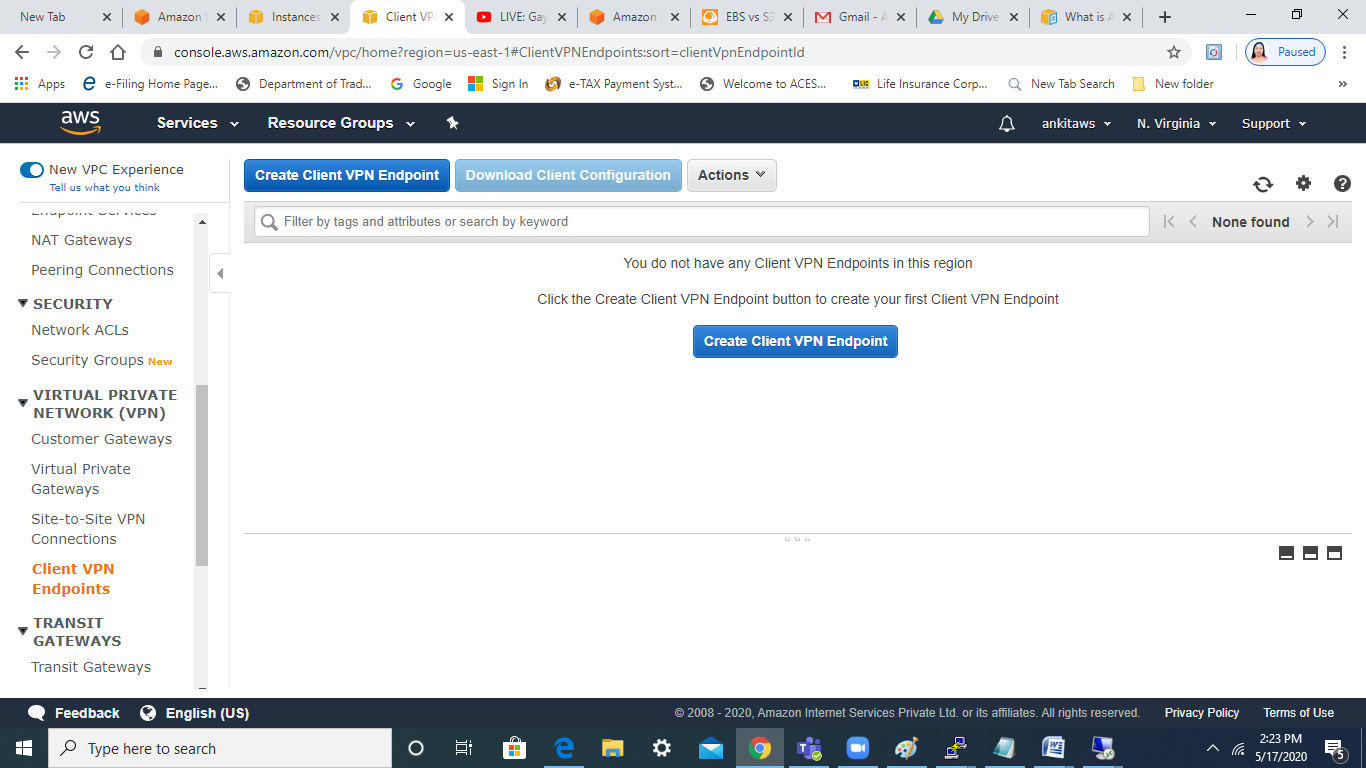
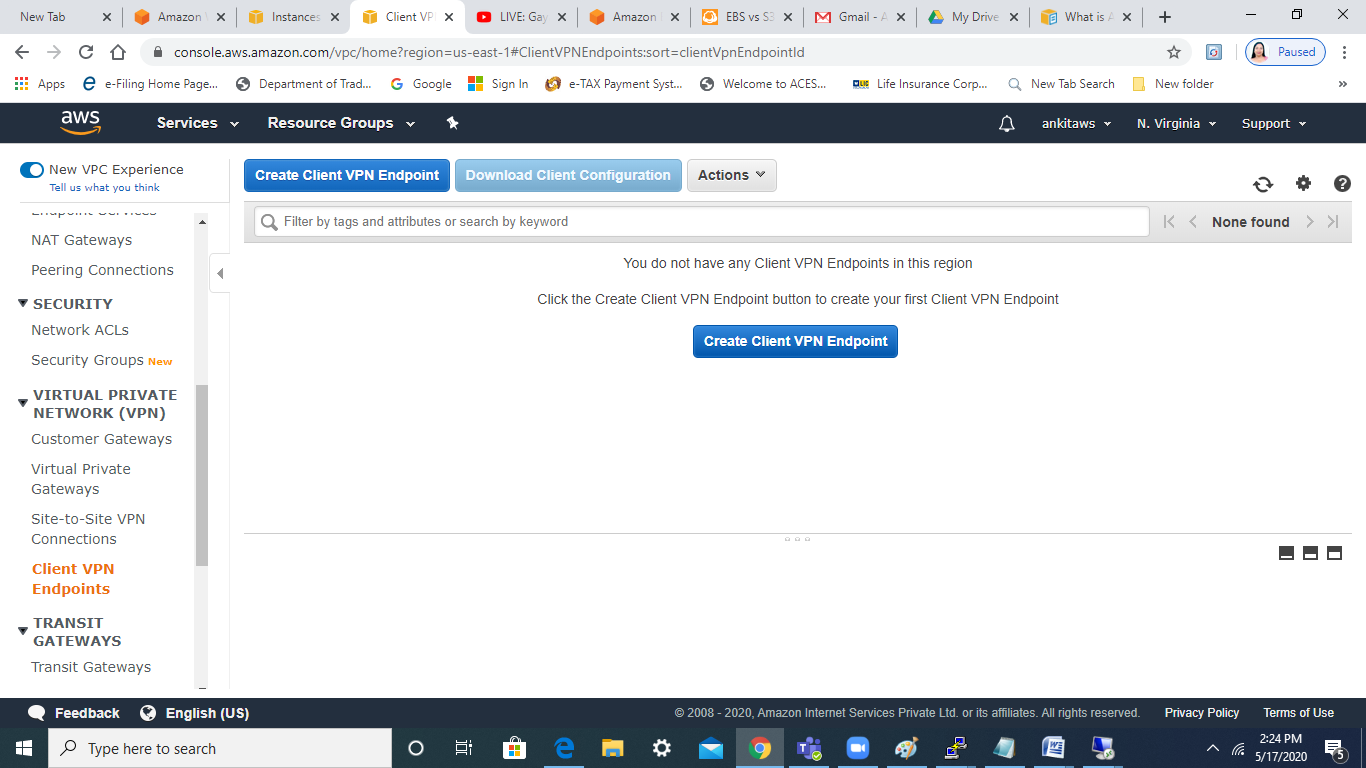
**How to set up client vpn**

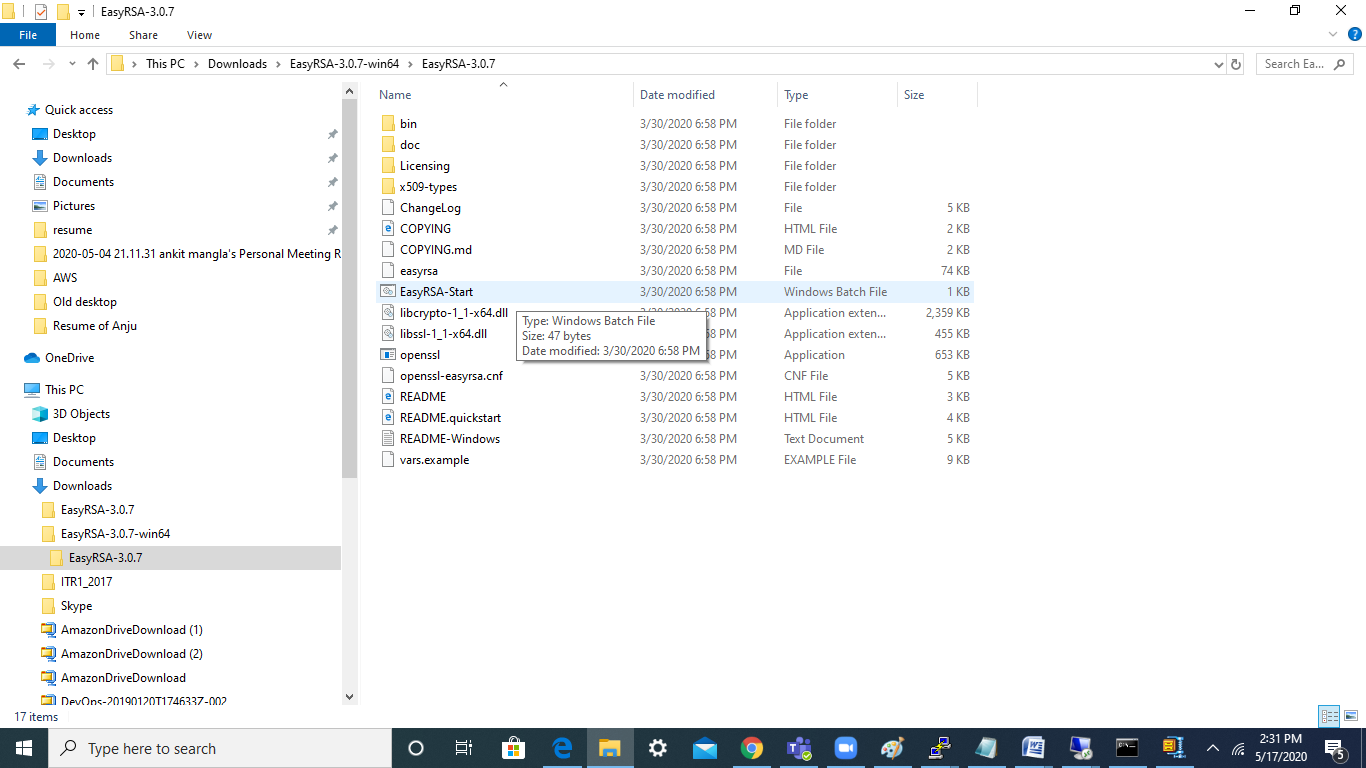
1. **Click on client-vpn endpoint in vpc window**

****

****

**2.As a pre-requisite , we need to create a server certificate and upload to ACM so that we can use it :-**

**2.1** Download the latest release for Windows at <https://github.com/OpenVPN/easy-rsa/releases>.



2.2 Initialize a new PKI environment.

$ ./easyrsa init-pki

2.3 Build a new certificate authority (CA).

./easyrsa build-ca nopass

2.4 Generate the server certificate and key.

./easyrsa build-server-full server nopass

2.5 Generate the client certificate and key.

Make sure to save the client certificate and the client private key because you will need them when you configure the client.

./easyrsa build-client-full client1.domain.tld nopass

2.6 Copy the server certificate and key and the client certificate and key to a custom folder and then navigate into the custom folder.

Before you copy the certificates and keys, create the custom folder by using the mkdir command. The following example creates a custom folder in your home directory.

mkdir ~/custom\_folder/

cp pki/ca.crt ~/custom\_folder/

cp pki/issued/server.crt ~/custom\_folder/

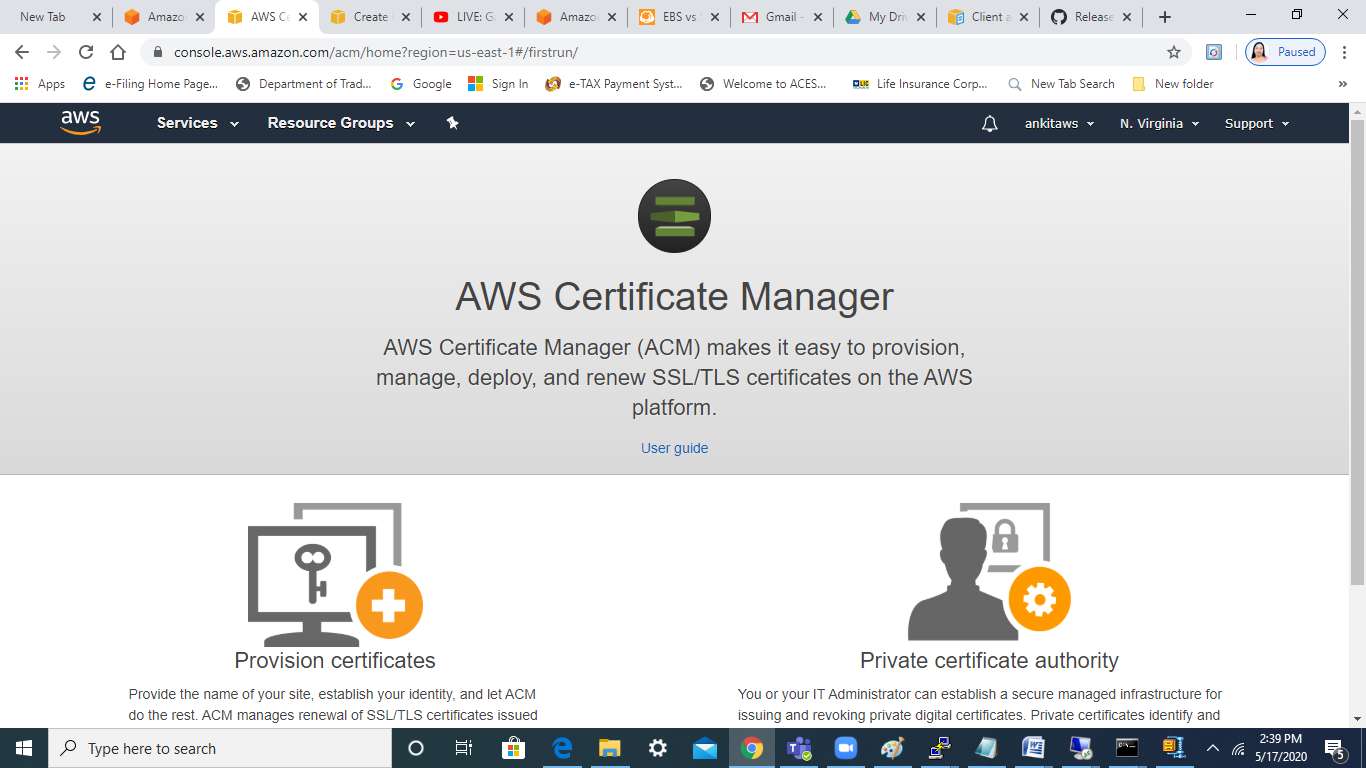
cp pki/private/server.key ~/custom\_folder/

