第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·安全技术· 文章编号：1000—3428(2008)07—0173—03 文献标识码：A 中图分类号：TP309

核心路由器中安全机制的分布式设计与实现

胡宇翔，兰巨龙，程东年，王浩学
（国家数字交换系统工程技术研究中心，郑州 450002）

摘 要：分析下一代可信网络的需求，讨论现有的几种设计方案，借鉴策略管理和数据处理相分离的思想，提出一种集中式管理的基于专用加密芯片的高性能核心路由器中安全机制的设计方案。系统测试结果表明，该方案在保障高效转发性能的基础上能够提供高性能的安全防护，基本满足下一代骨干网中的实时加解密需要。

关键词：核心路由器；安全机制；IPSec 协议；加密芯片

Distributed Design and Realization of Security Mechanism in Core Router

HU Yu-xiang, LAN Ju-long, CHENG Dong-nian, WANG Hao-xue
(National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002)

【Abstract】 Rethinking the requirements of next generation trustworthy network, this paper uses the idea of separate policy management from data processing for reference, and puts forward a design of security mechanism based on specific chips with distributed implementation and centralized management for high-performance core router. System test proves the correctness and feasibility of this design. It provides security protection with high performance on the foundation of high reliability, and meets the basic requirements of real-time encryption/decryption in next generation backbone.

【Key words】 core router; security mechanism; IPSec; cipher chip

1 概述

TCP/IP 协议是目前最流行的网络互联协议，它是 Internet 进行网际互联的基础。IP 网络的开放体系结构以及灵活有效的多业务增值能力是 Internet 迅速发展壮大的一个重要原因，但也正是这种开放灵活性导致基于 IP 的网络缺乏内在的可信性。存储转发“尽力而为”的设计思想使得网络中间节点对数据包的来源不验证、不审计，导致地址假冒、垃圾信息泛滥，大量的入侵和攻击行为无法跟踪。

以上矛盾的出现，使得研究开始逐渐集中到下一代可信网络上，其应该具有如下特性：

(1)实现传统意义上的安全性，即系统和信息的保密性、完整性、可用性。

(2)真实性，即用户身份、信息来源、信息内容的真实性。

(3)可审计性，即网络实体发起的任何行为都可追踪到实体本身。

(4)私密性，即用户的隐私是受到保护的，某些应用是可匿名的。

(5)抗毁性，在系统故障、恶意攻击的环境中，能够提供有效的服务。

(6)可控性，是指对违反网络安全政策的行为具有控制能力。

2 网络层安全协议简介

结合以上需求，IETF 专门成立了网络层安全协议工作组，来制定和推动一套称为 IPSec(IP Security)的网络层安全协议标准。其目标就是把安全特色集成到 IP 层，以便对 Internet 的安全业务提供低层的支持。

IETF于 2005 年 12 月公布了IPSec的最新版RFC[1]，并定义了网络层使用的安全服务，它面向IP层以上的数据保护，主要有如下的安全目标：

(1)身份验证：能够确保发送该数据的实体与其所声称的身份一致。

(2)完整性：能够可靠地确定数据在从源到目的地传送的过程中没有被修改。

(3)机密性：确保数据只能为预期的接收者使用，而不能为其他任何实体使用或读出。

(4)对包重放攻击的防御。

(5)访问控制：能够实现用户级的高安全访问控制。

针对这些安全目标，IPSec 安全体系主要由 3 个子协议构成：AH 协议，ESP 协议，IKE 协议。其中 AH 协议和 ESP 协议是针对数据传输处理的，进行数据包的加解密和完整性验证。IKE 协议主要完成密钥的自动协商和管理。

IPSec 中一个很重要的概念就是安全关联(SA)。为了保护一条数据流，仅有密钥是不够的，需要有一整套的数据来描述(比如密钥、生命期、数据流标识、加解密算法、验证算法等等)，即安全关联。所有的 SA 都由安全关联数据库(SAD)统一管理。

基金项目：国家“863”计划基金资助重点项目(2005AA121210)
作者简介：胡宇翔(1982－)，男，硕士研究生，主研方向：计算机网络及安全；兰巨龙，教授、博士生导师；程东年，教授；王浩学，博士
收稿日期：2007-04-30 **E-mail：**huyuxiang1982@yahoo.com.cn

