DDoS 防护

产品简介

腾讯云

文档目录

产品简介

产品概述

最近更新时间：2023-10-24 17:02:42

简介

DDoS 防护（Anti-DDoS）具有全面、高效、专业的 DDoS 防护能力，为企业组织提供 DDoS 基础防护、DDoS 高防包、DDoS 高防 IP 等多种 DDoS 解决方案，应对 DDoS 攻击问题。通过充足、优质的 DDoS 防护资源，结合持续进化的“自研+AI 智能识别”清洗算法，保障用户业务的稳定、安全运行。防护场景覆盖游戏、互联网、视频、金融、政府等行业。

产品套餐

DDoS 高防包

DDoS 高防包（标准版）

DDoS 高防包（标准版）是针对业务部署在境内的腾讯云用户。
腾讯云会给予全力防护，最高防护能力根据各区域的实际网络情况动态调整，无需更换 IP 地址，购买后只需绑定需要防护的 IP 即可使用。

DDoS 高防包（企业版）

DDoS 高防包（企业版）是针对业务部署在境内外的腾讯云用户。
具有境内外 T 级防护能力，需创建高防 EIP 并绑定才能最终生效。适用对业务安全要求较高的企业。丰富的防护能力可灵活选择配置，根据需求搭配购买，控制业务防护成本。

- 中国大陆地区：防护能力采用保底防护 + 弹性防护的方式。
- 境外地区：利用腾讯云高防清洗中心能力做全力防护。

> **说明：**
> - 中国大陆地区：北京、上海、广州。
> - 境外地区：中国香港、新加坡、东京、雅加达、硅谷、法兰克福、弗吉尼亚、圣保罗。
> - 全力防护：以成功防护每一次 DDoS 攻击为目标，整合当前本地清洗中心能力，全力对攻击进行抵御。境内外都具有 T 级防护能力。

DDoS 高防包（轻量版）

DDoS 高防包（轻量版）是针对腾讯云轻量应用服务（TencentCloud Lighthouse）用户的专属高防产品。
具有境内最高不超过10Gbps的全力防护能力，无需更换 IP 地址，购买后只需绑定需要防护的 IP 即可使用。是一款专为腾讯云轻量应用服务定制的轻量的防护产品。

DDoS 高防 IP

DDoS 高防 IP（大陆）、DDoS 高防 IP（境外标准版）

DDoS 高防 IP 是针对游戏、互联网及金融等业务遭受大流量DDoS 攻击导致用户服务不可用的情况而推出的付费防护服务。配置高防IP，将业务 IP 指向 DDoS 高防 IP 或业务的 DNS 域名解析到 CNAME 地址进行引流，所有公网流量将优先经过高防集群，攻击流量将在高防清洗中心进行清洗过滤，正常访问流量转发到业务源站服务器，从而确保源站业务的稳定可用。
DDoS 高防 IP 使用公网代理的接入方式，支持 TCP、UDP、HTTP、HTTPS 和 HTTP2 等协议，覆盖金融、电商、游戏等各类业务。

DDoS 高防 IP（境外企业版）

DDoS 高防 IP（境外企业版）是针对业务部署在腾讯云内的用户提升 DDoS 境外防护能力的付费产品。

- DDoS 高防 IP（境外企业版）提供全球各地10个腾讯云入口，分担各单个入口带宽压力，并提供全力防护服务。最大限度保证各地节点访问的畅通。
- Anycast 实现近源清洗、近源回注，提供全球 T 级防护能力。通过各清洗节点之后的正常业务流量将会近源回注到服务器，保证业务流量的畅通与低延迟。DDoS 高防 IP（境外企业版）直接对腾讯云上 IP 生效。

产品功能

多类型防护

防护分类	描述
畸形报文过滤	过滤 Frag Flood，Smurf，Stream Flood，Land Flood 攻击，过滤 IP 畸形包、TCP 畸形包、UDP 畸形包。
网络层 DDoS 攻击防护	过滤 UDP Flood、SYN Flood、TCP Flood、ICMP Flood、ACK Flood、FIN Flood、RST Flood、DNS/NTP/SSDP 等反射攻击、空连接。
应用层 DDoS 攻击防护	过滤 CC 攻击，支持 HTTP 自定义特征过滤如 host 过滤、user-agent 过滤、referer 过滤。

> **说明：**
> 应用层 DDoS 攻击防护仅支持 DDoS 高防 IP。

绑定和切换防护对象

DDoS 防护支持防护对象 IP 切换，满足您不同云资源公网 IP 需要防护的需求，支持切换的对象包括 CVM、CLB、WAF、NAT 网关等。

安全防护策略

DDoS 防护默认提供基础安全策略，策略基于 攻击画像、行为模式分析、AI 智能识别等防护算法，有效应对常见 DDoS 攻击行为。同时提供多样化、灵活的 DDoS 防护策略，您可根据特殊业务特点灵活设置，应对不断变化的攻击手法。

