

华恒科技嵌入式防火墙解决方案

随着网络应用的不断发展，网络安全显得越来越重要。市场对于防火墙产品的需求不断增加，现有的防火墙产品已经无法很好的满足用户的需求，诸多的厂商已经开始尝试往嵌入式方面发展。华恒科技作为业内领先的嵌入式技术开发商，将为安全领域提供有力的支持。本文将围绕嵌入式防火墙应用作相应的介绍。

一、行业概述

目前，黑客入侵与病毒发作事件在全球范围内的不断增加。由于网络应用的迅速发展，除以往熟知的病毒、垃圾邮件，以及黑客恶意攻击、网络钓鱼之外，也有来自企业内部的安全隐患等，这些问题困扰着每一个企业，形成了市场需求的土壤。有关报告显示，2005年第一季度全球网络安全专用设备和软件收入比去年第四季度增长5%，预计2006年第一季度将增长27%，达13亿美元。到2008年整个市场年收入有望增长至65亿美元。

国内的互联网技术在近几年内得到快速的普及和发展，网络用户数量也急剧膨胀。网络用户的增多，加上用户素质的参差不齐，增加了网络的不稳定因素。据调查表明，约有20%的网络入侵、黑客攻击事件来自中国。网络安全已经成为越来越多使用网络的公司、个人需要考虑的问题。越来越多的企业也将网络的安全性看作确保企业盈利能力的一项重要因素。2004年中国防火墙产品市场销售额约为15亿元，以国内目前持续发展的网络状况，对于防火墙等安全类产品的需求还在不断增长。不过目前网络安全产业还未最终成熟，业界尚未有明确的标准和规范，这给一些新进的公司制造了很多机会。

目前的防火墙产品的用户主要是企业用户，互联网已经改变了人们工作、联络、协作交流以及买卖的方式。网络的安全程度究竟如何？这是许多IT管理人员每天都会考虑的一个问题。现在来自网络的威胁已经不仅仅来自企业网络的外部，类似于服务外包与远程办公等新商务趋势的出现更进一步使企业的安全问题复杂化。

随着网络的发展，现在已经有越来越多的家庭网络用户。由于大部分住户的互联网服务都运行在开放的链路上，并且没有高级安全手段加以保护，家庭的PC计算机非常容易受到黑客的攻击。

可以想象，未来的防火墙应用必定越来越普及，这个普及不光面向各个公司、企业，也深入到家庭、个人；深入到每个网络节点、终端。应用的普及必定对产品的成本提出较为严格的要求，现有的防火墙产品大多数采用基于X86架构的PC机进行开发，在成本、体积、功耗、稳定性、乃至产品化方面都有所欠缺。嵌入式防火墙产品必定会有越来越广泛的应用，下文将以IXP425为例介绍基于嵌入式处理器开发的防火墙产品。

