

天翼云

1

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	上产品定义	3
操作指导	₹	4
1.2	2 控制台说明	4
1.3	3 快速入门	5
1.4	1 域名管理	12
1.5	5 安全分析	15
1.6	5 告警管理	17
1.7	7 业务分析	18
1.8	3 计费详情	19
1.9) 证书管理	19
常见问是	逦	21
1.1	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** e Cloud

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。

4

DDoS 高防控制台概览页:



下面逐一介绍概览页的模块展示:

- 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:

天英石 控制中心 服务列表 ・ 收藏 ・ ① 中文 ▼ ② ① □ 中文 ▼ ③ □ 中文 ▼ ③ □ 日本開始や全高可像化粉的存储服务器 □ 日本開始や全高可像化粉的存储服务器	兰州2 (P)	iwei7@chinateleco
	ġ.	共享带宽(0) 提供地域级带宽共享和复用能力
₩ 弹性伸缩服务 自动调整计算资源		弹性负载均衡 多台服务器间自动流量分发
安全 >		VPN连接(0) 远程安全接入VPC网络
管理与部署 > 版务器安全卫士(基础版) 全方位服务器安全保护服务	B	云间高速(标准版) 跨资源池云主机高速互联
→ 云监控 资源监控,告警通知 ◆ 终端杀毒 云主机云桌面病毒查杀	VPN	云间高速(尊享版) 跨资源池云主机高速互联
ご解析 DNS収成解析服务 应用市场 〜	R	云专线 用户本地数据中心与VPC专线互联

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:

			7		
域名接入 端口接入			-		
状态 请下拉选择	* 1028	请下拉选择			8ff 100 14
城名。	CNAME	四层防护	CC防护	状态	操作
	m 0	开启		• 启用	网站配置 防护配置 仲用 用
		开启		• 启用	网站配置 防护配置 启用 書
o	đ	开启		• 停用	网站配置 防护配置 停用 書
		开启	(T))	• 配置曲	网站配置 防护配置 店用 景

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:

首页 〉 业务接入 〉 域名接入 〉 域名接入

基本信息	
* 产日	高防DDOS (边缘云版) V
* 域名	
请求协议	
* 请求协议	HTTP HTTPS
服务端口	HTTP 80
回源配置	
* 源站	多个请用源站换行隔开
回源HOST	请输入回源HOST
回源协议	● HTTP ○ HTTPS ○ 跟随协议
回源端口	HTTP 80
	和定期以

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】。

域名接	入 端口接入						
转发端[□ 多端口查询以分号隔3	开题	8 多源站查询以分号	二 开 查询			
CNAME	duanlei.8686c.com	 				新增规则 删除	修改 导出
	转发协议	转发端口	源站端口	回源转发模式	源站	配置状态	操作
~	TCP		80	轮询		• 完成	修改 删除
	TCP		81	轮询		 完成 	修改 副除
	TCP		83	轮询		 配置中 	修改 删除
	ТСР		80	轮询		 配置中 	修改 删除
					< 🔳	2 3 4 5 > 10条/页	跳至 1 页

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:

新增规则	批單新增	×	新增规则	域名接入		
 温馨排 不支持 的防持 	最示 亦80、8080、443、8443第口的靖口接入配 户,建议您使用"域名投入",	置,关于以上述接口	 温馨 不支 的防 	提示 持80、8080、44 护,建议您使用" *	3、8443赌口的蜡口接》 观名接入"。	、配置,关于以上述接口
②类型 愛端口 ◎	TCP UDP			81 81 1.1.1.1		+ 导入TXT文件
原站发模式	轮询模式					
9占			 每行对应- 2、每行包含 间以空格分前 3、转发端口 	-条规则、多条现) 四个字段、从左到 1。 唯一值、罩站端口	则进行换行。 右依次时协议、转发端[、避站可多个、用、号4	

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:

咸名接入	端口接入							
状态	请下拉选择	*	域名	请下拉选择	• 查询		8fi1	销域 名
城名 🕫		CNAME		四层防护	CC防护	状态	操作	
	m B	ch	m 🖪	开启		• 启用	阿站配置 防护配置 停用	HI P
	n B	chei	m G	开启		 。 <	网站配置 防护配置 启用	ang pa

