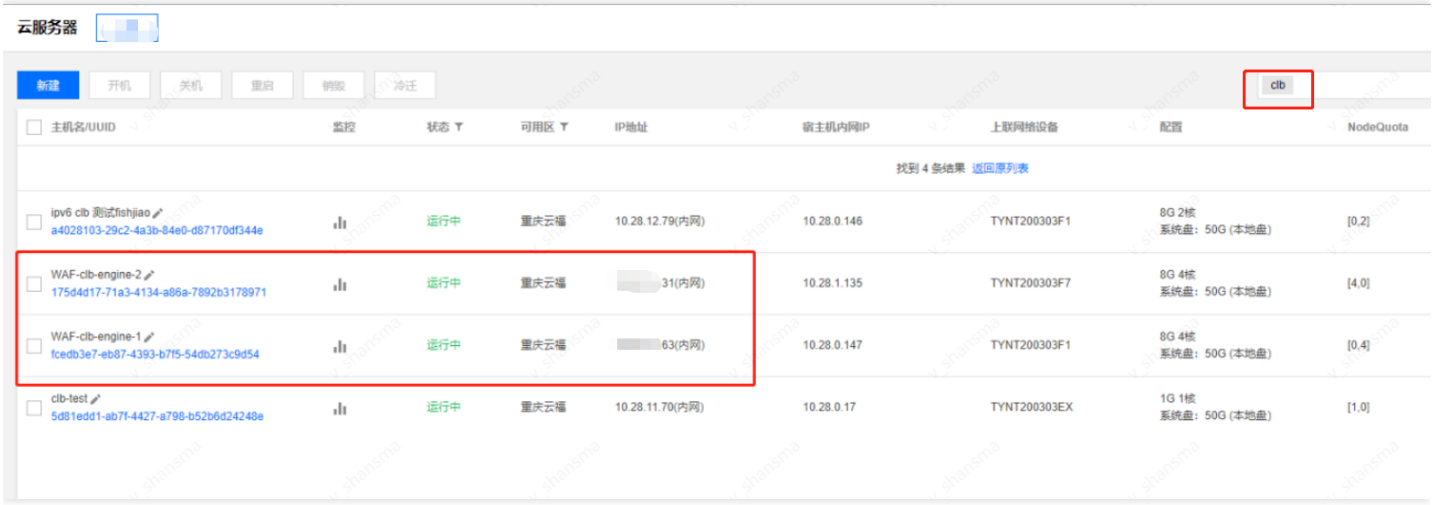
9. 点击监听器下的"开始创建"，输入要配置的域名，后续步骤参照"功能测试用例（负载均衡型）租户端"文档中"在负载均衡实例中绑定HTTP类型监听器"步骤操作即可；


lb-714c详情
基本信息
监听器管理
重定向配置
监控
温馨提示：当您配置了自定义重定向策略，原转发规则进行修改后，重定向策略会默认解除，需要重新配置。
HTTP/HTTPS监听器
新建
test(HTTP:788)
您还未创建转发规则，点击开始创建
监听器详情
名称 test
ID lbl-qgw9pkui
协议端口 HTTP:788
创建时间 2020-09-11 11:52:23
TCP/UDP监听器
新建
您还未创建监听器，点击开始创建

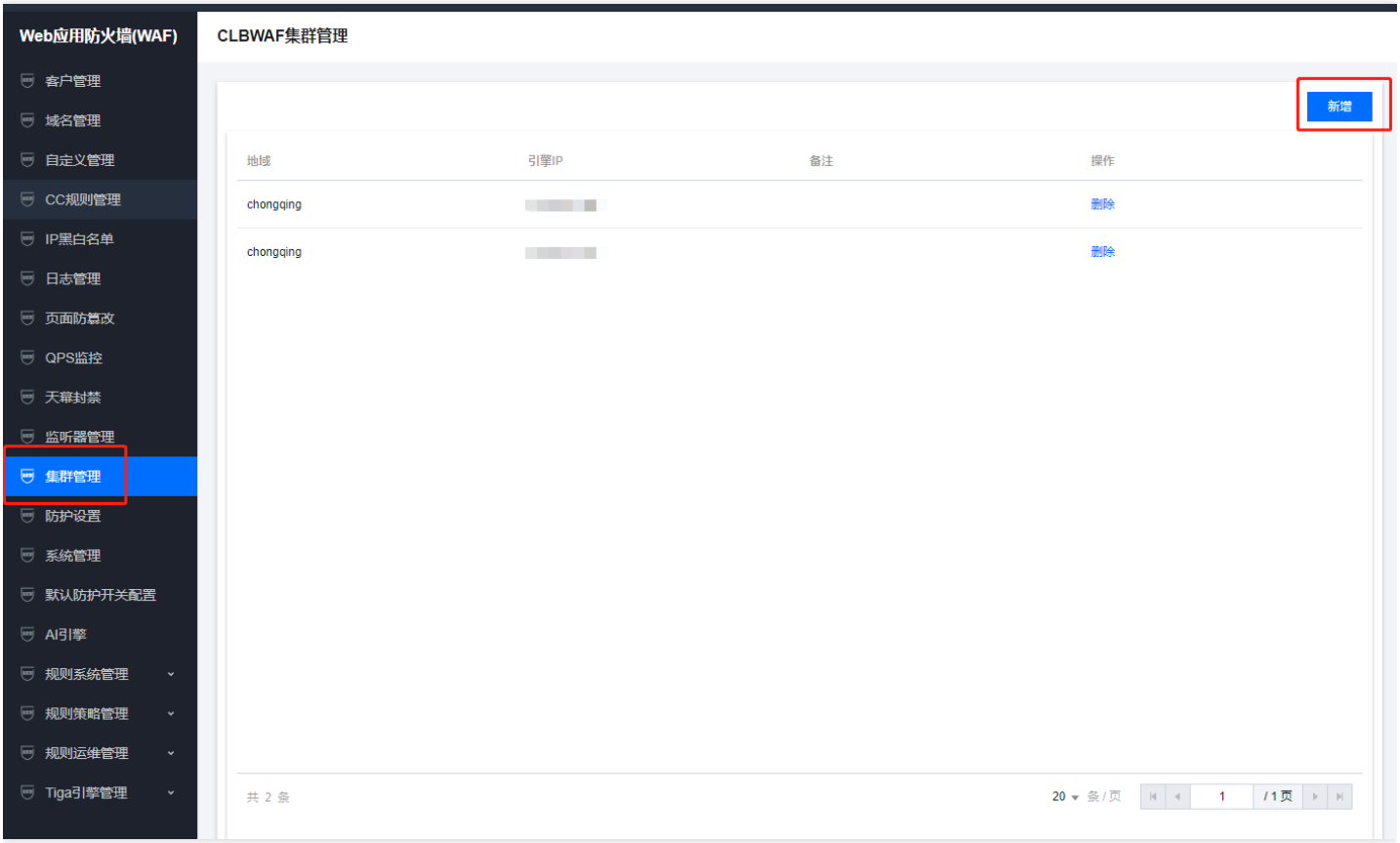


添加负载均衡型WAF的引擎节点：

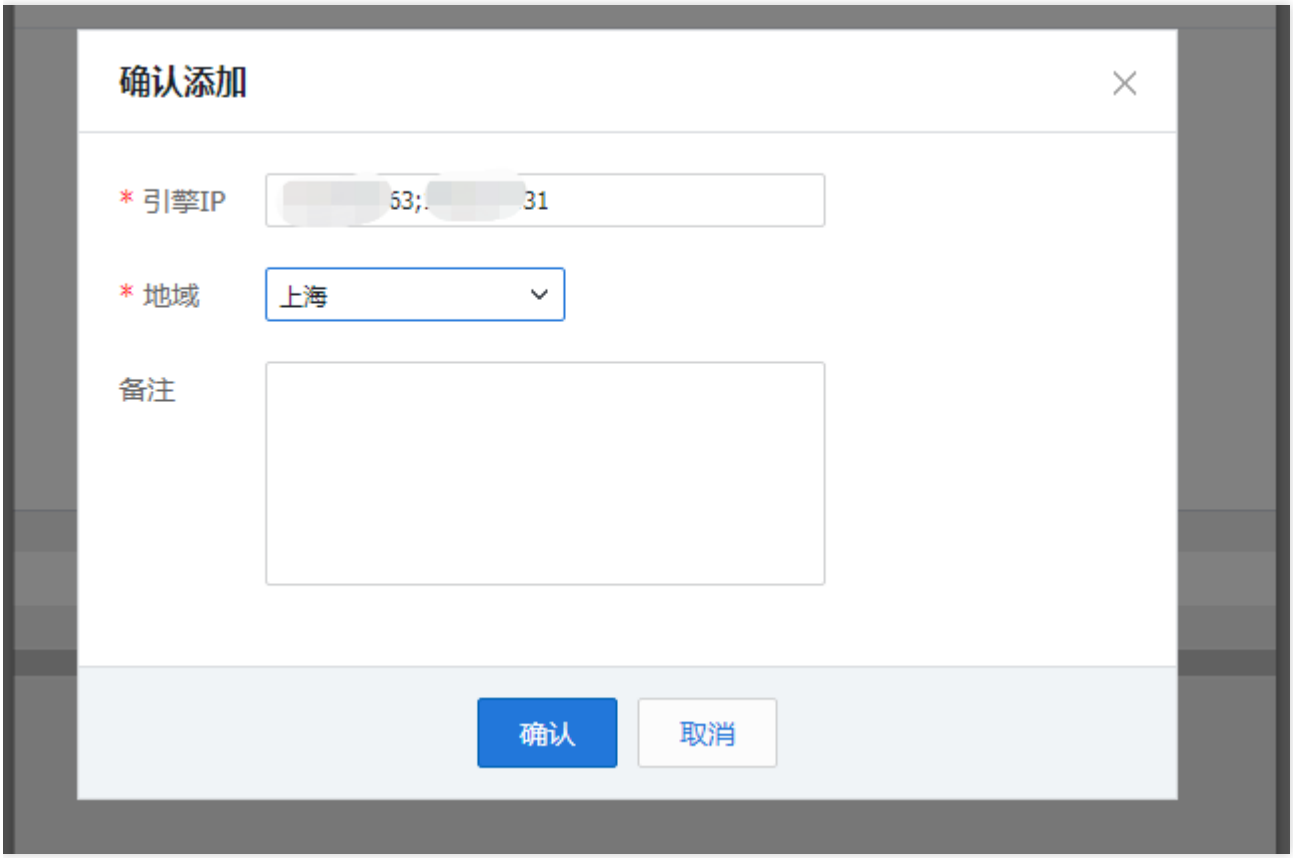
1. 登录运营端，云服务器中的虚拟机管理-运营端资源，找环境管理员申请后，分配引擎节点IP；



