



云应用防火墙（龙御）

产品文档





文档目录

产品简介

产品介绍

功能简介

主要功能

为何需要WAF

基础防御流程

产品优势

专业的网站防护能力

及时的补丁修复保障

稳定的高可用业务保障

ipv6安全防护

应用场景

政务网站防护

电商网站防护

金融网站防护

防数据泄密

操作指南

AI检测及管理

功能简介

注意事项

配置示例

CC 攻击防护设置

功能简介

配置示例

地域封禁设置

功能简介

配置说明

自定义策略防护设置

功能简介

注意事项

配置说明

IP黑白名单防护设置

功能简介

注意事项

配置示例



快速入门

- 一、添加域名
- 二、本地测试

常见问题

- 如何定位是否为龙御WAF拦截
- 如何分析拦截原因
- 日常运营中如何进行误拦截处置
- 如何进行AI引擎在线学习
- 如何添加自定义放行规则
- CLB型WAF域名访问故障时如何应急
- 龙御WAF中各类自定义配置的优先级是什么



产品简介

产品介绍

功能简介

最近更新时间: 2023-02-09 14:48:23

Web应用防火墙（Web Application Firewall, WAF）基于AI+规则进行Web攻击识别，实时阻断SQL注入、XSS跨站脚本、Webshell木马上传等常见的Web威胁攻击，并联动封禁产品进行恶意IP的封禁。

建行云为负载均衡WAF版本，通过域名与建行云七层负载均衡集群进行联动，对经过负载均衡的HTTP和HTTPS流量进行威胁检测，并将检测结果发送给负载均衡，负载均衡根据检测结果直接拦截页面或者向后端云服务器转发，实现业务转发和安全防护分离。



主要功能

最近更新时间: 2023-02-09 14:48:23

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、精准有效防御常见Web攻击，如SQL注入、XSS跨站脚本、CSRF跨站请求伪造、web应用漏洞攻击，Webshell木马上传等OWASP定义的十大Web安全威胁攻击
CC 攻击防御	多维度自定义精准访问控制、配合频率控制等对抗手段，高效控制访问频率及缓解CC 攻击问题
IP黑白名单	可设置某个域名或者APPID下所有域名的IP黑/白名单规则，只支持IPV4地址，CC防护命中的IP也在IP黑名单中查询到
自定义策略	自定义策略，根据租户需求可灵活配置,如对于来源ip、referer、请求路径、HTTP请求方法等。动作可选择放行、阻断、人机识别、观察、重定向。
地域封禁	地域封禁，按照内置地址库对境外国家/地区以及中国各大省市自治区进行封禁，阻断该区域的所有来源IP的访问，支持IPV4/IPV6地址
联动封禁	龙御waf对非自定义策略类拦截（自定义策略包括包括cc、ip黑名单、自定义阻断、地域封禁）联动天幕进行封禁操作，减小攻击成功的可能性



为何需要WAF

最近更新时间: 2023-02-09 14:48:23

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，被商业竞争对手利用数据）**

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、非法”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。

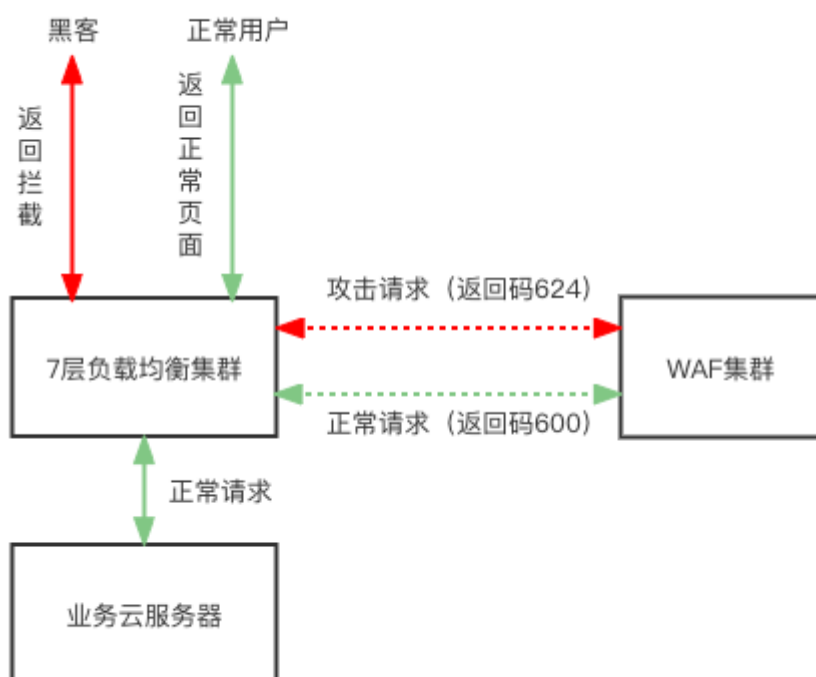
- **框架漏洞（补丁修复时段被攻击）**

很多 Web 系统基于常见的开源框架如 Struts2、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，很多攻击会在漏洞公布之后一天内就遍地开花。

基础防御流程

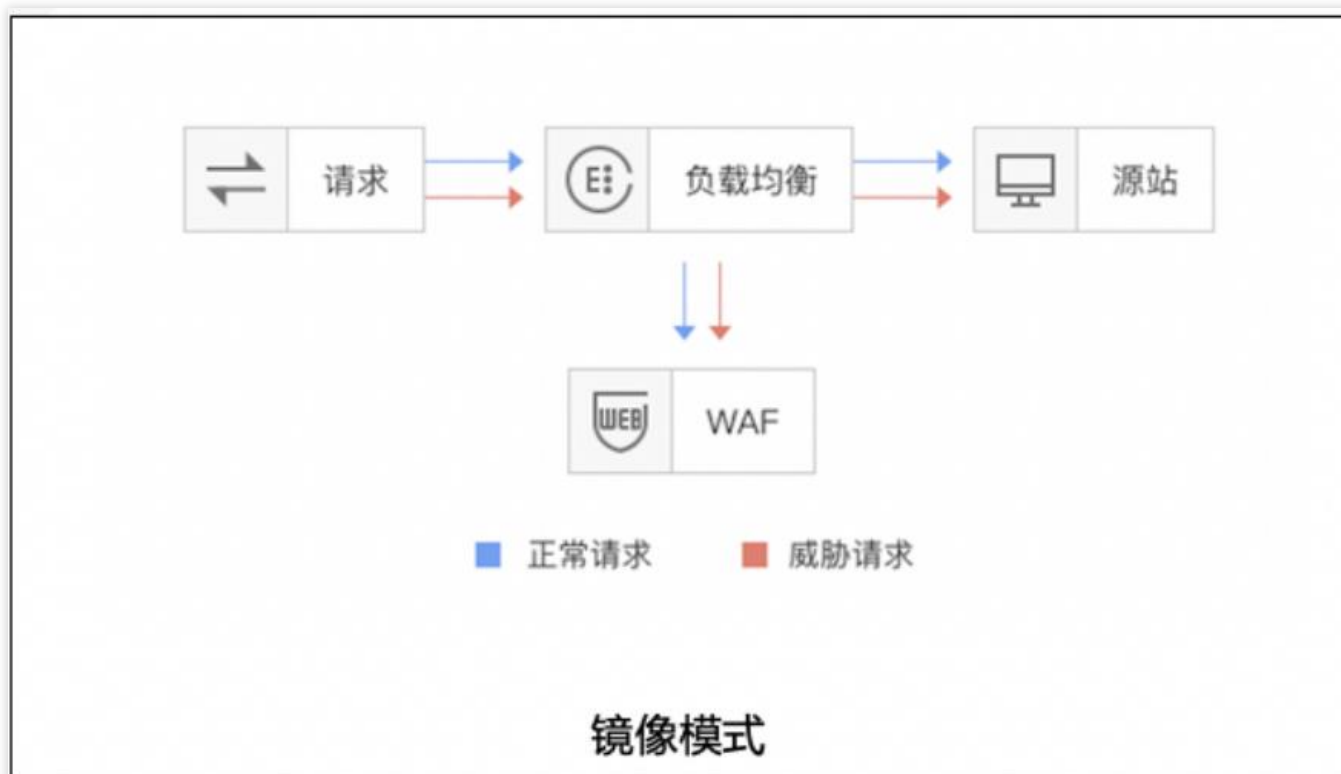
最近更新时间: 2023-02-09 14:48:23

WAF 通过配置域名和建行云七层负载均衡（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。

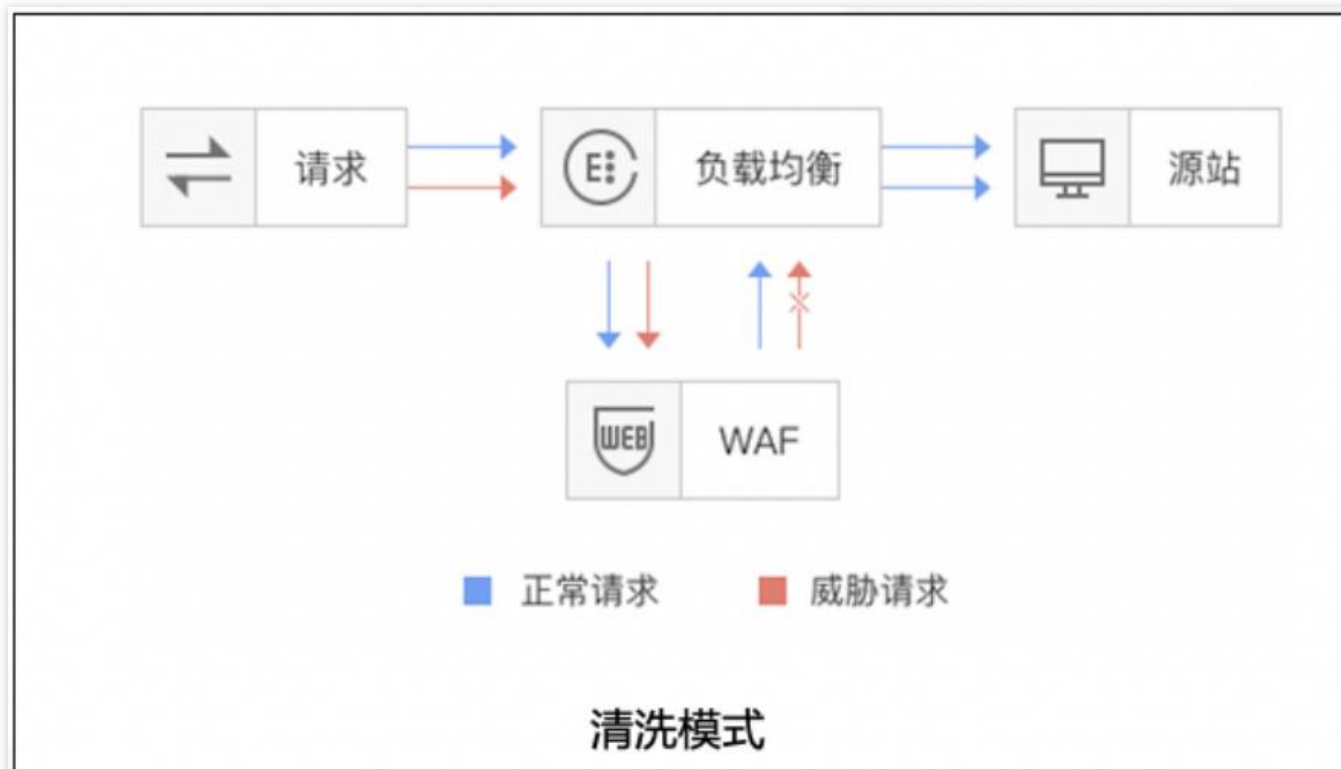


负载均衡型 WAF 提供两种流量处理模式：

- 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。





产品优势

专业的网站防护能力

最近更新时间: 2023-02-09 14:48:19

- 云应用防火墙（龙御）拥有千余条防御规则结合AI模型检测全面防护各种Web入侵攻击、专业攻防团队迭代防护系统，保障网站防御系统处于行业前沿。



及时的补丁修复保障

最近更新时间: 2023-02-09 14:48:19

- 可及时提供更新高危漏洞地补丁及常见通用型漏洞补丁服务。



稳定的高可用业务保障

最近更新时间: 2023-02-09 14:48:19

- 无感知接入，毫秒级延迟，域名接入 WAF 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。



ipv6安全防护

最近更新时间: 2023-02-09 14:48:19

- 通过和建行云负载均衡进行联动，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。



应用场景

政务网站防护

最近更新时间: 2023-02-09 14:48:19

- 一键接入防御，轻松配置，隐藏并保护源站，保证网站内容不被黑客入侵篡改。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

