天翼云

DDoS 高防（边缘云版）

控制台使用指南

中国电信股份有限公司云计算分公司

目录

1.1 产品定义 3
操作指导 4
1.2 控制台说明 4
1.3 快速入门 5
1.4 域名管理 12
1.5 安全分析 15
1.6 告警管理 17
1.7 业务分析 18
1.8 计费详情 19
1.9 证书管理 19
常见问题 21
1.10 操作类 21

产品介绍

1.1 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。

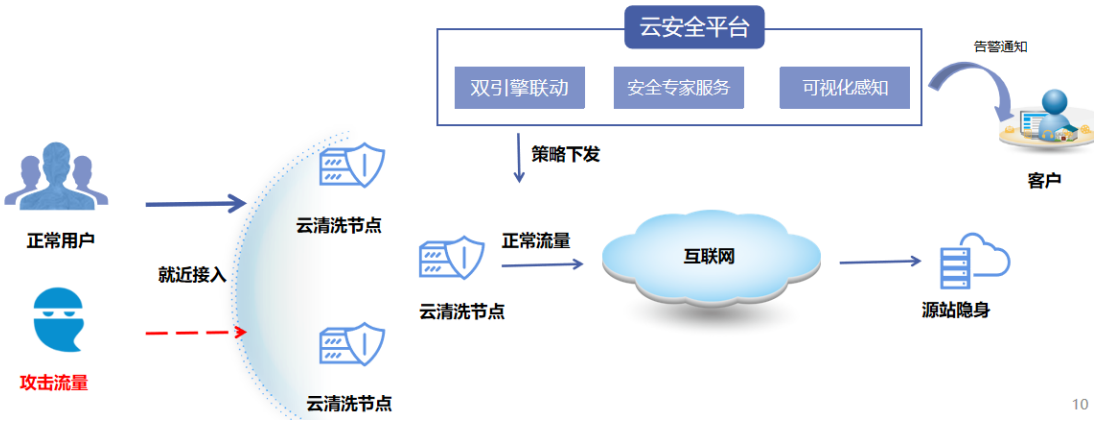
支持大规模流量清洗，清洗能力达到 T 级以上。

支持从网络层/传输层（L3/4）到应用层（L7）DDoS 攻击的防护。

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。

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。

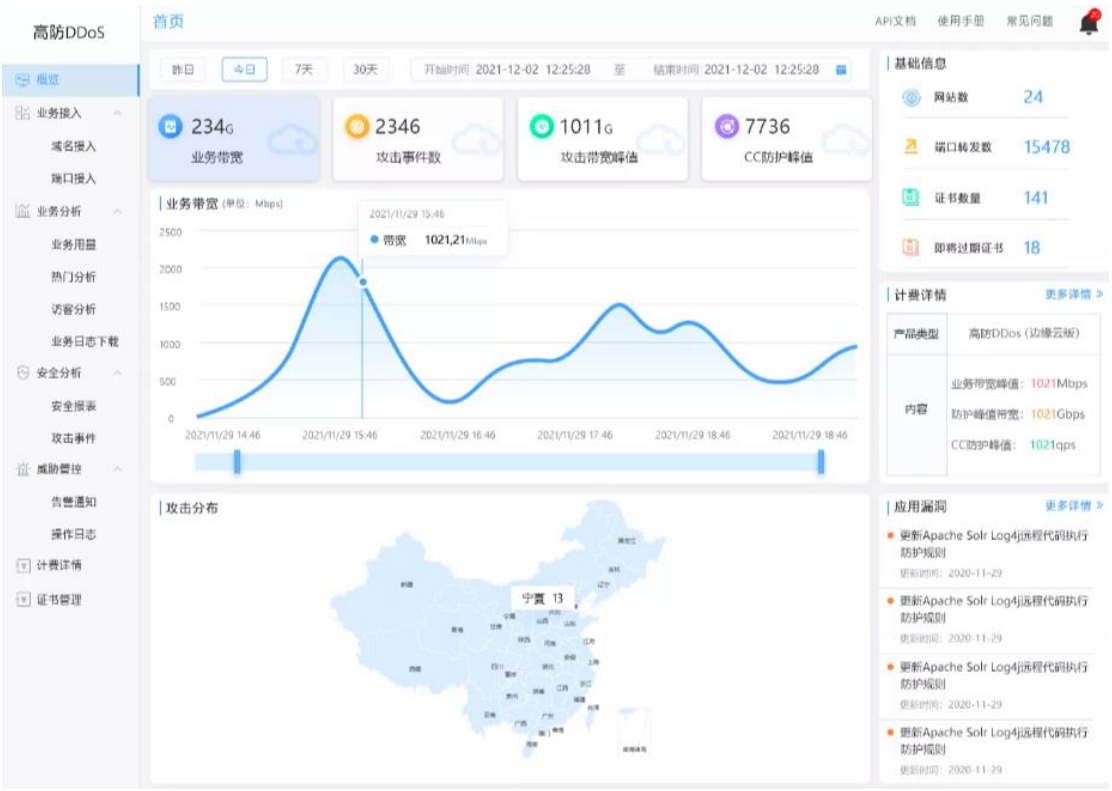
产品基本架构：



1.2 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。

DDoS 高防控制台概览页：



下面逐一介绍概览页的模块展示 ：

1. 基础数据：主要展示业务带宽、攻击事件数、防护峰值带宽和 CC 防护峰值等基础数据。

2. 业务带宽：展示所选时间周期内产生的业务带宽图。

