제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

홈게이트웨이에서의 고속 VPN 기능 구현 및 분석

김재명*, 박광로**
ETRI 홈네트워크팀
ETRI 홈네트워크팀장
E-mail : jaemkim@etri.re.kr

High-speed VPN Implementation and Analysis in Home Gateway System

JaeMyoung KIM*, Kwang-ro Park
*ETRI, Home Network Team
**ETRI, Home Network Team Head
E-mail : jaemkim@etri.re.kr

요 약

가입자 망 기술의 발달과 멀티미디어 통신 필요의 증대로 댁내에서도 다수의 PC 와 정보가전 기기를 하나로 묶는 홈네트워크가 구축되고 있으며, 이를 외부와 안전하게 연결하기 위한 요구가 증대되고 있다. 따라서, 초고속 외부망과 내부의 정보가전망을 하나로 연결하기 위한 홈게이트웨이가 개발 및 보급되고 있으며 홈게이트웨이 시스템에서 소프트웨어 혹은 하드웨어 방식으로 네트워크 보안 기능을 제공하고 있다.

그러나 하드웨어 방식을 사용하지 않는 임베디드 시스템 기반의 VPN 시스템은 대부분의 처리 시간의 암호화에 소요함으로 실제적인 사용자 요구사항에 정의된 통신 속도에 미치지 못한다.

이 글에서는 IPSec 기반 VPN 보안 기능을 모토롤라의 MPC180 보안 프로세서를 사용하여 하드웨어적으로 홈게이트웨이 시스템에 구현하여 그 성능을 분석한 결과 소프트웨어적으로는 만족할 수 없는 사용자 요구사항인 통신속도를 만족할 수 있음을 보였다.

1. 소개

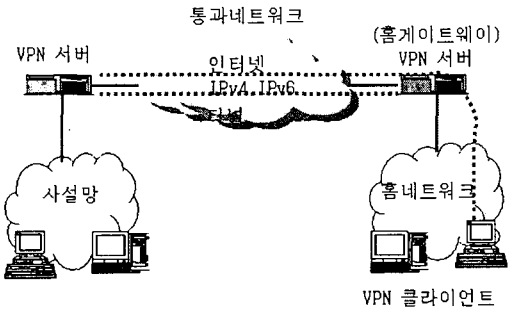
가입자 망 기술의 발달과 멀티미디어 통신 필요의 증대로 댁내에서도 다수의 PC 와 정보가전 기기를 하나로 묶는 홈네트워크가 구축되고 있으며, 이를 외부와 안전하게 연결하기 위한 요구가 증대되고 있다. 따라서, 초고속 외부망과 내부의 정보가전망을 하나로 연결하기 위한 홈게이트웨이가 개발 및 보급되고 있으며 홈게이트웨이 시스템에서 소프트웨어 혹은 하드웨어 방식으로 네트워크 보안 기능을 제공하고 있다. 그 대표적인 기능이 VPN(Virtual Private Network: 가상 사설망)으로 인터넷과 같은 신뢰할 수 없는 네트워크를 통해서 안전하게 데이터를 전송할 수 있도록 하는 기능으로 IPSec 프로토콜을 통해 구현되며, 홈네트워크에 연결된 정보가전 기기를 안전하게 외부와 연결할 필요가 있을 때 사용된다.

홈게이트웨이 VPN 기능을 제공하기 위해서는 다음과 같은 요소가 필요하다.

- VPN 서버/클라이언트 : VPN 접속을 허가/시도하는 시스템으로 원격접속이나 라우터 접속이 될 수 있다.
- 터널 : 전송되는 데이터가 캡슐화되어 접속되는 연결 통로이다.
- VPN 연결 : 전송되는 데이터가 암호화되거나 보호되는 보안성이 강화된 터널로 접속된 것.
- 터널링 프로토콜 : 터널을 생성 및 관리하고 비공개 데이터를 캡슐화하는데 사용되는 통신 표준 프로토콜.

통과 네트워크 : 캡슐화된 데이터가 통과하는 공유 혹은 사설 인터넷망이다.

