Web 应用防火墙（边缘云版）

用户使用指南

天翼云科技有限公司

目 录

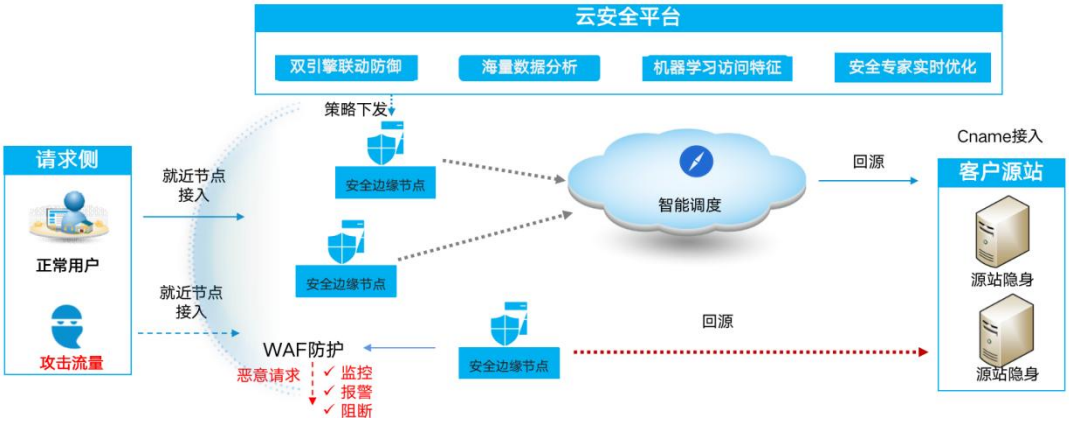
1.产品定义

Web 应用防火墙（边缘云版）依托天翼云的云安全节点形成云安全网络，结合云端大数据分析平台，为用户提供应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫、域名劫持等网站及 Web 业务安全防护问题，从而保障网站安全。

区别于传统 WAF 需要在源站前端部署，Web 应用防火墙把安全能力赋能在所有边缘节点；

利用分布式节点部署使计算能力更强，有效降低源站计算压力，提升了用户访问质量的同时保护了源站数据的安全；

安全加速基本架构：



2.操作指导

2.1 购买 web 应用防火墙（边缘云版）

2.1.1 订购

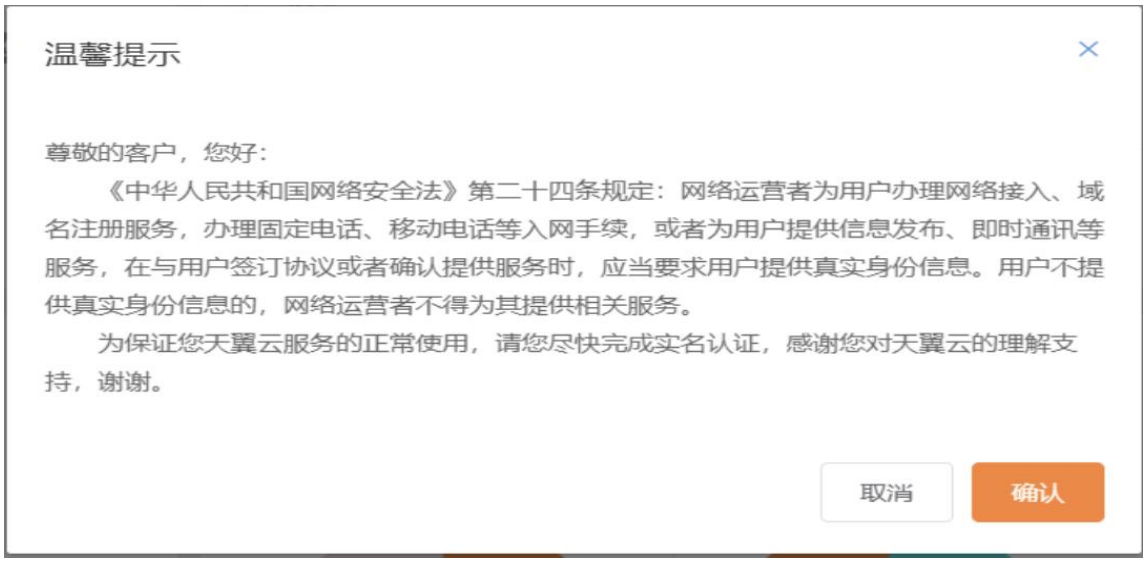
开通步骤如下：

步骤 1、注册并登录天翼云 http://www.ctyun.cn

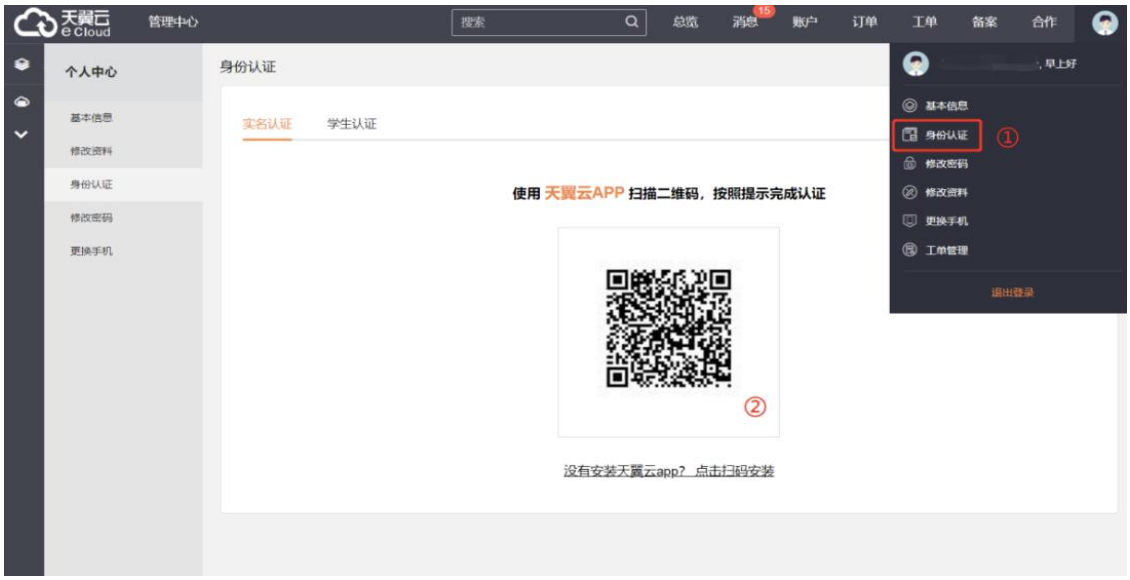
2-1 天翼云官网登录页面

步骤 2、未实名认证的用户请按提示完成实名认证才能开通服务

2-2 实名认证提醒

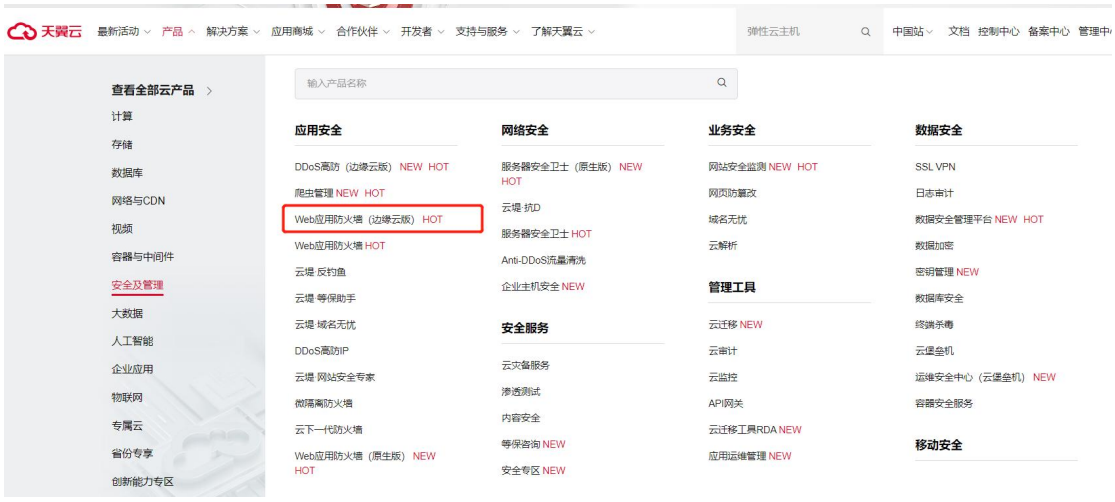


2-3 完成实名认证



步骤 3、实名认证后进入 Web 应用防火墙（边缘云版）产品详情页快速了解产品，之后单击【立即开通】；

2-4 产品详情页



步骤 4、在购买页面选择适合的套餐和扩展服务，勾选并阅读服务协议，确认无误后点击“立即开通”，web 应用防火墙（边缘云版）服务即开通；

2-5 产品开通页

步骤 5、web 应用防火墙（边缘云版）服务开通后，便可以根据操作手册去控制台开始接入您要防护的域名。

2.1.2 续费

支持续订操作，登录官网订单管理-产品-产品视图-产品续订，提交您的续订需求，续订规则详见如下链接：

https://www.ctyun.cn/document/10000038/10303747

2.1.3 变更

您如果有变更套餐的需求，您可以登录天翼云官网，在订单管理-产品中找到您的订单，点击“订购”提交您的变更需求。目前套餐变更只支持升级套餐，不支持降级套餐的操作。

2.1.3 退订

产品支持退订服务，登录官网-订单管理-产品-产品视图-退订管理，找到您要退订的订单，进行退订；客户套餐退订后，扩展服务也会一起退订

产品退订页面

2.2 域名管理

2.2.1 新增域名

简介

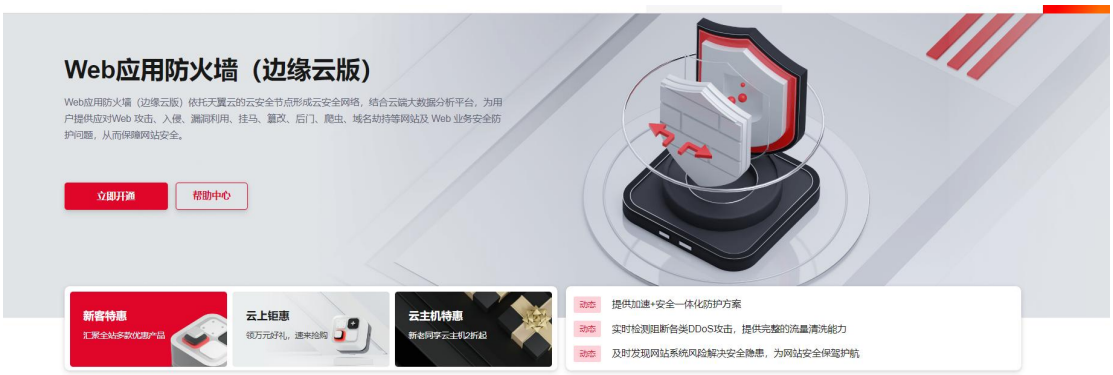
使用 WAF 服务前，需要先将网站接入到 WAF 服务。未完成接入前，您的安全防护功能将无法生效。本文档将指导您如何在控制台中接入域名。

