基于 IXP2400 网络处理器的 IPSec VPN 网关设计*)

刘延华　陈国龙　郭文忠
(福州大学数学与计算机科学学院　福州 350002)

摘　要　VPN 网关系统在网络安全中有着非常重要的应用。为了解决采用 X86 CPU 或 ASIC 平台设计 VPN 网关所存在的速度或灵活性上的不足，提出了一种采用网络处理器 IXP2400 的高速 IPSec VPN 网关设计与实现方案。仿真实验表明，系统达到了千兆级 VPN 网关要求，为研发高速 VPN 网关系统提供了一条新途径。

关键词　IPSec，VPN 网关，IXP2400，网络处理器

Design of IPSec Gateway Based on IXP2400 Network Processor

LIU Yan-hua　CHEN Guo-long　GUO Wen-zhong
(College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350002, China)

Abstract　VPN gateway is important in high-speed network security. To resolve the problem that is low-speed or low-flexibility based on X86 CPU and ASIC, proposed high-speed IPSec VPN design based on IXP2400. The simulation environment experiment proved that the new VPN gateway is high-speed over 1.0Gbps. And it supplies a new approach to design high-speed VPN gateway system.

Keywords　IPSec, VPN gateway, IXP2400, Network processor

1　引言

随着计算机网络技术和新业务的飞速发展，Internet 及其应用已经成为人们生活和工作中的一部分。由于无法确认网络接入方身份，使得与此相关的网络安全事件频频发生，给局域网的安全访问带来巨大挑战。作为一种可靠的网络安全接入技术，虚拟专用网络(VPN)技术就在这种背景下产生了。VPN 是通过访问控制、隧道技术、加密技术、认证技术等在公共的 Internet 上建立起临时(虚拟)安全通道，实现物理上分散而逻辑上统一的多个局域网之间的安全通信功能。VPN 安全网关能够为政府机关、企业和个人提供有效的安全通信保障，且通信费用低廉。

目前，VPN 网关功能的实现多被集成到防火墙系统中。实践证明，这种实现方式在千兆级以上高速网络环境下往往会形成一个通信瓶颈，较大程度地降低了网络可用性。为了解决通信瓶颈的问题，本文以 IXP2400 网络处理器为硬件实现平台，给出一种 IPSec VPN 安全网关的设计与实现方案，该 VPN 网关系统以独立运行形式设计，有效提高了 VPN 网关通信速度，为千兆高速网络的安全通信提供了可靠保障。

2　IXP2400 网络处理器

网络处理器(Network Processor)兼顾了 CPU 的灵活性和 ASIC 的高性能特征，具有并行高速处理、模块化设计、可编程、可扩展性好等特点，为网络设备的研发提供了一种新平台。目前，网络处理器已被成功应用于局域网、广域网的边缘/核心网、无线网络中，提供诸如路由、交换、服务质量(QoS)、安全监控、数据处理等各种网络应用服务。

IXP2400 是由 Intel 公司研发的第二代网络处理器，它采用 Intel 的因特网交换架构(IXA)，集成了 1 个通用的 XScale 核心处理器和 8 个独立可编程的 RISC 微引擎处理器，每个微引擎支持 8 个线程，其体系结构如图 1 所示。

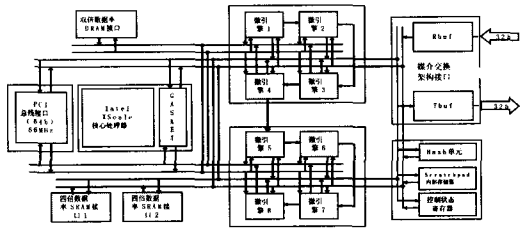

图 1　IXP2400 网络处理器体系结构

在软件设计中，XScale 核心处理器主要负责路由协议处理、系统管理和特殊 IP 分组处理等处理任务，适用于数据量小、处理复杂度较高的应用处理；微引擎处理器主要负责高速并行地接收、处理、转发网络数据包，适用于数据量大、处理复杂度低的快速网络数据处理业务。

IXP2400 采用了多级存储体系和多条独立的内部高速总线，从而提高了存储器访问和数据传输的效率。IXP2400 片内的 Scratchpad 存储器速度最快，主要用于实现数据存取、微引擎、线程之间同步机制；SRAM 采用四倍数据率的 SRAM 接口，主要用于快速存储查找表以及数据包头等常用的数据；SDRAM 采用双倍数据率的 DRAM 接口，主要用于大容量、高带宽的慢速数据的存储。

