고속 네트워크보안 시스템설계를 위한 암호프로세서의 성능 분석

김정태*, 류대현, 허창우
목원대학교, 한세대학교, 목원대학교

Hardware Architecture Analyses of Performance of Crypto-processor for High-speed Network Security System

Jung-Tae Kim, Dae-Hyun Ryu, Chang-woo Hur
Mokwon University, Hansei University, Mokwon University
E-mail : jtkim5068@hanmail.net

요 약

고속의 수십기가급의 VPN을 구현할 수 있는 제품은 방화벽시스템(Firewall), 라우터, 인터넷 게이트웨이, 원격 접속 서버(Remote Access Server), Windows NT Server, VPN 전용 장치 그리고 VPN 소프트웨어 등을 들 수 있지만, 현재까지 어떤 제품 그리고 기술도 지배적인 방법으로 대두되지는 않고 있다. 국내외적으로 수십Giga급 이상의 VPN 보안장비와 관련된 체계화된 이론의 부족으로 인하여 관련된 연구는 많이 부족한 현실이며, 체계적이고 전문적인 연구를 수행하기 위해서는 많은 연구활동이 필요하다. 결과적으로 향후 차세대 초고속 네트워크에서의 정보보호와 효과적인 네트워크 자원을 활용하기 위해서는 반드시 수십Giga급 이상의 VPN 보안장비에 대한 연구가 활발히 진행되리라 예상된다. 따라서 본 논문에서는 수십Giga급의 고속 정보보호시스템 구현 시 반드시 필요로 되는 암호화 칩의 성능을 비교 분석하고, 가능성을 제시한다.

Ⅰ. 서 론

네트워크의 속도는 날로 증가하고 있으며, 파생되는 서비스와 인터넷의 영향력은 더욱 커질 것으로 기대된다. 이로 인해 정보보호 분야는 이러한 변화 속에서 가장 주목받는 분야중의 하나가 될 것이며, 그 중에서도 암호학 이라는 수학적 배경에 의해 검증된 보안 솔루션인 VPN은 더욱 중요한 영역이 될 것이 분명하다. 현재에도 많은 군, 국가기관을 비롯한 많은 금융권과 산업체에서 VPN 솔루션을 도입했거나 도입을 고려하고 있으며, 선진국의 선도 업체들도 진보된 네트워크 환경과 고속의 네트워크 환경에 적합하도록 더 고성능의 제품을 만들기 위해 전력을 다하고 있다. 근래에 폭발적으로 보급된 초고속 인터넷 망의 덕택으로 인해 오늘날 우리 사회는 온라인상으로 정보를 손쉽게 주고받을 수 있게 되었을 뿐만 아니라, 온라인 전자 금융 거래를 비롯한 새로운 패러다임의 변화가 발생하게 되었다. 하지만 이러한 이면에는 개인 정보 유출, 전자 금융 거래 사고와 같은 새로운 사회적 문제가 대두되었으며, 이러한 문제점들을 미연에 방지할 수 있는 각종 정보보호 기술들이 요구되고 있다. 이러한 배경에서 방화벽(Firewall), 침입탐지 시스템(IDS), 가상사설망(VPN)과 같은 다양한 보안 솔루션들이 등장하게 되었으며, 최근 군, 국가 기관, 금융권과 산업계 등에서 그 수요가 끊이지 않고 발생하고 있다. 특히 IDC는 2005년에는 모든 인터넷 트래픽이 암호화되는 수준으로 발전할 것이라 예측하고 있다. 물론 하드웨어의 미래는 아직도 불투명하긴 하지만, PC에 암호 연산 프로세서가 기본적으로 탑재되는 날도 멀지 않을 것으로 예측하고 있다. 이러한 측면에서 볼 때 VPN 시장의 미래는 매우 밝은 편이며, 국외적으로도 국내적으로도 많은 업체들이 제품을 개발하여 시판하고 있다.

