天翼云·DDoS高防 IP

用户使用指南

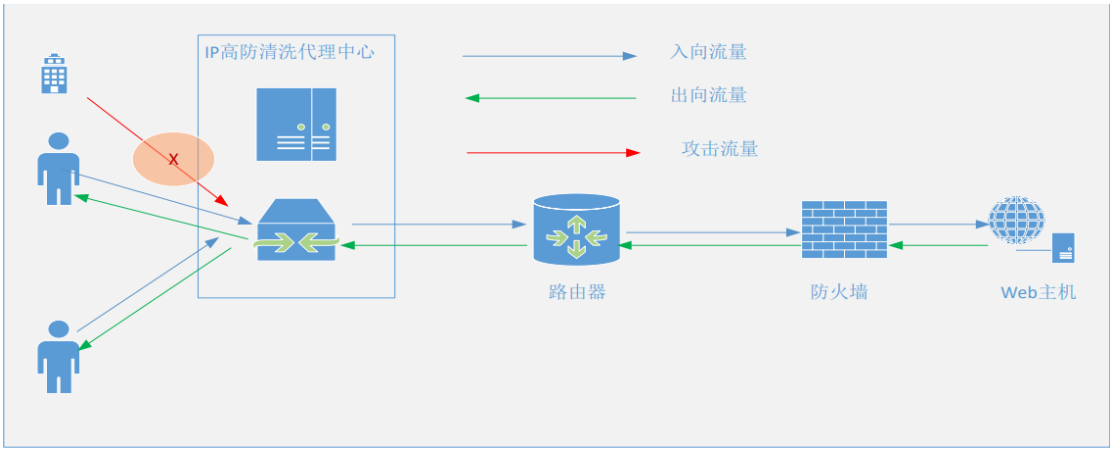
天翼云科技有限公司

目录

1. 产品介绍

1.1 产品定义

DDoS 高防 IP：DDoS 高防 IP 是针对互联网服务器在遭受大流量的攻击后导致服务不可用的情况下，推出的付费增值服务，用户可以通过配置高防 IP，将攻击流量引流到高防 IP，确保源站的稳定可靠。采用替身防御模式，接入防护后，业务 IP 返回的是天翼云高防节点 IP，源 IP 将不再暴露，彻底阻断针对源 IP 的攻击，确保源 IP 安全。



1.2 产品优势

针对 DDoS 高防的部署环境的灵活性

DDoS 高防的使用无需客户业务支撑主机为天翼云，任何厂商的主机均可以使用天翼云 DDoS 高防 IP 产品，客户只要有公网域名或公网 IP 地址均可以使用。

DDos 高防灵活的基础弹性带宽

DDoS 高防支持弹性防护带宽，当攻击流量超过保底防护带宽后将触发弹性带如未宽触发将不进行收费，以此可作为客户的弹性保障。

1.3 功能特性

采用替身防御模式，接入防护后，业务 IP 返回的是天翼云高防节点 IP，源 IP 将不再暴露，并且可 以对源地址做 ACL 控制，只有开通 ACL 策略的地址才能访问源地址，彻底阻断针对源 IP 的攻击，确 保源 IP 安全。

DDoS 防护

畸形报文过滤（过滤 FRAG flood，SMURF，STREAM flood，LAND flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包等）、传输层攻击防护（过滤 SYN flood，ACK flood，UDP flood， ICMP flood，Rstflood）、CC 攻击防护。

高防 IP 动态接入

产品分单点接入和动态接入，若用户选择动态接入，则系统为用户分配一个动态高防 IP，此 ip 可以在多个高防中心（华北 1、华东 1、华东 2）使用，实现高防 IP 负载调度的近源清洗。

隐藏源 IP

采用替身防御模式，接入防护后，业务 IP 返回的是天翼云高防节点 IP，源 IP 将不再暴露，并且可 以对源地址做 ACL 控制，只有开通 ACL 策略的地址才能访问源地址，彻底阻断针对源 IP 的攻击，确保源 IP 安全。

详细运行日志

提供清晰详细的攻击日志及防护报表，攻击报表支持手动导出。

告警通知

可以设置联系人，当源地址发生攻击时系统自动发送邮件和短信通知。

1.4 应用场景

场景 1：电商购买

某电商平台在遭受 DDoS 攻击时，网站无法正常访问甚至出现短暂的关闭，导致合法用户无法下单购买商品等，导致客户体验感降低用户量流失，如使用 DDoS 高防 IP 即可将攻击流量进行清洗区分将正常用户的流量进行放行的同时将攻击流量进行有效规避。

应用场景 2：数据泄露

部分客户在网站收到大规模 DDoS 攻击导致网站业务不可用的同时黑客可能会趁机窃取您业务的核心数据导致业务，导致部分用户以及网站信息的泄密，如使用 DDoS 高防可有效将异常流量隔绝在外避免黑客趁机窃取网站业务数据。

