VPN 기술

VPN 기술

✓인터넷망을 통해 사설망 연결

✓**VPN**의 장점
- ✓비용절약
- ✓보안성
- ✓확장성
- ✓Broadband기술과의 호환성

✓**VPN**의 종류
- ✓Site-to-Site VPN
- ✓Remote-Access VPN
- ✓GRE
- ✓DMVPN

✓**VPN** 구성요소
- ✓인터넷 연결
- ✓VPN Gateway
  - ✓Router
  - ✓FW
  - ✓VPN Concentrator
  - ✓ASA
- ✓VPN 터널 생성, 관리 소프트웨어

안전한 VPN 연결설정

- ✓캡슐화
  - ✓터널링
- ✓암호화
- ✓**Hash**
  - ✓데이터 무결성
- ✓인증

- ✓**Hash** 알고리즘
  - ✓MD5 : 128bit 공유키
  - ✓SHA-1(Secure Hash Algorithm 1) : 160bit 공유키

- ✓인증 방법
  - ✓Pre-shared key
  - ✓RSA 서명 : 인증서 교환

- ✓암호화
  - ✓암호화 알고리즘
  - ✓키 길이

- ✓암호화 알고리즘
  - ✓DES
    - ✓대칭키
    - ✓56bit 키
  - ✓3DES
  - ✓AES
    - ✓DES보다 강력
    - ✓3DES보다 효율적
    - ✓128,192,256bit 키
  - ✓**RSA**
    - ✓비대칭키
    - ✓512,768,1024bit 키

1. IPSEC VPN

IPSec VPN

- IP 보안을 위한 VPN 프로토콜 모음
- 인터넷 상에서 안전하게 데이터를 주고받기 위한 표준
- 인증, 암호화, 무결성 제공

IPSec 프레임워크 프로토콜

- **IKE(Internet Key Exchange)**
- 인증 헤더(AH) : 기밀성이 필요하지 않거나 허용되지 않을 때 사용
  - 인증
  - 무결성
- **ESP(Security Payload)**
  - 기밀성(선택)
  - 인증(선택)
  - 무결성

IPSec 운영모드

- ✓운영모드
  - ✓Transport 모드
    - ✓패킷 사이즈, remote-access VPN, 클라이언트 S/W
  - ✓Tunnel 모드
    - ✓Site to site VPN

동작 방식 흐름

1. 알고리즘/정책 협상
2. 키 교환 (DH 알고리즘)
3. 상호 인증 (PSK, 인증서 등)
4. SA 설정 → 데이터 암호화 시작

IPSec 구현 단계(site to site VPN)

- ✓IKE Phase 1 터널 설정(ISAKMP 터널)
- ✓IKE Phase 2 터널 설정(IPSec 터널)
- ✓Crypto map 적용

IKE Phase 1 터널 설정(ISAKMP 터널)

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash sha
R1(config-isakmp)#encryption aes 128
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#exit
R1(config)#crypto isakmp key C1sc0Press address 172.16.0.2

R2(config)#crypto isakmp policy 1
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#hash sha
R2(config-isakmp)#encryption aes 128
R2(config-isakmp)#group 2
R2(config-isakmp)#lifetime 86400
R2(config-isakmp)#exit
R2(config)#crypto isakmp key C1sc0Press address 172.16.0.1
```

IKE Phase 2 터널 설정(IPSec 터널)

```
R1(config)#crypto ipsec transform-set MYSET esp-aes esp-sha
R1(cfg-crypto-trans)#exit
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#crypto map R1_TO_R2 10 ipsec-isakmp
R1(config-crypto-map)#set peer 172.16.0.2
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set transform-set MYSET
```

```
R2(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
R2(cfg-crypto-trans)#exit
R2(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config)#crypto map R2_TO_R1 10 ipsec-isakmp
R2(config-crypto-map)#set peer 172.16.0.1
R2(config-crypto-map)#match address 101
R2(config-crypto-map)#set transform-set MYSET
```

Crypto map 적용

```
R1(config)#int s0/0
R1(config-if)#crypto map R1_TO_R2
R1(config-if)#exit
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.0.2

