天翼云·Web 应用防火墙（企业版）

用户使用指南

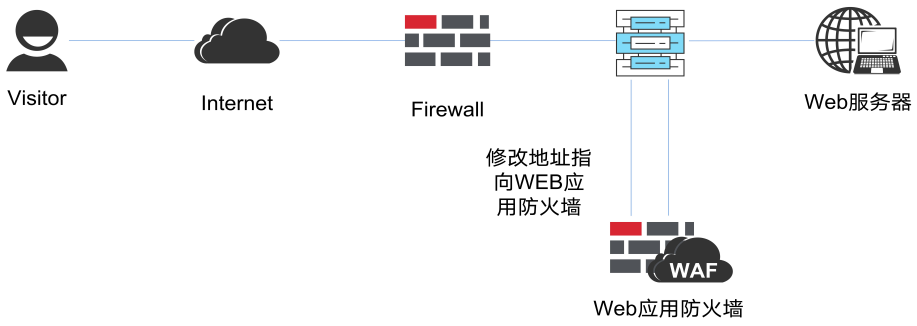
天翼云科技有限公司

目录

1. 产品介绍

1.1 产品定义

WEB 应用防火墙（以下简称“云 WAF”），基于云安全大数据实现，对客户网站提供一整套的 4-7 层应用安全防护方案，核心能力包括各类 WEB 应用安全防护、CC 攻击防护、0day 漏洞和未知威胁防护、BOT 行为管理和业务安全可视化分析等，能有效阻拦网站系统被篡改、被挂马、漏洞攻击，恶意扫描等黑客行为，充分保障用户网站安全。



1.2 功能特性

1.2.1 网络层防护

1）Http/HttpS Flood（CC 攻击）防护

1.2.2 应用层防护和功能

1）黑白名单：

对指定访问源加白名单，对恶意访问来源进行封禁，支持 IP、URL、Useragent（用户代理）、Referer。

（Http 访问来源）。

2）HTTP 协议规范攻击防护：

包括特殊字符过滤、请求方式、内容传输方式，例如：multipart/form-data，text/xml，

application/x-www-form-urlencoded。

3）注入攻击（form 和 URL 参数，post 和 get）防护

包括 SQL 注入防御、LDAP 注入防御、命令注入防护（OS 命令，webshell 等）、XPath 注入、Xml/Json

注入。

4）XSS 攻击访问

Form 和 URL 参数，post 和 get，包括三类攻击：存储式，反射式、基于 Dom 的 XSS。

5）目录遍历（Path Traversal）攻击防护。

6）认证管理和会话劫持攻击防护：

阻断认证管理、cookie 信息被盗用、会话劫持攻击。

7）内容过滤：

过滤 post form 和 get 参数。8）

Web 服务器漏洞探测攻击防护。阻

断 web 服务器漏洞探测。

9）爬虫防护：

限制阻断爬虫访问。

10）站点转换（URL rewrite）访问防护。

限制阻断访问站点转换访问。

11）网页检测到异常自动阻断源地址

12）认证管理和会话劫持

13）防护 CSRF

1.3 应用场景

1.3.1 政企教育医卫行业场景

场景特点：

政企行业、教育行业和医卫行业，包括门户网站作为提供给互联网用户获取 信息服务的重要渠道，多面临网页被篡改、网页挂马、跨站攻击、SQL 注入攻击等安全威胁，同时也面临上级单位和测评机构的监管压力。一旦发生安全事件， 将严重影响其形象和公信力。

能解决的问题：

政企类用户经常遭受来自境外地区的各类 sql 注入等类型攻击，通过waf 可以制定针对指定境外地区直接进行封禁，阻断所有来自风险地区的访问请求，以及waf 可以根据内置的策略等级模式将安全性要求较高的业务重点报障，有效将 99%的攻击自动进行禁封。

1.3.2 金融行业场景

场景特点：

金融行业面临注入、跨站等多种安全问题，导致用户账号密码泄露，危及用 户资金财产安全，进而严重影响企业的形象并承受经济损失。

能解决的问题：

网站遭遇大量web 暴力破解请求企图获取平台登录信息，如被获取登录信息后将进一步被攻击者进行渗透，如部署waf 可通过waf 内置 cc 策略以及暴力破解特征库自动阻断该类型请求并发送告警至自服务平台，大大增加了网站的安全等级，并且可以主动发现并进行禁封或进行攻击溯源。

1.3.3 电商行业场景

场景特点：

电商行业为 Web 应用攻击的重点对象，经常遭受黑客攻击，譬如非法篡改交易数据、盗取用户个人账号信息进行网络诈骗等，不仅危害了用户的个人利益，同时也严重影响了商家的形象。

能解决的问题：

网站遭遇大量请求以及异常连接导致用户服务性能严重下降影响正常用户业务服务，如部署waf 可通过 waf 爬虫策略将异常链接自动进行中断以及一部分常见的http 缓慢攻击等制定链接时长限制，降低网站因收到爬虫类会降低响应，也避免了给网站用户带来负面使用体验。

1.3.4 航空行业场景

场景特点：

航空行业、互联网售票平台等都拥有大量的旅客个人信息以及出行/未出行、行程信息，而这些信息经过黑色产业链，最终形成了退改签等诈骗活动，不仅危 害了旅客的个人利益，也给各平台造成了经济损失。

能解决的问题：

当固定类型系统发布漏洞，如 log4j 等，waf 集群策略库会收集现网所有关于web 安全方面的漏洞将在 24 小时内自动进行策略加固，无需用户侧手动接入完成 0day 相关安全报障，如客户侧针对安全方面不熟悉，可能无法第一时间收到通知，使用 waf 将大大降低客户应用业务被漏洞利用的风险。

2. 产品优势

天翼云 Web 应用防火墙为用户自助配置 Web 防护的能力，通过 DNS 牵引的方式，将业务流量牵引至 web 应用防火墙清洗设备，再由 web 应用防火墙清洗设备回源至源站，同时配套提供一个高度管控、灵活使用的管理平台，达到配置简单、服务资源监控方便的目标。

2.1 灵活的部署与应用方式

通过 DNS 解析方式接入，不需要安装任何软件，更不需要修改网站的任何代码，光速生效，一键启停，方便快捷。

2.2 灵活回源支持

waf 可以在云防护节点将https 业务流量转化为 http 业务流量回源，降低源站负载消耗，优化业务性能。

2.3 实时更新、智能学习的安全资料库

中国电信每天都在主动收集来自全世界的网站攻击手段、最新漏洞、补丁信息等安全资料，会比用户网站更早发现各类安全问题和攻击手段。一旦被认定为未知的安全问题和新型攻击手段，云防护平台将会自动更新所有安全节点的防护规则和监测范围，使所有加入云防护的网站免受未知攻击、漏洞等的危害。另外还会定期学习用户网站访问日志，不断细化为每一个网站量身定制的安全规则，不需用户人工干预，完善用户网站安全。

2.4 服务应急响应指标

网站安全防护服务为您提供 7×24 小时的专家团队技术支持，具备完善的故障监控、自动告警、快速响应等一系列应急响应机制。

2.5 专家级定制化安全报告

权威规则库，覆盖各类主流web 入侵类型，专业攻防团队实时更新防护系统。

2.6 特殊行为防护主动激励

主动识别绕过标准检测方法的恶意程序，在它们造成破坏之前减轻威胁。

3. 计费说明

3.1 计费模式

3.1.1 价格

基础套餐包 3488（元/月）

域名扩展包 540（元/月）

带宽扩展包 900（元/月）

基础套餐包月（元/月）	域名扩展包（元/月）	带宽扩展包（元/月）
3488	540	900

1、基础套餐：版本默认包含一个域名包（支持 10 个子域名防护(限制仅支持 1 个一级域名)、200MB

带宽

2、域名扩展包：每增加 1 个域名包规格，支持 10 个子域名防护(限制仅支持 1 个一级域名)

3、带宽扩展包：每单位规格 50MB，逐级增加，最大支持 1000MB

4、针对一次性包年付费服务，标准价格按照下述列表内容进行操作，且在订购时间期间不允许退订

一次性付费 1 年	一次性付费 2 年	一次性付费 3 年
包月标准价格*12*85%	包月标准价格*24*70%	包月标准价格*36*50%

3.1.2 订购

登录天翼云账号，在服务列表中找到安全组 Web 应用防火墙(企业版)，点击进入订购页面，如下图。

防护带宽默认显示 200M，域名包为 1 个，此为基础套餐包的量，用户可根据自己需求，增加防护带宽和域名包数量。并选择定能够时长。

采购参数建议：根据客户业务类型的不同针对带宽消耗也有所不同，其中视频播放类的业务对带宽消耗较大，如非视频播放类型业务对带宽消耗也会降低，相应支持QPS 也可增大,200mbps 最大可支持

