Analyses of Crypto Module for Gbps VPN System

Jung-Tae Kim, Jong-Wook Han, *Member, KIMICS*

Abstract—A VPN is widely used in a communications environment which access is controlled to permit peer connections only within a defined community of interest. It is constructed through some form of partitioning of a common underlying communication medium, where this underlying communications medium provides services to the network on a non-exclusive basis. In this paper, we have analyzed a variety of architecture to implement Giga bps VPN system. The proposed architecture will satisfy the needs of clients who adopt Giga bps VPN system in the various environments.

Index Terms— Giga VPN, Crypto processor, IPSec.

I. INTRODUCTION

Many enterprises use an Internet as a medium of getting information from outside world. However, It is essential for an enterprise to use the VPN(Virtual Private Network) to communicate with headquarter, branches and cooperating company. A VPN is a group of two or more computer systems typically connected to a private network with limited public network access. It communicates securely over a public network. In other words, a secure extension of a business private network can exchange information across a public network. A VPN can exist between an individual machine and a private network or a more LAN and a private network. In recent years, the Internet established itself as a popular vehicle for the exchange of data, much of this brought on by the progressive confidence gained by the implementation of security mechanisms in support of financial transactions. However, the above technology has a disadvantage such as a complexity of managing network and a degradation of network performance. The performance of the VPN is affected with two factors. One is affected by the speed of the Internet or public backbone network. The other is affected by the speed of the packet processing at the peer VPN. The developed VPN equipment can be implemented with software. Even though the VPN equipment is implemented by hardware, there are a few high-speed VPN equipments in today. Although the 100Mbps network is generally used in currently, the Gbps network equipment will be used in the near future. But the VPN equipment cannot meet requirement of the speed for these network equipments. If the VPN equipment has a security function, the performance degradation is serious during the encryption and decryption operation. Therefore, It is required the high-speed VPN equipment which is implemented by hardware. The VPN equipment based hardware on can be fully guaranteed the bandwidth of the physical network and have a flexible structure in accordance with the change of the network circumstances. We have analyzed the VPN system to satisfy the above conditions.

Manuscript received September 6, 2003.

This work was supported by Electronics & Communication Research Institute.

Jung-Tae Kim is with the Mokwon University, Department of Electronics & Information Security (phone: 82-42-829-7657; fax: 82-42-829-7653; e-mail: jtkim3050@mokwon.ac.kr).

Jong-Wook Han is with the ETRI, Division of Information Security Technology(phone: 82-42-860-4940; fax: 82-42-860-5611; e-mail: hanjw@etri.re.kr

II. OVERVIEW OF VPN PROTOCOL

The Internet can be easily accessed and flexibly extended by anybody, anywhere and anytime. On the hand it becomes an advantage to flexible use of network, in other hand it has a disadvantage that unauthorized people can access a system through the Internet. The data security is important for the VPN that can be established the private network over the public network. To satisfy the data security in the VPN, it is required an encryption, a user authentication, access control and tunneling. The tunneling is an essential function of a VPN. The capsulated frame with routed information and additional information sends information to the end point of the tunnel through a public network. In order to send information into final destination system, the arriving capsulated frame is also decapsulated. The PPTP(Point to Point Tunneling Protocol), L2TP(Layer Two Tunneling Protocol), and IPSec is widely used in tunneling protocol at the VPN system. The PPTP including Windows Operating System is common used in tunneling protocol to test VPN system. The L2TP which is mixed the PPTP with the L2F(Layer Two Forwarding) protocol proposed by the Cisco Co. is an appropriate protocol for the private VPN system. The IPSec is an Internet standard protocol to protect the IP packet. Recently almost VPN products meet the interface of the IPSec protocol. The ICSA(International Computer Security Association) gives an authentication feature for the VPN products. The key technology in the VPN is an encryption since data sends through a public network such as an Internet or an ISP(Information Service Provider). The tunneling protocol cannot make a satisfaction of the security in the VPN. Therefore, the encryption protocol is necessary to fully satisfy the security of the VPN. The encryption protocol shields data disclosed from unauthorized people. The tunneling protocol hides the route information from unauthorized people. Therefore, both protocols have

an equal importance at the VPN. The DES and triple-DES are a common encryption protocol at the VPN equipment. The key management gives the encrypted authentication key to a user of the VPN. ISAKMP (Internet Security Association Key Management Protocol)/ IKE(Internet Key Exchange) protocol is suggested by the IPSec. Every VPN products satisfy the requirements of the PAP(Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). Tunneling mechanism is shown in Figure 1.

