DDoS 基础防护

产品简介

产品文档

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

产品简介

产品概述

最近更新时间：2023-03-31 17:26:21

简介

DDoS 基础防护是腾讯云免费为云服务器（Cloud Virtual Machine，CVM）、负载均衡（Cloud Load Balancer，CLB）等资源提供的基础 DDoS 防护能力，满足日常安全运营需求。全量用户默认可享受不超过2Gbps防护。腾讯云会根据用户的安全信誉状态，动态调整封堵阈值。安全信誉状态与历史攻击情况、云上基础资源信息等相关。安全信誉过低会影响用户的免费防护能力，直到后续安全信誉恢复。DDoS 基础防护默认开启，实时监控网络流量，发现攻击立即清洗，为腾讯云上公网 IP 秒级开启防护。

说明

- 如需获得更高的 DDoS 防护能力，可选用对应规格的 DDoS 高防包服务，保证业务的日常运营需求。
- 轻量应用服务器均享受不超过2Gbps 防护（不区分用户类型）。

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。

报表管理

- 支持统计攻击事件及攻击流量。
- 支持自定义时间查看攻击报表。

产品优势

最近更新时间：2022-12-14 17:13:52

DDoS 基础防护是免费为腾讯云上用户提供的基础 DDoS 防护能力的服务，可满足用户日常安全运营需求。其产品优势如下：

无需任何配置，自动开启

无需采购昂贵清洗设备，默认为腾讯云上用户自动开启基础 DDoS 防护能力，无需安装。

优质防护资源

采用 BGP 防护资源，优质带宽，保障业务可用和稳定。腾讯云 BGP 链路对接 30家运营商，能有效减少跨网时延，保障用户访问速度。

实时检测，精准防护

基于自研防护集群和防护算法，实时检测，第一时间发现其中的攻击流量，秒级开启防护。基于优秀特征识别算法进行精确识别并清洗，能够有效防御常见 DDoS 攻击，包括但不限于 SYN Flood 及 ICMP Flood 等常见攻击。

应用场景

最近更新时间：2022-12-14 17:13:52

DDoS 基础防护能够为腾讯云上用户提供免费 DDoS 防护能力，满足日常安全运营需求，主要为遭受攻击概率不大，攻击流量不超过免费基础防护能力的云上用户业务提供防护。

> **说明**
> 如需获得更高的 DDoS 防护能力，可根据自身业务需求，选用对应规格的 DDoS 高防包服务，快速应对攻击。

相关概念

最近更新时间：2023-03-31 17:26:22

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。

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

封堵阈值

DDos 基础防护全部用户默认封堵阈值为不超过2Gbps。

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 攻击不仅影响受害者，也会对整个云网络造成严重影响，影响云内其他未被攻击的用户。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，不会考虑是正常流量或是攻击流量而区别收费。
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。
有关封堵的更多信息，请参见 封堵相关问题 。