二、网络处理器

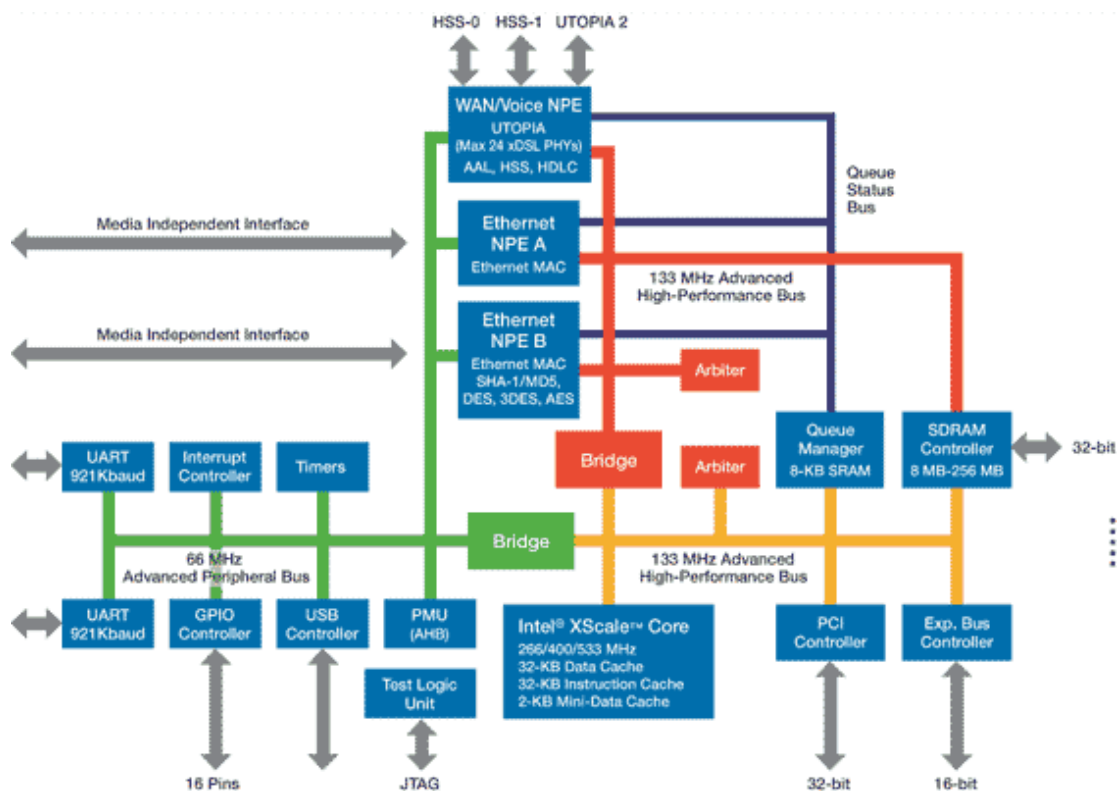
近年来，从国内的安全厂商开始进军高端网络安全市场，NP这个名词开始变得流行起来。NP即网络处理器(Network Processor)，即专门用于做网络数据处理的芯片。网络处理器在处理器家族中属于专用处理器，即专门为了特殊应用而设计的处理器，它有别于X86系列通用处理器。

目前提供NP芯片的厂家也很多，基本上都符合NPF指定的规范，就目前国内市场应用最为广泛的是INTEL公司的IXPXXX系列芯片，包括IXP4XX、IXP12XX、IXP24XX、IXP28XX等；以及FreemScale(原Motorola半导体)公司的MPCXXX系列芯片，包括

MPC8XX、MPC8XXX 等。IXP 系列 NP 处理器从体系结构上看基本上都一样，都是由一个 RISC 处理器加一个微引擎构成，RISC 处理器主要用于控制微引擎的运行，所以又称为控制层面，微引擎完成对网络数据包的处理，以实现高性能，所以又称为数据层面；不同 IXP 系列处理器主要是 RISC 的型号和主频，以及微引擎的个数有所不同。

IXP4xx

IXP4xx 的市场定位主要在中低端市场，因此使用基于 IXP4xx 芯片做出的网络安全产品也主要定位在中低端市场中。特别需要注意的是，IXP425 内嵌了一个加密引擎，支持一些公开的密码算法，如：3DES、AES、MD5、SHA1；因此特别适合于中低端 VPN/FIREWALL 产品的开发。



图一 IXP425 网络处理器架构

IXP425 处理器特性：

- 高达 533MHz 的 Intel® XScale® RISC 核心
- 三个网络处理器引擎
- 两个高速串行接口可以用来接 VoIP SLIC/CODEC 或 T1/D1
- 两个内置 MII 接口的 10/100 Base-T 以太网 MAC 性能可达线速
- UTOPIA 2 接口—多个 ADSL/G.SHDSL 或 VDSL 支持
- 33/66M PCI 2.2 标准接口，可连接达 4 个设备
- 硬件安全加速器 (Ipsec : DES、3DES、SHA1、MD5)
- USB 版本 1.1 设备控制器
- 两个 UARTS— 一个高速 UART (921.6 Kbps) 和一个控制台 UART (230.4 Kbps)
- 32 位 SDRAM 控制器，可支持到 256M 内存
- 16 个 GPIO 管脚

