DDoS 基础防护

用户操作指南

天翼云科技有限公司

目录

1 产品介绍

1.1 产品概述

1.1.1 产品定义

DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为公网 IP 提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。当 IP 的流量峰值超过 IP 的防护阈值时，IP 所在服务器和网络的稳定性会受到影响，根据用户协议，IP 会进入封禁状态，DDoS 基础防护产品会提供封禁状态数据和 DDoS 防护建议。若 DDoS 基础防护免费提供的基础 DDoS 防护阈值无法满足您的业务需求，您可选择天翼云或其他第三方 DDoS 高防产品防护自身在天翼云的业务 IP 免受 DDoS 攻击。以天翼云举例，如天翼云“DDOS 高防 IP”、天翼云“DDOS 高防（边缘云版）”等。

1.1.2 支持地域

目前 DDoS 基础防护产品支持如下资源池：华北 2、杭州 7、华南 2、华东 1、内蒙 6、呼和浩特 3。

1.1.3 支持防护的云产品

EIP 及绑定 EIP 的资源。免费的基础 DDoS 防护阈值无需配置，自动对资源池内所有 IPv4 和 IPv6 的公网 IP 生效。

1.1.4 产品性能

DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为公网 IP 提供免费的基础 DDoS 防护阈值，该基础 DDoS 防护阈值与公网 IP 带宽规格、公网 IP 绑定资产类型和具体资源池相关。

1、IP 带宽越大，分配的网络资源越多，能对抗的 DDoS 攻击峰值越高，DDoS 防护阈值越大。

2、IP 绑定的资产类型属于负载型的资产时，如 ELB、NAT 等，相较于 IP 绑定到 ECS 云主机资产，负载型资产本身分配的网络资源较多，能对抗的 DDoS 攻击峰值更高，DDoS 防护阈值更大。

3、资源池内所有 EIP 遭受的 DDoS 攻击最终都会对资源池网络造成影响，为防止资源池网络整体产生波动，资源池会设定一个 DDoS 防护阈值作为资源池防护的底线。该阈值被同一时间所有受攻击的 IP 均分，例如当多个 IP 同时被攻击时，受攻击的多个 IP 会均分该阈值。

公网 IP 的基础 DDoS 防护阈值为 IP 带宽 DDoS 防护阈值，IP 资产类型 DDoS 防护阈值，IP 资源池 DDoS 防护阈值中取最小值，因任意类型的阈值超限均会对 IP 所在资源池、服务器或网络产生稳定性影响，具体计算公式如下。计算结果为理论底线数值，当 IP 所在服务器和资源池网络畅通时，DDoS 基础防护会尽可能为 IP 提供更高的 DDoS 防护阈值。

IP 的基础 DDoS 防护阈值 = MIN（IP 带宽 DDoS 防护阈值，IP 资产类型 DDoS 防护阈值，IP 资源池 DDoS 防护阈值）

- IP 带宽 DDoS 防护阈值

IP 带宽	公网 IP 带宽 DDoS 防护阈值
IP 带宽 ≤ 200Mbps	2Gbps
200Mbps < IP 带宽 ≤ 500Mbps	5Gbps
500Mbps < IP 带宽	8Gbps

- IP 资产类型防护阈值

IP 绑定资产类型	公网 IP 资产类型 DDoS 防护阈值
ELB、NAT、VPN	8Gbps
vcpu（核数）≥ 4 规格 VM	5Gbps
vcpu（核数）= 2 规格 VM	2Gbps
vcpu（核数）= 1 规格 VM	1Gbps

- IP 资源池防护阈值

资源池	IP 资源池 DDoS 防护阈值
默认	15Gbps/同一时间遭受 DDoS 攻击的 IP 数量

1.2 产品优势

1.2.1 快捷易用，高效防护 DDoS 攻击

DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为公网 IP 提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。

1.2.2 清晰明确，提供丰富 DDoS 攻击情况

当 DDoS 攻击峰值超出 DDoS 防护阈值后，DDoS 基础防护产品提供 DDoS 攻击峰值和流量趋势信息，作为其他 DDoS 防护手段的规格参考，如 DDoS 高防攻击峰值规格。

1.2.3 综合全面，提供充分 DDoS 防护建议

为防止 DDoS 攻击峰值超出防护阈值进而影响业务，DDoS 基础防护产品向您提供多种 DDoS 防护建议和背景信息，包括配置 DDoS 高防、配置安全组、检查 IP 暴露情况等。

