차별화된 VPN 서비스를 위한 전략

장 준 형*, 이 경 근**
*하나로통신(주), **세종대학교
*zanga@hanaro.com, **kglee@sejong.ac.kr

A Strategy for Differentiated VPN Services

Joonhyung Chang*, Kyung Geun Lee**
*Hanaro Telecom, Inc., **Sejong University

요 약

VPN은 기존 공중망에서 물리적인 네트워크의 구성과 무관하게 터널링과 암호화를 통해 논리적으로 폐쇄된 사용자 그룹을 구성한다. 사용자 그룹별로는 암호화된 터널을 구성하여 독립적인 가상의 망을 연결하고, 이 터널들을 통해 데이터의 전송이 가능하므로, 인터넷을 마치 전용선처럼 이용하여 보다 저렴한 통신비용으로 인트라넷, 익스트라넷, 원격지 접속 등이 가능한 안전한 통신망을 구축할 수 있게 한다. 본 논문에서는 현재 널리 사용되고 있는 VPN의 대표적 기술 중의 하나인 터널링 기술의 특징을 개략적으로 살펴보고, 일본 기업들의 VPN 서비스 제공 사례들을 분석한 후, 통신사업자 관점에서 망 구성 방안과 차별화된 VPN 서비스를 위한 방안을 제시한다.

1. 머리말

인터넷은 기존산업의 전 부문에 걸쳐 효율성과 생산성 향상을 위한 전략적 도구로서 그 필요성이 급속히 증대되고 있다. 특히, 최근에 인터넷은 인트라넷이나 익스트라넷 등과 연계되어 기업에서의 전자상거래, SCM(Supply Chain Management), 통합업무패키지와 같은 중요한 어플리케이션에 이용되고 있다. 이렇게, 인터넷을 통해 지사나 거래선 등과 데이터를 주고받는 기회가 늘어나고, 그에 따라 기업통신망이 외부에 손쉽게 노출되게 됨에 따라 기업네트워크의 보안 확보가 중요한 과제로 제기 되었다.

이와 같이 변화된 환경에서 기업 사용자의 솔루션으로 암호화나 인증 기법을 사용하여 기업 네트워크 보안을 실현하는 수단으로 대두된 것이 VPN(Virtual Private Network) 서비스이다. 또한, VPN은 기존 전용회선 보다 저렴한 비용으로 안전하게 기업의 네트워크를 위탁관리할 수 있다는 장점이 있어 많이 선호되고 있다. 이러한 VPN 서비스를 위해 기존 방화벽과 라우터에 VPN 기능을 탑재하거나 트래픽의 집중에 따라 야기되는 성능 문제 등을 개선하기 위한 VPN 전용장비들도 많이 연구되고 있다. 그러나, 안정적인 서비스 제공을 위해 QoS 보장을 위한 대역폭 확보 및 다양한 VPN 제품들에 대해 VPN의 표준 프로토콜로 채택된 IPsec를 이용한 상호 운용성의 확립과 정책 데이터 모델의 확립이 시급한 실정이다[1].

본 논문은, 2절에서 VPN의 특성과 주요 기술인 터널링 프로토콜의 특징을 개략적으로 살펴보고, 다음 3절에서는 VPN의 국내외 서비스 동향과 특히 일본내 주요 통신 사업자의 서비스 제공 내용을 간략히 비교함으로써, 통신사업자 관점에서의 VPN 서비스 제공 모델을 도출해 내고자 한다. 끝으로 4절과 5절에서는 기존 가입자망을 이용한 VPN 망 구성 방안과 차별화된 VPN 서비스 제공 방안을 제시한 후 결론을 맺는다.

2. VPN의 특성과 주요 기술

가상사설망(VPN; Virtual Private Network)이란 자체 통신망을 보유하지 않은 가입자 자신이 공중망을 이용하여 사설 전용망과 동일한 기능의 서비스를 제공하는 네트워크의 한 형태로 프레임 릴레이, ATM(Asynchronous Transfer Mode), IP 등의 공중망에서 물리적인 네트워크의 구성과 무관하게 터널링과 암호화를 통해 논리적으로 폐쇄된 사용자 그룹을 구성한다.

