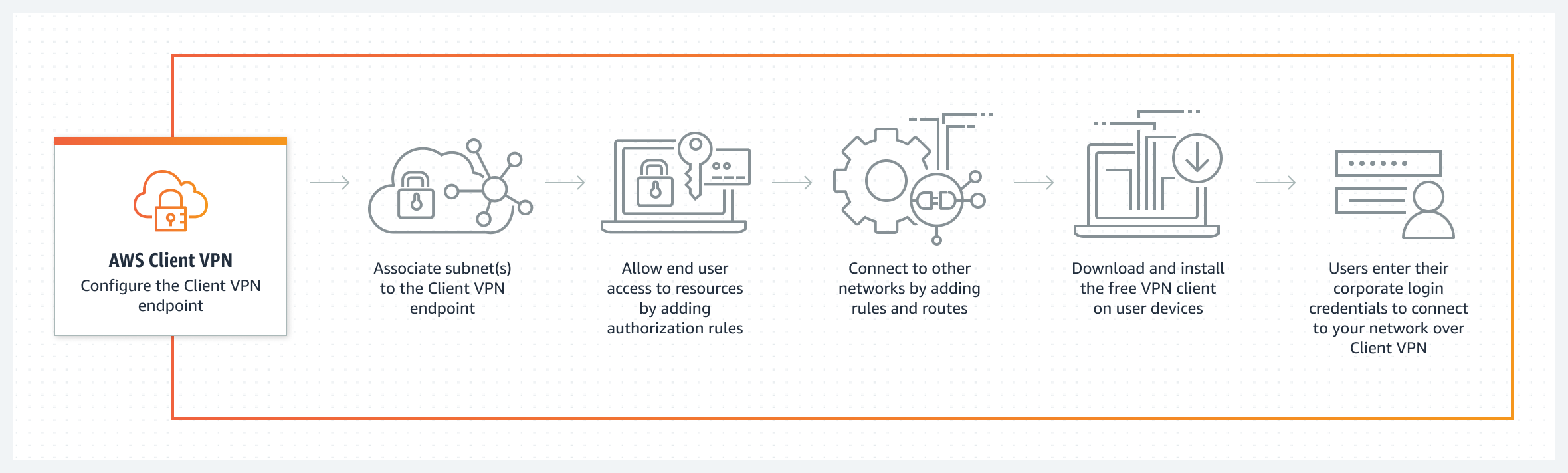
**AWS Client VPN | ACM**

[AWS Client VPN – Mutual authentication -certification-based]

