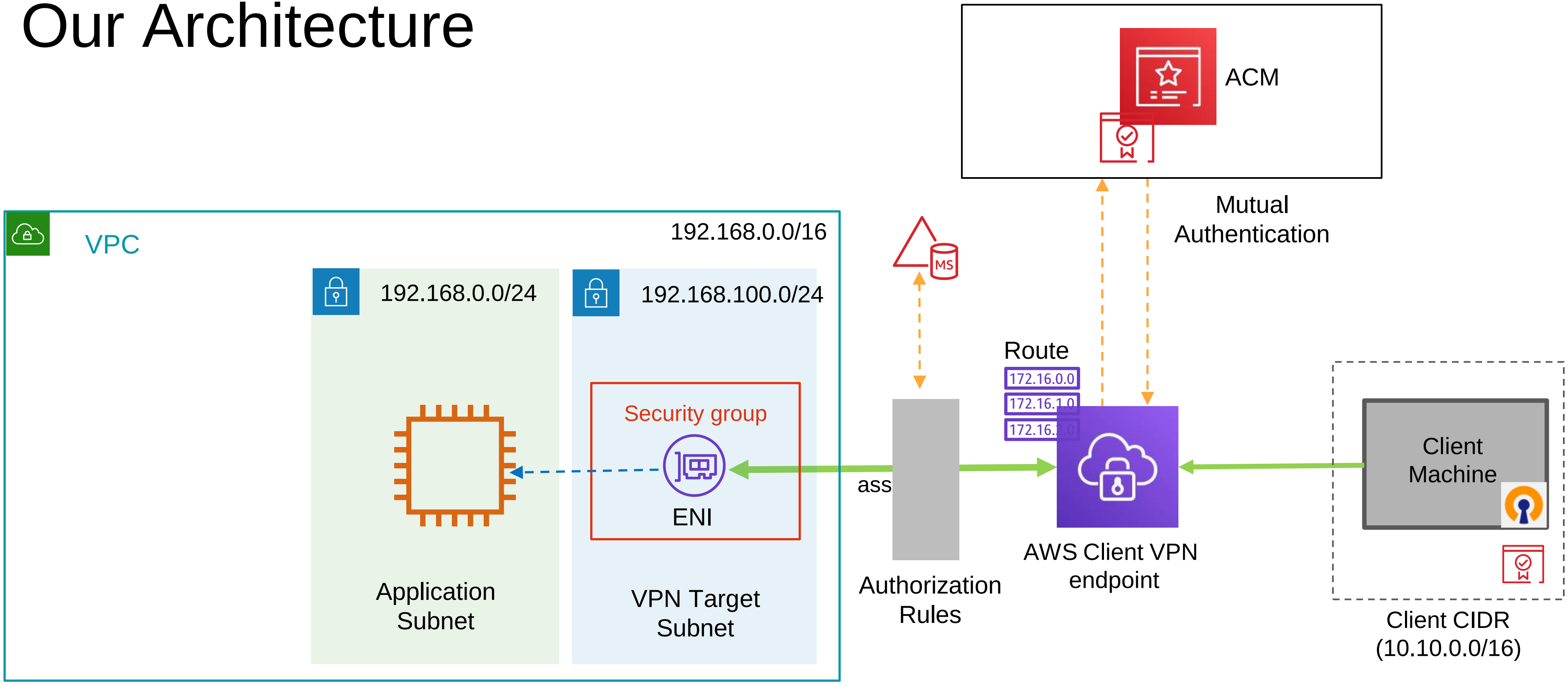
