다양한 트래픽을 이용한 VPN 프로토콜 성능 평가

오 승 희[†] · 채 기 준[††] · 남 택 용[†] · 손 승 원[†††]

요 약

오늘날 기업의 네트워크가 점차 확대되고 본사와 지사들간의 통신이 증가하면서, 공중망을 마치 사설망처럼 사용하여 안전한 데이터 전송을 통한 보안 유지, 비용 절감 그리고 운영 및 관리에 있어서의 유연성을 지닌 가상사설망이 등장하게 되었다. 현재 진행중인 가상사설망에 대한 연구는 터널링 방식이나 구현에만 그치고 있고, 실제 가상사설망을 설치하였을 경우 설치한 네트워크에 성능면에서 얼마만큼의 영향을 미치는지에 대한 연구가 부족한 상황이다. 따라서, 본 논문에서는 가상사설망을 설치했을 경우 네트워크에 미치는 영향을 파악하기 위해 직접 테스트베드를 구축하고, 실제 가상사설망 프로토콜들을 그 위에 설치한 후 트래픽을 생성하고 전송하여 실험해 보았다. 그 결과 2 계층 가상사설망을 설치한 경우가 3 계층 가상사설망을 설치한 경우보다 좋은 성능을 나타냈으며, L2TP와 IPSec을 혼합하여 설치한 경우가 성능과 보안 측면으로 비교할 때 IPSec만을 설치한 경우보다 더 낫다는 것이 확인되었다.

Performance Evaluation of VPN Protocols Using Various Traffic

Seung-Hee Oh[†] · Kijoon Chae[††] · Taekyong Nam[†] · Sungwon Sohn[†††]

ABSTRACT

Nowadays corporation networks are growing rapidly and they are needed to communicate with branch offices. Therefore, a VPN (Virtual Private Network) appears to reduce the cost of access and facilitate to manage and operate the enterprise network. Along with this trend, many studies have been done on VPN. It is important that the performance issues should be considered when VPN protocols are applied. However, most of them are limited on the tunneling methods and implementation of VPN and a few studies are performed on how installation of VPN affects the network. Therefore, in this paper, a testbed is constructed and VPN protocols are installed on it. Real traffic is generated and transmitted on the testbed to test how installing a VPN affects the network. As a result, layer 3 VPN protocol shows lower network performance than layer 2 VPN protocols. And we realize that the combination of L2TP and IPSec is the better method to install VPN than using IPSec only in the aspects of performance and security.

키워드 : 가상사설망(VPN), VPN, PPTP, L2TP, IPSec

1. 서 론

세계화 및 국제화와 발맞추어 많은 기업체들은 각 도시 또는 각 나라에 지점을 두고서 곳곳에 퍼져있는 지사들간에 안전하고 효율적으로 정보를 주고받기를 원하게 되었다. 이에 따라 이들간의 통신량이 두드러지게 증가하게 되었고, 정보를 교환하기 위해 사용하는 기존의 공중망 또는 전용망은 해외 전화를 이용하므로 비용이 증대되었으며, 여러 곳에 있는 각 지사들의 네트워크를 관리하고 운영하는데 드는 비용도 상당히 증가하였다. 가상사설망은 이런 시대적 흐름과 요구에 맞물려 공중망을 마치 사설망처럼 사용하여 안전한 데이터 전송을 통한 보안 유지, 비용 절감 그리고 운영 및 관리에 있어서의 유연성 보장이라는 세 가지 큰 장점을 가지고 등장하게 되었다.

지금까지 가상사설망을 설치하였을 경우에 얻을 수 있는 여러 가지 이점에 대한 논의는 지속되어왔으나, 특정 네트워크에 가상사설망을 설치하여 데이터를 송수신했을 경우 가상사설망이 설치된 계층별로 그 가상사설망이 트래픽 전송에 어떤 영향을 미치는지에 대한 연구는 아직까지 미미하다.

따라서 본 논문의 목적은 현재 인터넷을 사용하는 대부분의 이용자들에 의해 가장 빈번히 사용되는 트래픽을 가상사설망이 적용된 네트워크와 가상사설망이 적용되지 않은 네트워크에 종류와 양을 달리하면서 직접 전송하여, 가상사설망 설치가 네트워크에 미치는 영향을 알아보고자 한다. 이를 위해서, 가상사설망의 설치여부와 설치된 가상사설망 프로토콜의 종류에 따라 크게 7가지의 경우로 시나리오를 구성하고, 이에 따라 트래픽을 직접 생성하여 전송한다. 사용된 가상사설망 프로토콜은 2계층에서 적용되는 PPTP와 L2TP 그리고 3계층에서 적용되는 IPSec이다. 또한 현재

† 정 회 원 : 한국전자통신연구원 정보보호연구본부
†† 종신회원 : 이화여자대학교 컴퓨터학과 교수
††† 정 회 원 : 한국전자통신연구원 정보보호연구본부
논문접수 : 2001년 7월 27일, 심사완료 : 2001년 9월 24일

IETF를 통해서 좀 더 강력한 보안 제공을 위해 활발히 논의 중인 L2TP와 IPSec을 혼합하여 적용하는 경우에 대한 테스트 결과도 다룬다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 가상사설망 정의 및 터널링 기술에 대해 알아보고, 본 논문에서 사용된 가상사설망 프로토콜들에 대해 설명한다. 3장에서는 테스트베드가 구축된 환경과 테스트에서 사용된 트래픽 생성 및 분석 도구들에 대해 알아본다. 4장에서는 테스트를 통해 얻은 각 트래픽에 대한 결과를 비교·분석하며, 마지막으로 5장에서는 본 논문의 연구 결과와 향후 연구 계획에 대해서 기술한다.

2. 가상사설망 관련 연구

2.1 가상사설망 개요

가상사설망(Virtual Private Network)이란 기업의 네트워크를 구성할 때 전용 임대 회선 대신에 공중망(Public Network)을 이용하여 이것을 사설망(Private Network)처럼 사용하여 직접 운용 관리하는 것이다[1].

기업의 근무 환경이 많은 정보를 공유하는 방향으로 변화하게 됨에 따라 근로자들이 주어진 시간에 처리할 수 있는 업무가 확대되거나 근무 위치가 사무실에 국한되지 않고 집이나 업무 현장으로까지 넓혀짐으로 인하여 재택 근무자 또는 이동하는 근무자(Mobile Worker)가 증가되었다. 이러한 변화로 인하여 기업은 기업 내부에서의 정보 공유를 위한 근거리 망(Local Area Network : LAN)의 구성에서 벗어나 기업 네트워크를 확대하기 위해 외부와의 네트워크 구성이 필요하게 된 것이다. 따라서 기업은 외부와 연결된 네트워크 사이에서 자신의 정보를 안전하게 전송하기 위하여 사설망을 구성하게 되는데, 네트워크 구성에 막대한 시설 투자비용이 요구되고 네트워크 운영과 관리에 많은 인적, 금전적 요소가 요구되는 등의 문제점이 발생하게 된다. 따라서 이 같은 문제점들을 해결하고 공중망과 사설망의 단점을 해소하기 위해 가상사설망이 대두하게 되었다[2]. (그림 1)은 가상사설망의 설치 전후의 상태를 나타낸 것이다[3].

2.2 터널링(Tunneling) 기술

가상사설망을 구성하는 데 요구되는 기술은 크게 터널링 기술, 키 관리기술, 가상사설망 관리기술로 나누어진다. 여기서는 가상사설망에서 가장 중요한 핵심 기술인 보안 서비스를 가능하게 해주는 터널링 기술에 대해 살펴본다.

