DDoS 高防包

故障处理

产品文档

腾讯云

文档目录

故障处理
业务被大流量攻击导致封堵

最近更新时间：2022-08-16 11:43:31

现象描述

业务被大流量攻击导致 IP 封堵，业务无法访问。

可能原因

- 超过防护流量阈值，导致被封堵。
- 攻击还在持续，无法进行自动解封。

解决思路

默认情况下，封堵2~24小时后自动解封（具体封堵时长，请以实际封堵时长为准）。在紧急情况下，可申请DDoS应急防护。

DDoS 攻击未达到阈值业务 IP 被封堵

最近更新时间：2022-01-07 11:47:41

现象描述

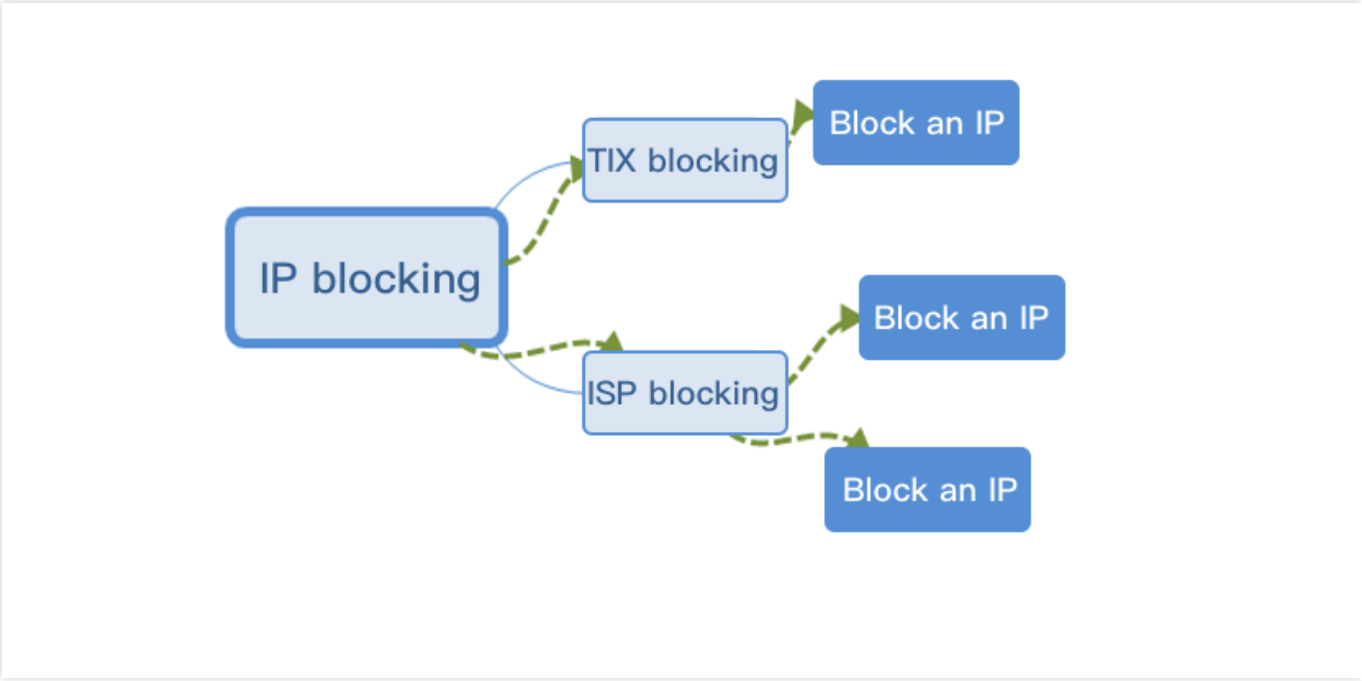
攻击流量没有达到购买封堵阈值，但 IP 被封堵。

可能原因

已购买 DDoS 高防包，所有出网口的攻击流量总和未达到购买阈值便进行封堵。 计算方式：所有出网口的攻击流量与购买阈值对比。

1. 根据封堵的节点位置分为两种封堵。
   - TIX 封堵：为腾讯的出口网关进行封堵，封堵的阈值是可调控的。
   - ISP 封堵：为运营商封堵，封堵的阈值基本固定的。

2. 在 ISP 封堵的情况下分为两种方式封堵。
   - 单 IP 封堵：当一个 IP 的流量达到某个出口单 IP 封堵阈值（根据出口带宽设置）时封堵。
   - 多 IP 封堵：当某个检测区间 IDC 的总流量（攻击流量 + 业务流量）超过多 IP 封堵阈值。



解决思路

等待攻击结束后进行自助解封或者自动解封。

处理步骤

1. 登录 DDoS 防护管理控制台，在左侧导航中，选择【自助解封】页面，查看自助解封剩余次数。
   - 若自助解封剩余次数为0，则跳转到 步骤5，或等待自动解封。
   - 若自助解封剩余次数不为0，则跳转到 步骤2。

   > 说明：
   > 自动解封时间，请参考控制台 解封操作 页面的“预计解封时间”项。

2. 查看攻击是否已停止，请单击 防护概览 查看。
   - 若是，则跳转到 步骤3。
   - 若否，待攻击停止时，继续执行解封操作，执行 步骤3。

   > 说明：
   > 攻击如果持续进行未停止，则无法进行解封，需等待攻击结束自助解封或自动解封。

3. 在左侧导航中，选择**自助解封** > **解封操作**，进入解封操作页面。

4. 在解封操作页面，找到状态为“自动解封中”的防护 IP，在右侧操作栏中，单击**解封**。

5. 不同DDoS防护产品的用户，建议如下：
   - 如果是 DDoS 基础防护用户，建议用户购买 高防包（支持防护地域：广州、上海和北京），首次绑定设备 可进行解封。
   - 如果是 DDoS 高防用户，建议用户 [升级防护套餐]（增加防护次数或防护 IP 数），可提前解除封堵。