最近更新时间: 2023-02-09 14:48:19

- 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，可设定对于指定url的cc防护(基于ip或session)，保障正常访问业务流畅。



金融网站防护

最近更新时间: 2023-02-09 14:48:19

- 一键接入防护，具备 Web 安全防护,可有效检测异常攻击行为，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。



防数据泄密

最近更新时间: 2023-02-09 14:48:19

- 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（HTTPFlood），通过在七层阻断海量的恶意请求，保障网站可用性。



操作指南

AI检测及管理

功能简介

最近更新时间: 2023-02-09 15:07:37

AI引擎是云 Web 应用防火墙率先应用基于机器学习的 Web 攻击检测技术，通过 AI 引擎的检测模型及学习能力，最大限度提高已知和未知 Web 威胁的检测率和捕获率，最大限度减少误报，并且灵活适应不断变化的 Web 应用。



注意事项

最近更新时间: 2023-02-09 15:07:37

添加AI漏报、误报后，AI模型会进行学习更新检测模型，请谨慎设置。



配置示例

最近更新时间: 2023-02-09 15:07:37

本章节将演示如何开启AI模型防护功能、对攻击负载进行AI模型的在线验证及误报的学习。

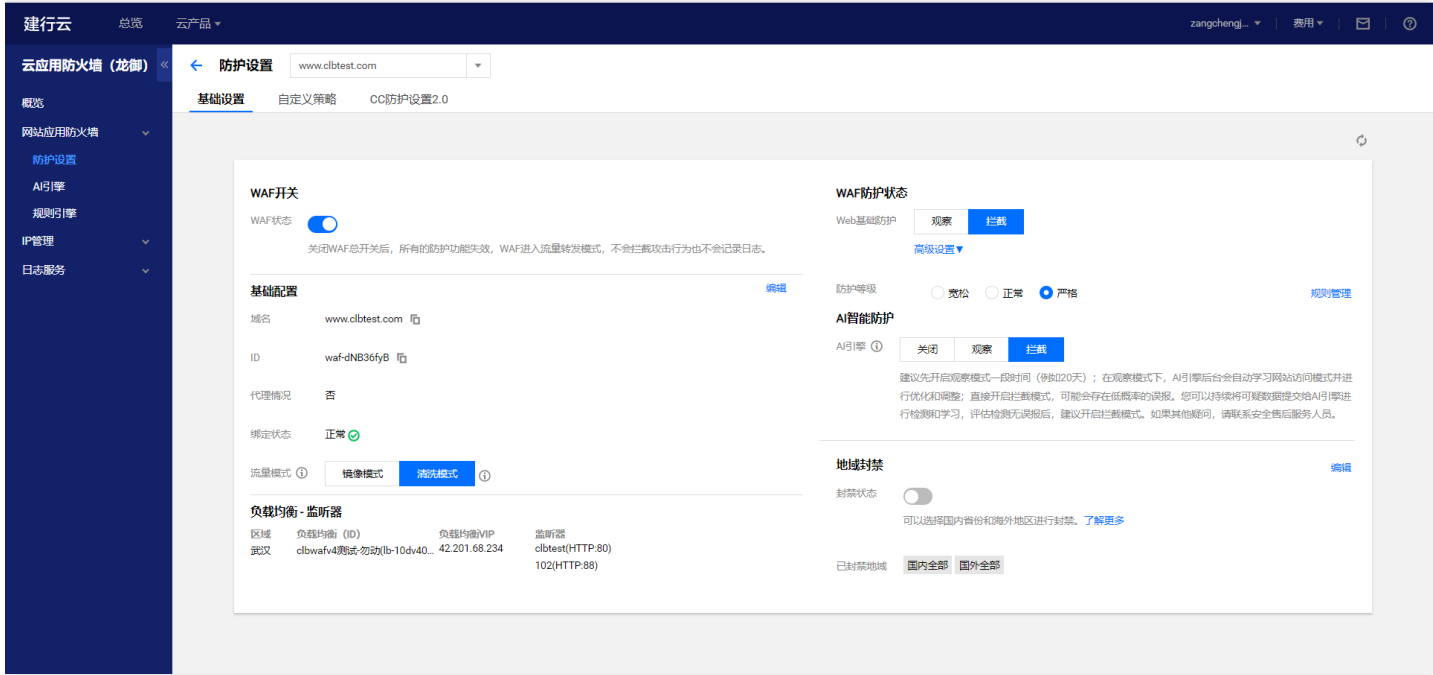
- 前置条件

相关测试域名已经配置了waf防护

- 示例

第一项：开启或关闭AI智能防护。

登陆租户控制台，进入云应用防火墙（龙御）界面下，选择相应域名点击防护配置，在基础防护下可以看到AI智能防护功能(AI引擎具有三个选项：1、关闭，指关闭AI引擎防护功能；2、观察，指AI引擎进行检测并记录相关日志但不进行拦截；3、拦截，指AI引擎既进行检测也进行拦截并记录拦截日志)。



第二项：利用AI引擎验证攻击负载。

登陆租户控制台，进入云应用防火墙（龙御）界面下，选择AI引擎标签，点击AI在线验证，添加负载内容，点击立即验证。如果验证为攻击，当请求内容中带有相关攻击负载会被AI引擎拦截并记录相关日志。



建行云

总览

云产品

云应用防火墙（龙御）

AI引擎

AI误报处理

AI漏报处理

AI在线验证

概览

网站应用防火墙

防护设置

AI引擎

规则引擎

IP管理

日志服务

AI在线验证，提供了判定数据是“正常”还是“威胁数据”（SQL注入、XSS、其他异常）的能力；您可以根据验证结果，一键提交误报或漏报，然后在误报或漏报页面进行学习。了解更多

访问地址 *

www.cibtest.com

验证参数 *

参数类型

参数名称

参数值

操作

GET参数

请输入参数名称

a=alert(123)

删除

新增

立即验证

验证结果

一键添加误报

验证结果

威胁数据

疑似攻击类型

XSS或SQL注入

攻击参数类型

GET参数

攻击参数原始值

a=alert(123)

攻击参数解码值

a=alert(123)

处理时间

0.8ms

攻击路径

/

攻击参数名称

无

第三项：对误报进行学习

登陆租户控制台，进入云应用防火墙（龙御）界面下，选择AI引擎标签，点击AI误报处理，手动添加负载内容（学习内容为a=alert（123）），点击添加，然后选中添加内容点击学习。

建行云

总览

云产品

云应用防火墙（龙御）

AI引擎

AI误报处理

AI漏报处理

AI在线验证

概览

网站应用防火墙

防护设置

AI引擎

规则引擎

IP管理

日志服务

您可以手动将误报的攻击添加到此处，也可以在AI引擎输出的攻击日志详情中点击“误报”添加；添加之后，点击“学习”，AI引擎会根据误报信息更新模型，优化算法。了解更多

手动添加

删除

学习

AI模型最后更新时间：2022-09-15 10:19:17

添加误报

Payload *

a=alert(123)

备注

备注，非必填项

添加

取消

共0项

每页显示行 20

1/1



建行云

总览

云产品

云应用防火墙（龙御）

概览

网站应用防火墙

防护设置

AI引擎

规则引擎

IP管理

日志服务

AI引擎

AI误报处理

AI漏报处理

AI在线验证

您可以手动将误报的攻击添加到此处，也可以在AI引擎输出的攻击日志详情中点击“误报”添加；添加之后，点击“学习”，AI引擎会根据误报信息更新模型、优化算法。[了解更多](#)

手动添加

删除

学习

AI模型最后更新时间：2022-09-15 10:21:05

☐	序号	ID	载荷	来源	备注	创建时间 ↓	状态 ↑
☐	1	63228bfdasec5100eb48ee4	a=alet(123)	手动添加	无	2022-09-15 10:20:45	已学习

共1项

每页显示行 20

1/1



CC 攻击防护设置

功能简介

最近更新时间: 2023-02-09 16:55:56

CC策略是指攻击者通过工具，模拟多个用户不断向网站发送连接请求，导致用户业务不可用，添加 CC 防护规则，可以帮助用户防护针对页面请求的 CC 攻击。

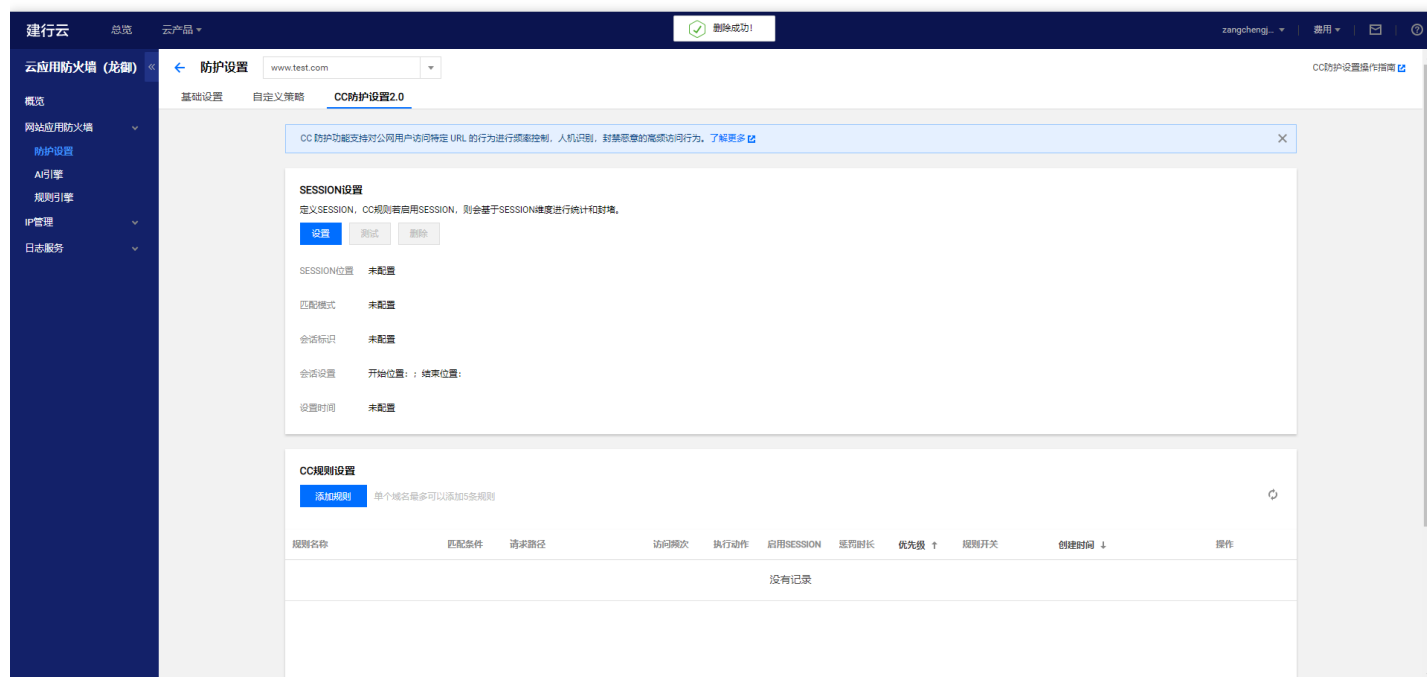


配置示例

最近更新时间: 2023-02-09 16:55:56

本配置示例可实现，当单个源 IP 在 10 秒内访问/test.html超过 10 次，恶意访问惩罚功能将封禁此源 IP 30 分钟。

1、进入云应用防火墙（龙御）主界面，单击【防护设置】，单击需要防护的站点域名，单击【CC防护设置】选项卡进入恶意访问惩罚配置界



2、单击【添加规则】，在规则名称输入框里面输入具体的规则名称、选择匹配条件（等于），具体的 URI (/test.html)，以及访问频次（10次10秒），选择执行动作封禁访问（也可以选择人机识别，人机识别采用一定的算法进行验证，如果验证失败后，将自动封禁访问），惩罚时长输入 10 分钟



