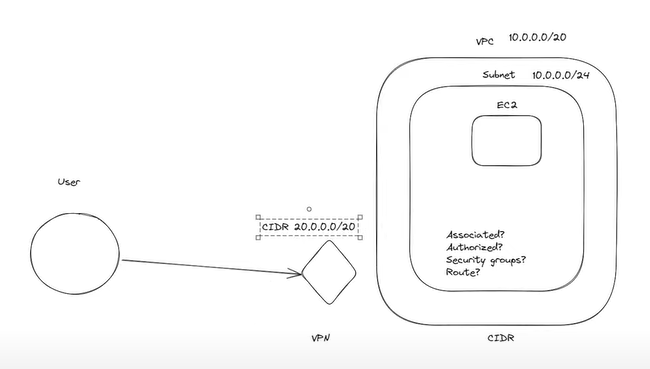
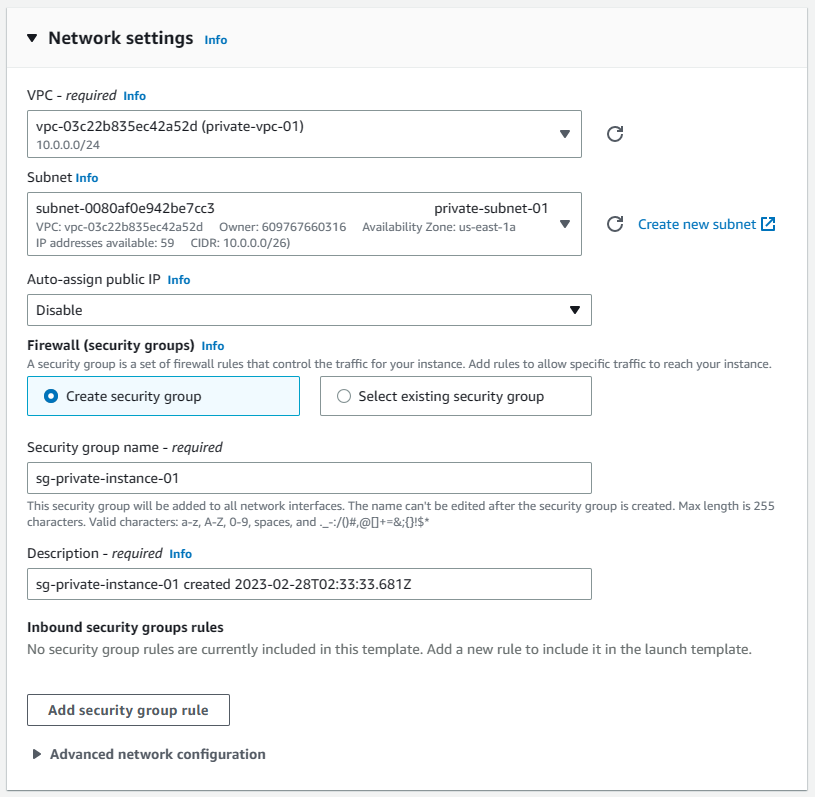
**AWS Client VPN Setup VPC**

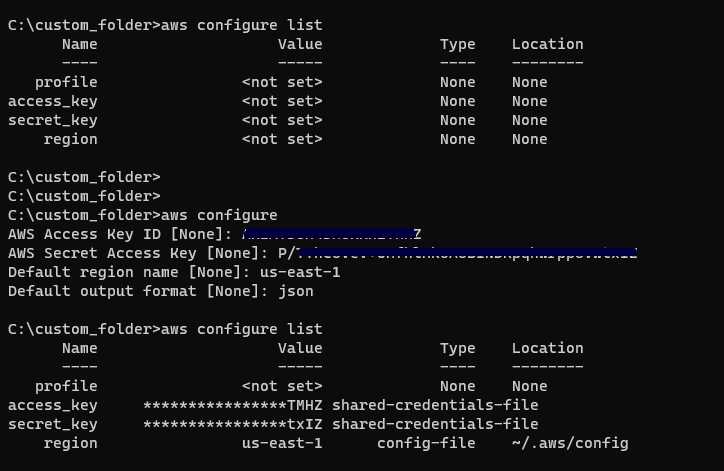
1. **Links** 
   1. [AWS Client VPN | Setup VPC from scratch - YouTube](https://www.youtube.com/watch?v=A-Sy5so0Nqs&ab_channel=theRDnotes)
   2. [Getting started with Client VPN - AWS Client VPN (amazon.com)](https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-getting-started.html#cvpn-getting-started-certs)
   3. [Installing or updating the latest version of the AWS CLI - AWS Command Line Interface (amazon.com)](https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html)
   4. [How do I fix the error "Unable to locate credentials" when I connect to my S3 bucket with AWS CLI? - YouTube](https://www.youtube.com/watch?v=UMUQs2PojdE&ab_channel=AmazonWebServices)
   5. [Client authentication - AWS Client VPN (amazon.com)](https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/client-authentication.html#mutual)
   6. [CIDR to IPv4 Address Range Utility Tool | IPAddressGuide](https://www.ipaddressguide.com/cidr)
2. **Diagram**



1. **Create a VPC with IP 10.0.0.0/24**
2. **Create a Subnet under created VPC with IP 10.0.0.0/26**
3. **Create Instance**
4. Select our created VPC and subnet,
5. Store key pair in “. pem” format for further use.
6. Disable Auto-assign public IP
7. Remove all security group rule



1. **Install and configure AWS CLI**
   1. Install AWS CLI from: [Installing or updating the latest version of the AWS CLI - AWS Command Line Interface (amazon.com)](https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html)
   2. Configuration AWS with access key and secret key



1. **To generate server and client certificates and keys and upload them to ACM**

Source: [Client authentication - AWS Client VPN (amazon.com)](https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/client-authentication.html#mutual)

1. Open the [EasyRSA releases](https://github.com/OpenVPN/easy-rsa/releases" \t "_blank) page and download the ZIP file for your version of Windows and extract it.
2. Open a command prompt and navigate to the location that the EasyRSA-3.x folder was extracted to.
3. Run the following command to open the EasyRSA 3 shell.

