# 엑스트라넷 VPN 구축을 위한 효율적 터널링 및 프로토콜 적용

장희진, 조용구. 소우영
한남대학교 컴퓨터공학과

# Applying Tenneling and Protocol for Extranet VPN Construction

Hui-Jin Jang, Young-Gu Jo. Woo-Young Soh
Dept. of Computer Engineering, HanNam University

**요 약**

엑스트라넷은 기업협력간 업무처리 또는 인증된 고객에게 서비스를 제공하기 위하여 사설망 서비스를 제공한다. 최근에는 비용이나 보안적 측면을 고려하여 기업간에 VPN을 이용한 엑스트라넷 구축이 활성화되고 있다. 엑스트라넷 VPN 구축 시 필요한 터널링 및 프로토콜은 아직까지 국내에서 표준화에 기반한 적용방안이나 권고가 부족한 실정이다. 본 논문에서는 엑스트라넷 VPN 구현형태에 따라 인트라넷 VPN과 원격접속 VPN으로 구분하여 터널링 및 프로토콜의 기능 및 성능을 비교 분석하여 두 가지 구분에 요구되는 서비스와 보안에 따라 효율적으로 터널링 및 프로토콜을 적용하는 방안에 대하여 논하고자 한다.

## 1. 서론

인터넷 기술 발전에 따라 기업의 인트라넷은 기업간 비즈니스 거래, 즉 엑스트라넷을 가속화하고 있다. 최근 비용과 보안적 측면을 고려하여 가상사설망(VPN: Virtual Private Network) 기술을 이용한 엑스트라넷 VPN 구축이 활성화되고 있다[1]. 그러나, 국내 경제업무의 엑스트라넷 VPN 의존도는 높아지고 있는 반면에 엑스트라넷 구축시 안정적인 유지관리를 위한 터널링 및 프로토콜 적용방안은 표준화에 기반해서 자세하게 정리되어진 권고는 미약한 상태이다. 이것은 엑스트라넷 VPN을 구축하려는 국내 기업들에게는 중요한 난점이다. 따라서, 본 논문에서는 엑스트라넷 VPN 구축방법을 엑스트라넷 VPN 구현형태에 따라 인트라넷 VPN과 원격접속 VPN으로 구분하여 요구되는 서비스와 보안에 따라, 대표적인 터널링 및 프로토콜의 기능과 성능에 대한 기존의 연구분석을 고려하여 효율적인 터널링 및 프로토콜 적용방안을 논하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 VPN 구현 기술인 터널링 및 프로토콜에 따른 각각의 기능과 성능에 대한 기존의 연구분석을 체계적으로 정리하고, 3장에서는 엑스트라넷 VPN구축을 위한 효율적인 터널링 및 프로토콜 적용방안으로 인트라넷 VPN과 원격접속 VPN에 대하여 논하고, 마지막으로 4장에서 본 논문의 결론과 향후 연구방향에 대해서 기술한다.

## 2. VPN 구현 기술

### 2.1 VPN 터널링

VPN은 '터널링'이라는 기법을 사용하여 일대일 연결시 '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 네트워크기반을 통과하는 프로토콜을 사용할 수 있으며 여러 전송지로부터의 데이터를 차별적으로 처리할 수 있다. 터널링은 패킷/프레임의 캡슐화, 전송 및 캡슐화 해제하는 과정을 포함한다.

터널은 크게 자동으로 생성되는 Compulsory 터널과 사용자의 요구에 의해 생성되는 Voluntary 터널로 나눌 수 있다. 즉, 말단 사용자 컴퓨터가 터널의 종료점을 PPP만 지원하는 ISP(Internet Service Provider)의 RAS(Remote Access Server)에 위치시킬지, 아니면 자신의 컴퓨터에 위치시킬지에 따라 터널의 종류가 결정된다[2].