가상사설망은 '터널링'이라는 기법을 사용하여 일대일 연결과 같은 '터널'을 형성하며, 데이터 패킷들은 이 터널을 통해 안전하게 전달된다. 터널링은 네트워크의 하부구조를 이용하여 하나의 네트워크에서 다른 네트워크로 자료를 전송하는 방법이다. 같은 네트워크 기반 아래에서 전송지에 따라 분리된 터널 사용이 가능하므로 서로 다른 네트워크 기반을 통과하는 프로토콜을 사용할 수 있으며 여러 전송지로부터의 데이터를 차별적으로 처리할 수 있다. 터널링은 패킷/프레임의 캡슐화(Encapsulation), 전송(Transmission) 및 캡슐화 해제하는 과정(Unencapsulation)을 포함한다[4].

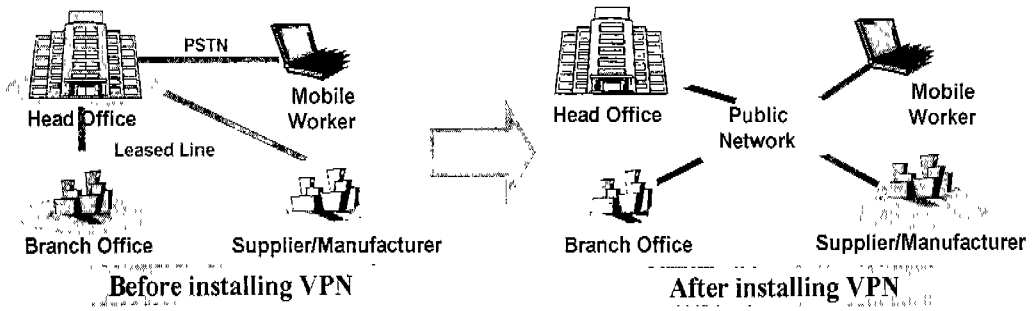
터널은 크게 사용자의 요구에 의해 생성되는 Voluntary 터널과 자동으로 생성되는 Compulsory 터널로 나눌 수 있다. 즉, 말단 사용자 컴퓨터가 터널의 종료점(Termination point)을 자신의 컴퓨터에 위치시킬지 PPP만 지원하는 ISP의 RAS에 위치시킬 지에 따라 터널의 종류가 결정된다[5].

2.2.1 Compulsory 터널

Compulsory 터널은 사용자의 요청 없이 자동적으로 생성되는 터널로 가상사설망이 가능한 다이얼-업 액세스 서버가 이 터널을 구성하고 생성하는 방식이다. Compulsory 터널에서는 사용자의 컴퓨터가 터널의 말단이 될 수 없으므로 사용자 컴퓨터와 터널 서버 사이에 존재하는 원격 접근 서버(Remote Access Server : RAS)와 같은 장치가 터널의 종단이 되며 터널 클라이언트로 작동한다.

(그림 2) Compulsory 터널링

사용자의 동의와 상관없이 자동으로 터널이 생성되기 때



(그림 1) 가상사설망(Virtual Private Network)

문에 말단 사용자에게 투명성을 제공할 수 있으며, Voluntary 터널링에 비해 다중 세션 전송에 필요한 네트워크 대역폭이 감소한다는 장점을 지니고 있다[6]. 또한 Compulsory 터널 방식은 인트라넷 밖에 있는 다른 서비스에 접근하려면 네트워크 관리자의 통제를 받아야 하고, 종단점이 미리 결정되어 사용자가 인터넷의 다른 부분에 접근할 수 없으므로 Voluntary 터널보다 나은 접근 제어를 제공한다. 반면에 말단 사용자의 컴퓨터와 RAS의 사이에 있는 초기 연결 링크가 터널 밖이므로 침입 위험이 증가하는 단점을 지니고 있다.

2.2.2 Voluntary 터널

Voluntary 터널은 특정한 목적으로 사용자가 직접 터널의 생성을 요구하는 방식이다. 즉, 사용자나 클라이언트 컴퓨터는 Voluntary 터널을 구성하고 생성하기 위해서 직접 가상사설망 요청을 발생시킨다. 이 경우, 사용자 컴퓨터는 터널 말단이 되며 터널 클라이언트로 작동한다.

특정 사용자 요구에 의해서 터널이 생성되며, 말단 사용자는 동시에 인터넷을 통해 안전한 터널을 열수 있고, 터널링 없는 기본 TCP/IP 프로토콜로 다른 인터넷 호스트에 접근 가능하다. 이 방식은 인터넷을 통해 보내지는 인트라넷 트래픽의 프라이버시와 데이터 무결성을 제공하기 위해서 사용된다. 게다가 사용자 컴퓨터까지 터널이 생성되므로 Compulsory 터널보다 강력한 보안을 제공하므로 현재 더 보편적으로 사용되고 있다.

(그림 3) Voluntary 터널링

본 논문에서는 이 두 가지 방식 중에서 강력한 보안을 제공해주는 Voluntary 터널링을 테스트베드에 적용하여 테스트하였다.

2.3 터널링 프로토콜(Tunneling Protocol)

터널링 프로토콜이란 터널 형성에 사용되는 프로토콜로써 터널이 형성되면 터널의 클라이언트와 서버는 둘 다 같은 터널링 프로토콜을 사용해야 한다. 터널링 기법은 프로토콜이 어디에서 동작하는지에 따라서 구분되며 OSI(Open Systems Interconnection) 참조 모델에서의 2계층, 3계층 또는 5계층 터널링 프로토콜을 기반으로 한다[7].

터널링 프로토콜 중 데이터 링크 계층에서 작동하는 2계층 프로토콜은 프레임 단위로 교환하며 전송될 점대점 프로토콜 프레임 상에 페이로드를 암호화한다. 2계층에서 동작하는 주요 터널링 프로토콜로는 PPTP(Point-to-Point Tunneling Protocol), L2F(Layer 2 Forwarding), L2TP(Layer 2 Tunneling Protocol)가 있다.

네트워크 계층인 3계층에서 동작하는 터널링 프로토콜은 패킷을 사용하며 대표적인 예로는 IP over IP와 IETF 표준에 의한 IP Security(IPSec)가 있다. 이 프로토콜은 IP 인터네트워크를 통하여 패킷을 전송하기 전에 부가적인 IP 헤더를 사용하여 IP 패킷을 암호화한다.

그밖에도 세션 계층에서 사용하는 터널링 프로토콜에는 SOCKS v5가 있는데, SOCKS v5는 응용 계층에서 필터링을 지원하기 위해 주로 사용된다. 이 방식은 2, 3계층 프로토콜들에 비해서 구현은 어려우나 응용 계층을 보호해 준다는 강력한 장점을 지니고 있다.

여기서는 본 논문의 테스트에서 직접 적용한 2계층 프로토콜인 PPTP와 L2TP, 3계층 프로토콜인 IPSec에 대해서 자세히 살펴본다.

2.3.1 2계층 프로토콜 : PPTP

PPTP는 PPTP 포럼에서 제안된 것으로 멀리 떨어져 있는 클라이언트와 사설망 사이에 안전한 연결을 제공하는 인터넷 인프라의 장점을 이용한다. PPTP는 GRE(Generic Routing Encapsulation) 프로토콜의 수정판을 사용하여 PPP(Point to Point Protocol) 패킷을 캡슐화하여 사용하므로 여러종류의 프로토콜(IP, IPX, NetBEUI)에서 사용가능한 유연성을 지니고 있다[7].