R1(config)#int s0/0
R1(config-if)#crypto map R2_TO_R1
R1(config-if)#exit
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.0.1
```

IPSec 확인

R1#sh crypto engine connections active
R1#sh crypto session
R1#sh crypto isakmp sa
R1#sh crypto ipsec sa

2.L2VPN

L2VPN이란

- **L2VPN**은 “L2(Frame 기반)를 터널링하는 **VPN** 기술”로, **MAC** 프레임 단위의 통신을 **ISP**망을 통해 다른 지점까지 연결하는 가상 사설망입니다.

왜 사용하는가?

✓지사와 본사를 같은 VLAN처럼 연결하고 싶을 때
✓VM이나 서버 간 L2 통신이 필요할 때
✓기존 L2 기반 프로토콜(예: STP, CDP 등)을 유지하며 통신하고 싶을 때
✓MPLS, VXLAN, GRE 등과 결합해 고성능 통신이 필요할 때

주요 구성 요소

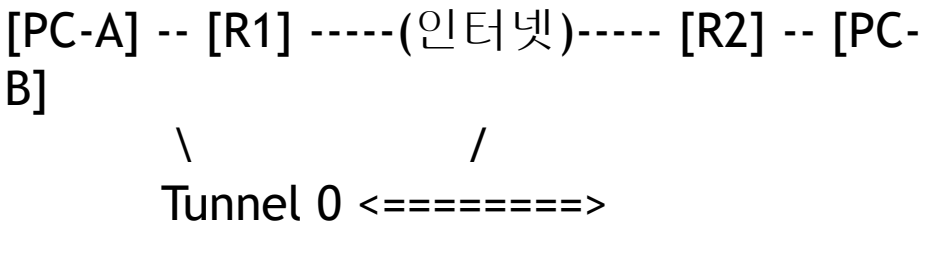
구성요소	설명
CE (Customer Edge)	고객측 라우터나 스위치 (일반적으로 L2장비)
PE (Provider Edge)	ISP측 라우터 (L2VPN을 구성하는 핵심 장비)
P (Provider)	백본 라우터, L2VPN의 경로를 중계
Pseudowire	PE-PE 사이를 연결하는 가상 회선 (L2 프레임을 캡슐화)

L2VPN의 주요 기술

기술	설명
VPWS (Virtual Private Wire Service)	1:1 연결, 포인트 투 포인트 L2VPN
VPLS (Virtual Private LAN Service)	1:N 또는 N:N 연결, 스위칭 허브처럼 동작
EVPN (Ethernet VPN)	MPLS + BGP + VXLAN 기반의 고급 L2VPN (데이터센터에서 사용)

GRE 터널 구성하기

- 지사 A와 B를 인터넷(IP망)으로 연결하고,
  양쪽 라우터 간에 **Tunnel을 통해 통신**하는 구조.



기본 설정 예

<R1>
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 tunnel source 192.168.1.1
 tunnel destination 192.168.2.1
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
ip route 192.168.2.0 255.255.255.0
FastEthernet0/0
ip route 10.0.0.0 255.255.255.0 Tunnel0

<R2>
interface Tunnel0
 ip address 10.0.0.2 255.255.255.0
 tunnel source 192.168.2.1
 tunnel destination 192.168.1.1
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
!
ip route 192.168.1.0 255.255.255.0
FastEthernet0/0
ip route 10.0.0.0 255.255.255.0 Tunnel0

- PC-A: IP 10.0.0.10 / GW: 10.0.0.1
- PC-B: IP 10.0.0.20 / GW: 10.0.0.2

⟶ ping 10.0.0.20 → 성공하면 GRE 터널이 정상적으로 작동!

3.SSLVPN

SSL

SSL(Secure Sockets Layer)은 웹사이트와 사용자 사이의 데이터를 안전하게 암호화해서 주고받게 해주는 보안 기술입니다.

SSL동작

•**클라이언트 Hello**
→ "안녕하세요! SSL 통신하고 싶어요!"
→ 사용할 암호화 알고리즘 리스트와 버전 등 전송
•**서버 Hello + 인증서 전달**
→ 서버는 자신의 **SSL 인증서**(공개키 포함)를 클라이언트에 전달
→ 브라우저는 이걸 보고 "이 서버 믿을 수 있나?" 검사
•**Pre-Master Secret 전달**
→ 클라이언트는 랜덤한 비밀 숫자를 만들어서
서버의 **공개키로 암호화**해 보냄 → 서버만 복호화 가능
•**세션키 생성 (양쪽 모두 같은 키 계산)**
→ 이 Pre-Master Secret을 바탕으로
클라이언트와 서버는 **같은 세션키**를 계산함
•**세션키로 안전한 통신 시작**
→ 이 키로 암호화된 데이터만 주고받음 (https 동작)

SSLvsTLS

항목	SSL (Secure Sockets Layer)	TLS (Transport Layer Security)
관계	TLS는 SSL의 **후속 버전**	SSL은 **이전 세대 기술**
버전	SSL 2.0, 3.0 (현재는 **폐기**)	TLS 1.0 → 1.1 → 1.2 → **1.3** (현재 최신)
보안성	여러 보안 취약점 존재 (POODLE 등)	보안 취약점 개선됨, 더 강력한 암호화
키 교환	RSA 기반 위주	RSA 외에도 **ECDHE 등 다양한 방식** 지원
메시지 인증	MAC-then-encrypt 방식	**Encrypt-then-MAC (또는 AEAD)**
표준화	넷스케이프(Netscape)가 개발	IETF에서 RFC로 표준화
지원 현황	**대부분의 브라우저/서버에서 사용 금지**	TLS 1.2 이상이 현재 업계 표준

Device Monitoring

SNMP 개요

✓관리자와 에이전트 간의 통신을 위한 메시지 형식을 제공

✓SNMP 구성 요소

- ✓SNMP 관리자
- ✓SNMP 에이전트
- ✓관리 정보 기반(MIB)

✓SNMP Message

- ✓Get
- ✓Set
- ✓trap

SNMP 버전

- ✓SNMPv1: RFC 1157
- ✓SNMPv2c: RFC 1901 ~ 1908
- ✓SNMPv3: RFC 2273 ~ 2275 네트워크를 통해 패킷을 인증 및 암호화 지원

- ✓V1과 v2c는 community string 이용하여 접근 제어
- ✓Community string은 plaintext password
  - ✓RO/RW 두 가지 유형

SNMP 설정 및 확인

