# 12주차 1차시 VPN 개요 및 분류

## 【학습목표】

1. VPN의 등장배경에 대해 설명할 수 있다.
2. VPN을 구성 형태 및 구현에 따른 분류로 설명할 수 있다.

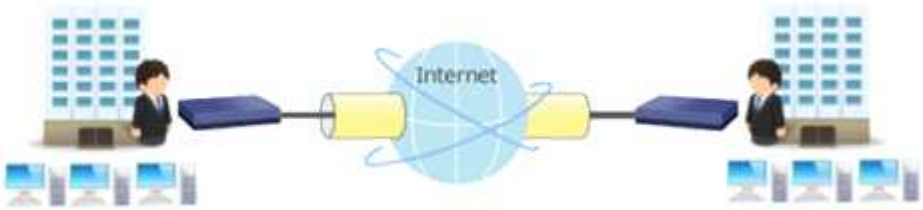
## 학습내용1 : VPN의 개요

### 1. VPN의 등장 배경

1) 공중 네트워크 vs. 사설 네트워크

- 공중 네트워크 (Public Network)
  - 전화망이나 인터넷처럼 모두에게 공개
  - 어느 누구와 언제든 정보 교환 가능
  - 보안성 취약
  - IP등의 공인된 표준을 따르는 통신 방법 채택


- 사설 네트워크 (Private Network)
  - 특정 조직 내에서만 사용되는 네트워크
  - 인증된 자만 사용
  - 보안성 우수
  - 거리에 따른 설치비용 부담
  - 관리 비용 부담

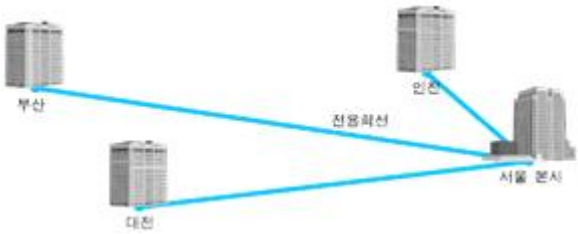


2) VPN 등장이유
- VPN은 인터넷을 기반으로 한 기업 업무 환경의 변화에 기인하여 등장
- 기업의 활동규모 및 지역 증가
- 사설망 구축 비용 급증

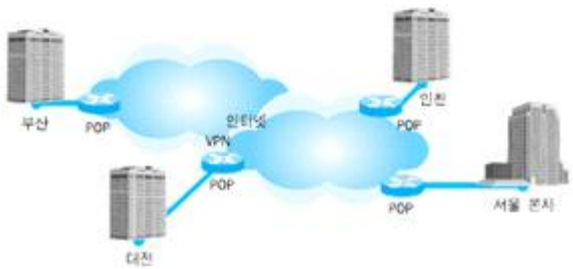

3) VPN 정의
- 공중망을 이용하여 사설망이 요구하는 서비스를 제공 할 수 있도록 구축한 망
- 공중망 내에서 마치 전용선처럼 사용할 수 있게 함
- 보안성 우수
  - 외부인으로부터 안전토록 주소 및 라우터 체계의 비공개
  - 데이터 암호화
  - 사용자 인증
  - 사용자 액세스 권한 제한

4) VPN 장점
- ISP(Internet Service Provider)들이 제공하는 인터넷 망을 이용하여 구축: 기존 사설망 구축에 드는 장비, 회선 비용 절감
- 해당 ISP가 있는 곳이면 어디서든 접속 가능
- 관리 비용 감소: ISP에서 망 관리
- 다양한 구축 방법
  - IPSec (IP Security Protocol)
  - MPLS (MultiProtocol Label Switching)
- 이동성 제공: ISP의 POP가 있는 곳이면 어디서든 접속가능
  - Mobility 증가(PDA, Notebook)을 이용한 접속 가능
- 네트워크의 유연성
  - 지사의 위치 이동 및 생성에도 ISP까지만 연결하면 됨

