主題

인터넷 VPN 서비스 기술 동향

한국통신 통신망연구소 이경근, 오채형, 김이한

차 례

I. 서 론

인터넷의 급격한 성장은 관련업계에 많은 변화를 주었다. 기업은 사업 영역의 글로벌화로 무한 경쟁의 시대를 맞게 되었으며, 기존 ISP(Internet Service Provider)는 신생 ISP들의 등장으로 인해 인터넷 접속서비스에 대한 가격 우위를 상실하게 되었다. 따라서 기업들은 사업영역의 전문화 함께 네트워크 운용에 대한 비용 절감이 요구되었으며, ISP들은 인터넷에서 신규 수익을 창출해야 하는 상황이 되었다.

오늘날 기업들은 네트워크에 대한 비용절감을 위하여 기존의 전용선이나 가상회선을 이용한 WAN 접속을 저렴한 비용으로 사업 영역을 전세계로 확장할 수 있는 인터넷을 이용하려 하고 있다. 그러나 인터넷의 개방형 특성은 신뢰적인 데이터 전송을 보장할 수 없기 때문에 기업들은 데이터의 보안과 전송로 대역을 보장받을 수 있는 서비스를 요구하였으며, ISP들도 단순 인터넷 접속서비스 이상의 고부가 서비스의 개발이 필요하게 되었다. 이러한 다양한 요구조건을 수용할 수 있는 기술로서 주목받고 있는 것이 인터넷을 이용한 가상사설망(이하 VPN)이다.

VPN(Virtual Private Network)은 공중망을 이용하여 사설망의 기능을 제공하는 가상의 사설 네트워크이다. 따라서 인터넷 VPN이란 IP 프로토콜로 구성되어 있는 공중 데이터망인 인터넷을 통해 사설망의 기능을 제공하는 것을 의미한다. 비연결형 네트워크인 인터넷 상에서 전달되는 정보의 프라이버시를 보장해 주기 위하여 인터넷 VPN은 보안 기능을 필수적으로 갖추어야 한다. 또한 인터넷 VPN은 새롭게 등장하고 있는 VoIP(Voice over IP), 영상회의 등 실시간성을 필요로 하는 인터넷 응용서비스를 지원하기 위해 QoS(Quality of Service)

도 제공되어야 한다.

현재 인터넷 VPN은 시장 형성 단계에 있지만, 무한한 잠재력을 갖추고 있어 표준화 단체, 개발업체 및 ISP들이 서비스 확대을 위해 많은 노력을 기울이고 있다. 물론 인터넷 VPN 서비스가 성공하기 위해서는 무엇보다 서비스 이용자와 제공자가 희망하는 수준의 기술이 제시되어야 한다.

본 고에서는 인터넷 VPN 서비스의 동향을 살펴보고, VPN 서비스를 제공하는데 필요한 다양한 요소 기술을 정리한 뒤, VPN 서비스의 사용자와 제공자들이 고려하여야 할 부분을 기술한다.

II. VPN 추진 동향

인터넷을 통해 VPN 서비스를 제공하기 위한 노력은 다양하게 전개되고 있다. 본 장에서는 인터넷 VPN 기술에 대한 표준화 동향과 최근 국내외 ISP의 VPN 서비스 동향 그리고 VPN 솔루션을 내놓고 있는 개발업체의 동향을 알아본다.

1. 표준화 동향

인터넷 VPN 기술에 대한 표준화는 IETF에서 주도적으로 수행하고 있다. IETF는 IP 백본망에서 VPN을 구현하는 방법을 제시하고는 있지만 특별히 하위 링크계층을 이용한 VPN 구성에 대해서는 언급하고 있지 않다.

IETF는 인터넷 초안(draft)을 통해 VPN 응용서비스와 구현에 있어 다음의 요구사항을 제시하고 있다.

- VPN에서 전달되는 트래픽(IP 주소 및 프로토콜)은 IP 백본망의 트래픽과 무관해야 한다.
- 어떤 형태로든 데이터에 대한 보안은 제공되어야 한다.
- QoS에 대한 신뢰성이 지원되어야 한다.

