DDoS 高防包

DDoS 基础防护

产品文档

腾讯云

文档目录

DDoS 基础防护
产品简介
产品概述

最近更新时间：2021-08-16 11:40:27

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。用户默认享受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。

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。

报表管理

支持对攻击事件及攻击流量的统计，支持自定义时间查看攻击报表。

产品优势

最近更新时间：2021-08-16 11:38:19

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：2021-08-16 11:38:19

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：2021-08-16 11:38:19

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 基础防护默认封堵阈值如下：

地区	普通用户	VIP 用户
中国大陆区域	2Gbps	10Gbps

地区	普通用户	VIP 用户
中国香港及海外区域	不超过2Gbps	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。

购买指南

最近更新时间：2021-08-16 11:38:19

- DDoS 基础防护为免费服务。
- 当您遇到问题时，请 联系我们 寻求相应的帮助。

操作指南

操作总览

最近更新时间：2021-08-16 11:38:19

您在使用 DDoS 基础防护时，可能碰到查看 DDoS 基础防护信息、统计报表、操作日志以及设置安全事件通知等问题，本文将介绍使用 DDoS 基础防护的常用操作。

DDoS 基础防护

查看防护配置

统计报表

查看统计报表

安全事件通知

设置安全事件通知

使用限制

最近更新时间：2021-08-16 11:38:19

防护对象限制

为腾讯云内 CVM、CLB 及 NAT 网关等云产品，提供免费的基础 DDoS 防护。

查看防护配置

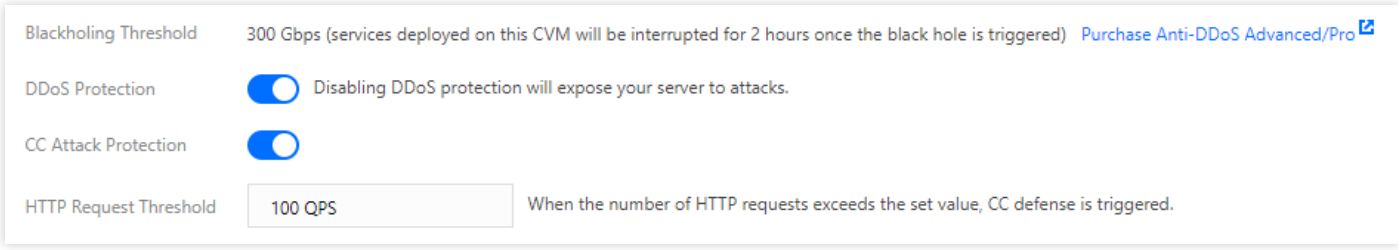
最近更新时间：2021-08-16 11:38:19

操作场景

登录 DDoS 防护管理控制台，可查看 DDoS 基础防护的防护详情，并进行防护配置修改。

操作步骤

1. 登录 DDoS 防护管理控制台，单击【DDoS 基础防护】。
2. 选择服务器类型和地区，单击目标主机名称。



> 说明：
> DDoS 防护默认为开启状态，当攻击发生时，将触发 DDoS 流量清洗防护，高防系统会对流量进行识别，并过滤恶意流量。
> 关闭 DDoS 防护可能导致服务器瘫痪，造成业务中断，需谨慎操作。

- 黑洞触发阈值
  显示当前该资源的防护阈值；表示当攻击流量超过阈值，将会触发封堵，导致一段时间内业务不能正常访问。如需提高 DDoS 防护能力，可根据业务需要，购买合适规格的高防产品。
- CC 防护
  默认为关闭状态，可单击自行开启，同时设置 HTTP 请求数阈值。当总 HTTP 请求数超过所设置的阈值时，将触发 CC 防护，高防系统会对请求进行识别，并过滤恶意请求。