```
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit host 172.16.3.110
R1(config-std-nacl)# exit
R1(config)# snmp-server community 4md!n0n1y RO SNMP_ACL
R1(config)# snmp-server location Lima, OH
R1(config)# snmp-server contact Jess Jang
R1(config)# end

R1# show snmp
Chassis: FTX1636848Z
Contact: Bob Smith
Location: Lima, OH
0 SNMP packets input
   0 Bad SNMP version errors
:
:
SNMP logging: enabled
   Logging to 172.16.3.10, 0/10, 359 sent, 0 dropped.
```

syslog

✓UDP 514

✓세 가지 기본 기능을 제공

- ✓모니터링 및 문제 해결을 위한 로깅 정보 수집
- ✓캡처되는 로깅 정보 유형 선택
- ✓캡처된 **syslog** 메시지의 대상 지정

✓모든 **syslog** 메시지에는 심각도 수준 및 기능이 포함

단계	심각도이름	설명
0	emergency	System 사용불가
1	Alert	즉각적인 대응 필요
2	Critical	심각한 상황
3	Error	에러 상황
4	Warning	경고 상황
5	Notification	주의
6	Informational	정보
7	debugging	디버그

syslog 설정 및 확인-1

✓Console/buffer (logging console/logging buffer)

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
  0 overruns, xml disabled, filtering disabled)
:
   Console logging: level debugging, 32 messages logged, xml disabled,
                    filtering disabled
  Buffer logging: level debugging, 32 messages logged, xml disabled,
                    filtering disabled
:
Log Buffer (8192 bytes):

*Jan 2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User
  License Agreement is accepted
*Jan 2 00:00:02.631: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
  Module name = c1900 Next reboot level = ipbasek9 and License = ipbasek9
able No such file or directory
<output omitted>
```

syslog 설정 및 확인-2

✓Syslog server 설정

✓Router(config)#logging 192.168.1.100

✓심각도 수준 설정

✓Router(config)#logging trap 4

✓Logging source-interface 설정

✓Router(config)#logging source-interface g0/0

R1# show logging
:
:
Trap logging: level warnings, 43 message lines logged
Logging to 192.168.1.3 (udp port 514, audit disabled,
link up),
4 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled

Network Time Protocol

✓장치 간에 타임스탬프가 일관되도록 시간 시계를 동기화하는 방법을 제공

```
R1(config)# ntp server 172.16.2.2
R1(config)# ^Z
R1#
R1# show ntp status
Clock is synchronized, stratum 8, reference is 172.16.2.2
:
R1# show ntp associations
address ref clock st when poll reach delay offset disp
*172.16.2.2 127.127.1.1 7 36 64 1 1.261 -0.001 7937.5
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, configured
```

```
R1(config)# ntp master
```