DDoS 高防包

常见问题

产品文档

腾讯云

文档目录

常见问题
封堵相关问题

最近更新时间：2019-12-23 15:30:02

DDoS 高防包所防护的 IP 被封堵了该怎么办？

如果正使用的 DDoS 高防包实例未调整到最高弹性防护峰值，可以在 DDoS 高防包管理控制台中更改 DDoS 高防包实例的弹性防护峰值，提升弹性防护能力，抵御更大的攻击流量。
另外，使用 DDoS 高防包的用户每天将拥有三次自助解封机会，可在紧急情况下，进行 自助解封。

为什么进行封堵？

腾讯云通过共享基础设施的方式降低用云成本，所有用户共享腾讯云的外网出口。当发生大流量攻击时，除了会影响被攻击对象，整个腾讯云的网络都可能会受到影响。为了避免攻击影响到其他未被攻击的用户，保障整个云平台网络的稳定，需要进行封堵。

为什么不提供免费无限抗攻击？

DDoS 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其它未被攻击的用户。DDoS 防御的成本非常高，一是带宽成本，二是清洗成本。其中最大的成本就是带宽费用，带宽费用以总流量计算，不会考虑是正常流量或是攻击流量而区别收费。
因此，腾讯云在成本可承受的范围内为云服务用户提供免费的 DDoS 基础防护服务，当攻击流量超出免费防护阈值时，腾讯云会屏蔽被攻击 IP 的外网流量。

为什么不能立即解除封堵？

通常 DDoS 攻击会持续一段时间，不会在封堵后立即停止，具体持续时间不定，腾讯云安全团队会根据大数据分析的结果，设定默认封堵时长。
由于封堵是在运营商网络部分生效，被攻击外网 IP 进入封堵后，腾讯云无法监控到攻击流量是否停止。如果在攻击未停止的情况下解除封堵，被攻击外网 IP 将再次进入封堵，同时在解除封堵至再次封堵生效的这段时间内，攻击流量将直接进入腾讯云的基础网络，可能会影响到云内其它客户。另外，封堵是腾讯云向运营商购买的服务，解封次数、频率都有限制。

紧急情况下，通过哪些途径可以提前解封？

1. 升级保底容量后，可自动提前解封。
2. 使用 DDoS 高防包的用户每天将拥有三次自助解封机会，可在紧急情况下，进行 自助解封。

为什么自助解封会有次数限制？有哪些限制？

封堵是腾讯云向运营商购买的服务，而运营商有明确的封堵解除时间和频率限制，所以封堵状态无法频繁手动解除。

使用 DDoS 高防包的用户每天将拥有**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。

如何连接已被封堵的服务器？

如需进行数据迁移等操作，可参考以下两种方式连接已被封堵的服务器：

- 通过同地域的其它云服务器通过内网 IP 连接被封堵服务器。
- 通过 云服务器控制台，在被封堵服务器所在行，单击【登录】即可通过浏览器 VNC 方式连接。

怎样预防被封堵？

购买 DDoS 高防包 时，可根据历史攻击流量数据，选择适当的防护峰值，尽可能地确保最大防护峰值大于攻击峰值。

怎样避免解封后再次被封堵？

建议您升级保底防护峰值或弹性防护峰值，提高防御能力。开启弹性防护可帮您抵御大规模流量攻击，且弹性防护按天按量灵活付费，有效节约您的安全成本。

功能相关问题

最近更新时间：2019-12-23 15:30:07

DDoS 高防包支持云外的 IP 接入防护吗？

不支持。DDoS 高防包仅对腾讯云内的公网 IP 提供 DDoS 防护支持。如需云外的防护，请 购买 DDoS 高防 IP。

如果绑定的资源已过期，DDoS 高防包实例还未过期，会怎么样？

DDoS 高防包实例是按月购买的，且以 IP 为媒介提供防护能力。如果绑定的防护对象资源过期，不及时更换 DDoS 高防包实例所绑定的 IP，那么该 DDoS 高防包实例在有效期内会持续为已绑定的 IP 提供防护，但该 IP 对应的资源不一定是您的。建议您及时为云服务续费，或更换新的防护对象 IP。