사용자 그룹별로는 암호화된 터널을 구성하여 독립적인 가상의 망을 연결하고 이 터널들을 통해 데이터를 전송한다. 그리고, 가입자 자신이 공중 통신망 내에서 소프트웨어적으로 망을 정의하고 변경할 수 있기 때문에 통신망 변경 시 물리적인 재구성이 필요치 않으며, 공중망을 마치 가입자 자신의 전용망과 같이 이를 직접 운용, 관리할 수 있다. 기업체나 기타 그룹간 인트라넷, 익스트라넷 등의 구축 시에 공중망을 이용하여 네트워크 구축비용을 줄일 수 있는 동시에, 보안성과 신뢰성을 확보할 수 있다는 장점을 갖고 있다. 특히, 본사와 위성 사무실간에 데이터를 전송하거나 원격지 혹은 재택 근무제를 운용하고 있는 업체의 경우 효과가 크다.

신뢰성과 안전성이 높은 VPN 서비스를 제공하기 위해서는 터널링 기술, 키 관리 기술, 그리고 VPN 관리기술 등의 제반 기술과 인증 및 암호화 기술, 그리고 부가적으로 라우터나 방화벽에서 제공하는 일부 보안 기술 등이 병행 되야 가능하다. 여기서는 특히 VPN의 주요 기술인 단대단 터널링 기술과 통신사업자의 인터넷 백본망에서 VPN을 구현하기 위한 기술에 대해 서술한다.

2.1. VPN 터널링 기술

터널링은 마치 송신자와 수신자 사이에 터널을 뚫는 것처럼 송신자가 보내는 데이터를 캡슐화하여 수신자 외에는 알아볼 수 없도록 데이터를 전송하는 기술로서, 어떠한 페이로드라도 수용할 수 있으며 GRE(Generic Routing Encapsulation)를 이용하여 여러 사용자가 동시에 여러 형태의 페이로드를 액세스할 수 있다. 또한 VPN을 이용하는 기업은 그들의 IP 주소를 망에 알리지 않고, 사용자가 기업에 액세스할 수 있도록 하며, 기업이 각각의 터널 연결을 필터링할 수 있게 한다.

다음 [표 1]에서 현재 VPN 서비스를 위해 구현되고 있는 대표적인 터널링 프로토콜인 PPTP(Point-to-Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), IPsec(Internet Protocol Security)의 특징을 비교 분석하였다[2][3][4].

[표 1] 대표적인 터널링 프로토콜의 비교

구분	PPTP	L2TP	IPsec
제안	마이크로소프트사	시스코시스템즈 외	IETF
모드	클라이언트와 서버간	클라이언트와 서버간	호스트 혹은 게이트웨이간 호스트와 게이트웨이간
목적	터널링을 통한 원격 접속	터널링을 통한 원격 접속	터널링을 통한 인트라넷,익스트라넷, 혹은 원격 접속
터널링 계층	계층2	계층2	계층3
캡슐화 가능한 프로토콜	IP, IPX, AppleTalk 등	IP, IPX, AppleTalk 등	IP
사용자 인증	비제공(PAP,CHAP, Kerberos,Token ID 등과 함께 사용)	비제공(PAP,CHAP, Kerberos,Token ID 등과 함께 사용)	비제공(PAP,CHAP, Kerberos,Token ID 등과 함께 사용)
패킷 인증	비제공(혹은 비표준)	구현시 IPsec참조	제공(AH 등의 사용)
패킷 암호화	벤더가 제정 표준	구현시 IPsec참조	제공(ESP 등의 사용)
키 관리 가능	비제공(혹은 비표준)	구현시 IPsec참조	제공(ISAKMP/Oakley 등의 사용)
제공 터널수	단일	복수	복수, VPN과 공중망에 동시 접속 가능

* PAP: Password Authentication Protocol
CHAP: Challenge-Handshake Authentication Protocol
AH: Authentication Header, ESP: Encapsulating Security Payload
ISAKMP: Internet Security Association and Key Management Protocol

