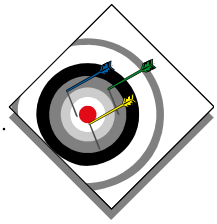


포/커/스

Giga 급 보안 프로세서 및 VPN 장비 기술 동향

김기현* 한종욱**

최근 급증하고 있는 온라인 거래와 다양한 인터넷 서비스의 확대로 네트워크 사용자는 데이터 전송 속도와 안전성 모두를 원한다. 그러나, 네트워크 환경에서 안전하면서 고속의 데이터 통신을 제공하기는 매우 어려운 문제다. 이는 네트워크 환경에서 안전을 위해 보안 기능을 강화할수록 각 패킷을 라우팅 하는데 필요한 작업량은 크게 증가하기 때문이다. 따라서 보안과 속도는 항상 trade-off 가 존재한다. 최근에 개발된 보안 프로세서들은 성능이 매우 향상되고, 많은 부분의 보안 관련 알고리즘이 하드웨어로 구현되어 있다. 이런 고속 보안 프로세서는 매우 큰 대역폭을 요구하는 현 네트워크 보안 솔루션 장비 개발에는 필수 요소가 된다. 본 문서에서는 Giga 급 VPN 장비를 구현하기 위해 필요한 Giga 급 보안 프로세서들의 성능 및 기능비교, 안전성, 활용성 등을 조사, 분석한다. 그리고, 높은 시장 점유율을 가지고 있는 보안 프로세서를 이용한 VPN 설계 방법을 소개하고, 고속 VPN 장비로 많이 판매되는 Cisco 사와 NetScreen 사의 VPN 장비를 비교 분석한다. ▧

목 차

* ETRI 사이버테러기술분석팀/선임연구원
** ETRI 사이버테러기술분석팀/팀장

Ⅰ. 서 론

최근 급증하고 있는 온라인 거래와 다양한 인터넷 서비스의 확대로 인하여 많은 사람들이 쉽게 정보를 주고 받거나, 얻을 수 있다. 그러나 바이러스 또는 해킹과 같은 사이버 테러로 인하여 개인의 사생활 정보 유출은 물론 국가적 안보까지 위협하고 있다. 이러한 네트워크 환경에서 정보를 보호하기 위한, 가상사설망(Virtual Private Network: VPN), 방화벽(Firewall), 침입탐지(Intrusion Detection System: IDS) 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 보

호 기술이다. 따라서 VPN 보안 장비는 이러한 두 가지 측면을 고려하여 설계되어야 한다. 무엇보다 VPN 의 보안 기능을 가능하게 해주는 기술은 크게 터널링 기술과 암호화 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. 본 문서에서는 Giga 급 VPN 보안 장비를 설계하는데 필요한 Giga 급 보안 프로세서의 성능 및 기능비교, 안전성, 활용성 등을 조사 분석하고자 한다. 또한 높은 시장 점유율을 가지고 있는 Giga 급 보안 프로세서를 이용한 간략한 VPN 설계 방법을 소개하고, 고속 VPN 장비로 많이 판매되는 Cisco 사와 NetScreen 사의 VPN 장비를 비교 분석한다.

II. Giga 급 보안 프로세서

고속 보안 프로세서는 서론에서 언급한 바와 같이 다양한 암호 알고리즘을 하드웨어로 구현한 것으로 많은 블록 암호 알고리즘과 공개키 알고리즘이 구현되어 있다. 블록 암호 알고리즘을 하드웨어로 구현한 고속 보안 프로세서를 이용하는 것은 Federal Information Processing Standard(FIPS) 140-1 또는 140-2 의 보안 레벨을 높일 수 있고, 3DES, RC4 와 같은 간략한 알고리즘의 구현뿐만 아니라 AES 등과 같은 복잡한 블록 암호 알고리즘의 속도를 높일 수 있기 때문이다. 본 장에서는 고속 보안 프로세서의 성능 및 기능비교, 안전성 등에 대하여 조사·분석한다.

1. 성능 비교

현 VPN 장비에서는 IPsec 기능이 대표적인 지원 프로토콜이며, 일반적으로 VPN 장비의 성능을 언급할 경우에도 IPsec 의 처리 속도를 성능으로 기술한다. IPsec 은 Internet Protocol(IP) 패킷의 무결성, 인증, 기밀성 등의 보안 서비스를 지원할 수 있는 보안 프로토콜의 개발을 위해 만들어 졌으며, 두개의 프로토콜로 구성되어 있다. 하나는 패킷의 무결성과 송신자 인증서비스를 위한 Authentication Header(AH) 프로토콜과, 다른 하나는 무결성과 인증서비스뿐만 아니라 기밀성 서비스를 추가로 제공하는 Encapsulating Security Payload(ESP) 프로토콜이 있다. AH 와 ESP 프로토콜은 독립적으로 사용될 수도 있고, 같이 사용될 수도 있다. 각각 AH 와 ESP 프로토콜은 Transport 모드와 Tunnel 모드로 동작된다. 기본적으로 Transport 모드는 IP 와