C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat

1. Initialize a new PKI environment.

# ./easyrsa init-pki

1. To build a new certificate authority (CA), run this command and follow the prompts.

# ./easyrsa build-ca nopass

1. Generate the server certificate and key.

# ./easyrsa build-server-full server nopass

1. Generate the client certificate and key.

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

You can optionally repeat this step for each client (end user) that requires a client certificate and key.

1. Exit the EasyRSA 3 shell.

# exit

1. 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 C:\ drive.

C:\Program Files\EasyRSA-3.x> mkdir C:\*custom\_folder*

C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\*custom\_folder*

C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\*custom\_folder*

C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\*custom\_folder*

C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:\*custom\_folder*

C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:\*custom\_folder*

C:\Program Files\EasyRSA-3.x> cd C:\*custom\_folder*

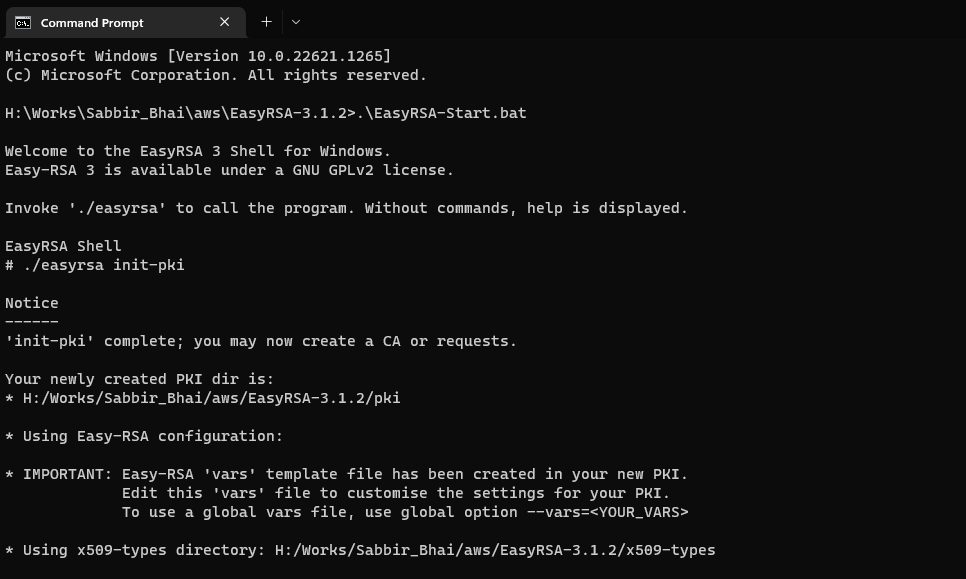
1. Upload the server certificate and key and the client certificate and key to ACM. Be sure to upload them in the same Region in which you intend to create the Client VPN endpoint. The following commands use the AWS CLI to upload the certificates. To upload the certificates using the ACM console instead, see [Import a certificate](https://docs.aws.amazon.com/acm/latest/userguide/import-certificate-api-cli.html) in the *AWS Certificate Manager User Guide*.

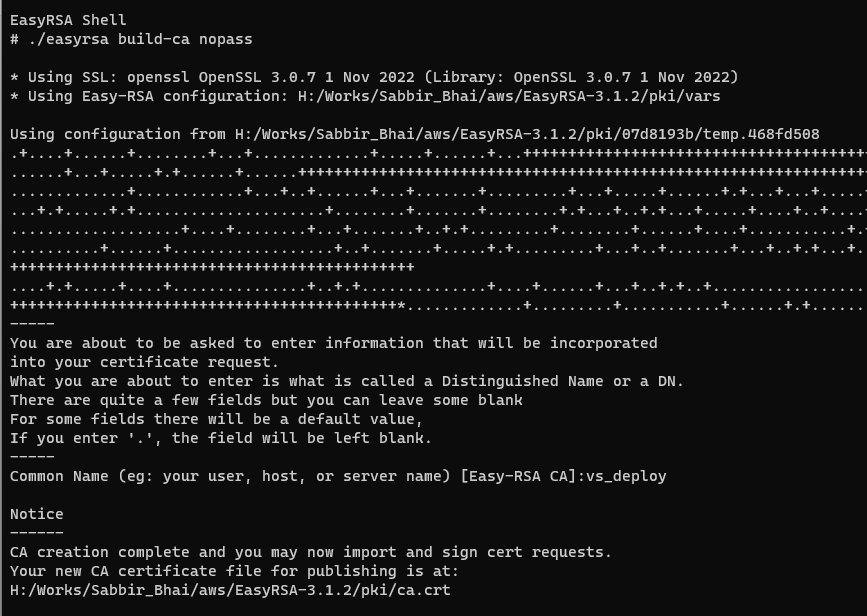
aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key --certificate-chain fileb://ca.crt --region [your-preferred-region]

aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt --region [your-preferred-region]

You do not necessarily need to upload the client certificate to ACM. If the server and client certificates have been issued by the same Certificate Authority (CA), you can use the server certificate ARN for both server and client when you create the Client VPN endpoint. In the steps above, the same CA has been used to create both certificates. However, the steps to upload the client certificate are included for completeness.

