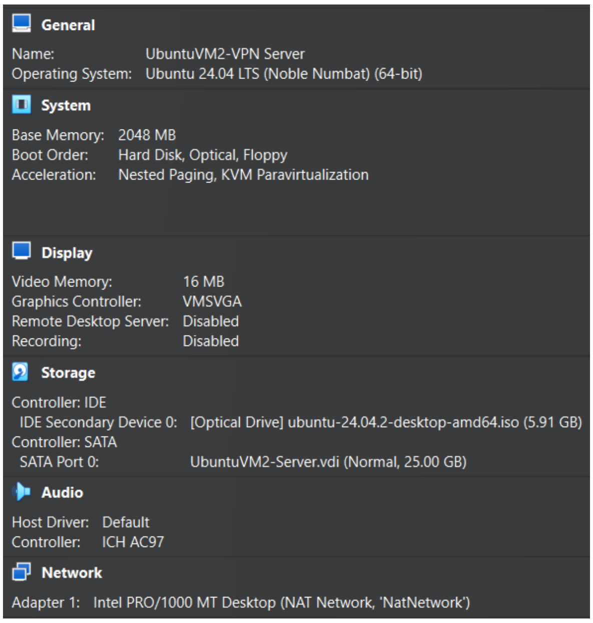
LAB: VPN CONFIGURATION AND SECURE COMMUNICATION

Steps taken to set up the VPN:

1. VM creation and network setup in VirtualBox

Create two virtual machines. One for VPN Server, and another one for VPN Client.



General

Name: UbuntuVM2-VPN Server
Operating System: Ubuntu 24.04 LTS (Noble Numbat) (64-bit)

System

Base Memory: 2048 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

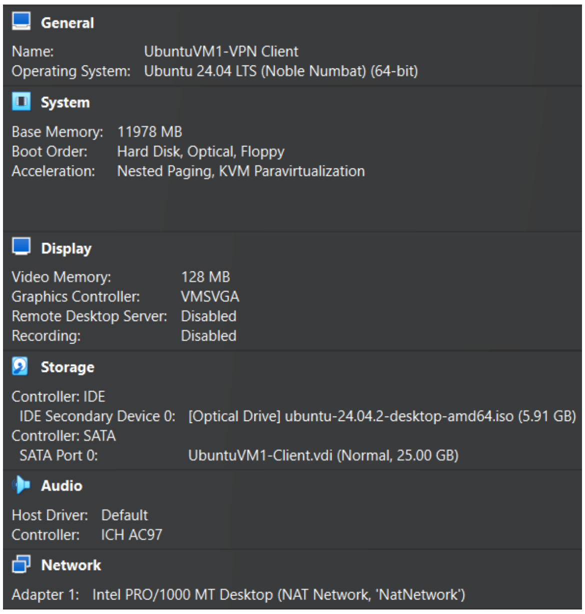
Controller: IDE
IDE Secondary Device 0: [Optical Drive] ubuntu-24.04.2-desktop-amd64.iso (5.91 GB)
Controller: SATA
SATA Port 0: UbuntuVM2-Server.vdi (Normal, 25.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')



General

Name: UbuntuVM1-VPN Client
Operating System: Ubuntu 24.04 LTS (Noble Numbat) (64-bit)

System

Base Memory: 11978 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] ubuntu-24.04.2-desktop-amd64.iso (5.91 GB)
Controller: SATA
SATA Port 0: UbuntuVM1-Client.vdi (Normal, 25.00 GB)

Audio

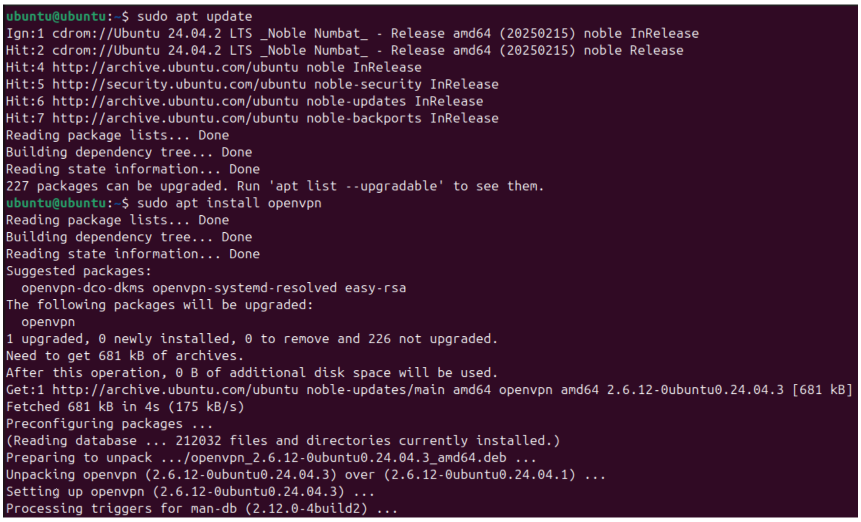
Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')

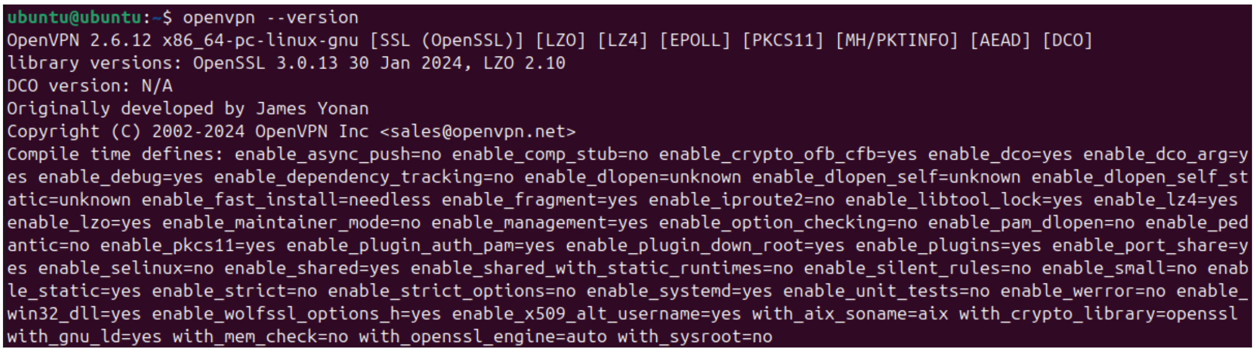
Notice that both VMs have been named respectively. Both have been assigned with more than 2 GB of RAM and 1/2CPUs. Also, they have been assigned to ubuntu 24.04 LTS 64-bit ISO image and use NAT network adapter to access the internet.