云应用防火墙（龙御）

概览

网站应用防火墙

防护设置

AI引擎

IP管理

日志服务

添加CC防护规则

规则名称 *
test

识别方式 *
☒ IP ☐ SESSION

匹配条件 *
相等

URI路径 *
/test.html

高级匹配 ①

访问频次 *
10 次 10秒 ①

执行动作 *
拦截 ①

惩罚时长 *
10 分钟 ①

优先级 *
- 50 +

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

添加 取消

3、单击【添加】保存规则，此时规则将会生效，惩罚恶意访问行为。

云应用防火墙（龙御）

概览

网站应用防火墙

防护设置

AI引擎

IP管理

日志服务

设置时间 未配置

CC规则设置

添加规则 单个域名最多可以添加5条规则

规则名称	匹配条件	请求路径	访问频次	执行动作	启用SESSION	惩罚时长	优先级 ↑	规则开关	创建时间 ↓	操作
test	相等	/test.html	10次/10秒	拦截	否	10分钟	50	☒	2020-07-03 15:12:06	编辑 删除

共1项

每页显示行 10 1/1



地域封禁设置

功能简介

最近更新时间: 2023-02-09 16:55:56

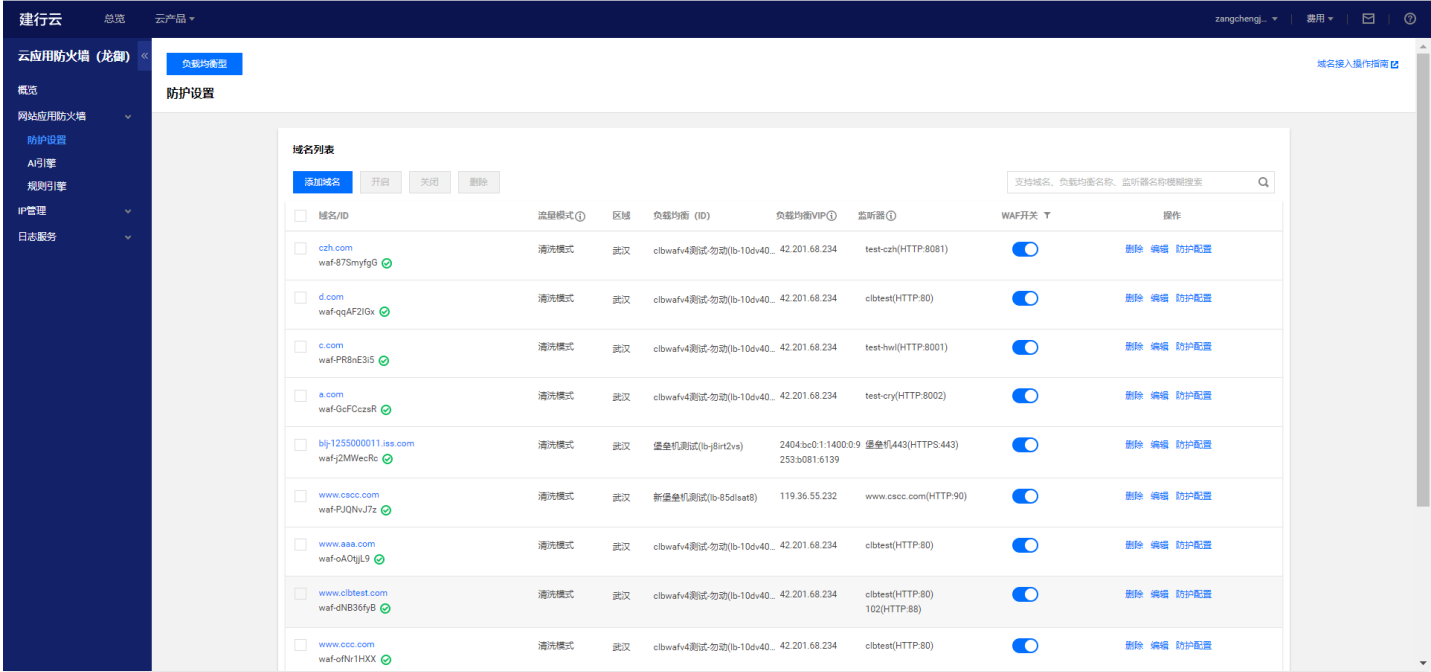
地域封禁指根据配置的地域（如北京），waf会根据配置的地域信息来拦截所在地域的ip地址的请求信息。目前支持IPV4/IPV6地址。



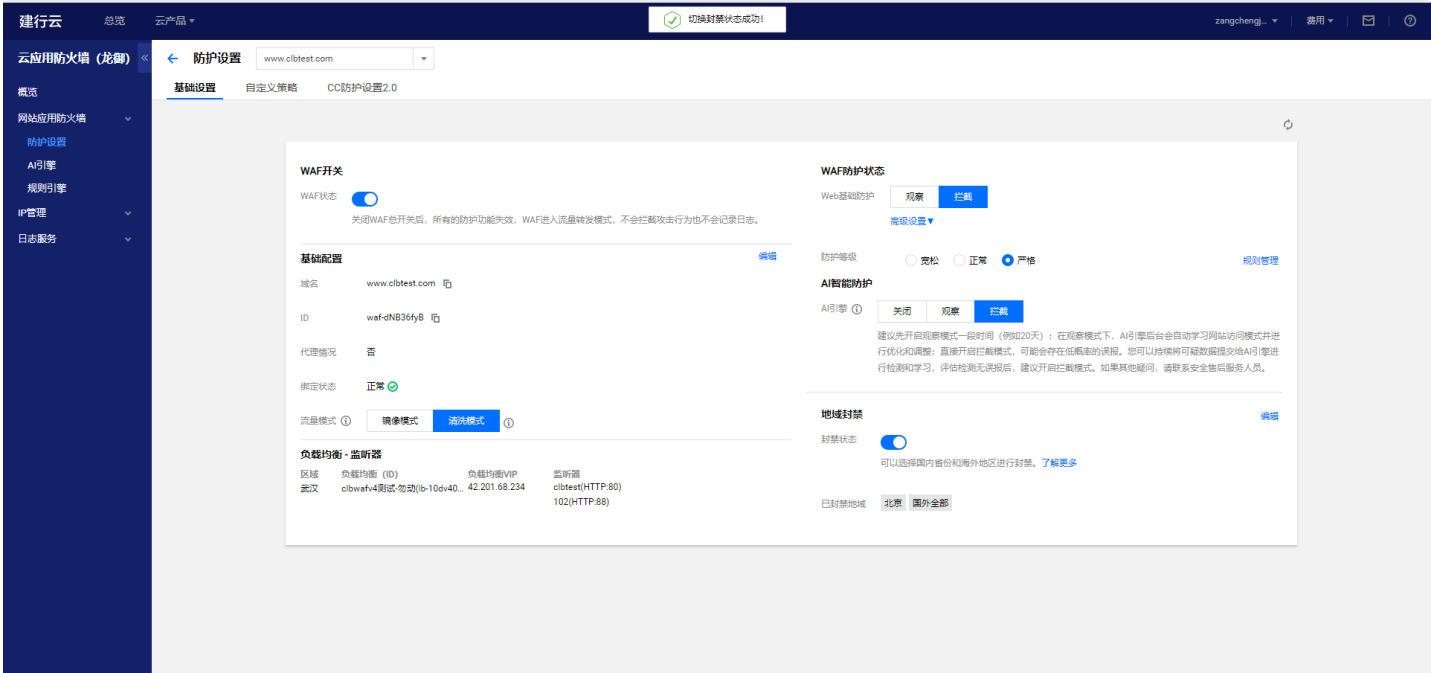
配置说明

最近更新时间: 2023-02-09 16:55:56

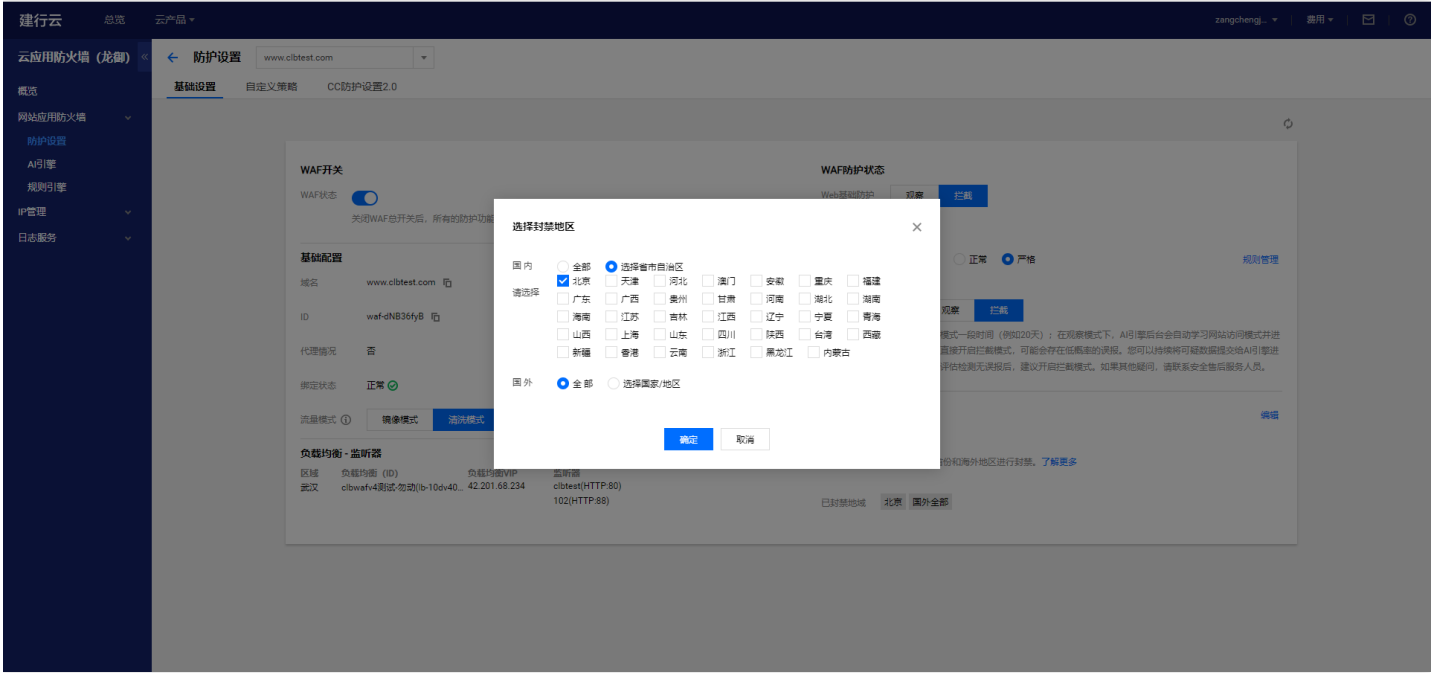
1、登录控制台，单击【网站应用防火墙】>【防护设置】，选择需要防护的域名。



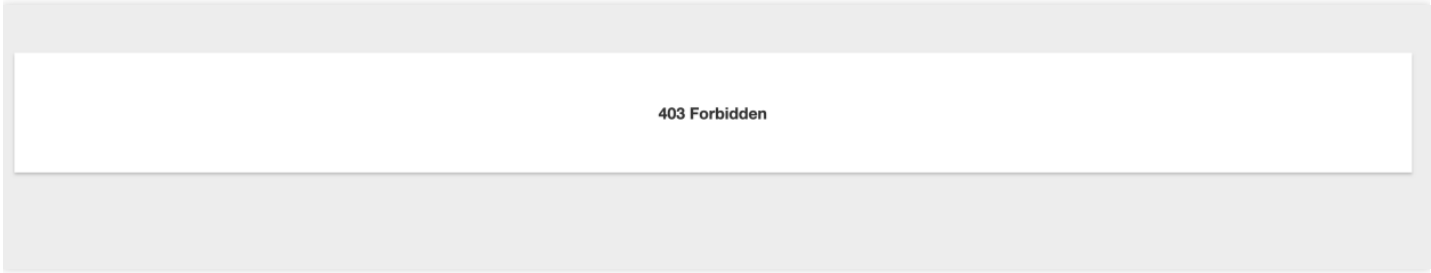
2、单击【基础设置】>【编辑封禁地区】，进入地域封禁配置界面。



3、勾选您要封禁的地区，单击【确定】。



4、此时，您选择封禁的地区将无法访问您的网站。以北京和国外为例，北京和国外被列入封禁地域后，以北京区域的IP 访问网站，云应用防火墙（龙御）会提示403 Forbidden。