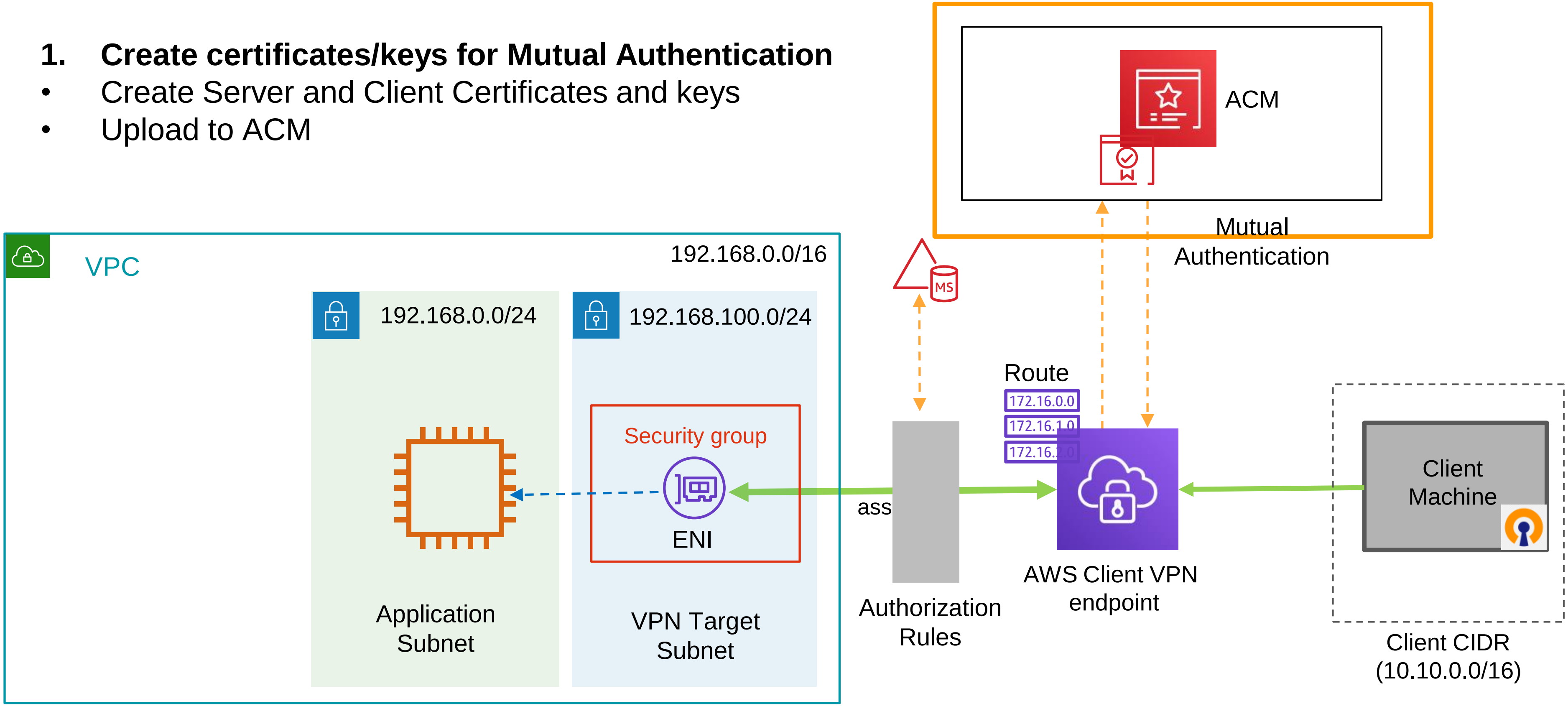
How to setup AWS Client VPN

