

# CSE 232: Programming Assignment 3

## Using Linux iptables

Due date: Oct 27, 2024

Total: 21 points

Ans 1

(a)

Set IPs for each VM as shown in the image:

- Client: 20.1.1.1/24 with default route to 20.1.1.2.
- Gateway VM: 20.1.1.2/24 on **enp0s8** (client side) and 40.1.1.2/24 on **enp0s9** (server side).
- Server 1: 40.1.1.1/24 with default route to 40.1.1.2.
- Server 2: 40.1.1.3/24 with default route to 40.1.1.2.

Network Interface with desired IP Address.

The image shows four terminal windows from Oracle VirtualBox, each displaying the output of the 'ip link' command to show network interface configurations:

- client [Running] - Oracle VirtualBox:** Shows interfaces enp0s3 (inet 10.0.2.15/24), enp0s8 (inet 20.1.1.1/24), and enp0s9 (inet 40.1.1.2/24).
- server1 [Running] - Oracle VirtualBox:** Shows interfaces enp0s3 (inet 10.0.2.15/24), enp0s8 (inet 20.1.1.2/24), and enp0s9 (inet 40.1.1.2/24).
- server2 [Running] - Oracle VirtualBox:** Shows interfaces enp0s3 (inet 10.0.2.15/24), enp0s8 (inet 40.1.1.1/24), and enp0s9 (inet 40.1.1.3/24).
- gateway [Running] - Oracle VirtualBox:** Shows interfaces enp0s8 (inet 20.1.1.2/24) and enp0s9 (inet 40.1.1.2/24).

Routes for All VMs.

```

client [Running] - Oracle VirtualBox
Oct 26 2012
File Machine View Input Devices Help
inet6 fe80::a00:27ff:fe0d:ad36/64 scope link
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:00:27:66:21:96 brd ff:ff:ff:ff:ff:ff
    inet 20.1.1.1/24 brd 20.1.1.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe66:2196/64 scope link
        valid_lft forever preferred_lft forever
client@client:~$ 

server1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:00:27:b6:f5:c9 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.1/24 brd 10.0.2.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb6:f5c9/64 scope link
        valid_lft forever preferred_lft forever
server1@server1:~$ ip route
default via 10.0.2.1 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
10.0.2.2 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
10.0.2.3 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
20.1.1.0/24 dev enp0s8 proto kernel scope link src 20.1.1.1
40.1.1.0/24 via 20.1.1.2 dev enp0s8 proto static
server1@server1:~$ 

client@client:~$ 

server2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:00:27:3c:85:a5 brd ff:ff:ff:ff:ff:ff
    inet 40.1.1.3/24 brd 40.1.1.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe3c:85a5/64 scope link
        valid_lft forever preferred_lft forever
server2@server2:~$ ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
10.0.2.2 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
10.0.2.3 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
20.1.1.1 via 40.1.1.2 dev enp0s8 proto static
40.1.1.0/24 dev enp0s8 proto kernel scope link src 40.1.1.3
server2@server2:~$ 

server1@server1:~$ 

gateway [Running] - Oracle VirtualBox
File Machine View Input Devices Help
inet6 fe80::a00:27ff:fe0d:ad36/64 scope link dynamic llngmpdui nroper lxi oute
    valid_lft 86143sec preferred_lft 14143sec
inet6 fe80::a00:27ff:feba:75c/64 scope link
    valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:00:27:63:3caf brd ff:ff:ff:ff:ff:ff
    inet 20.1.1.2/24 brd 20.1.1.255 scope global enp0s8
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fee3:3caf/64 scope link
            valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:00:27:f8:1cd1 brd ff:ff:ff:ff:ff:ff
    inet 40.1.1.2/24 brd 40.1.1.255 scope global enp0s9
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fef8:1cd1/64 scope link
            valid_lft forever preferred_lft forever
gateway@gateway:~$ 

client@client:~$ 

server1@server1:~$ 

server2@server2:~$ 

gateway@gateway:~$ 

```

(b)