2.2 백본망에서의 VPN 적용 기술

2.1절의 [표 1]에서 언급한 터널링 기술들은 단대단 VPN을 제공하는 방식으로 현재의 인터넷 백본망을 수정하지 않고, 터널을 설정하기를 원하는 종단 장비에 VPN 기능을 추가하여 VPN 서비스를 제공할 수 있다는 장점이 있다. 그러나, 인터넷을 매개로 하기 때문에 지연이나 성능에 취약하므로 QoS의 보장이 요구되는 기간 네트워크에는 부적합하다.

최근 인터넷의 급속한 성장은 백본망의 부담 증가와 서비스 품질 저하로 이어지고 있다. 따라서, 이러한 개선 노력으로 MPLS(Multi-Protocol Label Switching)과 WDM(Wavelength Division Multiplexing) 등과 같은 기술들이 적용되고 있다.

특히, MPLS는 레이블 교환 방식(Label Swapping)에 의한 가상 연결을 설정하여 트래픽을 전달한다. 따라서, VPN을 제공하는 기능뿐만 아니라 고속 패킷 전달과 다양한 QoS를 보장한다. 또한, MPLS를 지원하는 망에서 스위칭 경로를 설정할 때, 전체 네트워크의 혼잡을 최소화하도록 트래픽 엔지니어링을 적용할 수 있어, 백본망 자원의 효율적 사용과 서비스 품질의 향상이 가능하다. 그리고, MPLS는 IP와 ATM의 통합 백본망을 위한 적합한 방안으로 대두되고 있으며, 많은 통신사업자들은 VPN 서비스를 제공하기 위한 백본망 구축 방안으로 기존 라우터나 ATM에 MPLS를 적용하는 사례도 늘고 있다.

3. VPN의 국내외 서비스 동향

IDC의 보고서[5]에 따르면, 미국에서 현재 WAN 서비스를 이용하고 있는 업체 중 응답자의 약 64%가 IP-VPN을 이용하고 있거나 검토중 이라고 한다. 또한, IDC의 전 세계 VPN 서비스 시장 예측 자료[6]에서도 2000년 20억 달러 규모에서 2004년에 176억 달러 규모의 매출이 이루어지며 이 기간 동안 평균 72.9%성장이 예상된다고 밝혀, 향후 전통적인 WAN 서비스를 점차 대체해 나갈 것으로 예상된다.

현재, 국내 통신사업자 중 KT는 지난해부터 「엔텀VPN」을 제공하고 있으며, 향후 미국, 일본, 유럽 등과 총 10여 개 노드를 구축해 전 세계를 대상으로 글로벌 IP-VPN 서비스를 제공할 계획으로 있다. 한편, 데이콤은 기존의 CPE(Customer Premises Equipment) 기반 VPN과 별도로 국내 최초로 MPLS 기술을 적용한 「보라MVP」의 상용 서비스를 시작했으며, PSINET은 PVC (Permanent Virtual Connection)를 이용한 프레임 릴레이 기반 VPN과 인터넷 기반 IP-VPN 서비스를 동시에 제공하고 있다. 또한, 하나로통신은 일본의 AIH와 협력관계를 맺고 해외 IP-VPN 사업을 준비중이다. 지금까지 관심에만 머물렀던 VPN 서비스는 그동안 부진했던 실수요를 창출하기 위해 통신사업자들은 저마다 다양한 서비스와 새로운 기술을 접목시켜 시장 확대에 주력하고 있다[7].

현재, 국내에서의 VPN 서비스는 초기 단계로 그 효과를 검증하고 분석할 만한 사례를 들기에는 아직 시기상조이다. 따라서, [표 2]에서 VPN 서비스에 한발 앞선 일본 통신사업자의 VPN 서비스를 비교한 후, 각 기업들의 네트워크 구축 및 서비스 제공 사례들을 살펴보기로 한다.

