# How to setup VPN client endpoint

Generate server and client certificates:

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

1. Create temporary EC2 with IAM role containing “Administrator” permissions
2. Generate certificates on the EC2 by running the following commands:
   1. git clone <https://github.com/OpenVPN/easy-rsa.git>
      1. If git clone does not work 🡪 yum install git
   2. cd easy-rsa/easyrsa3
   3. ./easyrsa init-pki
   4. ./easyrsa build-ca nopass
   5. ./easyrsa build-server-full server nopass
   6. ./easyrsa build-client-full client1.domain.tld nopass
   7. mkdir ~/custom\_folder/
   8. cp pki/ca.crt ~/custom\_folder/
   9. cp pki/issued/server.crt ~/custom\_folder/
   10. cp pki/private/server.key ~/custom\_folder/
   11. cp pki/issued/client1.domain.tld.crt ~/custom\_folder
   12. cp pki/private/client1.domain.tld.key ~/custom\_folder/
   13. cd ~/custom\_folder/
   14. aws acm import-certificate --certificate fileb://server.crt --private-key fileb://server.key --certificate-chain fileb://ca.crt
   15. aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
3. Create VPN Endpoint:
   1. Go to the AWS VPC console and find “Client VPN endpoints” service.
   2. Click on Create VPN Endpoint button
   3. For the CIDR range define your VPC-s CIDR range. For example: 10.0.0.0/22
   4. Server cert -> select server cert.
      1. Use mutual authentication
   5. Client cert --> select server cert
   6. For the “DNS Server 1 IP address” define your VPC-s DNS server. If VPC CIDR range is 10.0.0.0/22 then this value is 10.0.0.2.
   7. “DNS Server 2 IP Address” set 8.8.8.8
   8. “Enable Split tunnel”
   9. VPC ID --> select your VPC
   10. For “Security group” it is highly advised to have a separate SG for this in order to control the traffic as you want. For that security group the only importance is that it must have outbound all enabled!   
       For inbound rules you can select what kind of ports are let in (for example SSH 22 only).
4. Now that the VPN Endpoint is created, next step is to select your VPN Endpoint and go to the “Target network associations” tab.
   1. Hit the Associate the target network button and Select **your VPC.**For subnet it does not matter which one you select from your VPC.
   2. Click on Associate target network button
5. Now navigate to the Authorization rules tab, and clidk on “Add authorization rule” button.
   1. Add whole VPC cider range, and “Allow access to all users”, except if you want to restrict it to specific users.
6. Wait for the state of your VPN endpoint to become Active and “Download the Client configuration” (on client VPN Endpoints console)
7. In the downloaded OVPN file, add the following sections to the end:
   1. <cert>  
      </cert>  
      <key>  
      </key>
8. Go to your EC2 instance, and find the previously created client certificate and list its contents:
   1. cat client1.domain.tld.crt
   2. Copy the content between (with these lines as well)
   3. -----BEGIN CERTIFICATE-----  
      -----END CERTIFICATE-----
   4. Copy it inside the <cert> section created in the downloaded OVPN file.
9. Execute the same with the key file:
   1. cat client1.domain.tld.crt
10. Delete this line if it exists in the OVPN file:
    1. **verify-x509-name server name**
11. When the VPN is in state Available, your chosen VPN client tool (*I recommend OpvenVpn Connect)* create a new profile, load the OVPN file and connect.
12. DONE! Your VPN connection should be up and running and you should be able to reach your EC2 instances in your subnet.

NOTE:  
Make sure that the security group of your instances allows in the Security group of the Client VPN Endpoint. You can either allow all traffic or only specific ports.