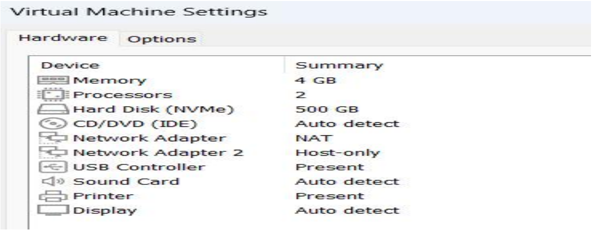
OpenVPN Server configuration

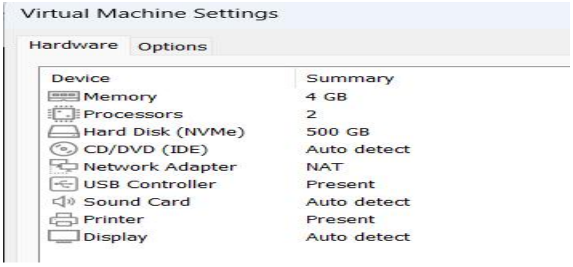
This document provides step by step guide to install OpenVPN server on CentOS 9 system. This lab requires 3 VM's . Update all the 3 systems with **sudo yum upadte -y** .

The OpenVPN Server VM requires 2 network cards. One network card in NAT mode and one in host only mode. Set the hostname of this machine as **openvpnserver**.



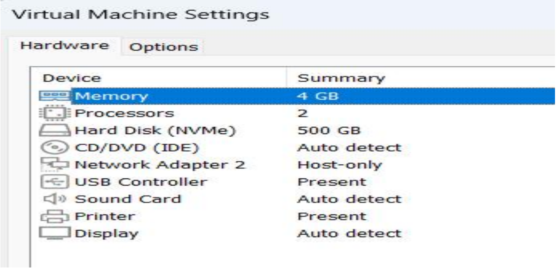
Device	Summary
Memory	4 GB
Processors	2
Hard Disk (NVMe)	500 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

The Remote client (VPN client) VM will have a single network card and it should be in NAT mode. Set the hostname for this machine as **client1**.



Device	Summary
Memory	4 GB
Processors	2
Hard Disk (NVMe)	500 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

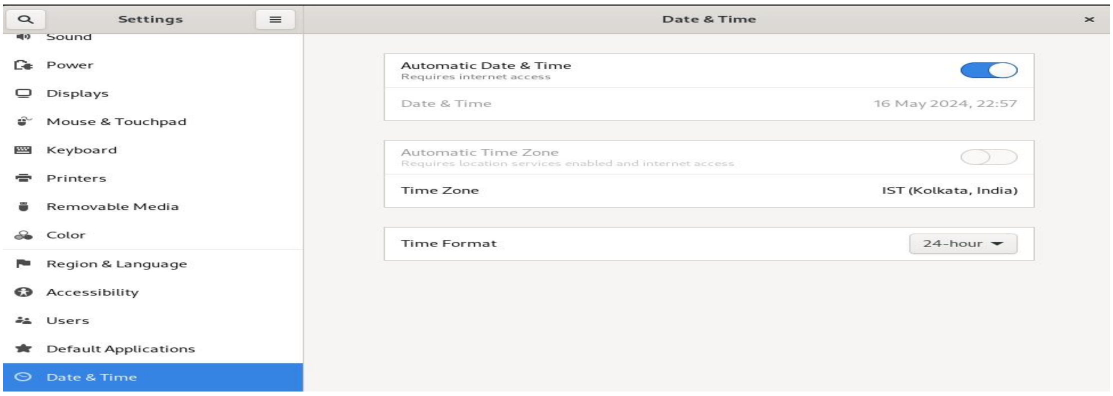
The LAN computer also will have a single network card and it should be in the host only mode.



Device	Summary
Memory	4 GB
Processors	2
Hard Disk (NVMe)	500 GB
CD/DVD (IDE)	Auto detect
Network Adapter 2	Host-only
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Create a user by name admin on all the 3 machines and provide that user sudo permissions.

