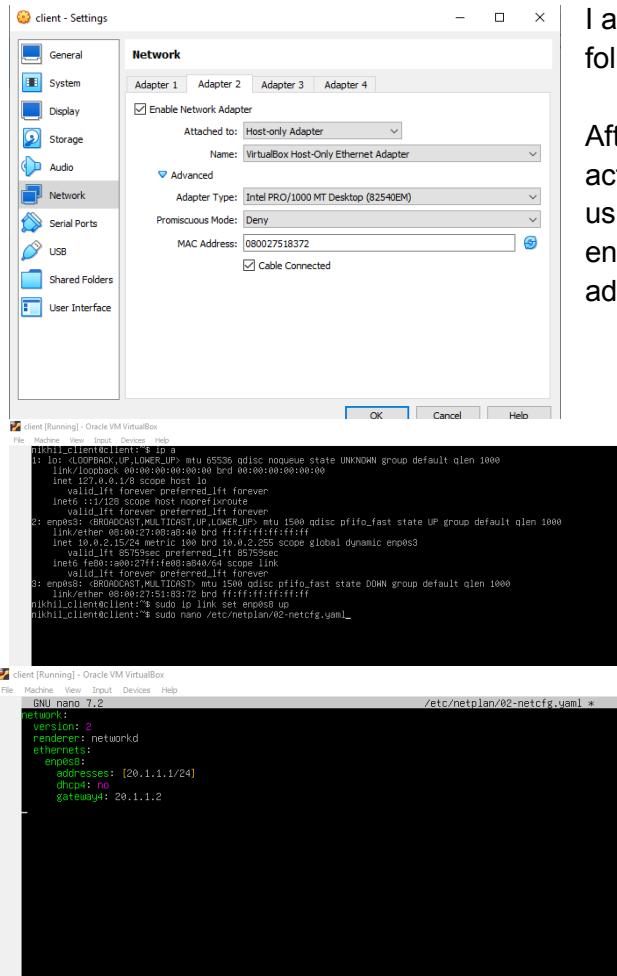


- 1) a) For the initial setup of four VM's I created 4 different VM's with each having OS Ubuntu server edition. After creating them I added a new Network adaptor available to each of the machines with the following configurations:-

For Client:-

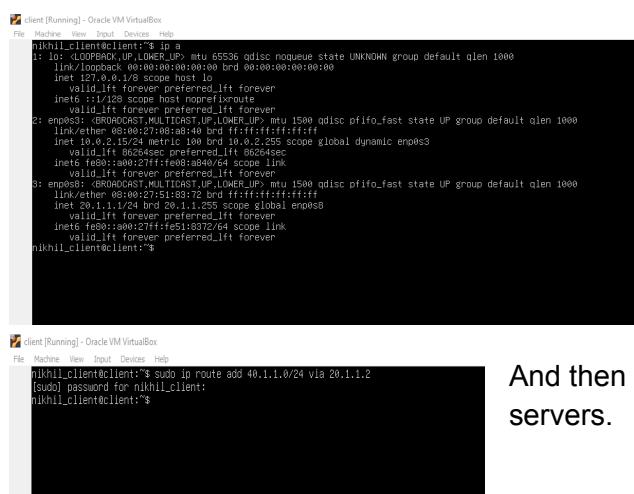


I added a new network adaptor with the following configuration.

After this I ran the command "ip a" and then activated the newly connected adaptor using "sudo ip link set enp0s8 up" here enp0s8 was the name of the network adaptor.

After this I ran "sudo nano /etc/netplan/02-netcfg.yaml" to add a new configuration for this network adaptor.

These are the things I added to the newly created yaml file. This sets the static IP assigned to client as "20.1.1.1" with subnet mask value as 24 and gateway IP as "20.1.1.2"

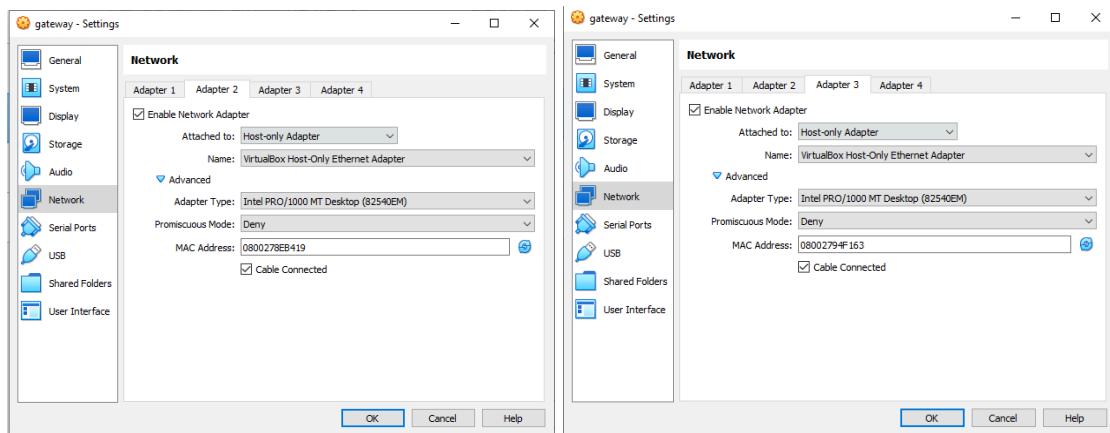


After this i applied this using command "sudo netplan apply" and then rebooted the system. This was the final output for "ip a".

And then added the route for communication with servers.

For gateway:-

There were 2 adaptors for the gateway, one for communicating with client and one for servers. Following are the configurations for both adaptors. (Adaptor 2&3).



```
nikhil_gateway@ gateway:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: enp0s3: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 08:00:27:8e:b4:19 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
            valid_lft 86390sec preferred_lft 86390sec
        inet6 fe80::a00:27ff:fe8e:b419/64 scope link
            valid_lft forever preferred_lft forever
3: enp0s8: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 08:00:27:94:f1:63 brd ff:ff:ff:ff:ff:ff
        nikhil_gateway@ gateway:~$ ip link set enp0s8 up
        RTNETLINK answers: Operation not permitted
        nikhil_gateway@ gateway:~$ sudo ip link set enp0s8 up
        [sudo] password for nikhil_gateway:
        nikhil_gateway@ gateway:~$ sudo ip link set enp0s9 up
        nikhil_gateway@ gateway:~$ sudo nano /etc/netplan/02-netcfg.yaml
```

After this I ran the command "ip a" and then activated the newly connected adaptors using "sudo ip link set enp0s8 up" and "sudo ip link set enp0s9 up" here, enp0s8 and enp0s9 were the name of the network adaptor. Then after this i added the new configurations for yaml files.

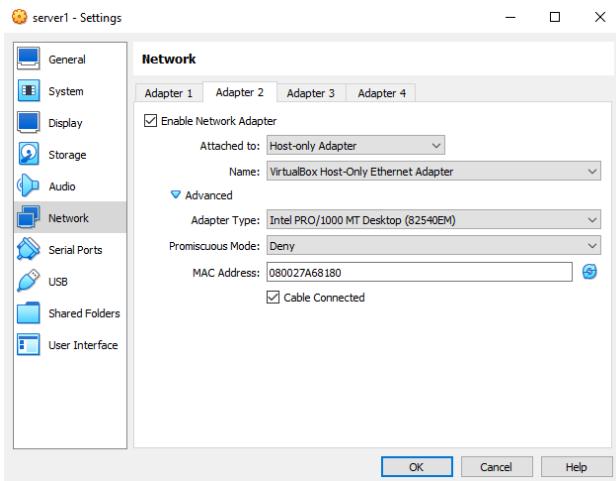
```
nikhil_gateway@ gateway:~$ nano /etc/netplan/02-netcfg.yaml
#cloud-config
# version: 2
# renderer: networkd
# ethernets:
#   eth0:
#     addresses: [20.1.1.2/24]
#     dhcpc: no
#     enp0s8:
#       addresses: [40.1.1.2/24]
#       dhcp4: no
```

These are the things I added to the newly created yaml file. This sets the static IP assigned to adaptor 2 (which communicates with client) as "20.1.1.2" with subnet mask value as 24 and adaptor 3 (for communicating with servers) as "40.1.1.2" with subnet mask as 24. And after this i applied this using "sudo netplan apply" and rebooted the system.

```
nikhil_gateway@ gateway:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: enp0s3: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 08:00:27:94:f1:63 brd ff:ff:ff:ff:ff:ff
        nikhil_gateway@ gateway:~$ ip link set enp0s8 up
        RTNETLINK answers: Operation not permitted
        nikhil_gateway@ gateway:~$ sudo ip link set enp0s8 up
        [sudo] password for nikhil_gateway:
        nikhil_gateway@ gateway:~$ sudo ip link set enp0s9 up
        nikhil_gateway@ gateway:~$ sudo nano /etc/netplan/02-netcfg.yaml
        nikhil_gateway@ gateway:~$
```

This is the final output for "ip a"

For server1:-



I added a new network adaptor with the following configuration.

```
[nikhil_server1@server1 ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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_lifeti...
```

```
[nikhil_server1@server1 ~]$ ip link set enp0s8 up
[nikhil_server1@server1 ~]$
```

After this I ran the command “ip a” and then activated the newly connected adaptor using “sudo ip link set enp0s8 up” here enp0s8 was the name of the network adaptor.

```
[nikhil_server1@server1 ~]$ nano /etc/netplan/02-netcfg.yaml
[nikhil_server1@server1 ~]$ sudo netplan apply
[nikhil_server1@server1 ~]$
```

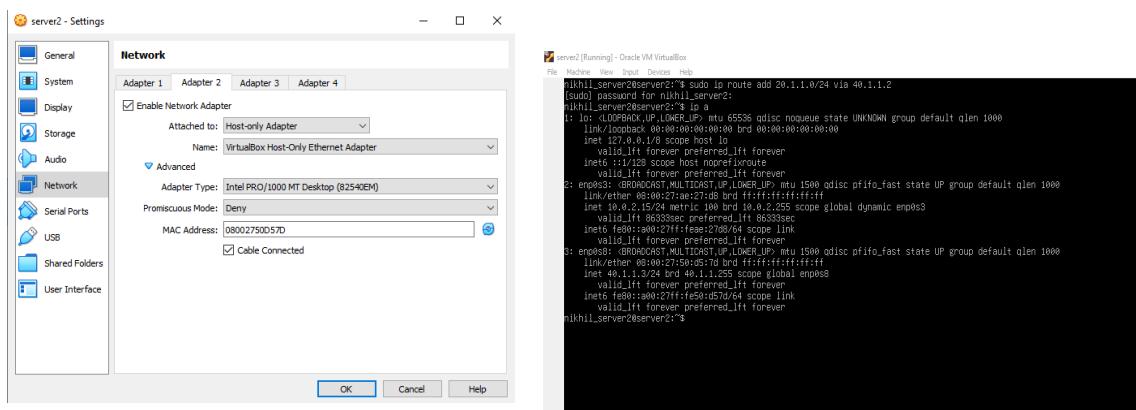
These are the things I added to the newly created yaml file. This sets the static IP assigned to server1 as “40.1.1.1” with subnet mask value as 24 and gateway IP as “40.1.1.2”. And after this applied these configurations.

```
[server1:Running] - Oracle VM VirtualBox  
File  
  
nikhil1_Server1@server1:~$ sudo ip route add 20.1.0.0/24 via 40.1.1.2  
[sudo] password for nikhil1-server1:  
nikhil1_Server1@server1:~$ ip a  
1: lo: <LOOPBACK,NOQUEUE,QDISC NOQUEUE> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback brd 00:00:00:00:00:00 state UNKNOWN group 0x2  
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo  
        valid_lft forever preferred_lft forever  
        link-layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff  
        valid_lft forever preferred_lft forever  
2: enp0s3: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 00:0c:29:1f:0e:0f brd ff:ff:ff:ff:ff:ff state DOWN  
    inet 10.0.2.15/24 brd 10.0.2.255 metric 100 brd 00:0c:29:1f:0e:0f state global dynamic enp0s3  
        valid_lft 86314sec preferred_lft 63014sec  
        link-layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff  
        valid_lft forever preferred_lft forever  
3: enp0s8: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 00:0c:29:7a:81:00 brd ff:ff:ff:ff:ff:ff state DOWN  
    inet 10.0.2.24/24 brd 10.0.2.255 metric 100 brd 00:0c:29:7a:81:00 state global enp0s8  
        valid_lft forever preferred_lft forever  
        link-layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff  
        valid_lft forever preferred_lft forever  
nikhil1_Server1@server1:~$
```

Here i added the route to connect to client using gateway using command “ip route add 20.1.1.0/24” via 40.1.1.2”. This is the final output for “ip a”

For server2:-

(Same things were done for server2 by just changing the route command and static IP address in yaml file).
enp0s8 is the new network adaptor.



