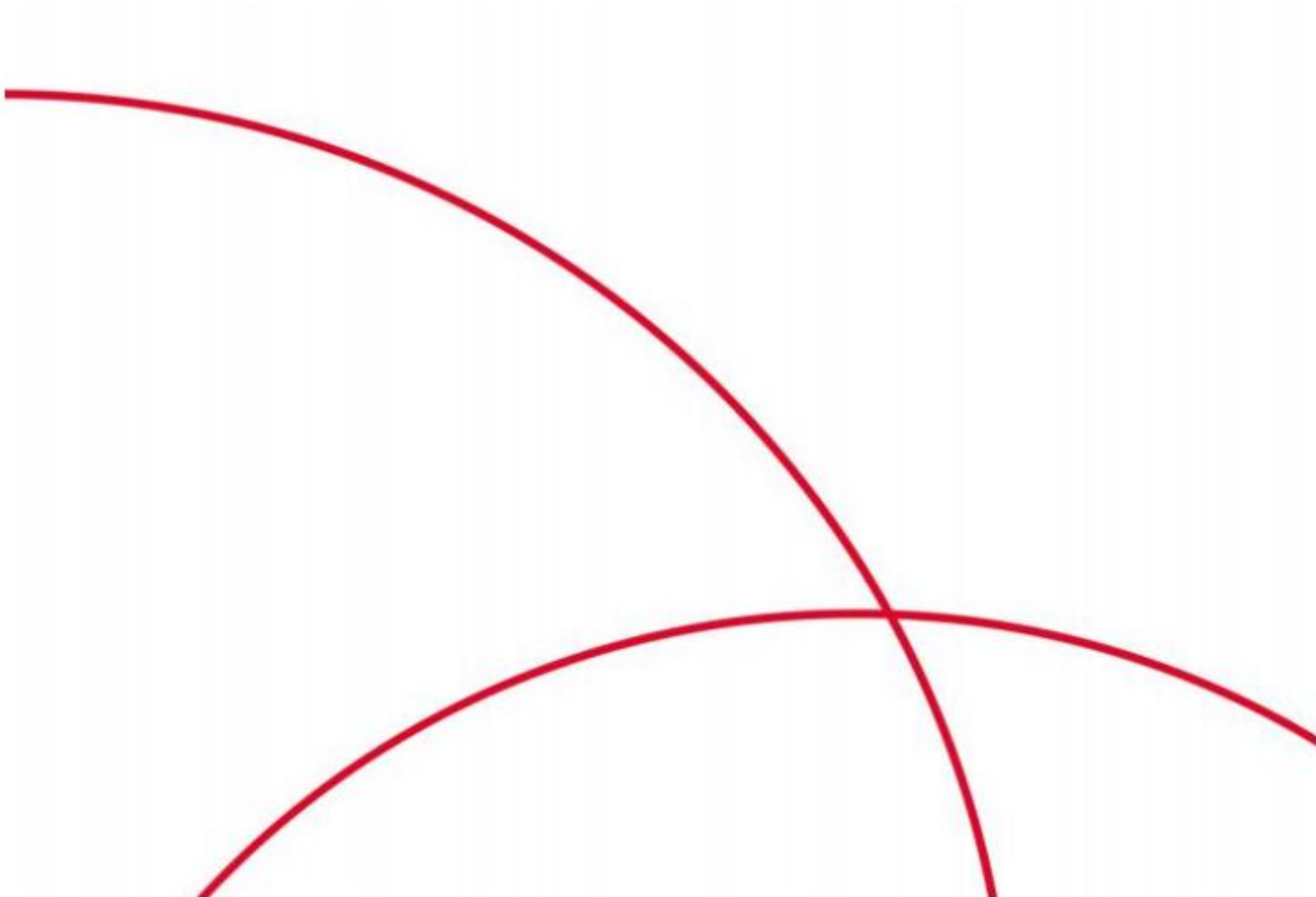
天翼云 DDoS 高防 IP

用户使用指南

天翼云科技有限公司



时间	版本	说明
2024-12-24	V1.1	更新
2024-12-20	V1.0	更新

■ **适用性声明**

本模板用于撰写天翼云科技有限公司内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

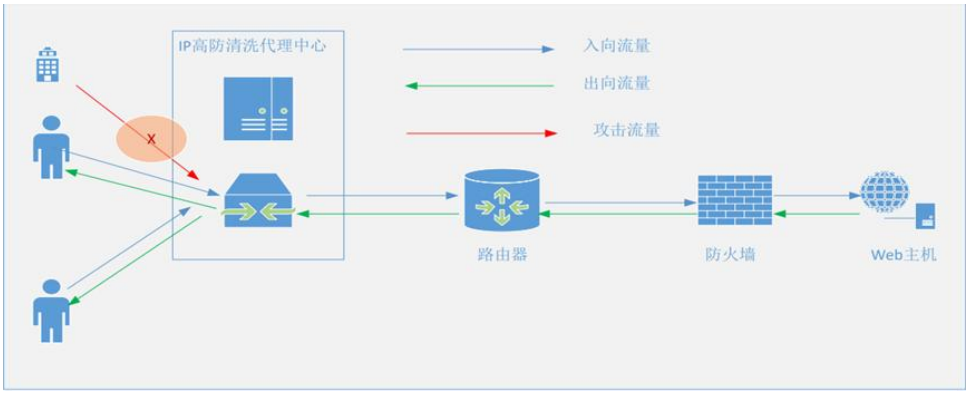
目录

一、产品简介

1.1 产品定义

“天翼云 DDoS 高防 IP”用户无需额外安装任何软件和部署硬件设备，无需人员培训，不受主备线路更换的限制，“天翼云 DDoS 高防 IP”将多个云平台业务统一配置天翼云抗 DDoS 服务，电信天翼云会为每个独立的一级域名网站提供高防解析域名/IP 地址，而后客户仅需将平台的域名 CNAME 解析更改新分配的高防服务 CNAME/IP 地址，接入高防机房平台即可享受全面的 DDoS 攻击防护服务。“天翼云 DDoS 高防 IP”依托 BGP 实现对攻击流量牵引导流的秒级全网生效，一条策略配置，全网生效。

DDoS 防护服务在客户使用流量监控服务基础之上，向用户提供“天翼云 DDoS 高防 IP”客户端、自服务界面、热线申告、邮箱申告四种服务方式。



1.2 产品优势

依托云网资源优势，结合三网线路，打造“运营商级自主专利”的高防平台，电信防护无上限，四层七层全覆盖，并叠加 DNS、国际加速、等保密评等竞品，支持 IaaS+SaaS 多元交付，可融合可定制，为各行业客户网络安全保驾护航。

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。

1.3 功能特性

全网防护：三网覆盖、DDoS 防护、流量牵引、分析溯源；

专属定制：Flowspec 定制、API 专属、IDC 定制、OTN 专属；

功能扩展：DNS 防护、国际加速、等保密评、其他扩展；

运维巡检：集约监控、智慧巡检、自助门户、威胁情报。

二、应用场景

2.1 电商购买场景

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，使用 DDoS 高防 IP 即可将攻击流量进行清洗，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。

2.2 数据泄露场景

部分客户在网站受到大规模 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。

2.3 恶性竞争场景

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洗，避免因带宽占用瓶颈导致无法提供正常服务。

说明：

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。

三、术语解释

3.1 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。

攻击者通常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。

3.2 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。

3.3 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。

3.4 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。

3.5 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。

四、计费说明

4.1 计费模式

DDoS 高防 IP 由 DDoS 流量防护能力费用、回源带宽费用、防护域名费用、防护端口费用组成。

4.1.1DDoS 流量防护能力费用

DDoS 防护能力	静态高防-包月（元/月）	静态高防-按需（元/天）	动态高防-包月（元/月）	动态高防-按需（元/天）
10Gpbs	4400	-	5720	-
20Gpbs	8400	1200	10920	1500
30Gpbs	13400	1900	17420	2500
40Gpbs	23400	3300	30420	4300
50Gpbs	33400	4800	43420	6200
60Gpbs	43400	6200	56420	8000
70Gpbs	53400	7600	69420	9900