应用场景 3：恶性竞争

部分行业存在恶性竞争，竞争对手可能会通过 DDoS 攻击恶意攻击您的服务，从而在行业竞争中获取优势，某游戏业务遭受了 DDoS 攻击，游戏玩家数量锐减，导致该游戏业务几天内迅速彻底下线，ddos 攻击主要集中于游戏行业，鉴于游戏行业数据以及业务实时性较高短时间的服务停止将引起用户的极大不满，可通过 DDoS 的清洗策略将针对带宽占用进程占用攻击进行有效清晰避免因带宽占用瓶颈导致无法提供正常服务。

应当避免的事项

DDoS 攻击是业内公认的行业公敌，DDoS 攻击不仅影响被攻击者，同时也会对服务商网络的稳定性造成影响，从而对处于同一网络下的其他用户业务也会造成损失。
计算机网络是一个共享环境，需要多方共同维护稳定，部分行为可能会给整体网络和其他租户的网络带来影响，以上问题均可通过 DDoS 高防产品接入通过内置的 DDoS 清洗策略进行防护，避免攻击问题导致进一步造成业务的重大损失。

1.5 名词解释

DDoS 攻击

分布式拒绝服务（Distributed Denial of Service，简称 DDoS ）将多台计算机联合起来作为攻击平台，通过远程连接利用恶意程序，对一个或多个目标发起 DDoS 攻击，消耗目标服务器性能或网络带宽，从而造成服务器无法正常地提供服务

常见的 DDoS 攻击包括以下几类：

网络层攻击

比较典型的攻击类型是 UDP 反射攻击，例如 NTP Flood 攻击。这类攻击主要利用大流量拥塞被攻击者的网络带宽，导致被攻击者的业务无法正常响应客户访问。

传输层攻击

比较典型的攻击类型包括 SYN Flood 攻击、连接数攻击等。这类攻击通过占用服务器的连接池资源从而达到拒绝服务的目的。

会话层攻击

比较典型的攻击类型是 SSL 连接攻击。这类攻击占用服务器的 SSL 会话资源从而达到拒绝服务的目的。

应用层攻击

比较典型的攻击类型包括 DNS flood 攻击、HTTP flood 攻击（即 CC 攻击）、游戏假人攻击等。这类攻击占用服务器的应用处理资源，极大地消耗服务器计算资源，从而达到拒绝服务的目的。

攻击原理

通常，攻击者使用一个非法账号将 DDoS 主控程序安装在一台计算机上，并在网络上的多台计算机上安装代理程序。在所设定的时间内，主控程序与大量代理程序进行通讯，代理程序收到指令时对目标发动攻击，主控程序甚至能在几秒钟内激活成百上千次代理程序的运行。

2. 计费说明

2.1 计费模式

DDoS 高防 IP 有 DDoS 流量防护能力、回源带宽费用、防护域名费用、防护端口费用 4 部分组成。

DDoS 流量防护能力费用：

DDoS 防护能力	静态高防		动态高防	
	包月 （元/月）	按需 （元/天）	包月 （元/月）	按需 （元/天）
10Gbps	4400	-	5720	-
20Gbps	8400	1200	10920	1500
30Gbps	13400	1900	17420	2500

40Gbps	23400	3300	30420	4300
50Gbps	33400	4800	43420	6200
60Gbps	43400	6200	56420	8000
70Gbps	53400	7600	69420	9900
80Gbps	63400	9000	82420	11800

以下规格，仅支持包年与按需订购：

DDoS 防护能力	静态高防		动态高防	
	包年 (元/年)	按需 (元/天)	包年 (元/年)	按需 (元/天)
100Gbps	139400	9200	181200	12000
300Gbps	224400	11000	291700	14300
400Gbps	411400	20200	534800	26200
500Gbps	1595300	55000	2073900	82500
600Gbps	1898800	64000	2468300	96000
700Gbps	2181800	74000	2836300	111000
1000Gbps	3029400	104000	3938200	135000
1500Gbps	4249800	145000	5524800	189000

（1）回源带宽费用：

回源带宽	≤100M	> 100M
定价	免费	100 元/M

默认 100M 回源带宽，增加步长为 50M，最大为 300M。

（2）防护域名费用：

防护域名	≤50 个	> 50 个
定价	免费	20 元/个

默认 50 个域名；增加步长 5 个，最大 200 个。

（3）防护端口费用：

防护端口	≤50 个	> 50 个
定价	免费	50 元/个

默认包含端口数 50 个，增加步长为 5 个，最大支持 100 个。

2.2 订购

1、 登录天翼云账号，在产品列表中找到安全组下的 DDoS 高防 IP，点击

如下按钮跳转订购页面。

2、 1）确认高防节点，当前提供了华北 1 和华东 2 两个节点。

华北 1：可以选择任意端口进行转发

华东 2：网站类业务： 支持 80,8080,8081,443,7443,8443；非网站类业务：可以选择任意端口进行转发；

2）选择业务类型，网站类业务需要填写域名个数。

3）选择保底防护带宽和弹性防护带宽，保底防护带宽包月计费，弹性防护带宽设置需要高于保底防护带宽值，在 DDos 攻击突破保底带宽值后触发弹性防护，进行 2 小时压制，1 次触发 24 小时有效。