다음 (그림 1)은 구성요소의 위치를 나타내고 있다. 홈게이트웨이가 VPN 서버의 역할을 하며 홈네트워크를 통해 VPN 클라이언트가 연결되거나 홈게이트웨이 VPN 서버를 통해 단말들이 VPN 망을 형성할 수 있음을 보여주고 있다.



(그림 1) VPN 구성요소

이러한 환경에서 홈게이트웨이의 보안 성능에 관한 판단 기준은 실제 사용자의 만족도는 외부적인 요인에 위해 좌우되나, 내적인 사용자 요구사항인 통신속도를 만족하여야 한다.

보안 프로세서는 하드웨어적인 처리로 홈게이트웨이 시스템 성능을 향상시키고 암호처리로 인한 처리지연을 줄일 뿐 아니라, 시스템의 부하감소로 인한 시스템의 안정성을 향상시킨다[1].

이 글에서는 IPSec 기반 VPN 보안 기능을 모토롤라의 MPC180 보안 프로세서를 사용하여 하드웨어적으로 홈게이트웨이 시스템에 구현하여 그 성능을 분석한 결과 소프트웨어적으로는 만족할 수 없는[2] 사용자 요구사항인 통신속도를 만족할 수 있음을 보였다.

2. MPC180 기반 보안 기능 구현

VPN 에서 보안기능을 가능하게 하는 주요 기술은 터널링 기술과 암호화 기술이다.

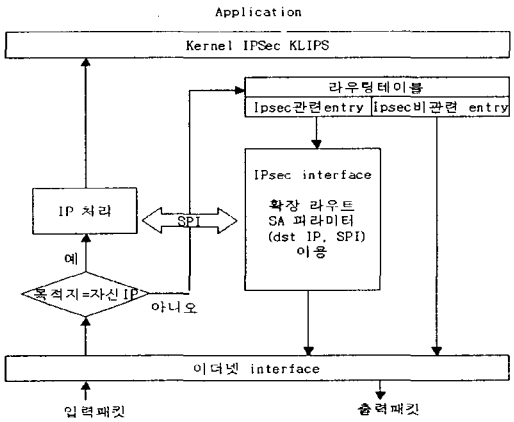
터널링 기술은 종단간에 IP 패킷의 캡슐화 기능, 압축 기능을 수행하며, PPTP, L2F, L2TP 등은 2 계층 터널링 프로토콜이다. 반면 IPSec 은 네트워크 계층인 3 계층에서 이루어지는 터널링 프로토콜로 IPv6 에는 필수 구현 프로토콜로 되어 있으나, 현재의 IPv4 프로토콜에서는 선택적으로 구현하도록 되어 있다.

암호화 기술은 인터넷을 통해 전달되는 IP 패킷이 스푸핑(spoofing), 스니핑(sniffing)등의 공격에 따른 정보의 외부 노출을 방지하기 위해 패킷의 송신자를 확인하는 인증, 전송중에 변경이 없음을 보장하는 Integrity, replay protection 및 전송되는 패킷의 내용을 숨기는 기밀성의 특성을 제공한다. 암호화 알고리즘으로는 DES, 3DES, RC4/5, IDEA, SEED, CAST 등이 있으며, 우리나라의 경우 SEED 암호화를 지원하고 있다.

홈게이트웨이 보안기능에서 제공되는 암호 알고리즘은 암호화를 위한 3DES, 암호 해쉬를 위한 SHA-1, 키교환을 위한 Diffie-Hellman Group 5(1024 bit MODP), 인증을 위한 대칭키 방식을 사용하고 있다.

IPSec 을 구현하는 방법에는 3 가지가 있으며, TCP/IP 의 소스가 공개되지 않은 환경에서 구현하기 위한 방법으로 기존 TCP/IP 스택과 네트워크 디바이스 드라이버 사이에 IPSec 스택을 넣어서 구현하는 BITS (Bump in the stack) 방법, 네트워크 선로상에 IPSec 기반 장비를 넣어서 구현하는 BITW (Bump in the wire) 방법 및 TCP/IP 소스가 공개되어 있는 경우 IPSec 을 통합하여 구현하는 통합 방법이 있다. 홈게이트웨이는 통합 방법으로 구현된 FreeS/WAN 을 이식하였다.