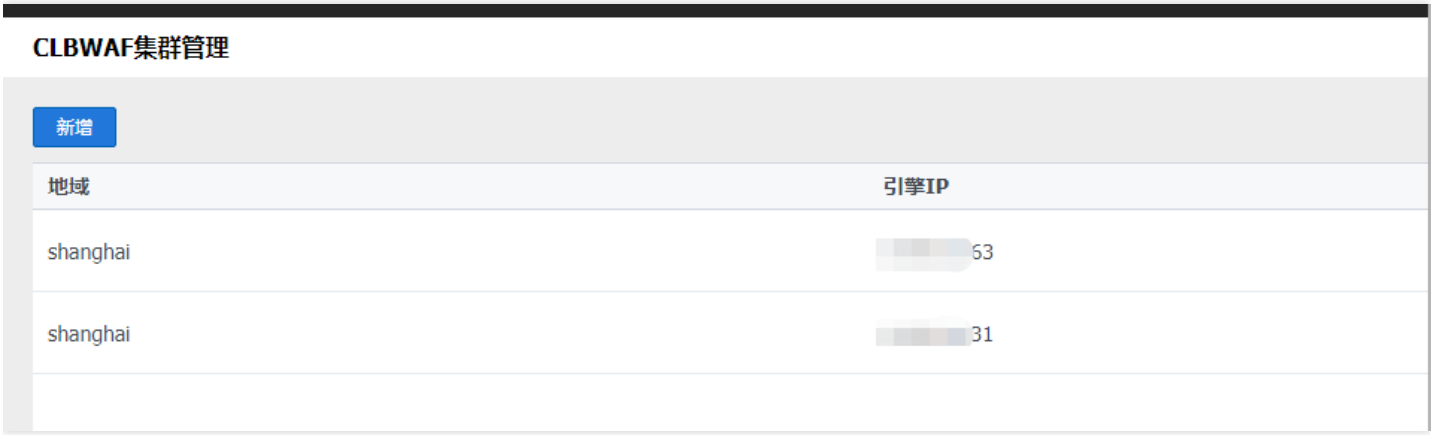
2. 登录WAF运营端，在集群管理中，点击【新增】；



3. 输入引擎IP，多个用";"隔开，点击【确认】；


确认添加
* 引擎IP
63;
31
* 地域
上海
备注
确认
取消

4. 新增成功；


CLBWAF集群管理
新增
地域
引擎IP
shanghai
63
shanghai
31

搭建SaaS型WAF源站

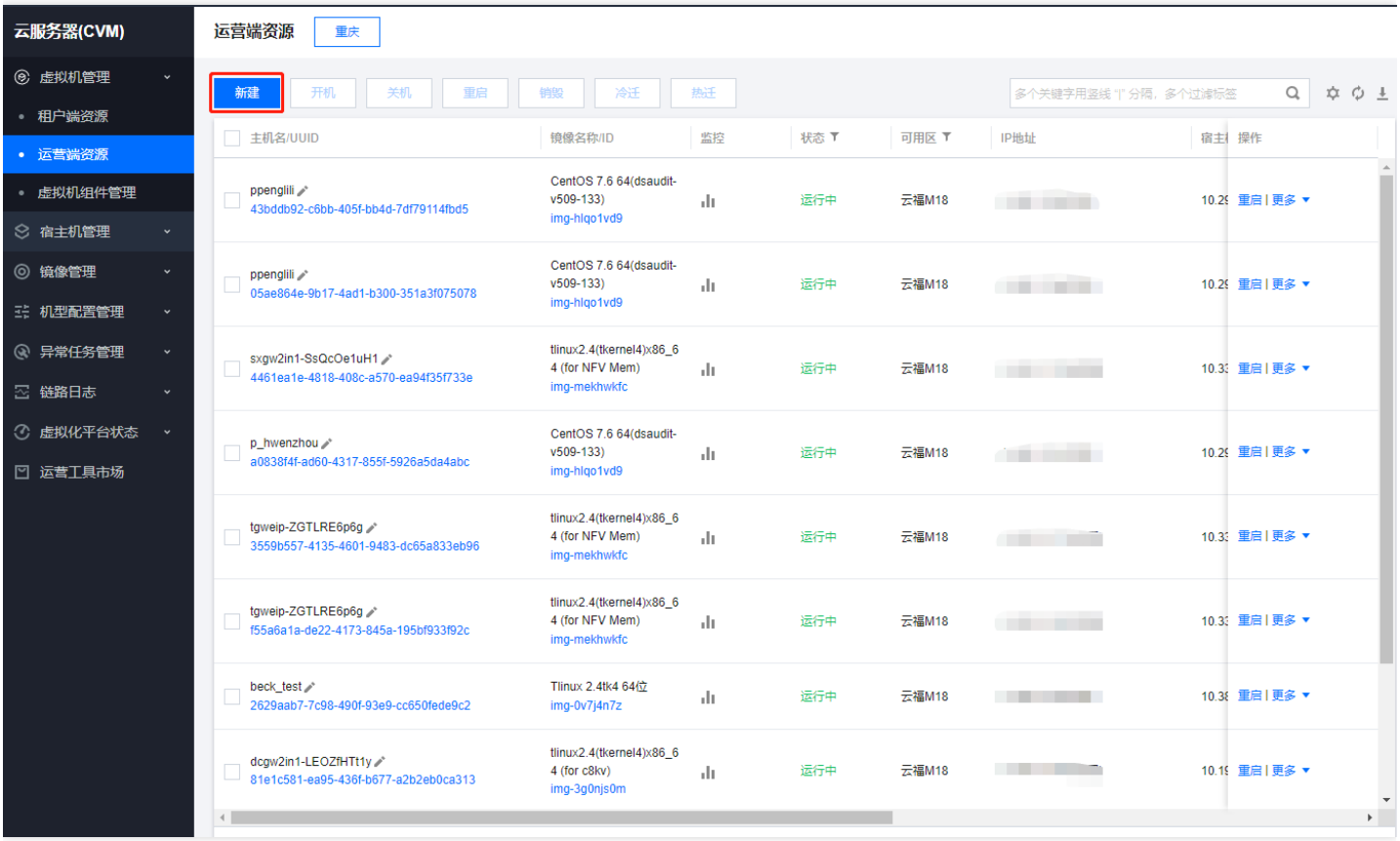
最近更新时间: 2024-12-19 17:12:00

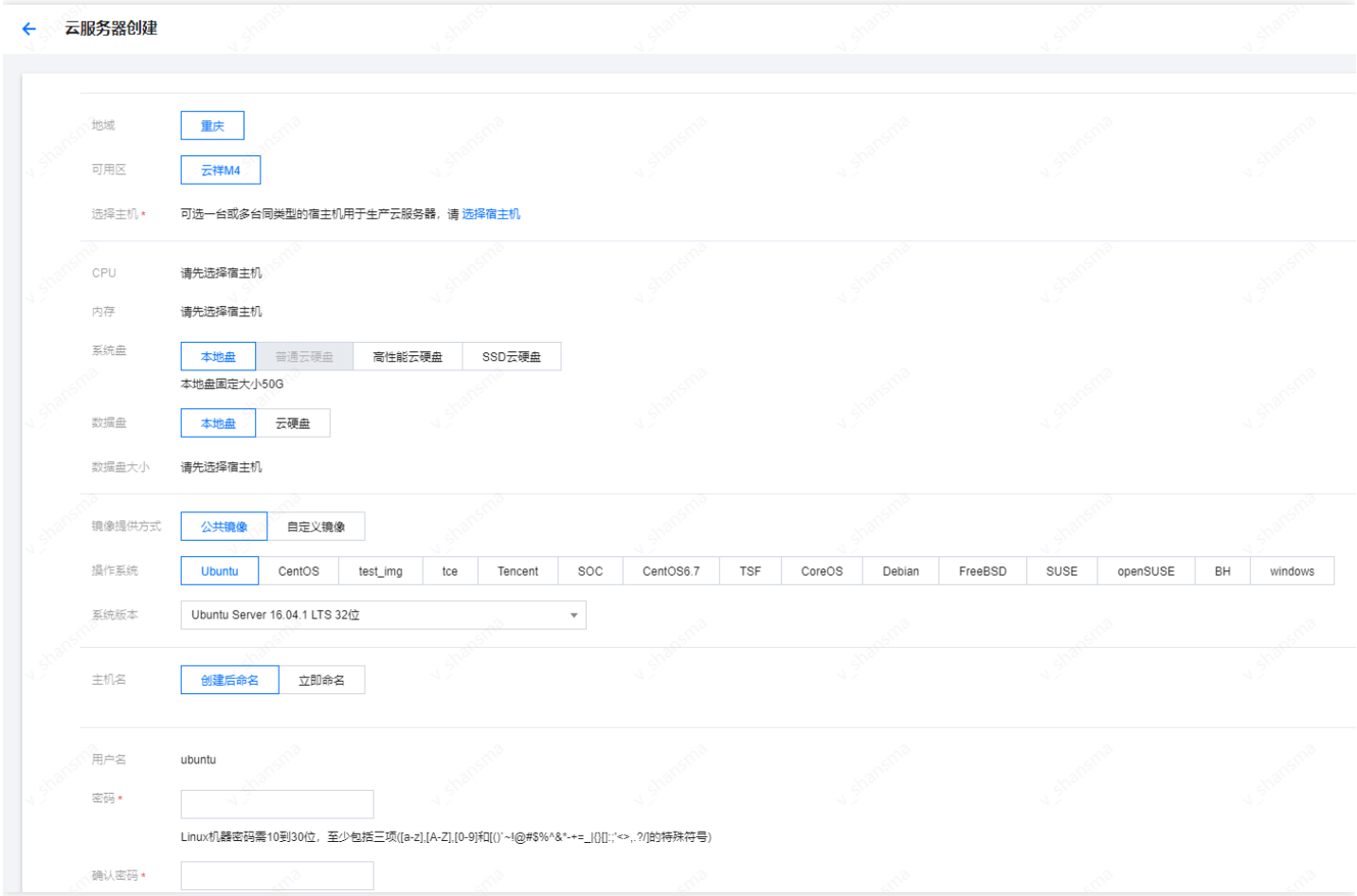
搭建SaaS型WAF源站

在新建SaaS型WAF域名时需要输入源站地址，源站地址只要与SaaS型WAF的引擎连通即可，源站IP可以使用内网IP，也可以使用外网IP。下面分别创建内网IP类型源站和外网IP类型源站。

1. 内网IP类型源站

1. 登录运营端选择云服务器创建CVM，点击运营端资源，点击【新建】；

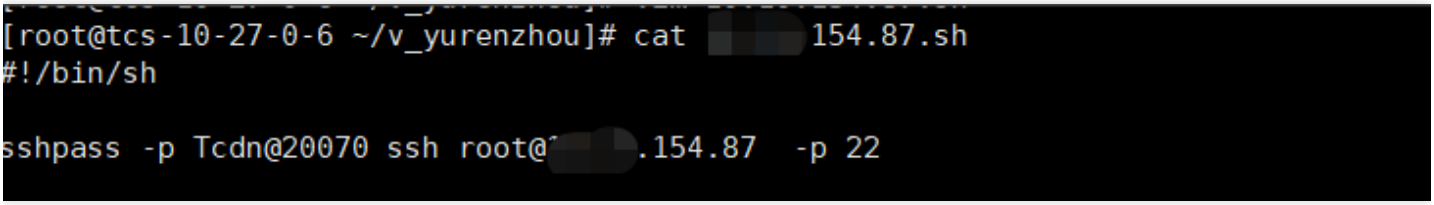




2. 在新建页面输入各项后，可以查看到新增的CVM;



3. 进入到新增的CVM中;



```
[root@tcs-10-27-0-6 ~/v_yurenzhou]# .  154.87.sh
Warning: Permanently added '  154.87' (ECDSA) to the list of known hosts.
[root@VM_154_87_linux ~]# ll
总用量 4
-rw-r--r-- 1 root root 90 1月   6 23:01 test
[root@VM_154_87_linux ~]# find / -name nginx
```

4. 在CVM中安装Nginx，输入命令 `yum install -y nginx` ;

```
[root@VM_154_87_linux ~]# yum -y install nginx
已加载插件：fastestmirror, langpacks
epel                                                     | 4.7 kB  00:00:00
extras                                                   | 2.9 kB  00:00:00
os                                                       | 3.6 kB  00:00:00
updates                                                  | 2.9 kB  00:00:00
