A 10 Giga VPN Accelerator Board for Trust Channel Security System

Ki Hyun Kim, Jang-Hee Yoo, and Kyo Il Chung

***Abstract*—**This paper proposes a VPN Accelerator Board (VPN-AB), a virtual private network (VPN) protocol designed for trust channel security system (TCSS). TCSS supports safety communication channel between security nodes in internet. It furnishes authentication, confidentiality, integrity, and access control to security node to transmit data packets with IPsec protocol. TCSS consists of internet key exchange block, security association block, and IPsec engine block. The internet key exchange block negotiates crypto algorithm and key used in IPsec engine block. Security Association blocks setting-up and manages security association information. IPsec engine block treats IPsec packets and consists of networking functions for communication. The IPsec engine block should be embodied by H/W and in-line mode transaction for high speed IPsec processing. Our VPN-AB is implemented with high speed security processor that supports many cryptographic algorithms and in-line mode. We evaluate a small TCSS communication environment, and measure a performance of VPN-AB in the environment. The experiment results show that VPN-AB gets a performance throughput of maximum 15.645Gbps when we set the IPsec protocol with 3DES-HMAC-MD5 tunnel mode.

***Keywords*—** TCSS(Trust Channel Security System), VPN(Virtual Private Network), IPsec, SSL, Security Processor, Security communication.

I. Introduction

TODAY, internet environment is made by high speed network and various information communication infra construction. In this way, outside effusion of top secret documents is occurring to important social problems. Also, Internet electronic commerce leaves convenience of life and is situating to social infra that dominate competitive power of enterprise and institution, society and country now. Hacking of the Internet is being on the increase as go as computerization is advanced like this, and need more efforts to solve problems that is happened in such various dysfunctions. A TCSS technique among this effort is one of method to provide safe data communication in network environment. But, it is very difficult problem to provide data communication of high speed as is safe on network environment such as present. As this strengthens security function for safety in network environment each packet to do Routing necessary amount of work done because increase greatly be. Therefore, Trade-Off always exists between security and speed [1]. A recent security processors offer user various function and very fast performance. These high speed security processors become a item that is essential to network security system that big width-band is required. Information protection technology such as VPN, Firewall, IDS(Intrusion Detection System) etc. are developed variously with network security equipments. Recently, equipments integrated by technologies more than two are announced. We propose a VPN acceleration board for trust channel security system to be used in router, gateway, and network devices [9], [10].

The rest of the paper is structured as follows. Section 2 provides a structure of TCSS. Detail unit functions of the system and data flow are presented. In session 3, architecture of VPN-AB is presented, and shows the board. Experiment, performance, and an investigation of test result are presented in session 4. Finally, conclusion is written in session 5.

II. TCSS

TCSS supports safety communication channel between security nodes in internet. It furnishes authentication, confidentiality, integrity, and access control to security node to forward data packets with IPsec protocol.

A. Structure of TCSS

Our TCSS (Fig. 1) consists of IKE (Internet Key Exchange) Block implemented on application, SA (Security Association) Management Block, and IPsec Engine Block operated in kernel and hardware. We implement IPsec engine block to VPN Accelerator Board. IKE block is a module that has some function to key exchange and negotiation for initial privet network channel between security nodes [6].

B. IKE Block

IKE block is a top module of VPN communication to support a trust channel between different security node and node on internet. It provides to us configuration setup, bi-direction authentication, IKE SA, and IPsec SA for key exchange and negotiation. IKE SA module performs phase 1 negotiation that creates key material with other security node, and IPsec SA

Manuscript received October 31, 2005. This work was supported in part by the Korea Department of the Ministry of Information and Communication.

Ki Hyun Kim is with the Electronic and Telecommunication Research Institute, Daejeon 305-350 KOREA (phone:82-42-860-6355; fax: 82-42-860-5022; e-mail: kihyun@ etri.re.kr).

Jang-Hee Yoo is with the Electronic and Telecommunication Research Institute, Daejeon 305-350 KOREA (phone:82-42-860-1324; fax: 82-42-860-5022; e-mail: jhy@ etri.re.kr).

