棋牌盾

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：2019-07-25 15:30:04

简介

棋牌盾是一款面向业务频繁遭受 DDoS 攻击、CC 攻击的游戏行业用户推出的针对性产品。棋牌盾采用业界独有的 IP 轮询技术，将业务分散至一批棋牌盾 IP，并配以灵活的用户隐藏和流量调度策略，低成本地抵御大流量攻击，确保核心业务不受影响。

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。

防护统计及分析

提供 DDoS 攻击、CC 攻击、转发流量、新建/并发连接数等多维度统计报表，帮助用户实时掌握业务和攻击情况。

支持的地域

棋牌盾服务目前仅支持上海地区购买，提供“按需购买棋牌盾 IP 资源”方式，使用按年预付费计费模式。

说明：

如有需要，请 提交工单 申请，或联系您的商务经理将您的账号添加至白名单后再进行购买。

产品优势

最近更新时间：2020-01-02 11:29:14

灵活调度

采用 IP 池轮询机制，根据用户业务不同级别分配 IP，通过灵活的用户隐藏和流量调度机制，有效缓解大流量 DDoS 攻击、CC 攻击，优先保障核心业务稳定可用。

接入便捷

提供 API 对接，无需客户端二次开发，无需更改架构。根据自身业务规模和安全需求购买棋牌盾 IP 资源，在控制台快速配置即可使用。

隐藏用户站点

采用替身防护方式，以棋牌盾 IP 应对 DDoS 攻击、CC 攻击，隐藏真实用户站点，阻断攻击对源站的影响，进一步保证源站安全。

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。

高性价比

支持定制 DDoS 防护解决方案，充分满足用户在不同阶段的业务需求，安全运营成本可控。

应用场景

最近更新时间：2020-01-02 11:30:58

棋牌盾是腾讯云 DDoS 防护产品系列中针对游戏行业的安全解决方案，专为游戏行业定制，解决游戏行业中复杂的 DDoS 攻击、CC 攻击问题，能够保证游戏业务遭受攻击时正常运行，主要适用于以下场景：

- 游戏行业频繁遭受 DDoS 攻击、CC 攻击的防护场景
- 对业务运营在稳定性、安全性要求较高的安全防护场景
- 对用户体验在实时性、流畅性要求较高的业务场景
- 需保障突发大流量攻击时，稳定核心业务的防护场景

相关概念

最近更新时间：2019-08-09 15:44:47

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

棋牌盾的 IP 遭受攻击且攻击流量峰值达到5Gbps时，会触发封堵。

封堵时长

棋牌盾的 IP 封堵时长均为30分钟。

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。