### Stage 1: Attempt to Ping Server Before Enabling Forwarding

- In this stage, client cannot reach Server 1 before IP forwarding is configured on the gateway

```

client@client:~$ ping 40.1.1.1
PING 40.1.1.1 (40.1.1.1) 56(84) bytes of data.
^C
--- 40.1.1.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3059ms
client@client:~$ 

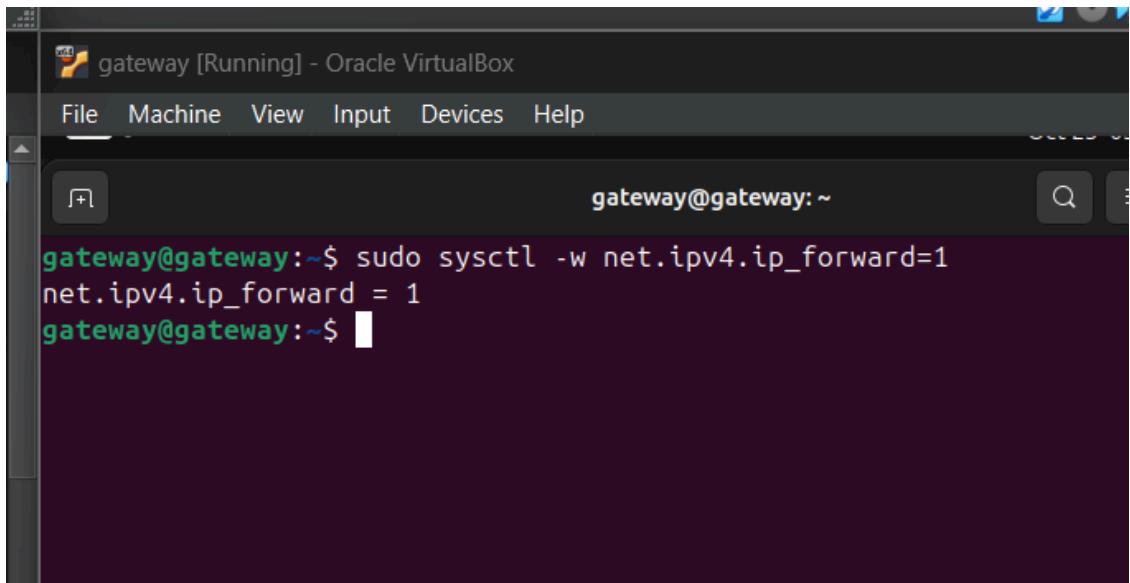
server1@server1:~$ 
server1@server1:~$ 

server2@server2:~$ 
server2@server2:~$ 

gateway@gateway:~$ 
gateway@gateway:~$ 

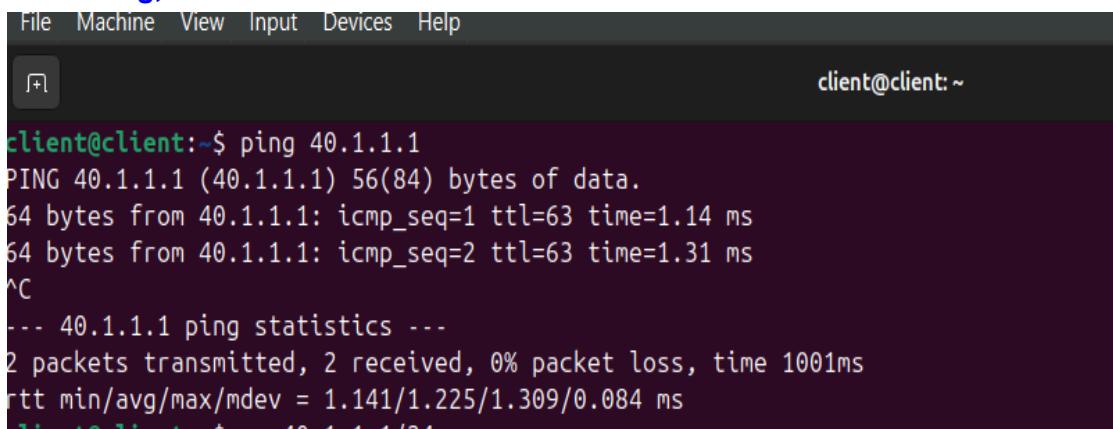
```

### Stage 2: Enable Forwarding and Successfully Ping Server



A screenshot of the Oracle VirtualBox interface showing a terminal window titled "gateway [Running] - Oracle VirtualBox". The window has a dark background and a light-colored command-line interface. The prompt "gateway@gateway: ~" is visible at the top right. Below it, the command "sudo sysctl -w net.ipv4.ip\_forward=1" is entered, followed by its output "net.ipv4.ip\_forward = 1". The command "gateway@gateway:~\$" is shown at the bottom.

- On the gateway, enable IP forwarding and configure iptables to allow traffic forwarding, as shown below:



A screenshot of the Oracle VirtualBox interface showing a terminal window titled "client@client: ~". The window has a dark background and a light-colored command-line interface. The prompt "client@client: ~" is visible at the top right. Below it, the command "ping 40.1.1.1" is entered, followed by its output showing two ICMP echo replies from the server at 40.1.1.1. The command "client@client:~\$" is shown at the bottom.

Ans 2

(a)