操作步骤

步骤一：进入 web 应用防火墙（边缘云版）控制台

1、打开天翼云官网 http://www.ctyun.cn，注册并登录；

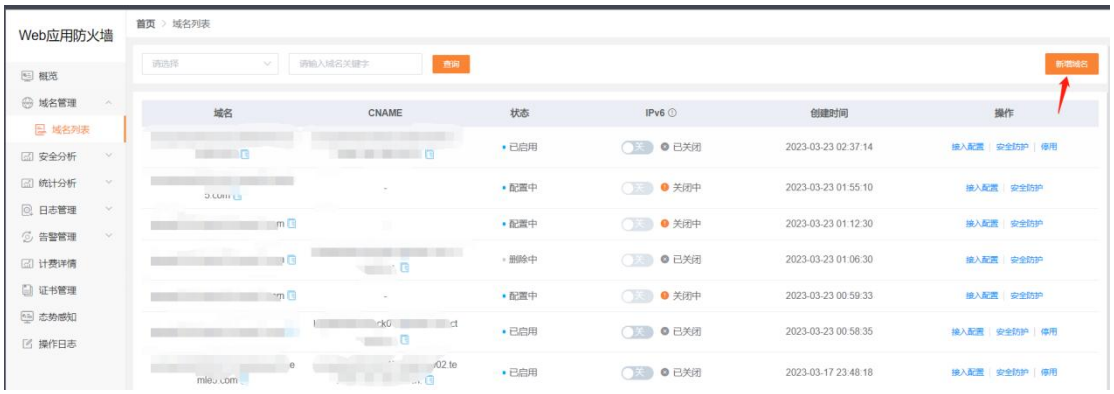
2、选择控制中心；



3、下拉选择安全，点击对应的 web 应用防火墙（边缘云版）进入客户控制台；

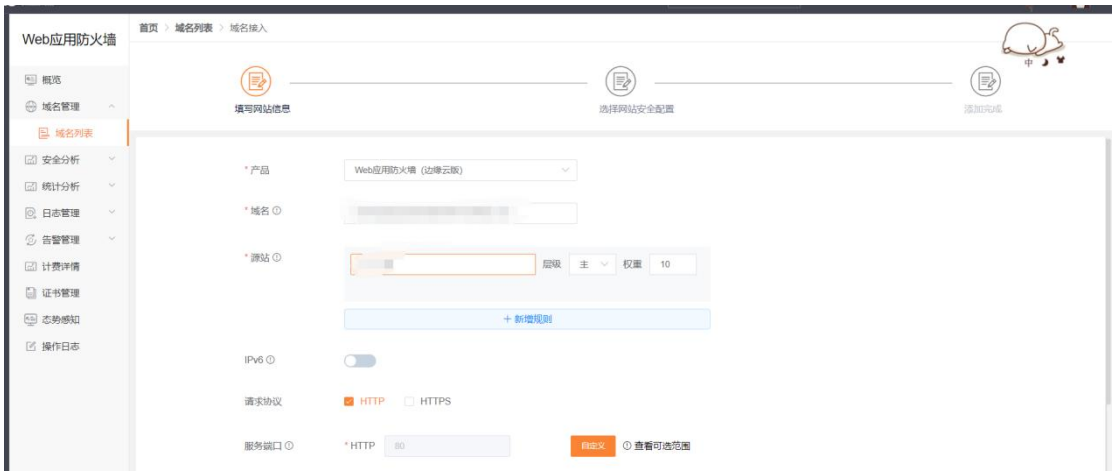
步骤二：添加域名

1、选择域名管理—域名列表，点击【添加域名】；



2、填写网站信息，

根据页面的引导填写域名的基本信息和源站设置；



配置项说明：

- 域名：填写需要接入 WAF 的域名；域名会进行域名归属权校验，

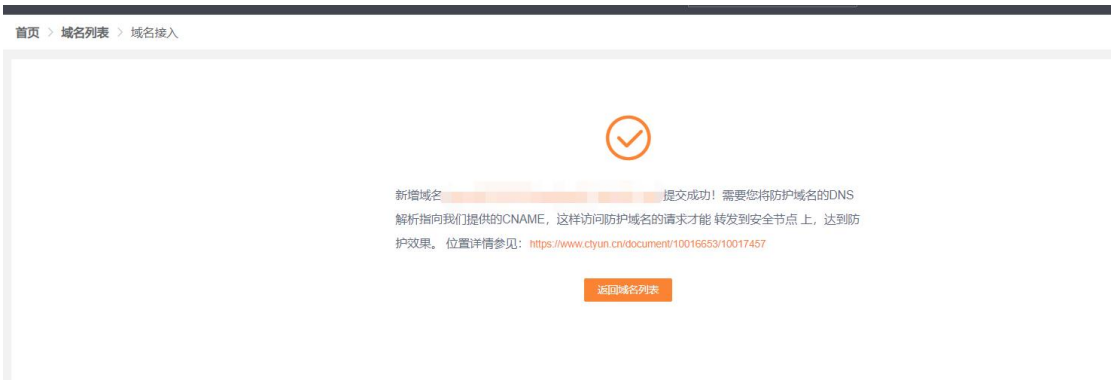
- 源站：支持 IP 或域名，最多可添加 60 个；
- IPv6 开关：开启 IPv6,开启后完成 IPV6 改造，如果要解决 ipv6 天窗问题（提升二、三级链接 ipv6 支持度），需要提交工单联系运营配置外链改造；
- 请求协议：支持选择 HTTP 和 HTTPS；
- 服务端口：默认端口为 80，如果有特殊端口需求，需要点击【自定义】，只有专业版和旗舰版支持配置特殊端口；
- 回源协议：目前仅 HTTP 协议回源支持自定义端口，HTTPS 协议回源使用 443 端口，跟随请求协议回源将根据请求指定的协议回源到您源站的 80 或 443 端口
- HTTP 源站端口：HTTP 默认端口为 80 端口，HTTPS 默认端口为 443 端口，也可以自定义端口；
- 回源 HOST：回源 host 决定了回源请求访问到源站的哪个站点，自定义配置时，请确保您的源站有配置相应的 HOST。如果源站是 IP 类型，回源 host 默认加速域名；如果

源站是域名类型，回源 host 默认是源站域名；

3，填写网站安全配置

完成网站配置后，单击【下一步】，根据配置指引，完成安全防护配置。

填写完安全配置后，单击【提交】，出现添加完成页面；

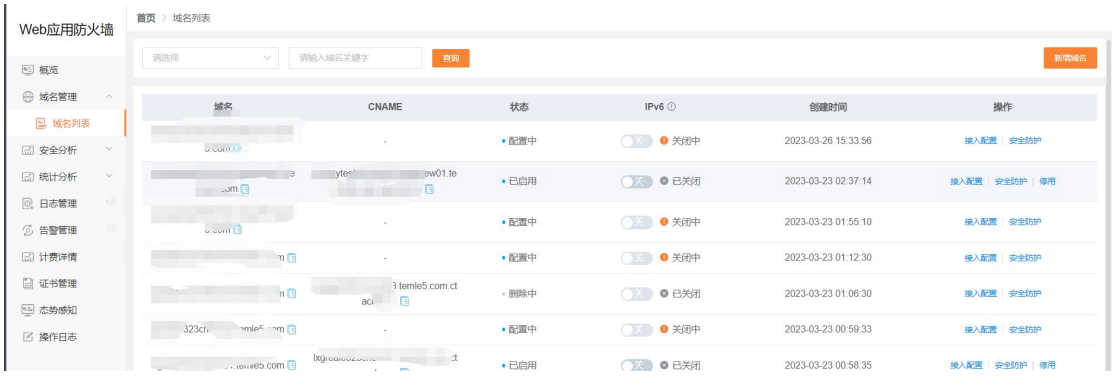


完成新增域名操作后，可通过【域名列表】查看该域名配置是否完成，通过域名的状态字段判断；

当域名状态为“配置中”时，表示域名配置没有完成，正在配置流转中。

当域名状态为“已启用”时，表示域名配置已经完成，您可以通过域名列表中提供的 CNAME 进行域名解析，接入 WAF 服务。

域名列表页



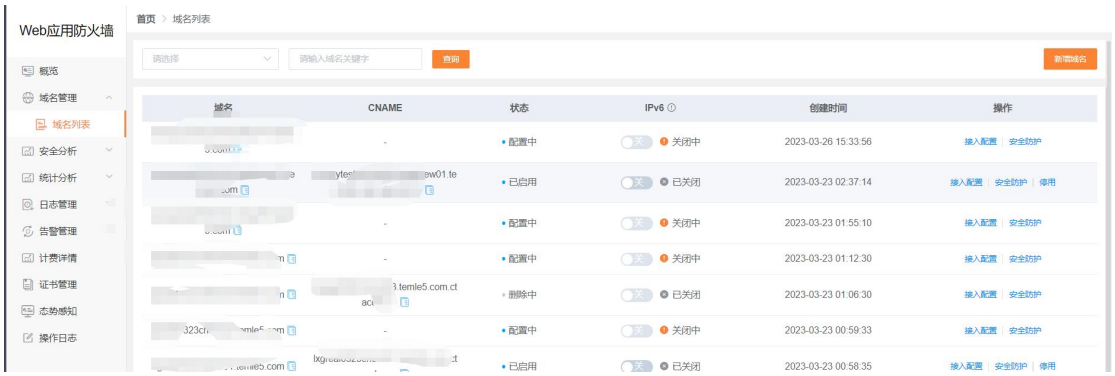
域名配置完成，生成域名 CNAME，域名状态变更为【已启用】

步骤三：配置 came

要启用 WAF 服务，需要您将防护域名的 DNS 解析指向我们提供的 CNAME，这样访问防护域名的请求才能转发到安全节点上，达到防护效果。

1、在控制台【域名管理】的域名列表中复制接入域名对应的 CNAME；

域名列表-复制 CNAME 页



2、前往您的域名解析(DNS)服务商(如阿里云解析（原万网）、腾讯云解析（原 DNSPod）、新网等)，添加该 CNAME 记录。下面以您的域名在新网为例，其他域名解析服务商请联系对应厂商技术支持处理。

3、登录新网的域名解析控制台，进入对应域名的域名解析页；

4、选择【添加新的别名】；

添加别名页

【记录类型】选择为 CNAME；

【主机记录】即域名的前缀。例如，要添加 testlive.ctyun.cn，前缀就是 testlive；

【记录值】填写为您复制的 CNAME 值；

解析线路和 TTL 默认值即可。

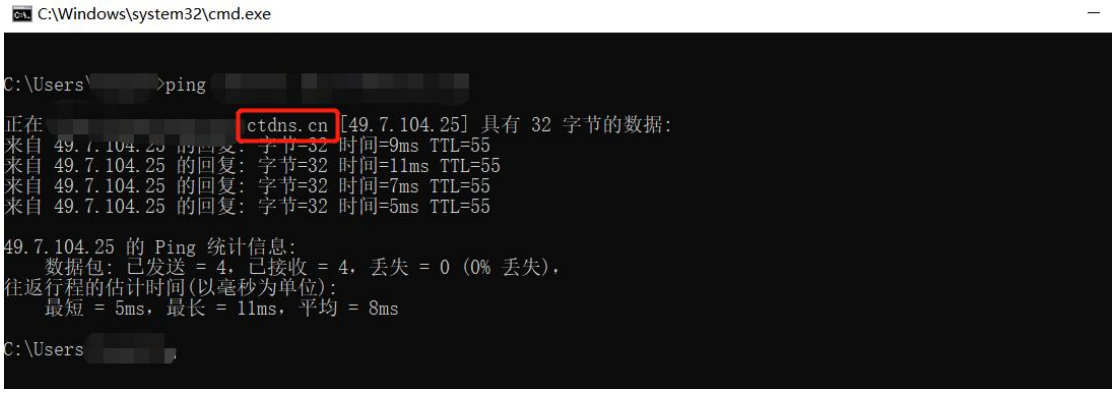
5、确认填写信息无误后，单击【提交】；

6、验证服务是否生效；

配置 CNAME 后，不同的服务商 CNAME 生效的时间也不同，一般新增的 CNAME 记录会立即生效，修改的 CNAME 记录会需要较长时间生效；

您可以 ping 或 dig 您所添加的加速域名，如果被指向*.ctdns.cn，即表示 CNAME 配置已经生效，功能也已生效。

检查域名指向页



注意:

配置 CNAME 完毕，CNAME 配置生效后，边缘安全加速平台—安全与加速服务服务生效

CNAME 配置生效时间：新增 CNAME 记录会实时生效，而修改 CNAME 记录需要最多 72 小时生效时间；

添加时如遇添加冲突，可考虑换一个防护域名，或参考以下“解析记录互斥规则” 调整记录;

解析记录互斥规则：

	NS	CNAME	A	URL	MX	TXT	AAAA	SRV	CAA
NS	可重复	X	X	X	X	X	X	X	X
CNAME	X	可重复	X	X	X	X	X	X	X
A	X	X	可重复	X	无限制	无限制	无限制	无限制	无限制
URL	X	X	X	X	无限制	无限制	X	无限制	无限制
MX	X	X	无限制	无限制	可重复	无限制	无限制	无限制	无限制
TXT	X	X	无限制	无限制	无限制	可重复	无限制	无限制	无限制
CAA	X	X	无限制	无限制	无限制	可重复	无限制	无限制	无限制
AAAA	X	X	无限制	X	无限制	无限制	可重复	无限制	无限制
SRV	X	X	无限制	无限制	无限制	无限制	无限制	可重复	无限制

在提示冲突的时候，说明已经有对应的记录，不允许重复添加或者说不能添加对应的记录，提供如下说明：

在 RR 值相同的情况下，同一条线路下，在几种不同类型的解析中不能共存(X 为不允许)

X：在相同的 RR 值情况下，同一条线路下，不同类型的解析记录不允许共存。如：已经设置了 www.example.com 的 A 记录，则不允许再设置 www.example.com 的 CNAME 记录；

无限制： 在相同的 RR 值情况下，同一条线路下，不同类型的解析记录可以共存。如：已经设置了 www.example.com 的 A 记录，则还可以再设置 www.example.com 的 MX 记录；

可重复： 指在同一类型下，同一条线路下，可设置相同的多条 RR 值。如：已经设置了 www.example.com 的 A 记录，还可以再设置 www.example.com 的 A 记录。

2.2.2 域名归属权限验证指南

简介

本文介绍在新增域名操作，如果需要域名归属权验证，要如何操作

客户可根据如下方法一、方法二，任意选择一种方式进行操作验证即可。

方法一：DNS 解析验证

示例为 ctcdn.cn 的解析配置

1、客户需在自己的域名解析服务商，添加天翼云控制台返回的 TXT 记录值（如下记录值仅为示例）；

记录类型	主机记录	记录值
TXT	dnsverify	202207060000002jar4fb2hc79iwjq5cdid87t7rci1sgp33exuyvez4kwonobxt

2、域名解析操作完成后，等待（建议 10 分钟）DNS 解析生效后即可进行解析验证。

解析命令：dig dnsverify.ctcdn.cn txt

```
$dig dnsverify.ctcdn.cn txt

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.7 <<>> dnsverify.ctcdn.cn txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14801
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dnsverify.ctcdn.cn.            IN      TXT

;; ANSWER SECTION:
dnsverify.ctcdn.cn.     600     IN      TXT     "202207060000002jar4fb2hc79iwjq5cdid87t7rci1sgp3

;; Query time: 93 msec
;; SERVER: 119.29.29.29#53(119.29.29.29)
;; WHEN: Fri Jul 29 10:42:31 CST 2022
;; MSG SIZE  rcvd: 124
```

