



天翼云 Web 应用防火墙（企业版）

用户使用指南

中国电信股份有限公司云计算分公司

目 录

1 产品概述	5
1.1 产品定义	5
1.2 WEB 应用防火墙产品功能	5
1、网络层防护	5
2、应用层防护和功能	5
1.3 常见名词说明	7
1.3.1 域名解析	7
1.3.2 WEB 应用	7
1.3.3 源站	7
1.3.4 回源 IP	7
1.3.5 CC 攻击	8
1.3.6 SSL 证书	8
1.3.7 访问控制	8
2 购买指南	8
2.1 价格	8
2.2 订购	9
2.3 续订	10
2.4 升级	11
2.5 退订	12

3 WAF 自服务控制台操作指南	12
3.1 WEB 应用防火墙防护接入.....	12
3.1.1 防护开通.....	12
3.1.2 本地验证测试.....	17
3.1.3 防护回源 IP 放行.....	21
3.1.4 域名解析.....	21
3.1.5 设置源站保护.....	22
3.1.6 获取客户端真实 IP.....	22
3.2 与 CDN 结合使用.....	22
3.3 防护策略说明.....	22
3.3.1 防护攻击类型示例.....	22
3.3.2 防护策略说明.....	26
3.3.3 调整防护策略.....	27
3.4 WEB 应用防火墙自服务平台使用说明.....	27
3.4.1 访问趋势总览.....	27
3.4.2 攻击概况总览.....	31
3.4.3 攻击日志查询.....	33
3.4.4 域名证书管理.....	35
3.4.5 黑白名单管理.....	37
3.4.6 全局黑白名单管理.....	38
3.5 WEB 应用防火墙防护配置管理.....	41

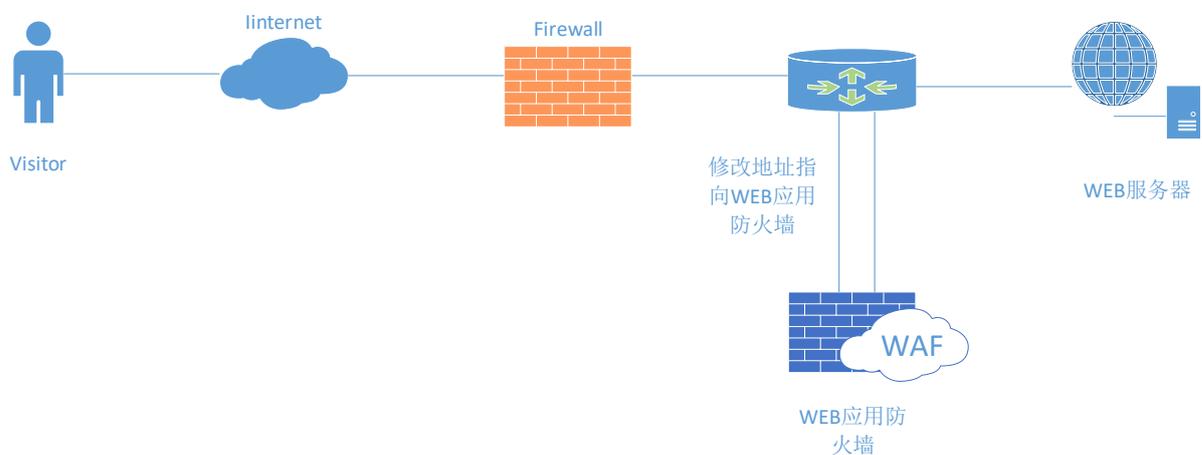
3.5.1 防护状态调整	41
3.5.2 https 强制跳转	41
3.5.3 自定义防护策略	42
4 售前常见问题	45
4.1 什么是 WEB 应用防火墙?	45
4.2 天翼云 WEB 应用防火墙是付费产品吗?	45
4.3 天翼云 WEB 应用防火墙流量牵引方式及步骤?	46
4.4 天翼云 WEB 应用防火墙支持 HTTPS 协议吗?	46
4.5 一个域名包支持多少个二级域名?	46
4.6 WEB 应用防火墙支持 IP 负载均衡吗?	46
4.7 天翼 WEB 应用防火墙需要关注的问题?	46
4.8 WEB 应用防火墙可以和 CDN 同时使用吗?	47
4.9 修改 CNAME 记录, 多长时间可以生效?	47
4.10 使用 WEB 应用防火墙会影响我们的网页备案吗?	47
4.11 什么是 CC 攻击?	47
5 售中常见问题	48
5.1 为什么要放行云 WAF 回源 IP 段?	48
5.2 如何放行云 WAF 回源 IP 段?	48
5.3 为什么要开通所有网站端口的 WAF 防护?	48
5.4 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?	48
5.5 如何放行云 WAF 回源 IP 段?	49

5.6	云 WAF 是否支持会话保持?	49
5.7	云 WAF 是否支持源站健康检查?	49
5.8	如何接入 WEB 应用防火墙防护	49
5.9	CNAME 解析变更提示冲突怎么办?	49
5.10	如何在万网中修改 DNS 解析	50
6	售后常见问题	52
6.1	售后联系方式	52
6.2	什么情况下产品会误拦截	53
3.3.1	什么情况会产品误拦截	53
6.3	修改 CNAME 后发现界面有拦截信息	54
6.4	修改 CNAME 后发现访问变慢	54
6.5	修改 CNAME 后发现网站无法访问	54
6.6	源站服务器侧响应异常怎么办?	54
6.7	关于特殊需求	54

1 产品概述

1.1 产品定义

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。



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。

1.2 Web 应用防火墙产品功能

1、网络层防护

1) Http/Https Flood (CC 攻击) 防护

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, webservell 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 常见名词说明

1.3.1 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。

1.3.2 WEB 应用

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

1.3.3 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。

1.3.4 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。

1.3.5 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。

1.3.6 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。

1.3.7 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。

2 购买指南

2.1 价格

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

备注：

- 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服务：

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%

2.2 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，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，此为套餐包的量，用户可根据自己需要，增加防护带宽和域名包数量。并选择定能够时长。

* 防护规格：企业版

* 防护说明：
 防护能力：
 1.防SQL注入、防XSS攻击、防Webshell上传、防目录遍历等
 2.防敏感隐私数据泄露、包括手机号、身份证、银行卡等重要隐私数据；
 3.云端自动最新Web 0day漏洞的防护规则；
 4.支持人机识别的数据风控防护、防黄牛、防恶意注册；
 5.基础的默认CC防护策略，缓解HTTP(s)Flood攻击；
 6.支持网页防篡改、盗链防护、管理后台的防暴力破解；
 7.支持常见HTTP头部字段的访问控制及复杂的多条件组合、过滤恶意特征请求；
 支持业务：
 支持HTTP、HTTPS(支持10个端口转发、不限于80、8080、443、8443端口
 业务请求：
 3000 (QPS)

* 防护带宽：

* 域名包： 可以防护一个一级域名下的10个域名。

◎ 购买量

* 购买时长：


 1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年

配置费用：
¥ 1744.00元

立即购买 我已阅读，理解并接受 [《天翼云Web应用防火墙服务协议》](#)

2.3 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】。

续订WAF防护 不清楚WAF防护的功能和作用，请单击[这里](#)。

资源信息

* 资源ID：

* 防护带宽：

* 域名包：

续费信息

* 续费时长：

1个月 2个月 3个月 4个月 5个月 6个月 7个月 8个月 9个月 10个月 11个月 1年 2年 3年

配置费用：

¥ 1744.00元

我已阅读，理解并接受 [《天翼云Web应用防火墙服务协议》](#)

2.4 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】。

○ 当前资源信息

- * 资源ID： a6f8b7ca86d64bbfbe2a60d5f5b8b035
- * 防护带宽： 200Mb
- * 域名包： 1个

○ 升级后防护带宽信息

- * 防护带宽： 400Mb 600Mb 800Mb 1000Mb
- * 域名包： 1 个 最多可以订购10个域名包，每个域名可以防护一个一级域名下的10个域名。

配置费用：

¥ 0.00元

立即购买

我已阅读，理解并接受 [《天翼云Web应用防火墙服务协议》](#)