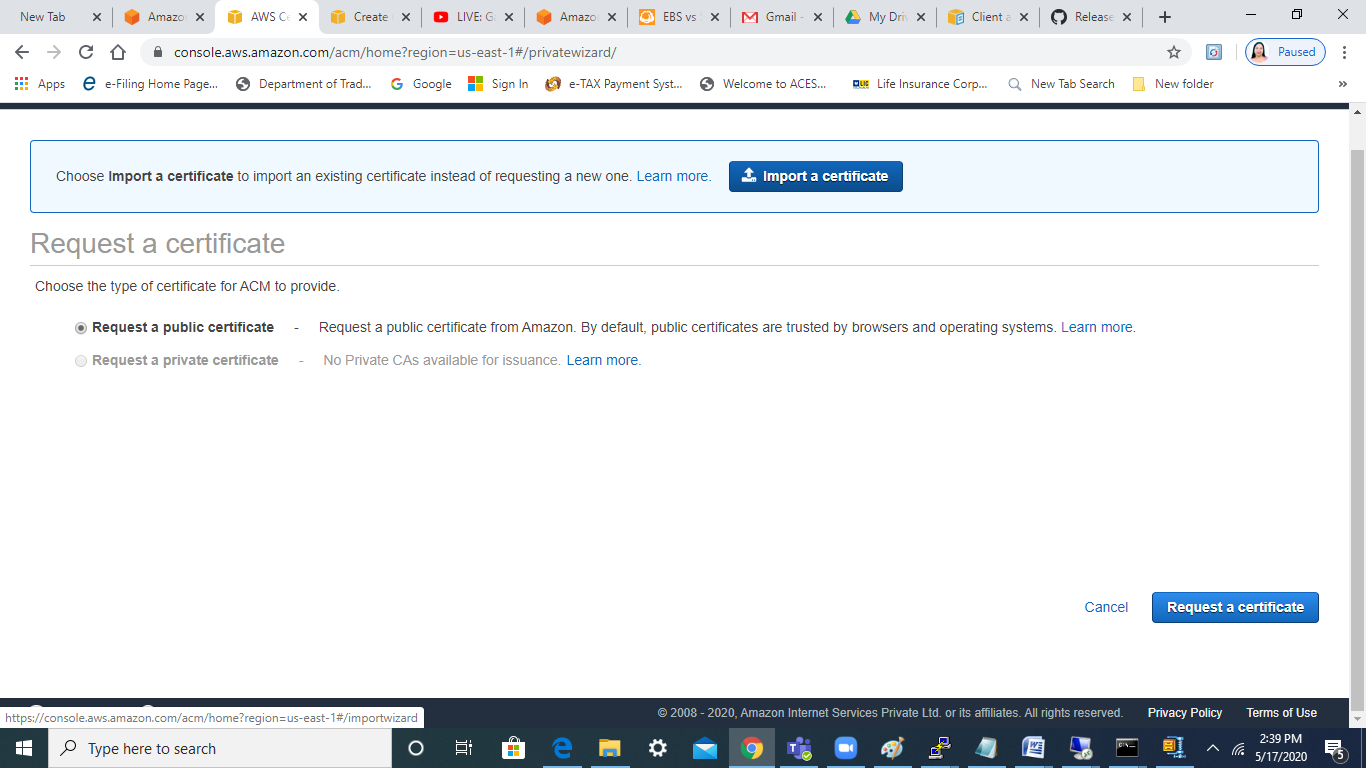
cp pki/issued/client1.domain.tld.crt ~/custom\_folder

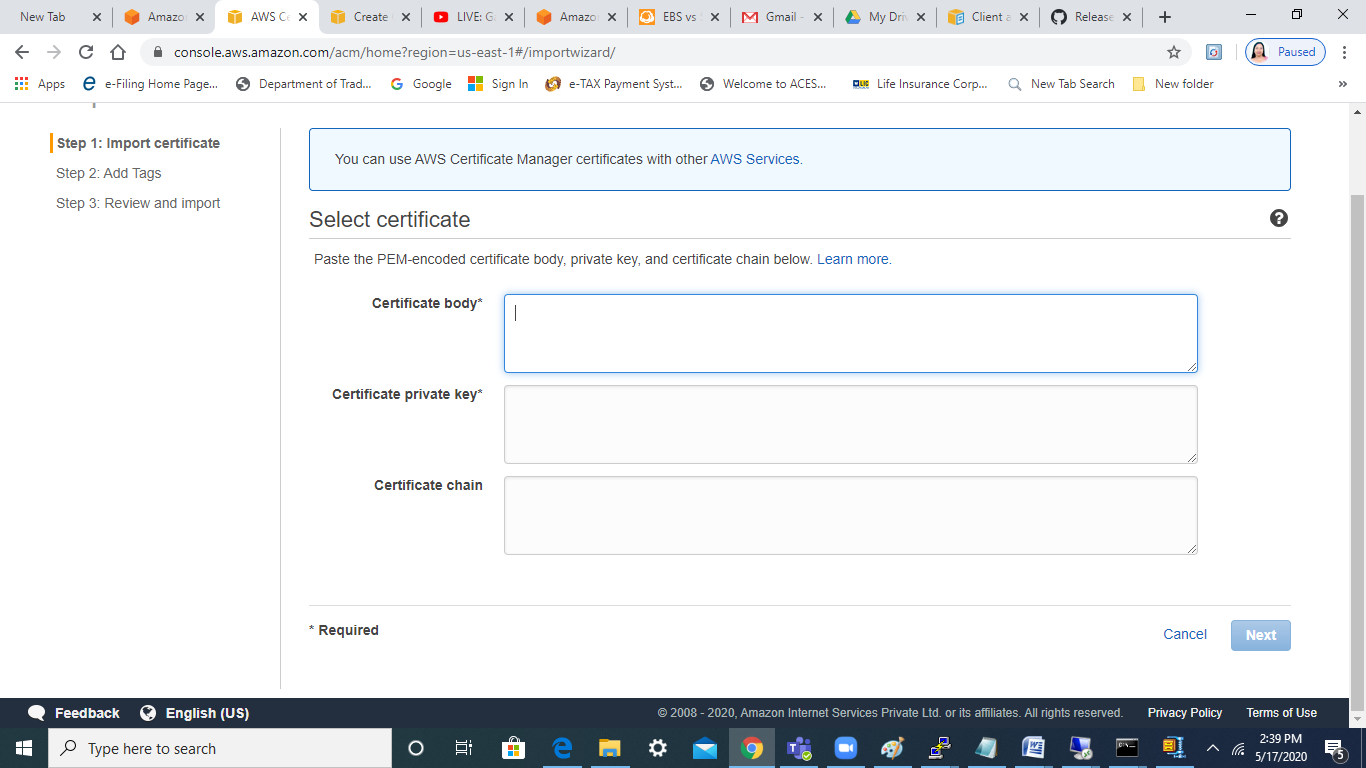
cp pki/private/client1.domain.tld.key ~/custom\_folder/

cd ~/custom\_folder/

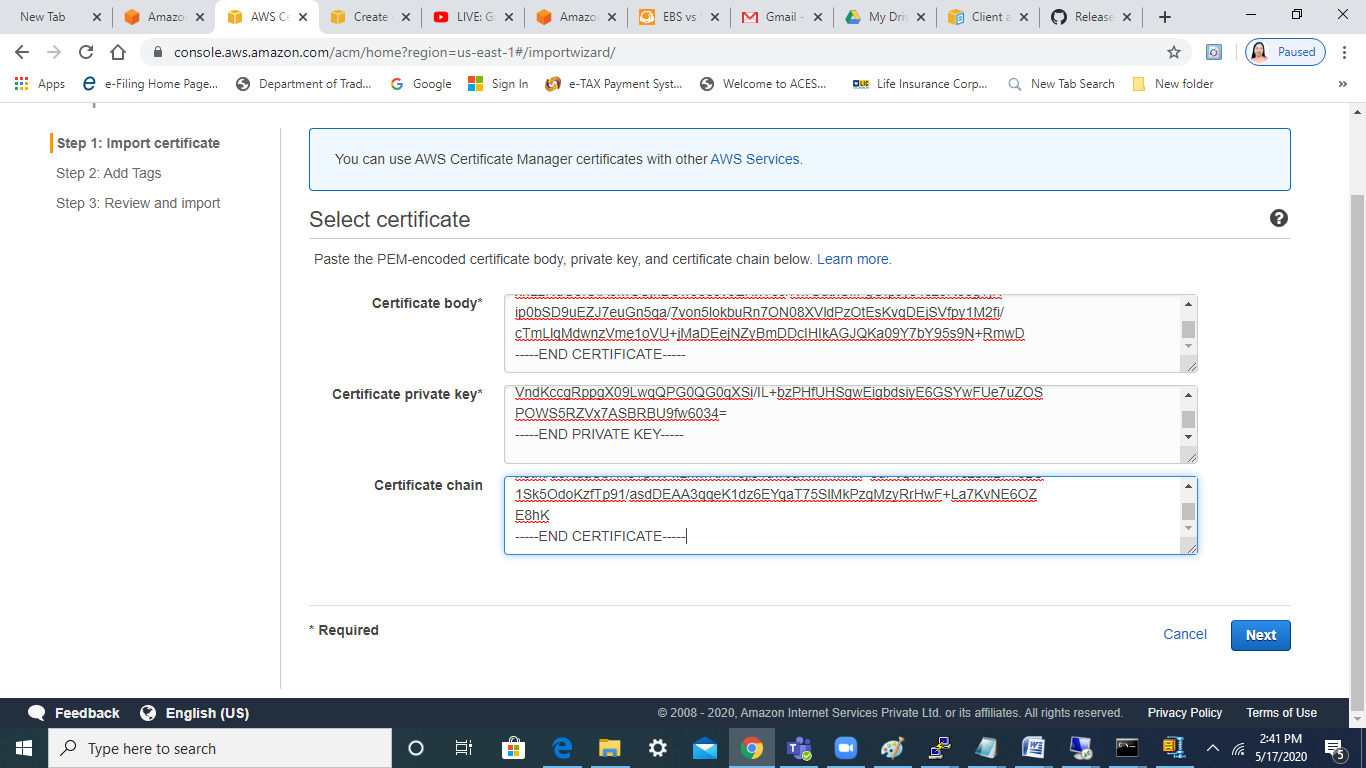
3.Once done , we need to upload certificate to ACM :-

