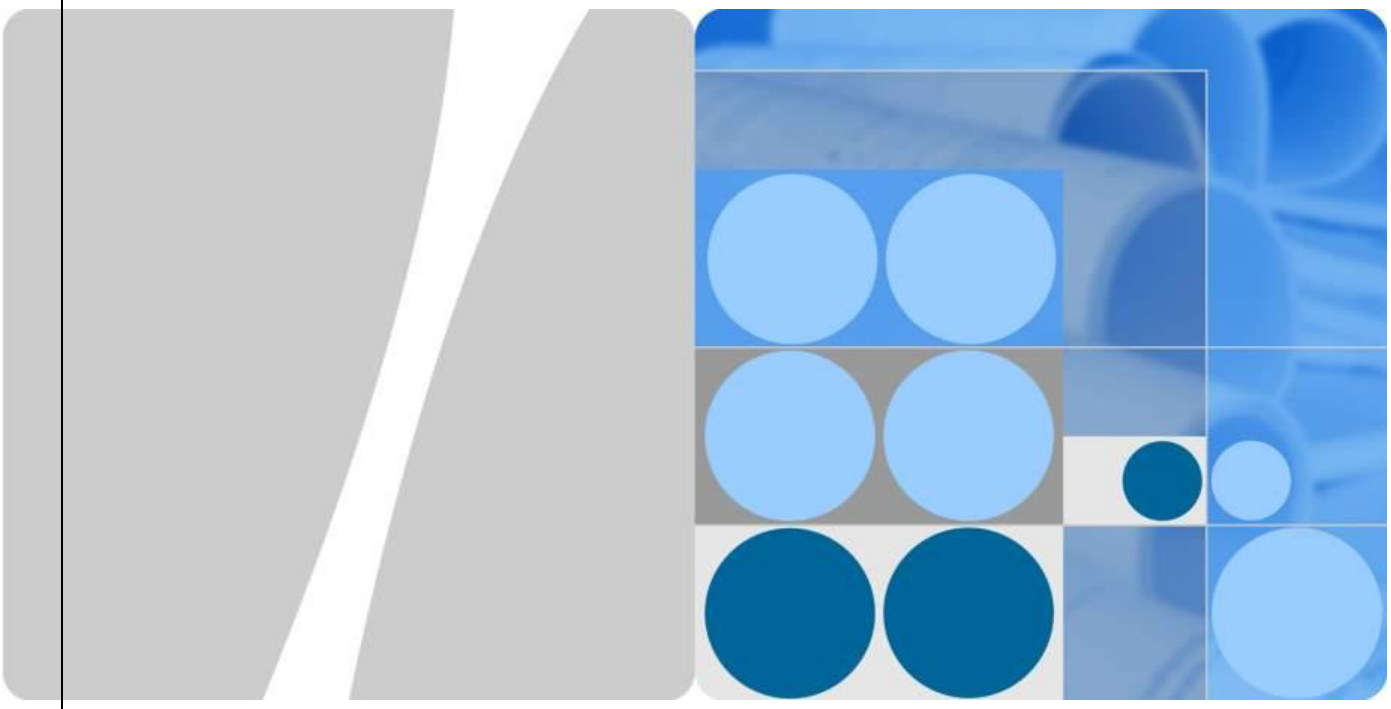


NIP 入侵检测与防御产品
销售策略指导书

(渠道版)

Issue V2.1

Date 2013-04-18

华为技术有限公司

HUAWEI

适用范围&修订记录

适用范围：适用于全球所有经华为企业业务认证的总经销商、一级经销商（VAP）及二级经销商

修订记录：

日期	版本	描述	作者
2013/4/8	1.0	该文档内容主要基于 NIP2013 年上半年的版本	华为公司

目 录

1 上市产品

1.1 上市全景图

2013 年 NIP 新上市四款产品，和前期上市的四款产品共八款产品完全覆盖目前 IPS/IDS 的主要场景。

1.2 产品销售状态概览

1.2.1 NIP 可销售主机型号

产品	产品系列	备注
NIP2000		
	NIP2030	分销产品

产品	产品系列	备注
	NIP2100	分销产品
	NIP2130	非分销产品(运营商不销售)
	NIP2150	非分销产品(运营商不销售)
	NIP2200	非分销产品
NIP5000		
	NIP5100	非分销产品
	NIP5200	非分销产品
	NIP5500	非分销产品
NIP2000D		
	NIP2030D	分销产品
	NIP2100D	分销产品
	NIP2130D	非分销产品(运营商不销售)
	NIP2150D	非分销产品(运营商不销售)
	NIP2200D	非分销产品
NIP5000D		
	NIP5100D	非分销产品
	NIP5200D	非分销产品
	NIP5500D	非分销产品