Please set correct time zone on all the three machines.



Date & Time

Automatic Date & Time — Requires internet access — on

Date & Time: 16 May 2024, 22:57

Automatic Time Zone — Requires location services enabled and internet access — off

Time Zone: IST (Kolkata, India)

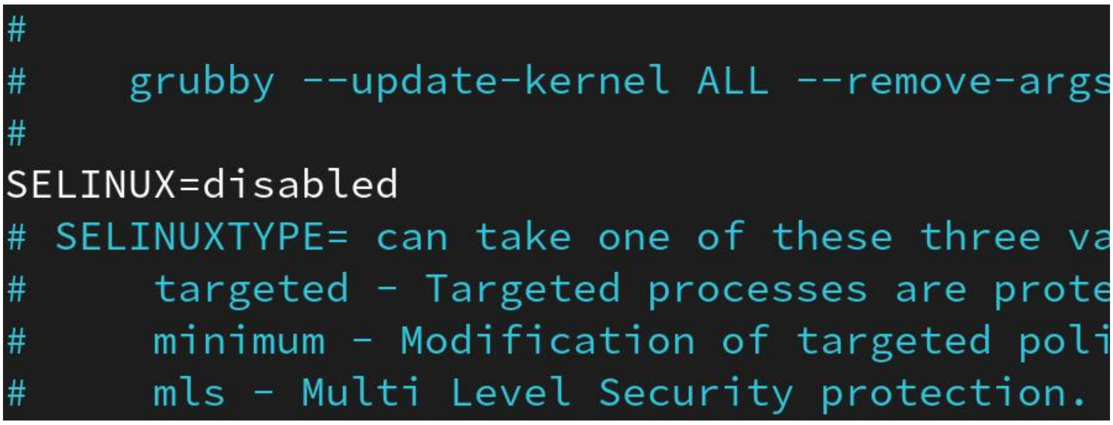
Time Format: 24-hour

OpenVPN Server configuration.

Perform the following steps on the VM which has 2 network cards I.e. the OpenVPN Server.

Disable Selinux

sudo vi /etc/selinux/config



```
#
#    grubby --update-kernel ALL --remove-args
#
SELINUX=disabled
# SELINUXTYPE= can take one of these three va
#     targeted - Targeted processes are prote
#     minimum - Modification of targeted poli
#     mls - Multi Level Security protection.
```

Save the file.

Give the command to set the current SELINUX status to permissive as the above setting will come in effect only after a system restart.

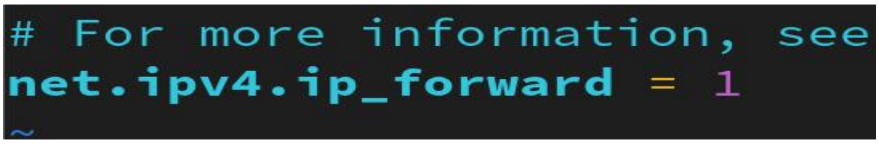
sudo setenforce 0

Next enable IP forwarding.

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

To make it permanent, edit **/etc/sysctl.conf** file and add following line.

sudo vi /etc/sysctl.conf



```
# For more information, see
net.ipv4.ip_forward = 1
~
```

Install following packages.

sudo dnf install epel-release -y

sudo dnf install openvpn wget tar -y

Then go to the /etc/openvpn directory.

cd /etc/openvpn

Download the EasyRSA package.

sudo wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.0.6/EasyRSA-unix-v3.0.6.tgz

Once the package is downloaded. Untar is using following command.