DDoS 高防包支持域名的防护吗？

不支持。若有域名防护以及应用层的防护需求，请 购买 DDoS 高防 IP。

DDoS 基础防护的防护带宽是2Gbps，又购买了 DDoS 高防包的套餐，最终的防护峰值是否会叠加？

用户享有的最终防护峰值，以 DDoS 高防包购买套餐里的防护峰值为准，不会叠加 DDoS 基础防护的默认防护带宽。
假设某云服务器的 IP 原本享有2Gbps的免费防护带宽。因经常遭受攻击，用户又为该 IP 购买了20Gbps的 DDoS 高防包套餐，则最大防护能力为20Gbps。

DDoS 高防包和 DDoS 高防 IP 的区别是什么？

- 防护对象：
  - DDoS 高防包只针对腾讯云内的服务提升 DDoS 防护能力。
  - DDoS 高防 IP 面向云外用户，为非腾讯云的业务 IP/域名提供防护。
- 接入：
  - DDoS 高防包的接入配置更加便捷，无需变更公网 IP 地址。
  - DDoS 高防 IP 需修改 DNS 解析或修改业务 IP 后才能接入防护。

DDoS 高防包与三网高防的区别是什么？

差异点	DDoS 高防包	三网高防
接入成本	无需更换服务器 IP，直接为云产品提升防御能力，即时生效，接入成本低	需要将服务器 IP 更换为三网 IP，填写域名与端口信息，配置相当复杂
访问质量	采用 BGP 带宽，减少跨网访问延迟，访问速度提升30%以上	无 BGP 带宽，网络延迟大，质量不佳

差异点	DDoS 高防包	三网高防
定价策略	计费灵活，支持保底+弹性，可共享	计费复杂，需要付流量费

计费相关问题

最近更新时间：2020-03-26 10:48:22

高防服务的弹性防护计费模式是否一样？如何计算的？

一样，都是按照当日可防护的攻击流量峰值对应弹性防护峰值区间进行计费，计费详情请参考 计费概述。
例如，您购买的 DDoS 高防包实例规格是20Gbps保底防护峰值 + 50Gbps弹性防护峰值。如果当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps。45Gbps已超过保底防护峰值范围触发弹性防护，且属于40Gbps < 弹性峰值 ≤ 50Gbps计费区间，当天产生弹性费用按照40Gbps < 弹性峰值 ≤ 50Gbps计费区间收取。

如果 DDoS 高防包所防护的 IP 因遭受大流量攻击被封堵，该部分攻击流量是否会列入计费？

DDoS 高防包服务的弹性防护计费规则是针对超出保底防护峰值且小于等于弹性防护峰值的攻击流量进行计费。被封堵即意味着攻击流量已超过所设置的弹性防护峰值，因此超出弹性防护峰值的部分攻击流量不在计费范围内。

购买弹性防护后，如果一个月都没有遭受攻击，是否需要费用？

这种情况下，您只需要支付保底防护的包月费用即可，不产生其它额外的费用。

若购买了100Gbps的保底防护，是否可以降到50Gbps？

不可以。保底防护级别仅支持升级，不支持降级。

业务遭受攻击过程中，是否支持升级弹性防护峰值？

支持。DDoS 高防包服务基础信息界面支持调整弹性防护峰值，支持调升也支持调降。不同地域支持的防护能力不同，弹性防护峰值的具体取值范围请参考 使用限制。

> 注意：
> 若当日发生的攻击已经产生计费，修改后次日将以最新的弹性防护峰值进行计费。

受防护的 IP 一天之内遭受多次攻击，是否需要收取多次费用呢？

DDoS 高防包服务是以当日防护的最高攻击流量峰值来计算，只收取一次费用。

如果购买了两个高防服务套餐，且两个高防服务实例遭受的攻击流量都超过保底防护，如何收取弹性防护费用？

弹性防护费用以产品实例为计算单位，如果两个高防服务实例都超过保底防护，则需要分别收取两个高防实例的弹性防护费用。