임호모듈을 내장한 네트워크프로세서를 이용한 고속 VPN 시스템 설계

김정태*

Design of High-speed VPN System for Network Processor with Embedded Crypto-module

Jung-Tae Kim*

요 약

본 논문에서는 임베디드 암호모듈을 내장한 네트워크프로세서의 고속 VPN 설계 방법에 대해서 알아본다. 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 연구 활동이 필요하다. 결과적으로 향후 차세대 초고속 네트워크에서의 정보보호와 효과적인 네트워크 자원을 활용하기 위해서는 반드시 수십Giga급 이상의 VPN 보안장비에 대한 연구가 활발히 진행되리라 예상된다.

ABSTRACT

Various research groups proposed various architecture of hardware VPN for the high performance VPN system. However, the VPN based on hardware researcher are focused only on the encryption acceleration. Soft based VPN is only useful when the network connection is slow. We have to consider the hardware performance (encryption/decryption processing capability, packet processing, architecture method) to implement hardware based VPN. In this paper, we have analysed architecture of hardware, consideration and problems for high-speed VPN system, From the result, we can choose the proper design guideline

키워드

가상사설망, 네트워크프로세서, 광대역통신망

I. 서 론

최근에 폭발적으로 보급된 초고속 인터넷 망의 덕택으로 인해 오늘날 우리 사회는 온라인상으로 정보를 손쉽게 주고받을 수 있게 되었을 뿐만 아니라, 온라인 전자금융 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, 침입탐지 시스템, 가상사설망과 같은 다양한 보안 솔루션들이 등장하게 되었으며, 최근 군, 국가 기관, 금

* 목원대학교 공과대학 정보전자영상공학부

접수일자 : 2006. 12. 29

용권과 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. 기존에 개발된 VPN(Virtual Private Network) 장비들은 대부분 소프트웨어적으로 구현되어 있다. 소프트웨어 방식의 VPN 장비는 성능 측면에서 피할 수 없는 한계점을 갖는다. 최근100 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 암복호화하는 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. 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. 본 논문에서는 고성능의 하드웨어 VPN 장비를 개발할 때 고려해야 할 이러한 문제점들에 대해 조사 분석하고, 타당한 설계 가이드라인을 제한다.

II. 초고속 VPN 시스템의 요구사항

VPN 가속 보드는 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 서비스를 제공하는 것을 목적으로 하여 다음과 같은 사항을 고려해야 한다.

- IPSec 기능 제공

IPSec 핵심 기능을 최대한 하드웨어적으로 구현함으로써 10Gbps 의 IPSec 처리를 지원한다. 이경우 Cavium 사의 Nitrox-II 보안 프로세서의 경우 최대한의 성능을 보유하고 있다. 또한 VPN 서비스 제공 및 신뢰 터널 형성 시 기존의 게이트웨이, 라우터, 네트워크 관리 시스템의 성능 저하가 최소화되도록 In-line 구조를 일반적으로 사용한다. 필요에 따라 게이트웨이, 라우터, 네트워크 관리 시스템에서 암/복호화 기능만의 사용이나 SSL 프로토콜의 사용이 용이하도록 Look-aside 구조를 채택한다.

- 다양한 네트워크 및 버스 인터페이스 제공
  VPN 가속 모듈을 보드화하여 고속으로 데이터를 효율적으로 처리하기 위하여 상용 MAC 칩과 Network Processor Unit(NPU) 에서 사용되고 있는 데이터 인터페이스를 제공한다.
- PIC/PIC-X 인터페이스: 32/64 BITS, 33/66/133 MHz. Host /Contol Processor
- SPI-2 인터페이스: OC192 Frammer/MAC 혹은 NIU
- 다양한 알고라즘 제공
  VPN 가속 모듈에서 제공되는 암호 알고리즘은 보안 시스템에서 많이 사용되는 암호 알고리즘들을 모두 지원할 수 있어야 한다. 또한 국내 표준 암호 알고리즘인 SEED가 지원되어야한다. 지원 알고리즘의 대표적 예는 다음과 같다.
  - 3DES/DES, AES, RC4, RA, SEED 등
- 인증 기능 제공
  다음과 같은 표준 알고리즘을 지원해야 한다.
  MD5, SHA-1, HMAC-MD5, HMACC-SHA-1
- 다양한보안 프로토콜을 지원
  VPN 가속 모듈의 경우 기본적으로 IPSec 보안 프로토콜을 이용한 VPN 서비스를 제공해야 하며 필요에 따라 SSL도 지원 가능해야 한다.