(1/7): epel/7/x86_64/group_gz                            |  95 kB  00:00:00
(2/7): extras/7/x86_64/primary_db                        | 206 kB  00:00:00
(3/7): os/7/x86_64/group_gz                              | 153 kB  00:00:00
(4/7): epel/7/x86_64/updateinfo                          | 1.0 MB  00:00:00
(5/7): os/7/x86_64/primary_db                            | 6.1 MB  00:00:00
(6/7): updates/7/x86_64/primary_db                       | 3.8 MB  00:00:00
(7/7): epel/7/x86_64/primary_db                          | 6.9 MB  00:00:00
Determining fastest mirrors
```

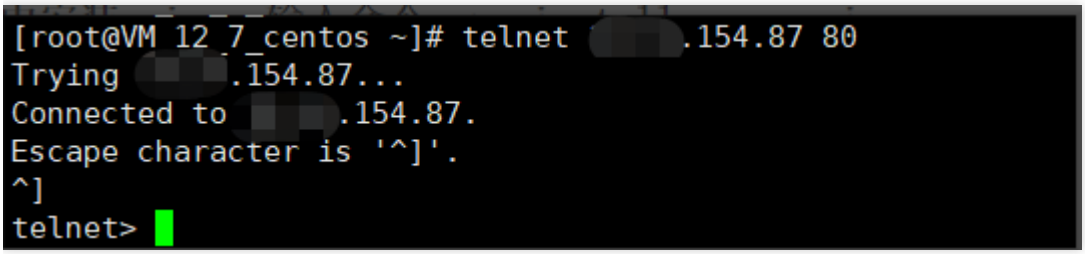
启动Nginx服务： `service nginx start`

查看80端口是否启用： `netstat -nap|grep nginx`

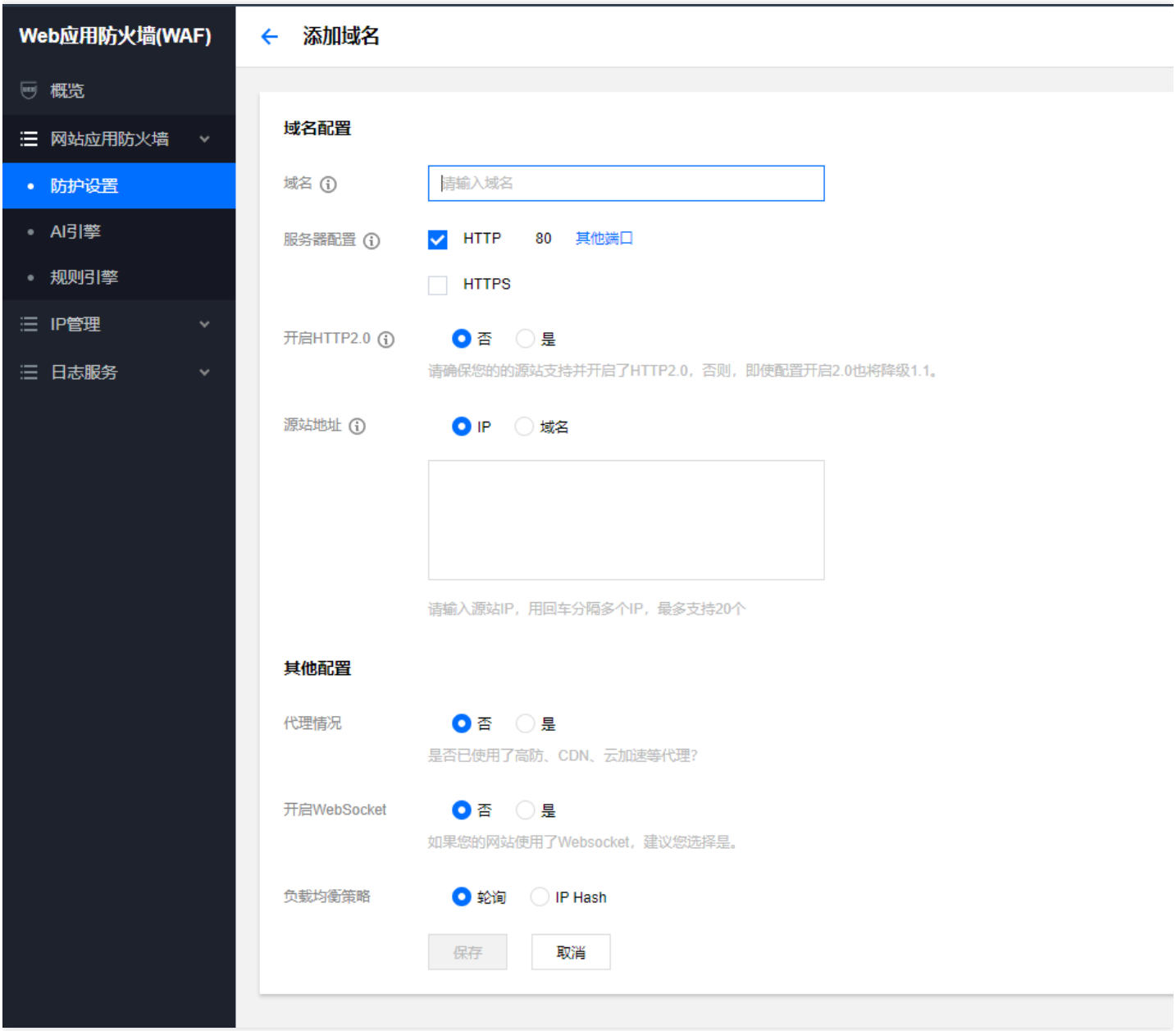
```
[root@VM_154_87_linux ~]# service nginx start
Redirecting to /bin/systemctl start nginx.service
[root@VM_154_87_linux ~]# netstat -nap |grep nginx
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      27979/nginx: master
tcp6       0      0 :::80                   :::*                    LISTEN      27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103293   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103296   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103295   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103294   27979/nginx: master
```

