华为NIP6000D下一代入侵检测

智能手机、iPad等终端大规模普及，微信、微博、Facebook、Twitter 成为最常见的网络应用，企业利用这些新的技术，大幅度提高员工效率及运营能力。同时，云计算、移动计算等新技术蓬勃发展，已经应用于企业运营的方方面面。企业网络边界变得模糊，这些技术增加了组织遭受攻击的风险，通过越来越多的安全事件，可以清楚的看到，信息安全的主要威胁发生了变化，面对新一代威胁，传统检测技术已很难见效。

华为NIP6000D系列产品坚持“全面检测、准确分析、多面展现”的IDS 产品理念，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，实现了更精准的检测能力，和更优化的管理体验，更好的实现对新一代威胁的检测，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。

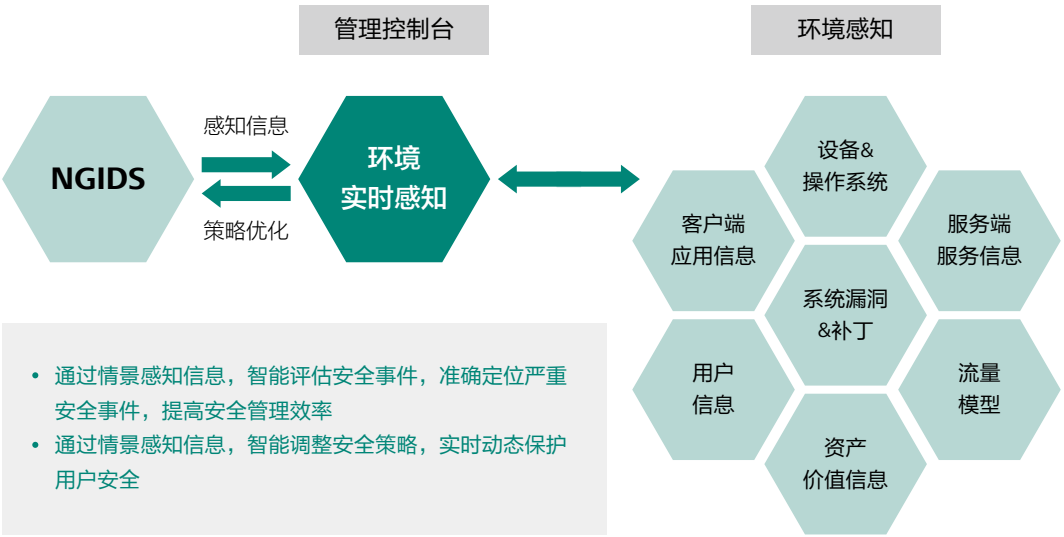
产品图片

NIP6000D系列

产品特性与优势

环境动态感知，实现策略调整智能化及日志分级管理

传统的IDS设备仅基于攻击报文的特征进行检测，却忽略了真实网络环境中受保护资产的实际情况，容易产生误报，导致管理员需要浪费大量的精力处理误报事件。NIP6000D通过对环境动态的感知，实现策略智能调整和日志分级管理功能解决此问题：



