情 報 保 護 學 會 誌
第 13 券 第 4 號, 2003. 8

보안프로세서의 동향 및 성능 비교

이 상 수*, 김 영 수*, 한 종 욱*, 정 교 일**, 손 승 원*

요 약

네트워크 보안 시장이 급성장하고 다양한 보안 기능들이 요구되면서, 점차 통합된 보안 시스템 제품들이 시장을 주도하고 있다. 즉, 기존의 라우터나 스위치 상에 보안 기능을 탑제함으로서 하나의 솔루션으로 네트워크와 보안을 모두 해결할 수 있는 제품들이 각광을 받게 되었다. 반면에 이러한 보안기능의 처리와 관련된 네트워크 장비의 성능 저하를 해결하기 위해 다수의 장비업체들은 보안 프로세서를 사용하고 있다. 본 고에서는 네트워크 보안 시장 및 이와 관련한 보안 프로세서의 최근의 제품 동향과 각 프로세서 업체들에 의해 제공되는 보안 프로세서들의 특징을 비교한다.

Ⅰ. 서 론

최근의 네트워크 시장에서는 대부분의 네트워크 업체에서 보안 기능을 구축한 네트워크 장비들을 출시하고 있다. 이는 인터넷이라는 거대한 네트워크 인프라를 통해 급속히 증가하고 있는 사이버 침해에 대응하기 위해 상당히 고무적인 사실이라 할 수 있다. 하나 한편으로는 기존의 네트워크 장비가 가지는 기능에 덧붙여 추가된 보안 기능의 처리에 따른 네트워크 장비의 성능저하라는 문제를 야기하였다. 이러한 문제는 순수한 네트워크 기능에서도 기존의 S/W 방식의 패킷처리가 가지는 성능상의 한계가 이미 나타나기 시작하였으며 이를 해결하기 위해 라우팅과 같은 네트워크 기능들을 고속으로 처리할 수 있는 네트워크 프로세서가 출현하게 되었다. 역사적으로 네트워크 프로세서는 1980년대 말경에 MIPS사와 모토롤러사 등에 의해 최초로 개발되어 졌으며, 이를 근거리 및 원거리 네트워크용 패킷 처리 칩으로 사용해왔다. 최근에는 MMC사, SiTera사, T.sqware사, Agere사, Maker사 등과 같은 업체들이 프로그램 가능한 네트워크 프로세서를 개발함으로써, 근거리 및 원거리 네트워크에서의 대역폭 문제를 효율적으로 다룰 수 있게 되었다. 현재 네트워크 프로세서는 대량의 정보가 오가는 네트워크에서 데이터 패킷의 전달을 통제하는 역할을 하는 칩, 라우터, 스위치 등의 네트워크 장비에서 포트간 트래픽 전송·지능형 스위칭 기능을 하는 프로그래밍 기능이 가능해, 다양한 멀티미디어 인터넷 트래픽 서비스를 제공하기 위한 인프라 구축의 핵심 부품으로 자리잡고 있다. 가장 먼저 이 시장에 눈독을 들이고 접근한 업체는 인텔, 그리고 그 뒤를 이어 IBM, 모토로라, 어기어 등이 속속 제품을 내놓고 국내 개발 업체들과 물밑 작업을 벌이고 있다. 특히 인텔사는 최근에 데이터 패킷 처리 칩 개발 업체인 Softcom 마이크로시스템사를 1억 5천만 달러로 인수하여 자체 네트워크 프로세서를 개발하고자 한다.

네트워크 프로세서의 경우와 마찬가지로 방화벽과 같은 보안 시스템 분야에 있어서도 기존의 S/W 방식에 의해 구현되었던 제품들의 성능 한계를 극복하기 위해 보안 프로세서라 불리는 별도의 칩을 이용하여 고속의 처리 성능을 제공하는 제품들이 시장을 장악하고 있는 추세이다. 또한 최근의 VPN 시장의 급성장에 따른 보안 프로세서 시장의 치열한 경쟁에 의해 보안 프로세서 업체들은 기능의 다양성과 함께 기가급의 고속 데이터 처리를 동시에 만족할 수 있는 프로세서 제품들을 출시되고 있다. 보안 프로세

* 한국전자통신연구원 네트워크보안연구부({sangsu, hanjw, blitzkrieg, swsohn}@etri.re.kr)
** 한국전자통신연구원 정보보호기반연구부(kyoil@etri.re.kr)

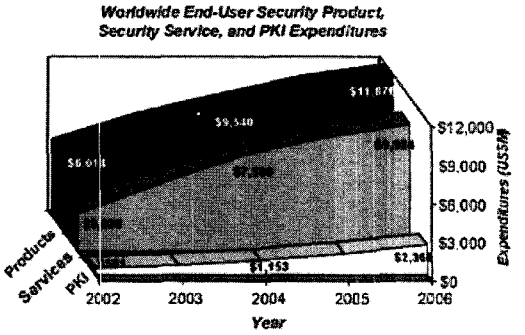
서시장에는 Hifn, Corrent, BroadCom 등의 다양한 업체들이 포진하고 있으며 최근 신생업체인 Cavium 사가 괄목할 만한 성장세를 보여주고 있다.