1.2.4 轻量延迟，业务防护无负担

DDoS 基础防护作用位置在资源池内，为您的池内 IP 提供原生级别的 DDoS 防护，不会对业务带来额外延迟影响，业务无负担使用防护功能。

1.3 名词解释

1.3.1 DDoS 攻击

分布式拒绝服务（DDoS）攻击是一种常见的网络攻击形式。攻击者从互联网的多个不同位置同时向一个或多个目标 IP 发起攻击，企图通过大规模互联网公网流量耗尽攻击目标的网络资源，使目标 IP 无法提供正常服务。例如 IP 带宽 100Mbps，存在远超 100Mbps 以上的入向访问流量，IP 服务质量会严重下降，此时 IP 可被视为遭受到了 DDoS 攻击。

1.3.2 DDoS 防护阈值

IP 的 DDoS 防护阈值指资源池分配给该 IP 的最大允许流量速率，当 IP 遭受到较大规模的 DDoS 攻击或 IP 本身的业务流量出现异常峰值情况，IP 的流量峰值可能会超过 IP 的 DDoS 防护阈值，此时 IP 所在服务器和网络的稳定性会受到影响，为确保其他租户的 IP 不受影响，根据用户协议，IP 会进入封禁状态。

1.3.3 DDoS 防护策略

IP 的 DDoS 防护策略指在 DDoS 防护阈值内，DDoS 基础防护产品对 IP 流量中可能的 DDoS 攻击流量进行判定和过滤的算法集合。在 DDoS 防护阈值内，用户可从 DDoS 基础防护产品开放的 DDoS 防护策略中选择 IP 的防护策略，DDoS 基础防护产品会根据用户选择的防护策略会对 IP 流量进行判断（是否为 DDoS 攻击流量）和清洗过滤，将清洗过滤后的流量回注 IP，尽可能保障 IP 可用。DDoS 防护策略可能会将部分异常或突增的业务流量判断为 DDoS 攻击流量并产生误清洗（如频繁发送 syn 报文的业务），建议用户根据业务情况选择合适的防护策略，若不需要清洗，可不选择 IP 的防护策略。

1.3.4 DDoS 封禁状态

DDoS 封禁状态是指公网 IP 的外网访问被阻断的状态。

1.3.5 流量峰值

流量峰值指一段时间内 IP 入向流量速率的最大值，当 IP 的流量峰值超过 DDoS 防护阈值和网络承受能力时，IP 所在服务器和网络的稳定性会受到影响，

根据用户协议，IP 会进入封禁状态。流量峰值可用于获知 DDoS 攻击强度，以此选用合适规格的 DDoS 高防产品。

1.3.6 DDoS 防护建议

DDoS 防护建议指 DDoS 基础防护产品为用户提供的避免遭受 DDoS 攻击和 DDoS 封禁的建议，包括配置安全组限制访问源，配置 DDoS 高防 IP，检查管控业务 IP 泄露渠道等。

1.4 约束与限制

1.4.1 开通限制

对于服务开通和使用，您需要通过实名认证，否则无法开通相关服务。

2 计费说明

DDoS 基础防护免费为客户提供基础服务，依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为公网 IP 提供免费的基础 DDoS 防护阈值，若 DDoS 基础防护提供的免费基础 DDoS 防护阈值无法满足您的业务需求，您可选择天翼云或其他第三方 DDoS 高防产品防护自身在天翼云的业务 IP 免受 DDoS 攻击。以天翼云举例，如天翼云“DDOS 高防 IP”、天翼云“DDOS 高防（边缘云版）”等。

3 快速入门

3.1 概述介绍

DDoS 基础防护产品主要面向业务价值较高和业务竞争性较强，易遭受 DDoS 攻击的客户。

客户可在 DDoS 基础防护产品中快速了解自身持有 IP 是否因 DDoS 攻击超出服务器承受能力而被封禁，了解导致封禁的攻击峰值强度和防护建议，以此作为采用其他 DDoS 高防防护手段的参考。

3.2 前提条件

1. 用户已登录天翼云官网平台。
2. 完成账号实名制认证，使用天翼云官网账号登录，进入控制台使用服务。
3. 用户持有弹性 EIP，若客户无公网业务则无需使用 DDoS 基础防护产品。

