# 天翼云

# DDoS 高防(边缘云版)

# 用户使用指南

天翼云科技有限公司

# 目 录

# 一、产品介绍

## （一）产品定义

DDoS 高防（边缘云版）是依托于丰富的云清洗节点，采用自主研发的高性能负载均衡服务，可实现网络层 100%清洗能力，支持 CC 等应用层防护，联动路由黑洞进行近源压制，形成完整的流量清洗能力，保障客户业务稳定、安全运行

## （二）产品架构


## （三）产品术语

### 1. 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。

## 2. CNAME 域名

控制台添加完域名后，您会得到一个给您分配的 CNAME 域名（该 CNAME 域名假如是*. ctdns.cn）， 您需要在您的 DNS 解析服务商添加 CNAME 记录，将自己的域名指向这个*. 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清洗的节点，达到清洗效果。

## 3. 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。

## 4. 域名接入

域名是用户提供的需要使用 DDoS 高防服务的域名，域名接入指的是您使用 DDoS 高防采用的方式，使用域名接入则默认提供 HTTP、HTTPS 七层的

转发服务。

## 5. 端口接入

端口是用户提供使用 DDoS 高防服务的端口，指的是用户请求端口。端口接入的方式是默认提供 TCP、UDP 四层的转发服务

## 6. 边缘清洗节点

天翼云边缘清洗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。终端用户通过连接边缘清洗节点，边缘清洗节点进行流量清洗后转发回源。

## 7. 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。

## 8. 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，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，节点回源时也使用 HTTP 协

议。

### 9. 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。

### 10. 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。

### 11. 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。

### 12. 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。

### 13. 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

## （四）产品功能

### 1. 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。

### 2. 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。

### 3. 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。

## （五） 产品优势

### 1. 全协议防护

支持从网络层/传输层（L3/4）到应用层（L7）DDoS 攻击的防护。

### 2. AI 大数据协同

依托强大的自研防护集群优势，结合 AI 智能引擎持续优化防护策略、IP 画像、行为模式分析、Cookie 挑战等多维算法，实现大数据联动防护。

### 3. 极简管理，弹性扩容

提供可视化管理界面，结合云原生、智能调度能力，实现资源动态扩容，满足用户三网防护需求。

### 4. 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。

### 5. 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

### 6. 透明的售卖机制

可根据需要选择套餐包产品或按量计费产品，费用透明，可控，灵活。

## （六）产品价值

### 1. T 级防御带宽，轻松应对流量型攻击

防护网络总带宽超 2T，能够快速持续在线对抗不断变化的 DDoS 攻击，实时保护在线业务稳定运行，有效遏制损失扩大。

### 2. 有效解决游戏离线、玩家无法登录

为处于 DDoS 攻击重灾区的游戏行业，有效解决因频繁的黑客攻击而导致的宽带堵塞、登录端口不可用、服务离线等致命问题。

### 3. 规避 DDoS 攻击导致的在线企业服务离线

领先的 DDoS 攻击防护能力，有效防御因 DDoS 攻击导致网页无法访问或访问速度变慢等安全问题，保障网站永久在线，稳定运行。避免用户流失、营销活动期间网站瘫痪、在线交易失败等直接或间接造成的经济损失。

### 4. 防止 DDoS 攻击导致的各大官网、系统瘫痪

为各行企业、政府网站等提供针对性的 DDoS 防护解决方案，保障业务连

续性、高可用性及高可靠性，减少安全投入和运维成本。规避恶意攻击导致的企业形象受损、网站无法访问等问题。

# 二、购买指南

## （一）价格

### 1. 计费说明

计费模式：混合计费模式

计费方式：预付费+后付费

| 计费方式 | 描述 | 说明 |
| --- | --- | --- |
| 套餐计费 | 按照购买的套餐进行计费 | 套餐为预付费，套餐为基础费用，套餐失效则扩展服务均失效 |
| 扩展服务 | 根据购买的扩展功能进行计费，包含域名数、端口数、业务带宽 | 扩展服务为预付费 |
| 弹性防护 | 按照业务需求购买弹性防护峰值，包含防护带宽、CC 防护 | 按需收费，根据超出保底带宽的部分产生后按照超出部分所属阶梯价格付费（按天收费），防护超过选定的最高防护带宽，则通过解析回源，2 小时后自动解封 |

## 2. 套餐标准资费

| 防护规格 | CC 防护能力（QPS） | 业务带宽 | 域名数 | 标准资费 |
|---|---|---|---|---|
| 1G | 10000 | 10 | 50（5 个一级） | 1860 元/月 |
| 10G | 50000 | 50 | 50（5 个一级） | 6860 元/月 |
| 30G | 120000 | 50 | 50（5 个一级） | 13860 元/月 |
| 50G | 160000 | 50 | 50（5 个一级） | 20860 元/月 |
| 100G | 400000 | 50 | 50（5 个一级） | 136000 元/年 |
| 300G | 2000000 | 50 | 50（5 个一级） | 216000 元/年 |
| 400G | 3000000 | 50 | 50（5 个一级） | 396000 元/年 |
| 500G | 4000000 | 50 | 50（5 个一级） | 1586000 元/年 |
| 600G | 5000000 | 50 | 50（5 个一级） | 1896000 元/年 |
| 800G | 6000000 | 50 | 50（5 个一级） | 2986600 元/年 |
| 1000G | 8000000 | 50 | 50（5 个一级） | 3026600 元/年 |
| 1500G | 10000000 | 50 | 50（5 个一级） | 4249600 元/年 |

计费项：国内

计费方式：套餐计费

计费周期：按月结算

## 3. 扩展服务标准资费

| 扩展服务 | 标准资费（月） | 功能描述 |
|---|---|---|

| | | |
|---|---|---|
| 带宽扩展 | 35 元/Mbps/月 | 实际业务带宽超过了产品套餐支持的带宽，可通过购买带宽扩展进行带宽补充 |
| 域名扩展 | 500 元/个包/月 | 1 个包支持 1 个主域名及该主域名下的 9 个子域名防护 |
| 端口扩展 | 50 元/个/月 | 端口可根据所需数量进行扩展购买 |