封堵自助解除

当攻击流量突发或 DDoS 防护的防护带宽较小，造成接入高防的业务 IP 被封堵时，您可通过控制台进行自助解除。

防护统计报表

- DDoS 高防包提供多维度流量报表及攻击防护详细信息，帮助您及时、准确了解 DDoS 高防包的防护效果。
- DDoS 高防 IP 提供 DDoS 攻击、CC 攻击、转发流量等多维度数据的统计与展示，帮助用户实时掌握业务和攻击情况，同时支持对攻击自动抓包，方便用户快速定位异常问题。
- DDoS 高防 IP（境外企业版）提供多维度流量报表及攻击防护详细信息，帮助您及时、准确了解境外 Anycast DDoS 高防 IP 的防护效果。

清洗模式自定义

DDoS 高防 IP 支持多种防护等级，提供自定义清洗阈值，用户可根据攻击情况灵活调整，对不同类型的 DDoS 攻击快速响应，充分匹配不同用户不同业务类型。

产品优势

最近更新时间：2023-07-21 09:44:22

DDoS 高防包

仅适用于腾讯云产品，包含 CVM、CLB、WAF、NAT 网关、轻量应用服务器等云产品，为其提供提升 DDoS 防护能力的付费安全服务，具有以下优势：

一键接入，零变更

无需进行业务变更，接入配置便捷，购买 DDoS 高防包后，仅需绑定需要防护的云产品 IP 地址即可使用，几分钟即可生效。

支持双协议防护

DDoS 高防包支持同时为 IPV6 和 IPV4 两种类型的 IP 提供防护，满足客户对 IPV6 类型服务器的防护需求，无需额外购买或升级高防包，绑定需要防护的云产品 IP 地址后即可实现 DDoS 防护。

超大防护资源

DDoS 高防包拥有超大 BGP 防护带宽，覆盖电信、联通、移动等不同运营商，轻松抵御 DDoS 攻击，满足活动大促、活动上线等重要业务的安全稳定性保障需求。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

极速访问体验

腾讯云 BGP 链路对接全国各地30家运营商，覆盖面广，能有效解决访问时延问题，保障各类用户群的访问速度，带来极速访问体验。

丰富的防护报表

DDoS 高防包提供多维度统计报表，展示清晰、准确的攻击防护流量，以及攻击详情信息，使用户及时了解攻击实况。

优化安全成本

简化计费方式，您可以根据业务规模及防护需要，灵活选择“防护 IP 数”，当遭受大流量攻击时，调用当前地域腾讯云最大 DDoS 防护能力提供全力防护，无需额外支付弹性费用，为您降低日常安全支出。

DDoS 高防 IP

DDoS 高防 IP（大陆）、DDoS 高防 IP（境外标准版）

DDoS 高防 IP（大陆）、DDoS 高防 IP（境外标准版）是腾讯云针对云外用户业务，在遭受大流量 DDoS 攻击后，导致服务不可用时，推出的付费产品，其产品优势如下：

超大防护资源

腾讯云 BGP 链路对接全国各地30家运营商，单客户单点可提供高达1T的 DDoS 防护能力。提供70万 QPS 的 CC 防护能力。境外数十个防护节点，高达400Gbps 防护能力，轻松应对各类 DDoS 攻击。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

极速访问体验

腾讯云 BGP 链路对接全国各地30家运营商，覆盖面广，能有效解决访问时延问题，保障各类用户群的访问速度，带来极速访问体验。

隐藏用户源站

DDoS 高防 IP（大陆）、DDoS 高防 IP（境外标准版）服务可对用户源站进行替换并隐藏。使用高防 IP 作为源站的对外服务地址，所有业务访问流量都经过高防 IP，将正常访问流量转发到源站，攻击流量的高防 IP 上被清洗，清洗干净后高防 IP 将干净流量返回给源站。

全业务支持

DDoS 高防 IP（大陆）、DDoS 高防 IP（境外标准版）服务支持网站和非网站业务，覆盖金融、电商、游戏、政府等各类业务，充分满足用户不同业务的安全防护需求。

定价灵活，优化成本

提供“保底防护+弹性防护”相结合计费方式，为用户降低日常安全费用，在需要时按需调整弹性防护，无需新增任何设备，无需调整配置。当攻击流量超过保底防护峰值时，腾讯云仍为用户继续防护，保障业务不中断，按当天实际攻击量付费。