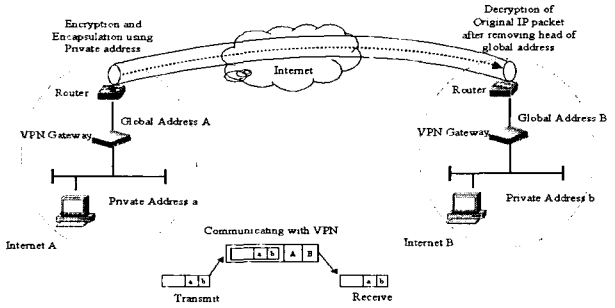

Fig. 1 Configuration of Tunneling Mechanism

Table. 1 Hiearchical VPN Protocol

Security Gateway	OSI Layer	Security Gateway
Application Proxy	Application Layer Presentation Layer	
Session Layer Proxy	Session Layer Transport Layer	Socks V5, SSL
Packet Filtering	Network Layer	ATMP, VTP, IPSec
	Data Link Layer	L2F, PPTP, L2TP
	Physical Layer	

III. IPSEC TECHNOLOGY

Two protocols such as AH(Authentication Header) and ESP(Encapsulation Security Payload) are secure service at the IPSec. The AH and ESP protocol are added into the IPV6(Internet Protocol Version 6) and IPV4 to provide security function. IP packet is divided into two parts that are header and payload. In order to apply security for the IP header, the AH header is added into the IP extended header. In order to apply security for the IP payload, the contents of user data are encapsulated as ESP protocol that is inserted into the IP header.

The AH protocol provides an access control, a connectionless integrity, a data origin authentication for IP datagram and anti-replay. Even though the server increments the sequence number as default, the anti-reply is not confirmed without checking the sequence number by the receiver side. The AH operates only a security for the immutable field of the IP header. The ESP header additionally serves as confidentiality for payload. All data including both TCP/UDP header and user data are encrypted in the tunnel mode of the ESP header. That is to say, entire packets captured by a user can be encrypted. Table 2 and Table 3 show the AH packet and ESP packet structure, respectively. Both the AH and the ESP are essential to encrypt packet and data which is implemented by the only inside security mechanism of the IP. The structure of the IPSec protocol is independent to other network protocol with modular property.

Table. 2 Configuration element of AH Packet

Security Protocol	Data Management Technology	Key Management Technology
• AH • ESP	• SPD • SAD	• IKE protocol

Table. 3 Configuration element of ESP Packet

Authentication Algorithm	Encryption Algorithm
• HMAC-MD5 • HMAC-SHA-1	• DES • Triple-DES, RC5, IDEA, Blowfish CAST-128

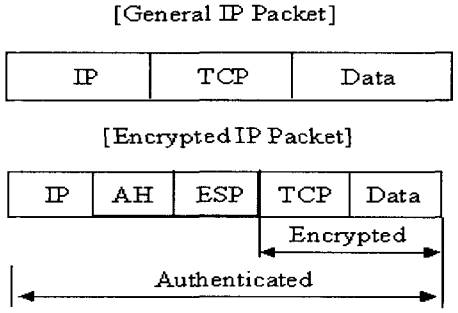

Fig. 2 General Packet and Encryption Packet Structure

IV. ANALYSES OF CRYPTO MODULE

It is essential crypto processor to operate high-speed encryption processing based on hardware technique in high-speed VPN system. We have analyzed the performance of crypto module published in today. Each crypto-module has a SSL, IPSec or both functions. For example, Nitrox II of Cavium company supports both SSL and IPSec function and has WEP protocol. Because most of resource is allocated in internal processing during each protocol, performance degrades when both functions are operated simultaneously. Contrary to other product, product of Corrent company supports only one function among both SSL and IPSec function. Performances of crypto-processor are mainly measured by three major point. Table 1, 2, and 3 show performance of a kind of processor[1].