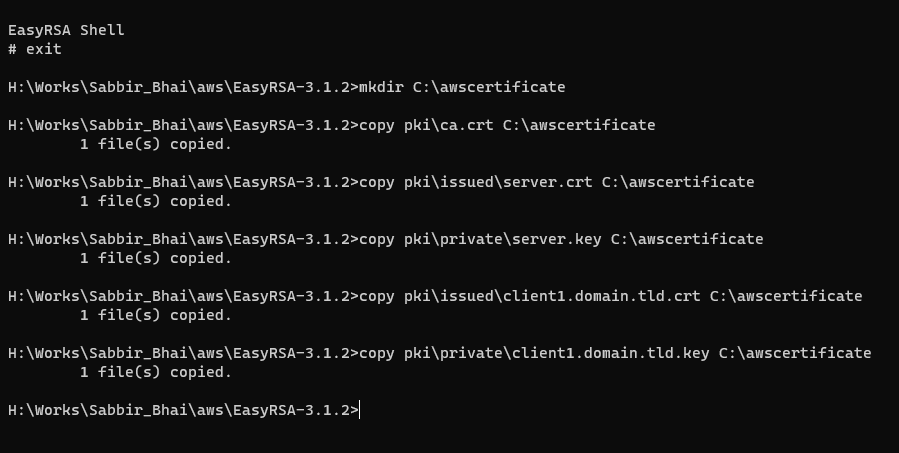
Demos:

