入侵检测、入侵防护到入侵管理 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E5_85_A5_E4_BE_B5_E6_A3_80_E6_c101_251016.htm 方正方通入侵检测系统自2001年推出以后，目前已发展到3.0版，方正方通入侵检测系统是具备2Gbps网络流量处理能力、同时支持八个监测端口的实时网络入侵检测系统。方通入侵检测系统可监控网络传输的数据流，自动检测和响应非授权活动、内部网络滥用和内部信息泄露等行为，使管理员在网络和系统受到危害之前发现并阻止非法入侵。方通入侵检测系统可在广域网上进行大规模、分布式部署，以及实现远程与集中相结合的分级管理。方通入侵检测系统的数据包处理能力能达到1,100,000pps(64字节，全双工)，当应用1000条规则时，最小化性能的衰减(低于5%)。 方正方通入侵防护系统结合防火墙和入侵检测技术结合入侵检测和防火墙两种技术，解决了以前防火墙在阻断有害流量时存在的问题：当阻断规则增加时，防火墙的性能快速下降。方通入侵防护系统改进数据包过滤引擎，以适合大量和动态的规则变化的需要，支持Failover功能，提供单向攻击阻塞功能(如蠕虫，缓冲区溢出漏洞攻击)，使用异常检测技术对未知攻击进行防御，同时还有对恶意流量(如蠕虫、病毒、黑客等)的防御功能。 方正方通企业级安全管理平台可以对不同安全系统进行集成化管理，这样将各个安全产品的单一管理点进行统一化管理，还可以进行远程控制管理，整个系统易于操作和管理，并且执行一致政策，降低用户的管理成本。 方正方通信息安全威胁管理系统可以监控未知的潜在威胁，提供整体的安全工具对付非正常

的网络征兆，并提供对威胁的决策支持功能。 方正方通信息安全威胁管理系统管理所有网络非正常使用及其所导致的威胁的集成化管理系统，在危急的事件发生之前，将威胁提早一步通知管理员，该系统倡导一个业务持续运转模型。方通信息安全威胁管理系统具有如下功能： 提供威胁传感器的整体管理，度量整体风险 威胁分析 通过过滤器(远程-本地，本地-远程，本地-本地)提供实时的会话状态 通过记录RawData建立会话校验功能 当前流量状态分析 分析有害数据流占总数据流的比率 用于审计的会话回放功能 实时事件分析 实时事件的获取、保存和报警，所有事件查询 入侵检测/防御/报警/流量统计/ e-mail/ web mail/ telnet/ ftp/ rlogin/ 硬盘共享 RawData日志/有害信息的检索 显示时间/攻击类型/风险/统计 入侵检测 基于网络误用、模式匹配、协议分析和异常检测 数据包/会话的检测模式 维护最大150万的并发会话 防火墙、IPS、ESM、网络设备、网管系统互操作 方通入侵检测产品线可以通过下面两个图解充分表述各产品的客户价值和产品关联性。