II. VPN 가속 모듈의 설계

VPN 가속 모듈은 크게, 보안프로세서, SEED 알고리즘, 그리고 SPI4-2 및 PCI 외부 인터페이스 부분으로 구성된다. 암호 프로세서는 Cavium 사의 Nitrox-II 보안 프로세서를 사용하여 두개의 SPI4-2 포트와 고속 데이터가 가능하다. 또한 제어 프로세서 및 보안 프로세서는 64 bit 66MHz 의 PCI 인터페이스로 데이터의 입출력 및 제어 모듈을 구성할 수 있다. Nitrox-II 에서 제공되는 SPI4-2 인터페이스는 최소 311MHz에서 최대 500mhz를 지원하여, 최소 9.7Gbps 에서 최대 15.6Gbps 까지의 데이터 전송율을 지원 가능하다.

3.1. 보안 프로세서부

일반적으로 보안프로세서의 선정은 설계하고자 하는 규격에 의해 결정되어진다. 본 내용에서는 Cavium 사의 Nitrox-II 보안 프로세서를 설명하고자 한다. 2003년도에 발표된 보안 프로세서로서 고속의 암호 처리 능력을 가지고 있으며, 다양한 프로토콜을 지원하는 암호 처리 단일 전용 칩이다. 이는 고속의 산술 연산 모듈과 랜덤 수 생성기, 해쉬 처리 모듈이 하드웨어로 구현 가능하다. 또한 SSL/TLS 도는 IPSec/IKE 암호 프로토콜을 지원한다. Nitrox-II 프로세서의 경우는 내부 코어가 Giga급 처리가 가능하도록 설계되어 있으며, 여러 암호 연산이 병렬로 처리 가능하도록 설계되어 있어 더욱더 고속 처리와 시스템의 융통성을 제공한다. Nitrox-II 프로세서의 기능 및 성능은 다음과 같다.

* 단일칩으로 SSL/TLS, IPSec/IKE와 같은 암/복호화 프로토콜을 고속으로 지원
* 기능적으로 In-Line 데이터 처리가 가능하여 Bump-in-the-wire 장비를 구현할 수 있고, 주변의 NPU와 Framer/MAC 등 장비와의 다양한 호환성을 제공
* L2 & L3 Parsing 이 가능
* Inbound 시 SA Lookup 기능 제공
* 다양한 알고리즘의 지원 가능
  - RSA와Diffie-Hellman
  - DES/3DES, AES. ARC4
  - MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
* 고속의프로토콜 구현
  - 최대40,000 SSL TPS
  - 최대 10,000 IKE Main Mode/sec(DH(1024bit) + RSA 의 동작속도를 의미함)
* 많은수의 IPSec SA 또는SSL Contexts 지원
  - 2M IPSec Sas, 512MB DDR-SDRAM 지원
  - 4M SSL Contects, 4GB DDR-SDRAM 환경
* 고속데이터 암호화
  - IPSec 응용 분야 : 5G ~ 20Gbps
  - SSL 응용분야 ; 최대 20Gbps
* 최대320 Mbps Random Number Generator
* 고속의 표준 인터페이스
  - PCI/PCI-X, 32/64-bit, 33/133MHz
* SPI4-2 Level 3-4 지원
  - Linux, BSD, Windows 등을 위한 S/W 드라이버 지원