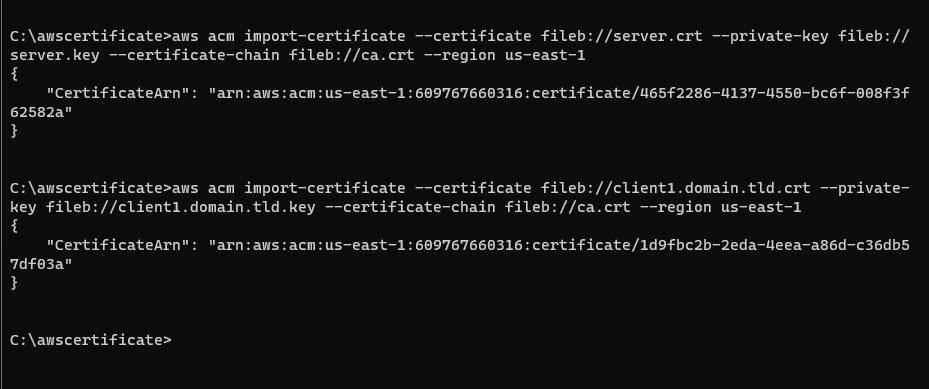




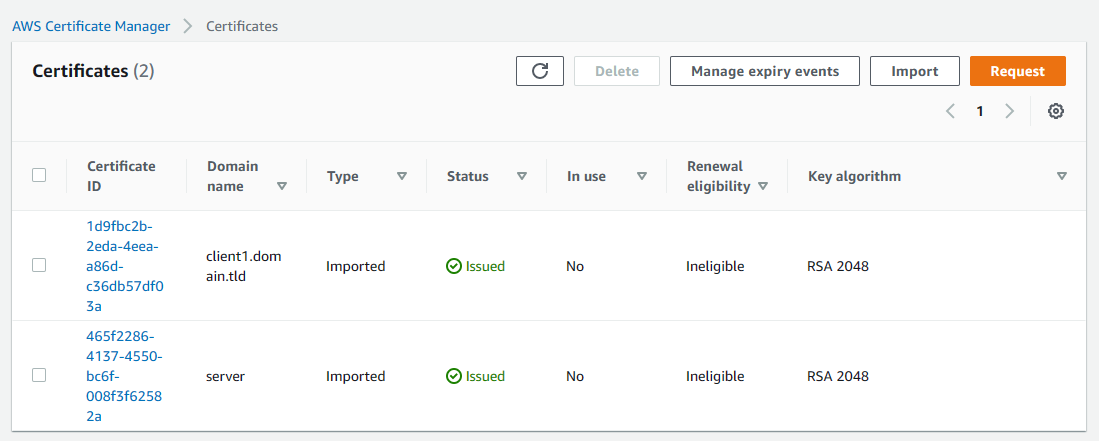




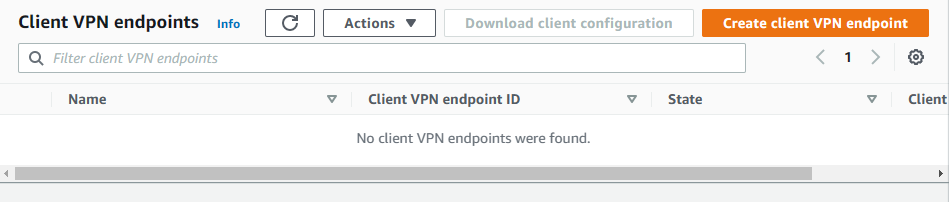




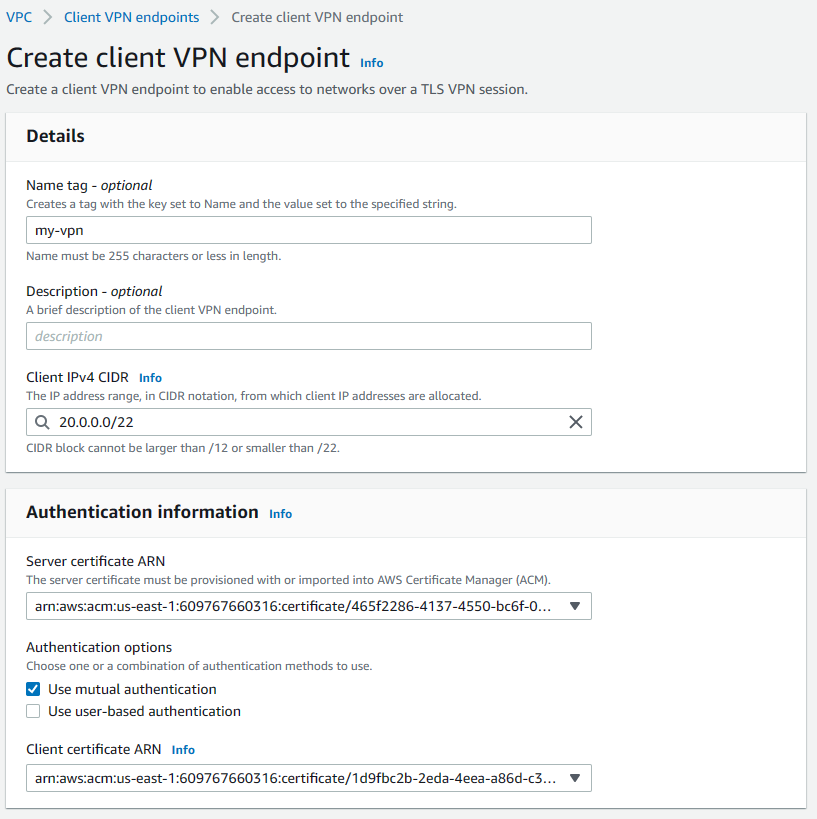
After all this process done check certificates on AWS console

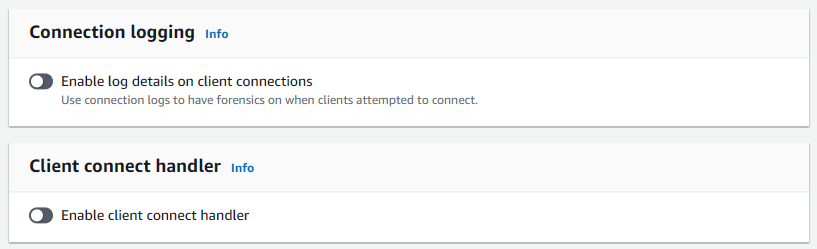


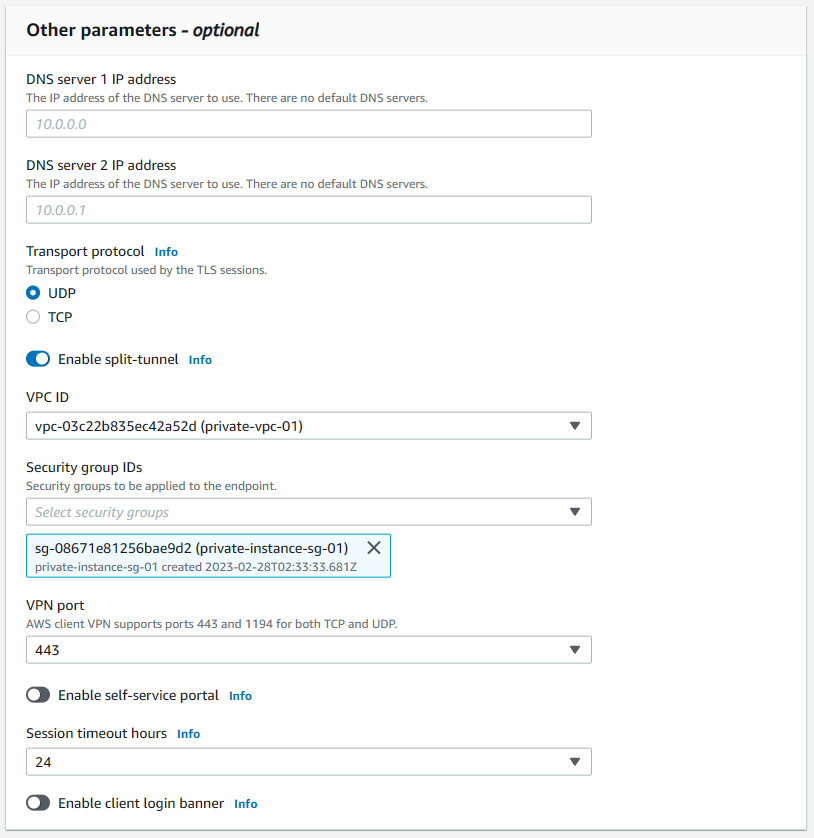
1. **Navigate to Services->VPC->VPN->Client VPN endpoints**