#### 2.1.1 Compulsory 터널

Compulsory 터널은 사용자의 요청 없이 자동적으로 생성되는 터널로 VPN이 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 RAS와 같은 장치가 터널의 종단이 되며 터널 클라이언트로 작동한다.

사용자 동의와 상관없이 자동으로 터널이 생성되기 때문에 말단 사용자에게 투명성을 제공하며, Voluntary 터널링에 비해 다중 세션 전송에 필요한 네트워크 대역폭이 감소한다는 장점을 지니고 있다. 또한 Compulsory 터널방식은 인트라넷밖에 있는 다른 서비스에 접근하려면 네트워크 관리자의 통제를 받아야 하고, 종단점이 미리 결정되어 사용자가 인터넷의 다른 부분에 접근할 수 없으므로 Voluntary 터널보다는 나은 접근제어를 제공한다. 반면에 말단 사용자의 컴퓨터와 RAS의 사이에 있는 초기 연결링크가 터널 밖이므로 침입위험이 증가하는 단점이 있다[2].

2.1.2 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 열 수 있고, 터널링이 없는 기본 TCP/IP 프로토콜로 다른 인터넷 호스트에 접근 가능하다. 이 방식은 인터넷을 통해 보내지는 인트라넷 트래픽의 프라이버시와 데이터 무결성을 제공하기 위해 사용된다. 게다가 사용자 컴퓨터까지 터널이 생성되므로 Compulsory 터널보다 강력한 보안을 제공하므로 현재 더 보편적으로 사용되고 있다[2].

### 2.2 VPN 프로토콜

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

2.2.1 2계층 프로토콜: PPTP/L2TP

Microsoft사의 PPTP(Point-to-Point Tunneling Protocol)와 인터넷 표준인(RFC 2661) L2TP(Layer 2 Tunneling Protocol)는 인터넷에서 원격 액세스 VPN을 구성하는데 가장 널리 사용되는 클라이언트/서버 기반의 터널링 프로토콜이다. 이 두 프로토콜은 모두 Layer 2의 PPP 트래픽에 대한 캡슐화를 통해 두 지점 간의 터널을 생성, 관리 및 소멸시켜주는 것이 기본 기능이며, 보안은 대부분 PPP에서 제공하는 보안기능에 의존한다. 그러므로, L2TP보다 강력한 보안을 위해 IPSec(IP Security)을 사용하도록 권고하고 있다[3][4].

PPTP와 L2TP는 유사한 Layer 2 터널링 서비스를 제공하지만 다음과 같은 차이점이 있다[2].

◆ PPTP와 L2TP의 차이점
(1) 두 프로토콜 모두 PPP 트래픽을 캡슐화하기 때문에, IP, IPX, NetBEUI, AppleTalk 등의 다양한 상위 로컬 네트워크 프로토콜을 사용할 수 있다. 그러나 PPTP는 transit internetwork이 IP 네트워일 것을 요구하는 반면, L2TP는 Packet-Oriented Point-to-Point 접속을 제공하는 네트워만 보장되면, 어떤 전송 프로토콜 상에서도 사용 가능하다.
(2) PPTP는 End-Point들 사이에 Single-Tunnel만을 지원하나, L2TP는 Multiple-Tunnel을 허용한다. 따라서 L2TP를 사용하면 QoS(Quality of Service)에 따라 서로 다른 터널을 이용할 수 있다.
(3) L2TP는 헤더 압축 및 Tunnel-End-Point 인증 (패킷단위의 인증이 아니라, Tunnel End-Point들의 Identity에 대한 인증) 기능을 제공하지만 PPTP에는 이런 기능이 없다. 두 프로토콜 모두에서 사용자 인증이나 데이터 암호화/압축 등의 보안기능은 PPP에서 제공하는 것을 사용한다.