Our Architecture



1. Create certificates/keys for Mutual Authentication

- Create Server and Client Certificates and keys
- Upload to ACM



https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/client-authentication.html#mutual

Create Server and Client certificates and keys

Run below commands from your workstation where you have AWS CLI installed (for linux)

1. Clone the easy-rsa repo

   ```
   $ git clone https://github.com/OpenVPN/easy-rsa.git
   $ cd easy-rsa/easyrsa3
   ```

2. Initialize PKI environment

   ```
   $ ./easyrsa init-pki
   ```

3. Create new Certification Authority (CA)

   ```
   $ ./easyrsa build-ca nopass
   ```

4. Generate the server certificate and key

   ```
   $ ./easyrsa build-server-full server nopass
   ```

Create Server and Client certificates and keys

5. Generate the client certificate and key

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

6. Copy server and client certificates and keys to one directory

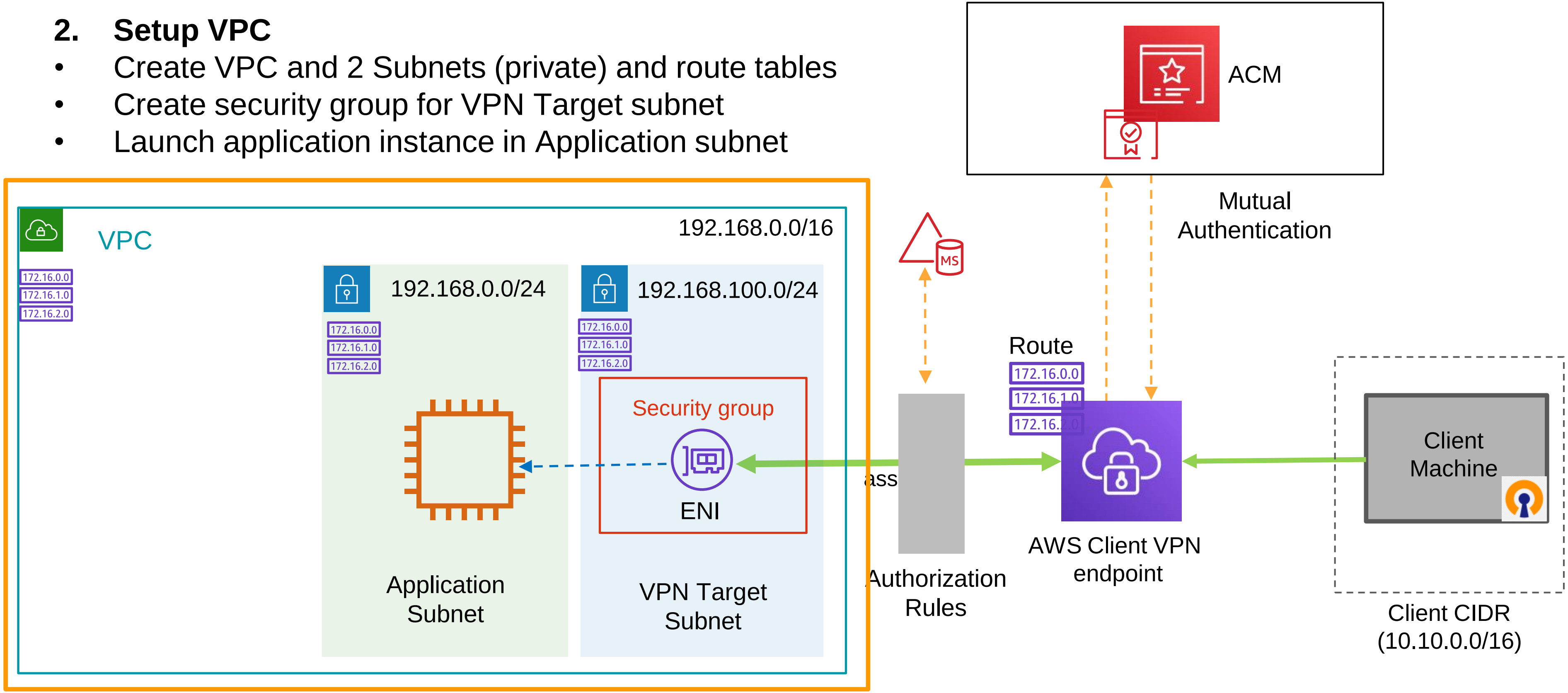
```
$ mkdir ~/demo
$ cp pki/ca.crt ~/demo/
$ cp pki/issued/server.crt ~/demo/
$ cp pki/private/server.key ~/demo/
$ cp pki/issued/client1.domain.tld.crt ~/demo/
$ cp pki/private/client1.domain.tld.key ~/demo/
$ cd ~/demo
```

