

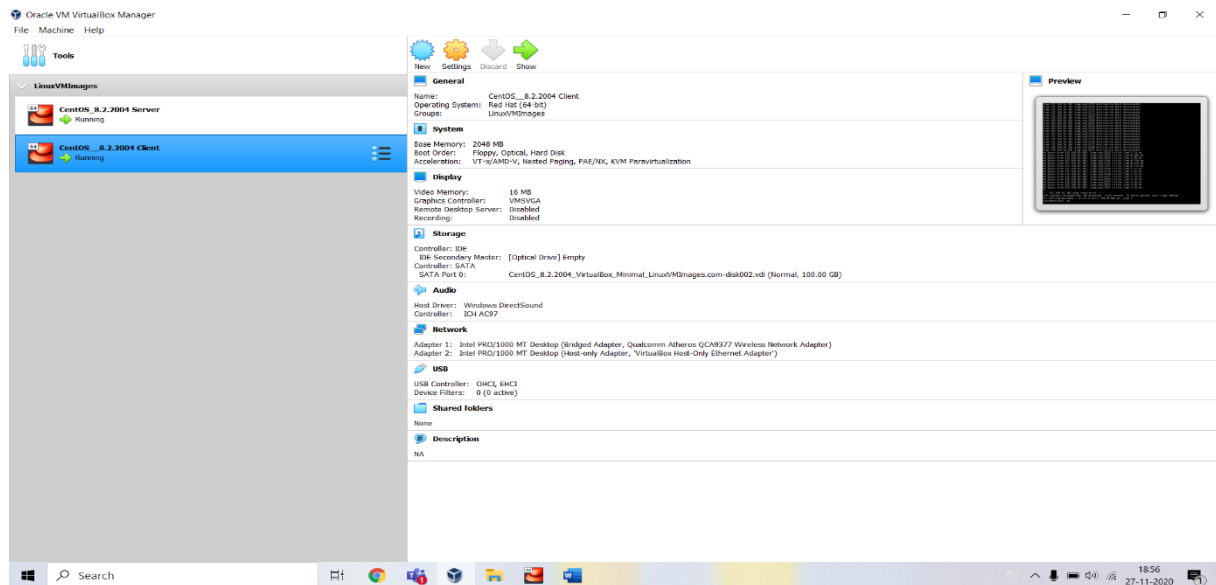
Report on VPN (Task 1)