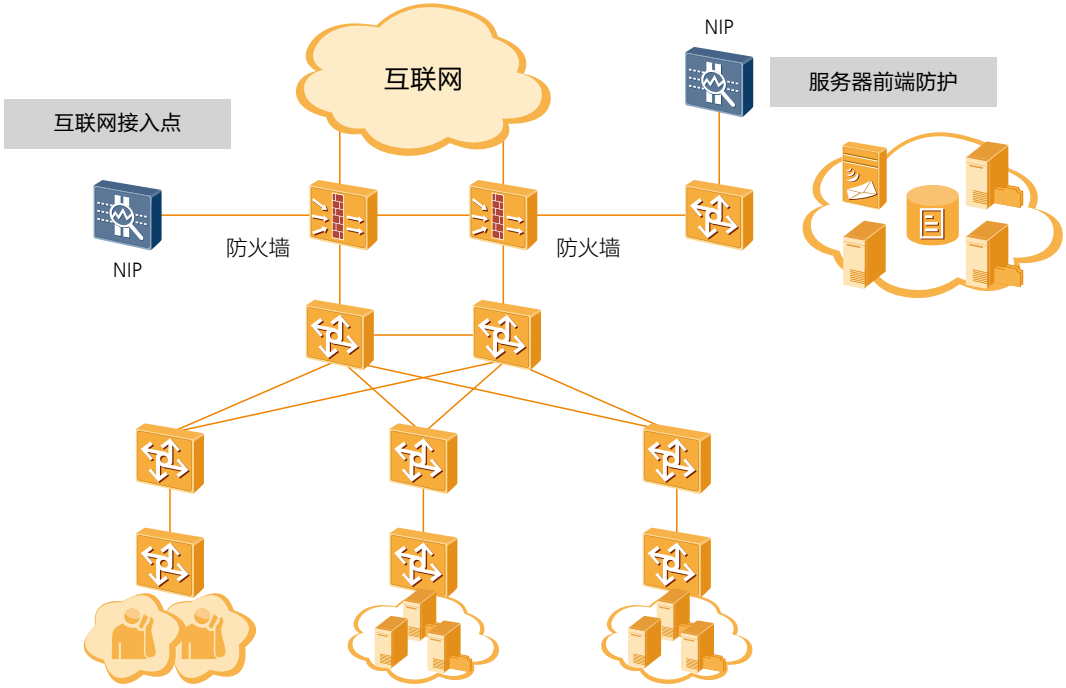
- NIP6000D感知受保护网络中的资产信息作为策略调整和风险评估的依据。支持手动录入、主动感知和第三方扫描软件导入资产信息，包括资产类型、操作系统、资产价值和开启的服务等
- 根据感知的资产信息，NIP6000D进行策略自动调整，基于感知到的资产信息选取合适的签名自动生成入侵检测策略，有针对性地防护，当环境有变化时，NIP6000D能第一时间感知相关的变化情况，及时自动调整或提醒管理员进行相关的策略调整以应对新的风险
- 当NIP6000D检测到攻击时，从签名中提取本次攻击针对的操作系统、服务等信息。然后将提取的信息与设备中存储的实际资产信息进行比对，同时根据资产的价值确定攻击事件的风险等级，并对这些告警日志进行分级管理，通过分级管理，可以帮助管理员过滤误报攻击事件、忽略非关键事件，重点聚焦高风险攻击事件
- 通过对环境的感知，获取所保护网络的静态安全风险，同时对攻击的实时检测，获取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

多重检测，全面防护

越来越多的信息资产连接到了互联网上，网络攻击和信息窃取形成巨大的产业链，这对下一代入侵防御产品的防护能力提出了更高要求。NIP6000D具备全面的深度防护功能：

- 入侵检测（IDS）：超过5000种漏洞特征的攻击检测。支持Web攻击识别，如跨站脚本攻击、SQL注入攻击等
- 防病毒（AV）：高性能病毒引擎，可防护500万种以上的病毒和木马，病毒特征库每日更新
- 服务器恶意外联检测：可以对重要服务器的外联进行检测，包括端口盗用检测和非法外联行为的检测，保护重要信息资产安全
- Anti-DDoS：可以识别和防范SYN flood、UDP flood等100+种网络层及应用层DDoS攻击

典型应用场景



互联网边界防护

此种场景NIP6000D一般旁路部署，旁挂在防火墙或交换机等网络设备上，交换机将需要检测的流量镜像到NIP6000D进行分析和检测。如果需要监控多条链路，可使用NIP6000D的多个接口同时接入。产品主要用来记录各类攻击事件和网络应用流量情况，进而进行网络安全事件审计和用户行为分析。