3.3 查看 DDoS 封禁情况

操作步骤

1. 选择“安全及管理 > 网络安全 > DDoS 基础防护”，进入 DDoS 基础防护控制台页面。点击“开通 DDoS 基础防护服务”。

2. 点击左侧导航栏“DDoS 封禁情况”页面。
3. 在页面中查看 DDoS 封禁情况，若表格无具体数据，代表当前无 IP 被封禁。
4. 在页面中查看 DDoS 封禁情况，可在“流量峰值”一列查看流量峰值信息，可在“操作”一列点击查看封禁前的流量情况，对攻击进一步了解。

4 操作指导

4.1 查看 DDoS 封禁情况及流量峰值

引言

天翼云 DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为客户提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。当 DDoS 攻击超过 DDoS 防护阈值和网络承受能力时，IP 会进入封禁状态，DDoS 基础防护提供封禁状态数据。供用户了解 DDoS 攻击情况和封禁情况，以便及时采取 DDoS 防护措施。

操作步骤

1. 选择“安全及管理 > 网络安全 > DDoS 基础防护”，进入 DDoS 基础防护控制台页面。

2. 点击左侧导航栏“DDoS 封禁情况”页面。
3. 在页面中查看 DDoS 封禁情况，若表格无具体数据，代表当前无 IP 被封禁。
4. 在页面中查看 DDoS 封禁情况，可在“流量峰值”一列查看流量峰值信息，可在“操作”一列点击查看封禁前的流量情况，对攻击进一步了解。

4.2 调整 IP 的 DDoS 防护策略

引言

天翼云 DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为客户提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。当 DDoS 攻击超过 DDoS 防护阈值和网络承受能力时，IP 会进入封禁状态。在 DDoS 防护阈值内，用户可从 DDoS 基础防护产品开放的 DDoS 防护策略中选择 IP 的防护策略，DDoS 基础防护产品会根据用户选择的防护策略会对 IP 流量进行判断（是否为 DDoS 攻击流量）和清洗过滤，将清洗过滤后的流量回注 IP，尽可能保障 IP 可用。DDoS 防护策略可能会将部分异常或突增的业务流量判断为 DDoS 攻击流量并产生误清洗（如频繁发送 syn 报文的业务），建议用户根据业务情况选择合适的防护策略，若不需要清洗，可不选择 IP 的防护策略。

操作步骤

1. 在产品服务列表中，选择“安全及管理 > 网络安全 > DDoS 基础防护”，进入 DDoS 基础防护控制台页面。
2. 单击页面顶部的区域选择框，选择区域。

3. 进入资产中心页面，在操作一列点击“修改防护策略”，调整 IP 的防护策略。默认可选的几种防护策略的名称代表策略适合防护的攻击大小，如 5G 防护策略代表适合防护 5Gbps 左右的流量和 DDoS 攻击，对规模更小的流量，可能不会清洗，直接放过该部分流量。建议您根据业务带宽大小，选择与业务带宽上限大小等同的防护策略，例如 300Mbps 带宽的 IP 适合选择 300Mbps 防护策略。

4.3 查看 DDoS 攻击事件

引言

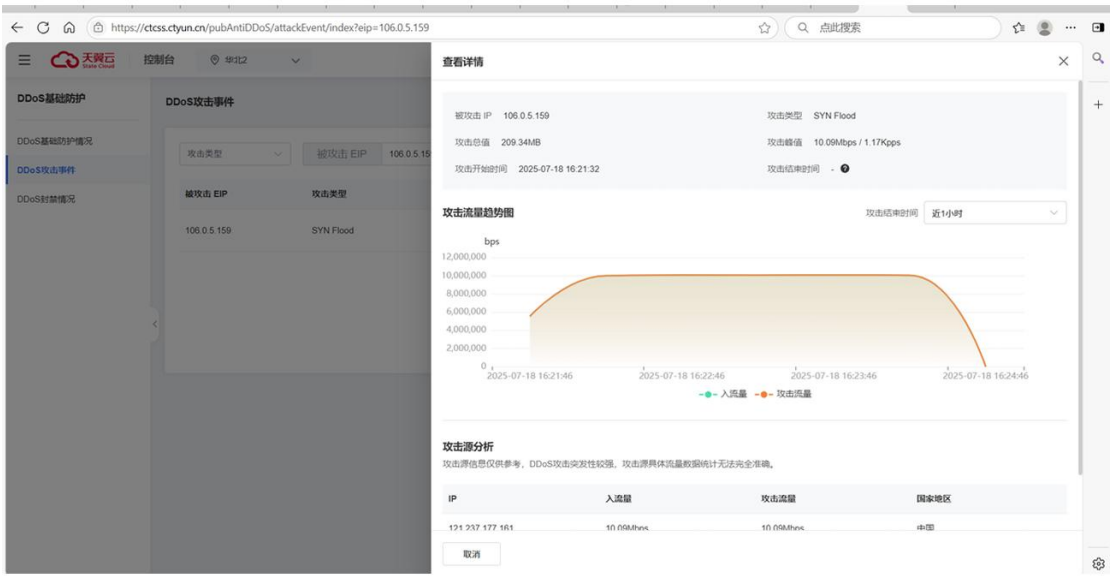
天翼云 DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为客户提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。当 DDoS 攻击超过 DDoS 防护阈值和网络承受能力时，IP 会进入封禁状态。在 DDoS 防护阈值内，用户可从 DDoS 基础防护产品开放的 DDoS 防护策略中选择 IP 的防护策略，DDoS 基础防护产品会根据用户选择的防护策略会对 IP 流量进行判断（是否为 DDoS 攻击流量）和清洗过滤。在您配置 IP 的 DDoS 防护策略后，若 DDoS 基础防护判断您 IP 流量中存在 DDoS 攻击流量并进行清洗过滤，会在 DDoS 攻击事件页面中记录攻击事件详情，您可查看详情来获取清洗量、攻击峰值、攻击源等攻击信息，以此判断是否需要调

