DDoS 高防 IP

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：2022-08-16 11:36:49

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。

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。

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，选择适当的防护带宽，尽可能地确保最大防护能力大于历史攻击流量峰值。

怎样避免解封后再次被封堵？

建议开启高弹性防护，可帮助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。

攻击相关问题

最近更新时间：2023-04-25 15:25:29

有 DDoS 攻击会通知吗？

在遭受 DDoS 攻击后，后台会进行告警通知推送。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。具体操作请参考 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业务，而并非针对服务器对应的 IP 和域名。
- 您的业务连接外网通信，就有风险遭受 DDoS 攻击。

购买了 DDoS 高防 IP 产品，为什么还是被攻击？

- 您的业务连接外网通信，就有风险遭受 DDoS 攻击。
- DDoS 高防 IP 产品保护您的业务在 DDoS 攻击下尽可能的不造成损失。

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。

DDoS 高防 IP 的攻击统计数据分为了哪几类？

DDoS 高防 IP 的攻击统计数据有攻击总流量，攻击包量，攻击总次数。

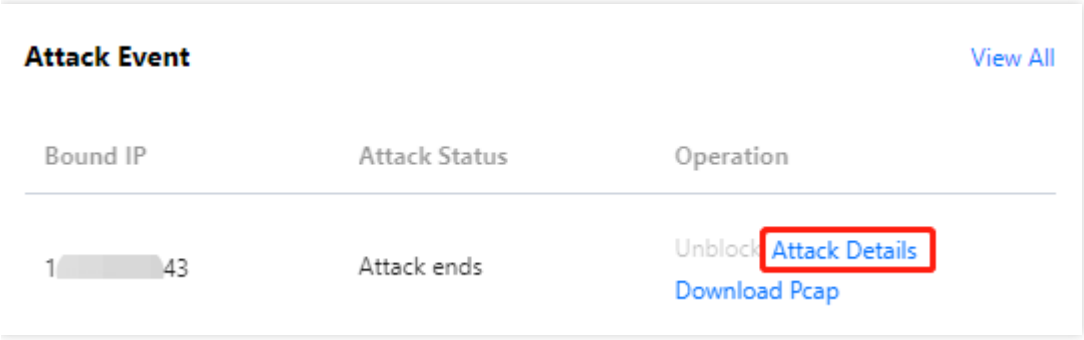
- **攻击总流量**：查看该时间范围内，所选择的高防 IP 遭受攻击事件中各协议总攻击流量的占比情况。
- **攻击包量**：查询该时间范围内，所选择的高防 IP 遭受攻击事件中各协议攻击包总数的占比情况。
- **攻击总次数**：查询该时间范围内，所选择的高防 IP 遭受的各攻击类型总次数占比情况。

在哪里可以查看服务器被攻击的日志？

在 防护概览 页面的最近安全事件模块中，可查看近期的攻击事件详情和日志。

攻击源 IP，哪里可以查看？

在 防护概览 页面的最近安全事件模块中，选择想查看的攻击事件，单击**查看详情**，支持查看攻击源信息、攻击源地区、产生的攻击流量及攻击包量大小。



轻量服务器被 DDoS 攻击，怎么办？

腾讯云内用户，购买 DDoS 高防 IP 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？

所有业务在中国大陆的云内用户，无需购买 DDoS 高防 IP，每个公网 IP 都享受平台赠送的基础 DDoS 防护，VIP 用户默认防护上限为10G，普通用户默认防护上限2G。境外地区用户统一都是2G。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。

功能相关问题

最近更新时间：2022-01-17 17:00:35

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。

> 说明：
> 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，也需将回源 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？

没有延迟，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？

新版 DDoS 高防 IP 服务暂不支持下载攻击包文件。

DDoS 高防 IP 在配置多个源站 IP 时如何负载？

- 网站业务采用默认轮询方式进行负载均衡。
- 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，最高支持500个。
- 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，最高支持500个。

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，请及时调整为更大的业务带宽。

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。

计费相关问题

最近更新时间：2022-01-28 10:47:08

想要中止高防IP服务怎么办？

DDoS 高防IP服务为后付费模式。当您想要结束该服务请务必提交工单至客服申请销毁资源，若资源未销毁，可能会持续产生费用。

- 当月申请资源销毁后本月各项费用不变（包年包月项的费用照常支付，按天按量计费项根据实际资源销毁时产生费用为准进行支付），资源销毁后该资源防护服务立即终止，次月资源不再计费。
- 整个销毁流程需要1-3个工作日完成，具体时长以实际操作时间为准（销毁期间可能会陆续产生防护费用）。

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，因此超出弹性防护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。

业务遭受攻击过程中，是否支持升级弹性防护带宽？

支持。DDoS 高防 IP 服务弹性防护带宽支持调升也支持调降。不同地域支持的防护能力不同，弹性防护带宽的范围请参考购买界面。

> 说明：
> 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带宽进行计费。

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。