丰富的攻击防护报表

提供精准的防护流量报表及攻击详情信息，使用户及时了解攻击实况。支持对攻击自动抓包，方便事后进行分析以及溯源。

DDoS 高防 IP（境外企业版）

贴合云原生的防护架构，一键接入

产品方案更贴合云原生的防护架构，接入配置便捷。购买 DDoS 高防 IP（境外企业版）后，只需要将高防实例关联到所需的防护对象，实现一键式接入，快速部署。

超大防护资源

DDoS 高防 IP（境外企业版）整合腾讯云中国大陆以外的高防清洗中心能力，覆盖境外10个清洗节点，提供全球 T 级防护能力，满足活动大促、活动上线等重要业务的安全稳定性保障需求。

领先的清洗能力

依托腾讯自研防护集群，采用 IP 画像、行为分析、Cookie 挑战等多维算法，并通过 AI 智能引擎持续更新防护算法，精准快速检测业务流量，灵活应对各类攻击行为。

稳定访问体验

腾讯云 BGP 链路对接多家运营商，覆盖面广，能有效解决访问时延问题保证网络质量。智能选择路由并自动完成网络调度，保障各类用户群的访问稳定性，带来稳定与流畅的访问体验。

丰富的防护报表

DDoS 高防 IP（境外企业版）提供多维度统计报表，展示清晰、准确的攻击防护流量，以及攻击详情信息，让用户及时了解攻击实况。

优化安全成本

1. 简化计费方式，您可以根据业务规模及防护需要，灵活选择 “防护 IP 数+无限次全力防护”，当遭受大流量攻击时：
   - 利用全球多个节点防护能力，来同时分担和抵御DDoS 攻击流量实现全力防护。
   - 采用调度&封堵结合的方式，为客户最大化提供的业务可用性，增加被攻击时的可用性。
2. 业务带宽按需后付费，季度售卖的灵活计费模式，为您降低日常安全支出。

应用场景

最近更新时间：2023-07-21 09:44:23

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 防护能有效保证游戏的可用性和持续性，保障游戏玩家流畅体验，同时为活动、新游戏发布或节假日游戏收入旺季时段保驾护航，确保游戏业务正常。

互联网

保证互联网网页的流畅访问，业务正常不中断，对电商大促等重大活动时段，提供安全护航。

金融

满足金融行业的合规性要求，保证线上交易的实时性及安全稳定性。

政府

满足国家政务云建设标准的安全需求，为重大会议、活动、敏感时期提供安全保障，保障民生服务正常可用，维护政府公信力。

企业

保障企业站点服务持续可用，避免 DDoS 攻击带来的经济及企业品牌形象损失问题，零硬件零维护，节省安全成本。

电商

电商境外业务遍布世界各地，伴随着不同地区的节日与各种促销，访问与订单不断上升。DDoS 防护能有效保障全球的业务正常不中断，对电商大促等重大活动时段，提供安全护航。

相关概念

最近更新时间：2023-07-21 09:44:23

DDoS 攻击

分布式拒绝服务攻击（DistributedDenial of Service，DDoS）是指攻击者通过网络远程控制大量僵尸主机向一个或多个目标发送大量攻击请求，堵塞目标服务器的网络带宽或耗尽目标服务器的系统资源，导致其无法响应正常的服务请求。

网络层 DDoS 攻击

网络层 DDoS 攻击主要是指攻击者利用大流量攻击拥塞目标服务器的网络带宽，消耗服务器系统层资源，导致目标服务器无法正常响应客户访问的攻击方式。
常见攻击类型包括 SYN Flood、ACK Flood、UDP Flood、ICMPFlood 以及 DNS/NTP/SSDP/memcached 反射型攻击。

CC 攻击

CC 攻击主要是指通过恶意占用目标服务器应用层资源，消耗处理性能，导致其无法正常提供服务的攻击方式。
常见的攻击类型包括基于 HTTP/HTTPS 的 GET/POST Flood、四层 CC 以及 Connection Flood 等攻击方式。

防护能力

防护能力指抵御 DDoS 攻击的能力， DDoS 防护服务承诺根据当前地域腾讯云最大 DDoS 防护能力提供全力防护。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云 DDoS 防护系统将自动对该 IP 的公网入向流量进行清洗。通过 BGP 路由协议将流量从原始网络路径中重定向到腾讯云 DDoS 清洗设备上，通过清洗设备对该 IP 的流量进行识别，丢弃攻击流量，将正常流量转发至目标 IP。
通常情况下，清洗不会影响正常访问，仅在特殊场景或清洗策略配置有误时，可能会对正常访问造成影响。当流量持续一定时间（根据攻击情况动态判断）没有异常时，清洗系统会判定攻击结束，停止清洗。

