12주차 2차시 VPN 구성

【학습목표】

1. 터널링 구성 방법에 대해 2계층과 3계층 터널링으로 나누어 설명할 수 있다.
2. VPN에서의 인증방법에 대해 설명할 수 있다.

학습내용1 : 터널링 구성

1. 정의

- 터널링이라 함은 송신자와 수신자 사이의 전송로에 외부로부터의 침입을 막기 위해 일종의 파이프를 구성하는 것으로, 이때 파이프는 터널링을 지원하는 프로토콜을 사용하여 구현하며 사설 네트워크와 같은 보안 기능을 지원
- 터널링 기술에서는 터널링되는 데이터를 페이로드(payload)라고 부르며, 터널링 구간에서 페이로드는 그저 전송되는 데이터로 취급되어 그 내용은 변경되지 않음

2. 2계층 터널링 프로토콜

1) 정의

- 터널링 프로토콜은 주로 사용자와 접속하고자 하는 위치의 LAN을 연결
- Client-to-LAN을 위한 Remote Access VPN에 주로 사용
- 다이얼 업을 이용하여 접속할 때 ID와 암호를 사용하여 인증절차를 거친 후에 터널링을 시작

2) 특징

- 2계층 레벨의 VPN 구성
- Client-Server Model
- PPP(Point-to-Point Protocol) 기반의 프로토콜
- 다이얼 업으로 연결에 대한 기본적인 보안성이 제공되지만, 암호화 기능 미흡
- ATM(Asynchronous Transfer Mode), Frame Relay 등 지원

3) VPN 터널 구성 방법

- 클라이언트 개시 VPN(Client-Initiated VPN)
  - PC등 사용자 장비에 VPN 지원 소프트웨어를 설치해야 함
  - 소규모의 네트워크에 사용됨
  - 인증절차 이후 NAS는 터널링 프로토콜에 관여하지 않음
  - 하나의 터널에 단 하나의 접속만이 존재
  - PPTP (Point-to-Point Tunneling Protocol)

(접속절차)

① 사용자는 근처 NAS로 접속
② 접속수단은 ID와 암호
③ 인증절차 완료 후 터널링 프로토콜을 이용하여 목적지의 게이트웨이와 VPN 터널링 설정

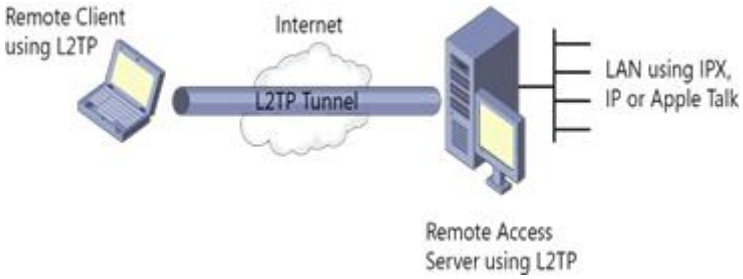
- NAS 개시 VPN(NAS-Initiated VPN)
  - 개인 PC에 별도의 장치 및 소프트웨어 불필요
  - NAS가 인증절차 및 터널링 프로토콜을 이용한 터널 생성에 책임
  - NAS에 VPN 기능 추가해야 함
  - 하나의 터널에 여러 사용자가 동시에 접속 가능
  - ISP의 NAS에서 기업의 Gateway까지 터널형성
  - 대규모 네트워크에 적합
  - L2F, L2TP
  - NAS가 인증 절차 및 VPN 터널링에 책임을 지므로 복잡해 짐
  - 하나의 터널에 대하여 다중접속을 지원하므로 클라이언트 개시 VPN보다 효율적인 네트워크 관리 가능

4) 2계층 프로토콜

- PPTP(Point-to-Point Tunneling Protocol)
  - 마이크로소프트(Microsoft) 사에서 개발
  - IP, IPX 또는 NetBEUI(Network BIOS Enhanced User Interface, IBM) 페이로드를 암호화 하고, IP헤더로 캡슐화 하여 전송
  - PPTP는 터널의 유지, 보수, 관리를 위하여 TCP연결을 사용하고
  - 이동사용자(Mobile user)가 서버(Home Server)에 접속하기에 용이하게 구성
  - 서버가 마이크로소프트사의 윈도 NT(Windows New Technology) 서버이어야 한다는 제약
  - 사용자는 별도의 PPTP 지원 소프트웨어를 사용해야 함
  - PPTP는 하나의 터널에 하나의 연결만을 지원하여 일대 일 통신만이 가능하다는 단점이 있었으나 현재는 다중접속을 지원
  - 클라이언트 개시 VPN에 사용됨

- L2F(Layer 2 Forwarding Protocol)
  - 시스코(Cisco Systems)사에서 제안되어진 프로토콜
  - NAS 개시 VPN 형
  - 사용자는 별도의 S/W 필요 없음
  - 하나의 터널에 여러 개의 연결을 지원, 다자간 통신 가능
  - 전송계층 프로토콜로 UDP(User Datagram Protocol) 사용

