NIP6000D下一代入侵检测系统

NIP 6320D

NIP 6330D/6620D/6650D

产品概述

NIP6000D系列产品是华为推出的新一代专业入侵检测产品（NGIDS），主要应用于企业、IDC、校园网和运营商等，为客户提供网络威胁检测，定位违反安全策略的流量，并且给出专业的处理措施指导，在不改变客户原有网络部署的情况下，协助保障客户网络免受网络中的各种威胁。

NIP6000D系列产品在传统IDS产品的基础上进行了扩展：增加对所保护的网络环境感知能力、深度应用感知能力、内容感知能力，以及对未知威胁的检测能力，相较传统IDS，实现了更精准的检测能力和更简洁的管理体验。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，显著降低部署复杂性，使整体的TCO 成本得到有效的控制。

产品特点

智能感知网络环境

- 通过对环境的感知，形成所保护网络的静态安全风险；
- 对攻击的实时检测，形成所保护网络的动态安全风险；
- 通过动态和静态的风险展示，全面深刻的展示所保护网络的风险；

安全策略自动调整

- 具备敏捷引擎，实现平滑升级以获得新的威胁信息及检测技术的能力；
- 根据安全风险，自适应的进行安全防御策略调整，有针对性地检测；
- 向管理员提供需要增加的针对该应用的安全策略或者自动增加该策略，实现及时有效的防御；

威胁日志智能分级管理

- 根据安全风险，以及检测日志信息进行综合分析，实现日志的分级管理；
- 识别15%真正有效的安全风险，大幅降低网络维护日志量，帮助管理员识别重要安全威胁；

签名更新快，漏洞及时检测

- 专业的签名开发团队密切跟踪全球知名安全组织和软件厂商发布的安全公告，并遵从国际权威组织CVE的兼容性认证要求，对这些威胁进行分析和验证；
- 通过遍布全球的蜜网，实时捕获最新的攻击、蠕虫病毒、木马等，提取威胁的特征，发现威胁的趋势；
- 华为能够在最短时间内发布最新的签名，及时升级检测引擎和签名库。

NIP6000D下一代入侵检测系统

产品规格

型号	NIP6320D	NIP6330D	NIP6620D	NIP6650D
产品性能	中端百兆	低端千兆	中端千兆	高端千兆
扩展性				
固定接口	4GE+2Combo	8GE+4SFP		
高度	1U			
尺寸（mm）	442 × 421 × 43.6			
重量	10KG			
硬盘	Optional single 300 GB hard disks (hot swappable).			
冗余电源	Optional			
AC 电源	100～240V			
DC电源	-			-48～-60V
功耗	170W			
工作环境	温度：0～45°C (不含硬盘)/5°C～40°C (包含硬盘)湿度：10%～90%			
功能特性				
IT环境感知	支持感知被保护IT资产的资产类型、操作系统，启用的服务等资产情况。			
日志分级管理	支持根据实际IT环境评估攻击事件风险等级，聚焦关键攻击事件、忽略低风险攻击事件。			
策略调整	根据环境感知的资产情况动态生成适合当前IT环境的入侵检测策略。			
应用层DDoS攻击检测	支持流量模型自学习； 支持检测应用层DDoS攻击：HTTP Flood、HTTPS Flood、DNS Flood、SIP Flood			
单包攻击检测	支持检测多种单包攻击和扫描类攻击：IP地址扫描、端口扫描;畸形报文类攻击：LAND攻击、Smurf攻击、Fraggle攻击、WinNuke、Ping of Death、Tear Drop、IP分片报文检测、TCP标记合法性检查;特殊报文控制类攻击：超大ICMP报文控制、ICMP不可达报文控制、ICMP重定向报文的控制、Tracert、源站选路选项IP报文控制、路由记录选项IP报文控制、时间戳选项IP报文控制			
入侵检测IDS	基于签名库检测蠕虫、木马、僵尸网络、跨站攻击、SQL注入等常见攻击。同时还支持自定义签名应对突发攻击。			
反病毒AV	支持检测上网、邮件、网络文件传输等场景下的病毒文件，阻止病毒文件传输。			
应用识别	基于应用识别特征库可识别P2P、IM、网络游戏、社交网络、视频、语音应用等6000+种应用协议。基于识别出的应用协议可以进行应用使用情况展示等处理。			
IPv6流量检测	支持IPv6网络部署及IPv6流量的威胁检测。			
隧道内流量检测	支持对VLAN、QinQ、MPLS、GRE、IPv4 over IPv6、IPv6 over IPv4隧道流量进行攻击检测。			
网络层DDoS攻击检测	支持流量模型自学习； 支持防范网络层DDoS攻击：SYN Flood、UDP Flood、ICMP Flood			
日志显示	支持流量日志、威胁日志、操作日志、系统日志、策略命中日志等多种日志类型供管理员查看，帮助管理员掌握网络事件。			
报表呈现	支持流量报表、威胁报表、策略命中报表等多种报表类型供管理员查看和订阅，帮助管理员了解网络流量状况、威胁状况。同时网管系统eSight还支持更综合、更丰富的报表。			
配置管理	支持通过Web界面、命令行（Console、Telnet、STelnet）、以及网管（SNMP）对设备进行管理。			
特征库升级	支持入侵防御特征库、应用识别特征库和反病毒特征库的离线和在线升级，使设备持续拥有最新的防护能力。			
故障诊断	支持可视化故障诊断功能，可以帮助管理员一次性完成所有可能原因的诊断，并且自动给出诊断结果和修复建议。			