2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

IP계층에서의 VPN 전송성능에 관한 연구

임형진*, 정태명**
성균관대학교 전기 전자 및 컴퓨터 공학부

e-mail:limhj@www.hallym.or.kr
tmchung@ece.skku.ac.kr

Secure VPN Performance in IP Layers

Hyung-Jin Lim* and Tai M. Chung**
School Of Electrical and Computer Engineering,
Sungkyunkwan University

요약

본 논문에서는 IPSec을 리눅스에서 구현하여 AH, ESP 프로토콜 사용시 노드간 성능을 측정하여 네트웍에서의 보안성능대 처리성능에 대하여 분석하였다.IPSec VPN은 노드간 호스트간 정보보호와 안전한 응용에 대하여 IP계층에서 구현된 보호서비스를 이용할수 있게 하지만 IPSec에서 사용하는 AH와 ESP에서의 인증데이터의 계산 및 비교, 암호화와 복호화에 의하여 IP프로토콜의 처리비용 및 통신에 대한 잠재비용이 증가하게 된다.이에 각 프로토콜에서 전송데이타 크기의 점진적 변경에 따라 커널에서 IPSec모듈내 처리 시간과 전체 데이터의 처리시간을 측정하여 보았다. 데이터 전송 크기가 증가함에 따라 Non IPSec 전송에 비하여 IPSsec 전송시 처리지연 시간의 차는 증대되었다. 본 논문에서는 이러한 성능차이를 야기하는 인자들을 평가하여 향후 기존 네트웍에 VPN도입시 성능대 보안에서의 정책결정의 기반이 될 수 있는 분석을 제시하고 있다.

1.서론

90년대 이후에 인터넷은 개인뿐만 아니라 기업체들에게 기업간 혹은 기업내부간의 새로운 통신매체로서 자리잡아 가고 있으며 21세기 정보화 시대에 있어 정보화 사회의 기반 구조가 되고 있다. 이러한 인터넷에는 많은 다른 기술들이 융합되어 있고, 신뢰성과 보안이 요구되어지는 통신영역기술들로서 계속 발전되어가고 있다. 기업측면에서는 분산된 기업내의 통신을 위하여 통신 사업자의 전송장비를 임대하여 사설 통신망을 구축해 왔으며 이는 그 범위, 규모에 따라 상당한 어려움과 많은 비용이 소요된다.

전용선에 의한 사설망이 아닌 인터넷 VPN으로의 변화는 저렴한 가격에, 유연성과 확장성을 제공할 수 있는 서비스를 제공할 수 있으나, 반면에 인터넷의 특징인 보안상의 위험, 인터넷의 성능을 예측할 수 없다는 단점을 갖고 있다. 이에 반해 터널링 프로토콜 사용을 통해 공중망을 통과하는 사설망의 트래픽들에 보안성을 제공하며, 성능에 있어서는 RSVP, MPLS와 같은 기술을 통하여 보장된 대역폭을 확보하고자 한다.[9,10,13,14]

터널을 형성할 수 있는 프로토콜은 각 계층별로 정의되어지나 IPSec은 IETF 표준 프로토콜로서 네트워크 계층의 프로토콜인 IP를 사용하면서 키 관리, 인증, 암호화기능을 제공하며, IPv4에서 구현이 가능한 대규모의 인터넷 환경에 적합한 보안 프로토콜이다.[11,15]

본 논문은 IP기반에 적용 가능한 IPSec을 리눅스에서 구현하여 AH, ESP프로토콜을 사용하여 노드간 네트웍의 영향을 측정하고자 하며 이는 향후 기존 네트웍에 VPN 도입시 보안성능과 처리성능의 비교는 적절한 정책결정에 기반이 될 수 있을 것이다. 이를 위하여 본 논문에서는 2장에서 현재 IETF 표준인 IPSec에 대하여 기술하고, 3장에서는 현재 구현된 IPSec 제품군의 성능을 비교하며 4장에서는 본 논문에서 구현된 리눅스상의 IPSec과 성능테스트방식, 성능테스트 결과와 분석을 보여준다.