1.2.2 NIP 板卡销售状态

板卡	板卡描述	备注
FIC-4GE-BYPASS	4GE 电口 Bypass 卡-含 HS 通用安全平台软件	只适用于 NIP2000/5000
FIC-2LINE-M-BYPASS	2 链路 LC/UPC 多模光接口 Bypass 保护卡-含 HS 通用安全平台软件	

FIC-2LINE-S-BYPASS	2 链路 LC/UPC 单模光接口 Bypass 保护卡-含 HS 通用安全平台软件	
FIC-8GE	8GE 电口卡-含 HS 通用安全平台软件	只适用于 NIP2000/NIP5000/NIP5000D
FIC-8SFP	8GE 光口 FIC 卡-含 HS 通用安全平台软件	
FIC-2SFP+	2*10GE 光口 FIC 卡-含 HS 通用安全平台软件	只适用于 NIP5000/NIP5000D
FIC-2SFP+8GE	2*10GE 光口+8GE 电口卡-含 HS 通用安全平台软件	不适用与 NIP5500/NIP5500D

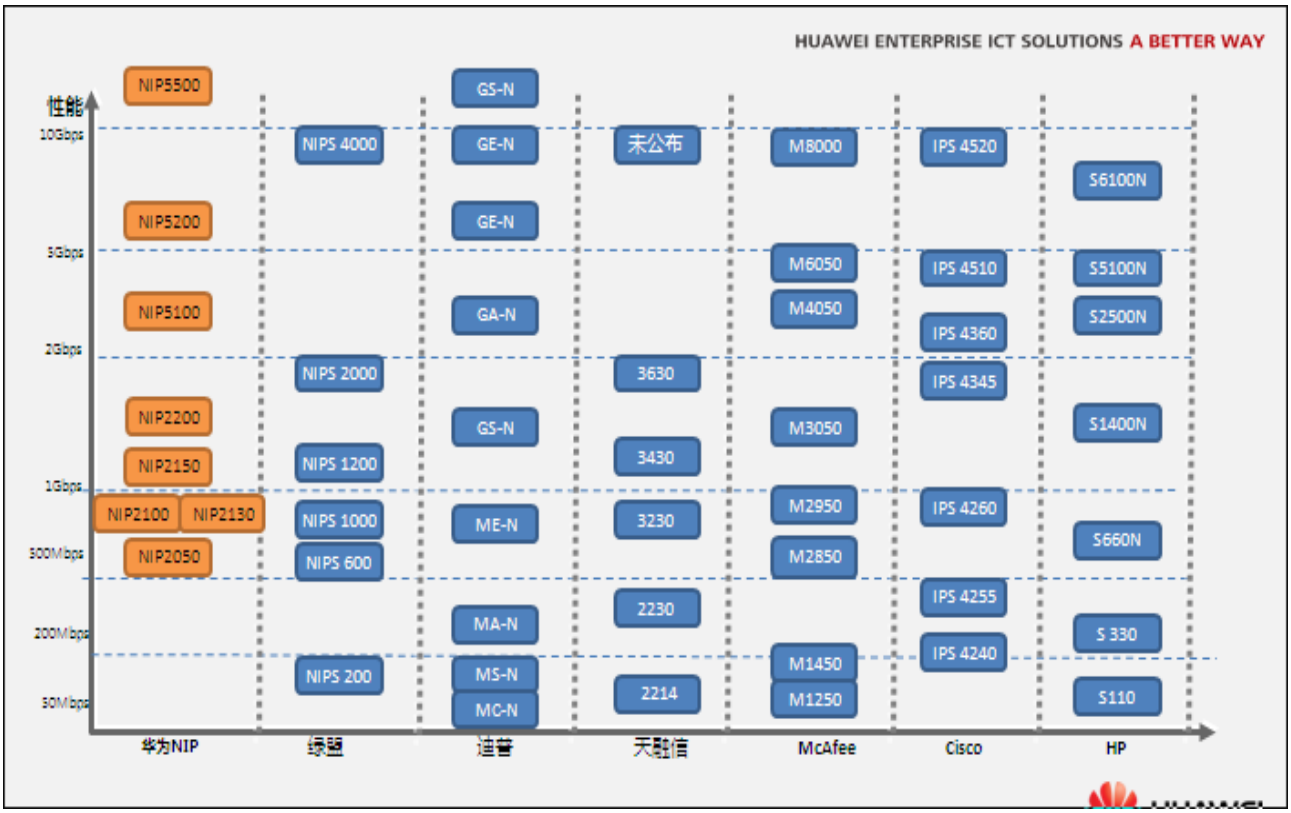
1.3 产品定位与卖点

1.3.1 NIP 产品定位与产品卖点

产品	定位	基本特点	卖点
NIP2050/ NIP2050D NIP2100/ NIP2100D NIP2130/ NIP2130D	1、中小企业互联网出口 2、企业部门隔离 3、中小企业分支互联	1、 **配置简单** 2、 多种攻击防护 3、 识别 1200+应用 4、 病毒防护	1、零配置上线，适用于小企业技术力量薄弱，管理方便； 2、识别应用种类多，便于带宽控制，提供员工的工作效率 3、攻击和病毒防护一体化，减少用户的投资
