天翼云 Web 应用防火墙（企业版）

用户使用指南

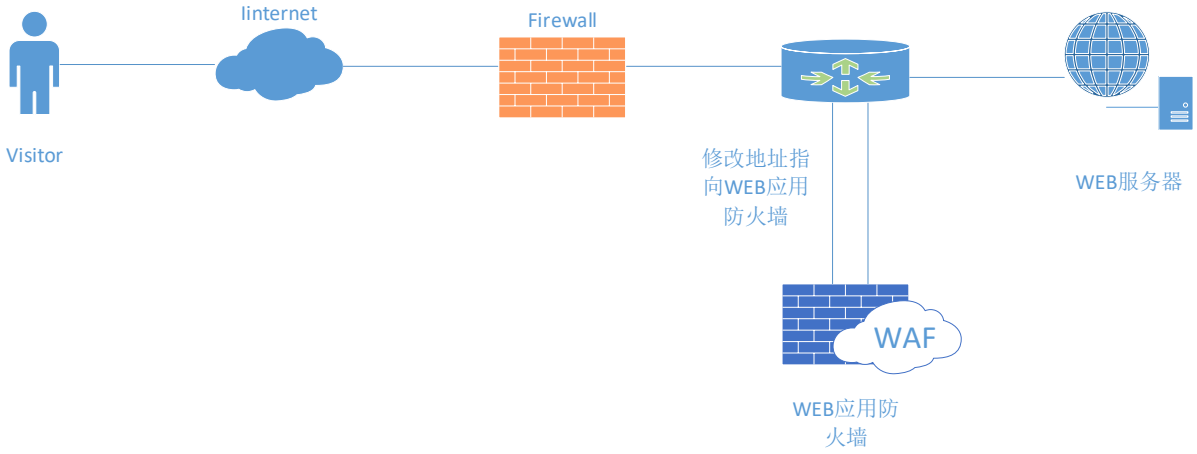
天翼云科技有限公司

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，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

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，此为基础套餐包的量，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。

