고속 VPN을 위한 패킷처리 가속기 개발

나종화[O*] 김종명** 류대현*
*한세대학교 IT학부, **(주)시큐어넥서스
{jhnha[O], dhryu}@hansei.ac.kr, jmkin@xecurenexus.com

A Development of the Packet Processing Accelerator for High Speed VPN

Jongwhoa Na[O*], Jongmeung Kim**, Daehyun Ryu*
*Dept. of IT, Hansei University, **Xecurenexus. Co.

요 약

VPN을 고속화하기 위한 패킷처리 가속기를 설계·구현하고 그 성능을 평가하였다. 본 논문에서 구현된 패킷처리 가속기는 IPIP처리, 암/복호 처리, HASH 처리, 무결성 검사 등의 IPsec 패킷처리 기능을 내장하고 있다. 기능 및 성능 시험을 통하여 최대 1Gbps이상의 속도로 패킷을 처리할 수 있다는 결과를 얻었다.

1. 서 론

최근 네트워크 환경이 기가비트급의 초고속 환경으로 바뀌면서 기가비트급의 고속 VPN에 대한 수요가 증가하고 있으며 기가비트 VPN에 대한 개발도 활발하게 이루어 지고 있다. 그러나 속도가 100 Mbps를 넘는 VPN을 개발하는 것은 매우 어렵다. 특히, 보안의 강도가 비교적 높은 3DES 알고리즘을 사용하는 경우의 성능 저하는 아주 크다고 알려져 있다. 전체 대역폭을 점유할 만한 정도의 대량의 패킷을 일일이 암·복호화하는 작업이 단순히 소프트웨어적으로만 처리하기에는 현재로서는 불가능한 작업이기 때문이다.

본 논문에서는 VPN을 고속화하기 위하여 암호 가속기(Crypto Card)를 이용한 패킷처리 가속기를 설계·구현하고 그 성능을 평가하였다. 제안된 패킷처리 가속기는 IPIP(IP-over-IP tunneling)처리, 암/복호 처리, HASH 처리, 무결성 검사 등의 IPsec 패킷처리 기능을 내장하고 있으며 최대 1Gbps 이상의 속도로 패킷을 처리하는 것을 목표로 하였다. 본 논문에서 개발한 패킷처리 가속기를 적용한 고속 VPN은 다양한 네트워크 환경에서 유연하게 VPN 사용자들의 요구 사항을 만족시킬 수 있을 것이다.

본 논문의 2장에서는 패킷처리 가속기의 구조 및 요구규격을 정의하고 3장에서는 패킷처리 가속기의 동작 개념과 동작 순서를 설명한다. 4장에서는 기능과 성능을 평가하고 5장에서 결론을 맺는다.

2. 패킷처리 가속기

VPN 게이트웨이는 IPsec 기능과 IKE기능을 가진다. IKE기능은 두 VPN간에 SA(Security Association)을 만들며, IPsec 기능은 SA를 바탕으로 Inbound 처리 와 Outbound처리를 수행하는 기능이다.

IPsec 기능은 IPIP처리와 암복호 연산과 HASH연산과 무결성검사를 필요로 한다. 이들 연산은 일반적으로 소프트웨어로 구현되어 있는데, CPU에 큰 부하를 요구하므로, 전체 VPN 시스템의 속도를 저하시킨다. 따라서, Crypto Card를 이용한 패킷 처리 가속기를 사용하여, 이들 연산을 수행함으로써, IPsec 기능을 매우 빠르게 처리하고, CPU의 부하를 크게 줄인다. 다음은 일반적인 VPN 시스템의 동작 개념도와 패킷처리 가속 기능을 갖는 VPN 게이트웨이의 동작 개념도이다.