[표 2] 해외(일본) 통신사업자의 VPN 서비스 비교

통신사업자명		KDDI	JAPAN텔레콤	NTT텔레콤
서비스명		ANDROMEGA IP-VPN서비스	SOLTERIA	Super VPN
VPN 실현방식		MPLS	MPLS	MPLS
서비스 시기		2000년 10월	2000년 4월	2000년 7월
1.5Mbps의 월 통신료	2거점접속	57만엔	58만엔	55만 6000엔
	5거점접속	142만 5000엔	143만 5000엔	139만엔
	10거점접속	285만엔	282만엔	278만엔
다이나믹 라우팅		Static라우팅(명시되어 있지는 않지만 BGP-4 제공)	제공(BGP-4)	제공(BGP-4)
서비스 품질 보증 계약 (SLA)		VPN 가동율: 99.9% 평균 지연시간: 월평균 35ms이하	비제공 (향후 도입 예정)	비제공(향후 도입 예정)
패킷 우선 제어		옵션으로 제공	제공 (라우터 설정 요금 부가)	비제공(향후 도입 예정)
다이얼 업 접속		가능	부가 (향후 도입 예정)	부가(향후 도입 예정)
VPN 그룹간의 통신		가능(월1000엔/거점)	가능(월1000엔/거점)	부가(향후 도입 예정)

* 통신료는 액세스 회선에 NTT 지역회사의 이코노미 전용선 디지털액세스 타입1 적용시 (거리구분은 15Km 이내)

[표 2]에서 보는 바와 같이 3사 모두가 기업을 대상으로 MPLS기반의 IP-VPN 서비스를 제공하고 있으며, 서비스 품질 보증(SLA; Service Level Agreement)의 도입과 패킷 우선 제어, 그리고 다이얼 업 접속 등과 같은 부가서비스를 현재 제공중에 있거나 향후 도입을 검토하고 있다.

우선, KDDI의 VPN서비스는 그룹사가 전개하고 있는 각종 서비스의 차세대 IP 기간망인 「PERSEUS」로 수용하기 위한 수단으로 위치를 부여하고 있다. KDDI는 액세스 회선의 선택폭의 다양함과 풍부한 부가서비스를 최대의 무기로 내세우고 있다. 즉, 고속 디지털 전용선이나 ATM 전용선 이외에, 「KDD원스터」의 가입자계 무선 액세스나, KDDI 국사와 고객의 오피스 빌딩 등을 직결하는 광 통신망「Metro ring」도 수용한다. 휴대전화의 다이얼 업 접속에서도, 타사보다 먼저 대응한다는 전략을 내세우고 있다. 특히, SLA를 도입하거나, 옵션으로 패킷 우선 제어를 가능케 하는 등, 부가서비스를 풍부하게 준비하여 차별화를 꾀하고 있다. 그리고, 프레임 릴레이 등과의 상호접속을 가능케 하여 기존의 서비스로부터의 이행을 쉽게 하는 데에도 주력하고 있다. 그러나, 라우팅 방식은 원칙적으로 Static 라우팅만 제공한다.

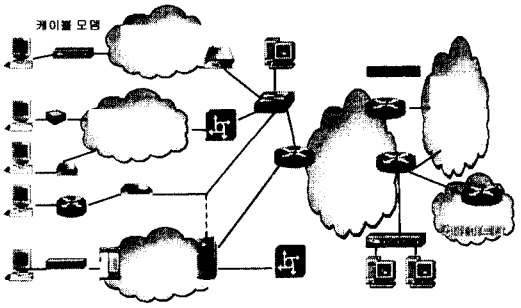
한편, JAPAN텔레콤은 IP-VPN 서비스를, 종래의 전용선 등의 통신 서비스와 다른 것으로 위치를 부여하고 있다. 그 서비스 목적을 기업 네트워크를 일괄적으로 담당하는 아웃소싱 서비스의 전개에 두고 있다. 따라서, 프레임 릴레이나 셀 릴레이

와의 상호접속 기능은 제공하지 않는다. 한편, 액세스 회선 부분의 요금체계도 액세스 기본료와 네트워크 접속 기본료로 나눈다. 특히, 액세스회선으로 ATM 전용선을 이용하는 경우 고객이 복수의 VPN과 접속을 원할 때, 물리적인 회선 1개로 각 VPN 그룹과 VP를 설정하여 다중으로 접속을 가능하게 한다.