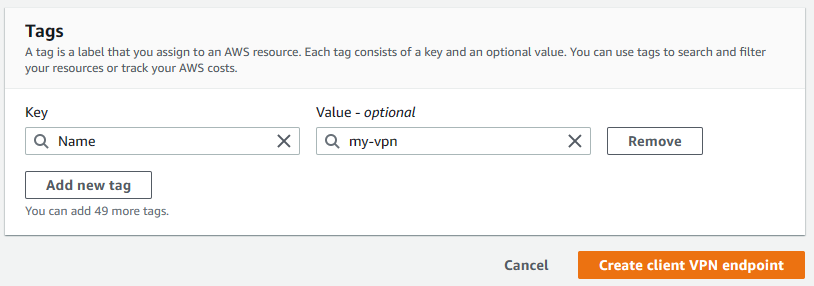


1. **Setup like below**

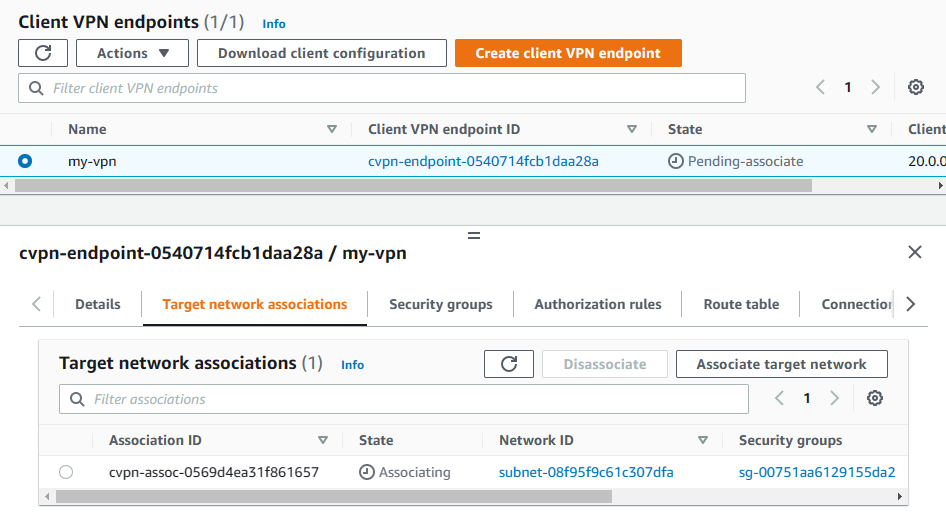




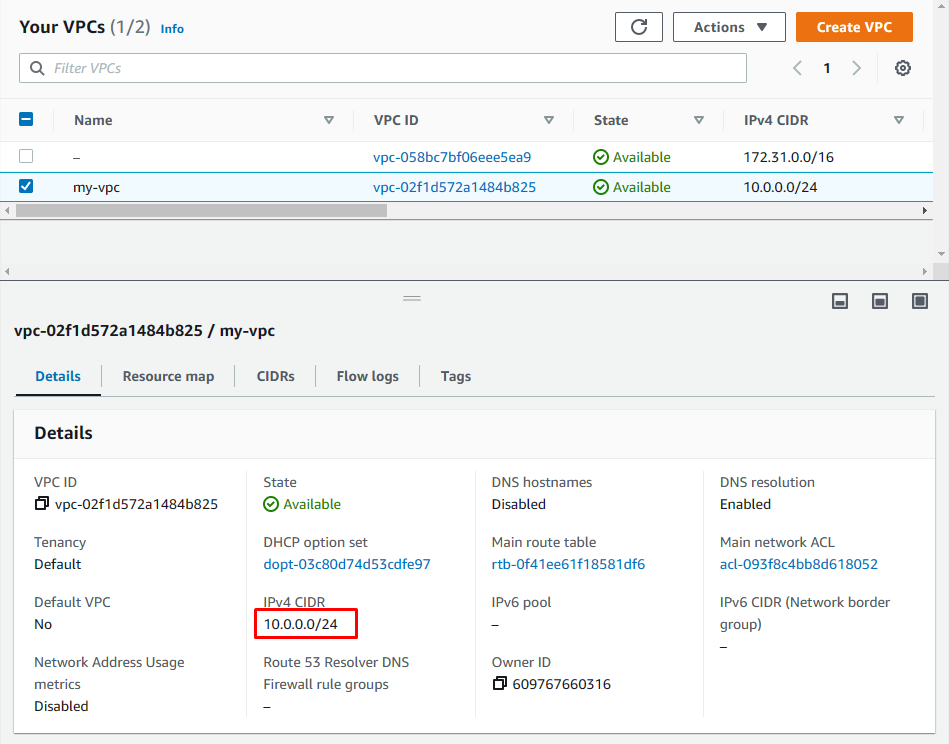


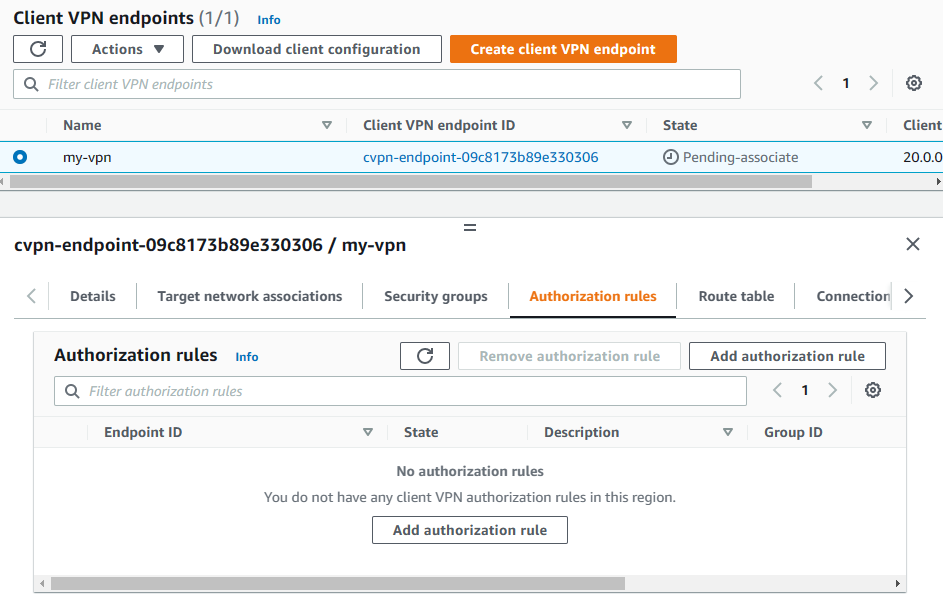


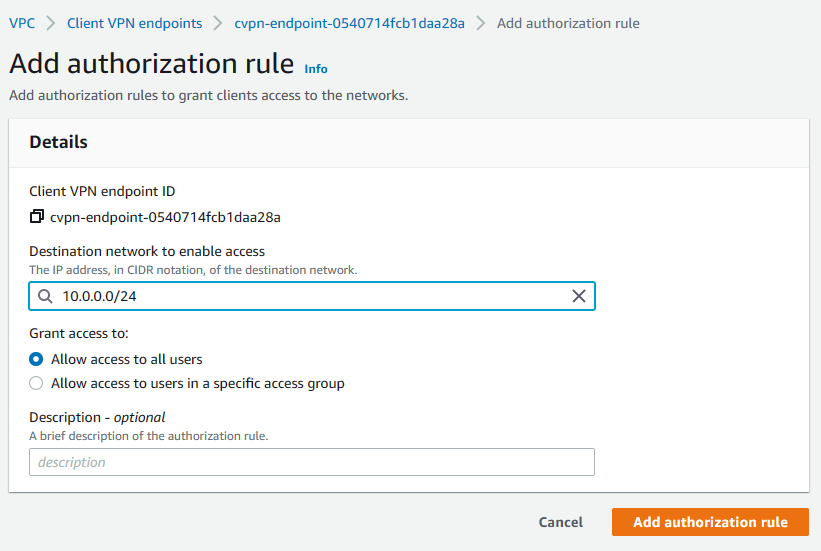
1. **Associate target network**



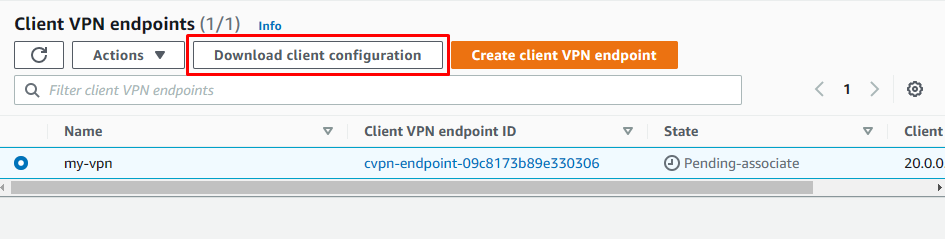
1. **Add authorization rules with VPC IP – get IP from VPC**







1. **Download client configuration and store it for further use**



1. **Open the Client VPN endpoint configuration file using your preferred text editor. Add <cert></cert> and <key></key> tags to the file. Place the contents of the client certificate and the contents of the private key between the corresponding tags, as such:**

