VPN - 실습가이드

최초 작성일 : 2024/02/02

최종 제출일 : 2024/02/05

김민경

목차

Ⅰ. 개념정리

1. VPN

1) 정의

• Virtual Private Network(가상 사설망)

• 공인 인터넷을 사이에 둔 사설망과 사설망이 사설 ip를 이용해 통신

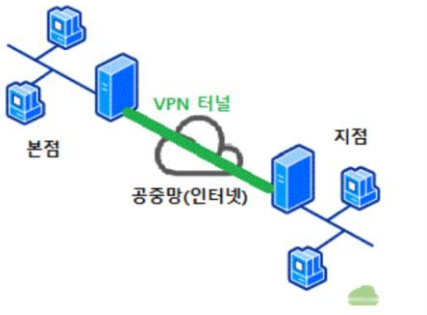
참고)

- **사설망** : 조직 내에서만 사용되는 네트워크 (보안성 우수, 비용 多)
- **공중망** : 모두에게 공개돼 네트워크(인터넷) (보안성 취약, 상대적으로 비용 小)

• 본점-지점을 사설망으로 연결 시⇒ 전용 회선으로 연결할 경우 성능은 뛰어나지만 비용 多

전용 회선대신 인터넷을 사설망처럼 안전한 전용 네트워크를 구성하자는 요구가 생겨 VPN이 나오게 됨

2) Tunneling (터널링)



• 공인 인터넷에서 IP Packet을 캡슐화(Encapsulation)함과 동시에 데이터의 암호화/인증방식을 협상함

• 이 협상과정을 거친 후에는 캡슐화된 패킷이 오고가기 때문에 아무리 인터넷 상이라고 하더라도 외부인이 패킷을 쉽게 탈취할 수 없음

2. OSPF

1) 정의

• Open Shortest Path First

• 동적 라우팅 프로토콜

• 대표적인 링크 상태 라우팅 프로토콜 (각 목적지까지의 최적 경로를 계산)

참고) 링크 상태 라우팅 프로토콜

• 인터넷에서 연결된 링크의 상태를 감시하여 최적의 경로를 선택하는 것

2) 장점

• area 단위로 구성되어 대규모 네트워크를 안정되게 운영할 수 있음

3. IPSec

1) 정의

• Internet Protocol Security

• Network 계층에서 ip 패킷을 암호화하고 인증하는 등의 보안을 위한 표준

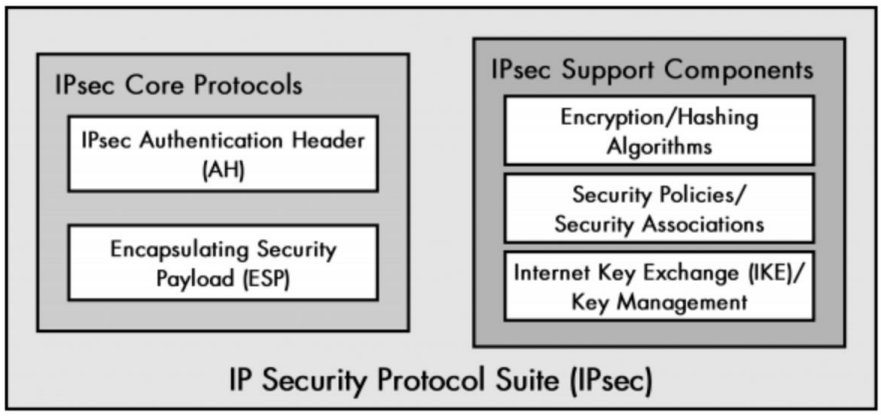
참고) 보안 관련 프로토콜

1) Application Layer - HTTPS, SSH, PGP, S/MIME
2) Transport Layer - SSL/TLS
3) Network Layer - IPsec, VPN
4) Data Link Layer - L2TP

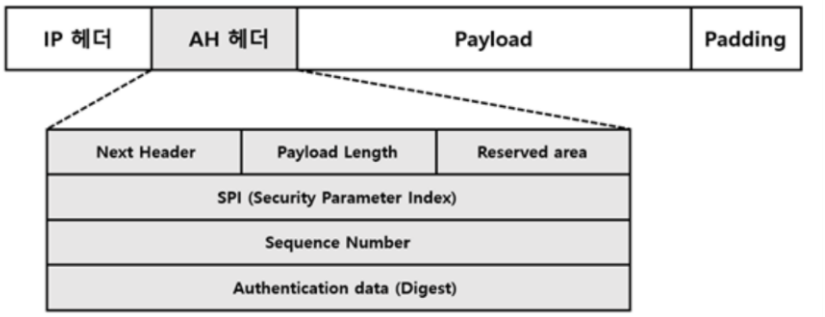
• VPN을 구현하는데 사용되는 프로토콜

2) 종류

• IPSec은 3개의 프로토콜의 모음임



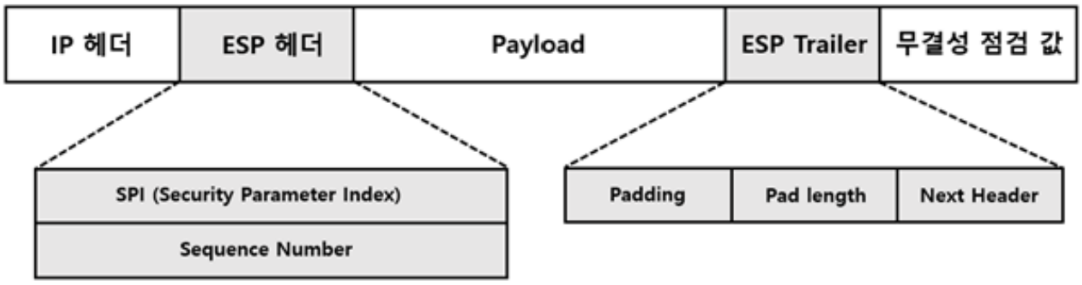
① AH (Authentication Header)



Authentication Header

- 패킷 인증 & 무결성을 체크함
- 패킷에 헤더를 추가하고, 이 헤더 안에 패킷 내용에 대한 암호화 해시값을 포함시킴
- 패킷을 수신한 호스트는 해시값을 이용해 패킷이 전송되는 도중에 변조되지 X는지 확인 가능함
- **암호화 기능 제공 X**