3. 攻击分布：展示所选时间周期内攻击数据的区域分布图。

4. 基础信息：接入网站数、端口转发数、证书情况。

5. 计费详情：查看购买的高防 DDoS 套餐情况。

6. 应用漏洞：平台监测到的公开漏洞风险公告。

1.3 快速入门

1.3.1 开通 DDoS 高防（边缘云版）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 DDoS 高防（边缘云版）服务；

第三步，实名认证后进入 DDoS 高防（边缘云版）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】，DDoS 高防（边缘云版）服务即开通；

第五步，DDoS 高防（边缘云版）服务开通后，便可以根据操作手册去 DDoS 高防控制台开始接入您要加速的域名了。

1.3.2 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（已注册的可直接登录）；

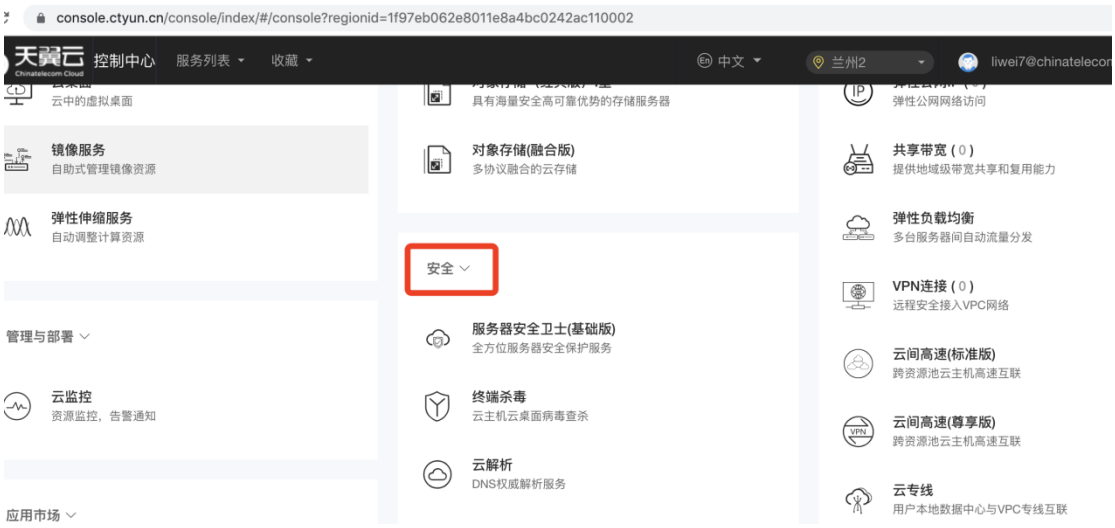
第二步，选择控制中心；

登录控制中心页：



第三步，下拉选择安全产品，点击对应的服务进入 DDoS 高防（边缘云版）客户控制台；

控制中心 DDoS 高防（边缘云版）页面：



1.3.3 添加域名

第一步，进入 DDoS 高防客户控制台，选择【业务接入-域名接入】，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、产品类型、以及域名配置和变更的入口。