So, for part (a) we just need to add a new yaml file configuration and configure the routes using command “`sudo ip route add <destination_ip> via <gateway_ip>`”.

b) To add the forwarding functionality we just need to run this on gateway “`sudo sysctl -w net.ipv4.ip_forward=1`”. Following is the screenshot for same:-

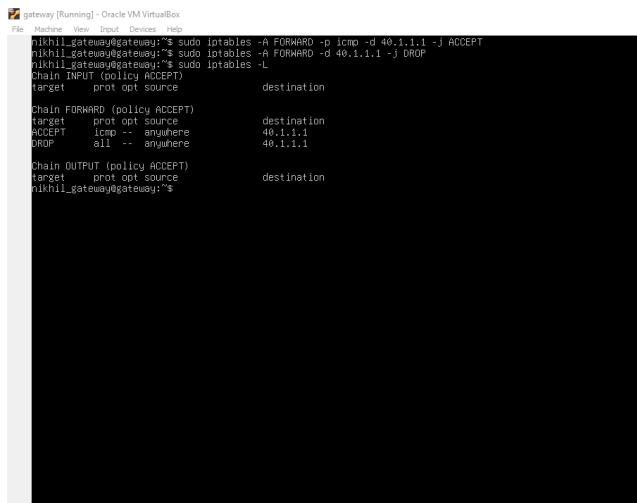
```
nikhil_gateway@nikhil-gateway:~$ sudo sysctl -w net.ipv4.ip_forward=1  
[sudo] password for nikhil_gateway:  
net.ipv4.ip_forward=1  
nikhil_gateway@nikhil-gateway:~$
```

- 2) a) To filter the traffic at the gateway VM we use the iptables command. At the gateway VM, we execute the following commands:-

```
sudo iptables -A FORWARD -p icmp -d 40.1.1.1 -j ACCEPT
sudo iptables -A FORWARD -d 40.1.1.1 -j DROP
```

Here the first command allows the ICMP packets (ping) to server1 and the next command drops every packet that has destination as server1 IP's address.

Following is the command on the gateway:-



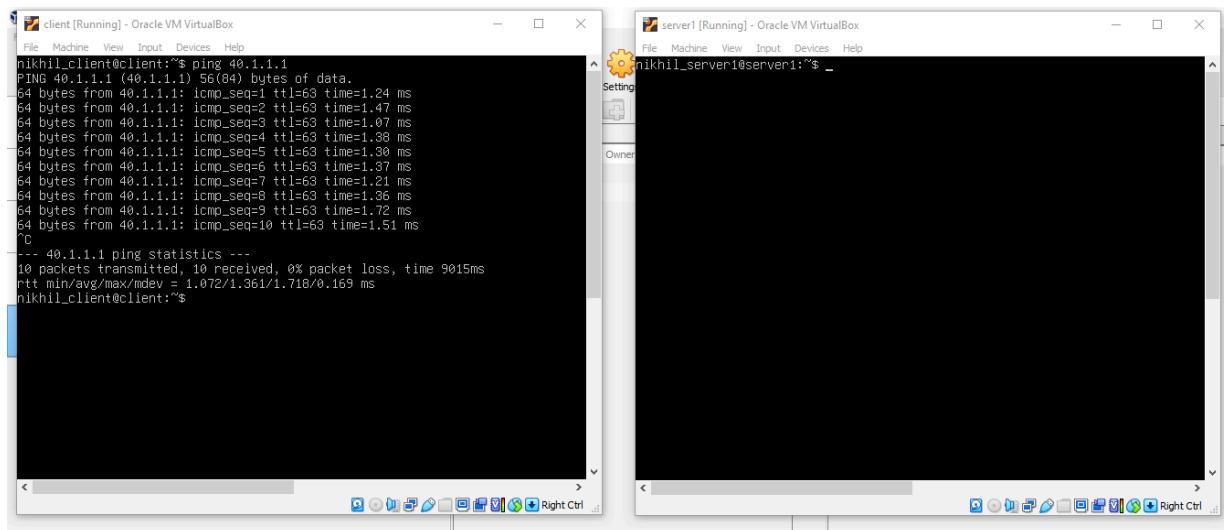
```
nikhil_gateway@gateway:~$ sudo iptables -A FORWARD -p icmp -d 40.1.1.1 -j ACCEPT
nikhil_gateway@gateway:~$ sudo iptables -A FORWARD -d 40.1.1.1 -j DROP
nikhil_gateway@gateway:~$ sudo iptables -L
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT    icmp  --  anywhere             40.1.1.1
DROP      all   --  anywhere             40.1.1.1

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
nikhil_gateway@gateway:~$
```

Tests after applying the traffic filtering commands:-

Test for ping on server1 and server2:-

Server1:-



client [Running] - Oracle VM VirtualBox

```
nikhil_client@client:~$ ping 40.1.1.1
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.
64 bytes from 40.1.1.1: icmp_seq=1 ttl=63 time=1.24 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=1.47 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=1.07 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=1.38 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=1.30 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=1.37 ms
64 bytes from 40.1.1.1: icmp_seq=7 ttl=63 time=1.21 ms
64 bytes from 40.1.1.1: icmp_seq=8 ttl=63 time=1.36 ms
64 bytes from 40.1.1.1: icmp_seq=9 ttl=63 time=1.72 ms
64 bytes from 40.1.1.1: icmp_seq=10 ttl=63 time=1.51 ms
^C
--- 40.1.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 1.072/1.361/1.718/0.169 ms
nikhil_client@client:~$
```

server1 [Running] - Oracle VM VirtualBox

```
nikhil_server1@server1:~$
```

Server2:-

```

client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ ping 40.1.1.3
PING 40.1.1.3 (40.1.1.3) 56(84) bytes of data.
64 bytes from 40.1.1.3: icmp_seq=1 ttl=63 time=1.09 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=1.25 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=1.38 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.26 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=1.72 ms
64 bytes from 40.1.1.3: icmp_seq=6 ttl=63 time=1.51 ms
64 bytes from 40.1.1.3: icmp_seq=7 ttl=63 time=1.15 ms
64 bytes from 40.1.1.3: icmp_seq=8 ttl=63 time=1.42 ms
64 bytes from 40.1.1.3: icmp_seq=9 ttl=63 time=1.44 ms
64 bytes from 40.1.1.3: icmp_seq=10 ttl=63 time=1.43 ms
--- 40.1.1.3 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 1.088/1.364/1.723/0.175 ms
^Cnikhil_client@client:~$ 

```

From these, it is clear that the ping worked for both the servers.

Test for TCP requests:-

Server1:-

```

client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ nc 40.1.1.1 5000
hi! from client to server1
^Cnikhil_client@client:~$ 

```

Here the tcp connection between client and server1 fails, which proves that traffic was filtered at the gateway and everything was blocked.

Server2:-

The image shows two terminal windows side-by-side. The left window, titled 'client [Running] - Oracle VM VirtualBox', contains the following command and output:

```
nikhil_client@client:~$ nc 40.1.1.3 5000
hi! from client to server2
hi! from server2
^C
nikhil_client@client:~$
```

The right window, titled 'server2 [Running] - Oracle VM VirtualBox', contains the following command and output:

```
nikhil_server2@server2:~$ nc -l -p 5000
hi! from client to server2
hi! from server2
nikhil_server2@server2:~$ _
```

Here the TCP connection was successful, which indicates that traffic filtering is successful, as everything was allowed for server2.

Test for UDP requests:-

Server1:-

The image shows two terminal windows side-by-side. The left window, titled 'client [Running] - Oracle VM VirtualBox', contains the following command and output:

```
nikhil_client@client:~$ nc -u 40.1.1.1 5000
hi! from client to server1
^C
nikhil_client@client:~$
```

The right window, titled 'server1 [Running] - Oracle VM VirtualBox', contains the following command and output:

```
nikhil_server1@server1:~$ nc -u -l -p 5000
^C
nikhil_server1@server1:~$
```

Here the UDP connection between client and server1 fails, which proves that traffic was filtered at the gateway and everything was blocked.

Server2:-

```

client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ nc -u -l -p 5000
nihil from client to server2
nihil from server2
^C
nikhil_client@client:~$


server2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings
Owner
nikhil_server2@server2:~$ nc -u -l -p 5000
nihil from client to server2
nihil from server2
nikhil_server2@server2:~$ 

```

Here the UDP connection was successful, which indicates that traffic filtering is successful, as everything was allowed for server2.