홈게이트웨이 VPN 은 IPSec 을 리눅스 운영체계에 구현한 KLIPS (Kernel Level IP Security)와 키 교환을 위한 IKE 기능을 구현한 데몬인 Pluto 로 구성되어 있다.[5]



(그림 2) IPSec 에서의 패킷 처리 흐름도

(그림 2)는 IPSec 기반 VPN 에서 패킷처리 흐름도이다. 홈네트워크인 사설망에서 입력되어 홈게이트웨이 VPN 서버로 출력되는 외부출력 패킷(outbound packet)은 시스템 관리자에 정의는 (표 1)의 정보를 가지고 있는 SPD(Security Policy Database : 보안정책 데이터 베이스)를 참고하여 기록된 규칙에 따라 처리된다. 만약 IPSec 프로토콜을 사용하면 SPD 에 저장된 SA(Security Association) 인덱스에 따라 처리한다.

(표 1) SPD 테이블 정보

규칙 #	출발지		목적지		동작	IPSec		Outbound SA index
	IP	포트	IP	포트		프로토콜	모드	
					IPSec Accept	AH ESP	Tunnel Transport	

외부망에서 입력되어 홈게이트웨이 VPN 서버를 거쳐 홈네트워크로 가는 외부입력 패킷(inbound packet)은 패킷의 헤더로부터 SPI, 목적지 IP, IPSec

데이터 처리 프로토콜의 정보를 인덱스로 하여 (표 2)의 정보 테이블에서 SA 의 존재 여부를 확인하고, 존재하면 사용 프로토콜에 따라 인증과 암호화 기능을 수행하여 암호화되지 않은 헤더를 가지고 SPD 를 검색하여 패킷의 포워딩, 폐기, 상위 계층으로 통과를 결정하게 된다.

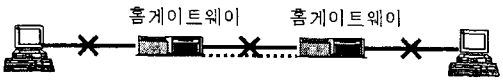
(표 2) SAD 테이블 정보

SA				IPSec				SPD
SPI	bundle	출발지 IP	목적지 IP	프로토콜	모드	타입	기타	규칙#
				AH ESP	Tunnel Transport	Outbound Inbound	Lifetime Key	

3. 고속 VPN 기능 분석

VPN 성능을 측정하기 위한 방법으로 Smartbits 와 같은 성능측정 장비를 사용하여 홈게이트웨이 VPN 자체의 성능을 측정할 수 있겠으나, 사용자 관점에서 성능을 측정할 수 있도록 (그림 3)과 같이 구성하여 위에서 제시한 실제적인 성능 측정이 가능하도록 netpipe 도구를 사용하여 제시하였다.

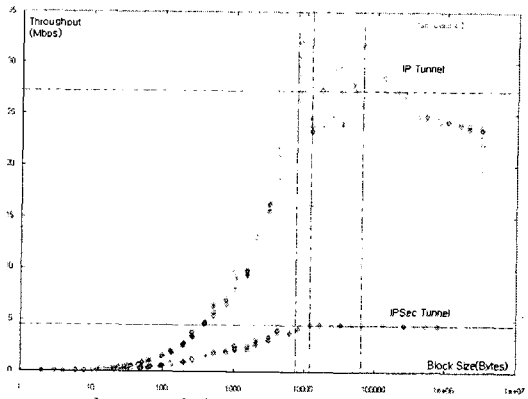
시험에 사용된 홈게이트웨이는 현재 개발 중으로 200MHz 의 클럭 속도를 가지는 MPC8260 프로세서를 사용하였으며, 실제적인 수행 환경에서 245 Dhrystone MIPS 의 속도를 가진다. 종단의 클라이언트는 550MHz 의 펜티움 III 프로세서와 Windows 를 사용하였다.



(그림 3) 성능측정 형상

홈게이트웨이와 클라이언트와의 연결은 네트워크 요소들의 간접적인 영향을 배제하기 위해 크로스케이블 사용하여 연결하였고, 홈네트워크 환경과 동일하게 구성하기 위해 내부는 사설 주소를 사용하여 연결하였다. VPN 서버의 경우 터널 모드로 동작 시에는 사설망간의 클라이언트의 통신이 가능하나, 일반적인 연결에서는 불가능하므로 IP 터널링을 사용하였다.