自定义策略防护设置

功能简介

最近更新时间: 2023-02-09 16:55:56

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，进行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。



注意事项

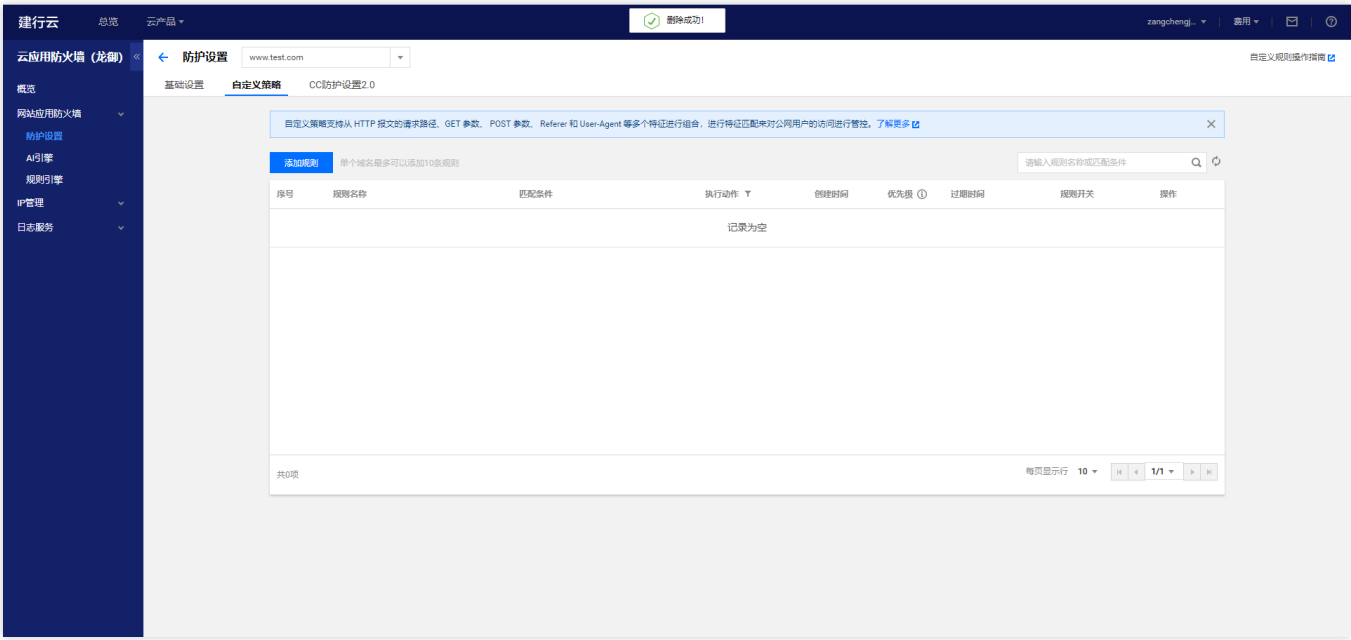
最近更新时间: 2023-02-09 16:55:56

- 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，也就是所有条件全部匹配策略才生效。
- 每个自定义策略匹配之后可以配置多种动作：放行、阻断、人机识别、观察、重定向。
- 如果选择放行模式，应尽量勾选继续执行其他防护，以减小白名单放行带来的风险。
- 如果是临时申请加白策略尽量指定截止时间。
- 自定义放行策略优于自定义阻断策略。

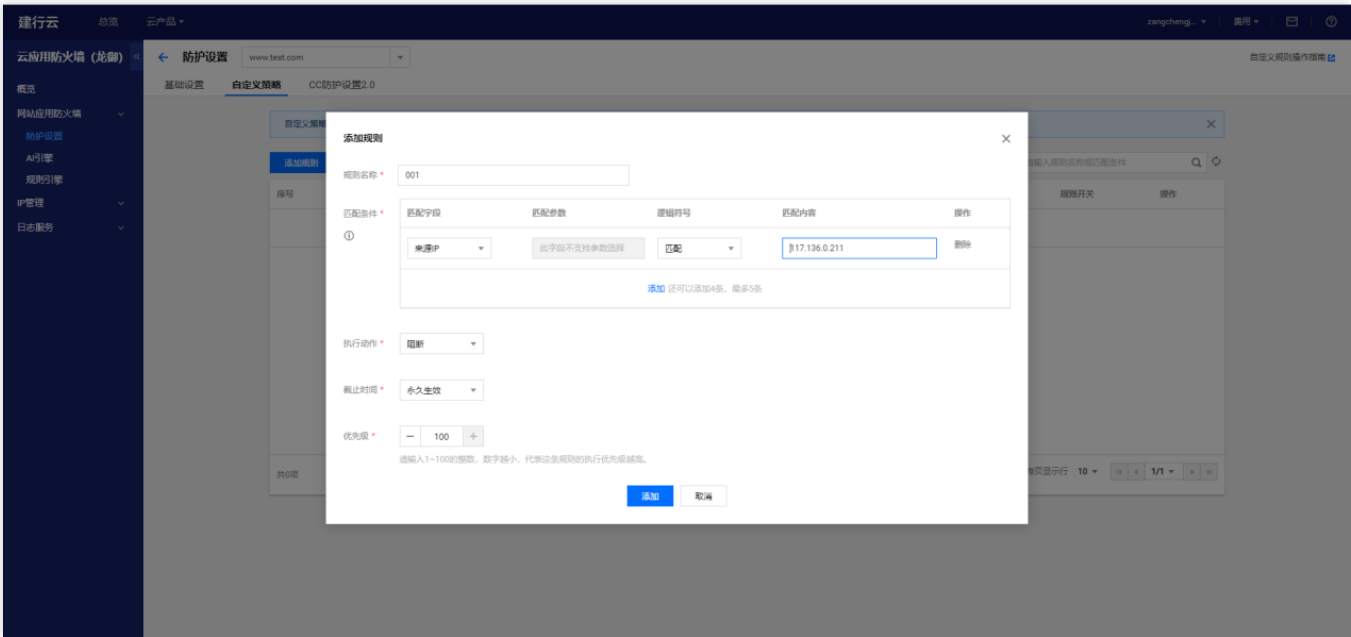
配置说明

最近更新时间: 2023-02-09 16:55:56

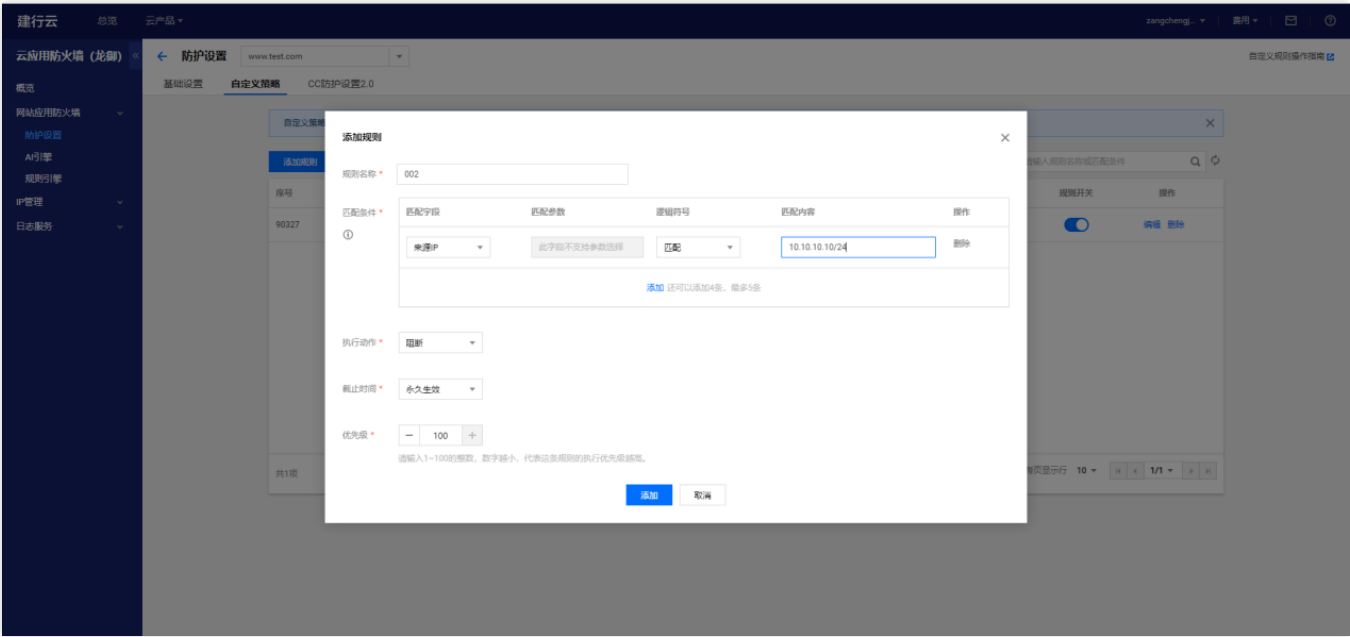
- 案例一：禁止特定 IP 地址访问指定站点
 - 1、登录控制台，单击【网站应用防火墙】>【防护设置】，选择需要防护的站点域名，单击【自定义策略】进入自定义策略配置界面。



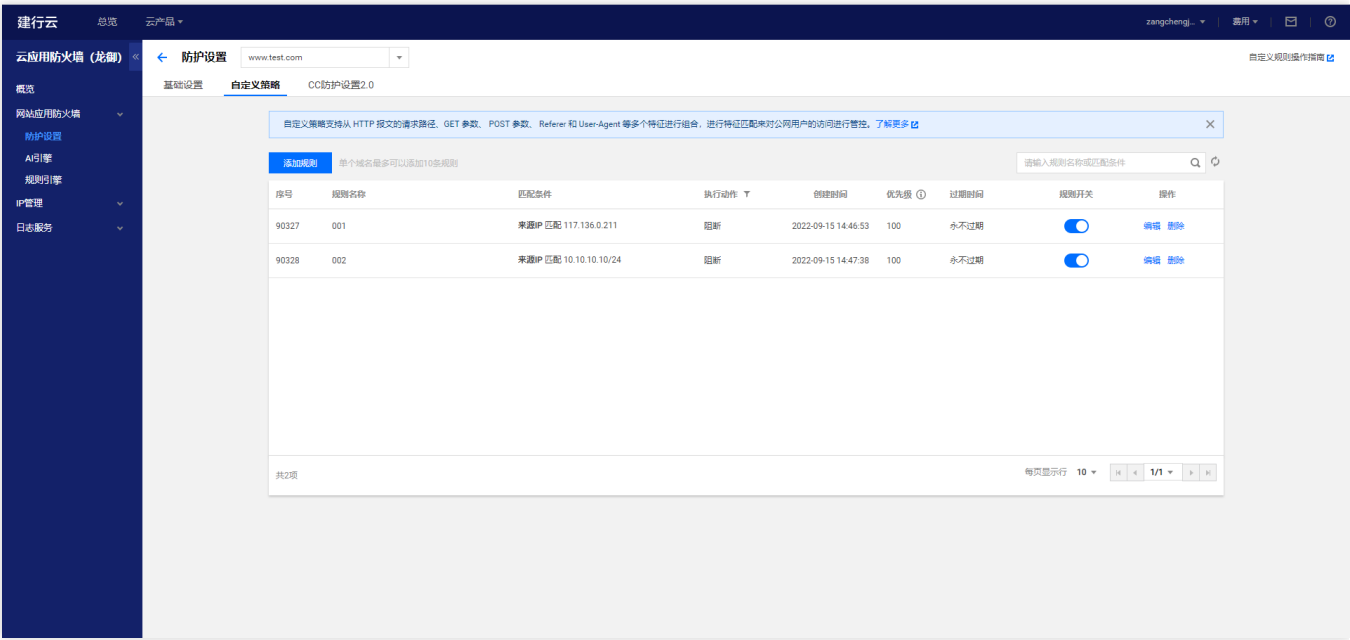
- 2、单击【添加规则】，输入规则名称（如 001），在匹配字段中选择一个字段（如来源 IP），逻辑符号选择匹配，匹配内容填入需要禁止访问的来源 IP（如117.136.0.211），选择执行（如阻断）。