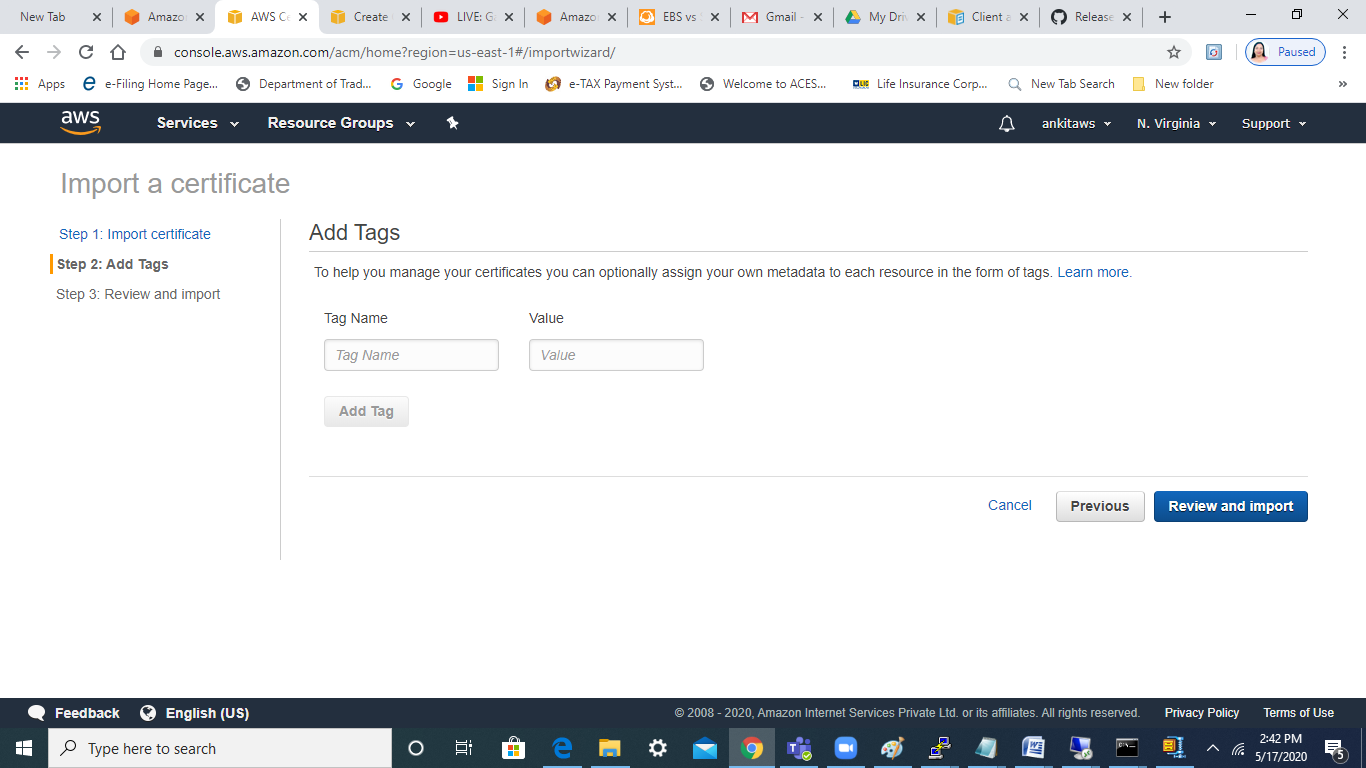


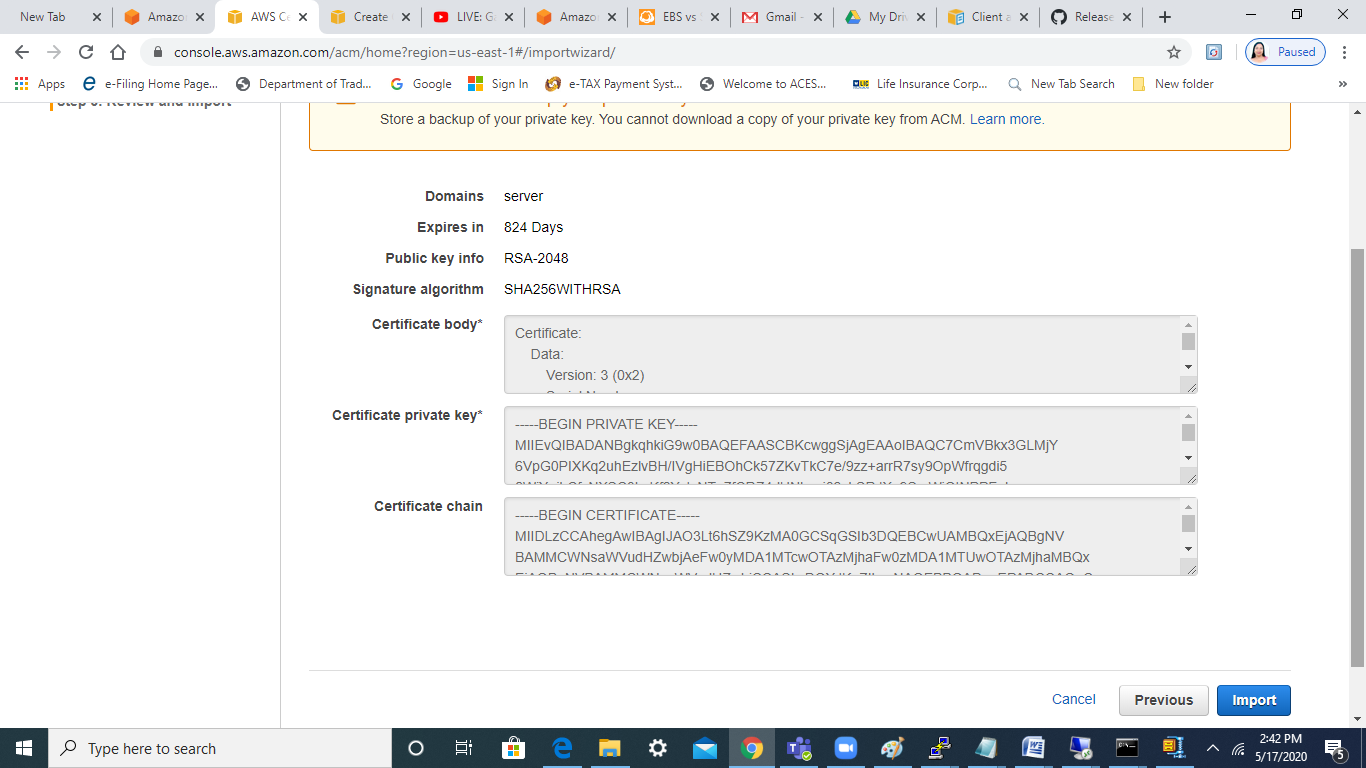


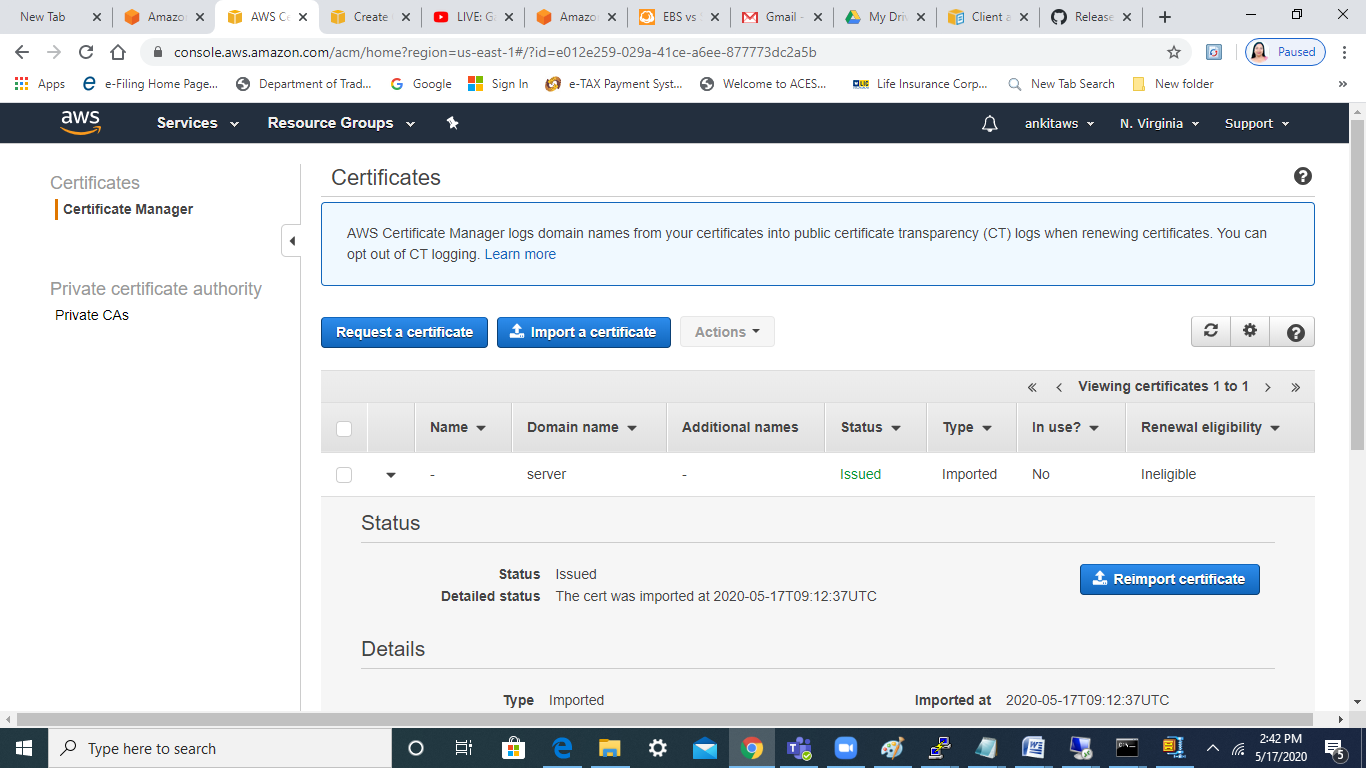


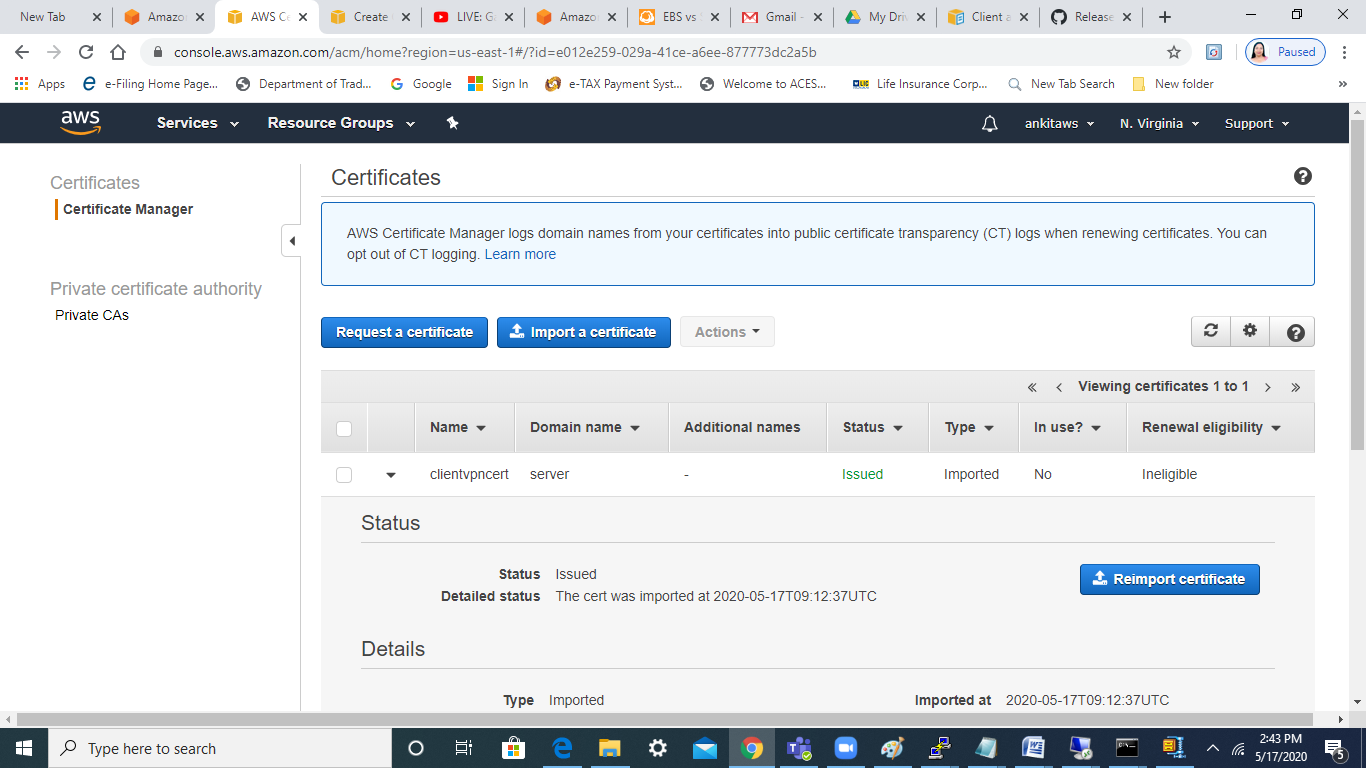
Upload all the three files :-



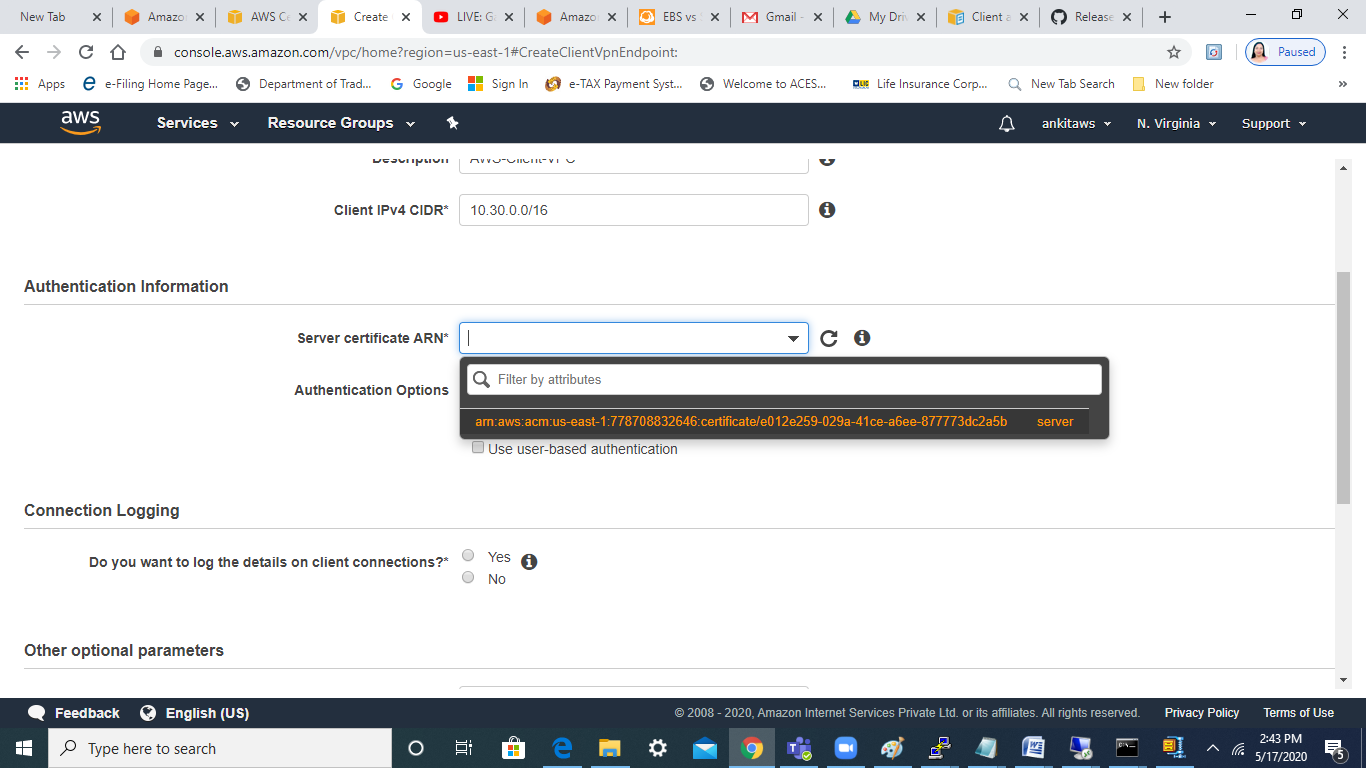




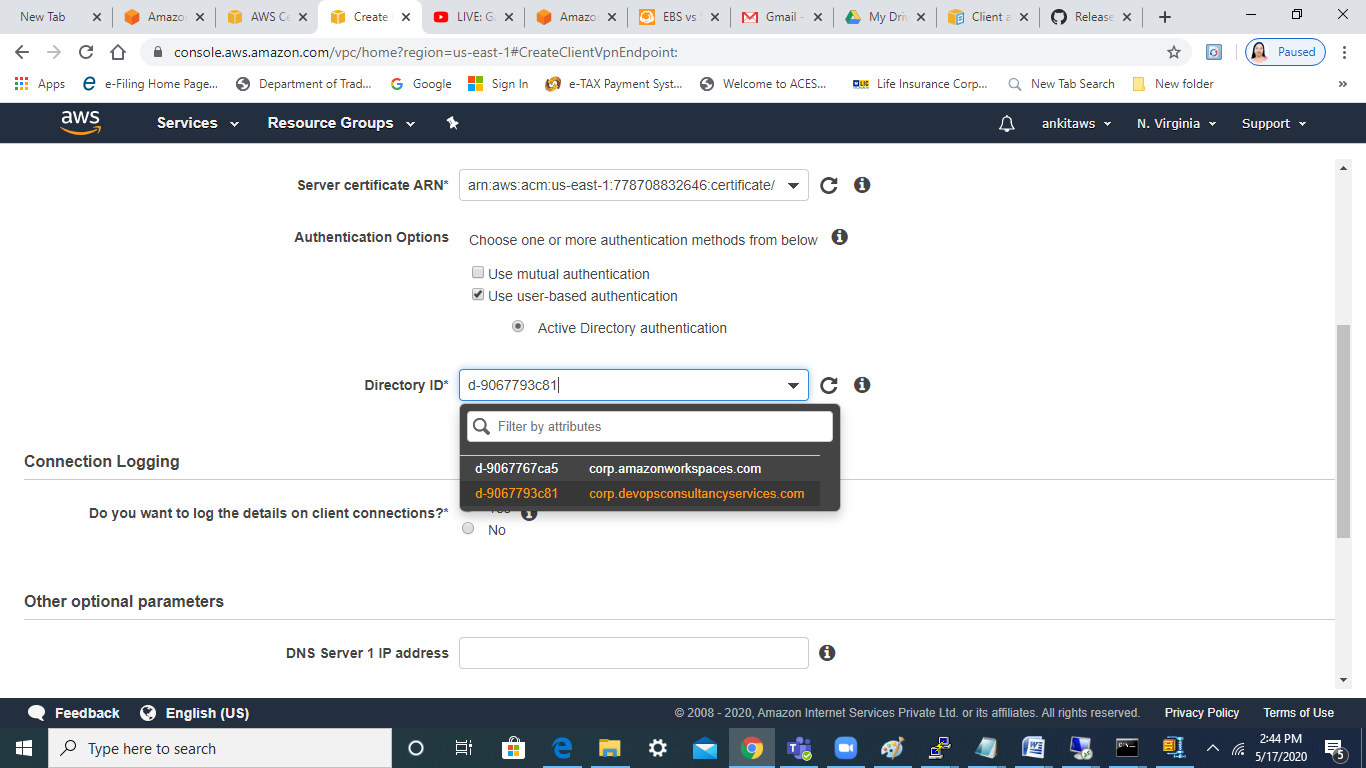