2.5 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。

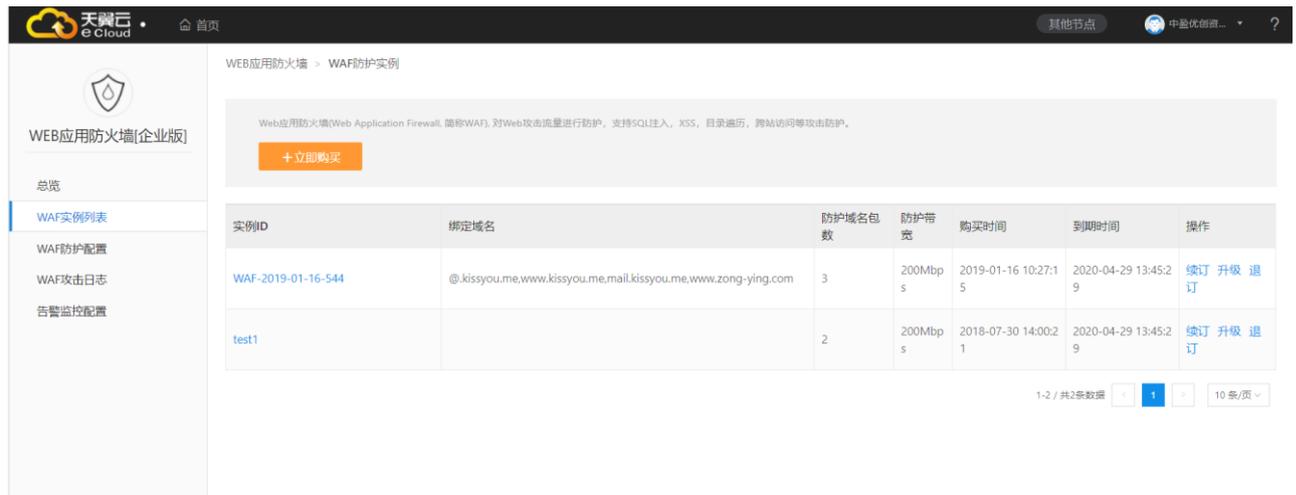
3 WAF 自服务控制台操作指南

3.1 Web 应用防火墙防护接入

3.1.1 防护开通

3.1.1.1 查看当前资源信息

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



WEB应用防火墙 > WAF防护实例

Web应用防火墙(Web Application Firewall, 简称WAF), 对Web攻击流量进行防护, 支持SQL注入, XSS, 目录遍历, 跨站访问等攻击防护。

[+立即购买](#)

实例ID	绑定域名	防护域名包数量	防护带宽	购买时间	到期时间	操作
WAF-2019-01-16-544	@.kissyou.me,www.kissyou.me,mail.kissyou.me,www.zong-ying.com	3	200Mbps	2019-01-16 10:27:15	2020-04-29 13:45:29	续订 升级 退订
test1		2	200Mbps	2018-07-30 14:00:21	2020-04-29 13:45:29	续订 升级 退订

1-2 / 共2条数据 1 10条/页

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，点击续订跳转至续订页面，选择续订时间，生成订单续订成功后，到期时间延长。

退订，点击退订跳转至退订页面，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

3.1.1.2 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](#)）

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；

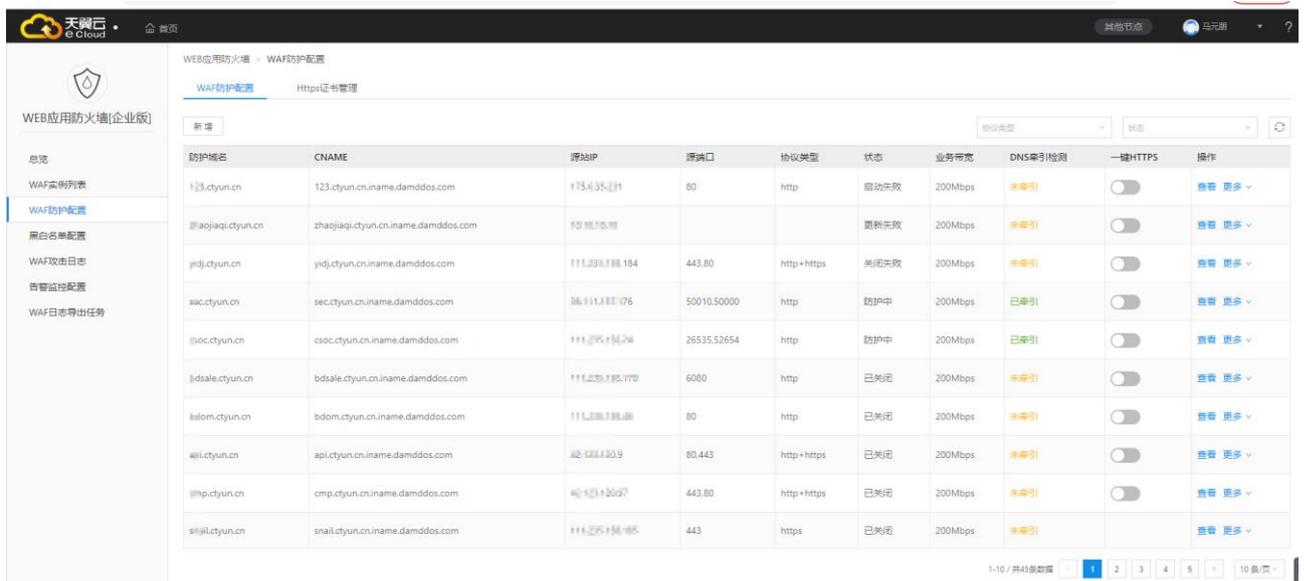
删除，点击删除，将当前的防护配置清除，需要确保防护域名指回源站；

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WAF防护配置
✕

* 实例ID:

* 业务带宽: Mbps

* 主数据中心:

备数据中心:

* 防护域名: .
输入主机域名: 如www.ctyun.cn; 如果为二级域名: 如abc.ctyun.cn; 如果为三级域名, 如ab.abc.ctyun.cn

* IP代理:

* 源站IP:
请输入单IP

* 协议类型:

* 源端口:
输入多组端口数据以英文逗号作为分隔

* 开启防护: 关闭
状态为关闭时, 防护配置只保存但不生效

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

* 防护域名: .
输入主机域名: 如www.ctyun.cn; 如果为二级域名: 如

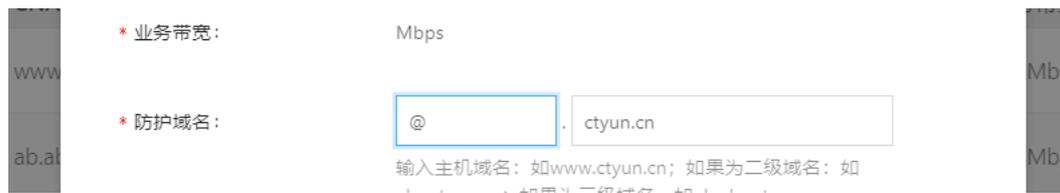
如为域名: 如 abc.ctyun.cn.com ,

* 防护域名: .

如为域名：如 M.abc.ctyun.cn



如为域名：ctyun.cn

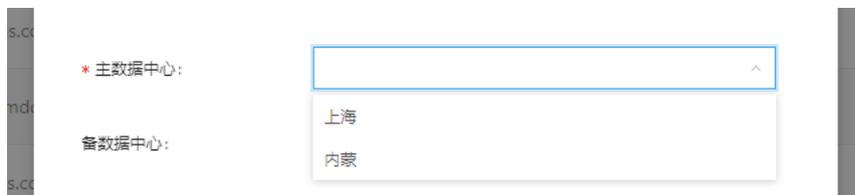


选择解析方式：

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、可根据需求选择上海或内蒙节点。



4、填入源站 IP；

5、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；

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）

如果为初次填入 https 证书，可以点击“新增证书”



新增证书

* 证书名称:

* 证书公钥:

* 证书私钥:

进入： 页面创建证书，证书创建成功后选择刚刚创建的证书。

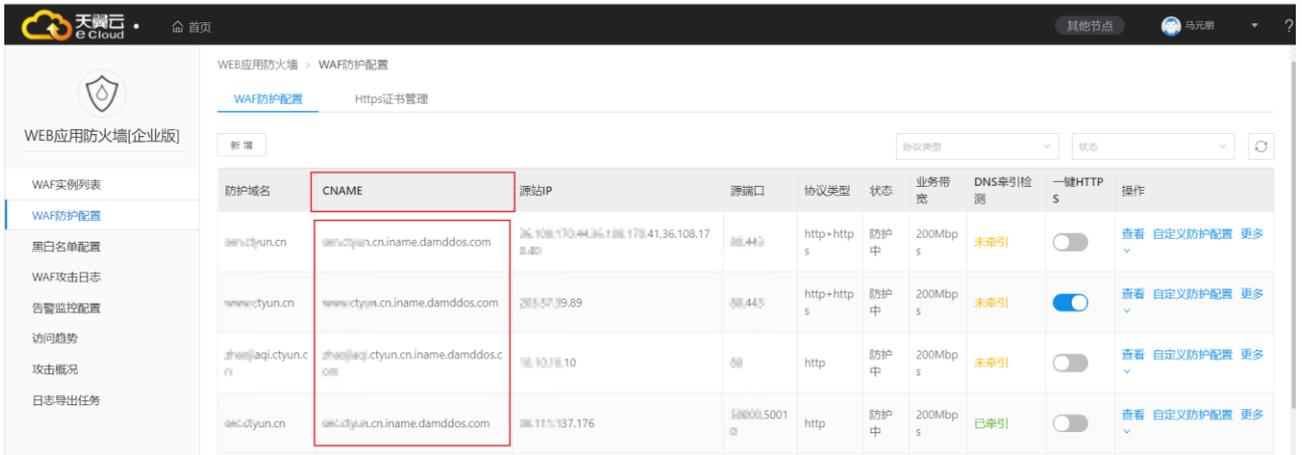
- 7、开启防护（默认勾选），如果未选中开启防护按钮，该配置不会生效，业务不会下发至 web 应用防火墙设备进行防护。
- 8、点击保存，确认后，正式下发防护配置。