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】。

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】。

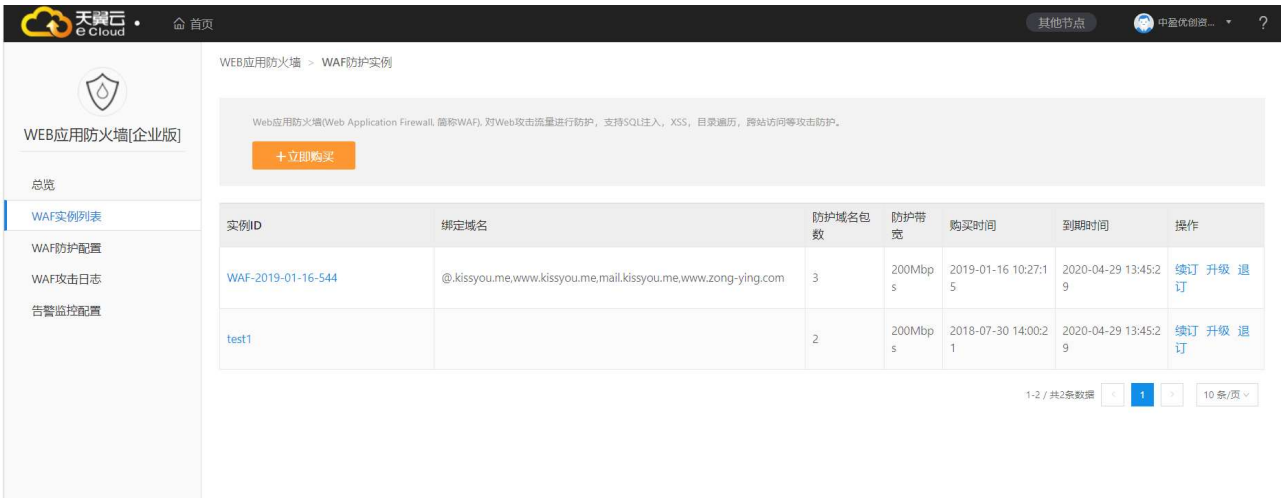
2.5 退订

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 WEB 应用防火墙管理

3.1 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

3.2 域名备案

3.2.1 Web 应用防火墙防护配置

