비용 절감, 신뢰성 확보 통해 영역 넓히는 VPN

1990년대 중반 처음 등장한 VPN은 기존의 전용회선을 공중망을 통한 암호화 터널을 통해 대체한다는 개념으로 비용 절감 효과를 커다란 장점으로 내세우며 시장에서 성장해 왔다. 초기에는 업체들마다 개별적인 기술을 통해 VPN을 구현했지만, 이제는 IPSec이나 SSL과 같은 표준화된 기술을 통해 급격한 보급을 이뤘으며, 이를 통해 점차 새로운 활용처를 찾아 나가고 있다.

박광청
kcpark@itbay.co.kr
아이티베이 정보보안컨설팅 팀장

연재순서

1. 보안기술 개요와 시큐리티 방법론(2007년 01월호)
2. 파이어월의 기술 개요와 향후 진화 방향(2007년 02월호)
3. **VPN(2007년 03월호)**
4. IDS(2007년 04월호)
5. IPS(2007년 05월호)
6. 바이러스월(2007년 06월호)
7. 웹 애플리케이션 파이어월(2007년 07월호)
8. 안티스팸, 안티스파이웨어(2007년 08월호)
9. UTM(2007년 09월호)
10. 엔드포인트 보안 방법론(2007년 10월호)

전 세계적으로 인터넷과 네트워크 인프라가 급성장하면서 각 기업체나 조직의 비즈니스 영역도 오프라인에서 온라인 환경으로 급속히 이전하고 있다. 이는 곧 수많은 전산 자원의 도입과 이들 간의 물리적 혹은 논리적 네트워크 연결을 필요로 한다는 것을 의미한다.

이같은 환경 변화에서 본사와 지사 간, 해외와 국내 간의 연결시 필연적으로 발생하는 비용 문제와 보안 문제를 동시에 해결할 수 있는 솔루션이 VPN(Virtual Private Network) 기술이며, 1990년대 중반 처음 기본 개념이 소개된 이후 뛰어난 비용절감 효과와 보안 신뢰성을 무기로 꾸준히 영역을 넓혀나가고 있다.

VPN의 주요 장점과 특징

VPN은 '인터넷과 같은 공중망(Public Network)을 이용해 사설 전용망(Private Network)의 효과를 얻는 기술로, 이를 구현하기 위한 하드웨어와 소프트웨어의 집합체'로 정의할 수 있으며, 암호화 기술, 인증 기술 그리고 터널링 프로토콜로 구성돼 있다.

VPN은 현재 일반화된 네트워크 기술로 인식되고 있지만, 그 개념과 역사는 짧지 않다. 과거에는 각 솔루션 업체별로 독자적인 기술을 채택함으로 인해 표준화가 진행되지 않았고, 무엇보다 VPN 기술의 안정성과 성능이 충분히 검증되지 않아 그리 활발하게 도입되지 않았다.

그러나 2000년대 초반 VPN 기술이 IPSec(IP Security) 프로토콜로 표준화되고, 크고 작은 사이트에 도입되기 시작하면서 안정성과 신뢰성이 검증되고, 이에 따라 주목받기 시작했다. VPN의 장점과 주요 특징을 정리하면 다음과 같다.

- 비용 절감

VPN은 낮은 비용으로 고비용의 전용회선을 대체함으로써 비용 절감 효과가 탁월하다. 예를 들어 서울과 뉴욕을 전용회선으로 연결할 때 지불되는 월 수천만 원의 고정 비용이 인터넷에 기반한 VPN 기술을 적용함으로써 수백만 원에서 수십만 원 수준으로 대폭 절감될 수 있다.

- 보안 신뢰성

VPN은 표준기술로 개방적인 인터넷 하부 구조와 검증된 암호화와 인증 프로토콜을 이용해, 전송되는 모든 데이터를 암호화해 처리하므로 기업이나 조직에서 요구하는 강력한 보안 요구사항을 만족시킬 수 있다.