Name: Aravindh Jawahar

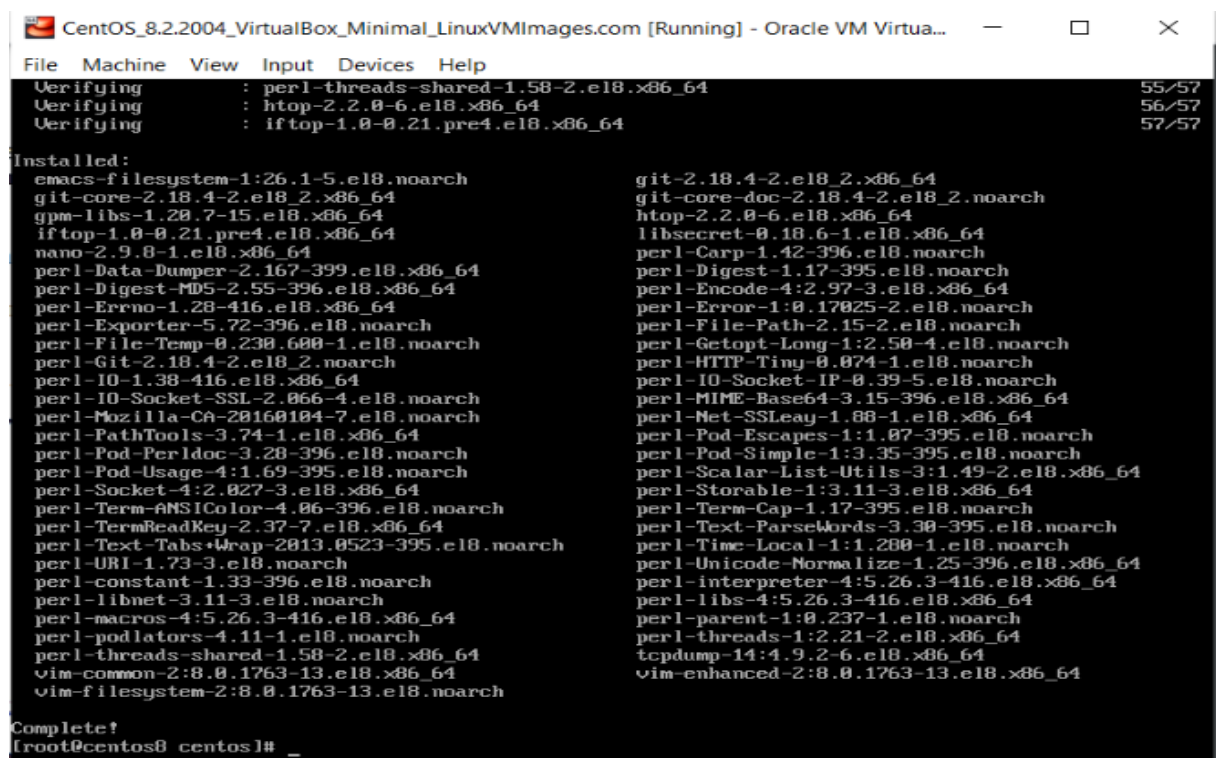
Course – 1 Introduction

Virtual Machines:

VM Server and VM Client



Installing **EPEL** release packages and **TCPDUMP** for monitoring the **TCP** packets transmission and receiving.