또한, NTT커뮤니케이션의 경우, 타사에 비해 통신료에서는 우위를 유지하고 있지만, 패킷 우선 제어, SLA, 혹은 익스트라넷에서의 VPN간 통신 등은 제공하지 않고 있다. 한편, NTT커뮤니케이션은 이전부터 제공해 왔던 프레임 릴레이/셀 릴레이를 기반으로 하는 서비스인 「Arcstar21」과 「Super VPN」의 분리를 고민하고 있다. 「Super VPN」에 SLA를 도입하는 경우 상대적으로 「Arcstar21」의 우위성 약화가 예상되어 고객의 유출을 우려하고 있다[8].

4. VPN 망 구성 및 서비스 차별화 방안

본 절에서는 차별화된 VPN 서비스를 제공하기 위한 망 구성 방법을 [그림1]과 같이 제안하며, 3절의 선행업체 사례에서 도출된 서비스 차별화 방안을 제시하고자한다. VPN 망 구성을 각각 백본망과 액세스망의 관점에서 차별화하기 위하여 다음과 같은 사항들이 고려되어야 한다.



[그림 1] 기존 가입자망을 이용한 VPN 망 구성

백본망은 MPLS 라우터나 WDM(Wavelength Division Multiplexing) 장치로 구축하여 IP 패킷을 고속으로 전송한다. MPLS는 2.2절에서 살펴본 바와 같이 VPN 기능을 제공할 뿐만 아니라, 서비스 품질 향상을 위한 QoS 보장과 트래픽 엔지니어링이 가능하고, 망의 확장에 효율적으로 대처할 수 있다. 또한, 망 내의 보안은 패킷에 라벨을 부여하여 통신 상대를 특정하여 IP망을 가상적으로 구분함으로써 확보한다. 또한, 고속의 라우터 사이는 WDM으로 연결하여 추가적인 광섬유 망의 구축 없이 전송 용량을 배가시키고 라우터의 처리 능력과 광링크의 전달 능력 사이의 격차를 해소할 수 있도록 한다.

한편, 액세스망은 기존의 PSTN/ISDN, 전용선, 그리고 초고속 인터넷 서비스를 위한 ADSL 망과 CATV/HFC(Hybrid Fiber Coaxial) 망 등 다양한 매체를 이용할 수 있다. 특히, 초고속 인터넷 서비스를 위한 ADSL 혹은 CATV/HFC 망을 VPN의 액세스망으로 이용할 경우 기존 전용회선 보다 저렴한 비용으로 광대역 VPN 서비스의 이용이 가능하다. 또한, 이동 가능한 원격접속 사용자가 VPN에 접속 가능하도록 PSTN 혹은 ISDN과 NAS(Network Access Server)를 연동시킨다. 만일, 액세스망의 안정성과 일정한 대역 확보가 요구되는 경우, 전용선을 이용한다. 이 경우 빌딩이나 아파트 단지 내에 설치되어 있는 광단국과 가입자 댁내에 DSU(Data Service Unit) 혹은 CSU(Channel Service Unit)를 사용하여 다양한 대역별 서비스 제공이 가능하도록 한다. 한편, 원격 접속자의 보안과 인증을 제공하기 위해, 표준 터널링 프로토콜인 L2TP와 IPsec를 채택하며, RADIUS(Remote Access Dial-in User Service)와 NAS를 연동하여 인증 시스템을 구성한다. 한편, 초고속 인터넷 서비스를 받는 경우의 가입자 인증은 B-RAS(Broadband-Remote Access System) 혹은 CMTS(Cable Modem Termination System)와 DHCP(Dynamic Host Configuration Protocol) 서버에서 IP주소의 동적 할당과 함께 이루어지게 한다.