이 요구사항을 기반으로 하여 IETF는 VPN 서비스를 다음 4가지 모델로 제시하고 있다.

- VLL(Virtual Leased Lines) : IP터널을 이용하여 VPN양단을 전용선으로 연결하는 방식
- VPRN(Virtual Private Routed Networks) : ISP 라우터 사이에 그물 형태의 IP터널을 구성하는 방식
- VPDN(Virtual Private Dial Networks) : 원격사용자가 ISP의 NAS를 이용하여 기업 VPN 서버와 터널을 형성하는 방식
- VPLS(Virtual Private LAN Segment) :IP상에서 LAN 세그먼트를 에뮬레이션 하는 방식

IETF는 위의 서비스 모델 중 일부는 특정 VPN 서비스를 제공하기 위해 함께 하고, 기반 기술도 공통으로 적용될 것으로 보고 있다.

2. 서비스 동향

현재 인터넷 VPN 서비스는 초보 단계에 있지만 국내외 ISP들은 향후 다양한 인터넷 응용서비스를 제공하는데 있어 매우 중요한 역할을 할 것으로 보고 있다. 따라서 대부분의 ISP들은 VPN 서비스를 제공하거나, 제공하기 위해 준비중에 있다.

국내 ISP는 주로 원격접속 VPN을 위주로 하고 있는 반면 국외 ISP는 원격접속과 LAN-to-LAN VPN 모두를 제공하고 있다. 특히 미국의 ISP들은 IP 백본망을 F/R(Frame Relay)나 ATM망을 사용함으로써 고객과의 SLA(Service Level Agreement) 계약을 통해 QoS를 강화한 VPN서비스를 제공하고 있다.

〈표 1〉과 〈표 2〉는 국내외 대표적인 ISP들의 VPN 서비스 제공 현황을 보여주고 있다.

	아이네트	데이콤	SK 텔레콤
서비스 명칭	아이네트 보안 VPN	천리안 가상사설망	네츠고 가상사설망
제공 서비스	원격접속 LAN-to-LAN	원격접속(01421)	원격접속(01442)
방 식	IPSec	L2TP	PPTP
솔루션	VPNet 전용장비	Cisco NAS 및 라우터	MS Windows NT
적용 업체	제일제당, 두산 등	데코, 이랜드 등	대교 등
특 징	암호화 데이터의 압축 기능 제공	접속 사용자 수에 따른 요금 체계 차별화	MCIS 기반 보안 기능 수행

표 1. 국내 ISP의 VPN 서비스 제공 현황

	AT&T	MCI	GTE
서비스 명칭	WorldNet VPNS	InternetMCI VPN	Site Patrol International
제공 서비스	원격접속 LAN-to-LAN	원격접속 LAN-to-LAN	원격접속
방 식	PPTP, L2TP, IPSec	IPSec	IPSec
솔루션	방화벽	방화벽	방화벽
특 징	NDS 서비스 NAT, 패킷 필터링 제공	글로벌 디렉토리 One-time 패스워드 인증	보안 모니터링 제공

표 2. 미국 ISP의 VPN 서비스 제공 현황

3. 개발업체 동향

대부분의 VPN 솔루션 개발업체는 기업을 대상으로 제품을 출시하고 있다. 현재 VPN 솔루션은 〈표 3〉과 같이 하드웨어, 방화벽 그리고 소프트웨어 형태로 구분되며 대부분 원격접속 VPN과 LAN-to-LAN VPN을 지원한다.