计费项：国内

计费方式：套餐计费

计费周期：按月结算

## 4. 弹性防护标准资费

| 防护带宽（Gbps） | CC 防护能力（QPS） | 标准价格（元/天） |
|---|---|---|
| 0Gbps<超出保底攻击量≤10Gbps | 0<超出保底攻击峰值≤40000 | 860 |
| 10Gbps<超出保底攻击量≤20Gbps | 40000<超出保底攻击峰值≤80000 | 1760 |
| 20Gbps<超出保底攻击量≤30Gbps | 80000<超出保底攻击峰值≤120000 | 2660 |
| 30Gbps<超出保底攻击量≤40Gbps | 120000<超出保底攻击峰值≤160000 | 3260 |
| 40Gbps<超出保底攻击量≤50Gbps | 160000<超出保底攻击峰值≤200000 | 4060 |
| 50Gbps<超出保底攻击量≤60Gbps | 200000<超出保底攻击峰值≤240000 | 4960 |

| | | |
|---|---|---|
| 60Gbps<超出保底攻击量≤70Gbps | 240000<超出保底攻击峰值≤280000 | 5760 |
| 70Gbps<超出保底攻击量≤80Gbps | 280000<超出保底攻击峰值≤320000 | 6560 |
| 80Gbps<超出保底攻击量≤100Gbps | 320000<超出保底攻击峰值≤400000 | 8160 |
| 100Gbps<超出保底攻击量≤150Gbps | 400000<超出保底攻击峰值≤600000 | 15060 |
| 150Gbps<超出保底攻击量≤200Gbps | 600000<超出保底攻击峰值≤800000 | 20160 |
| 200Gbps<超出保底攻击量≤500Gbps | 800000<超出保底攻击峰值≤2000000 | 66660 |
| 500Gbps<超出保底攻击量 | 2000000<超出保底攻击峰值 | 98860 |

计费项：国内

计费方式：按需

计费周期：按天结算

计费描述：购买时选定弹性防护最高防护峰值，若攻击带宽超出套餐带宽，则超出部分按照弹性防护阶梯按日收费，若超出弹性防护最高防护峰值，则解析回源，2 小时后解封。

例子：套餐购买 10G，50000QPS，弹性防护购买 20G ，80000 QPS

则若攻击带宽 10G 以内不进行额外收费，若攻击超过 10G，比如 15G，则超出的 5G 按照弹性防护收费，且落在第一阶梯[0-10G]以内按照 860 元/天收费。若攻击 25G，则攻击超过套餐的 15G，则落在第二阶梯[10-20G]以内按照 1760 元/天收费，若攻击 35G，则攻击超过弹窗的 25G，但最高弹性防护仅购买 20G，则不进行防护，直接解析回源，2 小时后在解析回来。

## （二）购买

开通天翼云 DDoS 高防（边缘云版）服务，需首先注册天翼云账户。

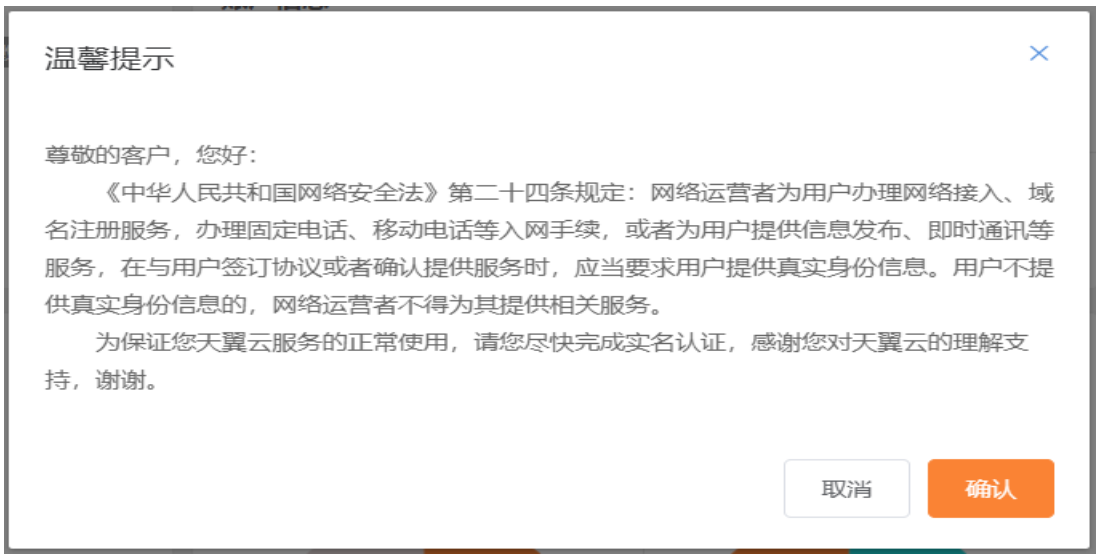
开通步骤如下：

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

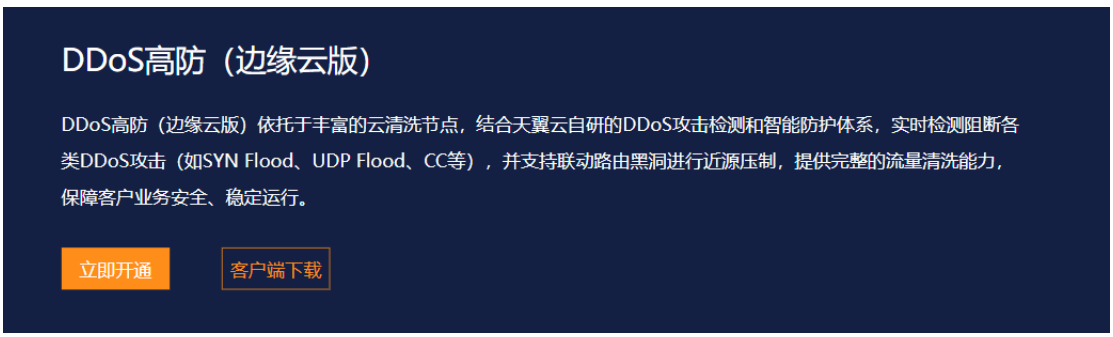
2-2 实名认证提醒




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



4）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”，产品即开通；

2-5 产品开通页

产品服务标准:

| 防护带宽(Gbps) | CC防护峰值(qps) | 标准价格(元/天) |
|---|---|---|
| 0Gbps<超出保底攻击量≤10Gbps | 0<超出保底攻击峰值≤40000 | 860 |
| 10Gbps<超出保底攻击量≤20Gbps | 40000<超出保底攻击峰值≤80000 | 1760 |
| 20Gbps<超出保底攻击量≤30Gbps | 80000<超出保底攻击峰值≤120000 | 2660 |
| 30Gbps<超出保底攻击量≤40Gbps | 120000<超出保底攻击峰值≤160000 | 3260 |
| 40Gbps<超出保底攻击量≤50Gbps | 160000<超出保底攻击峰值≤200000 | 4060 |
| 50Gbps<超出保底攻击量≤60Gbps | 200000<超出保底攻击峰值≤240000 | 4960 |
| 60Gbps<超出保底攻击量≤70Gbps | 240000<超出保底攻击峰值≤280000 | 5760 |
| 70Gbps<超出保底攻击量≤80Gbps | 280000<超出保底攻击峰值≤320000 | 6560 |
| 80Gbps<超出保底攻击量≤100Gbps | 320000<超出保底攻击峰值≤400000 | 8160 |
| 100Gbps<超出保底攻击量≤150Gbps | 400000<超出保底攻击峰值≤600000 | 15060 |
| 150Gbps<超出保底攻击量≤200Gbps | 600000<超出保底攻击峰值≤800000 | 20160 |
| 200Gbps<超出保底攻击量≤500Gbps | 800000<超出保底攻击峰值≤2000000 | 66660 |
| 500Gbps<超出保底攻击量 | 2000000<超出保底攻击峰值 | 98860 |

