10Giga 급 보안 프로세서를 이용한 VPN 가속보드 구현

김 기현*, 유 장희*, 정 교일*
한국전자통신연구원

Implementation of VPN Accelerator Board Used 10 Giga Security Processor

Ki Hyun Kim*, Jang-Hee Yoo*, Kyo Il Chung*
Electronics and Telecommunications Research Institute
E-mail : *kihyun@etri.re.kr

Abstract

Our country compares with advanced nations by supply of super high speed network and information communication infra construction has gone well very. Many people by extension of on-line transaction and various internet services can exchange, or get information easily in this environment. But, virus or poisonous information used to Cyber terror such as hacking was included within such a lot of information and such poisonous information are threatening national security as well as individual's private life. There were always security and speed among a lot of items to consider networks equipment from these circumstance to now when develop and install in trade-off relation. In this paper, we present a high speed VPN Acceleration Board(VPN-AB) that balances both speed and security requirements of high speed network environment. Our VPN-AB supports two VPN protocols, IPsec and SSL. The protocols have a many cryptographic algorithms, DES, 3DES, AES, MD5, and SHA-1, etc.. The acceleration board process data packets into the system with In-line mode. So it is possible that VPN-AB processes inbound and outbound packets by 10Gbps. We use Nitrox-II CN2560 security processor VPN-AB is designed using that supports many hardware security modules and two SPI-4.2 interfaces to design VPN-AB.

I. 서론

초고속통신망의 보급으로 우리나라의 정보화 수준은 다른 선진국에 비해 빠르게 앞서나가고 있다.. 그러나, 이렇듯 정보화가 발전될수록 인터넷의 해킹은 갈수록 늘어가고 있으며, 이러한 다양한 역기능에서 발생되는 문제점들을 해결하기 위해 더 많은 노력이 필요하다. 그러나 현재와 같은 네트워크 환경에서 네트워크 환경에서 안전을 위해 보안 기능을 강화 할수록 각 패킷을 라우팅하는데 필요한 작업량은 크게 증가하기 때문에 안전하면서 고속의 데이터 통신을 제공하기는 매우 어려운 일이다. 가상사설망(VPN : Virtual Private Network) 시스템 기술은 최근 네트워크 환경에서 안전한 데이터 통신을 제공하기 위한 방법 중 하나로 각광 받고 있다.

VPN 시스템뿐만 아니라 보안 통신 장비들의 설계 및 구현 시 보안과 속도는 항상 Trade-Off 를 통하여 제품의 성능이 결정된다. 최근에 개발된 보안 프로세서들은 성능이 매우 향상되고 많은 부분의 보안 관련 알고리즘이 하드웨어로 구현되어 있다. 이런 고속 보안 프로세서를 이용한 시스템은 매우 큰 대역폭을 요구하는 현 네트워크 보안 솔루션 장비 개발에는 필수 요소가 된다. 또한 네트워크 환경에서 정보를 보호하기 위한, 가상사설망(VPN : Virtual Private Network), 방화벽(Firewall), 침입탐지(IDS : Intrusion Detection System) 등과 같은 정보 보호 기술과 제품들이 다양하게 개발 되고 있다. 최근에는 2 개 이상의 기능이 통합된 장비들이 출시되고 있다.

이들 정보 보호 관련 기술 중 VPN 기술은 네트워크 망을 효율적으로 사용하기 위한 네트워크 기술이면서 동시에 네트워크 정보 보안을 위한 정보 보호 기술이다. 따라서 VPN 보안 장비는 이러한 두 가지 측면을 고려하여 설계되어야 한다. 무엇보다 VPN 의 보안 기능을 가능하게 해주는 기술은 크게 터널링 기술과 암호

