Analyses of Architecture based on Hardware for High-speed VPN System

Jung-Tae Kim*

* Dept of Electronic & Information Security Engineering, Mokwon University, Taejon, 302-729, Korea
Tel: +82-42-829-7657 Fax: +82-42-823-8506 E-mail: jtkim3050@mokwon.ac.kr

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.

1. 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 [1,2].

2. 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 with the L2F (Layer Two Forwarding) protocol proposed by the Cisco company 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) protocols are suggested by the IPSec. Every VPN products satisfy the requirements of the PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). Tunneling mechanism as shown in fig 1 [3].

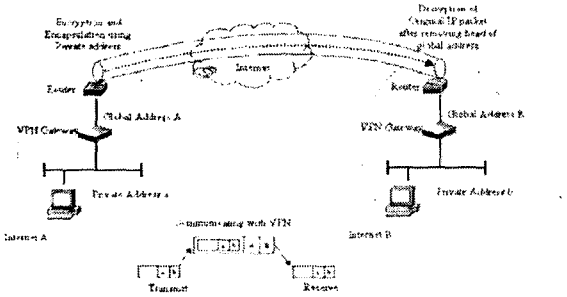

Fig. 1. Configuration of Tunneling Mechanism

3. ANALYSES OF CRYPTO MODULE

3.1 Security processor

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.

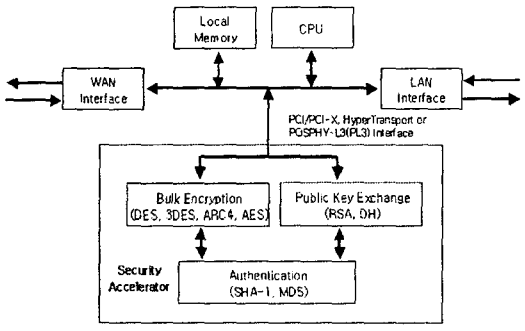

Fig. 2. Security Processor

3.2 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 [5, 10].

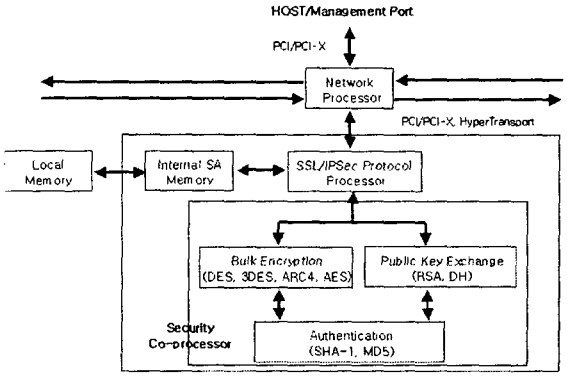

Fig. 3. Security Co-processor

3.3 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.

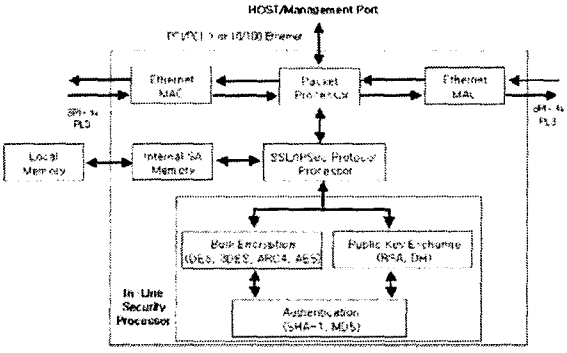

Fig. 4. In-line Security Processor

3.4 On-chip Security Engine

The encryption module such as IXP-2850 of Intel has a traditional packet engine and accelerated encryption engine. Because a bulk encryption engine is employed in network processor, this architecture is the best essential architecture type.