- 뛰어난 유연성

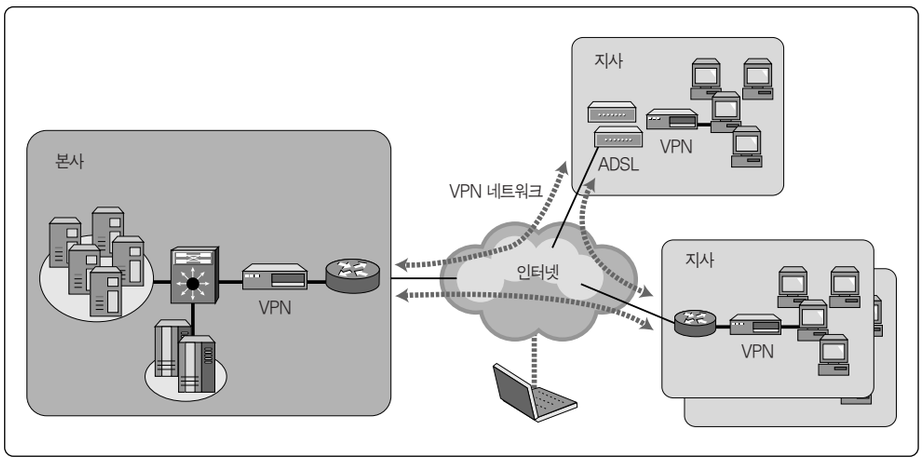
기업 비즈니스 영역의 확장에 따라 파트너나 고객과의 상호 접속 요구도 지속적으로 증가하고 있다. VPN은 기업 네트워크가 인트라

넷, 익스트라넷으로 확장시에도 유연하게 적용할 수 있으며, 특히 재택근무자나 파견근무자, 무선 단말을 이용하는 모바일 접속 요구도 수용할 수 있다.

• 뛰어난 상호 운용성

VPN은 파이어월이나 IDS, IPS 등과 같은 다른 보안 장비와도 상호 운영성이 뛰어나며, 이같은 솔루션과 통합을 통해 보다 한단계 높은 수준의 보안 시스템을 구축할 수 있다는 것이 장점이다.

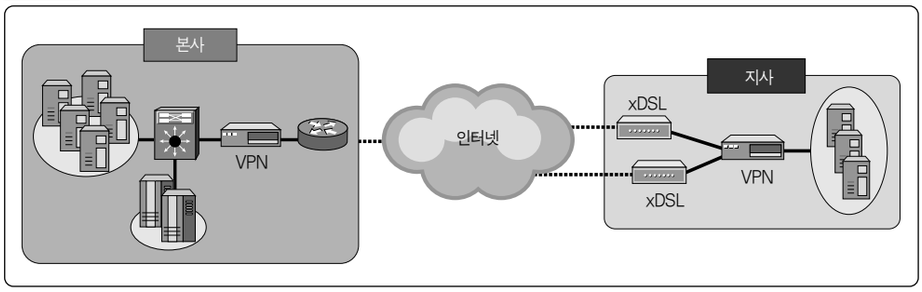
그림 1 VPN 개요



VPN 기술의 분류

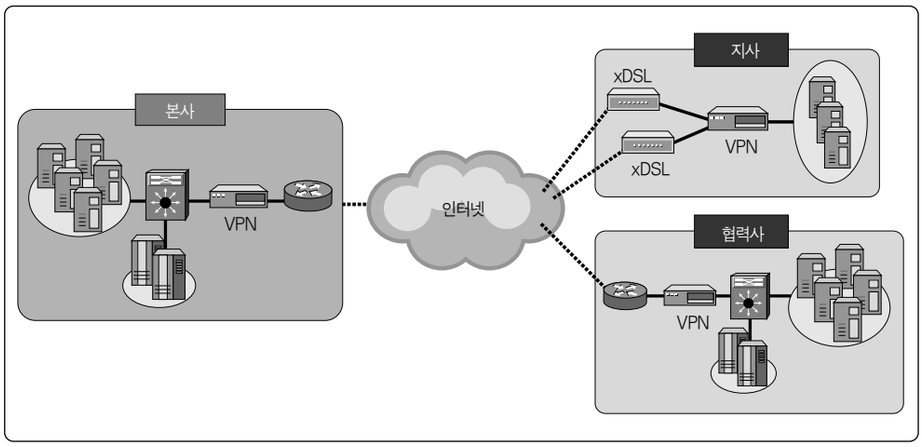
VPN은 적용 방식에 따라 기존 장비에서 추가로 VPN 기능을 구현하는 방식과 전용 장비를 이용하는 방식, 그리고 별도의 관리 서비스(Managed Service)를 이용하는 방식이 있다. 최근에는 성능과 안정성, 관리 편의성을 위해 VPN 전용 장비를 이용하는 방식이 많이 선호되고 있다.