3.1.2 本地验证测试

为了确保 WAF 转发正常，在修改 DNS 解析配置前，建议您先通过本地验证确保一切配置正常。进行此操作前，确保添加的防护域名（例如 portal.damddos.com）的源站服务器协议、地址、端口配置正确，如果“对外协议”类型存在“HTTPS”，也必须确保上传的证书和私钥正确。

3.1.2.1 本地接入云 WAF 测试

1) 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



防护域名	CNAME	源站IP	源端口	协议类型	状态	业务带宽	DNS牵引检测	一键HTTPS	操作
portal.ctyun.cn	portal.ctyun.cn.iname.damddos.com	36.111.137.176	80	http+https	防护中	200Mbps	未牵引	<input type="checkbox"/>	查看 自定义防护配置 更多
www.ctyun.cn	www.ctyun.cn.iname.damddos.com	36.111.137.176	80	http+https	防护中	200Mbps	未牵引	<input checked="" type="checkbox"/>	查看 自定义防护配置 更多
aqi.ctyun.cn	aqi.ctyun.cn.iname.damddos.com	36.111.137.176	80	http	防护中	200Mbps	未牵引	<input type="checkbox"/>	查看 自定义防护配置 更多
portal.ctyun.cn	portal.ctyun.cn.iname.damddos.com	36.111.137.176	80	http	防护中	200Mbps	已牵引	<input type="checkbox"/>	查看 自定义防护配置 更多

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。

```
C:\Users\>ping portal.damddos.com.iname.damddos.com
正在 Ping portal.damddos.com.iname.damddos.com [36.111.137.188] 具有 32 字节的数据:
请求超时。
请求超时。
```

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。

```

#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 192.168.1.1 rhino.acme.com          # source server
# 192.168.1.2 x.acme.com            # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
36.111.137.188 portal.damddos.com
    
```

3. 修改 hosts 文件后保存，然后本地 ping 一下被防护的域名。

```

C:\Users\>ping portal.damddos.com

正在 Ping portal.damddos.com [36.111.137.188] 具有 32 字节的数据:
来自 36.111.137.188 的回复: 字节=32 时间=25ms TTL=240
来自 36.111.137.188 的回复: 字节=32 时间=24ms TTL=240
来自 36.111.137.188 的回复: 字节=32 时间=24ms TTL=240
来自 36.111.137.188 的回复: 字节=32 时间=20ms TTL=240
    
```

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）。

```

C:\Users'>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
    
```

3.1.2.2 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，如图所示。

防护域名: 告警级别: 告警类型: 处理方式: 请求时间: 2021-03-15 00:00 - 2021-03-15 20:56

序号	ID	域名	请求方法	访问URL	告警级别	告警类型	客户端IP	地区	请求时间	处理方式	操作列
1	9996188168416918029	portal.damddos.com	GET	/url/ishi.asp=javascriptalert(/xss/)	高	跨站脚本攻击			2021-03-15 ...	阻断	详情 误拦截处理

3.1.3 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。

3.1.4 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

3.1.5 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。

3.1.6 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云堤安全防护工程师提供技术支持。

3.2 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。最佳部署架构：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，并告知云堤安全防护工程师进行提取配置，保证云 WAF 正常防护。

3.3 防护策略说明

3.3.1 防护攻击类型示例

云 WAF 支持防护的攻击示例如下：

攻击	攻击类型说明
----	--------

类型	
权限 滥用 攻击	攻击者利用服务端功能开放过多或权限限制不严格的漏洞，从而达到欺骗或绕过应用程序访问控制机制的攻击方式。
SQL 注入	攻击者通过把 SQL 命令插入到 Web 表单提交、输入 URI 或页面请求的查询字符串等手段，利用应用程序的数据库层上的安全漏洞，从而使数据库受到攻击，造成敏感数据窃取或删改，甚至进一步导致网站被嵌入恶意代码、植入后门等危害
身份 验证/ 授权 攻击	身份验证攻击对网站验证用户、服务或应用程序合法身份的方法进行攻击。授权攻击对网站确认用户、服务或应用程序执行请求操作权限的方法进行攻击。
暴力 破解	暴力破解是黑客通过猜测用户名和密码来访问网站登录页面的外部尝试；恶意用户多次尝试登录 URL，执行暴力攻击，运行许多用户名和密码组合，直到用户成功登录。
缓冲 区溢 出	缓冲区溢出攻击是针对程序设计缺陷，向程序输入缓冲区写入使之溢出的内容（通常是超过缓冲区能保存的最大数据量的数据），从而破坏程序运行、趁著中断之际并获取程序乃至系统的控制权。
命令 执行 攻击	命令执行攻击是指攻击者通过提交更改网页内容或 Web 应用程序的命令来操纵用户输入字段数据的攻击，目的是在远程服务器上执行 shell 命令以显示敏感数据，例如，服务器上的用户列表。
跨站 脚本 攻击	跨站脚本（XSS）是一种攻击技术，它强制网站回应攻击者提供的可执行代码，这些代码加载到用户的浏览器中，借助插入至网站的恶意代码进行传播，对网站用户进行攻击，达到盗取用户账号信息、钓鱼欺诈、身份盗用等目的。
跨站 请求 伪造	跨站请求伪造攻击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操作的攻击方法。CSRF 攻击可以包括汇款，股票交易，特权升级，应用程序修改或其他未经授权的访问。

攻击	
拒绝服务攻击	拒绝服务 (DoS) 通常由两种方式实现, 一是迫使服务器的缓冲区占满, 不接收新的请求; 二是使用 IP 欺骗, 迫使服务器把非法用户的连接复位, 同时影响合法用户的连接
逃避检测攻击	逃避检测攻击也叫攻击绕过技术, 攻击者试图伪装或隐藏攻击以避免被安全设备进行检测, 常见的逃避检测攻击有 HTTP 参数污染、00 截断、URL 编码绕过、Unicode 编码绕过、ASCII 码绕过、字符串拼接绕过、hex 编码绕过、大小写混杂字符绕过、多空格绕过、注释串绕过等。
目录遍历攻击	目录遍历攻击利用服务器相关 (存在安全漏洞的) 应用服务, 来恶意的获取服务器上本不可访问的文件访问权限。
强制浏览	强制浏览是一种针对受保护程度不佳的网站和 Web 应用程序的攻击技术, 它使攻击者能够访问他们不应该访问的资源。
HTTP 请求走私攻击	HTTP 请求走私常出现在当服务器接收 http 请求并将该请求转发给其他服务器时, 攻击尝试通过 Web 代理将一个请求封装在另一个请求中, 进行缓存度化或请求劫持等恶意行为
HTTP 响应拆分攻击	HTTP 响应拆分攻击也叫 CRLF 注入攻击, CR、LF 分别对应回车、换行符。攻击者通过插入 CRLF 字符后就可以实现在响应头部中插入任意数据, 控制响应的数据内容等目的, 以进行 XSS、会话固定漏洞攻击等恶意行为
信息泄露	信息泄露是指网站显示敏感数据, 例如开发人员的评论或错误消息, 有助于攻击者利用此类信息发现系统漏洞。
命令注入	注入攻击会利用各种其他应用程序中的弱点来注入或执行恶意代码。
JSON	攻击者试图传递解析器无法解析的 JSON 数据, 并且可能包含导致各种攻击的恶意代码, 例如拒绝服务或跨

解析 攻击	站点脚本
LDAP 注入 攻击	LDAP 注入是一种攻击技术，利用用户引入的参数生成 LDAP 查询，在有漏洞的环境中，这些参数没有得到合适的过滤，因而攻击者可以注入任意恶意代码。
恶意 文件 上传 攻击	恶意文件上传攻击尝试通过上传可能包含恶意代码的文件（如 webshell），企图控制服务器的攻击。。
非浏 览器 客户 端	非浏览器客户端攻击使用爬虫或其他自动化脚本工具来模拟人类活动，进行恶意机器人访问行为。
参数 篡改	参数篡改攻击尝试通过修改 HTTP 查询字符串中的参数来操纵和捕获数据。
路径 遍历	路径遍历攻击（也称为目录遍历）旨在访问存储在 Web 根文件夹之外的文件和目录。通过操纵带有“点-斜线 (...)”序列及其变化的文件或使用绝对文件路径来引用文件的变量，可以访问存储在文件系统上的任意文件和目录，包括应用程序源代码、配置和关键系统文件。
预测 资源 位置 攻击	预测资源位置攻击是一种用于发现隐藏的网站内容和功能的攻击技术。
HTTP 不合 规协	由 HTTP 协议参数，头部请求参数异常引发的拒绝服务或缓冲区溢出攻击等。

议	
其他	由于 Web 服务器本身安全和其他软件配置安全或漏洞引起的攻击。
漏洞	
攻击	

3.3.2 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和配置，观察模式调整步骤与云 WAF 日志查看可参考本文档 2.4 客户自服务平台使用说明。