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 설계하여야 한다. 본 보고서에서는 고성능의 하드웨어 VPN 장비를 개발할 때 고려해야 할 이러한 문제점들에 대해 조사 연구하고, 타당한 설계 가이드라인을 찾는 것을 목표로 하고 있다. 일반적으로 인터넷을 통해 보내어지는데이터의 기밀성과 근원지 및 목적지에 대한 인증과 관련된 보안 프로토콜과 알고리즘에 대한 이해가 반드시 필요하다. SSL과 IPSec의 주요한 차이점은 사용되는 프로토콜의 layer 이다. SSL 프로토콜은 응용 계층과 TCP/IP 계층 사이에 위치하며, HTTP와 같은 응용 계층에 대한 서비스를 제공한다. 본 프로토콜은 암호화된 데이터의 교환 뿐만이 아니라 호스트에 대해 필요할 경우에는 사용자에 대한 인증을 제공한다. SSL의 특징은 빠른 셋업과 안전한 연결이다. SSL은 대부분의 브라우저에 의해 지원되므로, 모든 웹 기반 클라이언트에게 적용될 수 있다.

신용 카드와 VPN 응용 분야에도 사용 가능하다. 이에반해, IPSec은 당초 VPN 응용 계층을 지원하기 위해 정의되었다. 따라서 본 보고서에서는 이러한 기밀성을 위해 사용되고 있는 기술에 대한 서비스와 기술적인 측면에 대해서 기술하기로 한다. 주로 SSL Accelerator과 IPSec Accelerator를 사용한다.

3.2. SSL Accelerator

SSL 연결의 구성은 서버와 클라이언트로 구성이 되는데, 클라이언트의 경우 소프트웨어적으로 SSL 의 기능을 수행할 수 잇도록 일반적으로 PC 상에서 이루어진다. 일반적으로 시장의 형성은주로 서버에서 이루어지며 초당 SSL 수천번의 Transaction을 수행한다. SSL 가속기의 경우 대개 PCI 카드의 형태로 서버에 내장되어 있다. SSL 기능의 칩들은 PCI 인터페이스를 가지고 있으며, 이러한 외부의 인터페이스와 연결이 용이하도록 단지 외부 메모리의 형태를 가진다. 웹스위치는 입력되는 패킷을 해석하고, 여러 개의 서버 중 한 개를 선택하여 할당하게 된다. 패킷을 첫번째로 복호화을 하지 않고 패킷의 속성을 접근할 수 없기 때문에, 이때 SSL의 사용은 웹 스위치에 대한 문제점을 야기 시킬 수 있다. 그러므로 Web-switch 공급업체들은 그들의 제품을 SSL의 최종끝단에 부가하여 사용하도록 만들었다. 다량의 SSL Traffic의 취급하기 위해서는 SSL 가속기가 반드시 필요하다. 일반적인 구성에서는Security chip은 NIU 와 연결하여 사용한다. Flow-through 구조의 경우에서는 classification coprocessor를 전반부에 위치시키고 SSL의 Traffic 을 복호화 시키는 구조를 가지도록 되어 있다. 또다른 경우에는 패킷 처리를 PCI를 통하여 수행함으로써, 고속의 속도에서 인터페이스의 문제가 주요 쟁점으로 될 수가 있으며, 특별히 SSL의 암호화되는 비율이 증가하면 할수록 더 많은 Traffic을 발생시킨다.

3.3. IPSec Accelerator

일반적으로 IPSec 게이트웨이는 Internet Key Exchange(IKE) 기능과 IPSec 기능을 포함한다. IKE는 두 VPN 장비 사이의 SA(Security Association)를 생성하고, IPSec은 inbounding processing과outbounding processing을 수행한다. IPSec 패킷 수행을 위한 기능은 IP processing, 암복호화 과정, Hash 기능, 무결정성 등을 포함한다. 일반적으로 이러한 기능을 수행하기 위해서는 기존에는 S/W 방법으로 구현하였으나 수행 시의 속도가 낮은 관계로 H/W 기반의 시스템 구현이 필요하게 되었다. 따라서, 암호화 칩을 사용한 IPSec 가속기의 개발이 필요하게 되었다. 이때 사용되는 암호화 칩은 IPSec 가속기의 일반적인 기능을 일반적으로 포함한다.