그림 2 인트라넷 VPN



오늘날 VPN 구성 방식은 크게 포인트 투 포인트 VPN과 포인트 투 멀티포인트 VPN으로 분류되며, 접속 방식과 구현 범위에 따라 인트라넷 VPN, 익스트라넷 VPN, 원격 VPN, SSL VPN 등으로 구분할 수 있다. 하지만 실제 업무 환경에서는 여러 가지 방식을 혼합해 사용하는 경우가 일반적이다.

그림 3 익스트라넷 VPN



• 인트라넷 VPN

인트라넷 VPN은 본사와 지사나 지점과 지점 네트워크의 연결에 VPN을 적용한 것이다. 이는 원격지 접속(Site-to-Site) VPN 형태이며, 전사적으로 일관된 보안 정책을 적용할 수 있다는 것이 장점이다.

• 익스트라넷 VPN

익스트라넷 VPN은 본사와 협력업체 혹은 기업과 고객간의 네트워크 연결에 VPN을 적용한 것으로, 비즈니스 영역 확대나 기업간 인수/합병(M&A) 등으로 인해 최근 많이 도입되고 있는 VPN 구성 방식이다.

익스트라넷 VPN은 서로 다른 조직간의 신뢰(Trust)를 기반으로 이루어지므로 특히 보안정책 및 설정상 오류로 인한 위협 등에 주의

그림 4 원격접속 VPN

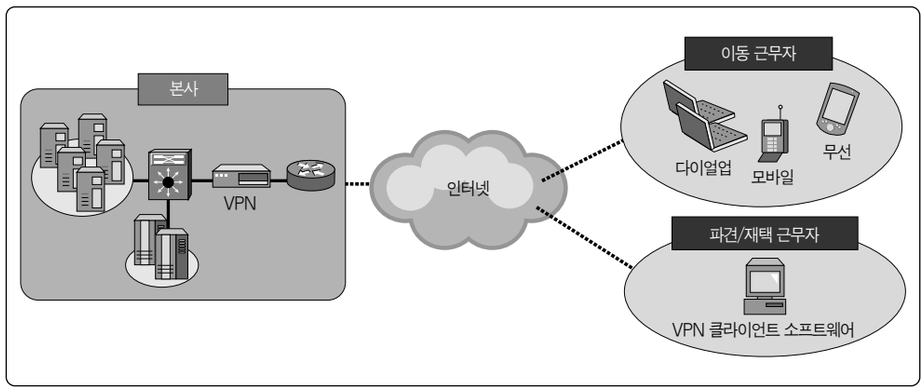


그림 5 SSL VPN

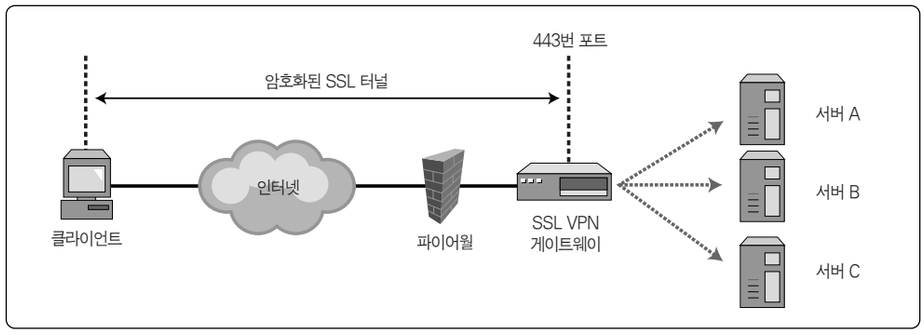


그림 6 VPN 터널링

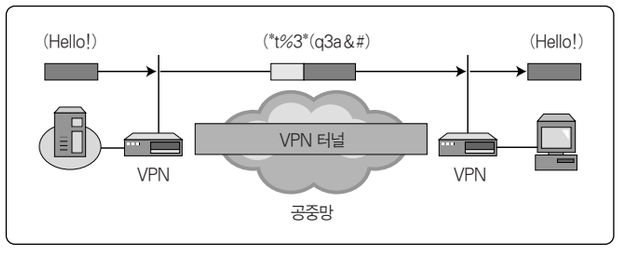
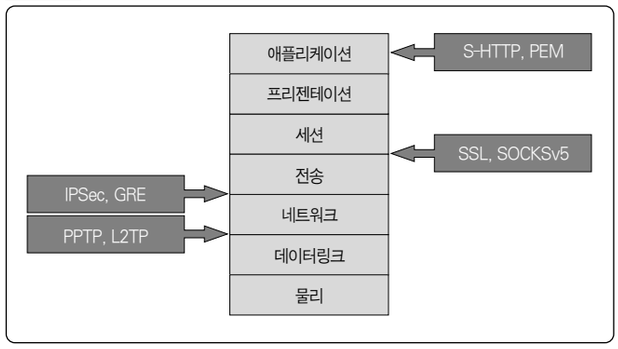


그림 7 OSI 7계층별 터널링 기술



를 요하며, 이기종 솔루션간 VPN을 구성하는 경우가 많으므로 실제 도입에 앞서 장비간 호환성과 운영상 이슈 사항에 대한 사전 검증이 필요하다.

• 원격접속 VPN

원격접속 VPN(Remote VPN)은 본사와 원격지 사용자간의 네트워크 연결에 VPN을 적용한 것으로 사용자들은 주로 암호화 처리 기능을 가진 전용 VPN 소프트웨어를 이용해 본사 네트워크에 접속한다.

원격접속 VPN 구성에서는 보안뿐 아니라 사용자 편의성도 중요시되는데, 관리 측면에서는 사용자 정보나 접속 관리, 그리고 효율적인 소프트웨어 배포와 교육 방안도 주요 검토 사항이 된다. 최근에는 이같은 원격접속 VPN의 번거로움을 대체할 수 있는 솔루션으로 일반 웹 브라우저를 통해 VPN 연결 기능을 제공할 수 있도록 SSL(Secure Socket Layer) 기술을 응용한 SSL VPN이 주목 받고 있다.