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；

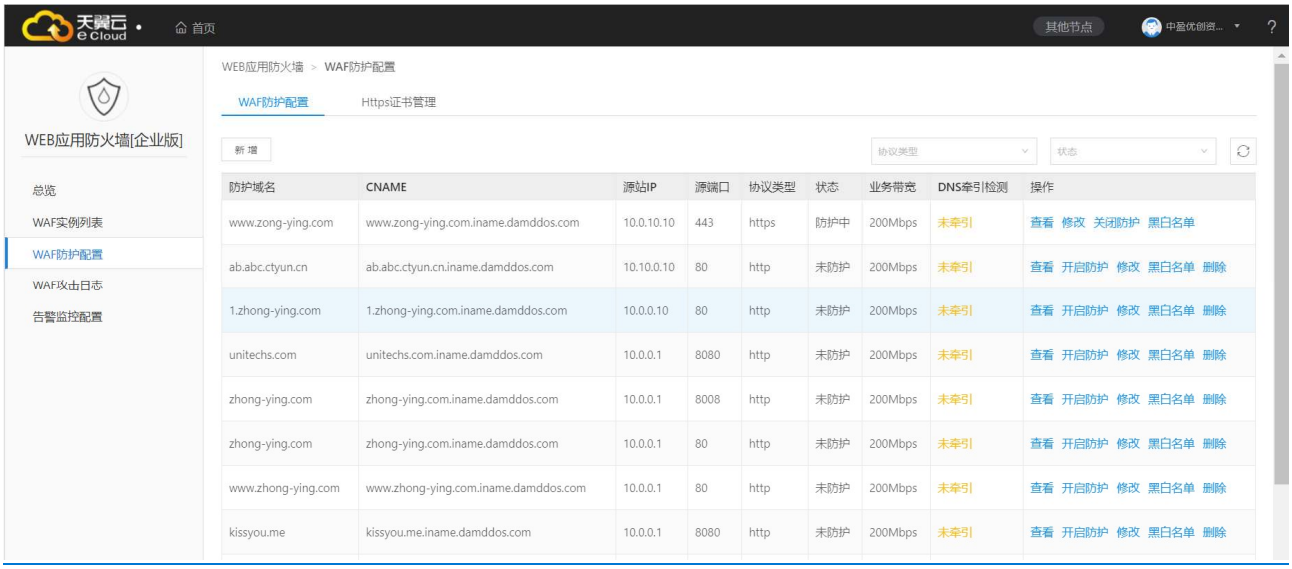
删除，点击删除，将当前的防护配置清除，需要确保防护域名指回源站；

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；

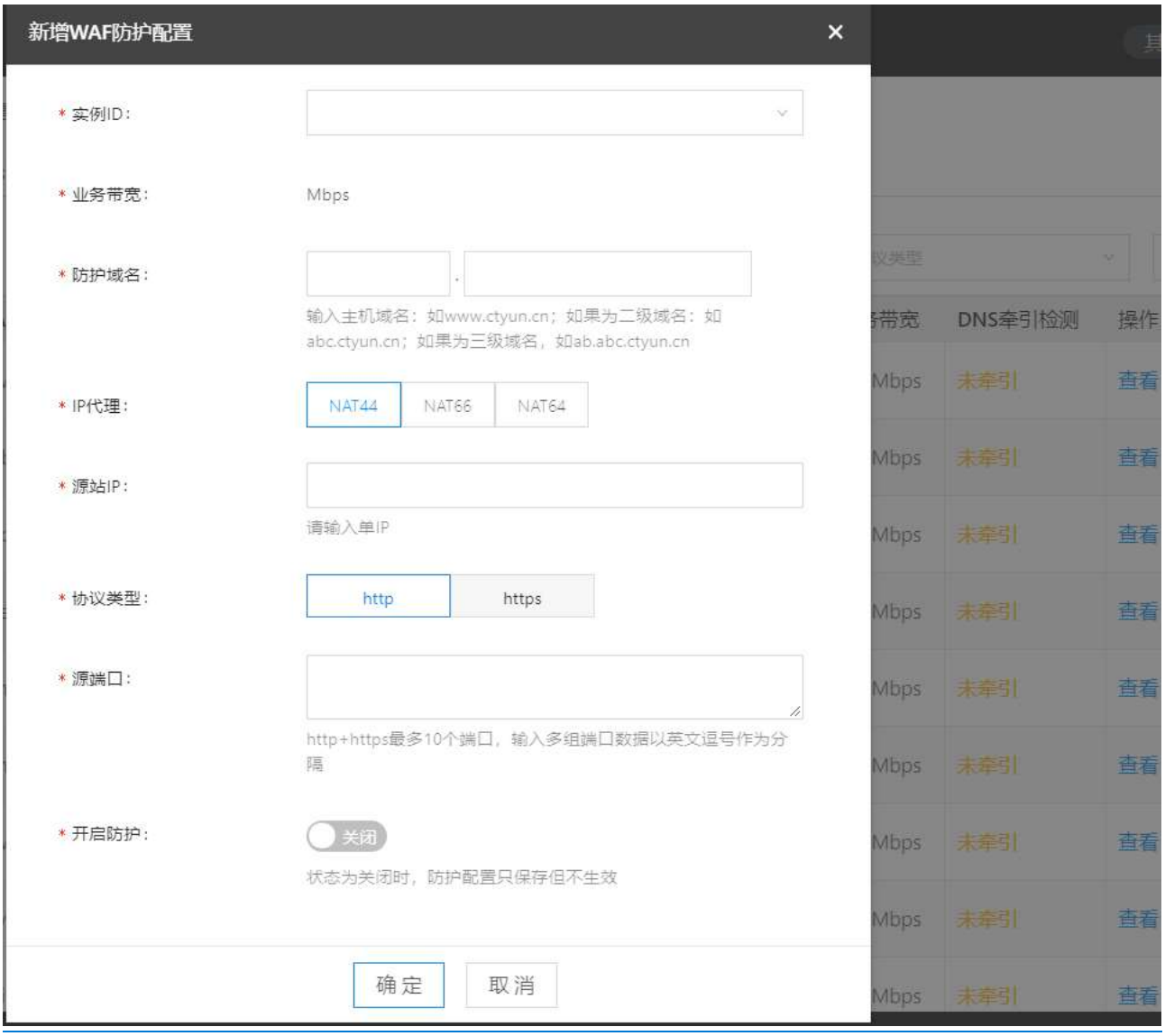
开启防护，开启已新增（或者关闭过）的防护配置，开启成功后，您可以联系域名服务商将 DNS 域名指向防护 Cname 地址，届时防护配置正式生效。