2. OpenVPN installation steps



```
ubuntu@ubuntu:~$ sudo apt update
Ign:1 cdrom://Ubuntu 24.04.2 LTS _Noble Numbat_ - Release amd64 (20250215) noble InRelease
Hit:2 cdrom://Ubuntu 24.04.2 LTS _Noble Numbat_ - Release amd64 (20250215) noble Release
Hit:4 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:6 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:7 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
227 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ubuntu:~$ sudo apt install openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  openvpn-dco-dkms openvpn-systemd-resolved easy-rsa
The following packages will be upgraded:
  openvpn
1 upgraded, 0 newly installed, 0 to remove and 226 not upgraded.
Need to get 681 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 openvpn amd64 2.6.12-0ubuntu0.24.04.3 [681 kB]
Fetched 681 kB in 4s (175 kB/s)
Preconfiguring packages ...
(Reading database ... 212032 files and directories currently installed.)
Preparing to unpack .../openvpn_2.6.12-0ubuntu0.24.04.3_amd64.deb ...
Unpacking openvpn (2.6.12-0ubuntu0.24.04.3) over (2.6.12-0ubuntu0.24.04.1) ...
Setting up openvpn (2.6.12-0ubuntu0.24.04.3) ...
Processing triggers for man-db (2.12.0-4build2) ...
```

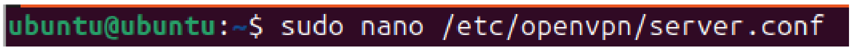
Run “sudo apt update” “sudo apt install openvpn” for both VMs



```
ubuntu@ubuntu:~$ openvpn --version
OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
DCO version: N/A
Originally developed by James Yonan
Copyright (C) 2002-2024 OpenVPN Inc <sales@openvpn.net>
Compile time defines: enable_async_push=no enable_comp_stub=no enable_crypto_ofb_cfb=yes enable_dco=yes enable_dco_arg=y
es enable_debug=yes enable_dependency_tracking=no enable_dlopen=unknown enable_dlopen_self=unknown enable_dlopen_self_st
atic=unknown enable_fast_install=needless enable_fragment=yes enable_iproute2=no enable_libtool_lock=yes enable_lz4=yes
enable_lzo=yes enable_maintainer_mode=no enable_management=yes enable_option_checking=no enable_pam_dlopen=no enable_ped
antic=no enable_pkcs11=yes enable_plugin_auth_pam=yes enable_plugin_down_root=yes enable_plugins=yes enable_port_share=y
es enable_selinux=no enable_shared=yes enable_shared_with_static_runtimes=no enable_silent_rules=no enable_small=no enab
le_static=yes enable_strict=no enable_strict_options=no enable_systemd=yes enable_unit_tests=no enable_werror=no enable_
win32_dll=yes enable_wolfssl_options_h=yes enable_x509_alt_username=yes with_aix_soname=aix with_crypto_library=openssl
with_gnu_ld=yes with_mem_check=no with_openssl_engine=auto with_sysroot=no
```

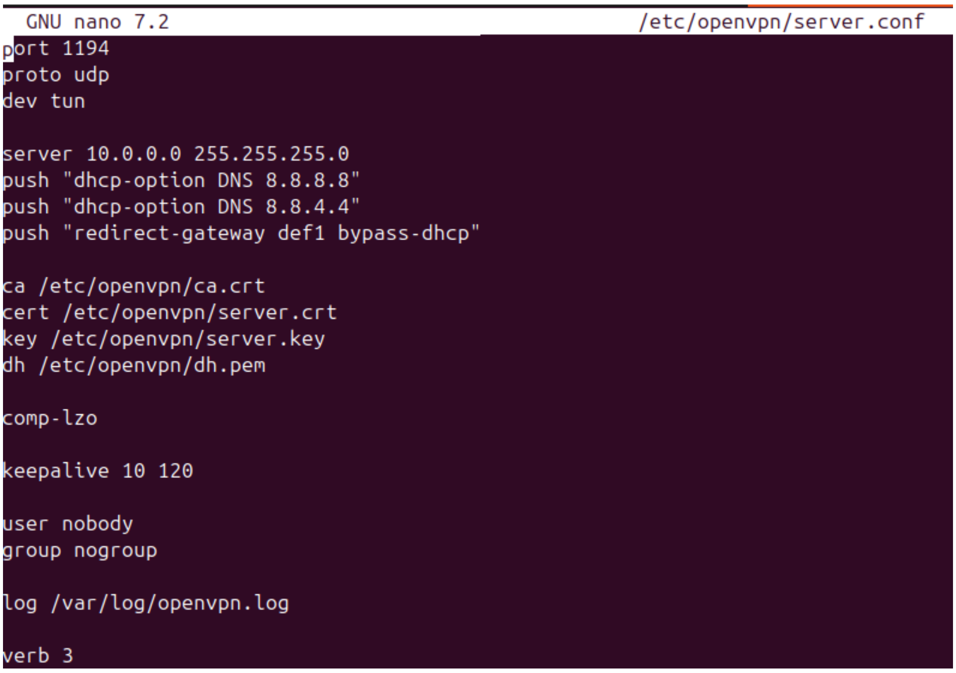
Run “openvpn --version” to verify the installation.

On VPN Server VM, run



```
ubuntu@ubuntu:~$ sudo nano /etc/openvpn/server.conf
```

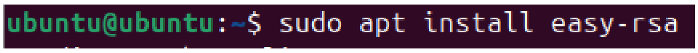
Then, continue config server.conf with basic server configuration:



```
  GNU nano 7.2                                   /etc/openvpn/server.conf
port 1194
proto udp
dev tun

server 10.0.0.0 255.255.255.0
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway def1 bypass-dhcp"

ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem

comp-lzo

keepalive 10 120

user nobody
group nogroup

log /var/log/openvpn.log

verb 3
```

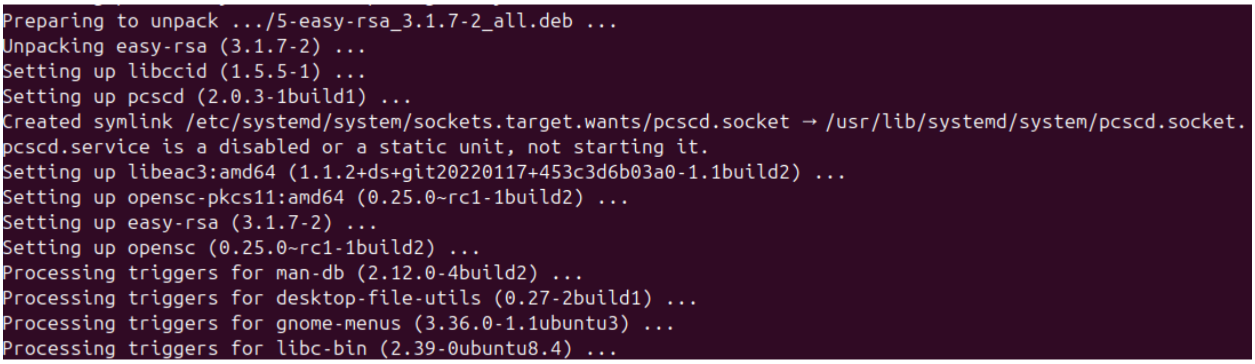
3. Certificate/key generation using EasyRSA