2장 IPSec의 개요

IPSec은 IETF에 의하여 표준화된 암호화와 관련된 시스템구조 및 키 관리 프로토콜로 IP계층의 확장된 형태로서 두 개체간에 통신에서 프라이버시와 인증 기능을 제공한다.

주요 구성요소에 의한 처리과정으로 IPSec은 시스템으로 하여금 보안 프로토콜을 선택하고, 암호화 알고리즘을 결정하며, 암호화 키를 결정 할 수 있게 함으로서 IP계층에서 보안

서비스를 제공할 수 있도록 한다. IPSec은 두 호스트사이, 두 보안 게이트웨이 사이, 또는 보안 게이트웨이와 호스트사이의 통신을 보호하기 위해 사용할 수 있다. IPSec이 제공할 수 있는 보안 서비스는 접근제어, 무결성, 데이터 출처인증, 재연된 패킷의 거부, 기밀성 그리고 제한된 트래픽 흐름 기밀성이다.[11]

IPSec의 보안프로토콜인 AH, ESP는 보호되는 데이터 영역에 따라 터널모드와 트랜트포트모드 두 가지 운용모드를 갖는다. 트랜스포트 모드는 일반적으로 보안 호스트 구현시 사용되며 상위 계층 프로토콜에 대한 보호 서비스를 제공한다. 터널모드의 경우 터널이 형성되는 시작점과 끝점을 인식할 수 있도록 하기 위해서 보안 호스트 및 게이트웨이 구현시 모두 적용되며 외부 IP헤더를 새로이 생성하여 내부 IP헤더를 포함한 IP패킷 전체에 대한 보호 서비스를 제공한다.[1,2,11]

IPsec 보안프로토콜인 AH는 전송패킷에 대하여 리프레이 방지와 IP데이터그램에 대한 인증, 무결성을 제공하며, ESP는 IP패킷의 비밀성과 무결성, 인증, 리플레이 방지 기능을 제공한다. ESP 암호화는 공유 대칭키를 사용하며 이를 통신 당사자간에 서로 교환하여 암호화 함수(DES, RSA)에 의해 암호화와 복호화에 사용한다. ESP가 인증 기능을 제공할 때 AH에서와 같은 인증(MD5, SHA-1)알고리즘을 사용한다.[4,5,11]

IPSec 처리과정은 IPSec헤더 생성과정과 메시지 인증 및 암호화 과정으로 구분된다. IPSec 헤더 생성은 IP와 TCP(또는 UDP)사이에 위치해야하고,AH인 경우 생성된 헤더의 인증 필드에 AH상위 계층에 대한 인증값을, ESP인 경우 생성된 헤더의 페이로드 필드에 ESP헤더 상위 계층에 대한 암호화한 값을 포함해야 한다.[3,6,7,11]

3장 IPSec제품의 성능비교

IPSec제품은 IPSec제품군의 일부로서 IPSec제품군이라함은 IPSec을 지원하는 호스트 시스템, 게이트웨이 시스템, 라우터 VPN서버, 방화벽 장비 및 이들 장비를 제어 통제하는 소프트웨어를 포함한다. 이러한 장비들은 복잡성, 규모, 범위 목적에 따라 다양하기 때문에 VPN구현시 표준안에 근거하는 적용기술과 이들에 대한 적절한 조합을 고려해야 한다. 현재 많은 수의 인터넷 장비 제조 업체에서 IPSec을 지원하는 제품들을 생산 판매하고 있으며 ICSA의 인증 제품 중심으로 그 성능을 비교해 보았다. ICSA는 항 바이러스 제품, 방화벽 IPSec/VPN장비, 암호화 장비 및 모니터링 장비 등 네트웍 보안과 관련된 장비에 대한 인증 서비스를 해주는 곳으로 인터넷에서 다중 벤더의 VPN 네트웍이 가능하도록 표준에 기반한 IPSec VPN기술에 대한 상호운용성을 보증하는데 목적을 두고 있다. 현재 Cisco를 비롯하여 IBM, Lucent등 대규모 인터넷 장비공급업체에서 생산된 IPSec제품들이 ICSA의 장비 보증 서비스를 통해 인증받고 있다. IPSec버전 1.0A 장비 제품 인증프로그램은 총 6가지로 인증제품간 상호운용성, IKE, IPSEC 프로토콜, 암호, 인증항목에 관하여 상세요구, 선택기능항목들에 대하여 테스트하여 현재 1.0A를 기반으로 한 IPSec장비인증을 마친 상태이며 현재는 범주 1.0A의 선택항목을 요구 항목으로 하여 범주 1.0B에 대한 테스트를 진행하고 있다.