2.2.2 3계층 프로토콜: IPSec

IPSec은 표준화 작업이 완성된 IP 계층의 보안을 위한 인터넷 표준으로 VPN 구현에 가장 널리 사용되는 기술이다. IPSec은 크게 IP 헤더를 포함하는 전체 패킷에 대한 인증 기능을 제공하는 AH (Authentication Header), IP 헤더 이외의 payload에 대한 암호화/인증 기능을 제공해 주는 ESP (Encapsulation Security Payload) 헤더, 그리고 AH/ESP를 포함한 각종 인터넷 보안서비스에 필요한 Security Association Negotiation 및 Key Management를 담당하는 ISAKMP/IKE (Internet Security Association and Key / Internet Key Exchange)로 구성된다.

IPSec의 Layer3 터널링과 PPTP/L2TP의 Layer 2 터널링의 장단점을 비교해 보면 다음과 같다[2].

◆ IPSec와 PPTP/L2TP의 차이점
(1) PPTP/L2TP는 IP 아닌 트래픽에 대해서도, 터널링이 가능하지만 IPSec은 IP 터널링만을 지원한다. 따라서 IP 외의 다양한 네트워 프로토콜을 사용하는 인트라넷에 대한 원격접속을 위해서는 PPTP/L2TP를 지원해야 한다.
(2) PPTP/L2TP는 사용자 단위의 인증, 동적 주소 할당 등이 가능하나, IPSec은 기본적으로 Host-to-Host 인증을 지원하며, fixed, routable IP address를 가정한다. 엄격한 액세스제어를 위해서는 사용자 인증이 필수적이므로 대부분의 IPSec 개발 업체들은 자체의 사용자 인증솔루션을 제공하고 있다.
(3) IPSec은 패킷 단위의 암호화/인증, 자동화된 키 관리 등의 네트워 계층 보안을 위한 기본 구조를 제공하지만, PPTP/L2TP는 단지 PPP 터널의 생성, 소멸, 관리를 주로 하며 PPP가 제공하는 외의 자체적인 보안기능이 거의 없다. 따라서 PPTP/L2TP는 보안을 위해 IPSec과 함께 사용할 것을 권장하고 있다.

2.2.3 5계층 프로토콜: SOCKS V5

SOCKS V5는 Authentication firewall traversal을 위한 순수한 Circuit-Level Proxy였던 SOCKS V4에 Client Authentication, Encryption, Encryption Negotiation, UDP Proxy 등 다양한 보안기능을 보강한 것으로 같은 Session Layer Security 프로토콜인 SSL/TLS와 결합되어 사용될 수 있으며, Session Layer Proxy로서 동작하므로 IPSec보다 정교한 액세스 제어 및 로깅 기능을 제공할 수 있다. IPSec 만큼 널리 알려지지는 않았으나, 최근에는 복잡한 네트워에 대한 관리 목적으로 사용되고 있다. SOCKS V5를 이용한 VPN은 하위계층의 터널링 프로토콜에 비해 뛰어난

액세스제어 기능을 제공한다[2][7].

다음 [표 1]은 위에서 살펴본 VPN 프로토콜들을 여러 가지 측면에서 비교하여 기업의 서비스와 보안요구에 효율적으로 적용하기 위하여 기술 특징들을 간략히 정리하여 나타낸 것이다[2].

| | PPTP | L2TP | IPSec | SOCKS V5 |
|---|---|---|---|---|
| Standardization | Microsoft | RFC 2661 | RFC 2401-2410 | RFC 1928, 1929, 1961 |
| OSI Layer | Layer 2 | Layer 2 | Layer 3 | Layer 5 |
| Mode | Client-Server | Client-Server | Peer-to-Peer | Client-Server |
| Protocols supported | IP, IPX, NetBEUI, AppleTalk, etc | IP, IPX, NetBEUI, AppleTalk, etc | IP | TCP, UDP/IP |
| Tunnel Services | Single PPP tunnel, Per-connection | Multiple PPP tunnels, Per-connection | Multipoint tunnels, Per-SA | Session-by-session basis |
| User authentication | None (by PPP) | None (by PPP) | None | Provided |
| Data authentication/ encryption | None (encryption provided by PPP) | None (encryption provided by PPP) (refer to IPSec) | Per-packet authentication/encryption by AH/ESP headers | Per-message authentication/encryption through GSS-API |
| Key management | None | None | ISAKMP/IKE | GSS-API/SSL |
| Access control | None (on server) | None (on server) | Packet filtering | Packet/content filtering, proxying |
| Best practices | Remote access | Remote access | LAN-to-LAN intranet | Extranet |
| Providers | Remote access vendor | Remote access vendor | Firewall, router, VPN vendors | Firewall, extranet VPN venders |

