文章编号:1001-2486(2003)02-0064-04

基于IPSec的下一代高性能安全处理器的体系结构*

张 怡, 孙志刚
(国防科技大学计算机学院, 湖南 长沙 410073)

摘 要:IPSec是目前适合所有Internet通信的惟一一种安全技术。通过分析IPSec的处理过程,指出网络安全处理器的使用是IPSec协议高效实现的关键,并详细介绍了目前典型安全处理器的结构和应用。由于目前的网络安全处理器无法满足OC-48及其以上速率接口的处理要求,对下一代高速网络安全处理器的体系结构进行了分析和预测。

关键词:IPSec;网络安全处理器;体系结构
中图分类号:TP393 文献标识码:A

Research on the Architecture of the Next Generation High-performance Network Security Processor Based on IPSec

ZHANG Yi, SUN Zhi-gang
(College of Computer, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: IPSec is the only security technology that can be used pervasively in the Internet. Through analyzing the process of IPSec, we point out that network security processor is the key component to implement IPSec protocol efficiently. The architecture and application of the security processor state-of-arts are introduced in detail. Because the processing power of the network security processor of the shelf can not satisfy the requirement of the ports with OC-48 speed or higher, the analysis and forecast of the next generation network security processor architecture is given at the end of the paper.

Key words: IPSec; network security processor; architecture

IPSec[1]是目前适合所有Internet通信的惟一一种安全技术。IPSec协议主要保证数据传输过程中的机密性、认证、数据完整性和有效性。由于IPSec隧道对其中通过的每个分组都加密,因此可保证VPN(Virtual Private Network)的安全性。在IPSec对IP报文进行保护之前,必须建立SA(Security Association),SA一般使用IKE(Internet Key Exchange)[2]动态建立。IKE使通信双方确定使用什么密钥对传输的数据进行加密和认证。IKE通常使用Diffie-Hellman和RSA算法,前者负责密钥的交换,后者负责鉴别通信双方的身份。由于Diffie-Hellman和RSA算法都需要大量的计算,因此IKE是IPSec中对计算量需求最大的部分。所幸的是,对持续数据流的加密而言,IKE交换发生的频率很低。

根据应用的不同需求,IPSec既可在主机上实现,也可能在某种安全网关(如路由器和防火墙)上实现。IPSec的实现会增加系统处理的开销,这种开销不但给系统带来额外的处理负担,而且还增加了系统设计和管理的复杂性。

为了提高系统对IPSec处理的性能,简化IPSec系统设计和实现的复杂性,Hifn、Broadcom等公司都推出了专门支持IPSec实现的安全处理器。这些处理器的特点是同时支持传输模式和通道模式下AH、ESP或AH+ESP协议的实现,支持AES(Advanced Encryption Standard)、DES、3DES和ARC4等加密算法,SHA和MD5等认证算法以及RSA、DSA、SSL、IKE和Diffie-Hellmann等公共密钥算法的硬件加速实现。

* 收稿日期:2002-09-18
基金项目:国家自然科学基金重大研究计划资助(90104001)
作者简介:张怡(1973—),女,助理研究员,博士。

1　典型的网络安全处理器及应用

Hifn 7854[3] 是 Hifn 公司最新推出的支持 OC-12 速率的安全加密芯片, 其结构如图 1 所示。安全压缩核以及公钥处理器是安全处理的主要功能部件。安全压缩核包括安全压缩处理引擎和动态协议处理单元(DPU)。安全压缩处理引擎包含流水的压缩、加密和认证单元; DPU 控制安全压缩引擎的处理并负责分析到达报文头以及控制输出报文的结构。公钥处理器内部包含随机数产生器, 用于硬件加速公钥或对称密钥的计算(密钥长度可达 2048 位)。