点击【新增域名】；

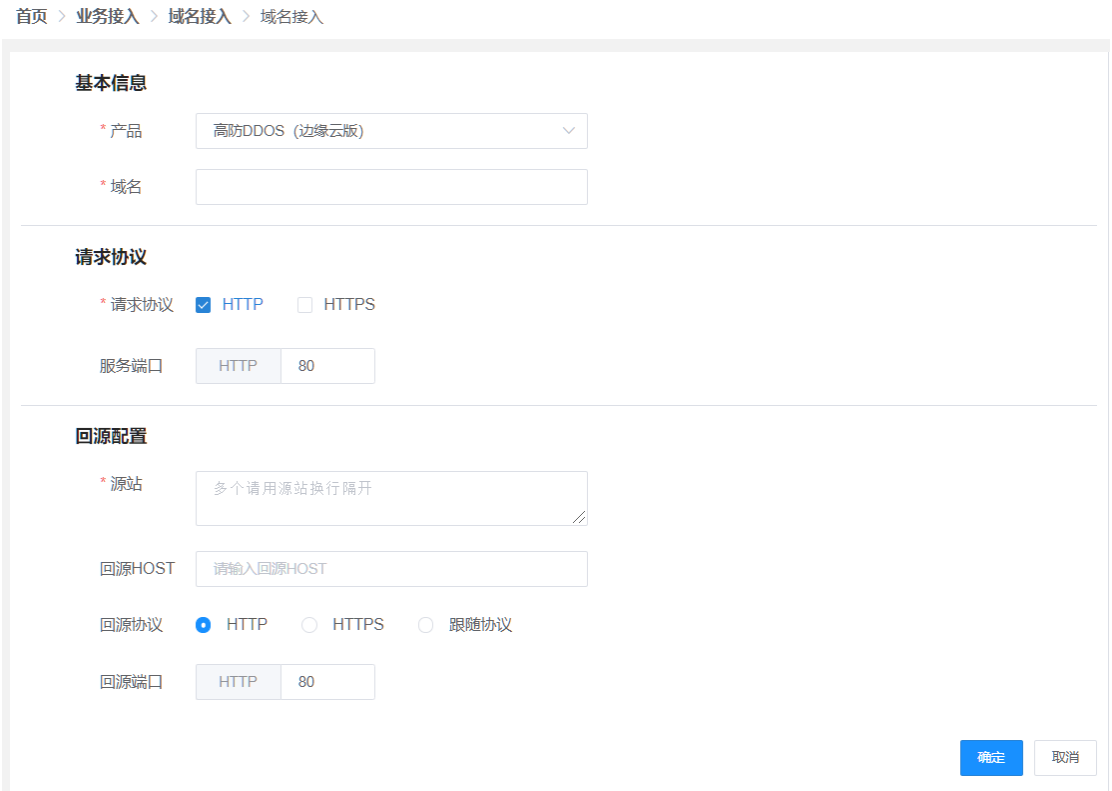
域名管理页面：



第二步，填写域名接入信息，并选择产品类型【高防 DDoS（边缘云版）】；

根据页面的引导填写域名的源站信息、请求协议、服务端口、回源协议和回源端口等信息；填写后，点击【确定】提交配置。

添加域名配置页：



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。

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。

1.3.4 添加端口

第一步，进入 DDoS 高防客户控制台，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】。



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，填写后点击【确认】进行提交；

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。

1.3.5 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 DDoS 高防控制台【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；

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】；

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】；

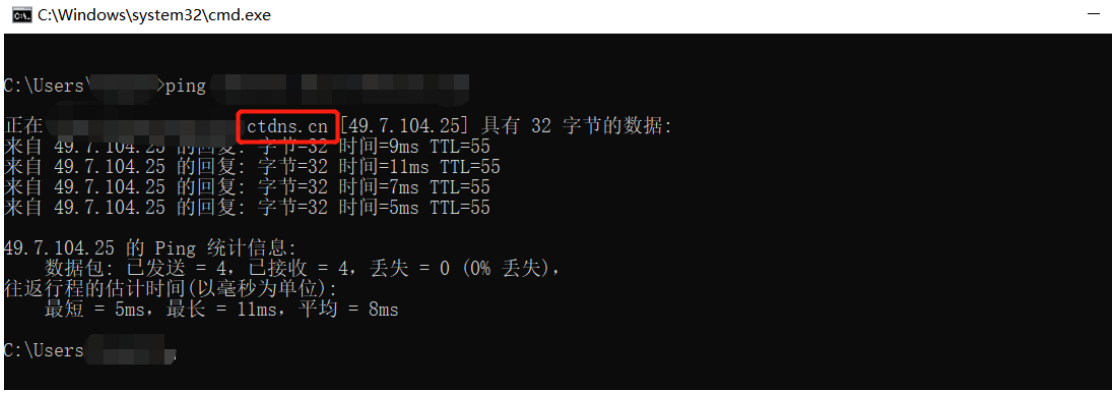
第六步，验证服务是否生效；

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。

检查域名指向页：



注意：

1）配置 CNAME 完毕，CNAME 配置生效后，DDoS 高防服务生效

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，可考虑换一个防护域名，或参考以下“解析记录互斥规则” 调整记录；

