대한산업공학회/한국경영과학회 2000 춘계공동학술대회 논문집. 2000년 4월 21-22일. 경남대학교
Session PB4.1

글로벌 환경에서의 효율적인 원격접속 시스템 구축에 관한 연구

이문성*, 이용일*, 김창은**
* 명지대학교 산업공학과 석사과정
** 명지대학교 산업공학과 교수

Abstract

현재 기업은 정보통신과 컴퓨터 기술의 비약적인 발전으로 본사와 지사 사이의 정보의 교환이 중요한 문제로 대두되고 있다. 특히 재택근무에 대한 관심이 높아지고 있으며 이에 대한 방편으로 RAS(Remote Access Server) 및 VPN(Virtual Private Network)에 대한 연구가 활발히 이루어지고 있다. 본 연구에서는 VPN 및 RAS서버의 효율적인 구축 방법을 제시하고자 한다.

1. 서론

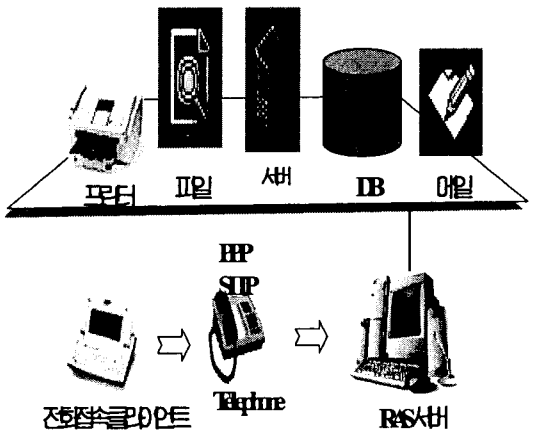
현재 기업환경은 글로벌하게 변하고 있으며 고전적인 기업 경영으로는 더 이상 급변하는 환경에 대처하기 힘들게 되었다. 특히 인터넷의 발전으로 원격접속에 의한 재택근무에 관심이 높아지고 있으며 이를 위한 RAS서버에 대한 연구 및 구축이 활발히 진행중에 있다. 아이네트, LG 인터넷, 삼성 SDS, SK 텔레콤, 한국통신, 데이콤 등 국내의 ISP(Internet Service Provider)가 최근 VPN 구현에 열을 올리고 있다. 기업의 경우 본사와 지사, 국내와 국외 정보 공유의 중요성이 어느때 보다도 중요하게 대두되고 있다. 한편 현재 우리나라의 경우 해킹의 우범지대 네트웍 보안이 어느때 보다도 중요하게 인식되고 있다. 본 연구에서는 원격접속을 위한 RAS 구축 및 보안을 위한 프로토콜의 결정과 VPN의 구축을 제시하고자 한다. 본 연구은 각 프로토콜별 차이를 비교하고 이에 따른 구축 방법을 제시하고자 한다.

2. 본론

2.1 RAS(Remote Access Server)

RAS는 Remote Access Server의 약자로써, 다양한 형태의 사용자를 광역통신망에 접근시키기 위하여 구성되는 서버를 뜻한다. RAS를 구성하는 매체로는 Terminal Server, Modem Access Server가 있으며, 현재 일반 가정에서의 Internet Access, 재택 근무, SOHO에서의 광역 망 Access, 원격 Monitoring 등에 이용되고 있다. RAS는 ISDN, Modem, X.25 Link를 포함하여 다양한 유형의 WAN접속을 지원한다.

아래의 [그림 1]은 일반적인 RAS서버의 이용을 나타낸 것이며, 이 경우 전화접속 클라이언트는 RAS서버에 접속하기 위해 PPP 및 SLIP 프로토콜을 이용하여 접속한다. 접속 후에는 로컬 네트웍의 자원을 NetBEUI나 TCP/IP, NWLINK등을 이용하여 엑세스하게 된다. RAS서버에 의해 IP를 할당받게 되며 RAS서버의 NetBIOS 게이트웨이와 IP와 IPX 게이트웨이를 통해 내부 네트웍과 통신을 할 수 있게 된다.