② ESP (Encapsulating Security Payload)



Encapsulating Security Payload

- 페이로드 부분을 암호화함
- 패킷이 중복 발생되지 않았는지 확인할 수 있도록 패킷 헤더에 시퀀스 번호를 추가
- **암호화 O**, 데이터 앞에 위치하는 것이 X닌 데이터를 감싸고 있음

③ IKE (Internet Key Exchange)

IKE 과정

1단계)

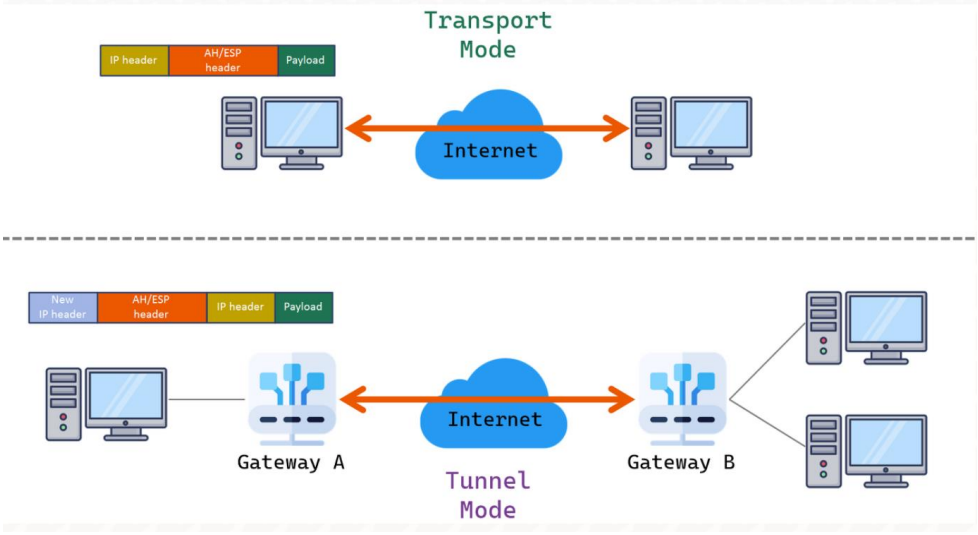
- IKE 알고리즘 자체의 SA를 설정하고 협상하는 단계
- 이후 IPSec SA 관련 설정들을 안전하게 협상하는데 필요한 여러 SA들을 설정하는 단계로, IPSec SA 설정을 위한 기초 작업

2단계)

- IPSec 알고리즘의 SA를 설정하고 협상하는 단계(실질적인 IPSec 연결을 설정하는 단계)
- IPSec에 사용할 Sequence Number Counter, Window 크기, AH/ESP 프로토콜 정보, Mode 등을 설정

3) 동작모드

- IPsec 패킷 헤더를 처리하는 방식에서 차이가 존재함



① Transport mode

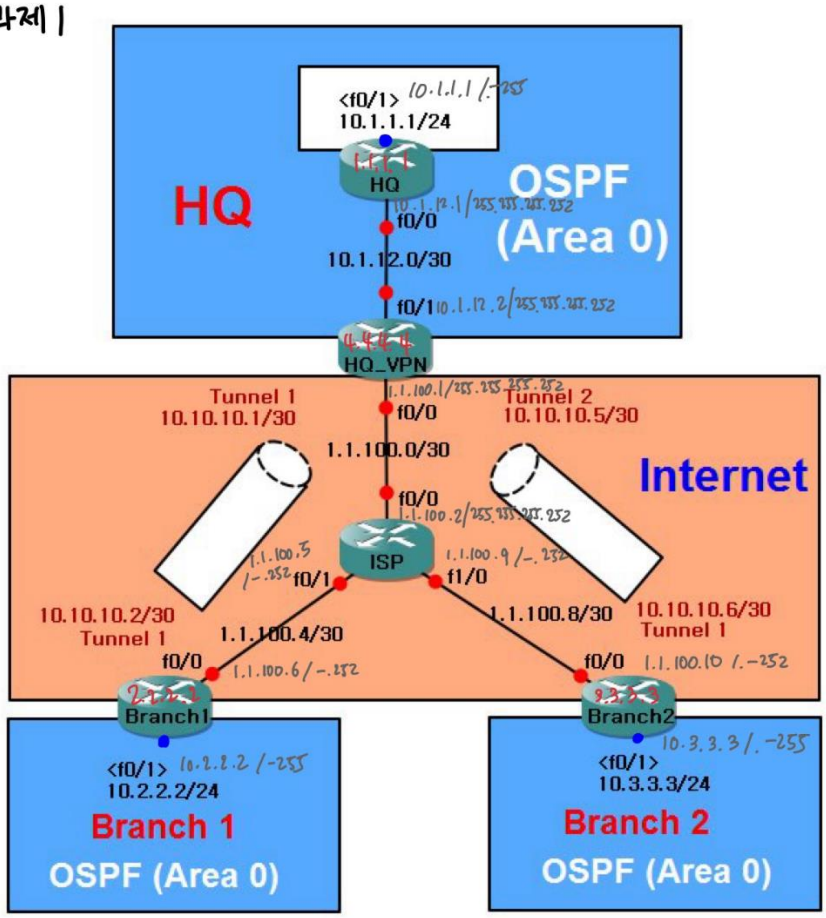
- 패킷의 **payload만 암호화**하고, 기존 패킷 헤더 데이터는 원상태 그대로 유지
- ESP/AH 헤더는 IP 헤더 뒤에 위치하고, 바로 그 뒤에 암호화된 데이터 페이로드가 뒤따름
- 일반적으로 호스트-게이트웨이or 호스트-호스트 간 직접 연결에 사용됨

② Tunnel mode

- **IP 헤더와 데이터 페이로드 부분까지 전부 빠짐없이 암호화**
- ESP/AH 헤더는 Transport mode와는 정반대로 IP 헤더보다 앞에 붙음
- 게이트웨이 간 연결에 주로 사용됨