T	翼7	=							
	Clou	ıd				1			
						_			
		域名接入	端口接入						
	^	转发端口	多端口查询以分号隔开	源	站 多源站查询以分号隔开	盘访			
	1	CLAME	duanlei.8686c.com)			新婚规则	修改 导出
	^		转发协议	转发端口	源站端口	回源转发模式	源站	配置状态	操作
			TCP	80	80	轮询	1.1.1.1	 完成 	修改 删除

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:

别名 (CNAME)(最多允许20条)	别名主机	TTL	操作	帮助
一共有0行,当前第1/0页,每页20行 首页 」	上一页下一页尾页到 页确定			
		3600		
漆加新的别名		提交 主:	只提交新加纪	录
域名前缀	控制台复制来的	りCNAME値		

【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:

C:\Windows\system32\cmd.exe
C:\Users\>ping
正在 来自 49.7.104.25 mprox 2. 字节-32 时间=9ms TTL=55 来自 49.7.104.25 的回复: 字节-32 时间=11ms TTL=55 来自 49.7.104.25 的回复: 字节=32 时间=11ms TTL=55 来自 49.7.104.25 的回复: 字节=32 时间=7ms TTL=55 来自 49.7.104.25 的回复: 字节=32 时间=5ms TTL=55
49.7.104.25 的 Ping 统计信息: 数据包: 己发送 = 4, 己接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 5ms,最长 = 11ms,平均 = 8ms
C:\Users

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	Α	URL	МХ	тхт	ΑΑΑΑ	SRV	CAA
NS	可重复	х	x	х	х	x	х	x	х
CNAME	x	可重复	x	х	х	x	х	x	x
А	x	х	可重复	х	无限制	无限制	无限制	无限制	无限制
URL	x	х	x	х	无限制	无限制	х	无限制	无限制
MX	x	х	无限制	无限制	可重复	无限制	无限制	无限制	无限制
ТХТ	x	х	无限制	无限制	无限制	可重复	无限制	无限制	无限制
CAA	x	х	无限制	无限制	无限制	可重复	无限制	无限制	无限制
AAAA	x	х	无限制	x	无限制	无限制	可重复	无限制	无限制
SRV	x	х	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

12



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

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

图 Http:// duanlei.8	686c.com 🗸 🗸		NX (M)
基本信息	基本信息 域名:duanlei 创建时间:202	8686c.com CNAME: duanlei.8686c.com.ctdns.cn 域者 1/12/08 12:23:53	5状态:已启用
请求协议 HTTP响应头 回源HTTP请求头	 回源配置 源站 ○ 回源协议 回源端口 	x000000000000000000000000000000000000	
	请求协议 请求协议 服务端口 ©	2 HTTP HTTPS HTTP 80	
	证书 ③ 强制跳转 ③ HTTP响应头	请下拉选择 / 二 上他文件 	新地
	参数	取值	操作

1.4.2 防护配置

大

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:

业劳论入 / 域名论入 / 配面前荷	P
网络配置 防护配置	
Http:// www.philling.com	
CC防护股票	59(E
防护开关 (井)	
防护機式 ③ ③ 网络	
检测条件 在5秒内,第5000个属实开始进行防护	
853991K-O 7200 Ø	



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

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

1.5.3 CC 攻击事件

名全部	昨天 🥎	天 7天 30天	开始时间 2021-12-02	12:25:28 童 信束时间	2021-12-02 12:25:28	回 重狗 号出
序号	被攻击域名	攻击开始时间	攻击结束时间	攻击峰值/OPS	攻击总次数	操作
1		2021/12/02 12:23:35				# #
2		2021/12/02 12:23:35				25
3		2021/12/02 12:23:35				88
4	λ	2021/12/02 12:23:35				88