Ⅱ. 암호프로세서의 기술동향

기존에 개발된 VPN 장비들은 대부분 소프트웨

어적으로 구현되어 있다. 소프트웨어 방식의 VPN 장비는 성능 측면에서 피할 수 없는 한계점을 갖는다. 최근 100 Mbps LAN이 이미 보편화된 네트워크 환경에서, 소프트웨어 기반의 VPN 장비는 하위 계층의 물리적 네트워크가 제공하는 대역폭을 충분히 지원하지 못한다. 또한 장비 내에서 패킷처리를 담당하는 프로세서의 계산 능력 중 대부분이 대량의 패킷을 일일이 암·복호화하는 과정에 소요되기 때문에 QoS, 멀티캐스팅 지원 등의 부가적인 서비스를 제공하는데 한계점을 보이고 있다. 따라서 하드웨어 기반의 VPN은 현재 네트워크 상황을 감안할 때 시장에서 경쟁력 있는 제품이 되려면 반드시 선택해야 하는 사항이다. 한편 현재 하위 물리적 네트워크 계층이 제공하는 대역폭을 완전히 지원하는 것 뿐 아니라, 추후 대역폭 증가를 감안할 수 있는 구조가 요구된다. 하드웨어 VPN 장비를 구현하는데 있어서 가장 신중하게 다루어야 할 요소는 암호화와 패킷 처리를 담당하는 보안 프로세서를 어떻게 선정하고, 충분한 처리 능력을 보장하기 위해서 전체 시스템 구조를 어떻게 설계할 것인가 하는 점이다. 현재 보안 프로세서 시장을 대부분 차지하고 있는 메이저 업체들은 Hifn, Cavium과 BroadCom을 비롯한 국외 업체들이다. <표1>에서 보이는 바와 같이 국내에도 초창기에는 여러 업체들이 암호연산 프로세서를 개발하였으나, 성능이 워낙 열악하고 시장성이 없었기 때문에 성능에 대한 자료가 불충분하며, 시간이 지나도 성능에 대한 향상이 거의 이루어지지 않고 있는 실정이다. 반면에 해외 업체들의 뛰어난 보안프로세서를 이용하여 우수한 하드웨어 기반의 VPN 장비를 개발하려는 시도는 국내의 몇몇 선도 업체에 의해서도 시작되었었다. 그러나 미비한 시장성과 개발 기술의 난이도, 전문 개발 인력의 부족 등으로 말미암아 차세대 네트워크 환경에 적합한 하드웨어 VPN 장비가 국내에서 개발되어 보고 된 예는 현재까지 없다. 고성능 보안 프로세서를 이용하여 수십Giga급의 성능을 낼 수 있는 하드웨어 VPN 장비를 구현할 때 제일 먼저 고려해야 할 점은 현존하는 다양한 보안 프로세서 중 어느 것을 선정하여 구현에 적용할 것인가 하는 점이다. 그 밖에도 시스템의 고 효율성을 위해 채택해야 할 하드웨어 구조, 각 구조별 구현에 소요되는 개발 기간 등을 고려하여 시스템을 디자인하여야 한다.

<표1> 국내 암호 연산 프로세서 제품 기능 및 성능

회사명/제품명	암호함수		성능	
	대칭키	공개키	대칭키	공개키
시큐어피아 (Crypto Engine)	SEED, DES, 3DES, AES	■	SEED(246Mb), DES(3DES(107Mb),AES(256Mb)	■
시큐어아이티 (지문인식 스마트카드)	■	■	■	■
아라리온(Cipher)	DES, SEED, 3DES	■	DES(50Mb)	■
퓨처시스템 (Secureway Gate 200)	3DES, RC5, CAST(128), Blowfish, Crypton	■	-	■
텔레시큐어(CNISTTM)	128bIT ENC Alg	■	5 Mb with 5V	■
시큐어테크놀러지 (암호프로세서, SOC101)	■	RSA	■	RSA(124Kbits/s)
시큐어테크놀러지 (암호프로세서 SOC, CryptoXL)	DES. SEED. 3DES. RC4 HASH (SHA1MD6)	■	SEED(200Mb), DES(245Mb), 3DES(80Mb)	■

