An IPSec Accelerator for the High-performance Virtual Private Networks

Dae-Hyun Ryu, Jong-Whoa Na, Seung-Jung Shin, Seung-Ju Jang and Jung-Tae Kim , *Member, KIMICS*

Abstract—A cost efficient IPSec Accelerator board utilizing a crypto chip and an entry-level Linux PC for the high performance VPN is presented in this paper. The IPIP (IP-over-IP tunneling) processing, encryption & decryption processing, HASH processing, and the integrity test functions of IPSec are processed in the IPSec Accelerator board. The proposed IPSec Accelerator has demonstrated successful execution of the required functions of the IPSec packet processing and verified its performance by processing the IPSec packets at the rate of over 1 Gbps.

Index Terms—VPN, IPSec, Accelerator.

I. INTRODUCTION

The VPN (virtual private network) provides a temporary secure connection service over a public network. The IP-VPN is virtual private networks using the Internet as public network. In order to save growing telecommunication costs, companies recently started to replace expensive leased lines and dial-up remote access by IP-VPN solutions that are cheaper, because they only use a local link to the company's Internet service provider (ISP). A further advantage of IP-VPN solutions is the global reach of the Internet. Some IP-VPN solutions even claim to be more secure than the traditional telecommunication approaches.

As the demand for the high-performance network is increasing rapidly, the demand for the high-performance VPN is also increasing. The performance of the VPN depends on the two main factors: (1) The transmission speed of the public backbone network and (2) the efficiency of the IPSec processing at the both ends of the VPN [1]. The development of the high-performance VPN over 100 Mbps is known to be extremely difficult because of the IPSec processing requires very complex and time-consuming processes such as the IPIP (IP-over-IP tunneling) processing, encryption/decryption processing, HASH processing, and the integrity testing. In particular, in the case of a VPN utilizing the 3DES algorithm, the performance degradation reaches to an unacceptable level because the each packet must be encrypted and decrypted individually by software. Therefore, various research groups proposed various architecture of hardware VPN for the high performance VPN system. However, the hardware VPN researches are focused only on the encryption acceleration only [2,3]. Software-based VPN is only useful when the network connection is slow [4,5].

In this paper, we propose a novel IPSec Accelerator hardware for a high performance VPN. Our approach differs from others in that every required operations of the VPN are processed at the hardware level. It should be noted that the IPIP processing also demand a considerable computational overhead to the system. Therefore, by the use of the IPSec Accelerator, a high-performance VPN can be realized in various network environments to satisfy various kinds of security requirements.

In the following section, the overview of IPSec and the architecture of the IPSec Accelerator are discussed. Then, the organization and the operation of the proposed accelerator are presented in chapter 3. Finally, the functions of the proposed accelerator are demonstrated and the performance of the accelerator is evaluated.

II. THE OVERVIEW OF THE IPSEC ACCELERATOR

2.1. The overview of IPSec

IPSec is a standards track proposal in the Internet Engineering Task Force (IETF) for IP security. IPSec provides encryption/decryption, authentication and key management functions. There are three major functionality in IPSec; First is the authentication process via an Authentication Header (AH), second is the encryption process using an Encapsulating Security Payload (ESP) and finally automated key management through the Internet Key Exchange (IKE) [6,7]. The following table 2 and 3 illustrates the components of IPSec and the security algorithm. The IPSec protocol introduced two main components, Authentication Header (AH) and IP Encapsulation Security Payload (ESP). The AH provides data origin authentication, connectionless integrity, and anti-replay protection services, but confidentiality for IP datagram. AH provides security services through access control, connectionless integrity, data origin authentication, and anti-replay service. In the case of the anti-replay service, the sender assigns a unique sequence number for each packet. Optionally, if the receiver wants to use the

Manuscript received January 9, 2003.

Dae-Hyun Ryu is with Hansei University (phone: 031-450-5228; fax: 031-450-5172; e-mail: dhryu@ hansei.ac.kr).

Jong-Whoa Na is with Hansei University (phone: 031-450-5158; fax: 031-450-5172; e-mail: jwna@ hansei.ac.kr).

Seung-Jung Shin is with Hansei University (phone: 031-450-5274; fax: 031-450-5172; e-mail: expersin@ hansei.ac.kr).

Sung-Ju Jang is with Dongeui University (phone: 51-890-1710 fax: 51-890-1619 e-mail: sjjang@dongeui.ac.kr).

