天翼云 安全加速

用户控制台使用指南

天翼云科技有限公司

目 录

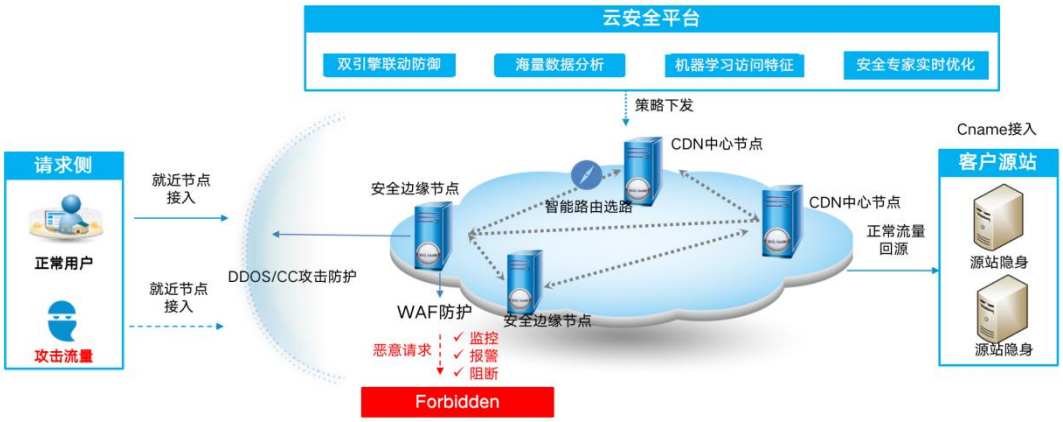
1.产品介绍

1.1 产品定义

CDN（CT–CDN，Content Delivery Network）,即内容分发网络，是中国电信依托分布于全国的网络节点搭建的一层虚拟网络。它将源站内容分发至最接近用户的节点，使用户可就近获取所需内容，解决因跨运营商访问、跨地域访问、服务器带宽及性能带来的访问延迟问题，提高用户访问的响应速度和成功率，适用于站点加速、点播、直播等场景。

安全加速（secure Content Delivery Network，SCDN），又名安全的内容分发网络。构建于电信云 CDN 平台之上，在 CDN 边缘节点中加入丰富的安全能力，形成一张安全加速的网络。兼具内容稳定加速与全方位安全防护，同时提升网页用户体验和源站的安全性。

安全加速基本架构:



1.2 术语解释

CNAME 记录

CNAME (Canonical Name)，即别名，用于把一个域名解析到另一个域名，当 DNS 系统在查询 CNAME 左面的名称的时候，都会转向 CNAME 右面的名称再进行查询，一直追踪到最后的 PTR 或 A 名称，成功查询后才会做出回应，否则失败。例如，您有一台服务器，使用 docs.example.com 访问，您又希望通过

documents.example.com 也能访问该服务器，那么就需要在您的 DNS 解析服务商添加一条 CNAME 记录，将 documents.example.com 指向

docs.example.com，添加该条 CNAME 记录后，所有访问 documents.example.com 的请求都会被转到 docs.example.com，获得相同的内容。

CNAME 域名

接入 CDN 时，在天翼云控制台添加完加速域名后，您会得到一个天翼云 CDN 给您分配的 CNAME 域名，（该 CNAME 域名一定是*. ctdns.cn），您需要在您的 DNS 解析服务商添加 CNAME 记录，将自己的加速域名指向这个*. ctdns.cn 的 CNAME 域名，这样该域名所有的请求才会都将转向天翼云 CDN 的节点，达到加速效果。

DNS

DNS 即 Domain Name System，是域名解析服务的意思。它在互联网的作用是：把域名转换成为网络可以识别的 ip 地址。人们习惯记忆域名，但机器间互相只认 IP 地址，域名与 IP 地址之间是一一对应的，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，整个过程是自动进行的。比如：上网时输入的 www.baidu.com 会自动转换成为 220.181.112.143。

常见的 DNS 解析服务商有：阿里云解析，万网解析，DNSPod，新网解析，Route53（AWS），Dyn，Cloudflare 等。

加速域名

加速域名是用户提供的需要使用 CDN 加速服务的域名，应用于网站、电子邮件等。

边缘节点

在天翼云所有文档中，边缘节点、CDN 节点、Cache 节点、缓存节点、加速节点、天翼云节点等都是指天翼云边缘节点。边缘节点是相对于网络的复杂结构而提出的一个概念，指距离最终用户接入具有较少的中间环节的网络节点，对最终接入用户有较好的响应能力和连接速度。其作用是将访问量较大的网页内容和对象保存在服务器前端的专用 Cache 设备上，以此来提高网站访问的速度和质量。

回源 HOST

回源 host 决定回源请求访问到源站上的具体某个站点。

例 1：源站是域名源站为 www.a.com，回源 host 为 www.b.com，那么实际回源是请求到 www.a.com 解析到的 IP，对应的主机上的站点 www.b.com。

例 2：源站是 IP 源站为 1.1.1.1，回源 host 为 www.b.com，那么实际回源的是 1.1.1.1 对应的主机上的站点 www.b.com。

协议回源

协议回源指回源时使用的协议和客户端访问资源时的协议保持一致，即如果客户端使用 HTTPS 方式请求资源，当 CDN 节点上未缓存该资源时，节点会使用相同的 HTTPS 方式回源获取资源；同理如果客户端使用 HTTP 协议的请求，CDN 节点回源时也使用 HTTP 协议。

过滤参数

过滤参数是指当 URL 请求中带“？”并携带参数请求到 CDN 节点的时候，CDN 节点在收到该请求后可根据配置决定是否将该带参数的 URL 请求回源站。当开启过滤参数时，该请求到 CDN 节点后会截取到没有参数的 URL 向源站请求。并且 CDN 节点仅保留一份副本。如果关闭该功能，则每个不同的 URL 都缓存不同的副本在 CDN 的节点上。

示例：

客户端发起请求“http://www.test.com/a.jpg?x=1”到 CDN 节点

开启“过滤参数”功能：

CDN 节点收到客户端请求后，向源站发起请求为：“http://www.test.com/a.jpg”（忽略参数 x=1），待源站响应“http://www.test.com/a.jpg”请求指向的内容、且 CDN 节点获取到该内容后，CDN 节点保留一份所获取内容的副本，然后向终端返回该内容。此后，在该内容副本的有效期内，客户端所有类似“http://www.test.com/a.jpg?参数”的请求，CDN 节点均返回存储的“http://www.test.com/a.jpg”副本。

关闭“过滤参数”功能：

对于所有类似“http://www.test.com/a.jpg?参数”的请求，每个不同的 URL 都缓存不同的副本在 CDN 的节点上。例如：“http://www.test.com/a.jpg?x=1”和“http://www.test.com/a.jpg?x=2”会缓存两份副本，根据源站返回的内容，这两份副本可能相同，也可能不同。

Web 安全

相关 Web 应用层面的安全问题与事件,包括各种 Web 组件、协议、应用等。

正则防护

经验规则集，自动为网站防御 SQL 注入、XSS 跨站、Webshell 上传、命令注入、后门隔离、非法文件请求、路径穿越、常见应用漏洞攻击等通用的 Web 攻击。

网站白名单

通过设置网站白名单，可以让满足条件的请求不经过任何 Web 应用防火墙防护模块的检测，直接访问源站服务器。

IP 黑名单

支持一键阻断来自指定 IP 地址、IP 地址段以及指定地理区域的 IP 地址的访问请求。

0day 漏洞

0Day 是指在系统商在知晓并发布相关补丁前就被掌握或者公开的漏洞信息。

CC 攻击

攻击者借助代理服务器生成指向受害主机的合法请求，实现 DDOS 和伪装就叫：CC(Challenge Collapsar)，CC 主要是攻击页面，属于应用层攻击。

防敏感信息泄露

帮助网站过滤服务器返回内容（异常页面或关键字）中的敏感信息（例如身份证号、银行卡号、电话号码和敏感词汇），脱敏展示敏感信息或返回默认异常响应页面。

网络爬虫

又称为网页蜘蛛，网络机器人，是一种按照一定的规则，自动地抓取万维网信息的程序或者脚本。

挖矿

过借助大量计算能力来计算产生虚拟货币。

DDoS

分布式拒绝服务攻击是指攻击的发出点是分布在不同地方，且所请求的服务往往要消耗大量的系统资源，造成目标主机无法为用户提供正常服务。

流量清洗

对流量进行实时监控，及时发现包括 DOS 攻击在内的异常流量，在不影响正常业务的前提下，清洗掉异常流量，主要是 DDOS、CC 这类攻击的主要处理手段

1.3 产品功能

WAF 功能

高级访问控制

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。

高级访问限速

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。

请求合规检测

请求方法检测：只允许指定请求方法访问网站。

请求协议检测：只允许指定协议版本访问网站。

请求头部缺失检测：请求缺少指定头部禁止访问网站。

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。

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。

Web 漏洞防护

针对请求数据进行漏洞检测，对异常数据进行拦截，防止攻击请求到达源站。

批量注册

通过对注册 URL 访问数量统计，进行阈值拦截，防止网站注册链接被恶意请求，造成正常客户无法使用。

暴力破解

对采用暴利破解的防护连接进行请求量统计，达到阈值数量后进行拦截，避免用户密码被破解，造成信息泄露。

Web 挖矿

通过检测网页上的挖矿信息，进行清理，移除异常数据，保证客户机器安全。

广告防护

通过对页面插入 js 进行检测，并对检测到的广告进行清除或者记录告警日志处理，使展示给用户的界面没有广告，同时可以针对检测出来的广告进行离线分析。

支持对广告配置白名单功能，针对特定的广告不进行清除与告警处理，满足客户的定制需求。

撞库防护

根据防护范围获取登录 post 包，从中得到用户名和密码并根据相应的加密方式进行解密；利用解密后的用户名和密码判断是否为撞库攻击，若为撞库攻击并且针对某一作用域在统计周期内达到拦截阈值，则进行相应拦截，保护网站用户密码被破解。