SA 一般是通过协商产生的，那么协商某个 SA 所需要的众多参数叫做安全策略(SP)。这些策略包括密钥协商的参数、算法、要保护的数据流等信息。众多的安全策略组成了安全策略数据库(SPD)。

IPSec 在网络层上对数据包进行安全处理，能够提供数据源验证、数据完整性、数据机密性、抗重放、访问控制等安全服务，使安全服务独立于各种应用程序，各种应用程序可以享用 IP 层提供的安全服务和密钥管理，而不必专门设计和实现自己的安全机制。同时，减少密钥协商的开销，也降低了产生安全漏洞的可能性。

3 高性能核心路由器中安全机制的设计

3.1 现有典型设计方案分析

IPSec 协议最典型的应用是在路由器中。通过在核心路由器上部署安全机制，可以在核心网上实现对通信双方真实身份的验证能力，能够对网上传输数据的完整性和隐私性保护，并且考虑到 IP 地址可软件配置等灵活性以及基于源 IP 地址的认证机制，可以有效防止网络业务流易被监听和捕获、IP 地址欺骗、信息泄露和原始信息被篡改等攻击。同时，IPSec 提供的安全服务共享程度高，实施 IPSec 可以最大程度地减少对周围设备的影响，减少人员培训和升级换代的费用。

高性能核心路由器作为下一代骨干网络中的关键设备，是整个网络安全的基础。在保证转发性能的前提下由核心路由器提供高性能的网络安全保护已经成为当前的研究热点。

路由器中部署安全机制有以下 4 种典型设计方案[2-4]：

(1)纯软件实现方案

采用纯软件 IPSec 加密算法和“ look-aside ”机制对 IPSec 报文进行处理。目前一些中、低端路由器较多采用这种实现方案。该方案的优点是：IPSec 的实现与网络层紧密集成在一起，更有利于诸如分段、PMTU 和套接字之类的网络服务的实现，并且有大量参考实现可供移植，灵活性强。缺点是：实际运行时，速度慢、开销大，无法适应高速路由器的性能需要。

(2)线缆中的块(BITW)实施结构

在这种实施方案中，IPSec 安全引擎被置于一个独立的设备(线卡)上，该设备直接连到路由器的物理接口。其优点是：独立的设备使得 IPSec 的实现可以和路由器其他部分分开，可以提高 IPSec 报文分组的处理速度。缺点是结构复杂，可扩展性差。

(3)FlowThrough 实现结构

NetOctave 公司的 FlowThrough 安全体系结构是一种高速的基于硬件的 IPSec 实现方式。它允许安全处理芯片直接连接到数据通路上，这样就消除了“ look aside ”实现方式的低效。FlowThrough 技术的优点是：速度快，结构简单。缺点是：整个系统的数据带宽受到 FlowThrough 芯片的限制，成为整个系统的瓶颈。

(4)基于网络处理器(NP)和 ASIC 的实现技术

NP 和 ASIC 是目前路由器硬件设计中应用日趋广泛的技术。ASIC 的使用虽然提高了效率，线卡上需采用更加高速、功能固定的 ASIC。这样做的优点是：效率高，实现简单，但是缺点也很明显：可编程能力差，扩展能力弱。

3.2 高性能核心路由器中安全机制的设计与实现

综合 3.1 节中路由器内部安全机制的 4 种部署方案，并综合考虑高性能安全路由器的自身结构、实现难度以及成本、系统性能等多种要素，本文提出一种基于专用加密芯片的高性能核心路由器中安全机制的分布式设计方案，并将此机制分为安全策略软件模块和安全模块，对网络层安全协议的几个基本构件进行分布式实现和集中式管理。

IPSec 安全策略软件采用软件方式在主控中实现，主要保障对 SAD、SPD 的配置及维护，IKE 也放在安全策略软件部分实现。考虑到线卡模块需对所有流经路由器的数据包进行策略查找处理，因此，在线路接口模块备份 SPD；转发模块需对数据包进行 SA 的查找，以判断数据包送往主控或者安全模块，因此在转发模块备份 SAD；同时考虑到需在安全模块备份加解密算法所需信息，设计方案采用在主控、线卡、转发和安全模块各子系统中分别存储 SPD 和 SAD，由 IPSec 安全策略软件集中管理这些数据库。IPSec 安全策略软件和线卡，转发、加解密模块之间采用内部千兆以太网相连，由 IPSec 安全策略软件生成 SPD 和 SAD 并下发给各个模块。