PPTP는 PPP에 의존하기 때문에 인증 메커니즘으로 PPP에서 제공하는 PAP, CHAP, MS-CHAP를 사용하고 데이터 암호화를 위해서는 마이크로소프트사에서 자체 개발한 MPPE를 사용한다. MPPE는 터널을 통해 전송하는 PPP 데이터 패킷을 IP 데이터그램으로 캡슐화한다. PPTP는 터널 말단 사이의 기본장치 관리와 구성에 대한 정보를 가진 제어 패킷과 일반 사용자 데이터를 담은 데이터 패킷을 따로 가지고 있으며 이것은 각각 다른 채널로 할당한다. PPTP는 제공되는 암호화가 약하고, 암호화 표준으로 확장이 어려우며 압축 방식이 독점적이어서 PPTP 인증이 상대적으로 약하다는 단점을 가지고 있다[6].

2.3.2 2계층 프로토콜 : L2TP

L2TP는 마이크로소프트의 PPTP와 시스코의 L2F를 통합하여 발전시킨 2계층 터널링 프로토콜로써, 클라이언트와 네트워크 접속 서버 사이에 PPP를 이용하여 다이얼-업 연결을 생성한다. 네트워크 서버가 말단 사용자를 인정하고 말단에 사용자를 위한 터널을 생성할지를 결정한 후에 전송할 데이터를 PPP 패킷으로 캡슐화하여 ISP에서 할당한 터널을 통해 보낸다. 이 때 원거리 사용자가 모뎀을 통해 LAC(L2TP Access Concentrator)에 접근하고 홈 네트워크의 LNS(L2TP Network Server)를 통해 터널링 된다[6].

PPP를 사용해서 다이얼-업 사용자에게 인증을 제공하는 것은 PPTP와 같으나 L2TP는 하나의 터널 안에 여러 개의

세션이 생성 가능하다. 즉, 다중 터널을 생성할 수 있고 각 터널에 다른 QoS 지원이 가능하다는 장점이 있다. 또한 L2TP는 IPSec이 IP 상에서만 적용 가능한 것과는 달리, 2계층 프로토콜로써 X.25, 프레임 릴레이, ATM 등과 같은 다양한 네트워크 상으로 PPP 프레임을 캡슐화할 수 있다. 역시 PPTP와 마찬가지로 데이터와 제어 메시지를 각각 가지고 있으나 한 스트림에 데이터 메시지와 제어 메시지를 넣어 동시에 전달한다는 점이 다르다. 게다가 IPSec의 인증과 암호화를 이용하여 강력한 보안을 제공할 수 있으며, 이 경우에는 L2TP의 인증이 추가적으로 필요하지 않게 된다. 또한 L2TP는 LAC와 LNS 사이의 흐름 제어를 구현함으로써 네트워크 트래픽을 줄일 수 있고 헤더를 압축하여 오버헤드를 감소시킬 수 있다[8, 9].

2.3.3 3계층 프로토콜 : IPSec

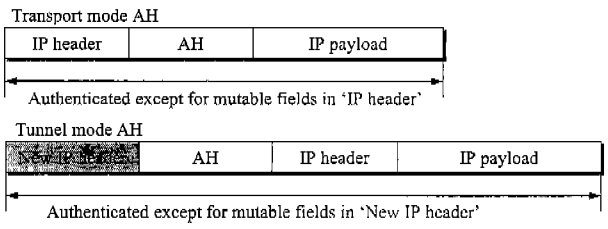
네트워크 계층의 IPSec은 네트워크 계층에 보안 서비스를 제공해 주는 메커니즘으로 현재 사용되고 있는 인터넷 프로토콜 표준인 IPv4 표준과 차세대 인터넷 프로토콜로 사용될 IPv6에 모두 보안 서비스를 제공할 수 있도록 설계되었다. 또한 현대 암호학의 기술들을 사용하고 있으며, 암호화와 인증이라는 강력한 암호학적 보안 서비스를 IP 패킷 단위로 제공해준다[6, 10].

IPSec은 인터넷망에서의 보안 문제인 인증, 접근통제, 비연결형 무결성, 기밀성, 재연(Replay) 공격 방지, 그리고 데이터 근원 인증등을 지원하기 위해 만들어진 것으로써 가상사설망 터널링을 위한 보안 서비스 제공에 적절하다.

IPSec은 AH(Authentication Header)와 ESP(Encapsulation Security Payload)의 두 가지 프로토콜과 IPSec의 보안 구조와 관련된 데이터베이스, 그리고 그 외에 IPSec을 사용하기 전에 터널을 형성할 양단간의 협상과정을 위한 키 관리 프로토콜이 필요하다. 다음은 IPSec의 주요 프로토콜인 AH와 ESP에 대해서 간략하게 살펴본다.

- AH (Authentication Header)

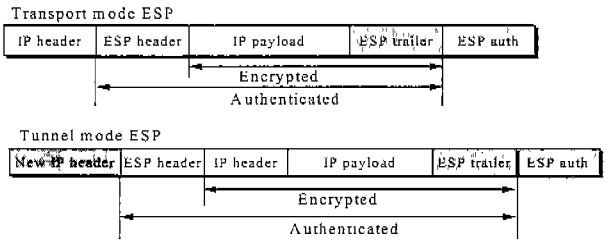
AH는 IP 데이터그램의 데이터 근원지에 대한 신원 인증과 데이터가 전송 도중에 변경되지 않았음을 확신해주는 무결성 보장을 위한 재연 공격 방지 기법을 포함한다. AH는 AH 헤더가 위치하는 곳에 따라서 트랜스포트 모드와 터널 모드의 두 가지 모드가 있다. 트랜스포트 모드는 원래의 IP 헤더를 그대로 이용하여 호스트간에 터널을 형성하는 데 주로 사용되고, 터널 모드는 데이터그램 전체를 AH로 캡슐화하고 새로운 IP 헤더를 추가하는 방식으로 송수신자를 새로 지정할 수 있으며 주로 보안 게이트웨이 사이의 터널 형성에 사용된다[11, 12].



(그림 4) AH 헤더

- ESP(Encapsulation Security Payload)

ESP는 IP 데이터그램에 기밀성을 제공하며 선택적으로 인증 기능까지도 제공할 수 있는 프로토콜이다. ESP를 사용하면 IP 패킷 자체가 DES(Data Encryption Standard) 혹은 Triple DES 방식으로 암호화되어 네트워크 상의 어떤 도청행위도 가능하지 못하도록 트레픽에 강력한 비밀성을 보장한다. 이때의 암호화 알고리즘이나 키 등은 터널의 종단간에 협상을 통해 조정된다. ESP도 AH와 마찬가지로 트랜스포트와 터널 모드의 두 가지로 캡슐화가 가능하며 (그림 5)는 이를 보여주고 있다[13-15].



(그림 5) ESP 헤더

AH와 ESP의 가장 두드러지는 차이점은 보호하는 데이터의 적용범위에 있다. ESP 헤더는 IP 헤더 안쪽에 위치하고 있기 때문에 제공되는 인증의 범위는 AH보다 좁으나 ESP는 AH가 제공하지 못하는 비밀성(암호화) 서비스를 제공한다. 만약 상위 계층의 프로토콜만 보호되어야 한다면 ESP 사용이 더 적절할 수 있으며 이는 ESP를 캡슐화하는 AH보다 공간을 효과적으로 사용할 수 있다. 또한 터널모드 ESP에 의해서 캡슐화되는 경우가 아니면 ESP는 목적지 옵션 헤더를 제외한 어떠한 IP 헤더 필드들도 보호하지 못하지만, AH는 IP 헤더의 일부분도 보호할 수 있다는 것이 다르다[16].

본 논문은 안전성을 최대화하여 테스트를 하였다. 따라서 터널 모드와 트랜스포트 모드 중에서 보다 높은 보안을 제공해 주는 터널 모드 방식을 적용하여 테스트를 하였다.