• SSL VPN

SSL은 웹 서버와 웹 브라우저간의 신뢰성 있는 통신을 보장하기 위해 1993년 넷스케이프에 의해 제안된 보안 프로토콜이다. 인터넷 프로토콜의 TCP 계층과 애플리케이션 계층 사이에서 동작하며, 현재 대부분의 웹 브라우저에서 기본적으로 지원된다.

SSL VPN은 이같은 SSL의 암호화/복호화 프로세스를 응용해 VPN에 적용한 것으로, 별도의 복잡한 절차 없이 웹 브라우저만으로 VPN을 구현할 수 있어 뛰어난 사용자 편의성과 관리 편의성을 보장할 수 있는 클라이언트리스 VPN(Clientless VPN) 솔루션이다. SSL VPN은 특히 최근 키워드가 되고 있는 유비쿼터스(Ubiquitous) 네트워크 기술과의 연계성 측면에서도 주목받고 있다.

SSL VPN은 웹 브라우저만으로 VPN 접속이 가능하기 때문에 클라이언트 운용환경과 무관하며, 별도의 VPN 소프트웨어 배포/설치가 필요없다는 장점 때문에 향후 원격접속 VPN을 대체할 것으로 전망되고 있다. 하지만 SSL의 특성 때문에 4계층에서 암호화/복호화를 수행하므로 지원할 수 있는 애플리케이션이 제한된다는 단점이 있다.

전체적으로 SSL VPN은 IPSec VPN과 동작방식이나 운영면에서 유사한 측면이 있다. 두 기술은 상호 배타적이라기보다는 보완적인 솔루션으로 고유영역을 지키면서 성장해 나갈 것으로 보인다.

표 1 주요 VPN 기술 비교

구분	PPTP	L2TP	IPSec	SOCKS V5
표준화 여부	마이크로소프트	RFC 2661	RFC 2401~2412	RFC 1928, 1929, 1961
제공 계층	2계층	2계층	3계층	5계층
제공 프로토콜	IP, IPX, NetBEUI 외	IP, IPX, NetBEUI 외	IP	TCP, UDP
사용자 인증	없음	없음	일부 가능	가능
데이터 암호화	없음(PPP 제공)	없음(PPP 제공)	패킷 단위 제공	메시지 단위 제공
키 관리	없음	없음	ISAKMP/Oakley, SKIP	GSS-API/SSL
터널링	Single PPP Tunnel /Connection	Multi PPP Tunnel /Connection	Multi PPP Tunnel /SA	Session
적용 VPN 모델	원격지 접속 VPN	원격지 접속 VPN	포인트 투 포인트 VPN 원격지 접속 VPN	포인트 투 포인트 VPN

