DDoS 防护

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：2024-05-06 15:10:20

DDoS 高防所防护的 IP 被封堵了该怎么办？

每天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。

如解封次数用完：

未购买 DDoS 高防用户，建议用户购买高防包，首次绑定设备可进行解封。
已购买 DDoS 高防用户，建议用户升级防护套餐，可提前解除封堵。
详情请参见：业务被大流量攻击导致封堵。

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。

会封堵多长时间？

封堵时长默认为2小时，实际封堵时长与封堵触发次数和攻击峰值相关，最长可达24小时。
封堵时长主要受以下因素影响：
攻击是否持续：若攻击一直持续，封堵时间会延长，封堵时间从延长时刻开始重新计算。
攻击是否频繁：被频繁攻击的用户遭遇持续攻击的概率较大，封堵时间会自动延长。
攻击流量大小：被超大型流量攻击的用户，封堵时间会自动延长。
说明：
针对个别封堵过于频繁的用户，腾讯云保留延长封堵时长和降低封堵阈值的权利。
关于查看封堵解除时间，请参见 查看封堵时间。

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？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。
使用 DDoS 高防包（轻量版）的用户每月提供3次自助解封能力，自助解封能力仅可用于解封轻量服务器资源。

IP 被封堵可以更换服务器 IP 吗?

封堵时不支持，解封后才能更换服务器 IP。
当您的服务器遭受 DDoS 被封堵后，不建议立即更换 IP。更换服务器 IP 并不能解决您的服务器被 DDoS 攻击的风险。频繁更换 IP，对后端防护系统的检测分析会产生一定影响，也会影响云平台的稳定性。因此，当您业务遇到多次 DDoS 攻击时，推荐您使用 DDoS 高防产品来提高您业务的防护能力，解决 DDoS 安全风险。

攻击相关问题

最近更新时间：2024-05-06 15:10:20

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？

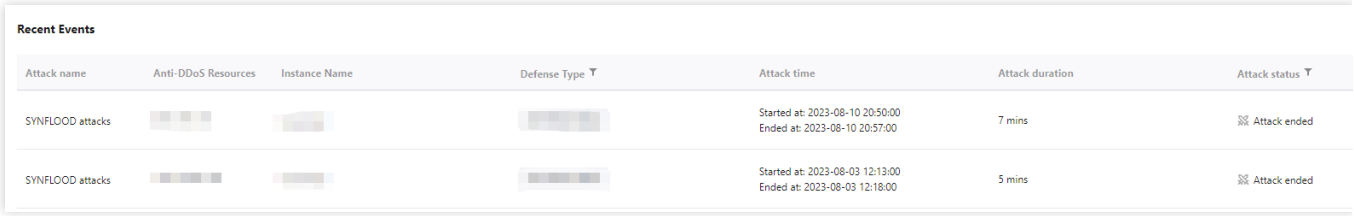
网络层攻击：常见攻击类型包括 UDP 反射攻击、SYN Flood 攻击及连接数攻击；这类攻击以消耗服务器带宽资源和连接资源从而达到拒绝服务的目的。
应用层攻击：常见攻击类型包括 DNS Flood 攻击、HTTP Flood 攻击及 CC 攻击；这类攻击以消耗服务器处理性能从而达到拒绝服务的目的。

在哪里可以查看服务器被攻击的日志？

在 防护概览 页面，可查看服务器在不同时间维度下的攻击日志。

攻击源 IP，哪里可以查看？

在 防护概览 页面，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 高防产品 能有效抵御 DDoS 攻击，保证您的服务器与业务正常运作。

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：2024-05-06 15:10:20

DDoS 高防包

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，请您购买 DDoS 高防 IP，支持网站域名和业务端口的接入防护。

DDoS 高防包支持防护 VPN 网关吗？

支持。

DDoS 高防包支持防护 AnycastEIP 吗？

AnycastEIP 不支持接入 DDoS 高防包，如需 DDoS 防护，请先购买 DDoS 高防 IP（境外企业版） 后在高防 IP 中进行绑定。

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

不会，用户享有的最终防护峰值，以 DDoS 高防包购买套餐里的防护能力为准，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 原本享有不超过2Gbps的免费防护带宽。因经常遭受攻击，用户又为该 IP 购买了 DDoS 高防包套餐，则最大防护能力为当前本地高防包资源的最大防护能力。

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 面向云内外用户，支持网站域名和业务端口接入防护。
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。
定价策略	按“防护IP数+防护次数”售卖，并提供全力防护，无额外弹性费用。	计费复杂，需要付流量费。

托管 IP 指的是？

托管 IP 指的是定制的网络路由方案，非 DDoS 高防包提供的能力，但 DDoS 高防包支持这种产品的防护。
如有托管 IP 的需求，可 提交工单 申请使用。

DDoS 高防包若超过防护的阈值有什么影响?

DDoS 高防包中没有阈值的概念。

轻量版高防包是否提供3次自助解封能力？

提供，轻量版高防包每月提供3次自助解封能力。

轻量版高防包自主解封功能，是否支持解封非 Lighthouse 资源?