3. 테스트베드 환경

본 장에서는 테스트가 이루어진 테스트베드의 구성 환경과 테스트에서 사용된 트래픽 관련 도구에 대해서 다룬다.

3.1 구성된 테스트베드

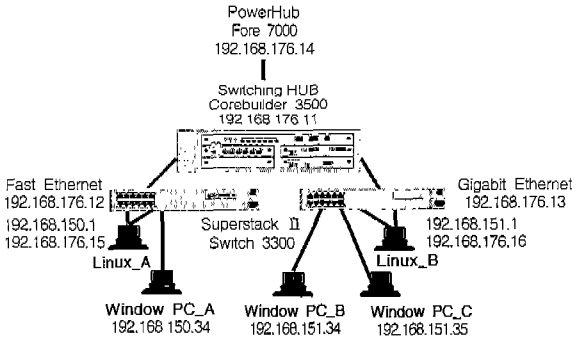
한 대의 라우팅 기능을 가진 3Com의 3계층 고성능 스위치인 Corebuilder 3500, 두 대의 3Com Superstack II 스위

치 3300 그리고 두 대의 리눅스 서버와 각각 다른 운영체제(98, 2000, NT)를 가진 윈도우즈 컴퓨터들로 이루어진 테스트베드의 구성은 (그림 6)과 같다[17].

각 리눅스 서버에는 레드햇 알짜(RedHat ALZZA) 리눅스 6.1이 설치되어 2.2.12-20 커널로 컴파일 하였다. 또한 각 리눅스 서버는 윈도우즈 컴퓨터가 트래픽을 보내고 받을 때 반드시 거쳐가야 하는 게이트웨이로 설정되어 있으며, 이를 가능하게 하기 위해서 Corebuilder 3500에서 제공하는 포트 기반 가상랜 기능을 사용하였다. 그리고 더미(dummy) 허브의 사용없이 윈도우즈 컴퓨터들이 리눅스에 직접 연결되어 있는 것처럼 구성하고, 서로 다른 네트워크를 통해 트래픽을 라우팅하기 위해서 각 리눅스 서버에는 두 개의 랜 카드를 설치하여 서로 다른 C 클래스 IP 주소를 가지고 있다. 또한 (그림 6)에서 PowerHub로 불리는 Fore 7000은 백본망과 연결되어 외부망(인터넷)으로도 나갈 수 있도록 구성되어 있다.

테스트베드에서 사용된 윈도우즈 컴퓨터들은 각기 다른 운영체제를 가지고 있다. 그 이유는 HTTP 트래픽을 측정하기 위한 WebBench의 세 가지 기본 요소 중 컨트롤러를 설치하기 위해 Windows NT가 요구되어지고, 2계층 가상사설망 프로토콜인 PPTP와 L2TP를 자체적으로 제공해 주기 위해서 Windows NT 4.0과 Windows 2000이 필요되며, 트래픽을 분석하는 도구인 NetXRay와 e-Watch를 설치하기 위해서 운영체제가 Windows 95/98이어야 하기 때문이다.

(그림 6)에서 Linux_A와 Linux_B에 가상사설망 테스트를 위해 필요한 2, 3계층 가상사설망 프로토콜 소스를 설치하였다. 웹상에서 다운로드받아 사용한 소스는 IPSec을 제공해주는 FreeS/WAN 프로젝트의 FreeS/WAN 1.3[18]과 PPTP를 제공해주는 Moretonbay의 PPTPD 1.0.0[19], 그리고 L2TP를 지원해주는 Marko의 L2TPD 0.6.1[20]이다. PPTP와 L2TP는 터널링을 하기 위해서 PPP가 사용되고, PPTP의 경우 인증을 위해 마이크로소프트사에서 제공하는 MPPE를 요구하므로 PPP-2.3.8과 MPPE도 리눅스 서버인 Linux_A와 Linux_B에 설치하였다. 모든 소스들은 리눅스용으로 GNU GPL(General Public License)에 의거하여 인터넷상에서 자유롭게 다운로드 받을 수 있으며 이를 수정하여 자유롭게 배포 가능하다.



(그림 6) 구성된 테스트베드

Window PC_A에서 Window PC_B와 Window PC_C까지는 앞의 2장에서 다루었던 터널의 두 가지 방식중 좀 더 강력한 보안을 제공해 주는 Voluntary 터널을 형성하였고, 현재 인터넷상에서 가장 많이 사용하는 멀티미디어 트래픽인 FTP, Telnet, HTTP, Ping을 트래픽 생성 도구들을 이용하여 각각 생성하고 이를 통해서 실험하였다.

3.2 실험에서 사용된 트래픽 도구

테스트베드에서 실험하기 위한 트래픽을 생성하고 결과를 비교, 분석하기 위해 사용한 트래픽 분석 도구들은 다음과 같다.

3.2.1 소나기(Sonagi)

Telnet 트래픽을 생성하기 위해서 한국항공대에서 개발한 트래픽 발생 도구인 소나기를 사용하였다. 소나기는 트래픽의 종류에 따라 각 헤더 필드에 송신지의 MAC 주소, 수신지의 MAC 주소, 송신지의 IP 주소, 수신지의 IP 주소와 트래픽의 종류를 구별해 주는 포트 값을 입력한다. 소나기에서는 헤더만 입력해 주고 패킷의 사이즈를 지정해 주면, 데이터 필드는 임의의 값으로 채워져 그 사이즈에 해당하는 패킷을 만들어 준다.

본 논문에서는 Telnet 패킷을 수집하여 분석한 결과를 토대로 패킷의 사이즈를 64바이트로 통일하였다. 단, 소나기에서는 트래픽을 발생할 때 전송 속도와 분포 등을 지정해 줄 수가 없어서 트래픽 발생시 네트워크 대역폭을 최대값으로 사용하여 전송하였다.

3.2.2 Dragon Server

FTP 트래픽을 Window PC_A에서 Window PC_B로 보내기 위해서 FTP 데몬 프로그램인 Dragon Server V2.1을 설치하였다. Dragon Server V2.1은 윈도우즈 컴퓨터를 텔넷 서버와 FTP 서버로 이용할수 있도록 해주는 응용 프로그램으로 무료 응용프로그램을 제공하는 사이트에서 구할 수 있다. Dragon Server V2.1은 일반적인 텔넷 서버와 FTP 서버가 제공하는 기능인 사용자 ID와 패스워드를 인증하고 사용자에 따라 서비스 권한을 제한시킬수 있으며 사용 가능한 디렉토리 정의가 가능하고 접근 가능한 IP주소를 한정할 수 있다.

3.2.3 WebBench

HTTP 트래픽을 생성하고 성능을 평가하기 위해서 ZDBOp (ZD Benchmark Operation)사에서 개발한 웹 서버 소프트웨어의 성능을 측정해 주는 도구인 WebBench를 사용하였다. WebBench는 각각 관련 프로그램을 수행하는 컨트롤러, 서버 그리고 클라이언트들로 구성되며, 서버의 성능은 초당 요청 수(Requests per second)와 처리율(Throughput)로 평가되며 점수가 높을수록 서버의 성능이 우수함을 나타낸다. WebBench는 클라이언트 PC를 사용하여 웹 브라우저를 시

뮬레이트하고, 클라이언트 PC는 실제 브라우저와는 달리 서버가 보내온 파일들을 보여주지 않고 그 파일에 대한 정보를 기록한 후 즉시 다음 요청을 보낸다[21].

WebBench 3.0 workload 트리는 웹사이트의 사용 패턴을 모델링한 것으로 여기에는 6,160개의 파일이 들어있고 총 크기는 약 61메가바이트이다. 여기서는 ZDBOp에서 제공하는 표준 테스트 데이터 중 하나인 zd_static_v30.tst를 사용하였는데 이것은 다수의 HTML, GIF 파일과 소수의 실행 파일들과 같은 정적 파일들로 구성되어 있다.