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。

1.4 域名管理

通过域名接入列表，进行管理已添加有的域名；可查看已添加的域名、对应的 CNAME、防护状态以及域名配置，其中域名配置包含网站配置、防护配置、停用或者

启用和删除操作；

【网站配置】点击进入可查看域名基础配置信息，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；

【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。

【停用】停止当前域名解析，停止域名服务；

【启用】恢复当前域名解析，启用域名服务；

【删除】从域名列表中删除该域名

1）当域名状态为【已启用】时，可以对域名配置进行【网站配置】、【防护配置】、【停用】【删除】操作；

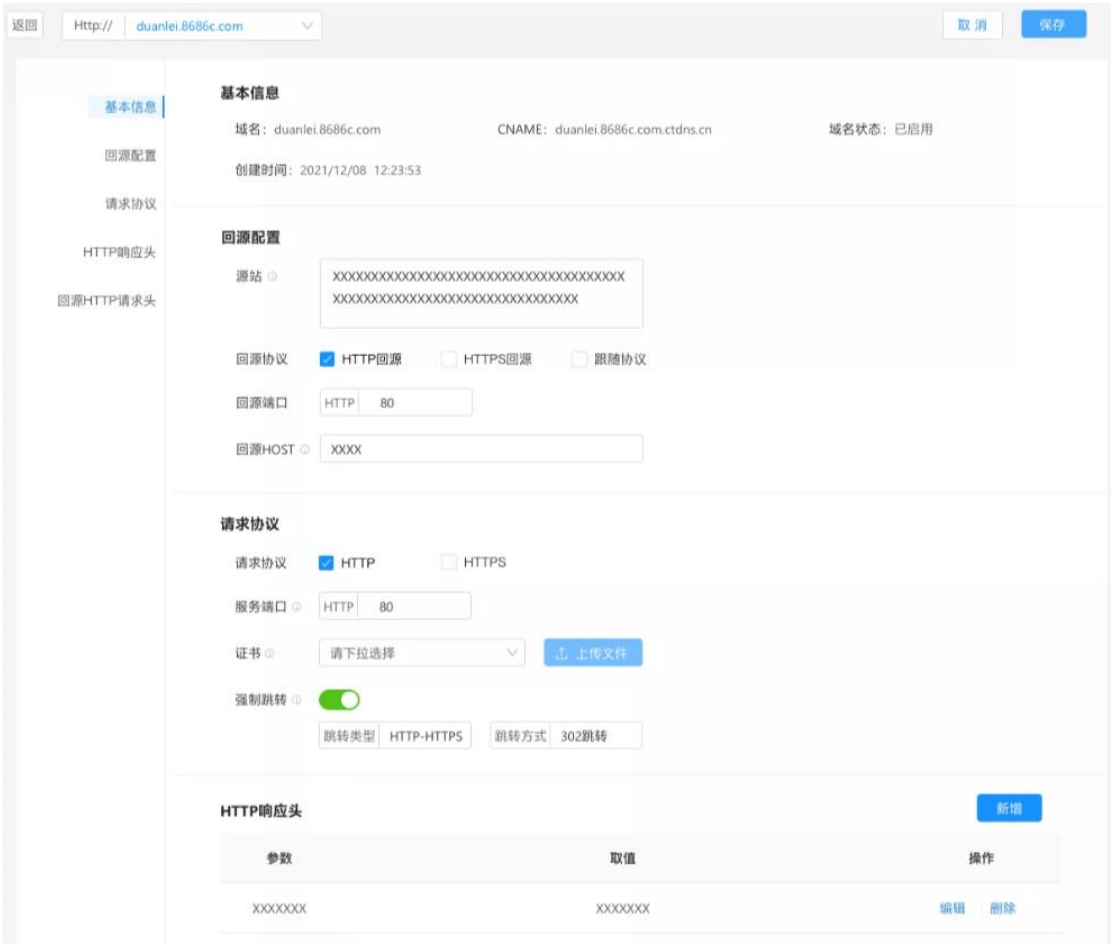
2）当域名状态为【配置中】时，可以对域名配置进行【网站配置】、【防护配置】的查看操作；