ICSA에서 IPSec에 대한 인증 절차를 통과한 제품들은 기본적으로 인증, 무결성 및 비밀성 제공을 위한 기본적인 요구사항들을 만족하고, 인증 레벨별로 3-DES의 지원여부나, 다른 암호화함수 지원 여부, 압축기능여부와 최종적으로 인증처리까지 테스트가 진행되고 있다.

대부분의 VPN장비들은 기본적으로 인터넷 표준 프로토콜인 IPSec을 지원하고 있고, 이러한 장비업체들은 보안관련 상품을 개발하는 곳으로서 기존의 파이어월시스템에 부가적인 기능으로서 IPSec기능을 부가하거나 네트웍 장비업체로서 기존의 라우터에 IPSec기능을 추가하고 있다. 사용자 인증을 위해서 공개키 알고리즘을 사용하고 있으며 이를 위해 다른 PKI를 제공하는 회사들(VeriSign, Entrust등)로부터 서비스들과 연동되고 있다. 암호화에 사용되는 알고리즘으로는 주로 56bit-DES를 사용하고 강한 인증을 위하여 168bit-3DES가 제공되고 있으며 일부 제품에서는 암호전용의 프로세서를 지원하고 있다. 기본적으로 사용되는 인증함수로서는 MD5(56bit), SHA1을 지원하고 있으며 또한 키관리에 있어서는 ISAKMP/Oakly, SKIP가 기본모드로 지원되고 있다.[17]

일부 제품명세서에서는 최대 사용 가능한 터널수가 명기되어 있으나 이는 전용프로세서 여부나 터널에 사용된 암호알고리즘, 제품에서 제공하는 대역폭에 따라 다르기 때문에 절대적 수치는 되지 않으며 단지 현재 판매되는 제품들에 대하여 한정된 대역폭에서 터널사용자수를 가늠하여 볼 수 있게 한다. 파이어월 장비와 통합된 모듈에서는 non IPSec 트래픽에 대한 bypass를 통하여 성능을 고려하였고, 일부 제품에서는 주 혹은 보조 게이트웨이를 통하여 single point failure에 대한 백업기능을 제공하고 있다. 본 논문에서 조사된 ICSA인증 제품들 이외에도 IPSec 제품들은 여러 업체에서 다양한 규모와 사양의 제품들이 생산되고 있다.[17]

4장. 성능평가 및 결과

4.1 IPSec 구현방식

본 논문에서는 리눅스 커널에서 IPSec의 일괄처리를 위해 새로운 버퍼를 할당하는 방식을 사용하였으며,

이 처리방식의 특징은 호스트 구현방식으로 순차적헤더 생성 순서를 유지하는 방식에 비해 성능에 있어서는 거의 차이를 보이지 않지만 기존의 커널 소스에 변경을 최소화하면서 트랜스포트 계층과의 독립성을 보장하고 IPSec헤더 생성 모듈과 처리모듈의 통합으로 인한 IPSec모듈의 확장성을 보장하고 있다. [12]

4.2 성능평가 환경

본 장에서는 위에서 기술한 리눅스에서 구현된 IPSec을 이용한 성능측정 방식에 대하여 기술한다.성능 측정은 다음과 같은 환경에서 평가되어진다.