On both VMs, run



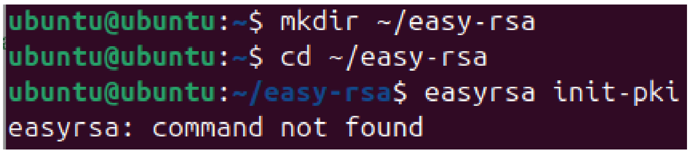
```
ubuntu@ubuntu:~$ sudo apt install easy-rsa
```

If successful, it should return something like this:



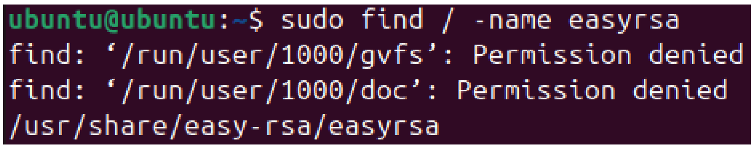
```
Preparing to unpack .../5-easy-rsa_3.1.7-2_all.deb ...
Unpacking easy-rsa (3.1.7-2) ...
Setting up libccid (1.5.5-1) ...
Setting up pcscd (2.0.3-1build1) ...
Created symlink /etc/systemd/system/sockets.target.wants/pcscd.socket → /usr/lib/systemd/system/pcscd.socket.
pcscd.service is a disabled or a static unit, not starting it.
Setting up libeac3:amd64 (1.1.2+ds+git20220117+453c3d6b03a0-1.1build2) ...
Setting up opensc-pkcs11:amd64 (0.25.0~rc1-1build2) ...
Setting up easy-rsa (3.1.7-2) ...
Setting up opensc (0.25.0~rc1-1build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for desktop-file-utils (0.27-2build1) ...
Processing triggers for gnome-menus (3.36.0-1.1ubuntu3) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
```

Continue to create a directory for EasyRSA and attempt to initialize EasyRSA PKI:



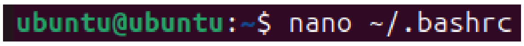
```
ubuntu@ubuntu:~$ mkdir ~/easy-rsa
ubuntu@ubuntu:~$ cd ~/easy-rsa
ubuntu@ubuntu:~/easy-rsa$ easyrsa init-pki
easyrsa: command not found
```

Try locating EasyRSA directory since the initialization above failed:



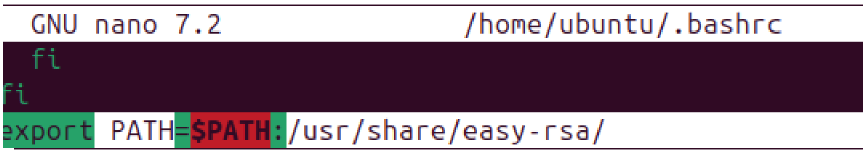
```
ubuntu@ubuntu:~$ sudo find / -name easyrsa
find: '/run/user/1000/gvfs': Permission denied
find: '/run/user/1000/doc': Permission denied
/usr/share/easy-rsa/easyrsa
```

Proceed to set EasyRSA Path:

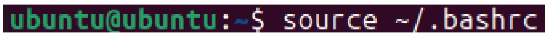
Run 

```
ubuntu@ubuntu:~$ nano ~/.bashrc
```

At this highlighted line at the end of the script:

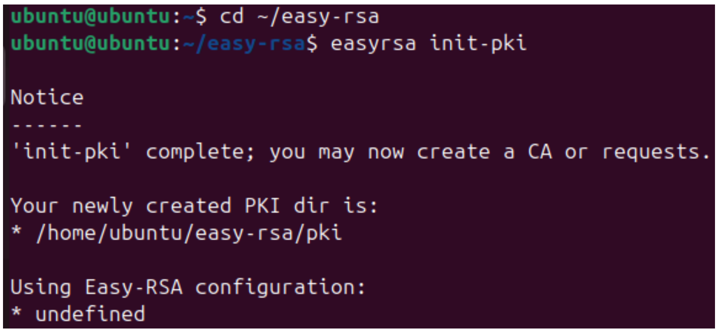


```
  GNU nano 7.2                    /home/ubuntu/.bashrc
  fi
fi
export PATH=$PATH:/usr/share/easy-rsa/
```

Don't forget to reload the shell configuration with 

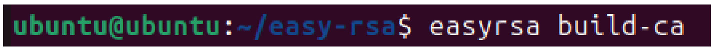
```
ubuntu@ubuntu:~$ source ~/.bashrc
```

Try reinitializing to verify the solution:

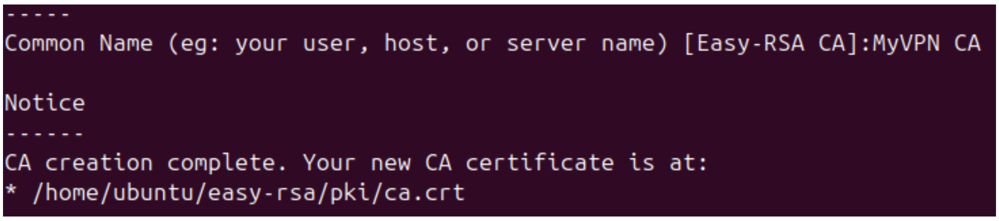


```
ubuntu@ubuntu:~$ cd ~/easy-rsa
ubuntu@ubuntu:~/easy-rsa$ easyrsa init-pki

Notice
------
'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* /home/ubuntu/easy-rsa/pki

Using Easy-RSA configuration:
* undefined
```

Then, on **VPN Server VM** only, build the Certificate Authority:

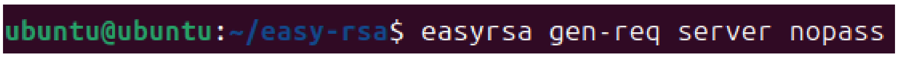


```
ubuntu@ubuntu:~/easy-rsa$ easyrsa build-ca
```

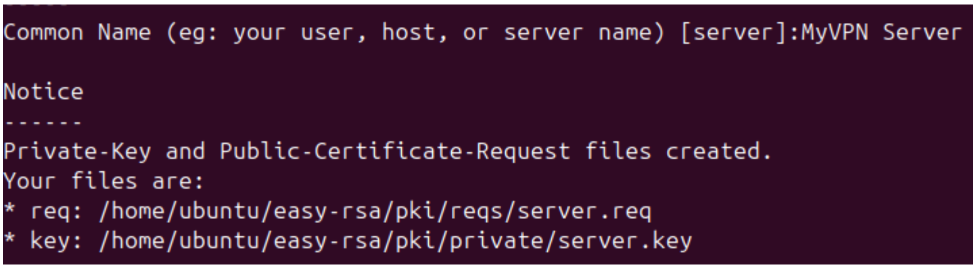


```
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:MyVPN CA

Notice
------
CA creation complete. Your new CA certificate is at:
* /home/ubuntu/easy-rsa/pki/ca.crt
```