7. Upload the certificate and keys to ACM

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key --certificate-chain fileb://ca.crt --region ap-south-1
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt --region ap-south-1
```

2. Setup VPC

- Create VPC and 2 Subnets (private) and route tables
- Create security group for VPN Target subnet
- Launch application instance in Application subnet

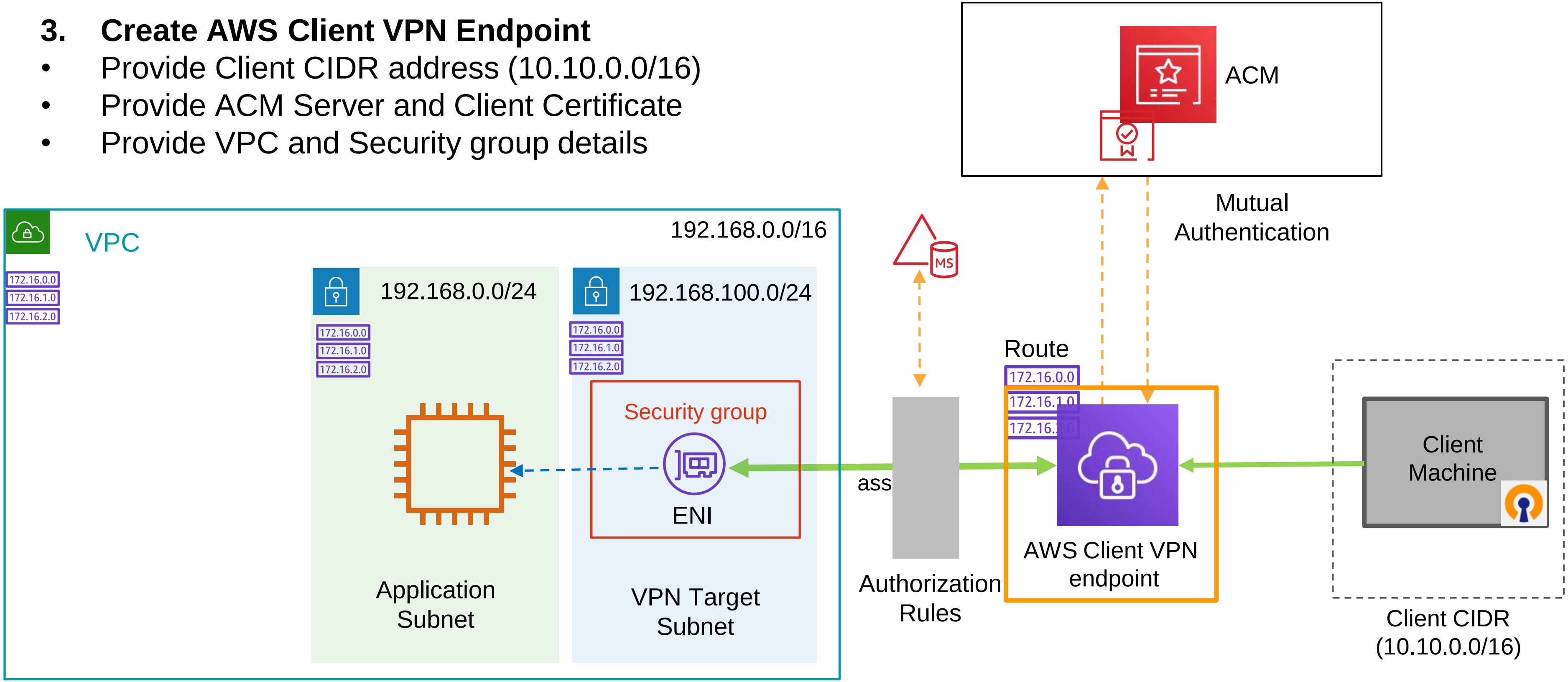


Steps to setup VPC

1. Create VPC (name=demo) with CIDR 192.168.0.0/16
2. Create private subnet “demo-app-1” with CIDR 192.168.0.0/24
3. Create corresponding route table “demo-app-rt” with just a local route & associate with subnet “demo-app-1”
4. Create private subnet “demo-client-vpn-1” with CIDR 192.168.100.0/24
5. Create corresponding route table “demo-client-vpn-rt” with just a local route & associate with subnet “demo-client-vpn-1”