표에서 보는 바와 같이 개발업체에서 제공하는

	하드웨어	방화벽	소프트웨어
보안성	좋음	중간	떨어짐
성 능	높음	중간	낮음
유연성	떨어짐	중간	좋음
관 리	떨어짐	중간	좋음
특 징	라우터에 보안기능의 하드웨어 칩화	방화벽에 VPN 보안기능 부가	OS 제공업체의 VPN 기능의 S/W 부가
제공업체	VPNet, Cisco 등	Checkpoint, TimeStep 등	Microsoft, Novell 등

표 3. VPN 솔루션별 기능 및 특징

VPN 솔루션은 다양하며 나름대로 장단점을 갖고 있다. 따라서 VPN을 구현하고자 하는 ISP나 기업은 사전에 자신의 네트워크를 고려한 적합한 솔루션을 선택해야 한다. 기존의 네트워크가 라우터를 기반으로 구성되어 있는 경우에는 하드웨어 솔루션이, 이미 방화벽을 통해 기본적인 보안 기능을 갖추고 있는 경우에는 방화벽 솔루션이, 그리고 서버를 기반으로 하여 네트워크가 구성되어 있으면 소프트웨어 솔루션이 적합할 것이다.

III. 인터넷 VPN 종류

VPN 서비스는 크게 원격접속(Remote Access) VPN과 LAN-to-LAN VPN으로 구분할 수 있다.

원격접속 VPN은 원격근무자나 현장근로자와 같은 이동사용자에게 위치에 상관없이 기업내 접속을 제공한다. 원격접속 VPN은 터널의 형태에 따라 사용자 기반 VPN과 네트워크 기반 VPN으로 나눌 수 있다.

LAN-to-LAN VPN은 서로 떨어져 있는 2개의 사이트간에 VPN 접속을 제공한다. LAN-to-LAN VPN에서도 기업 혹은 ISP의 종단(edge) 장치에서만 VPN 기능을 제공하는 종단장치 기반 VPN과 ISP의 네트워크에 존재하는 네트워크 장치 모두가 VPN 기능을 제공하는 네트워크 기반 VPN으로 구분할 수 있다. 다음 〈표 4〉 및 〈표 5〉와 (그림 1)은 각 VPN 서비스별로 특징과 구현 형태를 나타낸 것이다.

IV. 인터넷 VPN 구현 기술

경로 결정을 인접 노드간의 경로 계산에 의한 hop-by-hop 형태로 수행되는 비연결형 네트워크

	사용자 기반	네트워크 기반
터널 프로토콜	PPTP, IPSec	L2TP, L2F
터널 초기화	사용자 단말	ISP의 NAS
사용자 인증	기업 인증서버	ISP 혹은 기업 인증서버
관 리	기업	ISP
특 징	단-대-단 보안 제공 ISP와 무관하게 구축 가능	단일 ISP로 제한 프리미엄 서비스 제공 가능

표 4. 원격접속 VPN 서비스별 특징

	종단장치 기반	네트워크 기반
VPN 구성 요소	망 종단장치	ISP의 모든 네트워크 장치
터널 프로토콜	IPSec	MPLS
특 징	VPN 구성 간단 ISP와 무관하게 구축 가능	SLA 및 QoS 제공 가능

표 5. LAN-to-LAN VPN 서비스별 특징

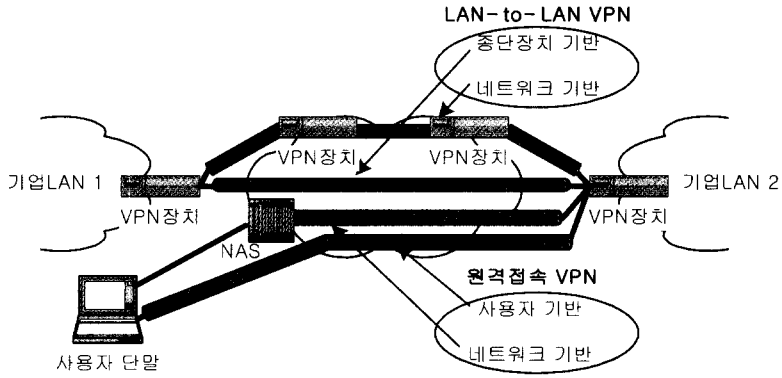


그림 1. 인터넷 VPN 서비스별 구현 형태

인 인터넷에서 가상의 연결형 네트워크를 제공하는 인터넷 VPN은 전달 데이터에 대해 프라이버시를 제공한다. 여기에 부가적으로 QoS를 제공함으로써 다양한 인터넷 응용서비스의 제공도 가능하다. 본 장에서는 인터넷 VPN 구현에 사용되는 다양한 보안 기술과 IP 백본망에 적용 가능한 QoS 기술을 알아본다.