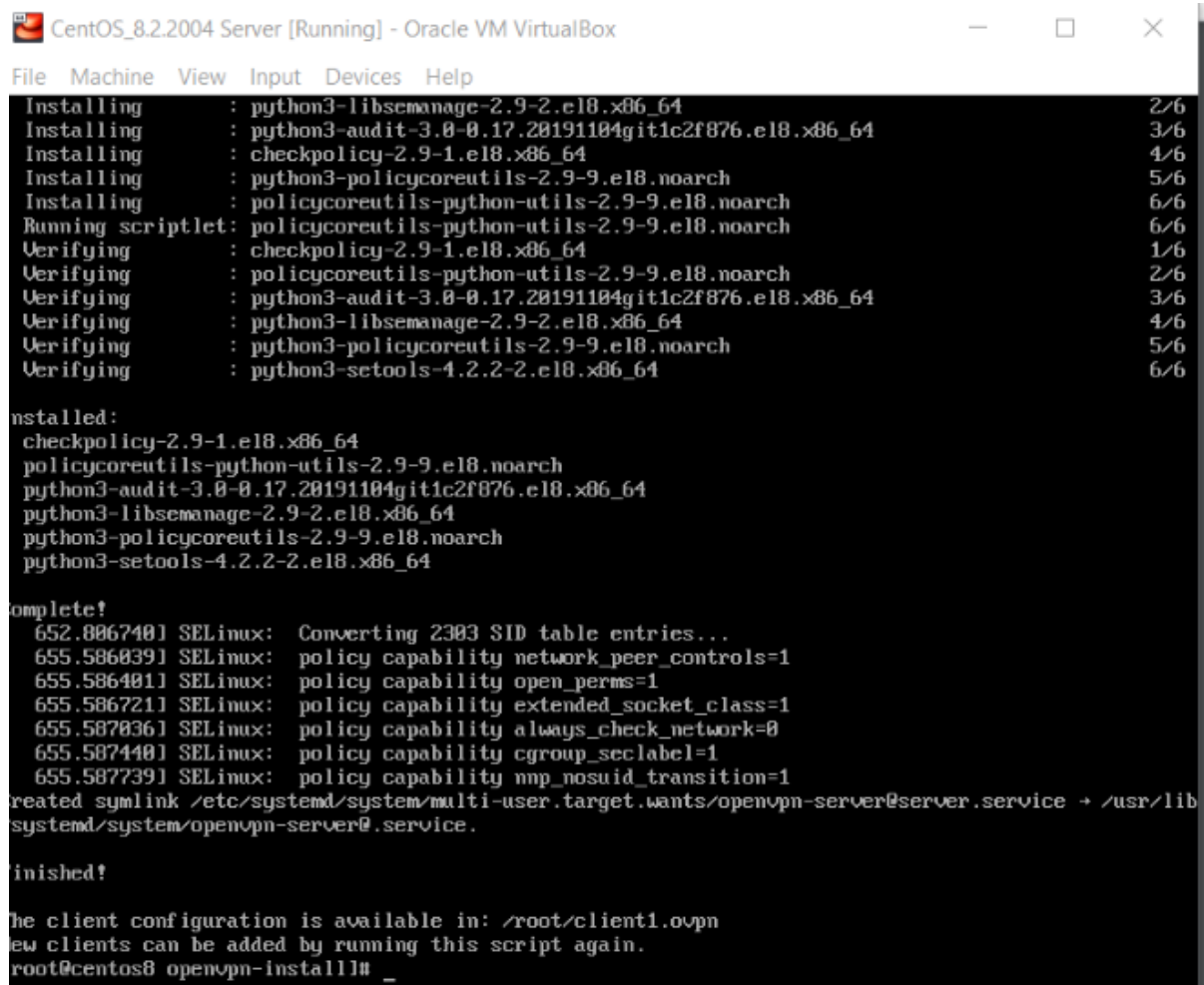


Cloning VPN installation script:

```
root@centos8 ~]# git clone https://github.com/Nyr/openvpn-install.git
Cloning into 'openvpn-install'...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 498 (delta 0), reused 1 (delta 0), pack-reused 487
Receiving objects: 100% (498/498), 157.79 KiB | 1.20 MiB/s, done.
Resolving deltas: 100% (254/254), done.
```

Installing **VPNServer** on Server machine:

```
[root@centos8 ~]# cd openvpn-install
[root@centos8 openvpn-install]# chmod +x openvpn-install.sh
[root@centos8 openvpn-install]#
```



```
CentOS_8.2.2004 Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Installing      : python3-libsemanage-2.9-2.el8.x86_64      2/6
Installing      : python3-audit-3.0-0.17.20191104git1c2f876.el8.x86_64 3/6
Installing      : checkpolicy-2.9-1.el8.x86_64             4/6
Installing      : python3-policycoreutils-2.9-9.el8.noarch  5/6
Installing      : policycoreutils-python-utils-2.9-9.el8.noarch 6/6
Running scriptlet: policycoreutils-python-utils-2.9-9.el8.noarch 6/6
Verifying       : checkpolicy-2.9-1.el8.x86_64             1/6
Verifying       : policycoreutils-python-utils-2.9-9.el8.noarch 2/6
