DPtech IDS2000 系列入侵检测系统

杭州迪普科技股份有限公司

产品概述

迪普科技 IDS2000 入侵检测系统是针对应用系统检测而设计的专业安全设备，为用户操作系统、中间件、数据库、邮件服务器、DNS 服务器和 FTP 服务器等核心资产提供专业的应用层安全检测。IDS2000 入侵检测系统具有全面的特征库、先进的双病毒引擎及专业的四大检测引擎可对层出不穷的漏洞威胁及攻击手段提供全面的检测和识别。

此外 IDS2000 入侵检测系统具有攻击监控平台以及未知威胁监控平台，全方位展示用户网络安全态势情况，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

■ **万条特征全面检测**

近万条攻击特征库，能为用户提供全方位的应用层攻击检测，有效识别如缓冲溢出、蠕虫、木马、病毒、SQL 注入等攻击。

■ **专业引擎精准识别**

专业的四大检测引擎：防逃逸检测引擎、协议智能推导引擎、协议语义解析引擎、虚拟环境检测引擎。

- 防逃逸检测引擎：精准识别分片逃逸、乱序逃逸、编码变形逃逸等各种变形攻击；
- 协议智能分析引擎：可识别多种协议，将流量按协议分类引入不同的过滤器进行检测；
- 协议语义解析引擎：对流量进行深度解析，不仅仅通过特征匹配方式，而是对当前的语义进行分析，保证对攻击威胁精准识别；
- 虚拟环境检测引擎：通过在虚拟环境中运行可疑文件，跟踪并记录其行为，基于大数据的统计分析及、以及动态行为分析等技术，有效识别 APT 攻击，保障网络安全。

■ **病毒引擎双重查验**

先进的双病毒检测引擎：流式病毒检测引擎、文件还原式病毒检测引擎，根据检测流量的不同智能选择检测引擎。

- 流式病毒扫描引擎：基于特征匹配方式快速识别病毒，且可在使用过程中不断地进行学习，增加特征库的数量，极大地提高病毒检测效率；
- 文件还原式病毒扫描引擎，通过提取和运行文件，基于静态特征和行为分析等技术发现文件中隐藏的恶意代码，精准识别病毒。

■ **威胁情报分析**

威胁情报分析服务结合威胁情报数据，提供本地化、全方位的威胁情报能力，对威胁来源进行实时采集、分析、分类、关联、研判，帮助用户发现潜在威胁，并且实现告警和拦截动作，同时为安全运维人员提供有价值的分析结果，提升响应速度。

■ **网络威胁可视化**

具有攻击、未知威胁监控平台，可实时展示整网网络态势、攻击趋势、攻击日志等，通过地图展示出来自全球的攻击分布情况，记录被攻击 IP 当前攻击阶段，实现攻击的溯源。对现网已知威胁和未知威胁进行全方位展示。

■ **行为识别应用管控**

内置 5000 多种协议特征，并且可基于用户需求自定义应用，管控用户及应用的网络访问行为。

■ **复杂网络轻松部署**

可在 IPv4/IPv6 双栈、MPLS VPN、BGP 等复杂网络环境中部署，并且能识别并检测 QinQ、PPPoE、MPLS、GRE 等特殊封装的网络报文。

产品系列

IDS2000-MA-XI

IDS2000-GC-XI

IDS2000-GA-XI

IDS2000-TS-XI

IDS2000-TM-XI

功能价值

产品功能	功能描述
攻击检测	具备全面的 4~7 层应用检测能力，支持对缓冲溢出攻击、蠕虫、木马、病毒 SQL 注入、恶意代码、网络钓鱼、暴力破解、弱口令扫描等攻击的识别与检测 内置专业的攻击特征库，提供近万条攻击特征，可完全兼容 CVE
四大检测引擎	具有防逃逸检测引擎、协议智能推导引擎、协议语义解析引擎及虚拟环境检测引擎，实现对攻击威胁的精准识别
专业病毒检测能力	具有流式病毒扫描及文件还原式病毒扫描两大病毒引擎，可进行灵活组合 通过自学习方式丰富流式病毒特征库，实现更高效检测处理
应用管控	支持 5000 多种应用协议特征库，可自定义应用，支持基于应用类型、时间等维度来对用户的访问行为进行管控
深度报文检测技术	支持 IPv4/IPv6 双栈、MPLS VPN、BGP 等复杂网络环境，且可以识别并检测 QinQ、PPPoE、MPLS、GRE 等特殊封装的网络报文
全面的 DDOS 攻击检测	支持 TCP、UDP、ICMP 等其他协议指纹防护，支持 SYN Flood 防护、DNS Flood 防护等
威胁情报分析	威胁情报分析服务结合威胁情报数据，提供本地化、全方位的威胁情报能力，对威胁来源进行实时采集、分析、分类、关联、研判，帮助用户发现潜在威胁，并且实现告警和拦截动作，同时为安全运维人员提供有价值的分析结果，提升响应速度
可视化管理	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 具有攻击监控及未知威胁监控平台，可对网络威胁进行全方位的展示
日志与报表	支持独立的日志服务器，日志可自动定时备份；内置多维度报表，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
多重高可靠性保障	具有多重高可靠性保障机制，支持关键部件冗余及热插拔，支持应用 Bypass 和 PFP 掉电保护、双机热备，可实现真正的无缝切换，确保网络安全稳定可靠运行

部署方式	支持旁路部署模式

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.dptech.com
服务热线：400-6100-598