1. 보안 기술

인터넷에서 데이터 프라이버시를 제공하는 보안 기술은 (그림 2)와 같이 TCP/IP 계층 별로 각기 다른 기술이 적용된다. 그러나 인터넷에서의 VPN은 개방형 네트워크의 기준이 되는 네트워크 계층, 즉 IP 계층 이하의 기술을 통해 구현된다. 여기에는 기본적으로 터널링이 필요하며 부가적으로 인증과 암호화가 함께 한다. 또한 기존 방화벽 솔루션에서 제공하는 NAT(Network Address Translation)와 패킷 필터링이 선택적으로 이용될 수 있다.

가. 터널링

비연결형 네트워크인 인터넷에서 가상의 연결형 서비스를 제공하는 터널링은 송신단과 수신단의 게이트웨이 사이에 미리 약속한 터널링 프로토콜을 사용하여 목적지를 향하는 패킷 정보를 공중 IP패킷

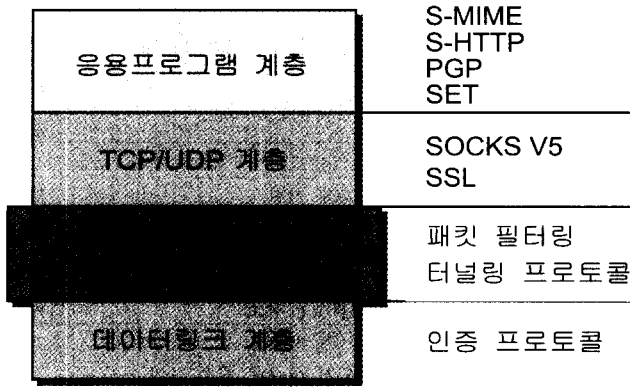


그림 2. TCP/IP 계층별 보안 기술

안으로 캡슐화하는 기능을 수행한다. 터널링 프로토콜은 캡슐화되는 패킷에 따라 2계층과 3계층으로 구분된다. 〈표 6〉은 각 계층별로 일반적으로 사용되는 프로토콜에 대한 특성을 나타내고 있다.

표에서 보는 바와 같이 3계층 터널 프로토콜인 IPSec[1]은 자체 보안 기능을 내장하고 있어 IP 네트워크 환경에서는 가장 훌륭한 솔루션이 된다. 반면 다중 네트워크 환경을 지원하고자 할 경우에는 2계층 터널 프로토콜인 PPTP[2]나 L2TP[3]를 사용하는 것이 적합하나 데이터에 대한 보안 기능을 제공하기 위해 추가적인 조치가 필요하다.

나. 인 증

인증은 송신자의 신원 확인을 통해 VPN 네트워크로의 접속을 허용하는 과정이다. 대부분 별도의 인증서버를 통해 인증 과정을 수행하며, 사용자 접속 허용과 함께 접근 제어와 계정 관리도 포함된다.

원격접속 VPN은 주로 단순 접속 허용 기능만을 수행하는 PAP(Password Authentication Protocol)과 CHAP(Challenge Handshake Authentication Protocol)을 기본으로 하고 접근 제어 및 계정 관리 기능을 갖고 있는 TACACS(Terminal Access Controller Access-Control System)와 RADIUS (Remote Authentication Dial-In User Service)[4]를 사용한다. 원격접속 VPN에서는 대부분 RADIUS 인증 방식을 사용한다. RADIUS는 인증 정보를 데이터베이스 형태로 관리하며 사용자 인증 이외에도 사용자 연결 관리를 위해 ISP의 NAS(Network Access Server)와 연동하여 인증 시스템을 구성함으로써 사용자 확장에 유리하다. 또한 RADIUS는 자체적으로 Proxy 기능을 갖고 있어 타 RADIUS서버에 대해 클라이언트 역할을 수행할 수 있어 매우 유연한 인증 방법을 제공한다.