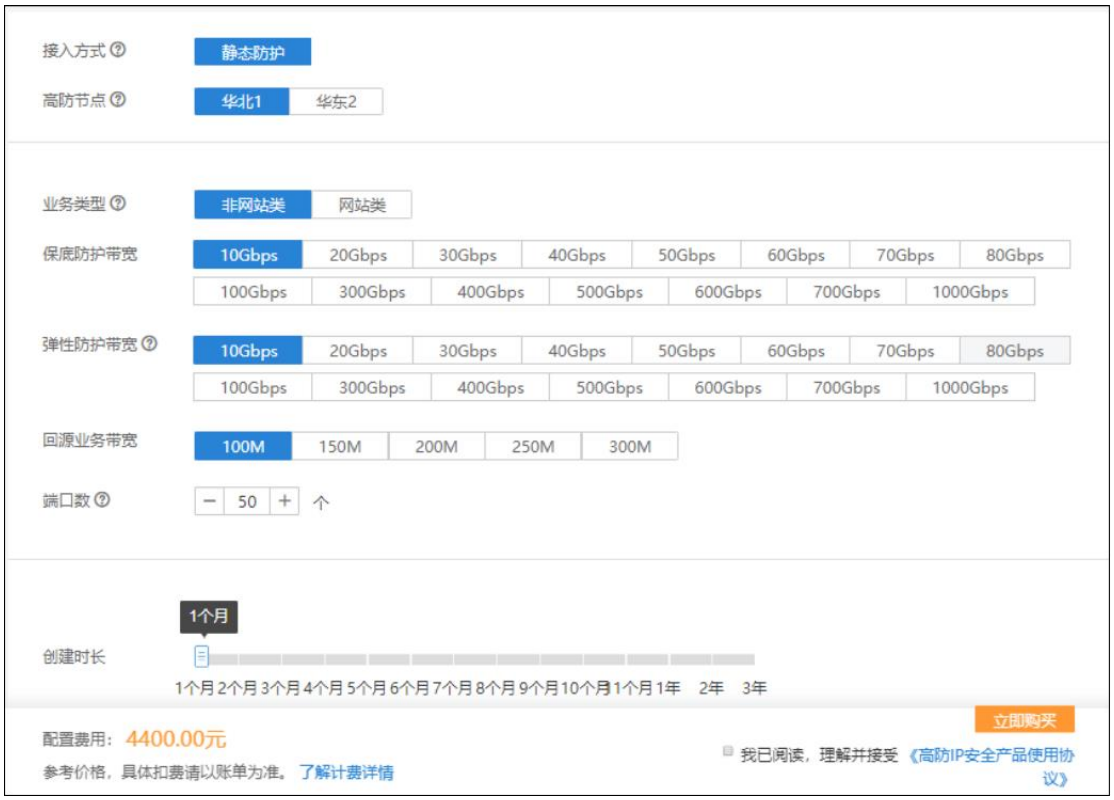
注：100Gbps 以上带宽只能包年订购。

4）设置回源带宽

5）设置端口数

6）选择订购时间

勾选协议，点击【立即购买】。



2.3 续订及退订

在产品实例列表点击【续订】，跳转续订页面，页面显示当前订购的产品规格，选择增购的时间，点击【立即购买】

天翼云

续订高防IP

资源信息

*资源ID：c770c2ff67db44f5bfc983f1bbb01a8d

*接入方式：单点防护

*高防节点：华北1

*保底防护带宽：10Gbps

*业务类型：非网站类

*回源业务带宽：100M

*端口数：20个

续费信息

1个月

*续费时长：1个月 2年 3年

配置费用：

¥ 4400.00元

立即购买

我已阅读，理解并接受 《高防IP安全产品使用协议》

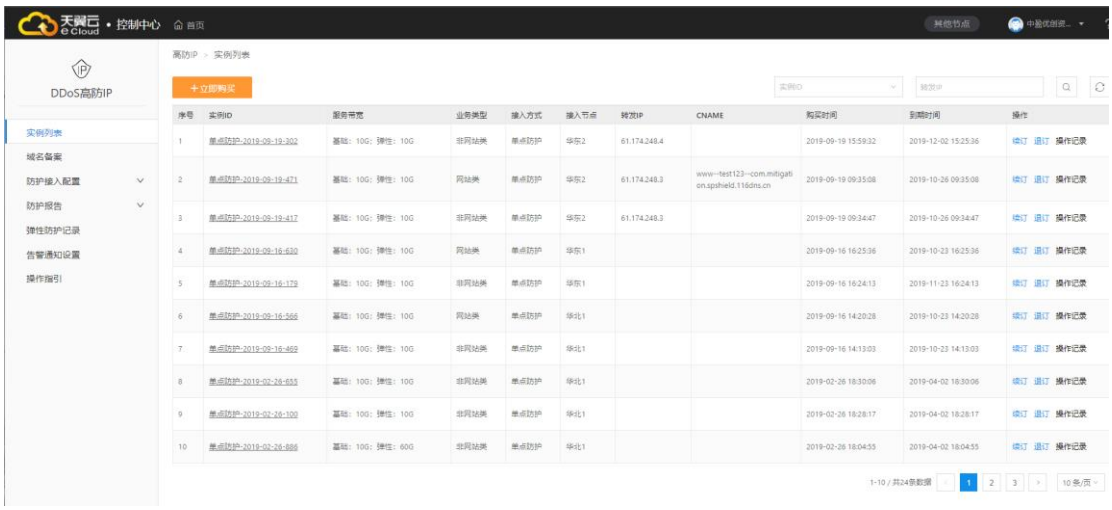
退订

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. 快速入门

3.1 实例列表

收到公测申请创建成功的通知后，重新登录天翼云控制中心下的高防 IP，点击【高防 IP】菜单，页 面显示客户购买的高防 IP 防护实例。购买后的实例可以续订及退订，用户新增高防 IP 防护时必须选择已经购买的实例 ID。



用户通过 BSS 购买高防 IP 实例后， BSS 通过接口把数据传送给高防 IP 自服务。相关信息通过实例