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：



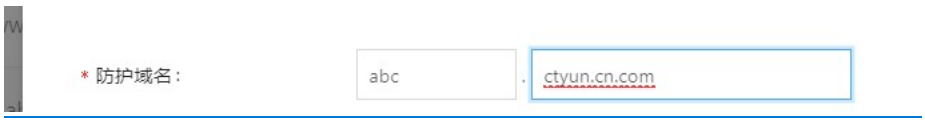
1、 选择实例 ID；

2、 输入防护域名；

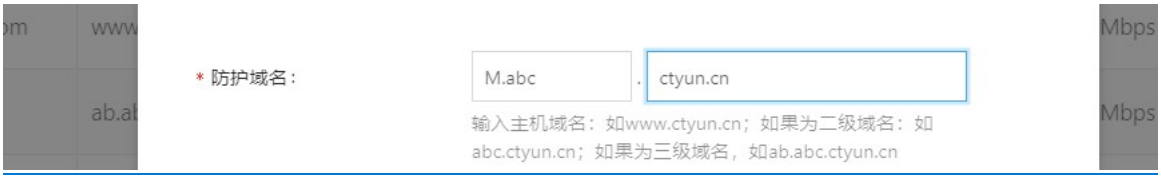
输入格式示例：

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

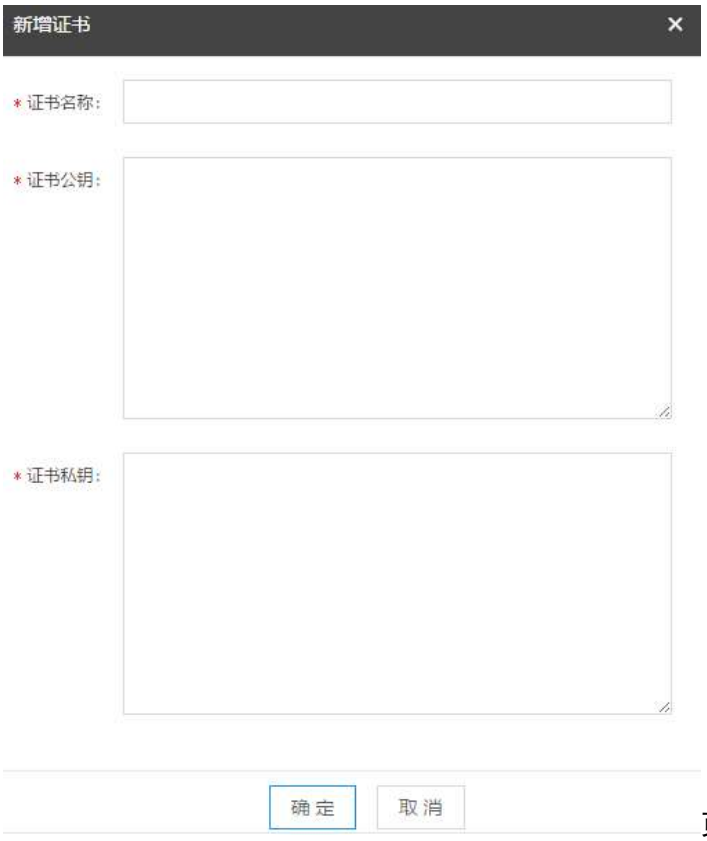
nat64 是指原站有 v4 的地址

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。

3.2.2 Web 应用防火墙 Https 证书管理