주요 VPN 기술과 구성 요소

VPN의 기본 개념은 터널링(Tunneling)으로 이는 '외부의 영향 없이 안전하게 정보를 전송할 수 있는 가상의 연결'을 의미하며, 캡슐화(Capsulation)와 디캡슐화(Decapsulation) 과정을 포함하고 있다. 시작 지점에서 목표 지점까지 가상 터널의 생성과 생성된 터널을 안전하게 관리하기 위한 암호화/인증과 키 관리(Key Management) 프로토콜이 VPN의 핵심 기술이다.

가장 대표적인 VPN 터널링 기술은 PPTP, L2F, L2TP, IPSec, SSL 등이 있다. 초기에는 업체마다 독자적인 터널링 기술을 사용함으로써 폐쇄적인 성격을 갖고 있었지만, 현재는 IPSec이나 SSL과 같은 표준화된 기술을 사용하는 것이 대세다. 터널이 형성되고 운용되는 계층에 따라 (표 1)과 같이 분류할 수 있다.

여기서는 VPN의 대표 기술인 IPSec의 주요 구성 요소에 대해 알아보겠다. IPSec은 IETF(Internet Engineering Task Force) 워킹 그룹에 의해 표준화된 보안 프로토콜로 스푸핑(Spoofing)이나 스니핑(Sniffing) 공격에 취약한 IP 프로토콜의 보안 문제점을 해결하고 네트워크 계층에서 신뢰성 있는 보안 연결을 보장하기 위한 목적으로 개발됐다.

IPSec은 네트워크 계층에서 암호화를 수행하기 때문에 애플리케이션과 독립적으로 구현할 수 있다는 장점이 있으며, 암호화 부분을 처리하기 위한 ESP 헤더와 인증 부분을 처리하기 위한 AH 헤더, 그리고 암호화 키 관리를 위한 키 관리 부분으로 구성돼 있다.

IPSec는 TCP/IP 스택보다 낮은 계층으로 이 계층은 각 컴퓨터의 보안 정책과 송신자와 수신자가 협상한 보안 결합에 의해 제어되며, 보안 정책은 필터와 보안 규칙들로 정의된다.

표 2 IPSec 주요 구성 요소

방 식	구 분	지원기능
헤더	AH	인증, 무결성
	ESP	인증, 무결성, 기밀성
키 교환 (Key Exchange)	ISAKMP/Oakley	보안 패러미터 협상
	Diffie-Hellman	공유 비밀키 생성
모드	트랜스포트 모드 (Transport Mode)	IP 페이로드만 적용 양쪽 끝 단 모두 IPSec 필수
	터널 모드(Tunnel Mode)	전체 데이터그램에 적용 중간 시스템에 의해 변경되지 않음
인크립션	인크립션 모드	DES, 3DES, RC4, IDEA, AES, SEED

그림 8 IPSec 패킷의 구조

• ESP

ESP(Encapsulation Security Payload)는 IP 페이로드(Payload) 데이터의 도청을 방지하고 데이터 기밀성을 보장하기 위해 VPN 터널 종단 간에 협상된 키와 암호화 알고리즘으로, 데이터 암호화와 인증과 무결성 서비스를 제공하는 역할을 한다.

ESP는 동작 방식에 따라 IP 헤더를 제외한 데이터그램(Datagram) 부분만 암호화하는 트랜스포트(Transport) 방식과 패킷 전체를 암호화 하는 터널(Tunnel) 방식이 있다

용 ■ 어 ■ 설 ■ 명

PPTP
Point to Point Tunneling Protocol. 마이크로소프트와 3Com이 공동 개발한 VPN 터널링 프로토콜로, 공중 네트워크를 통해 패킷 데이터를 안전하게 전송하기 위한 VPN 터널링 프로토콜 중 하나. 외부로부터의 액세스를 제어할 수 있기 때문에 엔드 투 엔드나 서버 투 서버 터널링에 적합하다. 윈도우 NT 서버에서 기본적으로 지원하며, 여타의 네트워크 장비에 탑재된다. 멀티프로토콜 인캡슐레이션 과정을 통해 IP, IPX, NetBEUI 등 어떤 형태의 패키지도 전송할 수 있다.