查看统计报表

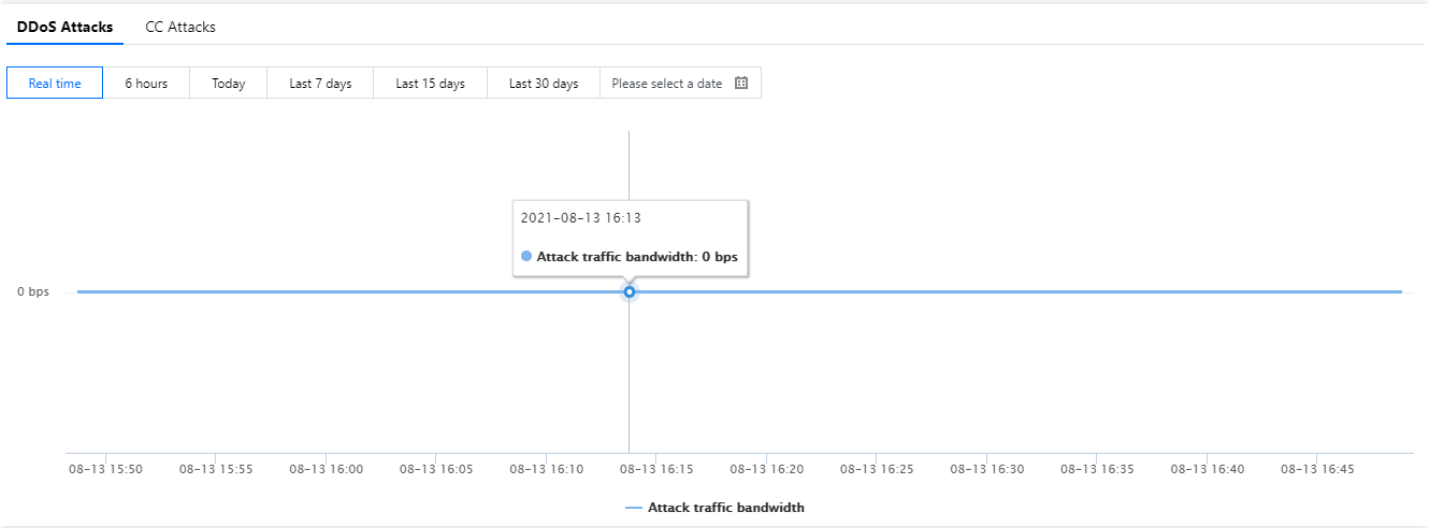
最近更新时间：2021-08-16 11:38:19

操作场景

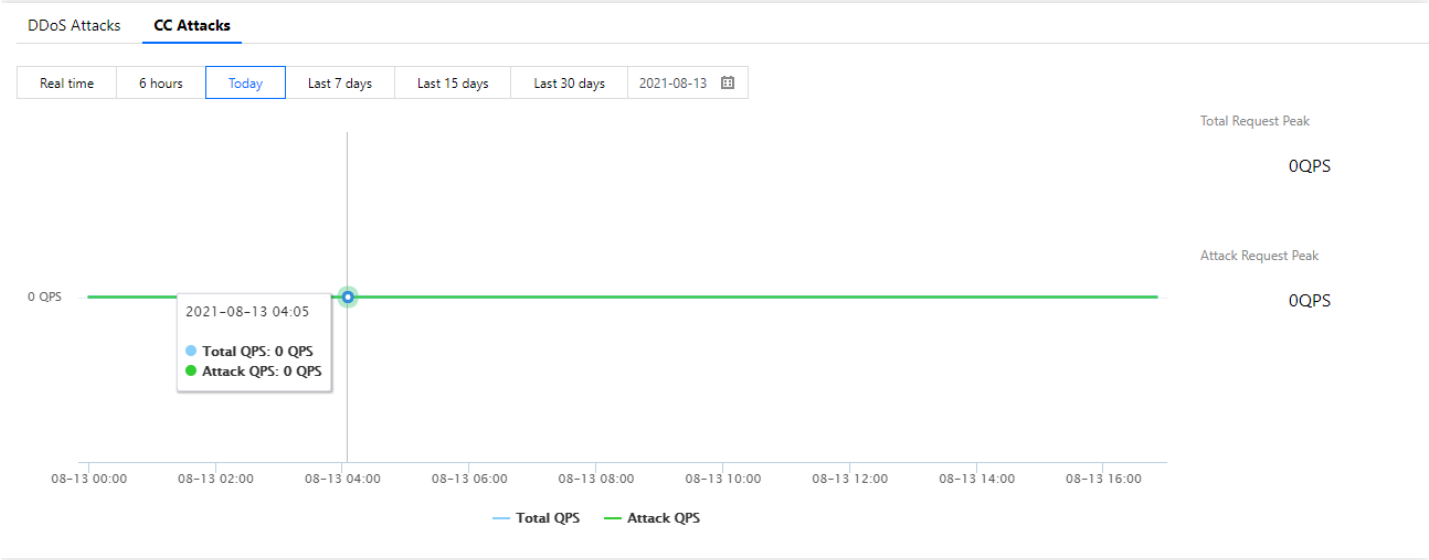
当用户收到 DDoS 攻击提醒信息或发现业务出现异常时，需要快速了解攻击情况，包括流量大小及当前防护效果等，在掌握足够信息后，才可以采取更有效的处理方式，第一时间保障业务正常。
DDoS 基础防护管理控制台的统计报表提供丰富的信息，可帮助用户快速了解当前业务遭受攻击的情况。