整 DDoS 防护策略，如业务突增或者业务本身流量特性容易被判定为 DDoS 攻击流量（如频繁发送 syn 报文的业务），产生误清洗影响业务时，可适当调大防护策略或取消选择防护策略。

当 DDoS 攻击超过 DDoS 防护阈值和网络承受能力时，IP 会进入封禁状态，此时 IP 流量会被阻拦在网络外，DDoS 基础防护产品无法获取 IP 流量信息并分析生成 DDoS 攻击事件。

操作步骤

1. 在产品服务列表中，选择“安全及管理 > 网络安全 > DDoS 基础防护”，进入 DDoS 基础防护控制台页面。
2. 单击页面顶部的区域选择框，选择区域。
3. 进入 DDoS 攻击事件页面，在“操作-查看详情”列，查看 DDoS 攻击事件。具体包括攻击峰值、攻击总量、攻击源、攻击趋势图等。



4.4 设置 DDoS 事件告警策略

引言

目前 DDoS 基础防护设置了以下告警事件可供客户配置告警策略，当告警事件发生时，告警策略会通知客户配置的对象。

1、IP 封禁事件：天翼云 DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为客户提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。当 IP 的流量峰值超过 DDoS 防护阈值和网络承受能力时，IP 会进入封禁状态。

2、攻击事件开始、结束：在 DDoS 防护阈值内，用户可从 DDoS 基础防护产品开放的 DDoS 防护策略中选择 IP 的防护策略，DDoS 基础防护产品会根据用户选择的防护策略会对 IP 流量进行判断（是否为 DDoS 攻击流量）和清洗过滤。若产生清洗行为，则会生成攻击事件。

操作步骤

1. 在产品服务列表中，选择“安全及管理 > 网络安全 > DDoS 基础防护”，进入 DDoS 基础防护控制台页面。

2. 进入告警中心页面，配置告警联系组。

3. 配置告警策略，选择需要告警的事件类型和要接收告警的告警联系组

5 常见问题

5.1 公网 IP 遭受 DDoS 攻击为什么会进入封禁状态?

同资源池的公网 IP 共用资源池的公网带宽，当 IP 遭受的 DDoS 攻击峰值或 IP 的公网业务流量远超 IP 的购买带宽时，IP 占用超出购买带宽的大量额外网络带宽，IP 所在的服务器和网络的稳定性会受到影响。此时为防止其他同资源池 IP 受到影响，遭受 DDoS 攻击的 IP 会进入封禁状态，无法在公网通信，从而释放 IP 占用的大量额外网络带宽，确保网络稳定。

为尽可能确保 IP 和网络的稳定可用，天翼云 DDoS 基础防护产品依托天翼云资源池网络，根据 IP 带宽、IP 资产类型和资源池网络情况为 IP 提供免费的基础 DDoS 防护阈值，在阈值内尽可能确保客户 IP 可用。当 IP 的流量峰值超过 IP 的防护阈值时，IP 所在服务器和网络的稳定性会受到影响，根据用户协议，IP 会进入封禁状态，DDoS 基础防护产品会提供封禁状态数据和 DDoS 防护建议。