敏感词防护

敏感词过滤：可配置针对银行卡、身份证、手机号进行页面过滤，防止网站敏感信息泄露。

特定信息例外：配置指定数据允许显示在界面上，针对企业公示信息配置，保证正常数据明文显示。

CSRF 防护

referer 控制：对页面请求中的 referer 这个请求头参数值进行限制，有效阻止因误触恶意链接导致的恶意链接页面 js 执行造成的用户损失。

扫描器控制：可以指定恶意扫描器所带 referer 内容限制恶意扫描器干扰正常业务。

简单爬虫限制：可以指定特定入口网站 referer 防止爬虫消耗资源。

Cookie 防护

cookie 加密：对指定 cookie 字段的值进行加密，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

Cookie 签名：对 cookie 签名防止因随意篡改导致的漏洞触发、未授权访问，也能在一定程度上限制基于 cookie 修改的爬虫。

Httponly 功能：限制 cookie 被 js 读取的功能，防止一些基于 cookie 的攻击，比如 xss、csrf 等。

抗 D 功能

CC 防护

针对异常请求配置 CC 阈值防护，当达到指定限制访问次数后，进行人机识别，防止非正常用户访问网站，造成网站资源耗尽。

网络层防护

针对异常请求配置网络层各个维度阈值防护，当达到设置的阈值时，实时阻断 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、各类反射攻击等攻击，防止非正常客户访问网站，造成网站资源耗尽。

1.4 产品优势

覆盖|丰富的资源覆盖

国内拥有丰富的节点覆盖承载能力，覆盖多运营商、主要省份和城市无盲点。、

加速节点可根据需求随时增加，致力于客户的发展壮大。

功能|特色的安全防护

敏感信息回显脱敏，保护用的身份证号、手机号和卡号等敏感信息

撞库攻击防护，防止网站撞库攻击，保护网站用户数据安全

恶意挖矿防护，识别 js 挖矿脚本，避免访问网站的用户被利用成“挖矿机”

客户端防广告，移除客户端被插入的广告，保护内容安全

安全|可靠的安全防护

分布式集群防护，单点故障自动转移，确保网站的高可用性

利用大平台优势，基于全网、全行业流量的攻击数据，结合机器学习算法，构建一套智能防护体系

精准防护，域名粒度的防护策略，结合客户自身业务定制化防护策略

维护|完善的售后服务

集中监控和分散维护相结合，NOC 工程师 7×24 小时集中监控，网络工程师 7×24 小时在线支持，所有节点都有现场服务工程师进行服务保障。

便捷|便捷的接入方式

零部署、零运维，使用 CNAME 接入，云端安全专家配置策略

安全加速一体化，基于 CDN 的架构，实现加速防护一体化

透明|透明的售卖机制

可根据需要选择资源套餐包产品或按量计费产品，费用透明，可控，灵活。

2.购买指南

2.1 价格

计费模式：混合计费模式
计费方式：预付费+后付费
【计费项说明】

计费方式	描述	说明
按流量	按照每日的实际流量计费。	适用于域名流量曲线波动较大，有带宽尖峰全天内带宽利用率小于 30%。
按带宽	按照每日带宽峰值计费每 5 分钟统计一个带宽峰值，每日得到 288 个值，取其中的最大值。	适用于域名流量曲线比较平稳全天内带宽利用率大于 30%。
资源包	一次性付费，资源包具有时效性。	当前计费类型为流量包，可以使用流量包，开通 https 可以使用静态 https 的请求数包
功能包	保底功能包，是开通安全产品默认开通	开通安全加速中的 waf 功能，默认开启 waf 基础防护包，开通抗 D 流量清洗功能，必须开通抗 D 流量清洗包

- 抗 D 流量清洗中的安全保底带宽套餐：带宽未超过保底值，则不额外收费。套餐含安全保底带宽、防护请求数 QPS、接入域名数等，按月付费。如果安全保底带宽不能满足需求，可以购买弹性带宽，当带宽超出购买防护带宽时，会停止防护服务。

流量计费

1. 流量标准资费

流量阶梯	标准资费
(0TB, 10TB]	0.2 元/GB
(10TB, 50TB]	0.18 元/GB

流量阶梯	标准资费
(50TB, +∞)	0.15 元/GB

计费项：国内
计费方式：按流量计费（阶梯计费模式）
计费周期：按日结算，定时扣费（每日 12：00 后出前一日账单并扣费，具体出账时间以系统为准）
计费场景：适用于域名流量曲线波动较大，全天内带宽利用率小于 30%，且有带宽尖峰的用户。

示例

假设 5 月 1 日至 5 月 2 日每日流量为 9TB;

5 月 3 日至 5 月 4 日每日流量为 25TB，则计费如表 2-2 所示:

流量计费示例

日期	流量（TB）	累积流量（TB）	区间分布	流量分布	计费标准（元/GB）	费用（元）	合计（元）
5.1	9	9	[0, 10）	9	0.2	1800	1800
5.2	9	18	[0, 10）	1	0.2	200	1640
			[10, 50)	8	0.18	1440	
5.3	25	43	[10, 50)	25	0.18	4500	4500
5.4	25	68	[10, 50)	7	0.18	1260	3960
			[50, +∞)	18	0.15	2700	

表 2-2 中:

5.1 日累积流量为 9TB，当日流量为 9TB，位于区间[0, 10），执行 200 元/TB0 价位的计费标准，合计费用 1800 元。

5.2 日累积流量为 18TB，当日流量为 9TB，其中 1TB 位于区间[0, 10），执行 200/TB 价位的计费标准，计 200 元；8TB 位于区间[10, 50)，执行 180/TB 价位的计费标准，计 1440 元；合计费用：1640 元。

5.3 日累积流量为 43TB，当日流量为 25TB，位于区间[10, 50)，执行 180 元/TB 的计费标准，合计费用 4500 元。

5.4 日累积流量为 68TB，当日流量为 25TB，其中 7TB 位于区间[10, 50)，执行 180/TB 价位的计费标准，计 1260 元；18TB 位于区间[50, +∞)，执行 150/TB 价位的计费标准，计 2700 元；合计费用：3960 元。

带宽计费

带宽标准资费

带宽阶梯	标准资费
(0M,100M]	0.67 元/Mbps
(100M,500M]	0.6 元/Mbps
(500M,5G]	0.53 元/Mbps
(5G,+∞)	0.49 元/Mbps
固定单价	0.67 元/Mbps

计费项：国内
计费方式：按日带宽峰值计费（阶梯计费模式）
计费周期：按日结算，定时扣费（每日 12:00 后出前一日账单并扣费，具体出账时间以系统为准）

示例

假设 5 月 1 日峰值带宽为 10Mbps，5 月 2 日峰值带宽为 10Gbps。

带宽计费示例

日期	峰值带宽	计价区间	标准资费 (元/Mbps)	金额
5 月 1 日	10Mbps	[0Mbps, 100Mbps)	0.67	6.7
5 月 2 日	10Gbps	(5G,+∞)	0.49	4900

- 5.1 日带宽峰值为 10Mbps，位于区间[0Mbps, 100Mbps)，执行 0.67 元/Mbps 价位的计费标准，合计费用 6.7 元，则日账单为 6.7 元。

- 5.2 日带宽峰值为 10Gbps，位于区间(5G,+∞)，执行 0.49 元/Mbps 价位的计算标准，合计费用 4900，则日账单为 4900 元。

请求数

2. 请求数标准资费

计费项	标准资费	说明
防护请求数	0.18 元/万次	开通 waf 防护功能，即有防护请求数的计费
静态 https 请求数	0.05 元/万次	如果使用 https 加速服务，即有 https 请求数的计费
动态请求数	0.15 元/万次	只订购了抗 D 服务功能，并开通了动态功能，会有动态请求数的计费

WAF 功能收费

WAF 防护	价格标准	价格
安全加速-WAF 基础防护	必选（包含 10 个域名、基础 WAF 防护功能）	2000 元/月
安全加速-WAF 防护请求数	按量收费，可购买套餐包	0.18 元/万次
安全加速-WAF 域名数量	按量收费，若基础防护不满足可购买	200 元/月/个

抗 D 功能收费

基础套餐

抗 D 防护	套餐内容	价格
安全加速-抗 D 服务套餐 1	域名：20 保底攻击峰值：10000QPS 防护带宽：1Gbps	1860 元/月
安全加速-抗 D 服务套餐 2	域名：20 保底攻击峰值：30000QPS 防护带宽：5Gbps	2860 元/月

安全加速-抗 D 服务套餐 3	域名：20 保底攻击峰值：50000QPS 防护带宽：10Gbps	4360 元/月
安全加速-抗 D 服务套餐 4	域名：50 保底攻击峰值：80000QPS 防护带宽：20Gbps	8360 元/月
安全加速-抗 D 服务套餐 5	域名：50 保底攻击峰值：120000QPS 防护带宽：30Gbps	13360 元/月
安全加速-抗 D 服务套餐 6	域名：50 保底攻击峰值：140000QPS 防护带宽：40Gbps	17660 元/月
安全加速-抗 D 服务套餐 7	域名：50 保底攻击峰值：160000QPS 防护带宽：50Gbps	20860 元/月
安全加速-抗 D 服务套餐 8	域名：50 保底攻击峰值：180000QPS 防护带宽：60Gbps	23860 元/月
安全加速-抗 D 服务套餐 9	域名：50 保底攻击峰值：200000QPS 防护带宽：70Gbps	25860 元/月
安全加速-抗 D 服务套餐 10	域名：50 保底攻击峰值：220000QPS 防护带宽：80Gbps	28860 元/月
安全加速-抗 D 服务套餐 11	域名：50 保底攻击峰值：240000QPS 防护带宽：90Gbps	31860 元/月
安全加速-抗 D 服务套餐 12	域名：50 保底攻击峰值：260000QPS 防护带宽：100Gbps	34860 元/月