3、同时，云应用防火墙（龙御）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）。



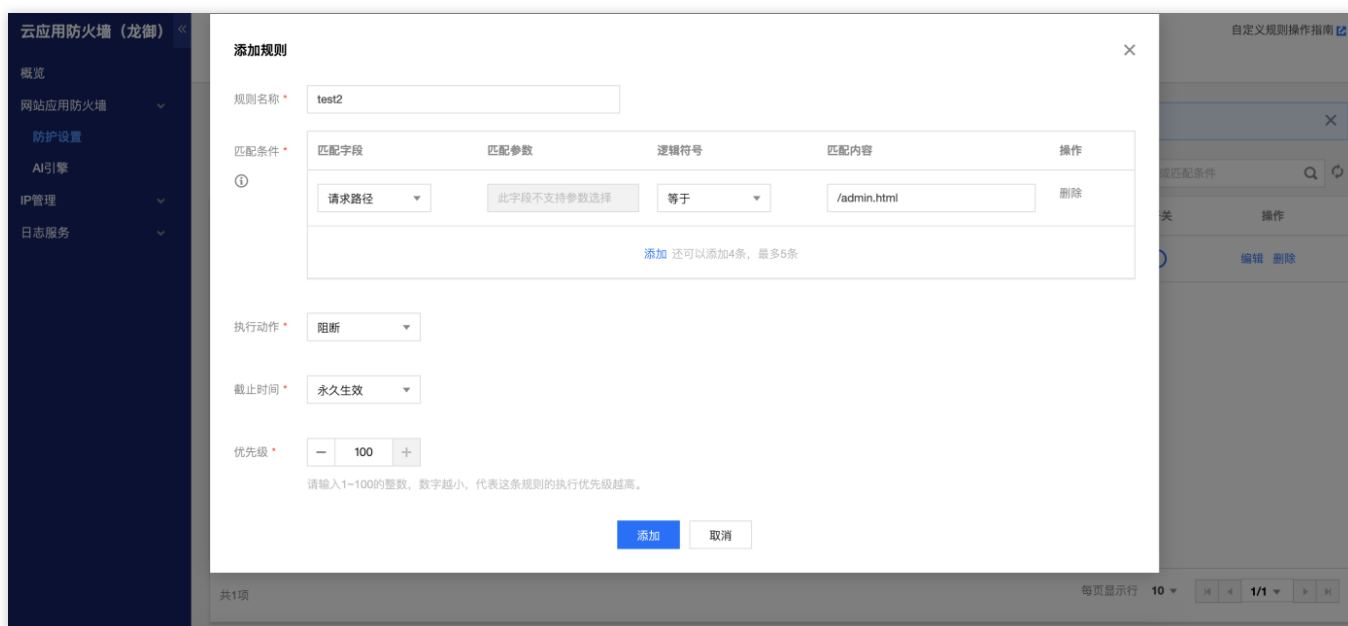
4、单击【确定】保存规则，此时规则将会生效，来自特定源 IP 的 HTTP 访问请求将会全部阻断。



• 案例二：禁止公网用户访问特定的Web资源

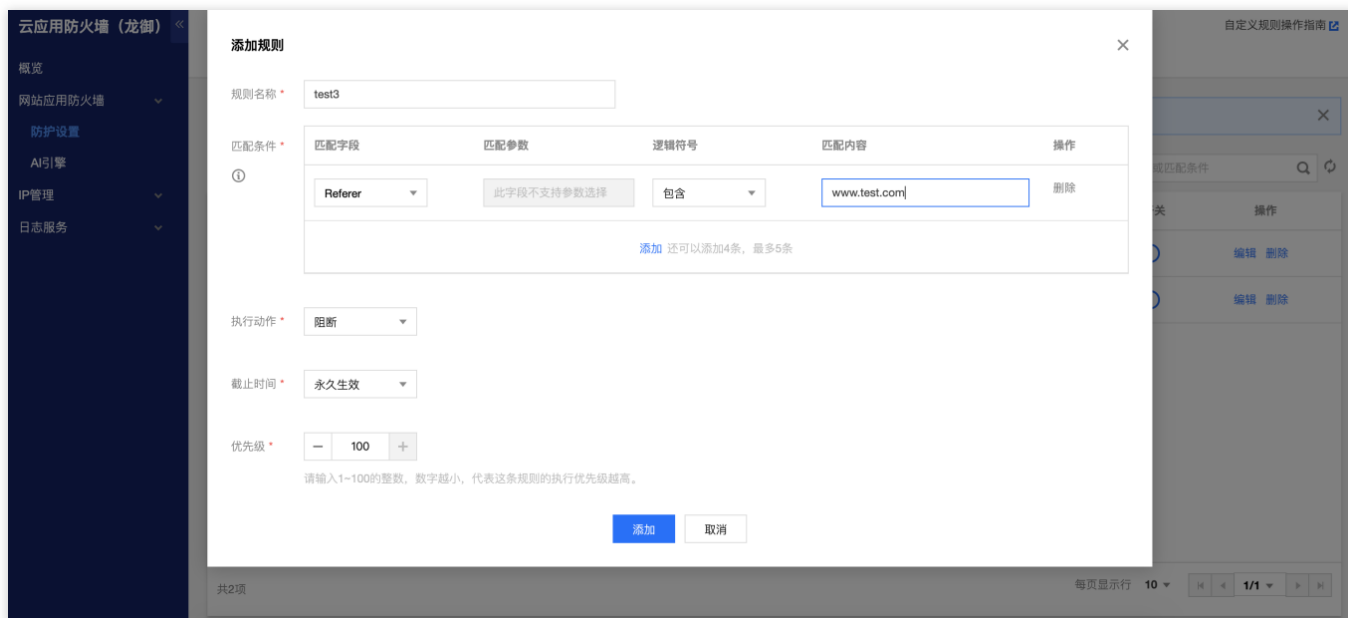
1、当网站管理员不希望公网用户访问某些特定的 Web 资源时（如管理后台/admin.html），可以在匹配字

段中选择请求路径，选择逻辑符号等于，匹配内容输入/admin.html，执行选择阻断进行配置。



- 案例三：禁止某个外部站点盗链获取资源

1、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。在匹配字段中选择 Referer，选择逻辑符号包含，匹配内容输入 www.test.com，执行选择阻断进行配置。





IP黑白名单防护设置

功能简介

最近更新时间: 2023-02-09 16:58:56

IP黑白名单管理，可设置某个域名或者APPID下所有域名的IP黑/白名单规则，只支持IPV4地址。CC防护命中的IP也在IP黑名单中查询到。



注意事项

最近更新时间: 2023-02-09 16:58:56

- 添加IP白名单后，此IP的任何访问都不会被阻断，请谨慎设置。
- IP黑白名单功能不支持添加网段。



配置示例

最近更新时间: 2023-02-09 16:58:56

• 添加网站黑名单

1、登录控制台，单击【网站应用防火墙】>【IP管理】>【IP黑白名单】，选择需要防护的站点域名（如www.test.com），单击【添加黑白名单】进入配置界面。

建行云

总览

云产品

云应用防火墙（龙御）

概览

网站应用防火墙

IP管理

IP黑白名单

IP封堵状态

日志服务

IP黑白名单

www.test.com

操作指南

在这里，您可以将一个或多个IP加入黑/白名单，实现精准的访问控制。需要注意的是：黑白名单的优先级仅低于WAF自定义放行策略，高于其他检测逻辑。
IP黑白名单优先级：全局白名单 > 域名白名单 > 域名黑名单 > 全局黑名单