3）当域名状态为【已停用】时，可以对域名配置进行【网站配置】、【防护配置】的查看、【启用】和【删除】操作；

1.4.1 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，点击编辑进入配置状态，可根据配置需求进行配置，配置完成后点击保存下发。

网站配置页：



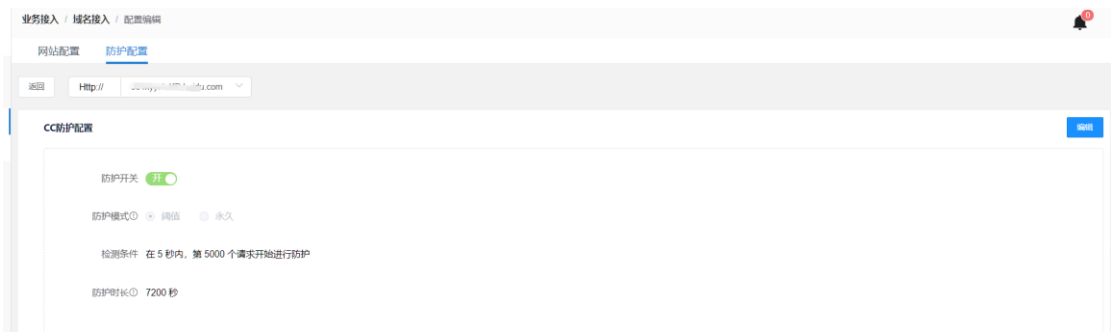
1.4.2 防护配置

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。

CC 防护开关如果为关闭，则不使用该功能，如果点击开启，则需要填写如下信息：

防护模式：可选“阈值”或者“永久”

防护配置页：



1.5 安全分析

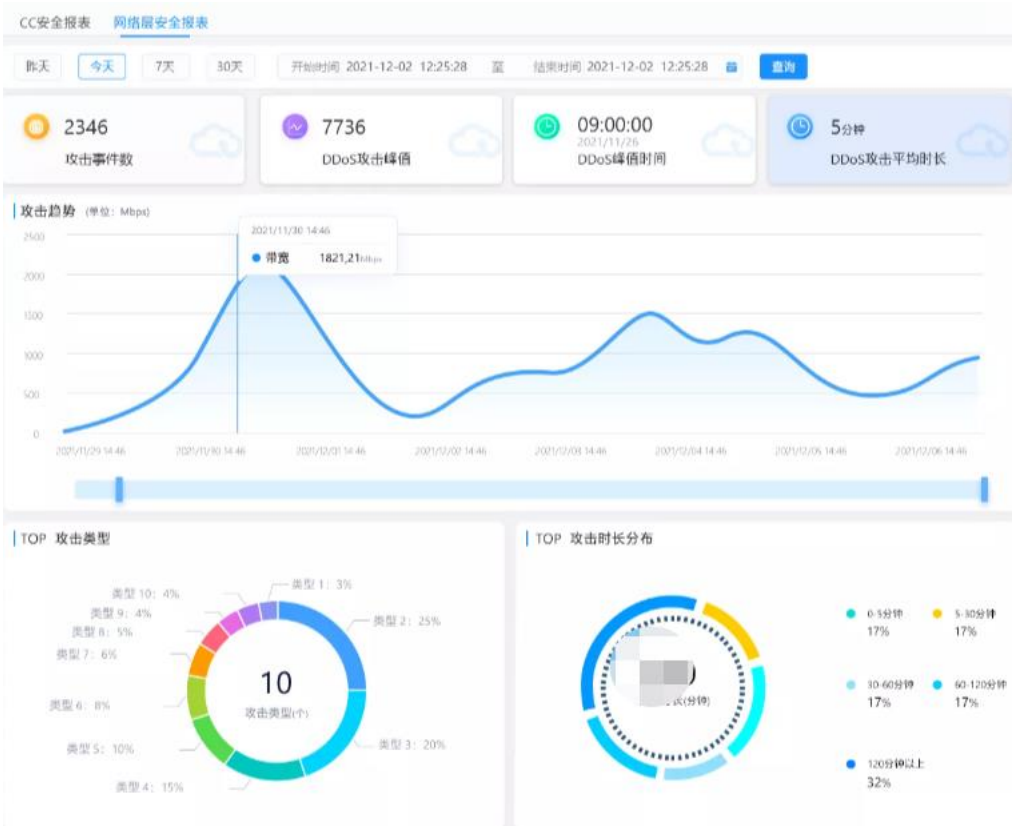
DDoS 高防客户控制平台的【安全分析】页面，包含 CC 安全以及网络层安全的【安全报表】和【安全事件】信息；选择跨度最长不能超过 31 天，仅能查询 3 个月内的数据。