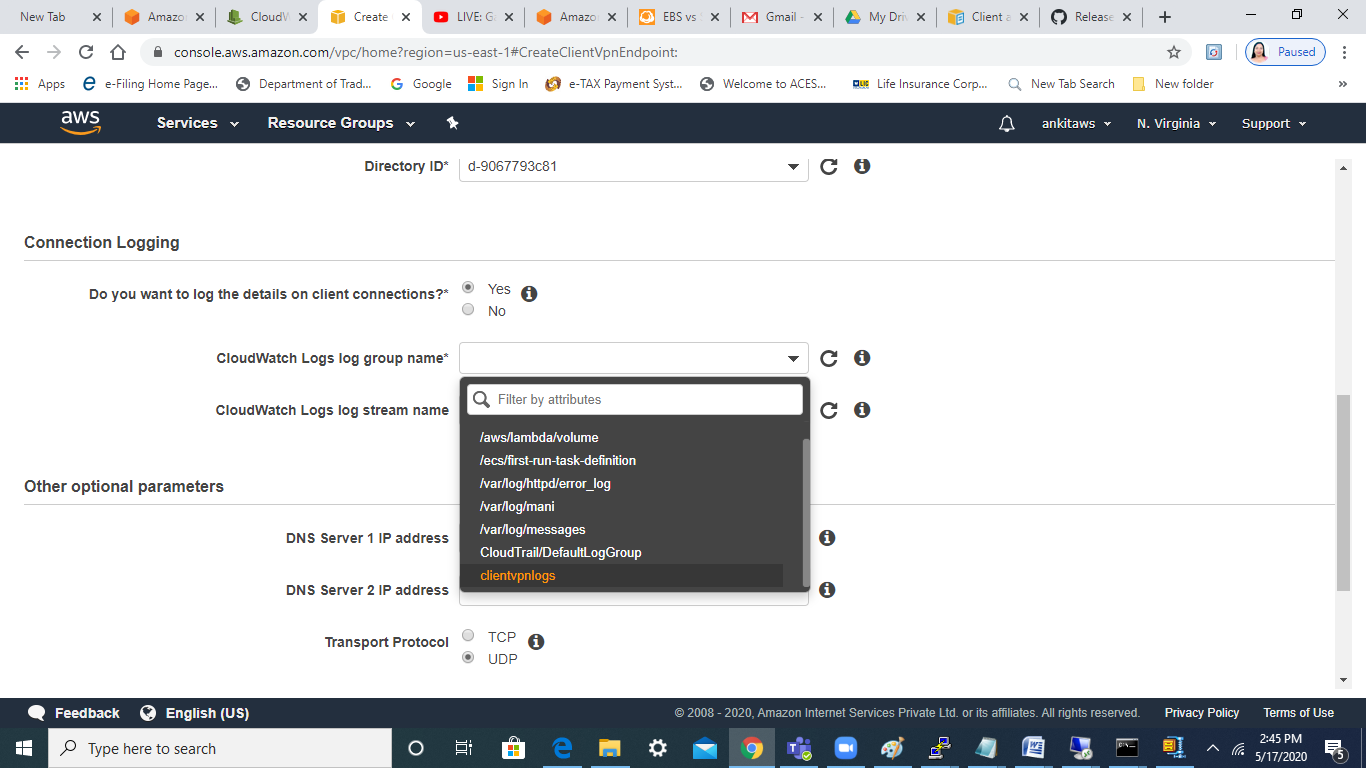


Once certificate is uploaded, then we can see the cert in ACM :-

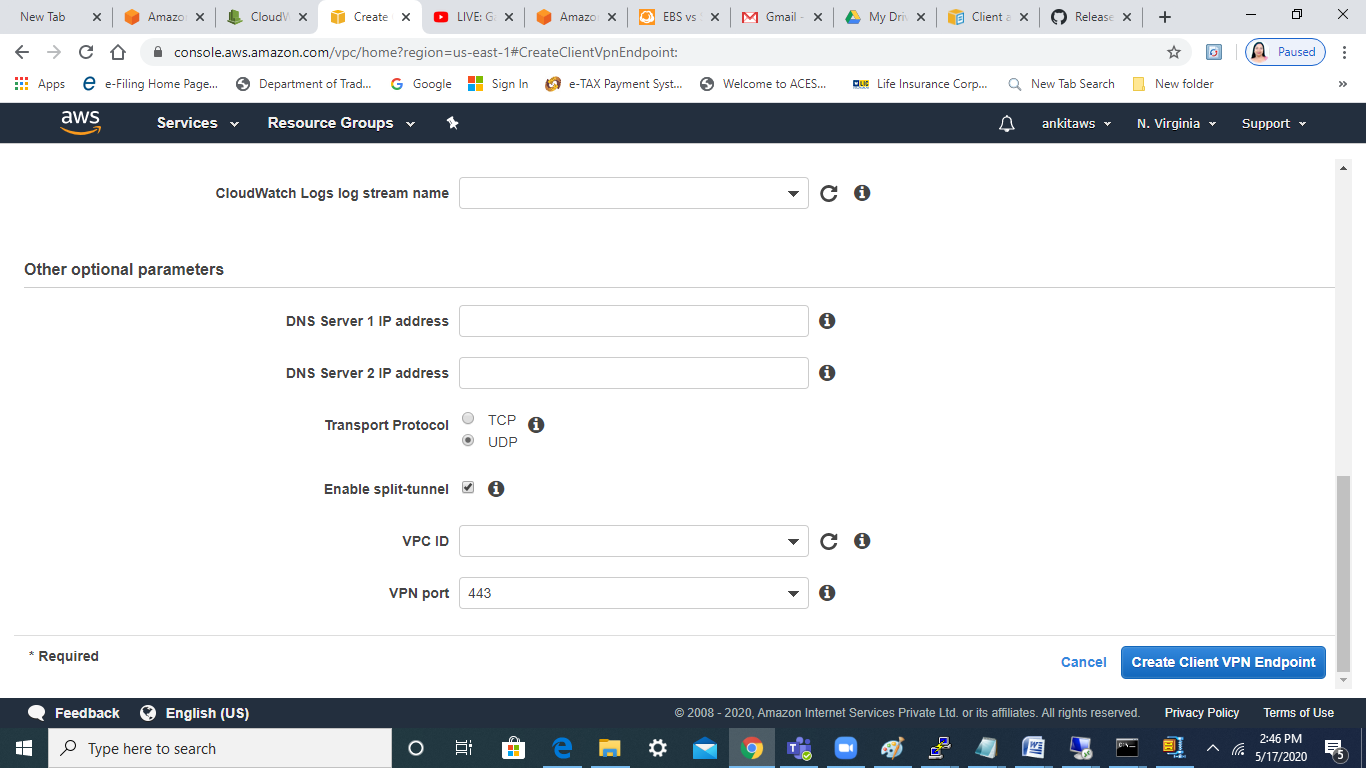


Choose user-based authentication so that we can use the AD that we created :-

