DDoS 基础防护

常见问题

产品文档

腾讯云

【版权声明】

【商标声明】

【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

常见问题
功能相关问题

最近更新时间：2023-03-06 10:49:03

如何启动 DDoS 基础防护?

目前用户只要购买了腾讯云内服务器，默认对其设备绑定的公网 IP 开启 DDoS 基础防护。

DDoS 基础防护应用场景包括哪些?

腾讯云 DDoS 基础防护应用于攻击频率不高且攻击峰值不超过基础防护阈值的 DDoS 攻击防护场景。当攻击流量超过一定流量时，将自动启动 DDoS 清洗设备进行流量清洗。

DDoS 基础防护的防护能力不能满足业务防护需求怎么办?

如果您的业务在北京，上海，广州的腾讯云内，推荐购买 DDoS 高防包 产品，提升 DDoS 防护能力。如需要更大防护能力，建议购买 DDoS 高防 IP 产品。

攻击相关问题

最近更新时间：2023-03-31 17:26:23

有 DDoS 攻击会通知吗?

在遭受 DDoS 攻击后，后台会推送告警通知。用户也可以根据需求自定义告警的阈值，当流量达到用户设定的警告阈值，将进行通知。具体操作请参见 设置安全事件通知 。

服务器没有使用，为什么也遭遇 DDoS 攻击?

- DDoS 攻击是指：黑客利用 DDoS 攻击器控制多台机器同时攻击来达到“妨碍正常使用者使用服务”的目的，一般主要是针对您的公网 IP 和域名。您的业务连接外网通信，就有风险遭受 DDOS 攻击。
- 您的业务连接外网通信，就有风险遭受 DDOS 攻击。

服务器被攻击，对方攻击的是什么?

服务器被攻击，一般攻击的是您的 IP 或者是业务。

常见攻击类型有哪些?

- 网络层攻击：常见攻击类型包括 UDP 反射攻击、SYN Flood 攻击及连接数攻击；这类攻击以消耗服务器带宽资源和连接资源从而达到拒绝服务的目的。
- 应用层攻击：常见攻击类型包括 DNS Flood 攻击、HTTP Flood 攻击及 CC 攻击；这类攻击以消耗服务器处理性能从而达到拒绝服务的目的。

轻量服务器被 DDoS 攻击，怎么办?

购买 轻量版高防包 能有效抵御 DDoS 攻击，保证您的服务器与业务正常运作。

服务器的防御值是多少? 如果被攻击达到了上限会怎么样呢?

基础防护的用户是最高不超过 2Gbps 带宽。达到免费防护阈值后，将会执行封堵策略，可能会影响您的业务。

攻击流量多少会判定为攻击?

只要流量被检测为含有攻击流量，即被判定为被攻击，不分大小。但是用户可以根据攻击流量的大小 设定告警 。

业务被 DDoS 攻击时，已将某访问源 IP 添加到高防包的黑名单，但该 IP 依然可以对业务进行访问，是 DDoS 高防没有起作用吗?

在添加进黑名单后，并不会立刻对黑名单访问源进行限制。当流量超过清洗阈值时，若黑名单中的 IP 进行访问，才将会被直接阻断。

DDoS 攻击流量超过封堵阈值时，会怎样?

在攻击流量超过封堵阈值的情况下会触发封堵策略，腾讯云会屏蔽一段时间外部对该 IP 的访问。如果急需恢复业务，建议购买腾讯云的 DDoS 高防包 产品或 DDoS 高防 IP 产品，以获得更大的 DDoS 防御能力。

封堵相关问题

最近更新时间：2023-05-09 11:42:12

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，影响云内其他未被攻击的用户。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他客户。另外，封堵及解封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?

将被封堵的未防护资产，绑定上已购买的 DDoS 高防包，即可提前解封。

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。

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：

- 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。

当 IP 被攻击封堵后，服务器的状态是如何的?

当腾讯云公网 IP 遭受大流量 DDoS 攻击，且攻击流量超出免费防护阈值时，腾讯云会暂时屏蔽被攻击 IP 所有入方向互联网流量（使该 IP 从互联网离线），避免 DDoS 攻击对客户资产产生更大损害，同时也避免单个 IP 被 DDoS 攻击而对云内其他客户产生影响。

怎样预防被封堵?

建议购买高防服务，并根据受到的攻击流量的峰值选择适当的高防容量，确保最大防护容量大于攻击峰值。

怎样避免解封后再次被封堵?

- 对于业务部署在腾讯云机房的用户：建议 购买 DDoS 高防包服务，提升 DDoS 高防能力，轻松应对攻击流量。
- 对于业务部署在非腾讯云机房的用户：建议 购买 DDoS 高防 IP 服务，轻松解决 DDoS 流量攻击困扰，保障服务器的正常运行。