sudo tar xvzf EasyRSA-unix-v3.0.6.tgz

Rename the directory to make it easy to access.
sudo mv EasyRSA-v3.0.6 easy-rsa

Go to that directory.
cd easy-rsa

Create a file by name vars.
vi vars

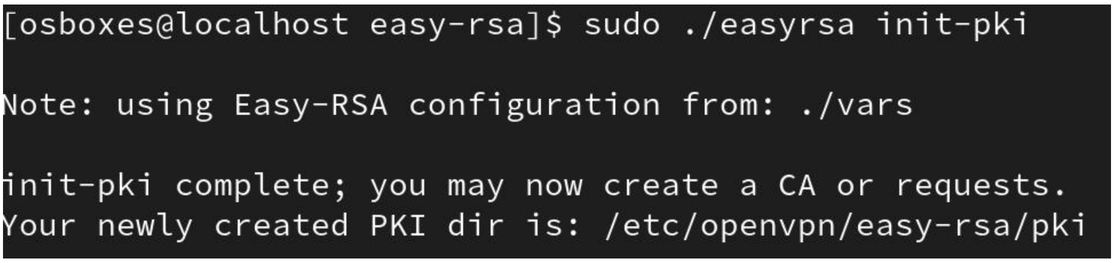
Add following into this file. Make changes if required.

```
set_var EASYRSA "$PWD"
set_var EASYRSA_PKI "$EASYRSA/pki"
set_var EASYRSA_DN "cn_only"
set_var EASYRSA_REQ_COUNTRY "IN"
set_var EASYRSA_REQ_PROVINCE "Maharastra"
set_var EASYRSA_REQ_CITY "Pune"
set_var EASYRSA_REQ_ORG "Demo Labs"
set_var EASYRSA_REQ_EMAIL ""
set_var EASYRSA_REQ_OU "Demo Labs CA"
set_var EASYRSA_KEY_SIZE 2048
set_var EASYRSA_ALGO rsa
set_var EASYRSA_CA_EXPIRE 7500
set_var EASYRSA_CERT_EXPIRE 365
set_var EASYRSA_NS_SUPPORT "no"
set_var EASYRSA_NS_COMMENT "Demo Labs"
set_var EASYRSA_EXT_DIR "$EASYRSA/x509-types"
set_var EASYRSA_SSL_CONF "$EASYRSA/openssl-easyrsa.cnf"
set_var EASYRSA_DIGEST "sha256"
```

Save the file.

Next initialize the PKI system.

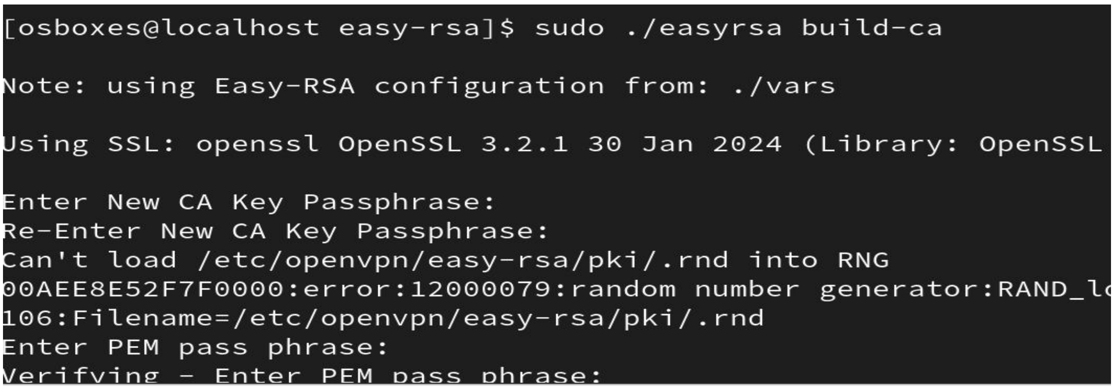
sudo ./easyrsa init-pki



```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa init-pki

Note: using Easy-RSA configuration from: ./vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/easy-rsa/pki
```

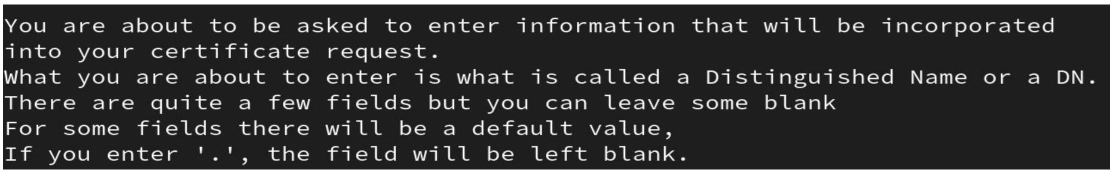
Netx build CA.