- 16 位可配置扩展总线
- ATM、TDM、以太网 MAC 过滤和 HDLC 支持
- 商用和扩展的温度选项

除应用于防火墙产品外，IXP425 还适合应用于以下产品应用：

- 无线家庭网关
- 路由器
- 交换机
- NAS 共享存储系统
- VoIP 网关
- 安全设备
- 工业控制

目前 Intel 新近推出的 IXP465 芯片，更适合安全类产品应用，该芯片有以下特性：

- Intel® IXP46X 系列网络处理器，适合中小企业通信及嵌入式网络应用
- 基于 Intel Xscale® 内核，主频可达 667MHz，满足高端应用需求
- 内置 LAN，WAN，I2C 和 SSP（同步串口）等资源，减少了整体成本，降低了开发难度
- 集成了加密功能，时钟同步，以及内存纠错功能，提高了性能和可靠性
- 兼容 Intel® IXP4XX 产品线软硬件设计规范，保证用户系列化产品的开发，软件可自由移植，减少研发投入，加快产品上市周期

IXP12XX

IXP 从 12XX 系列开始已经可以让软件开发人员根据不同的应用定制微引擎上的微码，以实现不同的功能，IXP12XX 拥有 6 个微引擎，每个微引擎上可以存储条 2k*32 位的指令，12XX 系列 NP 非常适合用来做包转发处理和 QOS 处理。

IXP24XX

从 2003 年开始，Intel 公司推出了 IXP24XX 系列的网络处理器，这款网络处理器比 12XX 系列的网络处理器在性能上有了质的变化，同时基于 IXP24XX 系列的板卡设计上也复杂了很多。目前国内有不少安全厂商开始使用基于这款芯片的板卡来设计网络安全设备，如防火墙，IDS。

理论上，使用一个 IXP2400 可以做到 4 个千兆口的线速，当然在实际防火墙应用中，还要兼顾分片报文重组，NAT，QOS，ARP 处理，深度检测等，这些功能加上去后，处理的时间就会有所增加。因此使用单 2400 做出的防火墙可能在单纯包转发上到达线速，但是用户并不是将一个防火墙当作路由器来用，而是需要它完成一系列安全处理功能，因此只要把包过滤、NAT、抗 DOS 攻击、抗蠕虫攻击等功能加上后，性能就会有所下降；目前据了解，已经有部分高端防火墙采用了基于 IXP24XX 芯片的板卡。

IXP28XX

IXP28XX 的 NP 处理器从性能上比 IXP24XX 的性能又增加了很多，可实现高达 10Gbps 的小包转发和传输管理。一个 IXP2800 的性能甚至要比两个 IXP2400 的性能要高，16 个完全可编程并行处理微引擎，累计可达到每秒 23.1G 的处理速度，但价格却更便宜；单从芯片的性能指标上看，IXP28XX 比 IXP24XX 更有可能做出千兆线速的网络安全设备。但是目前

还没有一家 NP 板卡厂商能够推出基于 IXP2800 的板卡，可能是由于 IXP2800 板卡的设计要比 IXP2400 板卡设计要更加复杂。不过 IXP2800 应该是高端防火墙的应用方向，在这方面产品计划的公司不妨委托华恒科技定制开发。