3.3.3 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。

3.4 Web 应用防火墙自服务平台使用说明

3.4.1 访问趋势总览

1. 点击菜单【访问趋势】，进入页面；

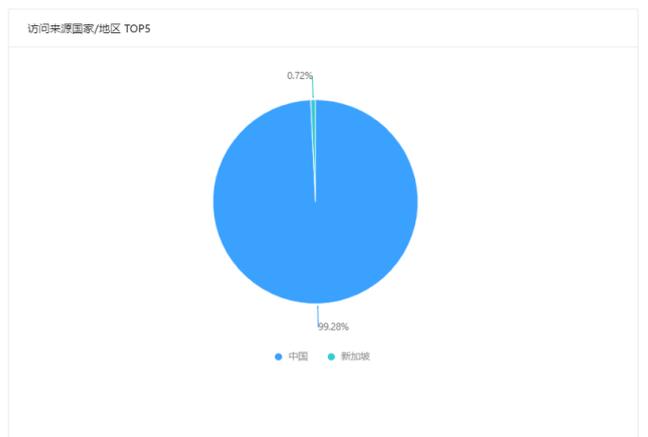
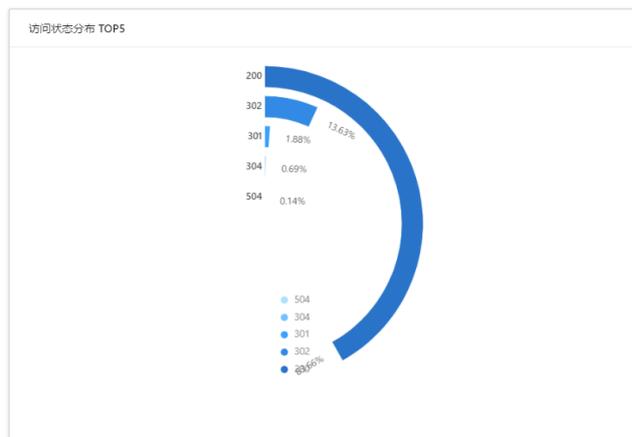
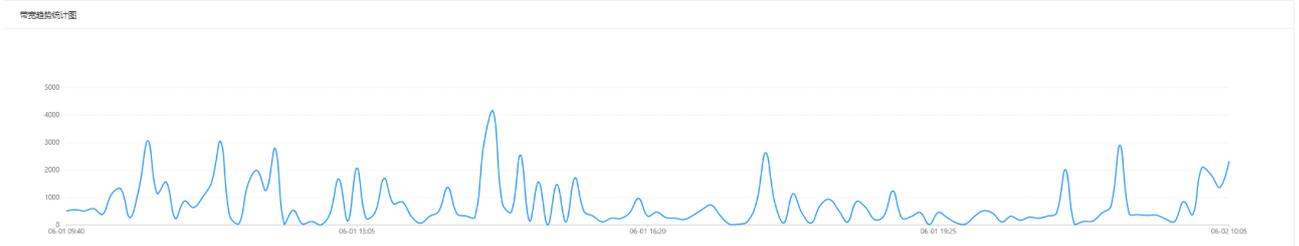
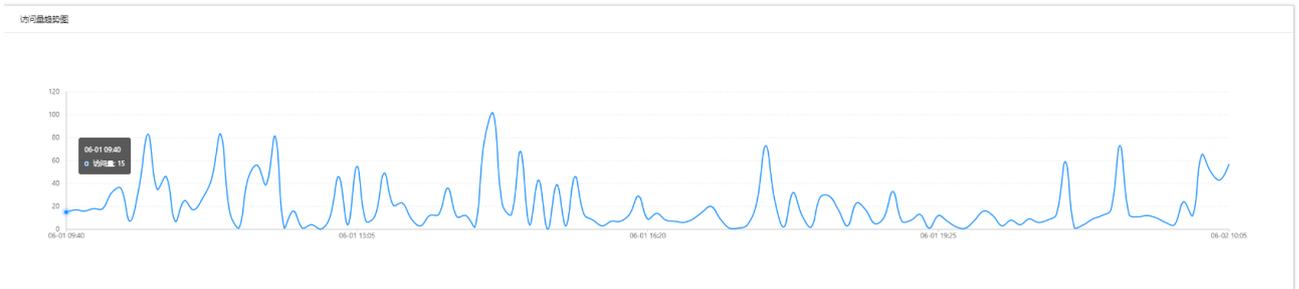
在“WAF 防护报表”页面，您可以查看昨天、今天、7 天、15 天、30 天及自定义时间所有防护网站的访问趋势。访问趋势包括访问总量与流量类型占比，响应码信息，带宽趋势统计以及访问来源国家/地区 TOP5、访问源 IP Top10、访问 URL Top10、访问来源区域 Top10 等防护数据。

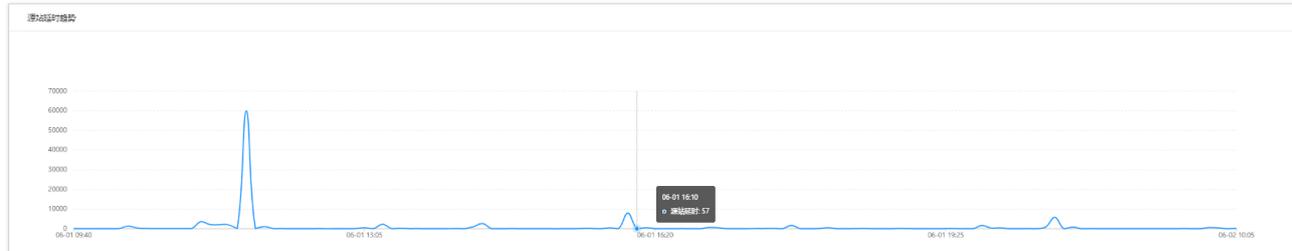
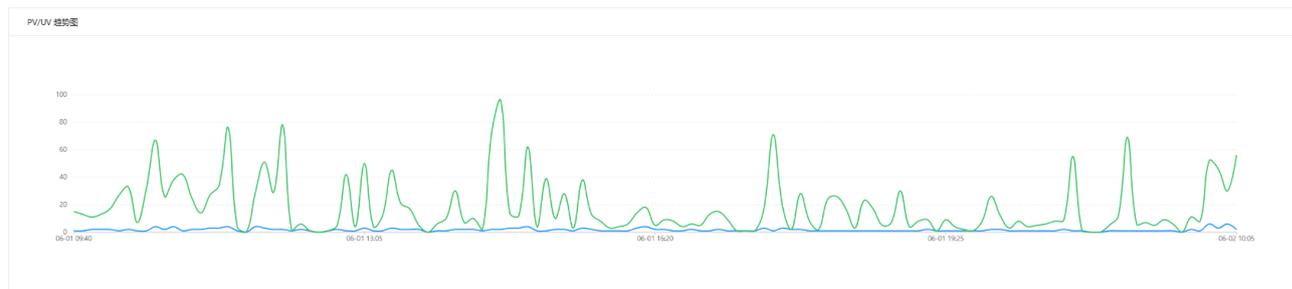
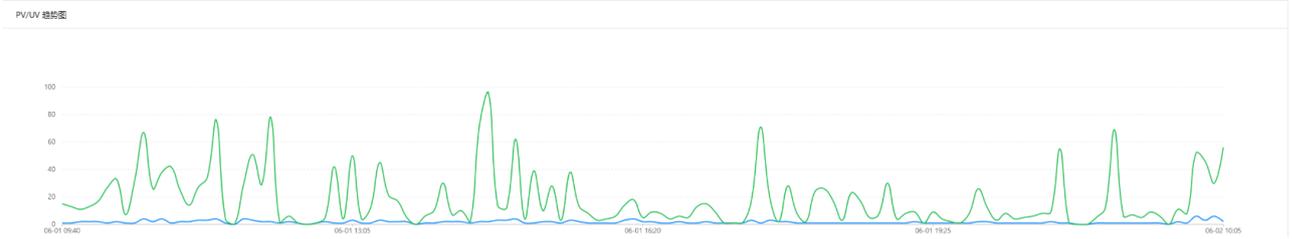
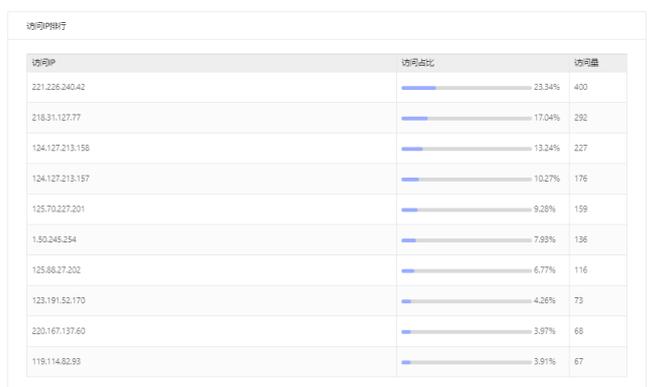
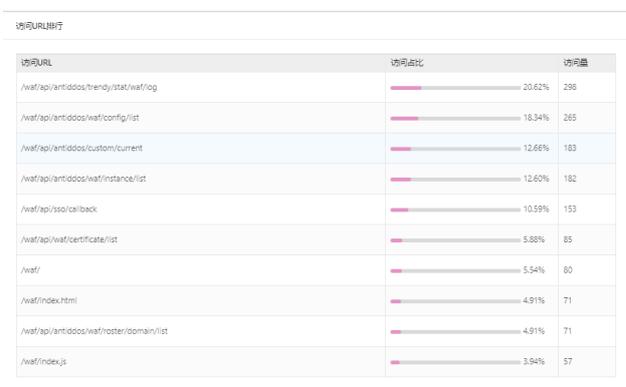
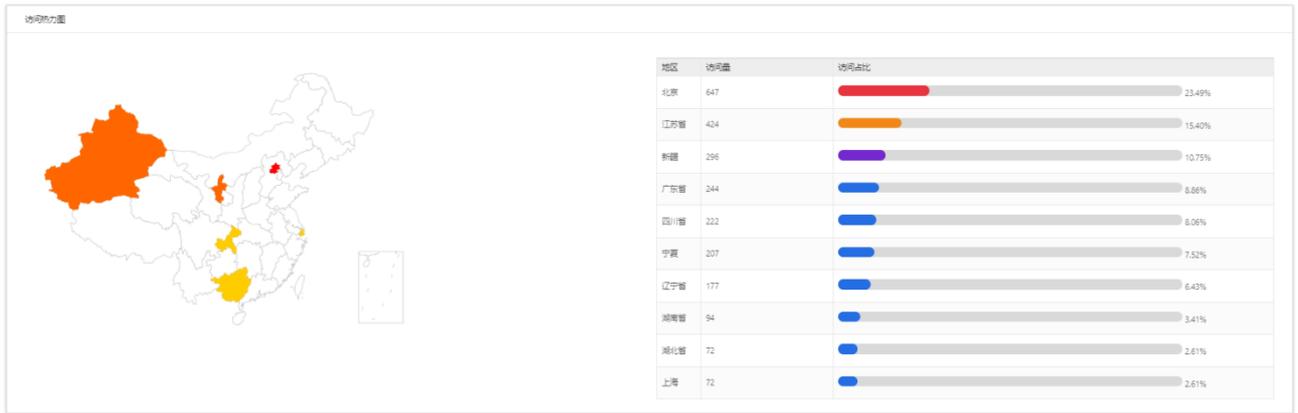
前提条件：