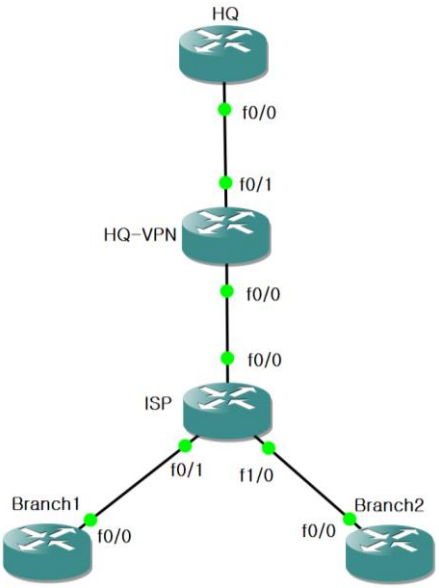
Ⅱ. 실습 1번

과제 I



1. 환경 구성

1) 다음과 같이 GNS로 환경 구성하기



2) 모든 라우터에 다음을 입력하기

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#no ip domain lookup // 명령어 잘못 입력 시 DNS 서버 찾지 않기
Branch2(config)#line c 0  // 콘솔 모드 진입
Branch2(config-line)#logg sy // log 메시지 동기화 설정
Branch2(config-line)#exec-timeout 0 // 세션 유지 시간 설정
Branch2(config-line)#exit
Branch2(config)#line vty 0 4  // 0~4번까지 총 5개의 텔넷 세션 설정하기
Branch2(config-line)#pass cisco // cisco라는 암호를 입력했을 때 접속 허용하기
Branch2(config-line)#end
Branch2#wr
Building configuration...
[OK]
Branch2#
```

- **no ip domain lookup** : 명령어가 x닌 것을 치면 도메인 네임으로 인식하고 DNS 서버를 찾음
- **logging synchronous** : 명령어 입력 도중에 시스템 메시지가 표시되면 자동으로 줄을 바꾸어 입력 중인 명령어를 다시 표시하게 하는 방법

3) ip 할당하기

3-1) HQ

```
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#int f0/1
HQ(config-if)#no sh
HQ(config-if)#ip add 10.1.1.
*Mar  1 00:28:25.223: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:28:26.223: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
HQ(config-if)#ip add 10.1.1.1 255.255.255.0
HQ(config-if)#no sh
HQ(config-if)#exit
HQ(config)#
```

```
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#int f0/0
HQ(config-if)#no sh
HQ(config-if)#ip add 10.
*Mar  1 00:29:58.507: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:29:59.507: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up
HQ(config-if)#ip add 10.1.12.1 255.255.255.252
HQ(config-if)#no sh
HQ(config-if)#end
HQ#w
*Mar  1 00:30:09.295: %SYS-5-CONFIG_I: Configured from console by console
HQ#wr
Building configuration...
[OK]
HQ#
```

3-2) HQ-VPN

```
HQ-VPN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN(config)#int f0/1
HQ-VPN(config-if)#no sh
HQ-VPN(config-if)#ip add 10.1.12.
*Mar  1 00:31:22.171: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:31:23.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
up
HQ-VPN(config-if)#ip add 10.1.12.2 255.255.255.252
HQ-VPN(config-if)#no sh
HQ-VPN(config-if)#exit
```

```
HQ-VPN(config)#int f0/0
HQ-VPN(config-if)#no sh
HQ-VPN(config-if)#ip add 1.1.100.1 2
*Mar  1 00:31:41.731: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:31:42.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
up
HQ-VPN(config-if)#ip add 1.1.100.1 255.255.255.252
HQ-VPN(config-if)#no sh
HQ-VPN(config-if)#end
HQ-VPN#wr
Building configuration...
```

3-3) ISP

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#int f0/0
ISP(config-if)#no sh
ISP(config-if)#ip add 1.1.
*Mar  1 00:34:55.535: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:34:56.535: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
up
ISP(config-if)#ip add 1.1.100.2 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
ISP(config)#
```

```
ISP(config)#int f0/1
ISP(config-if)#no sh
ISP(config-if)#ip add
*Mar  1 00:35:46.099: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:35:47.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, c
up
ISP(config-if)#ip add 1.1.100.5 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#exit
```

```
ISP(config)#int f1/0
ISP(config-if)#no sh
ISP(config-if)#ip add 1.1.100.9
*Mar  1 00:36:48.175: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar  1 00:36:49.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
up
ISP(config-if)#ip add 1.1.100.9 255.255.255.252
ISP(config-if)#no sh
ISP(config-if)#end
ISP#wr
Building configuration...
[OK]
```

3-4) Branch1

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#int f0/0
Branch1(config-if)#no sh
Branch1(config-if)#ip add 1.1.100.
*Mar  1 00:38:05.839: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:38:06.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
up
Branch1(config-if)#ip add 1.1.100.6 255.255.255.252
Branch1(config-if)#no sh
Branch1(config-if)#exit
```

```
Branch1(config)#int f0/1
Branch1(config-if)#no sh
Branch1(config-if)#ip add 10.2.2.2
*Mar  1 00:38:57.855: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:38:58.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, ch
up
Branch1(config-if)#ip add 10.2.2.2 255.255.255.0
Branch1(config-if)#end
Branch1#wr
Building configuration...
[OK]
```

3-5) Branch2

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#int f0/0
Branch2(config-if)#no sh
Branch2(config-if)#ip add 1.1.100.10
*Mar  1 00:40:38.403: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:40:39.403: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
up
Branch2(config-if)#ip add 1.1.100.10 255.255.255.252
Branch2(config-if)#exit
```

```
Branch2(config)#int f0/1
Branch2(config-if)#no sh
Branch2(config-if)#ip add 10.3.3
*Mar  1 00:41:28.295: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:41:29.295: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
up
Branch2(config-if)#ip add 10.3.3.3 255.255.255.0
Branch2(config-if)#end
Branch2#wr
Building configuration...

*Mar  1 00:41:34.775: %SYS-5-CONFIG I: Configured from console by console[OK]
```

4) ping 보내서 ip 할당 잘 되었는지 확인하기

- HQ: ping 10.1.12.2
- HQ-VPN: ping 1.1.100.2
- ISP: ping 1.1.100.6, ping 1.1.100.10