1.5.1 CC 安全报表

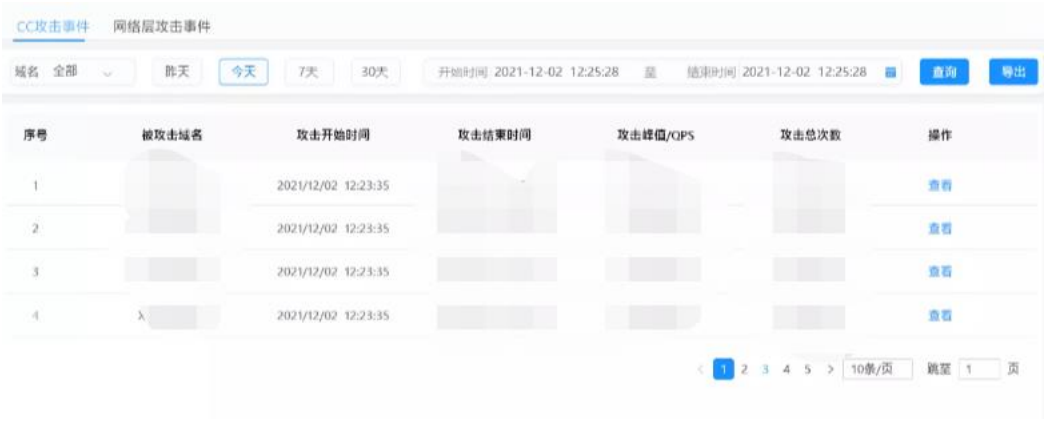
报表中展示所选域名、时间内的攻击事件情况。



1.5.2 网络层安全报表



1.5.3 CC 攻击事件



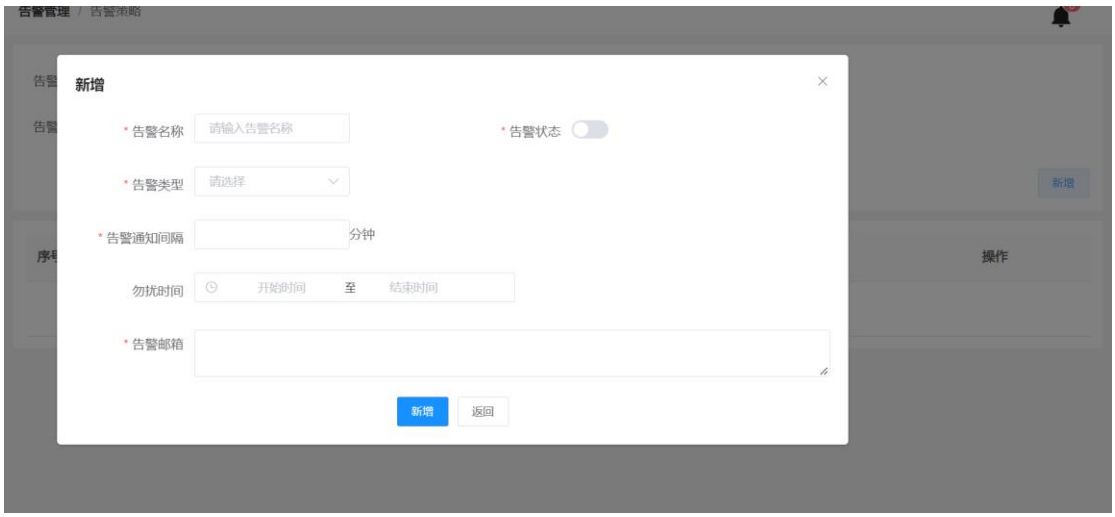
1.5.4 网络层攻击事件



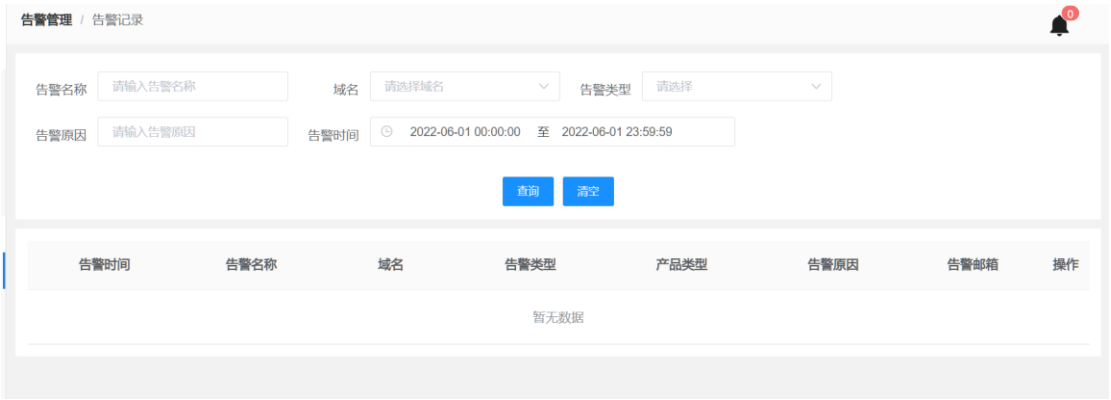
1.6 告警管理

在 DDoS 高防（边缘云版）的【告警管理】中，客户可以配置告警规则以及查看告警记录

告警配置页



告警记录列表页



1.7 业务分析

DDoS 高防客户控制平台的【业务分析】页面，客户可以下载日志、查看业务用量。

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。

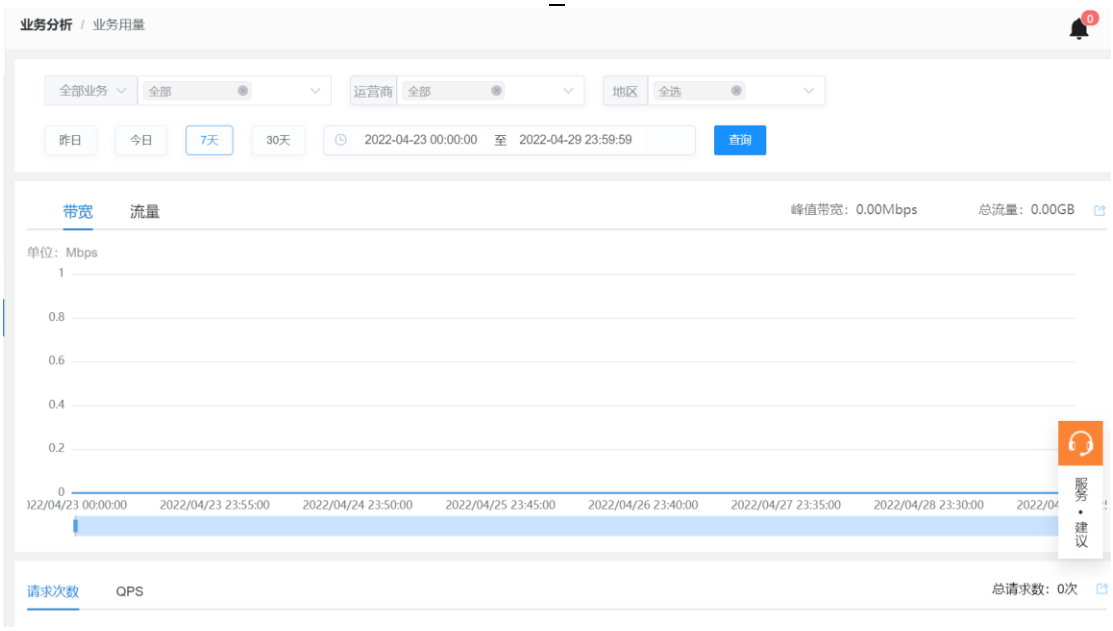
1.7.1 日志下载

结果展示的是您所选域名、时间内的日志数据，点击下载可保存到本地；



1.7.2 业务用量

查询条件支持分域名、端口、全部业务，运营商以及区域，按照所选时间展示数据。可查看对应带宽、流量、请求次数、QPS 和状态码数据。



1.8 计费详情

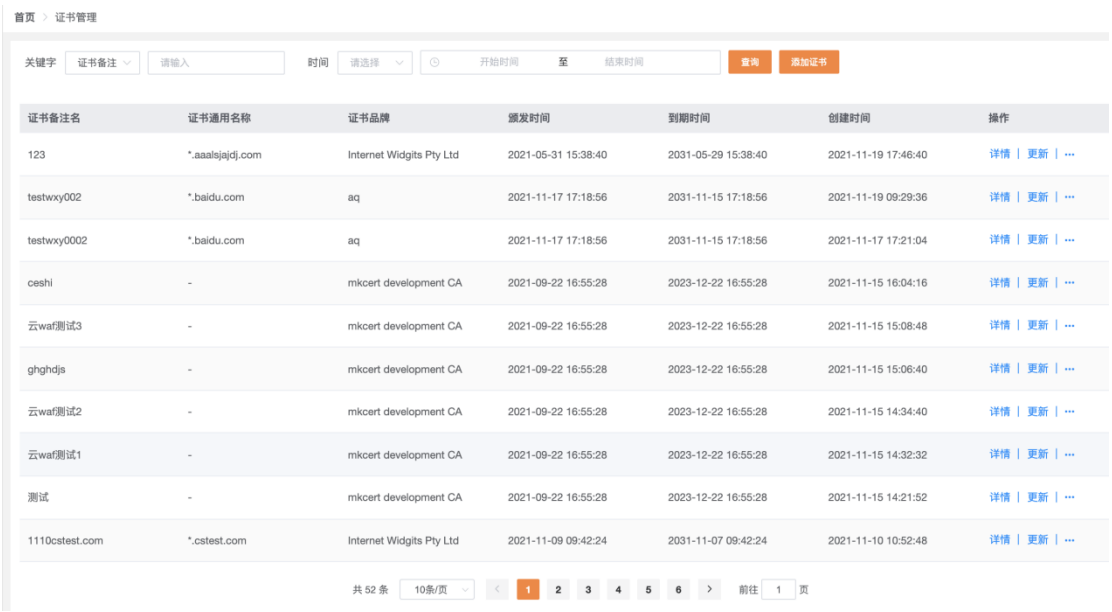
DDoS 高防客户控制平台的【计费详情】页面，客户查看购买的套餐情况。



1.9 证书管理

DDoS 高防客户控制台的【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：


首页 > 证书管理