Continue with generating the Server Certificate and Key:

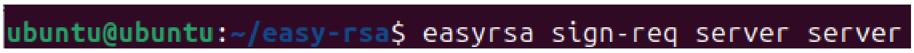


```
ubuntu@ubuntu:~/easy-rsa$ easyrsa gen-req server nopass
```

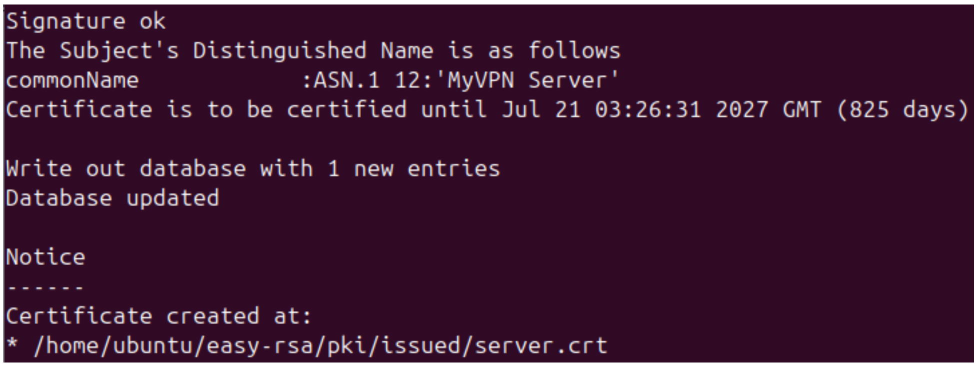


```
Common Name (eg: your user, host, or server name) [server]:MyVPN Server

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /home/ubuntu/easy-rsa/pki/reqs/server.req
* key: /home/ubuntu/easy-rsa/pki/private/server.key
```

Sign the server certificate:

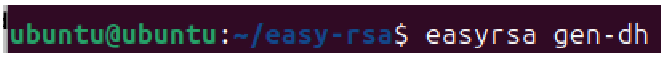


```
ubuntu@ubuntu:~/easy-rsa$ easyrsa sign-req server server
```

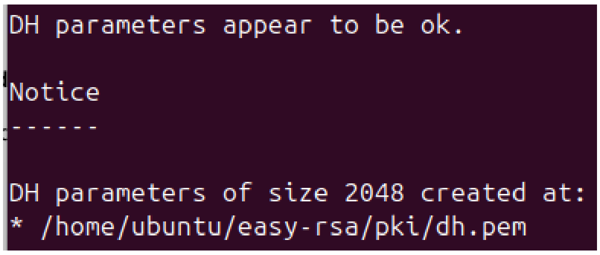


```
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'MyVPN Server'
Certificate is to be certified until Jul 21 03:26:31 2027 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /home/ubuntu/easy-rsa/pki/issued/server.crt
```

For the key exchange during VPN connection setup, generate the Diffie-Hellman (DH) Parameters:

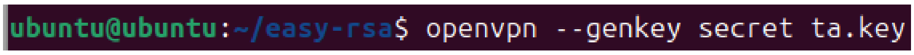


```
ubuntu@ubuntu:~/easy-rsa$ easyrsa gen-dh
```



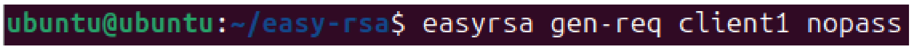
```
DH parameters appear to be ok.

Notice
------

DH parameters of size 2048 created at:
* /home/ubuntu/easy-rsa/pki/dh.pem
```

Optionally, generate the HMAC key for the additional layer of security for the OpenVPN server:

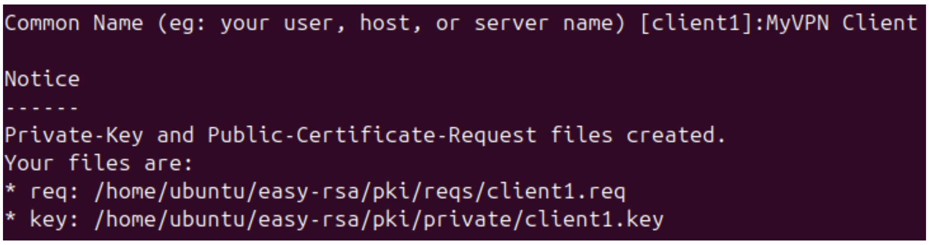


```
ubuntu@ubuntu:~/easy-rsa$ openvpn --genkey secret ta.key
```

Finally, generate client certificate and key so that it allows the VPN Client VM to connect to the OpenVPN server:

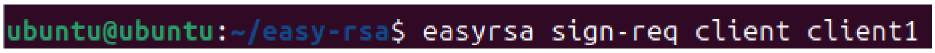


```
ubuntu@ubuntu:~/easy-rsa$ easyrsa gen-req client1 nopass
```

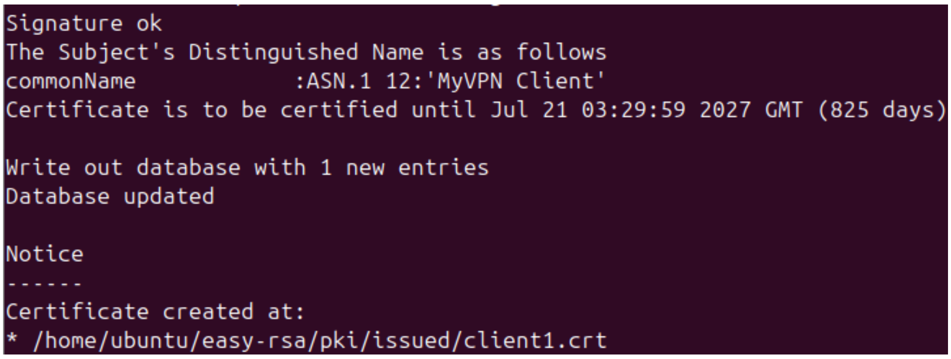


```
Common Name (eg: your user, host, or server name) [client1]:MyVPN Client

Notice
------
Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /home/ubuntu/easy-rsa/pki/reqs/client1.req
* key: /home/ubuntu/easy-rsa/pki/private/client1.key
```

Sign it:

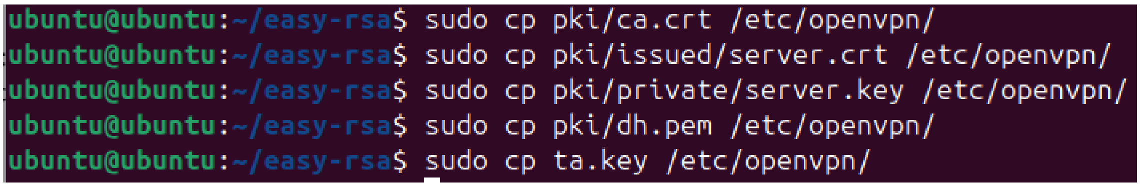


```
ubuntu@ubuntu:~/easy-rsa$ easyrsa sign-req client client1
```



```
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'MyVPN Client'
Certificate is to be certified until Jul 21 03:29:59 2027 GMT (825 days)

Write out database with 1 new entries
Database updated

Notice
------
Certificate created at:
* /home/ubuntu/easy-rsa/pki/issued/client1.crt
```