<cert>

Contents of client certificate (.crt) file

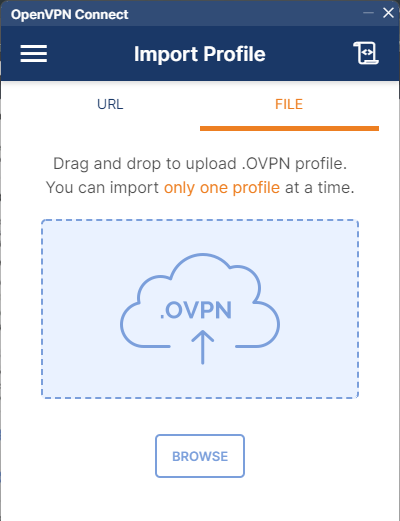
</cert>

<key>

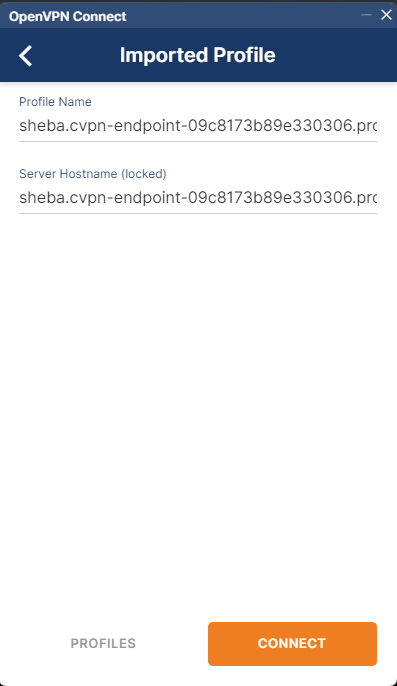
Contents of private key (.key) file

</key>

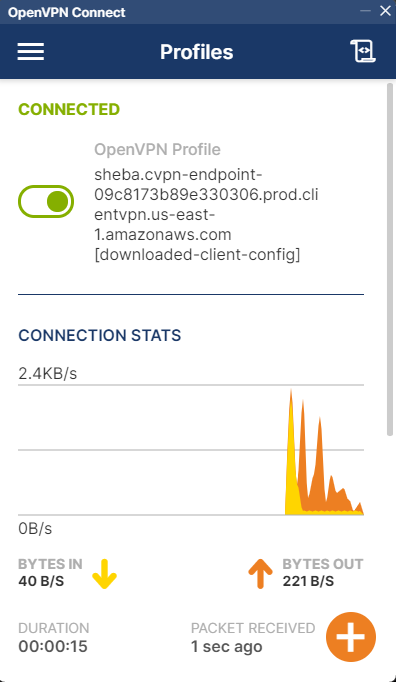
1. **Locate the line that specifies the Client VPN endpoint DNS name, and prepend a random string to it so that the format is random\_string.displayed\_DNS\_name. For example:**
   1. Original DNS name: cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com
   2. Modified DNS name: asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com
2. **Download and install OpenVPN** [Community Downloads | OpenVPN](https://openvpn.net/community-downloads/)
3. **Open OpenVPN**



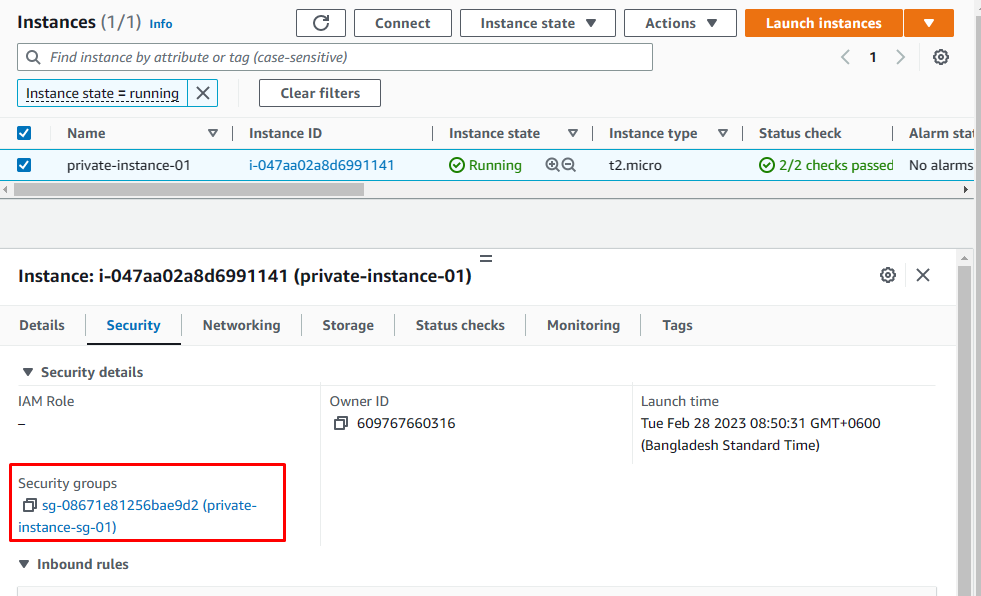
1. **Browse and select .ovpn file and click to connect**