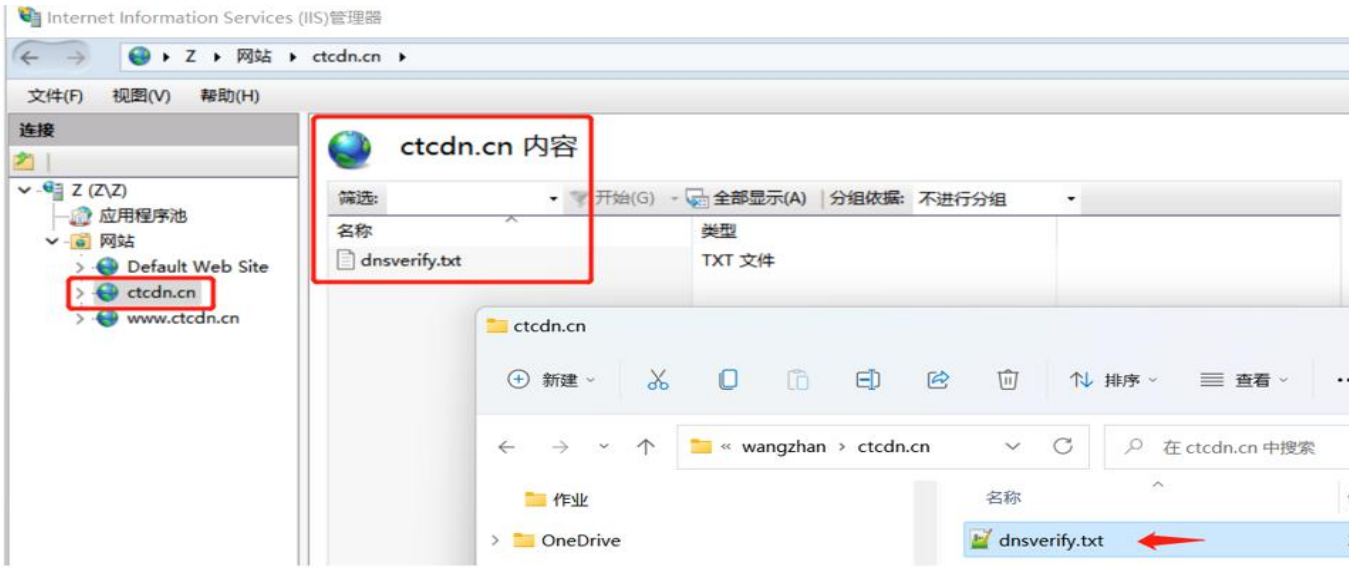
3、如解析出来的 txt 值和天翼云控制台返回的 TXT 记录值一致，则表示配置正确。

确认配置正确后，可前往天翼云控制台，在新增域名界面点击验证，验证通过就可以正常操作新增域名。

方法二：文件验证

示例为 ctcdn.cn 的解析配置

1、在您的源站根目录下，创建文件名为：dnsverify.txt 的文件，文件内容为天翼云控制台返回的 TXT 记录值（如下记录值仅为示例）

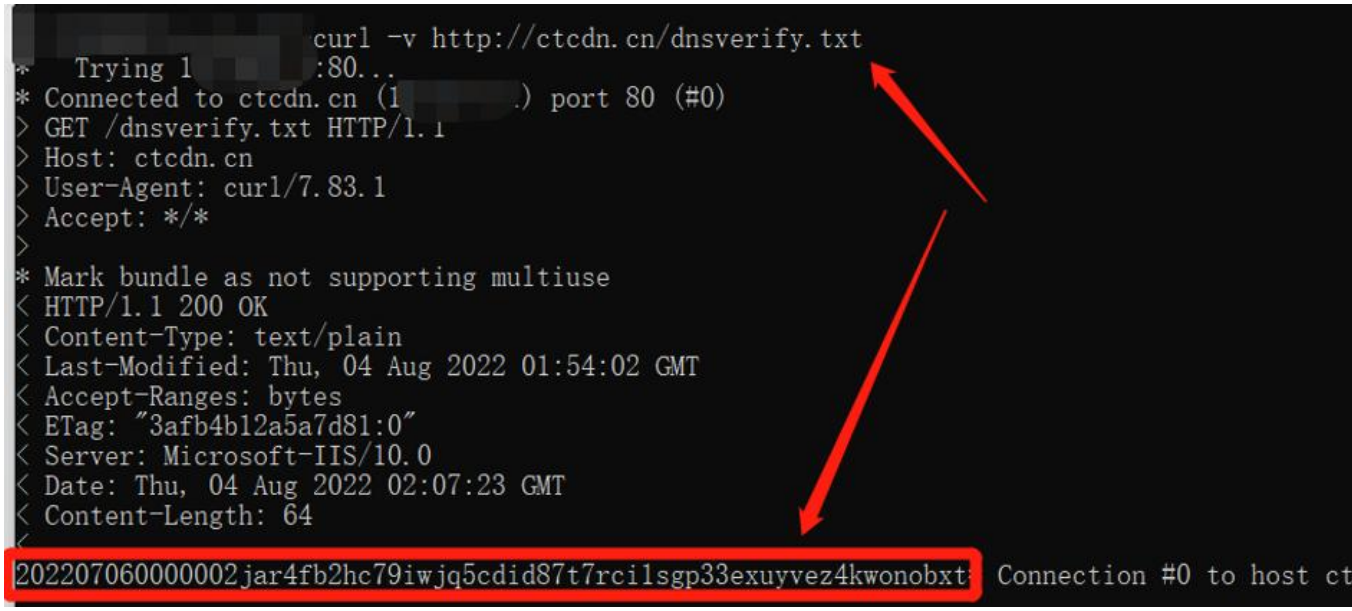


2、文件在源站根目录下创建完成后，即可进行访问验证（示例为访

问 http://ctcdn.cn/dnsverify.txt）

windows 验证：

linux 验证：



3、如访问展示的文件内容和天翼云控制台返回的 TXT 记录值一致，则表示配置正确。

确认配置正确后，可前往天翼云控制台，在新增域名界面点击验证，验证通过就可以正常操

作新增域名。

2.2.3 域名配置

简介

通过该模块可以对资源文件的回源地址进行管理以及配合源站实际业务场景进行更高级的

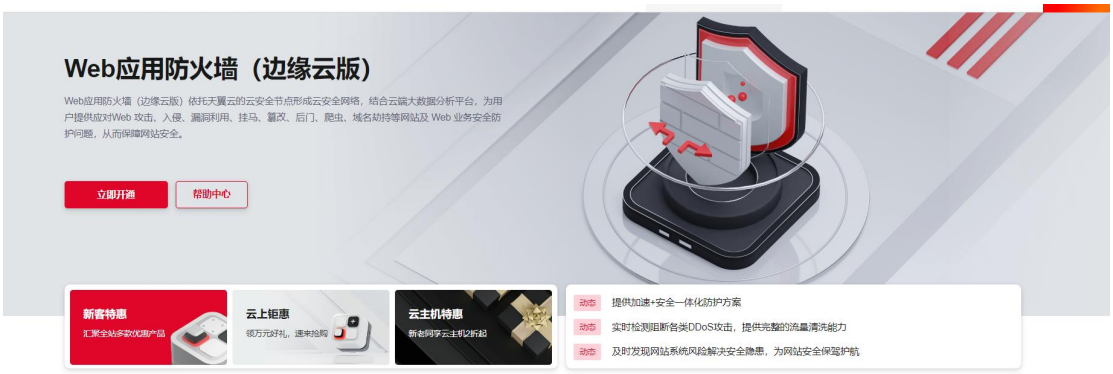
配置，包括源站配置、缓存配置等。

操作步骤

步骤一：进入边缘安全加速平台控制台

1、打开天翼云官网 http://www.ctyun.cn，注册并登录；

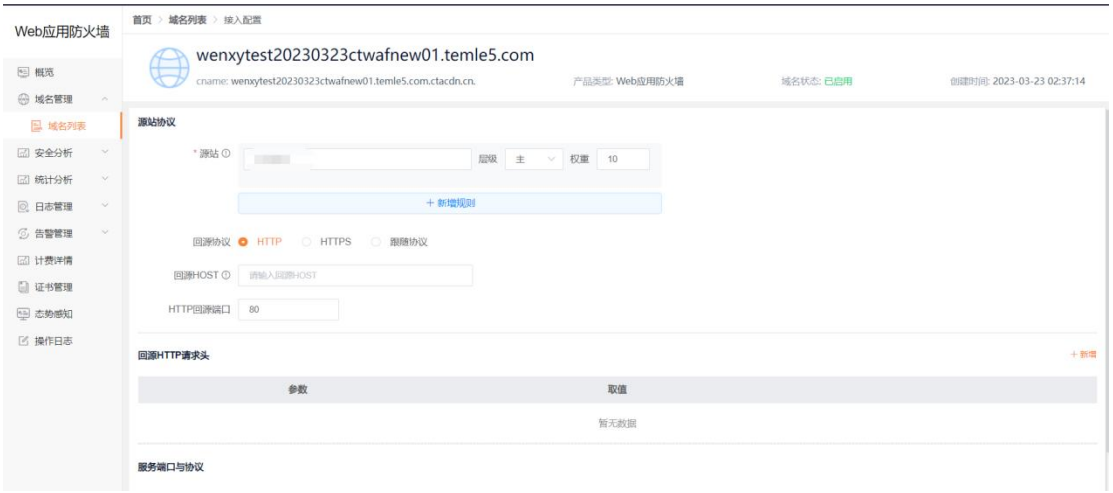
2、选择控制中心；



3、下拉选择安全，点击对应的 web 应用防火墙（边缘云版）进入客户控制台；

步骤二：编辑源站配置

1、选择域名管理—域名列表，点击【域名列表】—【接入配置】进入接入配置页面；



配置项说明：

- 源站：填写服务器地址需要为公网可达的 IP，同时配置 IPv4 和 IPv6 时，如勾选协议跟随，则来自 IPv6 的地址将总是转发到 IPv6 的源站，来自 IPv4 的地址将总是转发到 IPv4 的源站；如不勾选协议跟随，则不做区分，混合回源（即 IPv4 有可能回源到 IPv4

和 IPv6，IPv6 同理；只配置 IPv4 时，IPv4 和 IPv6 请求都将通过 IPv4 回源；

- 回源协议：目前仅 HTTP 协议回源支持自定义端口，HTTPS 协议回源使用 443 端口，跟随请求协议回源将根据请求指定的协议回源到您源站的 80 或 443 端口；
- 源站端口：HTTP 默认端口为 80 端口，HTTPS 默认端口为 443 端口，也可以自定义端口；
- 回源 HOST:回源 host 决定了回源请求访问到源站的哪个站点，默认值为加速域名。自定义配置时，请确保您的源站有配置相应的 HOST。
- 回源 HTTP 请求头：支持自定义配置回源 HTTP 请求头；

步骤三：编辑缓存配置

1、选择域名管理—域名列表，点击【域名列表】—【接入配置】进入域名配置页面；

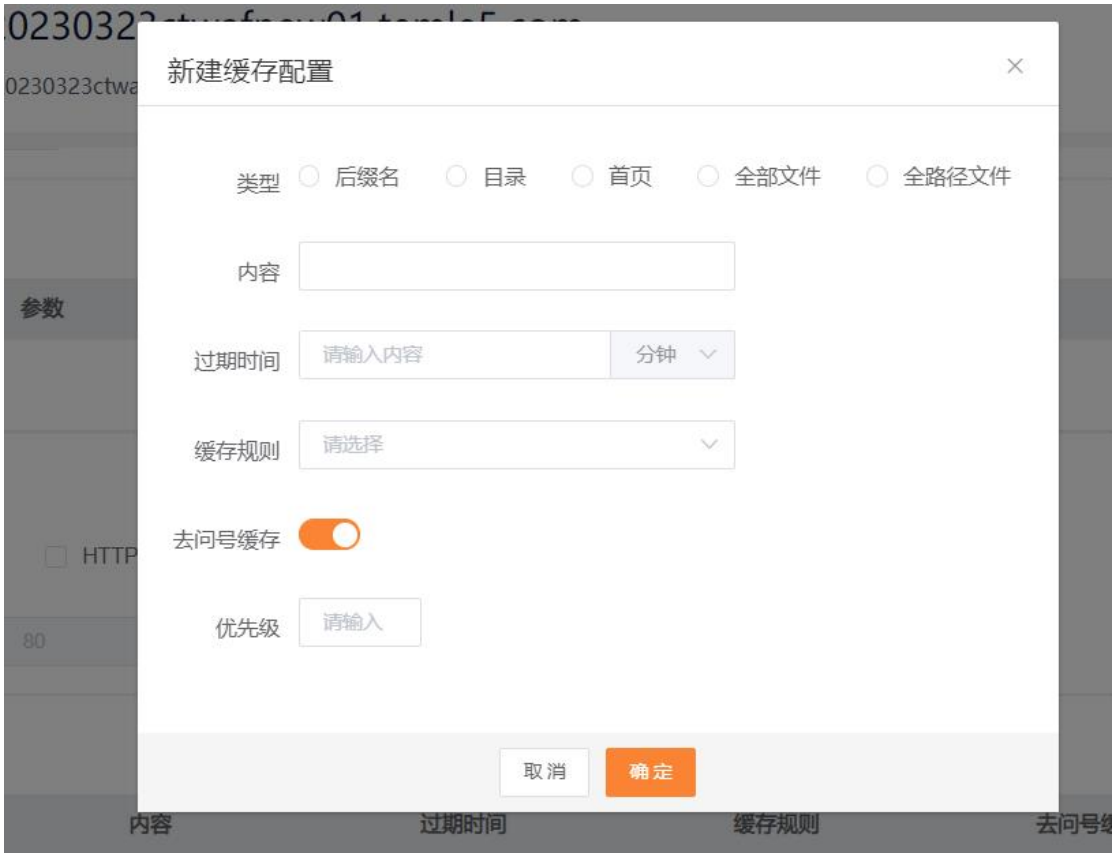
2、缓存配置是指中国电信天翼云 CDN 加速节点（包括边缘节点和中心节点）在缓存您的资源文件时遵循的一套过期规则，当资源文件处于过期状态时，此时用户请求会由节点发送至源站，重新获取资源中心内容并缓存至节点，同时返回给最终用户；当资源内容未过期时，用户请求到 CDN 加速节点后，会由节点直接响应用户请求。合理的配置资源文件缓存时间，能够有效的提升缓存命中率，降低回源率，节省您的源站带宽。

配置项说明：

- 缓存过期时间设置：

您可以根据业务需求配置边缘节点缓存目录和后缀名文件来设置缓存过期时间时间，从而减少请求回源对源站造成的压力以及保证源站内容更新的时效性。

当配置缓存过期时间时，类型选中目录，那么所填内容为文件缓存的路径，过期时间由您根据业务决定（一般支持 1 天、3 天、5 天）。类型选中后缀名时，所填写的内容为您业务所需要缓存文件的后缀名（动态文件不缓存）配置信息如下图所示：