Tests after removing the traffic filtering commands:-

Now I removed the earlier iptable entries from the gateway using the command:
sudo iptables -F

```

gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_gateway@gateway:~$ sudo iptables -A FORWARD -p icmp -d 40.1.1.1 -j ACCEPT
nikhil_gateway@gateway:~$ sudo iptables -A FORWARD -d 40.1.1.1 -j DROP
nikhil_gateway@gateway:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
          prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
  ACCEPT   icmp -- anywhere            40.1.1.1
  DROP    all  -- anywhere            40.1.1.1
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
nikhil_gateway@gateway:~$ sudo iptables -F
nikhil_gateway@gateway:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
          prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
          prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
nikhil_gateway@gateway:~$ 

```

Test for TCP:-

Server1:-

```

client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ nc -l -p 5000
nihil from client to server1
nihil from server1
^C
nikhil_client@client:~$

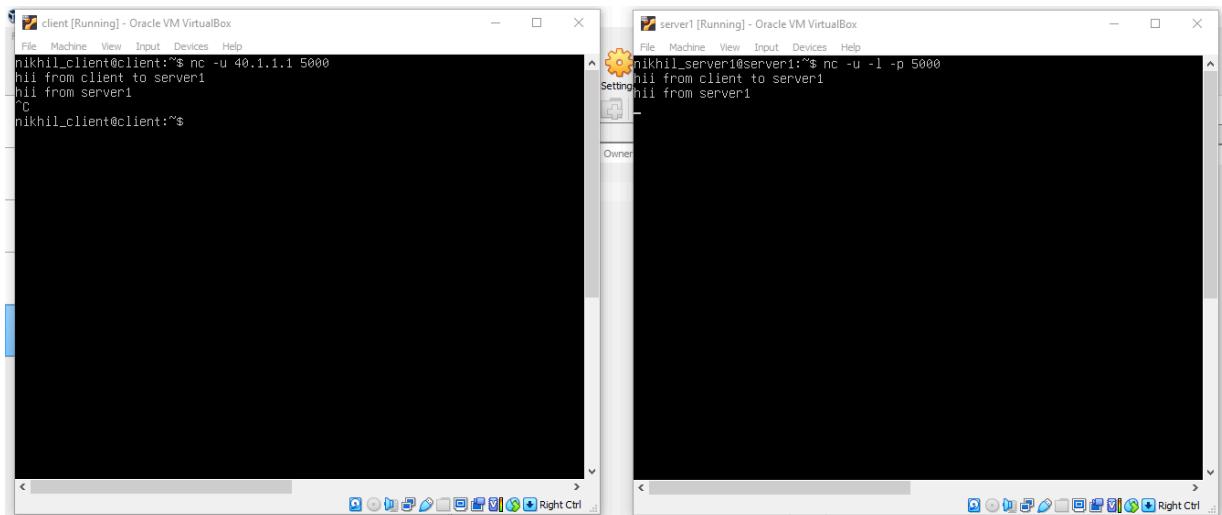

server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings
Owner
nikhil_server1@server1:~$ nc -l -p 5000
nihil from client to server1
nihil from server1
nikhil_server1@server1:~$ 

```

After removing the entries from the iptables for gateway, TCP connection between the client and server1 was successful.

Test for UDP:-

Server1:-



```
nikhil_client@client:~$ nc -u -l -p 5000
nhi from client to server1
nhi from server1
^C
nikhil_client@client:~$
```

```
nikhil_server1@server1:~$ nc -u -l -p 5000
nhi from client to server1
nhi from server1
```

After removing the entries from the iptables for gateway, UDP connection between the client and server1 was successful.

Both of these tests, after adding traffic filtering using iptables and after removing them from iptable at the gateway, clearly show that traffic filtering was successful and we were successfully able to block every traffic which was destined to server1 except ping.

b) To block all the traffic generated from the client that is: 20.1.1.1, we run the following commands on the gateway:-

```
sudo iptables -A FORWARD -p tcp -s 20.1.1.1 -j DROP
sudo iptables -A FORWARD -s 20.1.1.1 -j ACCEPT
```

Here the first command ensures that we drop all the TCP traffic generated by the client using the -p as tcp and -j as DROP for blocking the TCP traffic.

Following are the commands on the gateway:-

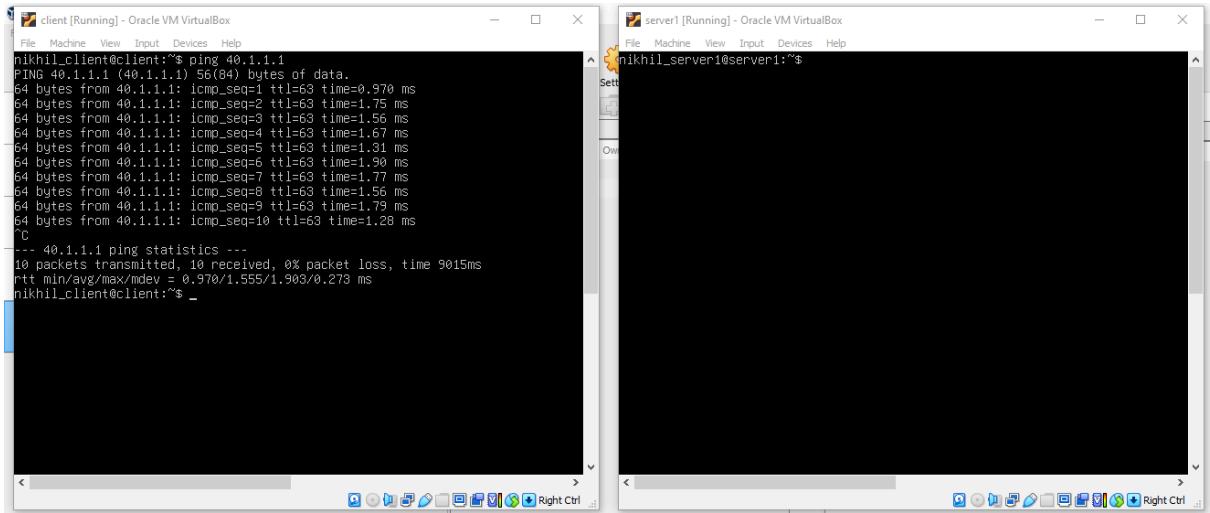


```
nikhil_gateway@gateway:~$ sudo iptables -A FORWARD -p tcp -s 20.1.1.1 -j DROP
nikhil_gateway@gateway:~$ sudo iptables -A FORWARD -s 20.1.1.1 -j ACCEPT
nikhil_gateway@gateway:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP      tcp  --  20.1.1.1            anywhere
ACCEPT    all  --  20.1.1.1            anywhere
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
nikhil_gateway@gateway:~$ _
```

Tests after applying the traffic filtering commands:-

Test for ping on server1 and server2:-

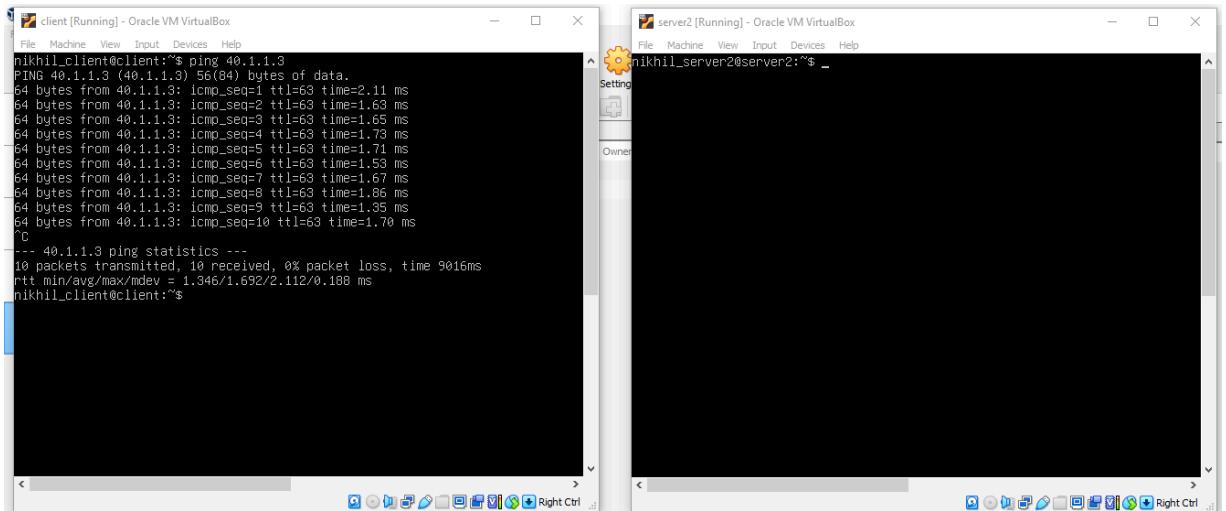
Server1:-



The screenshot shows two windows side-by-side. The left window is titled "client [Running] - Oracle VM VirtualBox" and the right window is titled "server1 [Running] - Oracle VM VirtualBox". Both windows have a black background and white text. The client window displays the output of a ping command to 40.1.1.1, showing 10 packets transmitted with 0% loss and a round-trip time of 9015ms. The server1 window is mostly blank, showing only the prompt "nikhil_server1@server1:~\$".

```
nikhil.client@client:~$ ping 40.1.1.1
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.
64 bytes from 40.1.1.1: icmp_seq=1 ttl=63 time=0.970 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=1.75 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=1.56 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=1.67 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=1.31 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=1.50 ms
64 bytes from 40.1.1.1: icmp_seq=7 ttl=63 time=1.77 ms
64 bytes from 40.1.1.1: icmp_seq=8 ttl=63 time=1.56 ms
64 bytes from 40.1.1.1: icmp_seq=9 ttl=63 time=1.79 ms
64 bytes from 40.1.1.1: icmp_seq=10 ttl=63 time=1.28 ms
^C
--- 40.1.1.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 0.970/1.555/1.903/0.273 ms
nikhil_client@client:~$ _
```

Server2:-



The screenshot shows two windows side-by-side. The left window is titled "client [Running] - Oracle VM VirtualBox" and the right window is titled "server2 [Running] - Oracle VM VirtualBox". Both windows have a black background and white text. The client window displays the output of a ping command to 40.1.1.3, showing 10 packets transmitted with 0% loss and a round-trip time of 9016ms. The server2 window is mostly blank, showing only the prompt "nikhil_server2@server2:~\$".

```
nikhil.client@client:~$ ping 40.1.1.3
PING 40.1.1.3 (40.1.1.3) 56(84) bytes of data.
64 bytes from 40.1.1.3: icmp_seq=1 ttl=63 time=2.11 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=1.63 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=1.65 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.73 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=1.71 ms
64 bytes from 40.1.1.3: icmp_seq=6 ttl=63 time=1.53 ms
64 bytes from 40.1.1.3: icmp_seq=7 ttl=63 time=1.67 ms
64 bytes from 40.1.1.3: icmp_seq=8 ttl=63 time=1.86 ms
64 bytes from 40.1.1.3: icmp_seq=9 ttl=63 time=1.35 ms
64 bytes from 40.1.1.3: icmp_seq=10 ttl=63 time=1.70 ms
^C
--- 40.1.1.3 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9016ms
rtt min/avg/max/mdev = 1.346/1.692/2.112/0.189 ms
nikhil_client@client:~$ _
```

From these, it is clear that the ping worked for both the servers.

Test for TCP requests:-

Server1:-

```

client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ nc 40.1.1.1 5000
hi! from client to server1
^C
nikhil_client@client:~$ 

server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_server1@server1:~$ nc -l -p 5000
Setting
Owner

```

Here the TCP connection between client and server1 fails, which proves that traffic was filtered at the gateway and only the TCP traffic was blocked which was generated by client.

Server2:-

Here the TCP connection between client and server2 fails, which proves that traffic was filtered at the gateway and only the TCP traffic was blocked which was generated by client.