- L2TP(Layer 2 Tunneling Protocol)
  - L2TP는 PPTP와 L2F를 결합한 방법
  - 마이크로소프트와 시스코에서 지원
  - 호환성이 우수
  - PPTP와 캡슐화 방법이 유사
  - IPSec을 이용하여 패킷을 암호화 하는 기능 보유
  - 인터넷, X.25, Frame Relay, ATM을 지원
  - 전송계층 프로토콜은 UDP 사용



5) PPTP와 L2TP의 차이점

	PPTP	L2TP
표준화	마이크로소프트사	RFC2661
터널 서비스	하나의 터널에 단 하나의 접속 (현재는 다중접속 지원)	터널 하나에 다수의 접속 가능
헤더압축	지원하지 않음	지원
터널인증	지원하지 않음	지원

3. 3계층 터널링 프로토콜

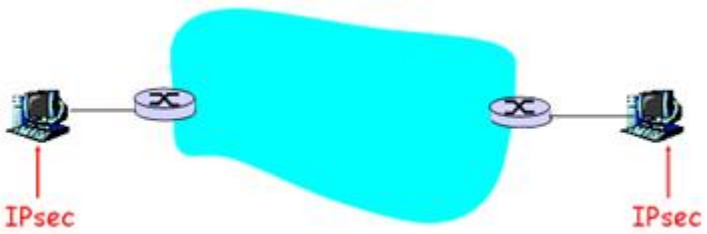
1) 정의

- IPSec 과 MPLS 로 대표되며, 주로 LAN-to-LAN VPN에 이용
- LAN-to-LAN VPN은 VPN 터널을 이용하여 통신하는 주체가 LAN 단위의 네트워크이며 주로 기업의 본사와 지사 사이의 네트워크를 말함
- 이를 채택한 네트워크 관리자는 원격 노드나 CPE(Customer Premises Equipment)에 특별한 소프트웨어를 설치할 필요가 없음
- 특징
  - 네트워크 계층 레벨의 VPN을 구성함
  - LAN-to-LAN 모델
  - 링크 계층과 독립적
  - 우수한 보안성
  - CPE에 특별한 변화 없이 구축 가능

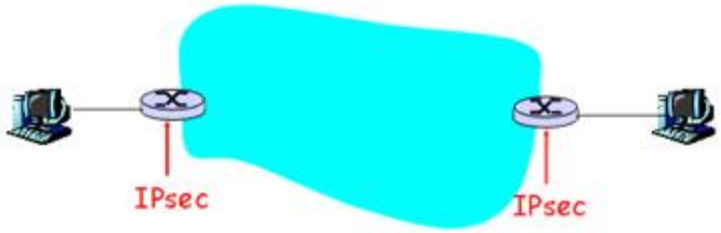
2) IPSec을 이용한 VPN

- IP망에서 안전하게 정보를 전송하는 표준화된 3계층 터널링 프로토콜
- IP계층의 보안을 위해 IETF에 의해 제안
- VPN 구현에 널리 쓰이고 있음
- IP데이터그램의 인증과 무결성, 기밀성을 제공
  - AH(Authentication Header)
  - ESP(Encapsulation Security)
- AH/ESP에 필요한 보안관련 협상(Security Association Negotiation)과 키 관리를 담당
  - ISAKMP/IKE(Internet Security Association and Key Management Protocol/Internet Key Exchange)
- 두 호스트 사이, 두 보안 게이트웨이 사이 또는 보안 게이트웨이와 호스트 사이의 통신을 보호하기 위해 사용

- IPSec의 두 가지 모드
  - 전송모드: IP 페이로드를 암호화하여 IP헤더로 캡슐화



- 터널모드
  - v IP 패킷을 모두 암호화하여 전송
  - v 터널의 종단점과 첫 번째 라우터 사이는 평문으로 전송, 라우터와 라우터 사이만 암호화되기 때문에 주로 망간 연결에 사용



- IPSec의 헤더
  - AH
    - v 인증 데이터와 순서번호 보유
    - v 송신자를 확인, 메시지가 송신되는 동안 수정되지 않았음을 보장
    - v 암호화 기능 없음
  - ESP
    - v IP 페이로드를 암호화하여 데이터 기밀성(Confidentiality)을 제공
    - v 제 3자의 악의에 의해 데이터가 노출되는 것을 차단
  - IPSec 터널링 헤더와 페이로드의 구조
    - v 왼쪽의 IP 헤더: IPSec을 이용하여 전송되는 네트워크 내에서 라우팅에 사용될 헤더
    - v 오른쪽의 IP 헤더: 송신측에서 전송한 IP 패킷의 헤더(실제 목적지로 보내지는)

학습내용2 : VPN 인증

1. VPN 에서의 인증

- 데이터 인증: 데이터의 변형 여부를 증명
- 사용자 인증: 송신자의 접근 권한을 부여
  예) 인터넷에서 볼 수 있는 사이트(Site) 접근 시 요구되어 지는 ID와 암호 등
- Remote Access VPN의 경우 언제 어디에서 접근할지 모르기 때문에 초기 VPN 접근 시 보안서버로부터 인증절차를 반드시 거쳐야 함
- 인증절차
  - Peer-Peer 방식
  - 클라이언트-서버(Client/Server) 방식

