**Create Certificate key using openssl**

**Domain 변경시 CN 부분(skills.변경 필요**

mkdir -p ~/myCA

cd ~/myCA

openssl genpkey -algorithm RSA -out ca.key -aes256

openssl req -new -x509 -days 3650 -key ca.key -out ca.crt -subj "/C=KR/ST=Seoul/L=Seoul/O=MyCompany/OU=IT/CN=skills.local"

# 서버 개인 키 생성

openssl genpkey -algorithm RSA -out server.key

# 서버 인증서 서명 요청(CSR) 생성

openssl req -new -key server.key -out server.csr -subj "/C=KR/ST=Seoul/L=Seoul/O=MyCompany/OU=IT/CN=server.skills.local"

# 서버 인증서를 CA로 서명

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 3650

# 클라이언트 개인 키 생성

openssl genpkey -algorithm RSA -out client1.key

# 클라이언트 인증서 서명 요청(CSR) 생성

openssl req -new -key client1.key -out client1.csr -subj "/C=KR/ST=Seoul/L=Seoul/O=MyCompany/OU=IT/CN=client1.skills.local"

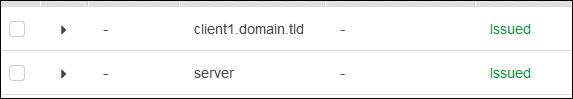
# 클라이언트 인증서를 CA로 서명

openssl x509 -req -in client1.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client1.crt -days 3650

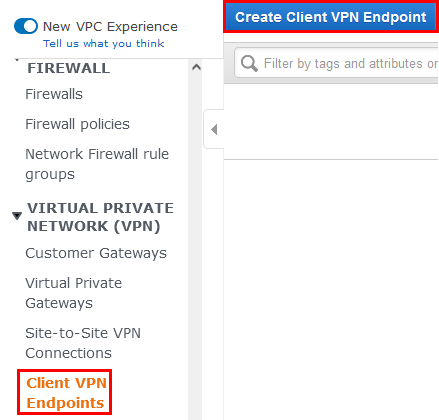
이제 사설에서 만든 OpenSSL 인증서를 AWS Certificate Manager로 가져오자

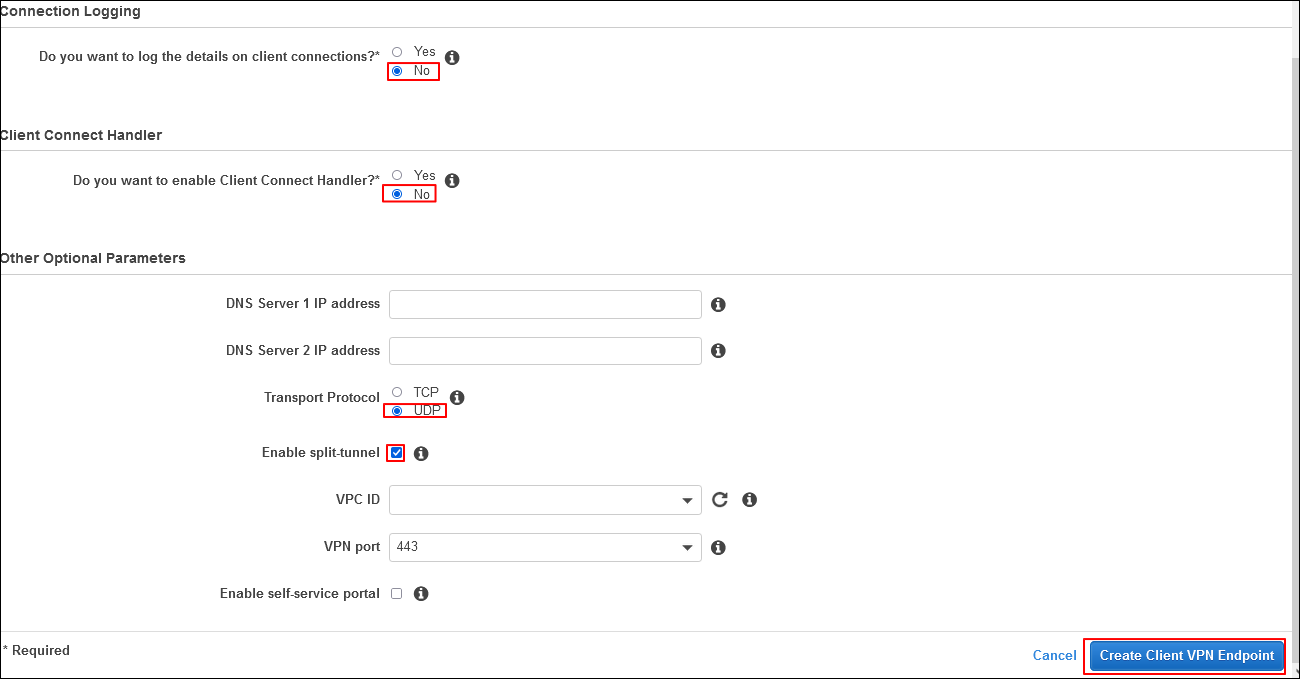
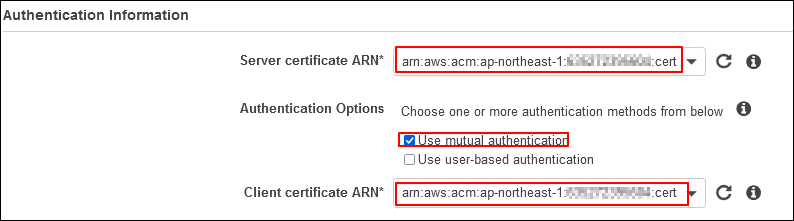
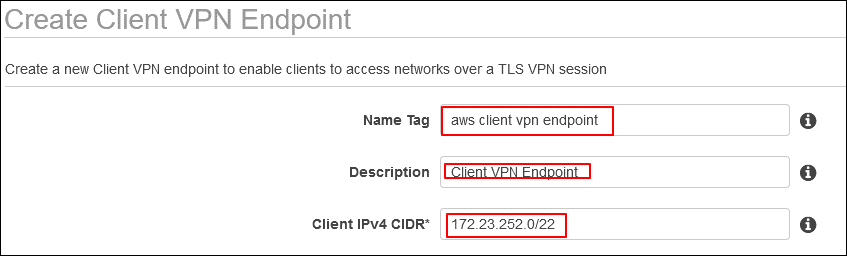
|  |
| --- |
| C:\certificate> aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key --certificate-chain fileb://ca.crt --regon ap-northeast-1  C:\certificate> aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt --regon ap-northeast-1 |