类别：黑名单

来源：全部

输入IP

高级筛选

查询

添加黑白名单

批量删除

导入数据

导出全部筛选结果

☐	序号	来源	IP地址	类别	更新时间	截止时间	备注	操作
没有记录								

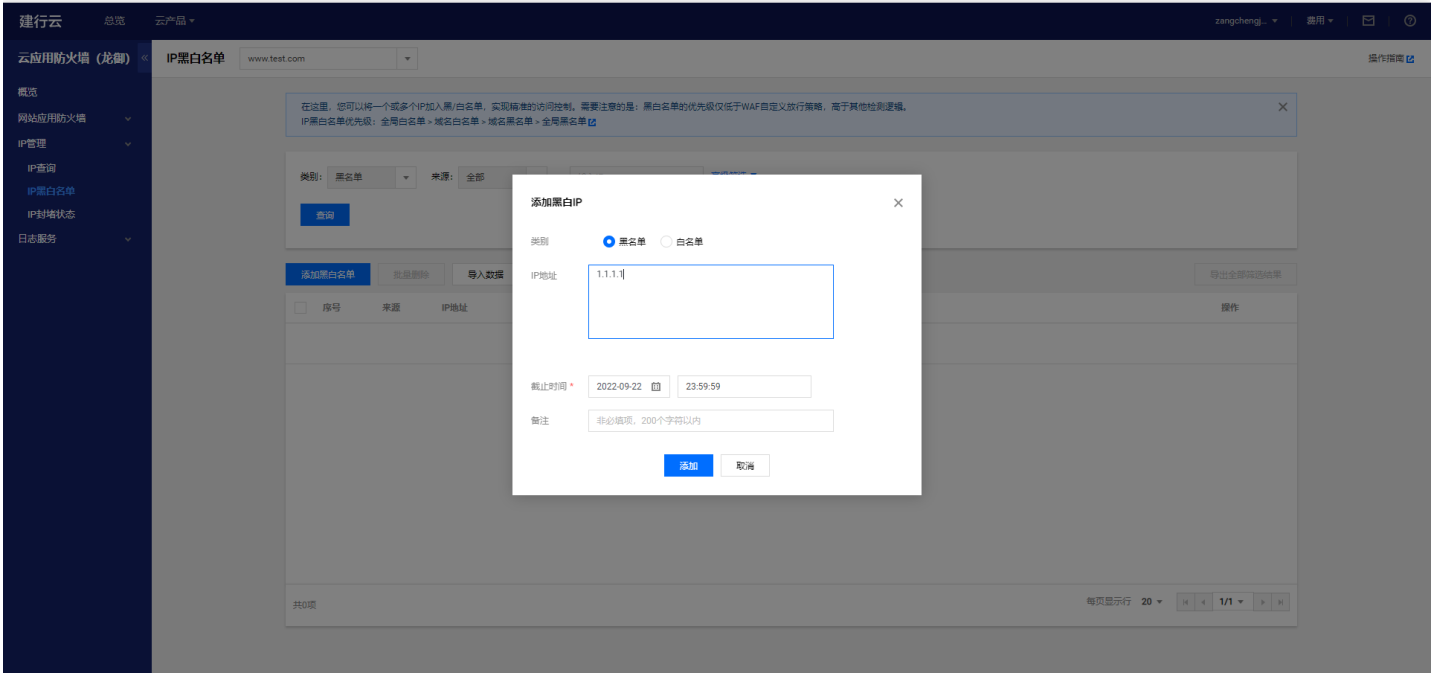
共0项

每页显示行 20

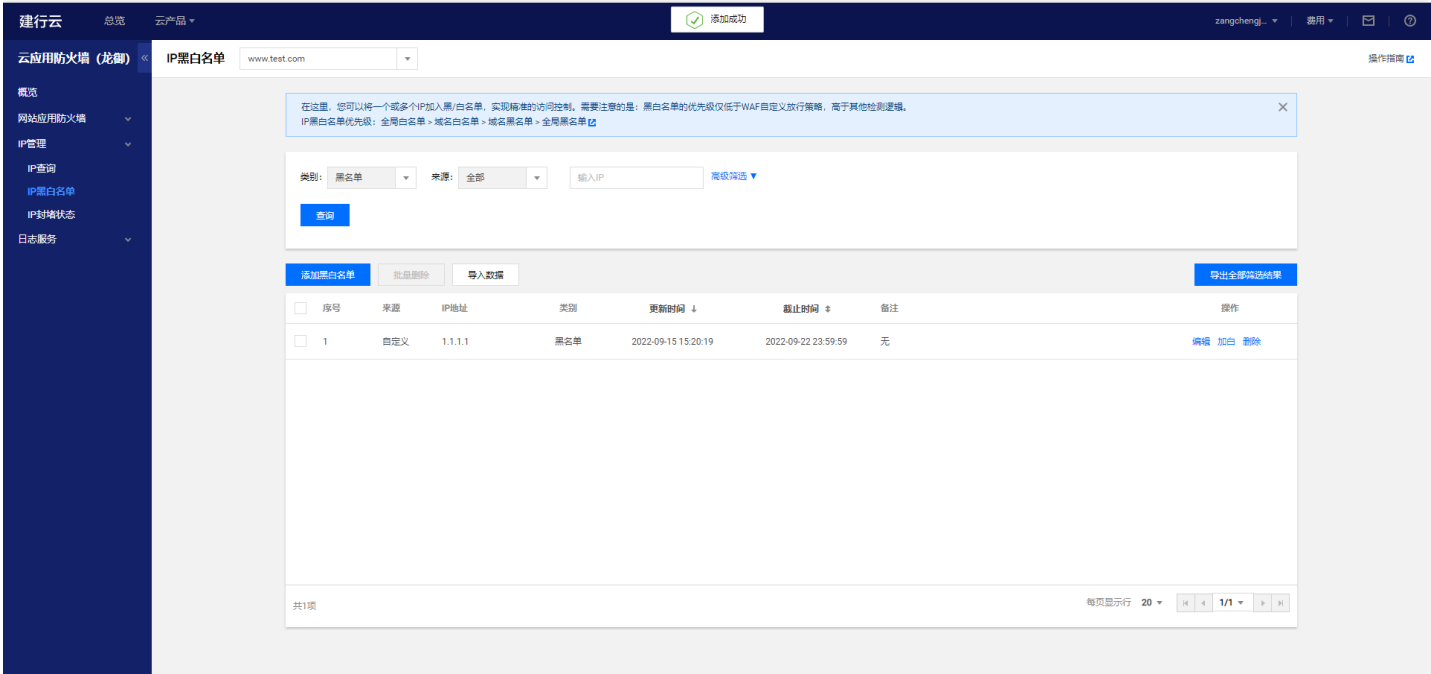
1/1



2、选择【黑名单】，输入IP（1.1.1.1），输入截止时间（2022-09-22 23:59:59）



3、单击【添加】保存规则，此时规则将会生效。此IP访问防护的站点域名（如 www.test.com）的任何页面都会被阻断，提示403 Forbidden。





快速入门

一、添加域名

最近更新时间: 2023-02-09 14:48:19

为了能够让云应用防火墙（龙御）识别需要防护的域名，您需要先在云应用防火墙（龙御）添加域名。下面以防护 www.clbtest.com 为例说明域名添加的步骤。

1、登录控制台，单击导航条【云应用防火墙（龙御）】选项卡，进入云应用防火墙（龙御）控制台。在左侧导航窗格中，单击【防护设置】，进入防护设置页面。

建行云

总览

云产品

云应用防火墙（龙御）

防护设置

域名列表

添加域名

开启

关闭

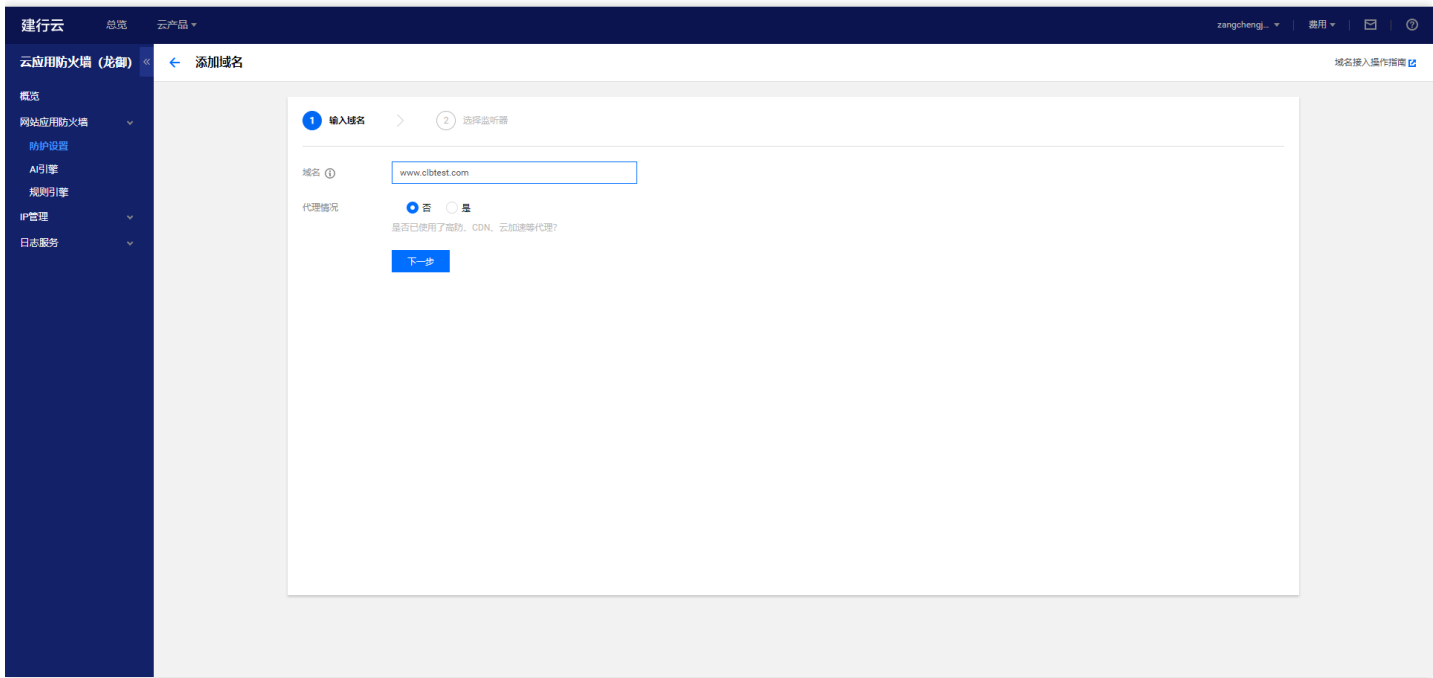
删除

支持域名、负载均衡名称、监听器名称模糊搜索

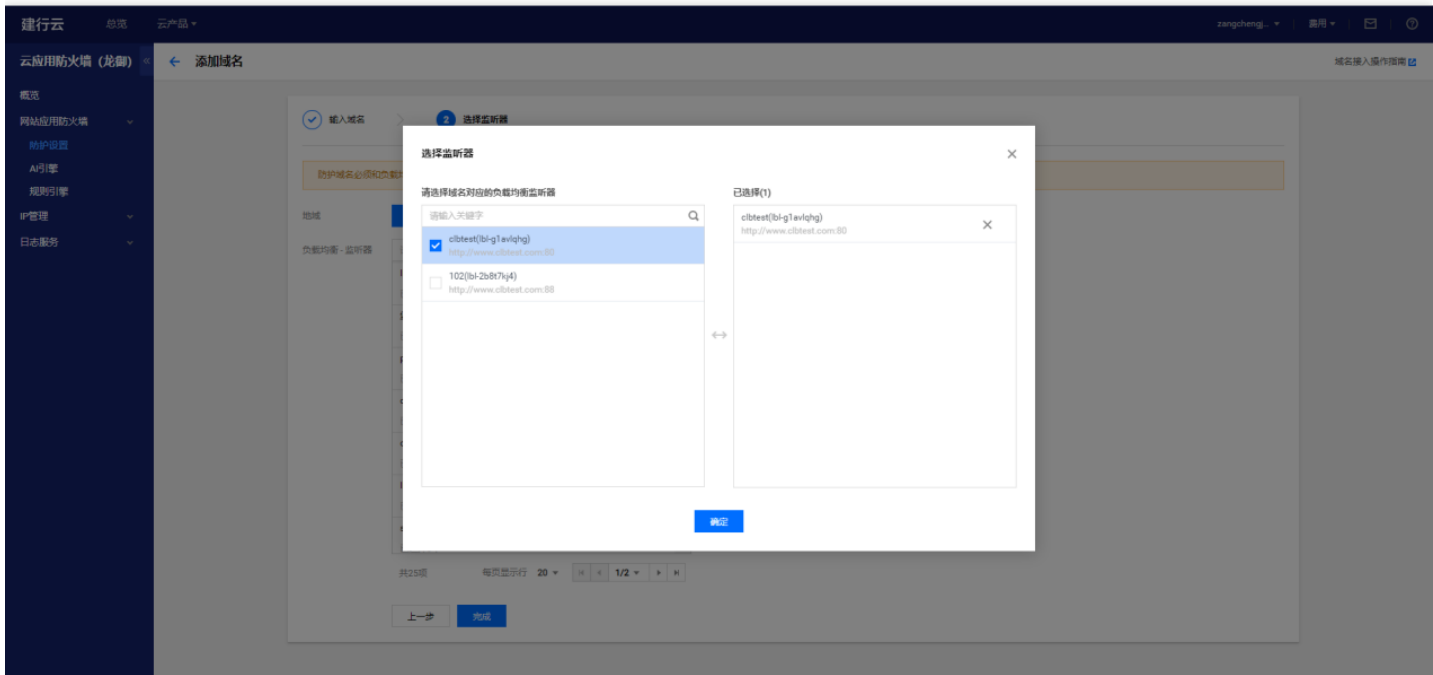
Q

☐ 域名/ID	流量模式①	区域	负载均衡 (ID)	负载均衡VIP①	监听器①	WAF开关	操作
☐ c2h.com waf-875myfg6	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	test-czh(HTTP:8081)		删除 编辑 防护配置
☐ d.com waf-qqAF2iGx	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置
☐ c.com waf-FR8hE3i5	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	test-hwl(HTTP:8001)		删除 编辑 防护配置
☐ a.com waf-GcFCcsR	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	test-cry(HTTP:8002)		删除 编辑 防护配置
☐ bj-1255000011.res.com waf-2MWecRc	清洗模式	武汉	堡垒机测试(b-8irt2va)	2404-bc0:1:1400:0:9 253:b081:6139	堡垒机443(HTTPS:443)		删除 编辑 防护配置
☐ www.csc.com waf-PJQNvJ7z	清洗模式	武汉	新堡垒机测试(b-85dixat8)	119.36.55.232	www.csc.com(HTTP:90)		删除 编辑 防护配置
☐ www.aaa.com waf-oA0qjl5	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置
☐ www.clbtest.com waf-dNB36fyB	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	clbtest(HTTP:80) 102(HTTP:88)		删除 编辑 防护配置
☐ www.ccc.com waf-ofNt1HXX	清洗模式	武汉	clbwafv4测试-勿动(b-10dv40...	42.201.68.234	clbtest(HTTP:80)		删除 编辑 防护配置