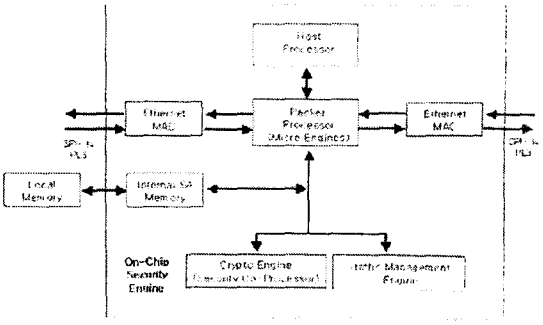

Fig. 5. On-Chip Security Engine

4. DESIGN OF THE VPN GATEWAY

The bus architecture to support wide bandwidth, the crypto-accelerator and optimized IPSec in kernel level are significant.

4.1 VPN Gateway Architecture

The figure 6 shows the entire structure of the VPN system. The IPSECPU with IPSec protocol and the IKE engine exchanges and negotiates a key. There are two DB in the VPN gateway. One is the SPD (Security Policy Database), which includes a source address, a destination address and a port number to keep security policy. The other is the SAD (Security Association DB), which keeps various algorithms for the partner VPN equipment and key lifetime. The SALU and the SPLU unit take a role in connecting between the SAD and the SPD in terms of incoming and outgoing packets. The VPN controller controls the SAD and SPD unit. The AG (Audit Generator) can remain a system log section for keeping an important event of the IPSEC/IKE and send a system log to the VPN manager. The data flow sequence of the VPN gateway is as follows: The VPN gateway queries the SPDB of the security policy by analyzing current packet header. If current packet is not an IPSec, the VPN gateway serves general routing without accessing the SPDB. But there are two cases for a general routing. One is that the IPSec encrypts data and performs hash operation if the SADB includes the SA for a current packet. If there is no SA for a current packet, the SALU activates the IKE engine to negotiate the SA and through both the IKE engine and peer [8,9].

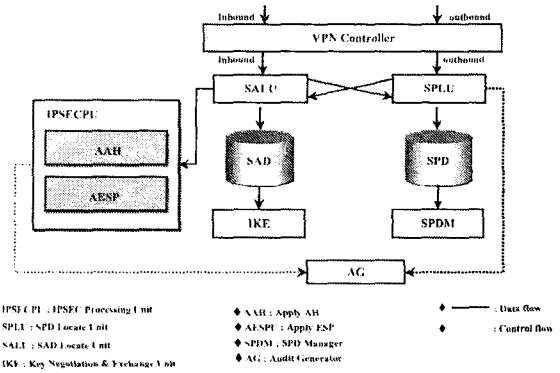

Fig. 6. VPN Gateway Architecture

4.2 Hardware Architecture of the VPN Gateway

Figure 7 shows the hardware architecture for the VPN gateway. The parts of degradation of performance for the VPN gateway are clear in terms of both bottleneck of the network traffic and a variety of encryption and hash algorithm. Therefore, to solve these two problems, we should improve the VPN gateway system [4,7]

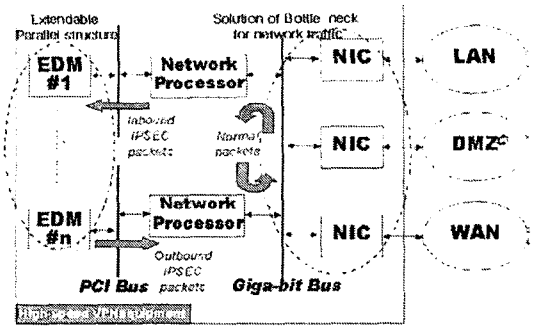

Fig. 7. Hardware Architecture for the Proposed VPN

The network processors with Gigabit IO bus and PCI bus become an import factor to solve a bottleneck of the VPN system. The extensible crypto-accelerator can be mounted onto the VPN gateway to reduce overhead of the encryption and hash algorithm. In addition, each crypto-accelerator can be used as independent PCI bus to reduce a bottleneck of traffic at the PCI bus [6].