TCP 헤더 사이에 AH 와 ESP 헤더가 들어가는 구조이고, Tunnel 모드에서는 기존의 IP 패킷의 내용 전부를 AH 또는 ESP 헤더 안에 넣고, 이 자료를 전송하기 위한 새로운 IP Header 를 형성하는 구조로 되어 있다. 이때 기술된 IPsec 성능은 IPsec 의 기능 중 암호 알고리즘에서는 3DES 처리 속도와 인증에서는 SHA-1 또는 MD5 의 처리 속도를 이야기 한다. 최근 출시되고 있는 Giga 급 IPsec 처리 보안 프로세서의 성능은 <표 1>과 같다.

<표 1> Giga 급 IPsec 보안 프로세서의 성능 비교

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

* IPsec 연산 속도는 3DES + SHA-1 을 사용한 자료임.
** IKE 성능은 1 초에 IKE handshakes 수행되는 횟수를 나타낸 것임.

고속의 IPsec 을 구현하기 위해서 AH 와 ESP 에 필요한 고속 암호 연산뿐만 아니라, Security Association(SA)를 위한 지원도 있어야 한다. SA 는 공개 키 기반의 IKE(Internet Key Exchange) 프로토콜을 기본으로 사용하며, 다른 프로토콜의 사용도 가능하다. IKE 프로토콜은 자동화된 SA 협상, 키 생성, 분배 및 갱신을 담당하며, IKE SA 협상 및 생성으로 IKE 키가 생성되는 1 단계와 IPsec SA 협상 및 생성으로 IPsec 키를 생성하는 2 단계로 동작한다. 따라서, 고속의 IPsec 연산을 구현하기 위해서는 IKE 전용 모듈 또는 프로세서가 있어야 한다.

<표 2> BCM5841 프로세서 종류 및 성능

모델	성능
BCM5841-1	4.8Gbps
BCM5841-2	2.4Gbps
BCM5841-3	1.2Gbps
BCM5841-4	0.6Gbps

<표 3> Nitrox-II 프로세서 종류 및 성능

모델	외부 I/O 인터페이스(분류 기준)	성능
CN2130	1 x SPI-3, PCI/PCI-X 64bit/133MHz	3Gbps
CN2240	2 x SPI-3, PCI/PCI-X 64bit/133MHz	6Gbps
CN2340	1 x SPI-3 & 1xSPI-4.2, PCI/PCI-X 64bit/133MHz	6Gbps
CN2450	1 x SPI-4.2, PCI/PCI-X 64bit/133MHz	10Gbps
CN2560	2 x SPI-4.2, PCI/PCI-X 64bit/133MHz	10Gbps

보안 프로세서에서 지원하는 IKE 성능은 <표 1>에 기술되어 있다. Broadcom 사의 BCM5841 과 NetOctave 사의 NSP4200 프로세서는 내부에 IKE 전용 모듈이 없어 IKE 전용 프로세서를 같이 설계해야 한다. 참고로, Broadcom BCM5841 과 Cavium Nitrox-Ⅱ 보안 프로세서를 세부적으로 분류하면 다음과 같다.

2. 안전성

보안 프로세서를 안전성의 측면에서 판단하는 가장 간단한 방법은 FIPS 140-1, FIPS 140-2 를 만족하는지 여부이다[13,14]. FIPS 140-1 은 1995 년 7 월 17 일 NIST(National Institute of Standard and Technology)와 CSL(Computer Systems Laboratory)이 CMV(Cryptographic Module Validation) 프로그램을 설립하여 연방정부의 정보처리 표준을 제정한 것으로 4 개의 레벨로 나누어져 있으며 11 개 분야의 보안요구사항을 규정하고 있다.

<표 4> FIPS 인증 레벨

Hifn (Hifn 8154)	Cavium (Nitrox-Ⅱ)	Broadcom (BCM5841)	Corrent (CR7120)	NetOctave (NSP4200)
FIPS 140-1 Level 3	FIPS 140-2	FIPS 140-1 Level 3	FIPS 140-2	-

FIPS140-1 의 각 레벨과 분야에 대한 상세한 내용은 참고 문헌 [13,14]를 참조하면 된다. FIPS 140-2 는 FIPS 140-1 을 대체하는 표준으로 2001 년 6 월 22 일 제정되었다. <표 1>에서 살펴본 제품에 대하여 FIPS 인증여부와 인증받은 레벨에 대하여 <표 4>에 있다. <표 4>는 본 문서를 작성하는 시점에 제품의 데이터 시트를 정리한 것으로 아직 인증을 받지 않은 제품도 뒤에 인증을 받을 것으로 예측되기 때문에 시장에 주는 영향은 없을 것으로 판단된다.