操作步骤

1. 登录 DDoS 防护管理控制台。
2. 在【DDoS 基础防护】页面，选择服务器类型和地区，单击目标主机名称。
3. 在【DDoS 攻击】页签，设置查询时间范围。
   - 在【攻击流量统计】区域，可以查看该时间段内的 DDoS 攻击流量趋势。
   - 在【DDoS 攻击记录】区域，可以查看该时间段内产生的 DDoS 攻击记录，包括每次攻击的开始时间、结束时间、是否触发封禁以及清洗流量值等信息。



4. 在【CC 攻击】页签，设置查询时间范围。可以查看该时间段内所防护 IP 的 CC 攻击请求次数统计及趋势。


DDoS Attacks
CC Attacks
Real time
6 hours
Today
Last 7 days
Last 15 days
Last 30 days
2021-08-13
Total Request Peak
0QPS
Attack Request Peak
0QPS
0 QPS
2021-08-13 04:05
Total QPS: 0 QPS
Attack QPS: 0 QPS
08-13 00:00
08-13 02:00
08-13 04:00
08-13 06:00
08-13 08:00
08-13 10:00
08-13 12:00
08-13 14:00
08-13 16:00
Total QPS
Attack QPS

设置安全事件通知

最近更新时间：2021-08-16 11:38:19

操作场景

当您所使用的腾讯云公网 IP 受到攻击、受攻击结束、IP 被封堵以及解除封堵时，将以站内信、短信、邮件或者电话的方式，向您推送告警信息：

- 攻击开始时，您将会收到攻击开始提示。
- 攻击结束后15分钟，您将收到攻击结束提示。
- IP 被封堵时，您将收到封堵提示。
- IP 解除封堵时，您将收到解除封堵提示。