Test for UDP requests:-

Server1:-

```

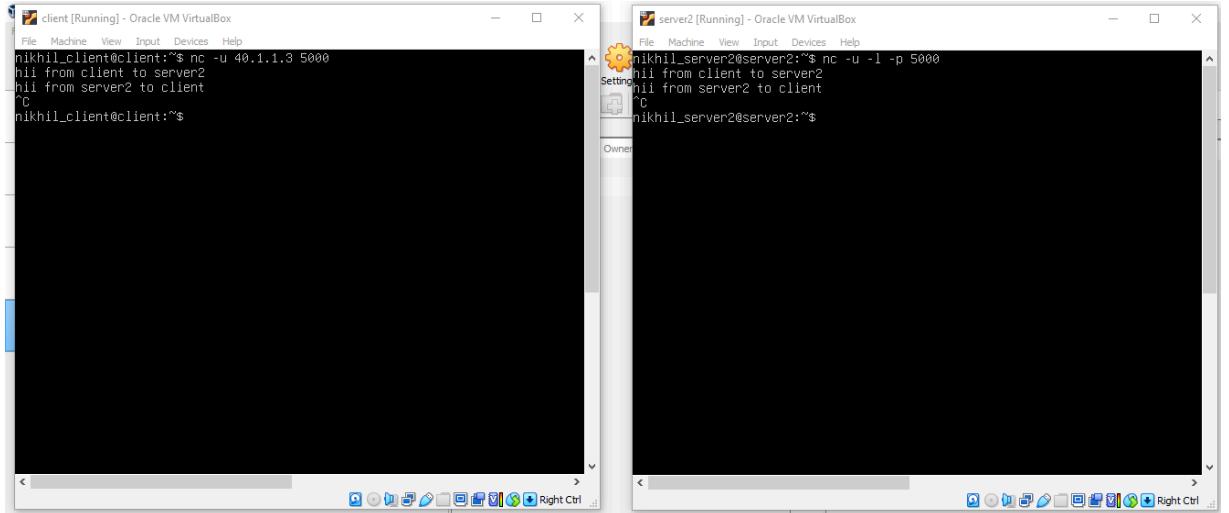
client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ nc -u 40.1.1.1 5000
hi! from client to server1
hi! from server1 to client
^C
nikhil_client@client:~$ _

server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_server1@server1:~$ nc -u -l -p 5000
Setting
Owner

```

Here the UDP connection between client and server1 is successful, which proves that traffic was filtered at the gateway and only the TCP traffic is getting blocked, and this time it was a UDP connection and hence was successful.

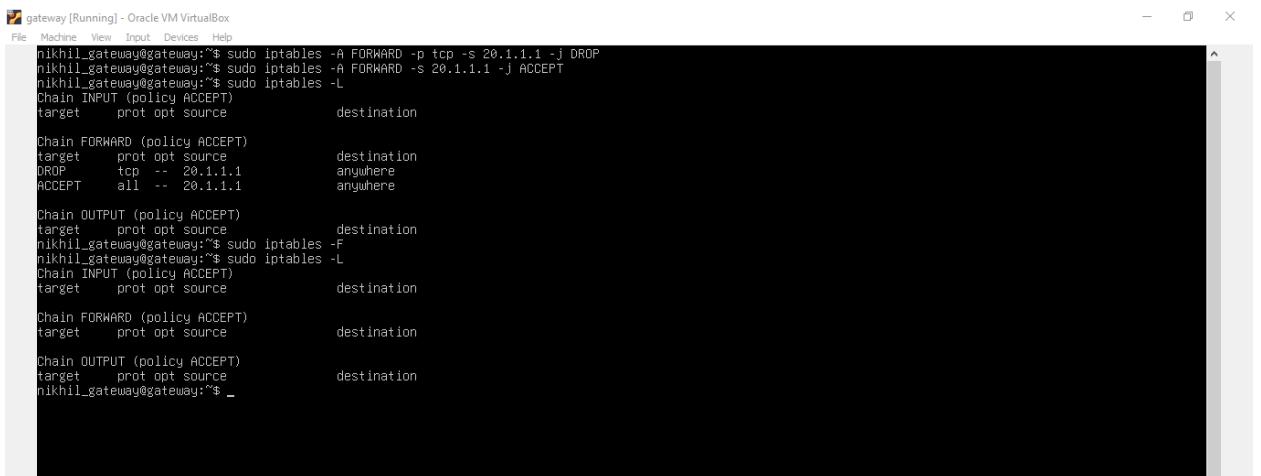
Server2:-



Here the UDP connection between client and server2 is successful, which proves that traffic was filtered at the gateway and only the TCP traffic is getting blocked, and this time it was a UDP connection and hence was successful.

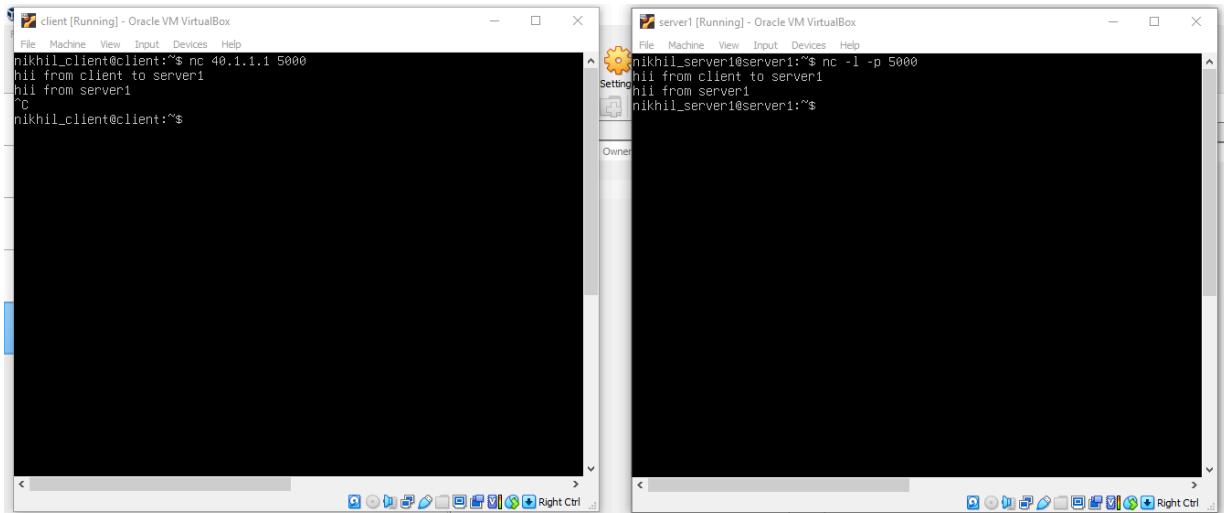
Tests after removing the traffic filtering commands:-

Now I removed the earlier iptable entries from the gateway using the command:
`sudo iptables -F`



Test for TCP requests:-

Server1:-



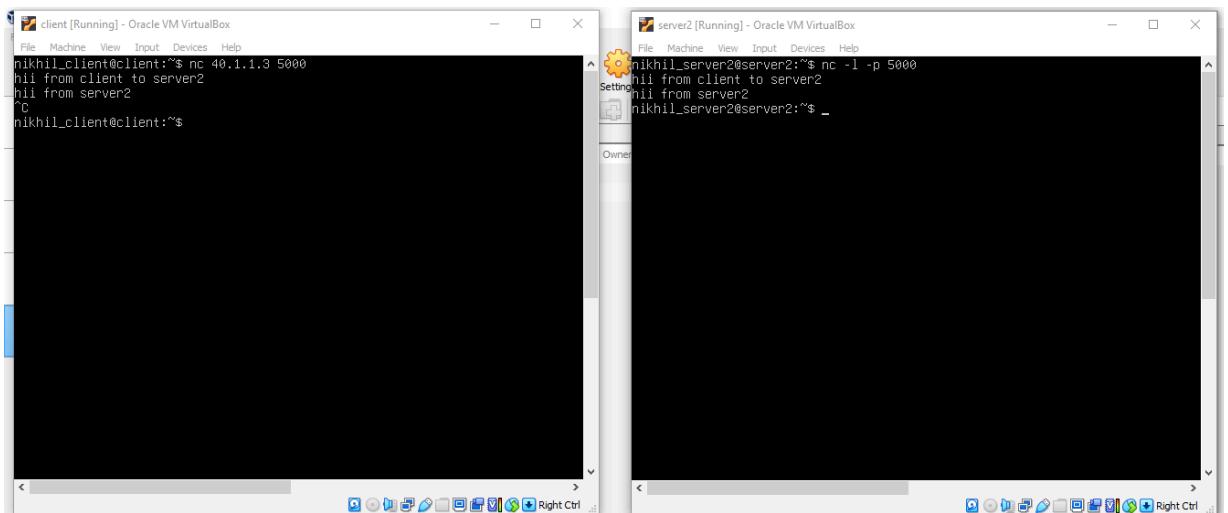
The image shows two terminal windows side-by-side. The left window is titled "client [Running] - Oracle VM VirtualBox" and the right window is titled "server1 [Running] - Oracle VM VirtualBox". Both windows have a black background and white text. In the client window, the user has run the command "nc 40.1.1.1 5000" and is receiving messages from the server. In the server window, the user has run the command "nc -l -p 5000" and is receiving messages from the client. The text in both windows reads:

```
nikhil_client@client:~$ nc 40.1.1.1 5000
hi! from client to server1
hi! from server1
^C
nikhil_client@client:~$
```

```
nikhil.server1@server1:~$ nc -l -p 5000
hi! from client to server1
hi! from server1
nikhil_server1@server1:~$
```

After removing the entries from the iptables for gateway, TCP connection between the client and server1 was successful.

Server2:-



The image shows two terminal windows side-by-side. The left window is titled "client [Running] - Oracle VM VirtualBox" and the right window is titled "server2 [Running] - Oracle VM VirtualBox". Both windows have a black background and white text. In the client window, the user has run the command "nc 40.1.1.3 5000" and is receiving messages from the server. In the server window, the user has run the command "nc -l -p 5000" and is receiving messages from the client. The text in both windows reads:

```
nikhil_client@client:~$ nc 40.1.1.3 5000
hi! from client to server2
hi! from server2
^C
nikhil_client@client:~$
```

```
nikhil_server2@server2:~$ nc -l -p 5000
hi! from client to server2
hi! from server2
nikhil_server2@server2:~$
```

After removing the entries from the iptables for gateway, TCP connection between the client and server2 was successful.

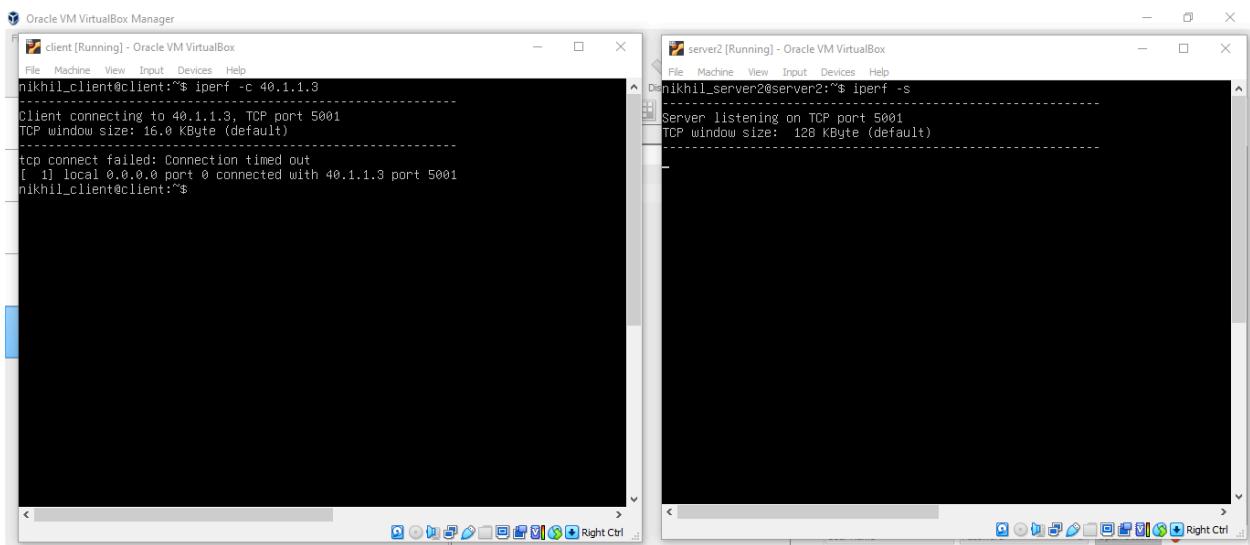
Both of these tests, after adding traffic filtering using iptables and after removing them from iptable at the gateway, clearly show that traffic filtering was successful and we were successfully able to block only the TCP traffic which was generated by the client- 20.1.1.1/24.