- 리눅스 커널 버전 : 3.0.35
- 구현에 사용된 언어 : C언어
- Network Interface Card Driver : 3Com EtherLink 3 3c509TP
- 네트웍 환경: Shared 10Mbps
- Host CPU: Pentium-3 550MHz

또한, 향후 IPSec기술에 가장 많은 응용서비스들로 사용이 예상되고 있는 SMTP, Telnet, FTP프로토콜들에 대하여 전송 패킷의 크기에 따르는 전송에 대한 처리속도를 1:1 호스트간 연결상에서 IPSec 전송모드와 프로토콜 그리고 사용되는 암호, 인증 함수를 측정인자들로 하여 테스트하였으며 non IPSec 트래픽에 대한 상대적 처리속도를 비교하였다.[8,16]

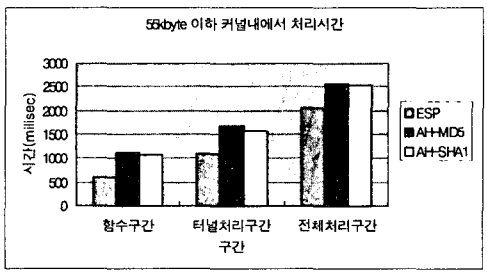
성능평가는 트랜스포트모드에서 AH, ESP 프로토콜에서 1byte부터 4Mbyte까지의 전송크기의 점진적 변경에 따라 커널에서 IPSec모듈내 처리 시간과 전체 데이터 처리시간을 체크했으며, 커널에서의 시간 측정은 위 구성도에서 select SPD의 전후와 각 암호, 인증함수를 호출하는 부분의 전후에서 측정하였다.

또한 인증에 사용되는 해쉬함수로서 128bit 키를 사용하는 SHA-1,MD5를 사용하였으며, 암호함수로서는 64비트의 키를 사용하는 DES-CBC를 사용하였다.

IPSec 구현에 있어서 SA와 키 관리 부분은 수동설정 방식을 사용하였으며, 각 전송프로토콜 별, 모드별로 SAD와 SPD의 파일을 수정하였다.SPD에는 선택자로서 송, 수신지 주소, 전송프로토콜, 송수신 포트가 기술되고, SAD에는 전송에 사용되는 암호, 인증알고리즘, 모드등의 정보들이 기술되며 데이터 전송시 관련정보를 통해 SAD를 참조하여 IPSec모듈이 동작된다.

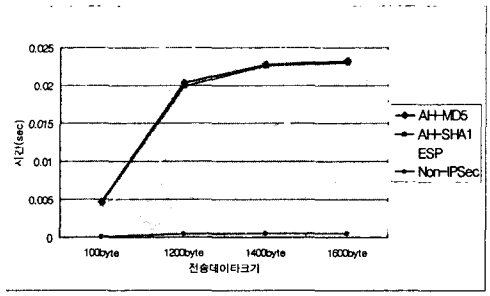
4.3 성능 평가 결과

우선 FTP전송에 대하여 테스트해 보았다.FTP 전송에 있어서 Non IPSec 전송을 측정의 비교기준으로 하여 IPSec데이타들을 측정하였다. 그림2는 56kbyte를 기준으로 데이터 전송시 보여주는 결과로 그림 2에서 보여주는 결과는 Non IPsec 전송에 비하여 IPSec전송데이타에서 더 많은 처리시간