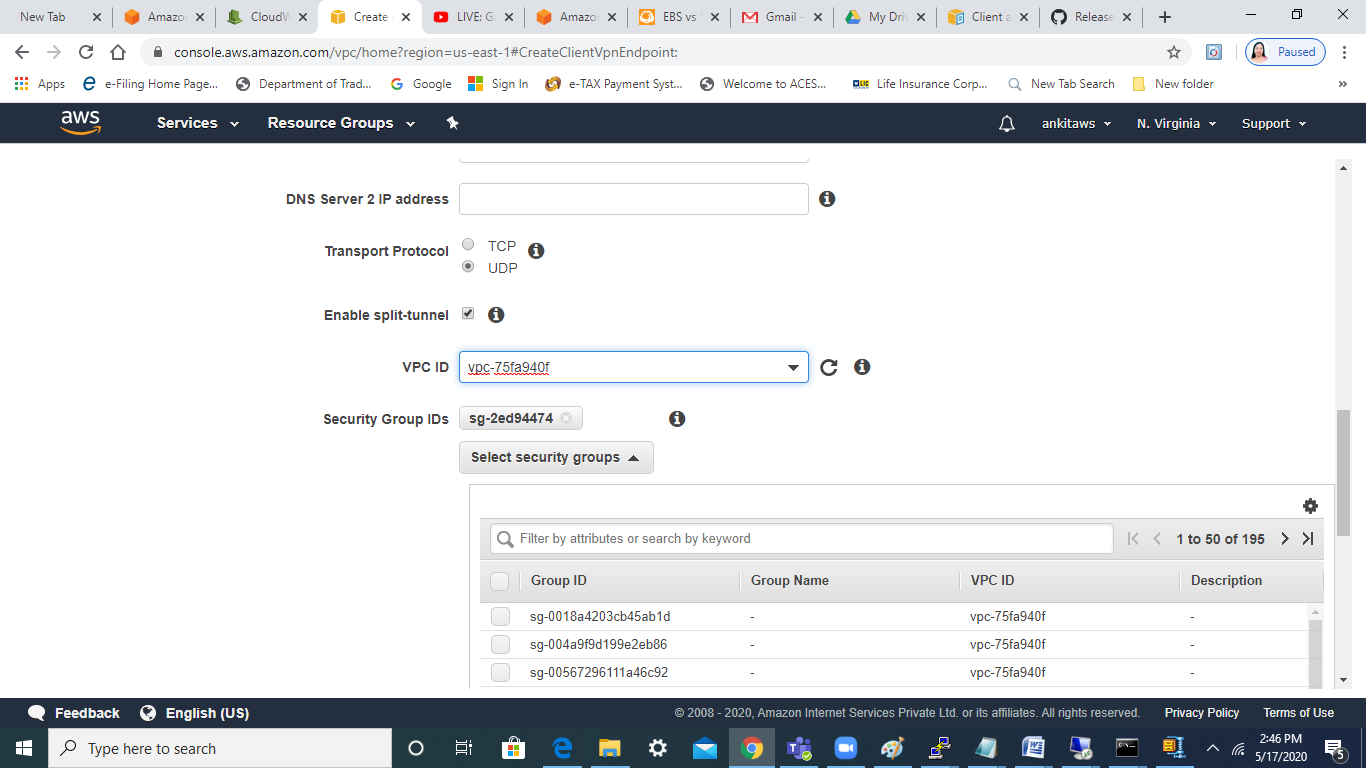


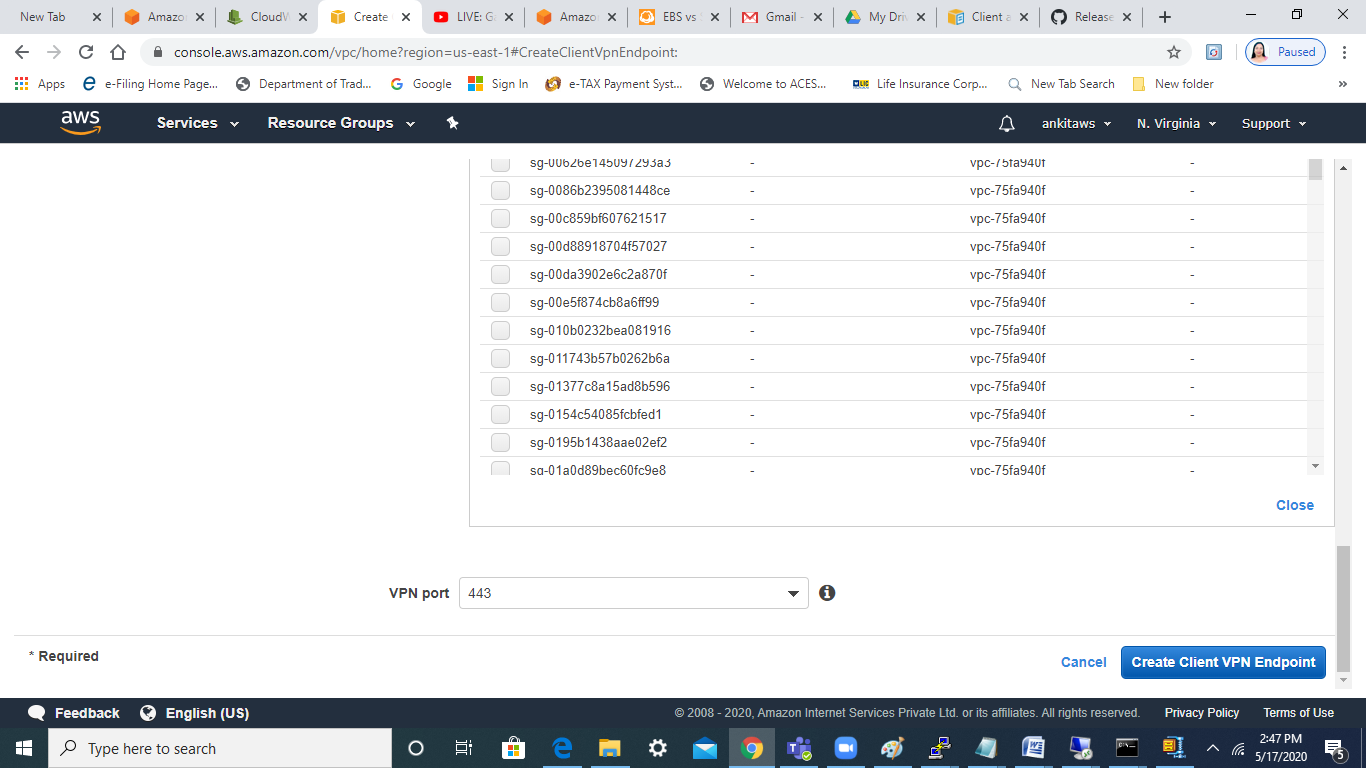


Select the split-tunnel :-

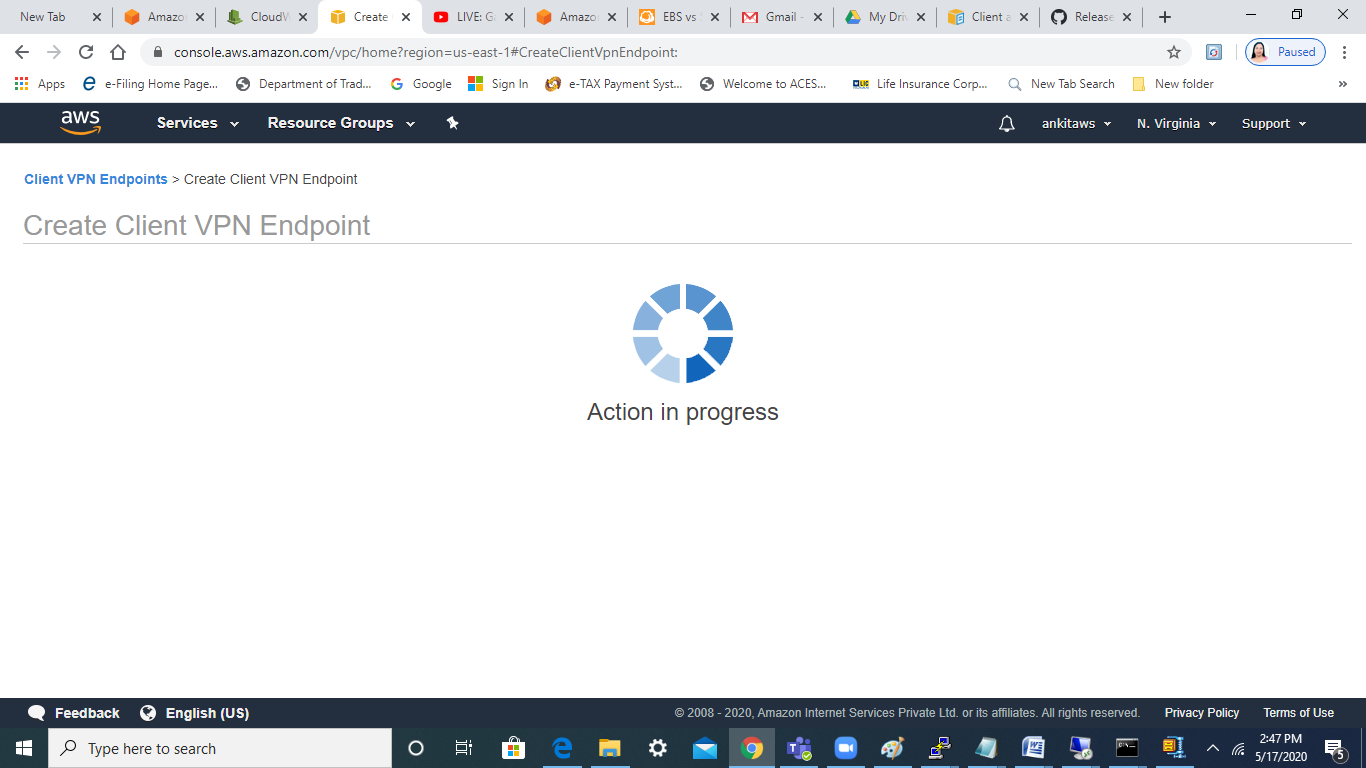


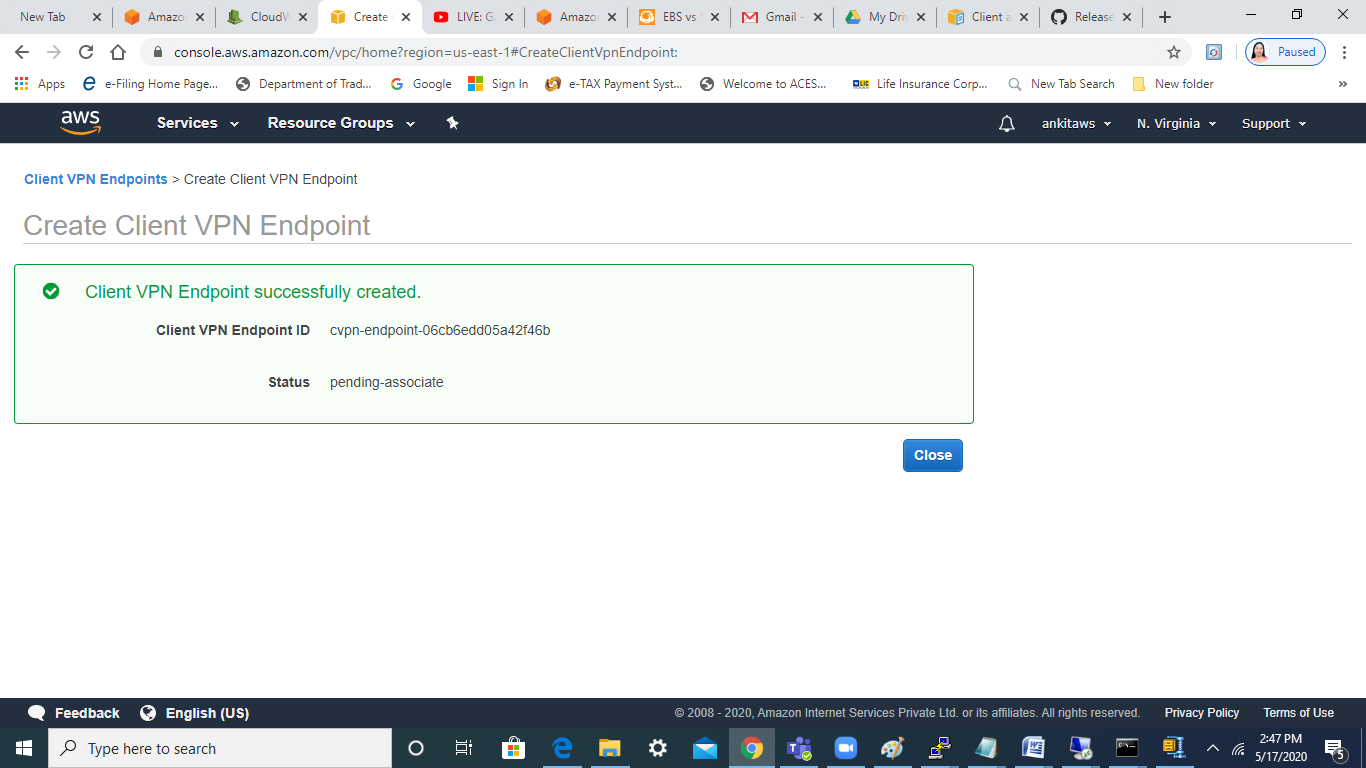
Select the appropriate SG and VPC :-

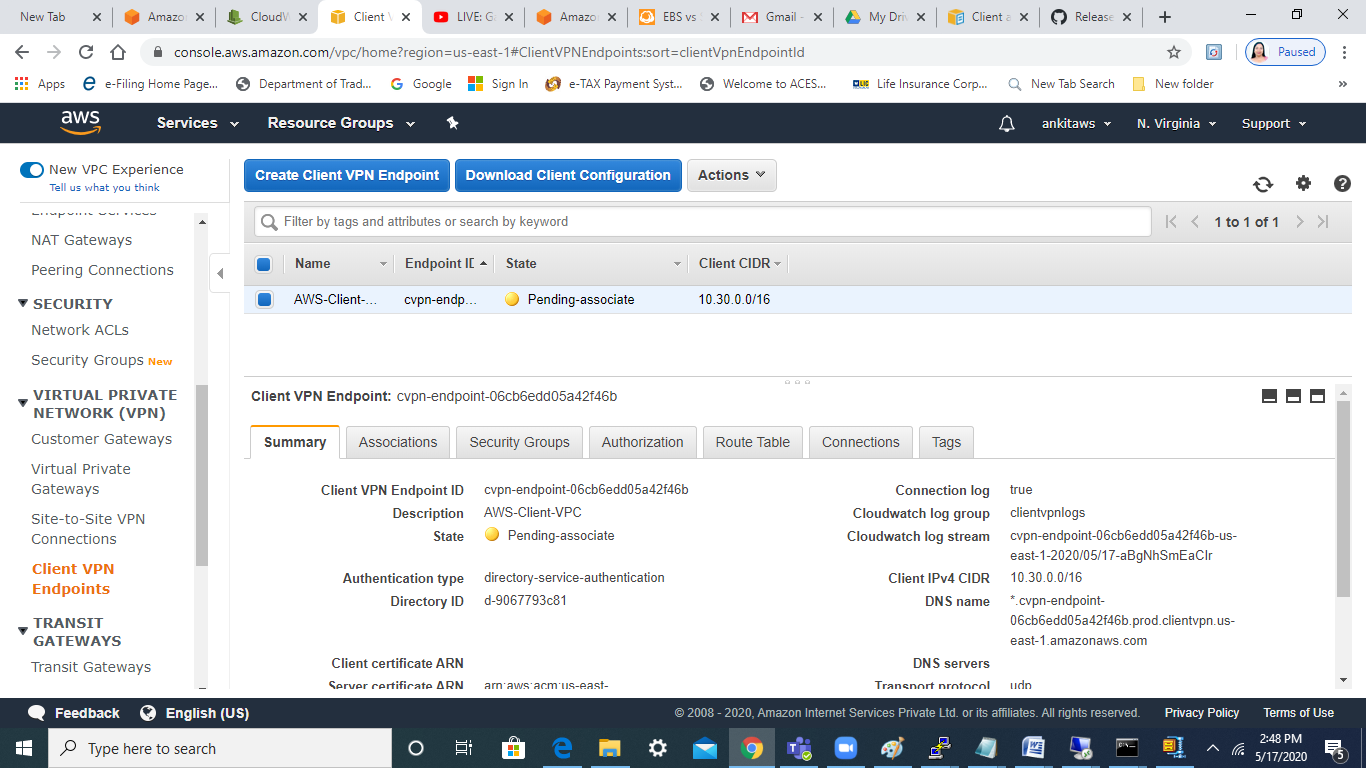




