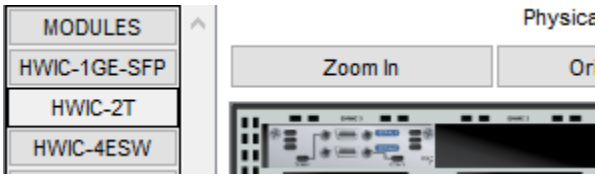
패킷트레이서 풀이

- HWIC-2T 모듈

2901 Router 의 전원을 꺼준 뒤 Physical 에서 일치하는 이름의 모듈을 넣어주면 된다.



HWIC-2T 모듈은 시리얼 연결(빨간 번개모양 선)을 해주기 위한 모듈이다.

- License Security 문구 확인 관련

과제에서 요구하는 VPN 설정을 위해서는 license 를 추가해주어야 한다. Conf t 모드에서 다음과 같이 진행해주면 된다.

license boot module c2900 technology-package securityk9

참고로 위 명령어에서 절반 이상은 tab 을 통해서 자동완성 할 수 있다. 실제로 입력할 때는 아래와 같이 하면 된다.

license [tab] [tab] [tab] [tab] secu[tab]

위 명령어를 입력했을 때 다음과 같은 내용이 출력되어야 정상적으로 진행되고 있는 것이다.

Activation of the software command line interface will be evidence of
your acceptance of this agreement.

ACCEPT? [yes/no]:

위 내용 외에 아마 많은 내용이 뜰텐데 맨 밑에 내용만 주목하면 된다. Yes 입력 후 Enter 를 눌러주면 된다. 그 다음 do wr 로 저장 후 reload 해주면 된다.

Reload 후 show run 했을 때 다음과 같은 내용이 있으면 정상적으로 적용된 것이다.

license boot module c2900 technology-package securityk9

- IPSec VPN

IPSec VPN 을 설정하기 위한 단계는 총 5 단계로 구분할 수 있다.

1. VPN tunnel 을 사용할 클라이언트 대역을 지정하는 ACL

2. ISAKMP policy, ISAKMP key

3. IPSec Transform-set

4. Crypto map

5. interface 에 적용

설정 진행의 경우 아래 영상을 참고로 진행되었다.

https://www.youtube.com/watch?v=Z7LwU6H5IGE&ab_channel=danscourses

먼저 첫 번째 단계인 ACL 이다.

ACL 을 지정하는 이유는 어떤 네트워크 대역이 VPN tunnel 을 통과할 지 지정하기 위해서 사용한다. 예를 들어, 192.168.1.0/24 대역이 VPN 을 사용해야 하면 ACL 을 아래와 같이 적용할 수 있다.

access-list <번호 혹은 이름> permit ip <출발 대역> <출발대역 와일드카드 마스크> <목적지 대역> <목적지 대역 와일드카드 마스크>

대역은 문제에 맞게 설정해주면 되고 ACL 번호나 이름은 문제지에서 제공된다면 해당되는 것을 사용하면 된다. 반대쪽 VPN Router 에서는 출발 대역과 목적지 대역을 반대로하여 작성해주면 된다.

다음으로 ISAKMP policy 를 설정해야 한다.

설정 진입의 경우 아래와 같이 할 수 있다.

crypto isakmp policy <policy number>

policy number 는 곧 우선순위이며 번호가 클수록 우선순위가 높다고 하지만 그건 우선 신경쓸 필요 없다. 문제에서 지정해준 값이 있다면 그 값을 사용하면 된다. 설정으로 접속하면 상태가 (config-isakmp)# 으로 변경된 것을 확인할 수 있다.

```
Router(config-isakmp)#
```

이 모드에서 필수로 설정해야 할 값은 encryption, authentication, group 세 가지 항목이다.

encryption 은 어떤 암호화 알고리즘을 사용하여 통신할 것인지 지정하는 것이며 3des, aes, des 총 세 가지를 패킷트레이서에서 지원한다. 지정된 값이 있을 경우 해당 값을 사용하면 된다. 만약 aes 를 사용할 경우 뒤에 key size 도 지정해주어야 하는데 이는 128, 192, 256 중에 지정해줄 수 있다.

authentication 은 어떤 인증을 사용할 것인지 지정하는 부분인데 선택지가 pre-share 방식밖에 없다. 따라서 아래와 같이 입력해주면 된다.

authentication pre-share

다음으로 group 은 diffie-hellman group 을 지정하는 부분인데 옵션으로는 1, 2, 5 가 있다. 이 중에 문제에서 지정된 값이 있다면 그 값을 사용하면 된다. 이론이 중요한 것은 아니기에 그냥 하라는대로 하면 된다.

위 세 가지를 지정해줬으면 exit 를 눌러서 (config)#으로 나와주면 된다. 다음으로 authentication 에 pre-share key 를 사용하므로 해당 key 를 지정해주어야 한다. 명령어 형식은 다음과 같다.

crypto isakmp key <key string> address <상대방 router 주소>

key string 의 경우 문제에서 지정되는 값으로 해주면 되고 상대방 Router 주소는 사이버 보안 문제를 기준으로 VPN 라우터에서 설정한다고 가정했을 때 RVPN router 에서 사용하는 외부 인터페이스 주소를 지정해주면 된다.

반대쪽 라우터에서는 상대방 router 주소만 바꿔서 똑같이 해주면 된다.

세 번째로는 transform-set 을 지정해주어야 한다. 얘는 진짜 이론적인 부분이 너무 쎄다.. 문제에서 어떤 걸 쓰라고 지정해주길 바라는 게 좋을 것 같다. 명령어의 사용법은 다음과 같다.

Crypto ipsec transform-set <이름> [옵션]

네 번째로 위에서 설정한 것들을 종합하여 map 을 만들어 주어야 한다.

crypto map <map 이름> <sequence number> ipsec-isakmp

먼저 맨 처음에 지정했던 ACL 을 설정해주어야 한다.

match address <번호 혹은 이름>

아까 이름으로 설정했다면 이름, 번호로 설정했다면 번호를 설정해주면 된다.

그 다음으로는 peer 설정 즉, 상대방 라우터를 지정해주어야 한다.

set peer <상대 라우터 주소>

상대 라우터를 지정했으면 아까 설정한 transform-set 도 설정해주어야 한다.

set transfom-set <transform-set 이름>

필수적으로 설정해야 할 항목들은 위 세 가지가 끝이다. exit 를 입력해서 나온 뒤 설정을 적용할 인터페이스에 들어가서 다음과 같이 입력해주면 된다.

crypto map <map 이름>