6. Create security group “demo-client-vpn-sg”
    - Do not add any inbound rules
    - All outbound should be allowed (All traffic – 0.0.0.0/0)
7. Launch application EC2 instance in “demo-app-1” subnet
    - Security group inbound rule should allow “All traffic” from security group “demo-client-vpn-sg” created in step 6

3. Create AWS Client VPN Endpoint

- Provide Client CIDR address (10.10.0.0/16)
- Provide ACM Server and Client Certificate
- Provide VPC and Security group details

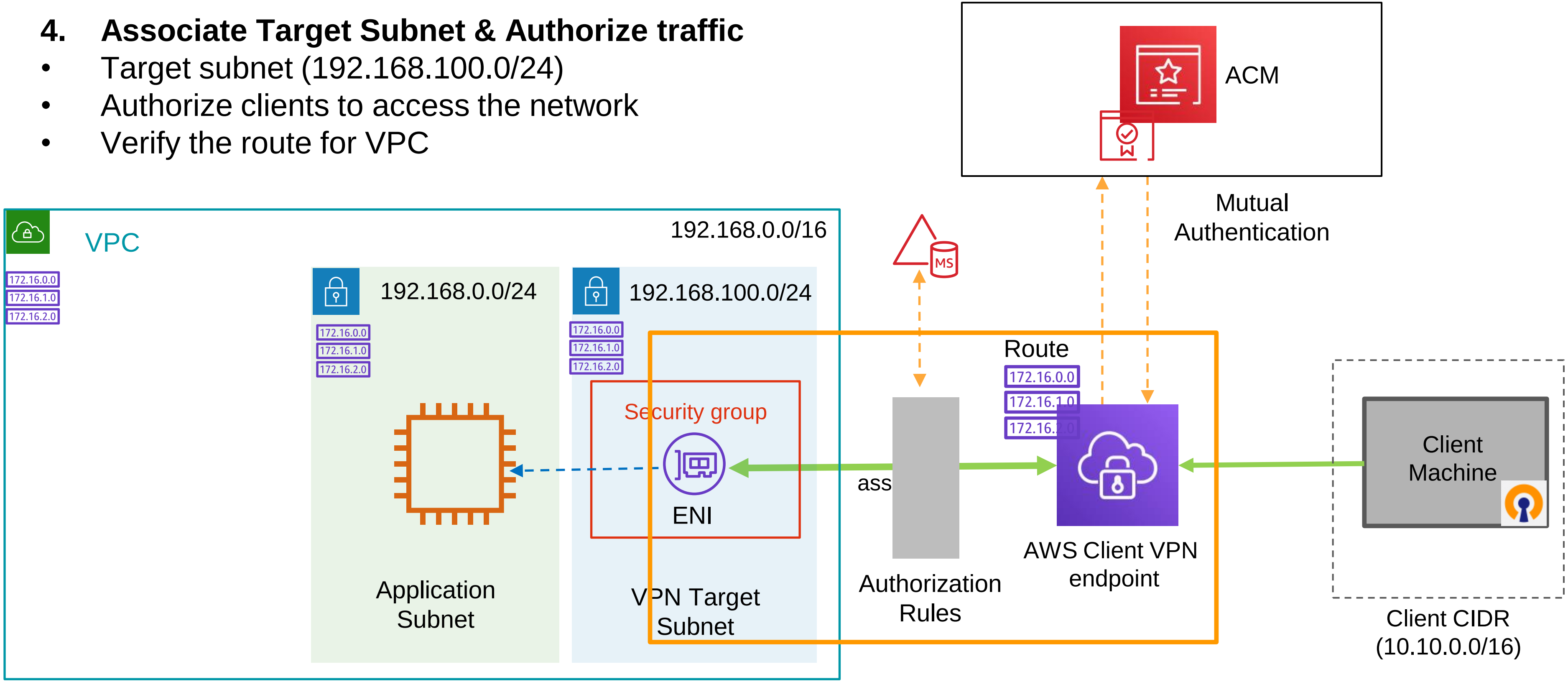


Steps to create Client VPN endpoint

- Provide name “demo-client-vpn-endpoint” and description
- Client IPv4 CIDR: 10.10.0.0/16
- Server Certificate ARN: Choose the Server Certificate created earlier
- Authentication Options: Choose “Use Mutual Authentication”