安全加速-抗 D 服务套餐 13	域名：50 保底攻击峰值：260000QPS 防护带宽：100Gbps	136000 元/年
安全加速-抗 D 服务套餐 14	域名：50 保底攻击峰值：2000000QPS 防护带宽：300Gbps	216000 元/年
安全加速-抗 D 服务套餐 15	域名：50 保底攻击峰值：3000000QPS 防护带宽：400Gbps	396000 元/年
安全加速-抗 D 服务套餐 16	域名：50 保底攻击峰值：4000000QPS 防护带宽：500Gbps	1586000 元/年
安全加速-抗 D 服务套餐 17	域名：50 保底攻击峰值：5000000QPS 防护带宽：600Gbps	1896000 元/年
安全加速-抗 D 服务套餐 18	域名：50 保底攻击峰值：6000000QPS 防护带宽：800Gbps	2986600 元/年
安全加速-抗 D 服务套餐 19	域名：50 保底攻击峰值：8000000QPS 防护带宽：1000Gbps	3026600 元/年
安全加速-抗 D 服务套餐 20	域名：50 保底攻击峰值：10000000QPS 防护带宽：1500Gbps	4249600 元/年

域名扩展

安全加速-抗 D 服务域名数量	按量扩展	200 元/月

弹性防护

	(超出保底攻击峰值）Gbps	**（超出保底攻击量）QPS**	**标准价格（元/天）**
安全加速-弹性防护	(0,10]	(0,40000]	860
	(10,20]	(40000,80000]	1760
	(20,30]	(80000,120000]	2660
	(30,40]	(120000,160000]	3260

	(40,50]	(160000,200000]	4060
	(50,60]	(200000,240000]	4960
	(60,70]	(240000,280000]	5760
	(70,80]	(280000,320000]	6560
	(80,100]	(320000,400000]	8160
	(100,150]	(400000,600000]	15060
	(150,200]	(600000,800000]	20160
	(200,500]	(800000,2000000]	66660
	(500,+∞]	(2000000,9999999]	98860

资源包

流量包标准资费

规格	套餐列表价
100GB	17（元/G）
500GB	85（元/G）
1TB	170（元/G）
5TB	850（元/G）
10TB	1700（元/G）
50TB	7650（元/G）
200TB	25500（元/G）
1PB	127500（元/G）

防护请求数包标准资费

规格	套餐列表价

100 万次	16 元
1000 万次	154 元
1 亿次	1530 元
10 亿次	15300 元
100 亿次	153000 元

静态 https 请求数包标准资费

规格	套餐列表价
1000 万次	40 元
1 亿次	360 元
10 亿次	3200 元
100 亿次	28000 元
1000 亿次	200000 元

资源包购买须知：

1、订购安全加速产品后，可支持订购安全加速的资源包，并根据所开功能对资源包进行抵扣。

使用条件：

1）计费方式为“流量“：开通安全加速和 WAF 防护的用户，可抵扣“安全加速流量包“、“防护请求数包”和”静态 https 请求数包“；开通安全加速和抗 D 服务的用户，可抵扣”安全加速流量包“和“静态 https 请求数包”。

2）计费方式为“日带宽“：开通安全加速和 WAF 防护的用户，可抵扣“防护请求数包”和“静态 https 请求数包”；开通安全加速和抗 D 服务的用户，可抵扣“静态 https 请求数包”；计费方式为“日带宽”不能抵扣流量包，需要变更计费方式为“流量”。

2、资源包可叠加购买，购买多个相同类型的资源包，抵扣顺序依据资源包的到期时间先后排序，有效期不叠加计算。

3、资源包不支持退订，资源包订购成功后，不支持退订退款；资源包到期后，未用完的资源自动清零，不支持结转。

4、资源包的有效期为自购买成功后一年内有效；“任一资源包用尽”或“有效期结束”，将自动转按量计费。

5、资源包中的"安全加速流量包"是供边缘节点上行和下行总流量使用；"日带宽"计费客户，如需使用"安全加速流量包"，需将计费方式变更为"流量"。

注意事项：

- 带宽利用率 = 实际使用流量 GB/（带宽峰值 Mbps x 10.54）。1Mbps 带宽每日 100%利用率产生的流量约为 10.54GB。
- CDN 计费的流量比日志中记录的流量多。因为 CDN 日志中记录的流量数据是应用层日志统计出的流量，但是实际网络请求中存在 TCP/IP 包头的消耗 和 TCP 重传消耗要比应用层统计到的流量高出 7%~15%，因此按照业界标准，应用于账单的计费数据会在控制台监控数据的基础上上浮 10%。
- 如果您的 CDN 月消费金额大于 10 万元，天翼云 CDN 可提供更灵活优惠的按月计费方式。您可以提交工单或拨打 400 电话联系客服。