- 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





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

3.4.2 攻击概况总览

点击菜单【攻击概况】，进入页面；

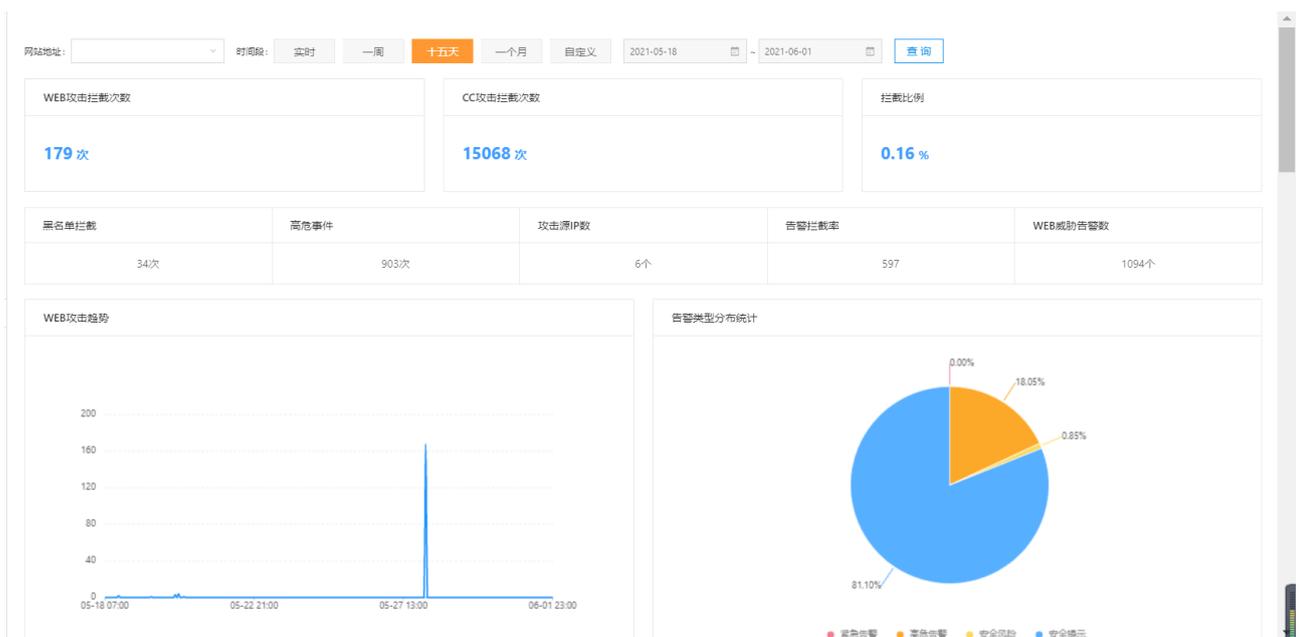
在“WAF 防护报表”页面，您可以查看实时、7 天、15 天、30 天及自定义时间所有防护网站的攻击趋势。访问趋势包括攻击拦截次数与拦截比例，告警类型分布统计以及攻击来源国家/地区 TOP5、攻击类型 TOP5、攻击 URL Top10、攻击 IP Top10 等防护数据。

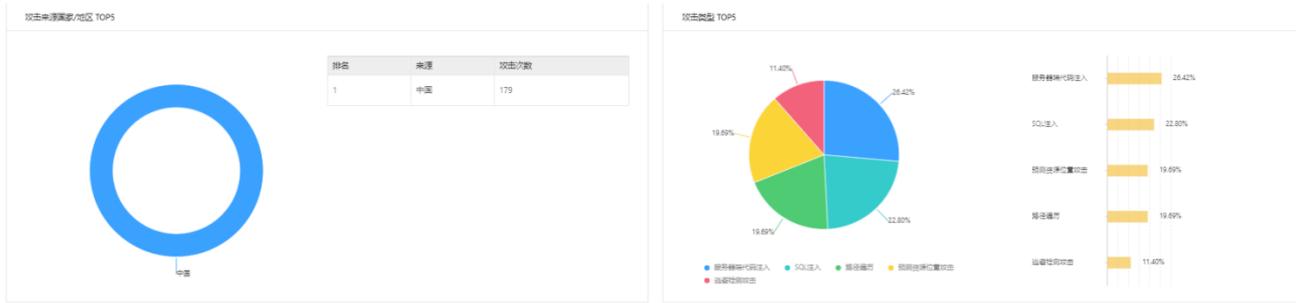
前提条件：

- 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。





攻击URL排行

访问URL	访问占比	访问量
/	50.00%	42
/index.php	15.48%	13
/waf/api/execute/waf/cog/status	8.33%	7
/etc/passwd	8.33%	7
/admin/	3.57%	3
/api/antiddos/waf/config/list	3.57%	3
/wis-wsapi/CoordinatorPortType	3.57%	3
/plus/captchaaction.php	2.38%	2
/webtools/control/xmirpc	2.38%	2
/user.php	2.38%	2

攻击IP排行

访问IP	访问占比	访问量
39.156.7.125	93.85%	168
183.236.101.114	4.47%	8
120.244.115.1	1.68%	3

域名	访问url	告警级别	告警类型	客户端IP	地区	请求时间	处理方式
secctyun.cn	/waf/api/antiddos/waf/config/update	安全提示	信誉地雷	221.226.240.42	江苏省	2021-05-18 11:30:00	已记录
secctyun.cn	/waf/api/antiddos/waf/strategy/open	安全提示	信誉地雷	183.129.156.122	浙江省	2021-05-18 12:46:00	已记录
secctyun.cn	/waf/api/antiddos/waf/config/open	安全提示	信誉地雷	221.226.240.42	江苏省	2021-05-18 15:00:00	已记录
secctyun.cn	/api/antiddos/waf/config/list	高危告警	SQL注入	120.244.115.1	北京	2021-05-18 15:10:00	已阻断
secctyun.cn	/waf/api/antiddos/waf/config/update	安全提示	信誉地雷	221.226.240.42	江苏省	2021-05-18 16:10:00	已记录
secctyun.cn	/waf/api/antiddos/waf/config/save	安全提示	信誉地雷	183.63.152.18	广东省	2021-05-18 23:05:00	已记录
secctyun.cn	/waf/api/antiddos/waf/config/open	安全提示	信誉地雷	42.46.115.228	湖南省	2021-05-19 10:00:00	已记录
secctyun.cn	/waf/api/antiddos/waf/config/save	安全提示	信誉地雷	221.226.240.42	江苏省	2021-05-19 12:55:00	已记录

攻击趋势参数说明

参数	说明
WEB 拦截	包含且不限于 SQL 注入, XSS 跨站、跨站请求伪造、参数污染、缓存溢出、Cookie 投毒、XML 注入、XML 解析漏洞、恶意文件上传、远程命令执行、文件包含、多层编译攻击、动态应用混淆、