Jung-Tae Kim is with Mokwon University (phone: 82-42-829-7657; fax: 82-42-829-7653; e-mail: jtkim3050@mokwon.ac.kr).

anti-replay service, it can test the sequence number for the validity. The AH protects only the immutable field of the IP header. Thus, for the fields manipulated by the network equipments,

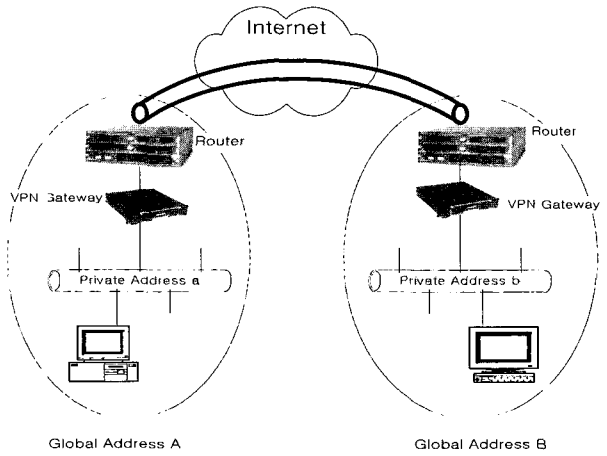

Fig. 1 The overview of the tunneling technology

Table 1 The components of the IPSec.

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

Table 2 Various Algorithms used in the IPSec.

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

the value '0' is assigned and the integrity is tested later using Integrity Check Value (ICV). In addition to the security services provided by the AH, the Encapsulation Security Payload (ESP) header provides confidentiality service. In the transport mode, TCP/UDP header and entire user data are encrypted. In the tunnel mode, the entire packet generated from the user is encrypted. The AH and ESP of IPSec is independent from the security and authentication algorithm used internally and do not need any additional security mechanism. In this way, IPSec provides modularity and computability between Internet users. The following figure contrasts the frame format of IP packet and IPSec packet. Performance of IPSec depends on the implementation details. Thus, the designer must consider the types of Operating System, the performance of the random number generator, the efficiency of the system management protocols, etc. Although these factors are not list in the standard, they are very important in the implementation of IPSec.

2.2. IPSec Accelerator

The VPN gateway includes the Internet Key Exchange (IKE) function and the IPSec function. The IKE function creates a Security Association (SA) between the two VPN and the IPSec function executes the inbound processing and the outbound processing. The functions for the IPSec packet processing are composed of the IPIP

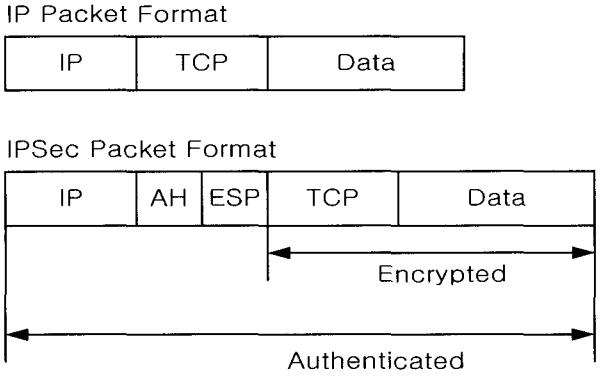

Fig. 2 IP packet and IPSec packet frame format

Table 3 The AH packet format

Next header	Payload length	Reserved
Security Parameters index (SPI)		
Sequence Number		
Authentication Data (MD5, SHA-1) (Variable length of 32 bit words)		

Table 4 The ESP packet format

Security parameters index(SPI)	
Sequence Number	
Payload Data (Variable length of 32 bit words)	
Padding (0 ~ 255 bytes)	
Pad length	Next header
Authentication Data (Variable length)	

processing, encryption and decryption processing, HASH calculation, and the Integrity testing. In general VPN system, these functions are implemented in software so that the VPN suffers from the slow execution speed. To overcome this speed problem, the IPSec Accelerator using the Crypto chip is developed. The Figure 1 illustrates the operation of the traditional VPN implemented with software, while the Figure 2 illustrates the proposed VPN utilizing the hardware accelerator.

The IPSec Accelerator uses the NITROX chip from the Cavium as the IPSec core chip [8]. The chip provides the IPSec packet processing functions such as the IPIP processing, encryption/decryption processing, HASH processing, and the Integrity testing. The Figure 3 illustrates the internal block diagram of the IPSec Accelerator.