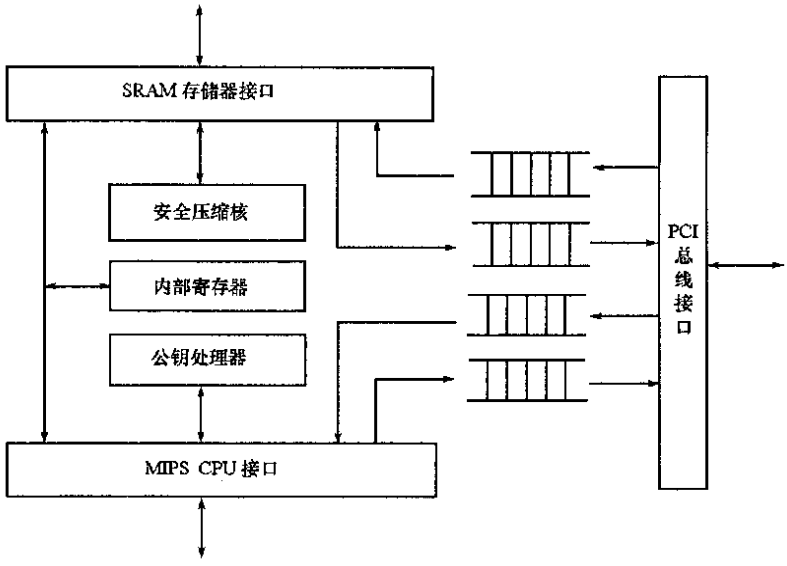

图 1　Hifn 7854 的基本结构

Fig. 1　Basic architecture of Hifn 7854

Hifn 7854 外接的 MIPS CPU 负责执行安全处理器的初始化、SA 的建立以及例外处理等功能, 与 IPSec 协议处理相关的各种数据结构存储在 SRAM 存储器中。关于 Hifn 7854 处理器的详细说明参见文献[3]。

Hifn 7854 处理器最大的优点是用硬件加速处理过程, 支持 OC-12 的端口速率, 因此可以满足网络主机对 IPSec 的处理要求; 同时, Hifn 处理器采用的 PCI 总线接口可以与目前大多数网络处理器(如 IBM 的 4GS3、Intel 的 IXP2000 等) 无缝结合, 在高速路由器[4] 的接口上实现通道模式的 IPSec。Hifn7854 的应用如图 2 所示。以安全处理器在主机上的应用为例(如图 2(a) 所示), 对接收到的 IPSec 报文的处理过程简要介绍如下:

(1) Host CPU 从网络接口接收到 IPSec 协议报文, 将其存放到系统内存中;

(2) Host CPU 根据 IPSec 头中的 SPI 域查找 SA, 若找不到, 丢弃该报文, 处理结束;

(3) 根据查找到的 SA, Host 在内存中生成报文处理的命令字, 并通知 Hifn 7854;

(4) Hifn 7854 通过 DMA 方式将该报文及处理命令字从系统内存拷贝到本地 SRAM 中排队;

(5) 安全压缩核读取报文的处理命令字, 并根据 SA 查找处理该报文控制信息, 包括使用的加密算法, 算法执行的上下文信息, DPU 开始执行的指令地址等;

(6) DPU 根据上述信息控制安全压缩处理引擎对报文进行处理, 并将处理后的报文和状态信息存到本地 SRAM 存储器中缓存;

(7) Hifn 7854 通过 DMA 方式将报文送回系统内存, 并通知 Host CPU;

(8) Host CPU 对报文进行其他处理(如送高层协议栈) 或继续转发该报文。

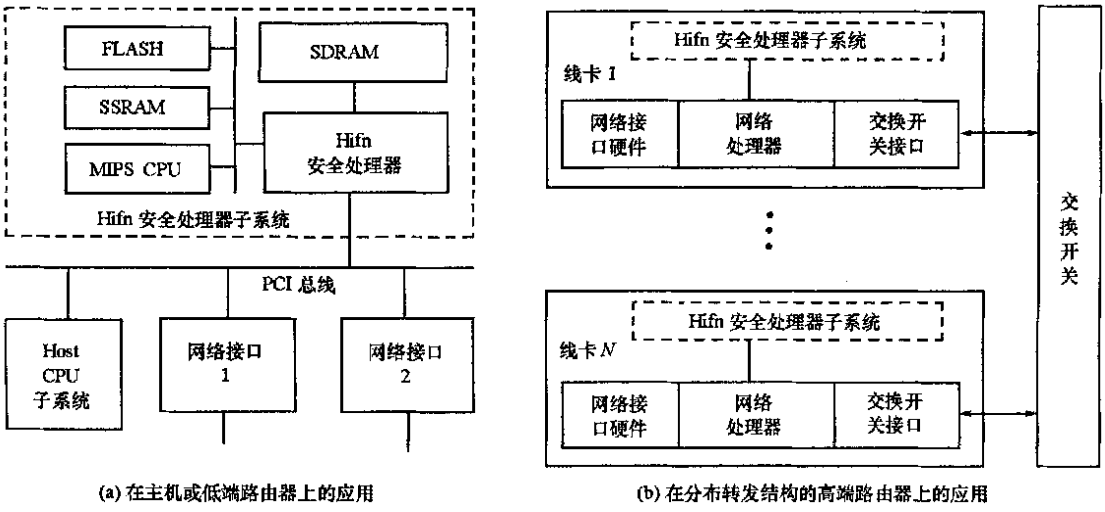

图 2 Hifn 安全处理器的应用

Fig. 2 Application of Hifn security processor

2 下一代高带宽网络安全处理器体系结构分析

下一代高带宽网络安全处理器是支持 OC-48 及其以上速率网络端口 IPSec 处理的安全处理器。这种处理器必须具有增强的数据加密计算能力和 I/O 能力。下一代高带宽网络安全处理器的实现必须依靠对现有体系结构的创新。