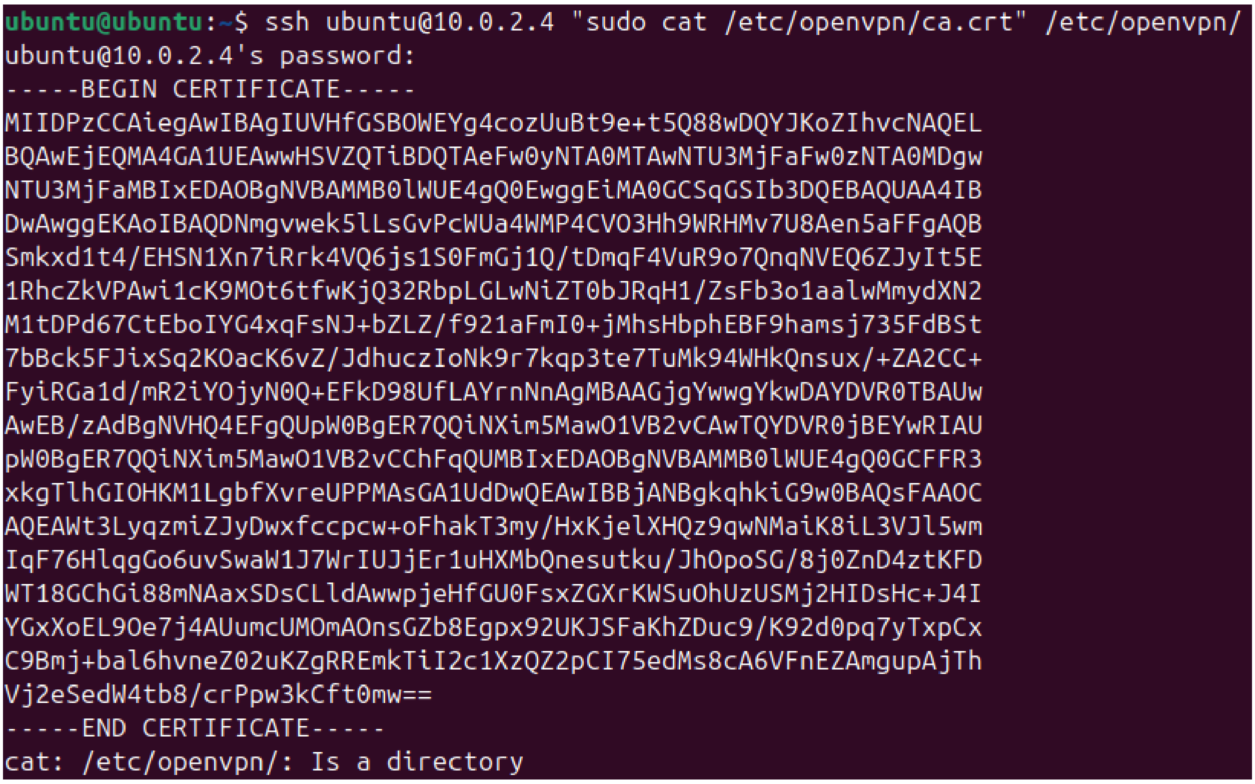
Then, organize all the necessary generated files by copying them to appropriate directories for OpenVPN:



```
ubuntu@ubuntu:~/easy-rsa$ sudo cp pki/ca.crt /etc/openvpn/
ubuntu@ubuntu:~/easy-rsa$ sudo cp pki/issued/server.crt /etc/openvpn/
ubuntu@ubuntu:~/easy-rsa$ sudo cp pki/private/server.key /etc/openvpn/
ubuntu@ubuntu:~/easy-rsa$ sudo cp pki/dh.pem /etc/openvpn/
ubuntu@ubuntu:~/easy-rsa$ sudo cp ta.key /etc/openvpn/
```

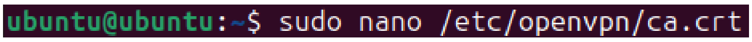
Now, it is time to copy the generated client certificates to the client machine. On the **Client VPN VM**:

Firstly, copied the ca.crt as follows:



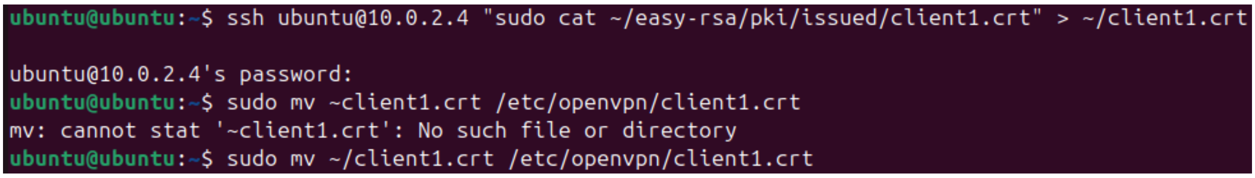
```
ubuntu@ubuntu:~$ ssh ubuntu@10.0.2.4 "sudo cat /etc/openvpn/ca.crt" /etc/openvpn/
ubuntu@10.0.2.4's password:
-----BEGIN CERTIFICATE-----
MIIDPzCCAiegAwIBAgIUVHfGSBOWEYg4cozUuBt9e+t5Q88wDQYJKoZIhvcNAQEL
BQAwEjEQMA4GA1UEAwwHSVZQTiBDQTAeFw0yNTA0MTAwNTU3MjFaFw0zNTA0MDgw
NTU3MjFaMBIxEDAOBgNVBAMMB0lWUE4gQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDNmgvwek5lLsGvPcWUa4WMP4CVO3Hh9WRHMv7U8Aen5aFFgAQB
Smkxd1t4/EHSN1Xn7iRrk4VQ6js1S0FmGj1Q/tDmqF4VuR9o7QnqNVEQ6ZJyIt5E
1RhcZkVPAwi1cK9MOt6tfwKjQ32RbpLGLwNiZT0bJRqH1/ZsFb3o1aalwMmydXN2
M1tDPd67CtEboIYG4xqFsNJ+bZLZ/f921aFmI0+jMhsHbphEBF9hamsj735FdBSt
7bBck5FJixSq2KOacK6vZ/JdhuczIoNk9r7kqp3te7TuMk94WHkQnsux/+ZA2CC+
FyiRGa1d/mR2iYOjyN0Q+EFkD98UfLAYrnNnAgMBAAGjgYwwgYkwDAYDVR0TBAUw
AwEB/zAdBgNVHQ4EFgQUpW0BgER7QQiNXim5MawO1VB2vCAwTQYDVR0jBEYwRIAU
pW0BgER7QQiNXim5MawO1VB2vCChFqQUMBIxEDAOBgNVBAMMB0lWUE4gQ0GCFFR3
xkgTlhGIOHKM1LgbfXvreUPPMAsGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQsFAAOC
AQEAWt3LyqzmiZJyDwxfccpcw+oFhakT3my/HxKjelXHQz9qwNMaiK8iL3VJl5wm
IqF76HlqgGo6uvSwaW1J7WrIUJjEr1uHXMbQnesutku/JhOpoSG/8j0ZnD4ztKFD
WT18GChGi88mNAaxSDsCLldAwwpjeHfGU0FsxZGXrKWSuOhUzUSMj2HIDsHc+J4I
YGxXoEL9Oe7j4AUumcUMOmAOnsGZb8Egpx92UKJSFaKhZDuc9/K92d0pq7yTxpCx
C9Bmj+bal6hvneZ02uKZgRREmkTiI2c1XzQZ2pCI75edMs8cA6VFnEZAmgupAjTh
Vj2eSedW4tb8/crPpw3kCft0mw==
-----END CERTIFICATE-----
cat: /etc/openvpn/: Is a directory
```