3.2 续订

在产品实例列表点击【续订】跳转续订页面，页面显示当前服务规格和购买时长，选择续订时长，点击【立即购买】。

3.3 升级

在产品实例列表点击【升级】跳转升级页面，页面显示当前服务规格和升级后规格，用户可以选择升级后的防护带宽和域名包数量，勾选协议，点击【立即购买】。

3.4 退订

退订需要人工审核，点击【退订】，提交退订理由。等待人工审核，审核完成后停止业务并退款。

4. Web 应用防火墙防护接入

4.1 防火墙配置

1.查看当前资源信息

Web 应用防火墙不涉及单独的登录方式，进入控制台需要登录天翼云官网后选择-控制台-web 应用防火墙企业版。

购买成功的客户请重新打开控制中心，选择 web 应用防火墙企业版

防护实例展示了实例 ID、防护域名包数量、防护带宽、购买时间、到期时间以及操作。

实例 ID：购买成功后系统自动分配实例 ID

防护域名包数量：每个防护域名包支持一个一级域名下包含二级域名在内 10 个防护配置；

防护带宽：防护的带宽；

购买时间：显示生成购买实例时间；

到期时间：显示实例到期时间；

操作：续订，点击续订转跳至续订页面，选择续订时间，生成订单续订成功后，到期时间延长。

退订，点击退订转跳至退订页面，点击确认退订，退订时请确认：务必将 DNS 指回服务器源站

IP，否则该域名的流量将无法正常转发。

升级，点击升级跳转至升级页面，选择要升级的域名包或带宽

4.2 域名防护配置添加

防护配置管理为用户提供域名防护的配置操作功能：

Web 应用防火墙防护配置列表显示如下，展示用户的防护配置清单列表，展示字段包括：

防护域名、CNAME、源站 IP、源端口、协议类型、状态、防护带宽、操作

防护域名：展示被防护的域名，例如；www.ctyun.com

CNAME：展示防护域名 CNAME（CNAME 规则：**源域名+.iname.damddos.com）**

133 WAF 自服务控制台操作指南

源站 IP：用户配置的最终服务客户的主机 IP

源端口:源站 IP 的对外服务端口

状态：展示配置的防护状态，包括防护、未防护、启动防护中、防护配置失败；

防护带宽：用户购买实例的业务带宽大小；

操作：查看，查看防护配置详情，不能进行修改；

删除，点击删除，将当前的防护配置清除，需要确保防护域名指回源站；

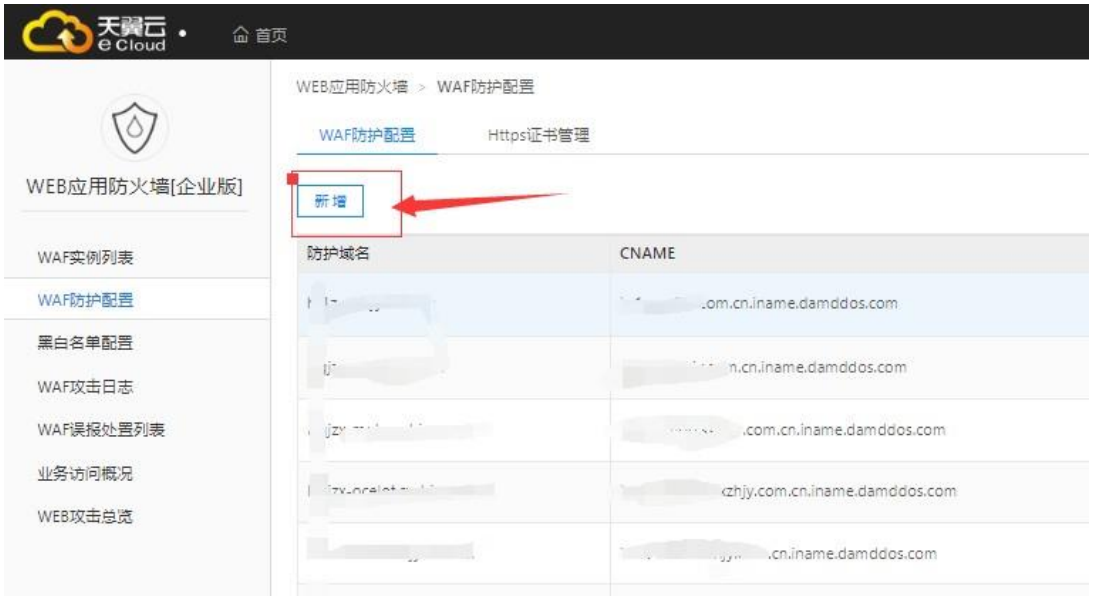
关闭防护，将正在防护中的任务关闭，需要确保防护域名指回源站；

开启防护，开启已新增（或者关闭过）的防护配置，开启成功后，您可以联系域名服务商

将 DNS 域名指向防护 Cname 地址，届时防护配置正式生效。

黑白名单，配置黑白名单，详见黑白名单配置。

修改，修改添加的防护配置（防护已经在关闭状态才可以修改）



新增：在 web 应用防火墙配置菜单下，点击新增，弹出 web 应用防火墙配置对话框：

新增防护配置详解：

选择实例 ID；实例即为默认开通资源，直接进行勾选即可

2、 选择数据中心；目前默认数据中心为内蒙，上海，广州，其中主选一个，备选一个，建议用户选择靠近自身资源部署地区的节点。

3、 输入防护域名；

输入格式示例：

防护网站域名：如 ctyun.cn

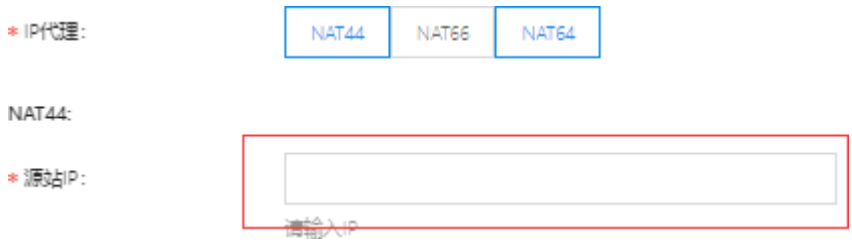
防护网站域名：如 www.ctyun.cn,

Ip 代理分为 nat44，nat66，nat64

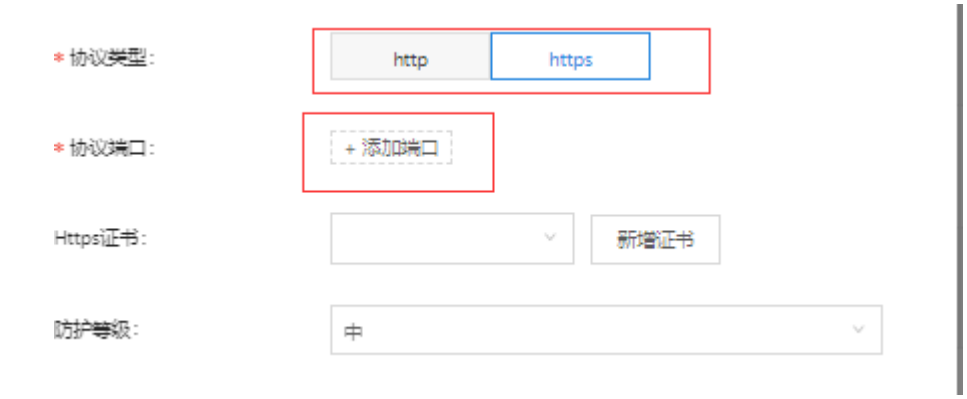
Nat44：网站如仅支持 ipv4 访问则单选 nat44，并且填写域名对应的公网 v4 地址至原站 ip 一栏。

Nat66：网站如同时支持 ipv4 以及 ipv6 访问则需要同时勾选

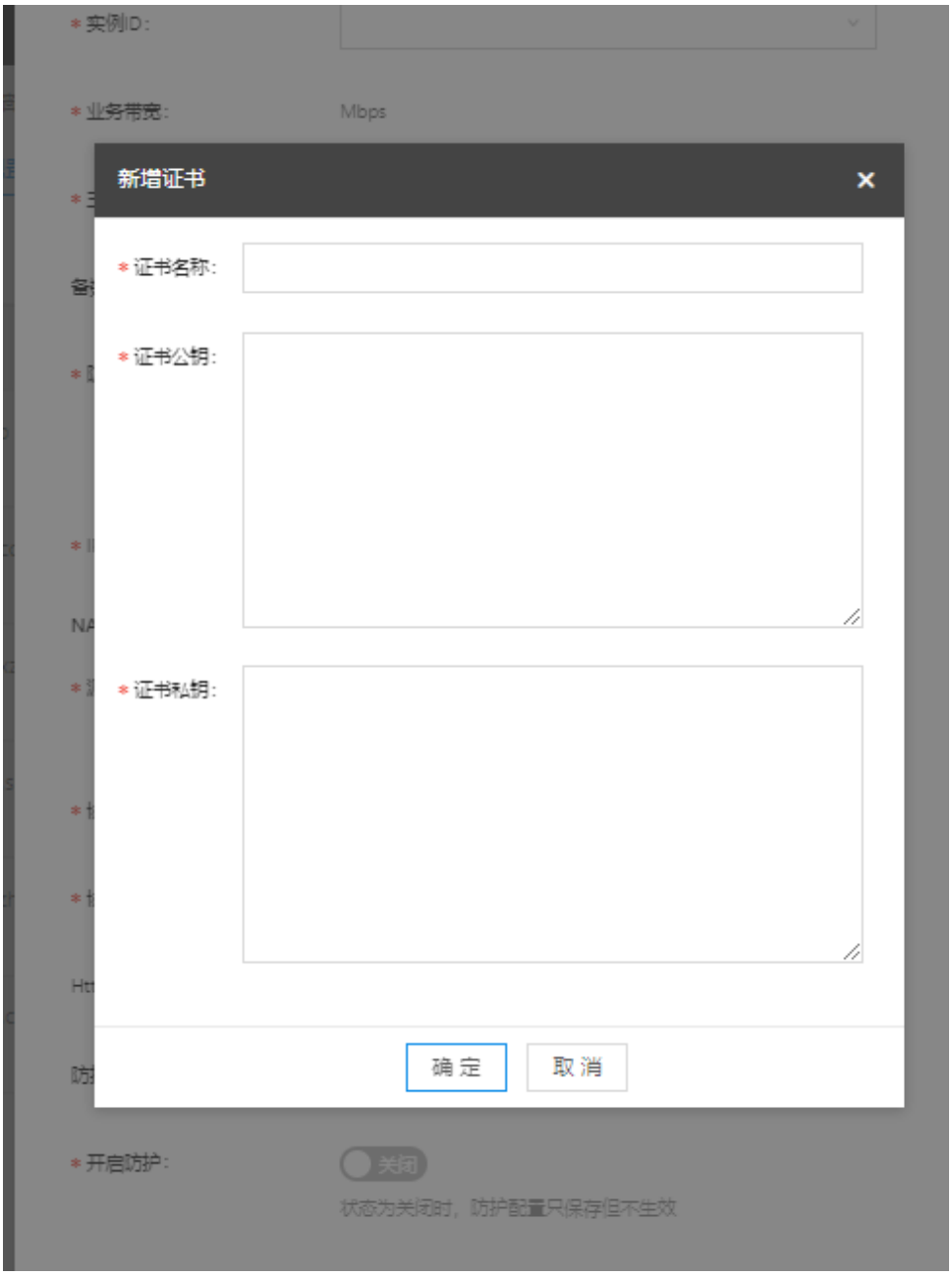
Nat64：在网站不支持 ipv6 的场景下，waf 可以协助网站支持ipv6 访问，waf 接收到 ipv6 请求后将流量转换成 ipv4 的形式发送给客户原站，需要同时勾选 nat44 与 nat64，原站 ip 侧应填写 ipv4 地址。



5.选择对应的协议进行端口添加。



如网站涉及 https 端口需要进行证书上传，点击新增证书



点击新增证书后弹出图上页面

证书名称：证书名称可自定义添加

证书公钥：一般情况下 https 证书需要从网站本身服务器上进行导出或联系域名服务商获取，证书一般以 pem 或 crt 结尾用文件形式打开后全量粘贴到图上公钥内。

证书私钥：私钥一般以 key 结尾，同样需要用文本形式打开后粘贴到图上私钥内点击确认。

6、 开启防护（默认勾选），如果未选中开启防护按钮，该配置不会生效，业务不会下发至 web 应用

防火墙设备进行防护。

点击保存，确认后，正式下发防护配置。

添加完显示应为图下

域名：域名为当前防护的域名

Cname：cname 地址为waf 配置成功后生成的代理地址（需要用户侧联系域名服务商将域名原本指向的记录值修改为waf 的地址）。

源 ip：源 ip 及配置waf 的目标地址，waf 接收请求后会将请求转发至当前配置的地址

源端口：waf 所配置的端口

状态：当配置处于防护中时为正常，配置状态为防护中时 cname 地址才可以被解析到

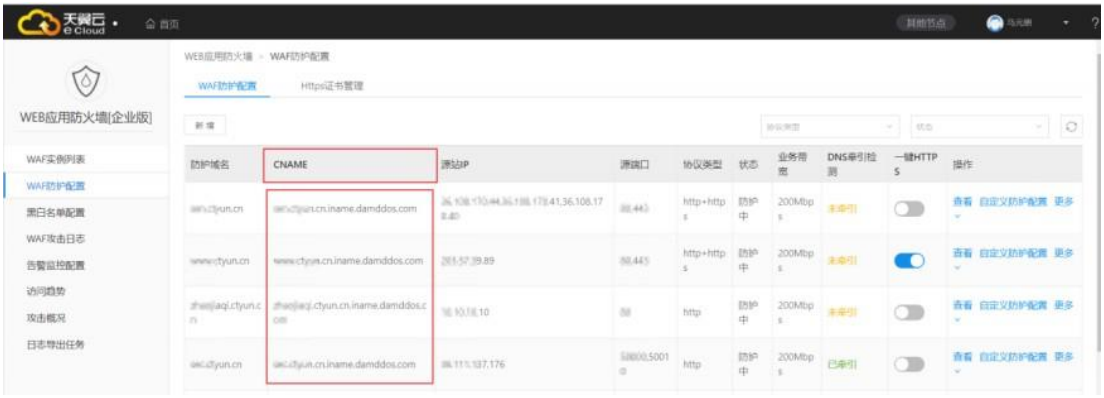
防护带宽：与当前资源相关，对应当前的资源规格

Dns 牵引检测：当用户将域名解析至 waf 后，此状态会在当天凌晨自动更新为已牵引

https 强制跳转：当域名同时开通 80 与 443 端口时勾选强制跳转会让所有访问 80 端口的流量自动跳转到 443（暂时只支持 80 跳转 443）.