Verifying       : python3-audit-3.0-0.17.20191104git1c2f876.el8.x86_64 3/6
Verifying       : python3-libsemanage-2.9-2.el8.x86_64     4/6
Verifying       : python3-policycoreutils-2.9-9.el8.noarch  5/6
Verifying       : python3-setools-4.2.2-2.el8.x86_64        6/6

Installed:
checkpolicy-2.9-1.el8.x86_64
policycoreutils-python-utils-2.9-9.el8.noarch
python3-audit-3.0-0.17.20191104git1c2f876.el8.x86_64
python3-libsemanage-2.9-2.el8.x86_64
python3-policycoreutils-2.9-9.el8.noarch
python3-setools-4.2.2-2.el8.x86_64

Complete!
652.806740] SELinux: Converting 2303 SID table entries...
655.586039] SELinux: policy capability network_peer_controls=1
655.586401] SELinux: policy capability open_perms=1
655.586721] SELinux: policy capability extended_socket_class=1
655.587036] SELinux: policy capability always_check_network=0
655.587440] SELinux: policy capability cgroup_sclabel=1
655.587739] SELinux: policy capability mnp_nosuid_transition=1
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service + /usr/lib
systemd/system/openvpn-server@.service.

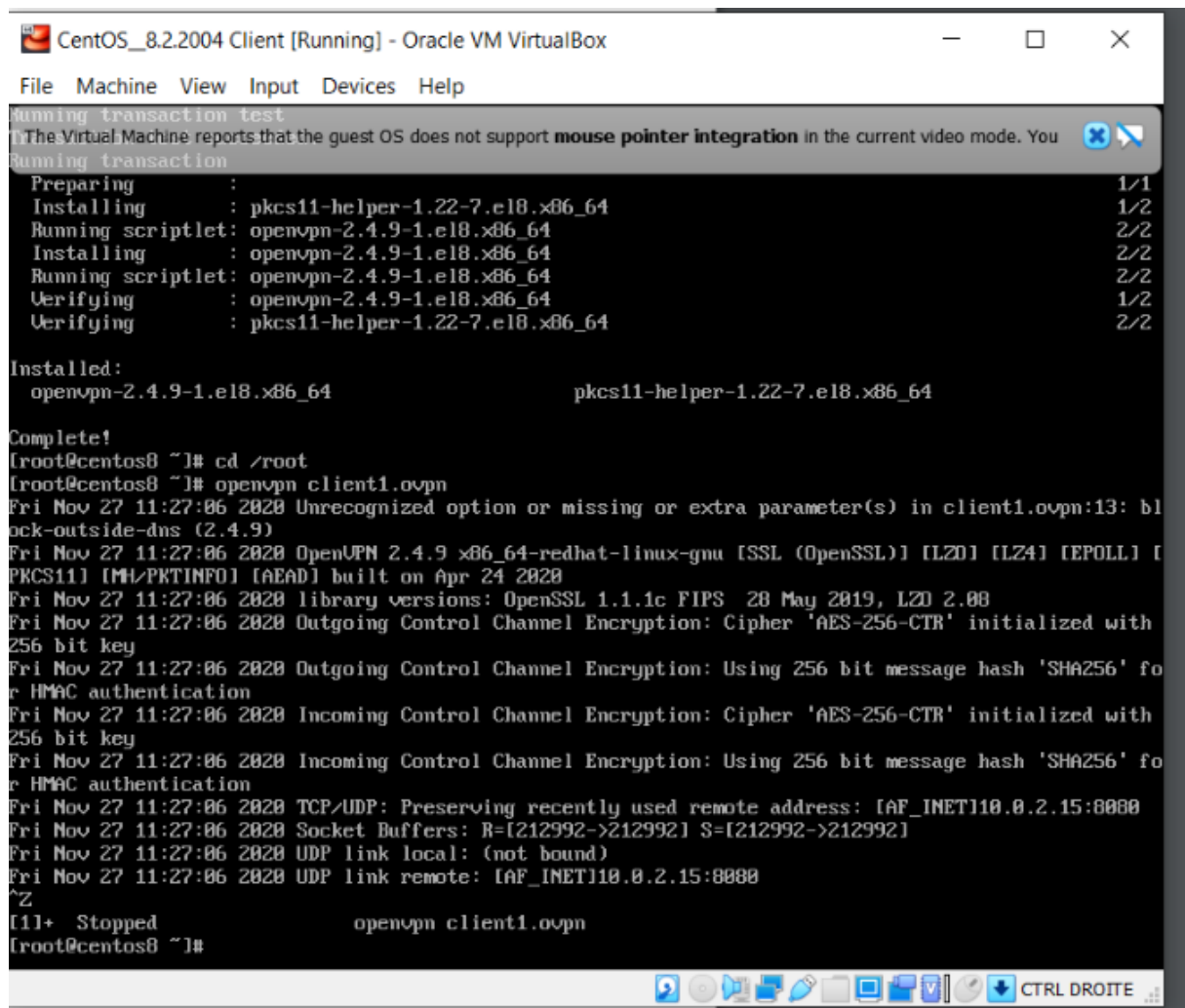
Finished!

The client configuration is available in: /root/client1.ovpn
New clients can be added by running this script again.
root@centos8 openvpn-install]#
```