표 2. VPN 기술 특징 비교[2]

### 2.3 다양한 트래픽을 이용한 VPN 프로토콜 성능 평가

기존의 다양한 트래픽을 이용한 VPN 프로토콜 성능 평가 연구 결과에 따르면 OSI의 7계층 중에서 2계층에 VPN을 적용한 경우보다 3계층에 VPN을 사용하는 경우에 트래픽 오버헤드가 증가함을 알 수 있으며 2, 3계층 VPN을 함께 적용한 경우가 보안을 더 철저하게 제공해주면서도 증대되는 트래픽 오버헤드가 적음을 알 수 있다[6].

5계층에서의 VPN을 사용하는 경우에도 트래픽 오버헤드가 증가하지만 증대되는 정도가 적음으로 엑스트라넷 VPN과 같은 정교한 보안정책 관리 요구를 위하여 2, 3, 5계층 VPN을 효율적으로 함께 적용해야 한다[7].

## 3. 엑스트라넷 VPN 구축을 위한 효율적 터널링 및 프로토콜 적용방안

기존의 연구와 표준안은 VPN 프로토콜 기능적 측면에 따라 단지 SOCKS V5를 적용하여 엑스트라넷 VPN을 구축할 것을 권고하고 있다[2]. 그러나 기업마다 요구되는 서비스와 보안에 따라 적용되어져야할 터널링 및 프로토콜은 각기 다를 수 있다.

엑스트라넷 VPN은 인트라넷 VPN과 원격접속 VPN이 결합된 총체적 형태이다. 본 장에서는 [그림 1]과 같이 범용적인 엑스트라넷 VPN 구조를 모델로 선정하여 구현형태에 따라 인트라넷 VPN과 원격접속 VPN으로 구분하고 각각의 요구되는 일반적인 서비스와 보안에 따라 앞장의 내용을 토대로 효율적인 터널링 및 프로토콜 적용방안에 대하여 논한다.

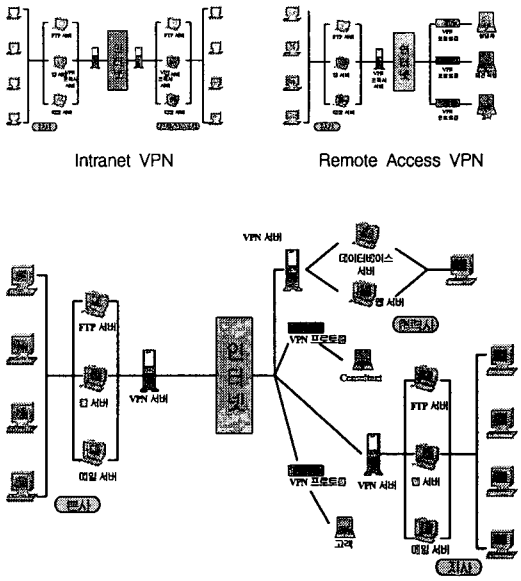


그림 1 Extranet VPN

기업들이 기업내부 위험성까지 보호하기 위해서는 VPN 클라이언트에 대해 종단간 보안솔루션을 구축하는 것이 중요하다[1]. 우선 앞장에서 기술한 두 가지 터널링 방식 중에서 네트워크 종단까지 강력한 보안을 제공하는 Voluntary 터널링을 전체로 적용하는 방안에 대하여 논한다.