본 고에서는 보안 본 문서는 네트워크 보안 시장에 대한 이해와 이 시장에서 요구되는 기술적 사항에 대해 고찰한다. 또한 최근 출시되고 있는 보안 프로세서들에 대하여, 성능(performance)과 통합 수준(level of Integration), 가용성(availability), 그리고 특징(features) 등의 항목에 따른 비교를 제시한다. 본 고의 구성은 다음과 같다. 우선 제2장에서는 네트워크 보안이 중요하게 된 배경을 알아보고, 시장을 주도하는 장비들인 VPN, 방화벽, 침입 탐지시스템 등을 통해 구성된 안전한 네트워크를 간략하게 살펴 본다. 제3장에서는, 네트워크 보안과 관련한 여러 보안 프로토콜과 암호 알고리즘들을 다루고, 제4장에서는 네트워크 보안 시장을 주도하고 있는 여러 벤더들의 보안 프로세서 제품들을 자세한 항목별로 나누어 비교한다. 이러한 비교를 통해 향후 네트워크 보안 시장의 발전 방향에 대해 가늠해 볼 수 있을 것이다.

II. 네트워크 보안

최근의 네트워크 보안 시장의 성장의 원동력은 다음과 같은 세 가지 요인으로 요약될 수 있다.

- 활발해진 전자상거래: 홈쇼핑이나 통합된 비즈니스 거래를 통해, 개인이나 기업은 신용 카드 정보나 은행 계좌 같은 민감한 정보들을 공중망으로 전송하고 있다. 따라서 노출된 공중망으로부터의 전자상거래의 내용을 보호할 수 있도록 네트워크 보안이 반드시 이루어져야 한다..
- 네트워크 트래픽의 증가: 기업들은 사업 확장을 위해 꾸준히 해외로 진출하고 있으며, 이에 따라 글로벌 사이트들과의 정보 공유를 위한 데이터의 송수신량이 지속적으로 증가되고 있는 추세이다. 이러한 대규모 트래픽이 전달되는 네트워크에서는 사소한 보안적 취약성의 파급효과가 상당히 크게 나타나게 된다.
- 공유 네트워크로의 전이: 고가의 전용선을 대신하기 위해, 많은 기업들은 인터넷을 이용한다. 하지만 사설망으로부터 공유망으로 네트워크가 전이되는데에 따르는 보안적인 문제점은 더욱 다양해졌다.



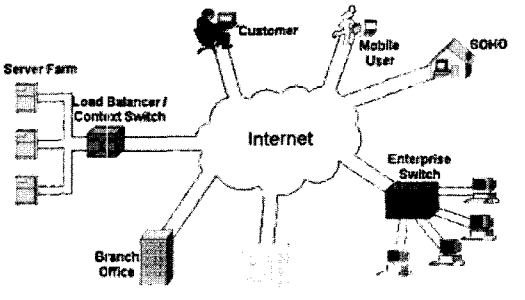
〔그림 1〕 보안 관련 시장 전망

이러한 보안 시장의 성장세를 반영하듯 Infonetics Research Inc.[1]는 〔그림 1〕과 같이 보안 제품, 보안 서비스, 그리고 PKI 분야가 2005년에는 200억 달러 정도 수익을 올릴 것으로 예상했다.

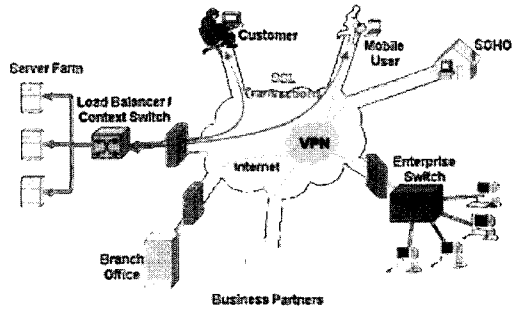
1. 네트워크 구성의 변천에 따른 보안 구조

다음 〔그림 2〕는 인터넷으로 연결된 일반적인 네트워크를 보여준다. 그림의 좌측에는 로드 밸런싱 스위치를 통해 고객들에게 웹-기반 서비스를 제공하는 서버군이 있고, 우측 하단부에는 한 회사 내의 기업 네트워크가 존재한다. 이러한 네트워크는 고객들, SOHO(Small or Home Office)의 원거리 종사자, 이동 중인 사용자, 비즈니스 파트너, 그리고 다수의 지점들과 인터넷을 통해 연결되어 있다. 이와 같은 네트워크 구조는 완벽한 연결성(connectivity)을 제공하지만, 보안에 대해서는 전혀 고려하지 않고 있다.

고객들이 인터넷 상에서 특정 상품을 주문하고 이에 대한 값을 지불하는 전자상거래의 경우, 보안의 보장이 필수적이며, 최근까지의 네트워크 보안은 주고 전자 상거래에 초점을 맞추어 왔다. SSL(Secure Socket Layer)은 이러한 인터넷에서의 전자 상거래에 가장 널리 사용되는 보안 프로토콜로써 노드간



〔그림 2〕 일반적인 네트워크 구성



〔그림 3〕 보안 솔루션에 의한 안전한 네트워크

의 안전한 정보를 교환할 수 있는 표준화된 종단간 솔루션을 제공한다.

하지만 최근의 네트워크 보안의 관심은 전자상거래 분야로부터 VPN(Virtual Private Network), 방화벽, 침입탐지시스템 등의 종합적인 보안 솔루션의 제공으로 옮겨가고 있다.

〔그림 3〕은 SSL 트랜잭션들과 하나의 VPN, 그리고 다수의 방화벽으로 구성된 안전한 네트워크를 보여준다.

VPN은 실지로는 인터넷과 같은 공용망을 사용하되 사용자에게는 전용망을 사용하는 것처럼 구성되는 안전한 네트워크 솔루션이다. 특히 이동 중인 사용자, 원거리 사무실, 그리고 SOHO 재택 근무자 등을 네트워크에 연결시키는 데에 사용될 수 있다.