[그림 2] RAS 작동 원리

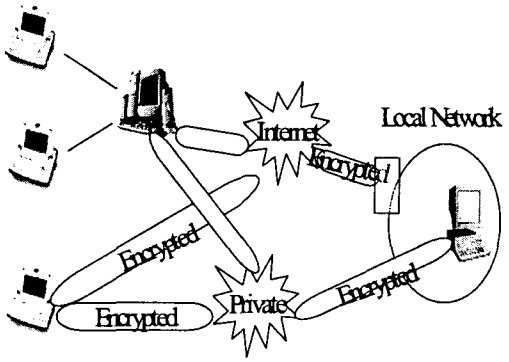
2.2 인터넷을 통한 네트웍 접근

인터넷의 폭발적인 사용에 따라 지역 전화요금으로 인터넷을 통해 전국 어디든 접속이 가능해 졌으며 본사와 지사의 연결 및 국내와 국외의 연결이 가능해 졌다.

2.2.1 VPN(Virtual Private Network)

VPN의 원 개념은 자체 정보통신망을 보유하지 않은 사용자도 공중데이터통신망을 이용해 마치 개인이 구축한 통신망과 같이 이를 직접 운영, 관리할 수 있는 것을 의미한다. 이를 위해 터널링기법을 이용하여 통신의 시작과 끝점 즉, 본사와 외부의 PC사이에 터널이라는 가상 통신 선로를 구축해 마치 전용선을 두 지점에 연결한 것처럼 이용하는 것을 의미한다. 터널내는 전용선처럼 되어 해킹을 방지하며, 터널을 통과하는 자료는 암호화되어

보안성을 제공한다. 이를 위해 MS(MicroSoft)사의 경우 PPTP, IPSec, L2TP 등의 프로토콜을 제시하였으며, 이를 이용하여 실제 자사의 인트라넷을 구축하여 사용 중이다.



[그림 3] VPN이용 예

이 경우 보안을 위해 각각을 터널링으로 연결하고 암호화를 통해 데이터를 보안한다.

2.2.2 VPN 국내외 동향

① 국내 동향

국내 VPN은 도입 단계로 어느 SP (Service Provider)도 완벽한 서비스를 제공하고 있지 못하다. 아이네트는 VPN 전용장비 업체인 VPNet의 VSU를 이용하여 초기 서비스를 제공하고 있으며 제일제당 등이 본사와 지사를 VPN을 통해 연결하고 있다. 또한 VPN구축 후 3개월 정도만에 투자비용을 회수했다. 데이콤은 천리안을 통해 VPDN을 제공하고 있으며, 최근 VPN 전용 01422망을 이용하여 서비스를 제공할 계획이다.

② 국외 동향

국외 VPN사업은 발전 단계로 SLA(Servise Level Agreement)를 지원하는 서비스에서부터 단순히 네트워크의 보안만을 지원하는 서비스까지 네트워크를 구성하는 방식에 따라 다수의 SP업체들이 다양한 형태로 VPN서비스를 지원하고 있다.

2.2.3 터널링 기법

터널링은 데이터 및 관련 사용자 정보 스트림이 인터넷에서 가상의 파이프를 통해 전달되도록 하는 것이다. 송신단은 소스 패킷을 터널링을 통해 IP패킷 내에 캡슐화하며, 인터넷을 통해 전달된 패킷은 수신단에서 터널링 해제를 통해 IP허더를 제거하고 난 후, 목적지 사이트로 전달된다. 터널링은 2계층과 3계층으로 분류되며, 이를 이용하여 VPN을 구축할 수 있다. 2계층 터널링의 경우 클라이언트-서버 모델로 원격접속 VPN에 적용되며, PPP패킷에 캡슐화된 IP데이터그램을 터널링한다. 현재 적용되는 프로토콜은 PPTP, L2TP 등이 있다. 3계층의 경우 IPSec이 이용된다.