3. 지원 암호 알고리즘

보안 프로세서의 선정에서 성능, 안전성과 함께 가장 많이 비교되는 부분은 지원 암호 알고리즘이다. 각 보안 프로세서에서 지원하는 암호 알고리즘은 Encryption 알고리즘, Authentication 알고리즘, Public-Key 알고리즘들로 분류된다.

<표 5>에서와 같이 조사한 대부분의 보안 프로세서들은 최근 새로 제안된 암호 알고리즘들까지 대부분 지원하고 있어, 시스템을 설계할 경우, 호환성을 위해서는 기본적으로 많이 사용되는 암호 알고리즘들을 지원하는 보안 프로세서의 사용이 필수적이다.

<표 5> 지원 프로토콜 및 암호 알고리즘

	Hifn (Hifn 8154)	Cavium (Nitrox-II)	Broadcom (BCM5841)	Corrent (CR7120)	NetOctave (NSP4200)
3DES(DES)	2.4Gbps	10Gbps	4.8Gbps	2.4Gbps	10Gbps
AES	128bit	256bit	256bit	Y	Y
RC4	Y	Y	N	N	N
HMAC	Y	Y	Y	Y	Y
MD5	Y	Y	Y	Y	Y
SHA-1	Y	Y	Y	Y	Y
RSA	Y	Y	N	Y	N
DH	Y	Y	N	Y	N
LZS	Y	N	N	N	N
RNG	Y	Y	N	Y	N

* LZS 는 데이터 압축 알고리즘으로 Hifn 사가 국제 특허권을 가지고 있다.

4. 지원 프로토콜

VPN 구현을 위해서는 여러 암호 알고리즘과 함께, SSL 과 IPsec 을 포함한 터널링 프로토콜인, L2F, PPTP, L2TP 등의 다양한 프로토콜이 지원되어야 한다. <표 6>에서는 각 고속 보안 프로세서에서 지원하는 프로토콜을 기술한다.

<표 6> 지원 프로토콜

	Hifn (Hifn 8154)	Cavium (Nitrox-II)	Broadcom (BCM5841)	Corrent (CR7120)	NetOctave (NSP4200)
IPsec	Y	Y	Y	Y	Y
PPTP	Y	N	N	N	N
L2TP	Y	N	N	N	N
SSL	Y	40,000 TPS	N	N	N

* TPS: Transaction Per Second 은 SSL 프로세서의 성능으로 초당 프로세서가 처리할 수 있는 새로운 SSL Transaction 수

IPsec 은 IP 패킷의 무결성, 인증, 기밀성 등의 보안 서비스를 지원하기 위한 보안 프로토콜의 개발을 위해서 만들어졌으며, AH 프로토콜과 ESP 프로토콜로 구성되어 있다. 또한 각각 AH 와 ESP 프로토콜은 Transport 모드와 Tunnel 모드로 동작된다.

PPTP(Point to Point Tunneling Protocol)는 쓰리콤과 마이크로소프트가 공동 개발한 VPN 보안 강화용 프로토콜이며, 강력한 보안 제공에 더해, IP 뿐 아니라 NetBEUI 나 IPX 와 같은 멀티 프로토콜을 지원한다는 장점을 제공한다

L2TP(Layer 2 Tunneling Protocol)란 PPTP 와 시스코의 L2F 프로토콜을 통합해 만든 프

로토콜로 원격 Dial-Up 접속을 통해 기업의 전산시스템에 접속하여 신뢰성 있는 양방향 데이터 통신을 제공하기 위해 만들었다.

SSL(Secure Socket Layer) 프로토콜은 처음에 Netscape 사에서 웹서버와 브라우저 사이의 보안을 위해 만들었다. SSL 은 Certificate Authority(CA)라 불리우는 서드 파티로부터 서버와 클라이언트의 인증을 하는데 사용된다.

5. 데이터 인터페이스

보안 프로세서를 선정하여 VPN 장비를 설계하는데 있어, 보안 프로세서가 지원하는 데이터 인터페이스는 매우 중요한 요소가 된다. 이러한 보안 프로세서의 데이터 인터페이스는 SEED 와 같은 상용 보안 프로세서에서 지원하지 않는 알고리즘의 칩셋을 함께 설계할 경우, 또는 MAC 이나 Frame 모듈과의 연결성, NPU(Network Processor Unit)와의 연결성, 마지막으로 시스템 호스터 프로세서와의 연결을 용이하게 한다. <표 7>은 각 보안 프로세서가 지원하는 데이터 인터페이스를 정리한 것이다.