화 기술이 있다. 터널링 프로토콜로는 PPTP, L2TP, IPsec 등이 있다. 이중 IPsec 은 가장 강력하고 융통성을 제공하는 터널링 프로토콜이며, VPN 보안 장비는 이를 기본적으로 지원해야 한다. 또한 고속 VPN 보안 장비에서 암호화 기능을 구현하기 위해서는 고속의 암호/복호 기능이 필요하며, 이를 구현하기 위해서는 고속 보안 프로세서의 사용이 필수적이다. [1]~[3]

본 논문의 2 장에서는 VPN-AB 및 VPN 시스템 구성 에 대해서 설명하고, 3 장에서는 각 모듈 별 세부 기능 및 동작 흐름을 상세하게 기술하고, 4 장에서는 VPN-AB 의 시험 및 고찰에 대해서 기술하고 , 마지막 5 장에서는 결론을 기술하였다.

II. VPN-AB 및 VPN 시스템

2.1. VPN-AB 의 개요

VPN-AB 는 네트워크 환경에서 게이트웨이, 라우터, 네트워크 관리 시스템, 또는 단말기 상호간의 데이터 및 제어 정보 등을 보호하기 위하여 IPsec 등을 기반으로 안전한 채널을 구축하고, 또한 시스템간의 사용자 트래픽에 대한 VPN 서비스를 제공하는 것을 목적으로 제작하는 하드웨어 보드이다.[6]

2.2 VPN 시스템 구성

VPN 시스템은 어플리케이션 영역에서 동작하는 IKE 블록, 커널 영역에서 H/W 를 기반으로 동작하는 IPsec 엔진 블록 및 SA 관리 블록으로 구성된다. VPN 시스템은 그림 1 과 같으며, IPsec 엔진 블록은 VPN-AB 로 구현하였다.

IKE 블록은 다른 보안 노드와의 신뢰 통신 채널을 설정하기 위한 키 교환 및 협상이 이루어지는 블록으로 Configuration 기능, 상호 인증 기능, IKE SA 현상 기능과 IPsec SA 협상 기능을 제공한다.

SA 관리 블록은 S/W 커널 영역에 존재하며, IKE 블록과 IPsec 엔진 블록간 SA 전송 및 기능을 담당한다.

IPsec 엔진 블록은 VPN 가속 기능을 수행하는 보드 형태로 구현되었다. 그리고 IPsec 패킷을 송/수신 할 때 실질적인 암/복호를 수행하며, H/W로 구현되어 고속 동작하는 블록으로, 기밀성 제공기능, 인증/무결성 제공 기능, 접근제어 기능 및 Fragmentation 처리 기능으로 구성된다.

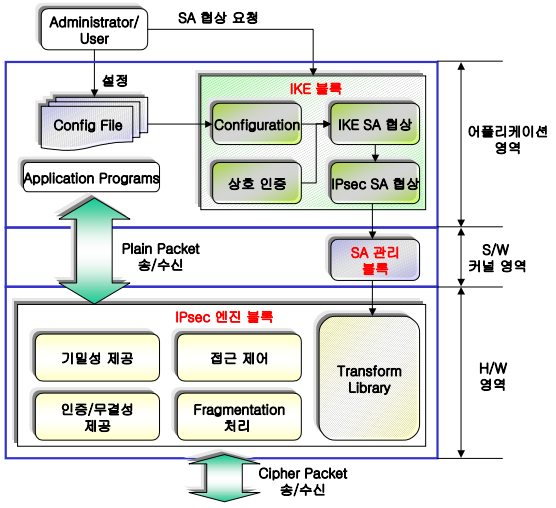

그림 1. VPN 시스템 구성

2.2.1 IKE 블록

IKE 블록은 Administrator 또는 사용자를 통해서 Configuration 설정 및 SA 협상 요청을 처리하는 어플리케이션 영역에 있으며, 크게 Configuration 기능 모듈과 SA 협상 모듈로 구성된다.[10][11] IKE 블록의 특징은 다음과 같다.

