DPtech 异常流量清洗系列

杭州迪普科技股份有限公司

产品概述

迪普科技异常流量检测/清洗系统基于迪普科技自主知识产权的高性能硬件平台 APP-X 及 L2~7 融合操作系统 Conplat 进行开发 ,是针对 DDoS(分布式拒绝服务)攻击防护而设计的专业安全设备。常见的 DDoS 攻击类型主要为流量型 DDoS 攻击和应用型 DDoS 攻击，随着互联网、物联网的不断发展，DDoS 攻击方式也在不断演变，黑客利用物联网智能设备构筑僵尸网络的攻击事件呈爆发式增长，混合型反射攻击也日益猖獗。由于 DDoS 攻击具备发起成本低，难度小，攻击行为难以检测，影响范围大等特点，DDoS 攻击也成为黑客最为青睐的攻击方式之一，从政府网站、高校在线考试系统到网上购物平台、游戏服务器乃至工控系统都成为黑客的 DDoS 攻击目标。

为了解决上述难题，迪普科技推出了 DPtech 异常流量检测/清洗系列产品，该系列是专业 DDoS 攻击防护设备，包括：异常流量检测 Probe3000、异常流量清洗 Guard3000、异常流量清洗业务管理平台，能够及时帮助用户发现网络中的各类 DDoS 攻击并实现对攻击流量的快速过滤，有效保护用户业务免遭攻击，最大可提供 T 级抗 DDoS 能力。此外，迪普科技异常流量检测/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。

产品特点

- **独创的威胁检测引擎**

  传统的异常流量清洗产品采用设定阈值的方式对 DDoS 攻击进行检测及防护，但应用型 DDoS 攻击流量小，攻击行为难以检测，简单的阈值限速方式无法有效防护。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，多重安全检测引擎可以对流量型 DDoS 和应用型 DDoS 进行深度检测和防御，可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。

- **多维度流量模型自学习能力**

  DPtech Probe3000 可基于报文信息以及常见的应用统计信息建立自动学习模型，并根据最新流量信息进行自动更新，这种智能学习对于发现未知攻击非常有效。

- **模糊攻击检测能力**

  常规的 DDoS 攻击防护技术一般都是针对由外网向内网的流量进行防护，而由内网向外网的出向流量攻击往往容易被忽视。但是用户内部网络向外网发起的 DDoS 攻击同样危害巨大，一方面内网攻击流量也会侵占网络带宽，大流量情况下甚至会引起断网事件；另一方面用户还可能需要为内网的 DDoS 攻击行为承担相关责任。因此，双向的 DDoS 攻击防护都是非常必要的。出向的 DDoS 攻击往往难以防范，因为目的 IP 数量极多且相对离散，为了解决这一问题，迪普科技通过模糊攻击检测技术智能分析出向流量目的 IP，并对这些目的 IP 进行针对性防护。

- **多租户自服务能力**

  随着云数据中心的广泛建立，抗 DDoS 能力作为云数据中心的核心安全能力之一，也必须具备为客户提供相关云服务的能力。云数据中心多租户场景下，租户可以根据自身网络情况需要自定义流量清洗方式、告警方式、查看清洗报告、配置清洗策略等。迪普科技异常流量检测/清洗系统支持按需为不同租户提供安全资源：租户拥有独立管理界面及管理权限，可自行配置安全策略，按需导出清洗报表。

- **溯源分析能力**

  异常流量检测/清洗系统作为网络中最关键的安全设备，需要保障整个网络的稳定性。用户除了需要对 DDoS 攻击进行检测与清洗外，还需要对攻击报文深入分析，但是 DDoS 攻击的溯源与分析一直都是运维管理人员最头疼的问题。迪普科技异常流量检测/清洗系统集成了一套抓包溯源和攻击自动分析的工具，可以有效帮助用户对 DDoS 攻击追踪溯源，并且支持攻击特征自动提取，方便管理员添加安全策略进行针对性防护。

■ **复杂网络适应能力**

迪普科技异常流量检测/清洗系统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。

■ **丰富的风险报表**

通过安全风险概况分析，让用户对自身业务系统在某段时间内的安全状况有直观了解。同时根据用户在这段时间内面临的安全威胁，异常流量检测/清洗系统会从被攻击 IP、攻击源 IP、攻击类型等维度全方位地帮助用户了解网络安全现状。

产品系列

Guard3000-Blade

Guard3000-TS

Guard3000-GE

Guard3000-GA

Probe3000-Blade

Probe3000-TS

Probe3000-GE

Probe3000-GA

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
协议漏洞威胁防护	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
全面 DDoS 攻击防范	支持基于 IPv4/v6 双栈下的 SYN/ACK Flood、ICMP Flood、UDP Flood、DNS Query Flood、HTTP Get Flood、CC、Connections Flood 等常见 DDoS 攻击手段的防护
多种异常流量检测方式	基于 NetFlow/NetStream/SFlow 协议的流量检测方式（DFI） 深度数据包检测方式（DPI）
攻击取证	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
丰富的网络特性	支持 BGP 引流 支持策略路由、MPLS VPN、GRE VPN、二层透传模式等回注方式
日志与报表	支持独立的日志服务器，日志可自动定时备份；内置数百种报表，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
系统监控	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
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

	Guard3000-Blade-S	Guard3000-Blade-A	Guard3000-Blade-N	Guard3000-Blade-E
吞吐量	6 Gbps	10Gbps	20Gbps	40Gbps
并发连接数	150 万	600 万	2400 万	3200 万
新建连接数	15 万/秒	50 万/秒	80 万/秒	120 万/秒

杭州迪普科技股份有限公司
地址：浙江省杭州市滨江区通和路 68 号中财大厦 6 楼
邮编：310051
官方网站：www.dptech.com
服务热线：400-6100-598