LAN-to-LAN VPN에서는 사용자 접속 인증보다 원격의 LAN 사이트에서 송신한 데이터 패킷에 대한 인증을 수행한다. 전달되는 패킷은 사전에 암호화 키와 암호화 알고리즘을 통해 암호화된다. 따라서 수신단에서는 암호화된 패킷의 해석을 위해 암

	2 계층		3 계층
모드	클라이언트-서버		호스트-호스트
프로토콜	PPTP	L2TP	IPSec
캡슐화	IP, IPX, AppleTalk 등	IP, IPX, AppleTalk 등	IP
VPN 서비스	원격접속 VPN	원격접속 VPN	원격접속 VPN LAN-to-LAN VPN
보안 사용자 인증 패킷 인증 패킷 암호화 키 관리	 자체 지원 제공 안됨 특정 솔루션 이용 제공 안됨	 자체 지원 IPSec 참조 IPSec 참조 IPSec 참조	 자체 지원 AH 헤더 ESP 헤더 IKE, SKIP
터널 프로토콜 특징	PPP 이용 동시 인터넷 접속 불가	PPP 이용 동시 인터넷 접속 불가	동시 인터넷 접속 가능

표 6. 계층별 프로토콜 특성

호화 키에 대한 인증을 수행하여야 한다. 현재 IPSec은 데이터 암호화에 사용되는 암호화 키의 신뢰성 보장을 위해 인증서(Certificates)를 사용한다. 이 인증서는 암호화 키의 소유자 이름을 포함하고 있어 이를 통해 인증된다. 인증서 포맷과 발행 및 사용 방법에 대한 규정은 ITU에서 X.509[5]로 표준화함으로써 이를 기반으로 하는 VPN 시스템은 상호연동이 가능하다.

다. 암호화

터널링을 통해 전달되는 패킷에 대해 좀 더 신뢰적인 보안 기능을 제공하기 위해 암호화 기능을 사용한다. 암호화 방식에는 비밀키 암호화 방식과 공개키 암호화 방식이 있다. 현재 VPN 구현에는 좀 더 안전한 방식인 공개키 암호화 방식을 사용한다. 공개키 암호화 방식은 비밀키 하나 만을 사용하여 암호화하는 비밀키 암호화 방식과는 달리 2개의 암호화 키를 조합하여 데이터를 암호화하는 방식이다. 공개키 암호화 방식에는 Diffie-Hellman 방식과 RSA 방식이 있다.

IP네트워크에서 터널링에 대한 국제 표준인 IPSec에서는 AH 헤더와 ESP 헤더 각각에 대해 암호화 방식을 규정하고 있다. AH헤더는 128-bit 암호화 키를 갖는 MD5 혹은 160-bit 암호화 키를 갖는 SHA-1과 연결되는 HMAC(Hash-based Message Authentication Code) 암호화 알고리즘을 요구한다. 그리고 ESP헤더는 56-bit DES(Data Encryption Standard) 암호화 키를 갖는 DES-CBC(Cipher Block Chaining)를 기본으로 요구한다.

암호화 방식은 VPN 서비스의 상용화 여부를 좌우할 수 있다. 전세계 많은 국가들이 국내 정보 보호를 목적으로 자국의 보안 소프트웨어를 사용토록 지정함으로써 인터넷을 통한 글로벌 VPN 구축을 어렵게 하고 있다. 또한 미국에서는 128-bit 암호화 키 방식을 북미를 제외한 해외로의 수출을 금지하고 있는 실정이다.

2. QoS 기술

인터넷 VPN 사용자를 대상으로 QoS 제공이 가능하기 위해서는 먼저 IP 네트워크에서의 QoS가 이루어져야 한다. 즉 단-대-단으로 사용자 트래픽에 대해 QoS를 보장하여야 한다.

본 절에서는 현재 IETF에서 활발하게 논의되고 있는 IP QoS 구조인 RSVP[6], Differentiates Service(이하 Diff-Serv)[7] 및 MPLS[8]에 대해 살펴본다.