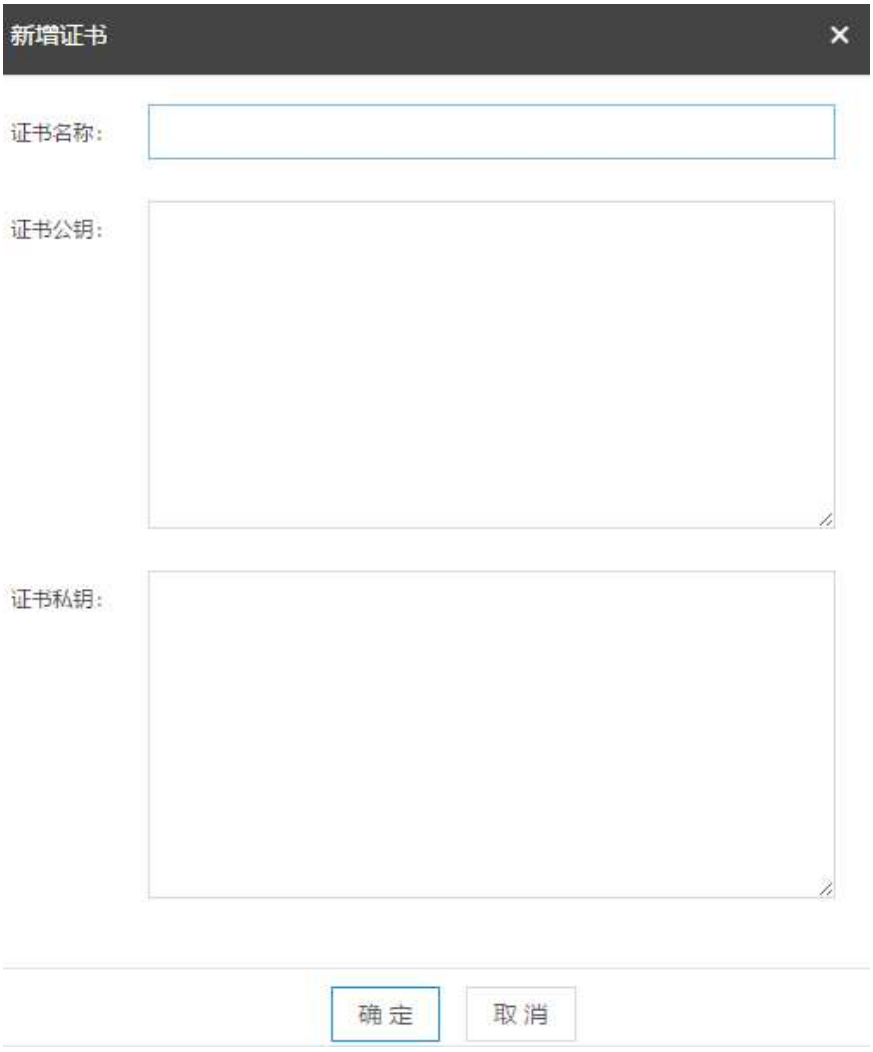
点击 https 证书管理 

，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。

3.2.3 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

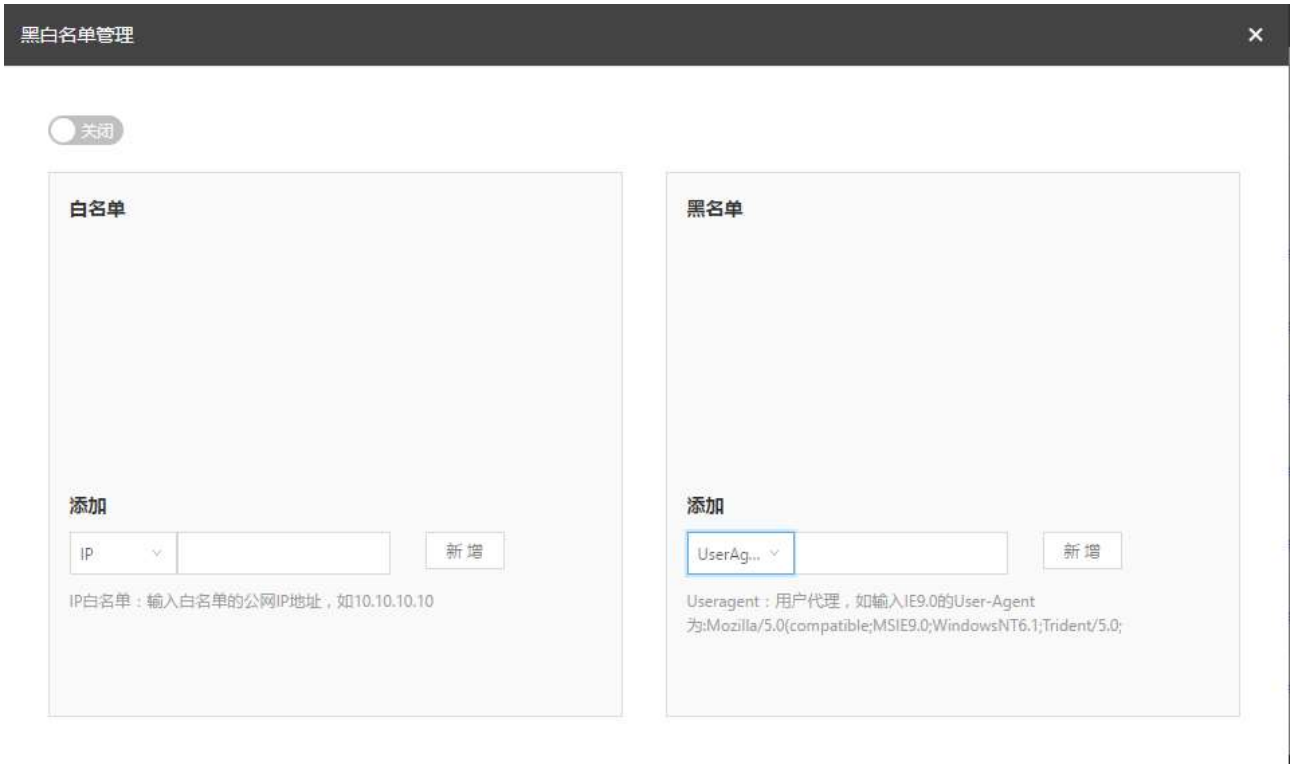
DNS 牵引指向 Cname 后，web 应用防火墙防护正式完成配置。

3.2.4 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

3.2.5 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；

