HUAWEI NIP2000D/5000D IDS

网络入侵检测系统

华为 NIP 系列入侵检测系统，面向大中企业、行业及运营商客户，为客户定位各种网络威胁， 以及违反安全策略的流量，并提供详实、有效的指导措施，进而实现防护- 检测-响应一体化的解决方案。NIP 入侵检测系统（IDS）融合了多种新一代的检测技术，坚持“全面检测、准确分析、多面展现”的 IDS 产品理念，是用户提升安全能力，完善安全保障措施的得力助手。

华为 NIP 系统，采用电信级的高可靠性设计，可在多种环境灵活的部署。产品提供零配置上线的部署能力，无需复杂的签名调整，无需人工设定网络参数及阈值基线，即可自动检测各种业务威胁。华为 NIP 产品显著降低了部署的复杂性，使整体的 TCO 成本得到有效的控制。

产品概述

前瞻性的全面检测

NIP 系统采用多种先进的检测技术，有效的检测各种已知或者未知的威胁：

- ✧ 采用协议智能识别技术，自动的区分不同应用和协议，无需人工设定协议端口；
- ✧ 基于漏洞的检测技术，以及基于攻击特征的检测技术，实时发现各种已知的攻击：漏洞利用、蠕虫木马等等；
- ✧ 协议异常检测、流量异常检测以及启发式检测技术，可以有效的发现未知漏洞及恶意软件产生的攻击。

华为安全研究团队，凭借 200+的高级研究人员，全球分布的数据采集及攻击收集能力，提供最新的安全情报定期，（每周）或紧急（当重大安全漏洞被发现）方式发布，通过云安全中心分发到 IDS 设备中，使用户的 IDS 设备在漏洞被公布的同时立刻具备检测零时差攻击的能力。

产品优势

- ✓ 全面检测新型威胁
  - ■ 检测最新恶意软件、零日攻击及 botnet；
  - ■ 300+安全研究人员，全球威胁采集，实时签名升级；
  - ■ 检测应用层 DDoS 攻击：DNS、HTTP、SIP 等；
- ✓ 检测精准
  - ■ 基于漏洞的检测技术，提供精准的检测；
  - ■ 自动学习业务流量基线，避免阈值配置错误；
- ✓ 易于使用，降低 TCO 成本
  - ■ 零配置上线，无需各种参数调整；
  - ■ 集中安全管理、实时安全监控；
  - ■ 应用流量可视化
- ✓ 高可靠性
  - ■ 电信级硬件设计，支持温度监控，支持风扇、电源等部件的热插拔

技术规格

型号	NIP2050D	NIP2100D	NIP2130D	NIP2150D	NIP2200D	NIP5100D	NIP5200D	NIP5500D
产品性能	低端百兆	高端百兆		基础千兆		中端千兆	高端千兆	万兆
扩展性								
专用管理口	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)	1×GE(RJ45)
固定接口	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4 × GE(combo)	4×GE(RJ45) 4×GE(combo)	4×GE(RJ45) 4×GE(combo) 2×10GE(SFP)
扩展槽位	—	—	—	—	—	3×FIC	3×FIC	2×FIC
扩展网络接口	—	—	—	—	—	8×GE(RJ45)、 8×GE(SFP) 2×10GE， 2×10GE+8GE	8×GE(RJ45)、 8×GE(SFP) 2×10GE， 2×10GE+8GE	8×GE(RJ45)、 8×GE(SFP) 2×10GE
关键特性								
攻击检测技术	✧ 协议智能识别、数据包及流重组、协议与文件还原、攻击特征检测、漏洞特征检测、流量自学习、网络行为异常检测、协议异常检测、高级逃避检测等							
服务器攻击检测	✧ 针对应用服务器提供全方位的安全威胁检测，解决以下问题：系统漏洞攻击、服务漏洞攻击、暴力破解、SQL 注入、跨站脚本							
客户端攻击检测	✧ 提供浏览器及其插件（Java、ActiveX 等）的威胁检测； ✧ 提供对 PDF、Word、Flash、AVI 等常见文件的威胁检测；							
恶意软件检测	✧ 木马蠕虫、间谍软件，远程控制、Botnet 及广告插件等灰色软件							
流量型攻击检测	✧ 畸形报文攻击检测、特殊报文检测、扫描类攻击检测、TCP/UDP 泛洪攻击检测； ✧ 应用层 DDoS 攻击检测：HTTP、HTTPs、DNS、SIP 等； ✧ 流量自学习：根据对客户正常流量的统计，设定流量型攻击的阈值；							
应用感知	✧ 支持 850+应用协议识别与管理，涵盖所有主流应用协议，如：P2P/IM/网络游戏/炒股软件/语音应用/在线视频/流媒体/Webmail/移动终端应用/远程登录等应用的识别及流量监控							
报警响应	✧ 实时警报、记入数据库、声音报警、Syslog、SNMP Trap、E-Mail、发送短信、设备联动、攻击报文抓取、TCP Reset							
设备管理	✧ 图形化界面配置、管理员分级管理、访问控制权限设置、设备集中管理； ✧ 引擎知识库定时升级、引擎知识库回滚、内网集中升级；							
日志报表监控	✧ 设备状态监控、事件信息记录备份、日志查询及过滤、网络状况实时监控、报表制定生成							
整机规格	整机规格							
尺寸（W×D×H）	442×560×43.6(mm)					442×560×43.6(mm)		
电源	AC：100～240V 50/60Hz 支持冗余					AC :100～240V 50/60Hz DC :-48～-60V 支持冗余		
最大功率	150W	150W	150W	150W	150W	300W	300W	300W
工作环境	温度：0~40℃ 湿度：10%～85% 不结露							
MTBF	12.67 年	12.67 年	12.67 年	12.67 年	12.67 年	12.67 年	12.67 年	12.67 年