2. OSPF 라우팅 설정하기

1) HQ

```
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#router ospf 1
HQ(config-router)#router-id 1.1.1.1
HQ(config-router)#network 10.1.1.1 0.0.0.0 area 0
HQ(config-router)#network 10.1.12.1 0.0.0.0 area 0
HQ(config-router)#end
HQ#wr
Building configuration...
[OK]
```

router-id 1.1.1.1 : Router ID를 1.1.1.1로 수동 설정하는 것

2) HQ-VPN

```
HQ-VPN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN(config)#router ospf 1
HQ-VPN(config-router)#router-id 4.4.4.4
HQ-VPN(config-router)#network 10.1.12.2 0.0.0.0 area 0
HQ-VPN(config-router)#
*Mar  1 01:26:24.131: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/1 f
ading Done
HQ-VPN(config-router)#default-information originate always
HQ-VPN(config-router)#exit
HQ-VPN(config)#
HQ-VPN(config)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.2
HQ-VPN(config)#end
HQ-VPN#wr
```

- **default-information originate always**

  : 기본 경로(default route) 정보를 생성하도록 라우터에 지시

  - `**default-information**`: 기본 경로 정보를 의미합니다.
  - `**originate**`: 해당 라우터에서 기본 경로 정보를 생성하라는 명령입니다.
  - `**always**`: 항상 기본 경로 정보를 생성하라는 옵션입니다.

- **ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.2**

  : 모든 트래픽을 f0/0 인터페이스를 통해 1.1.100.2로 보내는 기본 경로를 설정하는 것

3) Branch1

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.5
Branch1(config)#end wr
                   ^
% Invalid input detected at '^' marker.

Branch1(config)#end
Branch1#wr
```

- **ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.5** : 마찬가지로 ISP 쪽으로 Default 설정

4) Branch2

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.9
Branch2(config)#end
Branch2#wr
```

- **ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.9** : 마찬가지로 ISP 쪽으로 Default 설정

3. Tunnel 뚫고 개통하기

• 1.1.100.x 대역은 인터넷(공인) 대역임 → 사설과 사설 간의 Tunnel을 뚫어야 함

1) HQ-VPN에서 Tunnel 뚫기

1-1) Tunnel 1 (H1-VPN →Branch1)

```
HQ-VPN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN(config)#int tunnel 1
HQ-VPN(config-if)#ip add
*Mar  1 01:49:42.611: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
HQ-VPN(config-if)#ip add 10.10.10.1 255.255.255.252
HQ-VPN(config-if)#tunnel source 1.1.100.1
HQ-VPN(config-if)#tunnel destination 1.1.100.6
HQ-VPN(config-if)#tunnel mode gre i
*Mar  1 01:50:09.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
HQ-VPN(config-if)#tunnel mode gre ip
```

• **tunnel mode gre ip** : 라우터 간에 GRE 터널 설정할 때 사용하는 명령어

> **참고) GRE 터널**
>
> • Generic Routing Encapsulation
>
> • 현재 인터페이스가 GRE 터널로 설정되며, 이 터널을 통해 IP 패킷이 캡슐화되어 전송됨을 의미하는 명령어

1-2) Tunnel 2 (H1-VPN →Branch2)

```
HQ-VPN(config)#int tunnel 2
HQ-VPN(config-if)#ip add 10.1
*Mar  1 01:59:07.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to down
HQ-VPN(config-if)#ip add 10.10.10.5 255.255.255.252
HQ-VPN(config-if)#tunnel source 1.1.100.1
HQ-VPN(config-if)#tunnel destination 1.1.100.10
HQ-VPN(config-if)#tu
*Mar  1 01:59:53.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up
HQ-VPN(config-if)#tunnel mode gre ip
HQ-VPN(config-if)#exit
```

1-3) 공인 대역에서 OSPF 넣기

```
HQ-VPN(config)#router ospf 1
HQ-VPN(config-router)#network 10.10.10.1 0.0.0.0 area 0
HQ-VPN(config-router)#network 10.10.10.5 0.0.0.0 area 0
HQ-VPN(config-router)#end
HQ-VPN#wr
Building configuration...
```

2) Branch1, Branch2에서 Tunnel 개통하기

2-1) Branch 1에서 Tunnel 개통하기

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#int tunnel 1
Branch1(config-if)#ip add 10.10.10.2
*Mar  1 02:09:19.035: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
Branch1(config-if)#ip add 10.10.10.2 255.255.255.252
Branch1(config-if)#tunnel source 1.1.100.6
Branch1(config-if)#tunnel destination 1.1.100.1
Branch1(config-if)#tunnel mode gre ip
*Mar  1 02:10:34.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
Branch1(config-if)#tunnel mode gre ip
Branch1(config-if)#exit
```

2-2) Branch 1에서 OSPF 설정하기

• Tunnel 1 & f0/1의 ip를 넣음

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#router ospf 1
Branch1(config-router)#router-id 2.2.2.2
Branch1(config-router)#network 10.10.10.2 0.0.0.0 area 0
Branch1(config-router)#network
*Mar  1 02:13:47.147: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Tunnel1 fro
ne
Branch1(config-router)#network 10.2.2.2 0.0.0.0 area 0
Branch1(config-router)#
```

2-3) Branch 2에서 Tunnel 개통하기

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#int tunnel
% Incomplete command.

Branch2(config)#int tunnel 2
Branch2(config-if)#ip add 10
*Mar  1 02:15:49.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to dow
Branch2(config-if)#ip add 10.10.10.6 255.255.255.252
Branch2(config-if)#tunnel source 1.1.100.10
Branch2(config-if)#tunnel destination 1.1.100.1
Branch2(config-if)#tunnel mode
*Mar  1 02:16:22.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up
Branch2(config-if)#tunnel mode gre ip
Branch2(config-if)#exit
```

2-4) Branch 2에서 OSPF 설정하기

```
Branch2(config)#router ospf 1
Branch2(config-router)#router-id 3.3.3.3
Branch2(config-router)#network 10.10.10.6 0.0.0.0 area 0
Branch2(config-router)#network 1
*Mar  1 02:18:02.735: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Tunnel2 from LOADING to FULL, Loading Do
ne
Branch2(config-router)#network 10.3.3.3 0.0.0.0 area 0
Branch2(config-router)#end
Branch2#wr
Building configuration...
[OK]
```

3) 결과 확인하기

• 지금까지의 설정으로 Tunnel을 통해 Neighbor가 맺어진 것을 확인하기

show ip ospf nei : OSPF 프로토콜 이웃의 상태를 보여주는 명령어,

OSPF 이웃들의 상태, IP 주소, 인터페이스 등의 정보가 표시됨