列表进行展示，具体字段如下：

实例 ID：用户购买的实例 ID；

服务带宽：用户购买的防护带宽，包括基础带宽和弹性带宽。基础带宽采用包月形式收费。弹性带

宽按次收费，触发一次收费一次，24 小时内只触发一次弹性带宽费用；

业务类型：分为网站类和非网站类。

是否 BGP：非 BGP 节点，为单节点高防 IP。BGP 节点，在多个高防中心（华北 1、华东 1、华东 2）

都会生成一个 IP（同一个 IP），可以实现高防 IP 负载调度的近源清洗；

接入方式：包括华北 1、华东 1、华东 2；

代理地址：包括 cname 和代理 IP，网站类的防护为 cname，非网站类防护是代理 IP；

购买时间：实例购买时间；

到期时间：实例的到期时间；

端口（限制）：

源站 IP 限制为 20 个以内含 20 个；源站端口根据选择的防护节点有如下规则：

华北 1：可以选择任意端口进行转发

华东 2：网站类业务： 80,8080,8081,443,7443,8443 之一；非网站类业务：可以选择任意端口进行转发；

3.2 地址备案申请

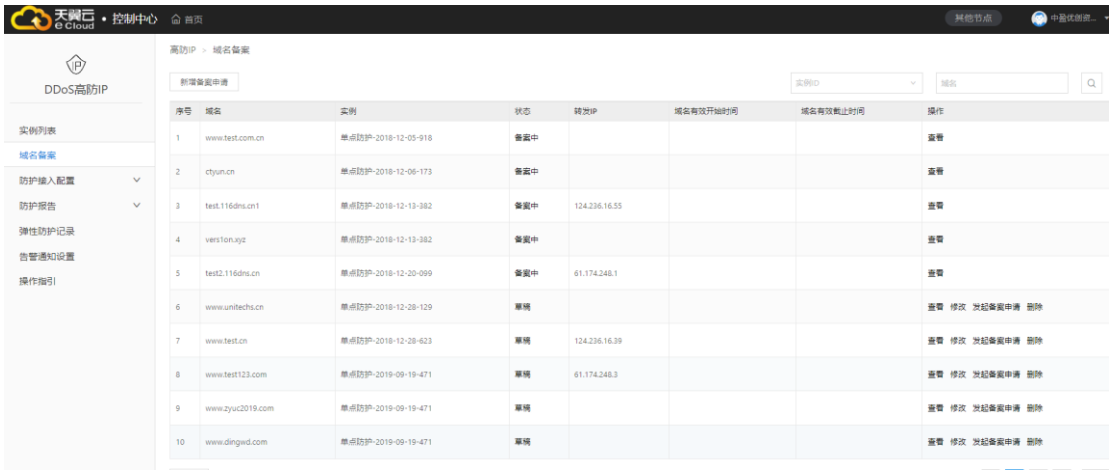
- 域名：展示被防护的域名，例如；www.ctyun.com
- 实例：展示购买的实例 ID
- 转发 IP：域名备案后高防 IP 自动分配一个地址
- 域名有效开始时间: 域名有效的开始时间
- 域名有效截止时间: 域名有效的截止时间，新建防护时网站有效时间必须在截止时间以前，否则