scp command is used to get the client1.ovpn from server system.

```
[root@centos8 ~]# scp root@192.168.56.102:/root/client1.ovpn .
root@192.168.56.102's password:
client1.ovpn                                100% 4989    528.0KB/s   00:00
[root@centos8 ~]#
```

Transferring client1.ovpn file from Server to client using **SCP** command and **credentials**:



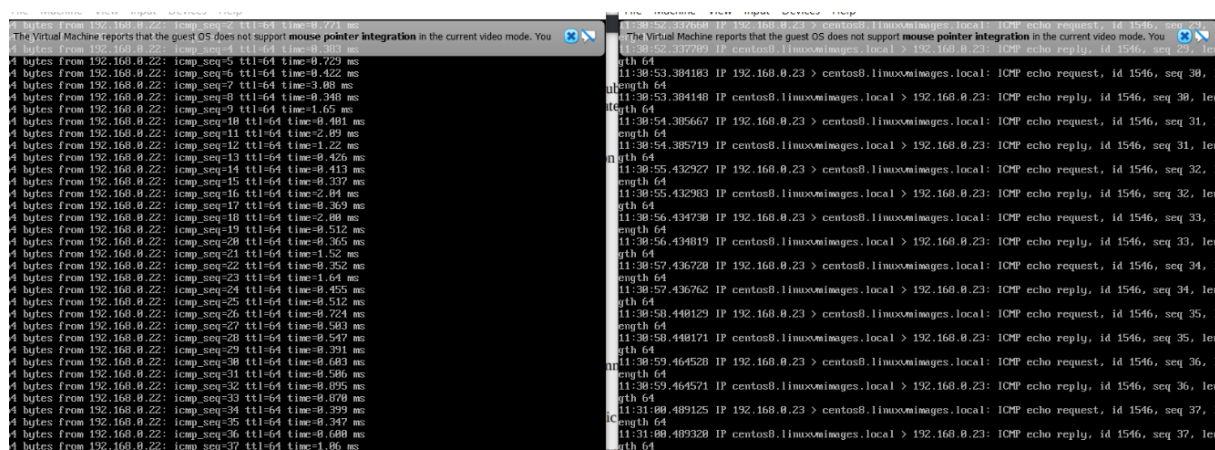
```
CentOS_8.2.0004 Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Running transaction test
The Virtual Machine reports that the guest OS does not support mouse pointer integration in the current video mode. You
Running transaction
Preparing : 1/1
Installing : pkcs11-helper-1.22-7.el8.x86_64 1/2
Running scriptlet: openvpn-2.4.9-1.el8.x86_64 2/2
Installing : openvpn-2.4.9-1.el8.x86_64 2/2
Running scriptlet: openvpn-2.4.9-1.el8.x86_64 2/2
Verifying : openvpn-2.4.9-1.el8.x86_64 1/2
Verifying : pkcs11-helper-1.22-7.el8.x86_64 2/2

Installed:
openvpn-2.4.9-1.el8.x86_64 pkcs11-helper-1.22-7.el8.x86_64

Complete!
[root@centos8 ~]# cd /root
[root@centos8 ~]# openvpn client1.ovpn
Fri Nov 27 11:27:06 2020 Unrecognized option or missing or extra parameter(s) in client1.ovpn:13: block-outside-dns (2.4.9)
Fri Nov 27 11:27:06 2020 OpenVPN 2.4.9 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PTINFO] [AEAD] built on Apr 24 2020
Fri Nov 27 11:27:06 2020 library versions: OpenSSL 1.1.1c FIPS 28 May 2019, LZO 2.08
Fri Nov 27 11:27:06 2020 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Fri Nov 27 11:27:06 2020 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Fri Nov 27 11:27:06 2020 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
Fri Nov 27 11:27:06 2020 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
Fri Nov 27 11:27:06 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]10.0.2.15:8080
Fri Nov 27 11:27:06 2020 Socket Buffers: R=[212992->212992] S=[212992->212992]
Fri Nov 27 11:27:06 2020 UDP link local: (not bound)
Fri Nov 27 11:27:06 2020 UDP link remote: [AF_INET]10.0.2.15:8080
^Z
[1]+ Stopped openvpn client1.ovpn
[root@centos8 ~]#
```