1) Capability of processing of SSL RSA transactions per seconds
2) Capability of generation of IKE Main model tunnel
3) Capability of IPSec bulk encryption

Table 4. Comparison of performance for Gbps IPSec crypto-processor

	Hifn (Hifn 8154)	Cavium (Nitrox-II)	Broadcom (BCM5841)	Corrent (CR7120)	NetOctave (NSP4200)
IPSec Computation	2 Gbps	10 Gbps	4.8 Gbps	2.4 Gbps	10 Gbps
IKE Capability	1,500	10,000	-	2,300	-

Table 5. BCM5841 processor type and performance

Model	Performance
BCM5841-1	4.8 Gbps
BCM5841-2	2.4 Gbps
BCM5841-3	1.2 Gbps
BCM5841-4	0.6 Gbps

Table 6. Nitrox-II processor type and performance

Model	External I/O Interface	Performance
CN2130	1xSPI-3, PCI-X 64bit / 133MHz	3 Gbps
CN2240	2xSPI-3, PCI-X 64bit / 133MHz	6 Gbps
CN2340	1xSPI-3 & 1xSPI-4.2, PCI-X 64bit / 133MHz	6 Gbps
CN2450	1xSPI-4.2, PCI-X 64bit / 133MHz	10 Gbps
CN2560	2xSPI-4.2	10 Gbps

A. Type of Crypto-module

Each crypto-processors are classified by architecture and function operating in VPN system[2-5].

• Security Accelerator

This encryption processor implements the bulk encryption only in IPSec or Diffie-Hellman algorithm of IKE. The Encryption processor works only overhead time taken when host CPU or network processor operates encryption processing. Generally, security accelerators include bulk encryption module, public key exchange and authentication module and connect to host CPU through PCI, PCI-x bus or Hyper Transport or POSPHY Level3 interface. CPU transfers data and parameter to Encryption processor through bus to drive encryption processor. Encryption processor transfers the processing results through DMA to main memory and gives signal to host CPU.

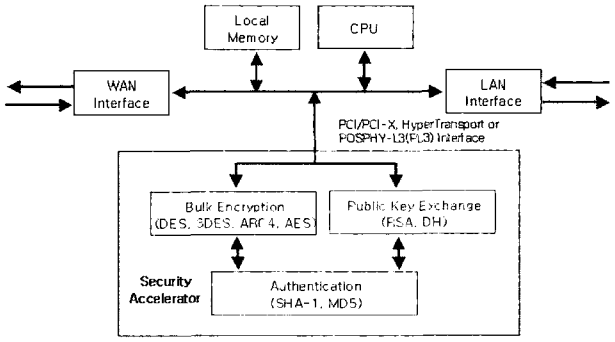

Fig. 3 Security Processor

• Security Co-processor

This processor treat with IPSec or SSL head processing including simple bulk Encryption function. Generally, It operates with network processor and is applicable to Look-Aside architecture. The main functions have PKI, authentication block, SSL and IPSec head processing function. Interfaces use PCI, PCI-X, HyperTransport or POSPHY-L3. The Encryption processors with function described above are BCM5820, BCM5821, BCM5840 and BCM5841 of Broadcom company, Nitrox+ series chips of Cavium and 8065, 8165, 8154, 8300, 8350 of Hifn company. Among the module, Nitrox+ chip of Cavium supports an allocation of bandwidth.

• In-line Security Processor

One part of interface transfers and receives a packet before encryption, the other part of interface transfers and receives a packet with encrypted packet and has a architecture with BITW(Bump In The Wire). As soon as the packet is encrypted , it transfers the next step through Ethernet MAC or SPI interface.