2.2 购买

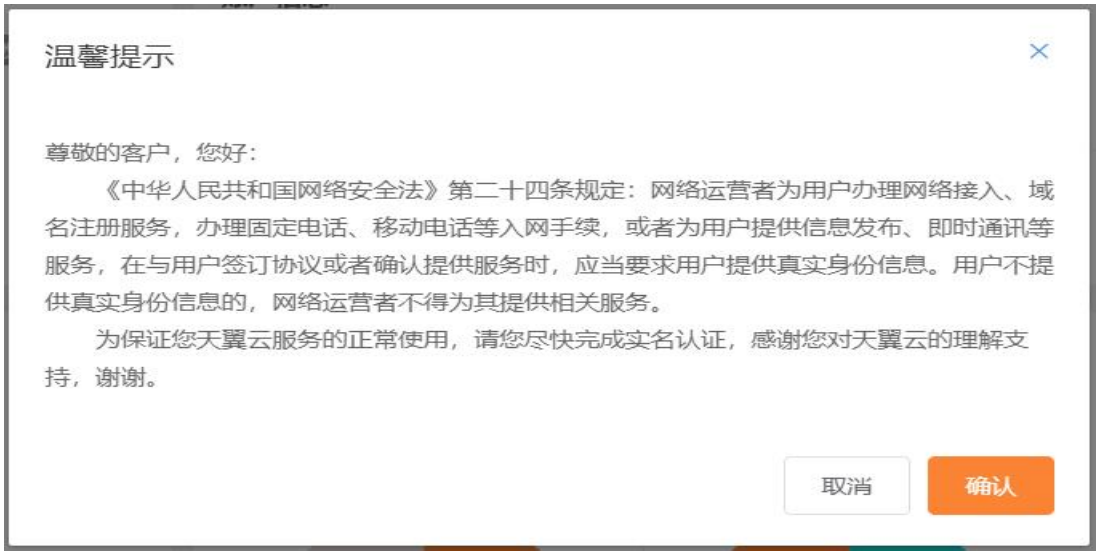
开通天翼云安全加速服务，需首先注册天翼云账户。
开通步骤如下：

1.注册并登录天翼云 http://www.ctyun.cn

2-1 天翼云官网登录页面

2.未实名认证的用户请按提示完成实名认证才能开通安全加速服务

2-2 实名认证提醒



2-3 完成实名认证

3.实名认证后进入安全加速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

5.在购买页面选择适合的功能和计费方式，勾选并阅读服务协议，确认无误后点击“立即开通”，安全加速服务即开通；

6.安全加速服务开通后，便可以根据操作手册去控制台开始接入您要加速的域名。

2.3 变更

您如果有变更计费的需求，您可以联系客户经理或天翼云客服，提供您的变更需求。

2.4 续费

续费步骤如下。

1.在天翼云官网，点击用户菜单下的“基本信息“；

2-6 登录页

2.进入“总览”页面，选择“账户充值”；

2-7 充值页面

3.进入现金充值页面，在充值金额中输入充值金额，点击“充值”；

2-8 输入金额页面

4.进入超级收银台页面，选择合适的支付方式完成付款；

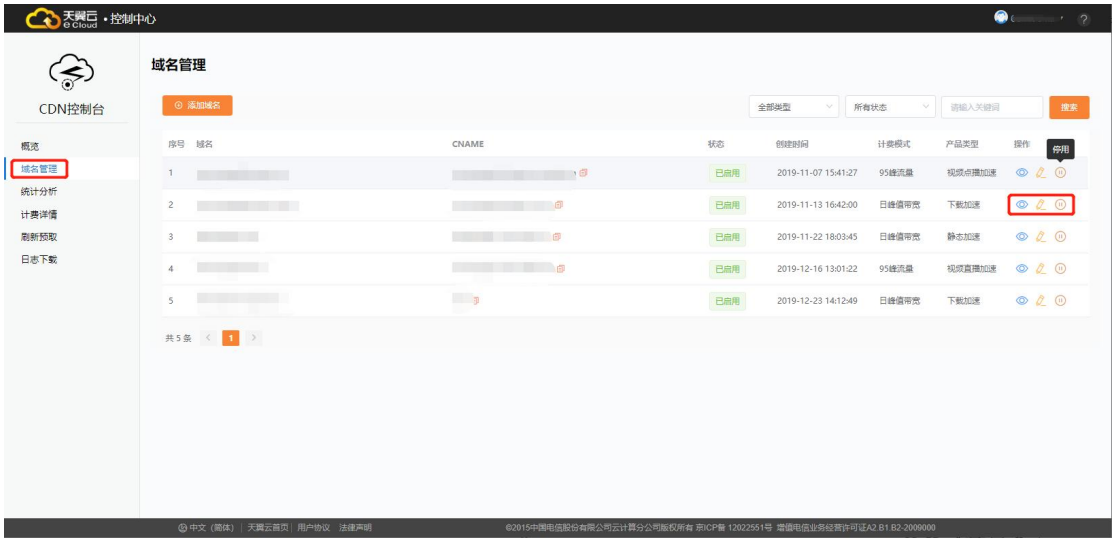
2-9 付款方式页

2.5 关停服务

客户在客户天翼云账户中没有费用并欠款的情况下，通知客户充值，并将关停客户的 CDN 安全加速服务。

客户也可以根据需求，进入客户控制台（http://cdn.ctyun.cn/）的“域名管理”页面，操作域名“停用”以及“启用”等操作。

2-10 域名管理页面



2.6 增值/定制内容申请

如果您有增值/定制的需求，您可以联系客户经理或天翼云客服，提交您的需求。

也可以进入官网以工单的形式提交您的需求。

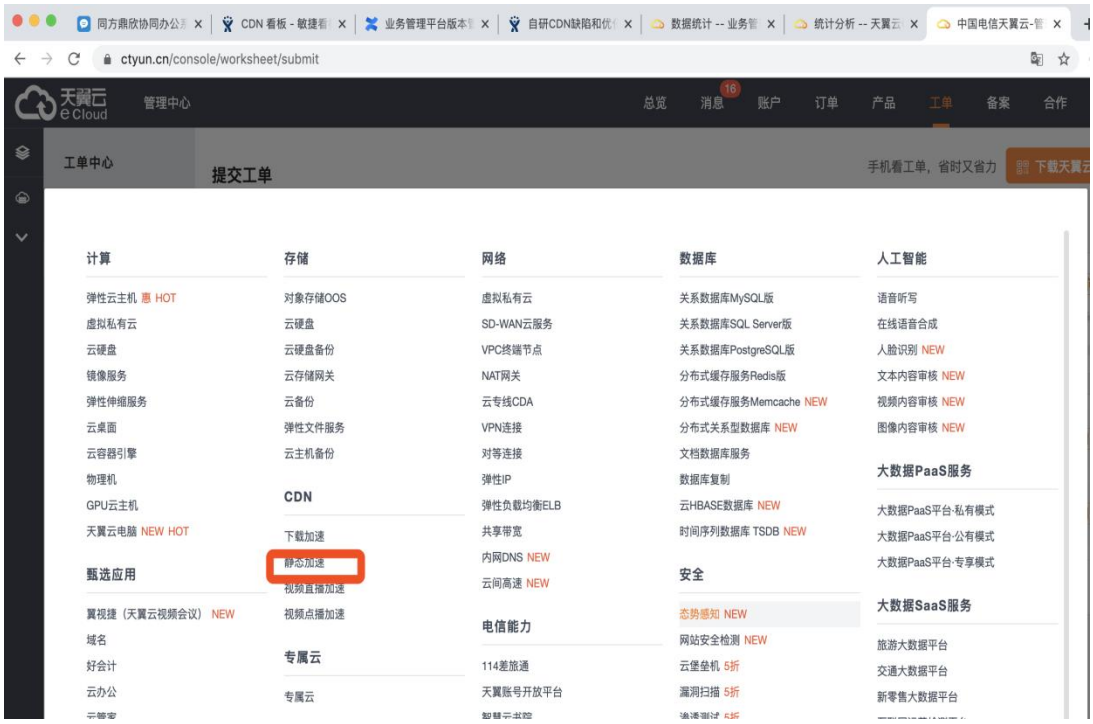
工单提交流程：

1. 登陆天翼云官网，点击用户菜单下的“工单管理“；

2-11 工单管理页面

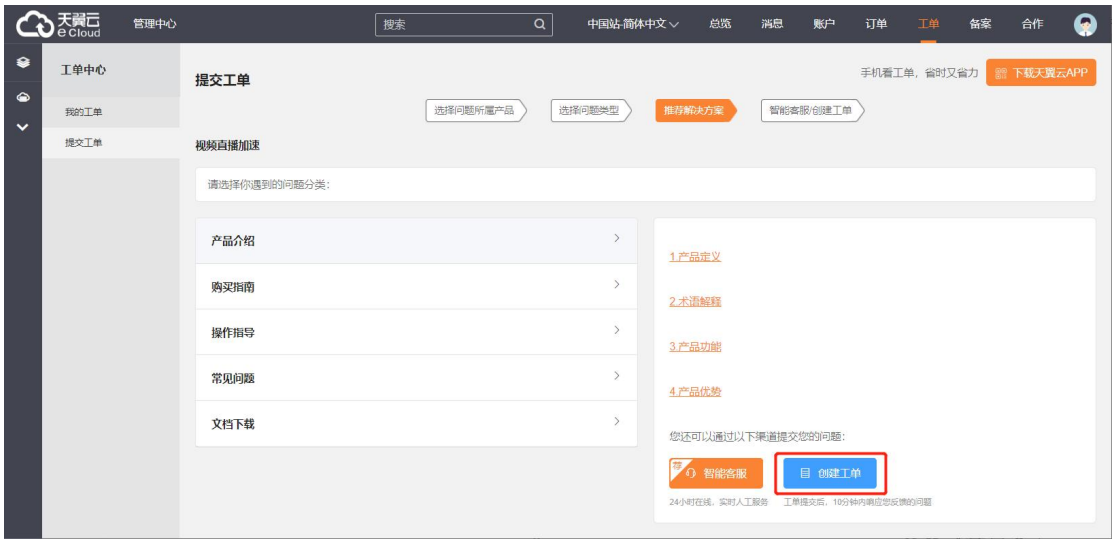
2. 进入“提交工单”页面，在安全加速业务处点击“提问”；

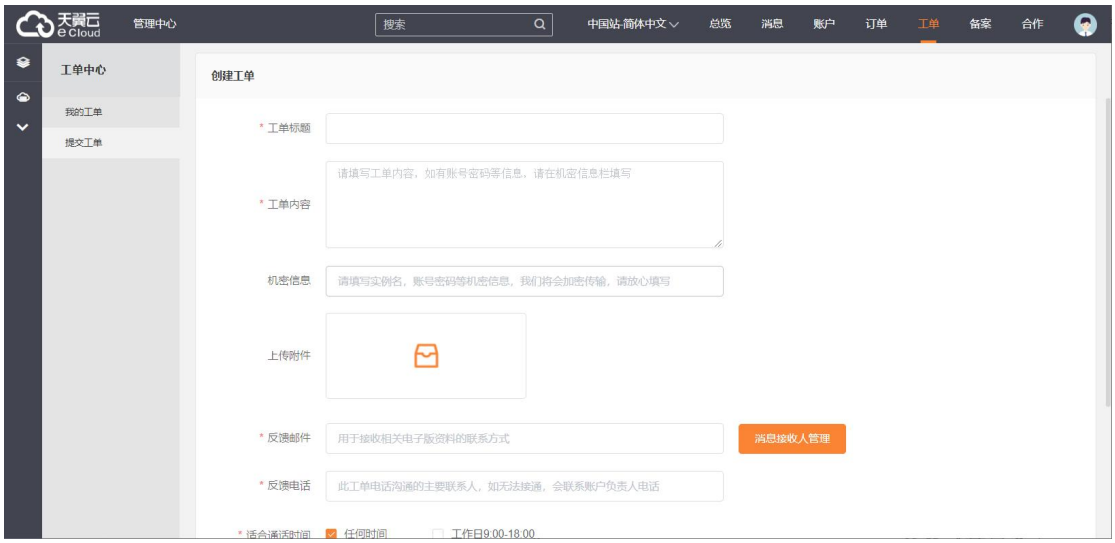
2-12 提交工单页面



3. 根据您的需求，选择“问题分类”，或“创建工单”