天翼**云** e Cloud

CC攻击事(件 网络层攻击事件					
昨天	今天 7天 30天	开始时间 2021-12-02	12:25:28	时间 2021-12-02 12:25:28	111 111 1111	
序号	攻击开始时间	攻击结束时间	攻击峰值带宽	攻击峰值时间	被攻击域名	操作
1	2021/12/02 12:25:35	2021/12/02 12:27:35				直看
2	2021/12/02 12:25:35	2021/12/02 12:27:35				查看
3	2021/12/02 12:25:35	2021/12/02 12:27:35				查看
4	2021/12/02 12:25:35	2021/12/02 12:27:35				直看
				< 1	2 3 4 5 > 10蔡/3	页 跳至 1 页

1



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

告警官地	■ / 告警策略					*
告鑒	新增				×	
告璧	* 告警名称	请输入告警名称		*告警状态		
	* 告警类型	请选择 ~				新聞
序制	* 告警通知间隔		分钟			操作
	勿扰时间	© 开始时间	至 结束时间			
	* 告警邮箱				4	
7.			新增。返回			

天翼 亡 e Cloud				1					
	告警记录	快列表页		_					
告警管理/ 台	持警记 录								P
告警名称 告警原因	请输入告警谷称 请输入告警册因	Ě	域名	前述評議名 ✓ ○ 2022-06-01 00:00:00 至 董師	告警类型 2022-06-01 23: 清 空	请选择 59:59	~		
告輩	附间	告警名称	ł	域名 告醫类型 暫无過	牧据	产品类型	告警原因	告警邮箱	操作

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;

选择域名 请送	选择	✓ 日期选择 开始日期 至	· 结束日期		
■ 序号	域名任务	提交时间	完成时间	文件大小	操作
1	w	2021/08/12 09:24:45	2021/12/12 09:24:45	1.25G	下载
2	uni financia.cn	2021/07/23 09:24:45	2021/11/23 09:24:45	345MB	下戰
3	xx ^l (j	2021/06/30 09:24:45	2021/10/30 09:24:45	678MB	下载
4		2021/06/01 09:24:45	2021/10/01 09:24:45	780MB	下载

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。

ouu		1				
业务分析 / 业务用量		_				4
全部业务 > 全部	 > 运营商 全部 		地区 全选	8 V		
昨日 今日 7天	30天 ③ 2022-04-23 0	0:00:00 至 2022-04-2	29 23:59:59	查询		
带宽 流量				峰值带宽:	0.00Mbps 总	总流量: 0.00GB
创立: Mbps 1						
0.8						
0.6						
0.4						C
0.2						<mark>0</mark> - الا
22/04/23 00:00:00 2022/04/23 23	:55:00 2022/04/24 23:50:00	2022/04/25 23:45:00	2022/04/26 23:40:00	2022/04/27 23:35:00	2022/04/28 23:30:00	9 2022/04 建 议
青求次数 QPS						总请求数:0次

1.8 计费详情

記

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。

套餐规格					
套餐内容	套餐详情	生效时间	到期时间	状态	5
DDoS高防(边缘云版)	业务带宽峰值: 50 kbps 主域名个数: 1 个 子域名个数: 9 个 端口个数: 5 个 防护带宽: 1Gbps CC防护: 10000 QPS	2021-11-16	2051-12-16	服务	5中
扩展服务					
扩展服务	服务内容	生效时间	到期时间	状态	操作
业务带宽	业务带宽峰值: 60 kbps	2021-11-16	9999-12-31	服务中	查看详情
端口数量	端口个数: 10 个	2021-11-16	9999-12-31	服务中	查看详情
域名数量	主域名个数: 1 个 子域名个数: 9 个	2021-11-16	9999-12-31	服务中	查看详情

您目前最高可防护 11Gbps,6010000 QPS,若防护超过购买的的最高防护量,则通过解析回源,2小时后自动解封。

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 ~ ① 开	始时间 至 结束时间	查询 添加	正书	
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		

2

新增证书页:

	VII G JI		纪末时间	
新增自有证书				×
* 证书备注名				
* 证书公钥(PEM格式)	请输入			1.
* 证书私钥(PEM格式)	请输入			li
温馨提示 证书公/私钥,目前只支持PEM格式 https://myssl.com/cert_convert.h	,其他格式请前往"证书 t <mark>ml</mark>	转换站点"进行转换 证书	5转换 站点:	
	取消	确定		



常见问题

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。

2

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。