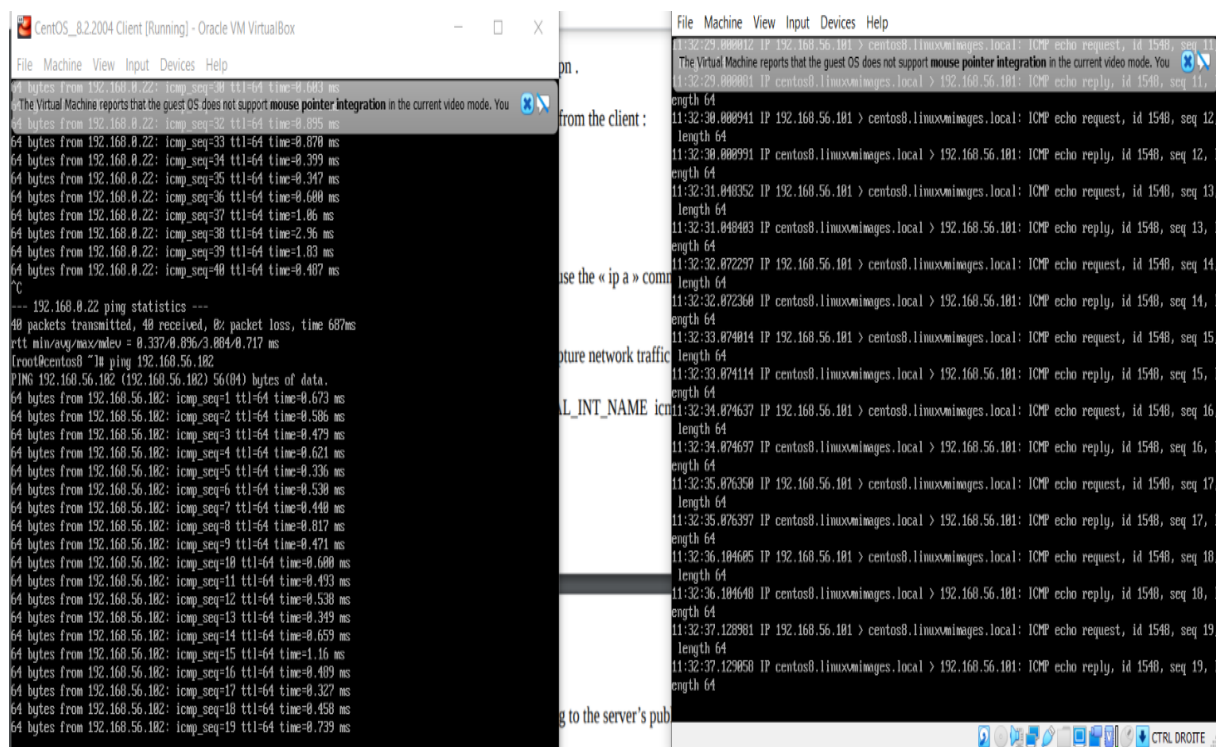
Ping on server physical IP address and it correspondent traffic on server



```
192.168.0.22: icmp_seq=1 ttl=64 time=0.729 ms
4 bytes from 192.168.0.22: icmp_seq=1 ttl=64 time=0.729 ms
4 bytes from 192.168.0.22: icmp_seq=2 ttl=64 time=0.422 ms
4 bytes from 192.168.0.22: icmp_seq=3 ttl=64 time=0.388 ms
4 bytes from 192.168.0.22: icmp_seq=4 ttl=64 time=0.348 ms
4 bytes from 192.168.0.22: icmp_seq=5 ttl=64 time=1.65 ms
4 bytes from 192.168.0.22: icmp_seq=6 ttl=64 time=0.401 ms
4 bytes from 192.168.0.22: icmp_seq=7 ttl=64 time=2.89 ms
4 bytes from 192.168.0.22: icmp_seq=8 ttl=64 time=1.22 ms
4 bytes from 192.168.0.22: icmp_seq=9 ttl=64 time=0.426 ms
4 bytes from 192.168.0.22: icmp_seq=10 ttl=64 time=0.413 ms
4 bytes from 192.168.0.22: icmp_seq=11 ttl=64 time=0.337 ms
4 bytes from 192.168.0.22: icmp_seq=12 ttl=64 time=2.84 ms
4 bytes from 192.168.0.22: icmp_seq=13 ttl=64 time=0.369 ms
4 bytes from 192.168.0.22: icmp_seq=14 ttl=64 time=0.452 ms
4 bytes from 192.168.0.22: icmp_seq=15 ttl=64 time=0.512 ms
4 bytes from 192.168.0.22: icmp_seq=16 ttl=64 time=0.365 ms
4 bytes from 192.168.0.22: icmp_seq=17 ttl=64 time=1.52 ms
4 bytes from 192.168.0.22: icmp_seq=18 ttl=64 time=0.352 ms
4 bytes from 192.168.0.22: icmp_seq=19 ttl=64 time=1.64 ms
4 bytes from 192.168.0.22: icmp_seq=20 ttl=64 time=0.365 ms
4 bytes from 192.168.0.22: icmp_seq=21 ttl=64 time=1.52 ms
4 bytes from 192.168.0.22: icmp_seq=22 ttl=64 time=0.352 ms
4 bytes from 192.168.0.22: icmp_seq=23 ttl=64 time=0.593 ms
4 bytes from 192.168.0.22: icmp_seq=24 ttl=64 time=0.547 ms
4 bytes from 192.168.0.22: icmp_seq=25 ttl=64 time=0.391 ms
4 bytes from 192.168.0.22: icmp_seq=26 ttl=64 time=0.399 ms
4 bytes from 192.168.0.22: icmp_seq=27 ttl=64 time=0.590 ms
4 bytes from 192.168.0.22: icmp_seq=28 ttl=64 time=0.895 ms
4 bytes from 192.168.0.22: icmp_seq=29 ttl=64 time=0.870 ms
4 bytes from 192.168.0.22: icmp_seq=30 ttl=64 time=0.399 ms
4 bytes from 192.168.0.22: icmp_seq=31 ttl=64 time=0.347 ms
4 bytes from 192.168.0.22: icmp_seq=32 ttl=64 time=0.680 ms
4 bytes from 192.168.0.22: icmp_seq=33 ttl=64 time=1.06 ms

192.168.0.23: icmp_seq=1 ttl=64 time=0.729 ms
4 bytes from 192.168.0.23: icmp_seq=1 ttl=64 time=0.729 ms
4 bytes from 192.168.0.23: icmp_seq=2 ttl=64 time=0.422 ms
4 bytes from 192.168.0.23: icmp_seq=3 ttl=64 time=0.388 ms
4 bytes from 192.168.0.23: icmp_seq=4 ttl=64 time=0.348 ms
4 bytes from 192.168.0.23: icmp_seq=5 ttl=64 time=1.65 ms