WebBench는 성능 측정결과를 11개의 테이블로 보여준다. 본 논문에서는 이 중 서버의 전반적인 점수를 보여주고, 테스트의 각 믹스에 대한 초당 요청수 및 처리율 그래프를 포함한 모든 결과를 총정리해서 보여주는 테이블 1과 클라이언트 수와 발생한 연결/전송 에러 수를 포함한 테스트 전반에 대한 부가적인 정보를 제공하는 테이블 2 그리고, 클라이언트들이 workload 파일의 사용 여부를 보여주는 테이블 3을 주로 이용하여 성능을 비교·분석하였다.

3.2.4 NetXRay

NetXRay는 다양한 주소, 프로토콜, 데이터 패턴 필터를 가지고 효율적이고 정확하게 패킷을 수집하고 패킷의 내용과 종류를 자세하게 분류하여 보여주는 기능을 가지고 있다. 또한 Dashboard를 통해서 현재 네트워크 상황을 살펴볼 수 있으며 Packets/s, Utilization, Octets/s, Errors/s, Drops/s 등과 같은 다양한 종류의 히스토리 샘플을 통해서 네트워크 상황을 모니터링하고 이에 대한 통계를 낼 수 있도록 해 준다. 그 외에도 트래픽에 들어갈 헤더와 내용들을 임의로 결정하여 트래픽을 생성할 수 있는 기능을 제공하고 있다.

본 테스트에서는 NetXRay를 이용해서 각 시나리오에 따른 Telnet 트래픽과 FTP 트래픽을 수집하고, 시나리오마다 네트워크의 상황이 어떻게 다른지를 히스토리 샘플을 저장하여 비교·분석하였다.

3.2.5 e-Watch

NetXRay와 마찬가지로 프로토콜을 분석할 수 있고 트래픽을 감시(모니터링)할 수 있게 해주는 소프트웨어로 한국항공대에서 만든 툴이다[21]. e-Watch는 링크 상에 존재하는 모든 패킷을 MAC 주소 또는 IP 주소를 사용하거나 프로토콜을 이용하여 패킷을 선별적으로 읽어들여 분석하는 패킷 수집 및 분석 기능과 네트워크에 보낼 패킷의 개수와 패킷의 길이, 그리고 어떤 종류의 패킷을 네트워크에 보낼 지를 결정하여 패킷을 생성하는 기능, 현재 접속된 링크의 전송되는 프레임의 분포율, 링크의 사용효율, 에러율 등을 실시간으로 감시하는 트래픽 모니터링 기능, 그리고 대부분 DOS에서 수행하는 ARP, NBTStat, Ping, Tracert, DNSlookup 등의 기능을 수행할 수 있다.

4. 테스트 결과 분석

여기서는 본 논문에서 설정한 시나리오들과 생성한 트래픽 종류별 테스트의 결과에 대한 비교·분석 결과를 알아본다.

4.1 테스트 시나리오

본 논문에서 2, 3계층 가상사설망 프로토콜인 PPTP, L2TP, IPSec을 각각 테스트베드에 설치하여 결과를 도출하였다. 이 때 사용한 테스트 시나리오는 다음과 같다.

- 가상사설망을 설치하지 않은 경우(Default)
- 2계층 가상사설망
  PPTP를 설치한 경우
  L2TP를 설치한 경우
- 3계층 가상사설망
  IPSec을 설치하고 ESP만 사용한 경우
  IPSec을 설치하고 AH와 ESP를 함께 사용한 경우
- 2, 3계층 가상사설망 혼합
  L2TP와 IPSec을 함께 적용하고 ESP만 사용한 경우
  L2TP와 IPSec을 함께 적용하고 AH와 ESP를 함께 사용한 경우

(그림 6)의 Linux_A와 Linux_B에 각각 2, 3계층 가상사설망 프로토콜인 PPTP와 L2TP, IPSec을 설치하고, 이들 프로토콜을 이용해서 Window PC_A에서 Window PC_B로 또는 Window PC_A에서 Window PC_C로 Voluntary 터널을 형성한다. 이렇게 각 시나리오별로 2, 3계층 가상사설망이 이루어진 가운데 FTP, Telnet, HTTP 그리고 Ping 트래픽을 생성하여 테스트한다. 특히 2, 3계층 가상사설망을 혼합한 경우는 Linux_A와 Linux_B에 L2TP와 IPSec을 동시에 이용하여 터널을 생성한 경우이다. 즉 3계층에서 IPSec이 적용된 IP 데이터그램을 다시 L2TP를 이용해서 이중으로 터널링한 것을 의미한다.

본 논문에서 2, 3계층 가상사설망 혼합 방식에서 2계층 가상사설망 프로토콜로 PPTP 대신에 L2TP을 적용한 이유는 L2TP가 IPSec가 더불어 표준으로 제정되는 과정에 있으며 현재 IETF에서 L2TP와 IPSec을 함께 사용하는 방식이 지속적으로 연구 중이기 때문이다[22].

4.2 테스트 결과

이 절에서는 FTP, Telnet, HTTP 트래픽과 Ping을 각 시나리오 별로 생성한 트래픽에 대한 테스트 결과를 알아본다. 본 논문에서는 네트워크의 성능 변화를 측정하기 위해서 지연 시간, 처리율, 이용률을 이용하여 비교 분석한다. 이 세 가지는 네트워크의 상황을 확인하기 위해 살펴보는 대표적인 파라미터들이기 때문이다. 지연 시간이란 일정한 양의 트래픽을 전송하는데 걸리는 총 시간이며, 처리율은 단위 시간당

처리할 수 있는 트래픽의 양을 나타내며, 이용률은 단위 시간당 네트워크 자원이 이용되는 정도를 표시한다.

4.2.1 FTP 트래픽

FTP에서 트래픽을 생성하기 위해 사용한 파일은 멀티미디어 트래픽에서 많이 사용되는 동영상 파일인 mpg, 음악 파일인 wav, 그리고 특정 소프트웨어를 다운로드 받아서 설치하는데 사용하는 실행파일인 exe로 구성되어 있다. 이 파일들의 내용은 <표 1>과 같고, 사용한 파일들의 총 크기는 약 150 MB이다.

〈표 1〉 FTP 트래픽에 사용된 파일들

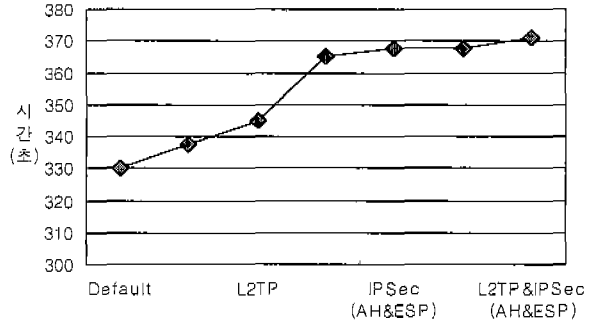
파일 종류	파일 크기
mpg	30,922KB
wav	53,307KB
	40,118KB
exe	29,280KB

FTP는 대역폭에 민감한 응용프로그램으로 처리율이 매우 중요하다. 따라서 본 논문에서는 다른 트래픽들의 이동 없이 대부분의 대역폭을 모두 사용하여 테스트의 정확도를 높였다. 또한 본 논문에서 나타난 결과값은 총 5번의 반복 테스트로 얻은 값들의 평균이다.