域名扩展包: 0

如果您需要防护的域名数量超过您购买套餐的域名数量，可以购买扩展包进行补充：一个扩展包支持1个主域名及域名下的9个子域名，1个包500元

端口数: 0

如果您需要防护的端口数量超过您购买套餐的端口数量，可以购买扩展包进行补充：一个端口50元

业务带宽: 0

0Mbps 500Mbps 1000Mbps 1500Mbps 2000Mbps 2500Mbps 3000Mbps

如果您需要的业务带宽量超过您购买套餐的使用量，可以购买扩展包进行补充：每M为35元

* 购买时长:

1个月 2个月 3个月 6个月 1年 2年 3年

自动续订: 余额充足时自动续订

费用合计
￥1488

| | 价格 | 名称 | 配置 | 说明 |
|---|---|---|---|---|
| ☑ | ￥1,488.00 | 套餐 | 保底防护带宽：1Gbps<br>CC防护能力：10000QPS<br>业务带宽：10M<br>端口数：50<br>域名数：50（5个一级） | 本产品已参加2022年安全产品8折促销活动，且包年购买时可享受包年折扣，具体促销说明如下：<br>1、安全促销活动：系统自动在标准价格的基础上计算8折优惠<br>2、包年折扣：包年订购时1年9折，2年8折，3年7.5折<br>3、安全促销活动与包年折扣不可同时享受，系统默认选择最优惠价格<br>4、安全促销活动促销时间为：2022年1月1日——2022年12月31日 |
| ☐ | ￥0.00 | 弹性防护 | 弹性带宽为按需计费，订购时费用为0，根据防护使用量阶梯计费 | |

