VPN 기술별 트래픽 부하 비교

박진형, 손주영
한국해양대학교 기계정보공학부

Comparison of Traffic Overheads of VPN Technologies

Jin-Hyeong Park, Jooyoung Son
Dept. of Mechanical and Information Engineering,
Korea Maritime University

요 약

1990년대 초반 Frame-Relay 망이 출현하면서부터 등장한 VPN 기술은 최근에도 많은 연구가 이루어지고 있다. 그러나 VPN을 형성하는 기술들이 매우 다양하고, 그 특성도 달라 실제 이용하는 측면에서는 어떤 기술에 기반한 VPN을 채택해야 하는지에 대한 기준이 분명하지 않다. 이런 기준의 하나로 VPN 기술에 따른 트래픽 부하를 들 수 있다. 따라서 본 논문에서는 현존하는 VPN 기술들에 의해 트래픽 부하가 실제 얼마나 부가하는지에 대한 실험 결과를 보인다. SP의 Frame-Relay나 ATM 망과 연동하여 ISP측에 기반통신망 없는 DSL 서비스 등을 가능케 했던 주역인 L2TP, Microsoft측에서 내어놓은 PPTP, MPLS VPN와 같이 최근에 많은 연구가 되고 있는 IP-VPN의 대표적인 예인 IPSec, 그리고 필드에서 실제 많이 구현되고 있는 조합인 IPSec/L2TP 기술에 대해 인터넷이 배제된 망에서 트래픽 부하를 측정하고 분석하였다. 이에 따라 향후 VPN 기술의 효율성 제고에 지침을 제공하고자 한다.

1. 서론

VPN 기술의 소개 이후에 많은 통신에 대한 수요를 가지고 있는 사이트에서 이용되고 있다. 이는 전용선을 설치하기에는 부족한 재원을 가지고 있거나 전용선을 설치할 만큼 많은 통신 수요가 있지 않은 경우, 경제적 이득을 제공하는 좋은 솔루션이 되고 있다.

그러나 VPN은 2 절에서 설명되는 것과 같이 매우 다양한 기술을 기반으로 형성될 수 있기 때문에, VPN 설치 시에 어떤 기술에 기반을 둘 것인지에 대한 판단을 하기가 매우 어렵다. 특히 향후 IPv6를 기반으로 하는 차세대 인터넷 환경에서는 더욱 보안성이 강화된 응용과 대규모 데이터를 발생시키는 멀티미디어 응용이 주가 될 것으로 예상이 되므로, VPN 통신망에 형성되는 트래픽 최적화는 매우 중요한 과제가 된다. VPN을 통해 사용되는 통신망에서의 응용의 성격에 맞추어 적절한 VPN 기반 기술을 선택함으로써 통신망의 부하를 최소화하고, 결과적으로 통신비용을 최대한 절감하는 효과를 얻을 수 있는 것이다.

이를 위해 본 논문에서는 현존하는 VPN 기술들에 의해 트래픽 부하가 실제 얼마나 부가하는지에 대한 실험 결과를 보인다. SP의 Frame-Relay나 ATM 망과 연동하여 ISP측에 기반통신망 없는 DSL 서비스 등을 가능케 했던 주역인 L2TP, Microsoft측에서 내어놓은 PPTP, MPLS VPN와 같이 최근에 많은 연구가 되고 있는 IP-VPN의 대표적인 예인 IPSec, 그리고 필드에서 실제 많이 구현되고 있는 조합인 IPSec/L2TP 기술에 대해 인터넷이 배제된 망에서 트래픽 부하를 측정하고 분석하였다. 이에 따라 향후 VPN 기술의 효율성 제고에 지침을 제공하고자 한다.

