NIP6000系列下一代专业入侵防御系统

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，传统技术已很难见效。

新一代威胁最重要的特征之一是基于零日漏洞的攻击，传统的防护技术需要一个较长的时间来生成可用的签名，而在这段时间内，攻击者可能已经对目标资产造成了重大危害。同时新一代威胁具有明确的目标性，攻击者长期有目的性地针对环境变化采用定制化的攻击手段，悄然之中达到了攻击目的。不断出现的攻击事件，清楚的展现了一个事实：传统技术不能完全抵御新一代威胁。当前网络环境下IT 设施的保护，需要一套全新的方法，即针对新一代威胁的解决方案。

NIP6000系列产品在传统IPS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，以及对未知威胁的防御能力，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与防护，保障客户应用和业务安全，实现对网络基础设施、服务器、客户端以及网络带宽性能的全面防护。

产品图

NIP6320/6610

NIP6330/6620/6650

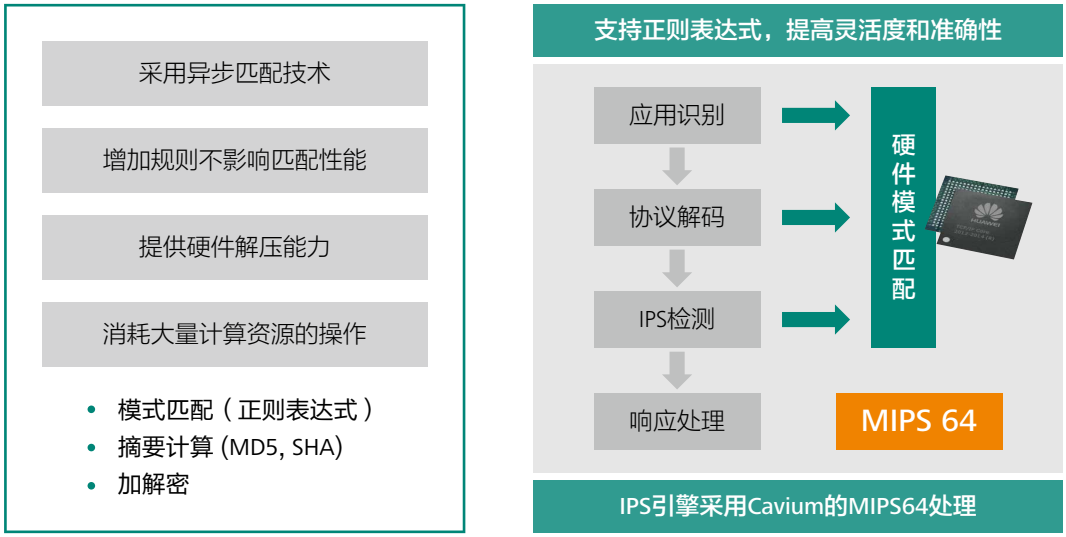
NIP6680

NIP6860

产品特性与优势

全新软硬件架构，产品性能业界领先

软件匹配引擎在处理正则表达式规则的时候，性能都比较低，极大的制约了设备检测性能，华为NGIPS引擎采用了全球领先的处理器提供商Cavium的MIPS64架构处理器，可以为IPS提供高性能的硬件模式匹配引擎，同时采用全新架构的智能感知引擎，在大流量深度检测的情况下仍保持高达15Gpbs的检测性能。