	恶意扫描、网站挂马、网站篡改、后门上传等黑客攻击以及针对 Web 应用框架和组件 漏洞发起的攻击。
CC 拦截	包括对 DNS Flood 攻击、SSL DDoS、Web Server 变种攻击、应用层快速攻击、CC 混合攻击等进行精准清洗和防护
高危事件	系统判定为攻击风险等级较高的攻击事件
攻击类型 TOP5	攻击次数 Top 5 的攻击类型以及各攻击类型的攻击次数。
攻击来源国家/地区 TOP5	攻击次数 Top 5 的地区以及来源各地区发起的攻击次数。
攻击 URL TOP10	受攻击统计次数 Top10 的 URL 以及各 URL 受攻击的次数。
攻击源 IP TOP10	攻击次数 Top 5 的攻击源 IP 以及各源 IP 发起的攻击次数。

3.4.3 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。

WEB应用防火墙 - 防护日志

域名 URL关键字 请求方法 告警级别
 状态码 客户端IP 地区
 日期范围 刷新 重置

序号	域名	请求方法	访问URL	告警级别	客户端IP	攻击类型	地区	请求时间	处理方式	操作
1	www.ctyun.cn	GET	/login	低	11.88.33	Abuse of Functionality/Command Execution	中国-北京	2021-06-02 09:37:04	告警	查看 误杀日志
2	www.ctyun.cn	GET	/vmcontrol/control	低	11.88.33	命令执行	中国-北京	2021-06-02 09:36:50	告警	查看 误杀日志
3	www.ctyun.cn	GET	/control/control	低	11.88.33	命令执行	中国-北京	2021-06-02 09:36:50	告警	查看 误杀日志
4	www.ctyun.cn	GET	/login	中	11.88.33	Abuse of Functionality/Command Execution	中国-北京	2021-06-02 09:36:49	告警	查看 误杀日志
5	www.ctyun.cn	GET	/control/control	低	11.88.33	命令执行	中国-北京	2021-06-02 09:36:48	告警	查看 误杀日志
6	www.ctyun.cn	GET	/vmcontrol/control	低	11.88.33	命令执行	中国-北京	2021-06-02 09:36:48	告警	查看 误杀日志
7	www.ctyun.cn	GET	/s/q04v3825t78f4mEho-3dVjy/WtHh2AHhokmmdMQrFLURa3V4uR26WBPDUqCA13Y7XU7zozpzcheww-a1Z_c7oEz48YjCY7qz2Fz_TPP9FRdLJxjCZHeBdEhQseivQ	低	11.88.33	Buffer Overflow/Command Execution	中国-北京	2021-06-02 09:36:43	告警	查看 误杀日志
8	www.ctyun.cn	GET	/gw/v1/portals/menu/GetTree	低	11.88.33	Abuse of Functionality/Command Execution	中国-北京	2021-06-02 09:36:42	告警	查看 误杀日志
9	www.ctyun.cn	GET	/h5/home/stat/q/s/vues-asp.js	较低	11.88.33	Abuse of Functionality/Command Execution	中国-北京	2021-06-02 09:36:42	告警	查看 误杀日志
10	www.ctyun.cn	GET	/gw/v1/portals/menu/GetTree	低	11.88.33	Abuse of Functionality/Command Execution	中国-北京	2021-06-02 09:36:42	告警	查看 误杀日志

1-10 / 共78条数据 1 2 3 4 5 6 7 8 9 10 条页

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
- ◆ 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）

查看
✕

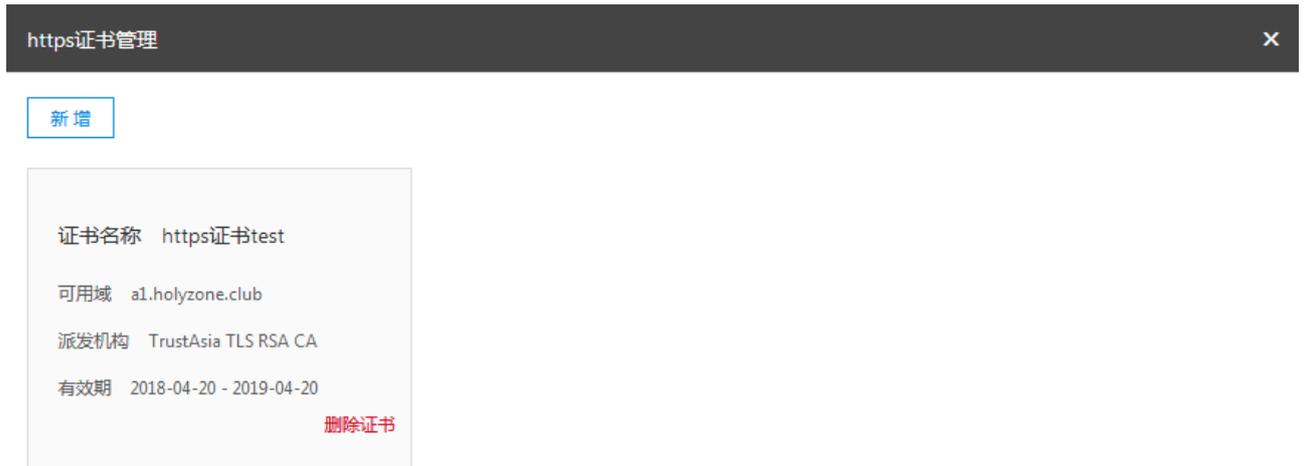
基础信息			
域名:	sec.ctyun.cn	ID:	1424352090519478077
攻击源IP:	115.206.124.172	告警等级:	低
攻击源端口:	64064	请求方式:	GET
攻击类型:	Information Leakage	匹配规则:	错误HTTP响应码
请求URL:	/dns/api/dns/instance/list	攻击时间:	2020-11-02 15:00:07
执行动作:	告警		
响应码:	500		
攻击IP详情			
地区:	CN	省份:	浙江
国家:	中国	地区:	杭州
运营商:	电信		
详细信息			
协议:	HTTP	协议版本:	1.1
Useragent:			
Referer:			

3.4.4 域名证书管理

点击 https 证书管理

[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：

新增证书
✕

证书名称:

证书公钥:

证书私钥:

确定
取消

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。

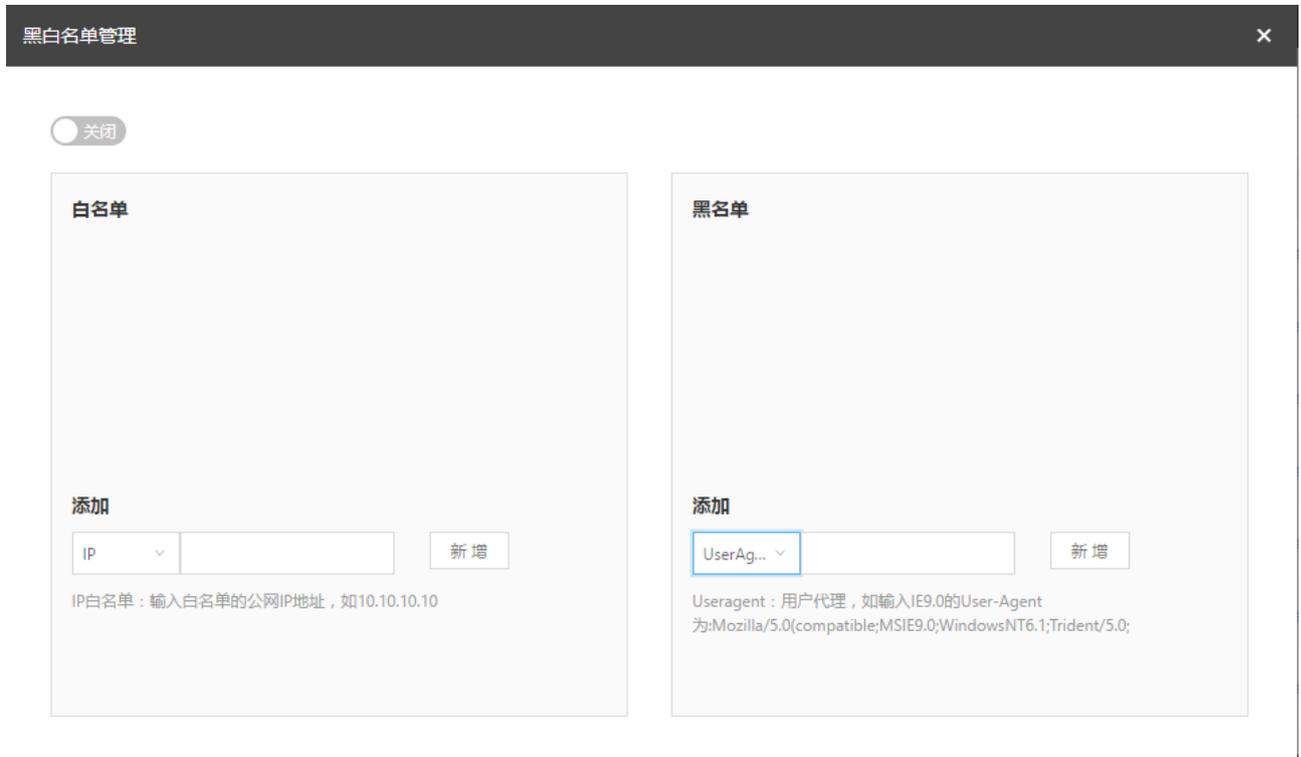
点击“删除证书”：删除证书时需要确认防护配置中（包括未启动的防护）未使用该证书，否则删除不成功。