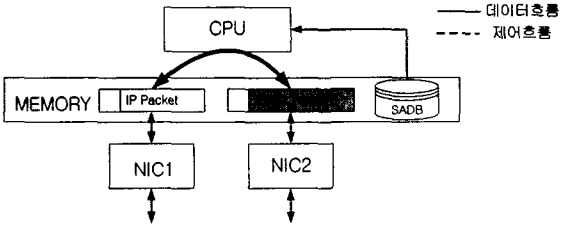

그림 1 소프트웨어 방식의 IPsec 처리

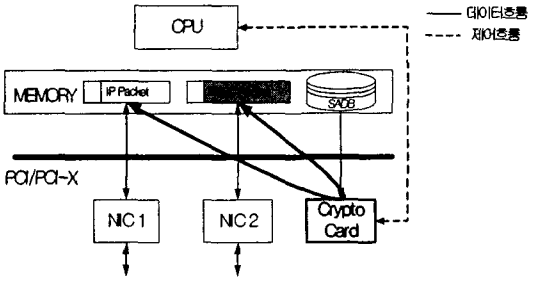

그림 2 패킷 처리 가속기를 사용한 IPsec 처리

본 논문에서는 cavium사의 NITROX 칩을 사용한 Crypto Card를 이용하여 패킷처리 가속기를 구현하였다[10]. Crypto Card는 IPIP처리, 암/복호 처리, HASH 처리, 무결성 검사 등의 IPsec 패킷처리 기능을 내장하고 있으며 내부 블록도는 다음과 같다.

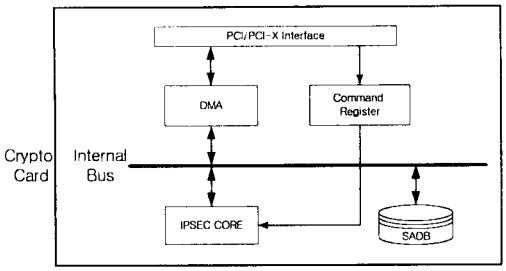

그림 3 Crypto Card의 내부 블록도

- PCI/PCI-X 인터페이스 : VPN 시스템 내의 호스트와 고속의 데이터 통신을 위하여 PCI/PCI-X를 지원한다.
- DMA : 호스트 메모리로부터 데이터를 고속으로 읽거나, 호스트 메모리로부터 데이터를 고속으로 기록한다.
- 명령 레지스터 : 호스트 CPU가 패킷처리 가속기에게 IPsec 처리를 명령 시, 처리할 패킷 수 또는 명령의 수를 이 레지스터에 기록하면, 가속기 내의 IPsec Core가 IPsec 처리를 수행한다.
- 내부버스(Internal Bus) : 패킷처리 가속기 내에서 데이터 송수신을 위한 64bit Bus이다.
- IPsec Core : 실제로 IPsec처리를 수행하는 Core이다.
- SADB : 패킷처리 가속기내에 부착된 메모리로서, SA를 저장한다. IPsec Core가 Host Memory로부터 입력된 패킷을 처리하고자 할때, 필요한 정보(키, IV 등)를 SADB에서 읽어온다.

본 논문에서 제안하는 패킷처리 가속기는 표 1과 같은 규격을 가진다.

표 1 제안된 패킷처리 가속기의 규격

구 성	사 양
PCI Interface	PCI/PCI-X(64bit, 64MHZ/100MHz/133MHz, Master & Target Modes)
Algorithm	RSA and Diffie-Hellman(groups 1,2,5) DES/3DES, AES, ARC4 MD5, SHA-1
Number of SAs	2,000,000 IPsec SAs with 512MB Local Memory

3. 패킷처리 가속기 동작 개념

패킷처리 가속기는 1Gbps이상의 데이터를 호스트 CPU와 통신하기 위하여 PCI/PCI-X 인터페이스를 지원한다. 또한, 자체 내장된 DMA를 사용하여 호스트 메모리의 Command와 입력 패킷을 읽어오거나, 출력 패킷을 호스트 메모리에 기록할 수 있다. 그림 4는 패킷처리기의 IPsec 처리 동작 개념도이다. Crypto Card의 패킷처리 동작 순서는 표2와 같다.