NIP2150/ NIP2150D NIP2200/ NIP2200D	1、中型企业互联网出口 2、中型企业分支互联 3、企业部门隔离	1、 **配置灵活** 2、 签名库默认开启率高 3、 识别 1200+应用	1、配置灵活，提供多种配置模板供用户多种场景使用； 2、高开启率确保攻击的高识别能力，保障用户业务安全 3、识别应用种类多，便于带宽控制，提供员工的工作效率
NIP5100/ NIP5100D NIP5200/	1、中大型企业互联网出口 2、中大型企业分支互	1、 **高性能** 2、 签名库高开率 3、 应用层 DDOS 攻击防护	1、NIP 保持在大流量场景依然保持检测与防御能力稳定，远胜于友商； 2、高达 85%的开启率，0 误报，极大

NIP5200D NIP5500 NIP5500D	联 3、数据中心出口防护		提高了大型企业的安全管理效率 3、对多种应用层的 DDOS 攻击防护，保护大型企业和数据中心的 WEB 应用安全

1.4 NIP 系列与友商对比关系



1.5 NIP 产品卖点

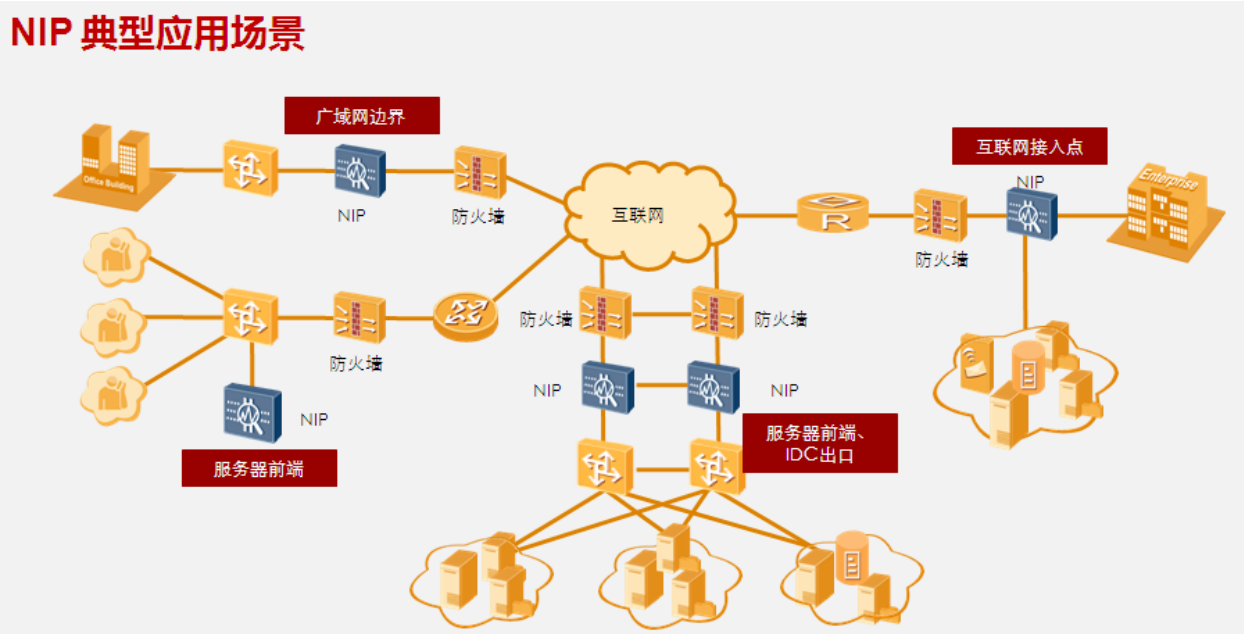
- **全面防护——场景全覆盖**
  - 提供最高达 12G 的 IPS 防护性能，全面覆盖用户各带宽场景；
  - 支持对用户服务器、客户端、互联网出口、分支互联、数据中心等部署场景入侵防护；
  - 提供服务器漏洞攻击防护、Web 应用防护、恶意软件控制、病毒防护、应用管控、网络层 DDoS 防护、应用层 DDoS 防护、上网客户端攻击防护等功能，全面覆盖各种攻击场景；
  - 强大的应用感知能力，识别应用 1200+，全面覆盖用户业务带宽控制；