封堵

当目标 IP 受到的攻击流量超过其封堵阈值时，腾讯云将通过运营商的服务屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。简而言之，当您的某个 IP 受到的攻击流量超过当前地域腾讯云最大防护能力时，腾讯云将屏蔽该 IP 的所有外网访问。当您的防护 IP 被封堵时，您可以登录管理控制台进行自助解封。

封堵阈值

DDoS 高防实例的防护 IP 的封堵阈值等于当前地域最大防护能力。

封堵时长

封堵时长默认为2小时，实际封堵时长与当日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。

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。

防护带宽

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。

> **说明：**
> - 弹性防护默认关闭。如需开启弹性防护，请在知悉弹性相关收费后自助开启。用户可以根据自身业务需求，随时调整弹性防护带宽。
> - 防护带宽仅支持高防 IP 和高防 IP 境外企业版。

弹性防护带宽的作用

开启弹性防护后，当攻击流量超过购买的保底防护能力且在弹性防护能力范围内时，腾讯云 DDoS 高防 IP 可继续为用户提供防护，保障业务访问持续性。

弹性防护如何收费

开启弹性防护后，当攻击流量超过保底防护能力时，会触发弹性防护并收取费用，取当天实际产生的最高攻击峰值所对应区间进行计费，账单次日生成。
例如，您购买的保底防护为20Gbps，且设置的弹性防护为50Gbps。若当天的实际攻击峰值为35Gbps，则需要支付10Gbps - 20Gbps区间的弹性防护费用。

封堵策略

最近更新时间：2023-07-21 09:44:23

什么是封堵

当目标 IP 受到的攻击流量超过其封堵阈值时，腾讯云将通过运营商的服务屏蔽该 IP 的所有外网访问，保护云平台其他用户免受影响。

> **说明：**
> - 封堵阈值：DDoS 高防实例防护 IP 的封堵阈值等于当前地域最大防护能力。
> - 全力防护指以成功防护每一次 DDoS 攻击为目标，整合当前本地清洗中心能力。

简而言之，当您的某个 IP 受到的攻击流量超过当前地域腾讯云最大防护能力时，腾讯云将屏蔽该 IP 的所有外网访问。

如何解除封堵?

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。

> **说明：**
> DDoS 高防包和 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。

若您无法等待封堵自动解封，可以参考 业务被大流量攻击导致封堵 进行处理。

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。

封堵时长

封堵时长默认为2小时，实际封堵时长与当日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。

相关产品

最近更新时间：2023-08-10 17:42:11

使用 DDoS 防护可为如下产品提升 DDoS 防护能力：

- 云服务器：是腾讯云提供的可扩展的计算服务。使用云服务器 CVM 避免了使用传统服务器时需要预估资源用量及前期投入的问题，帮助您在短时间内快速启动任意数量的云服务器并即时部署应用程序。
- 负载均衡：提供安全快捷的流量分发服务，访问流量经由 CLB 可以自动分配到云中的多台云服务器上，扩展系统的服务能力并消除单点故障。
- Web 应用防火墙：是一款基于 AI 的一站式 Web 业务运营风险防护方案。
- NAT 网关：是一种支持 IP 地址转换服务，提供 SNAT 和 DNAT 能力，可为私有网络（VPC）内的资源提供安全、高性能的 Internet 访问服务。
- VPN 连接：是一种基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的传输服务，它能帮您在 Internet 上快速构建一条安全、可靠的加密通道。
- 裸金属云服务器：是一种可按需购买、按量付费的物理服务器租赁服务，提供给您云端专用的高性能、安全隔离的物理服务器集群。
- 黑石负载均衡：通过虚拟服务地址（VIP），将位于同一可用区的多台物理服务器资源虚拟成一个高性能、高可用的应用服务池。
- 黑石弹性公网 IP：黑石弹性公网 IP（Elastic IP，EIP）地址是专用于动态云计算的 IP 地址，是可以独立申请的公网 IP 地址。
- 全球应用加速：是一款实现业务全球最佳访问延迟的 PAAS 类产品，依赖全球节点之间的高速通道、转发集群及智能路由技术，实现各地用户的就近接入，并将流量转发至源站，帮助业务解决全球用户访问卡顿或者延迟过高的问题。
- 弹性网卡：是绑定私有网络（Virtual Private Cloud，VPC）内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡对配置管理网络与搭建高可靠网络方案有较大帮助。
- 轻量应用服务器：是新一代开箱即用、面向轻量应用场景的云服务器产品，助力中小企业和开发者便捷高效的在云端构建网站、Web 应用、小程序/小游戏、App、电商应用、云盘/图床和各类开发测试环境，相比普通云服务器更加简单易用且更贴近应用，以套餐形式整体售卖基础云资源并提供高带宽流量包，将热门开源软件融合打包实现一键构建应用，提供极简上云体验。