가. RSVP

RSVP 프로토콜에서는 수신자와 송신자간에 단-대-단 시그널링을 이용하여 플로워에 대해 경로상에 있는 모든 라우터에서 자원이 예약된다. RSVP는 실시간 서비스와 최선형 서비스를 갖는 다자간 통신을 위한 새로운 인터넷 구조의 한 부분으로 미리 규정된 서비스를 지원할 수 있도록 송신측, 수신측 그리고 라우터간에 정보를 교환하는 프로토콜이다. RSVP는 PATH와 RESV 2개의 메시지를 통해 경로상의 라우터 및 송수신 호스트 사이에 대역폭이 결정된다.

현재 RSVP는 여러 ISP들이 함께 운용하는 대규모 멀티밴더 네트워크에서는 구현이 어렵거나 불가능하다. 즉, 네트워크에서 RSVP를 제대로 구현하기 위해서는 모든 라우터가 RSVP를 지원하지 않고서는 불가능하기 때문이다. 따라서 전체 네트워크보다 지역 네트워크를 구성하는 네트워크 장비에 탑재되어 WAN으로의 대역폭 요청에 사용하는 방향으로 진행되고 있다.

나. Diff-Serv

RSVP의 단기간 내의 구현 불가능에 따라 대안으로 Diff-Serv가 주목을 받고 있다. Diff-Serv는

상대적으로 우선 순위가 높은 패킷을 명시하여 다른 패킷에 비해 더 나은 서비스를 받게 하는 것이다. 이를 위한 방법으로 IP 패킷에 서비스 차등을 위한 우선순위 비트를 두어 네트워크 내의 라우터에서 이를 보고 패킷을 전달할 때 차별화하여 처리하는 개념이다. IP패킷의 TOS(Type of Service)를 위한 8-bit 중 PHB(Per-Hop Behavior)를 위해 6-bit만을 사용한다. PHB에 대한 실제 알고리즘이나 메커니즘은 라우터 개발업체에 따라 달리 구현되며 다양한 방식을 사용할 수 있다. 이 중에서 현재 2개의 비트를 사용하는 Diff-Serv 서비스로 보장형 서비스와 프리미엄 서비스가 있다.

보장형 서비스는 고객과 ISP사이에 SLA (Service Level Agreement) 계약을 맺음으로써 ISP는 고객에게 계약된 만큼의 할당 대역폭을 제공하는 서비스이다. 프리미엄 서비스는 고정된 PBR(Peak Bit Rate) 트래픽을 생성하는 고객과의 SLA 계약을 통해 낮은 지연과 지연 변이를 제공하는 서비스이다.

Diff-Serv 구조는 RSVP보다 시그널링을 최소화하고 각 노드에서 플로워 별 상태를 유지할 필요가 없어 훨씬 확장성이 좋다. 따라서 인터넷 백본망에서 구현 가능한 방법으로 떠오르고 있다.

다. MPLS

기존 라우터가 하나의 패킷을 처리하려면 먼저 패킷 헤더를 읽어 각 필드를 검사한 다음 패킷을 처리한다. 따라서 라우터의 처리 기능인 라우팅과 포워딩이 각 패킷 단위로 처리됨으로써 많은 시간이 요구된다. 이러한 오버헤드를 줄이기 위해 도입된 방식이 MPLS이다.

MPLS는 기존의 라우팅에서 사용하는 longest prefix match방식 대신 short label exact match 방식을 사용함으로써 고속의 포워딩 기술을 제공한다. 기존에는 매 Hop마다 패킷에 대한 포워딩 결정을 헤더의 내용과 라우팅 알고리즘에 기반을 두었지만 MPLS에서는 패킷이 망에 들어 올 때 한 번만 수행한다.