5. 在Saas引擎中ping和telnet cvm的IP地址及端口查看是否连通;

```
[root@VM_12_7_centos ~]# ping  .154.87
PING 10.10.154.87 (10.10.154.87) 56(84) bytes of data.
64 bytes from  .154.87: icmp_seq=1 ttl=53 time=0.823 ms
64 bytes from  .154.87: icmp_seq=2 ttl=53 time=0.832 ms
^C
--- .154.87 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.823/0.827/0.832/0.029 ms
```

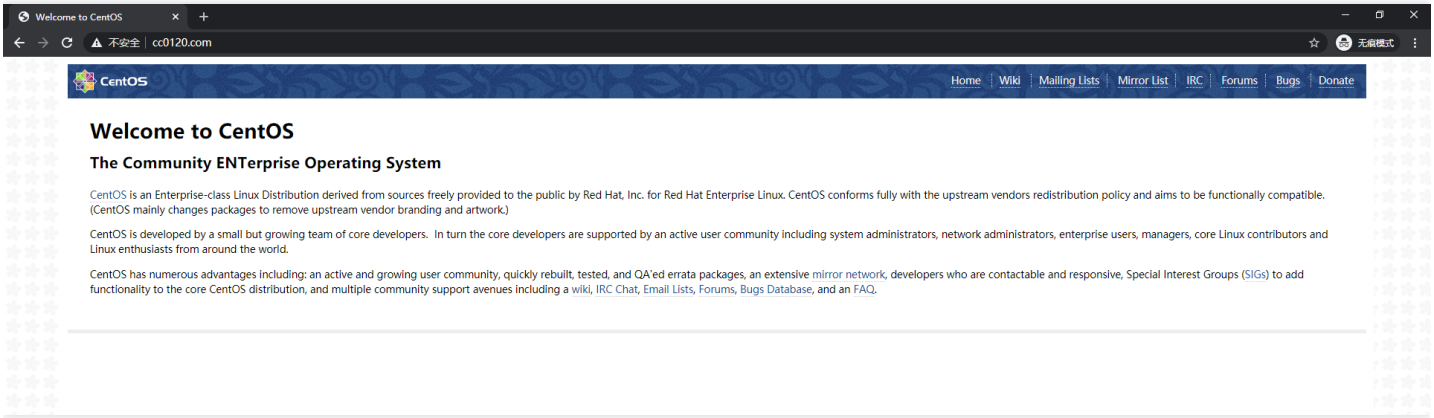


6. 在saas型WAF中新增域名,源站IP输入已申请CVM的IP地址;



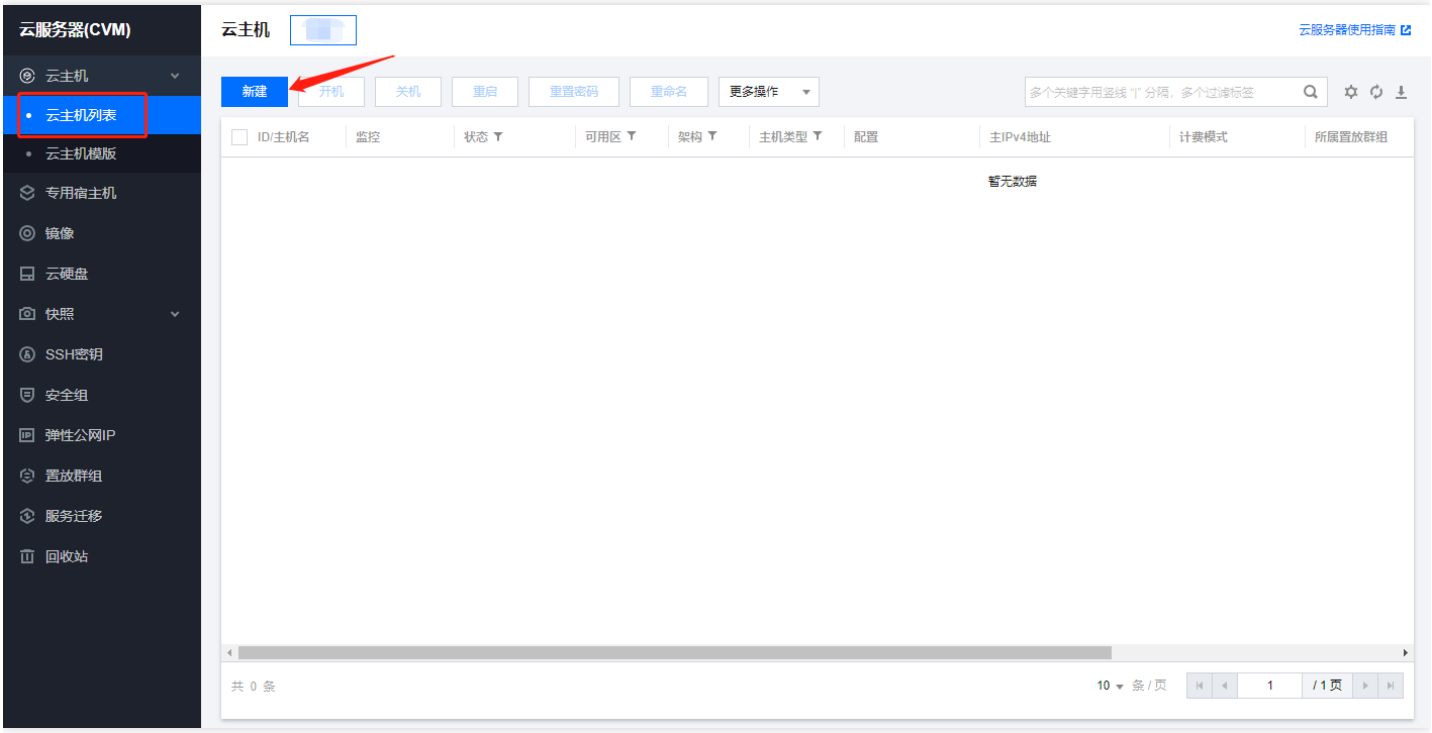


7. 配置host，访问新增域名，可以访问到内网IP类型的源站;