<표 7> 보안 프로세서가 지원하는 데이터 인터페이스

프로세서 종류	Bus Interface
Hifn(Hifn 8154)	- PCI 32/64bit, 33/66MHz - Streaming Bus(PL3:32bit 104MHz)
Cavium(Nitrox-II)	- PCI/PCI-X 32/64 bit, 33/66/133MHz - Dual SPI-3/SPI-4
Broadcom(BCM5841)	- BCM1250 과 연동 PCI 64bit - 2 x FIFO 16 Interface
Corrent(CR7120)	- PCI 32 bit, 66MHz
NetOctave(NSP4200)	- PCI-X 64bit 100MHz

PCI 인터페이스는 기본적으로 64 비트 66MHz 로 최대 4Gbps 까지 지원하며, PCI-X 는 64 비트 133MHz 로 8Gbps 의 데이터 전송 속도를 지원한다. Hifn 8154 의 Streaming 버스는 64bit 의 PCI 데이터 버스에서 상위 32bit 를 입력 전용으로, 32bit 의 출력 전용 Streaming 포트로 구성된다. Streaming 버스는 데이터 전용 버스로써 32bit 104MHz 로 동작하며, 이 경우 8154 의 PCI 는 32bit 제어 버스로 동작한다. SPI-3(System Packet Interface 3)은 32 비트 133MHz 로 최대 4Gbps 까지 지원하며, SPI-4 는 32 비트로 최대 1GHz 동작 속도를 지원한다.

6. 지원 운영체제

고속 보안 프로세서로 설계된 고속 보안 모듈은 기존의 라우터 또는 게이트웨이에 추가되어

<표 8> 지원 운영체제

Hifn (Hifn 8154)	Cavium (Nitrox-II)	Broadcom (BCM5841)	Corrent (CR7120)	NetOctave (NSP4200)
Linux	Y	Y	Y	Y
BSD OS	Y	Y	Y	Y
VxWorks	Y	Y	Y	Y
Windows	Y	Y	Y	N

VPN 기능을 수행한다. 따라서 고속 보안 모듈을 사용하기 위해서는 기존의 라우터와 게이트웨이의 개발 환경과 같은 운영체제의 드라이버 소프트웨어가 제공하여야 한다. <표 8>는 각 보안 프로세서 회사에서 지원하는 운영체제를 나타내고 있다.

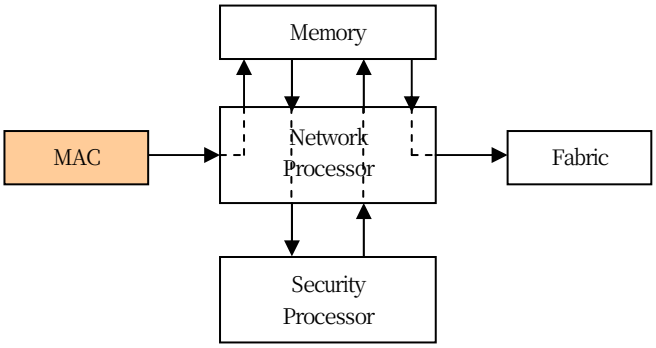
<표 8>에 기술된 보안 프로세서들 중 최근 개발되어 출시된 보안 프로세서인 경우 데이터시트와 달리 아직 지원이 되지 않는 운영체제가 있으며, 차후 지원될 것으로 기대된다. VPN 장비에 가장 많이 탑재된 칩은 Hifn 의 프로세서로 세계 시장의 많은 부분을 점유하고 있으며, 다음으로는 Broadcom 의 제품이 있다. 그러나, 최근 신생 기업 또는 시장 점유율이 조금 떨어지는 기업으로 Cavium, Corrent, 그리고 NetOctave 등이 있다. 각각의 고속 보안 프로세서는 각 프로세서의 특징이 있어, 설계하고자 하는 VPN 제품의 성격에 맞는 프로세서를 선택하는 것이 개발 기간을 단축시키는 방법이 될 것이다.

III. 보안프로세서에 따른 VPN 시스템 구조

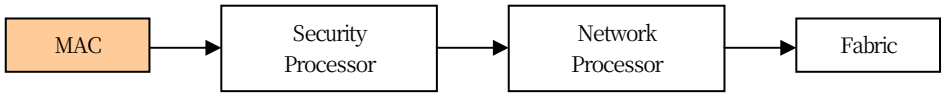
본 장에서는 Giga 급 보안 프로세서를 이용하여 VPN 장비를 구현할 경우 시스템 구현 방법에 대해서 기술한다. 보안 프로세서를 이용하여 보안 기능을 구현하는 방법은 크게 Look-aside 구조와 In-line 구조가 있다. (그림 1)은 네트워크 프로세서와 보안 프로세서의 Look-aside 구조와 In-line 구조를 잘 나타내고 있다.