기업 네트워크에서의 데이터 보호는 네트워크 보안의 또 다른 중요 이슈이다. 방화벽은 인가되지 않은 데이터가 네트워크 내부에 들어오거나 외부로 보내어지지 못하도록 하기 위해 들어오고 나가는 트래픽을 검사한다.

방화벽의 기능이 근원지 주소와 목적지 주소, 그리고 모든 패킷들의 내용을 검사하고, 이를 통해 원하지 않는 트래픽을 블록킹하는 것인 반면, 침입 탐지 및 방지(Intrusion Detection & Prevention)는 트래픽의 패턴까지 분석하는 기능이다. 피해를 줄 가능성이 있는 비정상적인 트래픽 패턴을 찾아내고, 의심되는 근원지로부터 오는 트래픽을 블록킹하는 기능을 한다. IDS(Intrusion Detection System)는 로컬 네트워크로부터의 모든 정보 요청을 탐지하고, 인가되지 않은 접속 허용을 막는다.

IDS는 또한 서비스 거부(Denial Of Service, DOS) 공격으로부터 네트워크를 보호한다. 여기서 DOS 공격은 네트워크 라우팅 시스템에 부하를 주기 위해, 여러 불특정 근원지로부터 엄청나게 많은 패킷들을 전송하는 공격을 의미한다.

2. 보안 시스템

최근까지의 네트워크 보안 시스템은 VPN, SSL, 방화벽, IDS 등을 개별적으로 구현한 단일 기능 시스템이었다. 암호 프로세싱 기능은 또한 표준 보안 프로세서(security processor)를 사용하는 보안 가속화 보드(security acceleration board)에 구현될 수 있다[2]. 여기에서 사용되는 보드는 다양한 네트워크 업체들의 시스템에 사용될 수 있는 일반적인 보드이다. 하나의 네트워크에 여러 보안 기능들이 필요해짐에 따라, 업체들은 통합 보안 시스템(integrated secu-rity system)들을 선보이고 있다. 전문 보안 시스템 업체들이 개발한 이러한 제품들은 VPN, SSL, 방화벽, IDS 등을 지원하는 유니트들이 하나로 통합되어 있는 형태이다. NetScreen사의 NetScreen-5000은 VPN, 방화벽, 그리고 DiffServ 방식의 트래픽 관리 등을 지원하는 통합 보안 시스템의 예이다. 기능에 따라 6에서 12 Gbit/s 정도의 성능을 갖는다[3].

네트워크 시스템 벤더들은 그들의 기존 네트워크 제품에 보안 기능을 추가한 제품들을 출시하고 있다. 예를 들어, Cisco 사는 최근에 Cisco Catalyst 6500 스위치 시리즈를 위한 보안 모듈들을 선보였다. Catalyst 보안 모듈은 5 Gbit/s 대역폭을 갖는 방화벽과, 1.9 Gbit/s를 지원하는 VPN 서비스 모듈, 그리고 초당 2,500개의 커넥션을 지원하는 SSL 서비스 모듈을 포함하고 있으며, 또한 네트워크 트래픽 모니터링과 문제 해결을 위한 네트워크 분석 모듈의 기능도 갖는다.

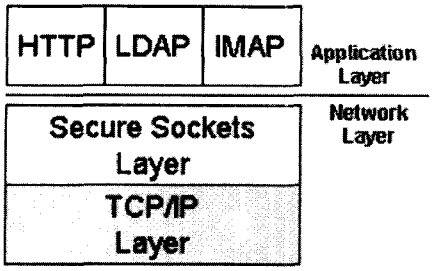
Ⅲ. 보안 프로토콜과 알고리즘

본 장에서는 인터넷을 통해 보내어지는 데이터의 기밀성과 근원지 및 목적지에 대한 인증과 관련한 보안 프로토콜 및 알고리즘에 대하여 살펴본다.

1. SSL(Secure Socket Layer)

SSL 프로토콜은 〔그림 4〕와 같이 어플리케이션 계층(Application layer)과 TCP/IP 계층(TCP/IP layer) 사이에 위치하며, http 같은 어플리케이션에 대한 서비스를 제공한다.

본 프로토콜은 암호화된 데이터의 교환 뿐 아니라 호스트에 대한, 필요할 경우에는 사용자에 대한, 인증(authentication)을 제공한다. SSL의 특징은 빠른



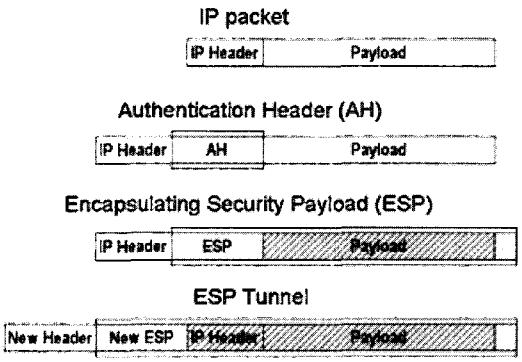
〔그림 4〕 네트워크 계층에서의 SSL의 위치

셋업과 안전한 연결이다. SSL은 대부분의 브라우저에 의해 지원되므로, 모든 웹 기반 클라이언트에게 적용될 수 있다. 신용 카드와 전자 거래 지원을 위해 개발되었으나, 지금은 VPN 어플리케이션으로도 사용되고 있다.

2. IPsec(IP Security)

IPsec은 당초 VPN 어플리케이션을 지원하기 위해 정의되었다. 이 네트워크 계층(Network layer) 보안 프로토콜은 상위 계층 어플리케이션들과 하부의 데이터 링크 계층(Data Link layer)에 투명성을 제공한다.