4 bytes from 192.168.0.23: icmp_seq=6 ttl=64 time=0.401 ms
4 bytes from 192.168.0.23: icmp_seq=7 ttl=64 time=2.89 ms
4 bytes from 192.168.0.23: icmp_seq=8 ttl=64 time=1.22 ms
4 bytes from 192.168.0.23: icmp_seq=9 ttl=64 time=0.426 ms
4 bytes from 192.168.0.23: icmp_seq=10 ttl=64 time=0.413 ms
4 bytes from 192.168.0.23: icmp_seq=11 ttl=64 time=0.337 ms
4 bytes from 192.168.0.23: icmp_seq=12 ttl=64 time=2.84 ms
4 bytes from 192.168.0.23: icmp_seq=13 ttl=64 time=0.369 ms
4 bytes from 192.168.0.23: icmp_seq=14 ttl=64 time=0.452 ms
4 bytes from 192.168.0.23: icmp_seq=15 ttl=64 time=0.512 ms
4 bytes from 192.168.0.23: icmp_seq=16 ttl=64 time=0.365 ms
4 bytes from 192.168.0.23: icmp_seq=17 ttl=64 time=1.52 ms
4 bytes from 192.168.0.23: icmp_seq=18 ttl=64 time=0.352 ms
4 bytes from 192.168.0.23: icmp_seq=19 ttl=64 time=1.64 ms
4 bytes from 192.168.0.23: icmp_seq=20 ttl=64 time=0.365 ms
4 bytes from 192.168.0.23: icmp_seq=21 ttl=64 time=1.52 ms
4 bytes from 192.168.0.23: icmp_seq=22 ttl=64 time=0.352 ms
4 bytes from 192.168.0.23: icmp_seq=23 ttl=64 time=0.593 ms
4 bytes from 192.168.0.23: icmp_seq=24 ttl=64 time=0.547 ms
4 bytes from 192.168.0.23: icmp_seq=25 ttl=64 time=0.391 ms
4 bytes from 192.168.0.23: icmp_seq=26 ttl=64 time=0.399 ms
4 bytes from 192.168.0.23: icmp_seq=27 ttl=64 time=0.590 ms
4 bytes from 192.168.0.23: icmp_seq=28 ttl=64 time=0.895 ms
4 bytes from 192.168.0.23: icmp_seq=29 ttl=64 time=0.870 ms
4 bytes from 192.168.0.23: icmp_seq=30 ttl=64 time=0.399 ms
4 bytes from 192.168.0.23: icmp_seq=31 ttl=64 time=0.347 ms
4 bytes from 192.168.0.23: icmp_seq=32 ttl=64 time=0.680 ms
4 bytes from 192.168.0.23: icmp_seq=33 ttl=64 time=1.06 ms
```

Ping on tunnel IP



(11) We cannot see the traffic on server for tunnel IP because tunnel is in virtual private network and it is not known by the client .

(12) In server machine we installed VPN server (open VPN) and started it by setting the transfer methods(UDP) along with the physical IP address of the server. Now the tunnel is created on the server machine with its corresponding IP address makes the virtual network. OVPN file which act as a certificate to communicate the server from client , this can be achieved by scp command. A ping on the server with its physical interface and its traffic can be seen on server using the tcpdump command. While ping on tunnel interface address , ping gets successful and we cannot see the traffic of ICMP on server because of its encryption over the virtual private network.