**Introduction**

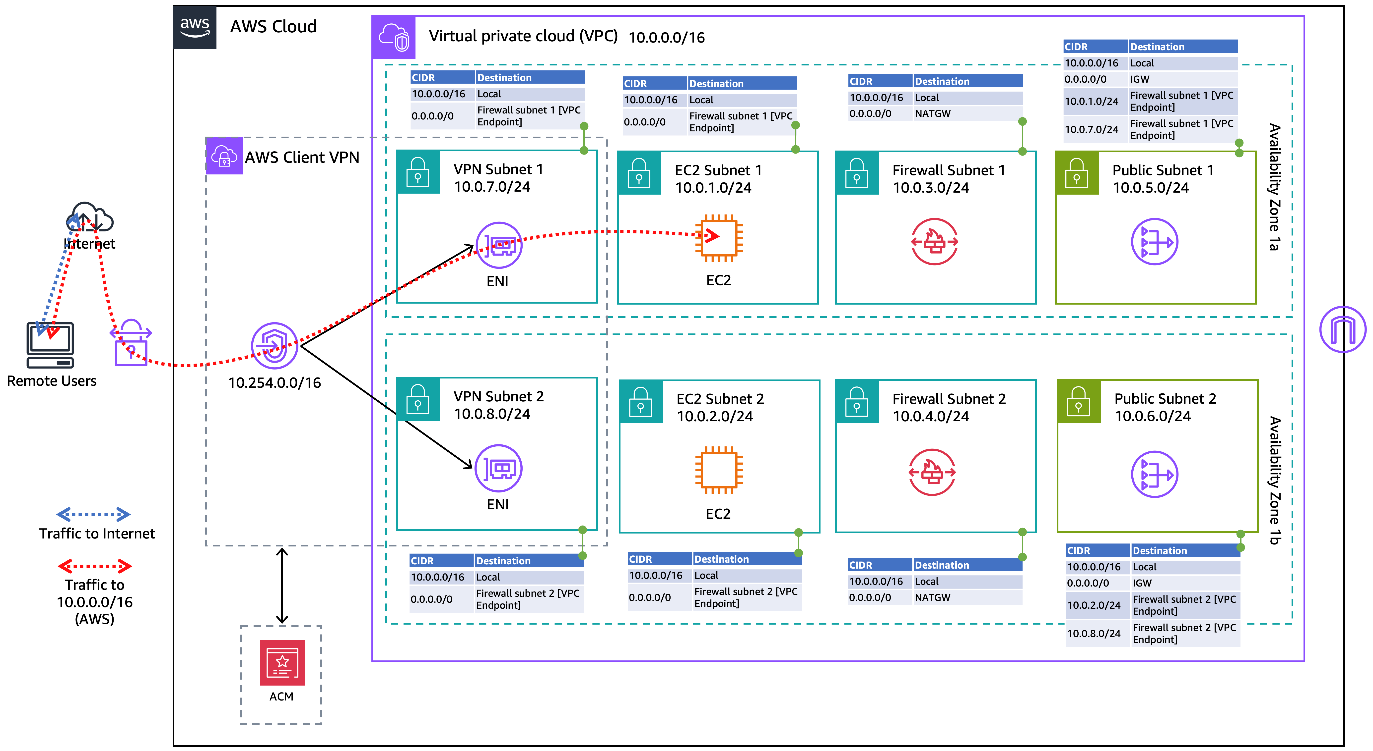
AWS Client VPN is a fully managed remote access VPN solution used by your remote workforce to securely access resources within both AWS and on-premises network.



**Project Description – Scenario**

In this project I will deploy AWS Client VPN based on an AWS CloudFormation configuration template and use ACM Certificate services for authentication, this project intend is to demonstrates connectivity to the EC2 instance inside the VPC.

**Architecture – Overview**



**Deploying AWS Client VPN using Infrastructure as Code [IAC]**

**A screenshot of a computer

Description automatically generated**

**RSA Certificate Creation with manual authentication**

Client VPN uses certificates to perform authentication between the client and the server. Certificates are a digital form of identification issued by a certificate authority (CA). The server uses client certificates to authenticate clients when they attempt to connect to the Client VPN endpoint. You must create a server certificate and key, and at least one client certificate and key.

RSA Certificates.