(그림 7)은 2, 3계층 가상사설망이 FTP 트래픽에 미치는 영향을 같은 양의 트래픽을 보내는 데 걸린 전송시간(Delay)의 차이를 통해서 보여주고 있다.

FTP 트래픽을 가상사설망이 적용된 네트워크에서 사용한 경우가 같은 양의 트래픽을 전송하는데 가상사설망을 사용하지 않은 경우에 비해 전송시간이 더 걸렸다.

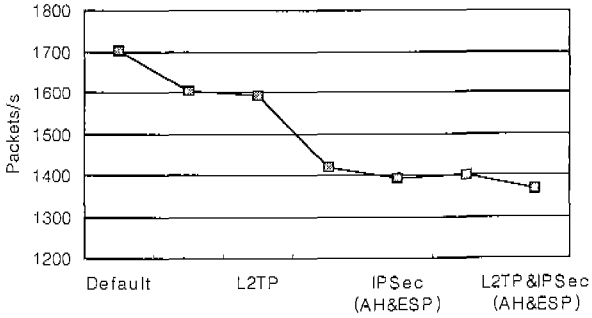
각 2, 3계층 가상사설망에서 초과 시간을 비교해 보면, PPTP와 L2TP를 설치한 경우는 약 2~5%가 증가되었고, IPSec을 설치한 네트워크는 10.6~11.3%가 증가되어 2계층 가상사설망보다 3계층 가상사설망을 설치한 경우가 더 많은 시간이 걸렸다. 여기서 주목해야 하는 부분은 바로 L2TP와 IPSec을 함께 사용한 경우에 추가적으로 요구된 시간은 11.3~12.5%로 2, 3계층 프로토콜을 각각 설치하였던 네트워크에 비해서 약간의 시간만이 초과되었다는 테스트 결과이다.



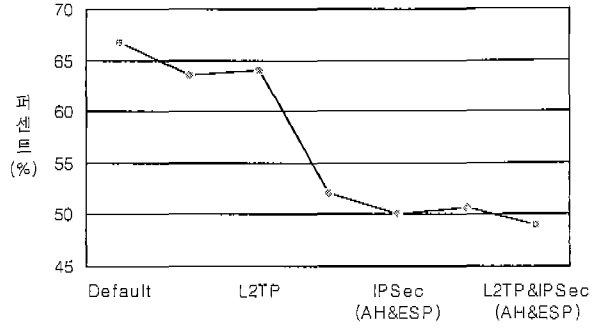
(그림 7) FTP에서 데이터를 전송하는데 걸린 시간

2계층 가상사설망의 경우 PPP를 이용하여 한 쪽에서 다이얼-업 연결을 통해 RAS에 연결한 후 터널을 생성한다. 그러므로 가상사설망을 사용하지 않은 경우보다 터널링 작업과정에 추가적인 시간이 요구된다. 3계층 가상사설망의 경우에는 AH와 ESP라는 두 가지 헤더를 각 패킷에 덧붙여 보내므로 송신하는 쪽에서 이들 헤더를 생성하고 수신하는 쪽에서 이 헤더들을 제거하는 단계들로 인해 가상사설망을 설치하지 않은 경우보다 시간이 더 많이 요구되었다. 그리고, IPSec에서는 ESP만 이용한 경우는 AH 뿐만 아니라 ESP까지 함께 사용한 경우 더 많은 헤더 생성과 암호화 과정이 요구되므로 같은 양의 트래픽을 보내는 데 더 많은 시간이 걸렸음을 알 수 있다.

FTP 트래픽 전송시에 나타난 초당 처리할 수 있는 최대 패킷 수를 나타내는 처리율과 최고 이용률은 서로 같은 경향을 보이고 있음을 (그림 8)과 (그림 9)를 통해 확인할 수 있다. 가상사설망을 설치하지 않은 경우가 가장 높은 수치를 나타냈고, 2계층 가상사설망을 설치한 경우가 3계층 가상사설망을 설치했을 때 보다 높은 수치를 나타냈다. 여기서 주목해야 한 부분은 전송시간과 마찬가지로 처리율과 이용률 역시 2, 3계층 가상사설망을 함께 사용했을 때는 3계층 가상사설망만 적용했을 때보다 아주 낮은 폭의 감소만을 보이고 있다는 것이다. 이것은 L2TP가 제공해 주는 터널링 생성에 소요되는 시간이 전체 트래픽을 전송하는 시간에 비해 짧다는 것으로 즉, 네트워크에 미치는 영향은 아주 미미하다는 것을 보여주는 것이다.



(그림 8) FTP에서 데이터 전송 시 나타난 최고 처리율



(그림 9) FTP에서 데이터 전송 시 네트워크 이용률

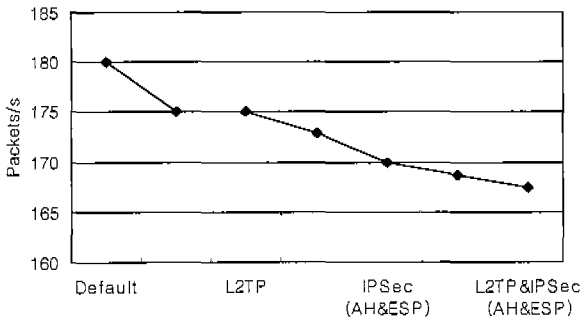
처리율의 경우 2계층 가상사설망을 설치했을 때 약 6~7% 정도 감소되었고, 3계층 가상사설망을 설치했을 때는 그보다 훨씬 큰 17~18% 정도가 감소되었다. 그러나 2, 3계층 가상사설망을 함께 설치한 경우에는 18~20%로 IPSec만 설치한 경우보다는 약간 낮은 결과가 나왔다.

(그림 9)에서 보여주는 이용률 역시 PPTP와 L2TP를 설치한 경우 약 3~4% 정도가 감소되었고, IPSec을 설치한 경우는 그보다 훨씬 많은 22~25% 정도가 감소되었다. 그러나 2, 3계층 가상사설망을 함께 설치한 경우에는 25~27%로 IPSec만 설치한 경우보다는 약간 낮은 결과가 나타났다.

4.2.2 Telnet 트래픽

Telnet 트래픽은 그 특성상 다양한 패킷 크기를 가지고 있다. 따라서 본 논문에서는 Telent 트래픽을 생성하기 앞서 패킷을 수집한 결과로 본 논문에서는 64바이트를 기준으로 테스트하였다. Telnet에서는 총 패킷 수와 총 패킷 수에 대한 각 종류별 패킷이 차지하는 퍼센트를 비교하여 시나리오별로 어떠한 차이가 있는지 알아본다.

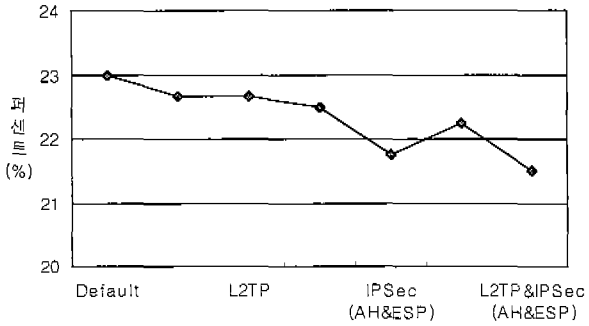
Telnet 트래픽을 이용한 테스트에서는 일정 데이터를 전송하는 데 걸리는 시간이 너무 짧아서 이 차이를 비교하는 것이 무의미하므로 최고 처리율과 네트워크 이용률만을 이용하여 그 결과를 비교 분석한다.