注意，DDoS 基础防护应对的 DDoS 攻击是指从公网到达 IP 所在资源池的 DDoS 攻击，若您在资源池内运行了云防火墙等具备一定 DDoS 识别和清洗能力的产品，其作用位置在资源池内部，从公网到达的 DDoS 攻击依然会影响 IP 所在网络的稳定。甚至当您的 EIP 绑定的 ECS 云主机关机时，若您的 IP 已暴露，仍有可能因业务竞争等原因遭受来自公网的 DDoS 攻击。以上资源池内的防护措施都无法避免触发 DDoS 封禁。

若 DDoS 基础防护提供的免费 DDoS 防护阈值无法满足您的业务需求，您可选择天翼云或其他第三方 DDoS 高防产品防护自身在天翼云的业务 IP 免受 DDoS

攻击。以天翼云举例，如天翼云“DDOS 高防 IP”、天翼云“DDOS 高防（边缘云版）”等。DDoS 高防产品的作用位置在 IP 所在的资源池外部。

5.2 公网 IP 进入封禁状态有什么依据?

您可在 DDoS 基础防护产品控制台查看 IP 进入封禁状态前的 DDoS 攻击峰值信息和 IP 流量状态，该攻击峰值已超过天翼云能提供的 DDoS 基础防护阈值，超出了服务器和网络的承受能力，为防止同地域其他 IP 受到影响，被攻击 IP 会进入封禁状态。

公网 IP 进入封禁状态的相关协议依据主要是天翼云产品服务协议通用服务条款中有关“DDoS”的部分协议，详见 https://www.ctyun.cn/portal/protocol/11042842。

5.3 公网 IP 封禁状态会持续多长时间?

当 IP 的流量峰值超过 DDoS 防护阈值和网络承受能力时，为防止其他同地域 IP 受到影响，被攻击 IP 会进入临时封禁状态 24 小时。

请注意，为防止 IP 所在的网络和资源池受影响，IP 的 DDoS 封禁实际生效位置在资源池网络之上的骨干网络，会将去往目的 IP 的流量丢弃，骨干网络操作需消耗较多网络资源，存在操作次数方面的限制，因此封禁时间目前较长，造成不便敬请谅解。同时，DDoS 攻击持续时间不定，如果在攻击未停止的情况下解除 DDoS 封禁，IP 的攻击流量会再次影响资源池稳定，因此 DDoS 封禁时间需设置的较长。

5.4 公网 IP 进入封禁状态是否有通知?

DDoS 封禁后会通过 EIP 所属账户的站内信、短信、邮箱渠道进行通知，告知封禁信息。除了账户所有人，您还可在在天翼云控制台-消息中心-消息订阅-消息管理-安全消息处配置多个消息接收人，比如将您业务的多位值班或运维人员配置到联系人中，此时安全消息短信会通知告知多个人。

封禁信息包含 EIP 遭受 DDoS 攻击的攻击日志数据，具体为 IP 和流量峰值。DDoS 基础防护仅能提供目的 IP 级别遭受 DDoS 大流量攻击的流量峰值数据，供客户知晓攻击强度，暂无法提供源 IP 级别或抓包级别的信息。您也可在 DDoS 基础防护控制台查看封禁相关信息。若您对源 IP 级别的 DDoS 攻击信息有强烈需求，您可选择天翼云或其他第三方 DDoS 高防产品防护自身在天翼云的业务 IP 免受 DDoS 攻击。以天翼云举例，如天翼云“DDOS 高防 IP”、天翼云“DDOS 高防（边缘云版）”等。天翼云和其他云厂商均提供有 DDoS 高防产品，一般可提供高防 IP 隐藏业务 IP、大流量攻击防护和攻击源分析能力。

5.5 如何提前解除封禁并恢复业务?

- 临时封禁

目前临时封禁仅能通过在临时封禁后购买配置 DDoS 高防，通过工单申请提前解封，或者等待封禁时间到期后自动解封。您可选择天翼云或其他第三方 DDoS 高防产品防护自身在天翼云的业务 IP 免受 DDoS 攻击。以天翼云举例，如天翼云“DDOS 高防 IP”、天翼云“DDOS 高防（边缘云版）”等。天翼云和其他云厂商均提供有 DDoS 高防产品，一般可提供高防 IP 隐藏业务 IP、大流量攻击防护和攻击源分析能力。

- 更换 EIP

若无法提前解除封禁，您也可考虑通过以下办法快速恢复业务。

1、购买或已持有其他未被 DDoS 封禁的公网 IP。

2、将已封禁 EIP 绑定的资产绑定到新的公网 IP，业务恢复。

IP 更换后，业务可能会重新遭到攻击，如果同账户资源频繁遭受 DDoS 封禁，攻击流量会频繁影响服务器和网络的稳定性，可能会引起天翼云平台对您账号的限制，包括但不限于停止新购资源权限。

5.6 公网 IP 如何增强 DDoS 防护能力?