2. VPN 기술 개요

1990년대 전용선을 설치하는데 드는 비용보다 저렴하면서도 전용선과 비슷한 기능을 제공해 주는 프레임 릴레이(Frame-Relay) 망이 등장을 하면서 전용선은 프레임 릴레이로 차츰 바뀌게 되었다. 그리고 신속한 패킷 전송을 위한 비동기전송모드(ATM) 기술이 등장하면서 일부 백본망들은 비동기전송모드로 구성되어 왔다. 하지만 이들 망들은 원격 접근(Remote Access)을 위해서는 적절치 못한 단점을 안고 있었고, 이 점을 해결하기 위해 L2F(Layer 2 Forwarding)를 계승한 L2TP(Layer 2 Tunneling Protocol)가 등장하게 되었다. L2TP는 IETF를 통하여 표준화된 IP 터널

링 프로토콜 중 한 가지로서 PPP 프레임을 캡슐화한 다음 X.25, IP, 프레임릴레이, 비동기전송모드 등의 망으로 전송하게 된다. L2TP가 등장하면서 ILECs나 IXCs와 같은 SP는 ISP측에 다이얼 업(dial-up) 서비스나 xDSL 서비스를 제공하게 되었으며 ISP측은 기반 통신망이 없이도 사용자에게 서비스를 제공할 수 있게 되었다.[1]

Microsoft에서 개발한 PPTP(Point to Point Tunneling Protocol) 기술은 터널링 프로토콜 중에서 개선된 GRE(Enhanced Generic Routing Encapsulation)를 사용하여 터널을 형성한다. PPTP는 터널의 유지보수를 위해 TCP 연결을 사용하며 인증과 암호화를 제공하기 위해 PPP를 이용하며 GRE를 이용해 내부의 데이터는 숨겨 전송한다.[2] 또, 응용 계층에서 사용자 ID와 암호로서 인증된 사용자를 구분하므로 장비와 IP 주소를 기반으로 인증을 하는 IPSec(IP Security)과는 달리 사용자 단위의 인증을 할 수 있다는 장점이 있다.

PPTP는 L2TP/IPSec이나 L2TP/PPP, 그리고 IPSec 등과 달리 NAT(Network Address Translation)와 연동해서 사용해도 문제가 되지 않는다는 장점이 있다. 그러나, 현재까지 드러난 PPTP의 가장 큰 문제점은 종단 대 종단이 아닌 중간장치를 거쳐서 터널을 형성하므로 패킷 자체에 대한 무결성 검사를 할 수 없기 때문에 보안상 취약점으로 가지고 있다는 점과, 터널당 한 개의 세션만 연결이 가능하여 사용할 수 있는 환경이 한정적이라는 점이다. 또한, PPTP는 비동기전송모드 망을 지원하지 못한다는 점이 단점이다.

최근에는 2계층 터널링 기술인 L2TP와 3계층 터널링 기술인 IPSec을 같이 사용하는 경우도 많다. 이는 L2TP의 동적 터널 할당(Dynamic Tunnel Allocation) 기능에 IPSec을 사용함으로써 더 보안이 강화된 환경에서 사용 가능하며 패킷의 무결성도 보장해 줄 수 있기 때문이다.[3] 그 이후 인터넷이 보급되고 백본망이 MPLS 망이나 IP 망으로 대체되면서 IP-VPN이 등장하게 되었고 IETF에 의해 IP Security(IPSec) 기술이 등장하게 되었다.

현재 IETF는 실행위원회(work group)를 두 개로 분리하여 MPLS-VPN과 IPSec-VPN에 대한 연구를 계속하고 있으며, IPSec 기술은 현재 종단간(end-to-end) 기술보다는 원격 접근(remote-access) 쪽에 많이 사용되는 기술이며 사용자 지점부터 SP의 POP 지점까지를 연결하여 서비스를 제공하고 있다.[4] 하지만 IPSec은 부하를 많이 가지는 특성에 따라 제한적으로 사용되고 있으며 높은 보안성을 요구하는 분야에서 주로 사용되고 있다.