- ■ 상호 인증을 위한 Pre-shared Key 방식 제공
- ■ 동시 양방향 SA 설정
- ■ phase 1 key exchange protocol : Diffie-Hellman, RSA
- ■ weak/semi-weak key check 기능 제공
- ■ 안전한 SA 협상 지원

2.2.2 SA 관리 블록

PF_KEY 기능 모듈은 협상된 SA 저장을 위해서 IKE 인터페이스를 제공하며 SADB API는IPsec 엔진 블록에 의한 접근을 허용한다.

2.2.3 IPsec 엔진 블록

IPsec 엔진 블록은 VPN-AB로, 보안 프로세서 및 주변 H/W 소자로 구현된다. 이렇게 구현된 IPsec 엔진 블록의 특징은 다음과 같다.

- ■ L2&L3 parsing
- ■ Inbound SA look up
- ■ 지원 암/복호 알고리즘
  - ✓ RSA, Diffie-Hellman(groups 1, 2, 5)
  - ✓ DES/3DES, AES, ARC4, SEED (Opt.)
  - ✓ MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
- ■ IPsec 관련 고속 처리 기능
  - ✓ 10,000 IKE Main Mode/sec
  - ✓ IPsec 어플리케이션을 위한 수 기가급 암/복호 처

리 지원

✓ 3DES + SHA-1 or 3DES + MD5

✓ 최대 320Mbps 난수 발생

■ 지원 인터페이스

✓ PCI/PCI-X, SPI-4.2

■ In-Line 패킷 처리 기능 지원(Bump In The Wire)

III.VPN-AB 설계

본 절에서는 앞 절에서 설명한 VPN 시스템을 고속으로 구현할 VPN-AB의 설계에 대해서 설명한다.

3.1 VPN-AB 전체구조 및 구성

그림 2는 현재 제작된 VPN-AB이며, 크게 보안 프로세서와 메모리를 포함한 보안 프로세서 모듈과 SPI4.2 및 PCI 인터페이스를 포함하는 외부 인터페이스 모듈, 그리고 가속 보드의 전원 및 동작 클럭을 공급하는 전원 모듈로 분류된다. 각 모듈에 대한 상세 내용은 다음과 같다.

3.2. 보안 프로세서 모듈

보안 프로세서 모듈은 여러 평가 방법에 의해 선정된 Nitrox-II 보안 프로세서를 중심으로 구현하였다.

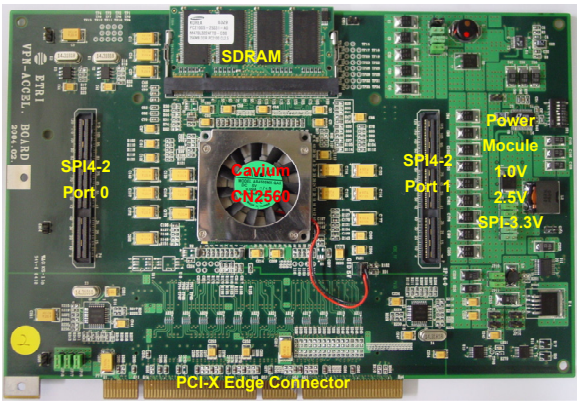

그림 2. VPN-AB

보안 프로세서 모듈에 사용된 Nitrox-II 보안 프로세서는 2003년 Cavium사에서 제작한 것으로, 2004년 중순에 안정화가 이루어졌으며, 앞 절에서 설명한 바와 같이 고속의 암호 처리 능력을 가지고 있으며, 다양한 프로토콜을 지원하는 암호처리 단일 칩이다. 이는 고속의 산술연산 모듈과 랜덤 수 생성기, 해쉬 처리 모듈이 하드웨어로 구현되어 있어 가능하며, 또한 SSL/TLS 또는 IPsec/IKE 암호 프로토콜을 지원한다. Nitrox-II 프로세서는 내부 코어가 Giga급 처리가 가능하도록 설계되어 있으며, 여러 암호 연산이 병렬로 처리 가능하도록 설계되어 있어, 더욱 고속 처리와 시스템 설계 융통성을 제공한다. [4] 현재 Cavium사에서 제공되고 있는 Nitrox-II CN2560 프로세서는 77MHz까지 입력이 가능하며 결과적으로 내부 Core는 77MHz의 4배인 308MHz로 동작한다.