"■" 지원되지 않음을 표시
"-" 해당되는 자료가 없음

III. 기술현황 분석

고속 VPN 장비 구현에는 하드웨어적으로 빠른 암호화 처리를 할 수 있는 보안 프로세서가 필수적이다. 현재 시장에서 많은 호응과 관심을 끄는 외국 제품과 벤더들은 다음과 같다. 각 보안 프로세서로는 SSL이나 IPSec, 또는 두가지 프로토콜 모두를 지원하기도 한다. 예를 들어 Cavium사의 Nitrox II는 SSL, IPSec 모두를 지원하며 이 밖에도 WEP 프로토콜도 지원하고 있으나, 내부적으로 자원들이 각 프로토콜마다 할당되므로 둘을 동시에 사용할 시 성능이 저하된다. 반면에 Corrent 사의 제품은 SSL이나 IPSec 둘 중 하나만을 지원하고 있다. 보안 프로세서의 성능은 크게 다음과 같이 세가지 메트릭에 의하여 측정된다.

1) 초당 SSL RSA Transactions 처리능력 2) IKE Main model Tunnel 생성능력 3) IPSEC Bulk Encryption 능력.

<표2> 보안 프로세서 벤더와 특징

회사	제품	특징
Broadcom	BCM5820	☞ 터널링 기법 사용하여 WAN 구간 보호 ☞ 터널간의 스위칭 기법 사용 ☞ 대규모의 터널과 고속의 터널간의 접속에 유리
Cavium	Nitrox CN1010 Nitrox CN1220 Nitrox CN1230 Nitrox CN1430 Nitrox CN1540	☞ 내부적으로 다수개의 암호화 엔진이 장착됨 ☞ 초당 IKE 터널 생성 능력과 초당 Bulk Encryption 성능이 가장 뛰어나다. ☞ IPSEC, SSL, WEP 등 다수개의 프로토콜에 대해서 동시에 처리가 가능하다.
Corrent	MAX TNT & Pipeline	☞ TAOS를 통하여 multi-protocol access와 라우팅 처리 ☞ L2TP 및 PPTP 터널링 프로토콜 지원 ☞ Secure Access Firewall, IPSec을 통하여 보안 기능 처리
Hifn	2210, 2212, 2216 Router	☞ 전용 회선이나 프레임 릴레이 서버 없이도 SNA 트래픽 캡슐화 가능

Layer N	FortKnox Policy Router	☞ Firewall, VPN, 대역폭 관리를 단일 제품으로 구현 가능 ☞ 대역폭 관리 기능으로 네트워크간의 통신 대역폭을 효율적으로 조절 가능
Zyfer	Cisco 1720	☞ WAN 인터페이스를 모듈 형태로 지원 ☞ WAN Access, Firewall, IPSec VPN을 통합한 제품

<표3> 보안 프로세서별 처리 성능

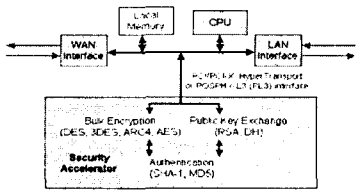
Product Name	SSL RSA Transactions per Second(1,024 bit)	IKE Main Mode Tunnels per Second	IPsec Bulk Encryption
BCM5820	800	1,200	310 Mbit/s
BCM5820	4,000	3,000	470 Mbit/s
BCM5820	N/S	N/S	2.4 Gbit/s
BCM5820	N/S	N/S	4.8 Gbit/s
Nitrox CN1010	7,000	3,000	1 Gbit/s
Nitrox CN1220	14,000	6,000	1.2 Gbit/s
Nitrox CN1230	28,000	12,000	2 Gbit/s
Nitrox CN1330	28,000	12,000	4 Gbit/s
Nitrox+ CN1430	28,000	12,000	2 Gbit/s
Nitrox+ CN1540	42,000	18,000	4 Gbit/s
Nitrox I	24,000	18,000	5 Gbit/s
Nitrox II	48,000	36,000	10 Gbit/s
CR7020	3,800	2,000	2.0 Gbit/s
CR7120	1,250	1,000	2.4 Gbit/s
HIPP II8065	4,500	1,750	500 Mbit/s
HIPP II8165	2,000	1,750	500 Mbit/s
HIPP II8154	906	1,000	2 Gbit/s
HIPP II8300	250	90	600 Mbit/s
HIPP II8350	400	150	4 Gbit/s
UltraLock	N/D	N/D	N/S
SKP-100	N/D	N/D	2.5 Gbit/s