不允许防护

状态：备案中、已备案、备案失效

操作：对于提交备案尚未通过的网站，可以对备案信息进行查看、修改、删除；对于已经备案成功的网站，只有查看按钮；

若需要发起备案，点击新增备案申请按钮，如图所示：

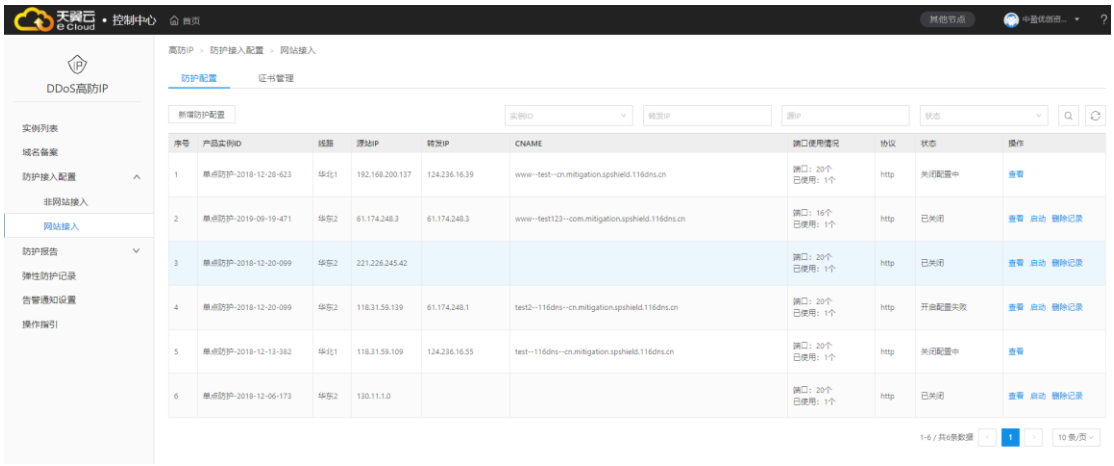


点击新增备案申请后弹出地址本案申请窗口：

输入相关信息后，点击确定，完成备案地址的提交工作，之后域名备案管理员（天翼云负责人）审批通过后用户可以开始进行网站防护；

3.3 防护接入管理

3.3.1 Web 网站接入



如果是 Web 网站接入，必须进入 Web 网站接入设置二级菜单；

字段包括：序号、实例 ID、线路、源站域名（唯一）、转发 IP 及 cname、端口使用情况（端口；已使用）；协议（http、https、https 和 http）、端口映射（源 ip：端口—转发端口）、acl 控制（状态+操作申请按钮）、状态（防护配置下发中、防护配置生成中、已生效、已关闭、下发关闭中、下发关闭失败）、操作（查看、修改、删除、关闭）

修改：web 网站接入修改展示不提供

查看：查看已经创建的防护信息

删除：对停止的的记录可以进行删除

关闭：停止的记录方可进行删除，点击停止时提示如下信息：

请确保

1、请先申请撤销原有 acl 控制，待 acl 控制失效后才可以关闭防护 *（如果没有 acl 控制则该条目）*

2、将 DNS 解析指回源站，或者将源站 IP 设置重置回防护前状态，否则流量将丢失

删除时，提示： 删除操作将删除防护配置和防护的历史数据

关闭状态下：对应状态为启动同一实例下生效的配置只有由一个，当创建新的防护接入配置时，该实例不能被选中停止、删除：停止调用天翼云接口删除业务配置，运营平台本身保存配置

点击新增防护配置：

选择实例（需为网站实例）、选择域名（在地址备案管理中已查到备案信息的域名）、线路、转发

IP、防护带宽、源站 IP（需要对源站 IP 限制，最多 20 个，？显示源站 IP 限制最多 20 个）、端口映 射（鼠标落在？上时，根据不同的线路显示不同，分别为“华北 1：可以选择任意端口进行转发；华东 1：网站类业务：限制输入 80 和 443 端口；华东 2：网站类业务： 限定选择 80,8080,8081,443,7443,8443 之一；

同时提示：如果转发 IP 映射端口相同，则采用负载均衡方式转发业务流量值源站”，填写端口映射关系，源站 IP+端口必须唯一，转发 IP 映射端口）、协议类型（https、http，

可同时选择，选择 https 时必须选择证书，如果没有证书必须新增证书并选择）；点击确认后：调用云堤用户配置接口并合入域名信息。

点击查看时：显示转发 IP、cname

ACL 控制：

天翼云完成防护配置后（Web 网站类对域名重新进行 IP 备案后），通过异步通知接口通知，状态变为已生效。

状态已生效后，为避免对源站 IP 的攻击，请在天翼云虚拟私有云控制中心进行 ACL 设置，限制源站

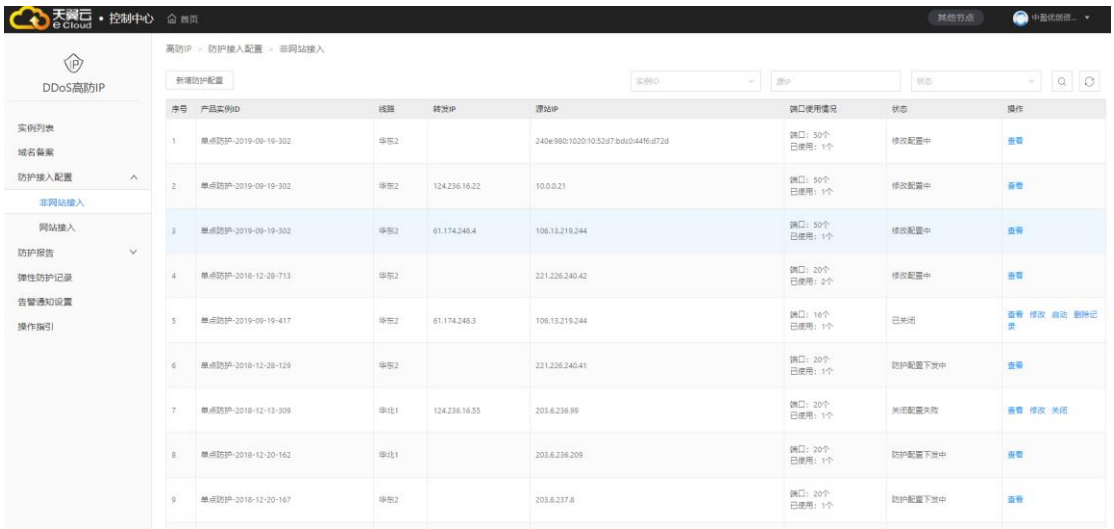
IP（XXX.xxx.XXX.XXX、XXX.xxx.XXX.XXX）除了转发 IP 外的任意访问。