3) a) For TCP:-

When I ran the iperf tests between the client (20.1.1.1) and server2 (40.1.1.3) for TCP, then it was not able to connect successfully, this is because, as we are using the same configuration obtained in q2, and hence there we have blocked the TCP connections originating from the client (20.1.1.1) by the command “sudo iptables -A FORWARD -p tcp -s 20.1.1.1 -j DROP”. Following is the screenshot for the same:-

Command used at server: iperf -s

Command used at client: iperf -c 40.1.1.3



```
nikhil_client@Client:~$ iperf -c 40.1.1.3
Client connecting to 40.1.1.3, TCP port 5001
TCP window size: 16.0 KByte (default)
[ 1] Local 0.0.0.0 port 0 connected with 40.1.1.3 port 5001
nikhil_client@Client:~$ 

D:\nihil\server2@server2:~$ iperf -s
Server listening on TCP port 5001
TCP window size: 128 KByte (default)
```

For UDP:-

I did a lot 2 tests for UDP connections between client (20.1.1.1) and server2 (40.1.1.1).

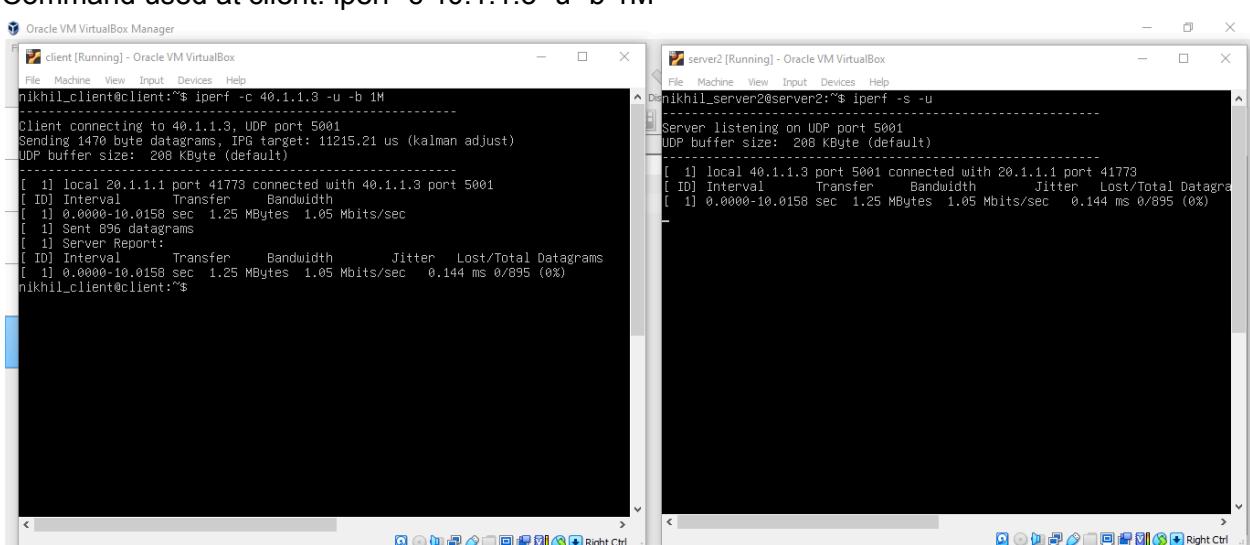
The following are these:-

Tests for different bandwidths:-

i) For 1Mbits/sec

Command used at server: iperf -s -u

Command used at client: iperf -c 40.1.1.3 -u -b 1M



```
nikhil_client@Client:~$ iperf -c 40.1.1.3 -u -b 1M
Client connecting to 40.1.1.3, UDP port 5001
Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust)
UDP buffer size: 208 KByte (default)

[ 1] local 20.1.1.1 port 41773 connected with 40.1.1.3 port 5001
[ ID] Interval Transfer Bandwidth
[ 1] 0.0000-10.0158 sec 1.25 MBytes 1.05 Mbit/sec
[ 1] Sent 896 datagrams
[ 1] Server Report:
[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0000-10.0158 sec 1.25 MBytes 1.05 Mbit/sec 0.144 ms 0/895 (0%)
nikhil_client@Client:~$ 

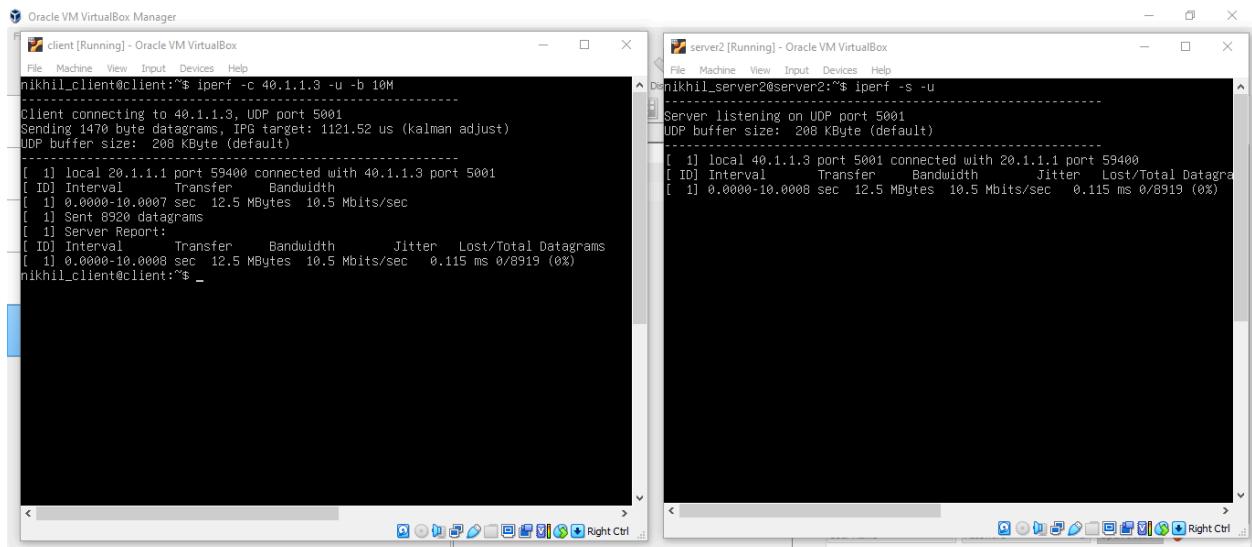
D:\nihil\server2@server2:~$ iperf -s -u
Server listening on UDP port 5001
UDP buffer size: 208 KByte (default)

[ 1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 41773
[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0000-10.0158 sec 1.25 MBytes 1.05 Mbit/sec 0.144 ms 0/895 (0%)
```

ii) For 10Mbits/sec

Command used at server: iperf -s -u

Command used at client: iperf -c 40.1.1.3 -u -b 10M



The image shows two Oracle VM VirtualBox terminal windows. The left window, titled 'client [Running] - Oracle VM VirtualBox', displays the command: 'nikhil_client@client:~\$ iperf -c 40.1.1.3 -u -b 10M'. The output shows a connection to port 5001 and a bandwidth of 10.5 Mbytes/sec. The right window, titled 'server2 [Running] - Oracle VM VirtualBox', displays the command: 'nikhil_server2@server2:~\$ iperf -s -u'. The output shows a listening port of 5001 and a connection from the client with a bandwidth of 10.5 Mbytes/sec.

```
nikhil_client@client:~$ iperf -c 40.1.1.3 -u -b 10M
Client connecting to 40.1.1.3, UDP port 5001
Sending 1470 byte datagrams, IPG target: 1121.52 us (kalman adjust)
UDP buffer size: 208 KByte (default)

[ 1] local 20.1.1.1 port 59400 connected with 40.1.1.3 port 5001
[ ID] Interval Transfer Bandwidth
[ 1] 0.0000-10.0007 sec 12.5 MBytes 10.5 Mbits/sec
[ 1] Sent 8920 datagrams
[ 1] Server Report:
[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0000-10.0008 sec 12.5 MBytes 10.5 Mbits/sec 0.115 ms 0/8919 (0%)
nikhil_client@client:~$ 

nikhil_server2@server2:~$ iperf -s -u
Server listening on UDP port 5001
UDP buffer size: 208 KByte (default)

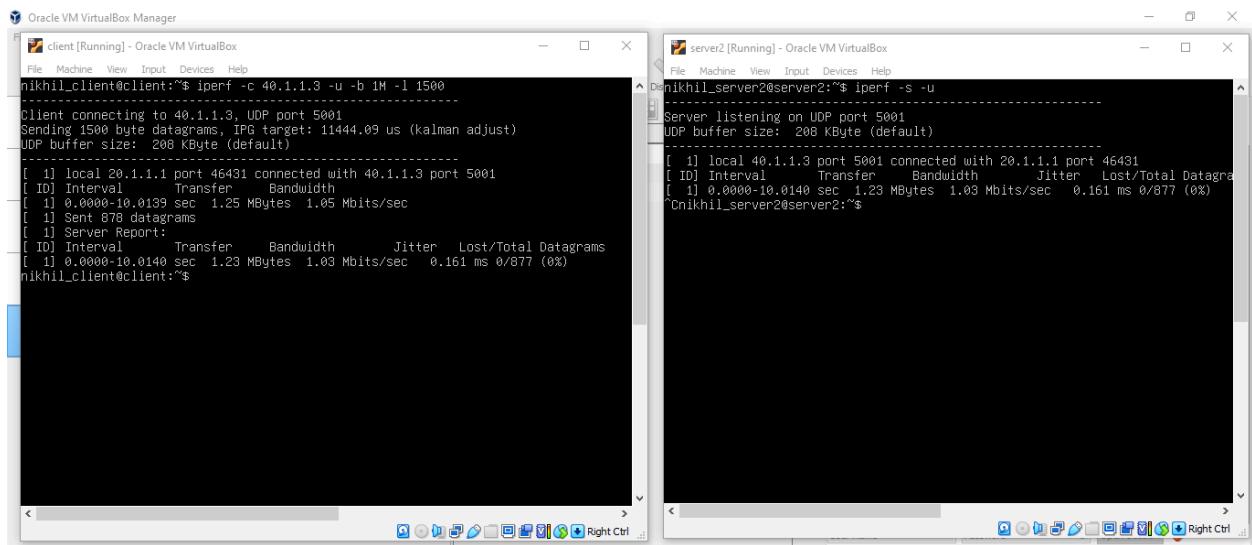
[ 1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 59400
[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0000-10.0000 sec 12.5 MBytes 10.5 Mbits/sec 0.115 ms 0/8919 (0%)
nikhil_server2@server2:~$ 
```

Interpretation:-

In both cases the target bandwidth was reached with .05 more for 1Mbps and 0.5 more for 10Mbps with 0% data loss between client and server. Jitter was almost the same for both cases. The more bandwidth achieved may be because of, iperf tries to achieve the target bandwidth by sending packets at calculated intervals. However, due to small variations in network timing (like packet scheduling or network congestion), packets may arrive at slightly different rates than expected.