- Client certificate ARN: Choose the Client Certificate created earlier
- Connection Logging: No
- Transport Protocol: TCP
- VPC ID: Choose “demo” VPC created in Step 2
- Security Group IDs: Select the “demo-client-vpn-sg” created earlier
- VPN port: 443
- Create Client VPN Endpoint

4. Associate Target Subnet & Authorize traffic

- Target subnet (192.168.100.0/24)
- Authorize clients to access the network
- Verify the route for VPC



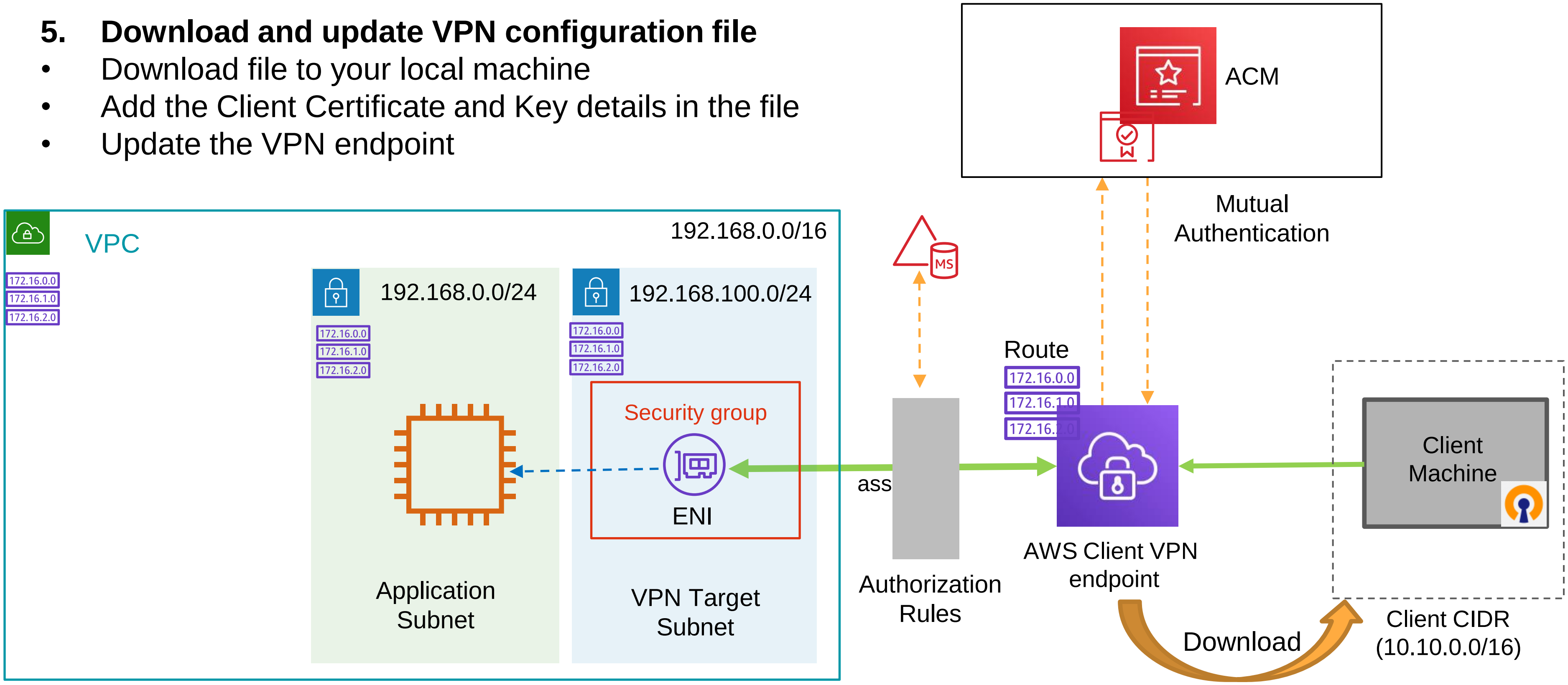
Steps to associate Target Subnet and Authorize traffic

- Select the Client VPN endpoint created earlier
- Go to Associations and associate the target subnet “demo-client-vpn-1”
- Go to Authorizations and choose Authorize Ingress
  - For Destination Networks to enable -> Enter the VPC IP address 192.168.0.0/16
  - Grant access to -> Choose ”Allow access to all users”