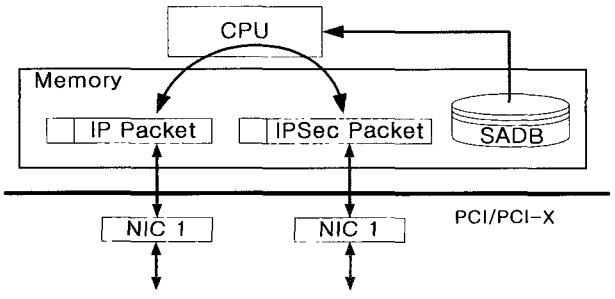

Fig. 3 Block diagram of the Software-based VPN.

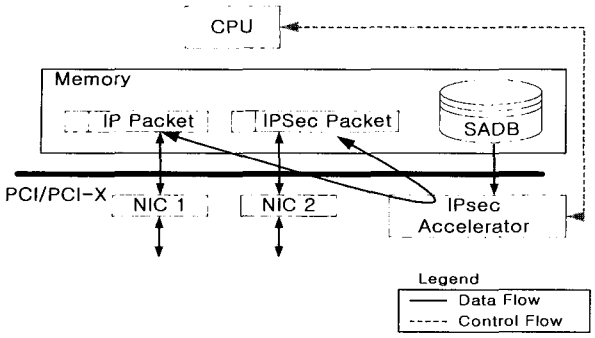

Fig. 4 Block diagram of the Hardware-based VPN.

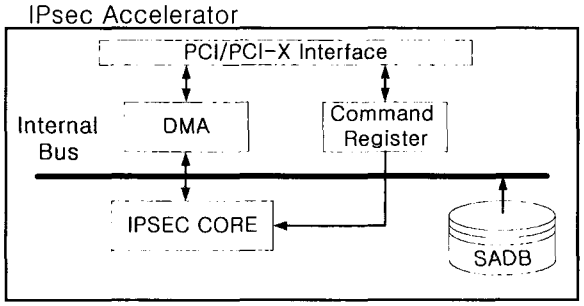

Fig. 5 Block diagram of the IPSec Accelerator

As shown in the above figure, the PCI/PCI-X interface connects the hosts with the IPSec Accelerator board. We used an entry-level Pentium4 PC configured with Hancom Linux 2.0 as a VPN host. The DMA block transfers data between the memory of the host and the VPN. When the host requests for the IPSec function to the PPA, the host initializes the Command Registers with the number of packets to be processed and the number of commands. Then the IPSec Core can performs its processing. The Internal Bus is a 64-bit data bus in the packet-processing accelerator. IPSec Core performs the IPSec functions.

Security Association Data Base (SADB) is the memory within the packet-processing accelerator, stores the SA. When the IPSec Core wants to process the packet from the Host memory, the necessary information such as Key and IV from the SADB. The specifications of the proposed IPSec Accelerator are summarized in the table 1.

Table 5 The Specifications of the IPSec Accelerator.

Name	Specification
PCI Interface	PCI/PCI-X (64bit, 64MHz/100MHz/ 133MHz, Master & Target Modes)
Algorithm	RSA and Diffie-Hellman (groups 1,2,5) DES/3DES, AES, ARC4 MD5, SHA-1
Number of SAs	2,000,000 IPSec SAs with 512MB Local Memory

III. THE OPERATION OF IPSEC ACCELERATOR

The IPSec Accelerator supports the PCI/PCI-X interface to communicate with the CPU of the Host at the rate of 1 Gbps or more. Also, the DMA can read the input packets and the commands from the host memory and write the output packet to the host memory. Figure 4 describes the detailed illustration of the operations of the IP sec. The steps executed in the packet-processing operations are list in the table 2.