2-13 问题分类和创建工单页面





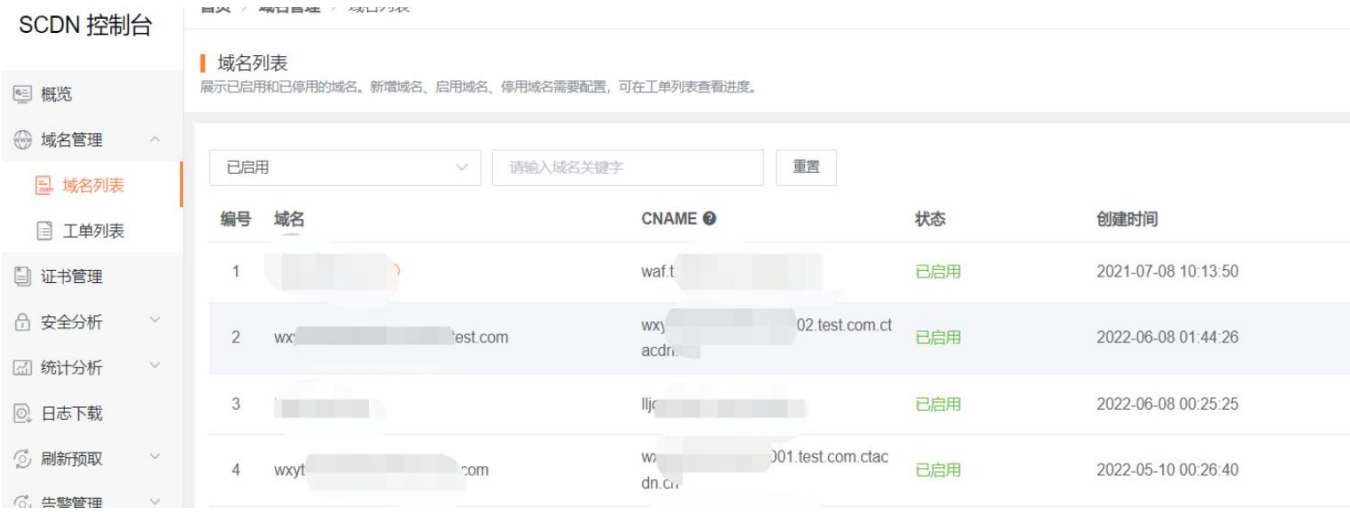
3.操作指导

3.1 加速配置

操作步骤

1.进入 SCDN 控制台

2.点击域名列表，可直接编辑加速配置，进入加速配置页面



3.可支持回源配置、HTTPS 配置、缓存配置、访问控制，配置完成后统一点击提交保存

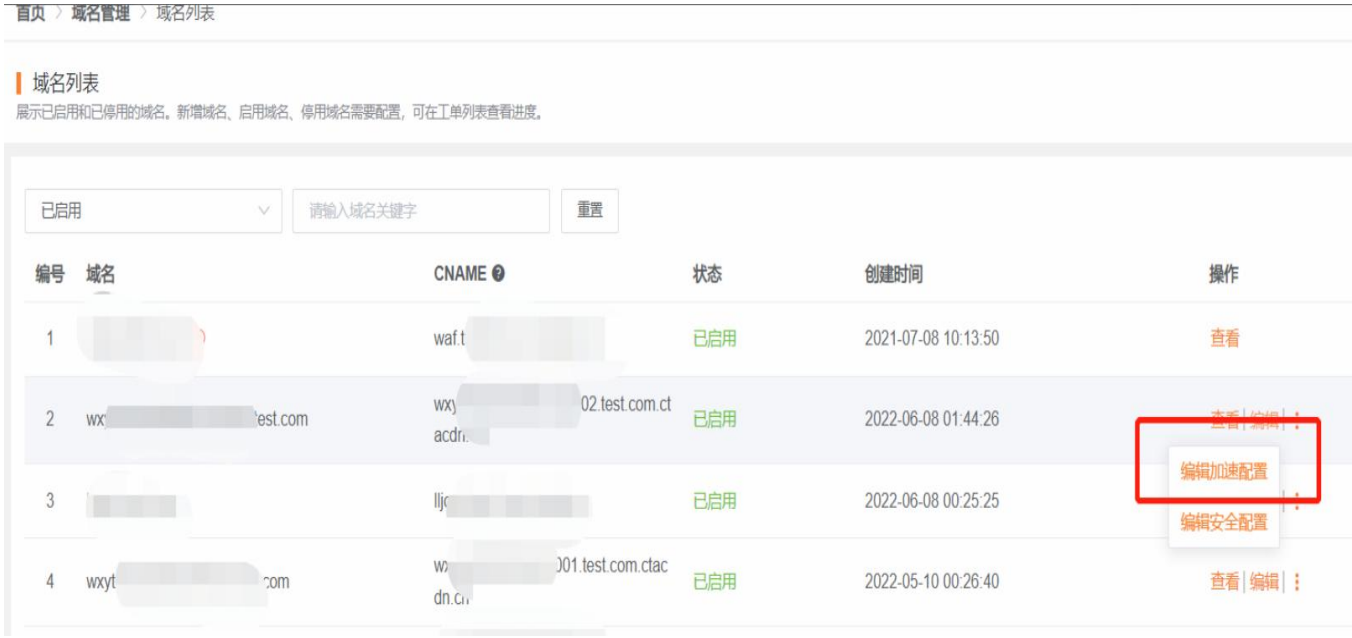
4.可通过工单列表进行查看配置进度

3.2 WAF 防护配置

操作步骤

1.进入 SCDN 控制台

2.点击域名列表，可直接编辑安全配置，进入安全配置页面



3.保证 WAF 防护已开启（需购买对应功能）

4.WAF 支持基础配置、高级防护、账户安全防护、访问控制、访问限速、合规检测、域名规则

图 安全防护配置页---基础配置

图 高级防护页


SCDN 控制台
概览
域名管理
域名列表
工单列表
证书管理
安全分析
统计分析
日志下载
刷新预取
计费详情
告警管理
态势感知大屏(限免)
首页 > 域名管理 > 域名列表 > 域名编辑
• 已启用
能力选项
基础配置
高级防护
账户安全防护
访问控制(安全)
合规检测
域名规则
BOT防护
抗D服务
CSRF防护
Cookie防护
数据脱敏防护
广告防护
CSRF防护模式:
关闭
拦截
告警

图 账户安全防护配置页


SCDN 控制台
概览
域名管理
域名列表
工单列表
证书管理
安全分析
统计分析
日志下载
刷新预取
计费详情
告警管理
态势感知大屏(限免)
首页 > 域名管理 > 域名列表 > 域名编辑
nle5.com • 已启用
能力选项
基础配置
高级防护
账户安全防护
访问控制(安全)
合规检测
域名规则
BOT防护
抗D服务
撞库防护
批量注册防护
暴力破解防护
关闭
开启
序号
域名

图 访问控制配置页


SCDN 控制台
概览
域名管理
域名列表
工单列表
证书管理
安全分析
统计分析
日志下载
刷新预取
计费详情
告警管理
态势感知大屏(限免)
首页 > 域名管理 > 域名列表 > 域名编辑
om • 已启用
能力选项
基础配置
高级防护
账户安全防护
访问控制(安全)
合规检测
域名规则
BOT防护
抗D服务
访问控制
频率控制
关闭
开启
控制ID
优先级

图 合规检测配置页


SCDN 控制台
概览
域名管理
域名列表
工单列表
证书管理
安全分析
统计分析
日志下载
刷新预取
计费详情
告警管理
态势感知大屏(限免)
首页 > 域名管理 > 域名列表 > 域名编辑
• 已启用
能力选项
基础配置
高级防护
账户安全防护
访问控制(安全)
合规检测
域名规则
BOT防护
抗D服务
合规检测
合规检测:
关闭
开启
序号
规则名称
1
all