Look-aside 구조는 입력된 패킷이 네트워크 프로세서를 통해서 메모리에 저장되고 보안 프로세싱이 필요로 하면 보안 프로세서에 의해서 처리된 다음, 다시 메모리에 저장되고, 네트워크 프로세서에 의해서 출력된다. 이 경우, 네트워크 프로세서와 보안 프로세서를 연결하는 데이터 전송 버스가 성능 제약 요소가 된다.

In-line 구조는 Look-aside 구조의 성능 문제를 해결하기 위해 제안된 방법으로 이 구조는 네트워크 프로세서와 보안 프로세서 사이의 복잡한 데이터 전송과 반송 과정이 없고, 네트워크 프로세서는 보안 프로세서에서 제공되는 평문 데이터 패킷만을 처리하는 장점이 있다. 그러나 이 구조에 사용될 보안 프로세서는 네트워크 프로세서가 제공하는 패킷 재구성 기능, 패킷 프로



(a) Look-aside 구조



(b) In-line 구조

(그림 1) 보안 시스템 구현 방법

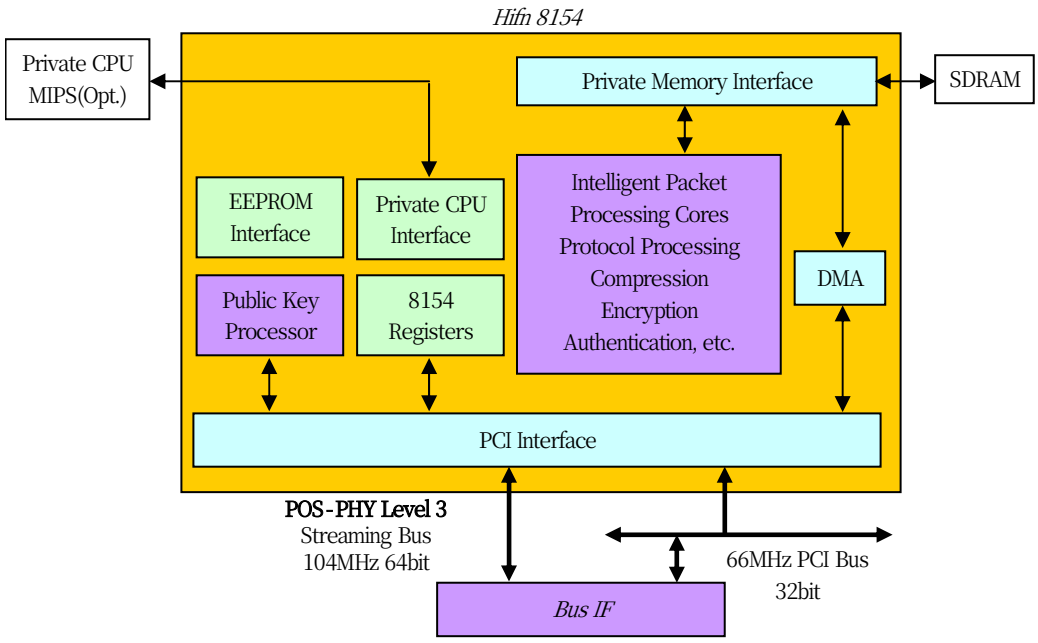
토콜 기능 등을 제공해야 한다. 즉, IPsec VPN 를 구현할 경우 사용될 보안 프로세서는 기본적으로 IPsec 에 필요한 많은 기능이 제공되어야 한다.

다음은 Hifn 8154 과 Nitrox-II 을 이용하여 Look-aside 구조의 IPsec VPN 과 In-line 구조의 IPsec VPN 을 간략한 블록도로 기술하고자 한다.

1. Look-aside 구조

Hifn 8154 보안 프로세서를 이용한 Look-aside 시스템 블록도는 (그림 2)와 같이 구성할 수 있다. 기본적으로 Hifn 8154 는 PCI 버스 인터페이스를 제공하여 호스트 프로세서 또는 네트워크 프로세서와 PCI 버스를 통한 데이터 전송이 가능하다. 패킷 전송 성능을 향상하기 위해서 Hifn 8154 에서는 독립된 PL3 의 Streaming Bus 인터페이스를 제공하며, In-line 구조의 시스템 설계도 제공한다. Streaming Bus 모드는 104MHz 32bit 의 데이터 전용 출력 핀과 PCI 버스의 상위 32bit 를 Streaming Bus 모드의 입력 핀으로 사용한다. 이 경우 PCI 버스의 나머지 하위 32bit 는 일반 목적의 66MHz 32bit PCI 버스로 사용한다.