sudo ./easyrsa build-ca



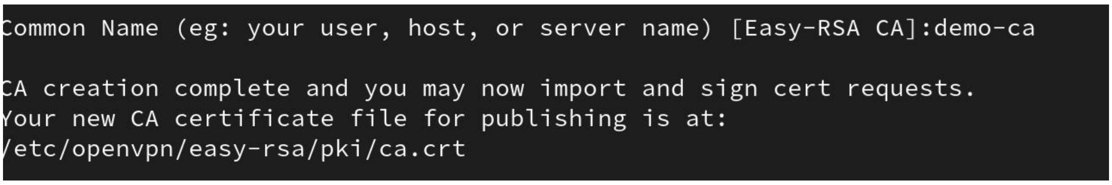
```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa build-ca

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Can't load /etc/openvpn/easy-rsa/pki/.rnd into RNG
00AEE8E52F7F0000:error:12000079:random number generator:RAND_lo
106:Filename=/etc/openvpn/easy-rsa/pki/.rnd
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Type a password for the CA. Remember this password as it will be required later while signing the certificates.



```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

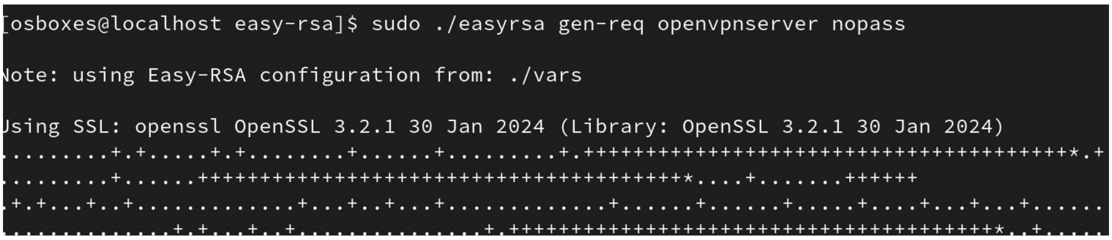
When it prompts for a common name for CA, enter a name. Here the name given is **demo-ca**.



```
ommon Name (eg: your user, host, or server name) [Easy-RSA CA]:demo-ca

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/pki/ca.crt
```

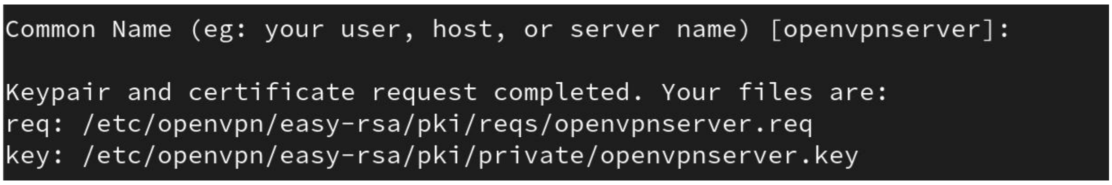
Now generate the certificate for the openvpnserver.

sudo ./easyrsa gen-req openvpnserver nopass



```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa gen-req openvpnserver nopass

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
........+.+.....+.+........+......+.........+.+++++++++++++++++++++++++++++++++++++++*.+
........+......+++++++++++++++++++++++++++++++++++++++*....+.......++++++
.+.+...+..+............+...+..+...+............+......+......+.....+....+...+...+......
.............+.+...+..+..............+.+++++++++++++++++++++++++++++++++++++++*..+.....
```