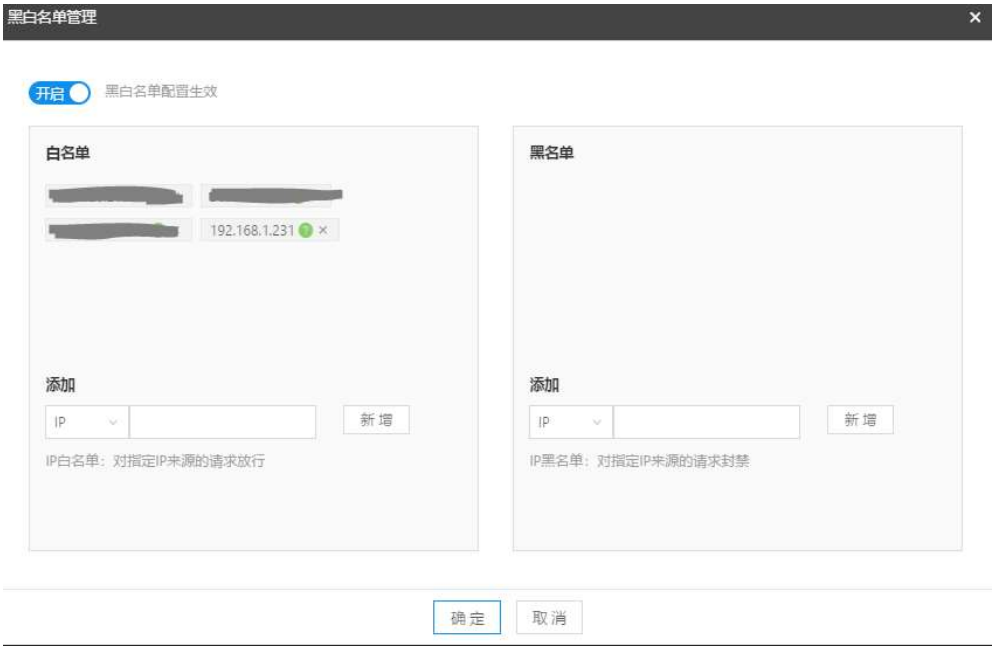
配置类型：即配置黑名单或者白名单

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

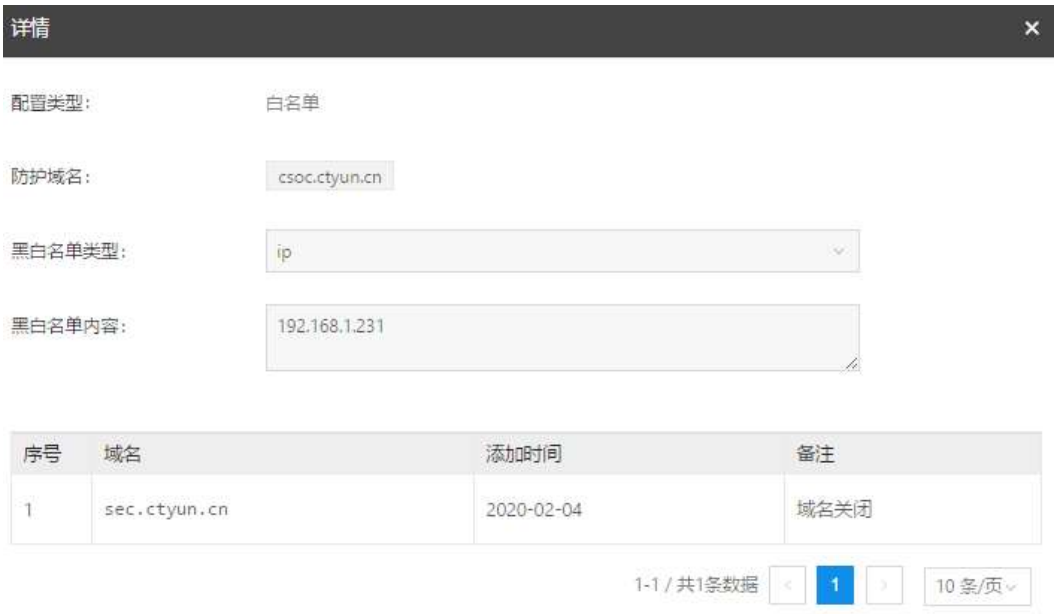
防护域名：即黑名单或者白名单配置后，对防护域下面在用的子域名进行关联，黑白名单将对关联的黑白名单生效，同时配置人员可以对关联的子域名进行人工删除/增加，精确实现对防护域下面的指定子域名进行黑白名单配置。

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，



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;