	2계층	3계층
프로토콜	PPTP, L2TP	IPSec
모드	클라이언트-서버	호스트-호스트
캡슐화 프로토콜	IP, IPX, Apple Talk	IP
인증	비표준화, 자체지원	IPSec
암호화	비표준화, 자체지원	IPSec
특징	PPPrl술 활용	다중 서비스지원

[표 1] 계층별 터널링 프로토콜

① PPTP : 2계층 프로토콜로써 기존 다이얼-업 접속에 사용되는 PPP 프로토콜을 기반으로 하고 있다. 현재 Windows NT, Windows 2000, Win 95/98이 지원 중이다.

② L2F : 원격지 사용자의 홈사이트에서 주소 할당이 이뤄지며 사용자 인증은 본사의 게이트웨이에서 이뤄진다. 접근 서버는 주어진 도메인과 사용자 ID가 VPN 사용자임을 증명한다. 기본적으로 PPP를 이용하고 TACACSA+ 와 RADIUS를 지원한다.

③ L2TP : 2계층으로 PPTP와 L2F를 통합한 것으로 PPP 프로토콜을 기반으로 한다. 일반적으로 2계층 프로토콜이 확장성이 약한데 비해 L2TP는 확장성이 크다. 그러나 강력한 확장성을 원할 때가 아니고 굳이 L2TP를 선택해야하는 이유가 있지 않다면 L2F를 이용한다.

	PPTP	L2TP
터널 초기화	클라이언트 PC NAS	NAS
기반 네트웍	IP	IP,ATM, X.25
인증	PAP, CHAP, MS-CHAP, RADIUS	PAP, CHAP, FAP, RADIUS
암호화	MPPE	IPSec
메시지 전달방식	개별 스트림	단일 스트림

[표 2] PPTP 와 L2TP의 차이점

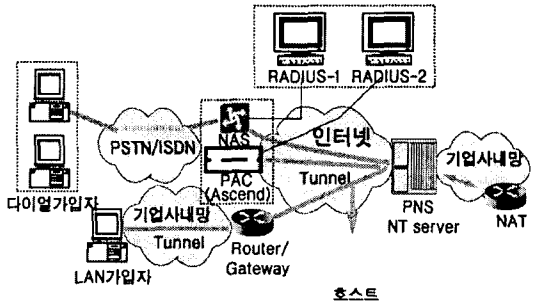
④ IPSec : 데이터 인증, 패킷 무결성, 데이터 신뢰성, 응답보호, 암호키 자동 관리 및 SA 등을 규정하고 있다. 이를 위해 IPSec은 AH, ESP, IKE 등 3개의 프로토콜을 정의하고 있다. 이는 매우 강력한 암호화를 적용한 프로토콜로 현재 IP네트워크에서 VPN보안의 표준으로 인식되고 있다.

2.2.4. 각 터널링별 VPN 구성

①PPTP를 이용한 NAS initiated VPN

다이얼업 가입자의 구분에 따라 ISP PAC 또는 NAS(Network Access Server)를 통하여 기업의 PNS(HP, Windows NT Server 4.0)에 접속할 수

있다.

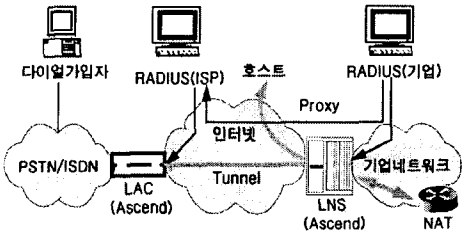


[그림 4] PPTP를 이용한 VPN 구성

[그림 3]의 NAS(Network Access Server)를 통하여 PNS에 접속하는 PPTP 가입자는 ISP 인증서버(RADIUS-1)로 부터 PPP인증을 거친 후에 IP를 할당 받고, 별도의 PPTP 클라이언트 프로그램을 구동하여 기업의 PNS에 VPN 접속한다. 한편, 별도의 PPTP 클라이언트 프로그램을 소유하지 않은 가입자는 PAC을 이용하여 RADIUS-2로 부터 PPTP 가입자 인증을 하고 PNS에 접속하여 PPTP 서비스를 제공받는다.