☐ 我已阅读，理解并接受《天翼云DDoS高防（边缘云版）服务协议》并确认以上费用项

订购

5）产品服务开通后，便可以根据操作手册去控制台开始接入您要服务的业务。

## （三）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。

## （四）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

## （五）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，并将关停客户的服务。

客户也可以根据需求，进入客户控制台的“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


## （六）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。

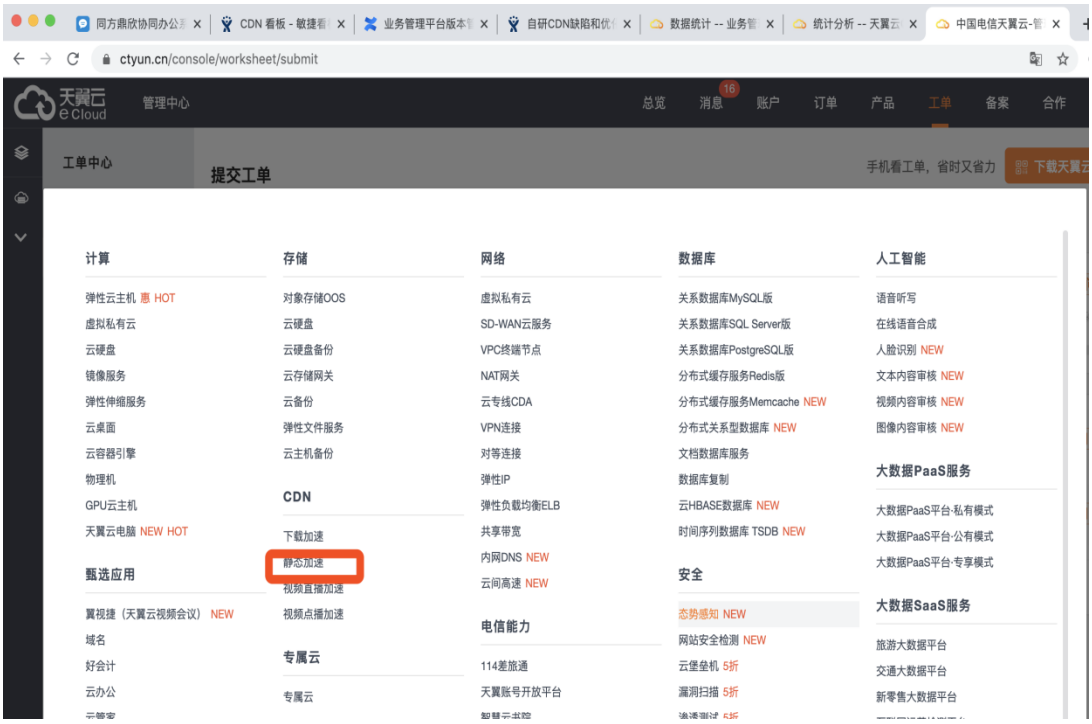
工单提交流程：

1）第一步，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

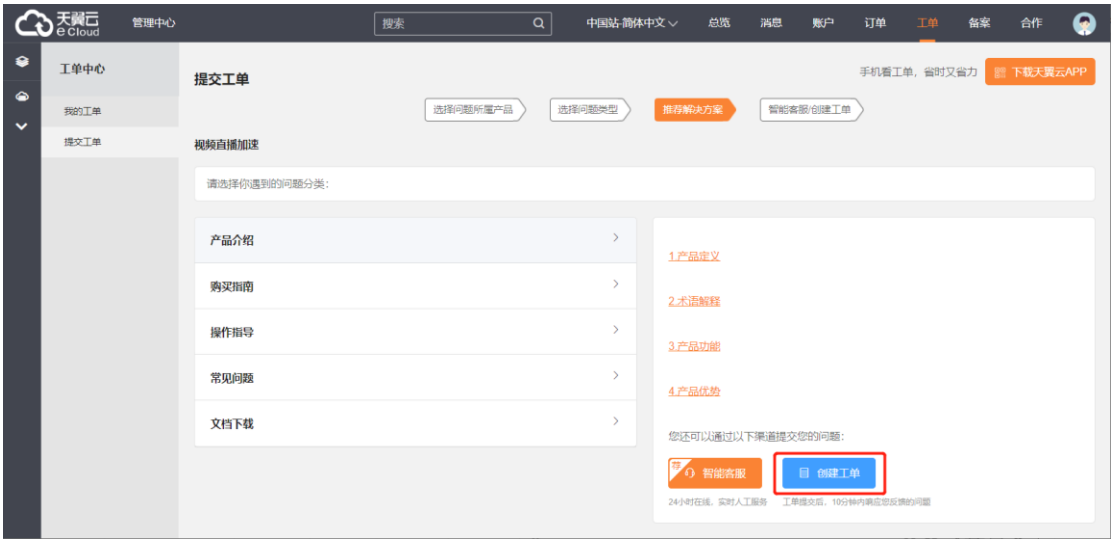

2）第二步，进入“提交工单”页面，在安产品业务处点击“提问”；

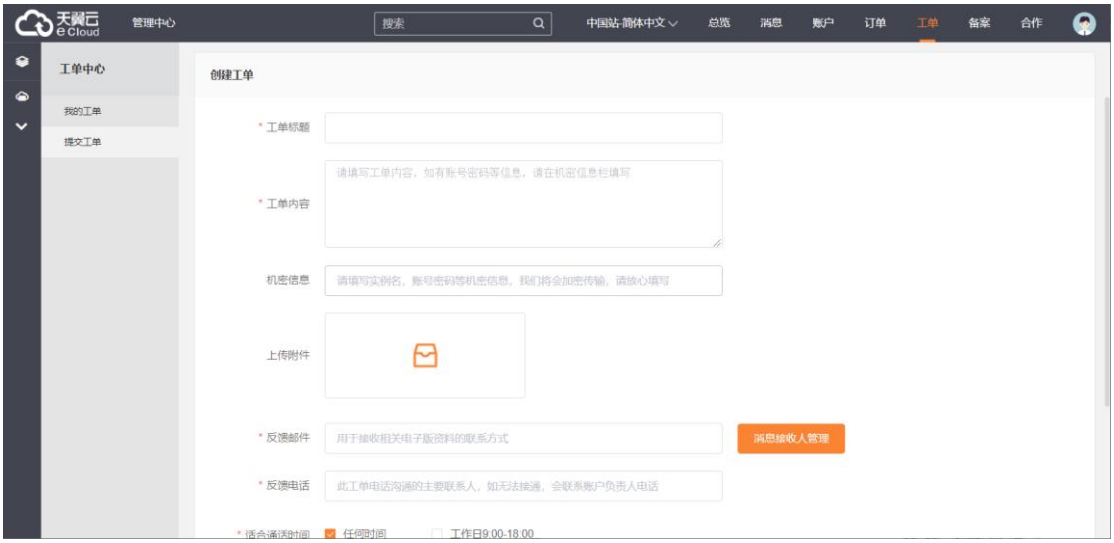
2-12 提交工单页面




3）第三步，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



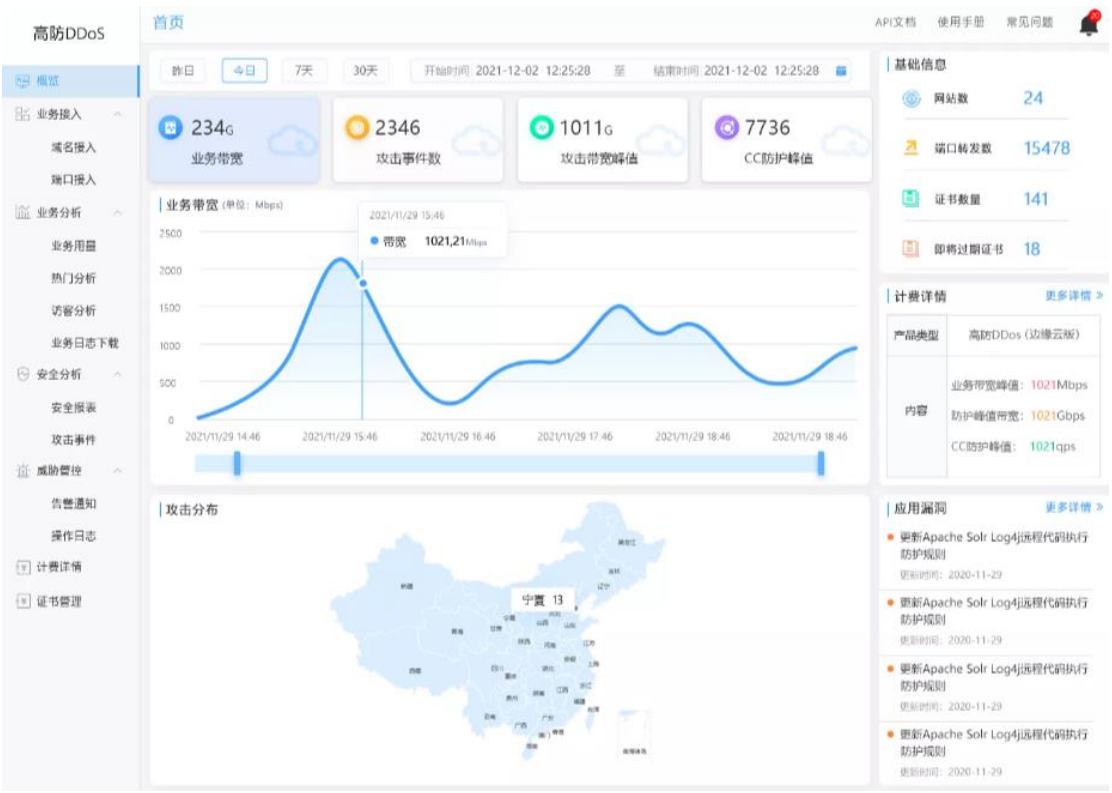




# 三、操作指导

## （一）控制台说明

天翼云 DDoS 高防控制台主要提供概览页面、域名接入、端口接入、安全分析、业务分析、日志下载等功能，方便您对业务情况进行管理。概览页集成了重要指标和核心功能的入口。