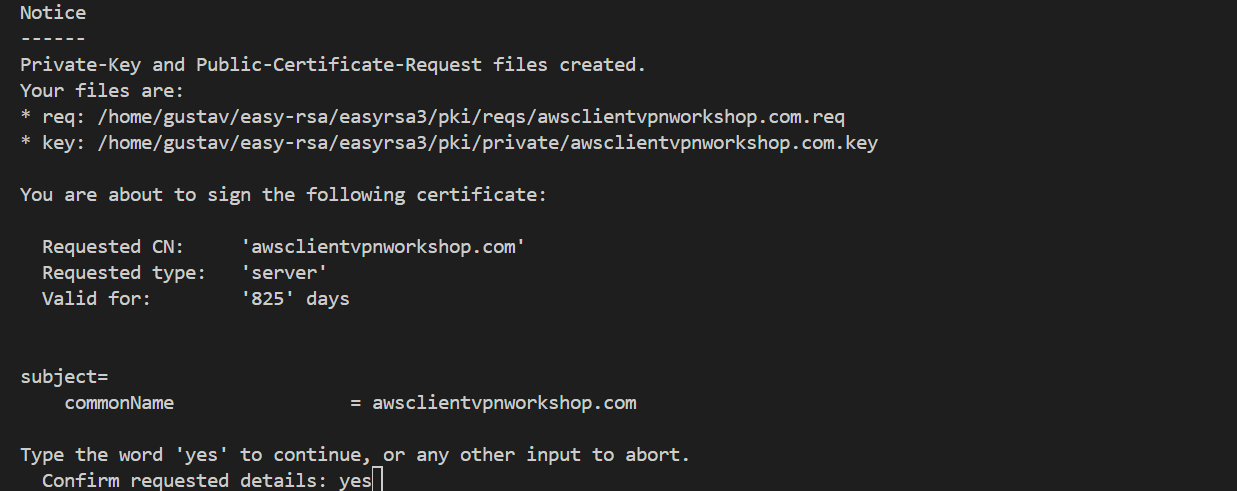
A computer screen shot of a program

Description automatically generated

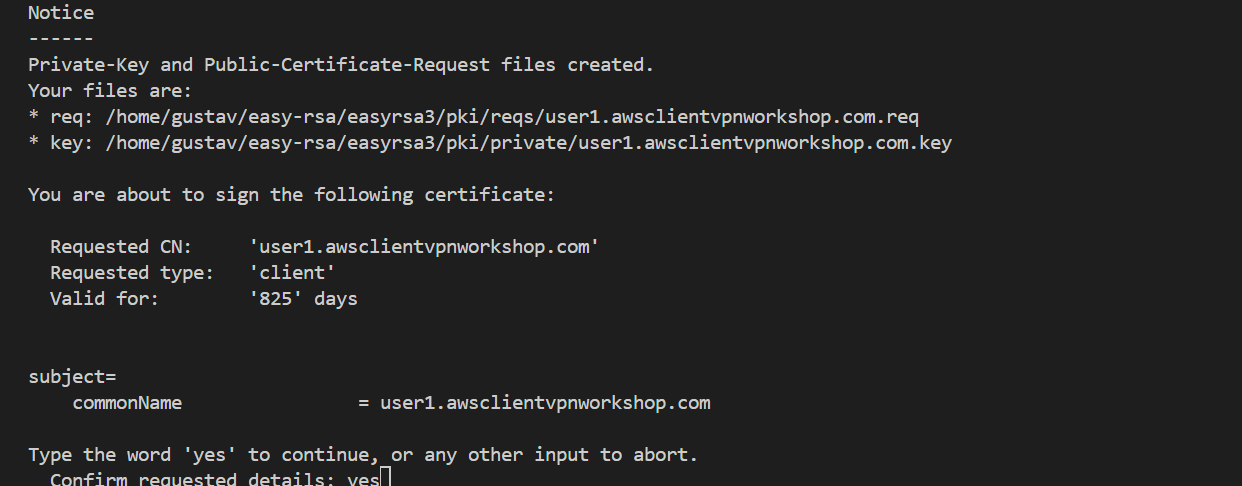
A black background with white text

Description automatically generated

Server keys with OpenVPN. Server



Client keys with OpenVPN. Server



**Upload to AWS Certificate Manager**

Upload certificates to AWS Certificate Manager for the Client VPN endpoint.

A screenshot of a computer

Description automatically generated

**Note-FYI**

*You must upload the server certificate to AWS Certificate Manager (ACM) and specify it when you create a Client VPN endpoint. When you upload the server certificate to ACM, you also specify the certificate authority (CA).*

**AWS Client VPN setup with Mutual authentication [certificate-based**

Creating a Client VPN endpoint will allow your clients to establish a VPN session. Clients can only establish a VPN connection after you associate at least one target network.

