DDoS 防护

常见问题

腾讯云

【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或95716。

文档目录

常见问题
封堵相关问题

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档 。

DDoS 高防服务的防护资源被封堵了该怎么办?

订阅 DDoS 高防服务后，单个腾讯云主账号每天拥有 3 次自助解封机会，当天操作自助解封超过 3 次后将无法进行自助解封操作。系统将在每天零点重置自助解封次数，当天未使用的自助解封次数不会累计到次日。
若解封次数用完：

- 未绑定 DDoS 高防套餐的资源（标准防护级别），建议绑定套餐并升级为增强防护或卓越防护级别，以提升防护容量，可提前解除封堵。
- 已绑定 DDoS 高防套餐的资源，可等待系统自动解封；同时建议升级套餐版本或加购防护能力扩展包，以提升防护容量应对下一次攻击。

为什么会被封堵?

当防护资源遭受的攻击流量超过其当前防护容量时，为避免影响云平台内其他未被攻击的用户，腾讯云将触发封堵。触发条件及原理详情请参见 封堵策略 。

会封堵多长时间?

封堵时长默认为 2 小时，最长可达 24 小时，实际时长受攻击是否持续、是否频繁、流量大小等因素影响，详情请参见 封堵策略 。

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侧生效，被攻击资源进入封堵后，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，被攻击资源将再次进入封堵，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用户。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。

为什么自助解封会有次数限制?

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。

攻击相关问题

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档。

遭受 DDoS 攻击时会收到通知吗?

会。当资源遭受 DDoS 攻击后，系统将进行告警通知推送。

资源没有对外提供服务，为什么也会遭遇 DDoS 攻击?

- DDoS 攻击是指攻击者利用大量僵尸主机同时发起攻击，目的是妨碍正常用户访问，攻击目标通常是您的资源 IP 或域名，而非针对某个具体的使用场景。
- 只要资源具备公网访问能力、对外暴露 IP 或域名，就存在遭受 DDoS 攻击的风险，与资源是否实际承载业务流量无关。

已绑定 DDoS 高防套餐，为什么仍然被攻击?

- 只要资源对外暴露公网访问能力，就存在被攻击的风险，这一点无法通过任何防护手段完全消除。
- DDoS 高防服务的作用是在遭受攻击时，尽可能保障您的业务不受攻击影响、维持正常访问，而非阻止攻击行为本身的发生。

常见的 DDoS 攻击类型有哪些?

- **网络层（L3/4）攻击**：常见类型包括 UDP Flood、SYN Flood、TCP Flood、ICMP Flood 及 DNS/NTP/SSDP 反射攻击等，通过消耗服务器带宽或连接资源使其无法正常服务。
- **应用层（L7）CC 攻击**：常见类型包括 HTTP/HTTPS Flood 等，通过消耗服务器处理性能使其无法正常服务。

详情请参见 产品概述 中的“多层 DDoS 防护”章节。

在哪里可以查看资源被攻击的日志与攻击来源?

在控制台的攻击分析页面，可查看攻击事件列表及详情，包括攻击源信息、攻击源地区、攻击流量及攻击包量大小等信息。

攻击流量达到多大才会被判定为“遭受攻击”？

只要流量被检测为含有攻击特征，即被判定为遭受攻击，不区分流量大小。

已将某访问源 IP 添加到黑名单，为什么该 IP 依然可以访问业务?

将 IP 添加至黑名单后，不会立即对该来源进行限制。当流量超过清洗阈值时，黑名单中的 IP 若继续访问，才会被直接阻断。

是否可以只为部分资源开启 DDoS 防护?

支持。您可以按需将云上资源、EO 域名、EO 四层代理实例等单独关联至防护实例，未关联的资源不受该防护实例影响。

计费相关问题

最近更新时间：2026-09-11 14:24:31

> **说明：**
> 2026年09月10日之后接入的客户适用于以下说明。若您为存量高防包或高防 IP 客户，请参考 历史相关文档 。

购买 DDoS 高防服务套餐后，是否立即生效?

购买套餐并绑定需要防护的资源后即可生效，通常几分钟内完成。

DDoS 防护清洗掉的攻击流量是否计费?

不计费。DDoS 防护清洗掉的攻击流量不产生费用，计费仅针对清洗后的正常业务流量，详情请参见 计费概述 。

是否支持仅在遭受攻击时才收费，未受攻击时不收费?

不支持。DDoS 高防服务采用订阅套餐制计费，基础套餐费用、业务规模费用、防护资源数费用均为必选项，按订阅套餐与实际业务规模、接入资源数计费，与是否遭受攻击无关。详情请参见 计费概述 。

如果当月没有遭受 DDoS 攻击，是否仍需要支付费用?

需要。基础套餐费用、业务规模费用、防护资源数费用均按订阅情况和用量计费，与是否遭受攻击无关；仅“全力防护次数”这一权益与攻击相关——实用版套餐每月提供 2 次全力防护，用完后自动降级为标准防护；尊享版套餐每月提供无限次全力防护。

实用版套餐的全力防护次数用完后，是否需要按次额外付费?

不需要。全力防护次数用完后，系统将自动降级按标准防护能力为您的资源提供防护，不会产生额外的按次费用；如需持续获得全力防护，可升配到尊享版套餐，详情请参见 升降配说明 。

遭受攻击时，全力防护次数具体如何触发和计算?

全力防护次数的触发与计算方式因防护资源类型而异：

- **云上资源（CVM、CLB、EIP 等，不含 EO 资源）**：当攻击流量超过 10,000 Mbps 时，将触发一次全力防护，持续 30 分钟；若攻击在 30 分钟内仍未停止，将自动启用下一次全力防护。若攻击事件导致资源被封堵，该次触发不消耗全力防护次数。
- **EO 资源**：按攻击事件次数计算全力防护次数，每次攻击事件消耗 1 次。由于单次攻击事件最长持续 24 小时，若实际攻击持续时间超过 24 小时，将被统计为 2 次攻击事件，消耗 2 次全力防护次数。若攻击事件导致资源被封堵，该次触发不消耗全力防护次数。

DDoS 高防套餐是否按账号计费?

是。DDoS 高防服务基础套餐按腾讯云主账号维度订阅和计费，同一账号下的多个防护实例共享同一套餐权益。

DDoS 高防服务套餐支持退款吗?

支持部分场景退款，具体规则请参见 退费说明 。