若您的 IP 频繁遭受 DDoS 攻击，超出 DDoS 基础防护阈值，频繁被封禁，建议您通过以下手段增强 DDoS 安全防护能力。

- 购买配置 DDoS 高防产品

天翼云和其他云厂商均提供有 DDoS 高防产品，一般可提供高防 IP 隐藏业务 IP、大流量攻击防护和攻击源分析能力，您可选择天翼云或其他第三方 DDoS 高防产品防护自身在天翼云的业务 IP 免受 DDoS 攻击。以天翼云举例，如天翼云“DDOS 高防 IP”、天翼云“DDOS 高防（边缘云版）”等。

客户业务 IP 被资源池外的高防 IP 保护后，高防 IP 代替业务 IP 暴露在公网上，攻击者仅能探知到高防 IP 并发起 DDoS 攻击，DDoS 攻击流量经过高防 IP 过滤清洗，清洗后的正常流量回注到业务 IP，该回注流量一般情况下不会远超 IP 购买带宽，不会超过服务器和网络的承受能力，因此不会触发 DDoS 基础防护的临时封禁。

同时请注意，若业务 IP 历史存在攻击，可能已被攻击者获知，即使配置 DDoS

高防，攻击者有可能绕过高防 IP 对业务 IP 发起攻击，若攻击流量过大，仍会超过 DDoS 基础防护阈值，触发临时封禁，因此建议在配置高防的同时，同步更换业务 IP 并限制仅能被高防 IP 访问，实现业务 IP 隐藏。

具体购买和配置请咨询 DDoS 高防产品对应产品方。

购买配置 DDoS 高防产品可提单提前解除临时封禁。

- 配置安全组

在绑定公网业务 IP 的主机配置安全组，使业务 IP 仅能被一部分 IP 及端口访问，实现在公网上隐藏该业务 IP。配置安全组适合业务模式为无需在公网暴露 IP 的业务。

同时请注意，若业务 IP 历史存在攻击，可能已被攻击者获知，即使配置安全组，攻击者无法探活业务 IP，仍有可能对业务 IP 发起攻击，若攻击流量过大，仍会超过 DDoS 基础防护阈值，触发临时封禁。因此建议在配置安全组的同时，同步更换业务 IP。

配置安全组无法解除临时封禁。

5.7 业务 IP 暴露后如何检查?

若业务 IP 历史存在攻击，可能已被攻击者获知，即使配置 DDoS 高防，攻击者有可能绕过高防 IP 对业务 IP 发起攻击，若攻击流量过大，仍会超过 DDoS 基础防护阈值，触发临时封禁，因此建议在配置高防的同时，同步更换业务 IP 并限制仅能被高防 IP 访问，实现业务 IP 隐藏。

在更换业务 IP 前建议对其他可能暴露业务 IP 的因素进行检查，避免新更换的业务 IP 通过其他渠道再次暴露。

- 网站信息泄露检查

检查业务网站是否存在回源 IP 等信息泄露。

检查业务网站是否存在可能泄露配置的命令执行漏洞。

- 服务器信息泄露检查

检查服务器是否存在后门程序。

- DNS 检查

检查是否存在域名直接解析到更换后的新 IP 的情况。

- 安全组检查

检查安全组是否限制新 IP 仅可被高防 IP 等授权 IP 访问，防止攻击者扫描获知新 IP 信息。

6 最佳实践

1、业务运行初期，客户业务未遭受 DDoS 攻击或遭受的 DDoS 攻击小于 DDoS 基础防护阈值，IP 不会进入封禁状态，网络可用。

2、随着业务发展和业务竞争增强，业务遭受 DDoS 攻击，攻击流量超过服务器和网络承受能力，IP 进入封禁状态。

3、客户接收到短信、邮件和站内信通知 IP 封禁情况和流量峰值情况。

4、客户进入 DDoS 基础防护产品复核流量峰值和封禁前流量趋势情况，查看产品文档中的防护建议。

5、客户根据防护建议购买天翼云或其他第三方 DDoS 高防产品，并同步更换业务 IP，实现业务 IP 的 DDoS 高防防护。