- 전용선을 이용한 사설망의 구축 예
  - 거리에 상관없이 망을 연결해야 하므로 구축비용이 큼




- 인터넷을 이용한 VPN 구축 예
  - 각 지사는 VPN 구축 계약이 된 ISP의 망 까지만 연결하면 되므로 구축 비용이 상대적으로 적게 듬

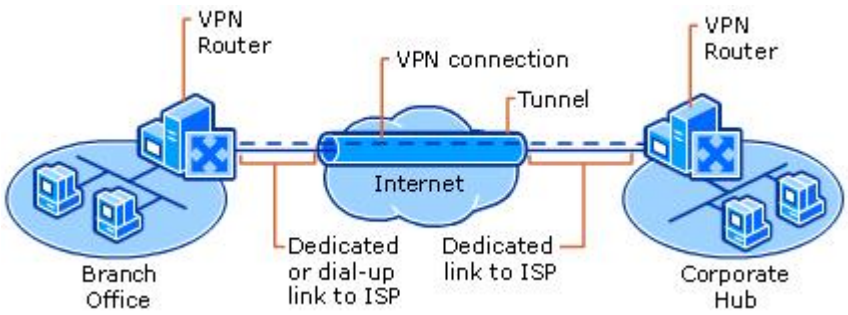



5) VPN 단점

- 표준의 부재: 명확한 표준이 없어 ISP마다 다른 기술을 채택하고 있음. 상이한 ISP간의 연동에 문제 발생
- 보안성 미약: IPSec 또는 MPLS를 이용한 보안성의 강화를 시도하고 있으나 암호화 기술의 노출 및 국가 차원의 정책적 보안의식 부족
- 성능: 인터넷 망을 이용하기 때문에 ISP의 VPN 성능 정책에 미치지 못하는 경우가 많음. 대부분 T1, E1등의 회선 사용으로 LAN의 성능(10/100Mbps)을 따라가지 못함

6) VPN 구현기술

- 암호화 기술 : 송신측이 데이터 전송 전에 암호화 하고 수신측은 이를 복호화 하여 보안성 강화
- 터널링 기술 : 전송하고자 하는 데이터를 특정 프로토콜로 캡슐화 하여 전송



7) VPN의 기능

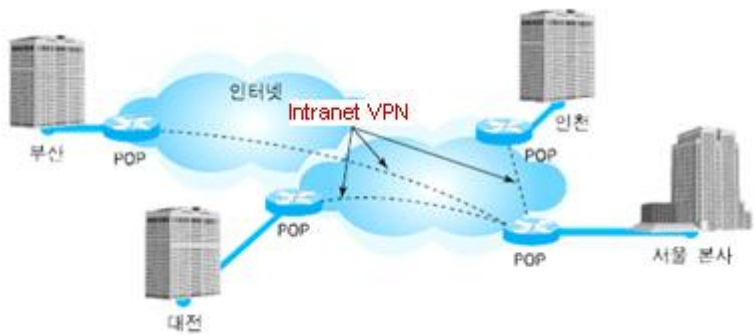
- 데이터 기밀성(Data Confidentiality): 데이터를 송·수신하는데 있어서 전송도중 데이터의 내용을 임의의 다른 사용자가 보았을 때 그 내용을 파악하지 못하도록 암호화 하여 전송
- 데이터 무결성(Data Integrity): 데이터의 송·수신 도중 데이터의 내용이 변경되지 않았음을 보장하는 기능으로 암호화 및 전자서명(Digital Signature)을 이용하여 보장
- 데이터 근원 인증(Data Origin Authentication): 데이터를 송·수신할 때 수신측이 수신한 데이터가 원래의 송신자에 의해서 전송되어 졌음을 확인 할 수 있는 서비스를 제공
- 접근 통제(Access Control): 인증된 사용자에게만 접근을 허용하는 기능으로 IPSec을 이용하여 사전 협상된 내용에 따라 통신을 하게 되며, 이러한 경우 협상 내용을 모르는 제 3자는 접근할 수 없게끔 하는 서비스를 제공

## 학습내용2 : VPN의 분류

### 1. 구성형태에 따른 분류

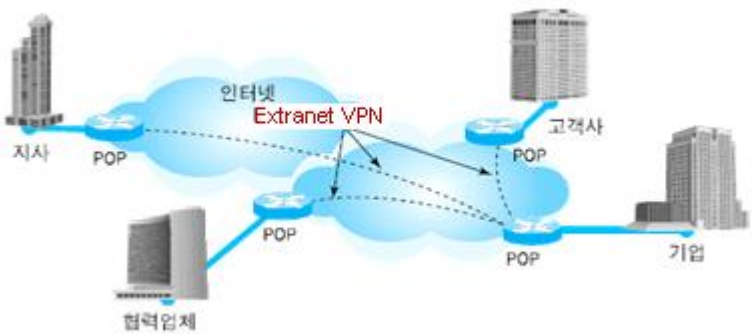
1) Intranet VPN

- 기업 내부를 LAN을 통해 연결, 넓게는 지사까지 연결
- 가장 단순한 형태의 VPN




2) Extranet VPN

- 관계 있는 고객사, 협력업체들까지 Intranet을 이용 가능하게 확장
- 트래픽이 본사로 집중되는 형태를 띄고 있어 대역폭 확보 중요
- RAS(Remote Access Service), 게이트웨이 등의 불편함 제거
- 고객들은 기업의 RAS가 아닌 ISP에 접속