2.2.4 域名列表

在【域名管理】中查看域名列表，可以查看已添加的防护域名信息，包括域名、CNAME、状态、创建时间、IPv6、创建时间和对应操作。

其中操作中包含【接入配置】、【安全防护】、【停用】、【启用】和【删除】：

【接入配置】点击可以查看和编辑当前域名的配置信息；

【安全防护】点击查看和编辑当前域名的安全防护配置；

【停用】停止当前域名解析，停止域名服务；

【启用】恢复当前域名解析，启用域名服务；

【删除】从域名列表中删除该域名

1）当域名状态为【已启用】时，可以单击【接入配置】、【安全防护】对域名配置查看和编辑、也可以进行【停用】操作；

2）当域名状态为【配置中】时，可以单击【接入配置】、【安全防护】对域名配置查看，但是不能编辑；

3）当域名状态为【已停用】时，可以单击【接入配置】、【安全防护】对域名配置查看，但是不能编辑，可以【启用】和【删除】操作；

2.3web 防护配置

2.3.1 安全基础配置

简介

本文介绍防护模式、处理动作、漏洞防护配置、静态文件后缀。

设置防护拦截防护模式

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入安全基础配置页面；

2、防护模式：设置为开启

3、处理动作：设置为拦截

配置项说明

（1）防护模式：域名防护开关；

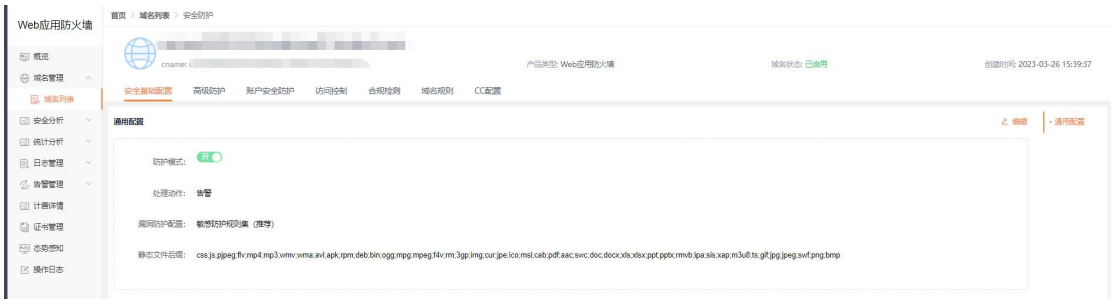
开启：开启 web 防护

关闭：关闭 web 防护，策略不生效

（2）处理动作：全局处理动作，

拦截：当处理动作为拦截时，请求触发策略处理动作是拦截

告警：当处理动作为告警时，请求触发策略处理动作是告警，如果单条防护策略的处理动作是拦截，生效也是告警。



调整域名规则防护模板

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入安全基础配置页面；

2、设置漏洞防护配置，根据下拉提示选择适配网页业务的模板；

全量防护规则集：适用于重保等级高，且允许一定程度误报的业务场景。该漏洞规则集防护包含全量规则，绝大部分规则处理动作为拦截（网站防护模式为拦截时则直接进行拦截），容易出现误报，请谨慎选择；

敏感防护规则集：适用于常规网站，且允许少量误报的业务场景。该漏洞规则集防护等级较为严格，容易误报的规则处理动作为告警，其他规则处理动作为拦截（网站防护模式为拦截时则直接进行拦截），存在一定误报可能性；

宽松防护规则集：适用于常规网站，允许存在一定漏报的业务场景。该漏洞规则集防护等级较为宽松，关

闭容易产生误报的规则，则可能存在一定漏报，接入后请及时关注；
PHP 防护规则集：适用于后台开发语言为 PHP 的网站业务。该漏洞规则集主要针对后台语言为 PHP 进行制定，关闭其他容易产生误报的规则，接入后请及时关注；
JAVA 防护规则集：适用于后台开发语言为 JAVA 的网站业务。该漏洞规则集主要针对后台语言为 JAVA 进行制定，关闭其他容易产生误报的规则，接入后请及时关注；
非 PHP 和 JAVA 防护集：适用于后台开发语言明确非 PHP 和 JAVA 网站业务。该漏洞规则集主要针对后台语言为非 PHP 和 JAVA 进行制定，关闭其他容易产生误报的规则，接入后请及时关注；
下载类业务规则集：适用于下载类业务，即包含 zip、rar、tar、gz 等下载类后缀的业务网站。该漏洞规则集主要针对下载类业务进行设定规则，关闭其他容易产生误报的规则，接入后请及时关注；

设置无需检测的文件后缀

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入安全基础配置页面；

2、在【静态文件后缀】输入框中输入无需检测的文件后续，多个用英文;分隔；

默认值：
css;js;pjpeg;flv;mp4;mp3;wmv;wma;avi;apk;rpm;deb;bin;ogg;mpg;mpeg;f4v;rm;3gp;img;cur;jpe;ico;msi;cab;pdf;aac;swc;doc;docx;xls;xlsx;ppt;pptx;rmvb;ipa;sis;xap;m3u8;ts;gif;jpg;jpeg;swf;png;bmp

2.3.2 域名规则

简介

域名规则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。

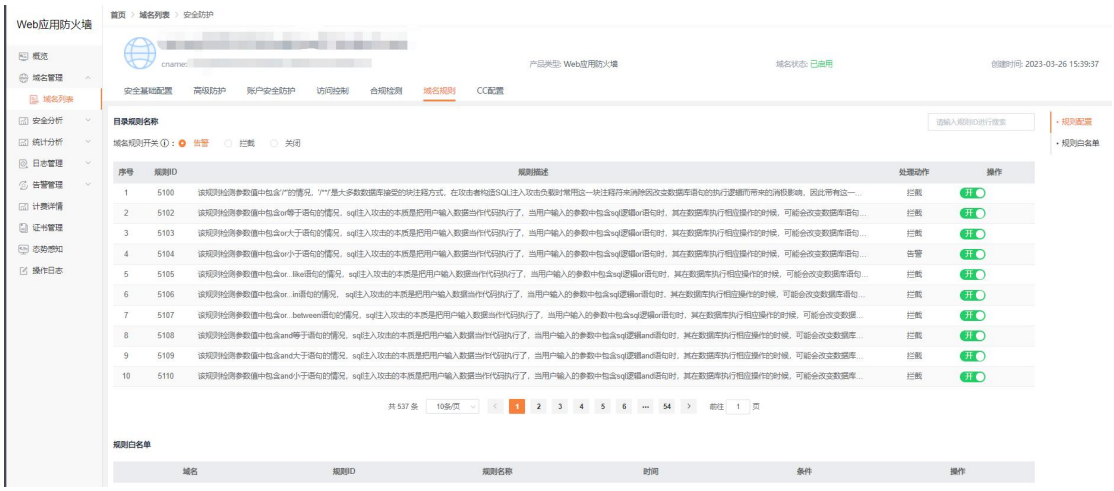
Web 防护规则防护引擎，目前防护 Web 攻击包括：SQL 注入、XSS 攻击、恶意扫描、命令注入攻击、Web 应用漏洞、WebShell 上传、不合规协议、木马后门等 17 类通用的 Web 攻击。

WAF 规则防护引擎，支持规则模板配置（安全基础配置—漏洞防护配置），用户可根据实际业务需要选择适合的模板，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。

开启或者关闭单条规则

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入域名规则配置页面；

2、在“域名规则”页签内，可基于域名实现对单条规则的开启与关闭；



2.3.3 合规检测

简介

web 防护可以根据用户实际配置的条件，检查 HTTP 协议头部，对 HTTP 请求信息中的方法以及参数长度等信息进行检测，对不符合的请求项进行拦截或告警。可以对以下情况进行检测：

1、请求方法检测：只允许指定请求方法访问网站。

2、请求协议检测：只允许指定协议版本访问网站。

3、请求头部缺失检测：请求缺少指定头部禁止访问网站。

4、数据重复检测：针对头部重复，参数重复进行拦截，禁止访问网站。

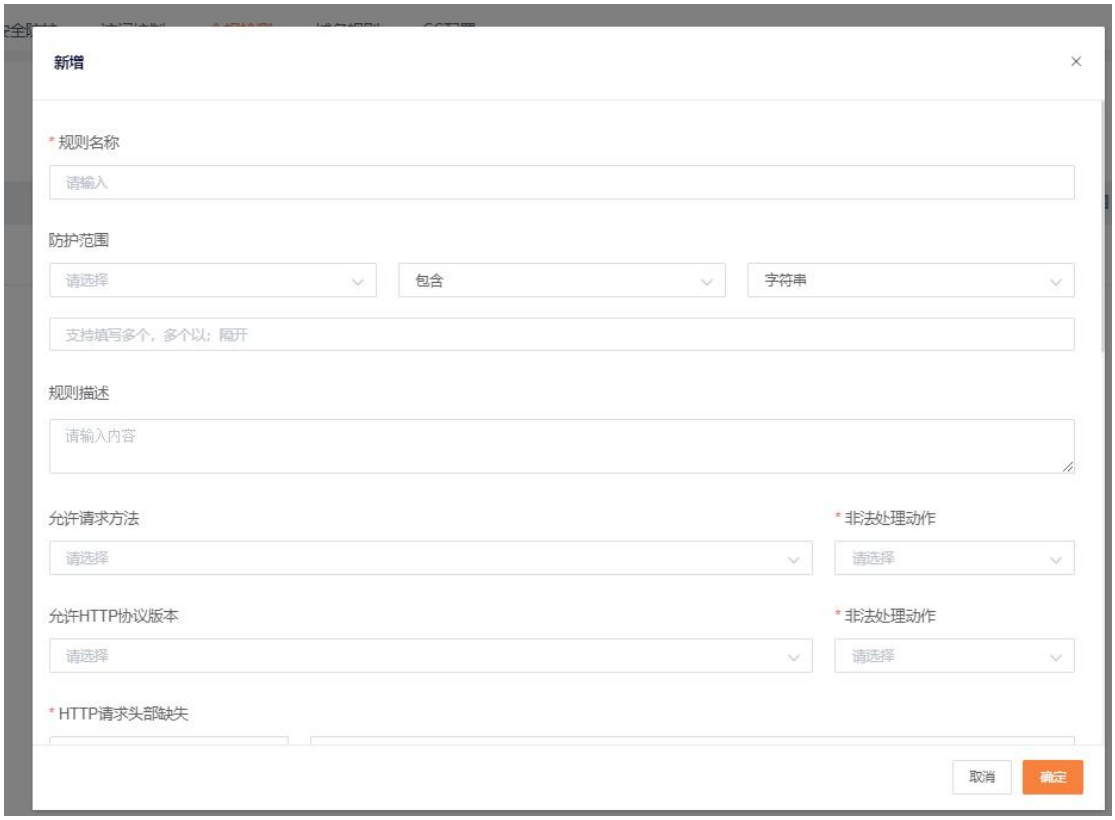
5、请求数据长度限制：针对请求 URL,头部参数进行长度限制，禁止访问网站。

设置合规检测策略

注意：域名新增时，会有一条全站合规检测的默认策略，可以通过【防护开关】来开启或者关闭。

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入合规检测配置页面；

2、在“合规检测”页签内，单击【新增】按钮，可以新增一条合规检测策略。



配置项说明：

规则名称：设置规则名称；

规则描述：设置规则描述；

防护范围：设置要防护的路径；

允许 HTTP 请求方法：设置允许的请求方法；

允许 HTTP 协议版本：设置允许的 HTTP 版本，限制非指定 HTTP 版本访问源站，保证源站针对性服务，不受黑客攻击；'

HTTP 请求头部缺失：请求缺失对应头部则告警或拦截。针对 HTTP 请求的头部进行缺失防护，当请求到达服务器时，检测到缺失头部时，进行相应处理动作

例外：如果有特殊的业务无法通过合规检测策略，可以进行加白，则请求不会进行合规检测策略校验。

2.3.4 CC 配置

简介

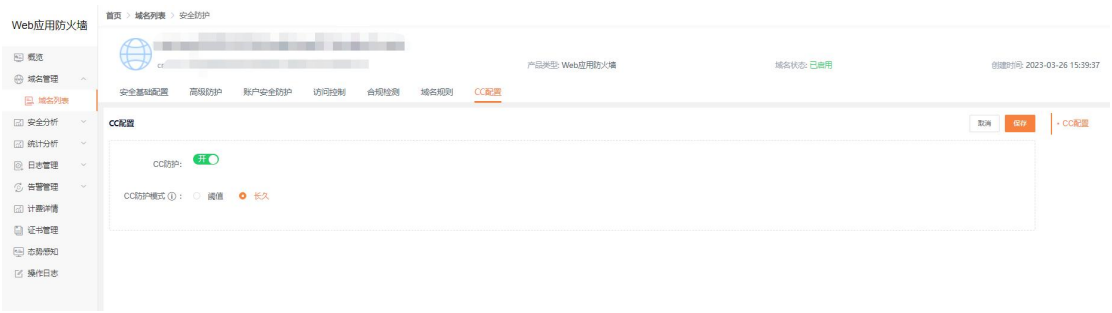
CC 防护根据访问者的 URL，频率、行为等访问特征，智能识别 CC 攻击，迅速识别 CC 攻击并进行拦截，在大规模 CC 攻击时可以避免源站资源耗尽，保证企业网站的正常访问。