Tests for different packet sizes with the same bandwidth:-

i) For 1500 bytes size:-



The image shows two Oracle VM VirtualBox terminal windows. The left window, titled 'client [Running] - Oracle VM VirtualBox', displays the command: 'nikhil_client@client:~\$ iperf -c 40.1.1.3 -u -b 1M -l 1500'. The output shows a connection to port 5001 and a bandwidth of 1.05 Mbytes/sec. The right window, titled 'server2 [Running] - Oracle VM VirtualBox', displays the command: 'nikhil_server2@server2:~\$ iperf -s -u'. The output shows a listening port of 5001 and a connection from the client with a bandwidth of 1.05 Mbytes/sec.

```
nikhil_client@client:~$ iperf -c 40.1.1.3 -u -b 1M -l 1500
Client connecting to 40.1.1.3, UDP port 5001
Sending 1500 byte datagrams, IPG target: 11444.09 us (kalman adjust)
UDP buffer size: 208 KByte (default)

[ 1] local 20.1.1.1 port 46431 connected with 40.1.1.3 port 5001
[ ID] Interval Transfer Bandwidth
[ 1] 0.0000-10.0135 sec 1.25 MBytes 1.05 Mbits/sec
[ 1] Sent 878 datagrams
[ 1] Server Report:
[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0000-10.0140 sec 1.23 MBytes 1.03 Mbits/sec 0.161 ms 0/877 (0%)
nikhil_client@client:~$ 

nikhil_server2@server2:~$ iperf -s -u
Server listening on UDP port 5001
UDP buffer size: 208 KByte (default)

[ 1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 46431
[ ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0000-10.0140 sec 1.23 MBytes 1.03 Mbits/sec 0.161 ms 0/877 (0%)
nikhil_server2@server2:~$ 
```

ii) For 2000 bytes size:-

The screenshot shows two terminal windows from Oracle VM VirtualBox Manager. The left window, titled 'client [Running] - Oracle VM VirtualBox', displays the command output for a client-side iPerf test:

```
nikhil_client@client:~$ iperf -c 40.1.1.3 -u -b 1M -l 2000
Client connecting to 40.1.1.3, UDP port 5001
Sending 2000 byte datagrams, IPG target: 15258.79 us (kalman adjust)
UDP buffer size: 200 KByte (default)
[  ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] local 20.1.1.1 port 55788 connected with 40.1.1.3 port 5001
[  1] 0.0000-10.0259 sec 1.26 MBytes 1.65 Mbits/sec
[  1] Sent 660 datagrams
[  1] Server Report:
[  1] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] 0.0000-10.0257 sec 946 KBytes 773 Kbits/sec 0.141 ms 0/659 (0%)
nikhil_client@client:~$
```

The right window, titled 'server2 [Running] - Oracle VM VirtualBox', displays the command output for a server-side iPerf test:

```
nikhil_server2@server2:~$ iperf -s -u
Server listening on UDP port 5001
UDP buffer size: 200 KByte (default)
[  1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 55788
[  1] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] 0.0000-10.0257 sec 946 KBytes 773 Kbits/sec 0.142 ms 0/659 (0%)
```

iii) For 5000 bytes size:-

The screenshot shows two terminal windows from Oracle VM VirtualBox Manager. The left window, titled 'client [Running] - Oracle VM VirtualBox', displays the command output for a client-side iPerf test:

```
nikhil_client@client:~$ iperf -c 40.1.1.3 -u -b 1M -l 5000
Client connecting to 40.1.1.3, UDP port 5001
Sending 5000 byte datagrams, IPG target: 38146.97 us (kalman adjust)
UDP buffer size: 200 KByte (default)
[  ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] local 20.1.1.1 port 55855 connected with 40.1.1.3 port 5001
[  1] 0.0000-10.0712 sec 1.27 MBytes 1.06 Mbits/sec
[  1] Sent 267 datagrams
[  1] Server Report:
[  1] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] 0.0000-10.0716 sec 382 KBytes 311 Kbits/sec 0.163 ms 0/266 (0%)
nikhil_client@client:~$
```

The right window, titled 'server2 [Running] - Oracle VM VirtualBox', displays the command output for a server-side iPerf test:

```
nikhil_server2@server2:~$ iperf -s -u
Server listening on UDP port 5001
UDP buffer size: 200 KByte (default)
[  1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 55855
[  1] 0.0000-10.0716 sec 382 KBytes 311 Kbits/sec 0.164 ms 0/266 (0%)
```

iv) For 10000 bytes size:-

The screenshot shows two terminal windows from Oracle VM VirtualBox Manager. The left window, titled 'client [Running] - Oracle VM VirtualBox', displays the command output for a client-side iPerf test:

```
nikhil_client@client:~$ iperf -c 40.1.1.3 -u -b 1M -l 10000
Client connecting to 40.1.1.3, UDP port 5001
Sending 10000 byte datagrams, IPG target: 76299.95 us (kalman adjust)
UDP buffer size: 200 KByte (default)
[  ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] local 20.1.1.1 port 60992 connected with 40.1.1.3 port 5001
[  1] 0.0000-10.1478 sec 1.29 MBytes 1.06 Mbits/sec
[  1] Sent 136 datagrams
[  1] Server Report:
[  1] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[  1] 0.0000-10.1480 sec 194 KBytes 156 Kbits/sec 0.327 ms 0/135 (0%)
nikhil_client@client:~$
```

The right window, titled 'server2 [Running] - Oracle VM VirtualBox', displays the command output for a server-side iPerf test:

```
nikhil_server2@server2:~$ iperf -s -u
Server listening on UDP port 5001
UDP buffer size: 200 KByte (default)
[  1] local 40.1.1.3 port 5001 connected with 20.1.1.1 port 60992
[  1] 0.0000-10.1480 sec 194 KBytes 156 Kbits/sec 0.327 ms 0/135 (0%)
```

Packet size in Bytes	Bandwidth in Mbps	Jitter in ms
1500	1.03	0.161
2000	0.731	0.141
5000	0.311	0.163
10000	0.156	0.327

Interpretation:-

1. Bandwidth decreases with increasing packet size because larger packets are harder to process, more likely to encounter fragmentation, cause more congestion, and require more buffer space. This reduces the efficiency of the network, causing a lower effective throughput.
 2. Jitter tends to increase for larger packets as network delays become more variable, especially when the network struggles to keep up with the large data load.

b) i) Following is the data for the same using ping 40.1.1.1 -c 100

```

Client [Running] - Oracle VM VirtualBox
File Edit View Insert Insert... Tools Help
# bytes from 40.1.1.1: icmp_seq=64 ttl=63 time=0.633 ms
# bytes from 40.1.1.1: icmp_seq=65 ttl=63 time=0.741 ms
# bytes from 40.1.1.1: icmp_seq=66 ttl=63 time=0.801 ms
# bytes from 40.1.1.1: icmp_seq=67 ttl=63 time=0.831 ms
# bytes from 40.1.1.1: icmp_seq=68 ttl=63 time=0.52 ms
# bytes from 40.1.1.1: icmp_seq=69 ttl=63 time=2.59 ms
# bytes from 40.1.1.1: icmp_seq=70 ttl=63 time=0.669 ms
# bytes from 40.1.1.1: icmp_seq=71 ttl=63 time=0.947 ms
# bytes from 40.1.1.1: icmp_seq=72 ttl=63 time=0.601 ms
# bytes from 40.1.1.1: icmp_seq=73 ttl=63 time=0.793 ms
# bytes from 40.1.1.1: icmp_seq=74 ttl=63 time=0.822 ms
# bytes from 40.1.1.1: icmp_seq=75 ttl=63 time=0.82 ms
# bytes from 40.1.1.1: icmp_seq=76 ttl=63 time=0.817 ms
# bytes from 40.1.1.1: icmp_seq=77 ttl=63 time=0.799 ms
# bytes from 40.1.1.1: icmp_seq=78 ttl=63 time=0.795 ms
# bytes from 40.1.1.1: icmp_seq=79 ttl=63 time=0.794 ms
# bytes from 40.1.1.1: icmp_seq=80 ttl=63 time=0.716 ms
# bytes from 40.1.1.1: icmp_seq=81 ttl=63 time=0.714 ms
# bytes from 40.1.1.1: icmp_seq=82 ttl=63 time=0.746 ms
# bytes from 40.1.1.1: icmp_seq=83 ttl=63 time=0.744 ms
# bytes from 40.1.1.1: icmp_seq=84 ttl=63 time=0.874 ms
# bytes from 40.1.1.1: icmp_seq=85 ttl=63 time=0.841 ms
# bytes from 40.1.1.1: icmp_seq=86 ttl=63 time=0.885 ms
# bytes from 40.1.1.1: icmp_seq=87 ttl=63 time=0.846 ms
# bytes from 40.1.1.1: icmp_seq=88 ttl=63 time=0.746 ms
# bytes from 40.1.1.1: icmp_seq=89 ttl=63 time=0.821 ms
# bytes from 40.1.1.1: icmp_seq=90 ttl=63 time=0.781 ms
# bytes from 40.1.1.1: icmp_seq=91 ttl=63 time=0.821 ms
# bytes from 40.1.1.1: icmp_seq=92 ttl=63 time=0.699 ms
# bytes from 40.1.1.1: icmp_seq=93 ttl=63 time=0.822 ms
# bytes from 40.1.1.1: icmp_seq=94 ttl=63 time=0.757 ms
# bytes from 40.1.1.1: icmp_seq=95 ttl=63 time=0.821 ms
# bytes from 40.1.1.1: icmp_seq=96 ttl=63 time=0.658 ms
# bytes from 40.1.1.1: icmp_seq=97 ttl=63 time=0.828 ms
# bytes from 40.1.1.1: icmp_seq=98 ttl=63 time=0.801 ms
# bytes from 40.1.1.1: icmp_seq=99 ttl=63 time=0.792 ms
# bytes from 40.1.1.1: icmp_seq=100 ttl=63 time=0.978 ms

--- 40.1.1.1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99125ms
rtt min/avg/max/mdev = 0.597/0.891/0.846/0.428 ms
nitchi@Client:~$ tshark -i ens3f -w /tmp/test.pcap
```