图 域名规则配置页

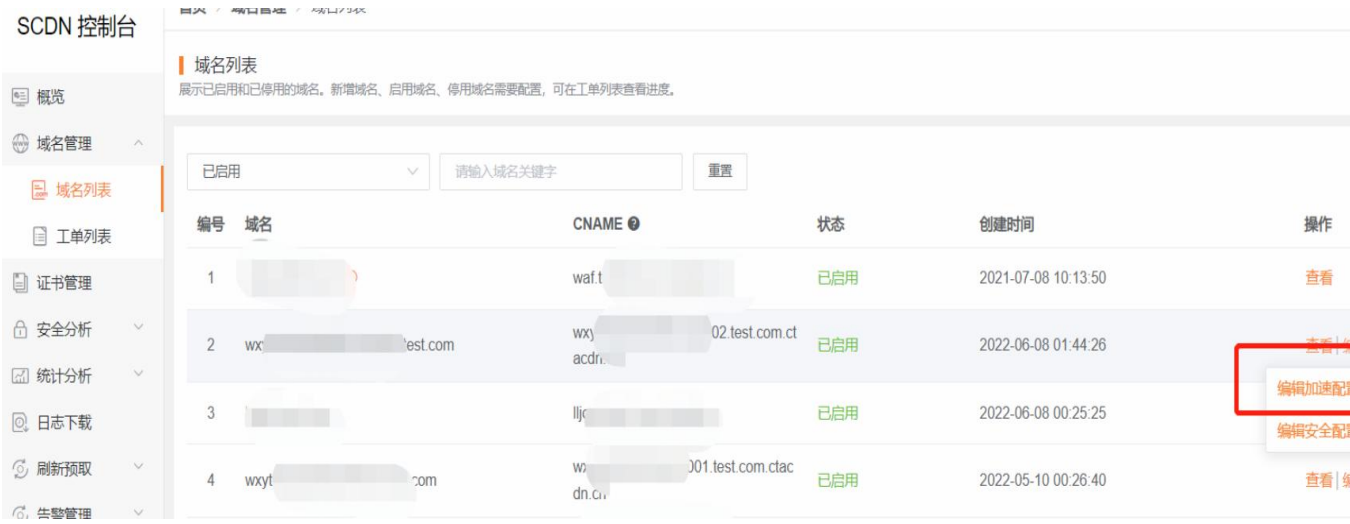
5.配置完成后可通过工单列表进行查看对应配置进度

3.3 抗 D 防护

操作步骤

1.进入 SCDN 控制台

2.点击域名列表，可直接编辑安全配置，进入安全配置页面



3.保证抗 D 防护已开启（需购买对应功能）

4.抗 D 支持 DDoS 防护、CC 防护功能配置

5.配置完成后可通过工单列表进行查看对应配置进度

3.4 证书管理

客户控制台的【证书管理】模块，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。

证书管理页

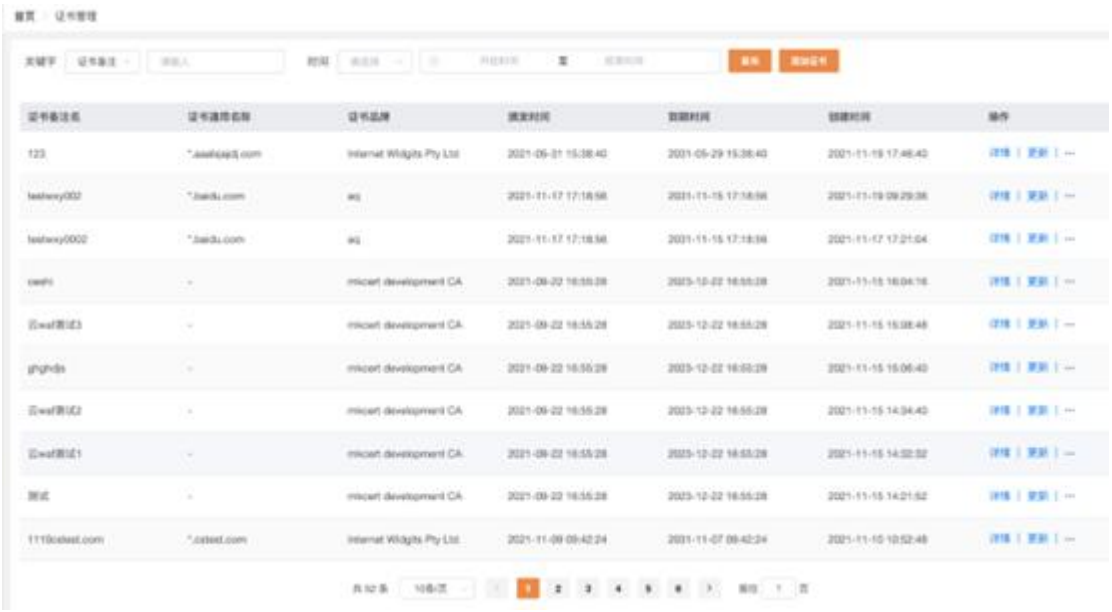


图 证书新增页

3.5 **统计分析**

简介

可通过筛选项进行组合查询，筛选项包括域名、业务类型、覆盖范围和时间等，其中必选项为域名和时间。

时间选择跨度最长不能超过 31 天。

安全分析

1.在天翼云 SCDN 客户控制台的【安全分析】页面，客户可以查看 waf、CC 攻击日志和 waf 报表分析、CC 报表分析情况。

2.界面中展示的是您所选域名、时间的攻击日志情况。

图 安全分析 waf 攻击日志

图 安全分析 CC 攻击日志

图 WAF 报表分析

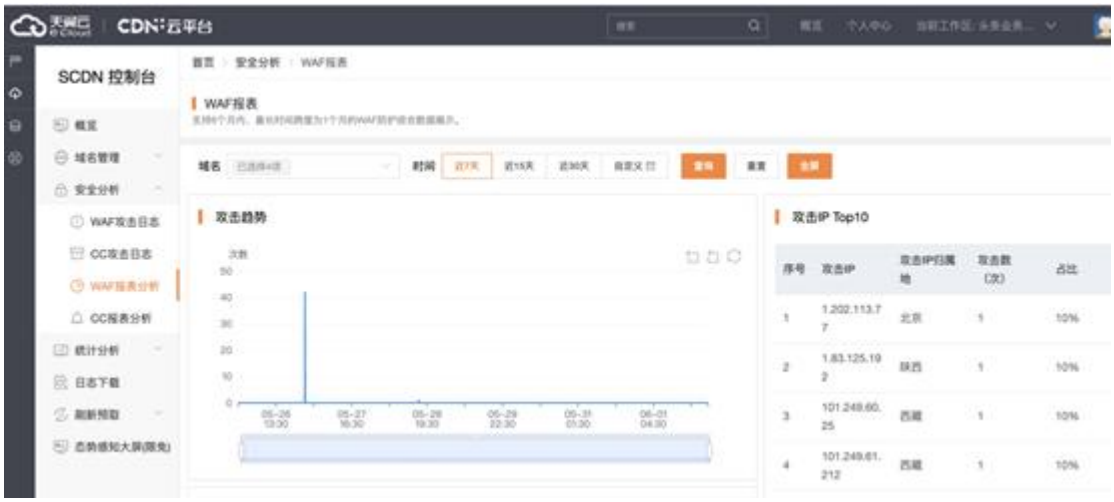


图 CC 报表分析

业务数据统计分析

1.带宽流量统计

1）在天翼云 SCDN 客户控制台的【统计分析-用量查询】页面，客户可以查看业务的使用情况。

2）界面中展示了所选择域名、时间的流量和带宽统计图表，包括总流量和平均流量信息；带宽峰值和 95 带宽峰值。

图 统计分析流量带宽

图 回源统计

3.在天翼云 SCDN 客户控制台的【统计分析-用量查询】页面，客户可以查看业务的回源情况。

4.界面中展示了所选择域名、时间的回源流量和回源带宽统计图。

图 统计分析回源流量带宽

图 请求数统计

5.在天翼云 SCDN 客户控制台的【统计分析-请求数】页面，客户可以查看其在使用 CDN。

6.界面中展示了所选择域名的总请求数、请求数峰值、请求数谷值等信息。

7.请求数统计包括：防护请求数、静态 https 请求数、动态请求数等。

图 请求数统计

命中率统计

1.在天翼云 SCDN 客户控制台的【统计分析-用量查询-命中率】页面，客户可以查看其在使用安全加速过程中，请求数及流量的命中情况，可以快速了解所选择时间段的整体命中情况。

2.界面中展示了请求数、流量的命中饼图和趋势图。

图 命中率统计

状态码统计

1.在天翼云 SCDN 客户控制台的【统计分析-用量查询-状态码】页面，客户可以查看其在使用安全加速过程中，不同状态码在不同时间点的趋势曲线图，很直观的展示了状态码的变化情况。

2.界面中展示了状态码总量、各状态码趋势图、次数和占比等信息。

图 状态码统计

3.6 安全分析

在天翼云 SCDN 客户控制台的【安全分析】页面，客户可以查看 waf、CC 攻击日志和 waf 报表分析、CC 报表分析情况；

界面中展示的是您所选域名、时间的攻击日志情况；

图 安全分析 waf 攻击日志

图 安全分析 CC 攻击日志


SCDN 控制台
概览
域名管理
证书管理
安全分析
WAF攻击日志
CC攻击日志
WAF报表分析
CC报表分析
抗D报表
网络层攻击事件
首页 > 安全分析 > 网络层攻击事件
网络层攻击事件
支持六个月内、最长时间跨度为一个月的网络层攻击事件查看。
攻击时间
近7天
近15天
近30天
自定义
查询
重置
序号
攻击开始时间
攻击结束时间
攻击状态
SCDN 控制台
概览
域名管理
证书管理
安全分析
WAF攻击日志
CC攻击日志
WAF报表分析
CC报表分析
首页 > 安全分析 > CC攻击日志
CC攻击日志
支持六个月内、最长时间跨度为一个月的CC攻击日志查看。
域名
已选择70项
攻击时间
近7天
近15天
序号
被攻击域名
起始攻击时间
攻击时间

图 WAF 报表分析


SCDN 控制台
概览
域名管理
证书管理
安全分析
WAF攻击日志
CC攻击日志
WAF报表分析
CC报表分析
抗D报表
网络层攻击事件
统计分析
日志下载
刷新预取
计费详情
告警管理
首页 > 安全分析 > WAF报表
WAF报表
支持6个月内、最长时间跨度为1个月的WAF防护综合数据展示。
选择域名
已选择70项
时间
近7天
近15天
近30天
请求数（次）
攻击趋势

图 CC 报表分析


SCDN 控制台
概览
域名管理
证书管理
安全分析
WAF攻击日志
CC攻击日志
WAF报表分析
CC报表分析
抗D报表
网络层攻击事件
统计分析
日志下载
刷新预取
计费详情
首页 > 安全分析 > cc报表
CC报表
支持6个月内、最长时间跨度为1个月的CC流量清洗综合数据展示。
域名
已选择70项
时间
近7天
近15天
近30天
CC攻击流量变化
攻击IP TOP10

图 抗 D 报表分析

图 网络层攻击事件

3.7 计费详情

CDN 部分计费按照 1000 进制从 Byte 换算到 Gbps。

套餐详情管理

安全加速的计费方式、WAF 防护的套餐与计费、抗 D 服务的套餐与计费。

图 计费详情

资源包管理

- 资源包购买成功后次日 00:00 时生效，自动抵扣所覆盖产品产生的数据，有效期为一年；
- 资源包购买后不支持退款，到期后未用完的资源将清零，不支持转移到其他资源包；
- 购买多个资源包时，当某个资源包用尽后默认自动开启下一个临近到期的相同类别的资源包；
- 当资源包用尽或者过期后，默认转为按需计费。

1.订购安全加速产品后，可支持订购安全加速的资源包，并根据所开功能对资源包进行抵扣。

使用条件：

1）计费方式为“流量“：开通安全加速和 WAF 防护的用户，可抵扣“安全加速流量包“、“防护请求数包”和”静态 https 请求数包“；开通安全加速和抗 D 服务的用户，可抵扣”安全加速流量包“和“静态 https 请求数包”。

2）计费方式为“日带宽“：开通安全加速和 WAF 防护的用户，可抵扣“防护请求数包”和“静态 https 请求数包”；开通安全加速和抗 D 服务的用户，可抵扣“静态 https 请求数包”；计费方式为“日带宽”不能抵扣流量包，需要变更计费方式为“流量”。

2.资源包可叠加购买，购买多个相同类型的资源包，抵扣顺序依据资源包的到期时间先后排序，有效期不叠加计算。

3.资源包不支持退订，资源包订购成功后，不支持退订退款；资源包到期后，未用完的资源自动清零，不支持结转。

4.资源包的有效期为自购买成功后一年内有效；“任一资源包用尽”或“有效期结束”，将自动转按量计费。

5.资源包中的”安全加速流量包“是供边缘节点上行和下行总流量使用；“日带宽”计费客户，如需使用“安全加速流量包”，需将计费方式变更为“流量”。可叠加购买：购买多个相同类型的资源包，抵扣顺序依据资源包的到期时间先后排序，有效期不叠加计算。

不支持退订：资源包订购成功后，不支持退订退款；资源包到期后，未用完的资源自动清零，不支持结转。

有效期：自购买成功后一年内有效；“任一资源包用尽”或“有效期结束”，将自动转按量计费。

图 资源包管理

3.8 刷新预取

CDN 提供资源的刷新和预取功能。通过刷新功能，您可以强制 CDN 节点回源并获取最新文件；通过预取功能您可以在业务高峰期预取热门资源，提高资源访问效率。

刷新

刷新功能是指提交 URL 刷新或目录刷新请求后，CDN 节点的缓存内容将会被强制过期，当您向 CDN 节点请求资源时，CDN 会直接回源站获取对应的资源返回给您，并将其缓存。刷新功能会降低缓存命中率。

图 刷新

预取

预取功能是指提交 URL 预取请求后，源站将会主动将对应的资源缓存到 CDN 节点，当您首次请求时，就能直接从 CDN 节点缓存中获取到最新的请求资源，无需再回源站获取。预取功能会提高缓存命中率。

图 预取

任务查看

在天翼云 CDN 客户控制台的【刷新预取】页面，点击【查看任务】，可以分别看到您已提交的 URL 刷新、目录刷新和 URL 预取任务的执行情况；

图 查看任务

注：大批量的缓存推送可能会引发高并发回源，如果源站出口带宽较小，建议分多次小批量操作。

3.9 日志下载

日志文件延迟时间：一般情况下延迟在 24 小时之内，但是也有可能超过 24 小时；

日志每隔一小时生成一次。具体分割成的文件数量根据该小时生成的日志量动态调整；

您可以下载最近 15 天的日志数据；

日志命名规则：log_加速域名_年月日时_开始时间_结束时间，例如：

log_www.test.ctyun.cn_2020010101_0000-5959.gz

图 日志下载

3.10 告警管理

图 告警配置页面


新增告警配置
* 开关
开启
关闭
* 告警名称
请输入告警名称
* 域名
请选择域名
* 攻击类型
请选择
* 统计周期
0
时
0
分
* 告警邮件发送频率周期
1
分钟
* 告警阈值
攻击数大于
1
次
勿扰时间
开始时间
至
结束时间
* 告警邮箱
支持输入多个邮箱，多个以;分隔