SSL
Secured Socket Layer. 인터넷을 통한 정보 교환시 보안 기능을 강화하기 위해 비자와 마스터카드가 인터넷과 전자상거래를 위해 만든 전자지불 프로토콜. 사용자 인증이 없으며 전자우편을 통해 인증서를 요청하고 발급하는 것이 특징이다. 이 방식은 데이터 전송시 상대방에 대한 인증을 확인하고 계좌번호, 입금액 등의 중요한 정보는 암호화해 보내게 돼. 때문에 데이터를 전송하는 중간에 해커가 데이터를 가로채더라도 암호화가 돼 볼 수 없다.

그림 9 IPSec 구조

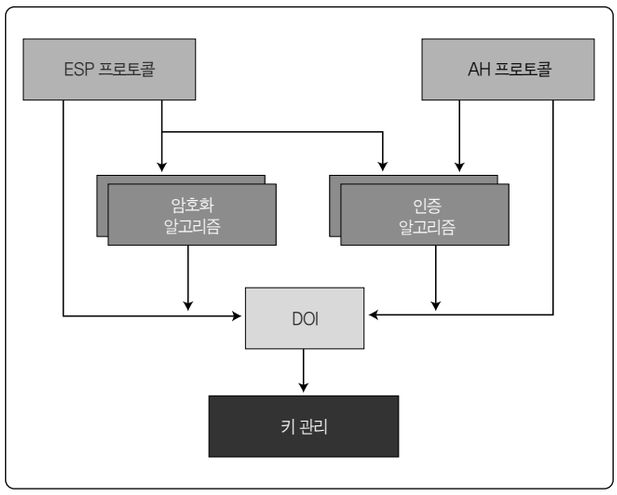


그림 10 ESP 프로토콜

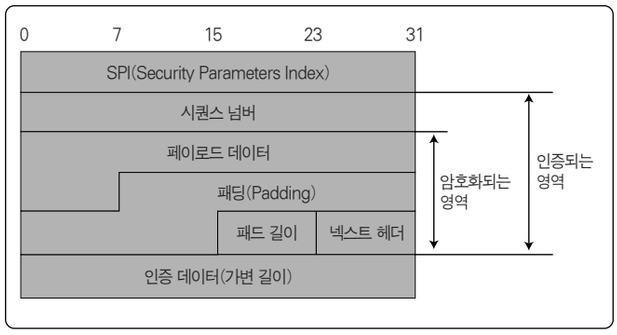
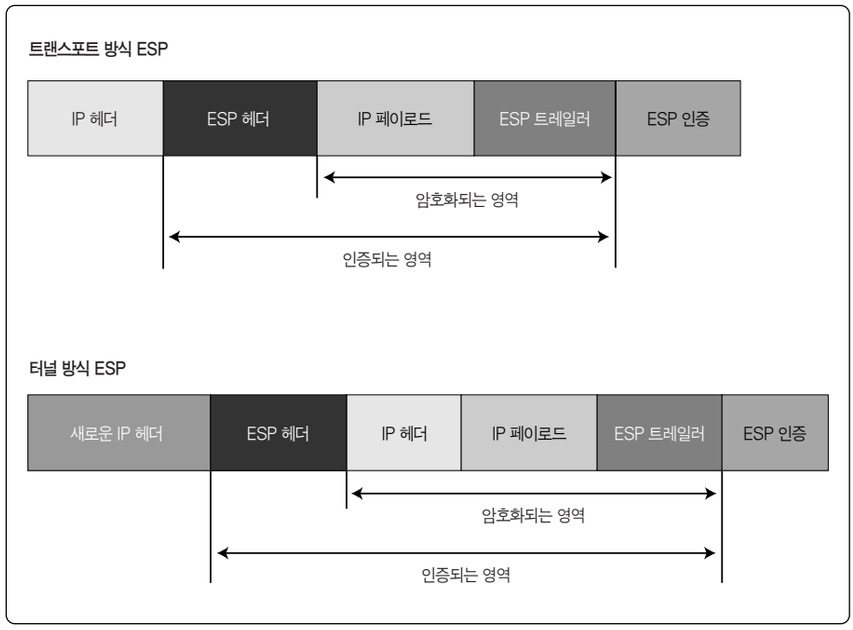


그림 11 ESP 트랜스포트 방식과 터널 방식



• AH

AH(Authentication Header)는 IP 헤더와 전송 헤더 사이에 위치하는 인증 헤더로 인증과 무결성을 검증하는 역할을 하며 내부에 포함된 인증 데이터와 일련번호를 기반으로 송신자 확인과 데이터 무결성 검증,재실행 공격을 방지하는데 사용된다.