3. VPN 부하 실험환경

3.1 End-to-end 실험환경

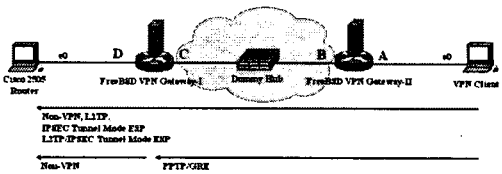

그림1. End-to-end 실험환경의 망구성도

VPN 클라이언트에서 Cisco 2505 라우터의 자체 내장형 HTTP 서버와의 통신, Telnet 서버로의 접속, 그리고 32 옥텟의 페이로드(Payload)를 갖는 Ping 서비스를 각각 실시하였다. PPTP의 경우는 Gateway-I에 PPTP 서버를 설치하여 클라이언트와의 사용자 인증을 한 후에 목적지까지 패킷을 전송하였다.

3.2 게이트웨이간 실험환경

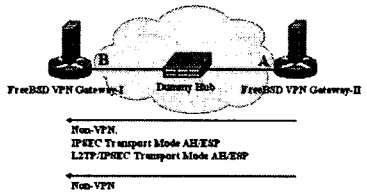

그림2. 게이트웨이간 실험환경의 망구성도

두 게이트웨이를 오가는 패킷을 대상을 VPN 기술을 적용하여 트래픽 양(패킷의 크기)을 분석하였다. 이때는 Gateway-II에서 Gateway-I으로 패킷 도달가능성 테스트(Packet Reachability Test)를 위한 대표적인 서비스인 Ping 서비스와 문자(Text) 전송을 위한 대표적인 서비스인 Telnet 서비스가 실험되어졌다.

표 1. Cisco 2505 라우터 사양

Device	Name
CPU	Motorola 68030 processor
OS	IOS version 12.0(20), C2500-IO-L
memory	8 MB flash/ 6 MB memory
Network	Ethernet e0 interface(10BaseT)

표 2. VPN 게이트웨이 사양

Device	Name
CPU	32-bit Intel PentiumIII processor
OS	FreeBSD 4.6 Stable
memory	128 MB
Network	Realtek RTL8139(A) LanCard (10BaseT)

표 3. VPN 클라이언트 시스템 사양

Device	Name
CPU	32-bit Intel PentiumII processor
OS	Windows 2000 Professional
Memory	128 MB
Network	3COM LanCard (10BaseT)

4. 실험 시나리오

먼저 VPN을 적용하지 않은 Non-VPN 모드에서 실험한다. 더미 허브에 다른 장비 및 장치들을 모두 배제한 상황에서 VPN 클라이언트를 비롯한 모든 장비에서 외부로부터의 패킷유입이 없는지 아니면 기타 디몬 프로세스(Daemon Process)나 라우팅 업데이트(Routing Update)에 의한 내부패킷 발생은 없는지 확인한 후 VPN 클라이언트에서 3.1, 3.2 절의 환경에 따라 실험을 한다. 패킷의 송수신 상황을 체크하기 위해 FreeBSD의 netstat명령을 사용하며 tcpdump와 tcpshow 프로그램을 사용한다. 이때 게이트웨이의 양단 인터페이스에서 패킷 송수신을 감시한다. PPTP, L2TP를 비롯한 여러 서비스를 위해 아래와 같이 설정한다.

1. PPTP Server: pptp server: Gateway-I
2. L2TP LNS, LAC[5]
   (1) l2tpd LNS: Gateway-I, LAC: Gateway-II
3. IPSec Gateway[6]
   (1) IPSec Stack implemented by KAME Project.[7]
   (2) Authentication : hmac-sha1 algorithm
   (3) Encryption : des-cbc algorithm

IPSec 게이트웨이의 설정 시 AH 모드와 ESP 모드를 같이 사용하는 경우는 제외하였으며, 모든 기술은 IP망에서 실험이 이루어졌다. 그리고, 두 게이트웨이는 불필요한 프로세스를 제거하여 동일한 기능을 하게 구성하였다.