图 告警记录查询页面

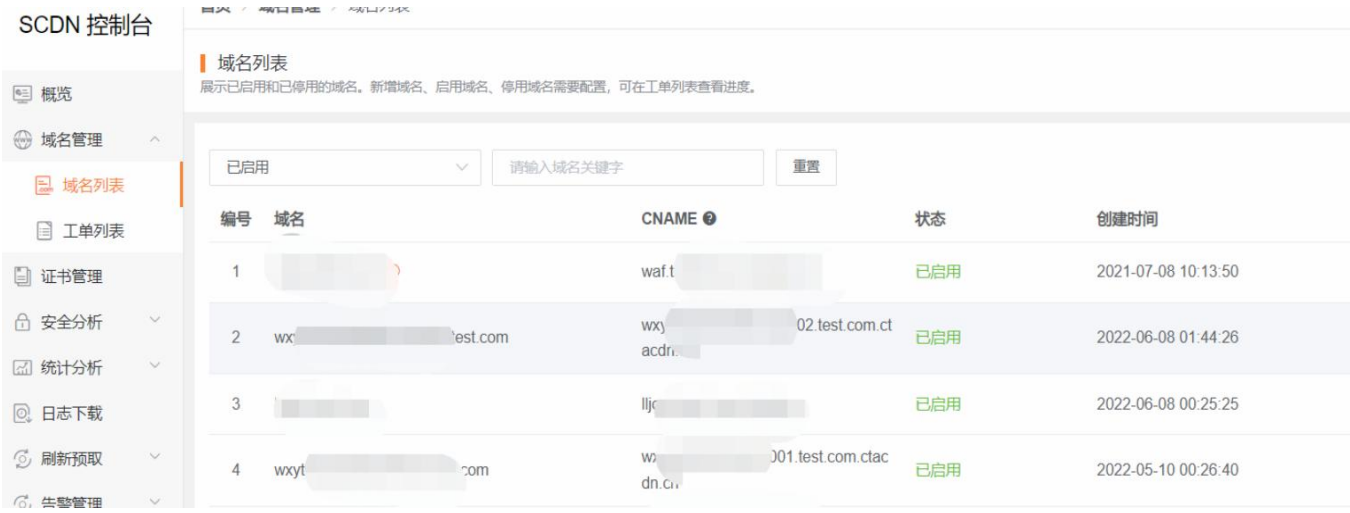

SCDN 控制台
概览
域名管理
证书管理
安全分析
统计分析
日志下载
刷新预取
告警管理
WAF告警
WAF告警
告警配置
告警列表
选择域名
已选择1项
状态
请选择状态
类型
请选择类型
时间
查询
重置
导出
域名
攻击数
状态
类型
告警邮箱
暂无数据
共 0 条
10条/页
1
前往
1
页

4.快速入门

购买安全加速服务

1.进入 SCDN 控制台

2.点击域名列表，可直接编辑加速配置，进入加速配置页面



3.可支持回源配置、HTTPS 配置、缓存配置、访问控制，配置完成后统一点击提交保存

4.可通过工单列表进行查看配置进度

进入客户控制台

1.打开天翼云官网 http://www.ctyun.cn，注册并登录；

2.选择控制台；

3.下拉选择 CDN 产品，点击对应的加速服务进入安全客户控制台；

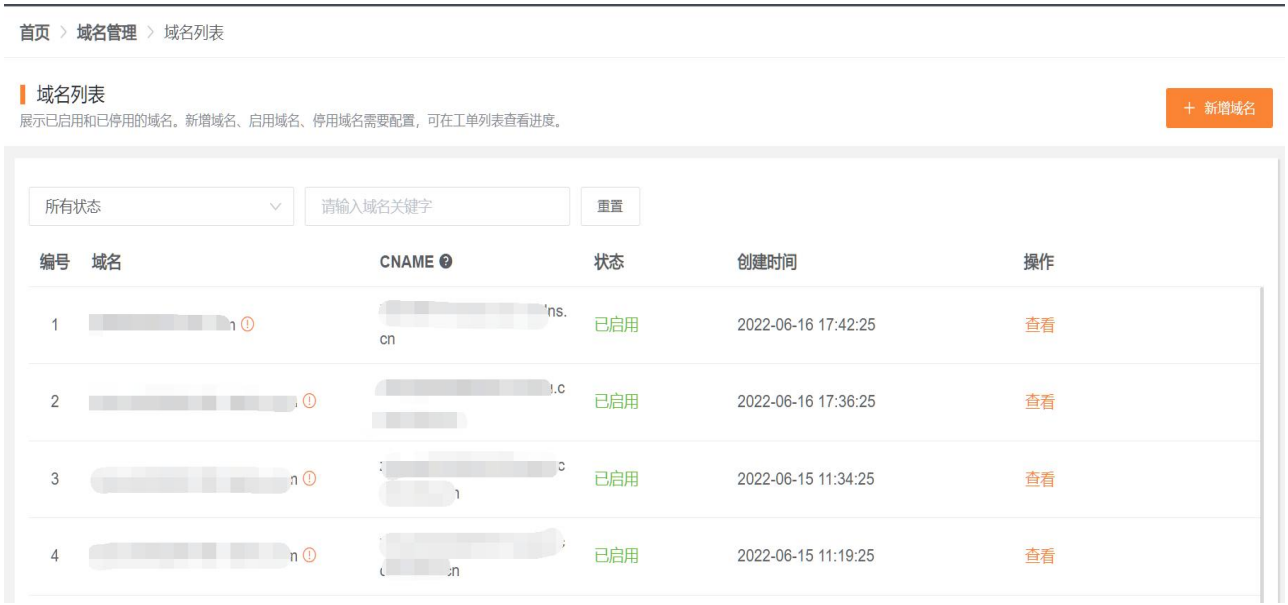
图 控制中心安全加速页面

添加域名配置

1.进入 SCDN 客户控制台，选择【域名管理】，这个页面您可以查看已添加的域名的信息，包括加速域名、CNAME、域名状态、创建时间、和产品类型等信息。

2.点击右上角【添加域名】；

图 域名管理页面



3.填写加速域名信息，并选择产品类型【安全加速】；

图 添加安全加速域名页

4.根据您的需求，选择您加速域名的【源站设置】、【缓存设置】、【访问控制】功能，并填写您的安全加速域名加速部分的相关配置；

图 域名配置信息页

可以选择填写需要配置的源站信息、HTTPS 证书访问、缓存以及访问控制等配置；

5.完成域名加速部分的填写后，需要配置安全配置。

图 安全配置页面

可根据需求进行配置 WAF、CC 防护，先开启开关后进行对应的相关配置

6.域名配置填写和确认无误后，点击【新增域名】按钮提交您的加速域名配置；

图【提交成功】页

7.完成新增域名操作后，可通过【工单列表】或直接点击查看进度，查看该域名配置过程中所处状态；后台人员审核并执行相关配置，配置最久需要 3 个工作日；

图 工单列表页

图 工单展示页

8.完成新增域名操作后，即域名状态为已完成，可通过【域名列表】查看该域名配置详情；

域名归属权限验证指南

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

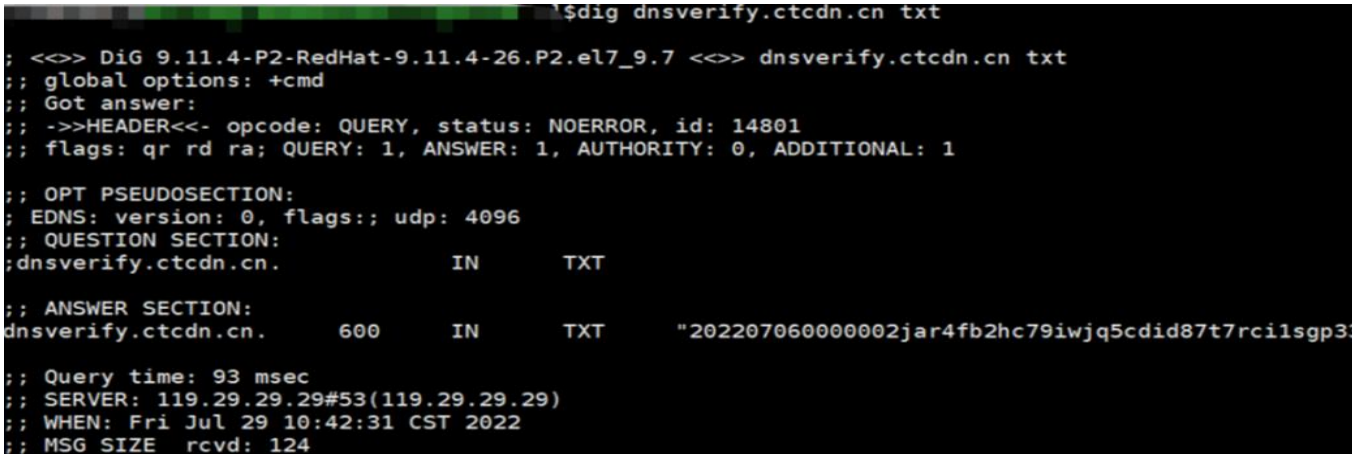
示例为 ctcdn.cn 的解析配置

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



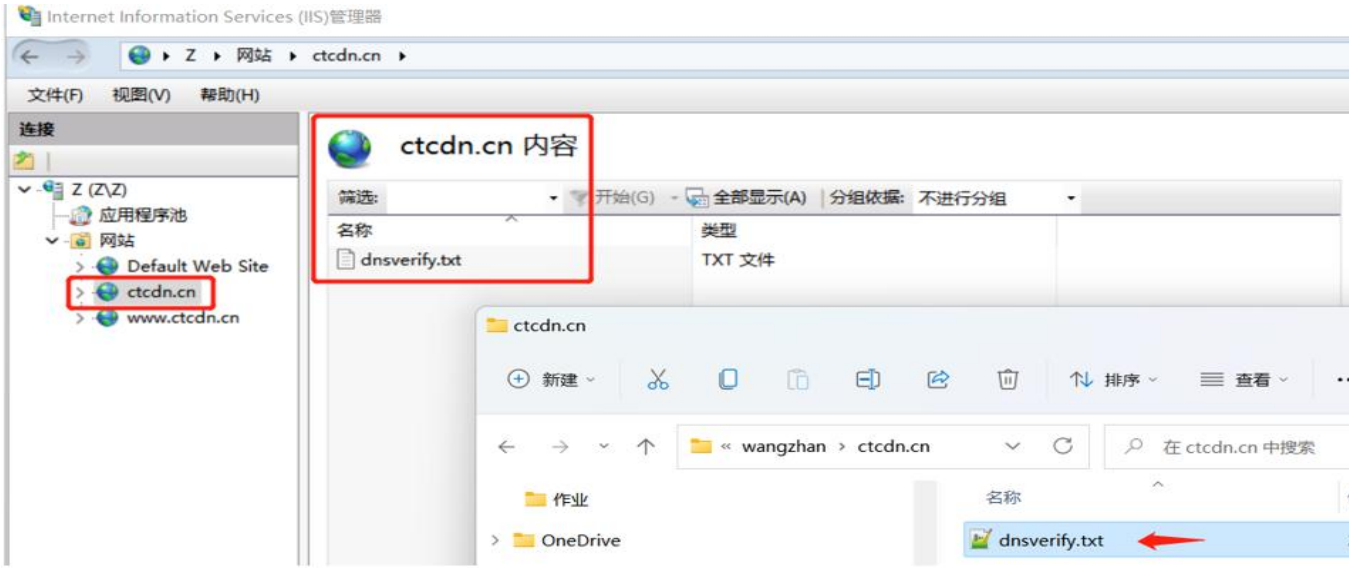
3、如解析出来的 txt 值和天翼云控制台返回的 TXT 记录值一致，则表示配置正确。