② L2TP를 이용한 NAS initiated VPN

[그림 4]는 VPN 가입자가 LAC(L2TP Access Concentrator)에서 LNS(L2TP Network Server)까지 생성된 터널을 통하여 기업의 RADIUS에서 인증을 받고 LNS로 부터 기업내의 사설 또는 공중 IP를 부여 받는 구조를 보여주며, 가입자가 사설 IP를 할당받는 경우 기업 내부의 NAT 장치를 통하여 인터넷 서비스를 이용하는 것을 나타내고 있다.

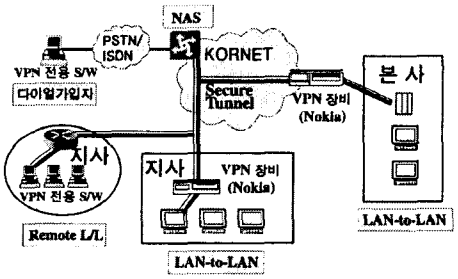


[그림 5] L2TP를 이용한 VPN 구성

[그림 4]의 LAC는 다이얼업 가입자에 대하여 PPP 인증을 하는 NAS 기능을 지원하며, 가입자의 프로파일을 분석하여 LNS와 L2TP 세션을 생성하는 기능을 한다. 예를 들면, "VPN.com" 회사의 "user" 라는 가입자(user@VPN.com)에 대하여 ISP의 인증서버는 기업(VPN.com)의 인증 서버로부터 가입자 인증을 확인할 수 있는 Proxy 인증 기능을 수행한다. 가입자 인증이 확인되면 기업의 LNS는 ISP LAC와 생성된 터널의 세션을 보장한다.

③ IPSec이용한 NAS initiated VPN

[그림 5]는 전용 VPN 장비와 S/W를 이용하여 LAN-to-LAN VPN 서비스 및 Client Initiated VPN 서비스를 구성한 것이다. 본사와 지사간에 별도의 VPN 장비를 이용하여 터널을 구성하고, 데이터의 암호화 및 NAT(Network Address Transla-tion)기능을 수행한다. VPN 장비를 구성하지 않는 소규모 LAN 가입자나 다이얼업 가입자는 기업이 소유한 VPN 장비와 연동되는 전용의 VPN S/W를 사용자 클라이언트에서 구동하여 Client Initiated VPN 서비스를 이용한다. [그림 5]와 같이 구성된 경우에는 지사와 본사간의 각각의 VPN 장비를 이용하여 보안정책을 기업 자체적으로 가질 수 있다는 장점도 있다. 보안정책의 주요 요소로는 가입자 IP를 이용한 라우팅 제한, 원격 가입자의 사용자 권한에 따른 라우팅 및 사용자 포트 등이 있으며, 이를 활용하여 보안을 강화할 수 있다.

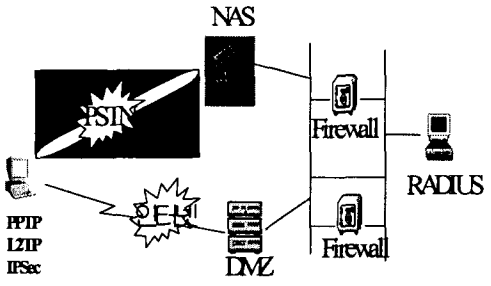


[그림 6] IPSec을 이용한 VPN 구성

VPN 장비를 이용한 LAN-to-LAN VPN

④ 보안을 고려한 VPN 구성

[그림 6]은 Firewall을 PSTN망과 인터넷망의 각 끝 지점에 두어 각각을 통해 들어오는 패킷이 일단 firewall을 통과한후 RADIUS를 통해 사용자 인증을 받은 경우로, 각각의 Firewall의 경우 하나가 다운되었을 경우에도 다른 한쪽을 거쳐 RADIUS로 통하도록 구성하였다.



[그림 7] VPN With NAS

2.2.5 VPN에 있어서 보안

VPN에 있어서 보안은 다음과 같은 방법으로 실행한다.