4.3 本地接入云 WAF 测试

获取 CNAME 值，您可以通过添加配置后在自服务界面 waf 防护配置重获取 waf 生成的 cname 记录值



2）ping“CNAME”值并记录“CNAME”对应的 IP 地址以域名 portal.damddos.com 为

例，该域名已添加到 WAF 的网站配置中，且 WAF 为其分配了以下 CNAME 值：

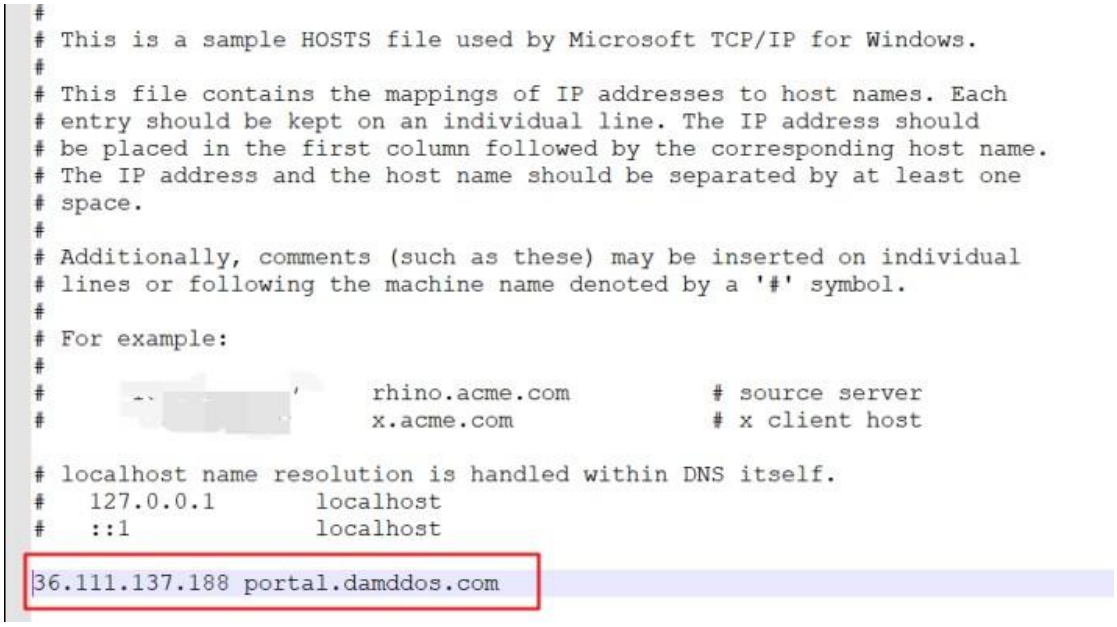
portal.damddos.com.iname.damddos.com。

在 Windows 中打开 cmd 命令行工具，运行 ping portal.damddos.com.iname.damddos.com 获取 WAF 的回源 IP。如图所 示，在响应结果中可以看到用来防护您的域名的 WAF 回源 IP

3）在本地修改 hosts 文件，将域名及“CNAME”对应的 WAF 回源 IP 添加到“hosts”文件。

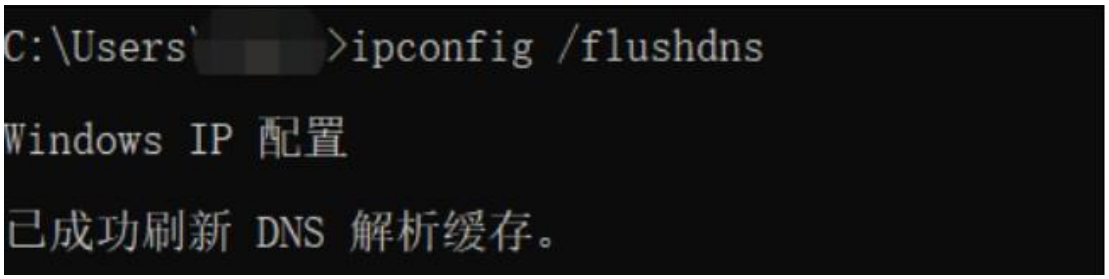
1. 用记事本或 notepad++等文本编辑器打开 hosts 文件，hosts 文件一般位于“C:\Windows\System32\drivers\etc\”路径下。

2. 在 hosts 文件添加记录内容，对应的 IP 地址即在上述步骤中获取的云 WAF 防护 IP 地址，后面的域名即被防护的域名



3. 修改 hosts 文件后保存，然后本地 ping 一下被防护的域名。

此时解析到的 IP 地址应该是 2 中绑定的云 WAF 防护 IP 地址。如果依然是源站地址. 可尝试刷新本地的 DNS 缓存（Windows 的 cmd 下可以使用 ipconfig /flushdns 命令）。



验证 WAF 正常转发

1）清理浏览器缓存，在浏览器中输入防护域名，测试网站域名是否能正常访问。

如果 hosts 绑定已经生效（域名已经本地解析为云 WAF 防护 IP）且云 WAF 的配置正确，访问该域名，预期网站能够正常打开。

2）手动模拟简单的 web 攻击命令，测试 Web 攻击请求。

1.waf 基础防护的状态默认设置为“拦截”模式。

2.清理浏览器缓存，在浏览器中输入

“https://portal.damddos.com/url/ril/ashi.asp=javascript:alert(/xss/)”模拟 SQL 注入攻击，测试 WAF 是否拦截了此条攻击，如图所示

3.在自服务平台导航树中，选择“WAF 防护日志”，进入“WAF 防护日志”页面，查看防护域名测试的各项数据。

4.4 接入前须知

4.4.1 防护回源 IP 放行

业务接入云 WAF 防护平台清洗后，所有请求的客户端源地址都会变为云 WAF 回源IP 段，从客户源站侧的安全设备或安全软件（如：IPS、网络防火墙、流量管理系统、本地 WAF 应用防火墙、网站安全狗与云锁等）可能认为是攻击行为进行封禁，造成云 WAF清洗 后的请求无法得到源站正常响应，因此客户侧需要根据所开通防护中心的回源 IP 段（内 蒙数据中心：36.111.137.0/24 与 203.57.157.0/24，北京数据中心：203.34.106.0/24，上海数据中 心：101.226.7.0/24，广州数据中心：203.32.204.0/24）

添加到源站侧的访问控制策略与安全 软件白名单中，避免由云 WAF 转发回源站的业务流量被判断为异常攻击造成误封禁，影响网站正常访问。

4.4.2 域名解析

配置成功后，防护配置的状态变为：“防护中”；

之后客户可以进行域名解析：

如域名：www.ctyun.com

需要客户联系 DNS 服务商将域名解析指向 Cname：www.ctyun.com.iname.damddos.com

即：源域名+.iname.damddos.com

DNS 牵引指向 Cname 后，web 应用防火墙防护正式完成配置。

记录类型	NS	CNAME	A	URL	MX	TXT	AAAA	SRV	CAA
NS	可重复	冲突	冲突	冲突	冲突	冲突	冲突	冲突	冲突
CNAME	冲突	可重复	冲突	冲突	冲突	冲突	冲突	冲突	冲突
A	冲突	冲突	可重复	冲突	不冲突	不冲突	不冲突	不冲突	不冲突
URL	冲突	冲突	冲突	冲突	不冲突	不冲突	冲突	不冲突	不冲突
MX	冲突	冲突	不冲突	不冲突	可重复	不冲突	不冲突	不冲突	不冲突
TXT	冲突	冲突	不冲突	不冲突	不冲突	可重复	不冲突	不冲突	不冲突
AAAA	冲突	冲突	不冲突	冲突	不冲突	不冲突	可重复	不冲突	不冲突
SRV	冲突	冲突	不冲突	不冲突	不冲突	不冲突	不冲突	可重复	不冲突
CAA	冲突	冲突	不冲突	不冲突	不冲突	不冲突	不冲突	不冲突	可重复

4.4.3 设置源站保护

出于安全性考虑，建议您在业务流量成功接入云 WAF 防护后，禁止通过 IP 直接访问业务，同时设置源站侧的访问控制策略，只允许云 WAF 回源 IP 段和其他可信任地址之内的 IP 访问业务，避免攻击者获取您的源站 IP 后绕过云 WAF 直接攻击源站。

4.4.4 获取客户端真实 IP

网站若使用了流量代理服务（如 CDN、DDoS 高防、云 WAF），达到源站的 IP 均将显 示为相关服务的代理回源 IP 地址，云WAF 在 HTTP 请求头部中默认插入了X-Forwarded-For 字段，用于记录客户端真实 IP，源站服务器可以通过解析回源请求中的

X-Forwarded-For 记录，获取客户端的真实 IP，各类型的 Web 应用服务器针对该字段的提取配置可联系安全防护工程师提供技术支持。

4.4.5 与 CDN 结合使用

云 WAF 与 CDN 完全兼容，可以通过与 CDN 的结合使用，为开启 CDN 内容加速的业务 同时提供 Web 攻击防护。 若已经接入 CDN 服务，将云 WAF 为防护域名分配的 CNAME 地址作为 CDN 的源站即可。

客户端 > CDN > 云 WAF > 源站，流量将按照用户 > CDN > WAF >源站的 架构回源。同时，需要您联系 CDN 服务商，将客户端的真实 IP 通过 client-IP 字段插入至HTTP 请求头部中，并告知安全防护工程师进行提取配置，保证云 WAF 正常防护。

4.4.6 防护策略说明

1）云 WAF 防护服务目前默认策略分为低、中、高与 AI 学习模式。各防护策略均包含上述攻击类型在内的安全防护，策略等级越高越严格，攻击漏拦截概率越小，对业务 访问影响程度可能更高（业务代码不规范也会触发阻断策略）。低级防护策略主要针对 攻击特征比较明显的违规请求，适用于站点存在较多不可控用户输入（如含有富文本编 辑器的网站业务）的业务场景；一般情况下，中级防护策略适用于绝大部分业务场景的 Web 防护需求；高级防护策略采用了最精细的防护颗粒度，适用于对业务安全性要求较高， 同时需要网站开发人员高度参与策略定制与防护过程的业务场景。如对站点业务流量特 征还不完全清楚，可以启用 AI 学习模式，该模式下 AI 学习引擎会自动学习网站的访问 模式与流量特征，经过 7 到 14 天的分类训练和流量学习后会对所有策略根据机器算法进 行评分，保留学习后符合标准的策略规则，大幅减少误报，提高对已知与未知 Web 安全 威胁的防护效果，同时，可联系天翼云安全工程师基于学习期间的攻防日志，进一步优化安全防护策略和配置。

2）接入云 WAF 防护服务后，当启用防护策略时，即便是低级防护策略，可能也会因为网站代码实现不够规范或用户通过非常规方式访问等情况，造成用户的上传搜索等正常操作有可能被误认为是攻击而拦截掉。当业务访问出现误报较多的情况，建议将防护模式调整为观察模式，通过自服务平台查看告警日志，并及时观察业务的正常使用情况发现误报请求后第一时间联系天翼云安全工程师优化安全防护策略。

4.4.7 调整防护策略

切换 CNAME 接入防护后，您可以通过登录自服务平台进行包括防护规则，CC 防护，地区封禁，攻击防绕过和 HTTP 合规性检测等功能在内的自定义防护配置调整。防护策略针对不同行业客户支持个性化定制，可直接联系天翼云指定的安全工程师提供技术支持，