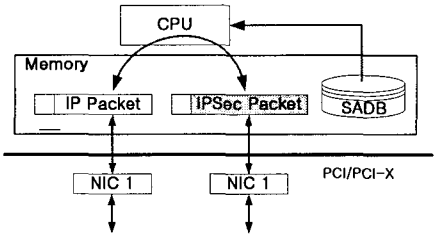

그림 1. 소프트웨어 기반 VPN 불럭도
Fig. 1. Diagram of VPN based on Software

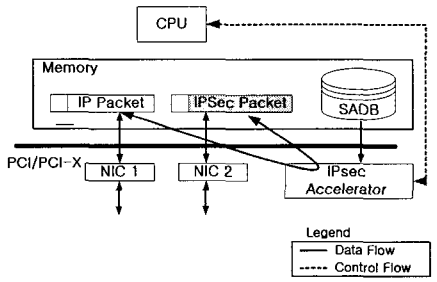

그림 2. 하드웨어 기반 VPN 불럭도
Fig. 2. Diagram of VPN based on Hardware

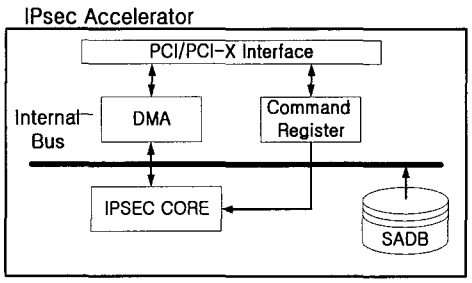

그림 3. IPSec 가속기의 블록도
Fig. 3. Block Diagram of IPSec Accelerator

그림3에서 보는 바와 같이 PCI/PCI-X 인터페이스는 IPSec 가속기 보드를 통하여 호스트와 연결된다. 이때 DMA 블록은 VPN과 호스트의 메모리 사이의 데이터 전송에 대해 제어한다.

Ⅳ. 네트워크프로세서를 이용한 시스템 설계

네트워크 프로세서는 하드웨어적으로 모든 프로토콜(Layer1 ~ Layer7)에 대해 처리가 가능한 소자이다. 특히, 다수개의 Microengine에서 병렬적으로 패킷 처리가 가능하기 때문에, 초고속 네트워크 장비 개발에 핵심이 되는 부품이 되고 있다. 네트워크 프로세서는 기존에 QoS 관리나 과금계산 등를 위한 어플리케이션 개발을 위해서 등장하였으나, 전용 컴파일러를 비롯한 툴키트의 부재 등의 문제점으로 인하여 최근까지 네트워크 프로세서가 사용된 제품이 비교적 적은 편이다. 최근에 인텔에서는 기존 IXP1200 시리즈를 발전시켜서 IXP2800 시리즈의 칩셋을 시장에 내어 놓고 있으며, 암호 가속모듈을 탑재한 IXP2850 칩을 선보이고 있다. IXP2850 내부에는 두개의 bulk 암호화 모듈이 들어있다. 그외의 하드웨어적 구조는 기존 IXP2800과 동일한다. Bulk crypto 모듈에서는 암복호화 기능, 공개키 가속 기능 등이 지원되지 않는 순수 bulk encryption/decryption만을 수행할 수 있다. 이 암호화 모듈 내부에는 아래 그림21과 같이 AES 블록이 1개, 3DES 코아가 2개 내장되었으며, SHA1 코아가 2개 내장되어 있다. 두 블록이 최대한 사용될 경우 초당 10Gbps 이상의 암복호화 성능을 발휘한다.

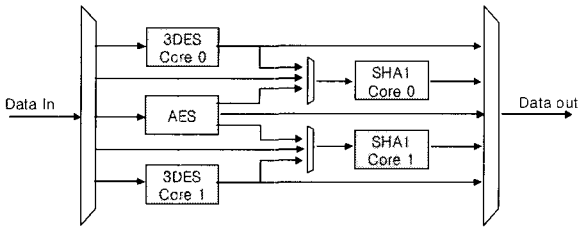

그림 4. IXP2850 내부의 Crypto 모듈 Block Diagram
Fig. 4. Block Diagram of Crypto Module Inside of IXP2850

위 그림 4에서 보이듯이 3DES, AES, SHA-1 알고리즘은 하드웨어적으로 가속이 되며 MD5, RC4 알고리즘은 소프트웨어적으로 miroengine에서 구현 되어 진다. 특히, AES 의 경우, 128비트 블록 사이즈, 128, 192, 256 비트 길이의 키에 대해서 지원한다. 두개의 crypto 모듈은 flow-through 구조를 지원하며, 하나의 모듈내에서도 여러 개의 알고리즘이 동시에 실행이 될 수 있기 때문에 패킷들은 interleaved 방식의 빠른 속도로 처리될 수 있도록 한다.