Minimum RTT: 0.597 ms

Maximum RTT: 3.460 ms

Avg RTT: 0.881 ms

ii) Following is the data for the same using ping 40.1.1.3 -c 100

Minimum RTT: 0.649 ms

Maximum RTT: 8.610 ms

Avg RTT: 0.922 ms

```

client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
54 bytes from 40.1.1.3: icmp_seq=64 ttl=63 time=0.065 ms
54 bytes from 40.1.1.3: icmp_seq=65 ttl=63 time=0.053 ms
54 bytes from 40.1.1.3: icmp_seq=66 ttl=63 time=0.053 ms
54 bytes from 40.1.1.3: icmp_seq=67 ttl=63 time=0.063 ms
54 bytes from 40.1.1.3: icmp_seq=68 ttl=63 time=0.063 ms
54 bytes from 40.1.1.3: icmp_seq=69 ttl=63 time=0.076 ms
54 bytes from 40.1.1.3: icmp_seq=70 ttl=63 time=0.079 ms
54 bytes from 40.1.1.3: icmp_seq=71 ttl=63 time=0.079 ms
54 bytes from 40.1.1.3: icmp_seq=72 ttl=63 time=0.027 ms
54 bytes from 40.1.1.3: icmp_seq=73 ttl=63 time=0.011 ms
54 bytes from 40.1.1.3: icmp_seq=74 ttl=63 time=0.011 ms
54 bytes from 40.1.1.3: icmp_seq=75 ttl=63 time=0.065 ms
54 bytes from 40.1.1.3: icmp_seq=76 ttl=63 time=0.054 ms
54 bytes from 40.1.1.3: icmp_seq=77 ttl=63 time=0.076 ms
54 bytes from 40.1.1.3: icmp_seq=78 ttl=63 time=0.089 ms
54 bytes from 40.1.1.3: icmp_seq=79 ttl=63 time=0.065 ms
54 bytes from 40.1.1.3: icmp_seq=80 ttl=63 time=0.012 ms
54 bytes from 40.1.1.3: icmp_seq=81 ttl=63 time=0.077 ms
54 bytes from 40.1.1.3: icmp_seq=82 ttl=63 time=0.069 ms
54 bytes from 40.1.1.3: icmp_seq=83 ttl=63 time=0.069 ms
54 bytes from 40.1.1.3: icmp_seq=84 ttl=63 time=0.024 ms
54 bytes from 40.1.1.3: icmp_seq=85 ttl=63 time=0.059 ms
54 bytes from 40.1.1.3: icmp_seq=86 ttl=63 time=0.046 ms
54 bytes from 40.1.1.3: icmp_seq=87 ttl=63 time=0.002 ms
54 bytes from 40.1.1.3: icmp_seq=88 ttl=63 time=0.055 ms
54 bytes from 40.1.1.3: icmp_seq=89 ttl=63 time=0.076 ms
54 bytes from 40.1.1.3: icmp_seq=90 ttl=63 time=0.056 ms
54 bytes from 40.1.1.3: icmp_seq=91 ttl=63 time=0.069 ms
54 bytes from 40.1.1.3: icmp_seq=92 ttl=63 time=0.066 ms
54 bytes from 40.1.1.3: icmp_seq=93 ttl=63 time=0.056 ms
54 bytes from 40.1.1.3: icmp_seq=94 ttl=63 time=0.076 ms
54 bytes from 40.1.1.3: icmp_seq=95 ttl=63 time=0.914 ms
54 bytes from 40.1.1.3: icmp_seq=96 ttl=63 time=0.861 ms
54 bytes from 40.1.1.3: icmp_seq=97 ttl=63 time=0.322 ms
54 bytes from 40.1.1.3: icmp_seq=98 ttl=63 time=0.739 ms
54 bytes from 40.1.1.3: icmp_seq=99 ttl=63 time=0.748 ms
54 bytes from 40.1.1.3: icmp_seq=100 ttl=63 time=0.749 ms
--- 40.1.1.3 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 99113ms
rtt min/avg/max/mdev = 0.649/0.922/8.610/0.843 ms
nikhil_client@client:~$
```

iii) There was no such “significant” difference between the two, but the maximum RTT for 40.1.1.3 was almost 3 times higher than 40.1.1.1. But the average RTT was almost the same, reasons for this are:-

1. Similar network path: Both IP addresses (40.1.1.1 and 40.1.1.3) are on the same subnet, meaning they follow the same route through the network infrastructure, resulting in similar round-trip times.
2. Same physical location: Both the IPs are hosted on VMs within the same physical machine, the RTT will be nearly identical because the physical distance between the source and destination is almost the same.

4) a) Command used: sudo iptables -t nat -A POSTROUTING -s 20.1.1.1/24 -j SNAT --to-source 40.1.1.2

b) Command used: sudo iptables -t nat -A PREROUTING -d 40.1.1.2 -j DNAT --to-destination 20.1.1.1

Below is the screenshot for these commands on gateway:-

```

gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_gateway@gateway:~$ sudo iptables -t nat -A POSTROUTING -s 20.1.1.1 -j SNAT --to-source 40.1.1.2
nikhil_gateway@gateway:~$ sudo iptables -t nat -A PREROUTING -d 40.1.1.2 -j DNAT --to-destination 20.1.1.1
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
nikhil_gateway@gateway:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT      all  --  anywhere            gateway          to:20.1.1.1
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT      all  --  20.1.1.1           anywhere          to:40.1.1.2
nikhil_gateway@gateway:~$
```

- c) Following is the traffic observed at each network interface using tcpdump:-
- i) At Client's Network Interface

```

File Machine View Input Devices Help
nkhil_client@client: ~$ sudo tshark -i enp0s8
[sudo] password for nkhil_client:
Running as user "root" and group "root". This could be dangerous.
Capturing on "enp0s8"
 0. 0.000000000 :: : f0:2:16 ICMPv6 90 Multicast Listener Report Message v2
 2 0.174682159 :: : f0:2:16 ICMPv6 90 Multicast Listener Report Message v2
 3 0.349364238 :: : f0:2:16 ICMPv6 90 Multicast Listener Report Message v2
 4 0.419561932 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 90 Multicast Listener Report Message v2
 5 2.310705495 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 90 Multicast Listener Report Message v2
 6 5.336417871 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 7 5.336417871 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 8 14.66521265 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 9 30.198938917 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
10 30.198938917 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
11 42.839527731 PCSSystemtec_5e0:d57d + Broadcast ARP 60 Who has 40.1.1.2? Tell 20.1.1.3
12 68.376645598 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
13 114.969539762 20.1.1.1 > 40.1.1.1 TCP 74 56014 + 5000 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3339823009 Tscr=0 WS=120
14 114.969539762 20.1.1.1 > 40.1.1.1 TCP 74 56014 + 5000 [SYN] Seq=9 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=3339823009 Tscr=0 WS=120
Ks=128
15 114.96158919 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823010 Tscr=2221798531
16 114.96158919 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823010 Tscr=2221798531
17 120.023941076 PCSSystemtec_51:83:72 + PCSSystemtec_8e:b4:19 ARP 60 Who has 20.1.1.2? Tell 20.1.1.1
18 120.024355384 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 20.1.1.2 is at 00:00:27:8e:b4:19
19 120.459427937 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 Who has 20.1.1.2? Tell 20.1.1.1
20 120.459427937 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 20.1.1.2 is at 00:00:27:8e:b4:19
21 120.939521050 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823009 Tscr=2221798531
22 120.941443020 40.1.1.1 > 20.1.1.1 TCP 66 56014 + 56014 [ACK] Seq=11 Ack=1 Win=65152 Len=0 Tsvl=222184511 Tscr=3339823009
23 120.941443020 40.1.1.1 > 20.1.1.1 TCP 66 56014 + 56014 [ACK] Seq=11 Ack=1 Win=65152 Len=0 Tsvl=222184511 Tscr=3339823009
24 120.949539168 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [ACK] Seq=17 Ack=17 Win=64256 Len=0 Tsvl=3339846452 Tscr=2221821973
25 148.07517395 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [FIN, ACK] Seq=17 Ack=17 Win=64256 Len=0 Tsvl=3339856124 Tscr=2221821973
26 148.0778614 20.1.1.1 > 40.1.1.1 TCP 66 56000 + 56014 [FIN, ACK] Seq=17 Ack=18 Win=65152 Len=0 Tsvl=2221801646 Tscr=3339856124
27 148.0778614 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [ACK] Seq=18 Ack=18 Win=64256 Len=0 Tsvl=3339856127 Tscr=2221801646
'C27 packets captured
nkhil_client@client: ~$ 

```

This shows that TCP connection between client and server1 was successful. And the right side image shows that client (20.1.1.1) is communicating with server1 (40.1.1.1), here the source and destination packet address didn't change, which is expected, as this change should only happen on gateway network interfaces.

ii) At Server1's Network Interface

```

File Machine View Input Devices Help
nkhil_server@server1: ~$ sudo tshark -i enp0s8
[sudo] password for nkhil_server:
Running as user "root" and group "root". This could be dangerous.
Capturing on "enp0s8"
 0. 0.000000000 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 2 0.174682159 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 3 0.349364238 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 4 0.419561932 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 5 2.310705495 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 6 5.336417871 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 7 5.336417871 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 8 14.66521265 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 9 30.198938917 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
10 30.198938917 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
11 42.839527731 PCSSystemtec_5e0:d57d + Broadcast ARP 60 Who has 20.1.1.2? Tell 40.1.1.1
12 68.376645598 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
13 114.969539762 20.1.1.1 > 40.1.1.1 TCP 74 56014 + 5000 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3339823009 Tscr=0 WS=120
14 114.969539762 20.1.1.1 > 40.1.1.1 TCP 74 56014 + 5000 [SYN] Seq=9 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=3339823009 Tscr=0 WS=120
Ks=128
15 114.96158919 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823010 Tscr=2221798531
16 114.96158919 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823010 Tscr=2221798531
17 120.023941076 PCSSystemtec_51:83:72 + PCSSystemtec_8e:b4:19 ARP 60 Who has 20.1.1.2? Tell 20.1.1.1
18 120.024355384 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 20.1.1.2 is at 00:00:27:8e:b4:19
19 120.459427937 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 Who has 20.1.1.2? Tell 20.1.1.1
20 120.459427937 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 20.1.1.2 is at 00:00:27:8e:b4:19
21 120.939521050 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823009 Tscr=2221798531
22 120.941443020 40.1.1.1 > 20.1.1.1 TCP 66 56014 + 56014 [ACK] Seq=11 Ack=1 Win=65152 Len=0 Tsvl=222184511 Tscr=3339823009
23 120.941443020 40.1.1.1 > 20.1.1.1 TCP 66 56014 + 56014 [ACK] Seq=11 Ack=1 Win=65152 Len=0 Tsvl=222184511 Tscr=3339823009
24 120.949539168 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [ACK] Seq=17 Ack=17 Win=64256 Len=0 Tsvl=3339846452 Tscr=2221821973
25 148.07517395 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [FIN, ACK] Seq=17 Ack=17 Win=64256 Len=0 Tsvl=3339856124 Tscr=2221821973
26 148.0778614 20.1.1.1 > 40.1.1.1 TCP 66 56000 + 56014 [FIN, ACK] Seq=17 Ack=18 Win=65152 Len=0 Tsvl=2221801646 Tscr=3339856124
27 148.0778614 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [ACK] Seq=18 Ack=18 Win=64256 Len=0 Tsvl=3339856127 Tscr=2221801646
'C28 packets captured
nkhil_server@server1: ~$ 

```

Left side image confirms that TCP connection between client and server1 was successful. Now, the right side image shows the source and destination packet address, here the connection is between 40.1.1.1 and 40.1.1.2, which means that it is between server1 and gateway's server-side network interface, and thus it proves that the source IP address was changed to 40.1.1.2 when packet was sent by the client.