<표3>에서 보이는 바와 같이 현재 발표된 프로세서 중에서는 Cavium사에서 발표한 제품이 10Gbps/s로 가장 우수한 성능을 보이고 있다.

나. 보안 프로세서의 네가지 사용 형태

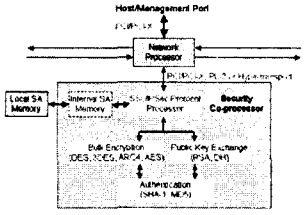
각 보안 프로세서는 VPN 시스템 내에서 담당하는 역할과 구조에 따라 다음과 같이 4가지 형태로 분류되어 질 수 있다.

- Security Accelerator: 이 보안 프로세서는 IPSec이나 IKE의 Diffie-Hellman 알고리즘에 대한 단순 벌크 암호화를 구현한다. 호스트 CPU나 네트워크 프로세서에서 암호화를 진행할 때 걸리는 오버헤드를 보안 프로세서가 떠맡는 역할을 한다. 일반적으로 Security Accelerator는 벌크 암호화, 공개키 교환, 인증 블록들을 포함하고 있으며 PCI, PCI-X버스 또는 Hyper Transport나 POSPHY 레벨3 인터페이스를 통해 호스트 CPU와 연결된다. CPU는 보안 프로세서를 구동할 때에는 필요한 데이터와 파라메터들을 버스를 통해 전송하면, 보안 프로세서는 그 처리결과를 DMA를 이용하여 메인 메모리에 올려놓고 호스트 CPU에 보고한다.



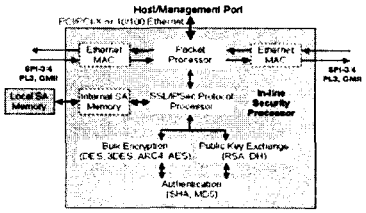
<그림1> ecurity Processor

- Security Co-Processor: 단순한 벌크 암호화 기능 이외에도 IPSec이나 SSL의 헤더 프로세싱도 같이 처리한다. 일반적으로 네트워크 프로세서와 같이 사용되며, Look-Aside 구조에서 사용되기 적합하다. 구체적으로 이 프로세서는 벌크 암호화, PKI, 인증블록, SSL, IPSec 헤더 처리 기능을 가진다. 인터페이스는 PCI, PCI-X, Hyper-Transport 또는 POSPHY-L3 등이 사용된다. 이 범주에 속하는 보안 프로세서로는 Broadcom의 BCM5820, BCM5821, BCM5840, BCM5841과 Cavium의 Nitrox, Nitrox+ 시리즈의 칩과 Nitrox I, Nitrox II 그리고, Hifn의 8065, 8165, 8154, 8300, 8350 등의 칩이 해당된다. 이중에서 Cavium의 Nitrox+ 칩은 대역폭 할당을 지원한다.



<그림2> Security Co-processor

- In-line Security Processor: 한쪽에서는 암호화 이전의 패킷이 송수신되고, 다른 한쪽에서는 암호화된 패킷이 송수신되는 BITW(Bump In The Wire) 구조에서 사용된다. 패킷이 암호화되자 마자 통합된 이더넷 MAC이나 SPI 인터페이스를 통하여 다음 단계에 전달이 된다.