① DHCP를 이용하여 원격 액세스 클라이언트의 IP 획득
② 강력한 암호화를 사용
③ EAP-TLS를 적용하여 스마트 카드를 사용
④ MS-Chap v2 같은 인증기법 이용
⑤ IPX 네트워크 아이디의 자동 할당을 사용
⑥ 동일 사용자에게 다중 정책을 설정하지 않음

2.2.5 적절한 프로토콜의 이용

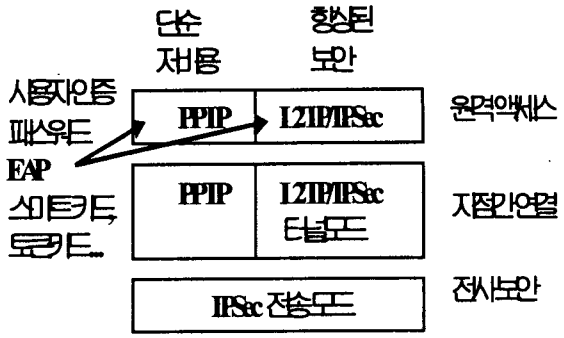
VPN은 인트라넷 VPN, 리모트 액세스 VPN, 익스트라넷 VPN 등으로 나뉘며 각각에는 적절한 프로토콜이 사용되어야 한다.

인트라넷 VPN의 경우 기업 내부의 부서를 LAN을 통해 연결하거나 넓게는 지방의 지사까지 연결하는 형태로 접석은 일시적이거나 영구적일 수 있다. 리모트 액세스의 경우 기업과 리모트/원격지 사원간의 접속으로 회선의 신뢰성과 Qos가 중요하다. 이 경우 인증도 중요한 문제가 될 수 있다. 익스트라넷의 경우 가장 확장되 의미의 VPN으로 전략적인 차원에서 자사의 직원뿐만 아니라 파트너, 고객까지 묶는 형태이다. 이 경우 가장 중요한 것은 트래픽 관리와 병목현상을 줄이는 것이다.

	PPTP/ PPP	L2TP/PPP IPSec Transport Mode	IPSec Transport Mode	IPSec Tunnel Mode
리모트액세스 VPN	X	X		
Branch Office VPN	X	X		IP Only
익스트라넷 VPN	X	X		IP Only
인터넷 보안			Unicast IP Only	

[표 3] 적절한 프로토콜 결정

[표-3]은 각각의 VPN 종류에 따른 프로토콜을 나타낸 것이다.



[그림 8] 윈도우 2000보안

[그림 7]의 경우 윈도우즈 2000보안과 비용에 대한 내용이다.

3. 결론

인터넷에서의 VPN은 많은 매력을 갖고 있다. 지역 사무소 및 외근 직원들이 전용 WAN보다 더 저렴한 비용으로, 인터넷을 통한 비즈니스 네트웍에 접속할 수 있는 새로운 방법이 제공되고 ISP에게는 새로운 비즈니스 기회를 제공한다. 이를 통해 상당한 WAN비용을 절감할 수 있다. 글로벌한 환경에서 VPN의 구축은 필수이며 이를 구축시 가장 중요한 이슈는 당연히 보안이라 할 수 있다. 구축 VPN의 종류와 보안의 정도 및 트래픽 관리에 따른 적절한 VPN 요소 기술의 선택이 중요하다 할 수 있다. 본 연구에서는 적절한 요소 기술의 결정 및 VPN 구축에 대해 연구하였으며 향후 연구 과제로는 QoS제공과 VPN 서비스 관리 기능을 제공할 수 있는 방안을 연구하여야 할 것이다.

[참고문헌]

[1] 이정수, 김이한 "인터넷 VPN 서비스 도입 방안", 1999
[2] 오채형, 이경근, 김성국 " 인터넷 VPN 서비스 시험 및 분석", 1999
[3] 김정준, "스마트카드 신기술 개발 동향 및 시장 전망", 1999
[4] on the net "VPN 구축" 1999, 8,9,10월호
[5] Don Benage, "Using Microsoft BackOffice" 1997
[6] Microsoft, "Supporting Microsoft Windows NT4.0 Core Technologies"
[7] Brian Quinton, "THE CASE FOR PACKETIZING VPNs ", 1999
[8] Mike Fratto, "Altiga Concentrates on VPN Security ", 1999