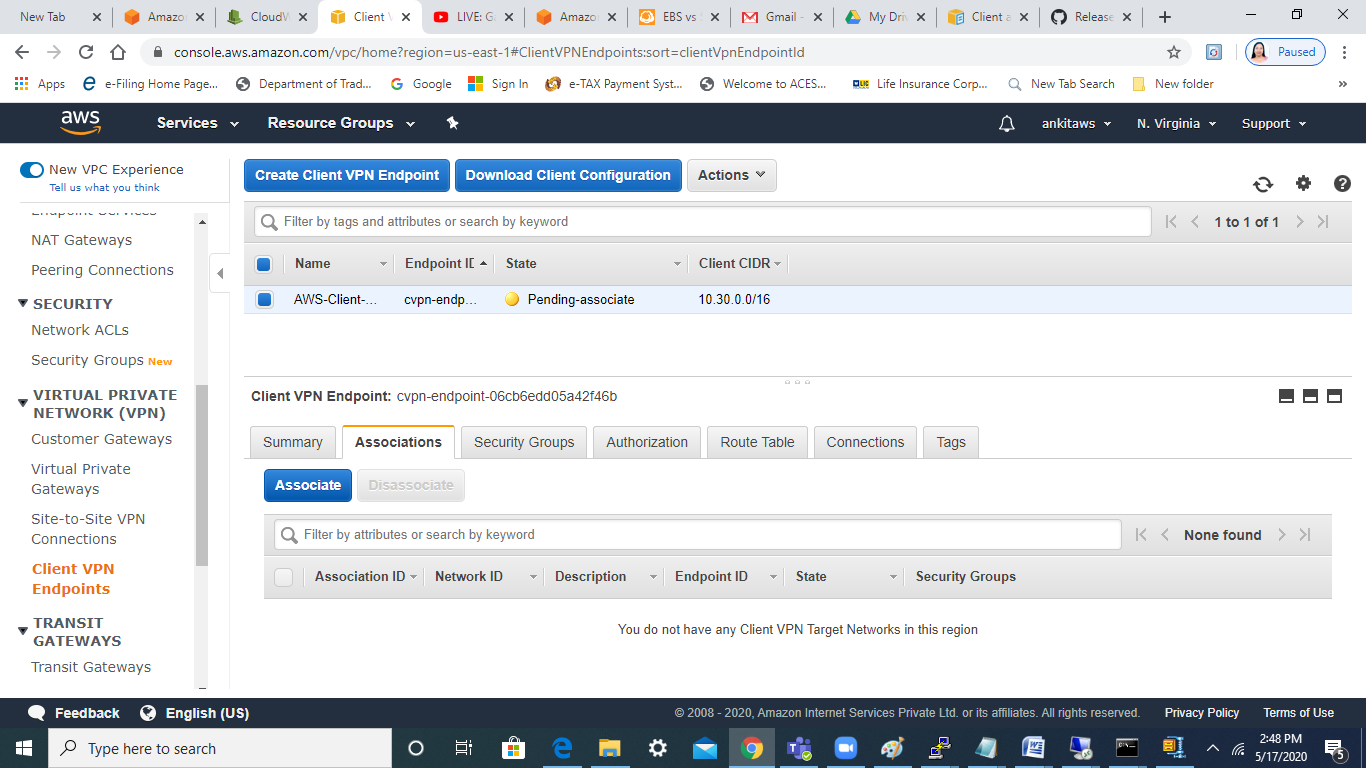
Click on create client vpn endpoint

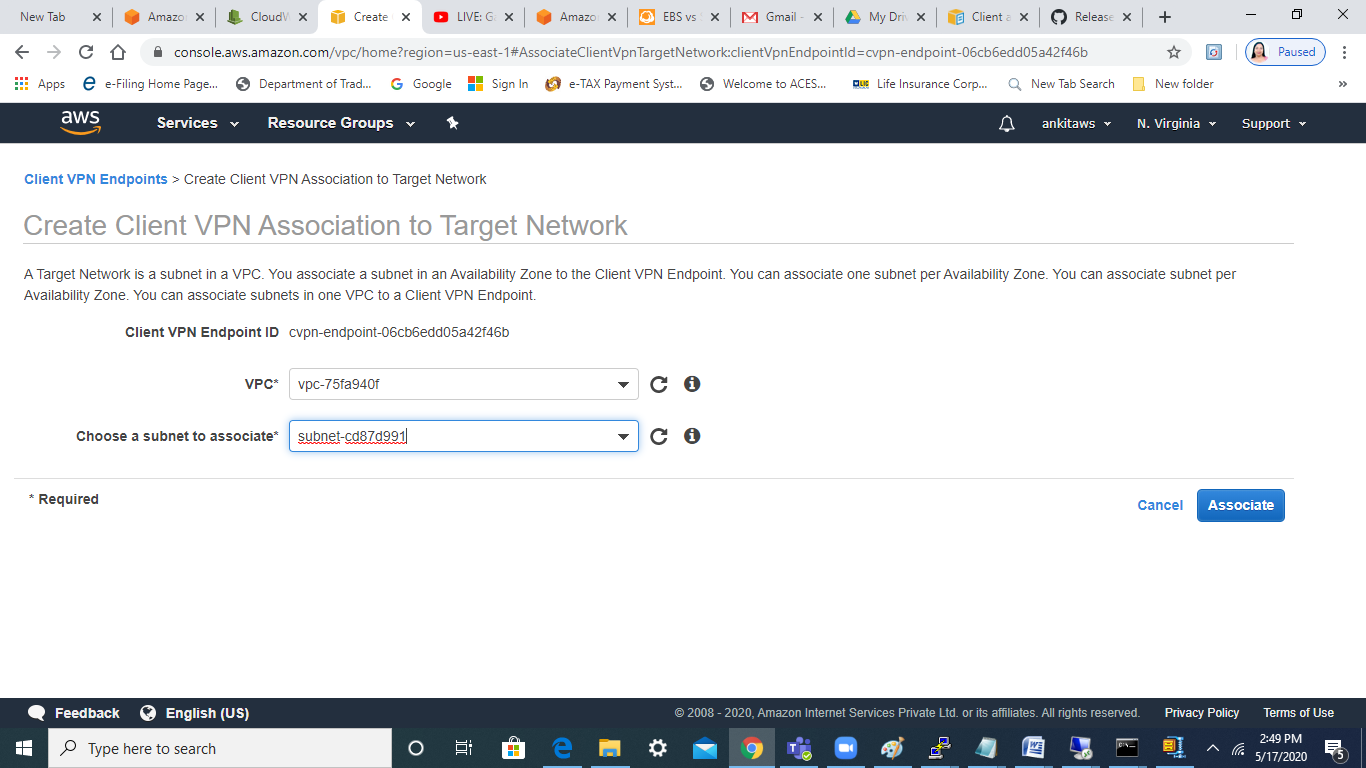


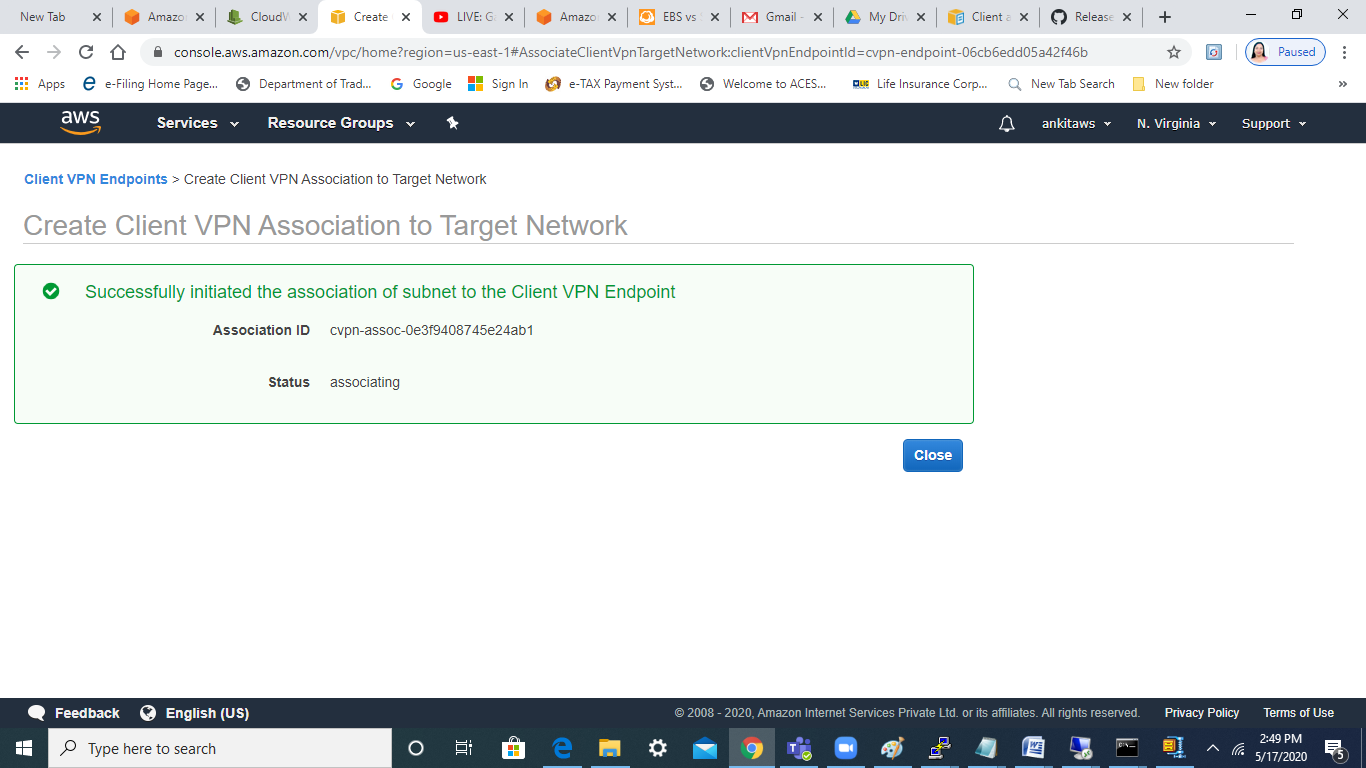




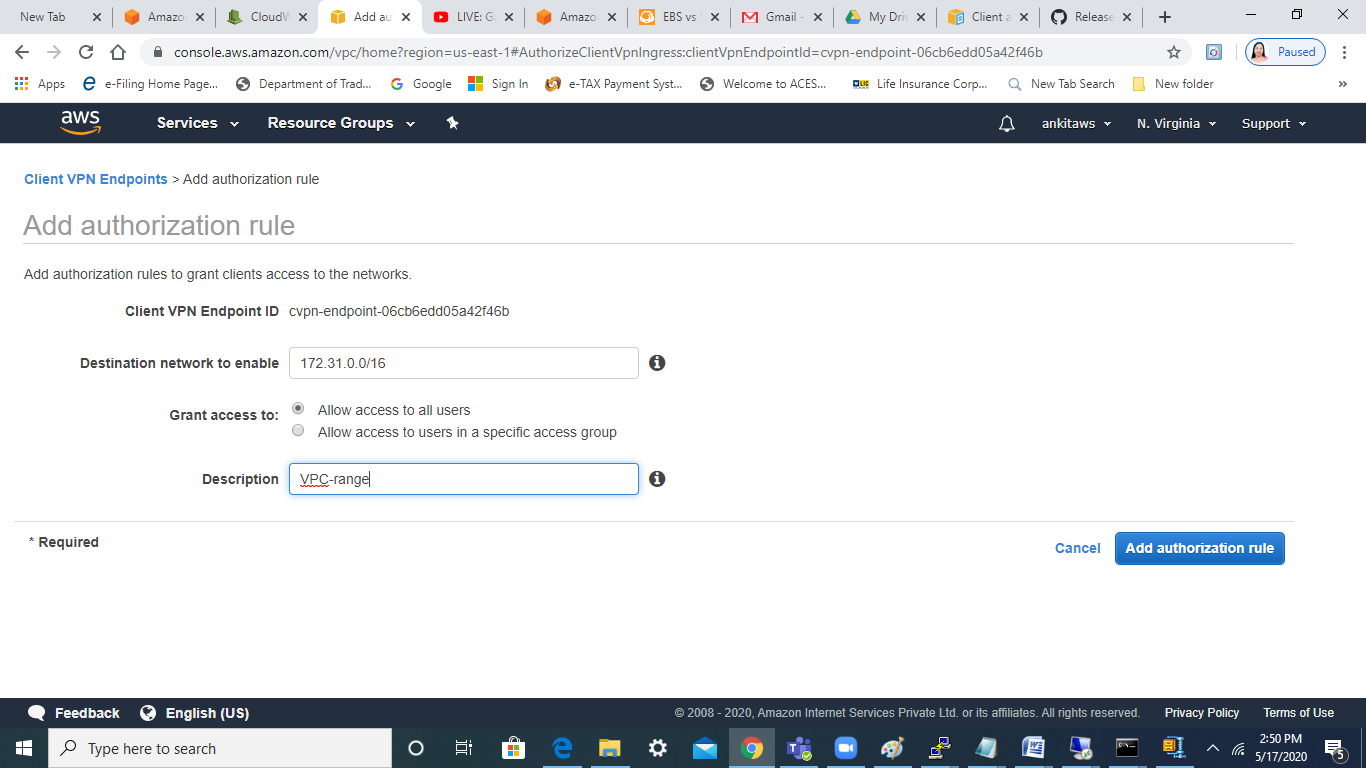
Now, associate the VPC and subnet that will act like a front-gate :-