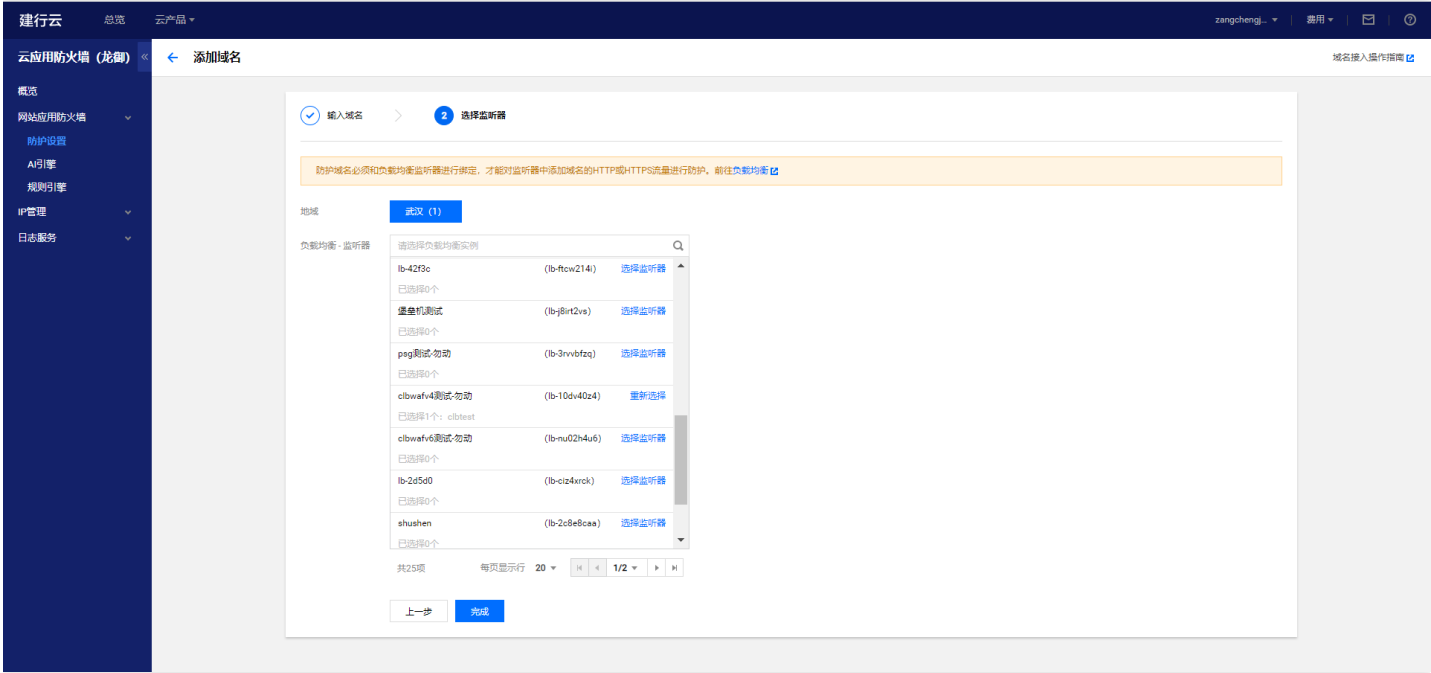
2、单击【添加域名】按钮，弹出添加域名窗口,输入要添加的域名，根据实际情况下选择是否已使用了CDN、高防、云加速等代理（代理模式选择“是”，WAF将通过XFF字段获取客户真实IP作为源地址）， 点击【下一步】验证域名是否已存在。



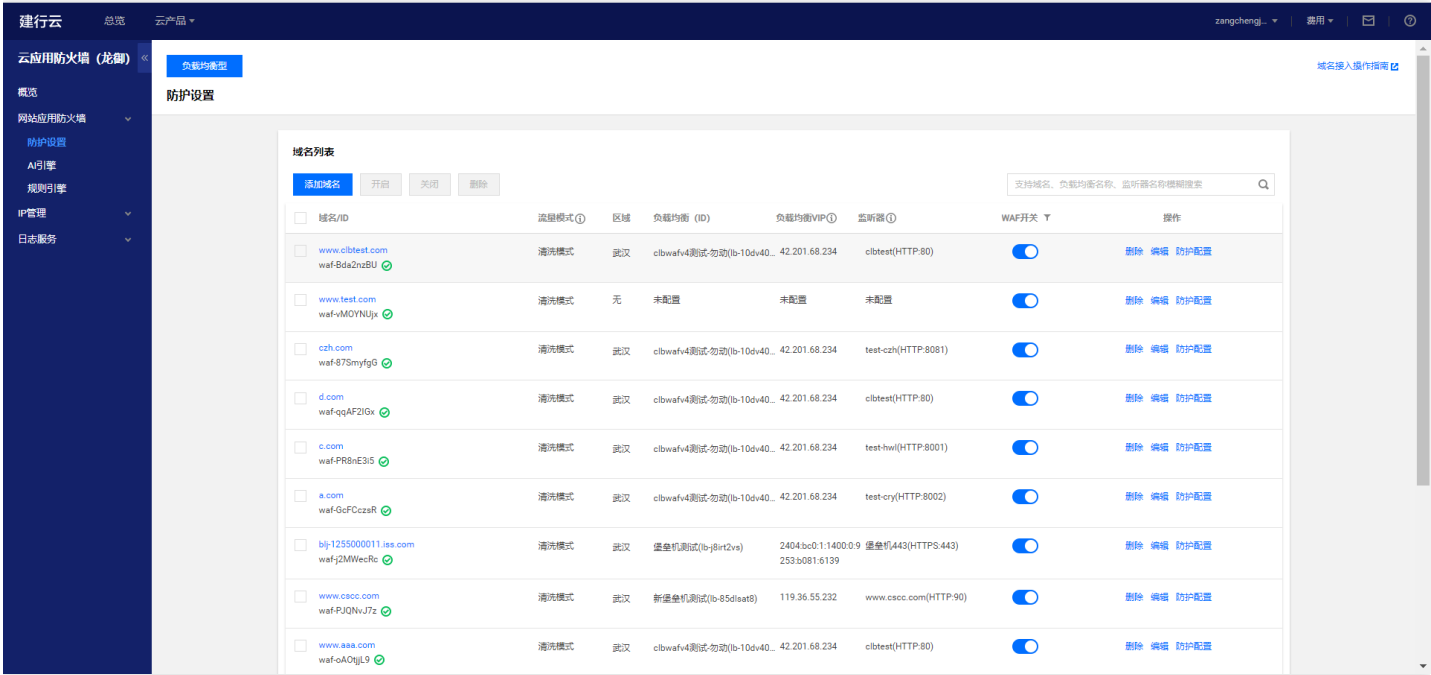
3、再次点击【下一步】按钮，弹出选择监听器界面（注：监听器配置的域名必须与waf添加的域名一致），选中监听器点击【确定】按钮。



4、点击【完成】按钮



5、此时域名 www.clbtest.com 添加完成



6、点击【防护配置】按钮，进行waf防护配置。【流量模式】选择为“清洗模式”，【Web基础防护】选择为“拦截”，高级设置下的【恶意文件检测】设定为“否”，【防护等级】选择为“严格”，【AI引擎】选择为“观察”（在观



察期间，持续对AI告警日志进行分析和学习，评估无误报后，开启拦截模式）

建行云

总览

云产品

云应用防火墙（龙御）

防护设置

www.cibtest.com

基础设置

自定义策略

CC防护设置2.0

WAF开关

WAF状态

关闭WAF总开关后，所有的防护功能失效。WAF进入流量转发模式，不会拦截攻击行为也不会记录日志。

基础配置

域名

www.cibtest.com

ID

waf-8da2nz8U

代理情况

否

绑定状态

正常

流量模式

观察模式

清洗模式

负载均衡 - 监听器

区域

负载均衡 (ID)

负载均衡VIP

监听器

武汉

cibwaf-4测试-包动(lb-10dv40...

42.201.68.234

cibtest(HTTP-80)

WAF防护状态

Web基础防护

观察

拦截

高级设置

防护等级

宽松

正常

严格

规则管理

AI智能防护

AI引擎

关闭

观察

拦截

建议先开启观察模式一段时间（例如20天）；在观察模式下，AI引擎后台会自动学习网站访问模式并进行优化和调整；直接开启拦截模式，可能会存在低概率的误报。您可以持续将可疑数据提交给AI引擎进行检测和学习，评估检测无误报后，建议开启拦截模式。如果其他疑问，请联系安全售后服务人员。

地域封禁

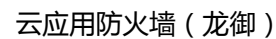
封禁状态

可以选择国内省份和海外地区进行封禁。

已封禁地域

北京

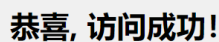
国外全部



最近更新时间: 2023-02-09 14:48:19

本地机器访问网站测试经过waf防护后正常请求页面是否返回正常及攻击请求是否拦截。

一、正确请求测试，通过浏览器访问域名 <http://www.clbtest.com>



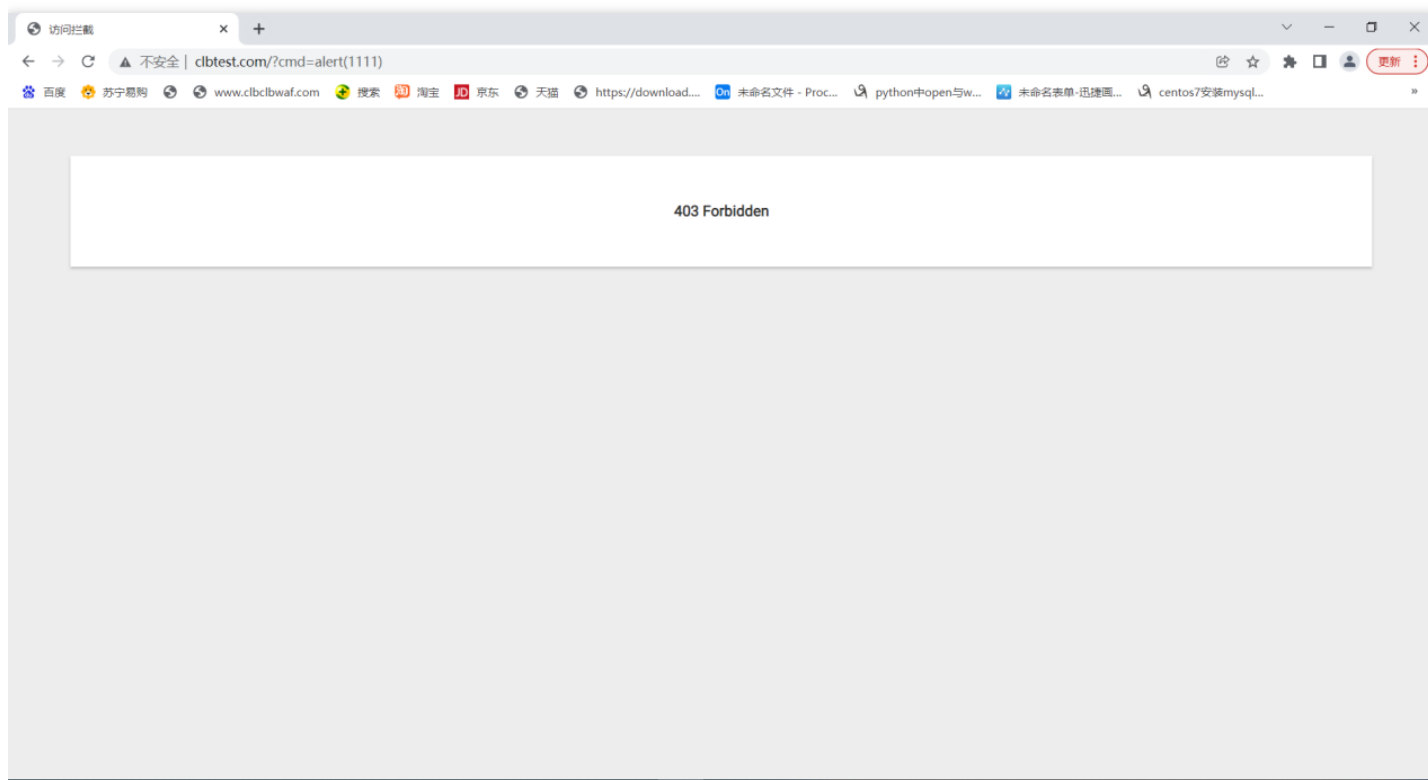
这是默认页

testtttttttttttttttttttttttttttttt

- 您可以修改、删除或覆盖本页面
- 相关信息，请登录控制台查看



二、攻击请求测试,通过浏览器访问域名 [http://www.clbtest.com/?Cmd=alert\(1111\)](http://www.clbtest.com/?Cmd=alert(1111))