상기 방법으로 실험한 경우 IP 터널을 사용한 경우 최대 32 Mbps, IPSec 터널을 사용한 경우 최대 4.6 Mbps 속도를 나타내었다. 전자의 경우 CPU 의 유휴율은 50~60%를 유지하나, 후자의 경우 4.6 Mbps 의 최고 성능을 가질 때 0%를 나타내고 있다. IPSec 터널의 경우 보내는 데이터이 양이 암호화 처리 능력을 초과하므로 라인의 속도에 무관에게 일정한 속도를 유지한다. 이는 암호화를 처리를 위해 MPC8260 처리 능력으로는 홈게이트웨이 VPN 서버 기능으로는 한계가 있으며, 하드웨어적인 암호화 방법을 도입해야 함을 의미한다.



(그림 4) IP 터널 및 IPSec 터널의 성능 비교

다른 예로서, 상기와 유사한 환경을 가지는 MPC8260 시스템(Linux 2.4.16, FreeS/WAN 1.95)을 상호 크로스 케이블로 연결하고 Smartbits 로 성능 측정한 결과[6]는 (표 3)과 같으며, 이는 VPN 동작환경 및 리소스를 고려하지 않은 측정방법으로 특히, 홈네트워크 환경은 사설망으로 구성되어 있으며 이를 처리하기 위한 오버헤드 등이 전혀 고려되지 않고 있다.

(표 3) IPSec 성능

	Normal	IPSec
64 바이트	15.9 Mbps	1.48 Mbps
1018 바이트	98.4 Mbps	6.07 Mbps

4. 결론

통합 방법으로 리눅스에 구현된 IPSec 프로토콜의 개념과 처리 흐름을 살펴 보고, MPC180 보안 프로세서에서 제공하는 암호화 알고리즘을 사용할 수 있도록 수정 구현하였다.

MPC180 보안 프로세서를 사용하여 구현한 VPN 시스템을 보안 기능이 제공되지 않는 IP 터널 기능과 소프트웨어적으로 구현된 VPN 터널 기능과 성능을 비교 분석한 결과, 암호를 적용하지 않는 IP 터널인 경우 25 Mbps 정도의 속도를 가지며, 암호화를 소프트웨어적으로 적용한 VPN 터널은 4.5 Mbps 정도인데 반해, MPC 180 보안 프로세서를 적용한 VPN 은 물리적인 성능은 15 Mbps 정도의 통신속도를 제공하나 성능측정 결과는 ADSL 최대 통신속도인 8 Mbps 로 분석되었다.

사용한 운영체계가 리눅스이며 커널 preemption 을 허용하지 않음을 감안할 때 적절한 속도라 사료되며 MPC180 보안 프로세서를 충분히 활용하기 위해서는 다중 쓰레드를 지원하는 운영체계의 사용도 필수적이라 할 수 있다.

참고문헌

[1] 주학수,주홍돈,김승주, "고속 암호연산 프로세서 개발현황," 정보보호학회지, 제 12 권 제 3 호, 2002.6.
[2] 김재명, 박광로, "홈게이트웨이에서의 IPSec 기반 VPN 기능 구현 및 성능측정 분석," COMSW 2002.
[3] Global Crossing, "Network-based IP VPN Performance," White Paper, 2001. 9.27. http://www.globalcrossing.com/xml/news/whitepapers/ipvpn_performance.pdf.
[4] 주간기술동향,"VPN 기술 및 시장 동향," 2002.04.10.
[5] Steve Burnmett and Stephen Paine, RSA Security's Official Guide to Cryptography, McGraw-Hill, 2001.
[6] http://ykjung99.netian.com/news/VPN_Perf.JPG
[7] Oleg Kolesnikov and Brian Hatch, Building Linux Virtual Private Networks, New Riders, 2002.
[8] Quinn O. Snell, Armin R. Mikler and John L.Gustafson, "NetPIPE: A Network Protocol Independent Performance Evaluator," http://www.scl.ameslab.gov/netpipe/.