80Gpbs	63400	9000	82420	11800

以下规格，仅支持包年/按需订购：

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

4.1.2 回源带宽费用

默认 100M 回源带宽，增加步长为 50M，最大为 300M。

回源带宽	≤100M	＞100M
定价	免费	100 元/M

4.1.3 防护域名费用

默认 50 个域名；增加步长 5 个，最大 200 个。

防护域名	≤50 个	＞50 个
定价	免费	20 元/个

4.1.4 防护端口费用

默认包含端口数 50 个，增加步长为 5 个，最大支持 100 个。

防护端口	≤50 个	＞50 个
定价	免费	50 元/个

4.2 订购

说明：

DDoS 高防 IP 不支持试用。若需要使用 DDoS 高防 IP，请参照本文订购步骤进行购买。

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“  ”跳转订购页面。

2. 按需购买

1）确认高防节点，当前提供了华北地区、华东地区、华南地区共 4 个节点。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 1：可以选择任意端口进行转发；

华东 2：可以选择任意端口进行转发；

华南 1：可以选择任意端口进行转发；

网站类业务：限定选择 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。

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，保底防护带宽包月计费。

注意

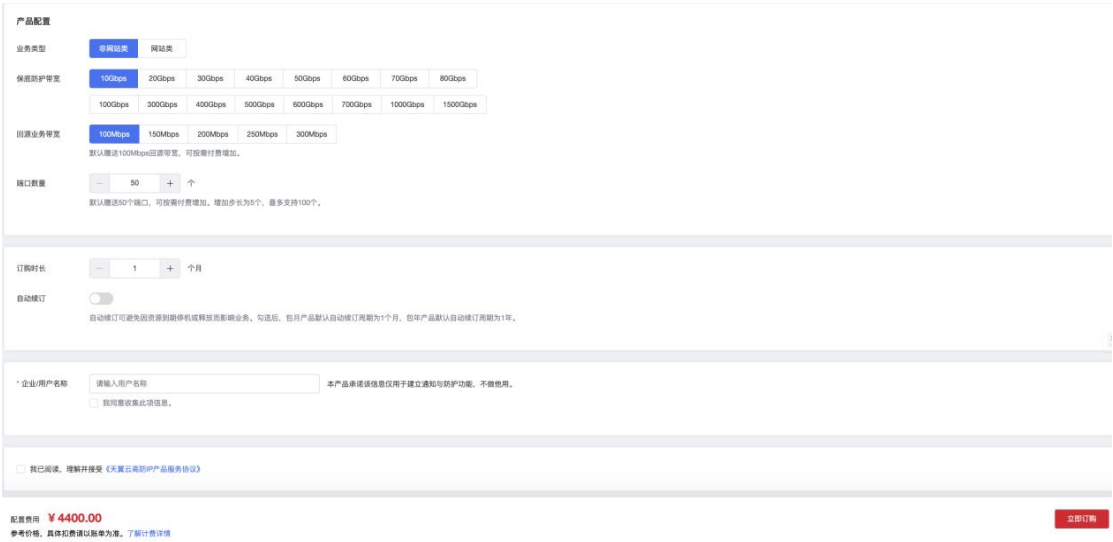
100Gbps 以上带宽只能包年订购。

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】。



4.3 续订及退订

4.3.1 续订

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，选择续订的时长，点击【立即购买】。

4.3.2 退订

在产品实例列表点击【退订】进入费用中心确认退订。

五、快速入门

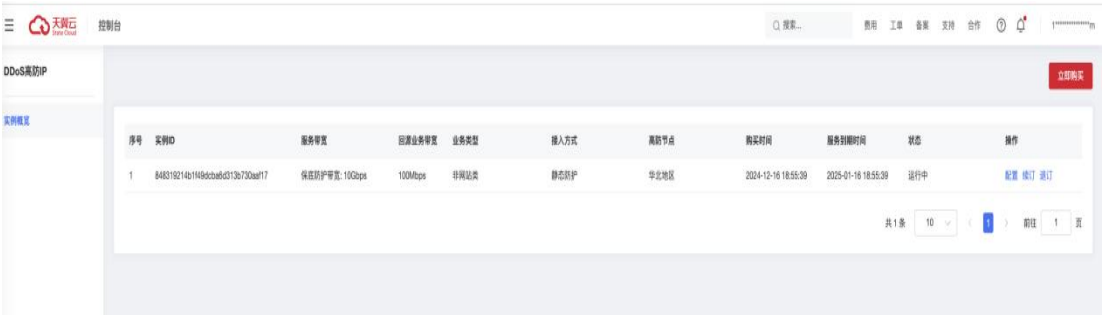
5.1 登录 DDoS 高防 IP 控制台

1.在天翼云官网 https://www.ctyun.cn/，点击控制中心。

2.选择“安全 > DDoS 高防 IP”，进入 DDoS 高防 IP 控制台。

5.2 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。



用户购买高防 IP 实例后，天翼云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；
- 回源业务带宽：用户购买的回源带宽；
- 业务类型：分为网站类和非网站类；
- 接入方式：
  - 静态防护，即非 BGP 节点，为单节点高防 IP；
  - 动态防护，即 BGP 节点，在多个高防中心（华北 1、华东 1、华东 2、华南）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；
- 高防节点：包括华北 地区、华东地区 1、华东地区 2、华南地区；
- 购买时间：实例购买时间；
- 到期时间：实例的到期时间。