安全模块采用单板设计，由专用高速加密芯片实现对数据报文的 IPSec 处理。本文选用完全自主开发成功并拥有自主知识产权的开弦 SSXII-B-01(支持 3DES 算法)和开弦 SSXII-B-03(支持 RIJNDAEL 算法)两款芯片，该系列加密芯片集合了算法实现和 CPU 的功能，具有芯片操作系统(MISC Chip Operating System)逻辑硬件内核和安全策略内核设计，是一种智能化的多种密码体制加密算法 IP 核。包处理模块，密码算法模块全部放到安全模块单板中实现。在路由器中该安全模块通过光背板与光交换网路相连，实现数据平面的高速传输；通过内部以太网与主控子系统交互，实现控制平面中控制命令的交互。

综上所述，图 1 给出了安全机制采用分布式模块实现结构在高性能安全路由器中的位置。

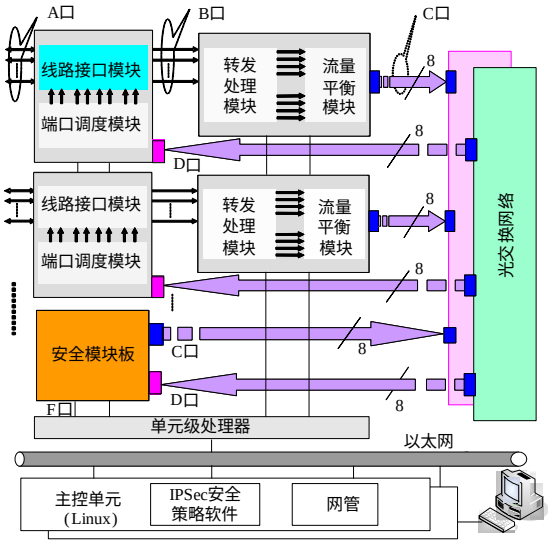

图 1 IPSec 在安全路由器中的实现方案

这种策略管理和数据处理相分离，SPD 和 SAD 分布式实现和集中式管理的思想是在安全路由器中实现高性能数据处理的必然途径，该结构优点如下：

(1)建立在现有体系结构基础上，延承了 IPv6 路由器数据路径与控制路径分离的设计思路，实现了 IPSec 封装/解封装高速处理与 SAD 维护、配置管理相分离。并且对原有系统的实现变动不大，减少了其他模块修改的工作量。

(2)模块分工建立在详细分析 IPSec 协议实现结构，并结合路由器原有体系的基础，合理分工，简化了实现。具体体

现在以下 2 点：

1)充分考虑 IKE 协议实现的复杂性和基于 Linux 平台的 IKE 协议实现程序的开源性，在主控 Linux 环境下实现 IKE 协议。

2)在转发模块实现 IPv6 包和 IPSec 包分离，安全模块只需专心于对安全性要求较高的报文的处理，从而提高了性能，并简化了模块的具体实现。

在该实现结构中，安全模块外部接口关系简单，只需与交换板、主控板 2 个外部接口进行数据交互。简洁的接口，减少了不必要的交互，从结构设计的层次上简化了实现的复杂度，保障了系统的性能。

4 系统性能分析

系统测试包括功能测试和性能测试。其中，为了保证系统功能的正确，在设计时引入了自检机制，定时进行系统状态检查，与标准的结果进行比较，保证了在系统出现异常时，进行系统复位，功能正确性的保证由此体现出来。下面主要讨论性能的测试，表 1 给出了 3DES 芯片 SSXII-B-01 与 SafeXcel-1842 加密芯片对比结果。

表 1 SSXII 与 SafeXcel-1842 性能参数对比表

比较项	SSXII-B-01	SafeXcel-1842
功能	支持 DES，3DES 加密算法，MD5 和 SHA-1 哈希算法	支持 DES，3DES，AES，ARC4 加密算法和 SHA-哈希算法
接口类型	RS232 接口和 PIO 接口	SPI-3 接口，PCI 接口
并行数据总线宽度/bit	64	64
最高并行接口工作频率/MHz	50	335
3DES 最高处理速度/(Gb·s^{-1})	3.41	2.6
MD5 最高处理速度/(Mb·s^{-1})	392	4
SHA-1 最高处理速度/(Mb·s^{-1})	392	6.4