Proceed to copy the content from ---BEGIN CERTIFICATE--- until ----END CERTIFICATE--- and paste it here



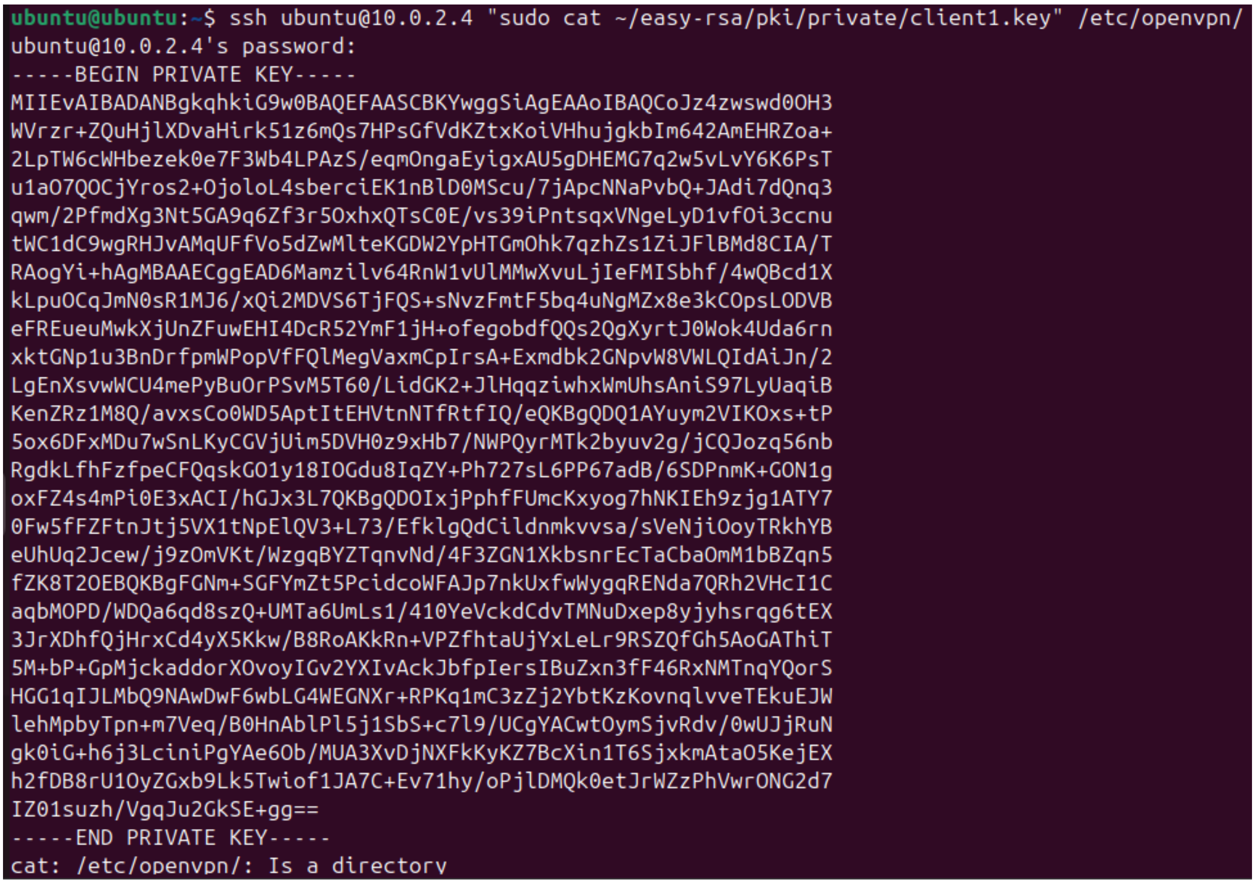
```
ubuntu@ubuntu:~$ sudo nano /etc/openvpn/ca.crt
```

Then, copied the client1.crt:



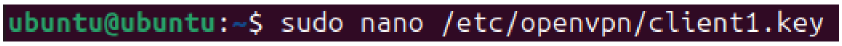
```
ubuntu@ubuntu:~$ ssh ubuntu@10.0.2.4 "sudo cat ~/easy-rsa/pki/issued/client1.crt" > ~/client1.crt

ubuntu@10.0.2.4's password:
ubuntu@ubuntu:~$ sudo mv ~client1.crt /etc/openvpn/client1.crt
mv: cannot stat '~client1.crt': No such file or directory
ubuntu@ubuntu:~$ sudo mv ~/client1.crt /etc/openvpn/client1.crt
```