网络处理器的出现为高速网络处理设备开发提供了良好的硬件支持平台，能够解决性能和灵活性的统一问题。如何

*)基金项目：国家自然科学基金项目(60673161)，福建省科技计划重点项目(2007H0023)，福州大学科技发展基金资助项目(2005-XY-10)。
刘延华　讲师，主要研究方向为网络信息安全、计算智能；**陈国龙**　教授，博士生导师，主要研究方向为计算智能、计算机网络；**郭文忠**　讲师，主要研究方向为计算智能、计算机网络。

合理科学地分配和利用 IXP2400 中的处理单元和存储单元，是提高网络处理器运行效率所需要研究的重要内容。

3 IPSec 技术概述

IPSec(IP Security)是由 IETF 的 IPSec 工作组定义的一种开放源代码框架。它由认证头 AH(Authentication Header)协议、封装安全载荷 ESP(Encapsulating Security Payload)协议和密钥交换 IKE(Internet Key Exchange)3 个部分组成，提供数据源认证、数据完整性、重播保护、密钥管理以及数据机密性等安全服务，以此实现基于 IP 层的安全保护。IPSec 安全体系结构如图 2 所示。

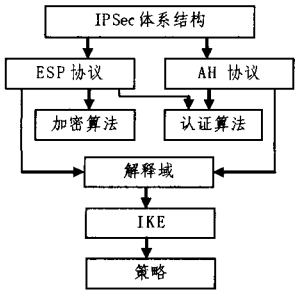

图 2 IPSec 安全体系结构

IPSec 有两种不同的工作模式：传输模式和隧道模式。传输模式用来保护上层协议，它规定在 IP 头与上层协议头之间需插入一个 IPSec 头；而隧道模式用来保护整个 IP 数据包，它将要保护的整个 IP 包封装到另一个 IP 数据包里，同时在外部与内部 IP 头之间插入一个 IPSec 头。

IPSec 主要使用两个协议来实现 IP 层的传输安全，即 AH 协议和 ESP 协议。AH 协议可为 IP 层提供无连接完整性、数据原始身份验证和一些可选的、有限的抗重播攻击服务。ESP 协议可为 IP 层提供机密性、数据源验证、抗重播、数据完整性以及有限的流量控制等安全服务。相比较，ESP 协议具有更高的安全性，但实现复杂性也较高。在实际应用中，为了达到更好的安全保护性能，通常使用 ESP 隧道模式。

4 基于 IXP2400 的 VPN 网关功能设计

4.1 系统功能模块结构图

本文采用基于隧道模式的 ESP 协议实现 IPSec VPN 网关系统，系统各功能模块及其关系如图 3 所示。

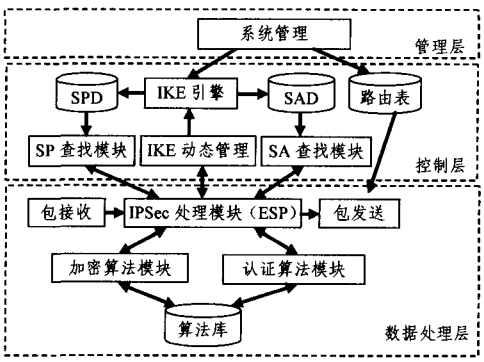

图 3 IPSec VPN 网关系统功能模块及其关系

从图 3 可看出，IPSec VPN 网关系统分为 3 个层次设计，这种设计结构适合采用网络处理器平台来实现。

1)管理层

该层功能模块由外接的普通计算机实现。主要实现的系统管理功能包括 SAD 管理、SPD 管理、路由管理、日志管理、数据统计等模块，实现 VPN 网关系统的日常维护功能。

2)控制层

该层功能主要在基于 Intel XScale 核实现，主要功能包括：

IKE 引擎：接收 IKE 手工管理和 IKE 动态管理两个模块产生的安全策略和安全联盟信息，处理转换后保存到 SPD 和 SAD 中，并通知 IPSec 处理模块安全策略已更新。

IKE 动态管理：该模块作为一个服务，运行在后台，根据 ISAKMP 协议，通过 UDP 500 端口与对方主机动态协商交换密钥，处理从 IPSec 处理模块发送来的密钥和安全策略请求。

SP 查找模块、SA 查找模块：它们分别接收来自 IPSec 处理模块的安全策略和安全联盟查询请求，负责从 SPD 和 SAD 中快速查找出相应信息，并将查询结果返回给 IPSec 处理模块。