- 入侵检测：检测外网针对内网的攻击、内网员工发起的攻击，通过日志和报表呈现攻击事件供企业管理员评估网络安全状况。同时提供攻击事件风险评估功能降低管理员评估难度
- 应用识别：识别并统计P2P、视频网站、即时通讯软件等应用流量，通过报表为企业管理员直观呈现企业的应用使用情况
- 防火墙联动：IDS设备防御能力弱，检测到攻击后可以通知防火墙阻断攻击流量
- 满足对政策合规性要求，如等保、涉密网等政府强制标准的遵从等

IDC/服务器前端检测

此种场景采用旁路部署，NIP6000D旁挂于交换机或路由器，外网和服务器之间的流量、服务器区之间的流量都通过分流或镜像的方式引流到NIP6000D进行检测。

- 入侵检测：检测外网针对内网的攻击、内网员工发起的攻击，通过日志和报表呈现攻击事件供企业管理员评估网络安全状况。同时提供攻击事件风险评估功能降低管理员评估难度
- 服务器恶意外联检测：防御服务器的恶意外联，防止价值信息外传
- 反病毒：对用户向服务器上传的文件进行病毒扫描，防止服务器感染病毒
- DDoS攻击检测：检测针对服务器的DoS/DDoS攻击造成服务器不可用

产品规格

整机规格：

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℃ (不含硬盘)/5℃～40℃ (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，然后动态生成适合当前IT环境的入侵防御策略。			
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，以便管理员聚焦处理关键攻击事件、忽略可能误报的攻击。			
策略调整	支持对现网流量应用类型自学习，然后根据流量中包含应用类型的风险级别选择是否需要进行入侵检测。			
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： 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	基于签名库防御蠕虫、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	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阻断、流量限制、应用使用情况展示等处理。
IPv6流量检测	支持对IPv6流量进行威胁检测。
隧道内流量检测	支持对VLAN、QinQ、MPLS、GRE、IPv4 over IPv6、IPv6 over IPv4隧道内流量进行攻击检测。
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、ARP 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还支持比单机更综合、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。

订购信息

NIP6000D产品报价项介绍

对外型号	NIP机型编码	中文描述
NIP6320D-AC	02350CWB	装配组件-NIP6320D-NIP6320D-AC-NIP6320D交流主机(4GE电+2GE Combo，含知识库升级服务12个月)
NIP6330D-AC	02350CWT	装配组件-NIP6330D-NIP6330D-AC-NIP6330D交流主机(8GE电+4GE光，含知识库升级服务12个月)
NIP6620D-AC	02350CWV	装配组件-NIP6620D-NIP6620D-AC-NIP6620D交流主机(8GE电+4GE光，含知识库升级服务12个月)
NIP6650D-AC	02350CWF	装配组件-NIP6650D-NIP6650D-AC-NIP6650D交流主机(8GE电+4GE光，2交流电源，含知识库升级服务12个月)
NIP6650D-DC	02350CWG	装配组件-NIP6650D-NIP6650D-DC-NIP6650D直流主机(8GE电+4GE光，2直流电源，含知识库升级服务12个月)
LIC-IPS12-NIP63-HM	88032TYS	软件费用-NIP6300-LIC-IPS12-NIP63-HM-知识库升级服务时间12个月
LIC-IPS24-NIP63-HM	88032TYT	软件费用-NIP6300-LIC-IPS24-NIP63-HM-知识库升级服务时间24个月
LIC-IPS12-NIP66-LG	88032UBQ	软件费用-NIP6620&NIP6620D-LIC-IPS12-NIP66-LG-知识库升级服务时间
LIC-IPS24-NIP66-LG	88032UBR	软件费用-NIP6620&NIP6620D-LIC-IPS24-NIP66-LG-知识库升级服务时间24个月
LIC-IPS12-NIP66-HG	88032UBU	软件费用-NIP6650&NIP6650D&NIP6680-LIC-IPS12-NIP66-HG-知识库升级服务时间12个月
LIC-IPS24-NIP66-HG	88032UBV	软件费用-NIP6650&NIP6650D&NIP6680-LIC-IPS24-NIP66-HG-知识库升级服务时间24个月