IPsec은 두 가지 모드를 제공하는데, 기존의 IP 헤더가 재사용되는 전송 모드(transport mode)와 TCP/IP 패킷 전체가 암호화되어 새로운 IP 헤더로 감싸지는 터널 모드(tunnel mode)가 그것이다. IPsec은 또한 AH(Authentication Header)와 ESP(Encapsulating Security Payload) 두 가지 프로토콜로 구성된다.



〔그림 5〕 IPsec 적용에 의한 패킷의 구성

3. 암호 알고리즘(Crypto API)

SSL과 IPsec 모두 각각 키 교환(key exchange), 인증(authentication), 암호화(encryption) 이렇게 세 가지 주 동작으로 구성된다. 암호화된 데이터가 전송되기 전에, 키 교환이 먼저 이루어져야 한다. 키 교환 프로토콜은 다수의 보안 협상(Security Association, SA)를 셋업하는데, 여기서 SA는 프로토콜, 목적지, 안전한 링크에 사용되는 보안 파라미터들을 정의하는 일 방향 협상이다. SSL 키 교환에 사용되는 주 암호 알고리즘은 RSA이다.

IPsec의 경우, IKE(Internet Key Exchange) 프로토콜이 사용된다. IKE는 Diffie-Hellman 키 교환 알고리즘에 기반하며 두 가지 동작 모드를 갖는다. 메인 모드(main mode)는 셋업과 데이터 교환에서 모두 SA를 사용하는 반면, 어그레시브 모드(aggressive mode) 또는 퀵 모드(quick mode)에서는 데이터 교환 시에만 SA를 사용한다.

근원지, 목적지, 또는 데이터에 대한 인증을 위해, DSA, MD5, 그리고 SHA-1 같은 여러 알고리즘들이 사용된다. IPsec은 여러 가지 벌크 암호화(bulk encryption) 알고리즘들을 정의하고 있지만, 3-DES가 가장 널리 사용되고 있다. 3-DES는 DES(Data Encryption Standard)를 세 번 적용한 것이다. 이를 대체할 수 있는 IPsec의 벌크 암호화 알고리즘은 비교적 최근에 고안된 AES(Advanced Encryption Standard)이다.

Ⅳ. 보안 프로세서의 성능 비교

성능 한계는 네트워크 보안의 폭넓은 구현을 막는 가장 큰 장벽이다. 모든 네트워크 환경에서 보안과 성능 사이에는 trade-off가 존재한다. 네트워크가 안전하게 구성되면 될수록, 각 패킷을 라우팅하는데 필요한 작업량은 크게 증가한다.

최근에 개발된 보안 프로세서들은 성능이 매우 좋을 뿐 아니라, 모든 보안 관련 프로세스들이 구현되어 있고, 호스트의 패킷 프로세싱 부하를 줄여주기도 한다. 이러한 높은 수준의 성능은 매우 큰 대역폭을 요구하는 네트워크 보안 솔루션 개발을 위한 필수 요소이다. 보안 프로세서는 성능 저하 없이 보안 기능들을 통합하는데 드는 비용을 현저하게 줄여줄 수 있다. 이는 암호 알고리즘들이 최적화되어 있는 실리콘 디바이스들이라 할 수 있다.

본 장에서는, 1 Gbit/s 또는 그 이상의 전송 속도에서 동작하는 보안 프로세서들에 대하여 그 성능을 비교한다. 위의 조건을 만족하는 제품들을 보유한 벤더들은 대략 다음과 같다.

- Broadcom Corp.
- Cavium Networks
- Corrent Corp.
- Hifn Inc.
- Layer N Networks Inc.
- Zyfer Inc.
- Intel Corp.
- NetOctave Inc.

Intel과 NetOctave는 위의 조건을 만족하는 제품들을 보유하고 있으나 여기서 다루는 성능 항목들에 대한 충분한 자료가 공개되어 있지 않으므로, 다른 여섯 벤더들의 제품만을 비교 대상으로 하였다.

1. 각 업체별 제품 현황과 주요 성능 비교

앞서 살펴본 것처럼 네트워크 보안에서 널리 사용되는 보안 프로토콜로는 SSL과 IPsec을 들 수 있다. 따라서 각 보안 프로세서 업체들도 이들을 지원하고 있다.

〔표 1〕은 업체별 제품 현황과 개별 제품들이 제공하고 있는 보안 프로토콜에 관한 비교 표이다.

〔표 1〕 보안 프로세서 별 지원 프로토콜

회사	제품명	제공프로토콜
Broad-Com	BCM5820 (A1)	SSL
	BCM5821 (A2)	SSL
	BCM5840 (A3)	IPsec
	BCM5841 (A4)	IPsec
Cavium	Nitrox CN1010 (B1)	SSL or IPsec
	Nitrox CN1220 (B2)	SSL or IPsec
	Nitrox CN1230 (B3)	SSL or IPsec
	Nitrox CN1330 (B4)	SSL or IPsec
	Nitrox+ CN1430 (B5)	SSL&IPsec
	Nitrox+ CN1540 (B6)	SSL&IPsec
	Nitrox I (B7)	SSL&IPsec
	Nitrox II (B8)	SSL&IPsec
Corrent	CR7020 (C1)	SSL or IPsec
	CR7120 (C2)	IPsec
HiFn	HIPP II 8065 (D1)	SSL
	HIPP II 8165 (D2)	SSL
	HIPP II 8154 (D3)	SSL&IPsec
	HIPP III 8300 (D4)	SSL&IPsec
	HIPP III 8350 (D5)	SSL&IPsec
LayerN	UltraLock (E1)	SSL
Zyfer	SKP-100 (F1)	SSL & IPse

이 표를 비교해보면 신생 업체인 Cavium은 최근의 시장 분위기를 반영하여 두 프로토콜을 모두 지원하고 있음을 알 수 있다. 하지만 각 프로토콜의 처리 기능들이 프로세서 내부적으로 할당되므로 두 프로토콜의 동시 처리 시에는 단일 프로토콜만을 처리할 때보다 성능이 저하되는 단점을 지닌다.