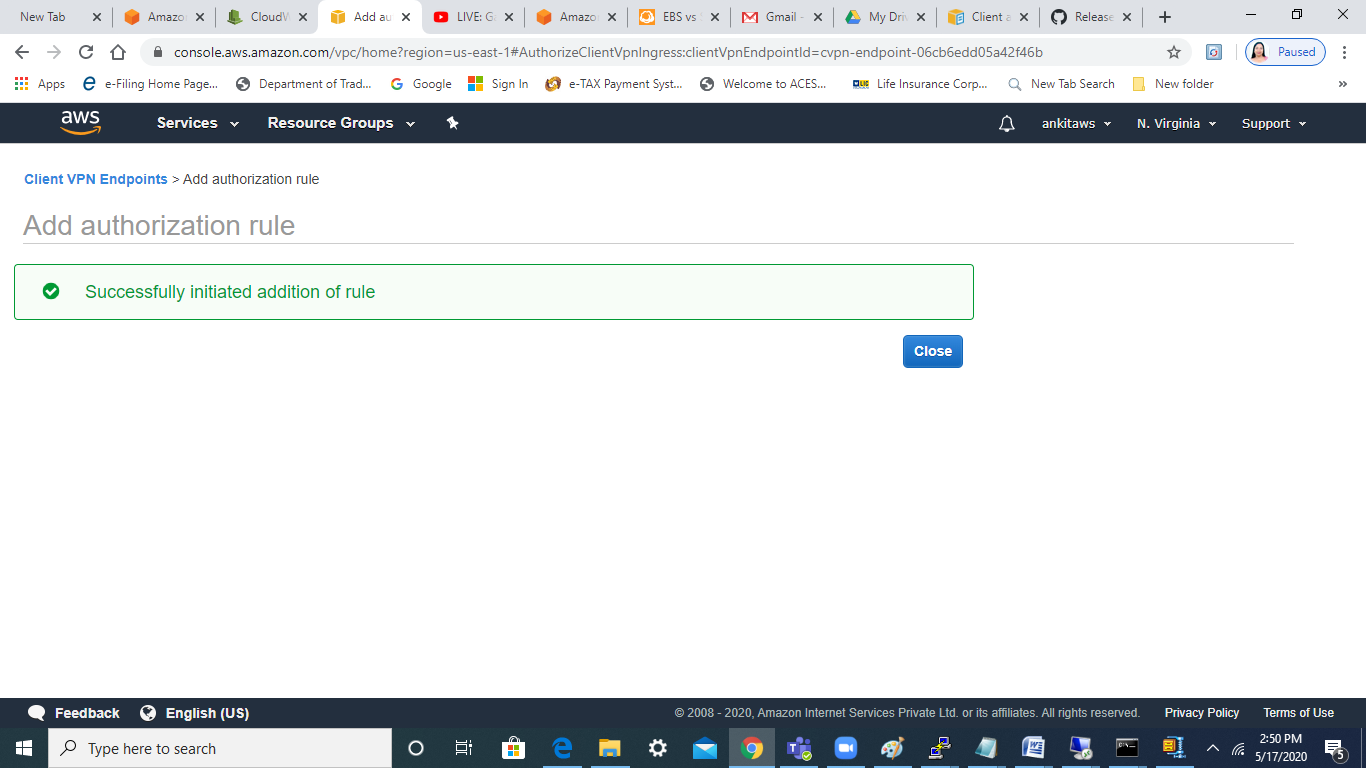




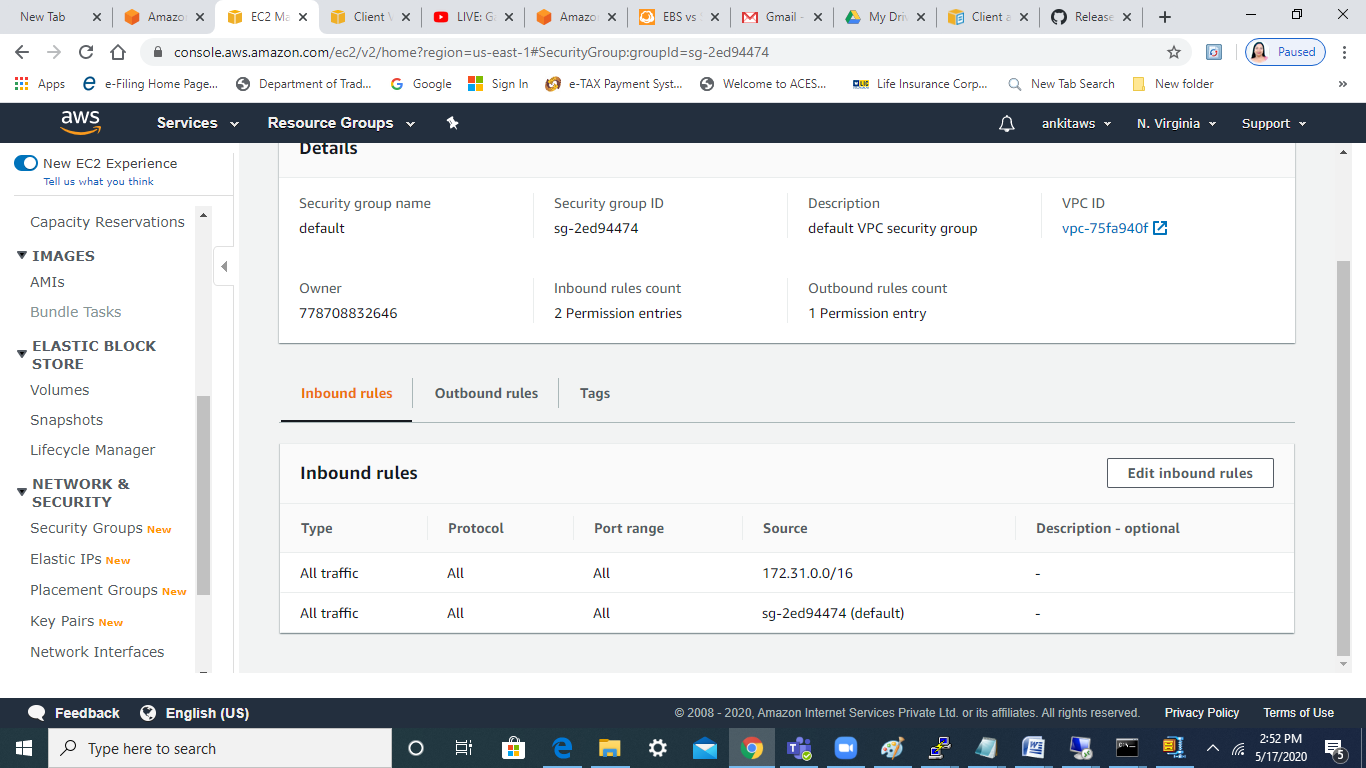


Last step is to authorize our VPC to act as ingress for this VPN :-

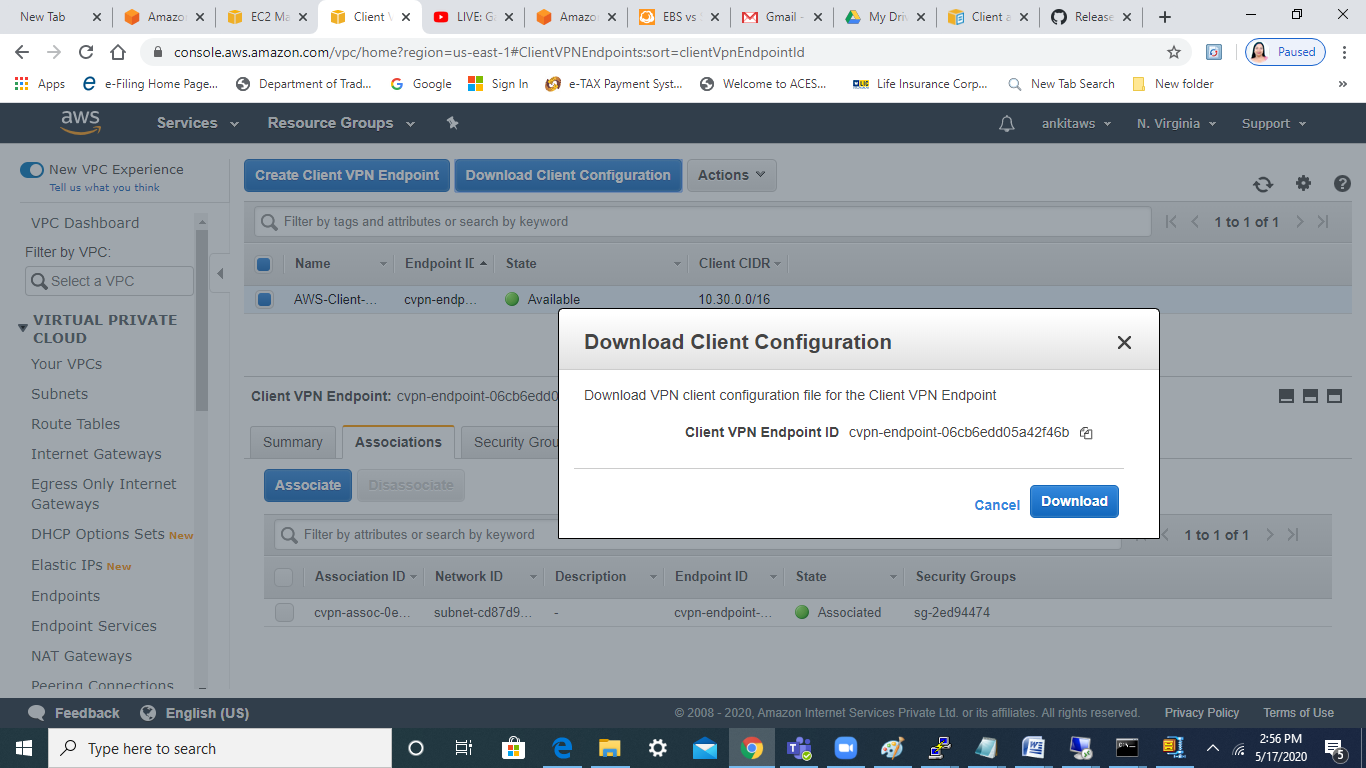


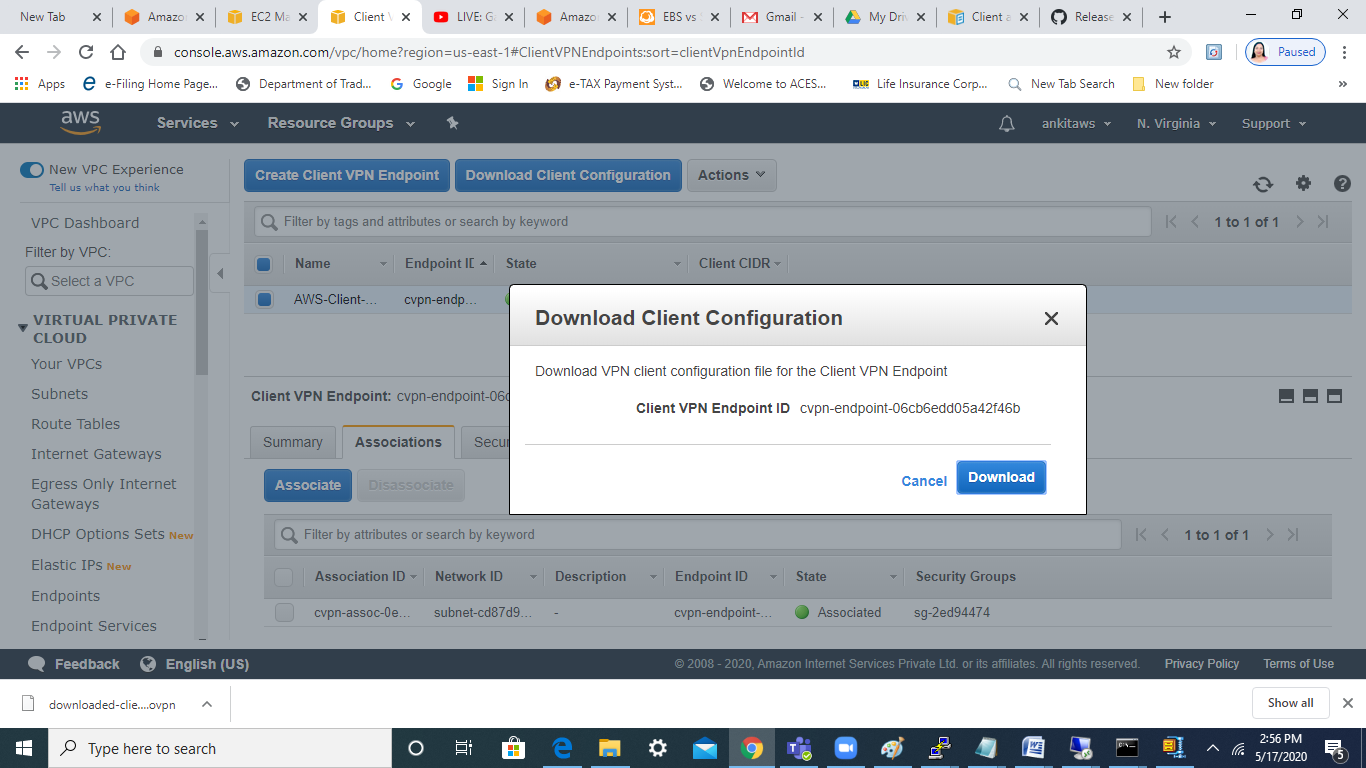


Also, please ensure that SG allows traffic of our vpc range

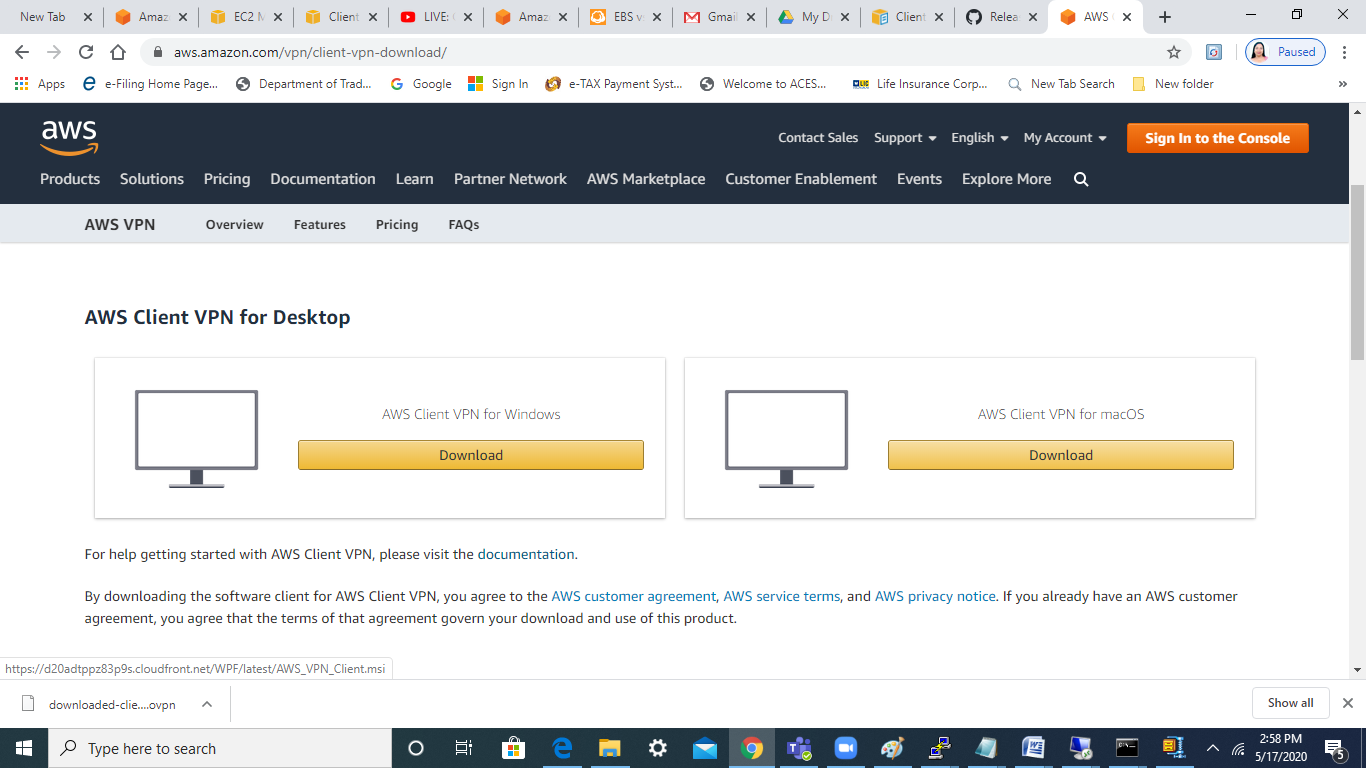


Download the client config file

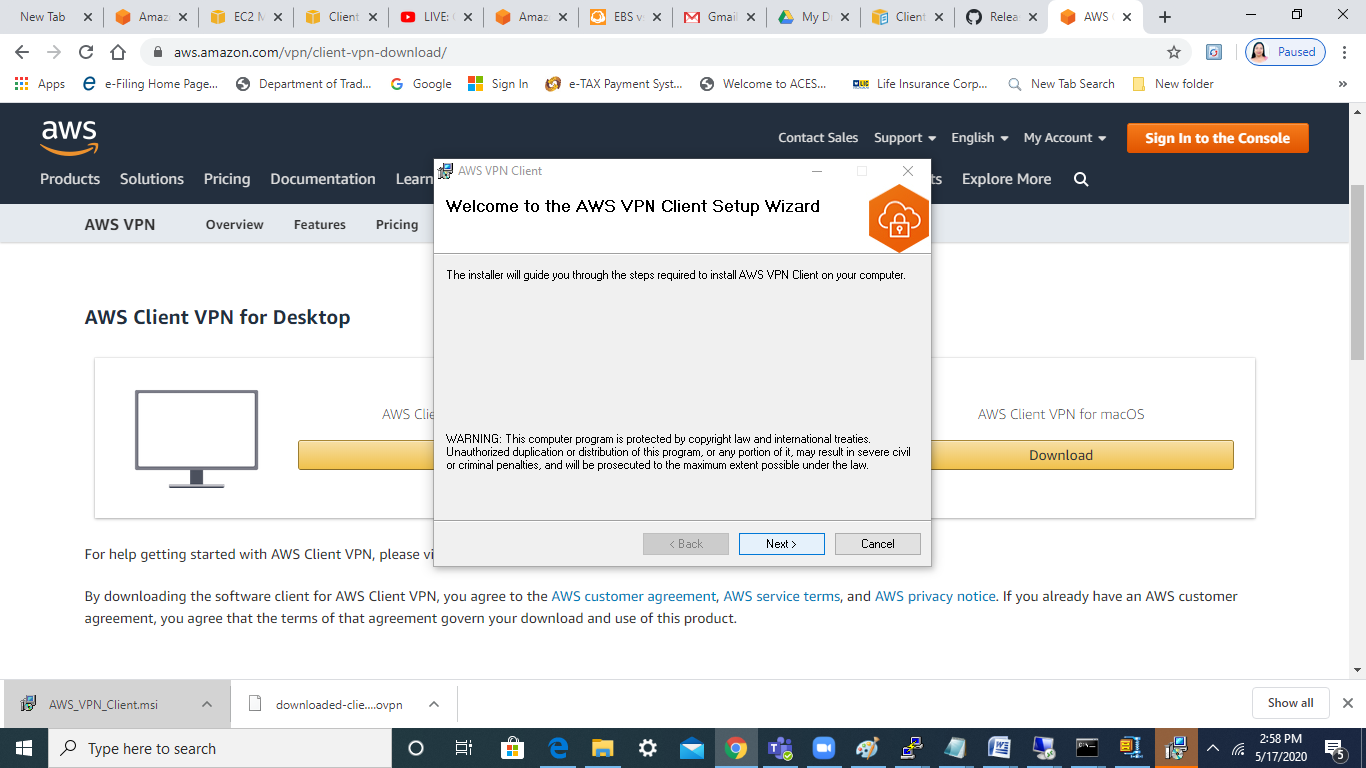




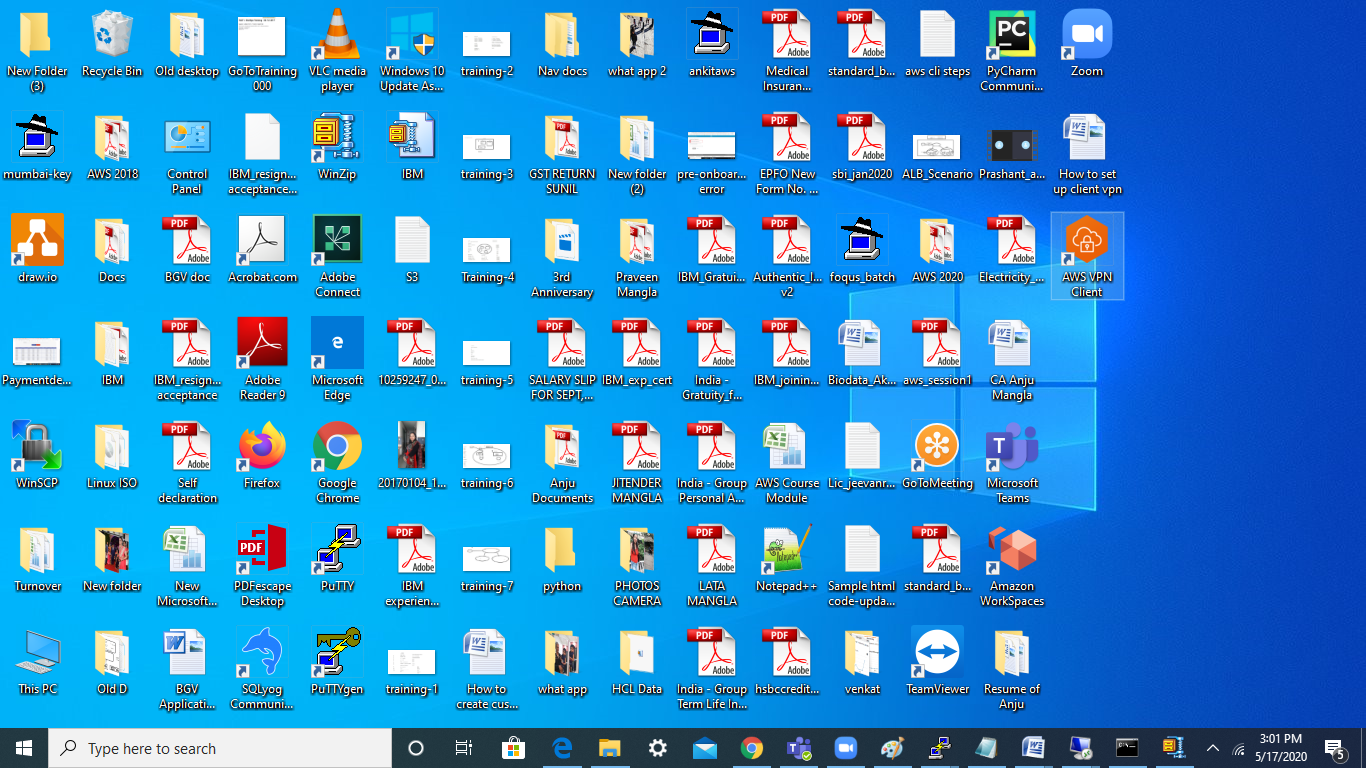
Last step is to download Amazon VPN client :-