iii) At Gateway's Network Interface

Client-side Interface

```

File Machine View Input Devices Help
nkhil_gateway@gateway: ~$ sudo tshark -i enp0s8
[sudo] password for nkhil_gateway:
Running as user "root" and group "root". This could be dangerous.
Capturing on "enp0s8"
 0. 0.000000000 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 2 0.174682159 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 3 0.349364238 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 4 0.419561932 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 5 2.310705495 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 6 5.336417871 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 7 5.336417871 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 8 14.66521265 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
 9 30.198938917 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
10 30.198938917 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
11 42.839527731 PCSSystemtec_5e0:d57d + Broadcast ARP 60 Who has 40.1.1.2? Tell 20.1.1.1
12 68.376645598 fe80::a00:27ff:fe50:d57d + f0:2:16 ICMPv6 70 Router Solicitation from 00:00:00:00:00:00
13 114.969539762 20.1.1.1 > 40.1.1.1 TCP 74 56014 + 5000 [SYN] Seq=9 Win=64240 Len=0 MSS=1460 SACK_PERM Tsvl=3339823009 Tscr=0 WS=120
14 114.969539762 20.1.1.1 > 40.1.1.1 TCP 74 56000 + 56014 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM Tsvl=2221798531 Tscr=3339823009 WS=120
Ks=128
15 114.96158919 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823010 Tscr=2221798531
16 114.96158919 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823010 Tscr=2221798531
17 120.023941076 PCSSystemtec_51:83:72 + PCSSystemtec_8e:b4:19 ARP 60 Who has 20.1.1.2? Tell 20.1.1.1
18 120.024355384 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 20.1.1.2 is at 00:00:27:8e:b4:19
19 120.459427937 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 Who has 20.1.1.2? Tell 20.1.1.1
20 120.459427937 PCSSystemtec_8e:b4:19 + PCSSystemtec_51:83:72 ARP 60 20.1.1.2 is at 00:00:27:8e:b4:19
21 120.939521050 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [PSH, ACK] Seq=11 Ack=1 Win=64256 Len=0 Tsvl=3339823009 Tscr=2221798531
22 120.941443020 40.1.1.1 > 20.1.1.1 TCP 66 56000 + 56014 [ACK] Seq=11 Ack=1 Win=65152 Len=0 Tsvl=222184511 Tscr=3339823009
23 120.941443020 40.1.1.1 > 20.1.1.1 TCP 66 56014 + 56014 [ACK] Seq=11 Ack=1 Win=65152 Len=0 Tsvl=222184511 Tscr=3339823009
24 120.949539168 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [ACK] Seq=17 Ack=17 Win=64256 Len=0 Tsvl=3339846452 Tscr=2221821973
25 148.07517395 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [FIN, ACK] Seq=17 Ack=17 Win=64256 Len=0 Tsvl=3339856124 Tscr=2221821973
26 148.0778614 20.1.1.1 > 40.1.1.1 TCP 66 56000 + 56014 [FIN, ACK] Seq=17 Ack=18 Win=65152 Len=0 Tsvl=2221801646 Tscr=3339856124
27 148.0778614 20.1.1.1 > 40.1.1.1 TCP 66 56014 + 5000 [ACK] Seq=18 Ack=18 Win=64256 Len=0 Tsvl=3339856127 Tscr=2221801646
'C015 packets captured
nkhil_gateway@gateway: ~$ 

```

Server side Interface

```
nikhil_gateway@gateway:~$ sudo tshark -i enp0s9
[sudo] password for nikhil_gateway:
Running as user "root" and group "root". This could be dangerous.
Capturing on enp0s9
  0.000000000  40.1.1.3 > 195.125.190.58 NTP 90 NTP Version 4, client
  2 10.250741533  40.1.1.3 > 91.169.91.157 NTP 90 NTP Version 4, client
  3 16.124662562  40.1.1.1 > 40.1.1.1  TCP 74 56014 > 5000 [SYN] Seq=0 Win=54240 Len=0 MSS=1460 SACK_PERM TStamp=3339823009 TSecr=0 WS=128
  4 16.125162715  40.1.1.1 > 40.1.1.2  TCP 74 5000 > 56014 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TStamp=3339823009 TSecr=3339823009 K
S=128
  5 16.125595583  40.1.1.2 > 40.1.1.1  TCP 66 56014 > 5000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=3339828988 TSecr=2221798531
  6 19.895547393  fe80::a0:27ff:fe50:d57d > ff02::2  ICMPv6 70 Router Solicitation from 00:00:27:50:d5:7d
  7 21.262422916 PCSSystemtec_a6:81:00 > PCSSystemtec_94:f1:63 ARP 60 Who has 40.1.1.2? Tell 40.1.1.1
  8 21.262445682 PCSSystemtec_94:f1:63 > PCSSystemtec_a6:81:00 ARP 42 Who has 40.1.1.1? Tell 40.1.1.2
  9 21.593046162 PCSSystemtec_94:f1:63 > PCSSystemtec_a6:81:00 ARP 42 Who has 40.1.1.1? Tell 40.1.1.2
  10 21.593795661 PCSSystemtec_a6:81:00 > PCSSystemtec_94:f1:63 ARP 60 40.1.1.1 is at 00:00:27:a6:81:80
  11 22.103929553  40.1.1.2 > 40.1.1.1  TCP 82 56014 > 5000 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=16 TStamp=3339828988 TSecr=2221798531
  12 22.104761840  40.1.1.1 > 40.1.1.2  TCP 66 5000 > 56014 [ACK] Seq=1 Ack=17 Win=65152 Len=0 TStamp=3339828988
  13 39.566891600  40.1.1.1 > 40.1.1.2  TCP 82 5000 > 56014 [PSH, ACK] Seq=1 Ack=17 Win=65152 Len=16 TStamp=2221821973 TSecr=3339828988
  14 39.567670387  40.1.1.2 > 40.1.1.1  TCP 66 56014 > 5000 [ACK] Seq=17 Ack=17 Win=64256 Len=0 TStamp=3339846452 TSecr=2221821973
  15 49.239174427  40.1.1.2 > 40.1.1.1  TCP 66 56014 > 5000 [FIN, ACK] Seq=17 Ack=17 Win=64256 Len=0 TStamp=3339856124 TSecr=2221821973
  16 49.240461754  40.1.1.1 > 40.1.1.2  TCP 66 5000 > 56014 [FIN, ACK] Seq=18 Ack=18 Win=65152 Len=0 TStamp=2221831646 TSecr=3339856124
  17 49.242168229  40.1.1.2 > 40.1.1.1  TCP 66 56014 > 5000 [ACK] Seq=18 Ack=18 Win=64256 Len=0 TStamp=3339856127 TSecr=2221831646
  18 54.360830088 PCSSystemtec_94:f1:63 > PCSSystemtec_a6:81:00 ARP 42 Who has 40.1.1.1? Tell 40.1.1.2
  19 54.361371846 PCSSystemtec_a6:81:00 > PCSSystemtec_94:f1:63 ARP 60 40.1.1.1 is at 00:00:27:a6:81:80
^C19 packets captured
nikhil_gateway@gateway:~$
```

From these images it is clear that source IP was changed to “40.1.1.2” and then after the response it was again reverted back to the original source IP address.

- 5) From q3 (b), both the servers have almost the same average RTT values with server1 having a slightly less time, and hence, we assign a probability of 0.8 to the server1 for load balancing.
Command used: -

1. sudo iptables -t nat -A PREROUTING -s 20.1.1.1/24 -m statistic --mode random --probability 0.8 -j DNAT --to-destination 40.1.1.1
2. sudo iptables -t nat -A PREROUTING -s 20.1.1.1/24 -j DNAT --to-destination 40.1.1.3

Here the first command routes 80% of the traffic to server1 (40.1.1.1) and second command assigns the remaining 20% of the traffic to server2 (40.1.1.3).

After this, we need to ensure that responses return through the gateway and hence we set up the source NAT:-

1. sudo iptables -t nat -A POSTROUTING -d 40.1.1.1/24 -j SNAT --to-source 40.1.1.2
2. sudo iptables -t nat -A POSTROUTING -d 40.1.1.3/24 -j SNAT --to-source 40.1.1.2

These will ensure that both the servers (40.1.1.1 and 40.1.1.3) send responses back through the gateway.

```
nikhil_gateway@gateway:~$ sudo iptables -t nat -A PREROUTING -s 20.1.1.1 -m statistic --mode random --probability 0.8 -j DNAT --to-destination 40.1.1.1
nikhil_gateway@gateway:~$ sudo iptables -t nat -A PREROUTING -s 20.1.1.1 -j DNAT --to-destination 40.1.1.3
nikhil_gateway@gateway:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source          destination
DNAT      all  --  20.1.1.1    anywhere       anywhere        statistic mode random probability 0.79999999981 to:40.1.1.1
DNAT      all  --  20.1.1.1    anywhere       anywhere        to:40.1.1.3

Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source          destination
DNAT      all  --  20.1.1.1    anywhere       anywhere        statistic mode random probability 0.79999999981 to:40.1.1.1
DNAT      all  --  20.1.1.1    anywhere       anywhere        to:40.1.1.3

Chain INPUT (policy ACCEPT)
target     prot opt source          destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
Chain POSTROUTING (policy ACCEPT)
target     prot opt source          destination
SNAT      all  --  anywhere     40.1.1.2        to:40.1.1.2
SNAT      all  --  anywhere     40.1.1.3        to:40.1.1.2
nikhil_gateway@gateway:~$
```

Now, to test it, we established a series of TCP connections between the client and the gateway's client interface (20.1.1.2) and then sent some messages to the 20.1.1.2, but some of these client connections get connected to the server1 and some to server2, with the majority being connected to the server1 as shown in the below image:-

The image displays three terminal windows from Oracle VM VirtualBox, each showing a different host machine (client, server1, and server2) and their respective IP addresses (20.1.1.2, 20.1.1.1, and 20.1.1.2).

- client [Running] - Oracle VM VirtualBox:** Shows the client's perspective. It attempts to connect to port 5000 on 20.1.1.2 but receives errors for invalid ports (500043r4t, 500043r4t). It then connects successfully to port 5000 on 20.1.1.1.
- server1 [Running] - Oracle VM VirtualBox:** Shows server1's perspective. It receives multiple connection requests from the client on port 5000. It lists the connections as 3rtg, 3rt4fg, bvfds, 5t6uh, and 3r4t yik.
- server2 [Running] - Oracle VM VirtualBox:** Shows server2's perspective. It receives one connection request from the client on port 5000, listed as 3frvt and 3r4tg5rt.

```
client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_client@client:~$ nc -u 20.1.1.2 5000
r4t
^C
nikhil_client@client:~$ nc -u 20.1.1.2 5000
r4tgbhn)C
nikhil_client@client:~$ nc -u 20.1.1.2 5000
retfghuijmjkjutv'C
nikhil_client@client:~$ nc -u 20.1.1.2 500043r4t
nc: port number invalid: 500043r4t
nikhil_client@client:~$ nc -u 20.1.1.2 500043r4t
nc: port number invalid: 500043r4t
nikhil_client@client:~$ nc -u 20.1.1.2 5000
3r4fg
bvfds
^C
nikhil_client@client:~$ nc -u 20.1.1.2 5000
5t6yh
^C
nikhil_client@client:~$ nc -u 20.1.1.2 5000
3frvt
^C
nikhil_client@client:~$ nc -u 20.1.1.2 5000
3r4tg5rt
^C
nikhil_client@client:~$ nc -u 20.1.1.2 5000
3r4t yik
^C
nikhil_client@client:~$ _
```

```
server1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_server1@server1:~$ nc -ul -k -p 5000
3rtg
3rt4fg
bvfds
5t6uh
3r4t yik
```

```
server2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
nikhil_server2@server2:~$ nc -ul -k -p 5000
3frvt
3r4tg5rt
```