3)数据处理层

VPN 网关系统中数据处理主要基于微引擎实现，通过多个微引擎，并行构成数据处理的快速通道。主要功能包括：

包接收、包发送模块：这两个功能模块分别负责数据包的流入和流出处理，主要包括包接收、路由处理、队列管理和包转发等功能，实现数据包的高速接收和转发。

认证算法模块：数据包处理中的安全模块的一个部分，用于数据包完整性检查、序列号检查和身份正确性验证，它是企业虚拟专网内部的安全通信保证。处理时，该模块根据 IPSec 处理模块指定的算法项从算法库中调用指定的认证算法，进行数据信息的有效认证。

加密算法模块：分布式的企业网络在进行内部互联时，数据包必须经过没有安全保障的互联网。为了保证内部数据的安全性，必须对数据进行加密。加密是根据双方第一次连接时约定的 SA(Security Association)。在处理时，该模块根据 IPSec 处理模块选定的加解密算法从算法库中调用指定加密算法，完成数据信息的加解密功能。

IPSec 处理模块：该模块为 VPN 系统的核心模块，包括输入数据处理和输出数据处理两部分，实现数据包进出 IPSec 网关的安全处理功能。为了保证处理速度和安全性能，本系统 IPSec 安全处理主要实现 ESP 隧道技术，不包括 AH 协议的实现。

4.2 IPSec 输入数据处理模块的设计

对于要进入 IPSec 网关的数据包，由 IPSec 输入数据处理模块负责从链路层接收，并放入 IP 接收队列，等待 ESP 安全处理。ESP 安全处理算法首先判断数据包目标 IP 地址是否为本机，如果目标地址为本机，则将数据包做重组处理后转到 ESP 隧道处理，否则将非本机数据包直接转到 IPSec 输出处理模块。IPSec 输入数据处理模块的具体处理流程如图 4 所示。

4.3 IPSec 输出数据处理模块的设计

对于输出 IPSec 网关的数据包，系统首先查询 SPD，检查是否需要对该报文进行 IPSec 处理。如果不需做安全处理，则直接将数据包转到包发送模块。如果需要做安全处理，则再查找是否存在有效的 SA。若无相应的 SA 存在，则激活 IKE 动态管理模块，同时丢弃当前数据包。查找 SA 成功后，根据 SA 进行 ESP 隧道安全处理，处理完毕后将数据包转到包发送模块。IPSec 输出数据处理模块的具体处理流程如图

5 所示。

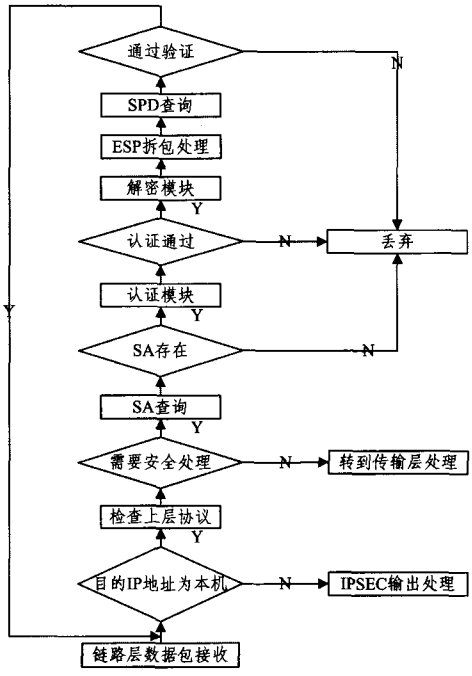

图 4　IPSec 输入处理流程图

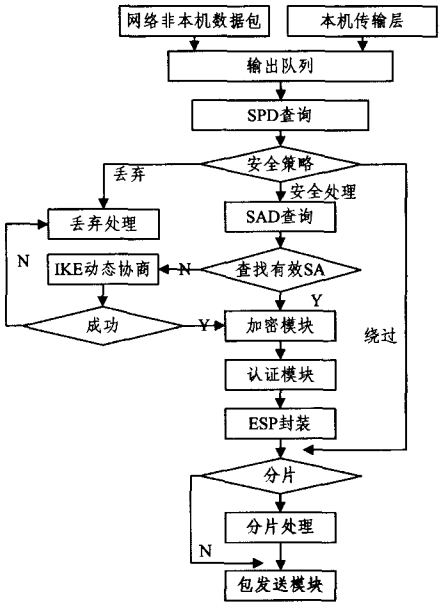

图 5　IPSec 输出处理流程图

5　系统的实现与分析

5.1　系统的实现

本 VPN 网关系统基于 ENP2611 板研发实现[1)]。Intel XScale 核心处理器运行 VxWorks 嵌入式操作系统，应用标准 C/C++语言来实现对控制层面各个功能模块的开发。在微引擎层面上，我们在 Windows 2000 操作系统环境下，应用 Intel 网络处理器集成开发环境 Developer WorkBench 4.1，以微 C 编码方式实现各个微引擎模块(微块)，编译后生成各个微块的可执行文档(扩展名为. UOF)。