Kyo Il Chung is with the Electronic and Telecommunication Research Institute, Daejeon 305-350 KOREA (phone:82-42-860-1920; fax: 82-42-860-5022; e-mail: kyoil@ etri.re.kr).

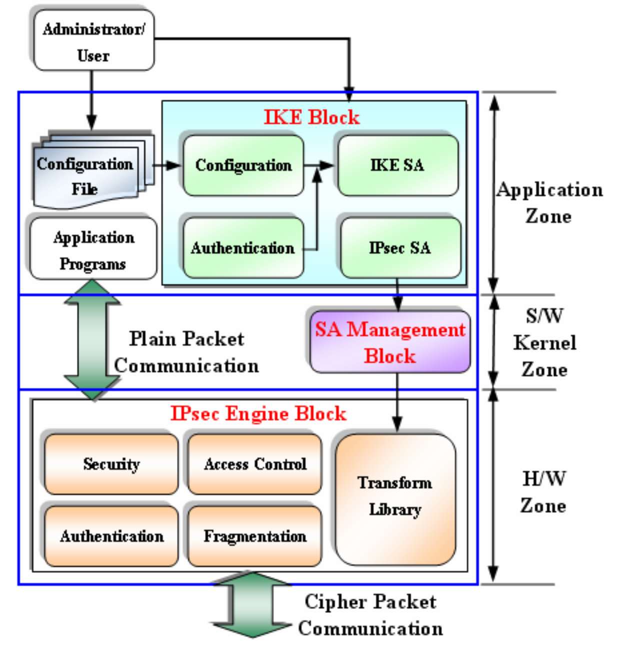


Fig. 1 Structure of TCSS

module performs phase 2 negotiations to create SA to use in IPsec engine block. Characteristic of IKE block is as following.

- Support Pre-shared key method for authentication
- Set up Bi-direction SA
- Phase 1 Key exchange Protocol : differ-Hellman, RSA
- Support Weak/semi-weak key check

C. SA Management Block

SA management block is in S/W kernel zone, and it transmits SA data from IKE block to IPsec engine block. The block consists of PF-Key, SADB, SADB API, and Inter-Process Communication. PF-Key is a interface module with IKE block. SA information is stored in SADB through SADB API. SADB is offered to IPsec engine block through inter-process communication.

D. IPsec Engine Block

IPsec engine block is operated in IP layer of TCSS. It provides various security services through compounding of security protocols (AH: Authentication Header, ESP: Encapsulation Security Payload) and security mode (Tunnel, Transport) for traffic that is transmitted between user host and network. Addition, it secures safety for all communication data including an IP hearer [9]-[11]. When the IPsec packets pass through the IPsec engine block, actually encryption and decryption, such as DES, 3-DES, AES, and RSA, are operated in this block. So, if a security network equipment designer wants to design a high speed security router or gateway about 10Gbps, he is able to implement this module by hardware.

III. VPN-AB Implementation

The VPN-AB provides a safe channel base on IPsec in network environment, gateway, router, and network

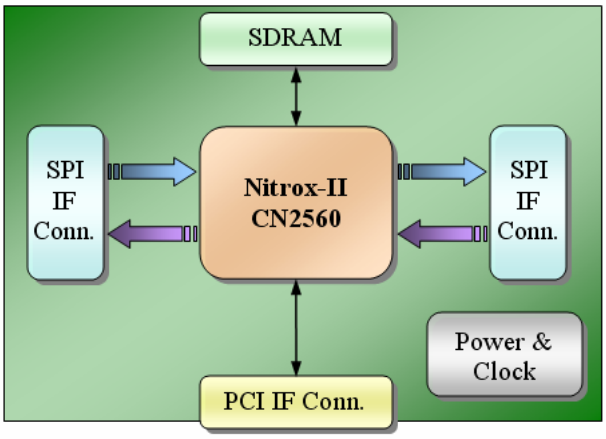


Fig. 2 Architecture of VPN-AB

management system. The channel is between security network node systems [2].