이에 반해 Corrent 7020 프로세서는 SSL이나 IPsec 중 하나만을 선별적으로 처리할 수 있도록 프로그래밍 될 수 있다.

〔표 2〕의 항목들은 성능 비교 중 가장 중요한 항목들이다. 다음과 같은 세 항목을 통해 각 제품들이 최대 성능을 낼 수 있게 된다.

다음 표를 가지고 비교할 때, SSL에서의 1024비트 서명 작업에 대한 초당 처리 개수와 IKE 메인 모드에서 초당 터널의 개수 및 3DES-CBC와 HMAC-SHA1의 알고리즘의 처리 성능 모두에서 Cavium이 타 업체를 앞서고 있는 것으로 나타난다.

〔표 2〕 제품별 처리 성능 비교

	SSL/RSA Transactions/Sec (1,024bit)	IKE/ Main Mode Tunnels/Sec	IPsec Bulk Encryption
A1	800	1,200	310 Mbit/s
A2	4,000	3,000	470 Mbit/s
A3	N/S	N/S	2.4 Gbit/s
A4	N/S	N/S	4.8 Gbit/s
B1	7,000	3,000	1 Gbit/s
B2	14,000	6,000	1.2 Gbit/s
B3	28,000	12,000	2 Gbit/s
B4	28,000	12,000	4 Gbit/s
B5	28,000	12,000	2 Gbit/s
B6	42,000	18,000	4 Gbit/s
B7	24,000	18,000	5 Gbit/s
B8	48,000	36,000	10 Gbit/s
C1	3,800	2,000	2.0 Gbit/s
C2	1,250	1,000	2.4 Gbit/s
D1	4,500	1,750	500 Mbit/s
D2	2,000	1,750	2 Gbit/s
D3	906	1,750	2 Gbit/s
D4	250	90	600 Mbit/s
D5	400	150	4 Gbit/s
E1	N/D	N/D	N/S
F1	N/D	N/D	2.5 Gbit/s

2. 디바이스 타입

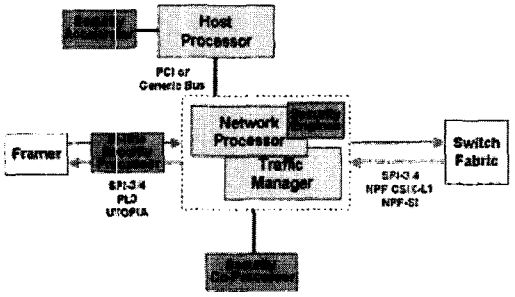
본 장에서는 보안 프로세서를 수행 기능에 따라 다음과 같이 네 가지 디바이스 타입으로 분류한다.

- 보안 가속기(Security Accelerator): 이 디바이스는 IPsec이나 IKE의 Diffie-Hellman 알고리즘에 대한 벌크 암호화를 구현한다. 보안 가속기는 IPsec이나 SSL의 속도를 높이기 위해 호스트 CPU나 네트워크 프로세서와 연동하여 사용된다.
- 보안 보조 프로세서(Security Co-Processor): 벌크 암호화뿐 아니라, SSL이나 IPsec의 헤더 프로세싱도 구현한다. 본 디바이스는 네트워크 프로세서와 함께 사용되며 일반적으로 어떠한 데이터가 디바이스를 오고 가는지를 파악하는 Look-Aside 인터페이스를 갖는다.
- 인라인 보안 프로세서(In-line Security Processor): 한쪽에서는 본래의 패킷을 송수신하고, 다른 한쪽에서는 암호화된 패킷을 송수신한다. 즉, BITW(Bump In The Wire) 형태로 구현되며, 통합된 이더넷 MAC을 포함한다.
- 보안 엔진(On-Chip Security Engine)의 칩상 구현: 최근 제품들은 벌크 암호화 엔진을 일반 네트워크 프로세서에 포함시킨다. Intel IXP-2850은 IXP-2800의 변형된 제품으로, 기존의 패킷 엔진들 뿐 아니라 다수의 암호 관련 엔진들도 포함하고 있다. 앞에서도 언급하였듯이, 본 디바이스의 암호 관련 성능은 공개되지 않았으므로, 표에는 포함시키지 않았다.

〔표 3〕 제품별 디바이스 형태

	Device Type
A1	Security Accelerator
A2	Security Accelerator
A3	Security Accelerator
A4	Security Accelerator
B1	Security Co-Processor
B2	Security Co-Processor
B3	Security Co-Processor
B4	Security Co-Processor
B5	Security Co-Processor
B6	Security Co-Processor
B7	In-Line Security Processor
B8	In-Line Security Processor
C1	Security Co-Processor
C2	In-Line Security Processor
D1	Security Co-Processor
D2	Security Co-Processor
D3	Security Co-Processor
D4	In-Line Security Processor
D5	In-Line Security Processor
E1	In-Line Security Processor
F1	In-Line Security Processor

〔그림 6〕은 라인 카드에서의 각 타입 디바이스들 - 가속 보안기, 보안 보조 프로세서, 인라인 보안 프로세서, 보안 엔진의 칩상 구현 - 의 위치를 보여준다.