4.1. Crypto Data Flow

다음 그림5는 IXP2850에서 crypto 모듈을 사용하여 패킷처리를 할 경우에 패킷들이 움직이게 되는 data flow step을 보여준다.

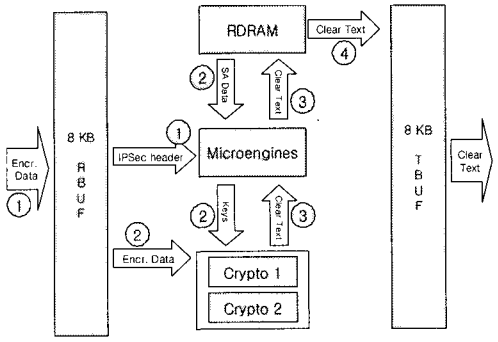

그림 5. IXP2850에서의 IPSEC 처리 과정
Fig. 1. Diagram of VPN based on Software

즉, 위의 그림 5는 IPSEC 패킷이 어떠한 과정을 거쳐서 처리될 수 있는지 그 과정을 보여주는 것이다. 간략히 다음과 같은 절차를 거친다.

가. IPSEC 패킷을 수신함.
- 하나의 thread는 RBUF에 최근 저장된 패킷에 상태 정보를 전달 받음
- RBUF 상태 정보를 처리함
- 만일 SOP 인 경우 (RBUF 에 헤더가 있는 경우)
- 패킷의 헤더를 읽어들임 (IPSEC 헤더 포함)
- IPV4 verify
- SPI (Security Parameter Index) 를 참조함
- Crypto 모듈을 할당함
- Data 버퍼를 할당함
- 파이프라인과정의 다음 thread에게 시그날을 전달함

나. IPSEC 패킷 처리
- 전단계로부터 신호를 받은 thread는 패킷처리를 계속함
- 만일 SOP라면 SA를 DRAM으로부터 microengine으로 로드함

- RBUF에 저장된 data를 crypto 모듈의 메모리 공간으로 옮김
- cipher와 HMAC 키를 crypto 모듈로 적재
- 파이프라인 과정의 다음 thread에게 시그날을 전달

다. IPSEC 갱신
- 전단계로부터 시그날을 받은 thread는 패킷처리를 계속함
- 만일 SOP이라면, SPI, sequence, IV를 hash 처리함
- payload 데이터를 복호화하고 hash 처리함
- 인증 데이터를 확인함
- IPV4의 유효성 테스트를 함
- 복호화된 데이터를 RDRAM 메모리 공간으로 옮김
- 파이프라인과정의 다음 thread에게 시그날을 전달함

라. 최종 IPSEC 처리단계
- 전단계로부터 시그날을 받은 thread는 패킷처리를 계속함
- IPSEC 정책을 수행
  : Anti-reply, Security policy database lookup, *Lifetime* 체크, *Counter* 갱신
- 파이프라인과정의 다음 thread에게 시그날을 전달
- 패킷 처리가 종료되면, TBUF로 옮김