표 2 패킷처리 가속기의 동작 순서

순번	실행 내용
1	IPsec 처리될 입력 패킷이 있으면, 호스트 CPU가 Command를 생성하고, 출력 패킷이 저장될 메모리 공간을 준비한다. 이때 Command는 처리 방법(Inbound/ Outbund처리), 입력 패킷의 저장 주소, 출력 패킷의 저장 주소, SADB의 SA 저장 주소를 저장하고 있다.
2	호스트 CPU가 처리될 Command의 주소와 Command의 수를 패킷처리 가속기의 Command Register에 기록한다.
3	Command Register에 Command의 수를 기록하면, Crypto Card는 IPsec 처리 동작을 시작한다.
4	IPsec Core가 Command Buffer의 Command를 읽어와서, 처리방법, 입력 패킷의 저장 주소, 출력 패킷의 저장 주소, SA 저장 주소를 분석한다.
5	Command에서 분석한 입력 패킷의 저장 주소에서 입력 패킷을 읽어온다
6	Command에서 분석한 SA의 저장 주소에서 SA관련 정보를 읽어온다
7	SA정보를 사용하여, Command의 처리방법에 따라, 입력 패킷을 처리한다. 처리된 결과인 출력 패킷을 출력 패킷 Buffer에 저장한다.

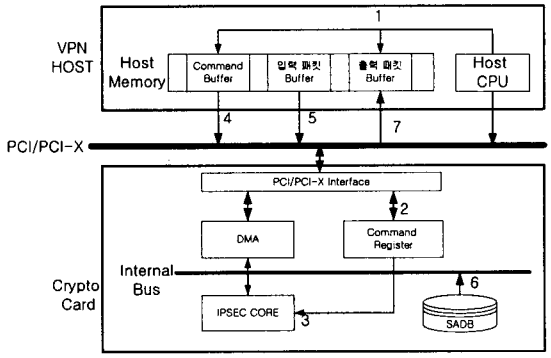

그림 4 패킷처리 가속기의 IPsec 처리 동작 개념도

4. 패킷처리 가속기 성능 평가

개발된 패킷처리 가속기의 IPsec 패킷처리 기능이 올바르게 동작하는지를 확인하고 IPsec 패킷처리 속도를 측정하였다. 표 3은 패킷처리 가속기의 기능/성능 시험 리스트이다.

본 논문에서는 기능/성능 시험을 수행하기 위해서, 별도의 시험 프로그램을 작성하였다. 사용자 모드에서 동작하는 시험 프로그램이 IP 패킷 길이와 패킷 수를 디바이스 드라이버에 입력한다. 이를 입력받은 디바이스 드라이버는 입력 버퍼와 명령 버퍼와 출력1버퍼와 출력2 버퍼를 메모리에 할당한다. 입력 버퍼에 IP 패킷을 생성하고, 명령 버퍼에 명령을 생성하는데, 이 명령은 입력 버퍼의 데이터를 Inbound 처리하여 출력1 버퍼에 저장하도록 하는 명령이다. 호스트 CPU는 패킷처리 가속기

에게 처리 시작을 알린 후, 모든 패킷이 처리되기까지 대기한다. 이 대기 시간을 측정하여, 성능을 출력한다. 이 때, 성능은 (입력패킷길이 * 패킷량 / 소요시간)으로 나타낸다. 동일한 방법으로 패킷의 Inbound 처리 성능을 구하는데, 명령 버퍼는 출력1버퍼의 IPsec 패킷을 Inbound처리하여 출력2버퍼에 저장하도록 한다. 그리고, 출력2버퍼의 IP Packet과 출력1버퍼의 IP 패킷이 동일하면, 암/복호화가 올바르게 동작한 것이다. 위의 시험 프로그램을 사용하여 측정된 패킷 가속기의 성능은 표 4과 같다. (호스트에서 패킷처리 가속기에 전달 가능한 명령의 최대 수는 15K개(=1024개/blocks * 15blocks)이다.)