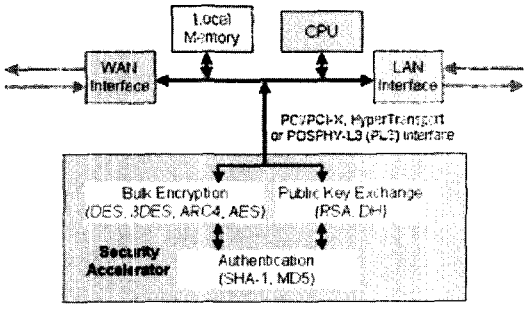


〔그림 6〕 보안 프로세서의 디바이스 타입

2.1 보안 가속기

〔그림 7〕은 벌크 암호화, 공개키 교환, 인증 블록들을 포함한 보안 가속기를 보여주고 있다.

각 블록은 암호 엔진들을 포함하고 있다. 보안 가속기는 PCI나 PCI-X 버스, 또는 HyperTransport



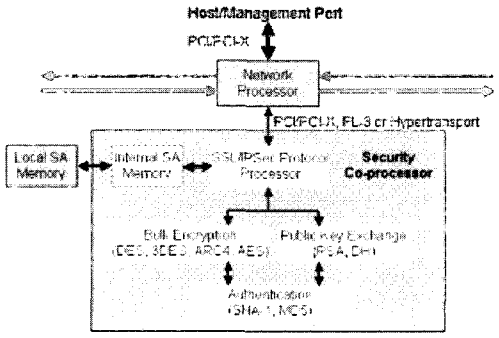
〔그림 7〕 보안 가속기 구조

나 POSPHY 레벨 3 인터페이스를 통해 호스트 CPU와 연결되어 있다. 패킷들은 WAN을 통해 수신되고 CPU에 의해 처리된다. CPU는 보안 가속기에게 필요한 암호 함수들을 요청한다. CPU는 보안 가속기가 필요로 하는 모든 파라미터들을 데이터와 함께 전송한다. 위의 예는 보안 기능들을 가속하기 위한 단순한 접근 방식이지만, 모든 보안 프로토콜 프로세싱이 호스트 CPU에서 이루어지고 암호화 패킷들이 버스를 통해 빈번히 지나다니게 되므로, 성능은 제한된다.

2.2 보안 보조 프로세서

보안 보조 프로세서는 [그림 8]에서도 보듯이, 벌크 암호화, PKI, 인증 블록 뿐 아니라, SSL과 IPsec 프로세싱 함수들도 포함하고 있다. 보안 보조 프로세서는 Look Aside 인터페이스를 가진 네트워크 프로세서와 주로 사용된다. 인터페이스는 PCI, PCI-X, HyperTransport, 또는 POSPHY-L3 등이다.

보안 보조 프로세서는 IPsec 프로토콜과 SSL 기록들을 다루기 위한 프로토콜 프로세서를 포함하고 있다. 프로토콜 프로세서는 SA(Security Association)를 다룰 필요가 있다. SA들은 로컬하게 저장되거나 패킷 단위로 네트워크 프로세서로부터 전송될 수 있다. 로컬 SA들은 칩 상의 메모리나 외부 메모리에 저장된다. 지원되는 로컬 SA의 개수는 사용 가능한 메모리 양에 좌우된다.



[그림 8] 보안 보조 프로세서 구조

[표 4]는 로컬 SA 저장을 위해 사용되는 메모리 타입과 로컬 SA와 칩상 SA 모두를 지원하는 SA의 개수를 보여준다.

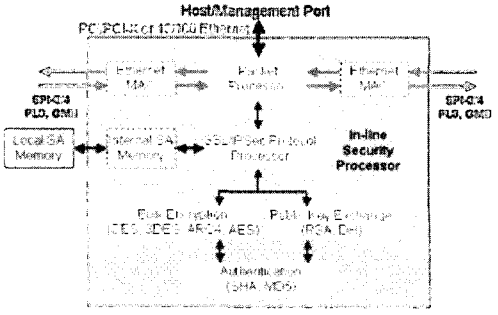
Cavium, Corrent, Hifn 등은 보안 보조 프로세서 제품을 보유하고 있다. Cavium Nitrox+ 디바이스는 [표 4]의 마지막 항목에서 보듯이 트래픽 우선 순위와 타입에 따른 대역폭 할당을 지원한다.

[표 4] 보안 보조 프로세서 타입의 성능 비교

	On-chip	Local Memory	Local SA	Band-width Allocation
A1	None	None	None	No
A2	None	None	None	No
A3	2,048	None	2,048	No
A4	None	Nome	None	No
B1	None	DDR DRAM	4M	No
B2	None	DDR DRAM	4M	No
B3	None	DDR DRAM	4M	No
B4	None	DDR DRAM	4M	No
B5	None	DDR DRAM	4M	Yes
B6	None	DDR DRAM	4M	Yes
B7	None	DDR DRAM	4M	Yes
B8	None	DDR DRAM	4M	Yes
C1	None	DDR SDRAM	Yes	No
C2	None	DDR SDRAM	Yes	No
D1	None	SDRAM	N/D	No
D2	None	SDRAM	N/D	No
D3	200	SDRAM	N/D	No
D4	200	SDRAM	256K	No
D5	None	SDRAM	256K	No
E1	256	DDR SDRAM	N/D	No
F1		N/D	1M	No

2.3 인라인 보안 프로세서

[그림 9]에서 보듯이 인라인 보안 프로세서들은 한 쪽에서는 기존 패킷들을 송수신하고, 다른 한 쪽에서는 암호화된 패킷들이 송수신된다. 이 디바이스는,



[그림 9] 인라인 보안 프로세서 구조

예를 들면 한쪽에는 IPsec 또 다른 한쪽에는 IP, 이렇게 프로토콜 기반이어야 한다(BITW 방식).