4.2. 네트워크 프로세서를 이용한 VPN 시스템의 장단점

네트워크 프로세서는 그 내부에 패킷처리에 최적화된 다수개의 microengine을 통하여 초고속으로 동작하는 다양한 부가 서비스를 제공하는 시스템 개발에 용이하다. IPSEC 패킷의 처리에서 bottleneck이 발생할 소지는 앞에서 언급한 바와 같이 두 경우가 있다. 첫번째는 control path bottleneck으로서 bulk encryption 자체가 많은 계산량을 요구하기 때문에 일정 수준 이상의 패킷 처리가 불가능할 수 있는 것이었으며, 나머지 경우는 data path bottleneck으로서 패킷 데이터가 전송되는 버스의 대역폭 한계에 의해 bottleneck이 발생할 수 있는 것이다. IXP 2850의 경우, 이 두 bottleneck에 대해서 충분히 좋은 솔루션을 제공할 수 있다. 먼저 control path bottleneck은 내장한 crypto 모듈 자체의 bulk encryption 성능이 10Gbps를 초과하므로 10G급 VPN 시스템의 bottleneck을 충분히 방지할 수 있다. 또한 IXP2850은 data path bottleneck을 방지하는 좋은 구조를 가진다. Security Coprocessor를 이용하는 VPN 시스템의 경우, 복호화할 패킷을 전달하고, 복호화 결과를 저장하기위해 메모리 버스를 두번 사용하게 된다. 특히, 10Gbps 이상의 고속 시스템에서 이와 같이 메모리 버스를 두번 사용하는 것은 큰 Overhead가 될 수 있다. 그러나, IXP2850의 경우, 내부 메모리 버스를 이용하고 외부 메모리 버스를 액세스하지 않아도 되므로 외부 버스를 그만큼 적게 사용해도 된다.

<표 1> 시스템 구현방식에 따른 장단점 비교

	장점	단점
IXP 2850 기반 시스템	- microengine 프로그램을 이용하여 다양한 부가서비스 제공이 용이함 - 내부 버스를 이용하여 암복호화된 데이터를 전송하므로 외부 메모리 버스의 대역폭 한계를 극복할 수 있음.	- 하드웨어적으로 지원되는 알고리즘의 종류가 적음. - microengine용 compiler를 비롯한 toolchain의 부족 - IPSEC 엔진 포팅/탑재의 어려움 - 신규 알고리즘 추가의 어려움 - 플랫폼간 이식이 어려움
Security Coprocessor 기반 시스템	- 다양한 알고리즘 지원 - IPSEC 엔진 탑재에 대한 기술적 지원	- QoS 관리, 과금 등의 부가서비스에 대한 배려가 부족함. - 타사 NP 또는 chip과의 연동 설계가 필수적임.

V. 결 론

결론적으로 네트워크 프로세서를 이용한 VPN 시스템은 제공할 수 있는 서비스의 종류나 구조 자체로는 매우 바람직하나, 그 구현 가능성에 대해서 정밀한 검토가 극히 필요한 실정이다. 네트워크 프로세서가 네트워크 장비 개발 분야에서 이슈가 된지 벌써 수년이 되었지만, 아직까지도 NP용 컴파일러가 제대로 만들어지지 못한 상황이다. 이렇게 열악한 상황에서 IPSEC 엔진을 NP에 탑재하고, 키교환, 패킷 필터링 등의 기타 부가서비스들을 모두 고려하여 제품을 개발하는 것은 결코 쉬운 일이 아니다. 또한 NP vendor 입장에서는 NP의 응용 분야가 VPN에 한정되는 것이 아니라, 고속 라우터, 방화벽 등 다양하므로 VPN에 대한 기술지원이 그만큼 미약한 면도 있다. 그러나 전용 Security Coprocessor를 제조하는 업체들은 자사의 칩이 시장성을 얻을 수 있도록 Application Note, Device driver 포팅 등의 개발 자료를 널리 배포하고 지원하고 있다. 이러한 현실적인 상황을 고려한다면 현재는 Security Coprocessor를 이용한 접근을

하는 것이 더욱 타당성이 있어 보이며 향후에는 수십기가급의 시스템 개발을 위해 Network Processor를 사용하는 것은 당연하다.

참고문헌

[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

[5] 정지훈 외2인, "IPsec 표준화 동향 및 제품 현황", 한국전자통신연구원 주간기술동향

저자소개

김 정 태(Jung-Tae Kim)

2001년 8월 연세대학교 대학원 전자공학과 박사

1991년 8월~1996년 2월 한국전자통신연구원(ETRI) 선임연구원

2002년 10월~현재 : 목원대학교 정보전자영상공학부 교수

※관심 분야 : Microwave photonics, Optically fed wireless communication system design, Information security system design, Network Security, ASIC Design.