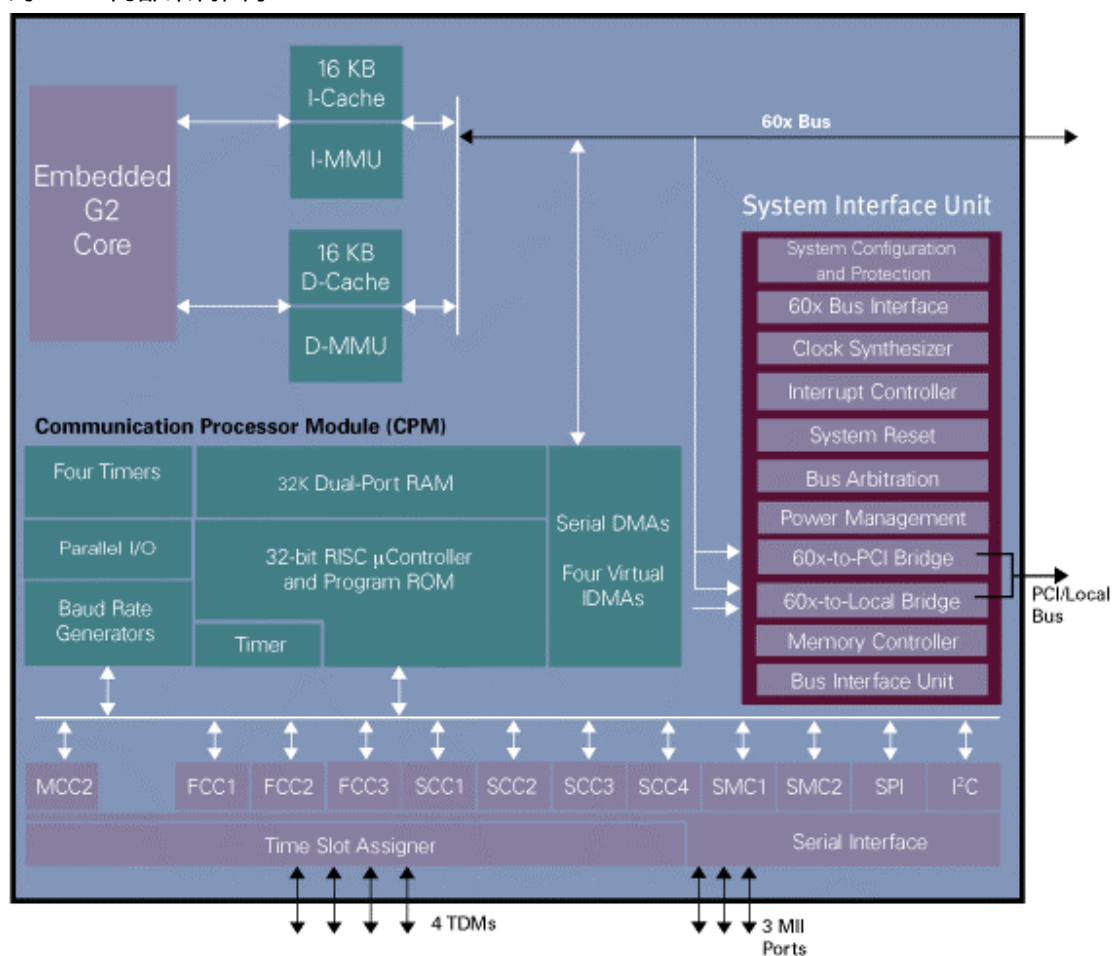
MPC8XX

MPC8XX 属于 Freescale MPC PowerQUICC 系列通讯处理器，针对嵌入式网络、安全、通讯产品应用提供了低成本的解决方案。该系列处理器主频一般在 100MHz 左右，同时集成了一个独立的通讯处理模块（CPM）负责通讯处理。内置了片上安全引擎、双百兆以太网口、USB，并且总线频率提高到 80MHz，满足更高系统总线吞吐速度；相应的成本、性能、功能都得到了进一步的改善。

MPC8XX 可以满足多种平台的开发和应用，主要有：低端防火墙、路由器、VPN 网关、家庭网络设备、无线网关等等。基于该系列低端处理器进行开发，有更大的可能深入到每一个网络终端，如作为 PCI 卡，或集成到 PC 主板上。

