DDoS 高防 IP

产品简介

产品文档

腾讯云

【版权声明】

【商标声明】

【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

产品简介
产品概述

最近更新时间：2022-08-16 15:28:12

简介

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。

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，支持 HTTP 自定义特征过滤如 host 过滤、user-agent 过滤、referer 过滤

安全防护策略

DDoS 高防 IP 默认提供基础安全策略，策略基于 IP 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，同时提供灵活防护策略，您可针对自身业务需求配置，提供针对性防护。

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。

封堵自助解除

当攻击流量突发或 DDoS 高防 IP 防护带宽较小，造成高防 IP 被封堵，您可在控制台安全防护概览界面进行自助解除。

防护统计及分析

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。

产品优势

最近更新时间：2020-07-07 17:19:07

DDoS 高防 IP 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900Gbps的防护能力。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 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，攻击流量在高防 IP 上被清洗后将干净流量返回给源站，增加源站安全性。

全业务支持

DDoS 高防 IP 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。

应用场景

最近更新时间：2020-07-07 17:19:07

游戏

游戏行业是 DDoS 攻击的重灾区，DDoS 高防 IP 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、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：2022-07-07 09:34:00

DDoS 攻击

分布式拒绝服务攻击（Distributed Denial of Service，DDoS）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冻结付费。
- 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。

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：2022-08-16 11:34:25

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。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 IP 最大防护能力时，腾讯云将屏蔽该 IP 的所有外网访问。当您的高防 IP 被封堵时，您可以登录 DDoS 高防 IP 控制台 进行自助解封。

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。