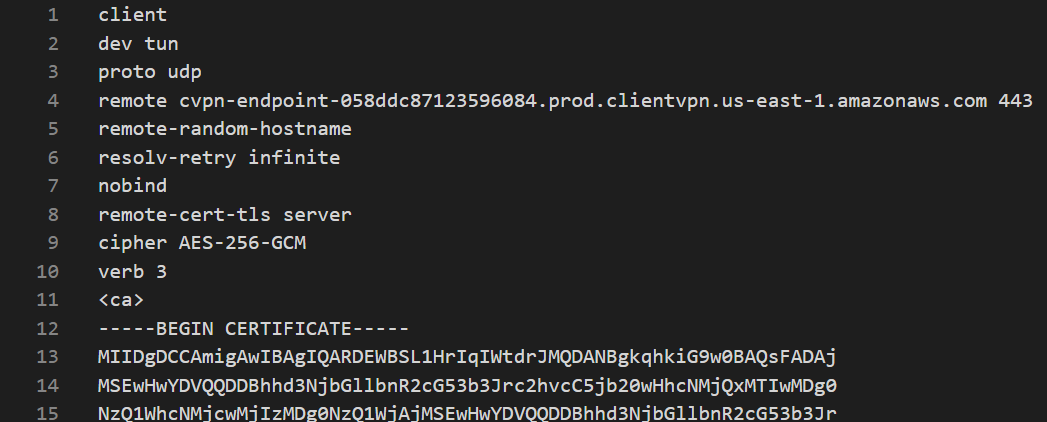
A screenshot of a computer

Description automatically generated

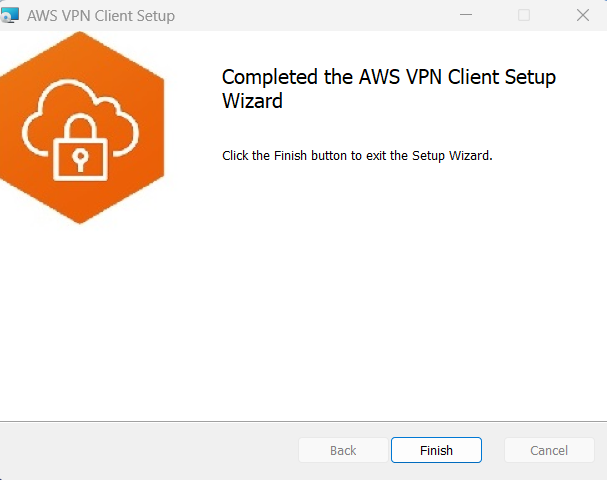
Clients can now establish a VPN connection and access resources in the VPC due to the authorization rules added.

**Download & customize Client VPN endpoint configuration file**

Prepare the Client VPN endpoint configuration file. The configuration file includes the Client VPN endpoint details and certificate information required to establish a VPN connection.

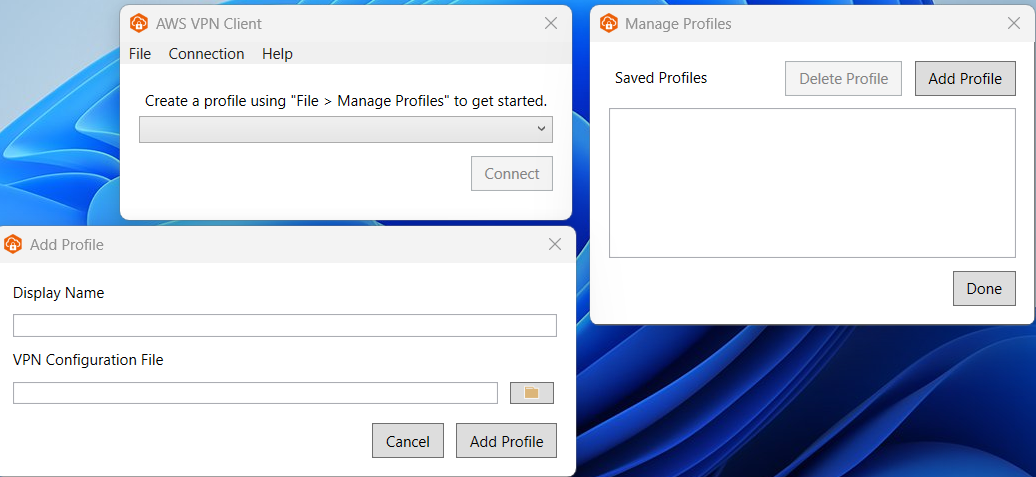


**Connect to AWS Client VPN endpoint with AWS provided client**

****

**Configured with VPN Configuration files**

This file is for the end users who needs to connect to the Client VPN endpoint it includes the Client VPN endpoint details and certificate information required to establish a VPN connection.

****

**Connected**

A screenshot of a computer

Description automatically generated

In this part I used the EC2 instance private IP address and then using **AWS provided client VPN** to connect to the AWS Client VPN endpoint and performed a ping test to confirm connectivity to the EC2 instance inside the VPC.