그러면 다음과 같이 인증서가 업로드 된 것을 알 수 있다.

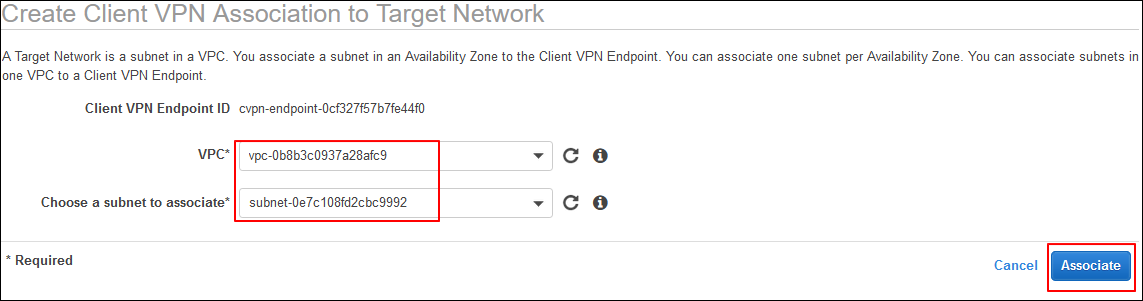
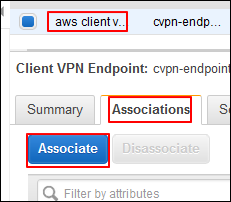


AWS Client VPN endpoint를 생성해주자.

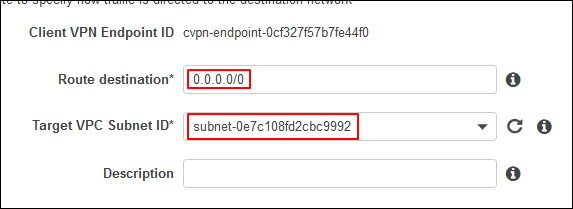
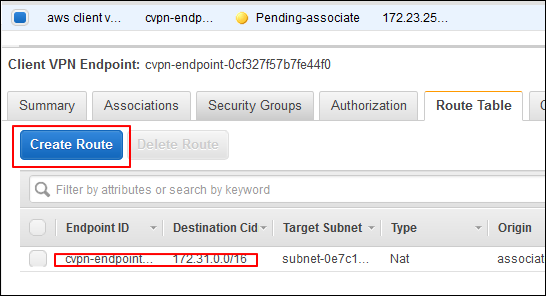