MPC82XX

MPC82XX 是 Freescale PowerQUICC II 系列高性能的综合通讯处理器，在 PowerQUICC 系列处理器的基础上性能得到进一步的提高。以下是 MPC82XX 具有代表性的一款处理器的 CPU 内部架构图示：



图二 MPC82XX 处理器架构

该系列的处理器拥有高效的双核结构，包含了 PowerPC 603e 内核以及一个独立的通

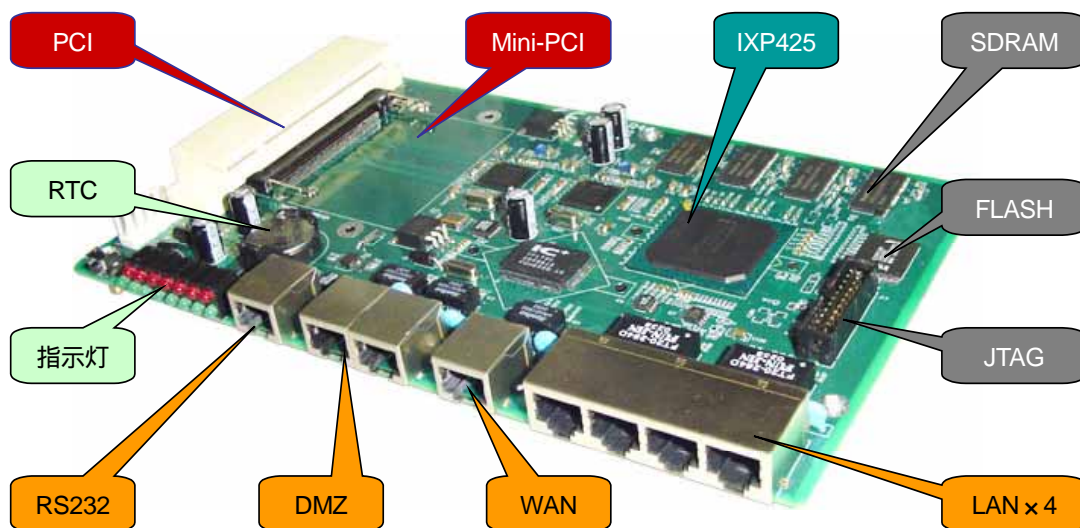
讯处理模块 (CPM)。处理器可高效的运行在 CPU 主频 400MHz，CPM 频率 200MHz，总线频率 100MHz。该系列处理器内置经济有效的安全引擎，可以支持工业标准的加密算法。为满足对成本敏感、安全性能要求高的网络应用，在处理器内部集成了专门的模块和丰富的外围接口。可以简化外围电路的设计要求，降低整体的器件成本和电路设计复杂度。

而软件开发方面，相关的应用软件可以在 PowerQUICC 和 PowerQUICC II 系列各个处理器平台上进行平滑移植，减少软件重复开发的可能，降低了研发的投入。

除基于 Intel Xscale 系列处理器的平台外，华恒科技还提供基于 [Freescale](#) (原 Motorola 半导体) PowerPC 系列网络处理器的 [开发平台](#) 和相关解决方案，为用户提供了更多的选择。

三、参考设计

目前华恒科技已经推出基于基于 IXP425 的 [嵌入式防火墙开发平台](#) 及解决方案。相应的参考设计见图二：



图三 HHXscale425-Firewall-R1 防火墙硬件平台

华恒科技作为业内领先的嵌入式 LINUX 平台供应商，具备提供成熟、领先的嵌入式 LINUX 系统软件以及稳定的底层设备驱动软件的能力；华恒科技基于 IXP425 平台整合了成熟的平台软件，推出具有较高性价比的嵌入式防火墙解决方案，同时能够在嵌入式 LINUX 软件开发上给予客户强大的技术支持。