인라인 보안 프로세서는 모든 패킷 프로세서를 포함한다. LayerN의 UltraLock 같은 제품은 TCP/IP 패킷 프로세서를 포함하기도 한다. TCP/IP 스택을 구현함으로써, 이 디바이스는 전체 SSL 프로세싱의 로드를 줄이는 프록시 호스트의 역할을 하게 된다.

3. 제품별 세부 특징

모든 보안 프로세서의 핵심은 암호 엔진이다. 엔진들을 병렬적으로 추가하면 성능이 향상된다. 암호 엔진에는 고정 기능(fixed function) 엔진과 프로그래밍 가능(programmable) 엔진 두 가지 타입이 있다.

고정 기능 엔진은 특정 알고리즘들을 통해 최적화되며 실리콘을 사용한다. 고정 기능 엔진을 장착한 보안 프로세서는 타입과 포함된 각 엔진의 수에 따라 한개 또는 두개의 어플리케이션으로 제한된다.

〔표 5〕 제품별 세부 특징-1

	Programm-able?	256-bit AES encryption	Network header Processing
A1	No	No	No
A2	No	No	No
A3	No	No	Yes
A4	No	Yes	Yes
B1	Yes	Yes	Yes
B2	Yes	Yes	Yes
B3	Yes	Yes	Yes
B4	Yes	Yes	Yes
B5	Yes	Yes	Yes
B6	Yes	Yes	Yes
B7	Yes	Yes	Yes
B8	Yes	Yes	Yes
C1	No	Yes	No
C2	Yes	Yes	Yes
D1	Yes	Yes	Yes
D2	Yes	Yes	Yes
D3	Yes	Yes	Yes
D4	Yes	Yes	Yes
D5	Yes	Yes	Yes
E1	No	Yes	Yes
F1	Yes	128bit	Yes

프로그래밍 가능 암호 엔진은 업체들에 의해 제공되는 코드를 사용하는 어떤 알고리즘도 지원 가능하다. 보안 프로세서가 출시된 후에는 언제라도 새 알고리즘을 추가할 수 있다. 암호 엔진에 대한 프로그래밍은 디바이스별, 그룹별, 또는 단독 엔진별로 수행될 수 있다.

〔표 5〕에서 보듯이 대부분의 제품들은 프로그래밍이 가능하다. 예외는 Broadcom사의 하드 코딩된 보안 가속기들과 Corrent사의 CR7020, 그리고 LayerN 사의 UltraLcok 등이다. 보안 프로세서는 RSA와 Diffie-Hellman 키 교환 뿐 아니라 3 DES와 ARC 4 벌크 암호화도 구현한다. 인증을 위해서는 SHA와 MD-5를 지원한다. Broadcom 사의 제품은 AES 역시 지원한다. Hifn사의 HIPP

〔표 6〕 제품별 세부 특징-2

	IO Type	IO Bandwidth	In-Line or Look-aside
A1	PCI	2.1 Gbit/s	Look-aside
A2	PCI	2.1 Gbit/s	Look-aside
A3	PL3	4.2 Gbit/s	Look-aside
A4	PL3/FIFO	6.4 Gbit/s	Look-aside
B1	PCI	2.1 Gbit/s	Look-aside
B2	PCI or PCI-X	2.1 or 4.2 Gbit/s	Look-aside
B3	PCI or PCI-X	2.1 or 4.2 Gbit/s	Look-aside
B4	Hyper transport	6.4 Gbit/s	Look-aside
B5	PCI/PCI-X	2.1 or 4.2 Gbit/s	Look-aside
B6	Hyper transport	6.4 Gbit/s	Look-aside
B7	1xSPI-3 or 2xSPI-3	4 or 8 Gbit/s	In-Line
B8	1xSPI-4.2 or 2xSPI-4.2	12 or 24 Gbit/s	In-Line
C1	PL3/PCI-X	6.4 Gbit/s	Look-aside
C2	PL3	6.4 Gbit/s	Both
D1	PL3 or 32/64bits PCI	6.4 Gbit/s	Look-aside
D2	PL3 or 32/64bits PCI	6.4 Gbit/s	Look-aside
D3	PL3 or 32/64bits PCI	6.4 Gbit/s	Look-aside
D4	GMII	6 Gbit/s	In-Line
D5	GMII	8 Gbit/s	In-Line
E1	GMII	4 Gbit/s	In-Line
F1	PL3	10 Gbit/s	In-Line

III 같은 보안 프로세서는 헤더 프로세싱을 지원하는데, 이는 모든 IPsec과 SSL 프로토콜을 수행한다는 의미이다.

〔표 6〕은 In-Line/Look Aside 설정과 I/O 타입, 그리고 주요 패킷 인터페이스의 대역폭을 보여주고 있다. 대역폭은 모든 패킷 인터페이스의 전체 대역폭이다.

대부분의 인라인 디바이스들은 POSPHY 레벨 3이나 SPI-4 인터페이스를 가지고 있다. 〔표 7〕에서 보듯이 통합 이더넷 MAC을 포함하는 Hifn HIPP III 같은 디바이스는 기가비트 이더넷 GMII 인터페이스를 지원한다.