5.4 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：

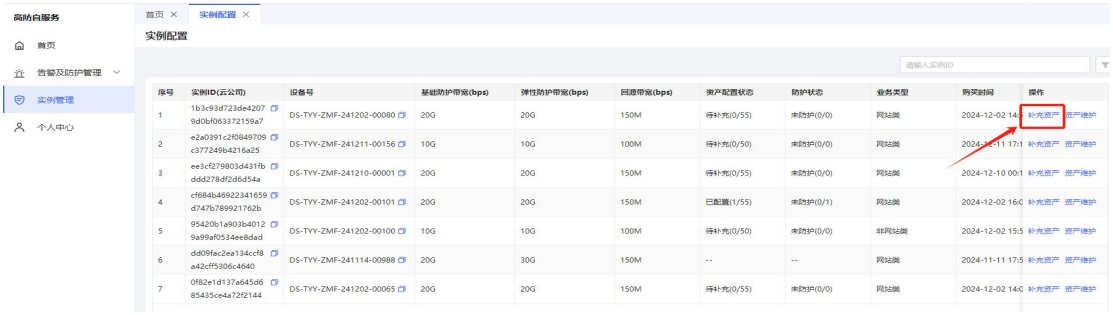
网站类业务： 80、8080、8081、443、7443、8443；

非网站类业务：除 80、443 端口外可以选择任意端口进行转发。

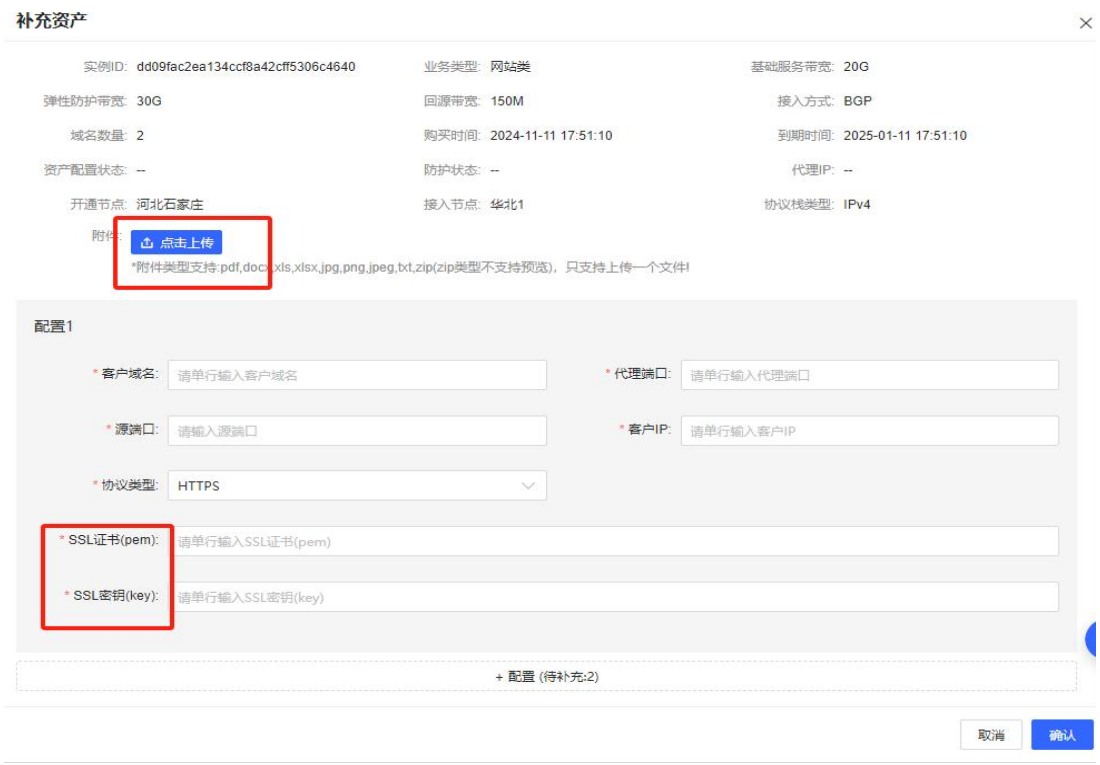
5.5 补充资产信息及备案

1. 选中购买实例后，点击“配置”。

2. 找到对应实例，选择“补充资产”，如曾经填写过资产，可点击“资产维护”。



3. 可进行地址备案和资产证书的补充，点击附件上传按钮可上传备案证明，当选择 HTTPS 协议时，需要上传证书及私钥。



4. 告警及防护管理

在左侧菜单选择“告警及防护管理”，可查询告警及防护记录。

5. 联系人管理

在左侧菜单选择“个人中心”，可查看现有联系人。点击“新增”，可新增联系人。

六、最佳实践

6.1 DDoS 攻击缓解

6.1.1 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。

6.1.2 优化业务架构

依托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。

- 屏蔽未经请求发送的 DNS 响应信息
- 丢弃快速重传数据包

- 启用 TTL
- 丢弃未知来源的 DNS 查询请求和响应数据
- 丢弃未经请求或突发的 DNS 请求
- 启动 DNS 客户端验证
- 对响应信息进行缓存处理
- 使用 ACL 的权限
- 利用 ACL、BCP38 及 IP 信誉功能

6.1.3 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。

七、常见问题

7.1 使用说明类

1.什么是 DDoS 高防 IP？

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。

2.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；天翼云协助帮您将对网站 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 。

3.如何选择静态防护、还是动态防护？