嵌入式防火墙使用先进的网络处理器专门硬件 (IXP425 Network Processor) 利用其优化的网络处理单元和集成的 VPN 硬件加密引擎。可部署在中小网络出口，可同总部网络搭建端对端的 VPN 连接，支持双方静态 IP 和一方动态 IP 的 VPN 连接，加密算法支持主流的 3DES、AES 等。

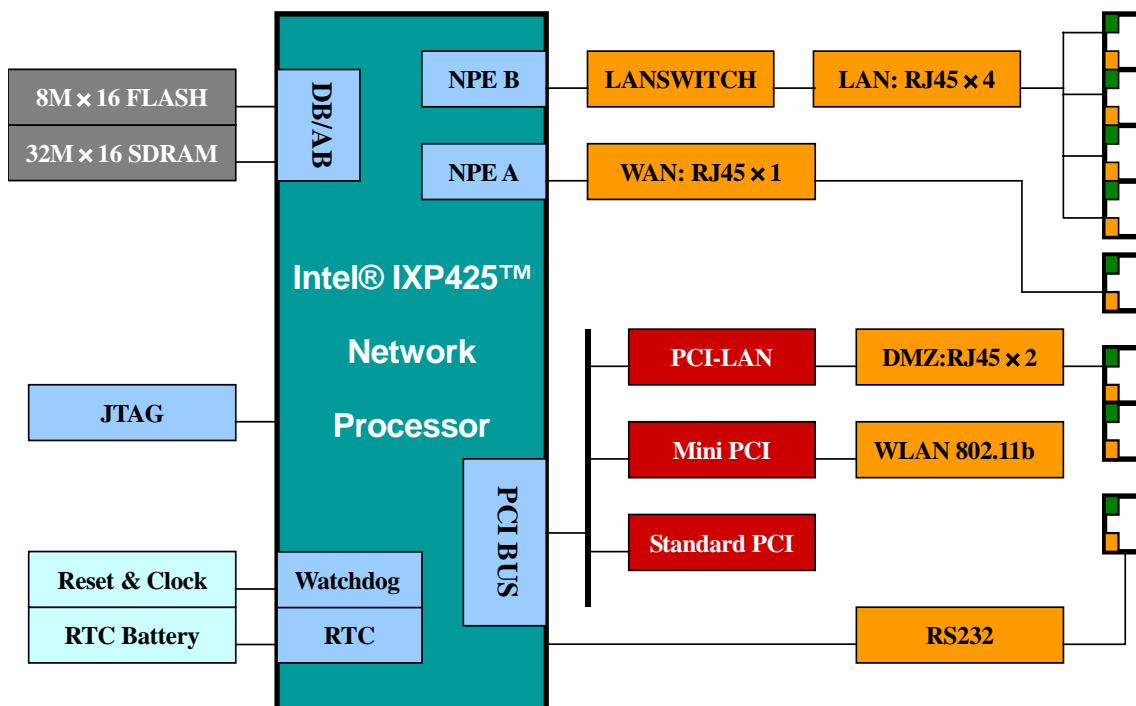
嵌入式防火墙产品可以满足任何百兆网络环境，无用户数目限制。可为用户提供宽带接入、防火墙、蠕虫防护、入侵检测、内容过滤、VPN 接入和日志审计多项安全需求。

防火墙设备属于网关设备，因此可靠性非常重要。嵌入式防火墙产品采用嵌入式体系结构，嵌入式处理器内置丰富的接口资源，可以简化外围电路设计，使硬件更加稳定；可有效避免传统的 x86 结构防火墙由于接插件松动引起防火墙的故障；同时嵌入式防火墙产品均

为低功耗设备，可有效避免传统的 x86 结构防火墙由于散热问题引起防火墙的死机现象。

嵌入式防火墙产品的性能、稳定性、实用性、功耗、体积等各方面都有优越的表现，相信在未来的网络安全应用领域得到更加广泛的应用。华恒科技期待与各安全产品厂商建立长期深入的技术与市场的合作。