### 3.1 인트라넷 VPN

본사, 지사, 협력사간(본사-to-지사-to-협력사)에는 기존의 다양한 트래픽을 이용한 VPN 프로토콜 성능평가[6]와 IETF(RFC 2041)의 VPN 프로토콜 표준의 권고에 근거하여 분석할 수 있으며, 기업간의 각종 업무처리에 대한 정보의 보안성을 강화하고 트래픽 오버헤드를 고려하여 L2TP와 IPSec을 함께 적용할 수 있을 것이다. 실제로 노키아의 VPN 솔루션제품평가에서도 L2TP와 IPSec을 함께 적용한 제품들이 대역폭 관리와 보안, 응용면에서 성능이 우수한 것으로 평가되고 있다[9].

#### 3.1.1 서비스에 따른 적용방안

본사와 지사간(본사-to-지사)에서는 IP이외에도 IPX, NetBEUI, AppleTalk 등을 이용하여 프린터와 같은 공유자원 등을 활용할 수 있는 업무가 가능해야 하고, 접속당 다중터널을 생성하여 QoS(Quality of Service)에 따라 효율적으로 서로 다른 터널을 이용하여 업무의 효율성을 높일 수 있어야한다. 또한 IPSec를 통한 충분한 암호화와 인증이 이

루어진 후에는 보다 빠른 업무처리를 위하여 트래픽 오버헤드가 가장 적은 2계층 프로토콜을 사용하는 것이 효율적이다. 이와 같이 요구되는 서비스들을 고려해 보면 L2TP를 적용하는 것이 가장 바람직하겠다.

3.1.2 보안에 따른 적용방안

본사와 협력사(본사-to-협력사) 혹은 지사와 협력사간(지사-to-협력사)에는 보안해야하는 정보와 공유해야할 정보를 제어할 수 있는 강력한 인증과 암호화가 요구되므로 L2TP에서 단순하게 적용되는 PPP의 암호화만으로는 이러한 보안 요구사항을 모두 만족하기는 어렵다. IPSec을 적용하여 AH/ESP에 따른 인증과 암호화, 더 나아가 ISAKMP/IKE의 키 관리를 사용해 보다 강력한 보안솔루션을 제공해야 한다.

### 3.2 원격접속 VPN

본사, 지사, 협력사와 Consultant, 고객간(본사, 지사, 협력사-to-Consultant, 고객 and Consultant-to-고객)에는 무엇보다 클라이언트 인증과 데이터 암호화에 따른 보다 정교한 보안정책 관리가 중요시되므로 IPSec보다 훨씬 정교한 접근제어 및 로깅 기능이 필요하다. Consultant와 고객에 대한 클라이언트 인증, 암호화 패러미터 협상(encryption negotiation), UDP 프락시 등 다양한 보안을 지원하는 SOCKS V5가 효율적인 적용방안일 것이다. 원격 접속을 위한 터널 생성과 트래픽 오버헤드를 고려하여 당연히 L2TP도 함께 적용하는 것이 바람직하다.

3.2.1 서비스에 따른 적용방안

기업과 클라이언트간(본사, 지사, 협력사-to-Consultant, 고객)에는 UDP프로토콜에 대한 서비스도 지원해야 하는 경우가 있다. 또한 비용적 측면을 고려해야 하고 윈도우 계통의 OS는 소스가 공개되어있지 않아 소프트웨어적으로 IPSec를 구현하는 것이 사실상 불가능하다고 할 수 있으며, 이동 단말의 특성상 사용하기 쉬워야 하므로 SOCKS V5를 적용하여 사용하는 것이 효율적일 것이다[7][10].