A. Architecture of VPN-AB

VPN-AB consists of security processor module, memory module, external I/O interface modules, and power & clocks modules, and the simple architecture of VPN-AB. We show a block diagram of VPN-AB and implemented board in Fig. 2 and Fig. 3. When supported IPsec and built trust channel, VPN-AB must support a In-Line scheme so that degradation in existing network security nodes may amount to minimum and it must provide Look-Aside architecture so that encryption/decryption and SSL protocol according to necessary may be easy. As a result, VPN-AB has high speed security processor, two SPI ports and PCI interface. We need SDRAM to store SA information. It is implemented by a DDR_SDRAM module that supports up to 133MHz input/output rate. We develop device driver program for VPN-AB in Montavista Linux.

B. Security Processor Module

We use Nitrox-II CN2560 security processor. It has two advantages, speed and security. Nitrox-II CN2560 security processor was manufactured in Cavium in 2003 Q4. It is a One-Chip security processor that has high performance to process cryptography and supports various protocols, as listed below [2]-[4].

- L2&L3 parsing
- Inbound SA look up
- Multi-Encryption/Decryption Algorithm Support
  - ✓ RSA, Diffie-Hellman(groups 1, 2, 5)
  - ✓ DES/3DES, AES, ARC4
  - ✓ MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
- Highest Protocol Processing
  - ✓ 10,000 IKE Main Mode/sec
  - ✓ High bulk data encryption
  - ✓ 5G to 20G for IPsec application
  - ✓ 3DES + SHA-1 or 3DES + MD5
  - ✓ Up to 320Mbps Random Generator
- High performance industry standard interfaces

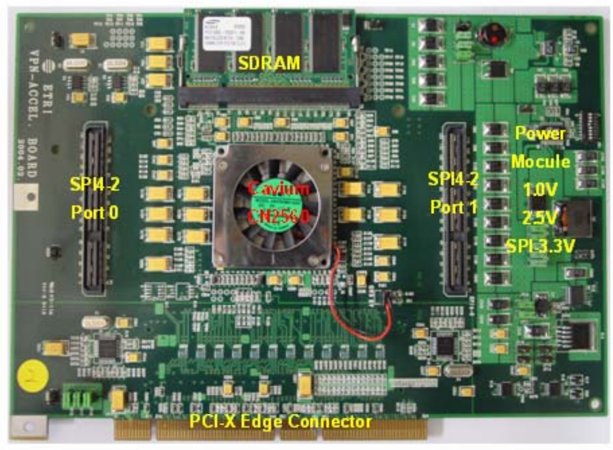


Fig. 3 VPN-AB

✓ PCI/PCI-X ; 32/64-bit, 33/66/133 MHz
✓ SPI-4 x 2 ports

Additionally, it supports SSL/TLS or IPsec/IKE security protocol. CN2560 security processor offers high speed transaction and flexibility because inside core and various crypto modules are operated with parallel scheme. Currently, Cavium announce a new CN2560 security process that gets a 77MHz input clock, as a result inside core clock is a 308MHz.

C. *External I/O Interface Module*

We have two SPI-4.2 ports for inbound and outbound data packets and PCI bus to transfer initialize security processor and IPsec configuration setup data. One SPI-4.2 port is used between security processor and Ethernet MAC processor, the other SPI-4.2 port is used between security processor and network processor [5]. We use a SAMTEC connector, because it guarantees to transmit 1.33GHz data packet through Differential pair connector.

We use a PCI bus to transfer initialize security processor and IPsec configuration setup data. Performance of PCI bus is 66bits 66MHz.

D. *Power & Clocks Module*

A Power module of VPN-AB is very carefully made by us, because Nitrox-II is very sensitive processor to power. Powers used in VPN-AB are generated by 3.3V and 5.0V that are supplied by PCI Edge Connector. Power module generates 1.0V, 2.5V, and SPI3.3V. Nitrox-II security processor uses 1.0V, 2.5V, and SPI 3.3V and they are inputted sequentially in Nitrox-II security processor. The power sequence is firstly SPI3.3, next 1.0V, finally VDD2.5V. If the input sequence is fail, Nitrox-II security processor is not working.