Hifn8154 으로 시스템을 설계할 경우 또 다른 특징으로는 Private CPU 를 가진다. Private CPU 는 Hifn 8154 에서 지원하지 않는 프로세스를 처리하며, 보안 프로세서를 포함하는 보안 모듈의 초기화, 보안 세션 셋업 등 여러 기능을 수행한다. 또한 Hifn 8154 보안 프로세서는 병



(그림 2) Hifn 8154 시스템 블록도

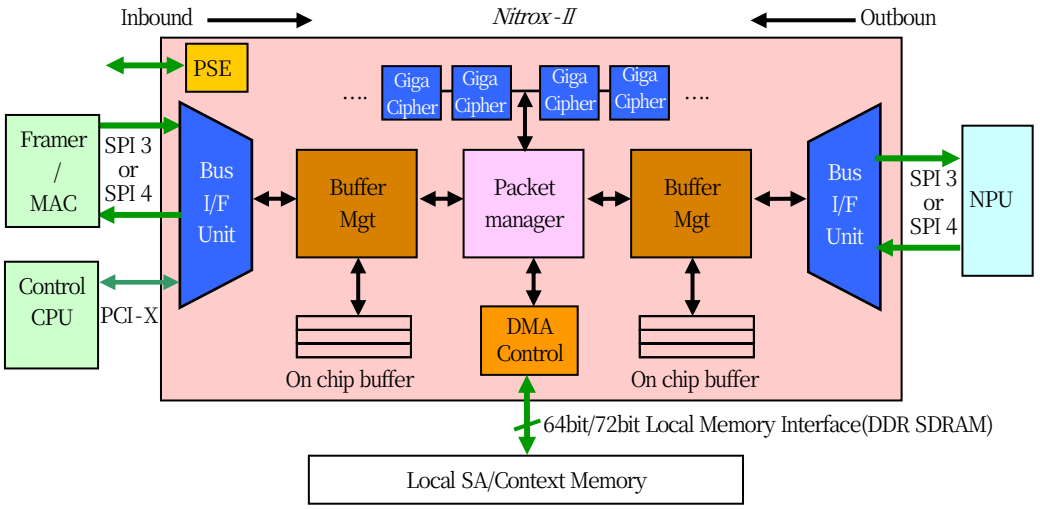
렬 설계가 가능하여 여러 Hifn 8154 보안 프로세서간의 로드 벨런싱을 수행한다. Hifn 8154 는 Private CPU 인터페이스로 MIPS CPU(32bit) 인터페이스를 지원하며, 다른 종류의 프로세서를 사용할 경우 인터페이스를 위한 부가 회로가 필요하다. Hifn 의 차기 보안 프로세서인 HIPP III 는 MIPS CPU 코어가 칩 내부에 내장된다.

이러한 look-aside 구조는 Hifn 8154 와 Brodcom BCM5841 를 이용하여 구현할 수 있다.

2. In-line 구조

Cavium Nitrox-II 보안 프로세서를 이용한 In-line 구조의 IPsec VPN 블록도는 (그림 3)에 나타나 있다.

Nitrox-II 보안 프로세서는 다양한 외부 인터페이스를 통하여 고속의 시스템 설계가 용이하다. Nitrox-II 보안 프로세서는 (그림 3)에서와 같이 64bit 400MHz DDR SDRAM 인터페이스를 제공하여 고속의 데이터 패킷 처리에 더욱 용이하다. 또한 호스트 프로세서를 위한 PCI-X/PCI 인터페이스는 SEED 를 위한 독립된 버스 인터페이스를 제공한다. Cavium Nitrox-II 보안 프로세서는 (그림 3)과 같은 In-line 구조뿐만 아니라 look aside 설계 방법도 제공한다. 이러한 In-line 구조는 Cavium Nitrox-II 보안 프로세서 또는 NetOctave NSP4200, Corrent CR1720 프로세서를 사용하여 구현할 수 있다.



(그림 3) Nitrox-Ⅱ 시스템 블록도

Ⅳ. VPN 장비 현황

VPN 장비 제조회사는 전세계적으로 많이 있으나, 본 고에서는 세계 시장 점유율 40~50%를 차지하고 있는 Cisco 사 장비, 고속 VPN 장비를 선도하고 있는 NetScreen 장비 그리고, 국내 업체의 장비에 대해서 살펴보고자 한다.