<그림3> In-line Security Processor

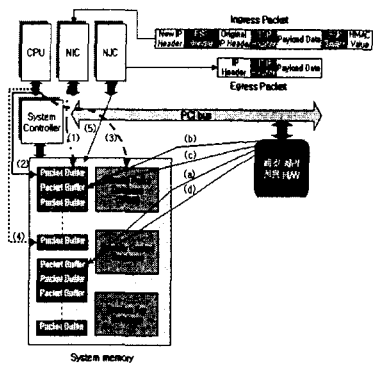
- On-Chip Security Engine: Intel의 IXP-2850 같은 제품은 기존의 패킷 엔진뿐만이 아니라 암호 가속 엔진들도 포함하고 있다. 따라서 벌크 암호화

엔진이 네트워크 프로세서 내에 있기 때문에 구조적으로는 가장 효율적인 형태라고 볼 수 있다.

다. VPN 시스템 구조

보안 프로세서가 사용된 VPN 시스템은 구현 방법에 따라 크게 Look-aside 구조와 Flow-through 구조가 있다. Look-aside 구조는 Ingress Packe (들어온 패킷)이 네트워크 프로세서나 호스트 CPU를 통해서 메모리에 저장되고 암복호화 프로세싱이 필요하면 보안 프로세서에 의해서 처리된 다음 다시 메모리에 저장되고 네트워크 프로세서나 호스트 CPU에 의해서 출력된다. 이 경우, 다음 <그림 4>에서 보이는 바와 같이 모든 패킷이 인터페이스 버스를 4번 이동하므로 데이터 전송 버스가 성능의 Bottleneck이 되는 경향이 있다. 특히, PCI-X 버스의 경우에는 8.5Gbps/sec (64bit * 133Mhz)가 최대 데이터 전송량인데, 각 패킷이 4번 이동해야 하므로 최도 2.5 Gbps 이상의 성능을 얻기가 불가능해 진다.

반면에 Flow-through 구조는 Look-aside 구조의 성능 문제를 해결하기 위해 네트워크 프로세서와 보안 프로세서 사이에 복잡한 데이터 전송 과정이 없기 때문에 높은 성능을 낼 수 있으나, 구현이 어려운 단점이 있다. 특히, 이 구조에 사용될 보안 프로세서는 네트워크 프로세서가 제공하는 패킷 프로세싱 기능, 패킷 프로토콜 처리 기능 등을 제공하여야 한다. 비교적 높은 암복호화 성능을 가진 Hifn8154나 Cavium Nitrox II 프로세서는 현재 Look-aside나 Flow-through 두 구조 모두 설계 가능하다. 하지만, Look-aside 구조는 내부 인터페이스 버스를 이용해서 데이터를 빈번하게 송수신 하



<그림4> Look-aside 구조에서의 패킷 흐름도

여야 하므로, 고속 VPN 구조에는 부적절하다. 특히 수십 Gbps를 지향하는 VPN 시스템에서는 매우 많은 데이터가 버스를 통해서 흘러가야 하므로 Flow-through 구조가 바람직하며, 현재 10Gbps 암복호화 성능을 가진 Nitrox II 프로세서의 경우에도 Flow-through 구조가 적합한 구조라고 밝히고 있다.

IV. 결 론

본논문에서는 수십Giga급 이상의 VPN 보안장비의 개발에서 필요로 하는 여러 가지의 요소 기술 등을 분석하고 실제적으로 구현 가능한 시스템의 구조적인 측면에서 연구를 하였다. 이러한 하드웨어 기반의 고속 VPN 설계 시술은 향후 수십 기가급의 통신망에서의 정보보호를 위해 중요한 수단이 되므로 이에 대한 집중적인 연구가 필요하리라 본다.

참고 문헌

[1] 주학수 외2인, "고속 암호연산 프로세서 개발현황", 정보보호학회지, 제12권 3호, 2002
[2] 이계상, "IPsec 표준화 동향", KISA 동향특집, 2000, 8.
[3] "8154 HIPP II Security Processor", http://www.hifn.com
[4] http://www.lightreading.com