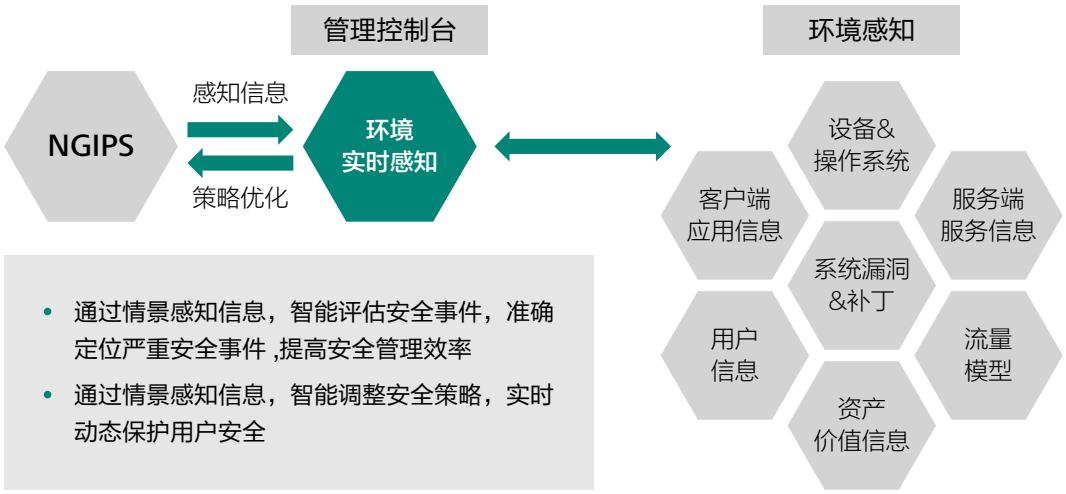


NIP6000系列下一代入侵防御采用全新的软硬结合一体化架构，对有规律、大批量、高运算能力要求的报文处理，采用专用多核平台由专用的协处理器硬件处理。对小规模的运算，仍然用软件处理。这样的处理方式让整体性能更高：

- 采用异步匹配技术，模式匹配中最消耗系统资源尤其是CPU资源的核心处理完全交给硬件的匹配引擎来处理，在匹配的同时不影响CPU处理其他业务，并行的处理大大提高报文处理效率和减低时延；
- 规则的增加不影响匹配的性能，硬件引擎能满足上万条威胁签名的同时加载，而传统的IPS引擎在加载大量的签名时匹配效率严重下降，造成设备性能降低，而用硬件匹配引擎则能完美解决这个问题；
- 提供ZIP等压缩文件的硬件解压能力， IPS引擎要对压缩的网页或者文件进行检测，就要有强大的解压缩引擎，而Cavium同样提供硬件解压缩能力，可以保证对ZIP等压缩包中的文件进行高性能的IPS检测。

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IPS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。NIP6000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：



- NIP6000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，NIP6000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防御策略，有针对性地防护，当环境有变化时，NIP6000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NIP6000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。

支持沙箱联动检测和信誉体系，APT威胁无所遁形

基于签名的威胁检测一般是针对已知漏洞的威胁检测，但是对于零日攻击和APT攻击的检测比较弱。检测APT攻击的最有效手段就是沙箱技术，通过沙箱技术构造一个隔离的威胁检测环境，然后将网络流量送入沙箱进行隔离分析并最终判断是否存在威胁：

- NIP6000从网络流量中识别并提取需要进行APT检测的文件类型，将文件送入本地/云端沙箱进行威胁分析；
- 本地/云端沙箱对文件进行解析，实时检测已知或未知威胁，然后沙箱将威胁检测结果反馈给NIP6000，并通过日志报表等形式展示威胁检测结果；
- 将威胁的具体攻击行为提交至云安全中心。云安全中心根据沙箱提交的威胁数据生成信誉信息和签名库并推送至NIP6000，从而提升NIP6000的快速威胁防御能力。

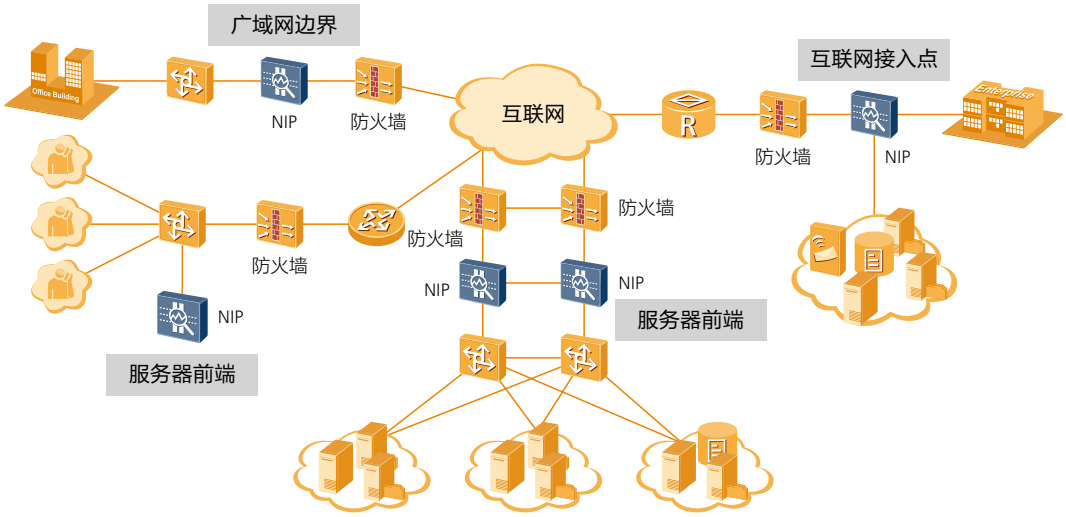
多重检测，全面防护

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。NIP6000具备全面的深度防护功能：

- **入侵防护（IPS）：**超过5000种漏洞特征的攻击检测和防御。支持Web攻击识别和防护，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；