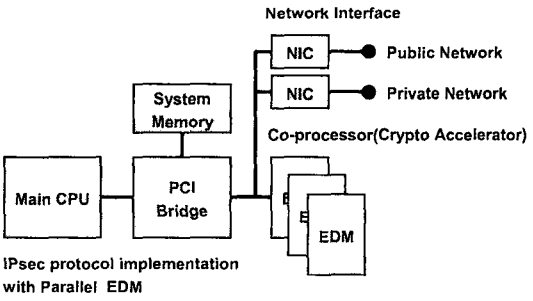

Fig. 8. Outline of the Hardware Architecture for the Proposed VPN

4.3 The Crypto-Accelerator

The crypto-accelerator module can be used as maximum three units such as PCI (Peripheral Component Interconnect) device. Figure 9 shows the crypto-accelerator architecture, which is related with the host CPU. The IPSec engine in the host puts a new packet into the PCI main memory and commands encryption/decryption/hash operation. The security parameters that can be used in a key or an algorithm will be given by searching the SADB. The queue for managing the encryption/decryption command handles

FIFO sequences. A real packet moves as soon as possible into the PCI shared memory through the DMA of the packet memory for the crypto-accelerator. The frequently used security parameter will be cached upon the SA memory to speed-up the system performance. The crypto-accelerator has a following features.:

- 640 Mbps Single DES, 214 Mbps Triple DES
- Diffie-Hellman Negotiate: < 29 ms (1024-Bit Modulus, 180-Bit Exponent)
- RSA 1024-Bit Sign: < 29 ms; RSA 1024-Bit Verify: 6 ms
- DSA Sign: < 39 ms; DSA Verify: <66 ms

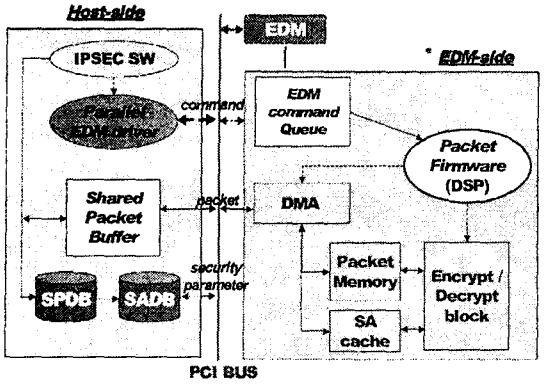

Fig. 9. Crypto-Accelerator Interface Architecture

4.4 Network processor with embedded crypto engine

Network processor supports a variety of service through the optimized micro-engine. The probabilities of producing of bottleneck in IPSec packet processing have two elements. The first element is control path bottleneck problem. It is impossible to operate packet processing because bulk encryption time is required lots of computational time. The second element is data path. The bottleneck is occurred because of the limit of bandwith of bus. IXP2850 can support a solution for the two bottleneck problems. Control path bottleneck have an above 10Gbps throughput with embedded crypto module. The architecture of IXP2850 has a good structure to solve a data path bottleneck [9].

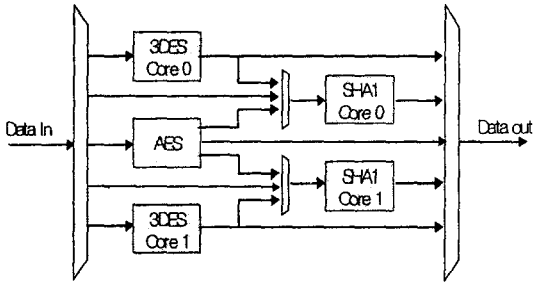

Fig. 10. Block diagram internal crypto module of IXP2850

5. 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] T. Braun, M. Kasumi, et al., "Virtual Private Network Architecture", IAM-99-01, April 1999.

[2] St. Kent, R. Atkinson: *Security Architecture for the Internet Protocol;* RFC 2401, Nov. 1998.

[3] Implementing Virtual Private Networks, Steven Brown, McGraw-Hill, 1999.

[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] http://www.hifn.com, "8154 HIPP II Security Processor"

[6] J. W. Yoon, Y. K. Kim, D. H. Ryu, "On a Implementation of High-Speed VPN Gateway with Parallel Architecture", WISC2001, Sept. 2001.

[7] 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.

[8] Hac-Su Ju,, et al., "Trend of development for High-speed Encryption processor", VOL., 12, KIISC, 2002

[9] http://www.intel.com

[10] Kye-sang Lee, "Trend of standard for IPSec," KISA, 2000.8

[11] http://www.lighttreading.com