- **准确检测——“零”误报，有效降低维护成本**
  - 基于先进的漏洞特征检测技术，检测精准，“零”误报，确保用户业务正常运行。
  - 签名库 85%默认开启率，确保系统上线即实时防护；
  - 签名库 80%的默认阻断率，自动阻截关键威胁，确保用户安全无忧。
- **易于使用——“零”配置上线**
  - 零配置上线：设备上电接通即可正常工作，无需复杂的签名调校及网络参数调整；
  - 丰富的策略模板：为各专门场景提供最简单的配置方式，便于客户实施定制化安全策略；
  - 实时系统监控及安全趋势监控，数十种分析报表，轻松掌握安全状态。

2 销售策略

2.1 销售策略综述

NIP 入侵检测与防御产品主打场景包括：



在这些场景中，NIP 主要的市场包括：局域网/园区网市场、数据中心市场、大型企业分支互联市场

2.2 局域网/园区网市场销售策略

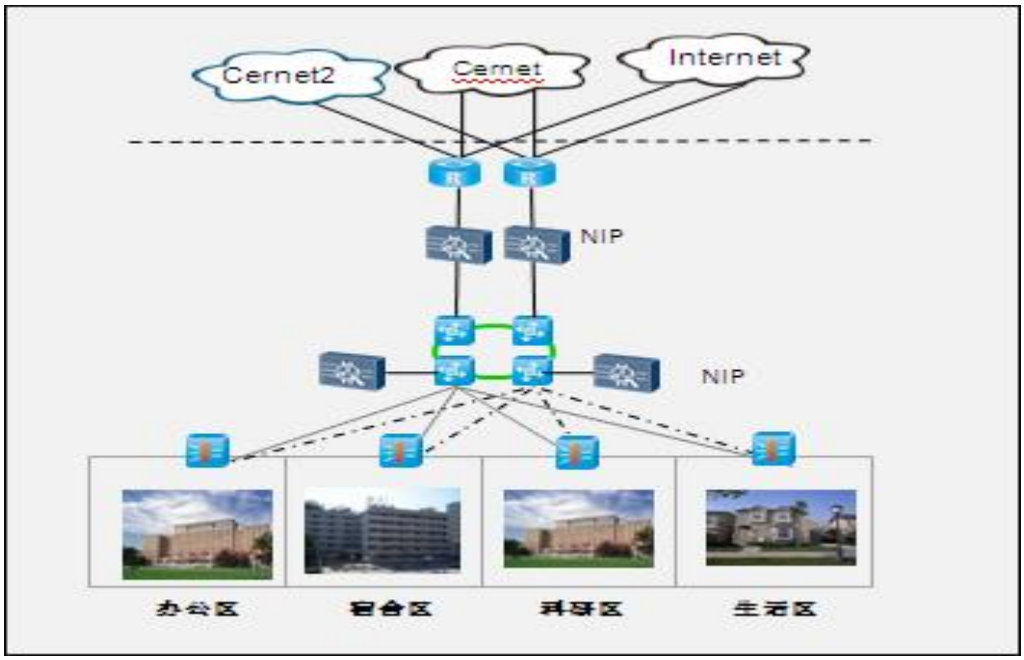
市场概述

企业局域网/园区网是 NIP 的重要市场，根据园区网络的规模和互联方式可以分为五类：具有异地远程分支的大型园区网、具有同城分支互联的大型园区网、独立的大型园区网、中型园区（大楼型园区）网络、中小企业办公网络。