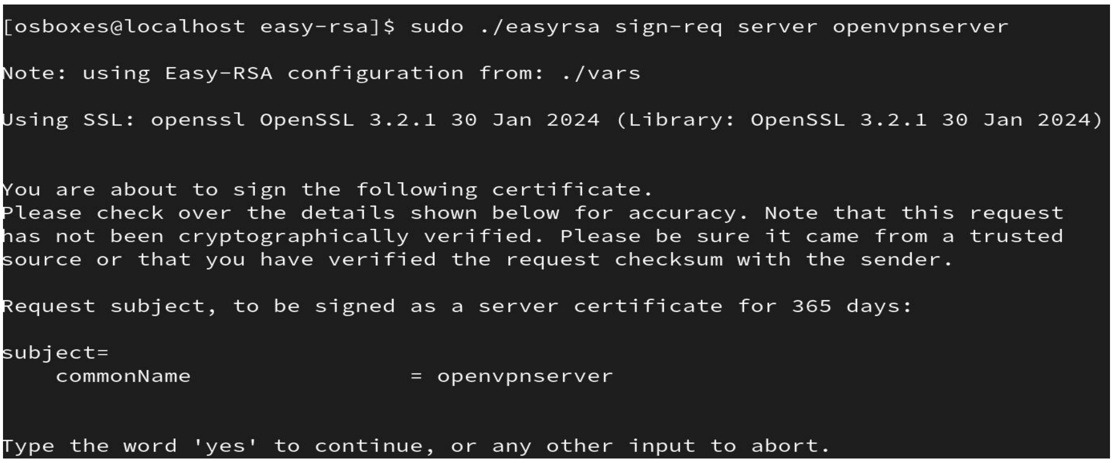
Press Enter at the prompt for the hostname as we will use the default openvpnserver.



```
Common Name (eg: your user, host, or server name) [openvpnserver]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/openvpnserver.req
key: /etc/openvpn/easy-rsa/pki/private/openvpnserver.key
```

Now get the certificate signed from CA.

sudo ./easyrsa sign-req server openvpnserver

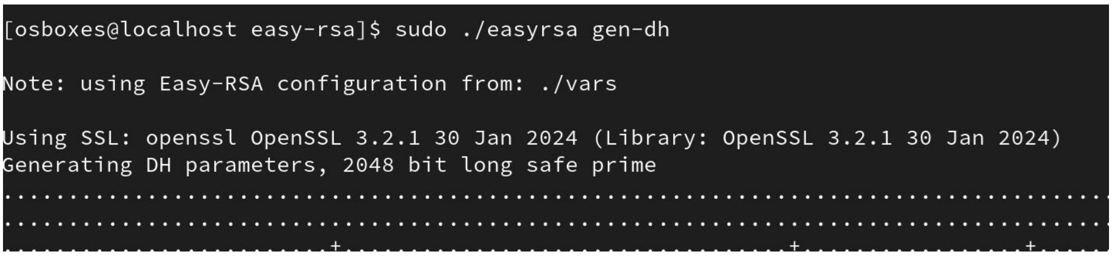


```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa sign-req server openvpnserver

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 365 days:

subject=
    commonName                = openvpnserver


Type the word 'yes' to continue, or any other input to abort.
```

Type yes at the above prompt.
Enter the CA password given in the above steps when prompted for the passphrase.

Next

sudo ./easyrsa gen-dh



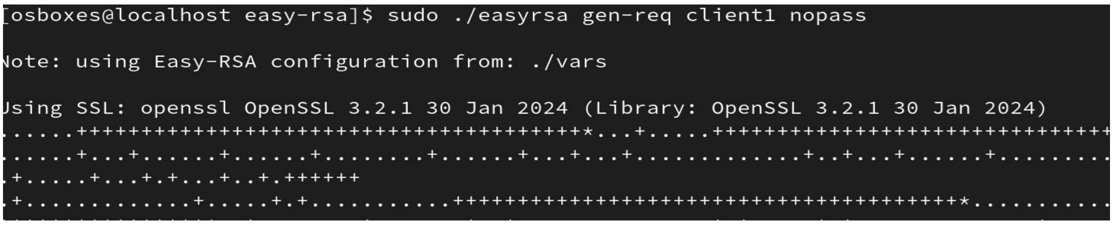
```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa gen-dh

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
Generating DH parameters, 2048 bit long safe prime
.....................................................................................
.....................................................................................
...........................+.................................+.................+.....
```