3-1 控制台概览页




## （二）快速入门

### 1. 开通安全加速服务

第一步，打开天翼云官网 http://www.ctyun.cn，注册并登录；

第二步，未实名认证的用户需按提示完成实名认证才能开通服务；

第三步，实名认证后进入产品详情页快速了解产品，之后单击【立即开通】；

第四步，在购买页面选择适合的计费方式和产品能力，确认订单，点击【立即开通】，服务即开通；

第五步，服务开通后，便可以根据操作手册去控制台开始接入您要接入的业务了。

## 2. 进入客户控制台

第一步，打开天翼云官网 http://www.ctyun.cn，注册并登录；

第二步，选择控制中心；

3-2 登录控制中心页面


第三步，下拉选择安全产品，点击对应的产品服务进入安全客户控制台；

3-3 控制中心安全加速页面


## 3. 添加域名

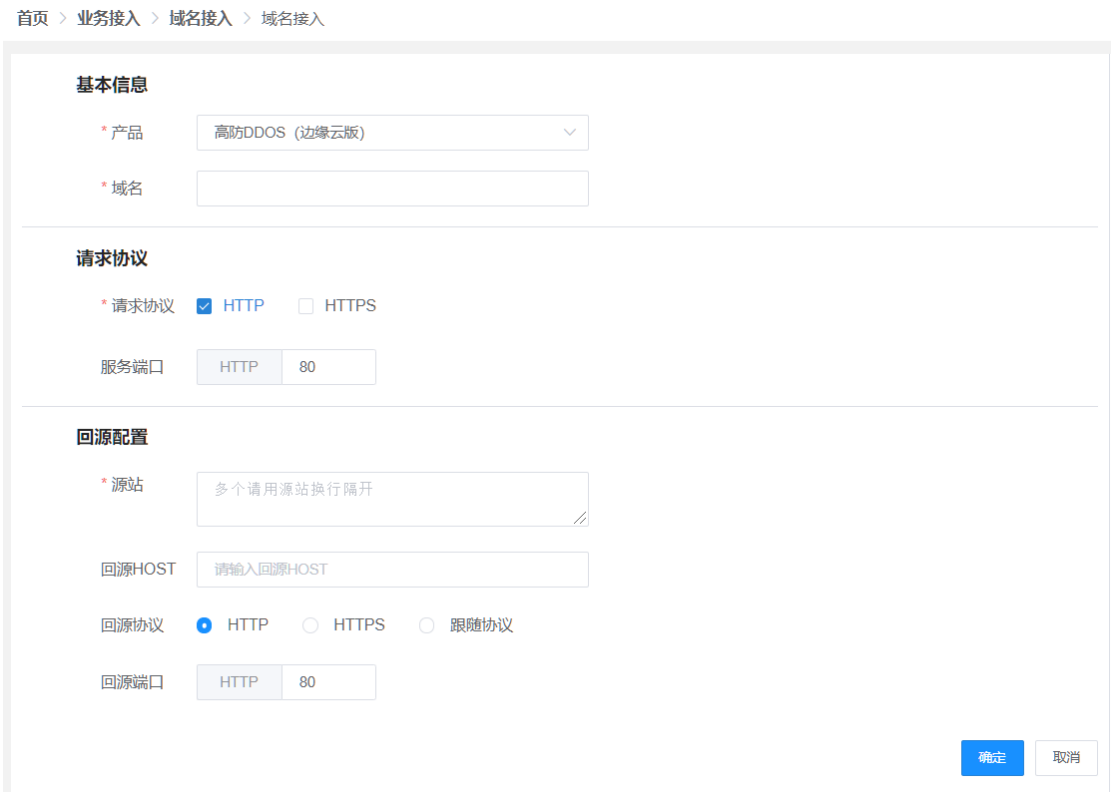
第一步，进入客户控制台，选择【业务接入】，这个页面您可以查看已添加的域名的信息，包括域名、CNAME、域名状态、产品类型等信息。

点击右上角【添加域名】；

3-4 域名管理页面


第二步，填写加速域名信息，并选择产品类型【DDoS 高防（边缘云版）】；

3-5 添加域名页




第三步，根据您的需求，填写对应配置，填写完成后进行提交配

置，首次接入需要进行资源分配，大概需要几个小时，请耐心等候。

域名配置完成，生成域名 CNAME，域名状态变更为【已启用】，即可以在【域名列表】进行对应加速域名配置的【查看/编辑/停用】等操作。

## 4. 添加端口

第一步，进入客户控制台，选择【业务接入-端口接入】，这个页面您可以查看已添加的端口的信息，包括端口、CNAME、CNAME 状态等信息，仅当 CNAME 状态为启用时才可使用，若停用则无法进行解析获得高防 IP。

点击右上角【新增规则】；

3-6 端口接入页面


第二步，填写端口信息，根据您的需求进行填写，支持批量增加，填写后进行提交；

3-7 添加端口页


首次接入需要进行资源分配，大概需要几个小时，请耐心等候。

端口首次配置完成后生成域名 CNAME，且为启用状态，后续针对该 CNAME 进行添加端口。并可在端口列表进行端口删除、修改等操作。

## 5. 配置 CNAME

要启用 DDoS 高防服务，需要您将域名或者业务的 DNS 解析指向我们提供的 CNAME，或者根据我们提供的 CNAME 进行解析出高防 IP 进行服务，这样访问的请求才能转发到高防节点上，达到清洗效果。