5.2　微块的部署方案

微引擎的分配是否合理是影响整个系统性能的一个重要条件。通过对 IPSec 协议和 IXP2400 网络处理器的技术分析，我们经过多次实验与优化，采用了如表 1 所示的微块部署方案。

表 1　VPN 网关中微块的部署结构

序号	微块名称	微块功能	微引擎数目
1	包接收	接收链路层微包，并组装，保存到 SRAM 中，进入网络处理队列	1
2	IPSec 处理	执行安全处理判断，调用相关模块，负责 IPSec 中数据包的 ESP 隧道处理	2
3	加解密模块	调用选定的加解密算法，完成数据的加解密	2
4	认证模块	依据选定的认证算法，实现合法验证功能	2
5	包发送	负责待发送数据包的队列管理、调度，并转发到链路层	1

5.3　功能和性能的仿真分析

为了测试所完成的 VPN 网关系统，我们首先在 Developer WorkBench 所提供的模拟环境下进行了仿真实验。模拟数据流配置如表 2 所示。

表 2　仿真环境模拟数据流的配置

模拟设备	模拟端口	模拟类型	模拟输入数据包
0(SPHY Rx) 输入设备	0	出 VPN 子网的端口	10 个普通的数据包
	1	入 VPN 子网的端口	10 序列号重复的数据包
	2	普通转发端口	10 个普通的数据包
	3.	普通转发端口	10 个普通的数据包
1(CSIX Tx) 输出设备	0	输出端口	

仿真执行过程中，模拟器首先仿真了接收数据包的过程，然后仿真了转发数据包的过程，其实验结果如图 6 和图 7 所示。

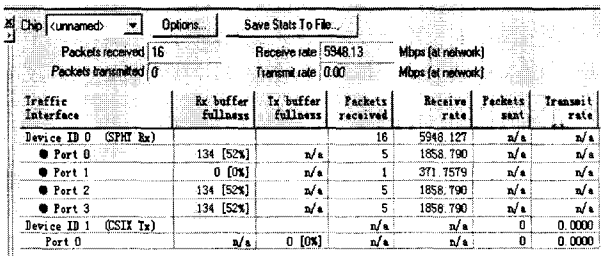

图 6　数据包接收过程

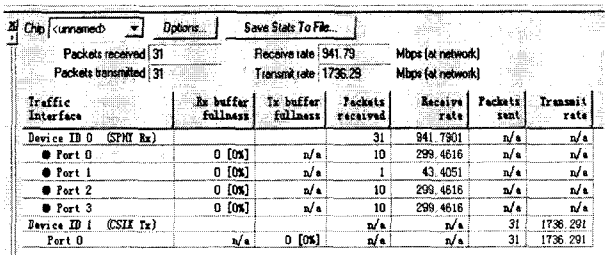

图 7　数据包输出(转发)过程

分析仿真实验结果，VPN 系统接收 31 个数据包，输出 31

(下转第 157 页)

1)　ENP2611 板内嵌一颗 Intel IXP2400 网络处理器芯片，以 PCI 接口形式与计算机连接。

了基于限制容差优势关系的不完备序值决策系统的粗集模型。限制容差优势关系在属性成百上千的情形下，两对象只要有一个属性值取值满足优势关系，同时在其余属性上取值无法比较时仍视为同类，这种条件仍然过于宽松，为解决该问题，在基于限制容差优势关系的不完备序值决策系统的粗集模型中，再引入集对分析方法。首先，通过设定相应的阈值将原不完备决策系统进行重划分；然后，使用基于联系度的限制相容优势关系确定类，并利用这些类获得相应的上下近似集；最后，笔者通过具体实例进行了验证。综上，本文工作都为从不完备序值决策系统中获取上下近似提供了新的理论方法和技术手段，其中通过阈值设定考虑了决策者的主观意愿，这与人机结合以人为本的系统方法论是一致的。

在本文的基础上，笔者下一步的研究方向是对基于限制容差优势关系的不完备序值决策系统中规则获取方法进行具体讨论与研究。

参 考 文 献

[1] Pawlak Z. Rough set[J]. International Journal of Computer and Information Sciences, 1982, 11(5): 341-356

[2] 王国胤. Rough 集理论在不完备信息系统中的扩充[J]. 计算机研究与发展, 2002, 39(10): 1238-1243

[3] Grzymala-Busse J W, Wang A Y. Modified algorithms LEM 1 and LEM2 for rule induction from data with missing attribute values // Proceeding of the Fifth International Workshop on Rough Sets and Soft Computing (RSSC'97) at the Third Joint Conference on Information Sciences (JCIS'97). Research TrianglePark, NC, March 1997: 69-72