如客户业务 IP 是单个运营商（电信或联通或移动等），选静态；

如客户业务 IP 是多个运营商（例如电信+移动，电信+联通，或三家都有），选动态防护。

4.保底防护带宽如何选择？

根据攻击带宽流量向上取整，例如遭受攻击 11Gbps，则选择 20Gbps。

5.回源业务带宽怎么选择？

根据购买业务 IP 的出向流量向上取整，默认 100Mbps。客户可根据服务器的出向流量来选择,通常 100Mbps 即可,最大支持 300Mbps，超过 300Mbps 则新增订单。

6.端口数怎么选择？

默认 50 个免费，最大 100 个（超过 100 个需下多套订单）

防护对象尽量是域名，且需要域名备案。需客户进入域名管理后

台，将域名的 CNAME 由原本的服务器地址解析指向至 DDoS 高防 IP，并在服务器防火墙侧将分配的 DDoS 高防 IP 地址加入白名单。

7.防护对象如果没有域名怎么办？

如果业务 IP 没被攻击，则相当于业务 IP 此时还未暴漏，需要客户端将访问 IP 修改为 DDoS 高防的 IP，此时终端客户需通过 DDoS 高防访问。

如果业务 IP 已经被攻击，相当于业务 IP 已经暴漏，此情况需要客户端 IP 修改为 DDoS 的 IP 高防的同时，需更换已有业务。

备注：如业务为 SIP 类终端与服务端传输始终会携带源站 IP 的业务，此情况则不适用 DDoS 高防 IP，需采用运营商原生清洗防护。

8.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。

9.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（华北地区、华东地区 1、华东地区 2、华南地区）使用，实现高防 IP 负载调度的近源清洗。

10.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。

11.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。

7.2 计费类

1.天翼云 DDoS 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。

2.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 10 个工作日的时间供客户进行续费。