四、系统架构



图四 HHXscale425-Firewall-R1 硬件系统架构

- 处理器采用 Intel IXP425，533MHz Xscale 内核
- IXP425 内置 FLASH、SDRAM 控制器，该硬件平台可选配 8-64M FLASH，64-256M SDRAM。
- 通过内置 NPEB MII 扩展 LANSWITCH 交换芯片，扩展 4 个 10/100M 局域网口；内置 NPEA 用作 100M 对外广域网接口；通过 PCI 接口扩展以太网 MAC + PHY 用作 DMZ 军事区网络接口。
- 提供 Mini-PCI 接口，扩展 802.11b WLAN 无线局域网通讯接口，满足无线连接的应用需求。
- 提供标准 PCI 接口，可扩展多种 PCI 卡设备，扩展多种接口功能。
- 用户可通过 RS232 串口对系统软件进行调试、设置；可以通过 JTAG 对系统进行调试、更新。
- 提供 RTC 实时钟，提供日历功能，满足日志备份的要求。
- 提供看门狗及复位电路，系统如意外死机可自动重启，保证连续工作的要求。

五、软件功能

基于华恒科技嵌入式防火墙平台，可以开发出具有强大系统性能和丰富软件功能的防火

墙产品：

防火墙类型	包过滤、状态检测、代理	
网络特性	10/100M 以太网口	共 6 个 RJ45 接口，4 个通过 LANSWITCH 扩展作为局域网通讯接口
		2 个有独立 MAC 的网口
		1 个可作为对外的 Wan 口
		1 个可作为 DMZ 区域接口
VPN (虚拟专用网)	建立 VPN 通道协议	支持 Ipsec、L2TP
	通用性	支持与其他厂商 VPN 网关互通
应用层防御	限制应用程序携带恶意代码	包含丰富的特征库
	防病毒	可包含丰富的病毒列表
	防 DoS 攻击	可抵御常见 DoS 攻击
	支持多种内容过滤协议	如：HTTP、SMTP、FTP、POP3、IMAP
其他安全特性	P2P 阻断	可通过防火墙设备阻断 BT、eDonkey 等 P2P 下载软件
	支持保存日志	保存至硬盘、电子盘、Syslog 服务器、U 盘等
	告警方式	邮件、日志、短信等
管理功能	虚拟防火墙	可虚拟成多台防火墙系统,可独立设置策略、帐号和审计功能,每个 VF 可识别 VLAN ID 和 IP 地址范围段
	支持身份认证	Built-in database、OS password、网关认证、RADIUS、LDAP
	支持 SNMP 版本	支持 V1、2、3
	支持带宽管理	支持带宽、浏览管理、监控
	支持专有软件管理	支持友好的图形界面管理、嵌入式 Webserver 管理
	支持中文管理	全中文的管理界面
	支持软件升级	可远程升级软件和固件