VPN을 구축하는 시 외부 클라이언트들의 모든 패킷을 SOCKS V5에 의하여 처리하는 것은 네트워크 처리 속도의 저하를 초래할 수 있다[7]. 그러므로 외부의 일반사용자들은 필요한 서비스에 따라 SOCKS V5와 L2TP를 효율적으로 함께 적용해가며 사용해야 할 것이다.

3.2.2 보안에 따른 적용방안

외부 클라이언트에 대해 인증, 메시지 보안 수준 협상, 권한 부여 등의 기능을 제공하여 보다 강력한 보안을 강화하기 위해서는 SOCKS V5를 사용해야 한다. 또한 UDP프로토콜 서비스에 따른 UDP Proxy 보안기능도 요구되므로 이 SOCKS V5를 적용해야 한다. 기업과 Consultant간(본사, 지사, 협력사-to-Consultant)에는 인증 후에 신뢰성을 인정하여 공유자원업무와 또한, 이에 따른 트래픽 오버헤드를 고려하여 보안이 요구되지 않는 업무에는 L2TP를 적용해야 한다.

그리고, SOCKS V5에서는 인증과 암호화를 위해 Kerberos에 입각한 GSS-API와 SSL을 사용하여 보다 강력한 효율적 암호화를 제공할 수 있다.

## 4. 결론

엑스트라넷 VPN 구현형태의 일부인 인트라넷 VPN과 원격접속 VPN으로 구분하여 요구되는 일반적인 서비스와 보안성을 만족하기 위해 인트라넷 VPN에서는 L2TP와 IPSec을 그리고, 원격접속 VPN에서는 L2TP와 SOCKS V5를 적용하는 방안에 대하여 논하였다. 구현 형태에 따라 요구되는 서비스와 보안을 고려한 L2TP, IPSec, SOCKS V5의 적용이 효율적인 엑스트라넷 VPN 구축 방안이 될 수 있을 것이다.

본 논문에서는 기존에 알려진 각 터널링 및 프로토콜의 기능과 성능을 분석하여 VPN 구현형태에 따라 요구되는 특정 서비스와 보안만을 고려한 효율적 적용방안에 대하여 논하였다. 따라서 대표적 모델에 대한 부분적인 적용 방안 외에 기업의 형태와 그에 따라 달라질 수도 있는 상세한 서비스나 보안에 대하여는 분석되지 않았다. 또한 QoS에 따른 네트워크의 트래픽 성능 분석이나 보안과 인증에 적용되는 암호알고리즘에 따른 분류, 그리고 다양한 보안솔루션과의 효율적 적용방안은 고려하지 못하였다. 그러나 논의된 터널링 및 프로토콜 적용방안은 표준화되지 않은 엑스트라넷 VPN 구축에 도움이 될 수 있을 것이다.

## [참고문헌]

[1] "VPN KnowledgeCentre", http://www.datanet.co.kr/tech_guide/vpn/
[2] 임채훈, "인터넷 보안: VPN, Firewall/IDS 기술", 한국통신학회 학술지 기고문, pp.3-9
[3] IBM, "The Layer 2 Tunneling Protocol(L2TP) in an IBM Virtual Private Network(VPN),"
[4] W. Townsley. A. Valencia. A. Rubens. G. Pall. G. Zorn. B. Palter. "Layer Two Tunneling Protocol(L2TP)" RFC 2661, IETF, 1999
[5] 강문희, "VPN(Virtual Private Network)기술의 개요", 통신정보보호학회지 제9권 제4호, 1999. 12.
[6] 오승희, "다양한 트래픽을 이용한 VPN 프로토콜 성능 평가", 정보처리학회논문지 C 제8-권 제6호
[7] 백석철, "SOCKS VPN 소개", 통신정보보호학회학회지 제9권 제4호, 1999. 12.
[8] IETF RFC 2401, Security Architecture for the Internet Protocol, 1998.
[9] "dataNet VPN 솔루션 4개제품 비교분석", http://www.datanet.co.kr/
[10] 강권학, "VPN의 개요", 안철수연구소