- Add Authorization Rule

5. Download and update VPN configuration file

- Download file to your local machine
- Add the Client Certificate and Key details in the file
- Update the VPN endpoint



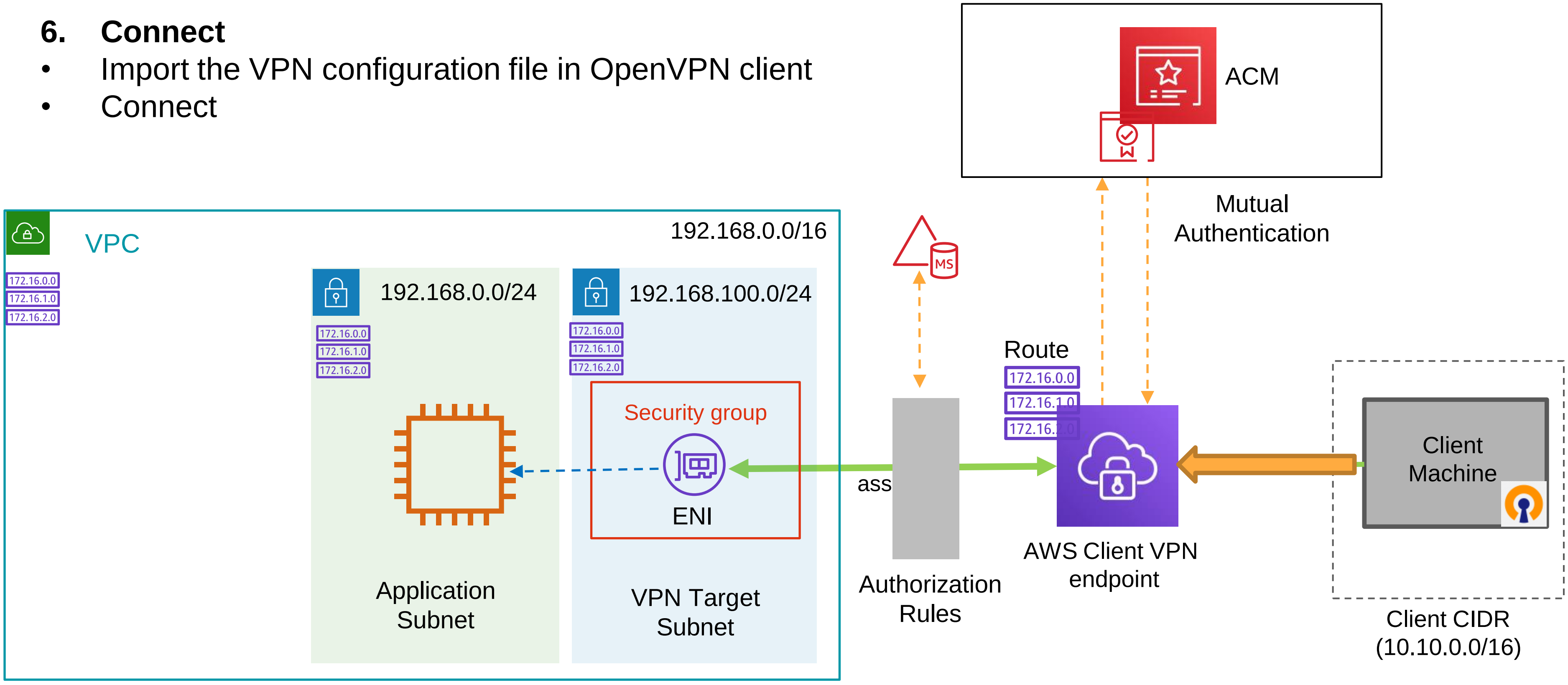
Steps to download and update VPN configuration file

- Select Client VPN endpoint and “Download Client Configuration” to your local workstation
- Copy the client certificate and client key created in Step 1 to any folder in local workstation
- Open the configuration file with any editor and add following lines
  - cert /path/to/client1.domain.tld.crt
  - key /path/to/client1.domain.tld.key

- Also, modify the endpoint dns name by adding random prefix
  - **Original**: cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com
  - **Modified**: xxxxxx.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com