常见问题

如何定位是否为龙御WAF拦截

最近更新时间: 2023-02-09 14:52:48

页面内容为“403 Forbidden”“、页面标题为“访问拦截”，页面的源代码包含”waf-empty“

注：客户端请求被拦截后，状态码返回200（CLB型WAF）

如使用CDN的业务，可能会缓存WAF的拦截页面。

```
<!DOCTYPE html>
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <title>访问拦截</title>
  <style>
    @charset "utf-8";body,html{height:100%;min-width:1220px;overflow-x:auto;position:relative;font-size:12px}
    .container{position:absolute;left:-201px;top:48px;right:0;bottom:0;transition:left .3s;transform:translate3d(0,0,0);background:#fff}
    .main{position:absolute;top:0;right:0;bottom:0;left:200px;background-color:#fff;overflow-y:auto;overflow-x:hidden}
    .clearfix:after,.clearfix:before{content:'';display:table}
    .clearfix:after{clear:both}.clr:after{content:'';display:table;clear:both}
    body,button,dd,dl,dt,form,h1,h2,h3,h4,h5,h6,input,legend,li,ol,p,select,table,textarea,ul{margin:0;padding:0}
    body,button,input,select,textarea{font-family:Roboto,San Francisco,"Helvetica Neue",Helvetica,Arial,PingFangSC-Light,"Hiragana Sans GB","WenQuanYi Micro Hei",'microsoft yahei'}
    .tc-g-u-l-l{width:100%}
    a.disabled{color:#bbb !important;cursor:default !important;text-decoration:none !important}
    .container{transform:none !important}
    .manage-area{padding-left:0 !important;padding-right:0 !important}.manage-area .manage-area-title{padding-left:20px !important;padding-right:20px !important;margin-left:0 !important}
    .waf-empty{max-width:1360px;margin-left:auto;margin-right:auto;padding:50px 20px;background-color:#fff;box-shadow:0 2px 3px 0 rgba(0,0,0,.2)}.waf-empty .console-empty{display:
  </style>
</body>
<div id="jsContainer" class="container" style="top:0;">
  <div class="main">
    <div class="manage-area">
      <div class="manage-area-main" style="margin-top: 50px;">
        <div class="attack-detail">
          <div class="tc-g">
            <div class="tc-g-u-l-l">
              <div class="waf-empty">
                <div class="console-empty">
                  <div class="empty-text">
                    <div><strong>403 Forbidden</strong></div>
                  </div>
                </div>
              </div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
  <!-- contain end -->
</div>
<!-- main end -->
</div>
</body>
</html>
```



如何分析拦截原因

最近更新时间: 2023-02-09 14:52:48

提供信息：域名、客户端IP、故障时间、URL、返回的页面内容

1、登录租户控制台，选择云产品-云应用防火墙（龙御）-日志服务-攻击日志

2、选择域名、时间段，输入客户端IP，点击查询

3、查看是否存在执行动作为拦截的攻击日志，根据具体的攻击类型+策略ID+策略名称分析具体原因

攻击类型为自定义策略（规则ID非0）、地域封禁拦截、IP黑白名单、CC策略拦截，则租户自行分析判断

攻击类型为AI引擎检出，租户需与安全处一起分析判断是否进行在线学习

其他攻击类型，租户需与安全处一起分析判断是否为正常拦截，是否可以添加白名单规则

建行云

总览

云产品

云应用防火墙（龙御）

攻击日志

日志查询

a.com

近1小时

近6小时

今天

昨天

近7天

2021-06-15 15:48:50 至 2021-06-15 23:59:59

全部风险等级

全部执行动作

全部攻击类型

输入策略ID

输入攻击源IP

查询

总数量: 0项

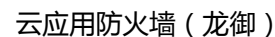
序号	被攻击网址	攻击源IP	攻击类型	策略ID ①	策略名称	攻击内容	攻击时间	执行动作	风险等级	操作
没有记录										



日常运营中如何进行误拦截处置

最近更新时间: 2023-02-09 14:52:48

- 1、排查客户IP地址是否已触发天幕联动封禁，如需解封客户IP可联系一线值班处理；
- 2、确认WAF拦截的告警类型，告警日志中的攻击类型字段包含规则引擎17种告警类型、AI引擎拦截、自定义策略、IP黑名单和CC拦截，对于不同类型告警需做不同处置；
- 3、对于规则引擎拦截，应急处置可通过告警日志获取触发的规则编号，关闭该条规则开关；后续根据规则编号查看规则内容及CVE信息等，根据攻击内容判断属于开发不合规问题还是误报，对于不合规情形需应用整改，对于误报可设置规则白名单；
- 4、对于AI引擎拦截，应急处置可将AI引擎切换为观察模式；分析引擎拦截原因，进行应用改造或AI模型学习或设置自定义放行策略不再勾选“继续执行AI引擎防护”等后续处置；
- 5、对于其他自定义类型拦截，需根据自身配置规则进行排查，关闭、删除或修改配置规则。



最近更新时间: 2023-02-09 14:52:48

1、在攻击日志中找到AI拦截的攻击内容，将攻击内容在AI在线验证界面进行验证。验证为威胁数据后，将威胁数据人工拆分成几段，分别验证，直到找打最小的威胁数据。

2、点击AI误报学习，手动添加威胁数据。

3、选中误报数据，点击学习。学习后再次进行AI在线验证，验证正常。

行云	总览	云产品		zhangcheng...	费用			
云应用防火墙（龙御）	请求方法	POST	风险等级	高危	运营商	联通	纬度	39.938884
概览	攻击时间	2021-06-15 16:49:08	匹配来源	其他				
网站应用防火墙	请求UUID	1c58388288142dc27772a4387d04e8a6-21cd641cd87	执行动作	拦截				
IP管理	请求URI	/operator/server/checkrule						
日志服务	攻击内容	#!/bin/bash\n#####\n#####author wen.lu@tendcloud.com\n#####\n#####\n#####parameters: Cdr\nom_name_dir Ks_name_dir Tmp_dir Mount_dir\n\nin\nauto_cd()\n\nin\nCdrom_name_dir=/home/remotecard/RHEL6_4_X86_64_Autoinstall_DVD_date +%Y%m%d\niso\n\nSource_file=/home/remotecard/rhel-server-6.4-x86_64-dvd.iso\n\nKs_name_dir=ks.cfg\n\nTmp_dir=/tmp/rhel6_4\n\nLabel=RHEL6_4_X86_64_Autoinstall_DVD\n\nMount_dir=/mnt\n\nif [-d \${Tmp_dir}]\n\nthen\n\necho " Tmp_dir is exists"\n\nelse\n\nmkdir \${Tmp_dir}\n\n&> /dev/null\n\nfi\n\nmount \${Source_file} -o loop \${Mount_dir}\n\n&> /dev/null\n\ncp -a \${Mount_dir}/\${Tmp_dir}/\n\n\${Tmp_dir}/\n\n####create file isolinux.cfg\n\nmv \${Tmp_dir}/isolinux/isolinux.cfg /isolinux.cfg.bak\n\n&> /dev/null\n\nncat << EOF >> \${Tmp_dir}/isolinux/isolinux.cfg\n\ndefault install\n\nprompt 1\n\n#timeout 600\n\n#timeout 30\n\n\n#display boot.msg\n\n#f1 b oot.msg\n\n#F2 options.msg\n\n#F3 general.msg\n\n#F4 param.msg\n\n#F5 rescue.msg\n\n\nlabel install\n\nkernel vmlinuz\n\nappend ks=cdr\n\n#ks.cfg\n\ninitrd=initrd.img\n\n\nlabel linux\n\nmenu label ^Install or upgrade an existing system\n\nmenu default\n\nlinux\n\nkernel vmlinuz\n\nappend initrd=initrd.img\n\n\nlabel vesalabel\n\nmenu label Install system with "basic video driver"\n\nkernel vmlinuz\n\nappend initrd=initrd.img\n\nxdriver=vesa\n\nnomodeset\n\n\nlabel rescue\n\nmenu label ^Rescue installed system\n\nkernel vmlinuz\n\nappend initrd=initrd.img\n\nrescue\n\n\nlabel local\n\nmenu label Boot from "local drive"\n\nlocalboot 0xffff\n\n\nlabel memtest86\n\nmenu label ^Memory test\n\nkernel memtest\n\nappend -\n\n\nEOF\n\n\numount \${Mount_dir}\n\n\nrm cp \${Ks_name_dir} \${Tmp_dir}\n\n\nrm cd \${Tmp_dir}\n\n\nfind -ty pe f -name "TRANS.TBL" xargs rm -fr\n\n\nrm -rf isolinux/boot.cat\n\n\nrm chmod +w isolinux"\n\n&> /dev/null\n\nfi						
添加误报	添加误报							



如何添加自定义放行规则

最近更新时间: 2023-02-09 14:55:27

- 1、登录租户控制台，选择云产品-云应用防火墙（龙御）-防护设置，点击域名，选择“防护配置”
- 2、选择自定义规则，点击“添加规则”，输入匹配条件，执行动作选择放行，并勾选继续执行剩余的检测防护，设置截止时间

添加规则

规则名称 *

请输入名称，最长50个字符

匹配条件 *

匹配字段

匹配参数

逻辑符号

匹配内容

操作

来源IP

此字段不支持参数选择

匹配

1.1.1.1

删除

添加

还可以添加4条，最多5条

执行动作 *

放行

放行规则优先于其他匹配操作执行

☒ 继续执行地域封禁防护

☒ 继续执行CC策略防护

☒ 继续执行WEB应用防护

☒ 继续执行AI引擎防护

☒ 继续执行信息防泄漏防护

截止时间 *

限定日期

2021-06-15

优先级 *

-

100

+

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。

添加

取消



CLB型WAF域名访问故障时如何应急

最近更新时间: 2023-02-09 14:55:27

- 1、关闭部分防护功能，包含AI引擎防护、WEB基础防护、恶意文件检测、流量模式
- 2、切换流量模式为镜像模式
- 3、关闭WAF防护
- 4、删除CLB型WAF的防护配置（应急后需恢复）

← 防护设置

www.d1.com

基础设置

自定义策略

CC防护设置2.0

WAF开关

WAF状态

☐

关闭WAF总开关后，所有的防护功能失效，WAF进入流量转发模式，不会拦截攻击行为也不会记录日志。

基础配置

编辑

域名

www.d1.com

ID

waf-ZxtlDhvk

代理情况

否

绑定状态

正常

流量模式

①

镜像模式

清洗模式

①

负载均衡 - 监听器

区域	负载均衡 (ID)	负载均衡VIP	监听器
武汉	clbwafv4测试-勿动(lb-10dv4...	42.201.68.234	100(HTTP:100)

WAF防护状态

Web基础防护

观察

拦截

高级设置

▲

恶意文件检测

☒ 否

☐ 是

防护等级

☒ 宽松

☐ 正常

☐ 严格

规则管理

AI智能防护

AI引擎

①

关闭

观察

拦截

建议先开启观察模式一段时间（例如20天）；在观察模式下，AI引擎后台会自动学习网站访问模式并进行优化和调整；直接开启拦截模式，可能会存在低概率的误报。您可以持续将可疑数据提交给AI引擎进行检测和学习，评估检测无误报后，建议开启拦截模式。如果其他疑问，请联系安全售后服务人员。

地域封禁

编辑

封禁状态

☐

可以选择国内省份和海外地区进行封禁。[了解更多](#)

已封禁地域

国内全部

国外全部

版权所有：建行云

第48 页 共49页



龙御WAF中各类自定义配置的优先级是什么

最近更新时间: 2023-02-09 14:55:27

全局IP白名单>域名IP白名单>域名IP黑名单>全局IP黑名单>自定义策略放行规则>CC策略>地域封禁>自定义策略拦截规则