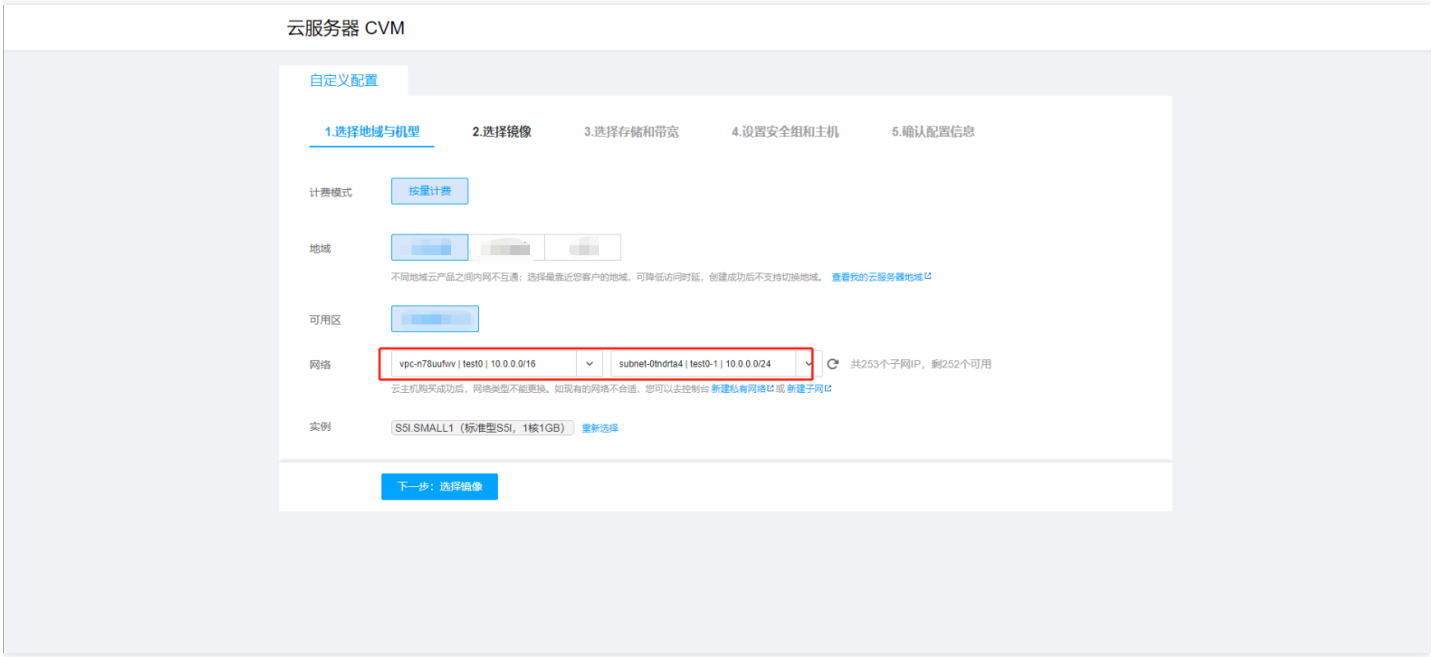


2. 外网IP类型源站

1. 登录租户端，购买CVM，进入到CVM页面，选择对应的地域，点击【新建】；



2. 所选网络需要与CLB网络一致，其余选项按照实际情况选择，点击【下一步：选择镜像】；



3. 按照实际情况选择镜像后，点击【下一步：选择存储和带宽】；



4. 按照实际情况选择存储和带宽后，点击【下一步：设置安全组和主机】；



5. 按照实际情况选择安全组合主机后，输入主机密码，点击【下一步：确认配置信息】；

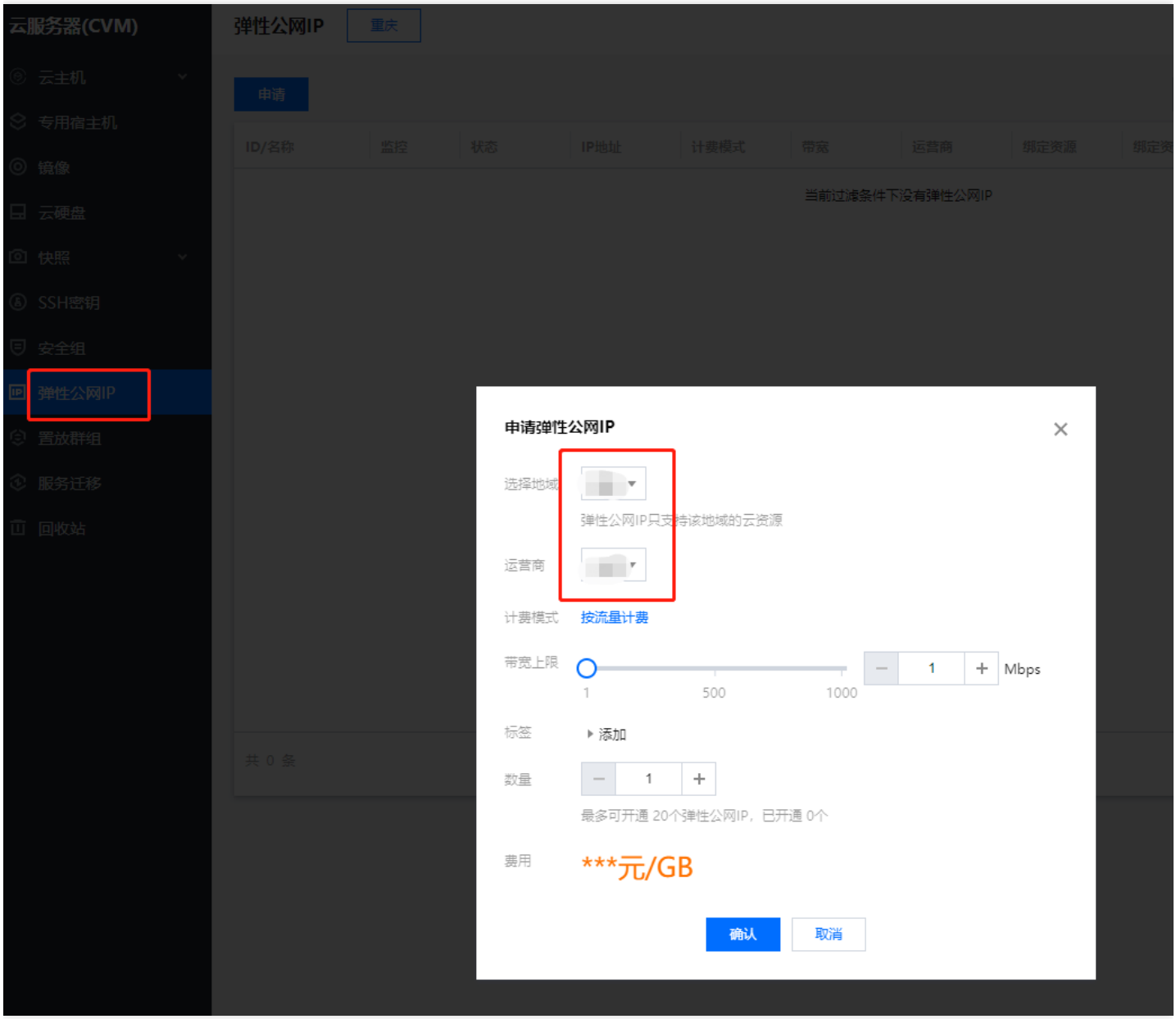




6. 查看到刚才所选的信息，确认无误后，点击【开通】；



7. 申请弹性公网IP地址，绑定CVM，CVM菜单下，点击【弹性公网IP】，选择与CVM相同的地域后，点击【申请】，按照实际情况选择各项；



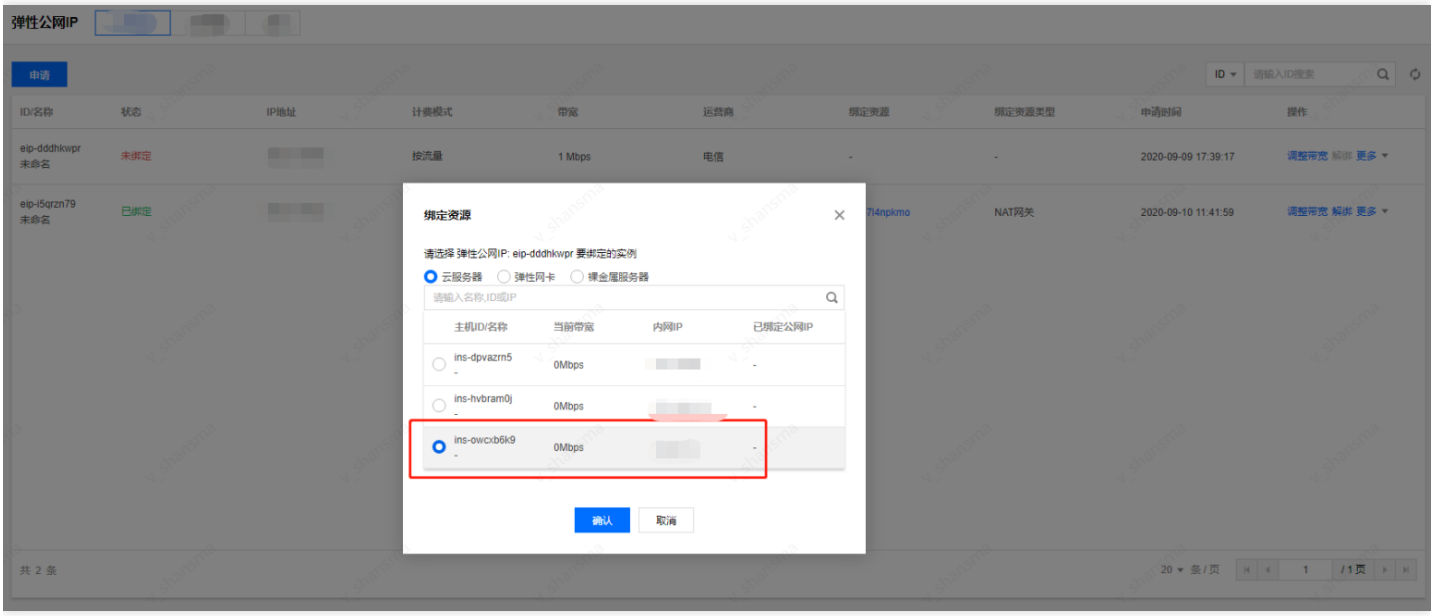
8. 点击【确认】，返回到弹性公网IP列表页面，可以查看到新建的弹性公网IP显示未绑定状态；