TABLE I
POWER CONSUMPTION OF VPN-AB

Voltage	1.0V	2.5V	PCI 3.3V	SPI 3.3V	Total
Power Consumption	9.0W	0.7W	0.8W	2.0W	12.5W

1.0V is used in internal core power of Nitrox-II security processor, and it is one of the most sensitive powers. Input & output pins and others parts of Nitrox-II security processor use 2.5V and SPI3.3V. And 3.3V is used in peripheral elements on VPN-AB. The power consumptions of each voltage are summarized in TABLE I. Power consumption of 1.0V is the most value, and its power margin is a little range, 1.0V ~ 1.1V. We use a 72 MHz Oscillator for core sync of Nitrox-II security processor and use a 33MHz Oscillator for SDRAM sync.

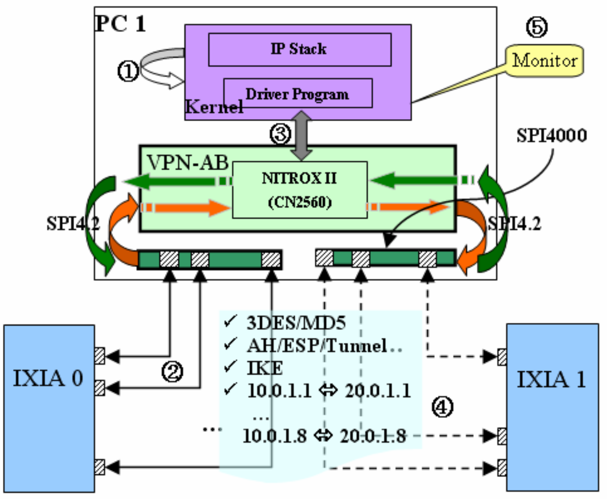


Fig. 4 Topology used in experiments

IV. EXPERIMENTATION

The main goal of the experimentation described here is to measure the data transmission performance on VPN-AB for using IPsec peer-to-peer communication.

A. *Experiment Setup*

We construct a test environment to use two IXIA and a VPN-AB (show Fig. 4). Network Interface Board for VPN-AB is an SPI4000 which is made by Cavium. SPI4000 has 1Gbps x 8ports and uses a Intel IXF1010 MAC process to generate SPI4.2 protocol signal. The SPI4.2 signal is inputted on SPI4.2 port of VPN-AB. The scenario of experiment is

① Security manager set a new security policy in IKE block through PCI

② VPN-AB receives up to 1Gbps null packet generated at each IXIA port through MAC board(SPI4000).

③ After receives SA information from SA manager block, VPN-AB performs IPsec Tunnel mode and generates IPsec packets.

④ IPsec packets, generated by VPN-AB, are transmitted to the other IXIA ports through the other SPI4000.

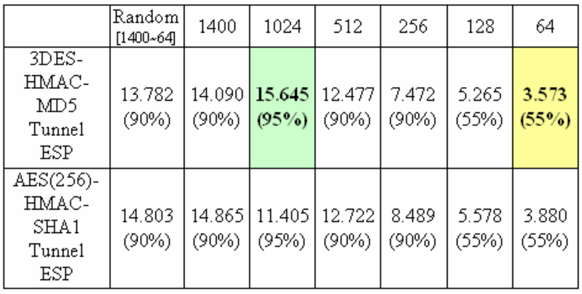
⑤ The performance of IPsec process is gained by monitor program in PC. The monitor program analysis all inbound and outbound packets.

⑥ The flow from ② to ④ is processed from IXIA 1 to IXIA 0 at the same time.

B. Results and Analysis

We analyze the proposed VPN-AB according to various payload size and policy of IPsec communication. 3DES and MD5 are fundamental crypto algorithms for encryption and authentication. At packet size of 1024 byte and policy of 3DES / HMAC / MD5 / Tunnel ESP, the performance of VPN-AB is up to 15.645Gpbs (TABLE II). We set maximum transmission rate of 95%. If IXIA generates data bits by higher rate than 95%, CRC error between two IXIA is happened. At payload size of 64 byte and the same policy, IXIA translates into a maximum theoretical throughput of 3.573 Gbps. We know that the total data bit rate is in inverse proportion to packet size.

