

DDoS 高防包

故障处理

产品文档



腾讯云

【 版权声明 】

©2013–2023 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

故障处理

业务被大流量攻击导致封堵

DDoS 攻击未达到阈值业务 IP 被封堵

故障处理

业务被大流量攻击导致封堵

最近更新时间：2022-07-26 09:56:35

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

- DDoS基础防护：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）。
- DDoS 高防用户每天拥有三次自助解封机会，当天超过三次后将无法进行解封操作。系统将在每天零点时重置自助解封次数，当天未使用的解封次数不会累计到次日。

如解封次数用完：

- 未购买 DDoS 高防包的客户，建议用户购买高防包，首次绑定设备可进行解封。
- 已购买 DDoS 高防包的客户，建议客户升级防护套餐，可提前解除封堵。

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](#)。

② 说明：

自动解封时间，请参考 DDoS 防护管理控制台 [自助解封](#) > [解封操作](#)页面的“预计解封时间”项。

解封操作

总配额数		当前已使用		当前未使用	
3 次		0 次		3 次	
IP	封堵时间	预计解封时间	状态		操作
1	2018-11-07 20:31:37	2018-11-07 22:31:37	自动解封中		解封

2. 查看攻击是否已停止，请选择 **DDoS 高防包** > [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**。

解封操作

总配额数		当前已使用		当前未使用	
3 次		0 次		3 次	
IP	封堵时间	预计解封时间	状态		操作
1	2018-11-07 20:31:37	2018-11-07 22:31:37	自动解封中		解封

5. 不同 DDoS 防护产品的用户，对应建议如下：

- 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。

DDoS 攻击未达到阈值业务 IP 被封堵

最近更新时间：2022-07-26 09:58:43

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

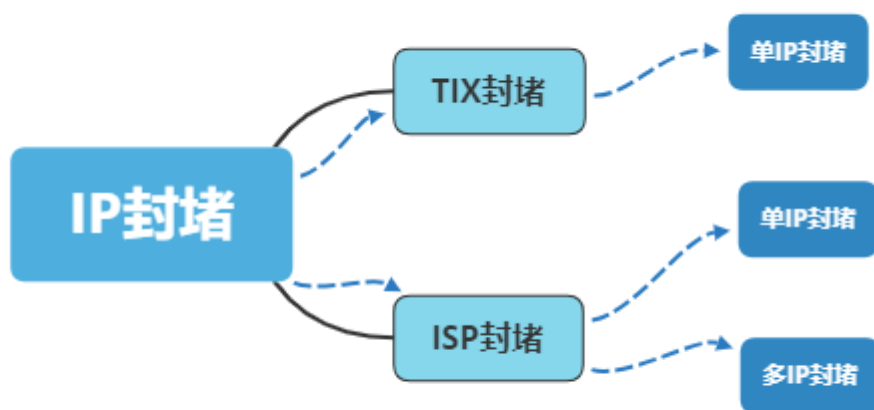
已购买 DDoS 高防包，所有出网口的攻击流量总和未达到购买阈值便进行封堵。计算方式：所有出网口的攻击流量与购买阈值对比。

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。

解封操作

总配额数		当前已使用	当前未使用	
3 次		0 次	3 次	
IP	封堵时间	预计解封时间	状态	操作
1 [IP地址]	2018-11-07 20:31:37	2018-11-07 22:31:37	自动解封中	解封

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](#)。

解封操作

总配额数		当前已使用	当前未使用	
3 次		0 次	3 次	
IP	封堵时间	预计解封时间	状态	操作
1 [IP地址]	2018-11-07 20:31:37	2018-11-07 22:31:37	自动解封中	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。