```
HQ-VPN#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:37    10.10.10.6      Tunnel2
2.2.2.2           0   FULL/  -        00:00:38    10.10.10.2      Tunnel1
1.1.1.1           1   FULL/DR         00:00:37    10.1.12.1       FastEthernet0/1
```

```
Branch1#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           0   FULL/  -        00:00:36    10.10.10.1      Tunnel1
```

```
Branch2#show ip ospf nei

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           0   FULL/  -        00:00:36    10.10.10.5      Tunnel2
```

4. GRE 프로토콜을 사용해 VPN 구축하기

1) IPSec 구성하기

• IKE Phase 1 (ISAKMP SA)

vpn 장비 간 사용할 인증키 (Authentication)	pre-share
암호화 방식 지정 (Encryption)	AES
무결성 확인	SHA
키 교환 방식 (Diffie-Hellman)	group2
보안 정책 적용 기간 (life-time)	7200

• IKE Phase 2 (IPSEC SA)

Mode	Tunnel
암호화 방식 지정 (Encryption)	AES
무결성 확인	SHA
보호 대상	GRE Tunnel 트래픽

1-1) HQ-VPN

```
HQ-VPN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN(config)#crypto isakmp policy 1
HQ-VPN(config-isakmp)#authentication pre-share
HQ-VPN(config-isakmp)#encryption aes
HQ-VPN(config-isakmp)#hash sha
HQ-VPN(config-isakmp)#group 2
HQ-VPN(config-isakmp)#lifetime 7200
HQ-VPN(config-isakmp)#exit
```

```
HQ-VPN(config)#crypto isakmp key cisco123 address 1.1.100.6
HQ-VPN(config)#crypto isakmp key cisco123 address 1.1.100.10
```

crypto isakmp //IKE 설정을 위한 명령어

key {공유키} //사용할 사전 공유키(pre-shared key) 설정

address {상대방의 IP 주소} //키 교환을 수행할 상대방의 IP 주소 지정

```
HQ-VPN(config)#crypto ipsec transform-set IPSEC_SA esp-aes esp-sha-hmac
HQ-VPN(cfg-crypto-trans)#mode tunnel
HQ-VPN(cfg-crypto-trans)#exit
```

crypto ipsec transform-set {이름} //IPsec transform set의 이름 지정

esp-aes //암호화 알고리즘으로 AES를 사용

esp-sha-hmac //해시 알고리즘으로 SHA 및 HMAC를 사용(데이터 무결성 검증에 사용됨)

• Access-list 만들기

```
HQ-VPN(config)#ip access-list extend HQ->Branch1
HQ-VPN(config-ext-nacl)#permit gre host 1.1.100.1 host 1.1.100.6
HQ-VPN(config-ext-nacl)#exit
HQ-VPN(config)#
HQ-VPN(config)#ip access-list extend HQ->Branch2
HQ-VPN(config-ext-nacl)#permit gre host 1.1.100.1 host 1.1.100.10
HQ-VPN(config-ext-nacl)#exit
```

ip access-list extend {목록 이름} //확장된 ip 접근 목록(extended ip acl) 설정 명령어

• Crypto map 만들기

```
HQ-VPN(config-crypto-map)#crypto map VPN_T 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
HQ-VPN(config-crypto-map)#match address HQ->Branch1
HQ-VPN(config-crypto-map)#set transform-set IPSEC_SA
HQ-VPN(config-crypto-map)#set peer 1.1.100.6
HQ-VPN(config-crypto-map)#exit
```

crypto map {이름} {시퀀스 번호} ipsec-isakmp //Crypto Map 생성&시퀀스 번호 지정

set peer {상대방 ip} //VPN 터널의 상대방 IP 주소 설정

```
HQ-VPN(config)#crypto map VPN_T 2 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
HQ-VPN(config-crypto-map)#match address HQ->Branch2
HQ-VPN(config-crypto-map)#set transform-set IPSEC_SA
HQ-VPN(config-crypto-map)#set peer 1.1.100.10
HQ-VPN(config-crypto-map)#exit
```

```
HQ-VPN(config)#int f0/0
HQ-VPN(config-if)#crypto map VPN_T
HQ-VPN(config-if)#end
HQ-VPN#
*Mar  1 04:44:24.270: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HQ-VPN#
*Mar  1 04:44:25.178: %SYS-5-CONFIG_I: Configured from console b
HQ-VPN#wr
Building configuration...
[OK]
```

1-2) Branch1

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#crypto isakmp policy 1
Branch1(config-isakmp)#authentication pre-share
Branch1(config-isakmp)#encryption aes
Branch1(config-isakmp)#hash sha
Branch1(config-isakmp)#group 2
Branch1(config-isakmp)#lifetime 7200
Branch1(config-isakmp)#exit
Branch1(config)#
Branch1(config)#crypto isakmp key cisco123 address 1.1.100.1
Branch1(config)#
Branch1(config)#crypto ipsec transform-set IPSEC_SA esp-aes esp-sha-hmac
```

• Access-list 만들기

```
Branch1(cfg-crypto-trans)#ip access-list extended Branch1->HQ
Branch1(config-ext-nacl)#permit gre host 1.1.100.6 host 1.1.100.1
Branch1(config-ext-nacl)#exit
```

```
Branch1(config)#crypto map VPN_T 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Branch1(config-crypto-map)#match address Branch1->HQ
Branch1(config-crypto-map)#set tansfor-set IPSEC_SA
                                ^
% Invalid input detected at '^' marker.

Branch1(config-crypto-map)#set tansform-set IPSEC_SA
                                ^
% Invalid input detected at '^' marker.

Branch1(config-crypto-map)#set transform-set IPSEC_SA
Branch1(config-crypto-map)#set peer 1.1.100.1
Branch1(config-crypto-map)#exit
```

```
Branch1(config)#int f0/0
Branch1(config-if)#crypto map VPN_T
Branch1(config-if)#end
Branch1#w
*Mar  1 04:52:49.486: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Branch1#wr
Building configuration...
[OK]
```

1-3) 확인하기

- Branch1 : **ping 10.1.1.1 source f0/1**

```
Branch1#ping 10.1.1.1 source f0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.2.2.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/93/
```

- HQ-VPN : **show crypto isakmp sa**

```
HQ-VPN#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
1.1.100.1       1.1.100.6       QM_IDLE           1001    0 ACTIVE
1.1.100.10      1.1.100.1       MM_NO_STATE          0    0 ACTIVE (deleted)
```

1-4) Branch2

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#cryto isakmp policy 1
               ^
% Invalid input detected at '^' marker.

