

DDoS 高防 IP

常见问题

产品文档



腾讯云

【版权声明】

©2013-2020 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【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。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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模式的承诺或保证。

文档目录

常见问题

封堵相关问题

功能相关问题

计费相关问题

常见问题

封堵相关问题

最近更新时间：2019-12-23 15:38:22

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，整个腾讯云的网路都可能会受到影响。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？

- 升级保底容量后，可自动提前解封。
- 使用 DDoS 高防 IP 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 IP 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。

怎样预防被封堵？

购买 DDoS 高防 IP 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 15:38:27

DDoS 高防 IP 支持腾讯云外用户接入防护吗？

支持。DDoS 高防 IP 可以防护任何公网服务器，包括但不限于在腾讯云、其他的云、IDC 机房等。

注意：

在中国大陆地区接入的域名必须按照工信部要求进行 ICP 备案。如果域名未备案，将不能提供 DDoS 高防服务。

DDoS 高防 IP 是否支持泛域名？

DDoS 高防 IP 网站业务转发规则配置中，支持对泛域名进行防护。

泛域名解析是指利用通配符（*）作为次级域名，以实现所有的次级域名均指向同一 IP。例如，支持配置 *.tencent.com。

DDoS 高防 IP 服务是否会自动将回源 IP 地址加入安全组？

不会。用户需手动将回源 IP 段添加至 CVM 安全组中。若用户在源站部署了防火墙或其它主机安全防护软件，也将回源 IP 段添加至相应的白名单中，防止将高防回源 IP 拦截或限速导致业务流量受损。

DDoS 高防 IP 中的源站 IP 可以填写内网 IP 吗？

DDoS 高防 IP 是通过公网进行回源的，不可以直接填写内网 IP。

修改 DDoS 高防 IP 服务的源站 IP 是否有延迟？

修改高防 IP 服务已防护的源站 IP 可秒级生效。

在 DDoS 高防 IP 服务控制台中，更改配置后大约需要多少时间生效？

DDoS 高防 IP 服务中更改配置是秒级生效的。

DDoS 高防 IP 的 IP 回源支持 IPv6 协议吗？

暂时不支持 IPv6 协议。

DDoS 高防 IP 服务是否支持 HTTPS 双向认证？

- 网站接入方式不支持 HTTPS 双向验证。
- 非网站接入且使用 TCP 转发方式时，支持 HTTPS 双向验证。

DDoS 高防 IP 服务是否有抓包文件？

DDoS 高防 IP 服务支持下载抓包文件，具体操作请参考 [查看统计报表](#)。

DDoS 高防 IP 在配置多个源站 IP 时如何负载？

- 网站业务采用源 IP 哈希方式进行负载均衡。
- 非网站业务采用加权轮询方式依次轮流转发。

DDoS 高防 IP 支持转发端口数及支持的域名数分别是多少？

- 转发端口数：TCP/UDP 协议支持转发规则条目总数，默认免费提供60个，支持扩展。
- 支持域名数：HTTP/HTTPS 协议支持转发规则条目总数，默认免费提供60个，支持扩展。

什么是业务带宽，超过之后会有什么影响？

购买的业务带宽是针对整个高防 IP 实例的，指该实例所有正常业务的 IN 或者 OUT 方向的流量。

如果用户的业务流量超过所赠送的规格，将触发流量限速，可能导致随机丢包。若持续出现这种情况，请及时升级更大的业务带宽。

说明：

购买 DDoS 高防 IP 服务，默认赠送100M转发业务带宽。

DDoS 高防 IP 服务是否支持会话保持？

DDoS 高防 IP 服务支持会话保持，默认不开启。非网站业务可以通过控制台进行配置操作，请参考 [配置会话保持](#)。

DDoS 高防 IP 服务是否支持健康检查？

非网站业务默认开启健康检查，建议使用默认值，如需要修改，请参考操作步骤 [配置健康检查](#)。

在用户业务绑定 DDoS 高防 IP 后，源站服务器未开启窗口因子 WS 时，访问源站为什么会出现速度慢？

高防服务器默认是开启窗口因子 WS（Window Scaling），若源站服务器未开启，将会导致接收稍大文件数据时，很快把滑动窗口占满出现延迟。建议用户将源站所有服务器开启 WS。关于 WS 的概念及示例说明，可前往腾讯社区 [TCP 速度慢？注意 WS 窗口因子](#) 了解。

计费相关问题

最近更新时间：2019-12-23 15:38:35

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 IP 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 IP 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 IP 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 IP 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 [产品概述](#)。

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 IP 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。