设置长久模式 CC 防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入 CC 配置页面；

2、在“CC 防护”页面内，单击【编辑配置】按钮；

3、【CC 防护】设置为开启，【CC 防护模式】设置为长久，则域名的每次访问都进行防护校验；



设置阈值模式 CC 防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入 CC 配置页面；

2、在“CC 防护”页面内，单击【编辑配置】按钮；

3、【CC 防护】设置为开启，【CC 防护模式】设置为阈值，则域名访问达到防护条件时进防护；

配置项说明：

在【统计周期】内达到【阈值】则接下来【防护时长】内符合条件的请求均进行防护校验。

2.3.5 CSRF 防护

简介

CSRF 一般指跨站请求伪造。跨站请求伪造(英语：Cross-site request forgery)，也被称为 one-click attack 或者 session riding，通常缩写为 CSRF 或者 XSRF， 是一种挟制用户在当前已登录的 Web 应用程序上执行非本意的操作的攻击方法。针对发起 CSRF 攻击进行防护

设置 CSRF 防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、单击【编辑】按钮，编辑 CSRF 防护策略；

配置项说明：

（1）开关：

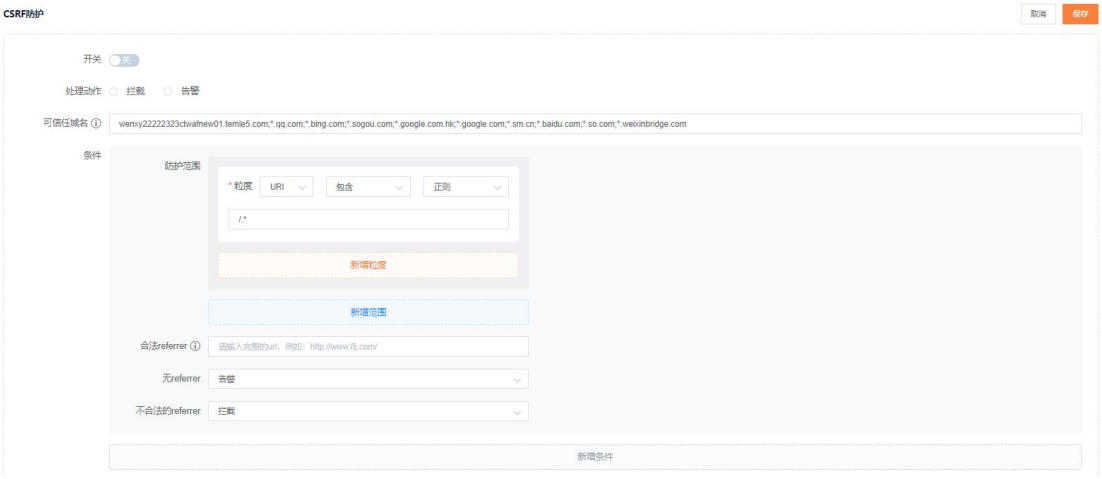
开启：开启 CSRF 防护

关闭：关闭 CSRF 防护

（2）处理动作：请求触发 CSRF 防护后的处理动作，可以选择告警或是拦截；
（3）可信任域名：当请求 referer 中含该域名，则该请求放行（可填多个域名，默认一级本域名）默认域名可进行修改；
（4）条件：
防护范围：设置要检测的请求范围，支持正则/字符串；

- URI：填写包含/不包含防护的 URI
- METHOD:填写包含/不包含的请求方法
- PATH：填写包含/不包含的 PATH

合法 referrer:填写合法 url，当请求 referer 精确匹配“合法 referrer”，则该请求放行
空 referrer 时执行操作：当请求没有 referrer 这个字段时候的处理动作；跳转，拦截，监控，放行（其中选择跳转后需要填跳转目的地址，默认当前域名首页）
不合法时执行操作：当请求 referer 没有在"可信任域名"、"合法 referrer"中，该请求的处理动作，拦截，监控，放行（其中选择跳转后需要填跳转目的地址，默认当前域名首页）



2.3.6 cookie 防护

简介
cookie 防护采用 cookie 加密、cookie 签名等方式对 cookie 字段的字进行加密或签名，防止敏感信息泄露以及防护一些使用 cookie 中的弱 key 进行权限绕过的漏洞利用，也能在一定程度上限制基于 cookie 修改的爬虫。
设置 cookie 防护策略
1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；
2、进入“cookie 防护”页签，单击【编辑】按钮，设置 cookie 防护策略；

配置项说明：

开关：控制策略的处理动作，可以选择开启或关闭；

防护模式：触发 cookie 防护后的执行动作，可以选择告警或拦截；

Cookie key 值：设置需要防护的 Cookie 名称，Cookie 必须有参数值，例如：set-cookie: SF_cookie_11=ENCRYPT_COOKIE1988262423afZ5ZEIzbEL%3D; Secure; SameSite=Strict，只有 SF_cookie_11、SameSite 可配置为 key；

防护过渡期：在过渡期内，检测失败不会进行拦截，只会清除 cookie 值；

防护动作：拦截/清除（拦截：Cookie 值检测不通过将拦截请求；清除：Cookie 检测不通过清除该 Cookie 回源）

防护方式：加密（对 Cookie 值进行加密，客户端查看到的值为加密后的内容）、签名（对 Cookie 值进行加密，客户端查看到的值为加密后的内容）；

例外：如果有特殊的业务无法通过 cookie 防护策略，可以进行加白，则请求不会进行 cookie 防护策略。

2.3.7 敏感词防护

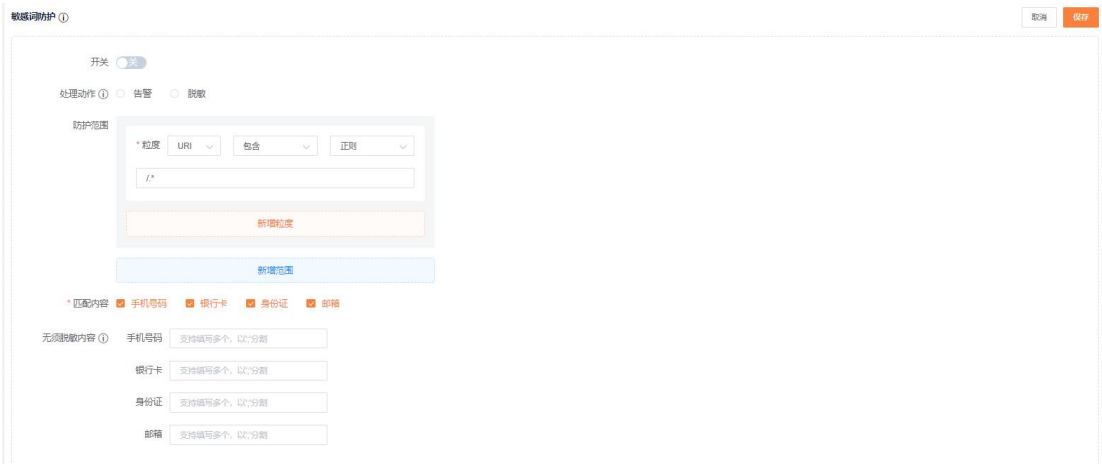
简介

敏感词防护功能支持对网站返回的内容进行脱敏展示，过滤内容包括敏感信息（如身份证、手机号、银行卡、邮箱等）。您可以根据实际需要设置敏感词防护规则，满足数据安全保护和等保合规需求。

设置敏感词防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、进入“敏感词防护”页面，可以配置敏感词防护策略；



配置项说明：

开关：设置敏感词防护策略的开关，可选择关闭或者开启；

处理动作：设置触发敏感词防护策略请求的处理动作，可选择告警或者脱敏；

防护范围：需要检测的范围，默认为全站；

匹配内容：设置需要脱敏处理的内容，可选择手机号码/银行卡/身份证/邮箱

例外：当部分敏感词不需要进行脱敏时，可以配置例外，如果填写多个要使用分号隔开

2.3.8 攻击挑战

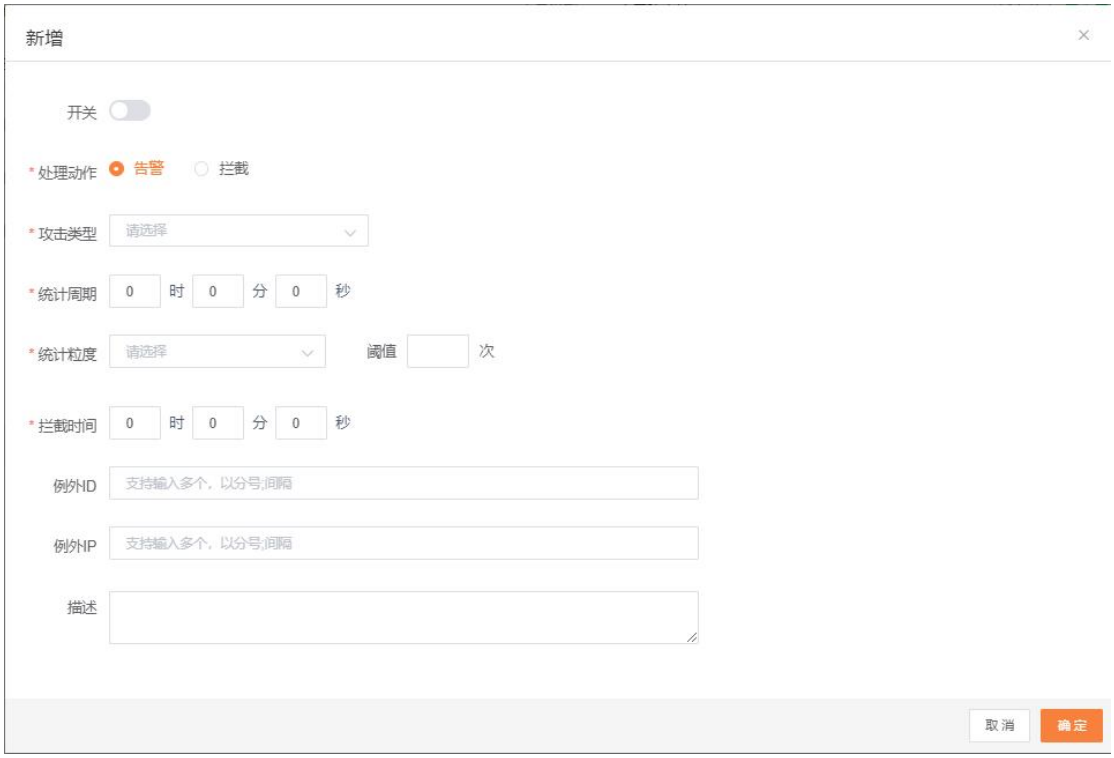
简介

攻击挑战指自动阻断在短时间内发起多次 Web 攻击（规则引擎触发）的客户端 IP，一段时间内阻止所有请求，阻断日志可以在 攻击日志 中查看，可以快速拦截恶意攻击 Web 的 IP，快速应对恶意扫描及代理、Web 攻击威胁等行为，可提升攻防对抗效率。

设置攻击挑战策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、进入“攻击挑战”页面，单击【新增】按钮；



配置项说明：

开关：防护策略开关，可选择开启或者关闭策略；

处理动作：请求触发攻击挑战策略后的处理动作，可选择拦截或者告警；

攻击类型：仅勾选的攻击类型会做统计。点击“全部”按钮就自动选中所有攻击类型；

触发条件：在【统计周期】内的【统计粒度】的请求数，触发的策略超过【阈值】次数，则执行【处理动作】；其中，统计粒度客户端 ip,客户端 ip_端口；

处理动作持续时间：指客户端 IP 满足触发条件后，处理动作会持续的时间；

例外 ID：例外的规则 ID，规则 ID 可在域名规则中查询；

例外客户端 IP：不需要过攻击挑战功能的客户端 IP；

2.3.9 广告防护

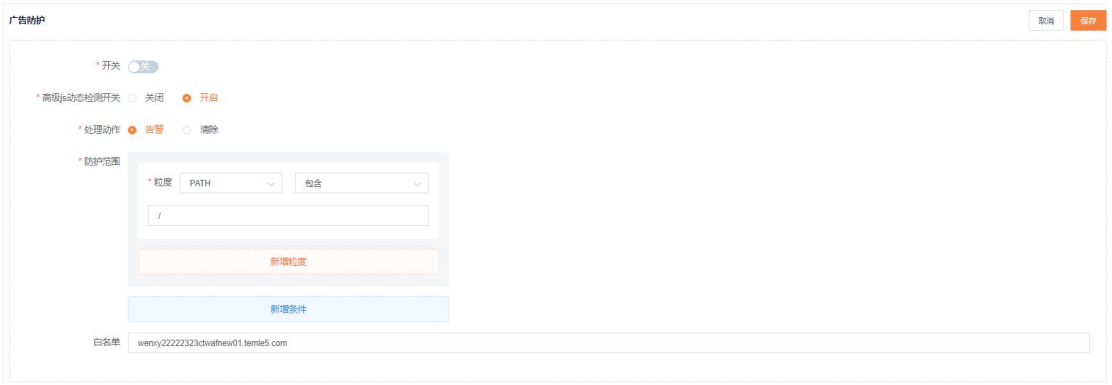
简介

天翼云 WAF 能解析源站响应页面代码，在 body 中插入广告检测 js 代码，实现广告防护和监测功能。

设置广告防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、进入“广告防护”页面，单击【编辑】按钮；



配置项说明：

开关：设置广告防护策略开启或者关闭；

高级 js 动态检测开关：

关闭：只检测页面已有广告内容（静态嵌入广告检测）

开启：将检测页面通过 js 动态添加元素内容，判断动态添加元素是否在白名单内，不再白名单则移除对应元素

处理动作：触发广告防护的处理动作，可选择告警或者清除；

防护范围：设置要配置广告防护的 URI；

（1）URI：设置防护要包含/不包含的 URI，例如：/home.jsp 支持填写多个 URI，用英文分隔符分隔；

（2）PATH：设置防护要包含/不包含的路径，例如：/匹配请求 URI 前缀，/表示全站，用英文分隔符分隔；

（3）多个粒度为且的逻辑；多个条件为或的关系；

白名单：外链白名单，当资源请求的链接来自设置的白名单时，不会进行广告处理，允许正常显示广告、图片

2.3.10 网页防篡改

简介

网页防篡改功能用于保护网站核心静态页面，通过对比源站响应与媒体存储中心缓存的响应，保护网站因为源站页面被恶意篡改带来的负面影响，同时您可以根据需要配置防篡改规则。

