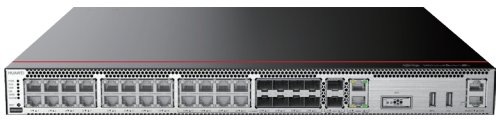
华为NIP6000E系列
新一代入侵防御系统

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。

NIP6000E系列产品在原有IPS产品的基础上进行了扩展：采用华为自研安全芯片，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



NIP6305E/6310E/6510E

NIP6550E/NIP6550ED

NIP6610E

NIP6620E-AC/DC

HUAWEI

产品特性与优势

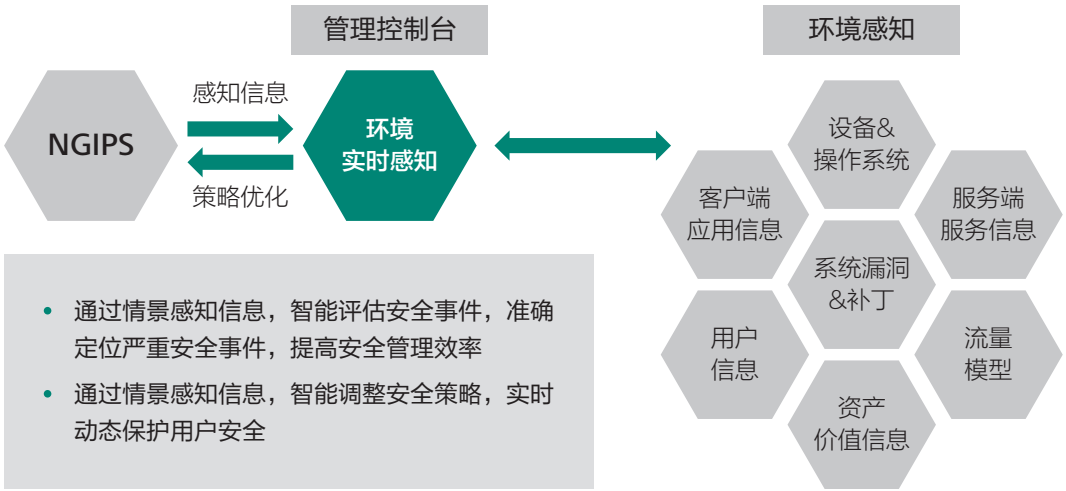
全新自研芯片，内置加速引擎，产品性能业界领先

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NIP6000E引擎采用了华为全新自研的安全专用SoC芯片Hi1213，可以为IPS提供高性能的硬件模式匹配引擎。

- 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，而自研芯片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。NIP6000E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：



- NIP6000E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，NIP6000E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，NIP6000E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NIP6000E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：

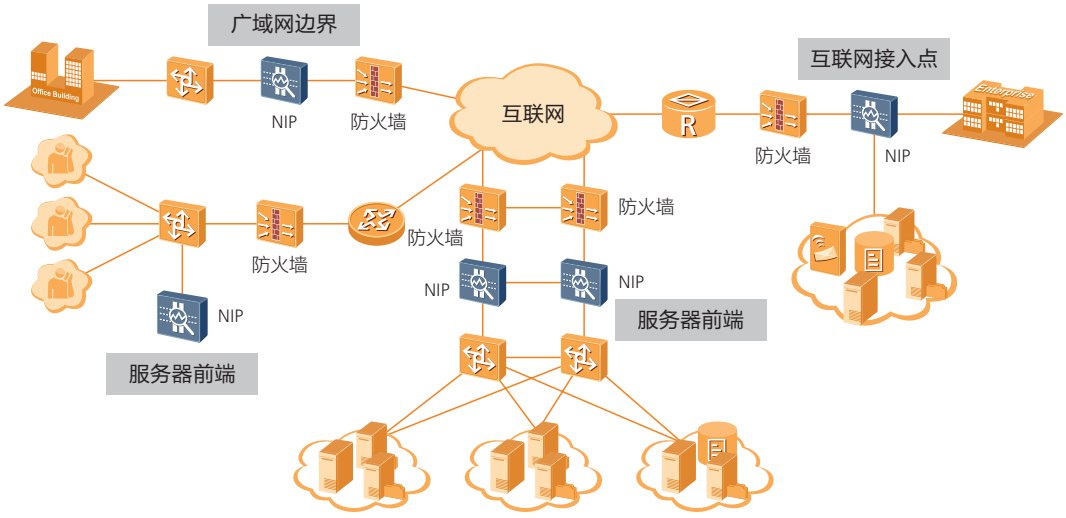
- NIP6000E从网络流量中识别并提取需要进行APT检测的文件类型，将文件送入本地/云端沙箱进行威胁分析；
- 本地/云端沙箱对文件进行解析，实时检测已知或未知威胁，然后沙箱将威胁检测结果反馈给NIP6000E，并通过日志报表等形式展示威胁检测结果；
- 将威胁的具体攻击行为提交至云安全中心。云安全中心根据沙箱提交的威胁数据生成信誉信息和签名库并推送至NIP6000E，从而提升NIP6000E的快速威胁防御能力。