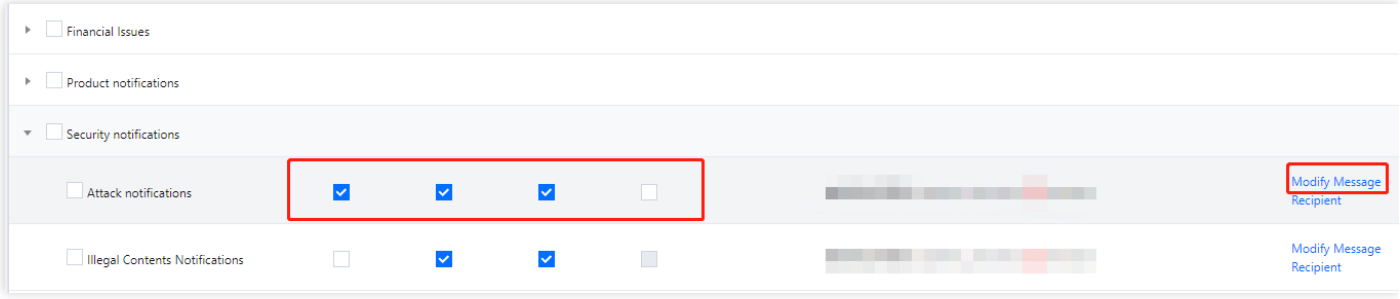
您可以根据实际情况修改告警信息的接收人和接收方式。

操作步骤

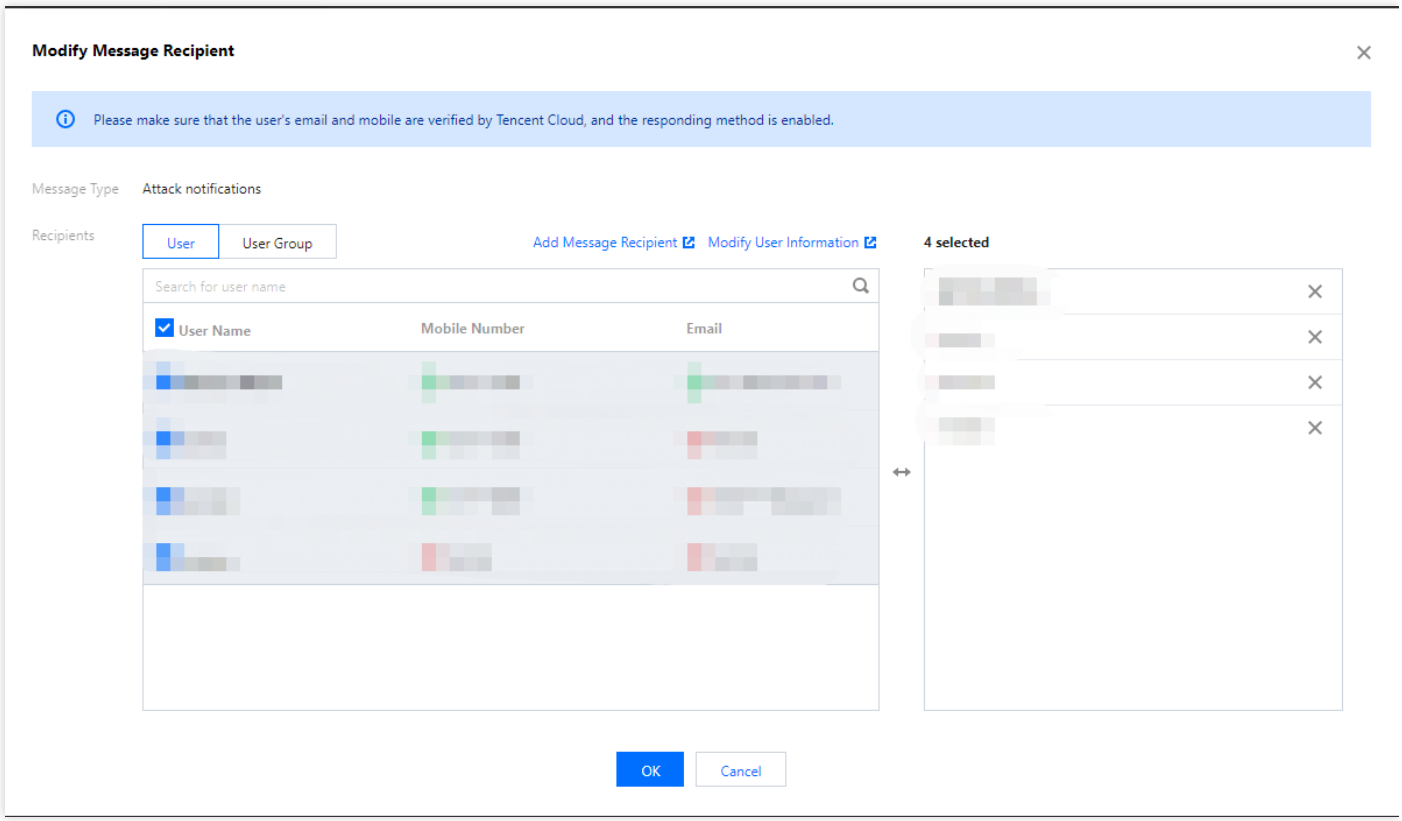
1. 登录您的腾讯云账号，进入 消息中心。

> 说明：
>
> 您也可以登录 控制台，单击右上角的 ，在弹出页面，单击【更多站内信】，进入消息中心。

2. 在左侧目录中单击【消息订阅】，进入消息列表。
3. 在消息列表中，在安全事件通知所在列，选择接收方式，单击【修改消息接收人】，进入修改消息接收人页面。



4. 在修改消息接收人页面，进行消息接收人的设置，设置完成后单击【确定】即可。



故障处理
公网 IP 遭遇 DDoS 攻击

最近更新时间：2021-08-16 11:38:19

现象描述

业务遭受 DDoS 大流量攻击，消耗目标服务器性能/网络带宽，造成服务器无法正常提供服务。

可能原因

用户 IP 遭受的攻击大小，超过了腾讯云赠送的基础防护能力（2Gbps）。

解决思路

- **更换公网 IP（攻击停止时，临时方案）**
  攻击者发起 DDoS 攻击是针对具体业务 IP，通过临时更换 IP，只能临时规避被封堵的问题，无法根本解决，攻击者可能随时针对新 IP 发起第二次攻击，产生二次影响。
- **购买高防产品（推荐方案）**
  通过购买 DDoS 高防产品，提升 IP 的防护能力，抵御大流量攻击，如攻击流量超过了高防包所在地域的能力，可按需选择更大防护能力的高防 IP 产品。

处理步骤

更换公网 IP（攻击停止时，临时方案）

更换公网 IP 相关限制如下：

- 单个账号单个地域不超过3次/天。
- 单台实例仅允许更换1次公网 IP。
- 更换后原公网 IP 将被释放。

更换操作详情，请参见 更换公网 IP 地址。

购买配置高防产品（推荐方案）

- 购买并配置 DDoS 高防包，请参见 购买指引 和 快速入门。
- 购买并配置 DDoS 高防 IP，请参见 购买指引 和 快速入门。

DDoS 高防包和 DDoS 高防 IP 的对比，请参见 DDoS 防护解决方案对比。