DDoS 高防 IP 专业版

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2019-12-23 15:40:48

简介

DDoS 高防 IP 专业版是 DDoS 防护基于腾讯丰富业务攻击防护实践积累，为互联网业务提供高可用、高性价比的应对 DDoS 攻击的安全防护产品，可解决超大流量的 DDoS 攻击。
相比 DDoS 高防 IP，DDoS 高防 IP 专业版支持跨地域 T 级大流量抗 DDoS 攻击，最高防护带宽可达1.7T。DDoS 高防 IP 专业版采用 CNAME 智能调度，实现多线路防护，即使遭遇封堵也能灵活切换，充分保障业务连续性。用户根据源站地域和所需防护能力购买 DDoS 高防 IP 专业版实例，即可实现 DDoS 防护需求。
通过配置 DDoS 高防 IP 专业版服务，将用户源站服务器所有访问流量牵引至高防 IP 集群并清洗攻击流量，并将过滤后的正常流量返回至源站服务器，从而保障用户业务稳定可用。

主要功能

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 攻击和 HTTP 慢速攻击，支持 HTTP 自定义特征过滤（如 host 过滤、user-agent 过滤、referer 过滤等）

高级安全策略自定义

DDoS 高防 IP 专业版提供最简化的云 DDoS 防护体验，同时也提供 DDoS 高级防护策略，用户可根据特殊业务应用防护需求和攻击行为灵活设置，对特定攻击行为进行针对性的防护。

清洗模式自定义

开放多套防护等级，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。

防护统计及分析

DDoS 高防 IP 专业版实时为用户提供详细的流量报表及攻击防护详细信息，便于用户了解当前业务的防护实况，同时支持对攻击数据进行抓包下载，让用户快速定位异常问题，保证业务稳健运行。

支持的地域

DDoS 高防 IP 专业版既支持同地域高防 IP 防护资源，也支持跨地域高防 IP 智能调度防护资源。
目前已开放高防 IP 专业版的地域包括：

- 中国内地（大陆）区域：华南地区（广州）、华东地区（上海）和华北地区（北京）。
- 境外区域：中国香港、中国台湾、日本东京、新加坡、韩国首尔、美西硅谷。

DDoS 高防 IP 专业版在不同地域提供的高防能力请参考如下表格：

地域	保底防护	弹性防护	最大防护能力
华南地区（广州）	20Gbps - 50Gbps	30Gbps - 1.7Tbps	1.7Tbps
华东地区（上海）	20Gbps -100Gbps	30Gbps - 1.7Tbps	1.7Tbps
华北地区（北京）	20Gbps - 50Gbps	30Gbps - 1.7Tbps	1.7Tbps
境外区域	20Gbps - 50Gbps	30Gbps - 400Gbps	400Gbps

> 说明：
> 建议选择最靠近源站的地域，可降低访问时延、提高访问速度。

产品优势

最近更新时间：2019-12-23 15:40:56

DDoS 高防 IP 专业版是腾讯云面向所有用户推出的抗 DDoS 攻击的付费产品，其产品优势如下：

CNAME 智能调度

采用 CNAME 智能调度，降低攻击对业务的影响。用户无需考虑地域资源，按所需防护能力购买即可。当遭遇超大攻击流量，系统智能切换防护线路，保证业务连续性。

超大防护资源

共享腾讯海量自营业务基础架构资源，具备丰富、强大的防护资源优势。中国内地（大陆）为单用户提供 T 级以上防护能力，境外支持高达400G防护能力，轻松抵御大流量 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，提供极速访问体验。

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，按当天实际攻击量收费。

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。

应用场景

最近更新时间：2019-12-23 15:41:01

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 高防 IP 专业版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，防止业务中断。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、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

保证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。

相关概念

最近更新时间：2019-12-23 15:41:05

DDoS 攻击

Distributed Denial of Service（DDoS），即分布式拒绝服务攻击，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、ICMP Flood 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。

防护峰值

防护峰值分为保底防护峰值和弹性防护峰值。

- 保底防护峰值：指高防服务实例的保底防护带宽能力，保底部分为按月预付费。
- 弹性防护峰值：指高防服务实例的最大弹性防护带宽能力，弹性部分为按天后付费。

若未开启弹性防护，则保底防护峰值为高防服务实例的最高防护峰值。 若已开启弹性防护，则弹性防护峰值作为高防服务实例的最高防护峰值。当攻击流量超过高防服务实例的最高防护峰值后触发封堵。

> 说明：
> 弹性防护默认关闭，如需开启弹性防护，请先在了解 弹性相关收费 后进行 购买 配置。

弹性防护峰值的作用

开启弹性防护后，当攻击流量峰值超过购买的保底防护峰值且在配置弹性防护峰值范围内时，腾讯云 DDoS 高防 IP 专业版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峰值时，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弹性防护区间进行计费，账单次日生成。
例如，您购买的保底防护为20Gbps，且配置的弹性防护为50Gbps。若当天的实际攻击峰值为35Gbps，则需要支付30Gbps - 40Gbps区间的弹性防护费用。
详细费用请参见 计费概述 。

清洗

当目标 IP 的公网网络流量超过设定的防护阈值时，腾讯云大禹系统将自动对该 IP 的公网入向流量进行清洗。通过策略路由将流量从原始网络路径中重定向到大禹系统的 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。

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您所购买的高防套餐最大 防护峰值 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 自助解封。

封堵阈值

DDoS 高防 IP 专业版实例的防护 IP 的封堵阈值等于实际购买的最大 防护峰值。DDoS 高防 IP 专业版有多种不同规格，详情请参考 计费概述。

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。被频繁攻击的用户被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。

> 注意：
> 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。

为什么不提供免费无限抗攻击

DDoS 攻击不仅影响被攻击对象，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，不会对正常流量和攻击流量区别收费。
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。

相关产品

最近更新时间：2019-12-23 15:41:09

更多相关产品信息，请参见下表：

产品名称	与 DDoS 高防 IP 专业版的关系
DDoS 高防 IP	DDoS 高防 IP 专业版实例中包含多个高防 IP，DDoS 高防 IP 专业版较 DDoS 高防 IP 具备更高的防护能力，可使用 DDoS 高防 IP 专业版替代 DDoS 高防 IP。
云解析	DDoS 高防 IP 专业版实例为用户提供 DNS CNAME，通过更改 CNAME 的 A 记录，将流量调度到与当前攻击匹配的高防 IP 上。