关键字 证书备注 请输入 时间 请选择 开始时间 至 结束时间 查询 添加证书
证书备注名 证书通用名称 证书品牌 颁发时间 到期时间 创建时间 操作
123 *.aaalsjajdj.com Internet Widgits Pty Ltd 2021-05-31 15:38:40 2031-05-29 15:38:40 2021-11-19 17:46:40 详情 | 更新 | ...
testwxy002 *.baidu.com aq 2021-11-17 17:18:56 2031-11-15 17:18:56 2021-11-19 09:29:36 详情 | 更新 | ...
testwxy0002 *.baidu.com aq 2021-11-17 17:18:56 2031-11-15 17:18:56 2021-11-17 17:21:04 详情 | 更新 | ...
ceshi - mkcert development CA 2021-09-22 16:55:28 2023-12-22 16:55:28 2021-11-15 16:04:16 详情 | 更新 | ...
云waf测试3 - mkcert development CA 2021-09-22 16:55:28 2023-12-22 16:55:28 2021-11-15 15:08:48 详情 | 更新 | ...
ghghdjs - mkcert development CA 2021-09-22 16:55:28 2023-12-22 16:55:28 2021-11-15 15:06:40 详情 | 更新 | ...
云waf测试2 - mkcert development CA 2021-09-22 16:55:28 2023-12-22 16:55:28 2021-11-15 14:34:40 详情 | 更新 | ...
云waf测试1 - mkcert development CA 2021-09-22 16:55:28 2023-12-22 16:55:28 2021-11-15 14:32:32 详情 | 更新 | ...
测试 - mkcert development CA 2021-09-22 16:55:28 2023-12-22 16:55:28 2021-11-15 14:21:52 详情 | 更新 | ...
1110cstest.com *.cstest.com Internet Widgits Pty Ltd 2021-11-09 09:42:24 2031-11-07 09:42:24 2021-11-10 10:52:48 详情 | 更新 | ...
共 52 条 10条/页 1 2 3 4 5 6 前往 1 页

新增证书页：


新增自有证书
* 证书备注名
* 证书公钥（PEM格式）
请输入
* 证书私钥（PEM格式）
请输入
温馨提示
证书公/私钥，目前只支持PEM格式，其他格式请前往“证书转换站点”进行转换 证书转换站点：
https://myssl.com/cert_convert.html
取 消
确 定

1.10 操作类

Q1

如何判断域名配置生效？

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？

A3

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。