由于安全模块只处理 IP 层的数据，因此在系统测试时需要 2 个 10 GbE 接口，用以完成物理层和链路层的处理。其中，一个接口连接路由器 R1，用以接收测试仪的数据报文，另一个接口则是将路由器 R2 的安全模块解密处理后的数据返回给测试仪进行分析。具体测试中，采由 AX4000 测试仪发送 IPv6 明文包。

测试中分别使用 3DES，128 bit 密钥；RIJNDAEL，128 bit 密钥；RIJNDAEL，192 bit 密钥 3 种情况分别测试不同包长在丢包率为 0 时的最高处理速度，结果如图 2、图 3 所示。

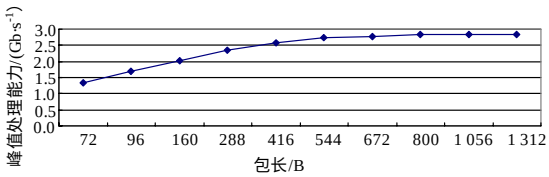

图 2 3DES算法，128 bit密钥，包长-峰值处理能力关系

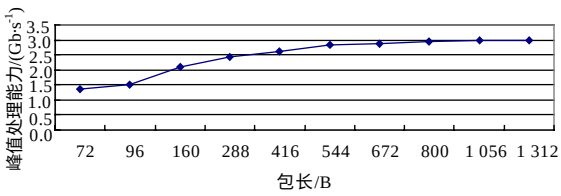

图 3 RIJNDAEL 算法，128 bit 密钥环境包长-峰值处理能力关系

测试数据表明：系统性能与不同环境下加密芯片处理速度相匹配，同时加解密芯片的处理能力仍是安全模块系统的性能瓶颈。根据亚太地区网络 APAN 进行的流量统计信息，统计意义上 IP 包的平均长度约为 508 B，根据图 3 和图 4，对平均包长而言，达到了需求中可支持 2.5 Gb/s 以上数据处理能力的要求。同时以上测试结果也验证了安全子系统设计与实现的正确性。

5 结束语

高性能核心路由器在传递网络信息时，不仅要保证高速，而且要保证其高安全性。而标准的 TCP/IP 协议并未涉及信息的加密传输，不能保证网络上信息的机密性和完整性，因此，数据保密性服务是基于 IP 的高性能核心路由器应支持的基本功能。同时，安全能力的提升与拥有自主知识产权的安全产品密不可分，只有核心技术的自主创新才可能有真正意义上的安全。结合加密芯片的特点以及高性能核心路由器的安全需要，本文通过引入并行流水结构和大容量表项存储、管理策略，设计并实现了安全模块，并通过了系统测试。高性能核心路由器中安全机制的引入，提升了核心路由器的安全处理能力，使其在军事、企业、机关等大型机构、专用网络中有了更为广泛的应用空间。

参考文献

[1] Kent S, Seo K. Security Architecture for the Internet Protocol[S]. RFC 4301, 2005-12.

[2] Hoffman P. Cryptographic Suites for IPsec[S]. RFC 4308, 2005-12.

[3] 徐 佳, 荆继武. 实现 IPSec 的一种方案[J]. 计算机工程, 2002, 28(1): 177-179.

[4] 刘 刚, 张德运. 基于 MPC8260 和 MPC 180 的安全路由器的设计与实现[J]. 计算机工程, 2005, 31(1): 119-121.

（上接第 172 页）

参考文献

[1] Dhir A, Durant G. 用FPGA实现安全处理[J]. 世界产品与技术, 2003, (6): 68-71.

[2] 钟雄光, 戎蒙恬, 陈 赟. 基于 FPGA 的 PCMCIA 加密网卡[J]. 计算机工程, 2005, 31(13): 179-180.

[3] 邵金祥, 陈利学. 基于状态机和流水线技术的 3DES加密算法及其FPGA设计[J]. 电子技术应用, 2005, (1): 69-71.

[4] 吴亚联, 段 斌. AES 密码计算构件的设计与应用[J]. 计算机工程, 2005, 31(21): 181-186.