The server certificates are generated . Copy them to the server directory as OpenVPN server requires these files in that directory.

```
 sudo  cp  pki/ca.crt    /etc/openvpn/server
sudo   cp    pki/dh.pem   /etc/openvpn/server
sudo  cp   pki/private/openvpnserver.key   /etc/openvpn/server
sudo  cp   pki/issued/openvpnserver.crt    /etc/openvpn/server
```

Generate Client Certificates

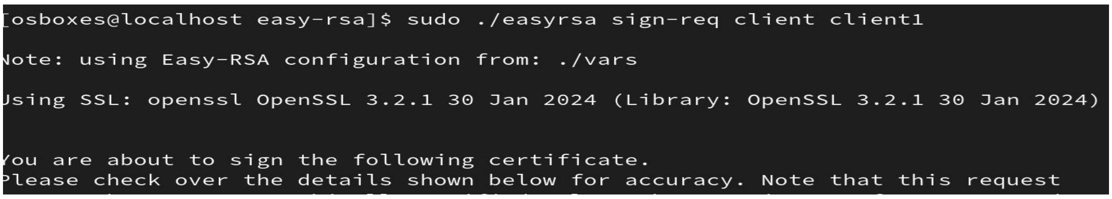
sudo ./easyrsa gen-req client1 nopass



```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa gen-req client1 nopass

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)
.....++++++++++++++++++++++++++++++++++++++++*...+.....+++++++++++++++++++++++++++++++
.....+...+......+......+........+......+...+...+.............+..+...+......+.........
.+.....+...+.+...+..+.++++++
.+.............+.....+.+...........++++++++++++++++++++++++++++++++++++++++*..........
```

Press Enter at the hostname prompt.
Next get the certificate signed from the CA.

sudo ./easyrsa sign-req client client1



```
[osboxes@localhost easy-rsa]$ sudo ./easyrsa sign-req client client1

Note: using Easy-RSA configuration from: ./vars

Using SSL: openssl OpenSSL 3.2.1 30 Jan 2024 (Library: OpenSSL 3.2.1 30 Jan 2024)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
```

Enter the CA password when prompted for the passphrase.

Copy client certificates to the client directory.

```
sudo  cp  pki/ca.crt   /etc/openvpn/client/
sudo  cp  pki/issued/client1.crt   /etc/openvpn/client
sudo  cp   pki/private/client1.key  /etc/openvpn/client
```

Now create the server.conf file.

```
sudo vi /etc/openvpn/server/server.conf
```

Add following to the file.

```
port 1194
proto udp
dev tun
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/openvpnserver.crt
key /etc/openvpn/server/openvpnserver.key
dh /etc/openvpn/server/dh.pem
server 10.8.0.0 255.255.255.0
#push "redirect-gateway def1"
push "route 192.168.237.0 255.255.255.0"  ### match this address to your LAN side network address.
#push "dhcp-option DNS 208.67.222.222"
#push "dhcp-option DNS 208.67.220.220"
duplicate-cn
cipher AES-256-CBC
tls-version-min 1.2
tls-cipher     TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
auth SHA512
auth-nocache
keepalive 20 60
persist-key
persist-tun
compress lz4
daemon
user nobody
group nobody
log-append /var/log/openvpn.log
verb 3
```

Save the file.
Now start and enable the OpenVPN server service.

```
sudo systemctl  start  openvpn-server@server
sudo systemctl  status openvpn-server@server
sudo systemctl  enable openvpn-server@server
```

Create client configuration file

sudo vi /etc/openvpn/client/client1.ovpn

Add following to the file.

```
client
dev tun
proto udp
remote vpn-server-ip 1194
ca ca.crt
cert client1.crt
key client1.key
cipher AES-256-CBC
auth SHA512
auth-nocache
tls-version-min 1.2
tls-cipher     TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-256-CBC-SHA256:TLS-
DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-WITH-AES-128-CBC-SHA256
resolv-retry infinite
compress lz4
nobind
persist-key
persist-tun
mute-replay-warnings
verb 3
```

Save the file.