보안 보조 프로세서나 인라인 보안 프로세서는 분리된 호스트 인터페이스를 갖는다. 이러한 인터페이스는 통합 이더넷 MAC을 갖는 PCI, PCI-X 또는 MII 등이다.

〔표 7〕 제품별 세부 특징-3

	MAC	Host Interface
A1	No	None
A2	No	None
A3	No	None
A4	No	None
B1	No	None
B2	No	None
B3	No	None
B4	No	None
B5	No	None
B6	No	None
B7	Yes	PCI 64/56
B8	Yes	PCI 64/56
C1	No	PCI-X
C2	No	PCI
D1	No	PCI
D2	No	PCI
D3	No	PCI
D4	3 GE	MII
D5	4 GE	MII
E1	2 GE	MII
F1	No	PCI

대부분의 벤더들은 자신들의 칩에 연동 가능한 제품 보드를 제공한다. 〔표 8〕은 OEM 보드를 보유하고 있는지 여부와 샘플로 사용 가능한지 여부 등을

〔표 8〕 제품별 세부 특징-4

	OEM board?	Sample Availability	Network header Processing
A1	Yes	Production	4W
A2	Yes	Production	.8W
A3	No	Production	3W
A4	No	Sampling	3W
B1	Yes	Production	2.8W
B2	Yes	Production	1W
B3	Yes	Production	4W
B4	Yes	Production	5W
B5	Yes	Production	5W
B6	Yes	Production	5W
B7	Planned	Jan. 2003	7W
B8	Planned	Jan. 2003	8W
C1	Yes	Production	10W
C2	Yes	Production	4W (Max)
D1	No	Production	6W (Max)
D2	No	Production	N/D
D3	No	Production	N/D
D4	No	Q2 2003	N/D
D5	No	Q2 2003	N/D
E1	No	Q1 2003	N/D
F1	Yes	N/D	N/D

나타낸다. 그리고 마지막 항목은 메모리를 배제한 전력 소비량을 나타내었다. 본 항목의 경우 몇몇 업체는 일반적인 전력 소비를 표기하고 있는 반면, 또 다른 업체들은 최대 소비 전력을 표기하고 있으므로, 이를 정확히 비교하는 것은 쉽지 않다.

V. 결 론

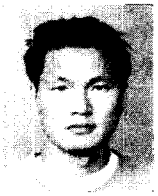
네트워크 보안 시장을 주도하는 VPN, 방화벽, 침입탐지시스템 등의 보안 장비들에 대해 간략하게 알아보았고, 이에 필요한 요소 기술들을 살펴보았으며, 이를 토대로 현재 출시되고 있거나 곧 출시될 예정인 보안 프로세서들을 고찰하였다. 각 보안 프로세서들에 대하여, 성능과 통합 수준, 가용성, 특징, 그리고 전력 등의 항목에 대하여 서로 비교하였다. 위와 같은 비교는 모든 장비에 대하여 동일한 환경에서 비교한 것이 아니므로, 위의 비교 내용을 전적으로 믿고, 우수하고 우수하지 않는 제품을 결정한다

는 것은 무리라고 판단된다. 여기에서는 보안 프로세서에 대하여 비교할만한 항목들을 도출하였다는데 그 의미를 찾는 것이 좋을 것이며, 본 항목들에 대한 비교를 통해 각 환경에 적합한 보안 프로세서를 선택하는 것이 좋을 것으로 생각된다.

참 고 문 헌

[1] Infornetics Inc., "www.infornetics.com".
[2] Security Processors, "www.lightreading.com/document.asp?doc_id=28307&print=true," 2003.
[3] NetScreen Technologies, Inc., "www.netscreen.com",

〈著 者 紹 介〉



이 상 수 (Sangsu Lee) 비회원

1999년 2월 : 경북대학교 전자공학과 졸업
2001년 2월 : 경북대학교 전자공학과 석사학위 취득
2001년 3월~현재 : 한국전자통신연구원 연구원 재직중
〈관심분야〉 정보보호, 네트워크 보안, Optical Security

김 영 수 (Youngsoo Kim) 비회원

1998년 2월 : 성균관대학교 정보공학과 졸업
2000년 2월 : 성균관대학교 컴퓨터공학과 석사학위 취득
2000년 2월~현재 : 한국전자통신연구원 연구원 재직중
관심분야 : 암호이론, 네트워크 보안

한 종 욱 (Jongwook Han) 비회원

1989년 2월 : 광운대학교 전자공학과 졸업
1991년 2월 : 광운대학교 전자공학과 석사학위 취득
2001년 2월 : 광운대학교 전자공학과 박사학위 취득
1991년 2월~현재 : 한국전자통신연구원 연구원 재직중
관심분야 : VPN System, Network Security, Optical Security

정 교 일 (Kyoil Chung) 종신회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 8월 : 한양대학교 산업대학원 전자계산학과 석사학위 취득
1997년 8월 : 한양대학교 대학원 전자공학과 박사학위 취득
현재 : 한국전자통신연구원 정보보호기반연구부 부장
관심분야 : IC Card, 보안, Biometrics, 국가기반보호, 신호처리

손 승 원 (Seongwon Sohn) 비회원

1984년 2월 : 경북대학교 전자공학과 졸업
1994년 2월 : 연세대학교 전자공학과 석사학위 취득
1999년 2월 : 충북대학교 컴퓨터공학과 박사학위 취득
현재 : 한국전자통신연구원 네트워크보안연구부 부장
관심분야 : 네트워크, 네트워크 보안