2.1 增强的数据加密计算能力

以 Hifn 7854 安全处理器芯片为例, 增加安全压缩核的工作频率或个数是提高数据加密处理能力的两条途径。在工艺水平不变的条件下, 增加安全压缩核的个数比提高频率更加可行。例如, 目前的网络处理器就普遍依靠增加内部处理单元的个数来提高处理性能。

然而安全处理器和网络处理器的处理模型并不一样。IPSec 的处理是面向一个会话(由相同 SPI 标识的报文流, 每个 IPSec 报文的处理过程必须检查其序列号并修改 SA), 而网络处理器的处理是面向单个报文。如果将属于一个 SPI 的两个报文分配到两个安全压缩核上并行处理, 必然会带来处理的错误, 因此必须将属于一个 IPSec 会话的报文分配到同一个安全压缩核上处理, 即同一个 SA 的数据只由一个安全压缩核读取和修改, 才能保证并行处理的正确性。

2.2 增强的数据 I/O 能力

除了加密计算能力以外, PCI 总线的带宽是影响安全处理器性能的另外一个主要因素。由于对于图2 中的应用, 安全处理器支持的端口速率最大只能到达 PCI 总线带宽的四分之一, 因此 PCI 总线(66MHz, 64 位) 将安全处理器性能约束在 1Gbps 左右, 下一代安全处理器的设计必须采用类似图 3(a) 所示的流接口(如 Utopia、Flex-bus 等)。使用流接口的另外一个优点就是可以在数据的接收和发送方向上各使用一个安全处理器来增加处理性能, 而对网络接口硬件和网络处理器透明。

2.3 安全处理器与网络处理器的集成与融合

我们认为, 下一代安全处理器发展的最终形式是与网络处理器融合, 即在同一个芯片内部同时实现网络处理器和安全处理器的功能。网络协议处理对 I/O 带宽要求较高, 不论是报文分类, 路由表查找还是调度, 都需要进行大量的查表(外部存储器访问) 操作; 而安全处理包含对大量数据的加密和解密, 对处理器的计算能力要求较高, 因此网络协议处理和安全协议处理对处理器资源的需求是互补的。

随着处理器内部多处理单元的使用, 不论是网络协议处理还是安全协议处理都需要首先对报文进行复杂的分类操作, 因此网络处理器和安全处理器实现的一些功能是重叠的, 两者融合将减少报文分类操作的次数。

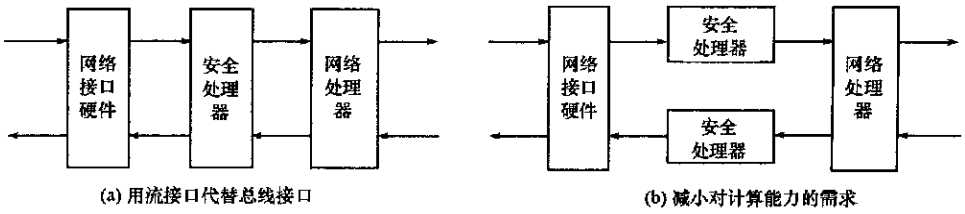

图 3　采用流接口的安全处理器的应用

Fig. 3　Application of security processor using stream interface

随着半导体工艺的进步, 单个芯片的集成度越来越高, 这使网络处理器和安全处理器的集成和融合成为可能, 加密和解密硬件加速器将以网络处理器内部的协处理器形式存在。

3　结束语

针对目前安全处理器性能无法满足安全路由器高速接口设计需要的特点, 分析了下一代高性能安全处理器的体系结构, 并指出与网络处理器的集成和融合将是高速安全处理器发展的最终形式。

参 考 文 献:

[1] Security Architecture for the Internet Protocol [S]. RFC2401.

[2] The Internet Key Exchange [S]. RFC2409.

[3] 7854 Network Security Processor Device Specification [R]. http://www.hifn.com.

[4] Craig Partridge, et al. A 50-Gbps IP Router [J]. IEEE/ACM Transaction on Networking, March 1998, 6(3).

(上接第 59 页)

参 考 文 献:

[1] 田永祥, 沈桐立, 葛孝贞, 等. 数值天气预报教程[M]. 北京: 气象出版社, 1995.

[2] PSU/NCAR Mesoscale Modeling System Tutorial Class Notes and User's Guide: MM5 Modeling System Version 3[R]. National Center for Atmospheric Research, January 2002.

[3] Michalaks J. A Runtime System Library for Parallel Finite Difference Models with Nesting[C]. Argonne National Laboratory Mathmatics and Computer Science Division, ANL/MCS TM-197, 1995.

[4] 金之雁, 王鼎兴. 一种有限差分格式负载平衡区域分解方法[C]. 数值预报与并行计算会议论文汇编, 2000: 150- 155.