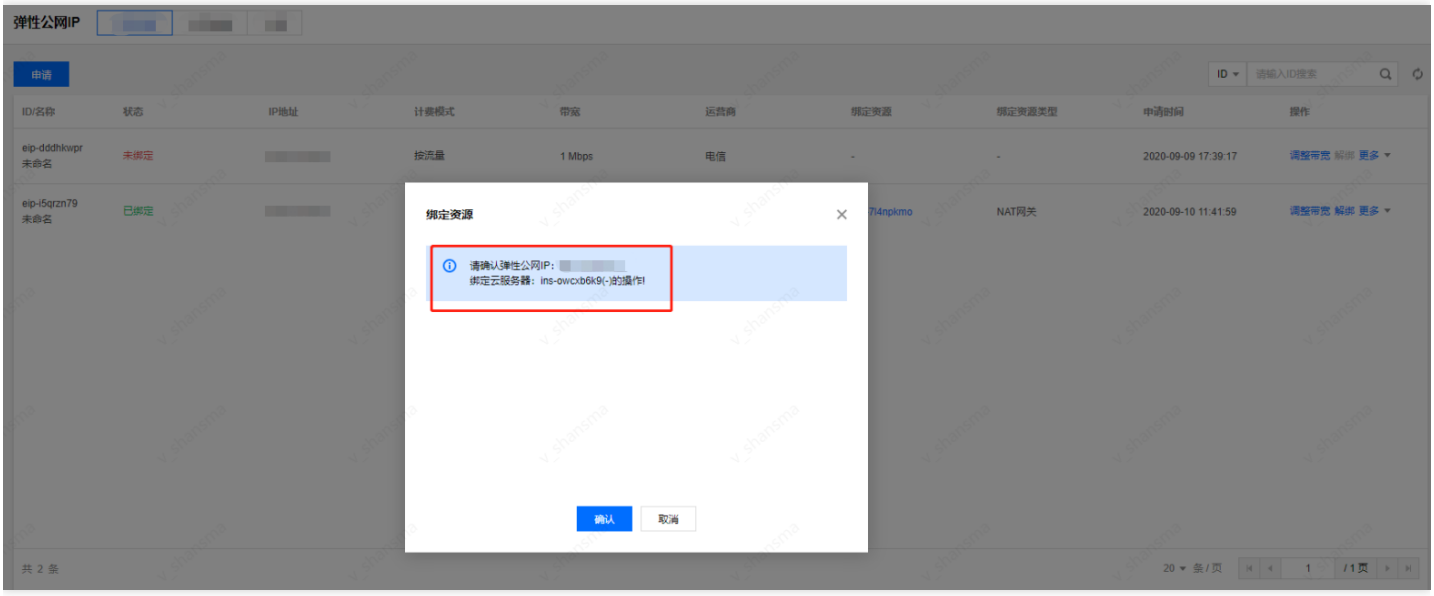
9. 点击弹性公网IP的"操作"栏，点击【更多】，选择【绑定】；



10. 选择要绑定的CVM，点击【确认】；



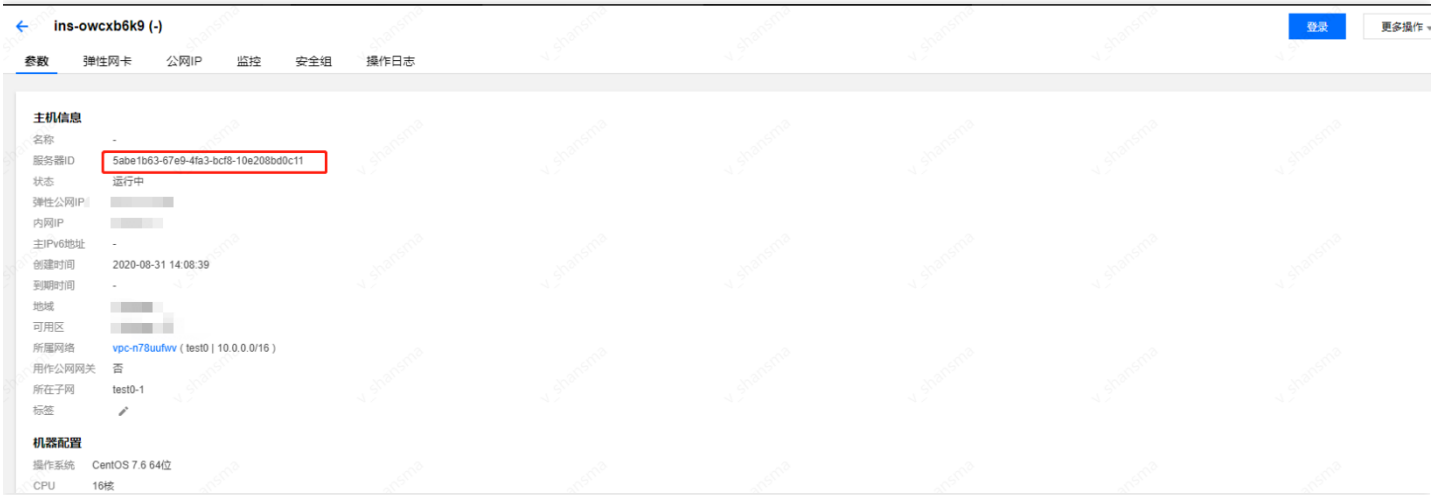
11. 查看需要确认的信息，确认无误后点击【确认】；



12. 返回到弹性公网IP列表页面，显示“已绑定”状态；



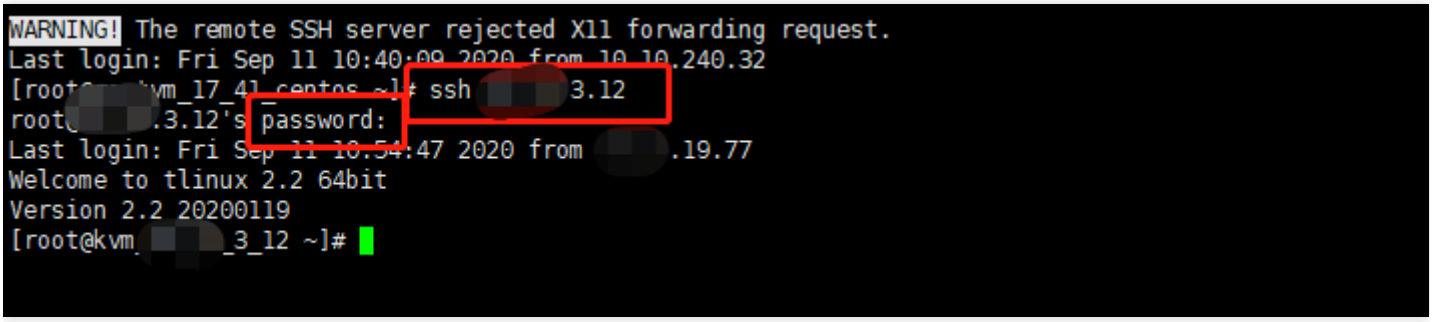
13. 安装Nginx，启用80端口，点击CVM的ID，进入到CVM参数页面，复制CVM的服务器ID；



14. 在运营端中CVM-租户端资源下，搜索框中选择UUID，粘贴刚才复制的服务器ID，可以查询到宿主机内网IP；

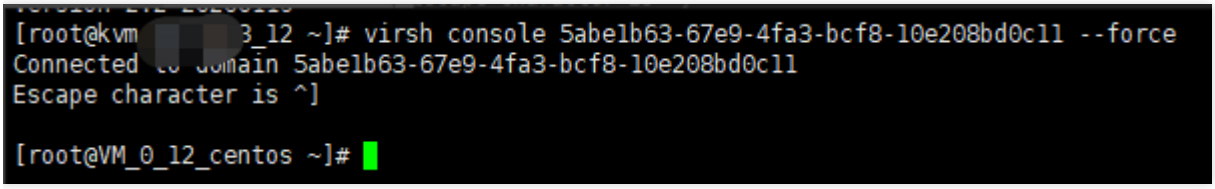


15. 登录到宿主机内网IP，输入命令：ssh 宿主机内网IP，密码为开通CVM时填入的密码；





16. 输入命令 `virsh console UUID --force` ，如virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force，进入到CVM中；