HTTPS 证书管理：

在 web 网站接入中通过 tab 页来进行展示

3.3.2 非网站接入

非网站接入配置与网站接入方式基本一致，但是不需要选择备案的域名，其防护的地址为 IP。



非网站接入：

可以对端口可以进行增加、删除等修改操作。

可以设置任意转发端口；

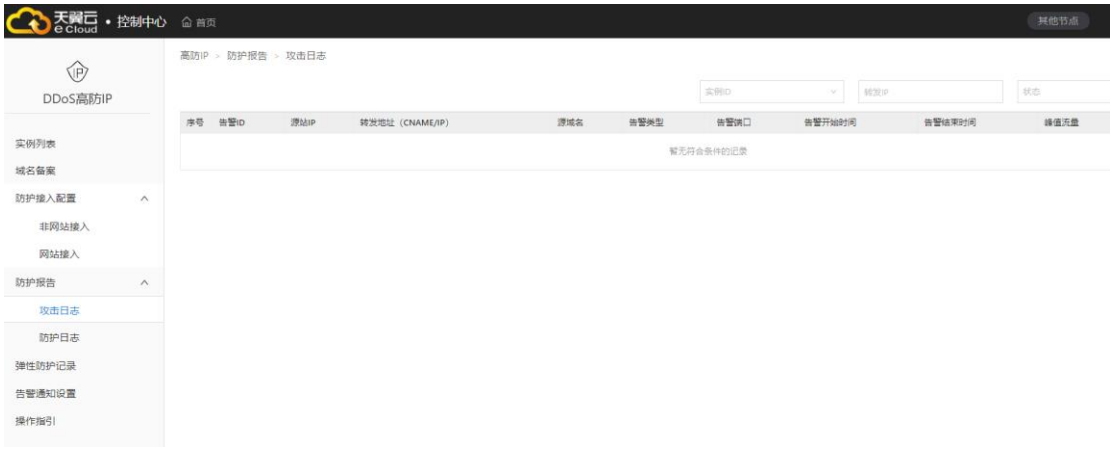
源站 IP 超过 20 时报错，提示： “源站 IP 超过范围，限制为 20 个以下”。

非网站接入可以进行修改，对源站 IP、端口进行修改。

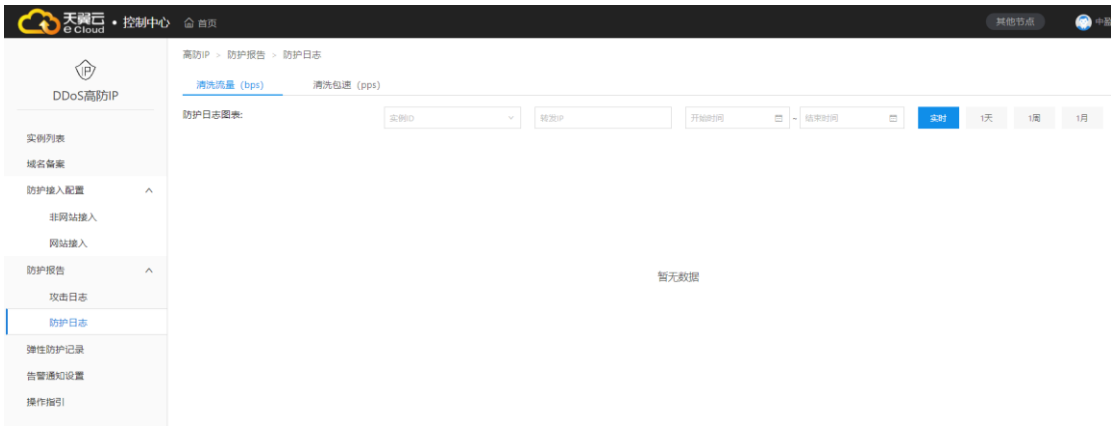
3.4 防护报表及告警

防护报表及告警下有两个菜单，分别是告警管理、防护报表

3.4.1 告警管理



告警列表：序号、告警 ID、源 IP、转发地址(如果为域名时，展示 CNAME 和 IP)、源域名、告警类型、告警端口、告警开始时间、结束时间、峰值流量（根据防护数据的流量值，展示告警开始到当前时间，如果已结束的为结束时间的峰值流量），状态（普通清洗、弹性清洗、压制中、已结束） 压制的状态由天翼云接口同步；弹性清洗由峰值流量超过基础防护值判断。