SA 정보를 저장하기 위한 4개의 DDR SDRAM Bank를 제공하며, 각 Bank에는 최대 512Mbyte까지 지원한다. 그러나 본 VPN-AB는 133MHz, 256Mbyte를 탑재한 하나의 Bank로 설계하였다.

Cavium에서는 Linux, BSD, Windows, VxWorks를 위한 S/W 드라이버 지원하며, 본 논문에서는 Linux 지원 SDK를 이용하여 개발하였다.[12]

3.3. 외부 인터페이스 모듈

VPN-AB에서 제공되는 SPI4-2 인터페이스는 최소 311MHz에서 최대 500MHz를 지원하여, 최소 9.7Gbps에서 최대 15.6Gbps까지의 데이터 전송률을 지원한다.[7] 본 가속보드에서는 288MHz의 Core 클럭으로 동기 되어 9G까지 동작이 가능하다. VPN-AB에서 PCI 인터페이스는 보안 프로세서의 초기화와 IPsec Configuration setup을 위한 마이크로 코드 다운로드를 위해 사용된다. [8]

3.4. 파워 모듈

VPN 가속 보드에 사용되는 전원은 PCI Edge Connector를 통해서 공급되는 3.3V와 5V 이다. 5V 전원을 통하여 Nitrox-II 프로세서에 사용되는 1.0V, 2.5V , SPI3.3V 전원들을 만들어 내며, 1.0V는 Nitrox-II 프로세서의 내부 코어 전원으로 사용되며, 2.5V와 SPI3.3V는 나머지 보안 프로세서의 내부 유닛에 사용된다. 그리고 보안 프로세서의 입출력 핀 신호들을 위해 PCI에서 입력된 3.3V를 사용한다. 각 전원의 소비전력은 표 1과 같다.

<표 1> 보안 프로세서 소비 전력

1V	2.5V	PCI3.3V	SPI3.3V	Total
9W	0.7W	0.8W	2W	12.5W

사용된 입력 클럭은 Core 동기를 위한 72MHz Oscillator 와 SDRAM 동기를 위한 33MHz Oscillator를 사용하였다.

IV. 시험 및 고찰

제작된 VPN-AB는 그림 3에서와 같이 실험 환경을 구성하여 시험을 하였다. 시험 환경에서는 CN2560

Nitrox-II 보안 프로세서 개발을 위해Cavium사에서 제작한 EB2500 보드의 SPI4000 보드를 이용하였다. 각 각의 SPI4000 보드는 8개의 1G ports를 제공하며, Intel IXF1010을 이용하여 SPI4.2 신호로 바꾼 다음 Nitrox-II 보안 프로세서로 입력된다. 그림 3에서와 같이 SPI4.2 Port는 SPI4000 보드와 케이블로 연결된다. 이러한 환경에서 시험 시나리오는 다음과 같다.

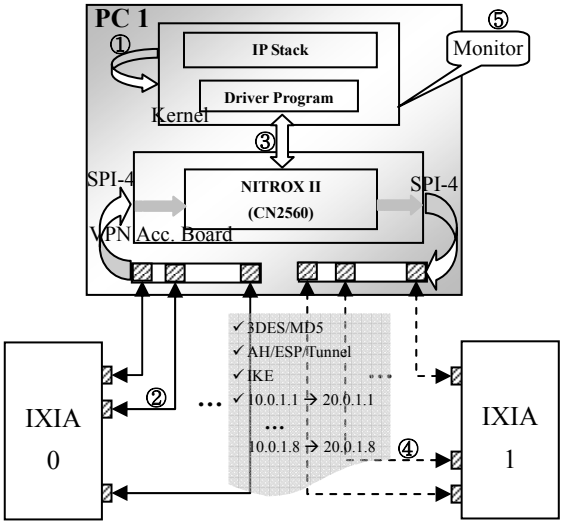

그림 3. 데모를 위한 망 및 인터페이스 구성도

① 보안 관리자가 PCI의 IKE 블록에 새로운 보안 정책을 적용시키고, VPN-AB의 각 Port에 입력될 IP에 대해서 고정 IPsec Configuration을 설정한다.