新增网页防篡改策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、进入“网页防篡改”页面，可以配置网页防篡改策略；

配置项说明：
防护状态：可以选择开启或者关闭策略；
规则名称：设置规则名称；
URL：填写需要防篡改防护的完整 URL 地址，例如 http://www.xxx.com/。该功能会自动获取页面下的所有静态资源
处理动作：拦截/告警/返回 WAF 缓存页面
域名是否有 CDN 加速：您的域名如果有 CDN 加速，则需要填写请求协议、源站 IP、回源端口、回源 HOST。

编辑网页防篡改策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；
2、进入“网页防篡改”页面，单击【编辑】；

删除网页防篡改策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；；
2、进入“网页防篡改”页面，单击【删除】按钮；

2.3.11 撞库防护

简介

撞库是恶意攻击者通过收集互联网已泄露或者暗网黑客交易的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站后，得到一系列可以登录的用户。很多用户在不同网站使用的是相同的帐号密码，因此黑客可以通过获取用户在 A 网站的账户密码从而尝试登录 B 网址，这就可以理解为撞库攻击。

新增撞库防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、进入“账号安全防护—撞库防护”页面，单击【新增】按钮；

配置项说明：

开关：可以选择开启或者关闭撞库防护策略；

处理动作：设置触发撞库策略的处理动作，可以选择拦截或告警；

登录页 URL：设置登录页面的 URL；

登录页数据请求 URL：先单击键盘 f12 或者抓包 然后点登录按钮，获得的那个登录数据请求的 url 地址。与登录页面 URL 可能是同一个，但是一般情况下动静态页面都是分离的，所以大概率是不同的页面；

登录 post 包：

（1）用户 Key：一般是 username，具体看您的网站是怎么定义 key；

加解密方式：不加密/base64/md5; 值的加密方式，用来解密用；

（2）密码 Key: 一般是 password，具体看您的网站是怎么定义 key

加解密方式：不加密/base64/md5; 值的加密方式，用来解密用；

触发条件：在【统计周期】内的【作用域】的请求数，请求次数超过【拦截阈值】次数，则执行【处理动作】；其中，作用域支持 CI、IP+UA、IP；

（1）CI:客户端 ID，订购扩展服务 BOT 管理后支持该作用域；

（2）IP+UA：客户端 IP 与客户端 UA；

（3）IP：客户端 IP；

密码有泄漏风险：判断密码存在泄露的处理方式,日志告警/重置密码/正常访问；

请求内容类型：” application/x-www-form-urlencoded”/"application/json"；正常 post 包的请求方式；

白名单：针对误拦设置白名单，可选粒度：URI、支持配置多条，多个粒度为“且”的逻辑，多个范围为“或”的关系；

编辑撞库策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入账户安全防护页面；

2、进入“撞库防护”页面，单击【编辑】；

删除撞库防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；；

2、进入“撞库防护”页面，单击【删除】按钮；

2.3.12 暴力破解防护

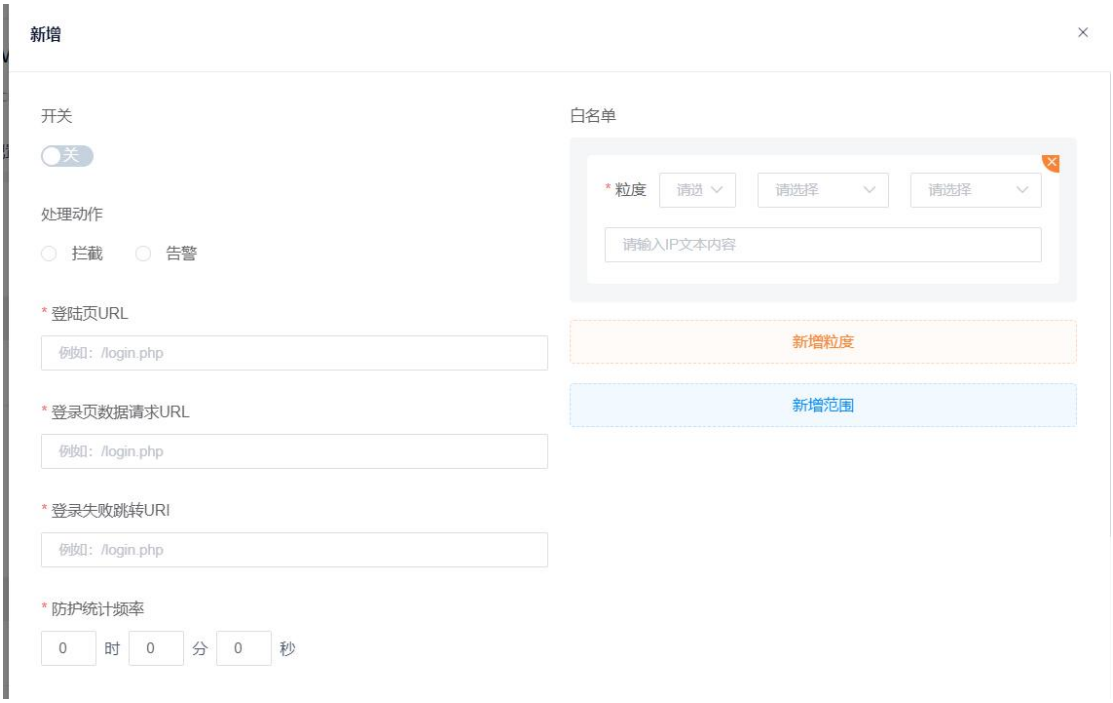
简介

暴力破解是指攻击者通过脚本等方式实现原有的尝试登录流程，不断重复尝试登录的一个过程，从理论上来看只要时间足够，所有的账号都有被暴力破解找到口令的可能，对普通用户爆破可以造成个人的财产损失，对网站管理员的账号爆破则可以危害公司资产。边缘云 WAF 主要通过爆破行为监控来防护。

新增暴力破解防护策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；

2、进入“账号安全防护—暴力破解防护”页面，单击【新增】按钮；



配置项说明：

开关：可以选择开启或者关闭暴力破解防护策略；

处理动作：设置触发暴力破解策略的处理动作，可以选择拦截或告警；

登录页 URL：设置登录页面的 URL；

登录页数据请求 URL：先单击键盘 f12 或者抓包 然后点登录按钮，获得的那个登录数据请求的 url 地址。与登录页面 URL 可能是同一个，但是一般情况下动静态页面都是分离的，所以大概率是不同的页面；

登录失败跳转 URI：设置登录失败后需要跳转的 uri;

触发条件：在【防护统计频率】内的【作用域】的请求数，请求次数超过【拦截阈值】次数，则执行【处理动作】，处理动作持续时间【拦截时间】；其中，作用域支持 CI、IP+UA、IP；

（1）CI:客户端 ID，订购扩展服务 BOT 管理后支持该作用域；

（2）IP+UA：客户端 IP 与客户端 UA；

（3）IP：客户端 IP；

白名单：针对误拦设置白名单，可选粒度：客户端 IP、支持配置多条，多个粒度为“且”的逻辑，多个范围为“或”的关系；

编辑暴力破解策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入账户安全防护页面；

2、进入“账户安全防护”中暴力破解页面，单击【编辑】；

删除暴力破解策略

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【安全防护】进入高级防护页面；；

2、进入“账户安全防护”中暴力破解页面，单击【删除】按钮；

2.4 访问控制

简介

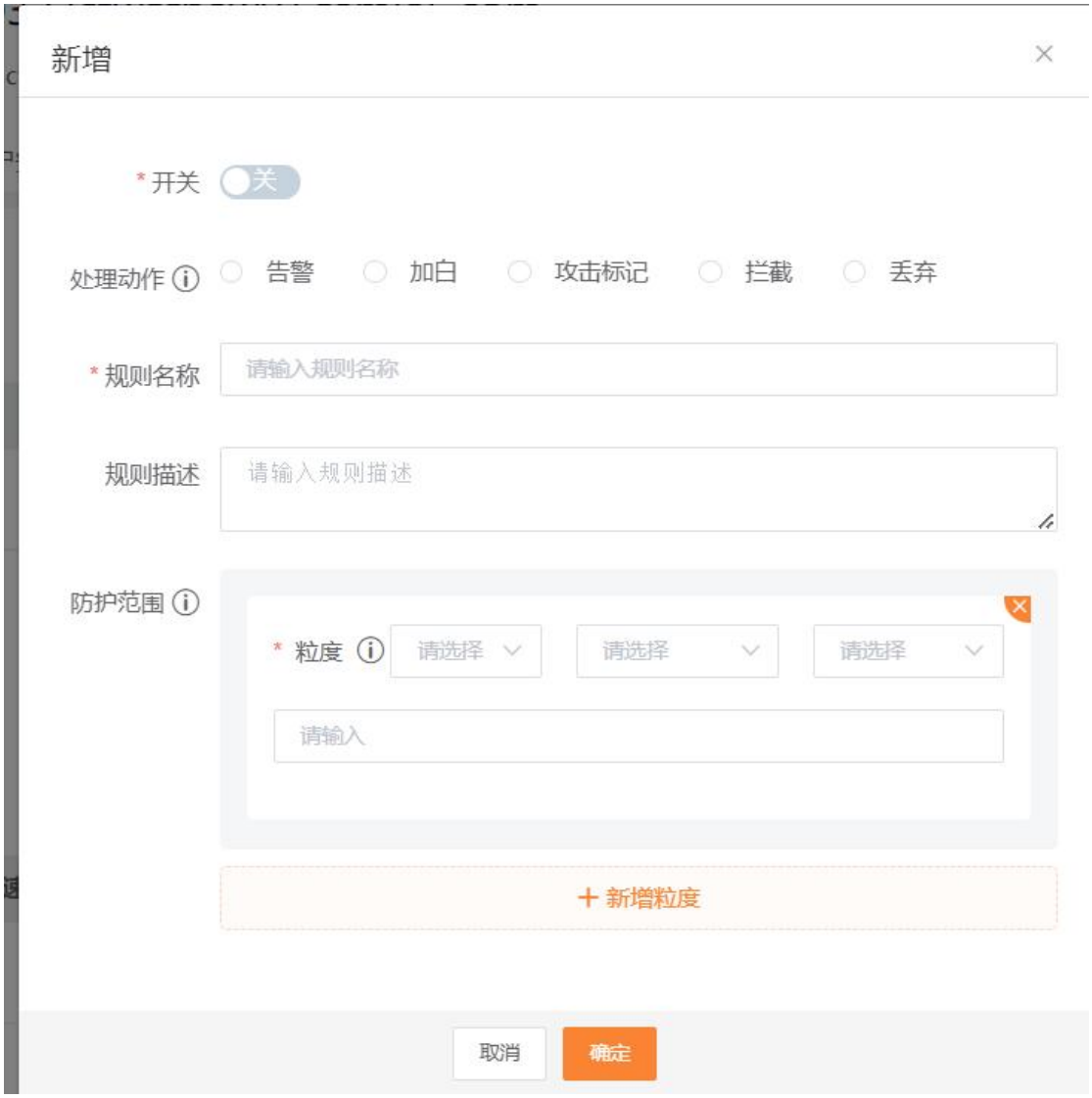
访问控制可针对 IP,IP 段，URI，CI，METHOD，请求地区，请求参数，请求头部，请求协议进行组合，设置白名单和黑名单，对请求进行拦截和放行，保证客户网站不受未知访问。

设置禁止特定 IP 地址访问域名

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【访问控制】进入访问控制页面；；

2、进入“访问控制”中页面，单击【新增】按钮；

3、在新增页面，输入规则名称（如拦截指定 IP），在匹配字段中选择一个字段（如 IP），逻辑符号选择包含，防护范围填入需要禁止访问的来源 IP（如 192.168.1.1），选择执行动作（如拦截），填写完成后，单击确定，保存规则。



设置地域封禁

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【访问控制】进入访问控制页面；

2、进入“访问控制”中页面，单击【新增】按钮；

3、在新增页面，输入规则名称（如拦截指定地域），在匹配字段中选择一个字段（如 GEO），逻辑符号选择包含，防护范围填入需要禁止访问地域（如欧洲），选择执行动作（如拦截），填写完成后，单击确定，保存规则。

2.5 频率控制

简介

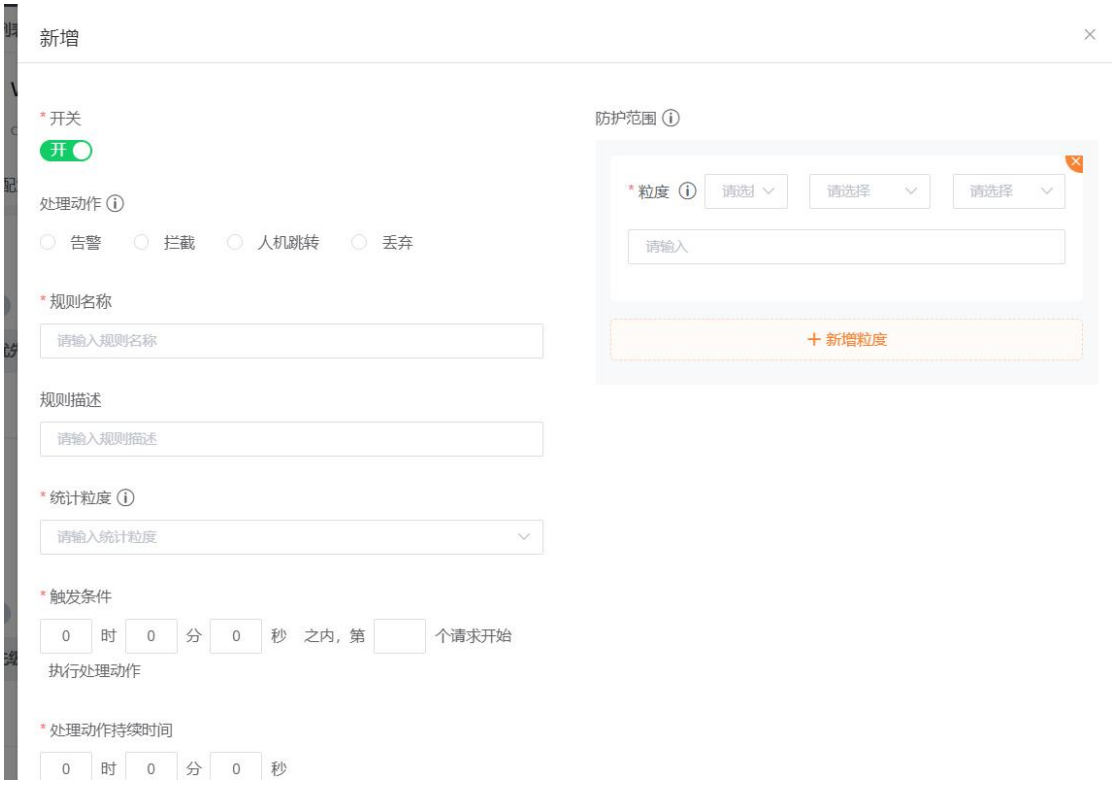
通过配置 IP,URL,ARGS,HEADER,COOKIE,UA,CI 等粒度，进行访问次数限制，防止客户资源被过度消耗。