(그림 10) Telnet에서 나타난 최고 처리율

(그림 10)은 본 논문에서 제시한 시나리오별로 Telnet 트래픽을 전송했을 경우 나타난 최고 처리율에 대한 것으로, FTP 트래픽을 전송했을 경우와 마찬가지로 가상사설망을 설치하지 않은 Default가 가장 높은 수치를 가지고 있으며 가상사설망을 설치한 나머지 경우에는 약간씩 감소된 수치를 보여주고 있다.

여기서 신중하게 고려해야할 부분이 버퍼의 사용량이다. 이것은 NetXRay에서 제공하는 버퍼 용량의 얼마만큼을 사용했는가 하는 것으로 특정 네트워크의 이용률을 나타낸다. 따라서, 버퍼 사용량을 비교해 보면 가상사설망을 설치하였을 경우가 설치하지 않았을 경우보다 버퍼를 적게 사용했음이 (그림 11)을 통해서 알 수 있다. 특히 IPSec에서 ESP만 사용한 경우와 AH와 ESP를 함께 사용한 경우의 차이가 두드러짐을 알 수 있다.



(그림 11) Telnet에서 나타난 네트워크 이용률

결론적으로, 각 시나리오별로 나타난 결과 차이는 거의 미미하다. 그 이유는 Telnet을 연결하여 통신을 할때 발생하는 패킷은 크게 64바이트 이하의 것이나 128~255바이트 사이의 것으로 패킷의 크기가 작고, 많은 양의 트래픽 이동을 요구하지 않는 Telnet 트래픽의 성격 때문이다. 따라서 가상사설망 설치 전후나 2, 3계층 가상사설망 사용 여부 그리고 3계층 가상사설망인 IPSec 사용에서 AH의 추가 사용 여부에 따라 눈에 띄는 트래픽의 변화는 거의 없음을 알 수 있다. 즉, FTP 트래픽과 마찬가지로 Telnet 트래픽도 L2TP와 IPSec을 동시에 적용한 네트워크의 경우가 3계층 가상사설망 프로토콜만을 사용한 경우보다 약간 낮은 성능 결과를 보여주고 있다. 이러한 차이는 FTP 트래픽에서 나타난 결과에 대한 이유와 같다.

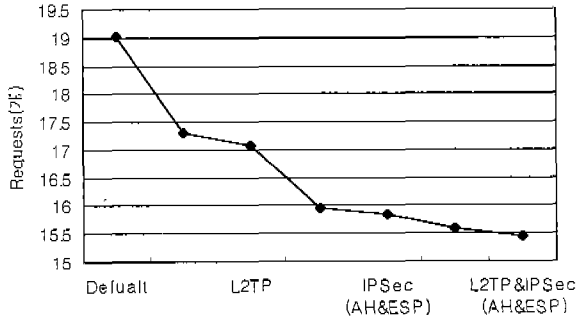
4.2.3 HTTP 트래픽

HTTP 트래픽 실험에서 사용된 테스트 데이터는 WebBench가 제공하는 표준 테스트 데이터 중 하나인 zd_static_v30.tst 이다. 이 테스트는 한 번에 약 82분 정도의 시간이 소요되며, 여러 가지 다양한 멀티미디어 트래픽들을 생성하여 결과를 도출하고, 생성되는 양방향 트래픽의 길이가 다양하므로 FTP나 Telnet 트래픽과는 달리 가상사설망 설치 여부에 따라 눈에 띄는 차이가 나타났다.

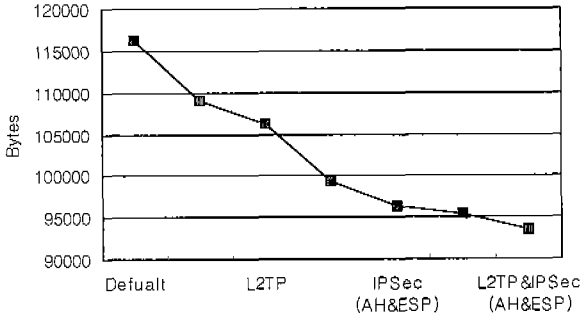
HTTP 트래픽에서의 성능 차이를 알아보기 위해서 WebBench에서 제공하는 테이블 중에서 결과를 총정리해서 보여주는 테이블 1과 각각 클라이언트에서 발생한 연결/전송 에러 수를 포함하는 테이블 2 그리고, 클라이언트들의 workload 파일의 사용여부를 보여주는 테이블 3을 사용한다. 테스트 결과 나타난 각 시나리오별 차이는 (그림 12)와 같다.

(그림 12)를 보면 Default의 초당 요청 수가 가상사설망을 설치한 다른 경우들에 비해 훨씬 높음을 알 수 있다. 앞서 언급했던 FTP 트래픽과 Telnet 트래픽과 같이 2계층 가상사설망이 3계층 가상사설망보다는 좋은전송 성능을 보여주고 있음을 확인할 수 있다. 그리고 IPSec에서 보안을 위한 헤더로 ESP만 사용한 경우와 AH와 ESP를 함께 사용한 경우의 초당 요청 수에는 거의 차이가 없었다. 이를 통해서 AH의 추가 사용이 HTTP 트래픽의 전송에 미치는 영향이 극히 미비함을 확인할 수 있었다. 마지막으로 2, 3

계층을 함께 사용한 경우에는 다른 트래픽 전송에서 나타난 바와 같이 3계층 가상사설망만을 사용한 경우보다 약간 저조한 결과가 나타났다.



(그림 12) HTTP에서 나타난 최대 초당 요청 수

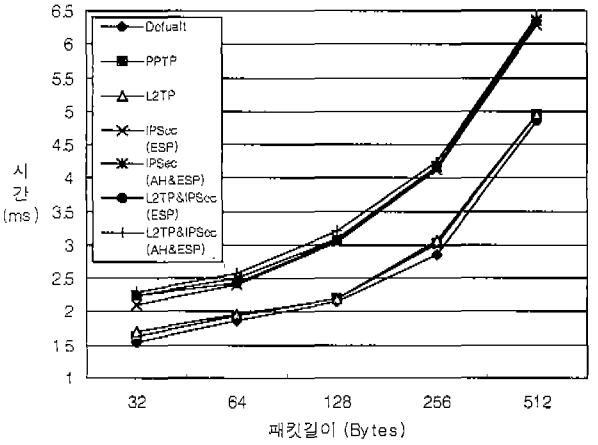


(그림 13) HTTP에서 나타난 최고 패킷 처리율

(그림 13)은 HTTP 트래픽에 대한 처리율을 나타내는 것이다. 초당 요청 수와 마찬가지로 HTTP 트래픽에서의 처리율은 가상사설망을 설치하지 않았을 경우가 월등히 높은 수치를 나타냈다. 이 차이가 다른 FTP나 Telnet 트래픽보다 큰 이유는 HTTP 트래픽에 대한 테스트가 오랜 시간 다양한 종류와 다른 길이의 패킷들이 서로 송수신된 결과를 보여 주는 것으로 일정한 길이의 패킷에 비해 서로 다른 길이의 패킷 전송이 성능 저하에 영향을 주었기 때문이다. 또한 2계층 가상사설망을 설치한 경우보다 3계층 가상사설망을 설치한 경우가 낮은 처리율을 나타냈다. 초당 요청 수와는 달리 HTTP 트래픽 처리율은 IPSec에서 ESP만 사용한 경우와 AH와 ESP를 동시에 사용한 경우에 약간의 차이가 나타났다. ESP만 사용한 경우가 AH를 함께 사용한 경우보다 약 3%정도 높은 처리율을 보였다. 그리고 L2TP와 IPSec을 함께 사용한 경우는 IPSec만을 사용한 경우보다 약 4%정도 낮은 처리율을 보여주고 있으나 전체에 미치는 영향은 미비함을 알 수 있다.