MPLS는 2계층 스위칭 기능과 3계층 라우팅 기능을 통합한 레이블 스위칭 방식으로 가입자망의 LSR(Label Switched Router)에서 목적지 주소에 대응하는 라벨을 할당하여 IP패킷 전단에 붙여 코어 라우터에서는 이 라벨에 의한 스위칭만 일어나도록 한다. 이러한 방식은 가입자망의 라우터들은 여전히 어떤 LSP들을 사용할 것인가를 결정하기 위해 IP헤더를 분석하지만 목적지 주소에 대응된 라벨을 더함으로써 이웃하는 노드들은 단순히 라벨에 의한 경로 식별을 통해 패킷을 전송한다.

MPLS는 스위치에 의한 고속 IP 포워딩과 다양한 스위치에 적용이 가능하며 IP멀티캐스팅 지원이 가능하다. 그리고 MPLS는 서로 다른 서비스 특성을 갖는 라벨 스위칭 경로를 생성하게 함으로써 QoS를 지원한다.

특히 MPLS는 IP 패킷 전단에 라벨을 통해 전달되는 형태로 앞서 언급한 터널링의 기본 개념인 패킷 캡슐화 기능을 갖추고 있으며 또한 MPLS 라우터를 계층적으로 더함으로써 다계층 터널링을 구현할 수 있어 LAN-to-LAN VPN서비스를 제공할 수 있다.

V. 서비스 고려사항

인터넷 VPN이 유용한 서비스로 자리잡기 위해서는 일정 수준의 기능들을 갖추어야 한다. 본 장에서는 서비스 이용자 및 제공자 측면에서 고려해야 할 사항을 열거한다.

1. 서비스 이용자

기업은 인터넷 VPN 서비스를 통해 비용 절감과 함께 사업 영역의 확장을 위해 보안, 상호연동성 및 관리 등에 대한 기준을 제시하여야 한다.

보안은 서비스 이용에 있어 가장 핵심 되는 기능으로 기업은 내부 및 외부에서의 불법적인 접근을 감시하고 점검이 가능한 객관적인 보안 측정 수단이 필요하다.

상호연동성은 VPN 서비스의 확장을 위해 시스템이 갖추어야 할 기능으로 기업은 사업영역을 확장하기 위해 다수의 ISP와 다양한 시스템을 통해 서비스를 제공받고자 할 것이다. 따라서 기업은 서비스 도입에 앞서 VPN 시스템이 국제 표준에 따라 구현되었는지 확인해야 한다. 이를 통해 기업은 VPN 서비스의 확장과 함께 보안을 필요로 하는 다양한 인터넷 응용서비스를 효율적으로 수용할 수 있다.

기업은 VPN 서비스의 운용과 확장이 용이하도록 관리 기능 중의 일부를 자체적으로 수행해야 한다. 여기에는 사용자 계정 등록/변경/삭제, 보안정책 수정, LAN-to-LAN VPN 연결 생성 및 삭제, 네트워크 사용량 해석 및 장애 정보의 검색 등이 있으며 ISP와의 협의를 통해 관리 가능한 범위를 결정해야 한다.

2. 서비스 제공자

VPN 서비스를 통해 수익 창출을 기대하는 ISP는 기업이 자체적으로 구현한 VPN 서비스와 차별화할 수 있는 관리형 VPN 서비스를 제공해야 한다. ISP가 관리형 VPN 서비스를 제공하기 위해서는 기본 관리, 통합구성 관리 및 통신서비스의 질 등에 대한 기준이 마련되어야 한다.

기본 관리 기능은 VPN 서비스 관리에 필요한 전반적인 기능으로 사용자 계정관리, 도움말, 원격접속 관리, 과금 정책, 사용량 검색 및 해석 등이 해당된다. 이 기능들은 기업에게 제공되어 관리 기능을 분담할 수 있다.

통합구성 관리 기능은 인터넷 및 인트라넷 자원을 효과적으로 통합 운용 관리하는 기능으로 ISP와 기업의 네트워크 시스템 사이의 원활한 통합이 요구된다. 통합에 있어 핵심되는 요소는 인증, 암호화 및 터널링을 포함하고 있는 보안 기술로, 특정 솔루션이 아닌 표준에 기반을 두어 글로벌하게 적용할 수 있어야 한다.