工程师将根据实际使用情况与攻防日志进行策略调整优化， 24 小时值班电话：400-810-9889 语音提示后，请按“2”转接人工服务。

5. 操作指导

5.1 Web 应用防火墙实例管理

购买成功的客户请重新打开控制中心，选择web 应用防火墙企业版

防护实例展示了实例 ID、防护域名包数量、防护带宽、购买时间、到期时间以及操作。

实例 ID：购买成功后系统自动分配实例 ID

防护域名包数量：每个防护域名包支持一个一级域名下包含二级域名在内 10 个防护配置；

防护带宽：防护的带宽；

购买时间：显示生成购买实例时间；

到期时间：显示实例到期时间；

操作：

续订，点击续订转跳至续订页面，选择续订时间，生成订单续订成功后，到期时间延长。

退订，点击退订转跳至退订页面，点击确认退订，退订时请确认：务必将 DNS 指回服务器源站 IP，否则该域名的流量将无法正常转发。

升级，点击升级跳转至升级页面，选择要升级的域名包或带宽。

5.2 防护配置菜单

在 Web 应用防火墙配置菜单下，点击新增，弹出WAF 配置对话框：

1、 选择实例ID；

2、 输入防护域名；

3、 填入源站IP；

4、 选择协议类型，填入源端口，http+https 最多共填入 10 个端口；

5、 选择防护级别，高、中、低；

6、 如果有 Https 情况下，需要选择 https 证书（https 证书可以通过新增https 证书实现上传）；

7、 开启防护（默认勾选），如果未选中开启防护，该配置项目将不会下发至WAF 设备进行WAF 防护;

8、 点击保存，确认后，正式下发防护配置。

5.3 域名备案

5.3.1 实例管理

防护配置管理为用户提供域名防护的配置操作功能：

1、 Web 应用防火墙防护配置列表

显示如下，展示用户的防护配置清单列表，展示字段包括：

防护域名、CNAME、源站 IP、源端口、协议类型、状态、防护带宽、操作

防护域名：展示被防护的域名，例如；www.ctyun.com

CNAME：展示防护域名 CNAME（CNAME 规则：源域名 +.iname.damddos.com）

源站 IP：用户配置的最终服务客户的主机 IP

源端口:源站 IP 的对外服务端口

状态：展示配置的防护状态，包括防护、未防护、启动防护中、防护配置失败；

防护带宽：用户购买实例的业务带宽大小；

操作：查看，查看防护配置详情，不能进行修改；

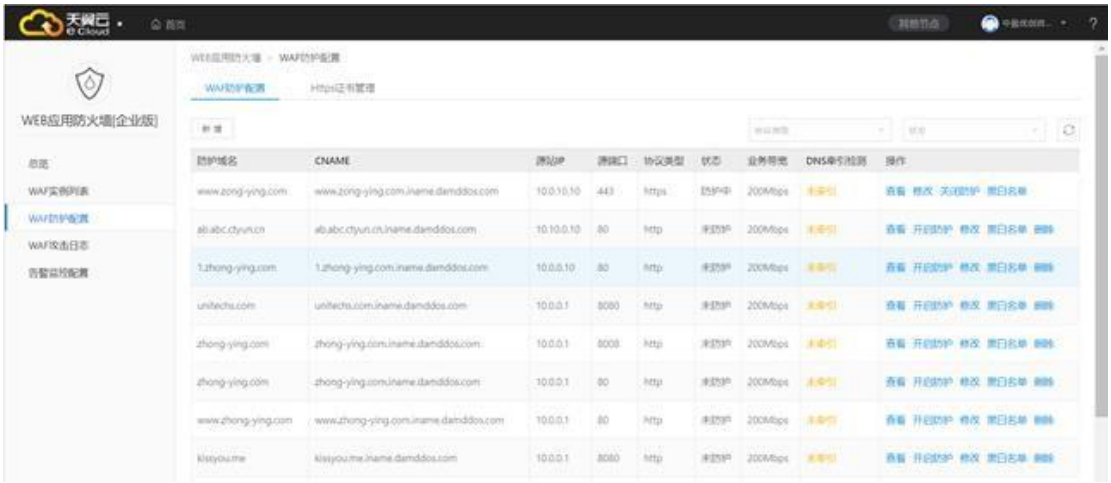
删除，点击删除，将当前的防护配置清除，需要确保防护域名指回源站；

关闭防护，将正在防护中的任务关闭，需要确保防护域名指回源站；

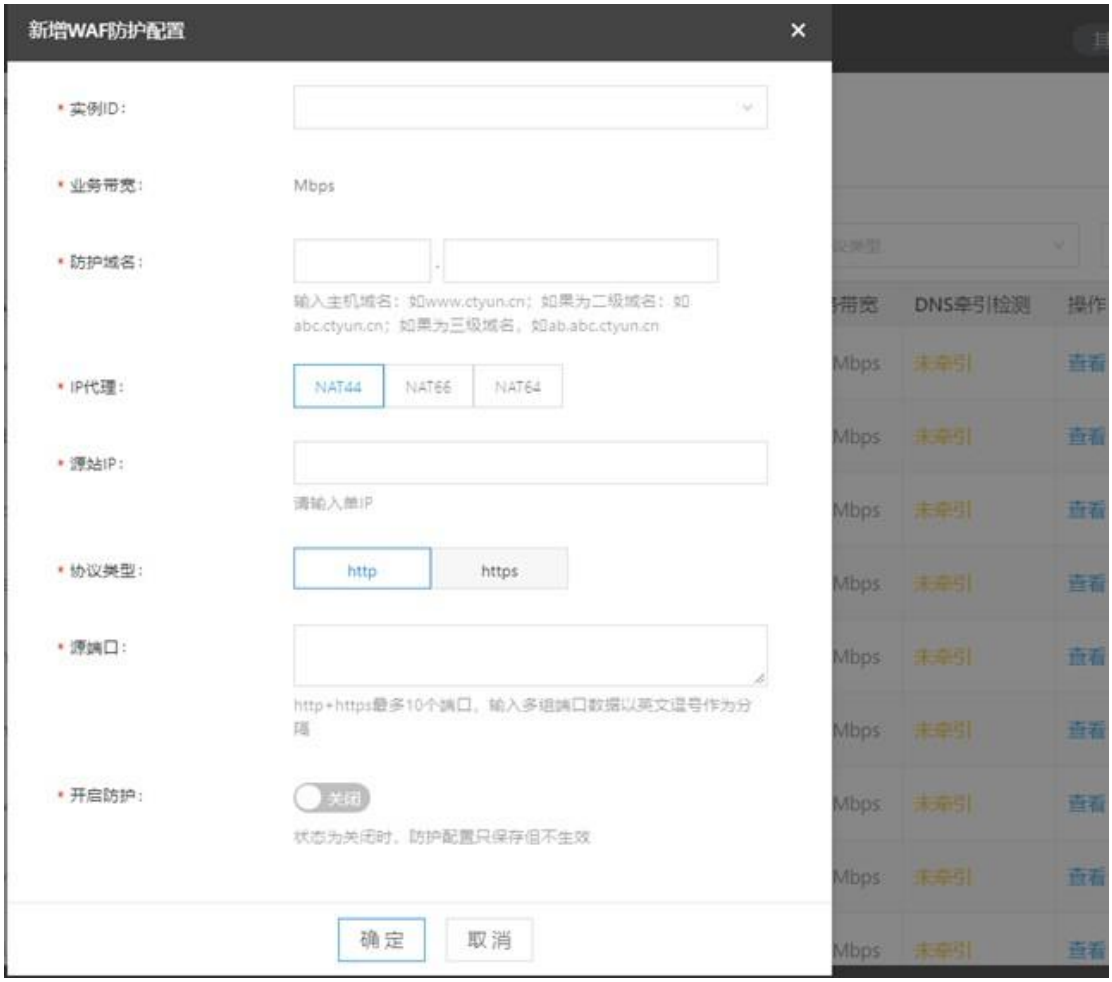
开启防护，开启已新增（或者关闭过）的防护配置，开启成功后，您可以联系域名服务商将 DNS 域名指向防护Cname 地址，届时防护配置正式生效。

黑白名单，配置黑白名单，详见黑白名单配置。

修改，修改添加的防护配置（防护已经在关闭状态才可以修改）



2、 新增：在web 应用防火墙配置菜单下，点击新增，弹出web 应用防火墙配置对话框：



1、 选择实例ID；

2、 输入防护域名；

输入格式示例：

防护网站域名：如www.ctyun.cn,

如为域名：如abc.ctyun.cn.com，

如为域名：如 M.abc.ctyun.cn

如为域名：ctyun.cn

选择解析方式；

如果域名仅支持ipv4 则选择 nat44

如果同时支持 ipv4 与 ipv6 则选择 nat44+nat66

nat64 是指原站有 v4 的地址

3、 填入源站IP；

4、 选择协议类型，填入源端口，http+https 最多合在一起最多填入 10 个端口，多个端口之间用英文逗号分隔；

5、 如果有 Https 情况下，需要选择https 证书（https 证书可以通过新增 https 证书实现上传）

如果为初次填入 https 证书，可以点击 “新增证书”

进入：页面创建证书，证书创建成功后选择刚刚创建的证书。

6、 开启防护（默认勾选），如果未选中开启防护按钮，该配置不会生效，业务不会下发至web 应用防火墙设备进行防护。

7、 点击保存，确认后，正式下发防护配置。

5.3.2 Https 证书管理

点击 https 证书管理 

，弹出 https 证书管理：

可以新增、删除证书。

Notice：删除证书需要确保证书未被使用或未被配置。

点击新增：

证书名称：输入证书名称，证书名称客户可以自行定义；

证书公钥：填入公钥字符串，如果用户公钥为文件格式，通过记事本打开公钥文件后，拷贝证书公钥字符串填入。

证书私钥：填入私钥字符串，如果用户私钥为文件格式，通过记事本打开私钥文件后，拷贝证书私钥字符串填入。

点击确认，保存公钥、私钥。

点击“删除证书”：删除证书时需要确认防护配置中（包括未启动的防护）未使用该证书，否则删除不成功。

5.3.3 域名解析

配置成功后，防护配置的状态变为：“防护中”；

之后客户可以进行域名解析：

如域名：www.ctyun.com

需要客户联系DNS 服务商将域名解析指向 Cname：
www.ctyun.com.iname.damddos.com

即：源域名+.iname.damddos.com

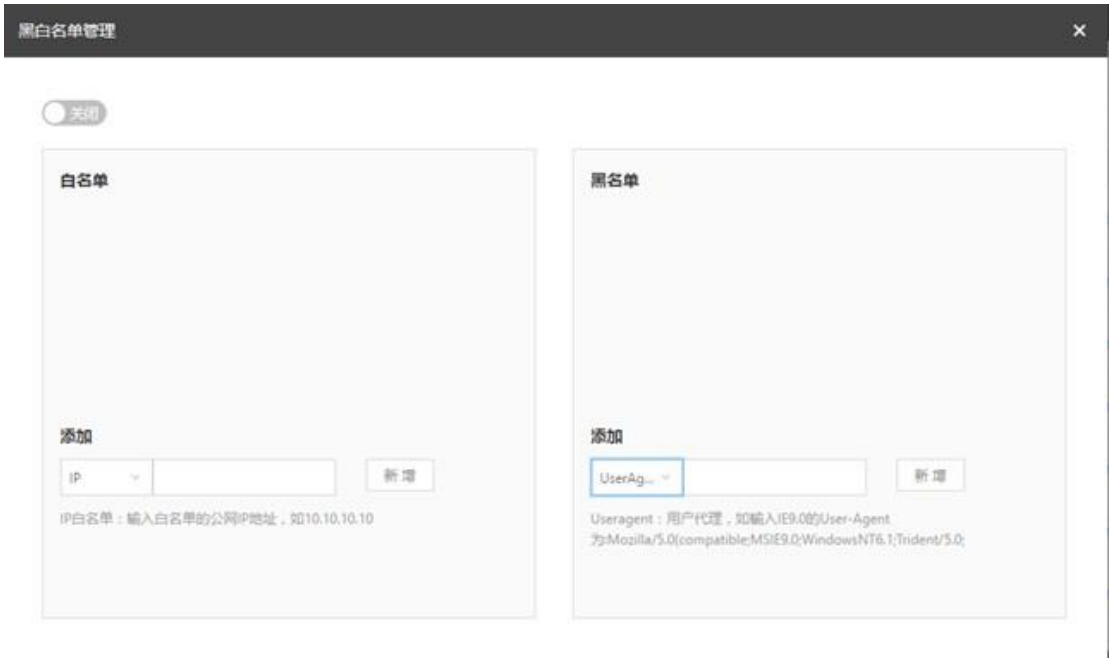
DNS 牵引指向 Cname 后，web 应用防火墙防护正式完成配置。

5.3.4 黑白名单管理

Web 应用防火墙防护可以配置黑白名单，配置的参数包括：IP、URL、UserAgent、Referer

黑名单：配置了黑名单，所有访问来源全部屏蔽。

白名单：配置了白名单，所有访问来源全部放行。



IP 黑白名单：输入黑白名单的公网 IP 地址，如 10.10.10.10；

URL 黑白名单：输入黑白名单的 URL 地址，如www.ctyun.cn；

Referer 黑白名单：指 HTTP 来源地址，比如如果点击一个网页的网址链接，那么浏览器会产生一个送到目标的 Web 服务器的 HTTP 请求，该请求中则会包含一个 Referer 字段（网页的地址），如网页URL 为 http://www.ctyun.cn/product/cda，则输入 http://www.ctyun.cn/product/cda；