Branch2(config)#crypto isakmp policy 1
Branch2(config-isakmp)#authentication pre-share
Branch2(config-isakmp)#encryption aes
Branch2(config-isakmp)#hash sha
Branch2(config-isakmp)#group 2
Branch2(config-isakmp)#lifetime 7200
Branch2(config-isakmp)#exit
```

```
Branch2(config)#crypto isakmp key cisco123 address 1.1.100.1
Branch2(config)#
Branch2(config)#crypto ipsec transfor-set IPSEC_SA esp-aes esp-sha-hmac
                               ^
% Invalid input detected at '^' marker.

Branch2(config)#crypto ipsec transform-set IPSEC_SA esp-aes esp-sha-hmac
```

- Access-list 만들기

```
Branch2(cfg-crypto-trans)#ip access-list extended Branch2->HQ
Branch2(config-ext-nacl)#permit gre host 1.1.100.10 host 1.1.100.1
Branch2(config-ext-nacl)#exit
```

```
Branch2(config)#crypto map VPN_T 1 ipsec-isakmp
Branch2(config-crypto-map)#match address Branch2->HQ
Branch2(config-crypto-map)#set transfor-set IPSEC_sA
                                            ^
% Invalid input detected at '^' marker.

Branch2(config-crypto-map)#set transform-set IPSEC_SA
Branch2(config-crypto-map)#set peer 1.1.100.1
Branch2(config-crypto-map)#exit
```

```
Branch2(config)#int f0/0
Branch2(config-if)#crypto map VPN_T
Branch2(config-if)#end
Branch2#wr
*Mar  1 05:27:57.542: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Branch2#wr
Building configuration...
[OK]
```

• ping 통신으로 확인하기

```
Branch2#ping 10.1.1.1 source f0/1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.3.3.3
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/94/
```

1-3) 확인하기

• HQ-VPN

```
HQ-VPN#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
1.1.100.1       1.1.100.6       QM_IDLE           1001    0 ACTIVE
1.1.100.1       1.1.100.10      QM_IDLE           1002    0 ACTIVE
```

```
HQ-VPN#show ip ospf ne

Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:31    10.10.10.6      Tunnel2
2.2.2.2           0   FULL/  -        00:00:35    10.10.10.2      Tunnel1
1.1.1.1           1   FULL/DR         00:00:36    10.1.12.1       FastEthernet0/1
```

2) 결과 확인하기

• Branch1 → HQ

```
Branch1#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/94
```

• HQ → Branch1

```
HQ#PING 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/92/104 ms
```

• Branch2 → HQ

```
Branch2#PING 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/95/12
```

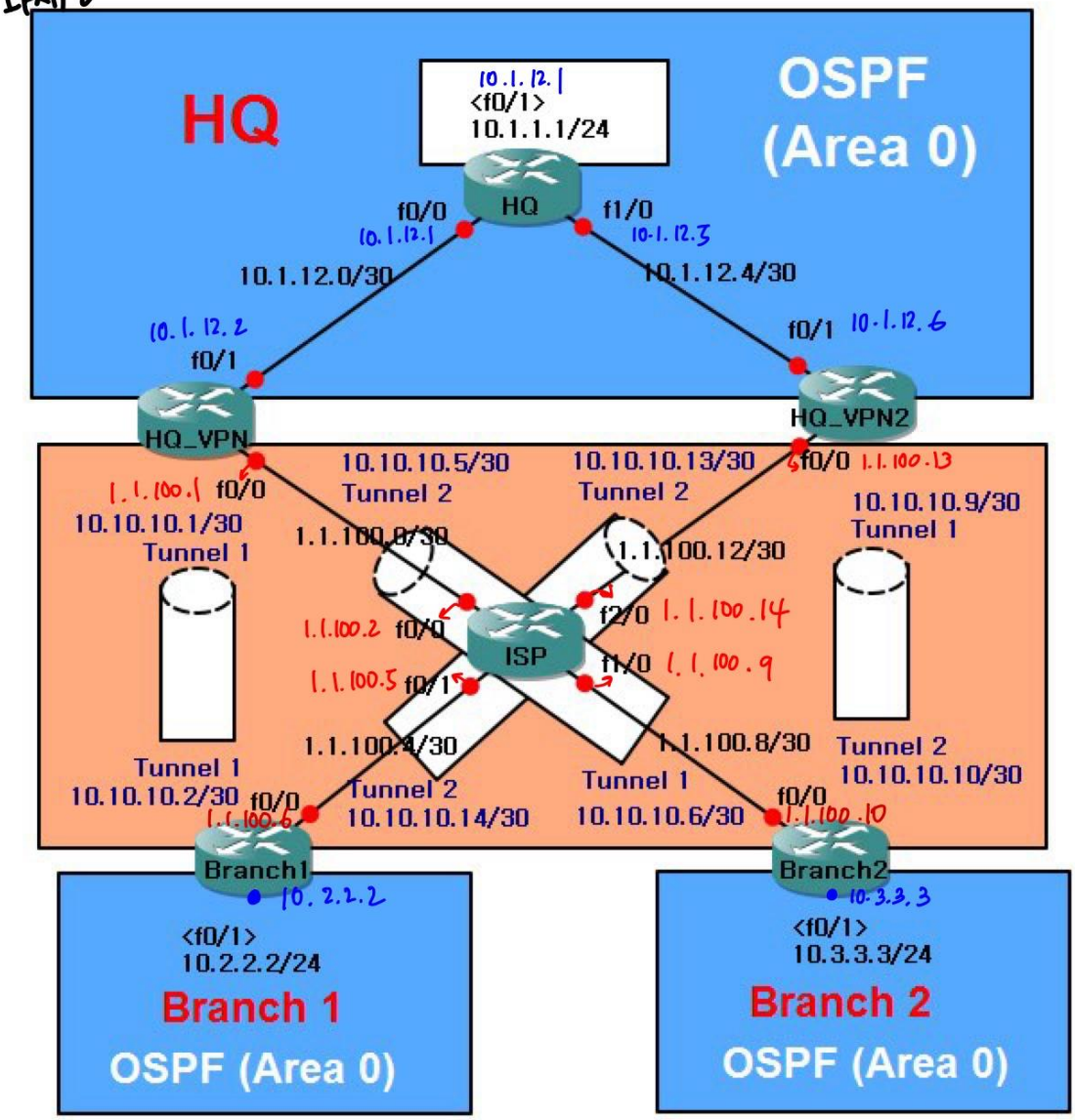
• HQ →Branch2