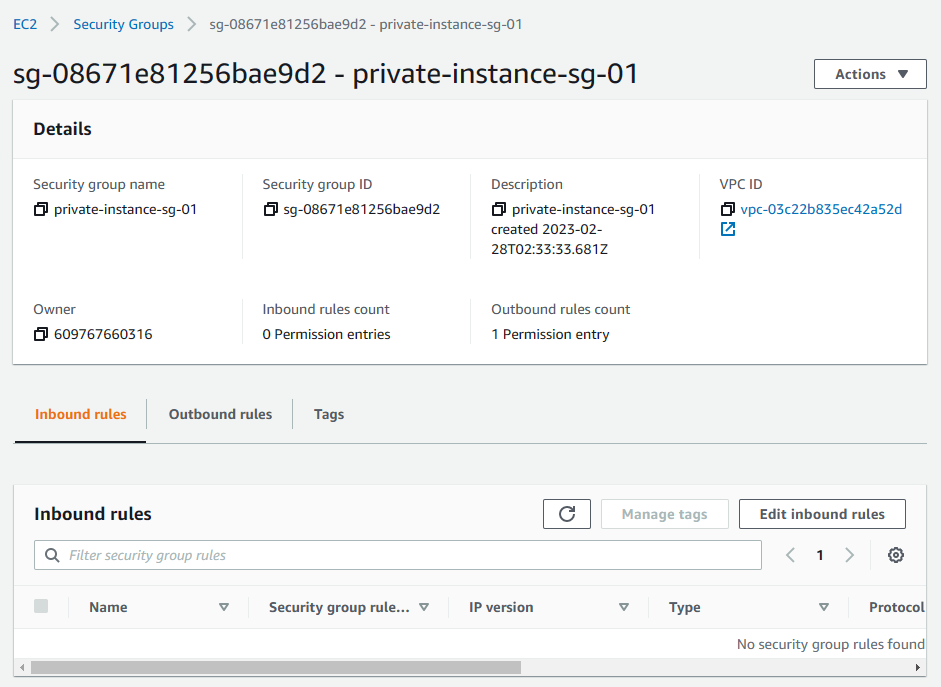
1. **If success is show like this**



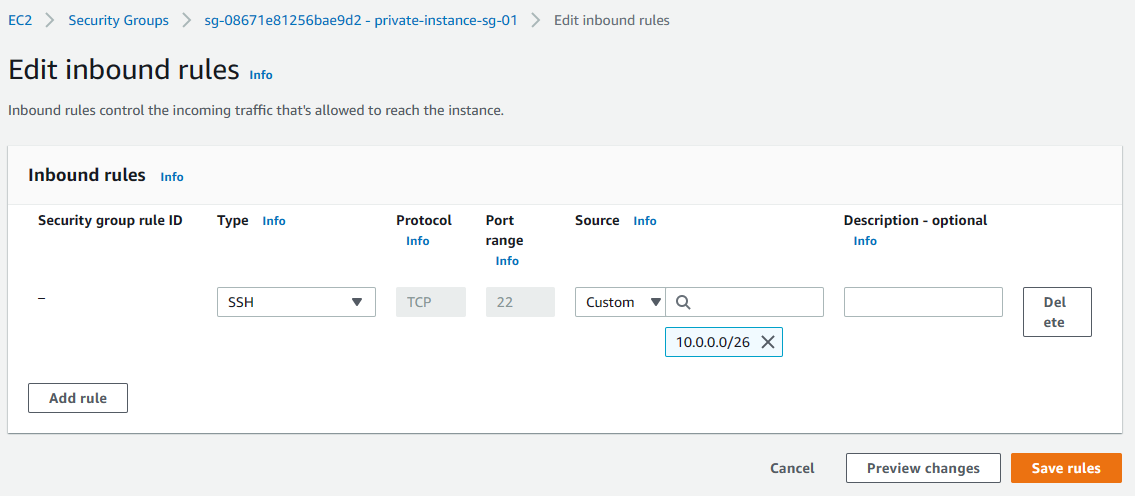
1. **Edit security group**



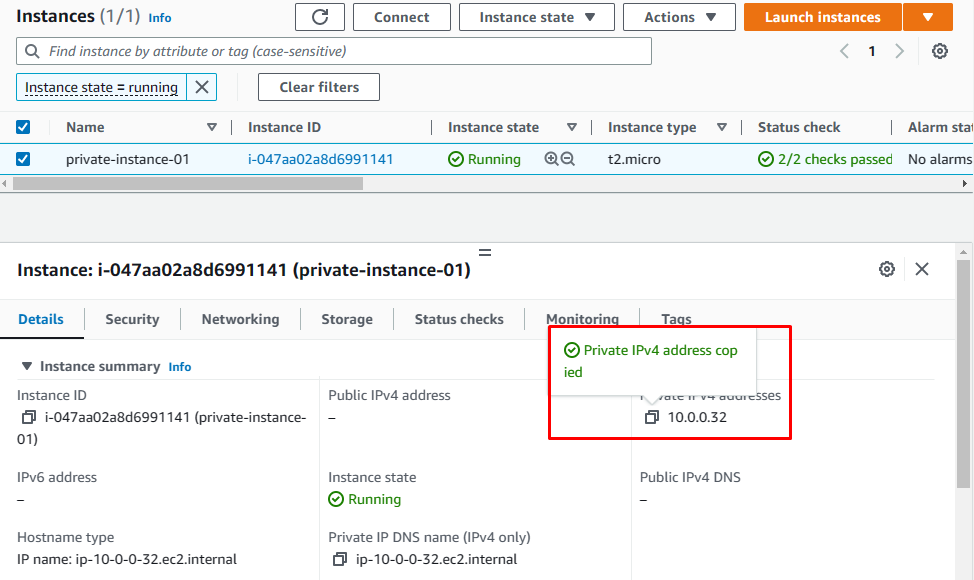
1. **Add inbound rules**



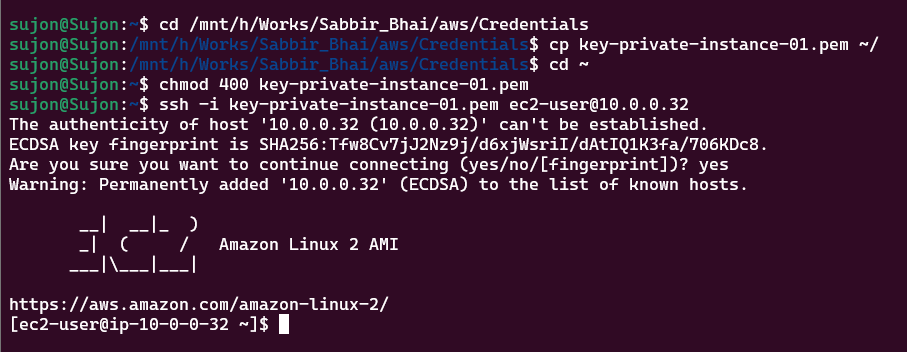
1. **Add role type=SSH and IP as 10.0.0.0/26 (our private subnet ID, only allow this IP)**



1. **Get private IP address from instance**



1. **Connect with Ubuntu terminal**



1. **Delete**
2. **Client VPN endpoints – disassociate**
3. **Client VPN endpoints – delete**
4. **Delete instance**
5. **Delete subnets**
6. **Delete VPC**
7. **Delete certificates**