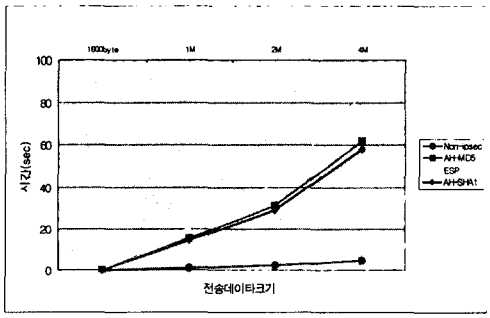


<그림1> 커널내에서의 처리시간

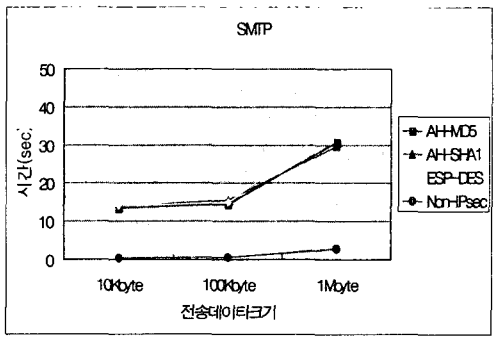
이 소요됨을 보여주고 있는데 100byte경우 처리시간에 대한 비율로 보면 Non IPSec에 대하여 AH, ESP가 각각 53배,42배의 처리시간이 증가하였다. 그러나 이는 시간 단위가 milisecond단위로서 초단위로 본다면 별 차이가 없다고 할 수 있다.1000byte 단위에서의 전송처리비율은 AH, ESP가 각각 40배,30배의 처리 시간이 증가하였다.56Kbyte이하 IPSec 트래픽의 처리시 인증시에 처리되는 시간이 암호화에 처리시간 보다 더 많은 시간이 소요되고 있음을 보여주고 있다.Non-IPSec에 비한 처리 시간의 증가는 그림 1에서 보여주는 것과 같이 IPSec 전송 데이터가 IPSec처리 모듈을 거



<그림2>56Kbyte이하 FTP 처리시간



<그림3> 56Kbyte이상 FTP처리시간



<그림4> SMTP에서의 처리시간

치면서 처리 시간이 더 소요되기 때문이며 각 프로토콜별 사용함수에 따른 처리시간의 차가 데이터 전송량에 따라 영향을 주어 Non IPSec전송에 비하여 처리시간이 증가함을 나타내주고 있다.

그림 3의 경우는 56Kbyte이상의 데이터 전송시 처리시간을 보여주는 것으로 AH, ESP에 대하여 12.4배,17.6배의 처리 시간의 증가를 보여주고 있다.56kbyte 이하데이타 처리 결과와의 차이로는 ESP처리시 AH프로토콜 처리에서보다 많은 시간이 소요되고 있다.전송데이타 크기가 증가할수록 Non IPSec전송보다 IPSec처리에서 현저한 시간이 소요되고 있음을 보여주고 있다. 도표에는 나타나지 않지만 10Mbyte 정도의 데이터 전송시는 전송호스트의 hanging현상도 나타났으며 이는 ESP, AH프로토콜을 처리하기 위해 CPU의 모든 자

원이 점유됨으로 생기는 현상이다.
SMTP 전송에 있어서는 전송파일의 크기가 10Kbyte일 경우 Non IPSec 전송에 비하여 IPSec 전송시간이 AH, ESP경우 35배,30배의 처리시간이 증가하였으나 1M의 파일을 전송하였을 경우 11배,13배의 처리시간이 증가하였다.FTP에서와 같이 전송파일을 크기가 증가할수록 ESP암호화 모듈에서의 처리시간이 더 소요되었다.