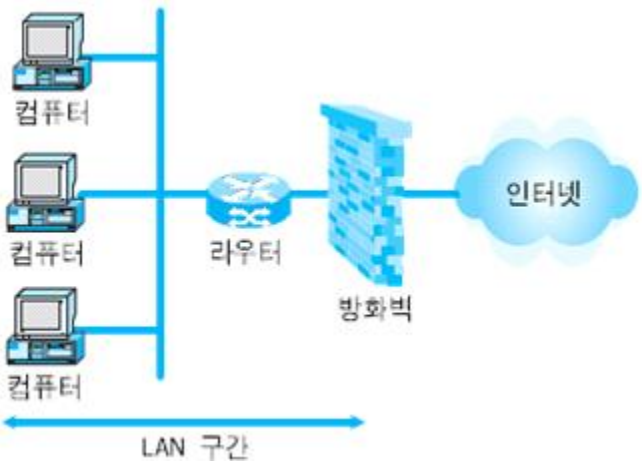
3) Remote Access VPN

- 기업의 원격지 사원간 접속
- 무선 및 전화접속을 이용하여 ISP의 NAS(Network Access Server)에 접속
- NAS는 사용자 접속 인증 절차 및 터널링 관련 기능을 수행, ISP는 NAS에 이러한 기능을 추가하여야 함


## 2. 구현형태에 따른 분류

1) 방화벽 형 VPN(방화벽 + VPN)

- 기존의 방화벽에 암호화·복호화 기술과 터널링으로 대표되는 VPN 기능을 추가함으로써 VPN망 구성
- 네트워크의 사용량은 점차적으로 증가하는 추세이며 이러한 트래픽의 증가는 방화벽을 통과하는 패킷의 수가 증가함
- 많은 양의 트래픽이 발생했을 경우, 방화벽의 성능저하 및 방화벽으로 인해 병목현상(Bottle neck) 초래



2) 라우터 형 VPN (라우터 + VPN)
- 주로 대규모 통신망에서 도입하는 방법
- 라우터나 접속서버(Access Server)에 VPN기능을 추가
- 라우터 내에 S/W 설치
- 별도의 H/W 설치
- 라우터 형 VPN의 성능은 VPN 터널 종단간의 라우터의 성능에 의해 좌우됨

3) VPN 서버형(기존 서버 + VPN)
- 메일 서버에 데이터 암호화·복호화와 사용자 인증 기능을 부가, 사용자에서 해당 서버와의 인증 절차를 거쳐 접속할 수 있도록 구성하는 방식
- 구현이 쉽고, 비용 측면에서 유리

4) 전용 시스템 VPN
- 기업의 내부와 사용자 사이에 보안의 유지가 필요한 부분에 인증 절차 및 데이터 암호화·복호화 기능을 수행할 수 있는 별도의 시스템을 두어 VPN을 구성
- 대부분 별도의 데이터베이스 장치를 필요
- 독립적인 측면에서 트래픽의 증가에 비교적 안정한 편
- VPN의 구축이 쉽고 그 확장성이 뛰어남
- 별도의 장비를 구입해야 하는 비용적 측면에서의 단점이 존재

**【학습정리】**

1. VPN이 갖는 장점으로는 ISP가 제공하는 인터넷 네트워크를 이용하여 구축할 수 있다는 점과 지사는 해당 ISP가 있는 곳이면 어디든 접속 가능하다는 점, 관리비용감소, 다양한 구축방법의 존재, 이동성 제공, 네트워크의 유연성 등을 들 수 있다. 반면, 단점으로는 표준의 부재, 보안성의 부족, 성능 등을 들 수 있다.

2. VPN은 구성 형태에 따라 Intranet VPN, Extranet VPN으로 나누며, 구현에 따라 방화벽형 VPN, 라우터형 VPN, VPN 서버형, 전용시스템 VPN으로 나누어볼 수 있다.