DPtech IPS2000 系列入侵防御系统

杭州迪普科技股份有限公司

产品概述

迪普科技 IPS2000 入侵防御系统是针对应用系统防护而设计的专业安全设备，产品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，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防护。迪普科技凭借强大的安全研究团队及独创的四大检测引擎可针对层出不穷的漏洞威胁及攻击手段，如 Java 反序列化漏洞、struts2 漏洞、鱼叉攻击、高级逃逸攻击、APT 攻击等提供有效全面的安全加固和防护。此外，迪普科技 IPS2000 入侵防御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 IPS 通常采用识别攻击特征的方式来实现攻击检测，但攻击变种层出不穷、业务应用种类繁杂，简单的特征识别方式容易造成较高的误报率及漏报率。DPtech IPS2000 采用迪普科技独创的四大检测引擎：防逃逸检测引擎确保变种攻击无法生效、协议智能推导引擎和协议语义解析引擎对流量进行深度检查与解析、虚拟环境检测引擎通过分析异常行为防护未知威胁，多重安全检测引擎确保入侵防御系统具有极低的误报率和漏报率。

- **防高级逃逸攻击技术**

  AET 高级逃逸技术是是黑客躲避安全检测，达到恶意攻击目的的一种高级入侵手段。目前比较主流的 AET 类型有以下几类：分片逃逸攻击、乱序逃逸攻击、编码变形逃逸攻击等。DPtech IPS2000 基于智能的数据包重组技术对分片报文、乱序报文、编码变形类报文进行深度检查，避免黑客绕过安全检测，使变种攻击无所遁形。

- **防数据泄露技术**

  面对复杂隐蔽的 APT 攻击，迪普科技安全研究团队深入剖析 APT 攻击方法，在 IPS2000 入侵防御系统上实现 APT 攻击的防护。DPtech IPS2000 通过黑客攻击链检测与还原引擎感知并还原黑客入侵全过程，对系统内部敏感数据、文件类型进行识别，实现对敏感数据使用情况的监控，从而达到防止数据泄露的目的，全方位的保证用户核心资料的安全性。

- **深度报文检测技术**

  DPtech IPS2000 支持丰富的网络特性，可部署于 IPv4/IPv6 双栈、MPLS VPN、BGP 等复杂网络环境下，可以识别并检测 QinQ、PPPoE、MPLS、GRE 等特殊封装的网络报文。

- **虚拟化技术**

  在云数据中心环境下，DPtech IPS2000 入侵防御系统可通过虚拟化技术将安全资源池化，按需为不同租户提供安全资源：租户拥有独立管理界面，可自行配置安全策略，按需分配吞吐、并发、新建等资源。

- **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，IPS 会对用户整体安全风险进行评级，包括高危、中危、低危和安全等。另外，针对攻击级别较高的攻击事件还可以提供安全解决方案。

产品系列

IPS2000-Blade-S

IPS2000-Blade-A

IPS2000-Blade-E

IPS2000-TM-E

IPS2000-TS-A

IPS2000-GA-E

IPS2000-GS-E

IPS2000-ME-N

IPS2000-MA-N

IPS2000-MS-N

IPS2000-MC-N

功能价值

技术优势	功能价值
部署灵活	支持在线模式、监听模式、混合模式
应用层攻击检测与防御	具备全面的 L4~7 应用检测与防御能力，支持对缓冲溢出攻击、蠕虫、木马、病毒、SQL 注入、网页篡改、恶意代码、网络钓鱼、间谍软件、DoS/DDoS、流量异常等攻击的防御
敏感数据保护能力	具备应用识别、敏感数据识别能力，可以基于时间生效相应的防护策略，对用户的关键数据进行保护
专业病毒防护能力	内置专业病毒库，可提供数十万条病毒库 支持防御文件型、网络型和混合型等各类病毒 支持新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒。
变种攻击防护能力	支持对分片逃逸、乱序逃逸、编码变形逃逸等变种攻击进行检测及防御
专业特征库团队	迪普科技专业特征库团队实时跟踪国内外最新安全技术，提供集漏洞库、病毒库、协议库于一体的专业特征库，特征库完全兼容 CVE。迪普科技是中国国家漏洞库的提供者之一
虚拟化能力	具备多租户环境下的资源统一划分、策略统一管理，不同租户之间可以实现转发隔离及安全自主监控
丰富网络特性	具备丰富的网络特性，可在 IPv4/IPv6 双栈、MPLS 等复杂网络环境下良好工作
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，可实现真正的无缝切换，确保网络安全稳定可靠运行
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
图形化管理	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

* 此特性仅在高端框式设备上支持

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.dptechnology.net
服务热线：400-6100-598