Next, copied the client1.key:



```
ubuntu@ubuntu:~$ ssh ubuntu@10.0.2.4 "sudo cat ~/easy-rsa/pki/private/client1.key" /etc/openvpn/
ubuntu@10.0.2.4's password:
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCoJz4zwswd0OH3
WVrzr+ZQuHjlXDvaHirk51z6mQs7HPsGfVdKZtxKoiVHhujgkbIm642AmEHRZoa+
2LpTW6cWHbezek0e7F3Wb4LPAzS/eqmOngaEyigxAU5gDHEMG7q2w5vLvY6K6PsT
u1aO7QOCjYros2+OjoloL4sberciEK1nBlD0MScu/7jApcNNaPvbQ+JAdi7dQnq3
qwm/2PfmdXg3Nt5GA9q6Zf3r5OxhxQTsC0E/vs39iPntsqxVNgeLyD1vfOi3ccnu
tWC1dC9wgRHJvAMqUFfVo5dZwMlteKGDW2YpHTGmOhk7qzhZs1ZiJFlBMd8CIA/T
RAogYi+hAgMBAAECggEAD6Mamzilv64RnW1vUlMMwXvuLjIeFMISbhf/4wQBcd1X
kLpuOCqJmN0sR1MJ6/xQi2MDVS6TjFQS+sNvzFmtF5bq4uNgMZx8e3kCOpsLODVB
eFREueuMwkXjUnZFuwEHI4DcR52YmF1jH+ofegobdfQQs2QgXyrtJ0Wok4Uda6rn
xktGNp1u3BnDrfpmWPopVfFQlMegVaxmCpIrsA+Exmdbk2GNpvW8VWLQIdAiJn/2
LgEnXsvwWCU4mePyBuOrPSvM5T60/LidGK2+JlHqqziwhxWmUhsAniS97LyUaqiB
KenZRz1M8Q/avxsCo0WD5AptItEHVtnNTfRtfIQ/eQKBgQDQ1AYuym2VIKOxs+tP
5ox6DFxMDu7wSnLKyCGVjUim5DVH0z9xHb7/NWPQyrMTk2byuv2g/jCQJozq56nb
RgdkLfhFzfpeCFQqskGO1y18IOGdu8IqZY+Ph727sL6PP67adB/6SDPnmK+GON1g
oxFZ4s4mPi0E3xACI/hGJx3L7QKBgQDOIxjPphfFUmcKxyog7hNKIEh9zjg1ATY7
0Fw5fFZFtnJtj5VX1tNpElQV3+L73/EfklgQdCildnmkvvsa/sVeNjiOoyTRkhYB
eUhUq2Jcew/j9zOmVKt/WzgqBYZTqnvNd/4F3ZGN1XkbsnrEcTaCbaOmM1bBZqn5
fZK8T2OEBQKBgFGNm+SGFYmZt5PcidcoWFAJp7nkUxfwWygqRENda7QRh2VHcI1C
aqbMOPD/WDQa6qd8szQ+UMTa6UmLs1/41OYeVckdCdvTMNuDxep8yjyhsrqg6tEX
3JrXDhfQjHrxCd4yX5Kkw/B8RoAKkRn+VPZfhtaUjYxLeLr9RSZQfGh5AoGAThiT
5M+bP+GpMjckaddorXOvoyIGv2YXIvAckJbfpIersIBuZxn3fF46RxNMTnqYQorS
HGG1qIJLMbQ9NAwDwF6wbLG4WEGNXr+RPKq1mC3zZj2YbtKzKovnqlvveTEkuEJW
lehMpbyTpn+m7Veq/B0HnAblPl5j1SbS+c7l9/UCgYACwtOymSjvRdv/0wUJjRuN
gk0iG+h6j3LciniPgYAe6Ob/MUA3XvDjNXFkKyKZ7BcXin1T6SjxkmAtaO5KejEX
h2fDB8rU1OyZGxb9Lk5Twiof1JA7C+Ev71hy/oPjlDMQk0etJrWZzPhVwrONG2d7
IZ01suzh/VgqJu2GkSE+gg==
-----END PRIVATE KEY-----
cat: /etc/openvpn/: Is a directory
```

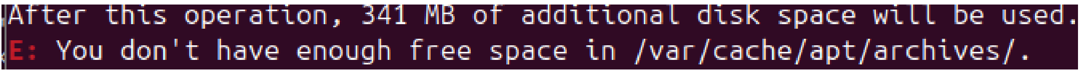
Proceed to copy the content from ---BEGIN CERTIFICATE--- until ----END CERTIFICATE--- and paste it here



```
ubuntu@ubuntu:~$ sudo nano /etc/openvpn/client1.key
```

Remark: Had to use ssh to view the file then create the files manually instead of directly using the scp due to storage constraint to install openssh-server at my Server VPN VM.

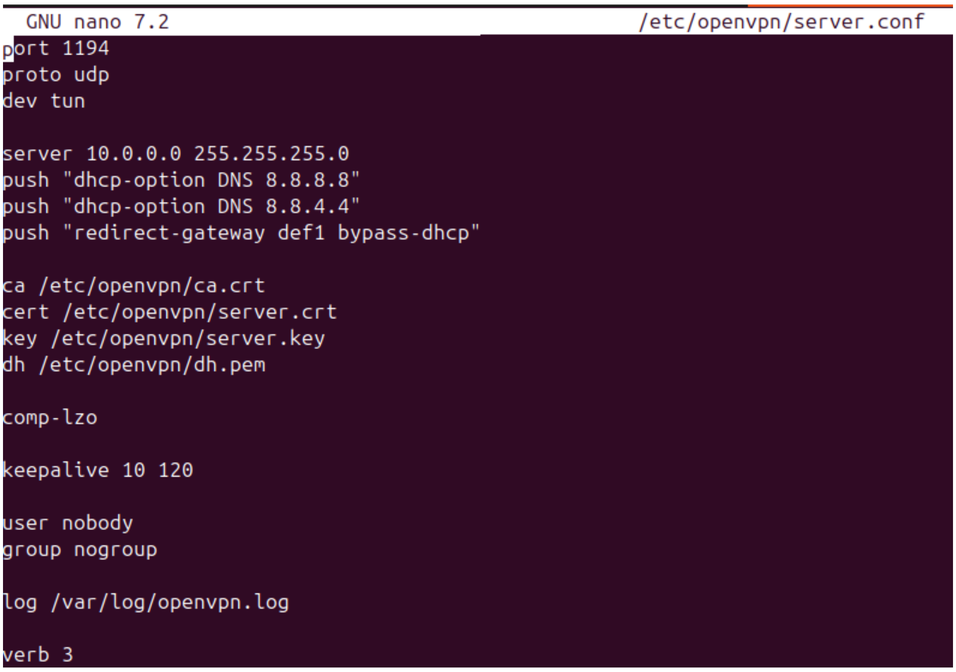
Proof:



```
After this operation, 341 MB of additional disk space will be used.
E: You don't have enough free space in /var/cache/apt/archives/.
```

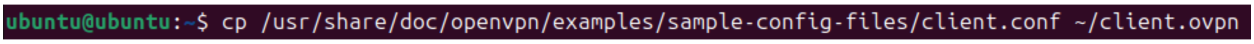
4. VPN server and client configuration

After successfully generating all the necessary files, I cross-checked the earlier configured server.conf to make sure it specifies the correct paths to the certificate and key files:



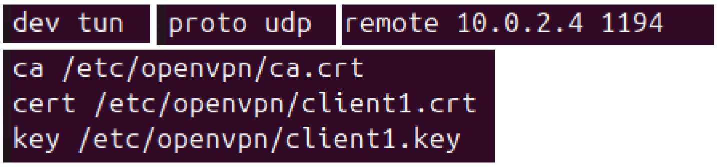
```
  GNU nano 7.2                                          /etc/openvpn/server.conf
port 1194
proto udp
dev tun

server 10.0.0.0 255.255.255.0
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway def1 bypass-dhcp"

ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem

comp-lzo

keepalive 10 120

user nobody
group nogroup

log /var/log/openvpn.log

verb 3
```

To generate client.ovpn, copy from a template file and rename it.