3.4.5 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

3.4.6 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；

新增配置
✕

配置类型：黑名单 白名单

防护域：

防护域名：sec.ctyun.cn ✕ csoc.ctyun.cn ✕

黑白名单类型：

黑白名单内容：

确定
取消

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。

配置类型	黑白名单类型	黑白名单内容	域名	添加时间	状态	操作
白名单	ip	192.168.1.231	sec.ctyun.cn,csoc.ctyun.cn	2020-02-04	开启	查看 关闭

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，

黑白名单管理
✕

开启 黑白名单配置生效

白名单

[Redacted]

[Redacted]

192.168.1.231 ✕

添加

IP ▾

新增

IP白名单：对指定IP来源的请求放行

黑名单

添加

IP ▾

新增

IP黑名单：对指定IP来源的请求封禁

确定
取消

点击  并确认，关闭全局黑白名单配置中详情展示：

详情
✕

配置类型：白名单

防护域名：csoc.ctyun.cn

黑白名单类型：ip ▾

黑白名单内容：192.168.1.231

序号	域名	添加时间	备注
1	sec.ctyun.cn	2020-02-04	域名关闭

1-1 / 共1条数据
<
1
>
10 条/页 ▾

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/##/也会匹配规则；

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;`

3.5 Web 应用防火墙防护配置管理

配置管理界面可用于开启防护/关闭防护，HTTPS 强制跳转，防护模式选择以及自定义防护配置，创建更有针对性的防护策略

3.5.1 防护状态调整

WAF 防护配置”界面点击“开启防护”弹出如下对话框：



点击确认或取消，确认是否开启防护，进入防护后的域名，可以选择“暂停防护”，暂停防护后云 WAF 将关闭所有防护功能，只进行业务请求的七层代理转发，此功能可用于检查是否为云 WAF 造成的业务异常与误拦截行为。

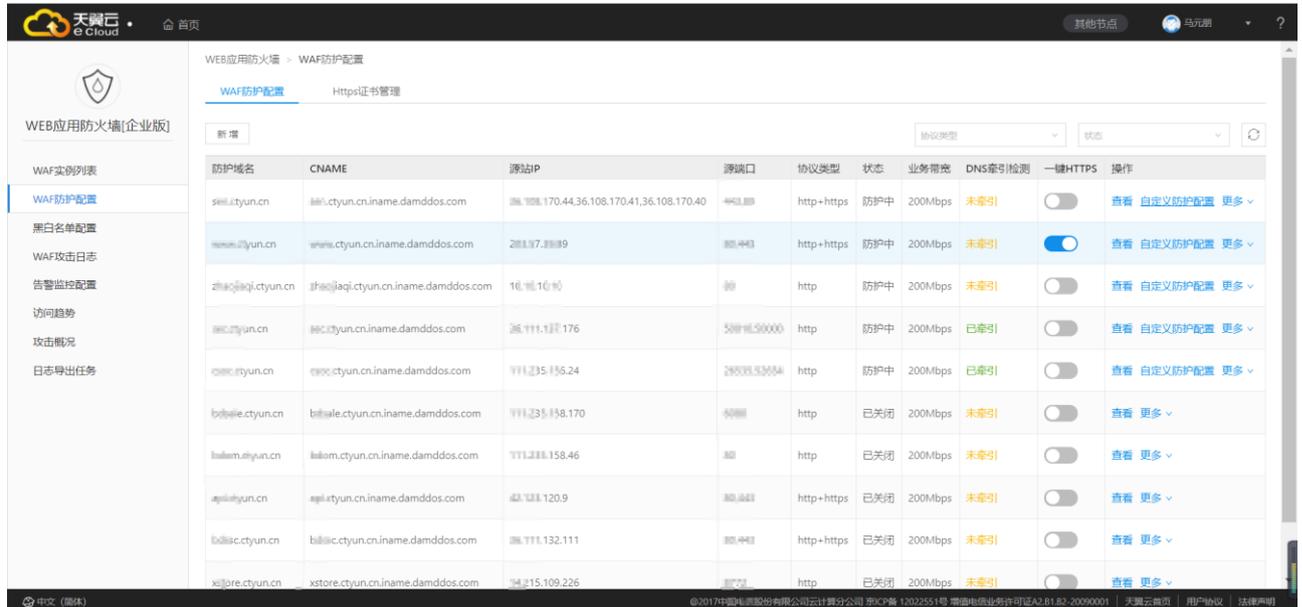
Web 应用防火墙防护配置中：

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运转，请确定关闭该域名的防护功能。

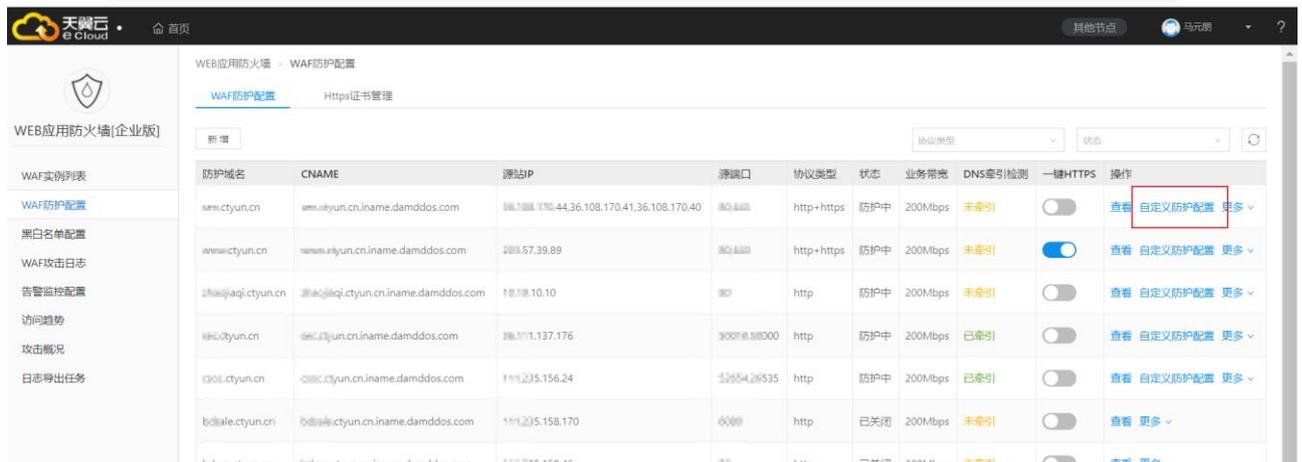
3.5.2 https 强制跳转

WAF 防护配置”界面点击“一键开启 HTTPS”开关。开启后，网站所有 HTTP 请求都将强制使用 HTTPS 协议访问业务，并默认跳转至 443 端口。因此，开启 HTTPS 跳转前，

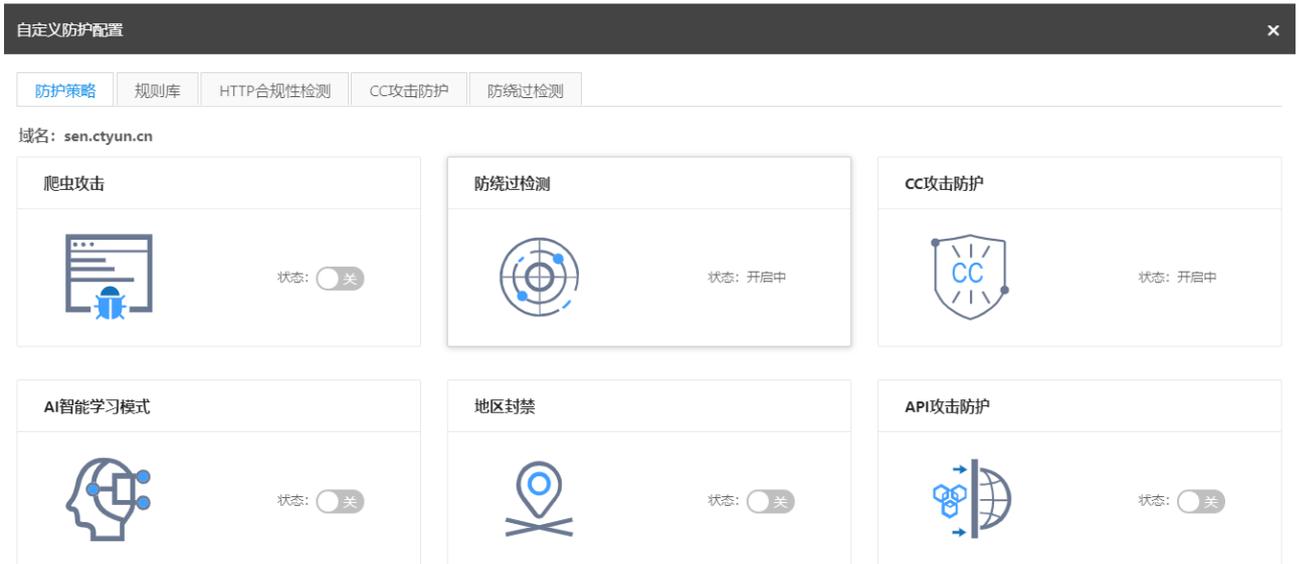
请确保业务支持 HTTPS 协议且 HTTPS 协议的 443 端口防护配置已开启。