4.2.4 Ping

Ping은 네트워크를 테스트하거나 진단하는데 사용하는 간단한 프로그램으로 네트워크 성능을 평가하기 위해서도 사용된 바 있다. 따라서, 본 논문에서도 Ping에서 패킷의 크기를 32바이트부터 1024바이트까지 변화시켜가면서 네트워크의 성능 변화를 테스트하였다. 즉, 가상사설망이 설치된 경우와 그렇지 않은 경우에 어떻게 다른 수신시간이 나타나는지 앞의 (그림 6)에서 Window PC_A와 Window PC_B 사이에 Ping을 생성하여 알아보고, 이 결과를 통해 네트워크의 성능을 평가하고자 한다. (그림 14)는 Ping을 이용하여 100개의 패킷을 각 시나리오별로 보낸 결과를 보여주고 있다.



(그림 14) Ping을 보냈을 때 걸린 시간

3계층 가상사설망을 설치한 경우와 2, 3계층 가상사설망을 혼합한 경우에 Ping을 보냈을 때는 패킷의 크기가 커질수록 그 차이가 적어짐을 알수 있으며, 2계층 가상사설망은 가상사설망이 설치되지 않은 경우와 일정한 증가폭을 가지고 있다. 역시 2계층 가상사설망만 설치한 경우는 가상사설망을 설치하지 않은 경우와 격차가 적었으며, 3계층 가상사설망이 설치한 경우는 가상사설망을 설치하지 않은 경우보다 심하게는 40%이상의 시간이 더 걸렸다. 앞서 보았던 FTP, Telnet, HTTP 트래픽과 마찬가지로 2, 3계층 가상사설망을 함께 사용한 경우는 3계층 가상사설망을 사용한 경우와 비교하여 1~3% 정도밖에 걸린 시간이 차이나지 않았다. 이로써 또 한번 2, 3계층 가상사설망을 함께 사용하는 것이 더 효율적인 방식임을 보여준다.

5. 결 론

본 논문에서는 가상사설망을 설치했을 경우 네트워크에 어떠한 영향을 미치는지에 대해 알아보았다. 여기서 다루었던 테스트를 통해서 OSI의 7계층 중에서 2계층에 가상사설망을 적용한 경우보다 3계층에 가상사설망을 사용하는 경우에 오버헤드가 증가함을 알수 있었으며, 2, 3계층 가상사설망을 함께 적용한 경우가 보안을 더 철저하게 제공해주면서도 증대되는 오버헤드의 폭이 적음을 알 수 있었다. 또한, 본 논문에서 다룬 FTP와 Telnet 트래픽의 결과는 거의 비슷하나 HTTP 트래픽의 경우 주고받는 데이터의 길이가 일정하지 않고 양방향 데이터 전송이어서 각 시나리오별로 결과의 차이가 나머지 트래픽에 비해서 두드러짐을 확인할

수 있었다. Ping의 경우에는 패킷의 길이가 길어짐에 따라 IPSec만 사용한 경우와 L2TP와 IPSec을 혼합한 경우에 걸리는 시간의 차이가 줄어들었음을 알 수 있었다. 그러므로 현재 IETF에서 진행중인 L2TP와 IPSec을 함께 사용하는 방안이 지금까지 제시되고 있는 가상사설망 적용 방식 중에서 가장 이상적이라고 할 수 있다.

향후에는 각 가상사설망 프로토콜에서 사용한 암호화 알고리즘을 알아보고, 이 암호화 알고리즘이 네트워크에 미치는 영향을 확인하여 가상사설망에 효율적이고 적합한 암호화 알고리즘을 제시할 수 있을 것이다.

참 고 문 헌

[1] "VPN," http : //www.sharpened.net/glossary/definition.php?vpn.

[2] Paul Ferguson and Geoff Huston, "What is a VPN," Cisco Systems ; Telstra Internet, Mar. 1998.

[3] 채기준, "가상사설망보안", 제5회 정보통신응용워크숍 차세대 네트워크 기술 발표집 II, pp.145-173.

[4] Microsoft Corporation, "Web Workshop-Virtual Private Networking : An Overview," http : //msdn.microsoft.com/workshop/server/feature/vpnovw.asp, May, 1998.

[5] IBM, "The Layer 2 Tunneling Protocol(L2TP) in an IBM Virtual Private Network(VPN)," IBM Networking White Papers, http : //www.networking.ibm.com/vpn/vpnwhite.html.

[6] Dave Kosiur, "Building and Managing Virtual Private Networks," Wiley Computer Publishing, 1998.

[7] IBM, "VPN Overview," IBM Networking White Papers : Voice-Data Integration in e-business, http : //www.networking.ibm.com/vpn/vpntech.html.

[8] "What is L2TP?," http : //www.postech.ac.kr/~leonardo/reseach/l2tp.htm.

[9] IETF RFC 2661, Layer Two Tunneling Protocol "L2TP," 1999.

[10] IETF RFC 2401, Security Architecture for the Internet Protocol, 1998.

[11] IETF RFC 2402, IP Authentication Header, 1998.

[12] IETF RFC 1827, IP Authentication using Keyed MD5, 1995.

[13] IETF RFC 2406, IP Encapsulating Security Payload (ESP), 1998.

[14] IETF RFC 1829, The ESP DES-CBC Transform, 1995.

[15] 정태명, "가상사설망(VPN)", 제6회 정보통신망 정보보호 워크숍 발표집, 1999.

[16] 주식회사 니츠 편저, "인터넷 보안 기술 -1", 도서출판 동서, pp.30-35.

[17] 3Com, "Corebuilder 3500 기종", http : //210.182.137.32/products/switches/400347.html.

[18] FreeS/WAN 홈페이지, http : //www.xs4all.nl/~freeswan/.

[19] PoPToP - The PPTP Server for Linux 홈페이지, http : //poptop.lineo.com/.

[20] L2TPD 홈페이지, http : //www.marko.net/l2tp/.

[21] 이화여자대학교, "정보보호시스템 성능평가 지표연구", 한국정보보호센터, 1999.

[22] Internet-draft, "Securing L2TP using IPSEC," http : //www.ietf.org/internet-drafts/draft-ietf-l2tpext-security-01.txt.

오 승 희

e-mail : seunghee5@etri.re.kr

1999년 전북대학교 컴퓨터과학과 이학사

2001년 이화여자대학교 컴퓨터학과 공학석사

2001년~현재 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀 연구원

관심분야 : 네트워크 보안, Active Network, VPN 등

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과 졸업(학사)

1984년 미국 Syracuse University 컴퓨터과학과(석사)

1990년 미국 North Carolina State University 컴퓨터공학과(공학박사)

1990년~1992년 미국 해군사관학교 컴퓨터과학과 조교수

1992년~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 네트워크 보안, 액티브 네트워크 보안 및 관리, 인터넷/무선통신망/고속통신망 프로토콜 및 성능분석

남 택 용

e-mail : tynam@etri.re.kr

1987년 충남대학교 계산통계학과 이학사

1990년 충남대학교 대학원 계산통계학과 이학석사

1987년~현재 한국전자통신연구원 정보보호연구본부 능동보안기술연구팀 팀장

관심분야 : 정보보호, 능동보안, 차세대네트워크구조 등

손 승 원

e-mail : swsohn@etri.re.kr

1984년 경북대학교 전자공학과 공학사

1994년 연세대학교 전자공학과 공학석사

1999년 충북대학교 컴퓨터공학과 공학박사

1983년~1986년 삼성전자 연구원

1986년~1991년 LG 전자(주) 중앙연구소 HI8mm 캠코더 팀장

1991년~현재 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장

관심분야 : IC Card, Biometry, Active Network 등