표 3 성능 시험 테스트

분류	순번	시험 내용	시험결과
기능시험	1	64byte길이의 IP 패킷을 입력받아 Outbound처리를 수행한다.	O
	2	위의 IPsec패킷을 다시 입력받아 Inbound 처리를 수행한다. 결과 패킷이 원래의 IP패킷과 동일한가?	O
	3	1000Byte, 1500Byte 길이의 IP 패킷으로 위의 시험 1,2를 반복한다.	O
	4	ESP-Transport Mode에 대하여 위의 시험 1,2,3를 반복한다.	O
	5	AH-Tunnel Mode, AH-Transport Mode에 대하여 위의 시험 1,2,3,4를 반복한다.	O
	6	알고리즘 3DES-SHA1-96, DES-SHA1-96, DES-MD5-96으로 위 시험을 1,2,3,4,5를 반복한다.	O
성능시험	7	64 Byte 길이의 IP 패킷 15K(15*1024)개를 호스트 메모리에 임의로 생성한 후, 패킷처리 가속기의 Outbound 처리(ESP, Tunnel Mode, 3DES-MD5-96)시의 성능을 측정한다.	-
	8	1400Byte길이의 패킷으로 위의 시험을 반복한다.	-
	9	위의 시험 7,8과 동일한 방법으로 Inbound 처리시의 성능을 측정한다.	-

5. 결 론

본 논문에서는 VPN을 고속화하기 위하여 Crypto Card를 이용한 패킷처리 가속기를 설계·구현하고 그 성능을 평가하였다. 제안된 패킷처리 가속기는 IPIP(IP-over-IP tunneling)처리, 암/복호 처리, HASH 처리, 무결성 검사 등의 IPsec 패킷처리 기능을 내장하고 있으며 최대 1Gbps이상의 속도로 패킷을 처리할 수 있다는 결과를 얻었다. 본 논문에서 개발한 패킷처리 가속기를 적용한 고속 VPN은 다양한 네트워크 환경에서 유연하게 VPN 사용자들의 요구 사항을 만족시킬 수 있을 것이다.

참 고 문 헌

[1] Implementing Virtual Private Networks, Steven Brown, McGraw-Hill, 1999.

[2] T.Braun, M.Kasumi, et al., "Virtual Private Network Architecture", IAM-99-01, April 1999.

[3] Mobile Virtual Private Network, draft-tzvetkov-mvpn-01.txt, Mobile IP Working Group Internet-Draft, Express March 2001

[4] 정태명, 가상사설망(VPN), NETSEC-KR 2000, 2000.5.

[5] 류대현, VPN 기술동향, 국제정보기기 및 보안기기전, 2001.4.

[6] 손승원, 국내외 VPN 기술동향 및 향후전망, 정보보호21C, 2000.10.

[7] 윤재우, 김영걸, 류대현 "병렬구조를 갖는 고속 VPN 게이트웨이 구현에 관한 연구" WISC2001, 2001.9.

[8] 신순자 외2인, "공인인증기반의 가상사설망 구축", pp.42-53, 한국통신학회지, 제18권9호. 2002

[9] 김정태, 류대현, 윤호건, "VPN 게이트웨이 고속화를 위한 하드웨어 구조연구" pp.101 - 107, 한국통신학회지, 제 27권 8T호, 2002.8.

[10] http://www.cavium.com/products.html

표 4 측정된 패킷 가속기의 성능(처리 속도는 입력 패킷량을 기준으로 계산한 값)

측정 조건	패킷길이 (Bytes)		입력 패킷량 (Bytes)		암호화 성능		복호화 성능	
	IP	IPsec	IP	IPsec	소요 시간 (msec)	처리 속도 (Mbps)	소요 시간 (msec)	처리 속도 (Mbps)
ESP, Tunnel Mode, 3DES-MD5-96	64	120	64KBytes	120K	1.25	420	1.14	842
			960KBytes	1.8M	18.6	423	16.2	890
			9.6MBytes	18M	187.2	420	162.3	890
	1400	1456	1400KBytes	1456K	7.2	1593	7.1	1640
			21MBytes	22M	102	1687	105	1680
			210MBytes	220M	1040	1654	1050	1680