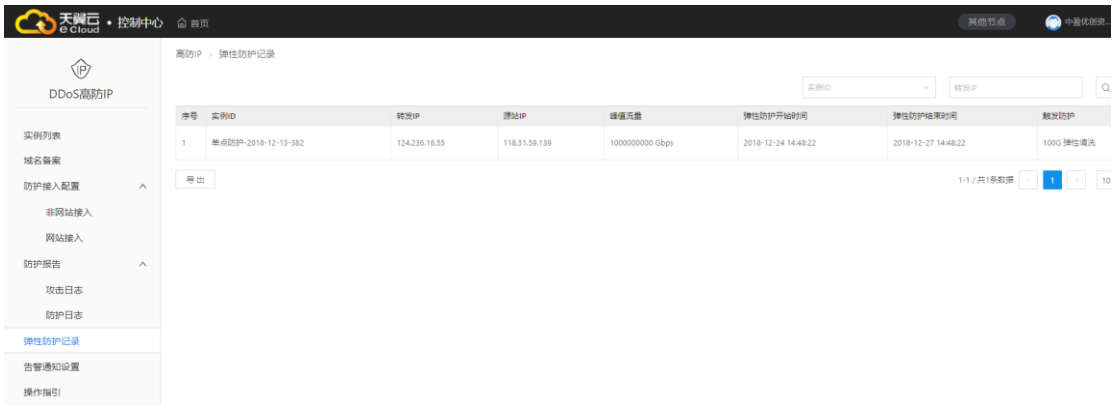


3.4.2 防护报表

分 tab 显示清洗流量（bps）、清洗包速（pps）

查询项为：实例列表、转发 IP、时间段（最长 24 小时区间，最多选择 1 个月内的）；实时（默认实 时，同时可以选择一天、一周、一月）页面不能展示所有打点信息，如果一天、一周、一月，去打点周期内的峰值流程数据。

3.5 弹性付费记录

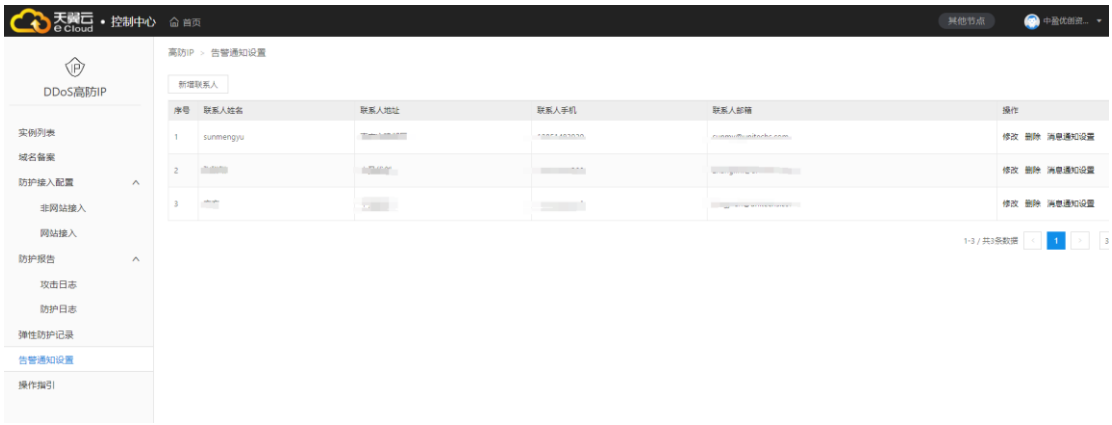


当用户触发 24 小时弹性防护时，触发记录。

弹性防护为：24 小时有效，超过 24 小时重新记录。

时间：为系统对业务流量进行监控，超过基础防护时触发防护弹性防护（如用户未购买弹性防护，则不产生弹性防护及弹性防护收费）计开始时间，+24 小时为结束时间。

3.6 告警通知设置



系统提供告警联系人功能，源地址发生告警后可以邮件和短信通知联系人。

点击新建通知联系人按钮，弹出通知联系人窗口，输入姓名、角色、手机号、邮箱后点击确定完成联系人添加。

消息设置

告警需要给设置的账号进行发送短信、邮件；

需要给登录的账号（账号为邮箱）发送邮件；

默认不选，由用户勾选；

短信模板：

攻击告警：

开始：“尊敬的客户，您的防护 IP{源站 IP}在 XX 时间被攻击，请关注，感谢您的使用，中国电信天翼云”；

结束：“尊敬的客户，您的防护 IP{源站 IP}已于 XX 时间结束告警，感谢您的使用，中国电信天翼云”