3.2.6 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。

3.2.7 暂停防护

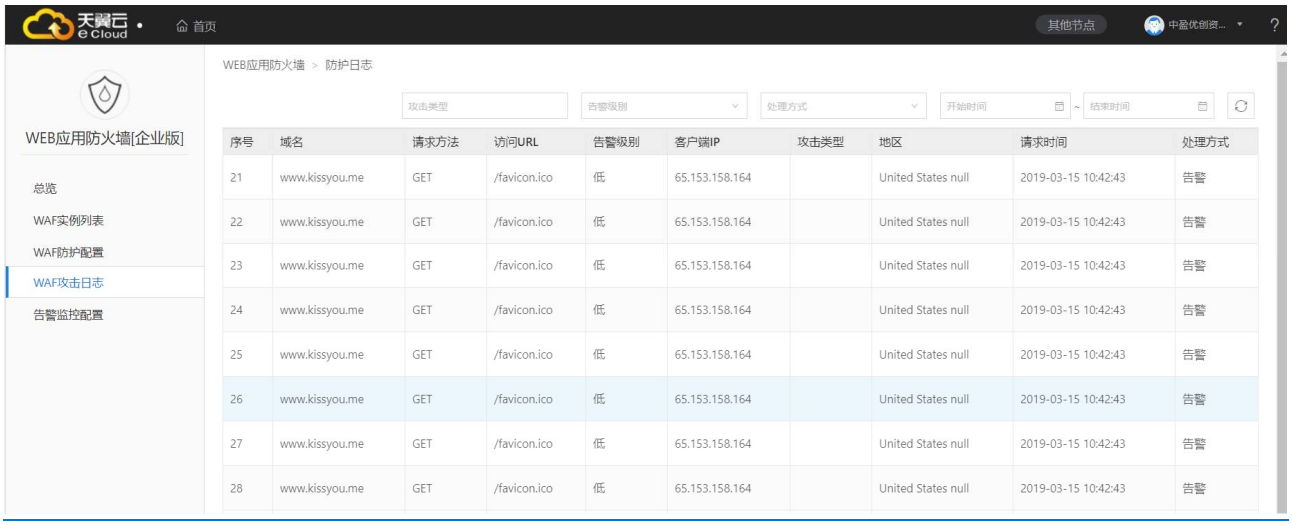
Web 应用防火墙防护配置中：

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。

3.3 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：

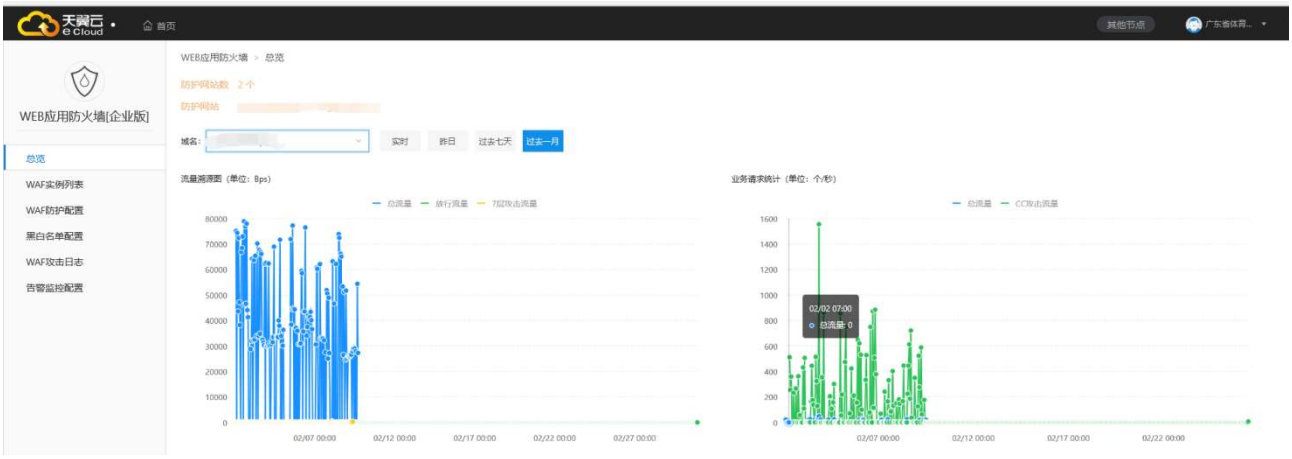
- 域名：告警域名
- 请求方法：http get/http post
- 访问 URL
- 告警级别
- 客户端 ip
- 地区
- 请求时间
- 处理方式