不支持，仅支持解封 Lighthouse 资源。

使用轻量服务器，需要购买那个版本的 DDoS 高防包？

两个版本 DDoS 高防包均可购买进行防护轻量服务器，区别在于防护能力和折扣力度，详情请参见 购买指南。

DDoS 高防 IP

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 安全防护策略中行为模式分析，具体是指什么行为模式？

行为模式分析主要包括查看是否有攻击特征的报文，查看是否有攻击不符合协议规范的报文，以及查看是否有异常连接攻击的特征等。您可根据业务特点灵活设置，应对不断变化的攻击手法，设置详情请参见 防护配置。

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。

什么是高防回源 IP 地址？

用户业务接入后，系统自动分配多个回源 IP 地址，回源 IP 地址作为高防 IP 的出口 IP，把经过清洗过滤的正常访问流量，导向到用户源站。使用的出口 IP 地址，即从源站上看到的业务流量来源 IP 地址。

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 如何区分4层还是7层转发？

DDoS 高防 IP 区分4层还是7层转发方式如下：
4层转发：使用 IP + 端口的方式，即“端口接入”的方式。
7层转发：使用域名接入的方式。

DDoS 高防 IP 的防护带宽是指什么？

防护带宽分为保底防护带宽和弹性防护带宽。
保底防护带宽：指高防 IP 实例的保底防护能力，保底部分为包年包月预付费。
弹性防护带宽：指高防 IP 实例的最大弹性防护能力，弹性部分为按天后付费。
若未开启弹性防护，则保底防护带宽为高防 IP 实例的最高防护能力。
若已开启弹性防护，则弹性防护带宽作为高防 IP 实例的最高防护能力。

当攻击流量超过高防 IP 实例的最高防护能力后触发封堵。

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。

CC 防护的 IP 黑白名单限额是多少，是否支持扩容？

CC 防护支持设置的 IP 黑白名单数为各50个。如需设置更多的 IP 黑白名单，可 提交工单 申请扩容。

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。
说明：
购买 DDoS 高防 IP 服务， 且业务在中国大陆的云内用户默认赠送 100Mbps 转发业务带宽；境外没有赠送。

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，请参见 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，请参见操作步骤 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，可联系我们了解。

计费相关问题

最近更新时间：2024-05-06 15:10:20

DDoS 高防包

DDoS 高防包购买后，是否即时生效？

购买且接入成功后立即生效。

流量每月最大值95消峰是如何计算的？

以5分钟粒度进行采样，1个自然月为统计时长。月底将所有的采样点按峰值从高到低排序，去掉5%的最高峰值采样点，以第95%个最高峰作为95计费点带宽。

例如：一月内每5分钟取一个流量点，1个小时12个点，1天12 × 24个点，一个月按30天算12 × 24 × 30 = 8640个点，把数值最高的5%的点去掉，剩下的最高带宽就是95计费的计费值。

DDoS 高防包的全力防护和 DDoS 高防 IP 的弹性防护计费方式有什么区别？

当遭受攻击时，自动调用该高防包实例所在地域的腾讯云最大 DDoS 防护能力提供全力防护。全力防护服务包含在高防包中，不额外产生弹性防护费用。
DDoS 高防 IP 服务的弹性防护计费按照当日产生最大攻击流量对应弹性防护区间带宽进行计费。

DDoS 高防 IP

购买 DDoS 高防 IP 后，怎么绑定 IP？

可以参考 网站业务接入 或 非网站业务接入 文档来绑定 IP。

如何选择线路？

购买 DDoS 高防 IP 时，若您的服务器是中国大陆的选择三网，一般非中国大陆的选择 BGP。

一个腾讯云账号可以同时购买多少个 DDoS 高防 IP ？

暂时没有什么数量上的限制，一般的购买量都是支持的，若是有特殊的极大的需求，无法成功购买，请 提交工单 联系我们获得帮助。

高防服务的弹性防护计费模式是否一样？如何计算的？

一样，触发弹性防护后，按照当天最高攻击峰值扣减保底防护后，所对应的弹性防护区间计费，计费详情请参见 计费概述。

例如，您购买的 DDoS 高防 IP 实例规格是30Gbps 保底防护带宽 + 60Gbps 弹性防护带宽。如果当天发生 DDoS 攻击事件且最高攻击流量峰值为45Gbps。45Gbps 已超过保底防护带宽范围且触发弹性防护，落入10Gbps ≤ （攻击峰值45Gbps - 保底防护带宽30Gbps = 15Gbps）＜ 20Gbps 计费区间，当天产生弹性费用按照10Gbps ≤ 弹性峰值 ＜ 20Gbps 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。

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。

DDoS 高防 IP 如何退款？

DDoS 高防 IP 服务不支持提前退订，不适用五天无理由退款。若您已使用了 DDoS 高防 IP 实例，一概不支持退款。