流量超出防护带宽：

“尊敬的客户，您的防护 IP{源站 IP}于 XX 时间攻击流量超过防护带宽上线{XXGbps}，进入压制状态，感谢您的使用，中国电信天翼云”；

“尊敬的客户，您的防护 IP{源站 IP}于 XX 时间攻击流量超过基础防护带宽{XXGbps}，进入弹性防护，感谢您的使用，中国电信天翼云”；

转发 IP 分配完成：

“尊敬的客户，您的{实例 ID}实例下申请的高防 IP 已与{XX 时间}分配且配置完成，为{转发 IP}，现在您可以将业务流量指向转发 IP 或者 cname 完成高防 IP 的设置，登录天翼感谢您的使用，中国

电信天翼云；

实例到期：

提前 7 天、3 天、1 天上午 9:30 分发送到期信息

“尊敬的客户，您的防护实例{XXXX}将于{XX}时间到期，请您尽快处理，截止到期时间未续订，届时实例下的域名监控配置将停止，感谢您的使用，中国电信天翼云”。

Acl 控制设置：

“尊敬的客户，您的防护实例{XXXX}的转发{转发 IP}已限制为只允许防护 IP{源站 IP}访问，acl 设置已完成，感谢您的使用，中国电信天翼云”。

“尊敬的客户，您的防护实例{XXXX}的转发{转发 IP}限制为只允许防护 IP{源站 IP}访问 acl 控制已撤销，感谢您的使用，中国电信天翼云”。

防护配置变更：

“尊敬的客户，您的防护实例{XXXX}的防护配置变更申请已完成配置修改，现在您可以将对源站 IP 进行设置完成高防 IP 的修改设置，感谢您的使用，中国电信天翼云”。

4. 最佳实践

DDos 攻击缓解最佳实践

建议客户通过以下方式缓解 DDos 攻击带来的影响

1. 缩小暴露面，隔离资源和不相关的业务，降低被攻击的风险。

配置安全组尽量避免将非业务必须的服务端口暴露在公网上，从而避免与业务无关的请求和访问。通过配置安全组可以有效防止系统被扫描或者意外暴露。

2. 优化业务架构，利用公共云的特性设计弹性伸缩和灾备切换的系统。

科学评估业务架构性能

在业务部署前期或运营期间，技术团队应该对业务架构进行压力测试，以评估现有架构的业务吞吐处理能力，为 DDos 防御提供详细的技术参数指导信息。

优化 DNS 解析

通过智能解析的方式优化 DNS 解析，可以有效避免 DNS 流量攻击产生的风险。同时，建议您将业务托管至多家 DNS 服务商，并可以从以下方面考虑优化 DNS 解析。

3 服务器安全加固，提升服务器自身的连接数等性能。

对服务器上的操作系统、软件服务进行安全加固，减少可被攻击的点，增大攻击方的攻击成本：

确保服务器的系统文件是最新的版本，并及时更新系统补丁。

对所有服务器主机进行检查，清楚访问者的来源。

过滤不必要的服务和端口。例如，对于 WWW 服务器，只开放 80 端口，将其他所有端口关闭，或在防火墙上设置阻止策略。

5. 常见问题

5.1 知识类

什么是 DDoS 高防 IP?

解答：高防 IP 是针对服务器在遭受大流量的攻击后导致服务不可用的情况下，推出的付费增值服务，用户可以通过配置高防 IP，将攻击流量引流到高防 IP，确保源站的稳定可靠。

天翼云 DDoS 高防 IP 购买后操作步骤?

接入防护配置设置，分配高防 IP（网站同步分配 cname），接入设置生效后进入防护配置；天翼云协 助帮你将对网站 IP 重新备案并分配 IP，该 IP 即为分配的转发 IP；完成后将在高防节点对转发 IP 进行业务设置，设置成功后将可以进入防护配置。

网站类：将域名解析重新设置指向 cname 地址。

非网站类：设置业务访问接入只转发 IP 完成防护配置。

天翼云 DDoS 高防 IP 支持 HTTPS 协议吗?

支持。

天翼云高防 IP 既支持 http，又支持 https，同时支持单个域名既有 https 又有 http。选择 https 时必须选择证书，如果没有证书必要新增证书并选择。

天翼云 DDoS 高防 IP 支持近源清洗吗?

产品分单点接入和动态接入，若用户选择动态接入，则系统为用户分配一个动态高防 IP，此 ip 可以在多个高防中心（华北 1、华东 1、华东 2）使用，实现高防 IP 负载调度的近源清洗。

天翼云 DDoS 高防 IP 需要关注的问题?

天翼云高防 IP 防护需要注意确保网站 DNS 牵引的正确性。

天翼云 DDoS 高防 IP 网站和非网站防护的区别是什么?

非网站接入配置与网站接入方式基本一致，但是不需要选择备案的域名，其防护的地址为 IP。

5.2 计费类

天翼云 DDoS否高防 IP 是付费产品吗?

天翼云高防 IP 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高防 IP 实例购买页面。

收费的标准详见天翼云 WAF 实例购买页面。

弹性带宽开通时是否收取费用?

开通弹性带宽开通资源时不会收取费用，当弹性带宽触发时会生成单独订单后需要客户侧进行支付。

防护实例过期后是否会直接终止业务?

防护资源过期后会留存客户配置一周的时间供客户进行续费。