2. Create another vm with installing openvpn client and you should create an openvpn client connect file(with extension .ovpn) providing the certificates. You should be able to connect to the vpn server and get an ip address from the LAN subnet that you assigned in the first vm.

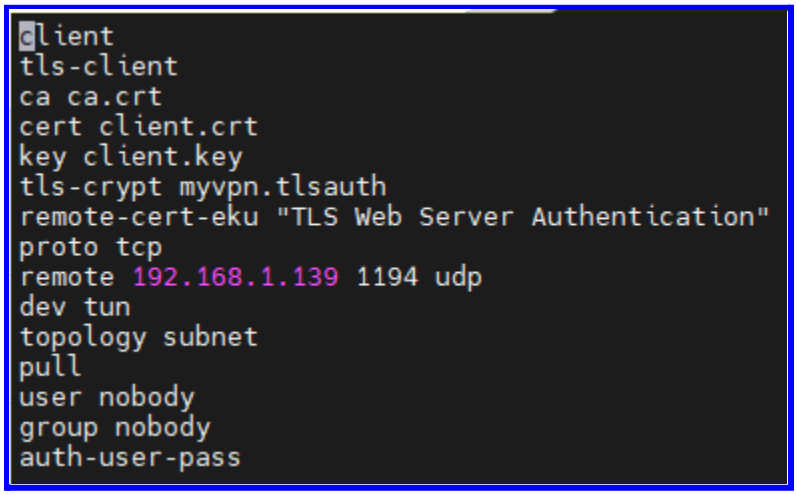
My other VM is ubuntu.

I created client.ovpn in the same directory where I have transferred the client keys so I have just mentioned the certificate names(**no need to give path**)

sudo nano client.ovpn

Add add following lines

client
tls-client
ca ca.crt
cert client.crt
key client.key
tls-crypt myvpn.tlsauth
remote-cert-eku "TLS Web Server Authentication"
proto tcp
remote 192.168.1.139 1194 udp
dev tun
topology subnet
pull
user nobody
group nobody
auth-user-pass



- To enable user-password authentication

- We need to create openvpn file in **/etc/pam.d/** directory in centos server where openVPN server is

sudo vi /etc/pam.d/openvpn
And add the following lines

auth required pam_unix.so shadow nodelay
account required pam_unix.so

```
auth    required        pam_unix.so     shadow  nodelay
account required        pam_unix.so
~
```

Now install openvpn-client to ubuntu server

sudo apt install -y openvpn

- To connect to openvpn server

sudo openvpn --config client.ovpn

- Ip address of ubuntu server before connecting to openvpn

```
bibek@bibek-lf:~/openclient$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:75:a8:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.142/24 brd 192.168.1.255 scope global dynamic noprefixroute e
np0s3
       valid_lft 55396sec preferred_lft 55396sec
    inet6 fe80::e9f4:8400:a73a:c0c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
bibek@bibek-lf:~/openclient$
```

- Give username and password

```
Sun Nov  7 01:44:07 2021 WARNING: file 'myvpn.tlsauth'
ible
Sun Nov  7 01:44:07 2021 OpenVPN 2.4.7 x86_64-pc-linux
 [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on J
Sun Nov  7 01:44:07 2021 library versions: OpenSSL 1.1
Enter Auth Username: bibek
Enter Auth Password: ********
Sun Nov  7 01:44:17 2021 WARNING: you are using user/g
 persist-tun -- this may cause restarts to fail
Sun Nov  7 01:44:17 2021 WARNING: you are using user/g
 persist-key -- this may cause restarts to fail
Sun Nov  7 01:44:17 2021 TCP/UDP: Preserving recently
```

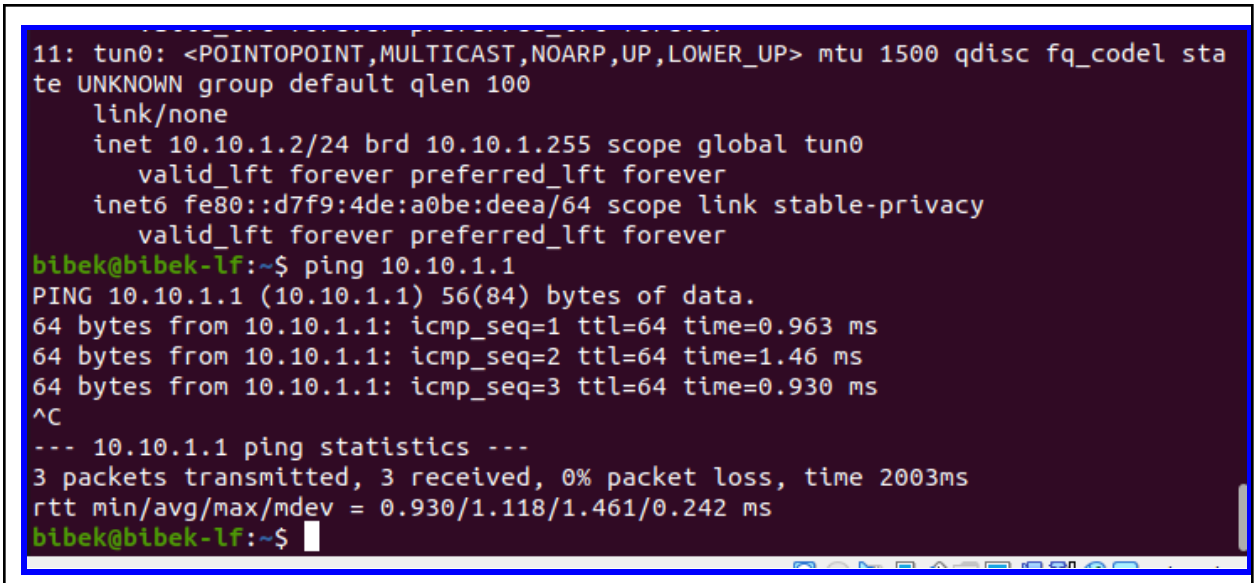
- Successfully connected

```
Sun Nov  7 01:44:17 2021 [server] Peer Connection Initiated with [AF_INET]192.16
8.1.139:1194
Sun Nov  7 01:44:18 2021 TUN/TAP device tun0 opened
Sun Nov  7 01:44:18 2021 /sbin/ip link set dev tun0 up mtu 1500
Sun Nov  7 01:44:18 2021 /sbin/ip addr add dev tun0 10.10.1.2/24 broadcast 10.10
.1.255
Sun Nov  7 01:44:18 2021 GID set to nobody
Sun Nov  7 01:44:18 2021 UID set to nobody
Sun Nov  7 01:44:18 2021 Initialization Sequence Completed
```

- New tunneling IP address after VPN connection

```
bibek@bibek-lf:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:75:a8:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.142/24 brd 192.168.1.255 scope global dynamic noprefixroute
enp0s3
       valid_lft 55135sec preferred_lft 55135sec
    inet6 fe80::e9f4:8400:a73a:c0c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
11: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel sta
te UNKNOWN group default qlen 100
    link/none
    inet 10.10.1.2/24 brd 10.10.1.255 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::d7f9:4de:a0be:deea/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
bibek@bibek-lf:~$
```

- Ping result to host only network



In this way OpenVPN is configured successfully and the client machine gets connected.