6. Connect

- Import the VPN configuration file in OpenVPN client
- Connect

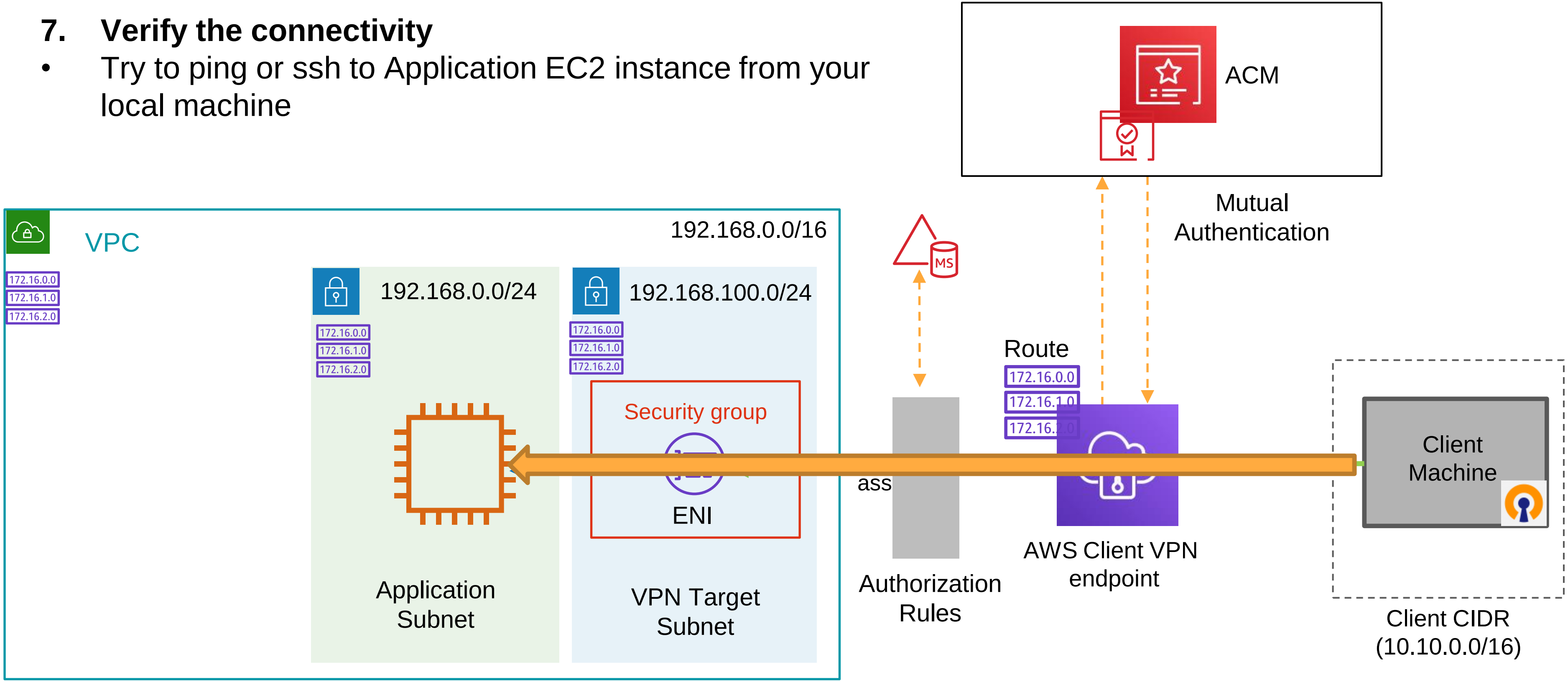


Steps to connect

- Pre-requisite: You should download and install OpenVPN client
  - https://openvpn.net/community-downloads/
- Import configuration file
- Connect

7. Verify the connectivity

- Try to ping or ssh to Application EC2 instance from your local machine



Steps to verify the VPN connection

- Get the private IP address of Application EC2 instance say 192.168.0.55
- Open the command prompt from your local workstation
    - ping 192.168.0.55
- If you are using Windows workstation, also try to open SSH connection to Application instance
- Try to access now internet from your local workstation
    - Browse any website -> Does not work
    - ping amazon.com -> Does not work
- Why ?