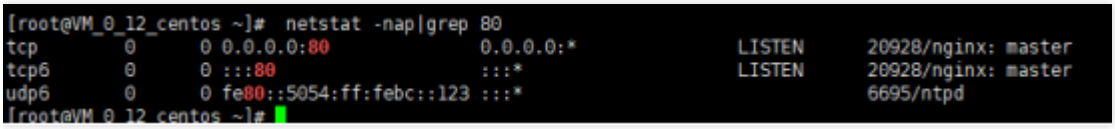


17. 进入后输入以下命令进行安装；

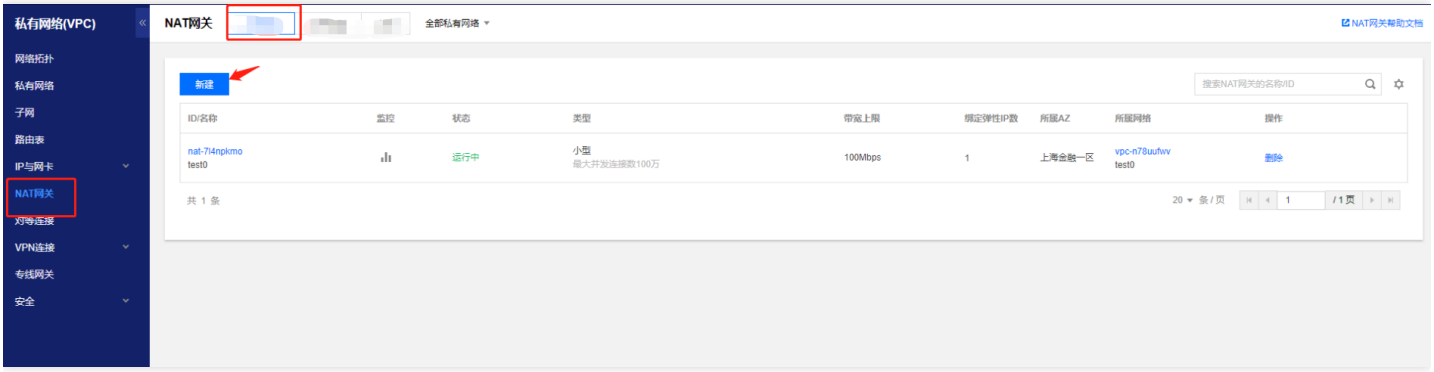
安装： `yum install -y nginx`

启动Nginx服务： `service nginx start`

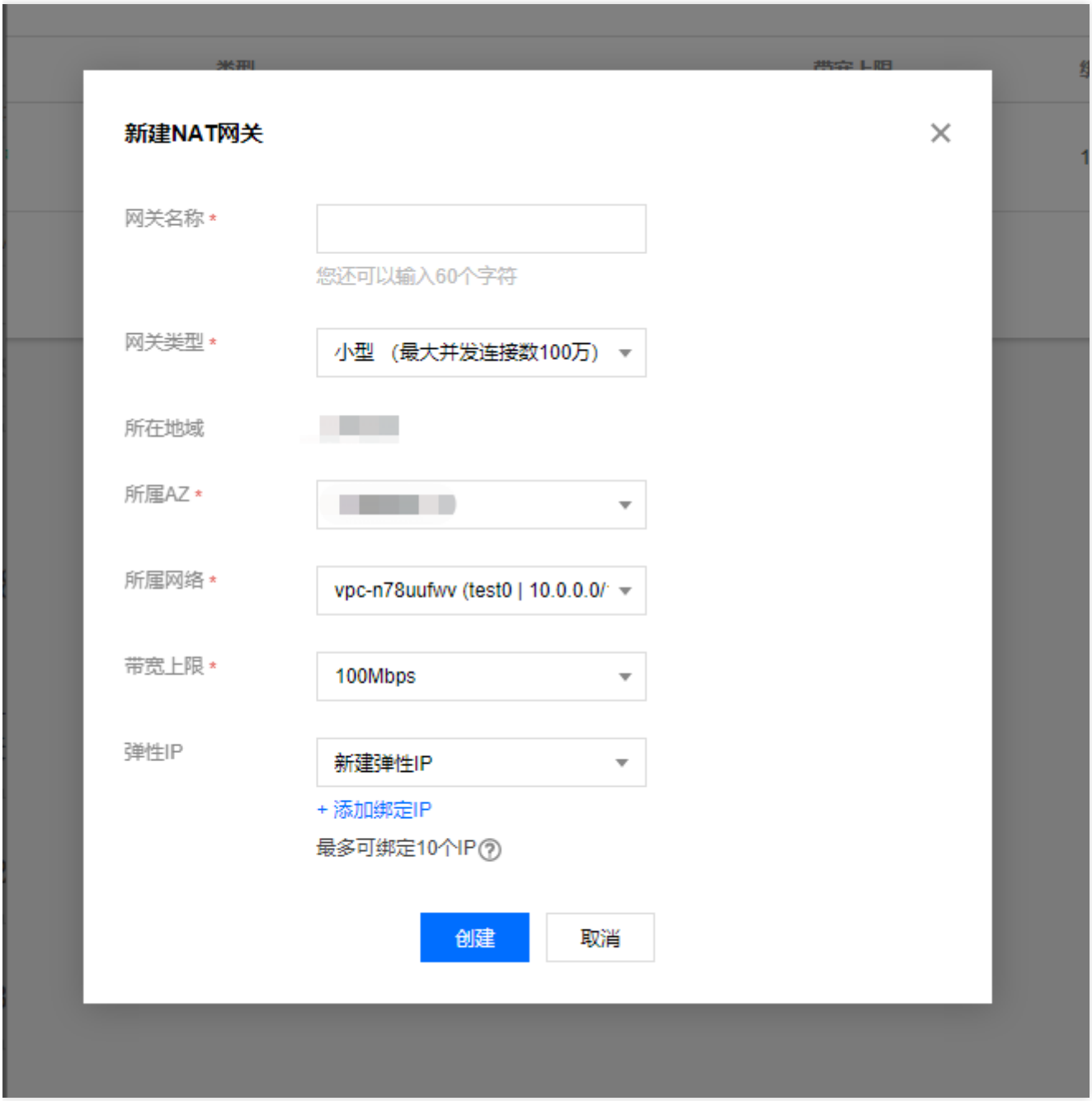
查看80端口是否启用： `netstat -nap|grep 80`



18. 由于有些客户公网ip地址禁止对外开放端口80和443，需要通过natgw把cvm的80端口转到其他端口，例如788，并在路由表中关联此网关（如不涉及此项请忽略步骤2.18-2.26）；私有网络菜单下选择NAT网关，选择对应的地域后，点击【新建】，新建NAT网关；