Useragent 黑白名单：Useragent 为用户代理，输入代理 Useragent 标识，如 IE9.0 的 Useragent 为:Mozilla/5.0(compatible;MSIE9.0;WindowsNT6.1;Trident/5.0;

当选择为关闭时，黑白名单配置不生效；

当选择为开启时，黑白名单配置生效。

5.3.5 全局黑白名单管理

Web 应用防火墙可以配置用户的全局黑白名单，即可以选择一个防护域即一级域名（选择防护域后，系统会关联这个域下面的所有域名）进行防护黑、白名单配置，配置的参数包括：配置类型，防护域、防护域名、黑白名单类型、黑白名单内容；

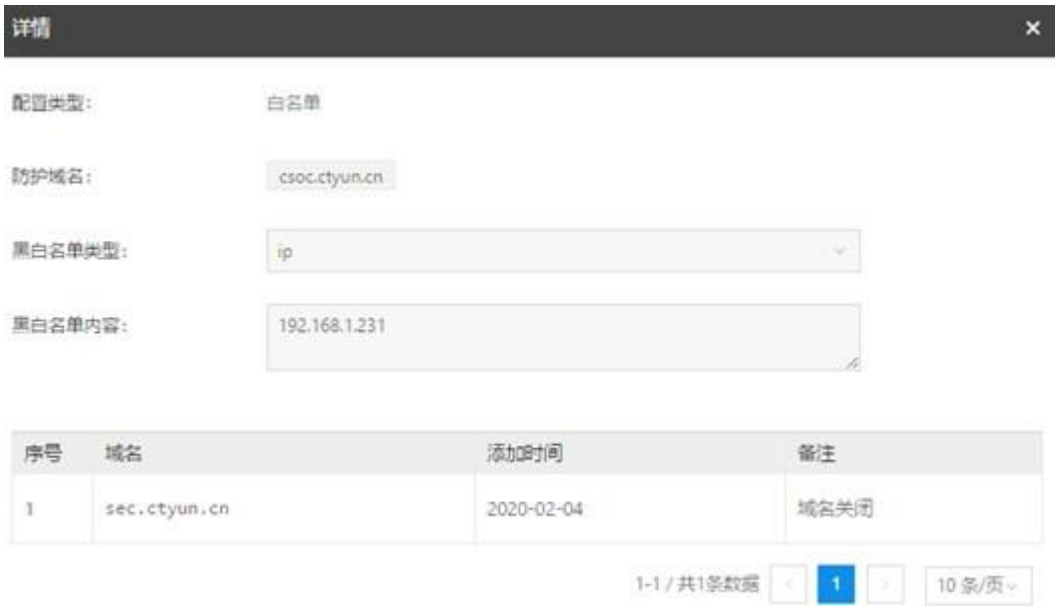
配置类型：即配置黑名单或者白名单

防护域：如www.ctyun.com、mail .ctyun.com 的防护域为 ctyun.com。

防护域名：即黑名单或者白名单配置后，对防护域下面在用的子域名进行关联，黑白名单将对关联的黑白名单生效，同时配置人员可以对关联的子域名进行人工删除/增加，精确实现对防护域下面的指定子域名进行黑白名单配置。

可以对黑白名单进行关闭，包括直接关闭以及在域名配置中对实现对单个域名的改配置的关闭，

点击 并确认，关闭全局黑白名单配置中详情展示：



黑白名单类型：包括 ip、referer、url、useragent 四种类型。

IP 黑白名单：输入黑白名单的公网 IP 地址，如 10.10.10.10；

URL 黑白名单：输入黑白名单的 URL 地址，如如访问 URL 为 https://www.ctyun.cn/console/index，则填入/console/index，支持模糊匹配，如当输入/console/index 后，https://www.ctyun.cn/console/index/##/也会匹规则；

Referer 黑白名单：指 HTTP 来源地址，比如如果点击一个网页的网址链接，那么浏览器会产生一个送到目标的 Web 服务器的 HTTP 请求，该请求中则会包含一个 Referer 字段（网页的地址），如网页为 http://www.ctyun.cn/product/cda，则输入 http://www.ctyun.cn/product/cda；

Useragent 黑白名单：Useragent 为用户代理，输入代理 Useragent 标识，如 IE9.0 的 Useragent 为:Mozilla/5.0(compatible;MSIE9.0;WindowsNT6.1;Trident/5.0。

5.3.6 关闭防护

Web 应用防火墙防护配置中：

点击关闭防护，关闭防护需要首先确保将 DNS 指回源站，否则该域名的流量将无法正常转发，请确定关闭该域名的防护功能。

5.3.7 暂停防护

Web 应用防火墙防护配置中：

点击暂停防护，web 应用防火墙会将原本经过 web 应用防火墙的流量全部放行给源站，不做拦截，此功能算是解决客户临时特殊需求时的缓解功能，点击恢复即可重新开启防护。

5.4 Https 证书管理

点击 https 证书管理，弹出 https 证书管理：

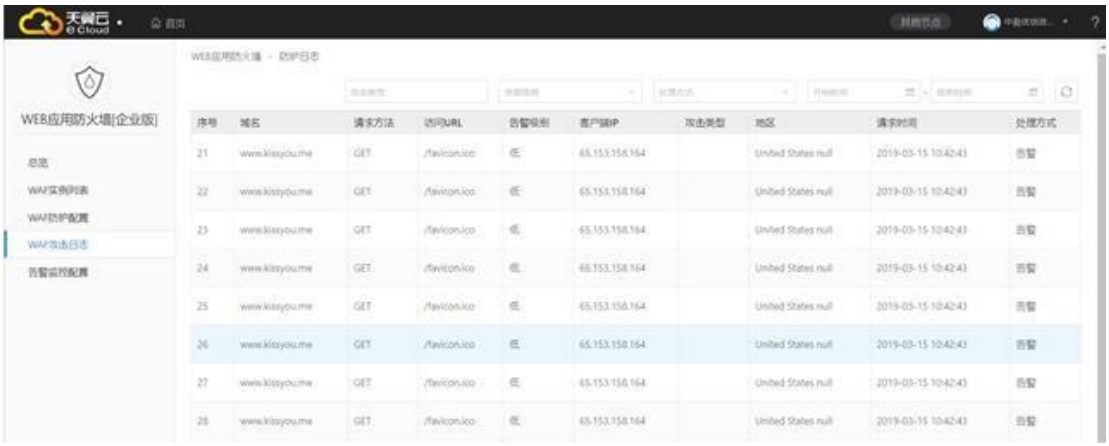
可以新增、删除证书。

注意：删除证书需要确保证书未在使用中以及防护配置中配置。

5.5 攻击日志

攻击日志展示被防护域名的所有攻击事件。

点击菜单【攻击日志】，进入【攻击日志】页面；



攻击日志显示：

- 域名：告警域名
- 请求方法：http get/http post
- 访问URL
- 告警级别
- 客户端 ip
- 地区
- 请求时间
    - 处理方式

5.6 黑白名单配置

Web 应用防火墙防护可以配置黑白名单，配置的参数包括：IP、URL、UserAgent、Referer

黑名单：配置了黑名单，所有访问来源全部屏蔽

白名单：配置了白名单，所有访问来源全部放行

点击菜单【攻击日志】，进入攻击日志页面，可以显示的字段包括，请求方法、访问URL、告警级别、地区、请求时间、处理方式。

5.7 总览

1. 点击菜单【总览】，进入页面；
2. 展示监控网站详情：
3. 域名数量及域名

4. 显示溯源图

- 攻击流量溯源图（BPS）

显示单个域名的通过Web 应用防火墙的每秒流量，包括总流量、CC 攻击流量、放行流量

- 攻击流量溯源图（TPS）

显示单个域名通过Web 应用防火墙的每秒访问数，包括总个数、CC 攻击个数。

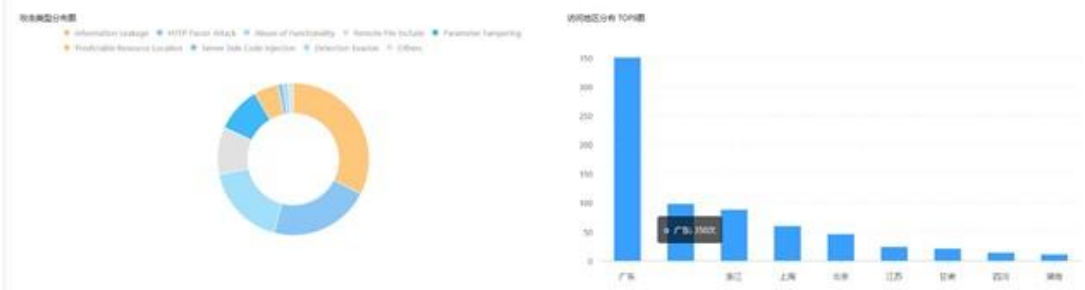
- 检测到的攻击访问 pv 数量

Web 阻断的数量也就是进行拦截的数量

UV（Unique Visitor）独立访客，统计 1 天内访问某站点的用户数

- 地区访问分布（地图）

展示按省份访问来源分布图



- 攻击类型分布

展示 TOP4+other 攻击类型分布饼状图

- 地区访问分布 Top5

展示 top5 攻击来源（省/市）柱状图

6. 自服务平台使用说明

6.1 访问趋势总览

1. 点击菜单【访问趋势】，进入页面；

在“WAF 防护报表”页面，您可以查看昨天、今天、7 天、15 天、30 天及自定义时间所有防护网站的访问趋势。访问趋势包括访问总量与流量类型占比，响应码信息，带 宽趋势统计以及访问来源国家/地区 TOP5、访问源 IP Top10、访问 URL Top10、访问来源区域 Top10 等防护数据。

