

产品概述

DDoS (Distributed Denial of Service) 攻击, 即分布式拒绝服务攻击, 是指攻击者利用大量“肉鸡”对攻击目标发动大规模的正常或非正常请求, 用以耗尽目标主机资源或网络资源, 从而使被攻击的主机不能为合法用户提供服务, 对用户造成经济或名誉上的损失。

迪普科技异常流量检测/清洗系列产品是专业的抗DDoS攻击防护设备, 包括: 异常流量检测产品Probe3000、异常流量清洗产品Guard3000以及业务管理平台, 能够及时发现网络中的各类DDoS攻击并实现对攻击流量的快速过滤。此外, 迪普科技异常流量检测与清洗系统还可为用户提供安全可视化服务, 帮助用户直观了解现网安全状况, 及时消除安全隐患。

产品特性

■ 电信级高可靠产品

基于迪普科技自主研发的高性能硬件架构平台, 单台清洗设备最高防护性能可达到T级别, 实现秒级响应, 快速阻断大规模DDoS攻击流量。迪普科技连续多年以第一名身份入围运营商抗DDoS产品集采名单, 超千台在网设备稳定运行, 持续为运营商网络提供安全保障。

■ 全面防护各类DDoS攻击

迪普科技异常流量检测/清洗系统采用独创的四大检测引擎: 多级特征检测引擎、流量智能调度引擎、智能指纹提取引擎和行为探测防护引擎, 凭借多重安全引擎的加持, 可以实现流量型DDoS攻击和应用型DDoS攻击的深度检测和防御, 可以有效防范当前主流的 DDoS 攻击, 如SYN Flood、UDP Flood、ICMP Flood、HTTP Flood、CC、DNS Flood、DNS 反射攻击、NTP 反射攻击等。

■ 双向攻击防护

常规的DDoS攻击流量清洗是针对固定的防护目标, 清洗入方向的异常流量。对于出方向的DDoS攻击流量, 存在攻击目标不确定性。异常流量检测/清洗产品通过模糊攻击检测技术智能分析出向流量目的 IP, 并开启全局清洗策略, 实现近源清洗效果, 满足特定场景下双向抗DDoS攻击防护需求。

■ 攻击溯源分析

在实现DDoS攻击检测与清洗之外, 迪普科技异常流量清洗产品集成了一套抓包溯源和攻击自动分析的工具, 支持抓取清洗前、清洗后、清洗丢弃的报文进行分析; 针对抓包文件可以进行攻击源IP溯源, 并提取攻击报文中的攻击特征, 简化防护策略配置难度。

■ 复杂网络适应能力

异常流量检测/清洗产品支持丰富的网络特性, 可部署于BGP、MPLS VPN等复杂网络环境下。旁路部署模式下, 支持通过BGP技术进行流量牵引, 流量回注技术可使用策略路由、VLAN、GRE、MPLS等技术, 满足不同组网环境下的抗DDoS防护需要。

■ 业务运营管理平台

为满足运维管理和抗DDoS服务运营需要, 迪普科技为运营商提供综合性的运营管理平台, 遵循“护自己、护他人”的理念, 在简化日常运维及攻击处置的同时可以为租户提供抗DDoS攻击防护服务, 通过可视化平台全面提升租户感知能力和使用体验。



Probe3000-GE-X



Probe3000-TM-XI



Guard3000-GS-X



Guard3000-GA-X



Guard3000-GE-XI



Guard3000-TM-XI



Guard3000-TA-XI



Guard3000-Blade-XA



Guard3000-Blade-17E

功能价值

技术优势	功能价值
部署灵活	支持旁路部署、在线部署模式
网络特性	支持静态/动态引流、BGP引流；支持策略路由、MPLS VPN、GRE VPN、二层透传模式等回注方式
检测方式	支持基于NetFlow/NetStream/Sflow等协议的流量检测方式（DFI） 支持基于深度数据包检测方式（DPI）
基本攻击防护	支持基于IPv4/v6双栈下的SYN/ACK Flood、ICMP Flood、UDP Flood、DNS Query Flood、Http Flood、Https Flood、CC、Connections Flood等常见DDoS攻击手段的防护
畸形包攻击防护	支持畸形包攻击防范，支持针对协议漏洞的畸形包攻击防范，比如Land、Smurf、Fraggle、Tear Drop、Winnuke
攻击抓包溯源	支持抓包溯源功能，支持抓取清洗前、清洗后、清洗丢弃的报文进行分析；针对抓包文件可以进行攻击源IP溯源，并提取攻击报文中的攻击特征下发到清洗设备过滤
系统状态监控	支持设备性能监控，可监控接口流量信息，CPU和内存利用率和在线状态监控
日志报表	支持独立的日志服务器，日志可自动定时备份；内置多种报表，可图形化的查询、审计、统计、检索内网用户的各种网络行为日志，方便管理者了解和掌控网络
设备管理	提供便捷的图形化管理界面，支持Web GUI、SSH、串口Console，并支持通过UMC网管平台集中管理
第三方联动	支持自有或第三方流量检测设备的联动，接收检测设备信息，并由流量清洗设备主动发起路由牵引和回注

杭州迪普科技股份有限公司

地址：浙江省杭州市滨江区月明路 595 号迪普科技

邮编：310051

官方网站：<https://www.dpotech.com>

服务热线：400-6100-598