3.4 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



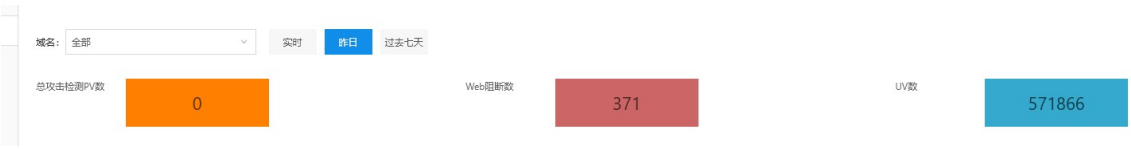
4. 显示溯源图

- 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。



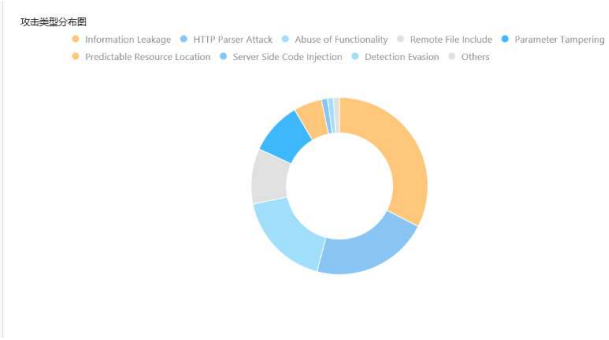
- 检测到的攻击访问 pv 数量

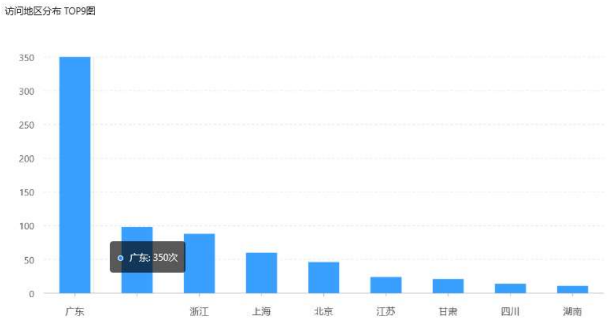
  Web 阻断的数量也就是进行拦截的数量

  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

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。

每个二级域名支持 10 个 IP 端口。

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 为何需要添加白名单到系统内网的安全设备中

答：网站成功接入云 web 应用防火墙平台后，所有网站访问请求将先流转到防护平台进行监控，经过滤后再返回到源站服务器。由于源站服务器收到的所有请求都来自 web 应用防火墙云平台的 IP，源站服务器上的安全软件（如安全狗、云锁）看来，这种行为很可疑，有可能触发屏蔽云 web 应用防火墙回源 IP 的操作。因此，在接入 web 应用防火墙平台前，您需要在源站服务器的安全软件上设置放行所有 web 应用防火墙平台的回源 IP。

5.2 如何添加白名单

答：打开源站服务器上的安全软件，将 web 应用防火墙平台 ip： 36.111.137.0/24 添加到白名单。

5.3 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；

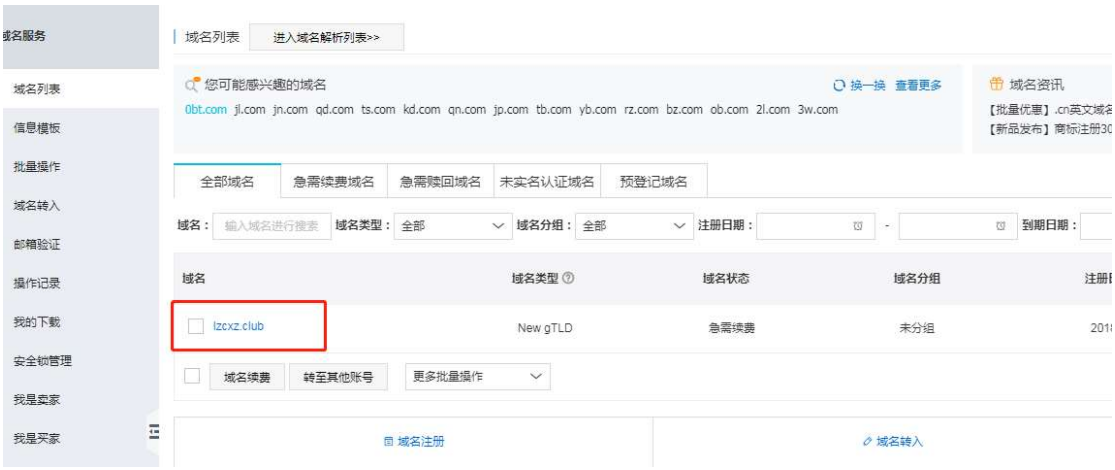
如果域名的 DNS 解析服务由第三方提供（如万网、新网等），登陆域名提供 DNS 解析的服务商网站进行修改；

5.4 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。

5.5 如何在万网中修改 DNS 解析

答：1.登陆万网 https://wanwang.aliyun.com/；


域名服务
域名列表
信息模板
批量操作
域名转入
邮箱验证
操作记录
我的下载
安全锁管理
我是卖家
我是买家
域名列表
进入域名解析列表>>
您可能感兴趣的域名
换一换 查看更多
0bt.com ji.com jn.com qd.com ts.com kd.com qn.com jp.com tb.com yb.com rz.com bz.com ob.com 2l.com 3w.com
域名资讯
全部域名
急需续费域名
急需赎回域名
未实名认证域名
预登记域名
域名：
输入域名进行搜索
域名类型：
全部
域名分组：
全部
注册日期：
到期日期：
域名
域名类型
域名状态
域名分组
lzcxz.club
New gTLD
急需续费
未分组
域名续费
转至其他账号
更多批量操作
域名注册
域名转入


基本信息 / lzcxz.club
基本信息
域名持有者过户
域名信息修改
域名持有者实名认证
DNS 修改
DNSSEC设置
自定义DNS Host
域名转出
安全设置
域名证书下载
域名解析
账号间转移
带价PUSH

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

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，如在请求的 POST 中包含“目录遍历”、“命令执行”、“onclick 参数”、“div tag: style 参数”等相关关键字，则会触发拦截，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 web 应用防火墙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，临时加白名单（使用后删除白名单）。

4）国际流量整体拦截

Web 应用防火墙支持针对 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 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。