前提条件：

1）已添加了防护域名并已完成了域名接入。

2）WAF 防护已开启。

操作步骤：

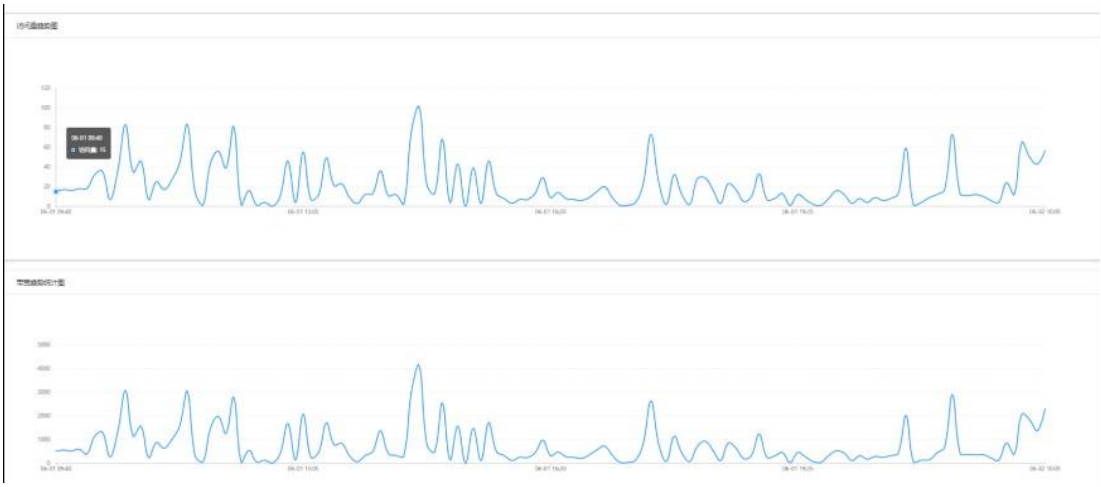
1）登录天翼云官网进入控制中心 web 应用防火墙企业版控制台

2）进入“访问趋势”页面。

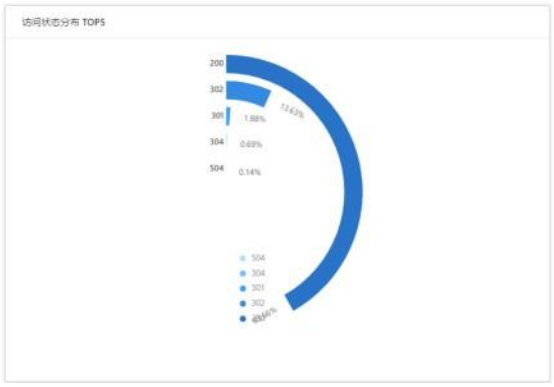
3） 在网站下拉列表中，选择要查看的网站（默认是所有在防域名数据汇总），以

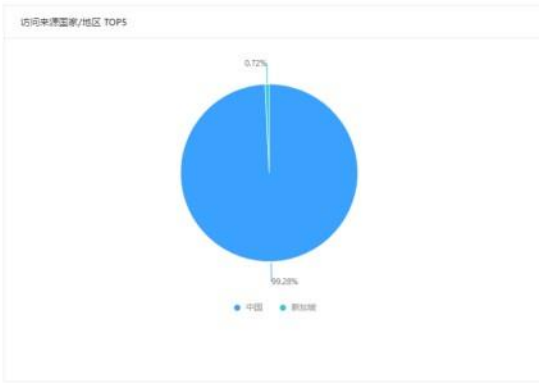
及选择查看的历史时间段（实时、7 天、15 天、30 天及自定义），可以查看统计的请求

次数和各类型的流量占比，以及详细的访问信息，如图所示，详细信息说明如表

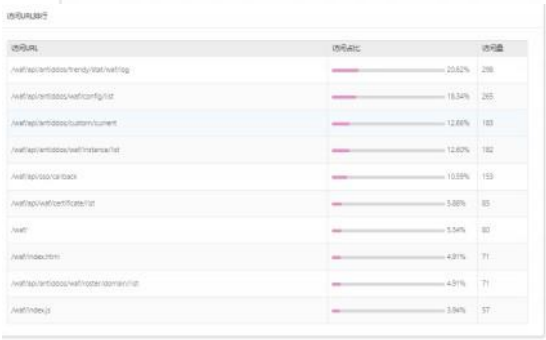


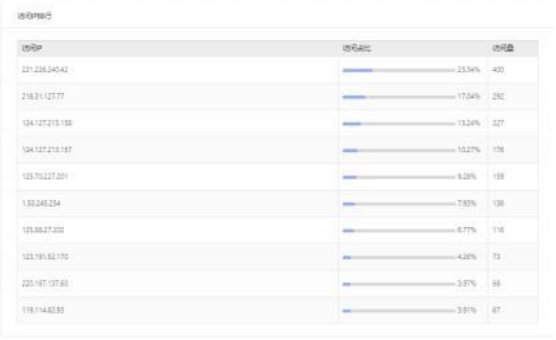
天翼云

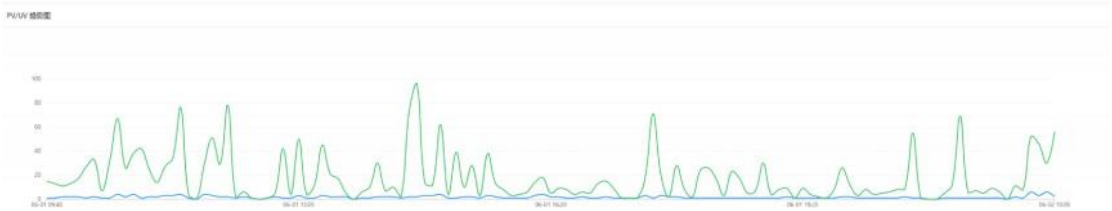

访问状态分布 TOP5
200
302
301
304
504
73.63%
1.88%
0.69%
0.14%
504
304
301
302


访问来源国家/地区 TOP5
0.72%
99.28%
中国


访问热力图
地区
访问量
访问占比


访问URL排行
访问URL
访问占比
访问量


访问IP排行
访问IP
访问占比
访问量


PV/UV 趋势图

访问趋势参数说明

参数	说明
访问总量	域名访问的总次数。
峰值带宽	域名防护支持的最大带宽。
流量类型占比	各类型流量在总流量的占比
PV（Page Views）值	即页面浏览量或点击量，是用来衡量一个网站或页面用户访问量
UV(unique visitor)值	即独立访客数，指访问某个站点或点击某个网页的的不同访问者(公网IP地址+每台电脑的唯一标识构成不同的访问者)的人数
接收请求数	指成功转发到服务器的请求数量
源站未响应	指天翼云将请求转发至源站服务器，但源站服务器没有对该请求进行处理或响应
白名单放行	指对 IP，URL 等添加过白名单的访问汇总
TPS 值	即服务器每秒处理的事务数
访问状态分布	可以查看“WAF 返回客户端”和“源站返回给 WAF”对应响应码以及响应占比。
访问来源国家/地区	访问次数 TOP 5 的地区以及来源各地区发起的访问次数。
访问 URL	访问统计次数 TOP 10 的 URL。
访问源 IP	访问统计次数 TOP 10 的 IP
源站延时	指一个数据包从 WAF 发送到网站服务器，然后再立即从网站服务器返回 WAF 的来回时间

6.2 攻击概况总览

点击菜单【攻击概况】，进入页面；

在“WAF 防护报表”页面，您可以查看实时、7 天、15 天、30 天及自定义时间所有防护网站的攻击趋势。访问趋势包括攻击拦截次数与拦截比例，告警类型分布统计以及攻击来源国家/地区 TOP5、攻击类型 TOP5、攻击 URL Top10、攻击 IP Top10 等防护数据。

前提条件：

1）已添加了防护域名并已完成了域名接入。

1）WAF 防护已开启。

操作步骤

1）登录天翼云官网进入控制中心 web 应用防火墙企业版控制台

2）进入“攻击趋势”页面。

3） 在网站下拉列表中，选择要查看的网站（默认是所有在防域名数据汇总），以

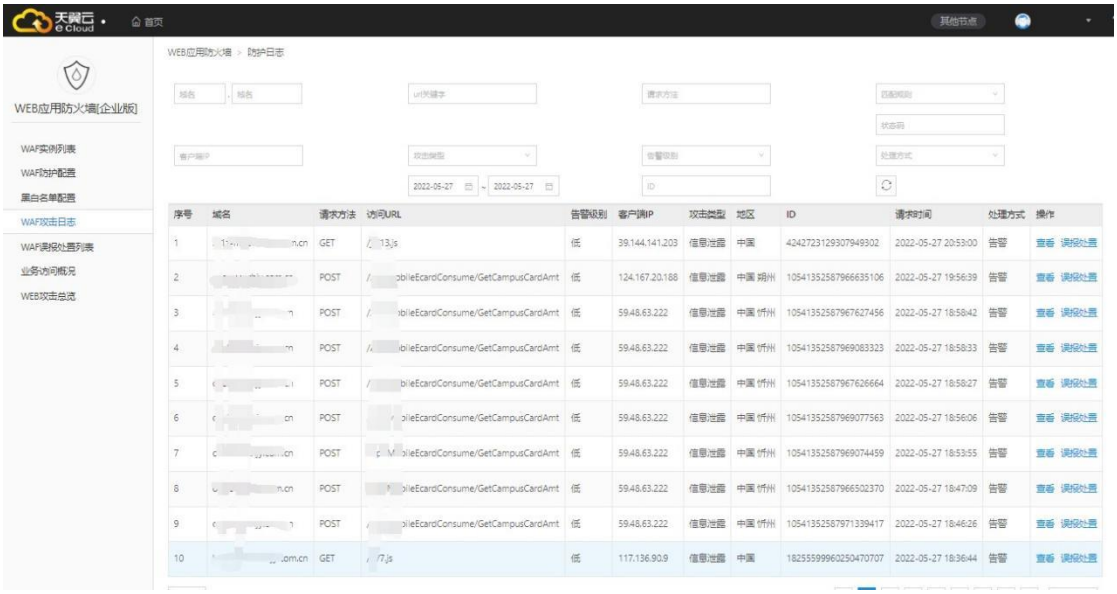
及选择查看的历史时间段（实时、7 天、15 天、30 天及自定义），可以查看统计的攻击次数和拦截占比，以及详细的攻击信息，如图所示，详细信息说明如表所示。

6.3 攻击日志查询

攻击日志展示被防护域名的所有攻击事件。

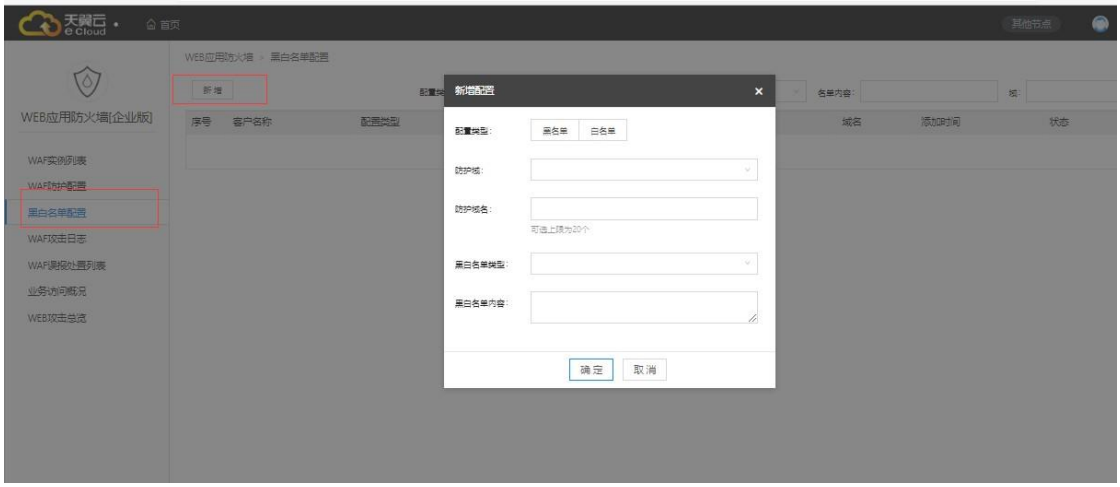
点击菜单【攻击日志】，进入【攻击日志】页面；

访问日志分析：可提供详细的访问日志分析，包括用户来源，访问 URL、告警级别、客户端 IP、访问者地域分布、请求时间、访问量统计等不同内容。并可进行全量日志查询，针对输入的内容进行筛选，包括告警级别、匹配规则、处理方式、请求时间段等内容。（默认针对客户域名存储防护日志周期为 180 天）



- 域名：告警域名
- 请求方法：http get/http post
- 访问 URL
- 告警级别
- 客户端 ip
- 地区
- 请求时间
- 处理方式
- 操作：可查看日志详细信息及对日志中的误杀进行处理（误杀处理效果不理想可联系运维协助调整策略）