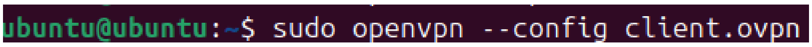
```
ubuntu@ubuntu:~$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf ~/client.ovpn
```

Proceed to edit all the critical info on the client.ovpn:



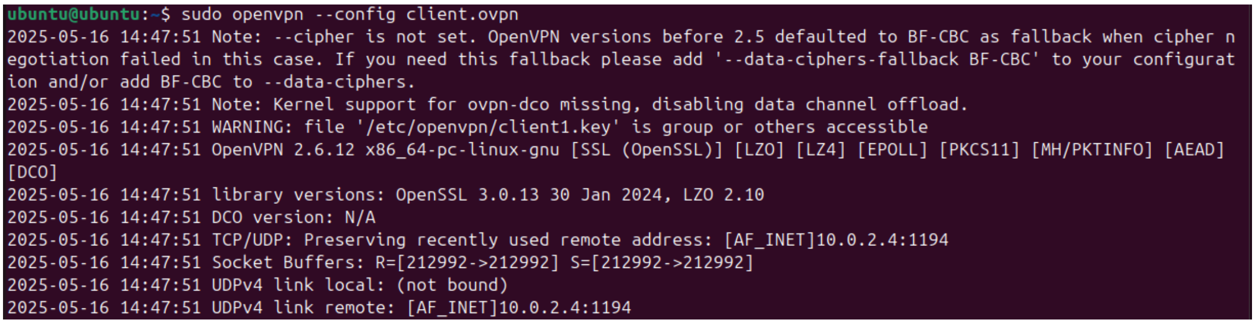
```
dev tun
proto udp
remote 10.0.2.4 1194
ca /etc/openvpn/ca.crt
cert /etc/openvpn/client1.crt
key /etc/openvpn/client1.key
```

5. Test the VPN Connection Between Server and Client



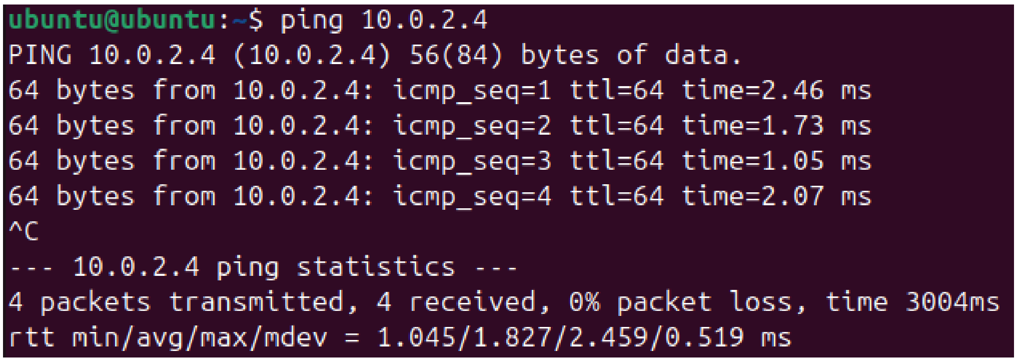
On **Client VPN VM**, run `ubuntu@ubuntu:~$ sudo openvpn --config client.ovpn` to start the VPN client on the client machine.

Make sure it's free from error:



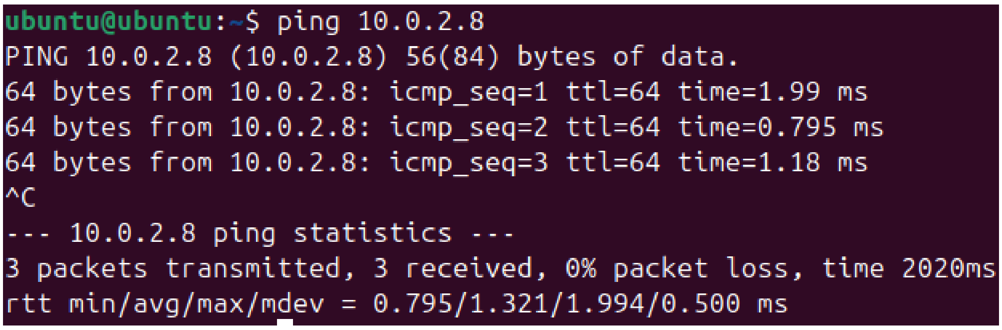
```
ubuntu@ubuntu:~$ sudo openvpn --config client.ovpn
2025-05-16 14:47:51 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher n
egotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configurat
ion and/or add BF-CBC to --data-ciphers.
2025-05-16 14:47:51 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2025-05-16 14:47:51 WARNING: file '/etc/openvpn/client1.key' is group or others accessible
2025-05-16 14:47:51 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD]
[DCO]
2025-05-16 14:47:51 library versions: OpenSSL 3.0.13 30 Jan 2024, LZO 2.10
2025-05-16 14:47:51 DCO version: N/A
2025-05-16 14:47:51 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.2.4:1194
2025-05-16 14:47:51 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-05-16 14:47:51 UDPv4 link local: (not bound)
2025-05-16 14:47:51 UDPv4 link remote: [AF_INET]10.0.2.4:1194
```

Ping from client to server:



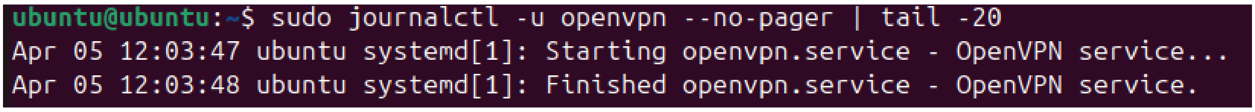
```
ubuntu@ubuntu:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=2.46 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.73 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=2.07 ms
^C
--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.045/1.827/2.459/0.519 ms
```

Ping from server to client:



```
ubuntu@ubuntu:~$ ping 10.0.2.8
PING 10.0.2.8 (10.0.2.8) 56(84) bytes of data.
64 bytes from 10.0.2.8: icmp_seq=1 ttl=64 time=1.99 ms
64 bytes from 10.0.2.8: icmp_seq=2 ttl=64 time=0.795 ms
64 bytes from 10.0.2.8: icmp_seq=3 ttl=64 time=1.18 ms
^C
--- 10.0.2.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.795/1.321/1.994/0.500 ms
```

Proof of successful VPN connection:



```
ubuntu@ubuntu:~$ sudo journalctl -u openvpn --no-pager | tail -20
Apr 05 12:03:47 ubuntu systemd[1]: Starting openvpn.service - OpenVPN service...
Apr 05 12:03:48 ubuntu systemd[1]: Finished openvpn.service - OpenVPN service.
```