전송측은 내부적으로 MD5, SHA-1 등의 해시(Hash) 알고리즘을 이용해 키 값과 IP 패킷의 인증값을 계산해 AH 인증 필드에 기록해 전송한다. 수신측에서는 동일한 키를 이용해 계산한 인증값과 인증 필드의 값을 비교해 검증한다.

AH도 IP 헤더와 데이터그램 부분만 암호화하는 트랜스포트 방식과 전체 패킷을 암호화하는 터널 방식이 있는데, AH는 ESP와는 달리 패킷 전체에 대한 데이터 암호화 기능은 제공하지 않는다.

• IKE

IKE(Internet Key Exchange)는 IETF 워킹 그룹에서 ISAKMP(Internet Security Association & Key Management Protocol)를 기반으로 오클리(Oakley) 키 알고리즘을 결합해 SA의 협상과 키 교환 메커니즘을 제공하기 위해 제안한 표준 프로토콜이다(RFC 2409).

현재 대다수의 VPN 솔루션에서 IKE를 기본 키 교환 프로토콜로 채택하고 있으며, 터널링을 구현하려는 두 시스템은 IKE에 의해 인증과 데이터 보안 방법을 협상하고, 상호 인증을 수행한 데이터 암호화에 사용할 공유키(Session Key)를 생성한다.

• DOI

DOI(Domain of Interpretation)는 터널링을 구현하려는 두 시스템이 IKE에 의해 정의된 암호화와 인증 프로토콜과 같은 다양한 값을 교환하는데 있어, 프로토콜로부터 정의된 값을 어떻게 해석할 것인지에 대한 내용을 담고 있다.

VPN의 새로운 애플리케이션, IBT

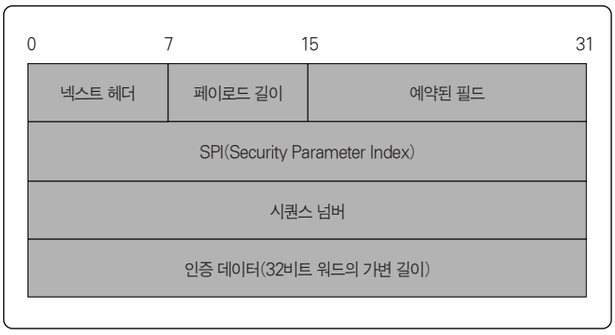
IBT(Internet Bonding Technology)는 다수의 네트워크 회선을 가상의 단일회선으로 묶어 속도를 향상시키는 네트워크 기술로, 낮은 비용으로 안정적인 전용회선 구축효과가 있어 최근 활용사례가 증가하고 있는 서비스다.

IBT는 내부적으로 VPN 터널링 기술을 이용한다. 그간 국내의 수많은 브로드밴드 VPN 구축 경험에서 축적된 멀티 터널링

(Multi-Tunneling) 기술과 회선 로드밸런싱 기술을 이용해 전용회선 수준의 안정성을 제공하고 있다. 또한 공인 IP 할당이 가능함에 따라 최근 전용회선의 대안으로 부상하고 있어 진화하고 있는 VPN 기술의 또 다른 면을 보여주고 있다.

특히 최근에는 일부 업체를 중심으로 IBT 기술을 기반으로 한 전용회선 서비스에 파이어월, IDS/IPS와 같은 보안 기능과 QoS와 같은 부가 기능을 통합하는 서비스도 선보이고 있는 추세다.