设置客户端 IP 访问域名首页次数限制

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【域名管理】—【域名列表】，单击域名列表操作【访问控制】进入频率控制页面；

2、进入“访问控制”中页面，单击【新增】按钮；

3、在新增页面，输入规则名称（如单 IP 访问首页次数限制），选择统计粒度（如 IP），在触发条件中设置触发条件（如在 59 秒内，低 5 个请求开始执行处理动作），选择处理动作（如拦截），填写完成后，单击确定，保存规则。



2.6 统计分析

2.6.1 业务分析

简介

业务分析模块可为客户提供带宽流量、请求数、状态码等指标。

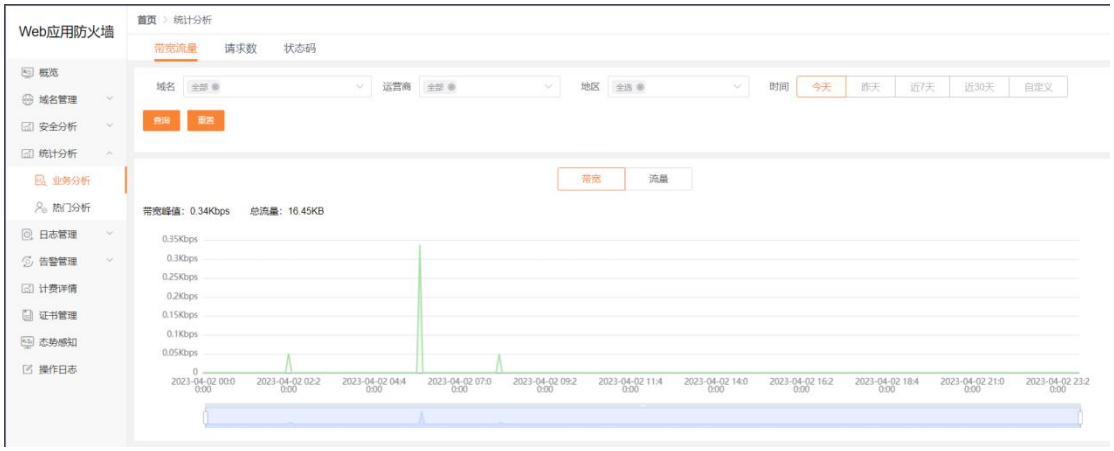
操作步骤

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【统计分析】—【业务分析】页面；

2、通过筛选项进行组合查询带宽流量、请求数、状态码等指标。筛选项包括域名、运营商、地区、时间。

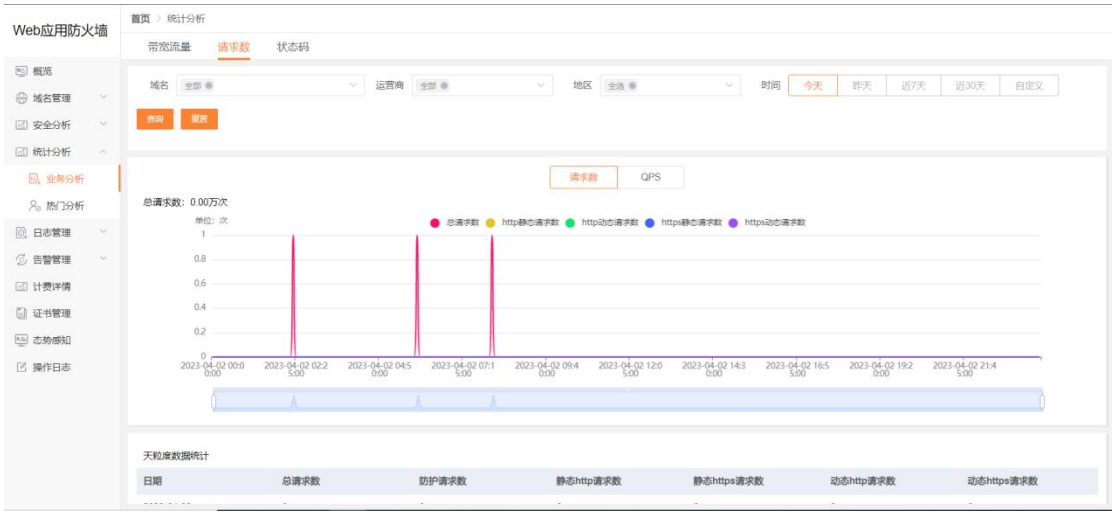
带宽流量

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的带宽和流量统计图表，可通过切换“带宽”和“流量”的按钮查看带宽和流量图，同时会给出查询时间范围内每日总流量、带宽峰值、峰值时间点。



请求数

界面中展示的是您所选范围、域名、运营商、地区、时间范围内的请求数和 QPS 统计图表，可通过切换“请求数”和“QPS”的按钮查看请求数和 QPS 图，请求数图表中包括了总请求数、动态 http 请求数、动态 https 请求数、静态 http 请求数、静态 https 请求数



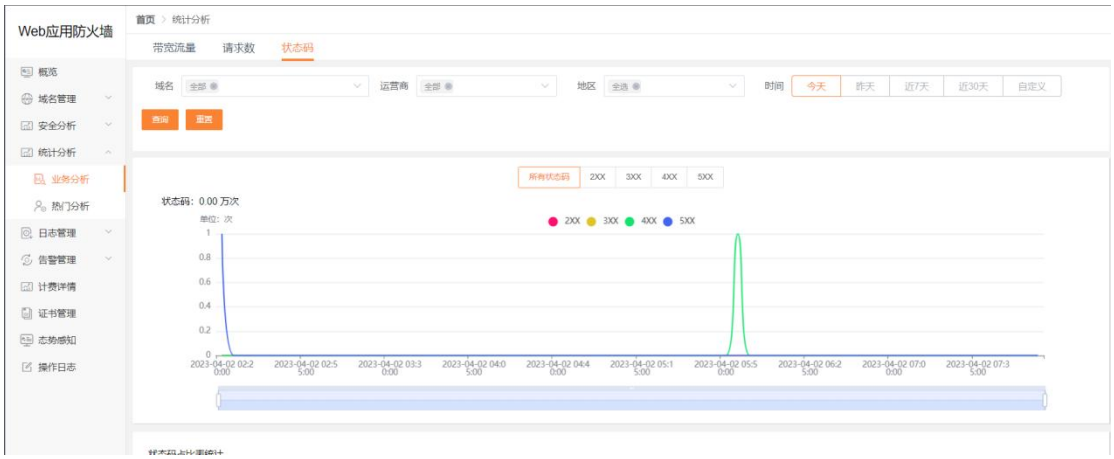
天粒度数据统计说明：

（1）没有开启 WAF 防护：防护请求数=0，总请求数=静态 http 请求数+静态 https 请求数+动态请求数+动态 https 请求数；

（2）开启 WAF 防护：动态请求数=0，总请求数=静态 http 请求数+静态 https 请求数+防护请求数；

状态码

界面中展示的是您所选域名、运营商、地区、时间范围内的状态码统计图表，可通过切换“所有状态码”、“2XX”、“3XX”、“4XX”、“5XX”的按钮查看不同状态码的图表，并显示查询时间范围内的总状态码量，同时展示状态码占比表和状态码占比饼图。



2.6.2 热门分析

简介

支持三个月内、最长时间跨度为一个月的热门数据统计，包括热门 Referer、热门域名、TOP 客户端 IP 统计，可根据访问次数优先和流量优先两种维度的排列。并支持数据下载导出，表格内容与页面一致。

操作步骤

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【统计分析】—【热门分析】页面；

热门 URL

热门 URL 可展示 TOP100 的 URL 及对应的流量、流量占比、访问次数、访问占比。选择“流量优先”时按照流量大小排序，选择“访问次数”时按照访问次数排序，并支持表格导出；

TOP 客户端 IP

TOP 客户端 IP 可将客户端 IP 按照“流量“或者”访问次数“排序，并展示客户端 IP 对应的流量、流量占比、访问次数、访问占比。并支持表格导出。

2.7 安全分析

2.7.1WAF 攻击报表

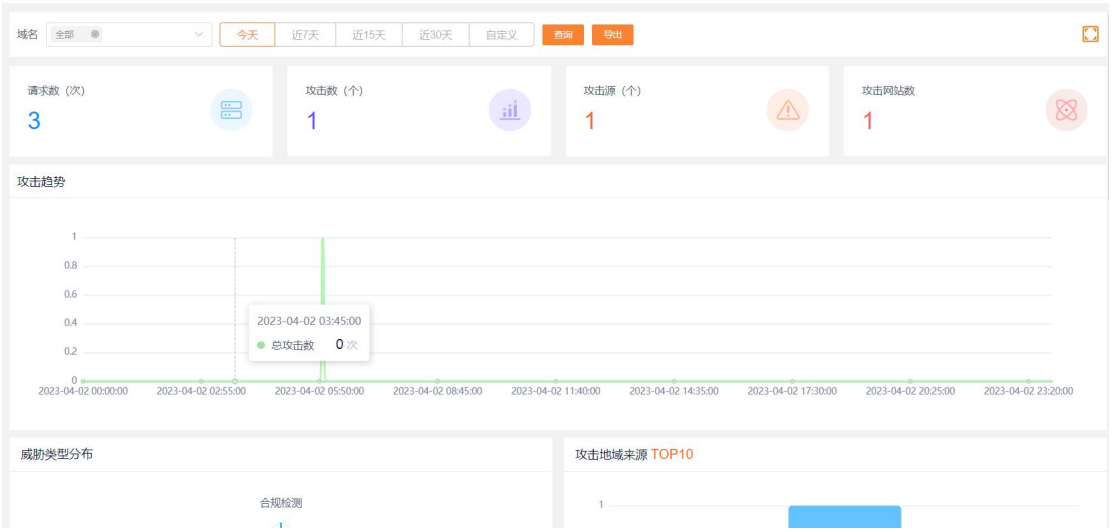
简介

可以通过 WAF 攻击报表，查看到攻击数、攻击趋势、威胁类型分布、攻击 IPTOP10、TOP 攻击 URL 等报表，并且支持导出报表

操作指导

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【安全分析】—【WAF 攻击报表】页面；

2、通过筛选 域名，查看单域名或者多域名的攻击数、攻击趋势等指标。筛选项包括域名、时间；



字段说明：

（1）请求数：展示所选域名的请求数；

（2）攻击数：展示所选域名的攻击请求数；

（3）攻击源：展示所选域名的攻击来源个数；

（4）攻击网站舒：展示所选域名中被攻击的域名个数；

（5）攻击趋势：展示所选域名被攻击的请求数分布；

（6）威胁类型分布：展示所选域名被攻击的类型的分布，包括：SQL 注入、代码执行等；

（7）攻击地域来源 TOP10:展示所选域名攻击来源分布最多的 10 个地区；

（8）攻击 IP TOP10: 展示所选域名收到攻击最多的 10 个 IP;