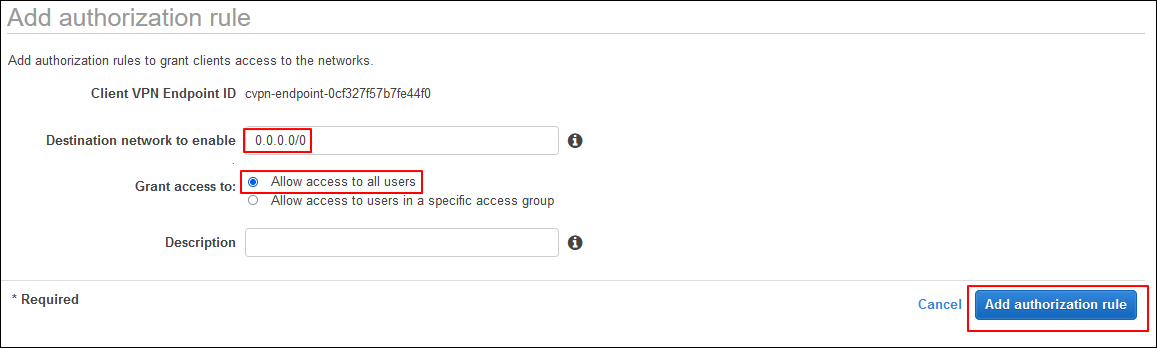
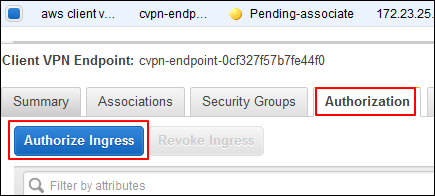
이제 VPC를 선택하고 연결할 Subnet을 추가하자



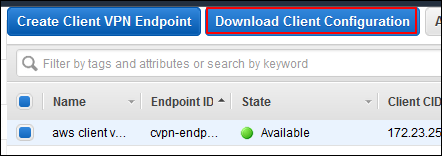
이제 Route를 설정 해주자.



그리고 이제 Authorization을 생성하자.



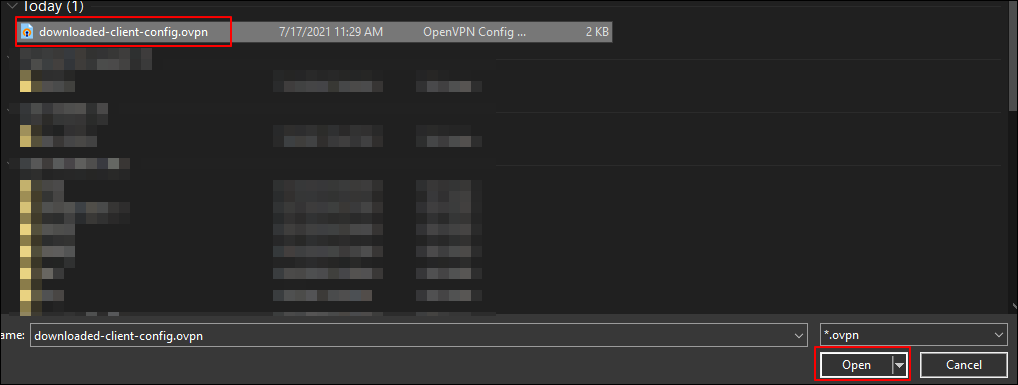
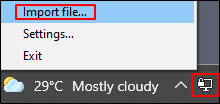
그리고 상태가 Pending-associate -> Availability 로 변경 되었으면 Download Client Configuration 버튼을 눌러 클라이언트 구성 파일(\*.ovpn)파일을 다운로드 해주자.



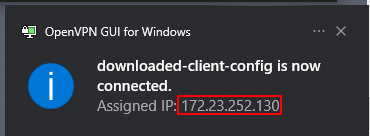
그리고 다운 받은 파일을 다음과 같이 수정해주자. (수정 된 부분을 빨간색으로 표시)

|  |
| --- |
| client  dev tun  proto udp  remote cvpn-endpoint-0cf327f57b7fe44f0.prod.clientvpn.ap-northeast-1.amazonaws.com 443  remote-random-hostname  resolv-retry infinite  nobind  remote-cert-tls server  cipher AES-256-GCM  verb 3  <ca>  -----BEGIN CERTIFICATE-----  <---- 생략 ---->  -----END CERTIFICATE-----  </ca>  <cert>  -----BEGIN CERTIFICATE-----  <Client 인증서의 crt 또는 cert파일>  -----END CERTIFICATE-----  </cert>  <key>  -----BEGIN PRIVATE KEY-----  <Client 인증서의 Key>  -----END PRIVATE KEY-----  </key>  reneg-sec 0 |

이런 식으로 수정 한 뒤 OpenVPN Client로 접속을 해주자.



그리고 다시 아이콘을 더블 클릭하면 다음과 같이 연결이 된다

  
그리고 AWS Management Console창에서 봐도 연결이 됬다고 나온다.