Add following rules to firewalld on the OpenVPN Server

```
 sudo firewall-cmd --permanent --add-service=openvpn
 sudo firewall-cmd --permanent --zone=trusted --add-service=openvpn
 sudo firewall-cmd --permanent --zone=trusted --change-interface=tun0
 sudo firewall-cmd --add-masquerade
 sudo firewall-cmd --permanent --add-masquerade

 sudo firewall-cmd --permanent --direct --passthrough ipv4 -t nat -A POSTROUTING -s 10.8.0.0/24  \
-o ens160 -j MASQUERADE

 sudo firewall-cmd --reload
```

From the Server copy client configuration files to the VPN (Remote) client machine.

sudo scp /etc/openvpn/client/*.* admin@vpn-client-ip:/home/admin

Replace **vpn-client-ip** with the actual IP address of the VPN client in the above command.

Now go to the VPN client machine. Login as admin user.

Install following packages.

```
sudo dnf install epel-release -y
sudo dnf install openvpn -y
```

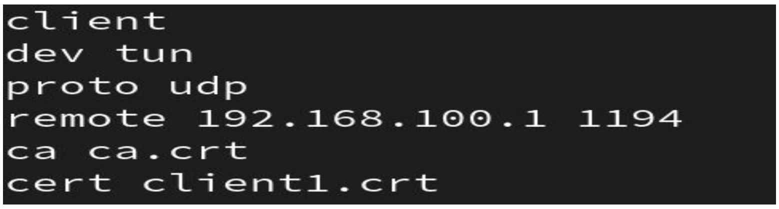
Once the packages are installed copy the files copied from the VPN server as below.

sudo setenforce 0

Disable SELINUX.

sudo cp /home/admin/ca.crt   /etc/openvpn/client
sudo cp /home/admin/client1.crt   /etc/openvpn/client
sudo cp /home/admin/client1.key   /etc/openvpn/client

Edit the client1.ovpn file. Put the server IP address in the remote field as shown below.

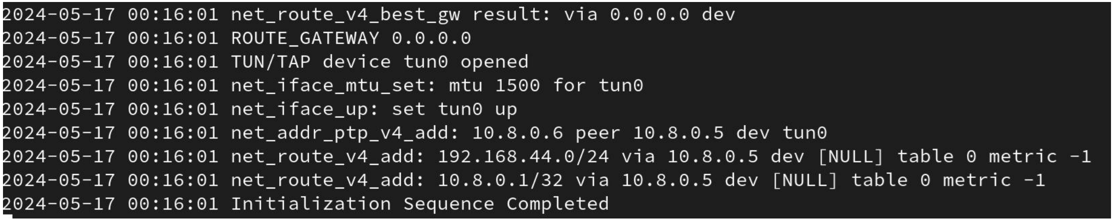


```
client
dev tun
proto udp
remote 192.168.100.1 1194
ca ca.crt
cert client1.crt
```

Now start the VPN connection with command,

sudo openvpn --config client1.ovpn

On successful connection you will get following messages.



```
2024-05-17 00:16:01 net_route_v4_best_gw result: via 0.0.0.0 dev
2024-05-17 00:16:01 ROUTE_GATEWAY 0.0.0.0
2024-05-17 00:16:01 TUN/TAP device tun0 opened
2024-05-17 00:16:01 net_iface_mtu_set: mtu 1500 for tun0
2024-05-17 00:16:01 net_iface_up: set tun0 up
2024-05-17 00:16:01 net_addr_ptp_v4_add: 10.8.0.6 peer 10.8.0.5 dev tun0
2024-05-17 00:16:01 net_route_v4_add: 192.168.44.0/24 via 10.8.0.5 dev [NULL] table 0 metric -1
2024-05-17 00:16:01 net_route_v4_add: 10.8.0.1/32 via 10.8.0.5 dev [NULL] table 0 metric -1
2024-05-17 00:16:01 Initialization Sequence Completed
```

The cursor will keep on blinking. You can not use this terminal now.

Open another terminal
check with

ip a

Ping to the LAN computer IP

ssh to the LAN computer IP.

Disconnect the VPN connection by pressing ctrl+C and check the above steps again.