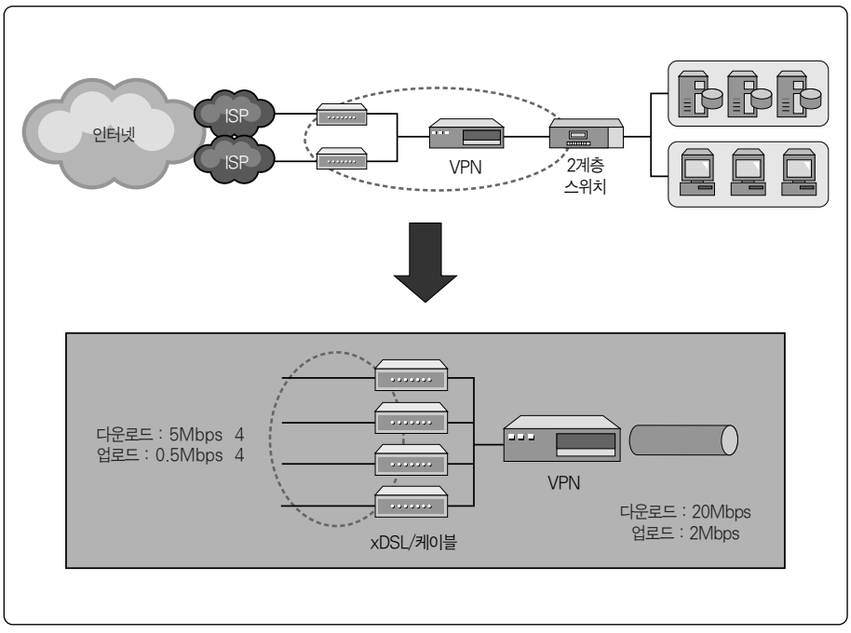
그림 12 ESP 프로토콜



VPN 기술 진화와 향후 전망

VPN 기술이 제공하는 비용 효율성과 검증된 신뢰성으로 인해 이미 국내외적으로 많은 도입이 이뤄졌다. 특히 표준화된 기술과 더불어 네트워크로 전송되는 모든 데이터의 암호화와 인증 기능 등 탁월한 보안성으로 인해 VPN은 이제 네트워크의 기본 보안기술로 인식되고 있다.

그림 13 IBT 기술 개요



특히, 국내의 VPN 환경은 전세계적으로 유래가 없을 정도로 발달한 초고속 통신 인프라를 기반으로 전용선 대비 가격대 성능비가 탁월한 xDSL/케이블 회선을 이용한 브로드밴드 VPN(Broadband VPN) 도입이 주를 이루고 있다.

그러나 현재까지의 대다수 VPN 구현 사례는 기존 전용회선의 고비용 구조를 해결하기 위한 것으로, 기존 애플리케이션을 연장해 운영하는 수준에 머무르고 있다. 이것은 현재의 IP VPN 기술이 별도의 장비를 사용하지 않는 한 안정된 품질을 제공하지 못하기 때문이다.

따라서 현재의 IP VPN 인프라에서 시간에 민감하거나, VoIP, VOD 등과 같이 일정한 대역폭을 요구하는 애플리케이션을 적용하기에는 한계가 있다. 이같은 부분은 MPLS VPN 등의 차세대 VPN 기술이 해결해야 할 과제라고 할 수 있다.

향후 IPv6가 일반화되고 IP 상에서의 트래픽 제어 기술(Traffic Management)이 발전하면 VoVPN(VoIP over VPN)이나 VPN 기반에서 신뢰성 있는 멀티미디어 서비스 운영도 가능할 것으로 보이며, 이미 일부 VPN 솔루션에서는 부분적으로 이같은 기능을 제공하고 있어 향후 성과가 주목되고 있다. NET

용 ■ 어 ■ 설 ■ 명

L2TP
Layer 2 Tunneling Protocol. IETF가 제안한 VPN 터널링 프로토콜 중 하나. 시스코 L2F의 한계를 극복하고자 L2F와 마이크로소프트의 PPTP를 적절히 통합시켜 탄생한 프로토콜로, 엔드 포인트 사이에 동시에 여러 개의 터널을 설정할 수 있다. 또, 관리자가 특정 채널에 대한 업무를 전담할 수 있도록 해 어느 정도의 QoS도 보장할 수 있으며, IPSec는 물론 애플토크나 IPX와 같은 비 IP 프로토콜도 지원한다.

IPSec
IP Layer Security Protocol. IETF(Internet Engieering Task Force)에서 개발한 보안 프로토콜로, IP 계층에서 데이터를 암호화해 전송하는 방법. AH/ESP 헤더를 이용한 IP 암호화와 키 관리 파트로 구성돼 있다.