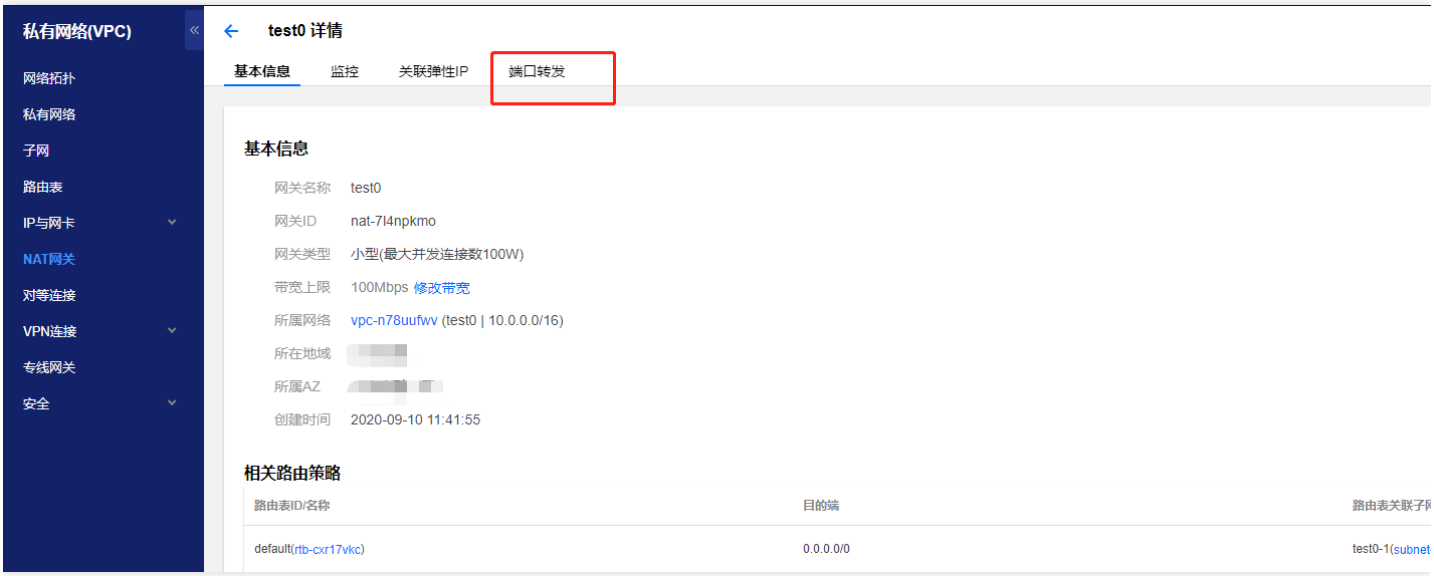
19. 按照实际情况输入各项，点击【创建】，返回到NAT网关列表页面；



20. 在新建的NAT网关中点击网关ID；



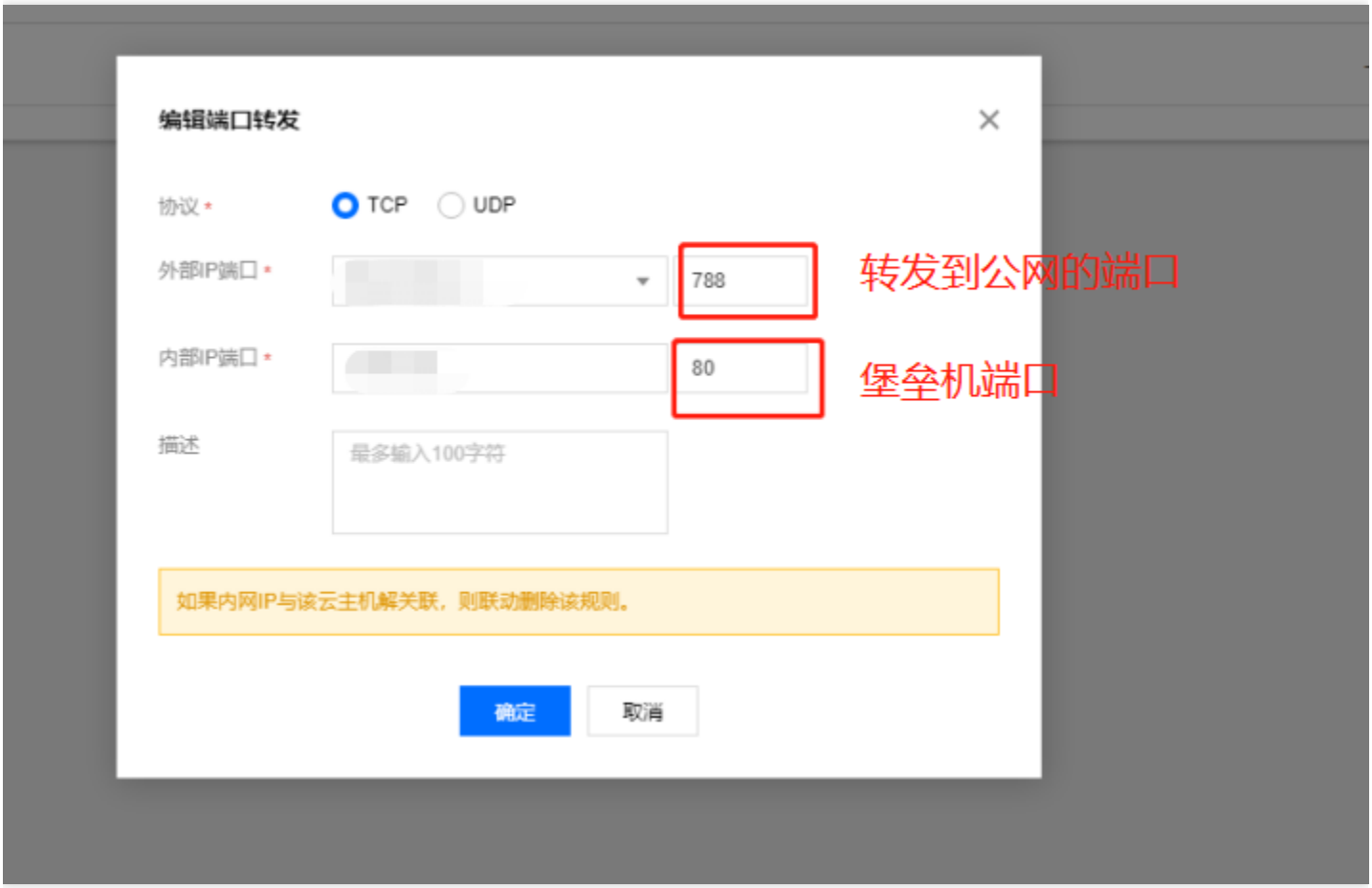
21. 点击端口转发；



22. 点击【新建】；



23. 添加转发端口；



24. 在私有网络下，选择路由表，在相应的地域下，点击【新建】，新建路由表；

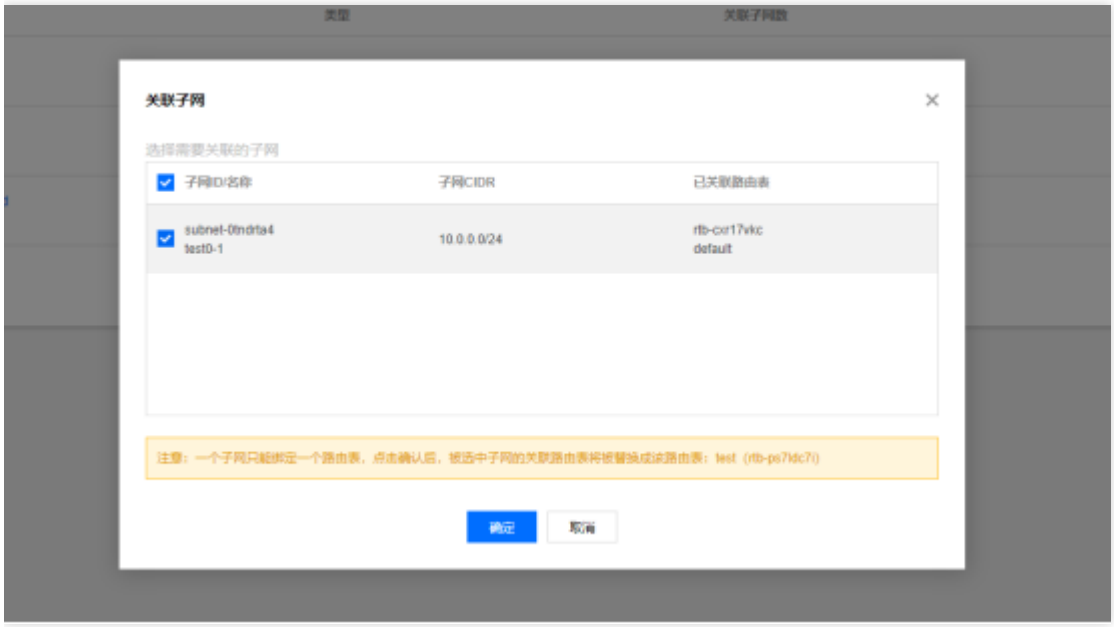


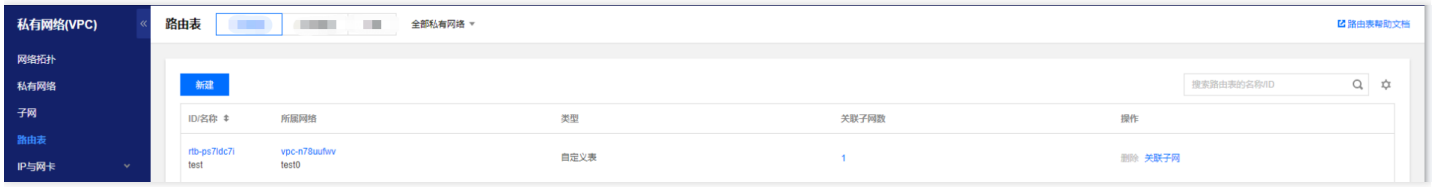


25. 输入各项后点击【创建】，策略选择已经添加的NAT网关；

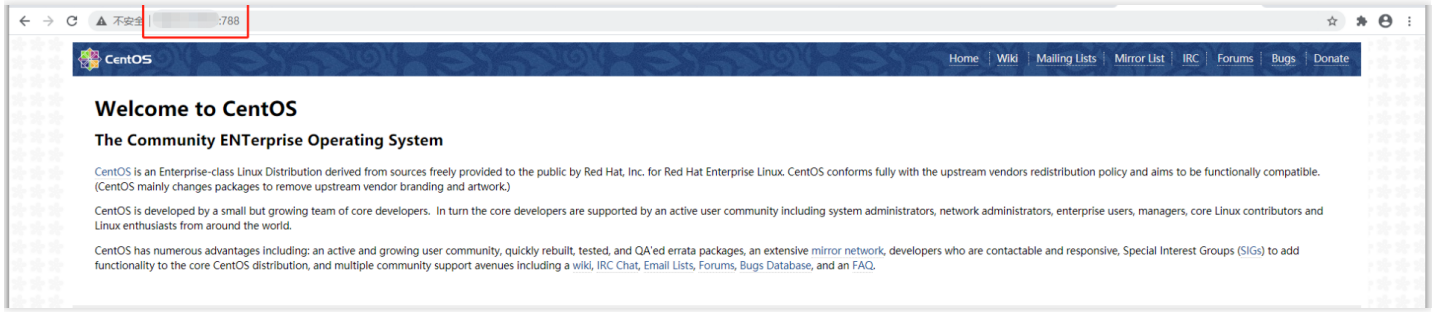


26. 提示需要关联子网，选择关联的子网后，点击【确定】，返回到路由表列表页面；





27. 访问http://公网ip:788/ 验证web网站是否正常



28. 在SaaS型WAF中新增域名,源站IP输入弹性IP的地址;


域名配置
域名
testsaaswaf0118.com
服务器配置
HTTP
80
其他端口
HTTPS
开启HTTP2.0
否
是
请确保您的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。
源站地址
IP
域名
请输入源站IP，用回车分隔多个IP，最多支持20个
其他配置
代理情况
否
是
是否已使用了高防、CDN、云加速等代理？
开启WebSocket
否
是
如果您的网站使用了Websocket，建议您选择是。
负载均衡策略
轮询
IP Hash
保存
取消


Web应用防火墙(WAF)
概览
网站应用防火墙
防护设置
AI引擎
IP管理
日志服务
SaaS型
负载均衡型
域名接入操作指南
防护设置
域名列表
添加域名
删除
域名
VIP地址
使用模式
回源IP地址
WAF开关
操作
testsaaswaf0118.com
109.244.100.200
规则：拦截模式
109.244.100.240
删除 编辑 防护配置

常见问题

常见问题

最近更新时间: 2024-12-19 17:12:00

非云内的服务器能否使用 Web 应用防火墙？

Web 应用防火墙支持云外机房用户接入，可以保护任何公网的服务器，包括但不限于云平台，包括其他厂商的云，IDC 等。

注意： 在中国内地（大陆）地区接入的域名必须按照工信部要求进行 ICP 备案。

Web 应用防火墙是否支持 HTTPS 防护？

Web 应用防火墙全面支持 HTTPS 业务。用户只需根据提示将 SSL 证书及私钥上传，Web 应用防火墙即可防护 HTTPS 业务流量。

Web 应用防火墙的源站 IP 可以填写内网 IP 吗？

Web 应用防火墙添加域名时，填写的源站地址必须是公网 IP 或者域名。内网IP需要和管理员确认。

Web 应用防火墙一个防护域名可以设置多少个回源 IP？

Web 应用防火墙一个防护域名最多可以设置20个回源 IP。

Web 应用防火墙配置多个源站时如何负载？

如果配置了多个回源 IP，Web 应用防火墙采用轮询的方式对访问请求进行负载均衡。

Web 应用防火墙是否支持健康检查？

Web 应用防火墙默认启用健康检查。Web 应用防火墙会对所有源站 IP 进行接入状态检测，如果某个源站 IP 没有响应，Web 应用防火墙将不再将请求转发到该源站 IP ，直到接入状态恢复正常。

Web 应用防火墙是否支持会话保持？

Web 应用防火墙支持会话保持，默认开启。

在 Web 应用防火墙的控制台中，更改配置后大约需要多少时间生效？

一般情况下，更改后的配置在10s内即可生效。

Web 应用防火墙是否会自动将回源 IP 段加入安全组？

不会自动将回源 IP 段添加到安全组。请参考快速入门将相应的回源 IP 加入到安全组。

如果上传文件被拦截，那使用 HTTPS 或者 SFTP 上传文件是否仍会拦截呢？

若没有使用 Web 应用防火墙不会被拦截，如果使用 Web 应用防火墙并且开启了拦截模式，使用 HTTP 或 HTTPS 上传恶意文件将会被拦截。但使用 SFTP 上传文件则不会被拦截，SFTP 是非 HTTP 或 HTTPS 协议，Web 应用防火墙不支持防护。

Web应用防火墙支持哪些非标端口？

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、9999、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