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，这对新一代入侵防御产品的防护能力提出了更高要求。NIP6000E具备全面的深度防护功能：

- **入侵防护（IPS）：**超过8000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NIP6000E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NIP6000E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NIP6000E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NIP6000E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		NIP6305E/ NIP6310E/NIP6510E	NIP6550E/ NIP6550ED	NIP6610E	NIP6620E-AC/DC
固定端口	业务口	2 × 10GE(SFP+) + 8 × GE Combo + 16 × GE	2 × 40G(QSFP+) + 12 × 10GE(SFP+) + 12 × GE	4 × 40GE(QSFP+) + 28 × 10GE(SFP+) + 2 × 10GE(SFP+) HA	2 × 100G(QSFP28) + 2 × 40G(QSFP+) + 20 × 10GE(SFP+)
	WAN	2 × GE	无	2 × 10GE(SFP+)	2 × 10GE(SFP+) HA
	USB	1 × USB2.0 + 1 × USB3.0	1 × USB3.0	1 × USB3.0	1 × USB3.0
外置存储		选配，支持M.2卡，64G/240G	选配2.5英寸形态硬盘，支持 SSD 240GB/HDD 1TB	选配2.5英寸形态硬盘，支持 SSD 240GB/HDD 1TB	选配2.5英寸形态硬盘，支持 SSD 240GB/HDD 1TB
产品型态		1U	1U	1U	1U
尺寸 (W × D × H，单位mm)		442 × 420 × 44	442 × 420 × 44	442 × 600 × 44	442 × 600 × 44
电源功率		60W	600W	1200W	交流：1200W 直流：1200W
电源输入电压		100-240V	100-240V	100-240V	交流：100-240V 直流：-48V～-60V
电源冗余		选配	标配	标配	标配
重量 (不含硬盘)		5.8kg	7.6kg	12kg	12kg
工作环境	温度	0～45℃	0～45℃	0～45℃	0～45℃
	湿度	5%-95%非凝露	5%-95%非凝露	5%-95%非凝露	5%-95%非凝露
存储环境	温度	-40℃～70℃	-40℃～70℃	-40℃～70℃	-40℃～70℃
	湿度	5%～95%	5%～95%	5%～95%	5%～95%
功能特性					
安全策略		一体化策略管理，内置场景模板，支持策略优先级设置，支持基于IP地址、应用、地理位置、时间段等对象下发指定的安全策略。			
应用识别与管控		识别6000+应用，访问控制精度到应用功能，例如：区分微信的文字和语音。 应用识别与入侵检测、防病毒、内容过滤相结合，提高检测性能和准确率。 支持用户自定义应用，支持应用标签分类。			
入侵防御		准确检测并防御针对操作系统、应用、服务器等各种漏洞的攻击，支持0 day攻击防护。 可防护各种针对web的攻击，包括SQL注入攻击和跨站脚本攻击等。 支持用户自定义签名 支持8000+签名数			

型号	NIP6305E/ NIP6310E/NIP6510E	NIP6550E/ NIP6550ED	NIP6610E	NIP6620E-AC/DC
反病毒	病毒库每日更新，可迅速检出超过500万种病毒。			
DoS/DDoS 攻击防护/检测	支持DDoS攻击防护，可防范SYN flood、UDP flood等种常见网络层DDoS攻击及HTTP、HTTPS、SIP、DNS等应用层DDoS攻击 支持智能学习流量模型			
SSL加密流量检测	可作为代理检测并防御隐藏在SSL加密流量中的威胁，包括入侵防御、防病毒、URL过滤等应用层防护。			
IPv6报文检测	支持IPv4/IPv6双栈，支持IPv6报文检测及防护			
隧道报文检测	支持VLAN、QinQ、MPLS、GRE、IPv4 over IPv6、IPv6 over IPv4等隧道报文检测			
安全态势感知	获取用户网络资产环境信息，支持对安全事件进行风险级别的校正及IPS策略调优			
基于信誉检测机制	支持IP信誉和C&C信誉，及时获取云端最新数据，有效检测和拦截恶意IP和恶意域名连接			
URL过滤	支持URL关键字检测及阻断，日志告警			
响应方式	日志告警、丢弃报文、阻断、限流、联动、SNMP Trap告警、邮件/短信/声音告警			
带宽管理	在识别业务应用的基础上，可管理每用户/IP使用的带宽，确保关键业务和关键用户的网络体验。			
日志及报表	支持日志查找、分析、备份 基于威胁事件、流量统计、协议统计等生成多维度报表，支持报表订阅 可以基于地理位置生成攻击态势地图和流量分布地图			
升级	支持在线自动及手动升级、离线升级、集中升级，系统支持U盘一键式升级、热补丁			
系统配置管理和维护	支持GUI图形化配置和命令行配置，支持远程管理和集中管理，提供独立的管理接口 管理员分权分域，支持本地安全认证、服务器认证等多种认证方式 支持诊断功能和系统资源监控			
部署方式及工作模式	支持接口对直路部署、旁路检测部署、直路/旁路混合部署； 支持单臂直路部署（二层交换机旁挂及三层网关旁挂）； 支持非对称路由报文检测，会话关联检测，支持单向报文检测模式； 支持二、三层基本转发，支持静态路由及动态路由协议			
高可靠性	支持“主备”和“负载分担”场景下的双机热备；支持硬件Bypass			