1. Cisco VPN 모듈

Cisco 사에서는 상당히 많은 종류의 게이트웨이 또는 라우터를 생산한다. 이들 장비들이

<표 9> Cisco 사의 VPN 보안 모듈

Cisco Part Number	지원 장비	성능(3DES)	Max Tunnels
MOD1700-VPN	1700s	4Mbps	100
AIM_VPN/BP	2610, 2620, 2650, 2600XM, 2691	10Mbps	300
AIM-VPN/EP	2650, 2600XM, 2691	14Mbps	800
AIM-VPN/HP	3660, 3745	40Mbps	800
AIM-VPN/EP Ⅱ	2691, 3725,	14Mbps	800
AIM-VPN/HP Ⅱ	3660, 3745	40Mbps	2,000
NM-VPN/MP	3620/40	18Mbps	800
WS-C650x-IPsec-K9 WS-SVC-IPsec-1	catalyst 6500, 7600s	2Gbps	8,000

AIM: Advanced Interface Module, BP: Base Performance, EP: Enhanced Performance, HP: High Performance

<표 10> Cisco 장비 지원 LAN 인터페이스

장비	지원 가능 LAN 인터페이스
1700 series	- 10/100 Based T
2600 series	- 단일 또는 듀얼 10/100 BaseT
3600 series	- 단일 또는 듀얼 10/100 BaseT - One-port 155Mbps OC-3
6500 series, 7600 series	- 10/100BASE-TX - 10Gbps 메트로 이더넷 - 10/100/1000BASE-TX - Giga Bit Interface Converter(GBIC) - 100BASE-FL 포트

IPsec VPN 기능을 제공하기 위해서는 VPN 보안 모듈이 시스템에 탑재되어야 한다. Cisco 에서 지원하는 VPN 보안 모듈을 정리하면 <표 9>와 같다.

MOD1700-VPN 모듈에서 AIM-VPN/EP II 모듈은 RSA, Diffie Hellman/SHA-1, MD-5 를 지원하고, AIM-VPN/HP II, NM-VPN/MP 모듈은 RSA, Diffie Hellman/SHA-1, MD-5/AES/LZS 를 지원한다. 마지막으로 Giga 급 처리를 지원하는 WS-C650x-IPsec-K9, WS-SVC-IPsec-1 모듈은 RSA, RADIUS, CHAP, PAP/HMAC-MD5, HMAC-SHA-1/IKE 를 지원한다. <표 9>에서 지원되는 Cisco 장비의 지원 LAN 인터페이스는 <표 10>에 나타나 있다.

2. NetScreen VPN 모듈

NetScreen 에서 제공하는 Giga 급 보안 장비는 NetScreen 5000 시리즈가 있다. NetScreen

<표 11> NetScreen 5000s 성능

NetScreen-5200	NetScreen-5400
- Maximum Performance * 4Gbps firewell 연산 * 2Gbps IPsec 연산 - 제공 인터페이스 * 최대 26 개 보안 인터페이스 제공 - 슬롯의 개수: 2	- Maximum Performance * 12Gbps firewell 연산 * 6Gbps IPsec 연산 - 제공 인터페이스 * 최대 78 개 보안 인터페이스 제공 - 슬롯의 개수: 4
- Capacity * 1,000,000 동시 세션 처리 * 25,000 IPsec VPN tunnels 처리 - FIPS-140 Level 2 - VPN 기능 * 3DES(168bit), AES(128bit), DES(56bit) 제공 * Remote access VPN, Site-to-Site VPN 제공 * L2TP with IPsec - IPsec Authentication * SHA-1, MD5, PKI	

* Firewell 연산 속도는 Bidirectional Firewall throughput 자료임.
* IPsec 연산 속도는 3DES + SHA-1 을 사용한 자료임.

<표 12> NetScreen Giga 급 VPN 모듈

8-port GigE(Gigabit Ethernet) SPM	24-port 10/100 Fast Ethernet & 2-port GigE SPM
- 8 개의 mini-GBIC interfaces - 2Gbps 3DES - 2 개의 GigaScreen-II ASIC 으로 구성	- 2 개의 mini-GBIC interface - 24 개의 10/100 interface - 1Gbps 3DES - 1 개의 GigaScreen-II ASIC 으로 구성

* SPM: Secure Port Module

5000 시리즈는 NetScreen-5200 과 NetScreen-5400 으로 구성된다.

각 모델에 대한 성능은 <표 12>에 간략하게 나타나 있다. NetScreen 은 VPN 지원을 위하여 자사에서 개발한 암호 가속 칩인 GigaScreen-II ASIC 칩을 사용한다. GigaScreen-II ASIC 칩은 2Gbps firewall, 1Gbps 3DES 처리 성능을 가진다. 또한 여러 보안 알고리즘이 최적의 형태로 구현되어 있어 패킷의 크기에 따른 성능 저하의 폭이 적으며, Programmability 기능이 우수하여 프로그램으로 패킷 분류 기능과 내용 검색 기능을 제공한다. <표 12>에는 GigaScreen-II 프로세서가 탑재된 Giga 급 VPN 모듈이 기술되어 있다. NetScreen 사에서 제공하는 두개의 Giga 급 VPN 모듈은 NetScreen-5200 또는 NetScreen-5400 모두에 탑재 가능하다.