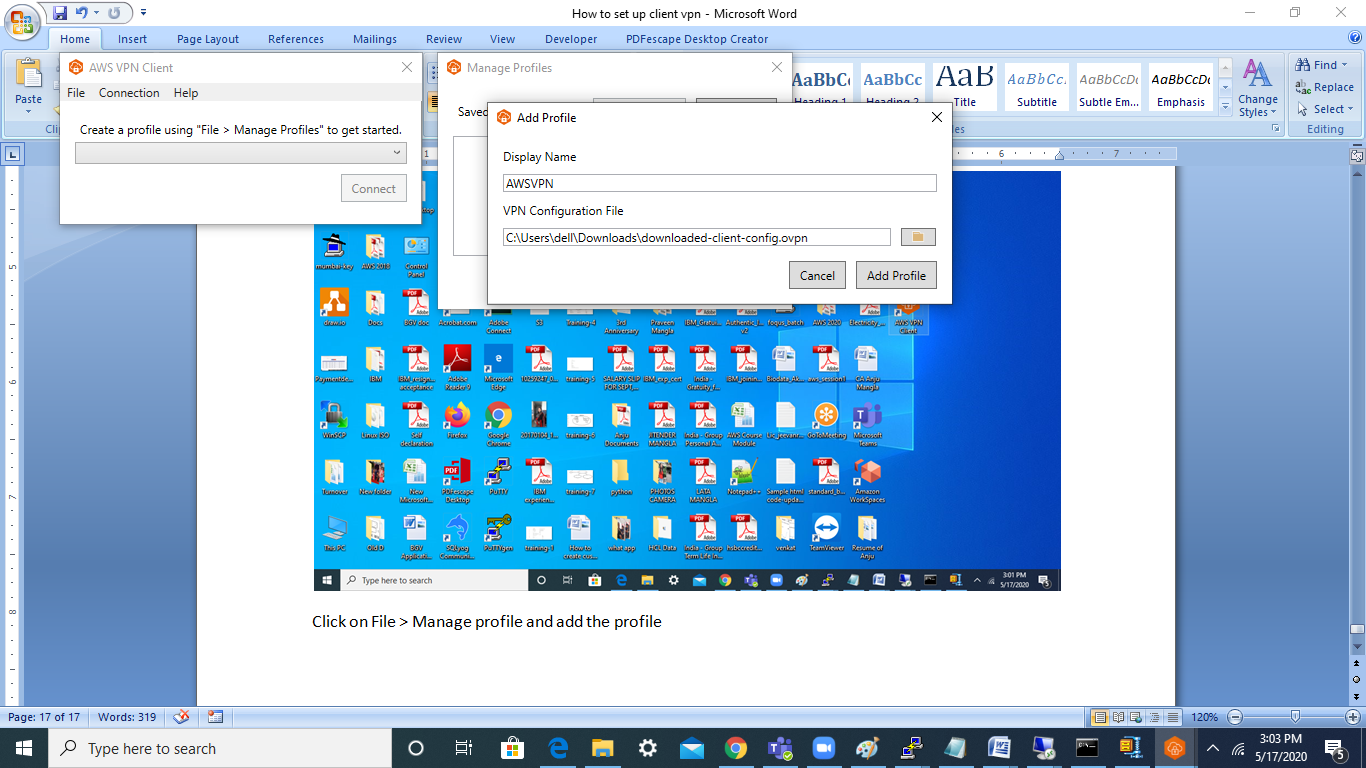
Install the vpn

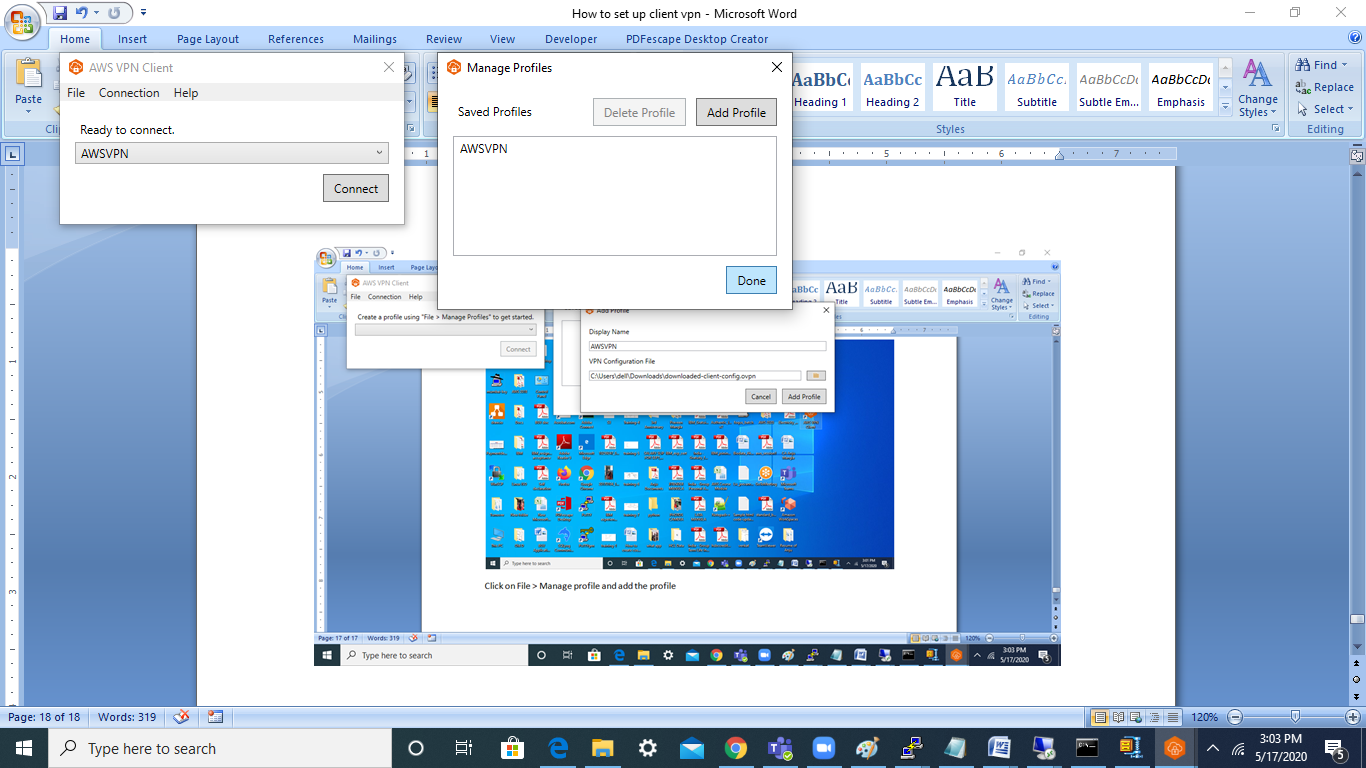


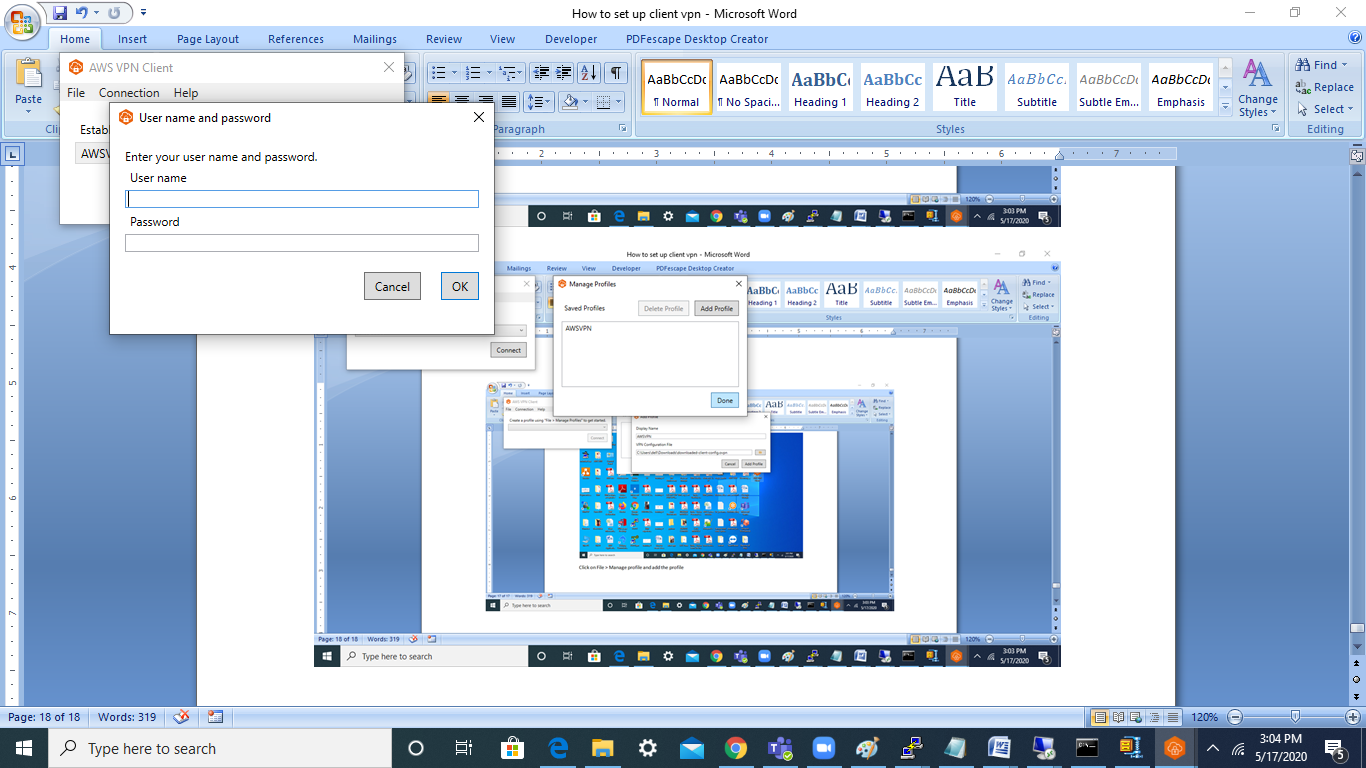
Once downloaded and installed , then we can see icon on the desktop :-



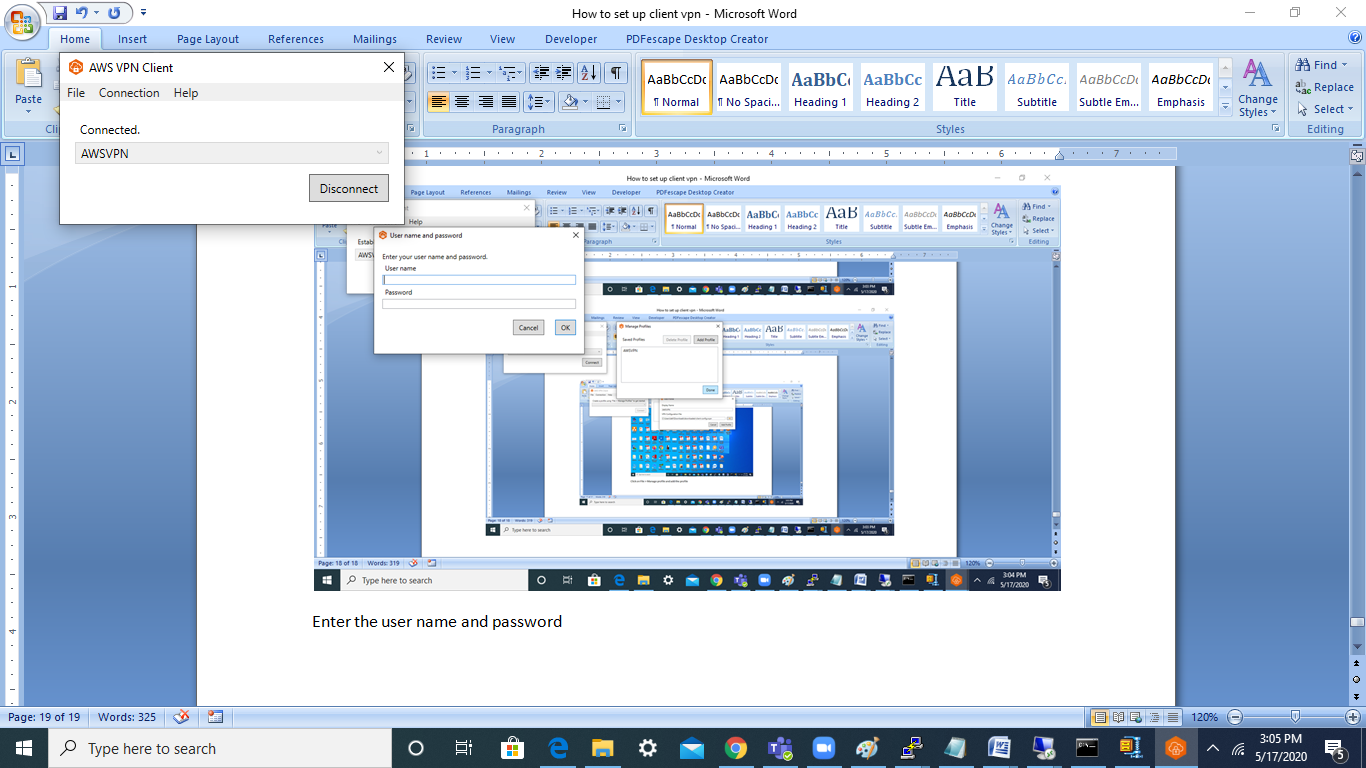
Click on File > Manage profile and add the profile







Enter the user name and password



**Testing**

Launch a ec2 instance and try to access the instance using private ip. On successful connection, we will connect login prompt as below :-