- **SSL解密：**通过代理方式，对SSL加密流量进行应用层安全防护，如IPS、AV、URL过滤等；
- **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NIP6000一般部署于出口防火墙或路由器后端、透明接入网络。如果需要保护多条链路，可使用NIP6000的多个接口对同时接入。

- **入侵防御：**防御来自互联网的蠕虫活动、针对浏览器和插件漏洞的攻击，使得企业办公网络健康运行。拦截基于漏洞攻击传播的木马或间谍程序活动，保护办公电脑的隐私、身份等关键数据信息；
- **反病毒：**对内网用户从Internet下载的文件进行病毒扫描，防止内网PC感染病毒；
- **URL过滤：**对内网用户访问的网站进行控制，防止用户随意访问网站而影响工作效率或者导致网络威胁；
- **应用控制：**对P2P、视频网站、即时通讯软件等应用流量进行合理控制，保证企业主要业务的顺畅运行。

IDS/服务器前端防护：

此种场景一般采用双机部署避免单点故障。部署位置有如下两种：直路部署于服务器前端，采用透明方式接入；或者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先引流到NIP6000处理后再回注到主链路。

- **入侵防御：**防御对Web、Mail、DNS等服务器的蠕虫活动、针对服务和平台的漏洞攻击。防御恶意软件造成服务器数据的损坏、篡改或失窃。防御针对Web应用的SQL注入攻击、各种扫描、猜测和窥探攻击；
- **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攻击防范：**防御针对服务器的DoS/DDoS攻击造成服务器不可用。

网络边界防护：

对于大中型企业，内网往往被划分为安全等级不同的多个区域，区域间有风险隔离、安全管控的需求。如部门边界、总部和分支机构之间等，实现了网络区域的安全隔离。

- **入侵防御：**实现网络安全逻辑隔离，检测、防止外部网络对本网的攻击探测等恶意行为，以及外部网络的蠕虫、木马向本网蔓延；
- **违规监控：**监控内部网络用户向外部网络的违规行为。

旁路监控：

旁路部署在网络中监控网络安全状况也是IPS产品的一种应用场景，此种场景下IPS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。在这种部署方式下一般不进行防御响应。旁挂在交换机上，交换机将需要检测的流量镜像到NIP6000进行分析和检测。

- **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；
- **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。

产品规格

整机规格：

型号	NIP6320	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680	NIP6860
产品性能	中端百兆		低端千兆	中端千兆	高端千兆	中端万兆	高端十万兆
扩展性							
固定接口	4GE+2Combo		8GE+4SFP			4*10GE+16GE+8SFP	无固定接口 支持： 24xGE，6x10GE，12x10GE，3x40GE，1x100GE
高度	1U					3U	14U
尺寸（mm）	442 × 421 × 43.6					442 × 415 × 130.5	442 × 650 × 620
重量	10KG					24KG	空箱 43.2kg 满配 112.9kg
硬盘	可选单个300GB硬盘（支持热插拔）					可选。支持300G硬盘（RAID1和热插拔）	不支持硬盘
冗余电源	可选				标准配置		
AC电源	100 ~ 240V						90V ~ 264V
DC电源	-				-48 ~ -60V		-72 to -38V

型号	NIP6320	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680	NIP6860
功耗	170W					350W	DC 典配：4025W， DC 最大：4823W AC 典配：4282W， AC 最大：5132W
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%						温度：0～45°C； 湿度：5%～85%
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，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，聚焦关键攻击事件、忽略低风险攻击事件。						
策略调整	支持对现网流量应用类型自学习，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。						
URL黑名单	通过URL黑名单禁止用户访问某些网址，达到管理员工上网行为的目的。						
应用层DDoS攻击防范	支持流量模型自学习； 支持防范应用层DDoS攻击：HTTP Flood、HTTPS Flood、DNS Flood、SIP Flood						
SSL流量检测	支持对HTTPS流量进行解密并进行威胁检测。						
单包攻击防范	支持防范多种单包攻击：扫描类攻击：IP地址扫描、端口扫描；畸形报文类攻击：IP Spoofing、LAND攻击、Smurf攻击、Fraggle攻击、WinNuke、Ping of Death、Tear Drop、IP分片报文检测、ARP欺骗、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						
入侵防御IPS	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。						
APT检测	基于信誉体系和沙箱技术检测APT攻击，NIP6000将疑似文件送入沙箱进行检测，然后根据沙箱的检测结果展示攻击事件。						
反病毒AV	病毒库每日更新，可迅速检出超过500万种病毒。						
恶意文件检测	从各个文件传输协议（HTTP、SMB、FTP、SMTP、POP3、IMAP、NFS）中提取文件，并进入针对文件的检测引擎进行检测						
应用识别与控制	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IPv6网络部署及IPv6流量的威胁检测与防护。						
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攻击防范	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；						