5장. 결론

본 논문은 IP계층 IPSec VPN에서 전송 프로토콜과 모드에 따라 응용계층 프로토콜들의 전송성능에 관한 성능을 테스트하였다. IPSec VPN은 노드간 호스트간 정보보호와 안전한 응용에 대하여 IP 계층에서 구현된 보호서비스를 이용할 수 있게 한다. 하지만 IPSec에서 사용하는 AH와 ESP의 사용은 IP프로토콜의 처리비용의 증가로 인해 보안성능은 증대시키지만 처리성능을 감소시킬 수 있다. 이점을 감안하여 성능테스트를 한 결과 Non IPSec전송에 비하여 ESP와 AH에서 사용하는 암호/인증 함수에 의해 전송량에 대한 처리지연이 나타났으며 수백 바이트 범위에서는 인증 함수에서, 수천 바이트 이상에서는 암호함수에 의한 더 많은 처리 지연이 나타났으며 Non IPSec 전송에 비하여 전송량이 증가할수록 심한 지연이 나타났다.
성능테스트 결과 전송패킷크기와 사용하는 암호, 인증함수, 호스트의 CPU속도, IPSec의 구현방식이 IPSec 전송성능에 영향을 주는 인자로 나타났다.telnet 경우 1byte단위의 통신방식을 사용하기 때문에 IPSec전송에 의한 처리시간 지연은 적다. 그러나 파일전송의 경우 전송용량이 증가하게되면 10여배 정도의 처리지연이 나타나고 있다. 축적 전송방식의 SMTP 경우에서도 전송 량이 증가할수록 데이타를 물리계층으로 내보내기까지의 지연시간이 증가했다.
본 논문의 성능테스트에서처럼 IPSec의 구현이 호스트 기반, 라우터 기반 구현됨에 있어서 전송량의 증가에 따라 CPU가 암호, 인증 처리로 인해 모든 CPU자원을 점유하게되어 hanging현상을 유발할 수 도 있다. IPSec의 도입이 기존 네트웍에 부가적인 서비스형태로 제공되어질 때 보안 강도의 유지와 기존 서비스들에 영향을 최소화하는 CPU성능을 유지하거나 부가적인 전용 암호화 모듈이 필요하다.
IPSec 모드에는 AH, ESP, Bypass 모드가 있으나, 본 논문에서는 IPSec을 통한 전송 데이타의 보호에 있어서 처리시간을 Non IPSec트래픽에 대하여 비교하였다.Non IPSec트래픽과 Bypass 모드의 전송처리시간은 구현방식에 따라 차이가 날 수 있음을 고려해야 한다. 본 논문에 구현된 Bypass 모드는 Non IPSec 전송에 비해 3-4배의 전송시간이 더 걸렸으며 이는 IPSec 모듈의 추가에 따른 커널 루틴의 변경 때문이었다.
많은 네트웍 업체들에서 VPN장비를 제공하고 있으며 구축하는 업체들에서는 기존의 네트웍에 진화모델로서의 적용이라고 할 때 현재 네트웍의 트래픽의 형태에 따라 보안강도를 조정해야 할 필요가 있다. 기존 네트웍에 VPN적용은 수백 바이트 이하 단위의 인터넷 트래픽에 적절한 방식일수 있으며 지연에 민감한 동영상 등의 대용량 전송방식에는 적합하지 않다고 할 수 있다.

참고문헌

[1] S. Kent, R. Atkinson, " IP Authentication Header", RFC 2402, November 1998
[2] S. Kent, R. Atkinson, " IP Encapsulating Security Payload(ESP)" , RFC 2406, November 1998
[3] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol" , RFC 2401, November 1998
[4] C. Madson, R. Glenn, "The Use of HMAC-MD5 within ESP and AH",RFC 2403, November 1998
[5] C. Madson, R. Glenn, "The Use of HMAC-SHA1 within ESP and AH", RFC 2404, November 1998
[6] Michael Beck, Harald Bohme,Mirko Dzidzka, Ulrich Kunitz, Rover Magnus,Dirk Verworner, "Linux Kernel Internals",SecondEdition, Addison-Wesley, pp227-247, 1998
[7] Gary R. Wright ,W.Richard Stevens,"TCP/IP Illustrated, Volume 2(1)", Addison Wesley, pp205-246, Jaunary 1995
[8] Charlie Scott, Paul Wolfe&Mike Erwin, "Virtual Private Network",pp135-161 O Reilly, 1999
[9] Dave Kosiur, "Virtual Private Network" ,WILEY, 1998
[10] Steven Brown,"Implementing Virtual Private Networks", McGraw-Hill, pp97-140, 1999
[11] Naganand Doraswamy, Dan Harking, "IPsec", Prentice Hall PTR, 1999
[12] 권윤주, 김현주, 정태명, "리눅스상에서의 IPSec 구현에 관한 연구, 한국 정보처리학회 추계 학 술 발표 논문집 제6권 2호,1999
[13] Brian Quirton, "The CASE from packeting VPNs", IEEE computer Society (TELEPHONY), 1999
[14] Wray West, "The ABC of Remote Access VPNs", IEEE Computer Society (BUSINESS COMMUNICATIONS REVIEW) ,1999
[15] Thomas J. routt and Jerry A.keterly, "Securing VPNS:Architectural Approach", COMMUNICATIONS Review, 1999
[16] http://etlars,etri.re.kr/Etlars/industry/jungidong/952/95304
[17] http://www.icsa.net/html/communities/ipsec/certification/certified_products/index.shtml