1) Peer-Peer 방식
- 독립적인 2개의 호스트 간에 요청 및 응답을 통한 사용자 인증
- PAP(Password Authentication Protocol)
  - two-way handshaking 방식
  - 인증을 요청하는 호스트에서 사용자 ID와 암호를 일반 텍스트 형태로 전달
  - 인증 정보의 외부 노출이 손쉽게 이루어 질 수 있음
- CHAP(Challenge Handshake Authentication Protocol)
  - three-way handshaking 방식
  - 인증서버는 호스트로 challenge 메시지를 보내면, 호스트는 보안을 위해 해시 함수(Hash function)를 이용하여 계산한 값을 보내고 그런 다음 인증서버는 값이 일치하면 인증하는 방식
- Peer-Peer 방식은 동일한 호스트를 사용하는 사용자 별로 차별화된 네트워크 접근 권한을 할당할 수 없다는 단점을 갖고 있음

2) 클라이언트-서버(Client/Server) 방식
- 보안 관리 기능에 대해 좀 더 편리하고 유연하게 제공하기 위한 방식
- TACACS (Terminal Access Controller Access-Control System)
  - 인증에 필요한 사용자 ID, 암호, PINs 및 암호키 정보를 인증서버에서 데이터베이스 형태로 관리, 클라이언트로부터의 인증 요청을 처리
  - 사용자와 서버 사이에 전달되는 모든 데이터는 일반 텍스트 형태
  - TACACS+에서는 MD(Message-Digest), 즉 해시 함수를 추가하여 인증 데이터에 대한 보안 기능을 강화
  - TACACS+는 멀티프로토콜 로그인(Multiprotocol login)을 지원
  - IP 이외에도 IPX, AppleTalk 등의 네트워크에서도 로그인이 가능
- RADIUS(Remote Access Dial-In User Service)
  - 사용자 인증 이외에도 사용자 연결 관리를 위해 NAS와 연동
  - NAS는 사용자가 네트워크로의 접속을 제공하는 서버 기능을 제공하면서 동시에 RADIUS에 대해 클라이언트 역할을 수행
  - RADIUS도 TACACS와 마찬가지로 인증서버에서 인증에 관련된 정보를 단일의 데이터베이스 형태로 관리
  - RADIUS서버와 클라이언트는 사용자 암호의 안전한 송수신을 위해 비밀키 암호화 방식을 사용

2. VPN 에서의 암호화

- 정보를 제 3자로부터 숨기는 작업으로 암호화 알고리즘을 이용

1) 비밀키 알고리즘

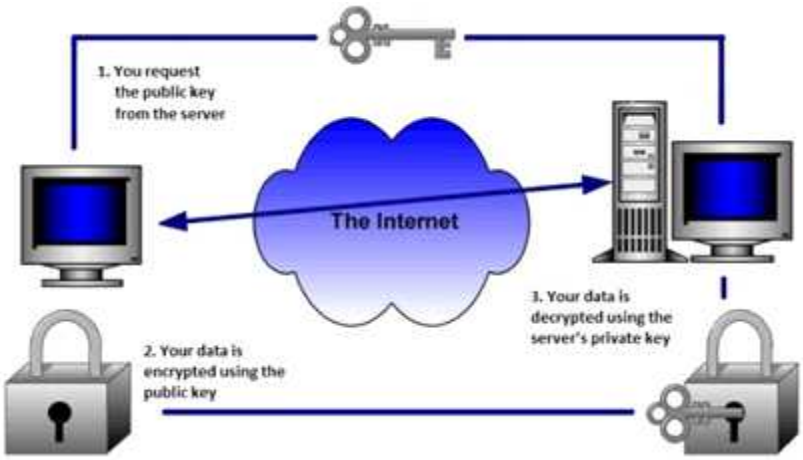
- 암호화/복호화를 동일한 키를 사용하여 수행
- 키를 알고 있는 사람만이 해당 정보를 평문으로 복호화 가능
- DES(Data Encryption Standard), 3DES

2) 공개키 알고리즘

- 암호화 키와 복호화 키 중 암호화 키는 공개키로,
- 복호화 키는 개인키(비공개)로 사용
- 각 호스트가 공개키를 사용하여 암호화 하면 이에 적합한 개인키를 가진 사람만 이를 복호화 가능

3) RSA (Rivest,Shamir,Adleman)

- 대표적인 공개키 암호화 방식
- 1978년 로널드 라이베스트(R), 아디 샤미르(S), 레너드 애들먼(A)이 체계화
- 1983년 MIT가 특허 등록 (2000년 9월 특허 만료 상태)



【학습정리】

1. VPN을 구성하기 위해서 반드시 구현되어야 할 몇 가지 중요한 기술들이 있는데, 터널링과 인증절차 및 암호화에 관련된 기술이다.

2. 터널링은 데이터를 터널링 프로토콜을 이용하여 캡슐화하는 것으로 2계층 터널링 프로토콜에는 PPTP, L2F, L2TP가 있으며, 3계층 터널링 프로토콜에는 IPSec이 있다.