2.7.2 CC 攻击报表

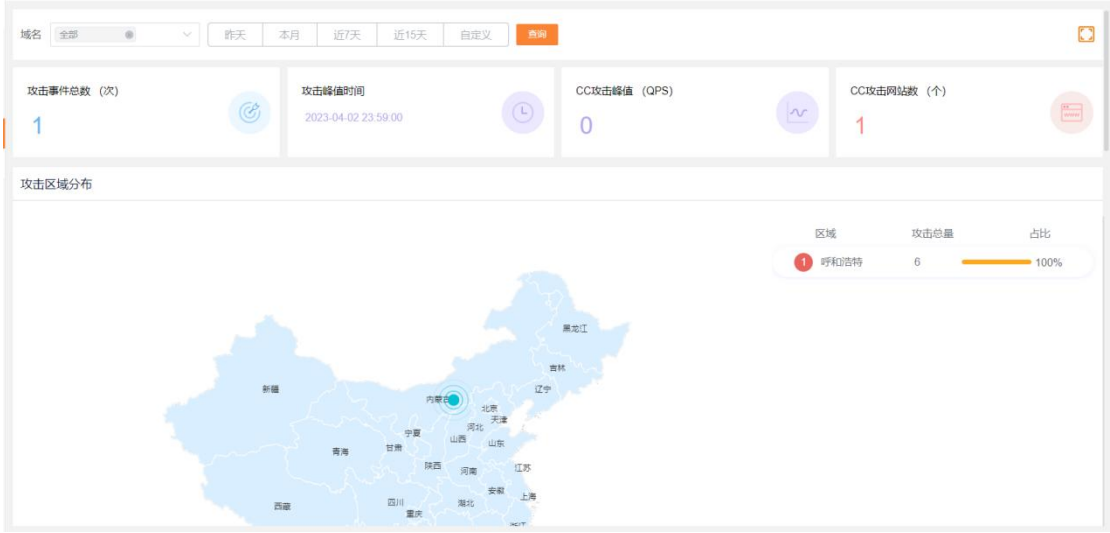
简介

可以通过 CC 攻击报表，查看到攻击事件数、攻击峰值时间、CC 攻击峰值、CC 攻击网站数等报表

操作指导

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【安全分析】—【CC 攻击报表】页面；

2、通过筛选 域名，查看单域名或者多域名的攻击数、攻击趋势等指标。筛选项包括域名、时间；



字段说明：

（1）攻击事件数：展示所选域名的攻击事件数；

（2）攻击峰值时间：展示所选域名产生 CC 攻击峰值的时间；

（3）CC 攻击峰值：展示所选域名的 CC 攻击峰值；

（4）CC 攻击网站数：展示所选域名中被 CC 攻击的域名个数；

（5）攻击区域分布：展示所选域名攻击来源分布；

（6）攻击趋势：展示所选域名 CC 攻击请求数的分布；

（7）TOP 攻击域名：展示所选域名中被 CC 攻击的请求数域名排名；

（8）TOP URL：展示所选域名中被 CC 攻击的请求数 URL 排名；

（9）TOP 攻击 IP：展示所选域名收到攻击最多的 10 个 IP；

2.8 告警管理

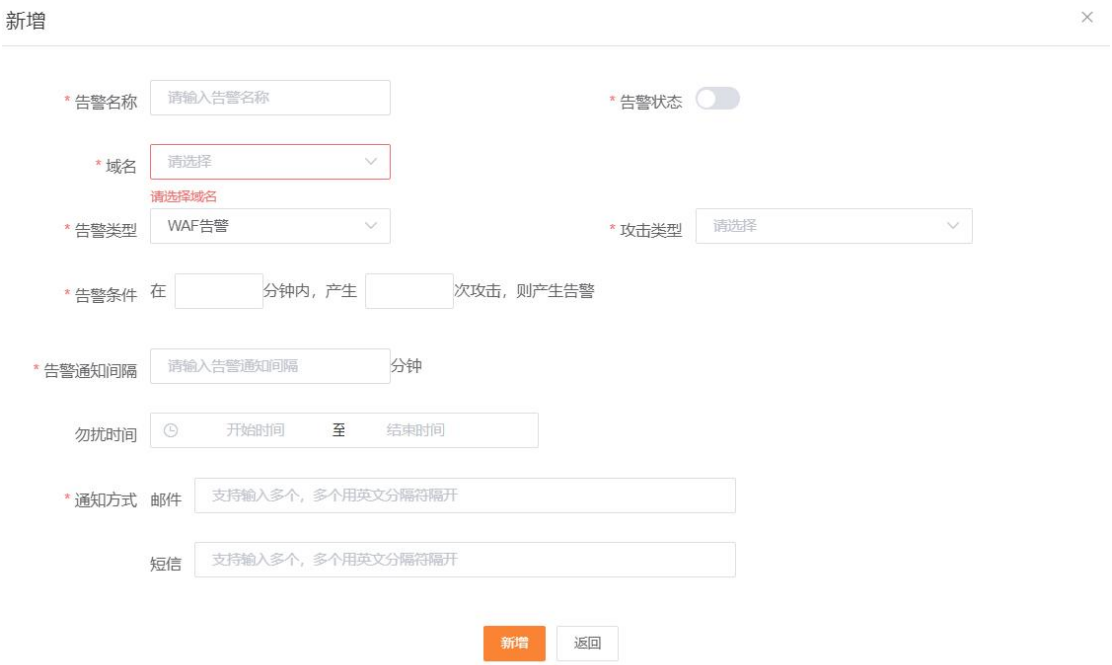
简介

网站接入天翼云 WAF 后，您可以通过设置告警，使 WAF 在网站请求流量中检测到攻击事件、异常流量时向您发送告警通知，帮助您及时掌握业务的安全状态。本文介绍如何设置告警和查看告警。

操作步骤

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【告警管理】—【告警配置】页面；

2、单击【新增】按钮，可以根据需要配置适合的告警，支持配置的告警类型有 WAF 攻击和 CC 攻击；



3、已配置的告警，可以在【告警管理】—【告警列表】中查看；

2.9 日志管理

2.9.1 攻击日志

简介

天翼云 WAF 默认提供攻击日志，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 6 个月内日志，并且支持导出攻击日志。

操作步骤

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【日志管理】—【攻击日志】页面；

2、通过筛选项进行组合查询攻击日志。筛选项包括域名、攻击类型、处理动作、规则 ID、日期；

日志字段说明：

（1）攻击 IP：发起请求的客户端 IP；

（2）请求方式：客户端的请求方法；

（3）URI：请求的 URI；

（4）攻击类型：详细攻击类型；

（5）状态码：响应的状态码；

（6）处理动作：请求的处理动作；

（7）攻击时间：攻击请求发生的时间；

（8）攻击详情：能够查看攻击客户端 IP 的详细属性，比如地域归属、UA 等；

3、单击【导出】按钮，能够导出攻击日志；

2.9.2 业务日志下载

简介

天翼云 WAF 默认提供业务的访问日志，支持单个日志和批量下载，默认支持下载 15 天的离线访问日志。

2.9.3 CC 攻击日志

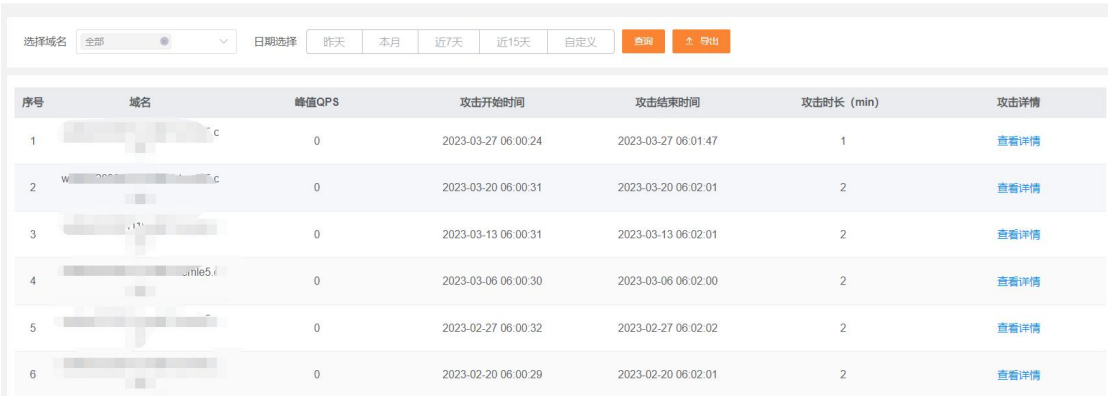
简介

天翼云 WAF 默认提供 CC 攻击日志，详细记录 CC 攻击事件攻击产生的时间、攻击时长和攻击详情，并且支持导出攻击事件。

操作步骤

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【日志管理】—【CC 攻击日志】页面；

2、通过筛选项进行组合查询攻击日志。筛选项包括域名、日期；



字段说明：

（1）峰值 QPS：CC 攻击峰值 QPS；

（2）攻击开始时间：CC 攻击开始的时间；

（3）攻击结束时间：CC 攻击结束的时间；

（4）攻击时长：CC 攻击持续的时间；

（5）攻击详情：

CC 攻击流量变化：CC 攻击 QPS 变化趋势；

攻击 IP：攻击请求数最高的前 10 个客户端 IP；

被攻击 URL：被攻击请求数最高的前 10 个 URL；

2.10 计费详情

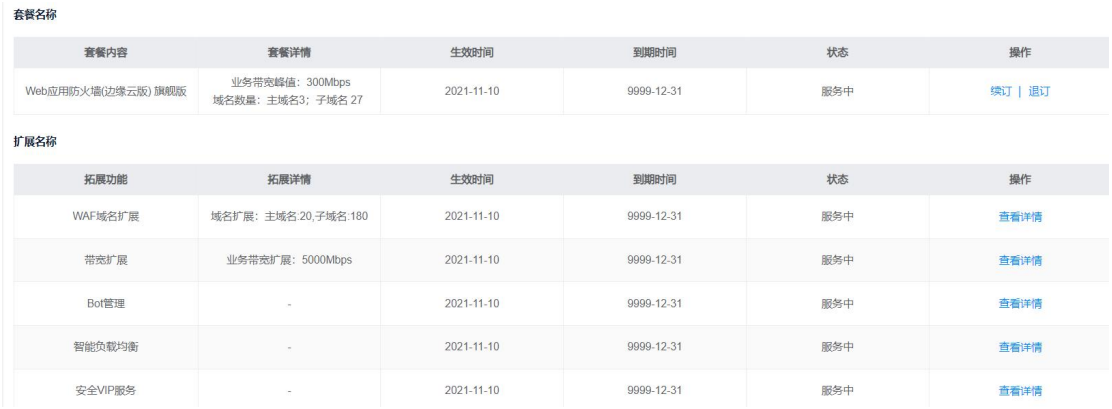
简介

您可以通过计费详情页面查看购买的套餐版本和扩展服务，以及可用域名的数量。

操作指导

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【计费详情】页面；

2、可以在【计费详情】页面中，查看到订购的套餐版本和扩展服务；



2.11 证书管理

简介

客户在证书管理模块可以上传证书，查看证书详情、更新证书、证书对应绑定的域名以及删除证书

新增证书

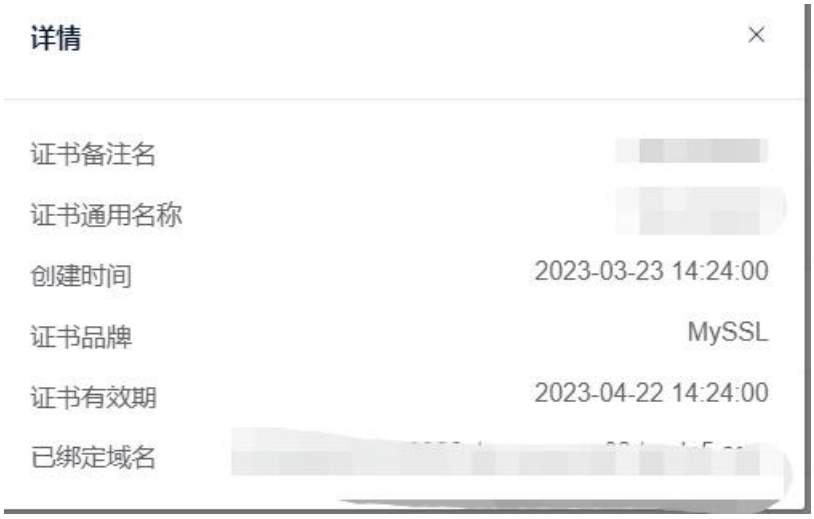
1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【证书管理】页面，单击【添加证书】按钮；

2、您需要填写证书备注名、证书公钥以及证书私钥。其中公钥和私钥支持 PEM 格式。填写完毕后，点击“确定”按钮。

查看证书

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【证书管理】页面，单击【详情】按钮；

2、可查看证书有效期和已绑定的域名；



证书删除

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【证书管理】页面，单击【删除】按钮；但是删除证书的前提是，该证书没有关联域名；

2.12 态势感知

简介

您如果购买力态势感知大屏服务，可以在控制台查看时时的安全态势感知服务。安全态势感知服务根据客户维度，时时展示客户业务整体的攻击情况，主要包括：攻击来源 IP、攻击 TOP URL、攻击域名 TOP 排行、攻击类型分布、攻击类型趋势、攻击来源 TOP 排行、攻击趋势和滚动式的安全威胁信息等。

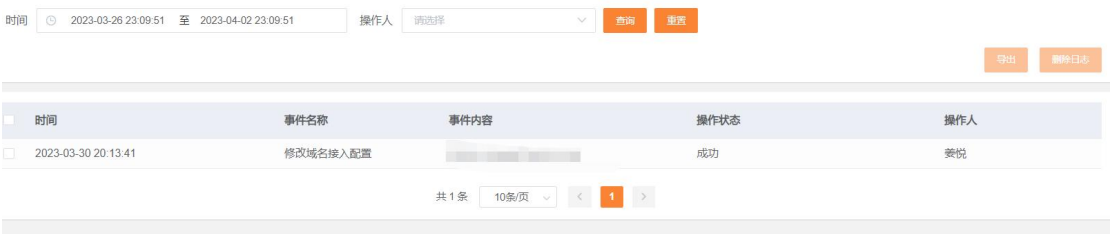
2.13 操作日志

简介

天翼云 WAF 提供操作日志，用于您查看网站的操作记录，支持查询、导出、删除操作记录。

操作指导

1、登录 web 应用防火墙（边缘云版）控制台，在左侧导航栏中选择【操作日志】页面；
2、用户可以通过时间和操作人筛选；



3.常见问题

1. 操作类

Q1

如何判断 Web 应用防火墙配置生效?

A1

可 ping、dig 所添加的域名，若转向到*.ctycdn.com，即说明配置成功，Web 应用防火墙配置生效。

Q2

使用天翼云 Web 应用防火墙配置后，需要对部分恶意 IP 进行屏蔽，以保护站点数据和流量负载，可以通过控制台进行自助配置吗?

A2

天翼云 Web 应用防火墙配置可以通过配置黑名单的方式限制 IP 访问，以及各种方式的访问控制和限速功能都可以在控制台进行自助配置。

Q3

天翼云 Web 应用防火墙目前支持哪些账户安全防护的功能，可以通过控制台进行自助配置吗?

A3

天翼云 Web 应用防火墙配置目前支持撞库防护、暴力破解防护、批量注册防护等功能，用以保证账户的安全，并支持在控制台进行自助配置。