또한, 3절에서 언급한 선행업체의 사례로부터 서비스 차별화를 위하여는 다음의 방안이 모색되어야 한다.

첫째, VPN이 저렴한 비용으로 기업의 네트워크를 아웃소싱을 통해 안전하게 위탁 관리하기 위한 방안으로 제시됨에 따라서, 고속디지털전용선, 프레임 릴레이, ATM 등과 같은 고객측의 다양한 액세스 환경에 적절히 대응하여야 하고, 네트워크 속도 보장, 패킷 우선 제어 등 QoS를 가능케 하는 다양한 부가 서비스의 제공으로 서비스의 차별화를 꾀하여야 할 것이다. 특히, 데이터 암호화, 사용자 인증, 방화벽, 그리고 바이러스 대책 등이 통합적으로 운영되는 신뢰성 있는 보안시스템을 제공한다면, 부정적인 인식으로 VPN 도입을 미뤄오던 상당수의 기업 고객들을 확보할 수 있을 것으로 예상된다.

둘째, VPN과 데이터 센터에서 제공하는 서버 호스팅 혹은 하우징과 같은 서비스를 연계하거나, VPN과 ASP(Application Service Provider)를 조합한 서비스를 제공한다.

셋째, 향후 국제통신 수요가 IP기반의 서비스로 전환될 것으로 예상됨에 따라서, 타 글로벌 사업자와의 지속적인 제휴를 확대하여 국제회선 구축비용을 절감함과 동시에 국내외에 진출해 있는 기업들을 대상으로 국제 VPN 서비스를 제공함으로써 글로벌 사업자로서의 위상을 갖출 필요가 있다고 본다.

넷째로 향후 막대한 기업 음성 시장을 확보하기 위해서 VPN과 VoIP 망과의 연동을 통한 Voice over IP-based VPN 등의 서비스 개발이 필요하다. 특히, 지연에 가장 민감한 음성통화 품질을 확보하기 위해서 QoS 보장과 서비스 품질 보증(SLA; Service Level Agreement)의 도입이 요구된다.

5. 결론

VPN은 최근에 네트워킹분야에 있어서 가장 중요한 핵심 이슈 중의 하나이며, 향후 전체 기업 네트워킹의 가장 중요한 분야가 될 것으로 예상된다. 앞선 사례 분석에서 알 수 있는 것과 같이, 통신사업자의 망 구축 방안과 서비스 제공 전략은 바로 고객의 서비스 선택 포인트가 된다는 것을 알 수 있다.

VPN 서비스를 제공하는 통신사업자들은 고속 패킷 전달과 QoS가 보장되는 망 구성 전략과 아울러 기업들이 VPN서비스에 대해 갖고 있는 부정적인 인식을 변화시킬 수 있는 다양한 서비스 제공 방안 연구와 적극적인 홍보가 필요하다. 또한, VPN 서비스를 단순히 고도의 보안성과 신뢰성이 요구되는 기존 전용회선 등에 대한 경쟁 서비스가 아닌, 기업 업무 전체의 효율성을 높이고 비용을 절감할 수 있는 인트라넷 혹은 익스트라넷 등의 구축 모델로 지향해 나가야 할 것이다.

참고문헌

[1] "가상사설망 기술 및 표준화 동향", 지식정보센터 주간기술동향 통권958호, 2000. 8.

[2] K. Hamzeh, et al., "Point-to-Point Tunneling Protocol(PPTP)", IETF, RFC 2637, July 1999.

[3] W. Townsley, et al., "Layer Two Tunneling Protocol(L2TP)", IETF, RFC 2661, August 1999.

[4] Black, Uyles D., "*Internet security protocols: protecting IP traffic*", Prentice Hall PTR, 2000.

[5] "IP VPN service: a demand-side view", IDC, 2000. 12.

[6] "Secure managed IP VPNs: End-User Requirements and Service-Provider Opportunities", IDC Bulletin, 2000. 10.

[7] "통신업계동향", 하나로통신, 2001. 8.

[8] "사업자의 전략을 반영하는 IP-VPN 서비스", Nikkei Communications, 2000. 10.