型号	NIP6320	NIP6610	NIP6330	NIP6620	NIP6650	NIP6680	NIP6860
IP隔离	支持将产生攻击的源/目的IP地址加入黑名单，阻断对应IP的后续报文。						
双机热备	支持VRRP、VGMP、HRP等双机热备协议。提供完善的双机热备处理机制，保证主机发生故障时，业务可以自动平滑切换到备机上运行。						
硬件Bypass	通过插入Bypass卡，实现系统工作异常（包括软件异常、硬件故障、设备掉电等严重故障）时流量直通功能，保障业务不中断。						
日志显示	支持流量日志、威胁日志、URL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。						

订购信息

NIP6000产品报价项介绍

对外型号	NIP机型编码	中文描述
NIP6610-AC	02350CVY	装配组件-NIP6610-NIP6610-AC-NIP6610交流主机(4GE电+2GE Combo，含知识库升级服务12个月)
NIP6320-AC	02350CWA	装配组件-NIP6320-NIP6320-AC-NIP6320交流主机(4GE电+2GE Combo，含知识库升级服务12个月)
NIP6330-AC	02350CWC	装配组件-NIP6330-NIP6330-AC-NIP6330交流主机(8GE电+4GE光，含知识库升级服务12个月)
NIP6620-AC	02350CWU	装配组件-NIP6620-NIP6620-AC-NIP6620交流主机(8GE电+4GE光，含知识库升级服务12个月)
NIP6650-AC	02350CWD	装配组件-NIP6650-NIP6650-AC-NIP6650交流主机(8GE电+4GE光，2交流电源，含知识库升级服务12个月)
NIP6650-DC	02350CWE	装配组件-NIP6650-NIP6650-DC-NIP6650直流主机(8GE电+4GE光，2直流电源，含知识库升级服务12个月)
NIP6680-AC	02350CWH	装配组件-NIP6680-NIP6680-AC-NIP6680交流主机(16GE电+8GE光+4*10GE光，2交流电源，含知识库升级服务12个月)
NIP6680-DC	02350CWJ	装配组件-NIP6680-NIP6680-DC-NIP6680直流主机(16GE电+8GE光+4*10GE光，2直流电源，含知识库升级服务12个月)

对外型号	NIP机型编码	中文描述
LIC-AV12-NIP63-HM	88032TYQ	软件费用-NIP6300-LIC-AV12-NIP63-HM-反病毒升级服务时间12个月
LIC-AV24-NIP63-HM	88032TYR	软件费用-NIP6300-LIC-AV24-NIP63-HM-反病毒升级服务时间24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-AV12-NIP66-LM	88032UBJ	软件费用-NIP6610-LIC-AV12-NIP66-LM-反病毒升级服务时间12个月
LIC-AV24-NIP66-LM	88032UBK	软件费用-NIP6610-LIC-AV24-NIP66-LM-反病毒升级服务时间24个月
LIC-IPS12-NIP66-LM	88032UBL	软件费用-NIP6610-LIC-IPS12-NIP66-LM-知识库升级服务时间12个月
LIC-IPS24-NIP66-LM	88032UBM	软件费用-NIP6610-LIC-IPS24-NIP66-LM-知识库升级服务时间24个月
LIC-AV12-NIP66-LG	88032UBN	软件费用-NIP6620&NIP6620D-LIC-AV12-NIP66-LG-反病毒升级服务时间12个月
LIC-AV24-NIP66-LG	88032UBP	软件费用-NIP6620&NIP6620D-LIC-AV24-NIP66-LG-反病毒升级服务时间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-AV12-NIP66-HG	88032UBS	软件费用-NIP6650&NIP6650D&NIP6680-LIC-AV12-NIP66-HG-反病毒升级服务时间12个月
LIC-AV24-NIP66-HG	88032UBT	软件费用-NIP6650&NIP6650D&NIP6680-LIC-AV24-NIP66-HG-反病毒升级服务时间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