第一步，在控制台【业务接入】的域名列表或者端口列表中复制加速域名对应的 CNAME；

3-8 复制 CNAME 页


第二步，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。

第三步，登录新网的域名解析控制台，进入对应域名的域名解析页；

第四步，选择【添加新的别名】；

3-9 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。

第五步，确认填写信息无误后，单击【提交】；

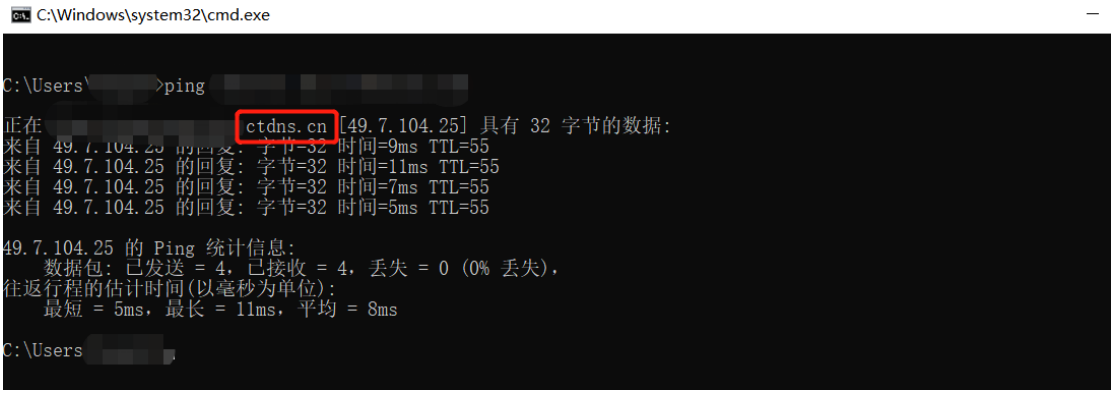
第六步，验证服务是否生效；

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

时间生效；

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

3-10 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；

3-11 解析记录互斥规则

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

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

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

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

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

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

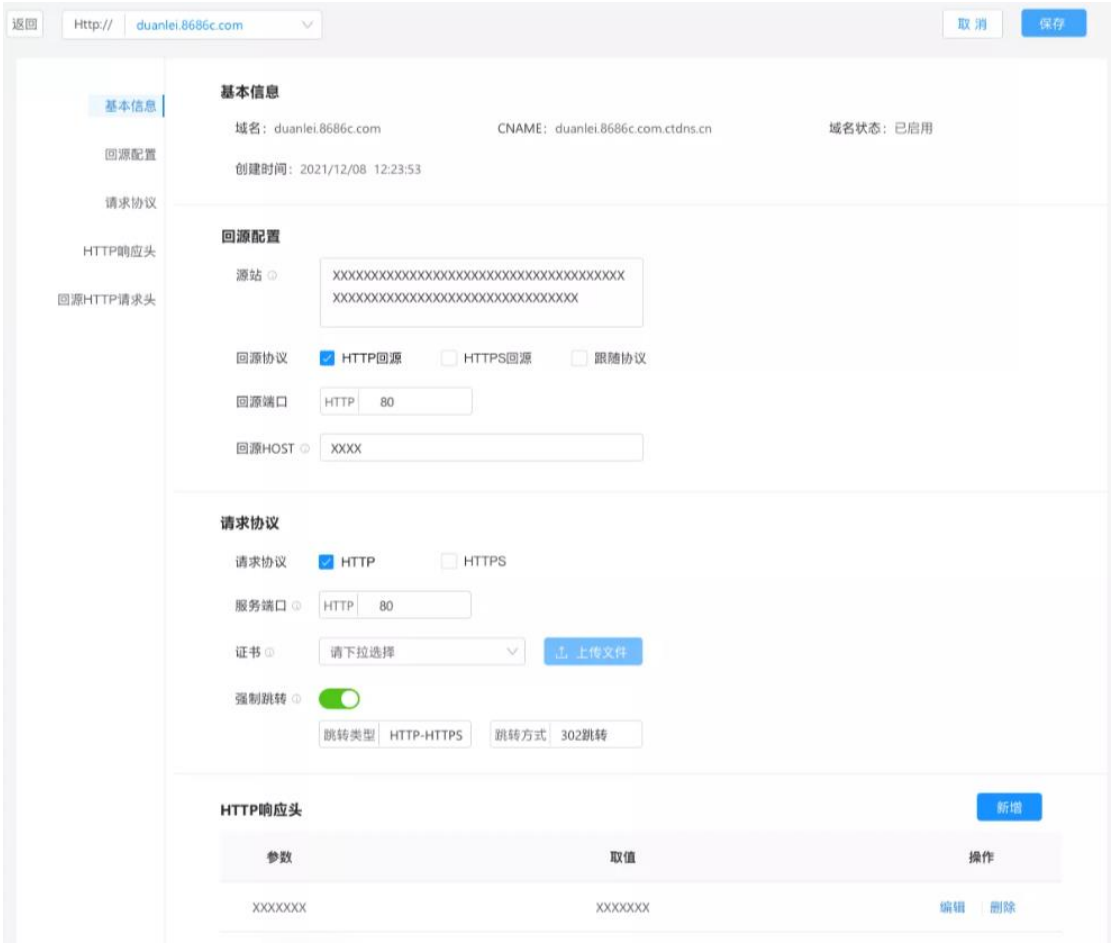
## （三）域名配置管理

通过域名接入列表，进行管理已添加有的域名；域名配置包含网站配置、防护配置

## 1. 网站配置

网站配置包含基础信息、回源配置、请求协议、HTTP 响应头、回源 HTTP 请求头等配置，可根据配置需求进行配置，配置完成后点击保存下发。

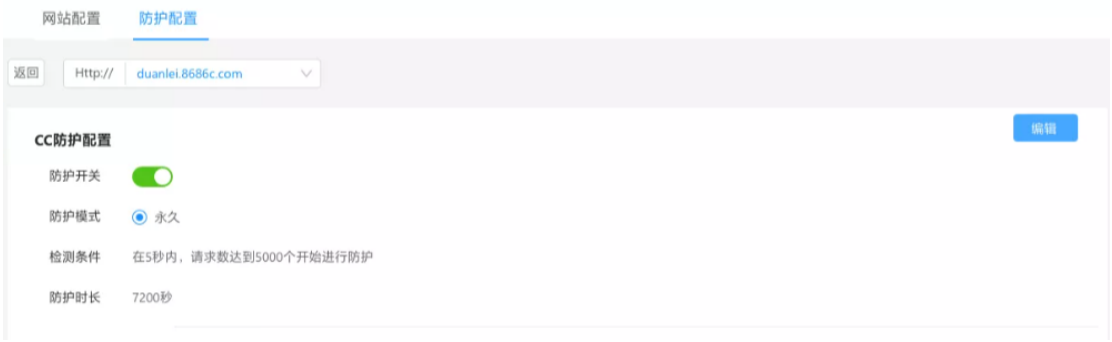
3-12 网站配置




## 2. 防护配置

防护配置主要包含 CC 防护策略配置，默认关闭，可根据业务需求进行开启。

3-13 防护配置

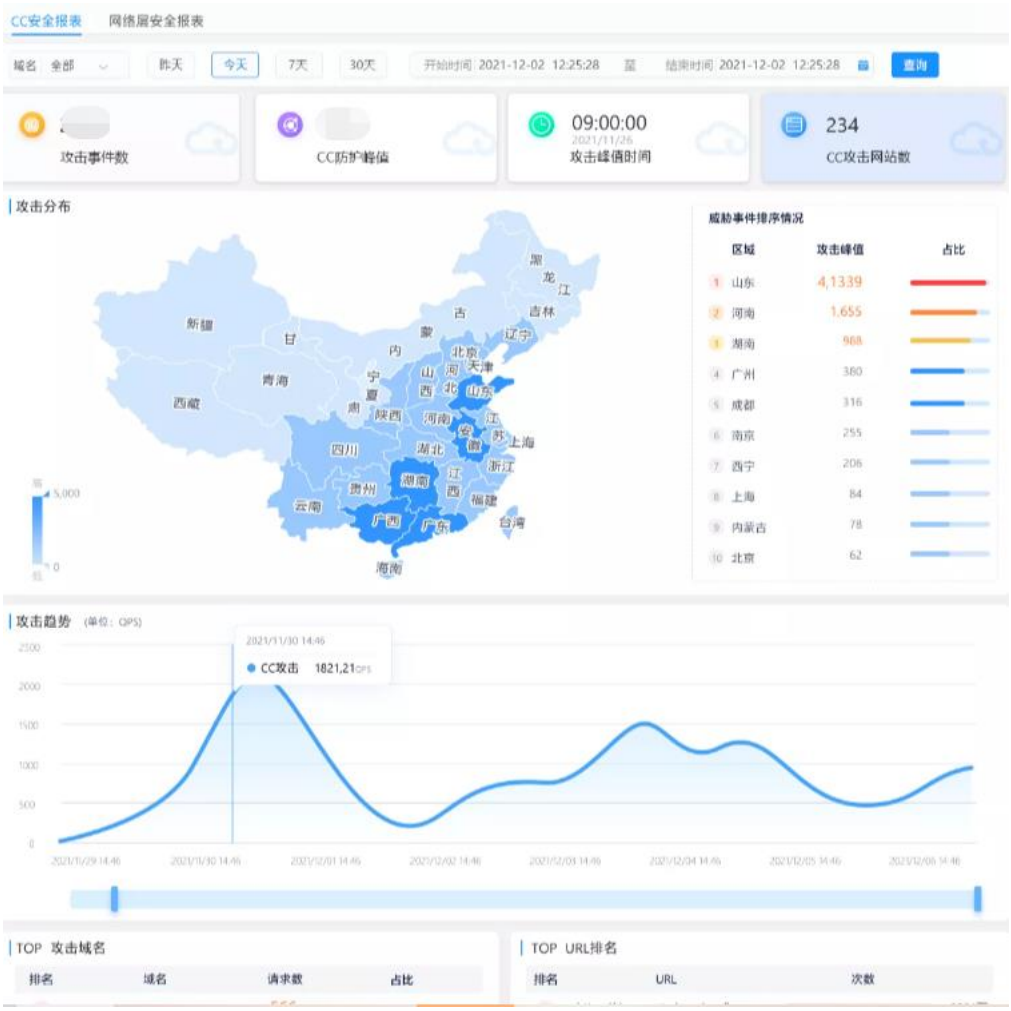



## （四）安全分析

时间选择跨度最长不能超过 31 天，仅能查询 3 个月内的数据

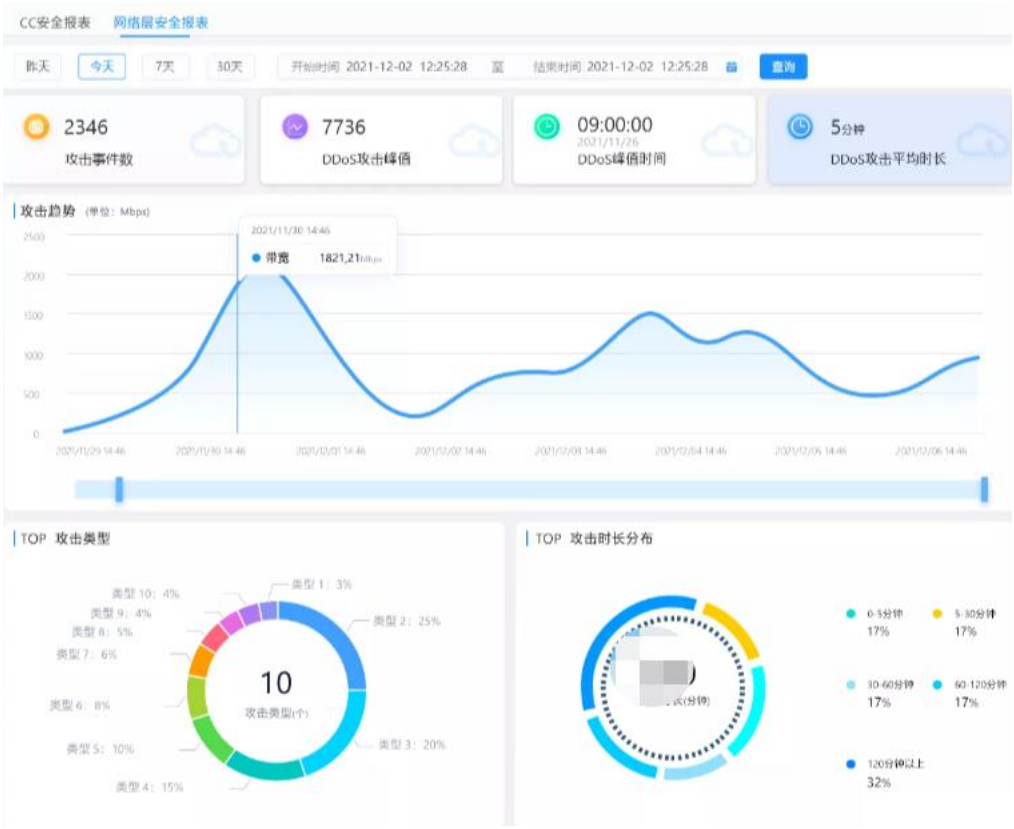