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

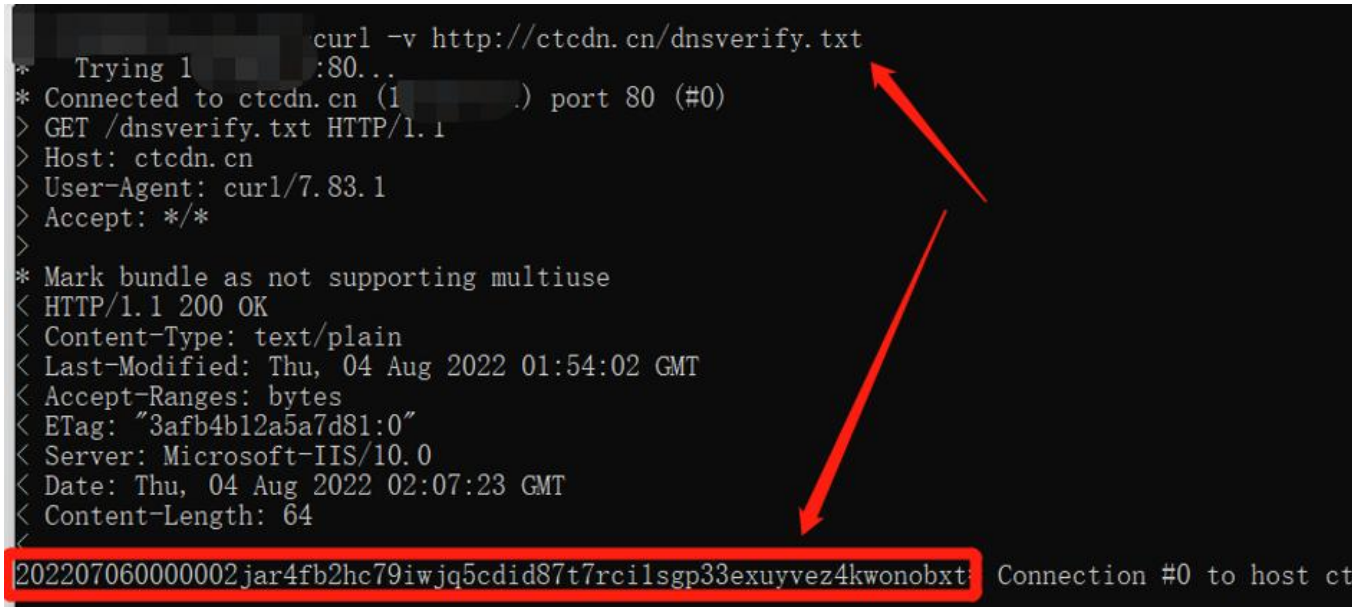
1、在您的源站根目录下，创建文件名为：dnsverify.txt 的文件，文件内容为天翼云控制台返回的 TXT 记录值（如下记录值仅为示例）



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。

配置 CNAME

要启用 CDN 安全加速服务，需要您将加速域名的 DNS 解析指向我们提供的 CNAME，这样访问加速域名的请求才能转发到 CDN 节点上，达到加速效果。

1.在控制台【域名管理】的域名列表中复制加速域名对应的 CNAME；

图 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】；

图 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。

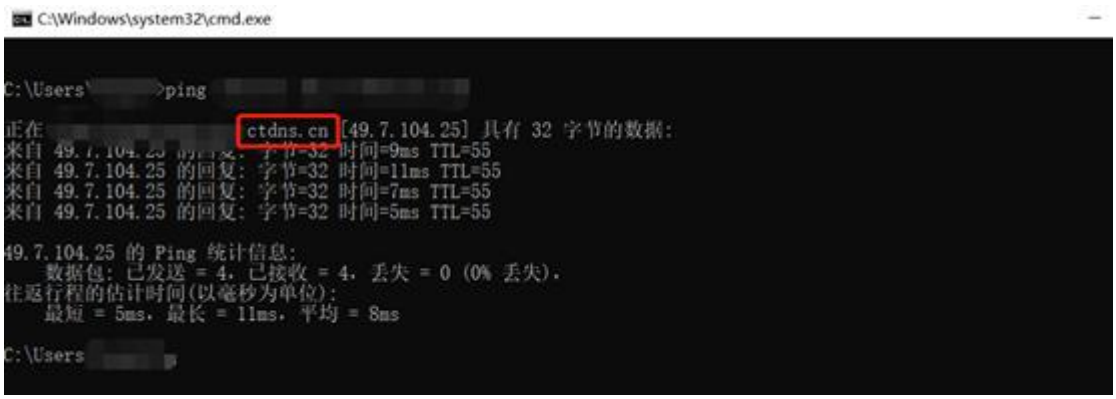
5.确认填写信息无误后，单击【提交】；

6.验证 CDN 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，CDN 功能也已生效。

图 检查域名指向页



注意:

1.配置 CNAME 完毕，CNAME 配置生效后，安全加速服务生效

2.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;

3.添加时如遇添加冲突，可考虑换一个加速域名，或参考以下“解析记录互斥规则” 调整记录;

3-13 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)

1.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；

2.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；

3.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。

5.常见问题

5.1 计费类

Q1

停用安全加速服务后，为什么仍有一部分费用产生?

A1

造成该情况的原因主要有以下两种:

1. 在停用安全加速服务后，若客户 LocalDNS 服务器中缓存未过期，LocalDNS 会继续把访问已停用安全加速域名的请求解析到加速节点，造成少量安全加速流量计费。
2. 一些下载类软件也存在 LocalDNS 缓存，在这部分缓存过期前，下载类软件也会把访问已停用安全加速域名的请求解析到加速节点上，造成少量安全加速流量计费。

Q2

安全加速中基础带宽方式中日流量计费和日带宽峰值计费是否支持互相变更计费方式?

A2

此两种计费方式之间可以自由切换，新的计费方式将在下一个计费周期生效。需需要注意的是，一个计费周期内，仅能变更一次。

Q3

安全加速的收费项都有哪些?

A3

安全加速主要有两个功能项：waf 防护功能和抗 D 功能，每个功能项下面会有不同的计费项
当用户开通了 waf 防护功能时:
计费项包括：waf 防护包+上行+下行总带宽的日峰值带宽/流量+防护请求数+静态 https 请求数，按日扣费
当用户开通了抗 D 功能时:
计费项包括：抗 D 套餐包+弹性带宽阶梯+上行+下行总带宽的日峰值带宽/流量+静态 https 请求数+动态请求数
当用户同时开通 waf 防护功能和抗 D 功能时:
计费项包括：waf 防护包+上行+下行总带宽的日峰值带宽+防护请求数+抗 D 套餐包+弹性带宽阶梯+静态 https 请求数

Q4

安全加速，但是没有开启 https 的功能，是否需要收费

A4

使用安全加速，但是没有使用 https 的功能，是不会针对 https 的请求数去收取费用的。

5.2 开通类

Q1

怎么样开通安全加速服务和使用?

A2

安全加速服务的开通首先需要注册天翼云官网的账号,通过产品栏目找到安全加速,选择相应的功能，点击开通；开通后会跳转到 SCDN 控制台，在控制台上配置安全加速的域名，配置成功后天翼云安全加速会提供域名对应的 cname，客户切入 cname 后，开始使用天翼云的安全加速服务。

Q2

欠费后安全加速服务会被关停吗?

A2

账户余额不足以支付服务费用将导致欠费，发生欠费后，安全加速服务的域名将被关停。

Q3

关停安全加速服务后怎样重新开启服务?

A3

客户补足欠款后，客户的天翼云账号恢复使用，被停止的域名需要客户到控制台域名管理模块，点击启用域名，开启被停用的域名，当域名状态变更为已启用后，支持客户随时切换到安全加速平台。

Q4

安全加速配置完成后大概多久生效?

A4

安全加速配置完成后一般 120 分钟内生效，若 120 分钟后仍未生效，请提交工单处理。

Q5

接入安全加速的域名有什么要求吗?

A5

接入安全加速服务的域名，需要在工信部完成备案，且源站的业务内容必须合法。

Q6

关闭加速服务后，域名配置会保留吗？

A6

欠费导致服务关闭，域名配置会保留，但不会继续为所配置域名提供加速服务。

Q7

删除加速域名后，域名配置会保留吗？

A7

删除域名后，其配置将不会保留。

Q8

域名被封禁如何解封？

A8

提交工单。

Q9

安全加速服务被暂停了，为什么？

A9

业务被暂停有以下几种情况：

欠费

未备案或备案已过期

内容违规

5.3 操作类

Q1

如何判断安全加速配置生效？

A1

可 ping、dig 所添加的域名，若转向到*.ctycdn.com，即说明配置成功，安全加速生效。

Q2

使用天翼云安全加速后，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

天翼云安全加速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

天翼云安全加速目前支持哪些防盗链实现方法，可以通过控制台进行自助配置吗？

A3

天翼云安全加速目前支持的防盗链有请求头信息（referer 信息、用户 IP 信息、cookie 信息、User-Agent 信息等）防盗链，可以根据用户需求在控制台进行配置。

5.4 使用限制

Q1

用户是否可以直接购买资源包进行使用？

A1

不可以，用户在使用资源包前，需要开通安全加速的按需产品，开通安全加速的按需产品后，才可以购买资源包进行抵扣，资源包用尽后，直接转为按量计费。

Q2

如果用户为日带宽计费，是否可以购买流量包？

A2

用户如果是日带宽计费，可以购买流量包，但是不会抵扣，当变更为流量计费模式后，会抵扣购买的流量包。