6.4 黑白名单管理



Waf 支持添加黑白名单，需选择对应域名以及黑白名单类型，内容进行添加

黑名单：配置了黑名单，所有访问来源全部屏蔽。

白名单：配置了白名单，所有访问来源全部放行。

IP 黑白名单：输入黑白名单的公网 IP 地址，如 10.10.10.10；

URL 黑白名单：输入黑白名单的 URL 地址，如 www.ctyun.cn；

Referer 黑白名单：指 HTTP 来源地址，比如如果点击一个网页的网址链接，那么浏览器会产生一

个送到目标的 Web 服务器的 HTTP 请求，该请求中则会包含一个 Referer 字段（网页的地址），

如网页 URL 为 http://www.ctyun.cn/product/cda，则输入 http://www.ctyun.cn/product/cda；

Useragent 黑白名单：Useragent 为用户代理，输入代理 Useragent 标识，如 IE9.0 的 Useragent

为:Mozilla/5.0(compatible;MSIE9.0;WindowsNT6.1;Trident/5.0;

黑白名单类型：包括 ip、referer、url、useragent 四种类型。

IP 黑白名单：输入黑白名单的公网 IP 地址，如 10.10.10.10；

URL 黑白名单：输入黑白名单的 URL 地址，如如访问 URL 为 https://www.ctyun.cn/console/index，

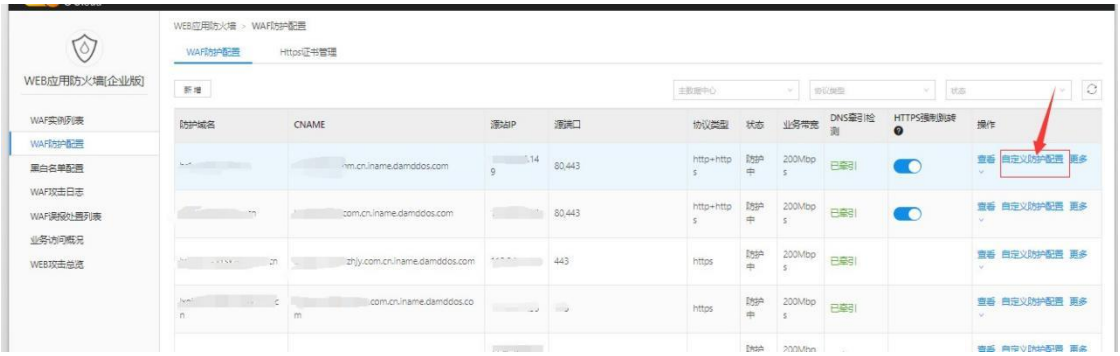
则填入/console/index，支持模糊匹配，如当输入/console/index 后，

https://www.ctyun.cn/console/index/##/也会匹规则；3 WAF 自服务控制台操作指南

Referer 黑白名单：指 HTTP 来源地址，比如如果点击一个网页的网址链接，那么浏览器会产生一

个送到目标的 Web 服务器的 HTTP 请求，该请求中则会包含一个 Referer 字段（网页的地址），如网页为 http://www.ctyun.cn/product/cda，则输入 http://www.ctyun.cn/product/cda； Useragent 黑白名单：Useragent 为用户代理，输入代理 Useragent 标识，如 IE9.0 的 Useragent 为:Mozilla/5.0(compatible;MSIE9.0;WindowsNT6.1;Trident/5.0;

6.5 自定义防护策略

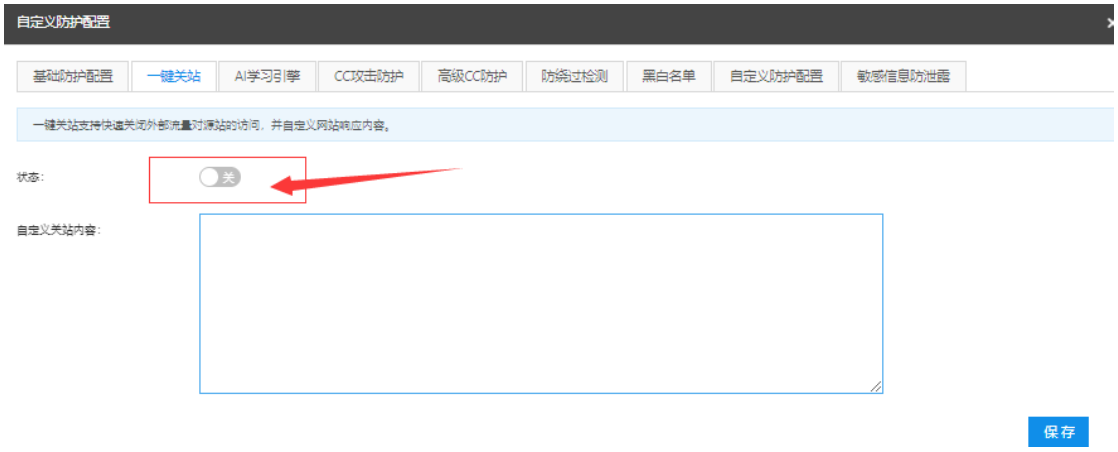


1.基础防护配置

通过此界面可以将waf 当前防护模式进行调整，可以由阻断模式调整到观察模式可

通过设置当前网站的应用系统与编程语言等业务信息，制定更加符合业务场景的 Web 入侵防护规则集。

2..一键关站

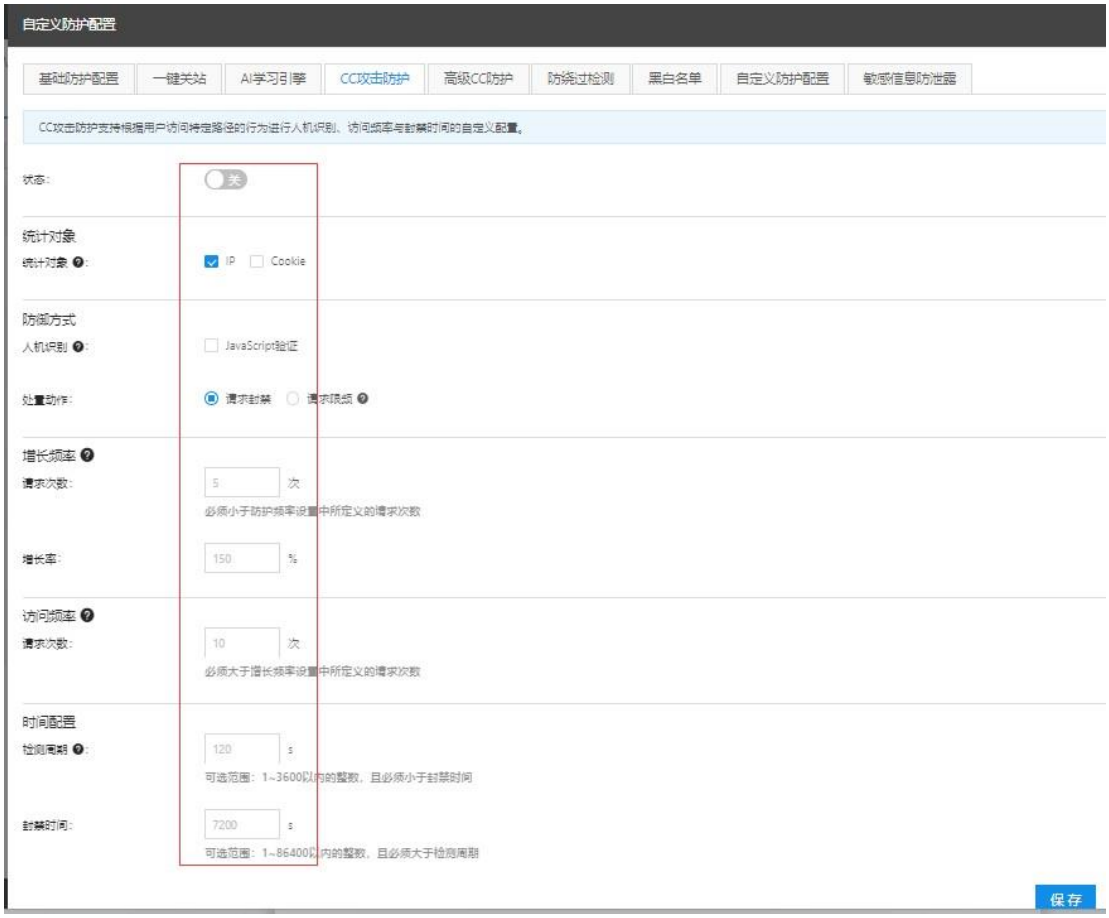


一键关站支持快速关闭外部流量对源站的访问，并自定义网站响应内容。

AI 智能学习模式

AI 学习引擎通过自动学习网站的流量特征与访问模式，同时对业务数据进行分类训练，提高对已知与未知Web 安全威胁的防护效果。

cc 防护策略



CC 攻击防护支持根据用户访问特定路径的行为进行人机识别、访问频率与封禁时间的自定义配置。

高级 cc 策略

高级CC 防护支持对特定的 URL 设置访问保护，有效缓解针对性的 CC 攻击

防绕过检测

防绕过检测支持配置各类绕过WAF 防护技术的检测，包含了不同应用系统下攻击者绕过 WAF 检测的规避技术类型

黑白名单配置

此模块可针对单个域名进行黑白名单添加操作

8. 可针对 url 进行自定义防护过配置过滤指定敏感信息

9.敏感信息防泄漏

敏感信息防泄露支持自定义过滤网页响应内容中的敏感信息，如身份证号、手机号、银行卡号等，进行加密显示。

7. 常见名词说明

7.1 域名解析

域名解析（Domain Name Resolution）指互联网上服务器相互间通过 IP 地址来建立通信，但是为了方便记忆，采用域名代替 IP 地址标识站点地址，让人们通过注册的域名可以方便地访问到业务的一种服务。域名解析就是域名到 IP 地址的转换过程。常用域名解析类型：

- A 记录：用来指定域名的 IPv4 地址。
- AAAA 记录：用来指定域名的 IPv6 地址。
- CNAM 记录：将域名指向另一个域名，再由另一个域名来提供 IP 地址，

最常用 CNAME 的场景包括使用 CDN、云 WAF、企业邮箱与高防 DDOS 等。

- MX 记录：用于电子邮件系统发邮件时根据收信人的地址后缀来定位邮

件服务器。

- TXT 记录：用于对域名进行标识和说明，进行 SPF 反垃圾邮件。

7.2 应用

Web 应用（Web Application）指通过浏览器即可访问的应用程序。

7.3 源站

源站（Source Application Server）指实际业务所处的站点，通常也代指源站公网 IP 及后端到达真实应用服务器间的整个网络拓扑环境。

7.4 回源 IP

回源 IP（Return Source IP Address）指开启云 WAF 防护后，云 WAF 用来与源站服务器建立网络连接的公网 IP 地址。

7.5 CC 攻击

CC 攻击（Challenge Collapsar Attack）指攻击者借助自动化工具脚本模拟多个用户持续向网站发送大量合法请求，造成服务器资源耗尽直至业务不可用。

7.6 SSL 证书

SSL 证书（Secure Sockets Layer）及其继任者 TLS（Transport Layer Security）是网络通信的一种安全协议，具有服务器身份验证和数据传输加密功能，为互联网间的数据传输提供安全性与完整性保障。SSL 证书遵循 SSL 协议，可安装在服务器上，实现数据传输加密。

7.7 访问控制

访问控制（Access Control）指防火墙或云服务器安全组上的一种有状态的包过滤设置，可以根据设定的条件对业务服务器接口上的数据包进行过滤，用于设置单台或多台服务器的网络访问控制，对服务器的出入向流量进行安全过滤。