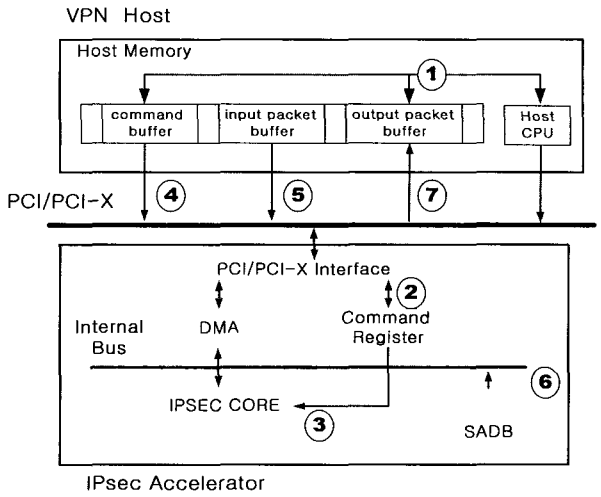

Fig. 6 The operation of the IPSec Accelerator

Table 6 Detailed explanation of the sequences in Figure 6

Sequence	Operations to be executed
1	If there are input packets for the IPSec processing, the host generates the commands and prepares the memory space for the output packets. The commands include processing method (i.e. inbound processing or outbound processing), the memory address of the input packets and output packets, the SA address of the SADB.
2	The host CPU initializes the command registers of the Packet-Processing Accelerator with the address of the command and the number of the command.
3	When the number of commands is stored at the command register, the Crypto chip starts the IPSec processing.
4	IPSec Core reads the command from the command buffer to determine the processing method, the address of the input/output packet, and the address of the SA.
5	Accelerator reads the input packets from the memory.
6	Accelerator reads the SA-related information from the memory.
7	Process the input packets using the SA information and the processing method. The output packets are stored at the output packet buffer.

IV. PERFORMANCE EVALUATION OF THE IPSEC ACCERELATOR

The function of the IPSec packet processing of the IPSec Accelerator is verified and the performance of the IPSec packet processing of the accelerator is evaluated. The test items for the packet-processing accelerator are listed in the Table 7. For the purpose of the function test and the system performance evaluation, we wrote an additional test program as shown in the Figure 7. First,

the test program performs outbound processing with the packets of various sizes and reports the result of the evaluation. Then it performs inbound processing with packets of various sizes and reports the results. To perform the outbound processing, the test program specifies the number of packet and the length of the packet to the device driver. The device driver allocates memory for the input buffer, the command buffer, and the two output buffers. Next, the test program creates the test packets and stores them at the input buffer. Also, it creates commands for the outbound processing and stores the results at the output buffer 1. When these are ready, the host CPU initiates the outbound processing and records the waiting time until the last packet is finished. The recorded waiting time is used to calculate the performance of the outbound processing as follows:

Performance of the outbound process
= (The length of the input packet × the number of input packet) ÷ waiting time

Using the similar method, the performance of the inbound packet processing can be calculated. The commands for the inbound process are created and the packets in the output buffer 1 are used as inputs to the inbound process. When these are ready, the host can start the inbound process and the results are saved at the output buffer 2. Now, if the IP packet of the output buffer 1 and the IP packet of the output buffer 2 are the same, this implies that the encryption and decryption process are executed correctly. The measurement results of the performance parameters using the test program are listed in the Table 8. The performance of the inbound process can be calculated as follows:

Performance of the inbound process
= (The length of the output buffer 1 × the number of output packet) ÷ waiting time

Table 7 The results of the function tests.

Measurement Condition	Length of a packet (Bytes)		The number of packets (Bytes)	
	IP	IPSec	IP	IPSec
ESP Tunnel Mode 3DES-MD5-96	64	120	64KBytes	120K
			960KBytes	1.8M
			9.6MBytes	18M
	1400	1456	1400KBytes	1456K
			21MBytes	22M
			210MBytes	220M

Table 8 The results of the performance tests

Measurement Condition	Length of a packet (BYTES)		Decryption PERFORMANCE	
	IP	IPSec	Wait time (MS)	Processing speed (MBPS)
ESP Tunnel Mode 3DES-MD5-96	64	120	1.14	842
			16.2	890
			162.3	890
	1400	1456	7.1	1640
			105	1680
			1050	1680