## 1. CC 安全报表

3-14 CC 安全报表



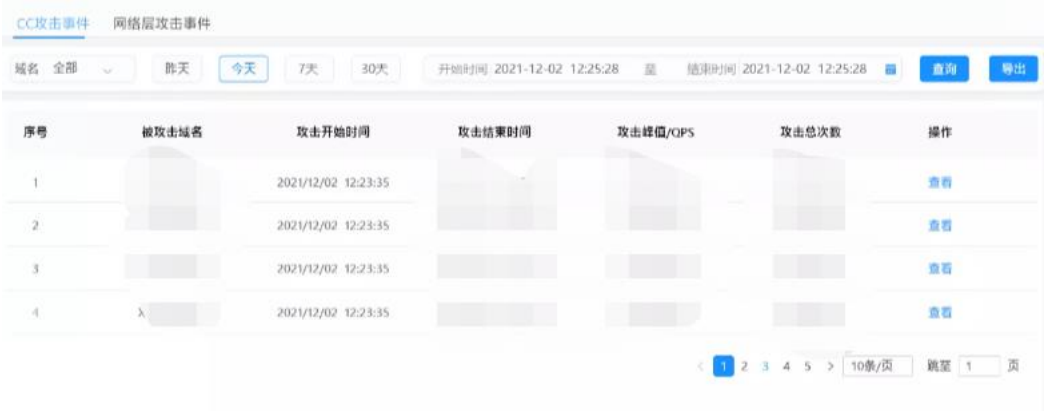
## 2. 网络层安全报表

3-15 网络层安全报表




## 3. CC 攻击事件

3-16 CC 攻击事件




## 4. 网络层攻击事件

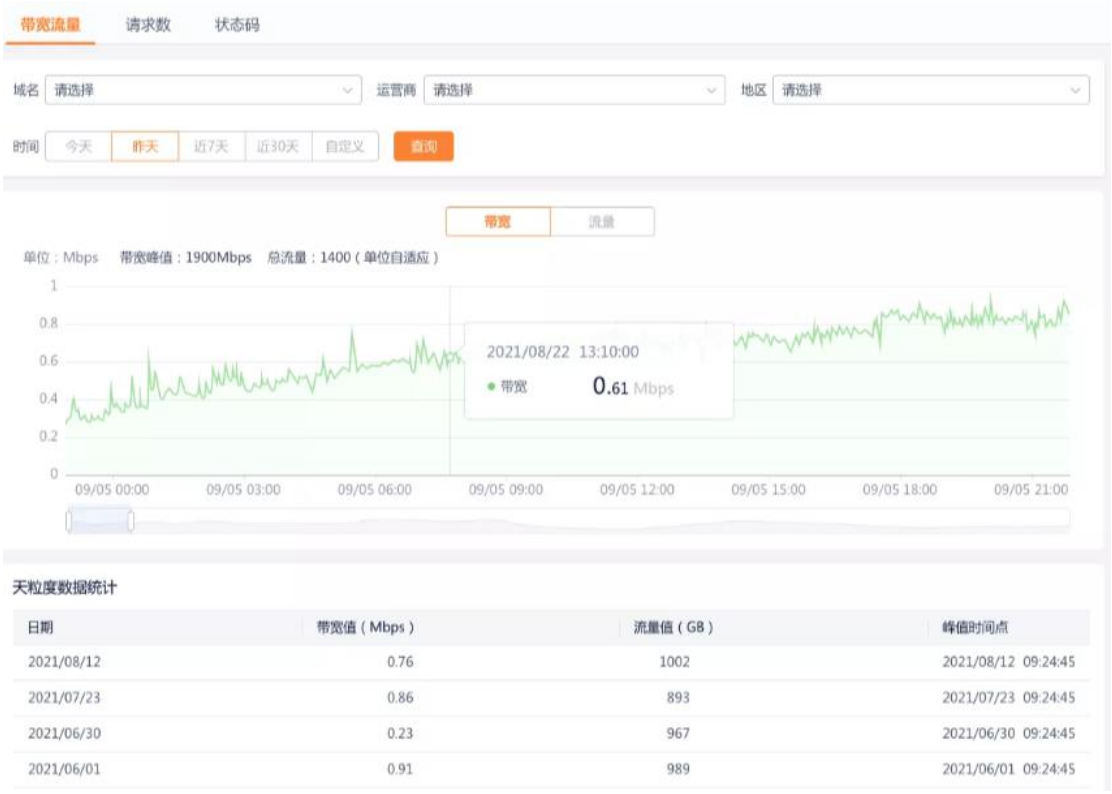
3-17 网络层攻击事件


## （五）业务分析

时间选择跨度最长不能超过 31 天，仅能查询 3 个月内的数据

### 1. 带宽流量统计

3-18 带宽流量统计




### 2. 日志下载

3-19 日志下载


## （六）计费详情

可查看购买的套餐情况

3-20 计费详情


# 四、常见问题

## （一）计费类

Q1：停用域名服务后，为什么仍有一部分带宽产生？

A1：造成该情况的原因主要有以下两种：

1）在停用域名服务后，若客户 LocalDNS 服务器中缓存未过期，LocalDNS

会继续把访问已停用域名的请求解析到节点，造成少量计费。

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：产品收费项都有哪些？

A2：产品主要是包周期+按需收费，主要包含套餐+扩展服务是包周期按月订购，弹性防护是按需按天收费，详情见上方 2-1 价格说明

Q3：弹性防护和套餐如何选购？

A3：弹性防护需要根据您自身希望防护的最高防护带宽-套餐所带的防护带宽，则是您需要选购的弹性防护值，比如您希望防护 100G 带宽，选购的套餐已包含 20G 防护带宽，则弹性防护购买 80G 带宽。

若您频繁被攻击建议买更大的套餐，套餐是按月收费，若您仅是偶尔被攻击且攻击量不确定，可以购买弹性防护作为保险，弹性防护是按天按需进行收费

Q4：弹性防护收费该如何理解？

A4：购买时选定弹性防护最高防护峰值，若攻击带宽超出套餐带宽，则超出部分按照弹性防护阶梯按日收费，若超出弹性防护最高防护峰值，则解析回源，2 小时后解封。

例子：套餐购买 10G，50000QPS，弹性防护购买 20G ，80000 QPS 则若攻击带宽 10G 以内不进行额外收费，若攻击超过 10G，比如 15G，则超出的 5G 按照弹性防护收费，且落在第一阶梯[0-10G]以内按照 860 元/天收

费。若攻击 25G，则攻击超过套餐的 15G，则落在第二阶梯[10-20G]以内按照 1760 元/天收费，若攻击 35G，则攻击超过弹窗的 25G，但最高弹性防护仅购买 20G，则不进行防护，直接解析回源，2 小时后在解析回来。

Q5：购买套餐后，套餐内包含的带宽和域名数量不够怎么办？

A5：如果套餐内包含的用量不够，可以通过扩展服务来补充，扩展服务购买成功后，计费和域名数量总使用量是套餐内的量和扩展服务用量之和。