TABLE II
PERFORMANCE OF VPN-AB



	Random [1400~64]	1400	1024	512	256	128	64
3DES-HMAC-MD5 Tunnel ESP	13.782 (90%)	14.090 (90%)	**15.645 (95%)**	12.477 (90%)	7.472 (90%)	5.265 (55%)	**3.573 (55%)**
AES(256)-HMAC-SHA1 Tunnel ESP	14.803 (90%)	14.865 (90%)	11.405 (95%)	12.722 (90%)	8.489 (90%)	5.578 (55%)	3.880 (55%)

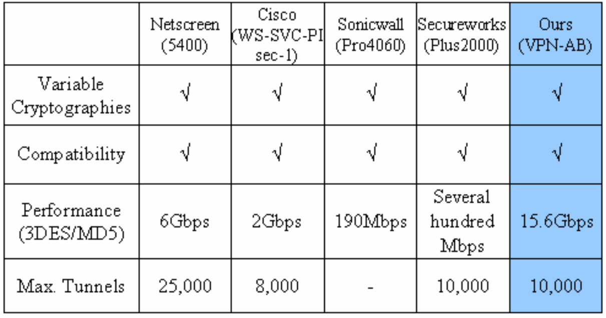
The performance comparison results with other VPN equipments are such as TABLE III. The first compare item is variable cryptographies for encryption, decryption, and authentication. Generally, most of all VPN systems support variable cryptographies. The second, a VPN equipment must offer compatibility with IPsec Freeswan (S/W) firstly and other equipments that are already used in internet. All equipments including VPN-AB satisfy the condition. Performance of IPsec is measured in same condition that is a 3DES / HMAC / MD5 / Tunnel / ESP. VPN-AB has the highest score value of 15.6Gbps. The number of tunnels is very important factor in SSL VPN [8]. Netwcreen 5400 offers maximum tunnels of 25,000. VPN-AB and Plus 2000 of Secureworks support no small tunnels of 10,000. We demonstrate the superiority of VPN-AB on Table 3.

V. CONCLUSION

Recently, developed security processors are improved very performance, and security algorithms of a lot part were implemented by hardware. These high speed security processors are essential elements in development of network security equipments used in wide band network. In this paper, we propose a VPN accelerator board (VPN-AB) with performance of 10Gbps. And the VPN-AB provides flexibility to support both in-line mode and look-aside mode, and supports compatibility with other VPN equipments that are already used in network environment.

We are developing a new enhanced VPN accelerator board for a high speed router system that is developed with Intel IXP2800 network processor. We are tuning a SIP-4.2 interface between network processor (IXP2800) and Security Processor (Nitrox-II CN2560).

TABLE III
COMPARE WITH OTHER IPSEC VPN EQUIPMENTS



	Netscreen (5400)	Cisco (WS-SVC-PI sec-1)	Sonicwall (Pro4060)	Secureworks (Plus2000)	Ours (VPN-AB)
Variable Cryptographies	√	√	√	√	√
Compatibility	√	√	√	√	√
Performance (3DES/MD5)	6Gbps	2Gbps	190Mbps	Several hundred Mbps	15.6Gbps
Max. Tunnels	25,000	8,000	-	10,000	10,000

REFERENCES

[1] Neil Gammage, "Security Application Note," Motorola Canada, 2001.

[2] "Nitrox-II Security Processor CN25xx Family Hardware Manual Rev0.1," Cavium, 2003.

[3] "CN-EB2200 Schematic Rev AX01," Cavium, 2003.

[4] "CN-EB2500 Schematic Rev AX01," Cavium, 2003.

[5] "System Packet Interface Level 4(SPI-4) Phase 2:OC-192 System Interface for Physical and Link Layer Devices," 2001.

[6] "IPsec Security Policy Requirements," IETE Internet.

[7] "Nitrox-II Software Architecture Manual," Cavium 2004.

[8] Eric Rescorla, "SSL and TLS Designing and Building Secure System," Addison-Wesley, 2001.

[9] Uyless Black, "Internet Security Protocols Protecting IP Traffic," Prentice Hall PTR, 2000.

[10] Naganand Doraswamy, Dan Harkins, "IPsec : The New Security Standard for the Internet, Intranets, and Virtual Private Networks," Prentice Hall PTR, 1999.

[11] Elizabeth Kaufman, Andrew Newman, "Implementing IPsec : Making Security work on VPNs, Intranets, and Extranets," John wiley & Sons, 1999.