② VPN-AB는 IXIA의 각 Port에서 생성된 1Gbps의 Null 패킷을 MAC 보드(SPI-4000) 통해서 4개의 Port로 수신한다.

③ SA 관리 블록으로부터 해당 SA를 수신해서 IPsec Tunnel mode 처리를 수행하여 IPsec 패킷을 생성한다.

④ 생성된 IPsec 패킷은 다른 MAC 보드를 통해서 IXIA Port로 전달된다.

⑤ IPsec 처리 성능은 PCI에서 VPN-AB의 모니터 프로그램을 통해서 입력 데이터 패킷 및 출력되는 IPsec 처리 패킷의 데이터 전송률을 분석한다.

VPN-AB 성능 시험 결과는 <표 2>에서와 같다.

<표 2 VPN-AB 성능 시험 (단위 : Gbps)

	Random [64~1400]	1024	256	64
3DES-HMAC-MD5 Tunnel ESP	13.789 (80%)	15.645 (95%)	7.472 (70%)	3.573 (55%)
AES(256)-HMAC-SHA1 Tunnel ESP	13.782 (90%)		7.572 (90%)	
	14.034 (80%)	11.405 (95%)	8.521 (70%)	3.880 (55%)
	14.803 (90%)	14.924 (90%)	8.489 (90%)	

현재 Cavium에서 제공되고 있는 칩은 계속된 Upgrade가 되고 있으며, 최근 구매된 Y0418 데이터 코드 칩은 시험 결과를 통하여 많은 부분 안정된 것으로 기대 된다.

V. 결론

본 논문에서는 10 Giga급 VPN-AB 설계 및 구현 결과에 대해서 기술하였다. 본 시스템은 상용 VPN 장비와의 호환성을 위하여 상용 VPN 장비에서 사용되는 암호 알고리즘은 모두 지원하도록 설계하였다. 또한 두 개의 SPI-4.2 인터페이스와 PCI 인터페이스를 지원하여 고속 처리에 유리한 In-Line 구조 지원하도록 설계 하였다.

현재 여러 가지 시험을 통하여 그 성능을 검증하고 있다. NP(Network Processor)와 연동된 보안 라우터 시스템에 본 VPN-AB 모듈을 이용하고 있으며, 본 VPN-AB 모듈의 초대 성능 시험은 NP와 연동된 시스템에서 시연이 가능할 것이다.

참고문헌

[1] 주학수, 주홍돈, 김승주, "고속 암호연산 프로세서 개발현황", 정보보호학회지, 제12권 3호, 2002

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

[3] 이계상, "IPsec 표준화 동향", KISA동향특집, 2000. 8

[4] “NITROX-II Security Processor CN25xx Family Hardware Manual Rev0.1”, Cavium, 2003. 6.

[5] "CN-EB2200 Schematic Rev AX01", Cavium, 2003. 5

[6] "CN-EB2500 Schematic Rev AX01", Cavium, 2003. 2.

[7] “차세대 암호 알고리듬 동향”, 류희수, 정교일, 한국전자통신연구원/주간기술동향, 1052호, 2002. 6.

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

[9] “NGSS 시스템 설계서”, 한국전자통신원구원, 2003.6.

[10]“IPsec Security Policy Requirements”, IETF Internet-Draft

[11] “IPsec Configuration Policy Information Model”, IETF Internet-Draft

[12]“Nitrox II Software Architecture Manual”, Cavium 2004