5. 실험결과

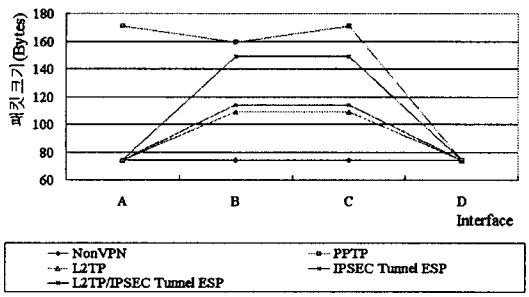

그림3. 그림1의 환경에서 Ping서비스 실험시 부하 비교

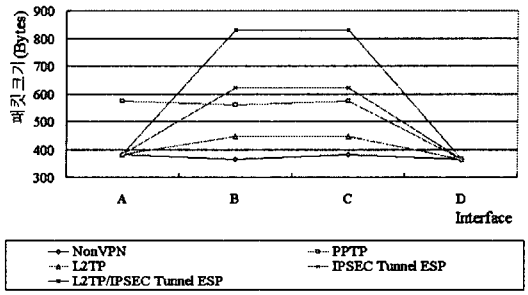

그림4. 그림1의 환경에서 Telnet서비스 실험시 부하 비교

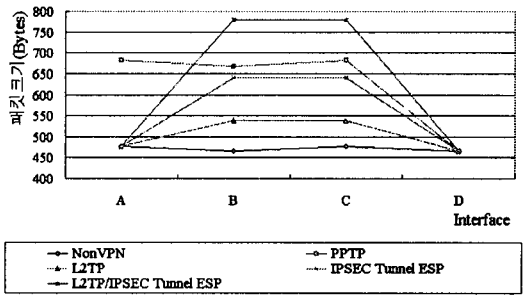

그림5. 그림1의 환경에서 HTTP서비스 실험시 부하 비교

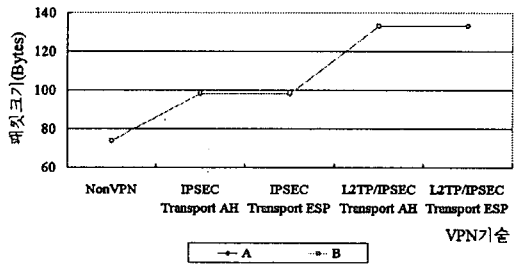

그림6. 그림2의 환경에서 ping서비스 실험시 부하 비교

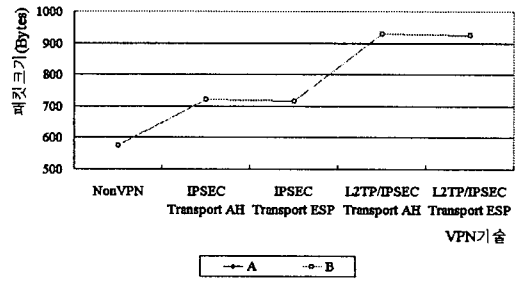

그림7. 그림2의 환경에서 telnet서비스 실험시 부하 비교

그림 3의 결과를 보면 종단간(End-to-end) 환경하의 Ping 서비스에서는 PPTP가 가장 큰 부하를 나타

냈으며 특히 클라이언트 측에서는 모든 기술에 대해 부하가 일정하게 작용이 되는 반면, PPTP만 Non-VPN에 비해 약 2.31배의 부하가 발생했으며, PPTP 서버로 가기 위해 GRE 터널을 통과하는 과정에서도 약 2.12~2.31배의 부하가 발생하는 것을 볼 수 있다. L2TP나 IPSec, L2TP/IPSec은 전체적으로 약 1.47~2.01배의 부하가 발생하며 게이트웨이사이의 터널간에는 부하가 대칭적으로 발생하였다.

문자 데이터 전달을 위한 대표적인 서비스인 telnet의 경우, 그림 4와 같이 대부분의 부하가 사다리꼴 형태로 발생하고 있으며, 두 게이트웨이간에 형성이 되어 있는 터널간에는 일정한 크기의 부하가 대칭적으로 발생하였다. 다만, PPTP만 부하가 클라이언트 쪽에 약 1.5배 정도로 크게 발생한다는 점이 특징이나 터널 내에서는 전체 그래프에서도 약 1.5배의 부하가 발생해 약 2.0배 이상 부하가 발생하는 IPSec보다는 부하가 적게 발생하는 것을 알 수 있다. 가장 부하가 크게 나타난 것은 L2TP/IPSec 이었으며 약 2.2배의 부하가 발생하였다.