注：性能数据是在理想环境下测试得出，实际情况会因现网情况不同而出现变化。

订购信息

NIP6000E产品报价项介绍

对外型号	NIP机型编码	中文描述
LIC-NIP6305E-IPS-1Y	88035DBA	IPS特征库升级12个月(适用于NIP6305E)
LIC-NIP6305E-IPS-3Y	88035DBB	IPS特征库升级36个月(适用于NIP6305E)
LIC-NIP6310E-IPS-1Y	88035LNY	IPS特征库升级12个月(适用于NIP6310E)
LIC-NIP6310E-IPS-3Y	88035LPB	IPS特征库升级36个月(适用于NIP6310E)
LIC-NIP6510E-IPS-1Y	88035DBC	IPS特征库升级12个月(适用于NIP6510E)
LIC-NIP6510E-IPS-3Y	88035DBD	IPS特征库升级36个月(适用于NIP6510E)
LIC-NIP6550E-IPS-1Y	88035LPC	IPS特征库升级12个月(适用于NIP6550E)
LIC-NIP6550E-IPS-3Y	88035LPD	IPS特征库升级36个月(适用于NIP6550E)
LIC-NIP6610E-IPS-1Y	88035HME	IPS特征库升级12个月(适用于NIP6610E)
LIC-NIP6610E-IPS-3Y	88035HML	IPS特征库升级36个月(适用于NIP6610E)
LIC-NIP6620E-IPS-1Y	88035LPE	IPS特征库升级12个月(适用于NIP6620E)
LIC-NIP6620E-IPS-3Y	88035LPF	IPS特征库升级36个月(适用于NIP6620E)
LIC-NIP6305E-AV-1Y	88035DBE	AV特征库升级12个月(适用于NIP6305E)
LIC-NIP6305E-AV-3Y	88035DBF	AV特征库升级36个月(适用于NIP6305E)
LIC-NIP6310E-AV-1Y	88035LPP	AV特征库升级12个月(适用于NIP6310E)
LIC-NIP6310E-AV-3Y	88035LPQ	AV特征库升级36个月(适用于NIP6310E)
LIC-NIP6510E-AV-1Y	88035DBG	AV特征库升级12个月(适用于NIP6510E)
LIC-NIP6510E-AV-3Y	88035DBH	AV特征库升级36个月(适用于NIP6510E)
LIC-NIP6550E-AV-1Y	88035LPR	AV特征库升级12个月(适用于NIP6550E)
LIC-NIP6550E-AV-3Y	88035LPS	AV特征库升级36个月(适用于NIP6550E)
LIC-NIP6610E-AV-1Y	88035HMM	AV特征库升级12个月(适用于NIP6610E)
LIC-NIP6610E-AV-3Y	88035HMN	AV特征库升级36个月(适用于NIP6610E)
LIC-NIP6620E-AV-1Y	88035LPT	AV特征库升级12个月(适用于NIP6620E)
LIC-NIP6620E-AV-3Y	88035LPU	AV特征库升级36个月(适用于NIP6620E)
LIC-NIP6305E-CS-1Y	88035DBN	云沙箱检测服务12个月(适用于NIP6305E)

对外型号	NIP机型编码	中文描述
LIC-NIP6305E-CS-3Y	88035DBP	云沙箱检测服务36个月(适用于NIP6305E)
LIC-NIP6310E-CS-1Y	88035LQK	云沙箱检测服务12个月(适用于NIP6310E)
LIC-NIP6310E-CS-3Y	88035LQL	云沙箱检测服务36个月(适用于NIP6310E)
LIC-NIP6510E-CS-1Y	88035DBQ	云沙箱检测服务12个月(适用于NIP6510E)
LIC-NIP6510E-CS-3Y	88035DBR	云沙箱检测服务36个月(适用于NIP6510E)
LIC-NIP6550E-CS-1Y	88035LQM	云沙箱检测服务12个月(适用于NIP6550E)
LIC-NIP6550E-CS-3Y	88035LQN	云沙箱检测服务36个月(适用于NIP6550E)
LIC-NIP6610E-CS-1Y	88035HMP	云沙箱检测服务12个月(适用于NIP6610E)
LIC-NIP6610E-CS-3Y	88035HMQ	云沙箱检测服务36个月(适用于NIP6610E)
LIC-NIP6620E-CS-1Y	88035LQY	云沙箱检测服务12个月(适用于NIP6620E)
LIC-NIP6620E-CS-3Y	88035LRA	云沙箱检测服务36个月(适用于NIP6620E)
LIC-NIP-E-SECD	88035DHF	加密流量检测功能(适用于NIP-E)