3.5.3 自定义防护策略



客户可在防护配置末尾处点击自定义防护策略进入策略自定义界面



3.5.3.1 设置攻击防绕过

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



3.5.3.2 设置 CC 攻击防护

自定义 CC 防护支持根据公网 IP 访问行为进行人机识别，访问频率与封禁时间的自定义配置

The screenshot displays the '自定义防护配置' (Custom Protection Configuration) interface. It features several tabs: '防护策略' (Protection Strategy), '规则库' (Rule Library), 'HTTP合规性检测' (HTTP Compliance Detection), 'CC攻击防护' (CC Attack Protection), and '防绕过检测' (Anti-Bypass Detection). The 'CC攻击防护' tab is active, showing a yellow banner with the text: '自定义CC防护支持根据公网IP访问行为进行人机识别，访问频率与封禁时间的自定义配置'. Below this, the configuration is organized into sections: '防御方式' (Defense Method) with options for '人机识别' (Human Machine Identification) including '图片验证' (Image Verification) and 'JavaScript验证' (JavaScript Verification); '处置动作' (Action) with radio buttons for '请求阻断' (Request Blocking) and '请求限频' (Request Rate Limiting); '增长频率' (Growth Rate) with input fields for '请求次数' (Request Count) set to 5 and '增长率' (Growth Rate) set to 150%; '访问频率' (Access Frequency) with input fields for '请求次数' (Request Count) set to 10; and '时间配置' (Time Configuration) with input fields for '检测周期' (Detection Cycle) set to 120s and '封禁时间' (Ban Time) set to 7200s. A '保存' (Save) button is located at the bottom right.

3.5.3.3 设置 AI 学习模式

自学习模式是先对流量进行一些检测，只会产生告警但是不进行阻断，在经过 7 天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

3.5.3.4 设置地区封禁

开启后禁封国外的访问流量

3.5.3.5 设置 HTTP 合规性检测

HTTP 合规性检测支持对 HTTP 请求中携带的 header 与参数数量进行自定义配置

自定义防护配置

防护策略 规则库 **HTTP 合规性检测** CC攻击防护 防绕过检测

HTTP 合规性检测支持对 HTTP 请求中携带的 header 与参数数量进行自定义配置

域名: sen.ctyun.cn

最大请求头数量:
可选范围: 1~150, HTTP 请求携带的 header 数量上限

最大请求参数数量:
可选范围: 1~5000, HTTP 请求携带的参数数量上限, 过多的参数数量将造成缓冲区溢出和应用程序崩溃等问题

保存

4 售前常见问题

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,

4.2 天翼云 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。

4.3 天翼云 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。

4.4 天翼云 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。

4.5 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。

4.6 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。

4.7 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。

4.8 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。

4.9 修改 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。

4.10 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。

4.11 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

5 售中常见问题

5.1 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至防护平台进行检测，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。

5.2 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。

5.3 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。

5.4 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？

1. 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。

5.5 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。

5.6 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，请联系云堤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。

5.7 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，请联系云堤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。

5.8 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；

5.9 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。

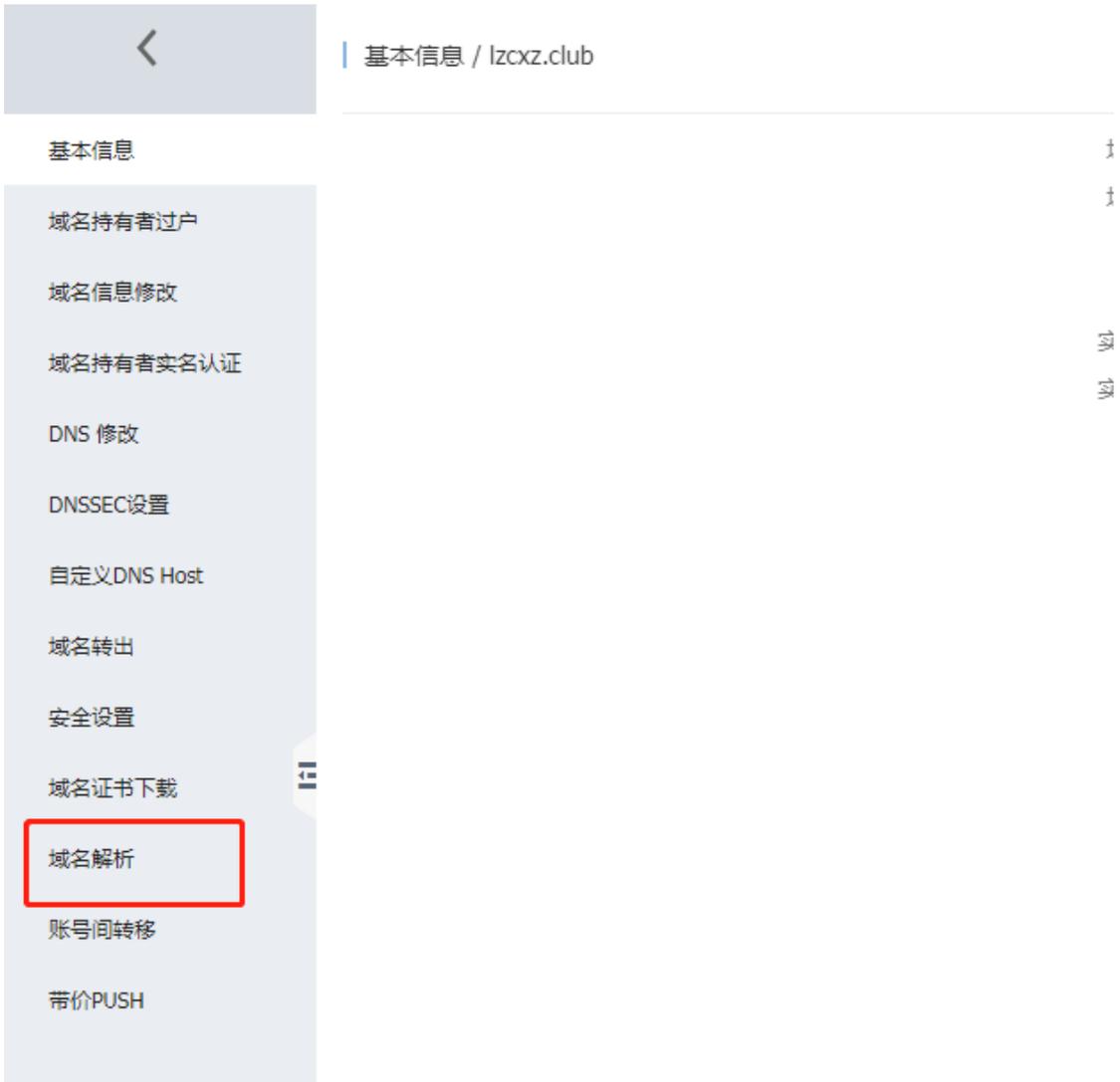
5.10 如何在万网中修改 DNS 解析

答：1. 登陆万网 <https://wanwang.aliyun.com/>;



The screenshot shows the '域名列表' (Domain List) page in the Wanwang console. The interface includes a search bar for domains, filter tabs for '全部域名', '急需续费域名', '急需赎回域名', '未实名认证域名', and '预登记域名'. A table lists domains with columns for '域名', '域名类型', '域名状态', '域名分组', and '注册日期'. The domain 'lzcxz.club' is highlighted with a red box. Below the table are buttons for '域名续费', '转至其他账号', and '更多批量操作'. At the bottom, there are links for '域名注册' and '域名转入'.

域名	域名类型	域名状态	域名分组	注册日期
<input type="checkbox"/> lzcxz.club	New gTLD	急需续费	未分组	2011



修改记录

记录类型: CNAME- 将域名指向另外一个域名

主机记录: www .lzcxz.club ?

解析线路: 默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路... ?

* 记录值: www.qhxncsjg.gov.cn.iname.damddos.com

* TTL: 10 分钟

取消 确定

2. 将您原来的域名 cname 修改为 web 应用防火墙提供的域名。
3. 修改完成后点击[提交], 完成修改。

6 售后常见问题

6.1 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 18701344717

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。

6.2 什么情况下产品会误拦截

3.3.1 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 WebsheII 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。

6.3 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）；

6.4 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；

6.5 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；

6.6 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。

6.7 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。