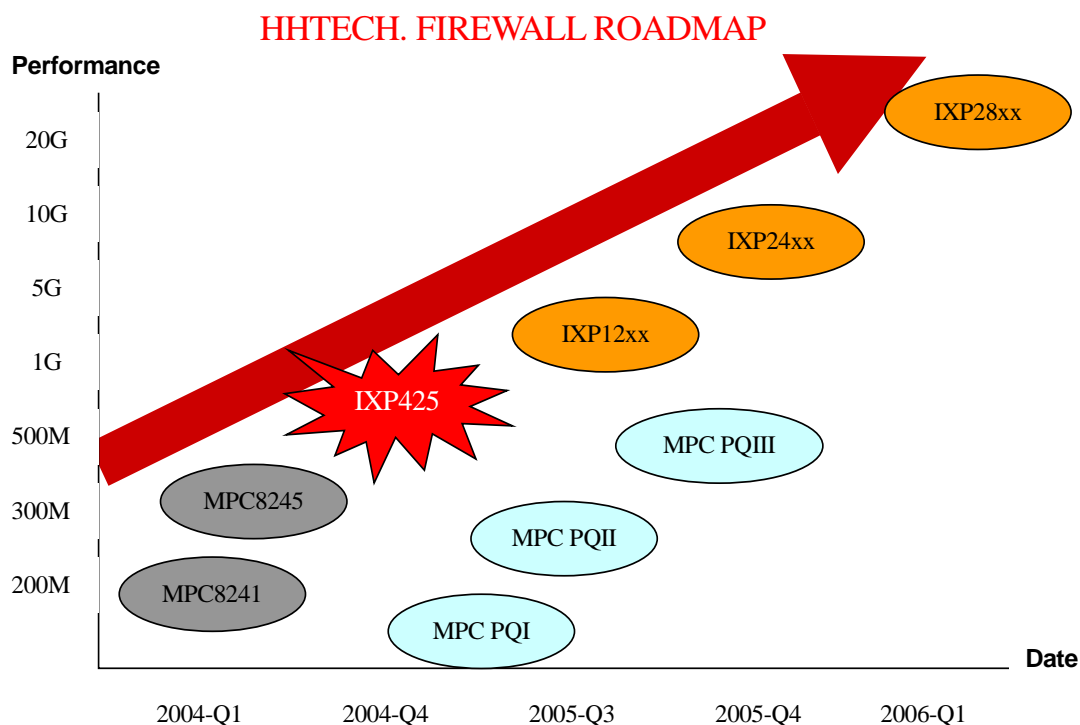
六、平台优势

成熟的平台软件以及稳定的底层设备驱动软件：华恒科技是一家领先的嵌入式 LINUX 平台供应商；具备提供成熟、领先的嵌入式 LINUX 系统软件以及稳定的底层设备驱动软件的能力；在嵌入式 LINUX 软件开发上能够给予客户强大的技术支持。例如：华恒在 LINUX 内核以及应用程序的裁减、各种 uClibc 库的使用和调试上具有丰富的开发和技术支持经验；华恒在消费电子类设备上甚至实现了 3 秒启动整机系统、所有应用程序不超过 1M 字节的记录。

富有经验和强大实力的硬件制造能力和质量保障体系：华恒科技在网络通信以及工业控制的硬件板级制造方面，具备 10K 量的硬件设备制造能力，并且与国内最好的 PCB 生产制造、焊接加工、机箱加工的工厂结成了紧密的合作伙伴关系。华恒能够为纯软件客户提供一站式采购定制服务。例如：广州某客户的广州街头售贩机硬件、南京某客户的银行 VPN 路由器硬件、北京某客户的智能交通公交站牌信息监控设备硬件都是源自华恒科技的硬件批量 OEM 设计、生产制造与质量控制。

完善、丰富的嵌入式平台产品线，统一的软件编程接口：华恒科技的嵌入式处理器平台主频分别为 50MHz、80MHz、133MHz、166MHz、200MHz、350MHz、400MHz、533MHz、667MHz、800MHz、1GHz、1.25GHz；不仅主频分布均匀，适用于各种档次的产品，而且硬件接口非常丰富；更重要的是，这些平台全部采用华恒统一的嵌入式 LINUX 发行版本和开发调试工具，华恒的用户很容易随之扩展其产品线，用户甚至不用修改其软件代码，只需

要重新进行程序的编译即可，可移植性非常强，极大地节约了人力物力的投入，争取了产品上市时间。



图五 华恒科技嵌入式防火墙平台 ROADMAP

七、订购方式

型号	类型	数量	供货期
HHXscale425-Firewall-E1	OEM	1K 量起定	1 个月
HHXscale425-Firewall-EP	ODM, 修改产品存储容量	1K 量起定	2 个月
HHXscale425-Firewall-R1	开发平台	不限	现货
HHPPC8245-4FEC-R1	开发平台	不限	现货

华恒科技市场部：

电话：+86-551-5325652，5325653，5325173

传真：+86-551-5325323

Email：market@hcn.com

网站：www.hcn.com