8. 常见问题

8.1 计费类

8.1.1 一个域名包支持多少个二级域名？

一个域名包支持包含一个一级域名（www.baidu.com）以及这个一级域名下二级域名(如 abc.baidu.com)总计十个域名的防护。如果超过 10 个，需要购买实例增加域名包数量以支持域名防护。

8.1.2 选择带宽是否需要和网站业务带宽匹配？

是的，waf 额定最低标准带宽为 200mbps，真实业务带不能高于这个标准，如高于标准 200mbps，则需要拓展带宽包。

8.1.3 线上是否支持试用订购？

不支持。

试用暂时只支持线下渠道，需联系客户经理进行试用订。 ‘

8.1.4 WEB 应用防火墙是付费产品吗？

天翼云 Web 应用防火墙作为天翼云安全业务的一个重要产品，作为付费的增值业务服务产品提供给天翼云客户，需要用户购买。 收费的标准详见天翼云 web 应用防火墙实例购买页面。

8.1.5 产品是否可以试用，使用周期为多长时间？

答：支持试用，周期为三个月。

8.2 操作类

8.2.1 如何接入 web 应用防火墙防护

答：只需要通过修改网站 CNAME 记录即可。如果域名的 DNS 解析服务在自建的服务器，登陆控制台直接修改即可； 如果域名的 DNS 解析服务由第三方提供（如万网、新网等），登陆域名提供 DNS 解析的服务商网站进行修改。

8.2.2 WEB 应用防火墙支持 HTTPS 协议吗？

支持。

天翼云 web 应用防火墙既支持 http，又支持 https，同时支持单个域名既有 https 又有 http。

8.2.3 Web 应用防火墙支持 IP 负载均衡吗？

不支持，天翼云 Web 应用防火墙只支持单个 IP 的访问，不支持 IP 负载均衡。

8.2.4 WEB 应用防火墙流量牵引方式及步骤？

天翼云 Web 应用防火墙采用 DNS 牵引的方式，属于常引流。

在 web 应用防火墙自服务页面中防护配置生效后，需要客户联系 DNS 服务器商将网站域名解析指向

CNAME 地址，CNAME 规则为：防护域名+.iname.damddos.com，例如原域名 www.ctyun.cn，CNAME 为 www.

ctyun.cn.iname.damddos.com）。

如果用户需要关闭实例、关闭防护，首选需要确保已经联系 DNS 服务商将域名指向切换至源地址，否

则将影响客户的正常访问。

服务到期需要尽快续费，或者需要确保配置失效时将 DNS 指回源站。

8.2.5 为什么要放行云 WAF 回源 IP 段？

答：网站成功接入云 WAF 防护后，所有业务请求将先流转到防护平台进行检测，经过滤后返回到源站服务器。由于源站服务器收到的所有请求都来自云 WAF 平台的 IP，源站服务器上的安全软件（如安全组、防火墙、安全狗、云锁）很可能认为云 WAF 回源 IP 在进行攻击而进行封禁，造成误封禁的云 WAF 回源 IP 的所有请求将无法得到源站的正常响应。因此，在网站接入云 WAF 后，需确保源站侧已将云 WAF 所有回源 IP 加入访问控制安全组与相关安全软件白名单进行放行，避免出现网站无法打开或响应缓慢等情况。

8.2.6 为什么要开通所有网站端口的 WAF 防护？

答：域名接入云 WAF 防护后，该域名所有公网业务请求都会通过 CNAME 解析牵引至云 WAF，未在云 WAF 侧开通防护配置的端口请求则无法被接收，并且丢弃。因此，需要提供完整的域名及域名所开放端口列表。如未将同一域名下所有端口业务接入云 WAF 进行 防护，将影响该域名下未接入防护的端口业务正常访问。

8.2.7 如何放行云 WAF 回源 IP 段？

答：打开源站服务器上的安全软件与访问控制安全组，根据防护开通的所属数据中心中心将云 WAF 平台回源 IP 地址段（内蒙数据中心：36.111.137.0/24 与 203.57.157.0/24，北京数据中心：203.34.106.0/24，上海数据中心：101.226.7.0/24，广州数据中心：203.32.204.0/24）添加到白名单。

8.2.8 云 WAF 是否支持会话保持？

答：支持会话保持，但是默认不开启。如果需要启用会话保持，请联系安全防护工程师根据实际业务需求进行会话保持策略配置的调整。

8.2.9 云 WAF 是否支持源站健康检查？

2. 答：支持对源站 IP 的健康检查，但是默认不开启。如果需要启用源站健康检查，请联系安全防护工程师根据实际业务需求进行健康检查配置的调整。

8.2.10 为什么第三方漏洞扫描工具会检测到域名其他未开放的端口？

答：云WAF 默认开放部分端口用于网站接入和防护服务，对于已接入云 WAF 防护的网站，云WAF 不会转发任何未开通防护的端口业务请求回到源站。因此，不会对源站服务带来任何安全风险和威胁。关于第三方扫描工具对于网站的端口检测，需以源站公网 IP 开放的端口为准。

8.3 管理类

8.3.1 什么情况下产品会误拦截

答： 1）网站代码不规范导致拦截当网站代码不规范时，可能会因为触发防护策略而产生被拦截情况，云 WAF 启用了实时更新的恶意威胁规则集，针对 Webshell 上传、SQL 注入、XSS 等常见的 Web 攻击行为特征（如 ini_set(、=javascript:）进行检测。同时会将请求中部分直接传递的原始 SQL 语句、JAVASCRIPT 代码判定为潜在的安全风险，进行封禁。此外，URL 中含有敏感路径（如 /root、/temp、/admin），以及可能导致路径遍历的特殊字符（如../、.%5c../）也会被判定为高危访问进行封禁，因此，规范的网站代码编写会大幅减少被拦截的概率。

2）网站接口数据传输规则导致拦截 网站存在接口的情况下，当产生调用时，因该行为非人工访问行为，可能会被云 WAF 判定为非浏览器或程序化访问，从而产生拦截，此情况下需要将发起接口调用的源地址加白名单解决。

3）用户端行为疑似人工 DDoS 攻击导致拦截 用户频繁点击某一个 URL，或者频繁下载同一个文件等行为，均可能会被判定为 DDoS 攻击，进而会产生拦截。此种情况下，须由用户确认是否正常操作后，加入 CC 防护白名单。

4）国际流量整体拦截 云 WAF 支持针对 IP 地址的国家地理位置限制，当开启该限制后，国际流量将被阻断，只有国内流量才能通过。该策略主要用户客户的网站使用对象全部为国内的情况下，可以避免来自国际的各类攻击、渗透行为。

8.3.2 如何放行云 WAF 回源 IP 段？

答：打开源站服务器上的安全软件与访问控制安全组，根据防护开通的所属数据中心中心将云 WAF 平台回源 IP 地址段（内蒙数据中心：36.111.137.0/24 与 203.57.157.0/24，北京数据中心：203.34.106.0/24，上海数据中心：101.226.7.0/24，广州数据中心：203.32.204.0/24）添加到白名单。

8.3.3 CNAME 记录，多长时间可以生效？

答：这取决于您在当前的域名服务提供商设置的域名记录超时时间，以及当前域名服务提供商 NS 记录刷新的时间。一般情况，NS 记录的刷新一般不会超过 48 小时。

8.3.4 CNAME 解析变更提示冲突怎么办？

答：对于同一个主机记录，CNAME 解析记录值只能填写一个。不同 DNS 解析记录类型间存在冲突。例如，对于同一个主机记录，CNAME 记录与 A 记录、MX 记录、TXT 记录等其他记录互相冲突。在无法直接修改记录类型的情况下，您可以先删除存在冲突的其他记录，再添加一条新的 CNAME 记录。

8.3.5 修改 CNAME 后发现界面有拦截信息

答：根据拦截页面的联系方式联系电信 7*24 小时值班人员处理或者微信沟通群（提供拦截截图及相关 ID 信息）。

8.3.6 修改 CNAME 后发现访问变慢

答：需工程师抓包查看从发送请求到接收响应时间差；客户侧同时抓包查看接收请求到发送响应时间差，对比分析排查访问延迟出现的问题原因。

8.3.7 修改 CNAME 后发现网站无法访问

答：1）域名解析有问题，访客清除 DNS 缓存或者修改 DNS 解决；

2）SYN 重传或 request 重传，需确认 web 应用防火墙发送的 SYN 客户侧是否有接收到。客户侧协助抓 包定位是否接收到 SYN 并且响应 SYN ACK。

8.3.8 源站服务器侧响应异常怎么办？

答：若是源站服务器侧直接响应回复的异常信息，云 WAF 拦截导致的访问异常是不会有服务器侧的响应的，类似“请勿重复提交” “上传失败”这样的弹窗应属于服务器响应，不是云 WAF 拦截导致的，如这样大规模的访问异常需要排查一下应用服务器的工作状态（例如进程、CPU、内存、Web 日志等）是否存在异常并修复异常。

8.3.9 验证WAF 是否可以防御自动化工具发起的攻击？

答：满足，但是需要厂家配合测试。

8.4 知识类

8.4.1 什么是 WEB 应用防火墙？

Web 应用防火墙：Web Application Firewall，简称:WAF。 Web 应用防火墙是通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 Web 应用提供保护的一款产品，承担了抵御常见的 SQL 注入、XSS、 远程命令执行、目录遍历等攻击的作用。

8.4.2 什么是 CC 攻击？

答：CC 是一个应用层的 DDoS， 是发生在 TCP3 次握手已经完成之后，所以发送的 IP 都是真实的。CC 攻击的原理很简单，就是对一些消耗资源较大的应用页面不断地发起正常的请求，以达到消耗服务端资源的目的，在 web 应用中，查询数据库、读写硬盘文件的操作，相对都会消耗比较多的资源。一个简单的例子，一个小的网站，可能被搜索引擎、信息收集等系统的爬虫爬死，或者是扫描器扫死，这与应用层的 DDoS 攻击的结果很像。

8.4.3 使用 web 应用防火墙会影响我们的网页备案吗？

答：不会，web 应用防火墙的本质是一种网站在线加速和防护服务，没有影响用户网站所在的机房。和传统 CDN 类似，使用 CDN 会改变网站的解析 IP，但是并不会影响网站的备案。

8.4.4 天翼 WEB 应用防火墙需要关注的问题？

天翼云 web 应用防火墙防护需要注意确保 DNS 牵引的正确性。

天翼云 web 应用防火墙面向的客户为采用天翼云主机作为网站服务的客户，客户购买服务前提必须提供正确的网站域名。

8.4.5 Web 应用防火墙可以和 CDN 同时使用吗？

答：只要您当前的 CDN 服务商支持通过 CNAME 的方式指定回源服务器，就可以同时使用。 存在的潜在问题： 对客户端访问流量拦截，web 应用防火墙会返回一个拦截页面。而 cdn 缓存拦截页面后，会导致 正常用户访问该资源时无论是否违规，得到的都是之前的拦截页面，从而影响正常访问。 经过 cdn 后，客户端的真实 IP 会被 cdn 替换掉，因此在业务出现问题时，排障会比较困难，定位问题点需时较长。经过 cdn 后，真实的客户端会被 cdn 隐藏，web 应用防火墙的部分功能将会失效，如基于源 IP 频率的检测、基于地理位置、IP 情报库等功能无法使用。

8.5 服务类

8.5.1 售后联系方式

Web 应用防火墙服务开通及使用过程涉及本手册中的步骤，需严格根据手册指导进行操作，若因操作不当或策略过于严格，从而影响防护开通及使用，请及时联系安全防护工程师，安全防护工程师

24 小时在线配合，联系方式如下：

24 小时值班热线 400-810-9889

或联系本地电信客户经理，或在 web 应用防火墙微信群中反馈。

8.5.2 关于特殊需求

如有针对带宽，域名等条件有特殊需求请联系客户经理或运维人员沟通。

9. 相关协议

9.1 服务条款

帮助中心-法律声明获取地址：https://www.ctyun.cn/portal/protocol/10009256