[4] Grzymala-Busse J W. On the unknown attribute values in learning from examples // Proceeding of the 6th International Symposium on Methodologies for Intelligent Systems (ISMIS-91). Charlotte, North Carolina, October 1991. Lecture Notes in Artificial Intelligence, vol. 542. Berlin, Heidelberg, New York, Springer-Verlag, 1991: 368-377

[5] Kryszkiewicz M. Rough set approach to incomplete information systems[J]. Information Sciences, 1998, 112: 39-49

[6] Stefanowski J, Tsoukias A. Incomplete information tables and rough classification[J]. Computational Intelligence, 2001, 17: 545-566

[7] Pawlak Z. Rough set theory and its applications to data analysis [J]. Cybernetics and Systems, 1998, 29: 661-688

[8] Pawlak Z. Rough sets and intelligent data analysis [J]. Information Sciences, 2002, 147: 1-12

[9] Mavrotas G, Trifillis P. Multi-criteria decision analysis with minimum information: Combining DEA with MAVT[J]. Computers & Operations Research, 2006, 33(8): 2083-2098

[10] Pawlak Z, Slowinski R. Rough set approach to multi-attribute decision analysis [J]. European Journal of Operations Research, 1994, 7(2): 359-443

[11] Hewett R, Leuchner J. Knowledge discovery with second-order relations [J]. Knowledge and Information Systems, 2002, 4(4): 413-439

[12] Greco S, Matarazzo B, Slowiński R. Rough approximation by dominance relations. International Journal of Intelligent Systems, 2002, 17: 153-171

[13] Greco S, Matarazzo B, Slowiński R. Rough sets theory for multicriteria decision analysis. European Journal of Operational Research, 2002, 129: 1-47

[14] Shao Ming-wen, Zhang wen-xiu. Dominance relation and rules in an incomplete ordered information system [J]. International journal of intelligent systems, 2005, 20: 13-27

[15] Yang Xi-bei, Yang Jing-yu, Chen Wu, et al. Dominance-based rough set approach and knowledge reductions in incomplete ordered information system [J]. Information Sciences, 2008, 178 (4), 1219-1234

[16] 赵克勤. 集对分析及其初步应用[M]. 杭州：浙江科学出版社, 2000

[17] 黄兵，周献中. 不完备信息系统中基于联系度的粗集模型拓展[J]. 系统工程理论与实践, 2004, 24(1): 88-92

(上接第 108 页)

个数据包，转发率 100%，没有出现丢包，同时输入和输出的处理速率均大于 1.0Gbps。另外，由于本系统在 ESP 协议实现中加入防重放攻击策略，使得端口 1 的数据包仅有 1 个被接收，其余 9 个重复(序列号相同)的数据包则被丢弃，防重放功能成功实现。为了测试加解密功能，在模拟数据流制作时，我们特地将端口 1 数据包中的数据配置为端口 0 中数据包的加密值，即端口 1 的数据包解密后刚好等同于端口 0 的数据包，而端口 0 的数据包加密后刚好等同于端口 1 的数据包。通过分析系统的运行日志文件(.log)，系统成功实现了 ESP 协议中的加解密功能。

结束语 本文基于 IXP2400 网络处理器平台，设计并实现了一款千兆级 IPSec VPN 网关系统。通过仿真实验表明，本系统实现了 VPN 安全处理功能，且运行速率在 1.0GBPs，达到了千兆环境下的应用要求。由于 IXP2400 网络处理器的结构复杂性，所实现的 VPN 网关在 IPSEC 处理算法和微块划分等方面还有待进一步改进和优化。

参 考 文 献

[1] http://www.intelcom/design/network/products/npfamily/ixp2400.htm-Intel

[2] Kent S, Atkinson R. Security Architecture for the Internet Protocol. RFC2401 [EB/OL], http://www.ietf.org/html.charters/IPSec-charter.html, 1998

[3] http://www.intel com /design/network/ixa.htm-Intel

[4] 王彬. 基于 NP 的多功能网关研究与设计. 硕士论文. 福州大学, 2005

[5] 施恩，郑爱蓉，杨彬，等. 基于网络处理器的高性能 IPSec VPN 的设计方案. 计算机应用研究, 2005

[6] 石晶林，程胜，孙江明. 网络处理器原理、设计和应用. 清华大学出版社, 2003

[7] 高海英，薛元星，辛阳. VPN 技术. 机械工业出版社, 2004