```
HQ#ping 10.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/92/
```

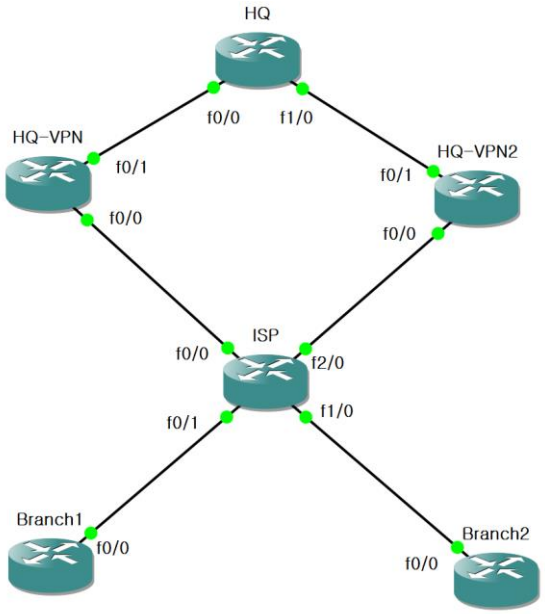
Ⅲ. 실습 2번

과제2



1. 환경 구성

1) 다음과 같이 GNS로 환경 구성하기



2) 모든 라우터에 다음을 입력하기

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#no ip domain lookup
Branch1(config)#line c 0
Branch1(config-line)#logg sy
Branch1(config-line)#exec-timeout 0
Branch1(config-line)#exit
Branch1(config)#line vty 0 4
Branch1(config-line)#pass cisco
Branch1(config-line)#end
Branch1#wr
Building configuration...
[OK]
```

3) ip 할당하기

```
HQ#show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.12.1       YES manual up                    up
FastEthernet0/1            10.1.1.1        YES manual up                    up
FastEthernet1/0            10.1.12.5       YES manual up                    up
```

```
HQ-VPN(config)#do show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            1.1.100.1       YES manual up                    up
FastEthernet0/1            10.1.12.2       YES manual up                    up
```

```
HQ-VPN2(config)#do show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            1.1.100.13      YES manual up                    up
FastEthernet0/1            10.1.12.6       YES manual up                    up
```

```
ISP#show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            1.1.100.2       YES manual up                    up
FastEthernet0/1            1.1.100.5       YES manual up                    up
FastEthernet1/0            1.1.100.9       YES manual up                    up
FastEthernet2/0            1.1.100.14      YES manual up                    up
ISP#
```

```
Branch1(config)#do show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            1.1.100.6       YES manual up                    up
FastEthernet0/1            10.2.2.2        YES manual up                    up
```

```
Branch2(config)#do show ip int b
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            1.1.100.10      YES manual up                    up
FastEthernet0/1            10.3.3.3        YES manual up                    up
```

2. Tunnel 만들기

• HQ-VPN → Branch1

```
HQ-VPN(config-router)#int tunnel 1
HQ-VPN(config-if)#ip add 10.
*Mar  1 00:43:06.407: %LINEPROTO-5-UPDOWN: Line protocol on
HQ-VPN(config-if)#ip add 10.10.10.1 255.255.255.252
HQ-VPN(config-if)#tunnel source 1.1.100.1
HQ-VPN(config-if)#tunnel destination 1.1.100.6
HQ-VPN(config-if)#exut
                  ^
% Invalid input detected at '^' marker.

HQ-VPN(config-if)#exit
```

• HQ-VPN → Branch2

```
HQ-VPN(config)#int tunnel 2
HQ-VPN(config-if)#
*Mar  1 00:43:58.827: %LINEPROTO-5-UPDOWN: Line protocol on
HQ-VPN(config-if)#ip add 10.10.10.5 255.255.255.252
HQ-VPN(config-if)# tunnel source 1.1.100.1
HQ-VPN(config-if)#tunnel destination 1.1.100.10
HQ-VPN(config-if)#end
HQ-VPN#wr
Building configuration...
[OK]
```

• HQ-VPN 2 → Branch1

```
HQ-VPN2(config)#int tunnel 3
HQ-VPN2(config-if)#
*Mar  1 00:46:24.663: %LINEPROTO-5-UPDOWN: Line protocol o
HQ-VPN2(config-if)# ip add 10.10.10.13 255.255.255.252
HQ-VPN2(config-if)#tunnel source 1.1.100.13
HQ-VPN2(config-if)#tunnel destination 1.1.100.6
HQ-VPN2(config-if)#exit
```

• HQ-VPN 2 → Branch2

```
HQ-VPN2(config)#int tunnel 4
HQ-VPN2(config-if)#
*Mar  1 00:47:43.439: %LINEPROTO-5-UPDOWN: Line protoc
HQ-VPN2(config-if)#ip add 10.10.10.9 255.255.255.252
HQ-VPN2(config-if)#tunnel source 1.1.100.13
HQ-VPN2(config-if)#tunnel destination 1.1.100.10
HQ-VPN2(config-if)#end
HQ-VPN2#wr
```