按照园区网络层次一般可以分为 3 个层次：接入层、汇聚层、核心层。大型园区网可能还有数据中心和远程灾备系统，小型园区可能汇聚层与核心层合一。

产品选型策略

在该场景下，NIP 可以部署在不同的位置，可以部署于互联网出口，也可以部署在核心层。



部署在互联网出口的主要功能：

① 防范来自互联网的攻击者对园区网内恶意攻击攻击

② 防范来自互联网的木马、蠕虫、病毒等进入园区网

③ 挂马的恶意网页防护，确保内网用户上网安全

④ P2P 等网络滥用流量限制

部署在核心层的主要功能：

① 汇聚层部署实现安全压力下移，在更靠近攻击源和保护目标的地方实现安全防御

② 防范内网恶意或误用的用户产生的安全威胁

③ 核心层部署 NIP，在园区网核心节点处实现应用层安全威胁监控

设备选型推荐如下：

网络层次	主推设备	产品亮点
万兆园区网	NIP5500/NIP5500D	真性能，0 误报
中型企业局域网	NIP5200/NIP5200D/NIP5100/NIP5100D	0 误报，高开启率，多场景模板
中小型企业局域网	NIP2000/NIP2000D 系列	0 配置，多应用识别控制

竞争引导策略

局域网/园区网引导策略归纳为如下几条：

- **配置简单**：NIP 产品可以实现零配置上线，快速部署，实现即插即用。
- **默认开启率高**：NIP 默认的检测开启率和阻断率都达到 80%以上，不需要复杂的配置即可实现实时的检测与防护，极大降低了设备上线的复杂性，提高安全运维的效率。
- **应用控制**：NIP 可以实现 1200+的应用识别，可以实现精细化的带宽控制，保证了正常业务的体验，提高员工的工作效率

2.3 数据中心市场销售策略

市场概述

数据中心（Data Center）是一个重要的网络服务平台，它通过与某一骨干网高速连接，借助丰富的内容资源向企业或网站提供大规模、高质量、安全可靠的专业化服务器托管、空间租用、网络带宽批发等业务。

数据中心 IP 网络设备的层次可以分为：接入层、（汇聚层）、核心层（很多扁平化的大型数据中心没有汇聚层）。中小型数据中心可能汇聚层与核心层合一。

部署在数据中心可以实现如下功能：

① 提供虚拟软件补丁服务，防护系统漏洞（包括 Windows、非 Windows 系统漏洞、中间件漏洞、应用软件漏洞）

② 抵御来自内网攻击，保护核心服务器和核心数据

③ 防范恶意攻击者对数据中心的敏感信息窃取、拒绝服务等

④ 保护数据中心的业务安全、业务连续性和业务性能。

⑤ SQL 注入、跨站等基于 Web 的安全防护

⑥ 防范网页挂马

设备选型推荐如下：

网络层次	主推设备	产品亮点

数据中心	NIP5500/NIP5500D	真性能，0 误报

竞争引导策略

数据中心引导策略归纳为如下几条：

- **检测性能稳定**：NIP 在万兆的用户真实环境中，能保持检测与防护性能稳定，保证了对各种攻击的实时检测，有效的保护了数据中心安全。

- **0 误报**：NIP 在各种流量场景下，在保持高检测率的同时，实现零误报，减少安全运维工作量，提高安全运维的效率。

- **应用层 DDOS 攻击防护**：NIP 实现对应用层 DDOS 的攻击检测与防护，有效保护数据中心的各种应用服务器和 WEB 服务器的工作效率。

2.4 销售模式

NIP 采用主机+软件升级 LICENSE 的模式进行销售；

对于基础知识库升级，默认主机配送一年，如果需要可以单独采购一年期或者三件期 license；

对于防病毒知识库：默认主机不开启该功能，如果需要改功能，则需要采购该 LICNESE，，如果需要，可以采购一年期或三年期。