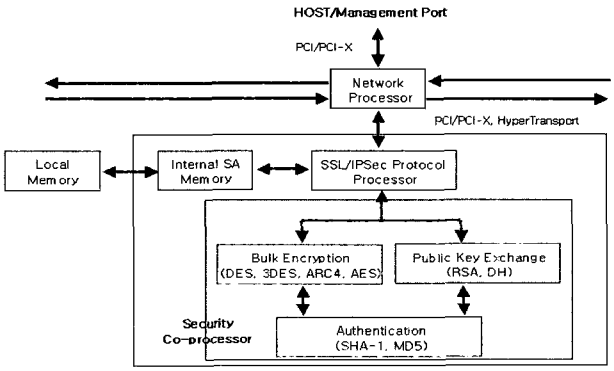

Fig. 4 Security Co-processor

• On-chip Security Engine

The encryption module such as IXP-2850 of Intel has a

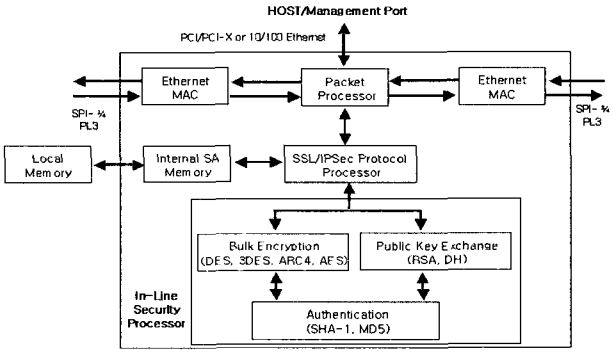

Fig. 5 In-line Security Processor

conventional packet engine and accelerated encryption engine. Because a bulk encryption engine is employed in network processor, this architecture is the best essential architecture type.

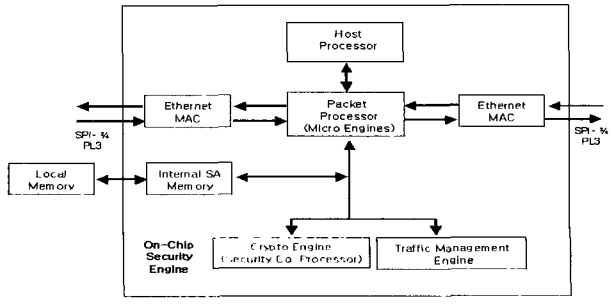

Fig. 6 On-Chip Security Engine

V. CONSIDERATIONS OF DESIGN FOR GBPS VPN SYSTEM

- Encryption Performance
  - Encryption algorithm type which can be supplied: 3DES, AES, RSA, MD-5, etc.
  - Encryption Speed: Performace of Bulk Encryption, the number of tunneling operated per second
  - Supplied protocol: IPSec, SSL, etc.
- Supplied Architecture
  - Usage of a Look-Aside and In-line architecture.
- Interface Connectivity
  - Connection of MAC or Framer: SPI-3, SPI-4.2, PL3, HyperTransport, etc.
  - Connection of Network processor and Host CPU: CSIX, PCI, PCI-X, etc.
  - External SA Memory access method and speed: SDRAM, RDRAM
- Flexibility
  - Easy to implement other encryption algorithm
    : Possibility of attaching SEED chip or applicable to new encryption algorithm
    : Performance upgrade using parallel architecture
- Authentication
  - FIPS 140-1, FIP 140-2

Table. 7 Comparisons of Architecture

Look-Aside Architecture	In-Line Architecture
•Generation of Bottle Neck In Bus-Interface (Limited to extensibility) •Easy to Implement	• Advantage to High Performance • Difficult to Implement

VI. CONCLUSION

We have analyzed the architecture to implement a Giga-speed VPN system. VPN system based on hardware is essential to realize Giga bps VPN system. To implement Giga-speed VPN, we have to consider the element of solution such as encryption function or interface. The crypto processor with high-speed is essential to realized encryption function, and it is easy to implement its function. Network processor employing encryption engine such as Intel IXP 2850 processor supports a variety of service. We need to study architecture to implement high-speed VPN system for future work.

REFERENCES

[1] Hac-Su Ju,, et al., "Trend of development for High-speed Encryption processor", VOL., 12, KIISC, 2002.
[2] Kye-sang Lee, "Trend of standard for IPSec," KISA, 2000. 8.
[3] http://www.hifn.com, "8154 HIPP II Security Processor"
[4] http://www.lighttreading.com
[5] http://www.intel.com

Jung-Tae Kim
Received his B.S. degree in Electronic Engineering from Yeungnam University in 1989 and M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 1991 and 1996, respectively. From 1991 to 1996, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 2002, he joined the department of Electronic and Information security Engineering, Mokwon University, Korea, where he is presently a professor. His research interest is in the area of Information security system technology that includes Network security system design, Chaos Cryptosystem and Wireless Communication.

Jong-Wook Han
Received the BS, MS, and Ph.D. degrees in the Dept. of electronic engineering from Kwangwoon University, Seoul, Korea, in 1985, 1991, and 2001. Since 1991, he has been with Information Security Technology Division in Electronics and Telecommunications Research Institute (ETRI). His research interests include VPN, network security, optical security, quantum cryptography.