Q6：DDoS 高防套餐是否支持变更？

A6：目前套餐支持升级，暂时不支持降级，本月升级，次月生效。

Q7：DDoS 高防是否按需收费？

A7：目前套餐以及扩展服务的带宽、域名、端口不支持按需收费，需要进行提前购买，防护带宽可购买弹性防护，弹性防护按需收费。

## （二）开通类

Q1：怎么样开通高防 DDoS 服务和使用？

A2:产品开通首先需要注册天翼云官网的账号，通过产品栏目找到产品，选择相应的功能，点击开通；开通后会跳转到 DDoS 高防控制台，在控制台上配置域名或者端口，配置成功后会提供对应的 cname，客户切入 cname 后，开始使用天翼云的服务。

Q2：欠费后服务会被关停吗？

A2：账户余额不足以支付服务费用将导致欠费，发生欠费后，域名或者端口将被关停。

Q3：关停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，被停止的域名或者端口需要客户到控制台域名管理模块，点击启用，开启被停用的域名或者 CNAME，当域名或 CNAME 状态变更为已启用后，即服务已启用客户可解析过来。

Q4：端口或域名配置完成后大概多久生效？

A4：首次配置涉及高防 IP 分配，时间较久，需要大概 1-5 小时，若二次接入，则仅需 1 小时左右，若需要紧急处理或时间较久未生效，则可联系技术支持或提交工单处理。

Q5：接入的域名有什么要求吗？

A5：接入的域名，需要在工信部完成备案，且源站的业务内容必须合法。

Q6：接入的端口有什么要求吗？

A6：接入端口因国家备案要求，所以不支持 80，8080，443，8443 端口接入，有该端口需求可使用域名接入

此外端口有预留部分内部端口，详情可见控制台实时更新。

Q7：关闭服务后，配置会保留吗？

A7：欠费或人工手动关停导致服务关闭，域名配置会保留，但不会继续为所配置的端口或域名提供服务；若需启用可直接启用配置，若将配置进行删除，则底层不保留配置，则无法进行恢复。

Q8：服务被暂停了，为什么？

A8：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

## （三）操作类

Q1：如何判断配置生效？

A1：可 ping、dig 所添加的域名，若转向到提供的 CNAME，即说明配置成功，已新增生效。

Q2：域名自助操作可操作哪些配置？

A2：可操作域名的网站配置，包含源站协议、回源 HOST、回源头部、请求协议等；防护配置目前仅提供 CC 防护自助配置

Q3：端口转发可操作哪些配置？

A3：包含转发端口、协议、源站、源站端口

Q4：DDoS 高防支持哪些协议接入？

A4：DDoS 高防支持域名进行 HTTP、HTTPS 接入，并且同时支持 Websocket、Websockets 接入，端口进行 TCP、UDP 协议接入。