• Branch1 → HQ-VPN

```
Branch1(config)#int tunnel 1
Branch1(config-if)#
*Mar  1 00:49:27.747: %LINEPROTO-5-UPDOWN: Line protocol on
Branch1(config-if)#ip add 10.10.10.2 255.255.255.252
Branch1(config-if)#tunnel source 1.1.100.6
Branch1(config-if)#tunnel destination 1.1.100.1
Branch1(config-if)#exit
```

• Branch2 → HQ-VPN2

```
Branch1(config)#int tunnel 3
Branch1(config-if)#
*Mar  1 00:49:58.283: %LINEPROTO-5-UPDOWN: Line p
Branch1(config-if)#ip add 10.10.10.14 255.255.255
Branch1(config-if)#
Branch1(config-if)#tunnel source 1.1.100.6
Branch1(config-if)#tunnel destination 1.1.100.13
Branch1(config-if)#end
Branch1#wr
Building configuration...
```

• Branch2 → HQ-VPN

```
Branch2(config)#int tunnel 2
Branch2(config-if)#
*Mar  1 00:51:20.267: %LINEPROTO-5-UPDOWN: Line pro
Branch2(config-if)#ip add 10.10.10.6 255.255.255.25
Branch2(config-if)#tunnel source 1.1.100.10
Branch2(config-if)#tunnel destination 1.1.100.1
Branch2(config-if)#exit
```

• Branch2 → HQ-VPN2

```
Branch2(config)#int tunnel 4
Branch2(config-if)#
*Mar  1 00:51:44.715: %LINEPROTO-5-UPDOWN: Line pr
Branch2(config-if)#ip add 10.10.10.10 255.255.255.
Branch2(config-if)#tunnel source 1.1.100.10
Branch2(config-if)#tunnel destination 1.1.100.13
Branch2(config-if)#end
Branch2#wr
Building configuration...
[OK]
```

3. OSPF 라우팅 설정하기

```
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#router ospf 1
HQ(config-router)#router-id 1.1.1.1
HQ(config-router)#network 10.1.1.1 0.0.0.0 area 0
HQ(config-router)#network 10.1.12.1 0.0.0.0 area 0
HQ(config-router)#network 10.1.12.5 0.0.0.0 area 0
HQ(config-router)#end
HQ#wr
Building configuration...
```

```
HQ-VPN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN(config)#router ospf 1
HQ-VPN(config-router)#network 10.1.12.2 0.0.0.0 area 0
HQ-VPN(config-router)#network 10.10.10.1 0.0.0.0 area 0
HQ-VPN(config-router)#network 10.10.10.5 0.0.0.0 area 0
HQ-VPN(config-router)#
HQ-VPN(config-router)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.2
```

- ISP 쪽으로 Default 설정하기

```
HQ-VPN2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN2(config)#router ospf 1
HQ-VPN2(config-router)#router-id 5.5.5.5
HQ-VPN2(config-router)#network 10.1.12.6 0.0.0.0 area 0
HQ-VPN2(config-router)#
*Mar  1 00:56:15.115: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/1 from LOADING to F
ading Done
HQ-VPN2(config-router)#network 10.10.10.13 0.0.0.0 area 0
HQ-VPN2(config-router)#network 10.10.10.9 0.0.0.0 area 0
HQ-VPN2(config-router)#
HQ-VPN2(config-router)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.14
HQ-VPN2(config)#end
HQ-VPN2#wr
```

- ISP 쪽으로 Default 설정하기

```
Branch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch1(config)#router ospf
% Incomplete command.

Branch1(config)#router ospf 1
Branch1(config-router)#router-id 2.2.2.2
Branch1(config-router)#network 10.10.10.2 0.0.0.0 area 0
Branch1(config-router)#network 10.10.10.14 0.0.0.0 area 0
Branch1(config-router)#network 10.2.2.2 0.0.0.0 area 0
Branch1(config-router)#exit
Branch1(config)#
Branch1(config)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.5
Branch1(config)#end
Branch1#wr
```

- ISP 쪽으로 Default 설정하기

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#router ospf 1
Branch2(config-router)#router-id 3.3.3.3
Branch2(config-router)#network 10.10.10.6 0.0.0.0 area 0
Branch2(config-router)#network 10.10.10.10 0.0.0.0 area 0
Branch2(config-router)#network 10.3.3.3 0.0.0.0 area 0
Branch2(config-router)#exit
Branch2(config)#
Branch2(config)#ip route 0.0.0.0 0.0.0.0 f0/0 1.1.100.9
```

- ISP 쪽으로 Default 설정하기

3. VPN 터널 암호화

- 실습 1에서 했던 방식처럼 진행하면 됨

```
HQ-VPN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ-VPN(config)#crypto isakmp policy 10
HQ-VPN(config-isakmp)#encr
HQ-VPN(config-isakmp)#encryption aes 256
HQ-VPN(config-isakmp)#hash sha
HQ-VPN(config-isakmp)#authentication pre-share
HQ-VPN(config-isakmp)#group 5
HQ-VPN(config-isakmp)#life time 3600
                           ^
% Invalid input detected at '^' marker.

HQ-VPN(config-isakmp)#exit
HQ-VPN(config)#crypto isakmp policy 10
HQ-VPN(config-isakmp)#lifetime 3600
HQ-VPN(config-isakmp)#exit
```


- 결과

```
HQ-VPN(config-if)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
1.1.100.10      1.1.100.1       MM_NO_STATE          0    0 ACTIVE
1.1.100.1       1.1.100.6       QM_IDLE           1001    0 ACTIVE
```

```
HQ-VPN2(config-if)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
1.1.100.13      1.1.100.6       QM_IDLE           1001    0 ACTIVE
1.1.100.10      1.1.100.13      MM_NO_STATE          0    0 ACTIVE
1.1.100.10      1.1.100.13      MM_NO_STATE          0    0 ACTIVE (deleted)
```

```
Branch1(config-if)#do sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
1.1.100.1       1.1.100.6       QM_IDLE           1001    0 ACTIVE
1.1.100.13      1.1.100.6       QM_IDLE           1002    0 ACTIVE
```

```
Branch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch2(config)#do show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

- 아무것도 뜨지 않는다,,, 설정을 잘못 했나보다..

참고자료

https://selene0301.tistory.com/64

https://nirsa.tistory.com/32

https://ddongwon.tistory.com/62

https://pyromaniac.me/44

https://ddongwon.tistory.com/62