통신서비스의 질은 VPN 서비스의 성능 수준을 나타내는 것이다. 서비스의 질적 향상을 위해 ISP는 기업에게 SLA를 제공해야 하며, 향후에는 여러 ISP와 연동되는 글로벌 SLA도 고려하여야 한다. 또한 기업들의 다이얼-업, ISDN, xDSL 및 무선 등과 같은 다양한 가입자망을 통한 VPN 접속 요구를 수용할 수 있도록 ISP는 다중 접속 POP(Point of Presence)을 갖추어야 한다. 데이터 전달 속도를 보장하는 VPN을 제공하기 위해 ISP는 로컬 IP 망에서 QoS를 제공해야 하며, 향후 타 ISP와 연계한 VPN 서비스에서도 QoS를 제공할 수 있도록 표준에 기반을 둔 네트워크의 고도화가 이루어져야 한다.

VI. 결 론

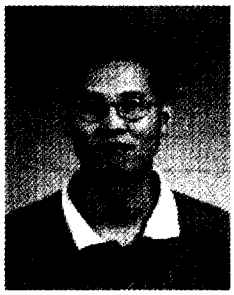
인터넷을 통한 통신비용 절감과 접속 영역의 확장에도 불구하고 기업은 신뢰적인 데이터의 전달을 요구하고 있으며, 단순 인터넷 접속 서비스만 제공하는 ISP들도 신규 수익 창출을 위해 새로운 부가서비스를 찾고 있다. 이러한 요구조건을 만족할 수 있는 기술로서 인터넷 VPN이 주목을 받고 있다.

인터넷 VPN은 개방형 특성을 갖고 있는 인터넷에 보안 기능을 부가한 것이다. 인터넷 VPN 서비스는 제공자의 구성 및 제공 방식에 따라 몇 가지 형태로 구분되며 이용자의 요구 조건과 수용 방법에 따라 적절하게 조합한 형태로 제공된다. 본 고에서는 먼저 인터넷 VPN과 관련하여 업계의 동향을 살펴보고 VPN 서비스 제공에 있어 필요한 요소 기술을 정리하며 사용자와 제공자의 관점에서 고려하여야 할 사항들을 고찰하였다.

인터넷 VPN은 단일의 표준화, 네트워크 성능 유지 및 인터넷 서비스 품질 보장 등 아직 많은 부분에 대하여 해결책이 제시되어야 한다. 그러나 이 분야의 연구는 활발히 진행되고 있으며, 따라서 향후 인터넷에서 다양한 응용서비스를 이용하는데 VPN이 기반 플랫폼으로 자리할 것이다.

※ 참고문헌

1. RFC 1825 Security Architecture for the Internet Protocol.
2. http://www.microsoft.com/NTServer/commserv/techdetails/prodarch/understanding_pptp.asp.
3. Internet draft, Layer Two Tunneling Protocol, draft-ietf-pptpext-l2tp-10.txt
4. RFC 2138, Remote Authentication Dial-In User Service.
5. RFC2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
6. RFC2205, Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification.
7. Internet draft, Differentiated Services Operational Model and Definitions.
8. Internet draft, A Framework for Multiprotocol Label Switching.



이 경 근

1991년 경북대학교 전자공학과 학사
1993년 경북대학교 전자공학과 석사
1993년~현재 한국통신 통신망연구소 인터넷플랫폼연구실 전임연구원
※관심분야 : 인터넷 기술

오 채 형

1993년 전북대학교 전자공학과 학사
1995년 전북대학교 전자공학과 석사
1995년~현재 한국통신 통신망연구소 인터넷플랫폼연구실 전임연구원
※관심분야 : 인터넷 기술 및 네트워크 설계

김 이 한

1988년 충남대학교 전자공학과 학사
1990년 한국과학기술원 전기 및 전자공학과 석사
1995년 한국과학기술원 전기 및 전자공학과 박사
1995년~현재 한국통신 통신망연구소 인터넷플랫폼연구실 선임연구원
※관심분야 : 차세대 인터넷 기술, 네트워크 서비스