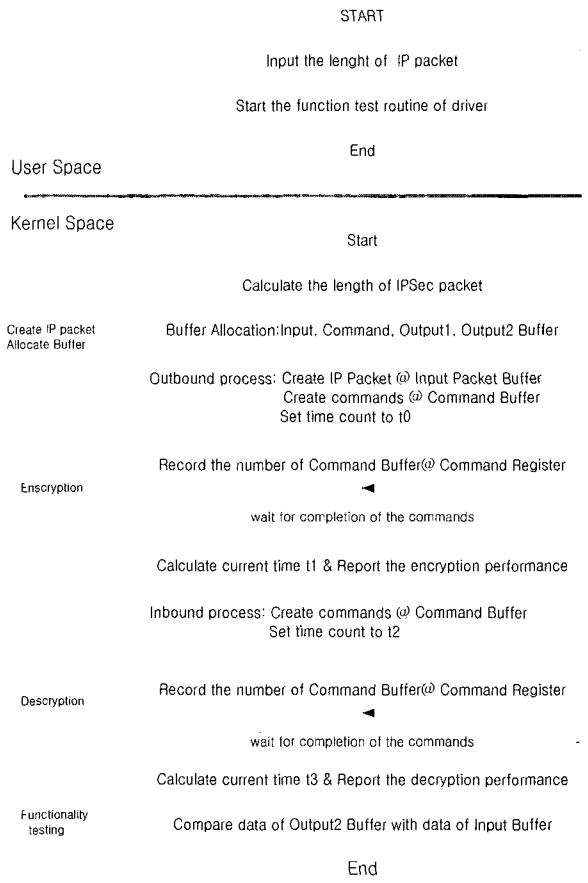

Fig. 7 The flowchart of the test program

V. CONCLUSION

A cost efficient and high performance VPN system using a hardware IPSec accelerator board and an entry-level Linux PC is proposed. The prototype is implemented and the performance is evaluated. The proposed accelerator successfully executed the required functions of the IPSec packet processing such as the IPIP (IP-over-IP tunneling) processing, encryption/decryption processing, HASH processing. The proposed IPSec Accelerator based VPN demonstrated the Gigabit VPN system could be realized.

REFERENCES

[1] T. Braun, M. Kasumi, et al., "Virtual Private Network Architecture", IAM-99-01, April 1999.
[2] J. W. Yoon, Y. K. Kim, D. H. Ryu, "On a Implementation of High-Speed VPN Gateway with Parallel Architecture", WISC2001, Sept. 2001.
[3] J. T. Kim, D. H. Ryu, H. K. Moon, "A Study on the VPN Gateway Architecture for Speed Acceleration", pp.101 - 107, Journal of KICS, Vol. 27, No. 8T, Aug. 2002.

[4] C. J. C. Pena, J. Evans, "Performance evaluation of software Virtual Private Networks", 25th Annual IEEE Conference on Local Computer Networks (LCN'00), pp. 522-523, Nov. 2000.
[5] J.P. McGregor, R.B. Lee, "Performance impact of data compression on virtual private network transactions", 25th Annual IEEE Conference on Local Computer Networks (LCN'00), pp.501-510, Nov. 2000.
[6] St. Kent, R. Atkinson: *Security Architecture for the Internet Protocol;* RFC 2401, Nov. 1998.
[7] Implementing Virtual Private Networks, Steven Brown, McGraw-Hill, 1999.
[8] http://www.cavium.com/products.html

Dae-Hyun Ryu
Received his B.S. degree, M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Busan National University in 1983, 1985 and 1997, respectively. From 1987 to 1998, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 1998, he joined the department of IT, Hansei University, Korea. His research interest is in the area of Digital image processing, Digital watermark and Information security system design.

Jong-Whoa Na
Received his B.S. degree in Electronic Engineering from Sogang University in 1985, M.S. degree in Computer Engineering from the Wayne State University, Detroit, MI., U.S.A. in 1988, and Ph.D. degree in Computer Engineering from the University of Arizona, AZ., U.S.A. in 1994. Currently, he is an assistant professor in computer engineering department. His research interests include optical computing, ubiquitous computing, and context-aware computing systems.

Seung-Jung Shin
Received his B.S. degree in Management from Hansung University in 1984 and M.S. degrees in Marketing from the Sejung University in 1988 and M.S. degrees in Electronic Engineering from the Kunkuk University in 1994 and Ph.D. degrees in Management Information Security from the Kukmin University in 1999, respectively. From 1990 to 1994, he joined at Teasung MIS, where he worked as Technical Director. From 1995 to 2003, he joined the department of Electronic and Information security Management, Joongbu University, Korea, In 2003, he joined the department of Information Technology, Hansei University, Korea, where he is presently a professor. His research interest is in the area of Network communication technology that includes Information Message security system design, Mobile system and Wireless Communication.

Seung-Ju Jang
Received a B.Sc. degree in Computer Science and Statistics, and M.Sc. degree, and his Ph.D. in Computer Engineering, all from Busan National University, in 1985, 1991, and 1996, respectively. He is a member of IEEE and ACM. He has been an associate Professor in the Department of Computer Engineering at Dongeui University since 1996. He was a member of ETRI(Electronic and Telecommunication Research Institute) in Daejon, Korea, from 1987 to 1996, and developed the National Administration Multiprocessor Minicomputer during those years. His current research interests include fault-tolerant computing systems, distributed systems in the UNIX Operating Systems, multimedia operating systems, security system, and parallel algorithms.

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 technology that includes Information security system design, Network security and crypto-processor design.