8-port GigE SPM 에서 한 개의 GigaScreen-II ASIC 프로세서는 4-port 를 담당한다. 따라서 각 4-port 당 1 개의 GigaScreen-II ASIC 이 사용되며, 각 4-port 에서 최대 1Gbps 의 3DES 성능이 지원된다, 결과적으로 NetScreen-5400 에서 8-port GigE SPM 을 사용할 경우 최대 2Gbps 의 3DES 성능을 기대할 수 있다.

3. 국내 Giga VPN 모듈

국내 몇몇 장비는 외국 제품들과 충분한 경쟁력을 가지고 있다고 평가되고 있다. 국내 VPN 장비 업체들은 각각의 응용 부분에 맞는 상품을 개발하여 독자적인 기술력을 가지며, 시장을 점

<표 13> 국내 VPN 장비 현황

업체명	Top Model
시큐아이닷컴	NXG2000
퓨쳐시스템	SecuwayGate 6000E
어울림정보기술	Secuworks Plus3000
이노크래프트	EzoneVPN5500
시큐어소프트	수호신앱솔루트 1000
싸이버텍홀딩스	씨티 VPN8800
시큐어넥서스	시큐어 VPN3000
Infnis	SoligateVPN QoS 1000
Nex-G	Vforce5100

유하고 있다. <표 13>는 각 VPN 장비 업체에서 개발 완료, 또는 진행중인 최고의 성능을 제공하는 제품들이 기술되어 있다. 대부분의 장비는 500Mbps 에서 1Gbps 의 성능을 나타내며, 응용 분야에 따라 50Mbps 에서 100Mbps 의 성능을 나타내는 장비도 있다.

결과적으로 아직 국내에서는 단일 장비로써 2.5Gbps 이상의 VPN 을 지원하는 장비는 없는 상태이며, 몇 업체에서는 내년에 수 Gbps 급의 장비를 출시할 계획으로 준비하고 있다.

V. 결 론

Giga 급 고속 VPN 장비를 설계하기 위해서 고속 보안 프로세서의 성능, 기능을 비교하였고, 간략한 블록 설계, 그리고 고속 VPN 장비의 성능 및 VPN 지원 모듈에 대해서 알아 보았다. 보안 프로세서들의 비교는 동일한 환경에 장착된 성능이 아니므로 전적으로 믿는 것 보다는, 자신의 사용 목적에 적합한 용량 및 성능을 고려하여야 한다. 따라서 공통의 비교 카테고리를 다양한 측면에서 작성한 후, 이들 카테고리별로 각 제품들의 성능을 비교해 보아야 한다.

<참 고 문 헌>

[1] 주학수, 주홍돈, 김승주, “고속 암호연산 프로세서 개발현황,” 정보보호학회지, 제 12 권 3 호, 2002.

[2] Neil Gammage, “Security Application Note,” Motorola Canada, 2001.

[3] 이계상, “IPsec 표준화 동향,” KISA 동향특집, 2000. 8.

[4] “8154 HIPP II Security Processor,” available at http://www.hifn.com/products/8154.html

[5] “BCM5841 Multi-Gigabit Security Processor,” available at http://www.broadcom.com/products/5841.html

[6] “Nitrox-II Security Processor Hardware Manual,” Cavium networks, Doc:CN2xxx-HM

[7] “Nitrox Security Macro Processor SDK and Evaluation Board,” available at http://www.Cavium.com

[8] “Packet Armor CR7120 IPsec Security Processor,” available at http://www.corrent.com/products_packet.phtml

[9] “NSP4200 IPsec Security Processor,” available at http://www.netoctave.com

[10] “고속 라우터에서의 VPN 기능 구현 방안,” 한국전자통신연구원, R&D News 2002. 3.

[11] 정재훈, “VPN 보안 장치,” KT 연구개발본부, 표준화 동향과 쟁점, 2001. 8.

[12] 정지훈, 이종태, 손승원, “IPsec 표준화 동향 및 제품 현황,” 한국전자통신연구원 주간기술동향 통권 952 호, 2000. 6. 28, pp.1-17.

[13] FIPS PUB140-1, “Security Requirements and Cryptographic Modules,” 1994 Jan. 11.

[14] FIPS PUB140-2, “Security Requirements and Cryptographic Modules,” 2002 Dec. 11,