현재 가장 대표적인 멀티미디어 전송 프로토콜인 HTTP(웹 브라우징)의 경우, 그림 5와 같이 L2TP/IPSec이 Non-VPN의 약 1.7배의 부하를 발생하였다. 또, PPTP가 약 1.5배를, IPSec이 그 다음으로 1.4배의 부하를 각각 나타내었다.

게이트웨이간의 실험결과인 그림 6과 7을 보면 역시 마찬가지로 L2TP/IPSec이 가장 큰 Non-VPN의 1.8배의 부하를 보였으며 AH 모드와 ESP 모드간에는 거의 차이를 보이지 않았으나 미세하게 AH모드가 많은 부하를 나타내었다.

실험 결과를 분석하면, PPTP는 ping과 같이 OSI 하위 계층에서 처리되는 패킷의 경우, 가장 많은 부하를 발생하고, 대체적으로 IPSec과 LT2P/IPSec은 과중한 부하를 나타내는 것으로 드러났다. 둘 가운데서도 L2TP/IPSec은 2중 터널을 형성하기 때문에 가장 많은 부하를 가져온다는 것을 실중할 수 있었다. 따라서 VPN을 이용하는 측면에서 활용되는 응용이 주로 보안성이 중요한 것인 경우에는 무거운 부하를 발생시킴에도 불구하고, 패킷의 무결성 보장을 위해 L2TP/IPSec을 기반으로 하는 VPN을 형성하는 것이 좋을 것이다. 반면, 실시간적이면서 대규모의 데이터 전송이 필수적인 멀티미디어 응용이 주류를 이루는 경우에는 가장 트래픽 부하 면에서 가벼운 L2TP 기반 VPN을 형성하는 것이 통신망의 효율성 측면에서 가장 유리한 선택으로 보인다.

6. 결론

본 논문에서는 가상사설망 기술 가운데 대표적인 L2TP, PPTP, 그리고 L2TP/IPSec을 실제로 구성하여 통신망에 걸리는 트래픽 부하 정도를 게이트웨이 사이에서의 부하의 정도와 클라이언트, 서버 쪽에서의 부하를 통해 실험하고 분석하였다. IP-VPN 기술은 IP 백본망에서 사용되는 IPSec과 같은 IP-VPN 기술과 프레임 릴레이, 비동기전송모드 등의 기존의 망들과 연동 가능할 뿐만 아니라 VoIP 서비스까지 포함하여 신속하게 처리 가능한 MPLS-VPN 기술로 크게 나눠져 발전되게 될 것이다[4]. 여기서 원격 접근(Remote-Access)에 주로 사용될 수 있는 L2TP/IPSec 조합의 남은 과제는 L2TP의 부하를 어느 정도 해소해 줄 수 있는 헤더 압축(Header Compression) 기술의 개발과, IPSec에서의 사용자 인증 문제이다. 이들이 조만간 개발된다면 차세대 인터넷인 IPv6 망에서의 이동 통신 수요(Mobile workforce)까지도 충분히 수용할 수 있는 원격 접근(Remote-Access) 서비스와 종단간(End-to-End) 서비스에서 입지를 굳힐 수 있을 것으로 예상된다.

[참고문헌]

[1] Jenny Carless, Ray Irani, "Layer 2 and Layer 3 VPNs.", pp1-2, Cisco systems, 2002.

[2] "PPTP Traffic Analysis.", The Cable Guy - January 2003", pp4-5, Microsoft, 2003.

[3] "Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability.", p7, Microsoft, 2000.

[4] Imran Qureshi, Stephen Wong, and Lauren Hasenhuttl, "Virtual Private Network Architectures - Comparing Multiprotocol Label Switching, IPSec, and a Combined Approach", Cisco Systems, pp. 1-5, 2003.

[5] "Sample LNS and LAC configs", marko.net mailing list. Thu, 24 Sep 1998.

[6] Josh Tiefenbach, "FreeBSD IPsec mini-HOWTO, Jan". 2001.

[7] Kame Project, http://www.kame.net/