**(a) Block All Traffic Except Ping to Server (40.1.1.1/24)**

1. Set up iptables to allow only ICMP (ping) traffic and block everything else to the 40.1.1.0/24 network:

```

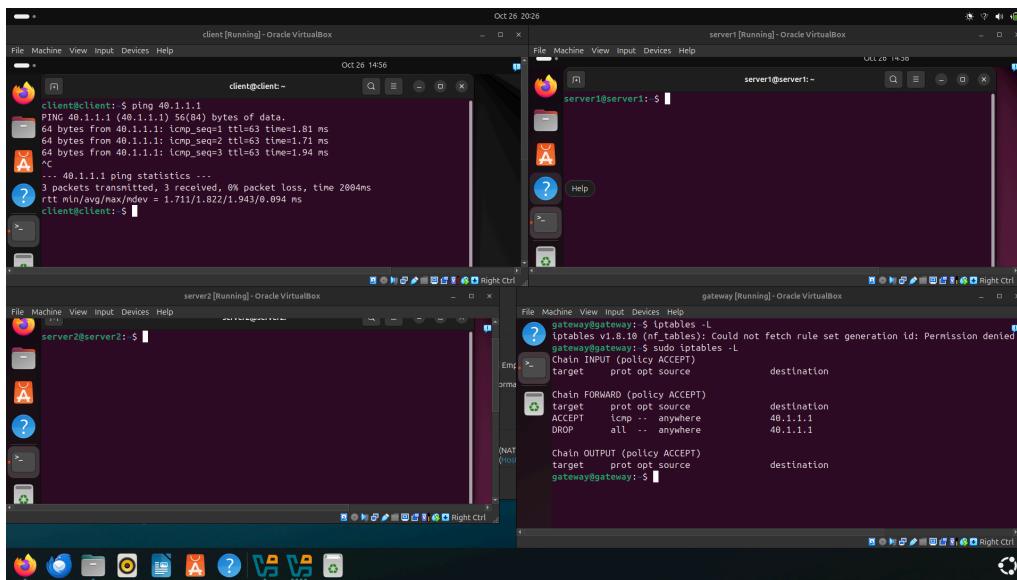
root@gateway: /home/gateway
gateway@gateway:/$ sudo iptables -A FORWARD -p icmp -d 40.1.1.1 -j ACCEPT
gateway@gateway:/$ sudo iptables -A FORWARD -d 40.1.1.1 -j DROP
gateway@gateway:/$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source          destination
              prot opt 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

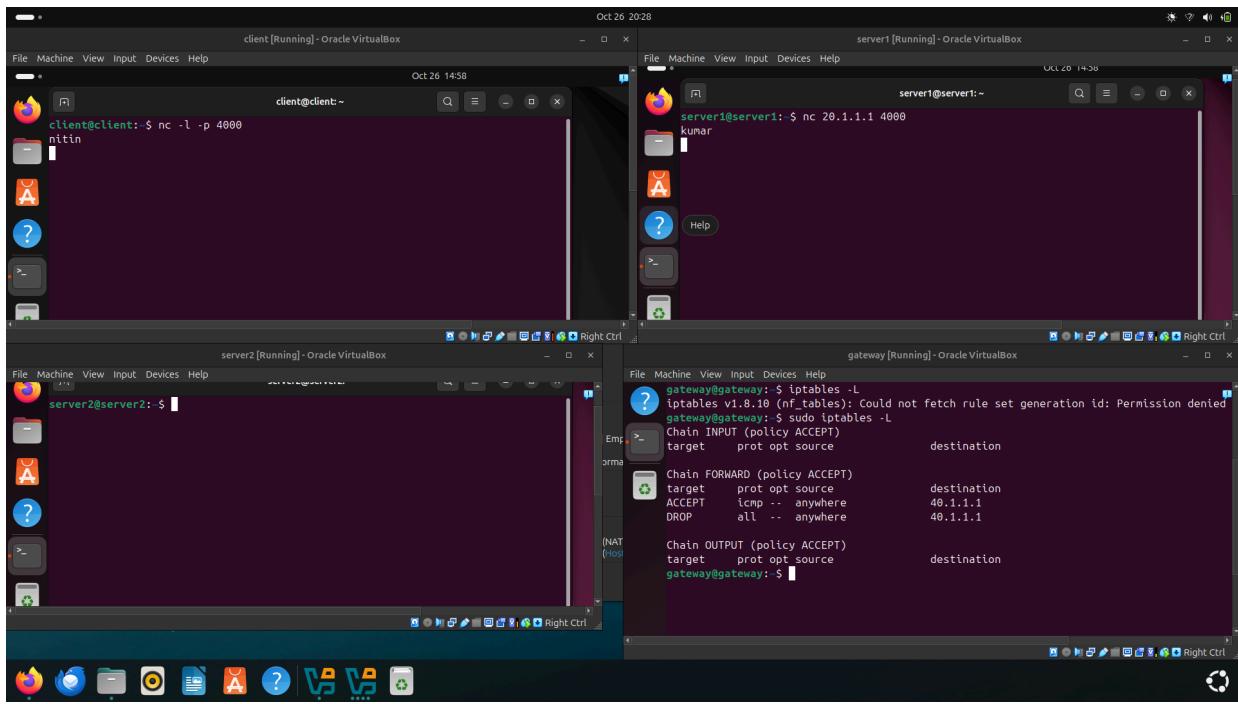
Chain OUTPUT (policy ACCEPT)
target      prot opt source          destination
gateway@gateway:/$ 

```

**PROOF 1:**  
**Showing ping working well in IMAGE GIVE BELOW:**



**PROOF 2:**  
**Showing dropping tcp packets in IMAGE GIVE BELOW:**



(b) Block Only TCP Traffic from 20.1.1.0/24

1. Set up iptables to block only TCP traffic originating from the 20.1.1.0/24 network:

```

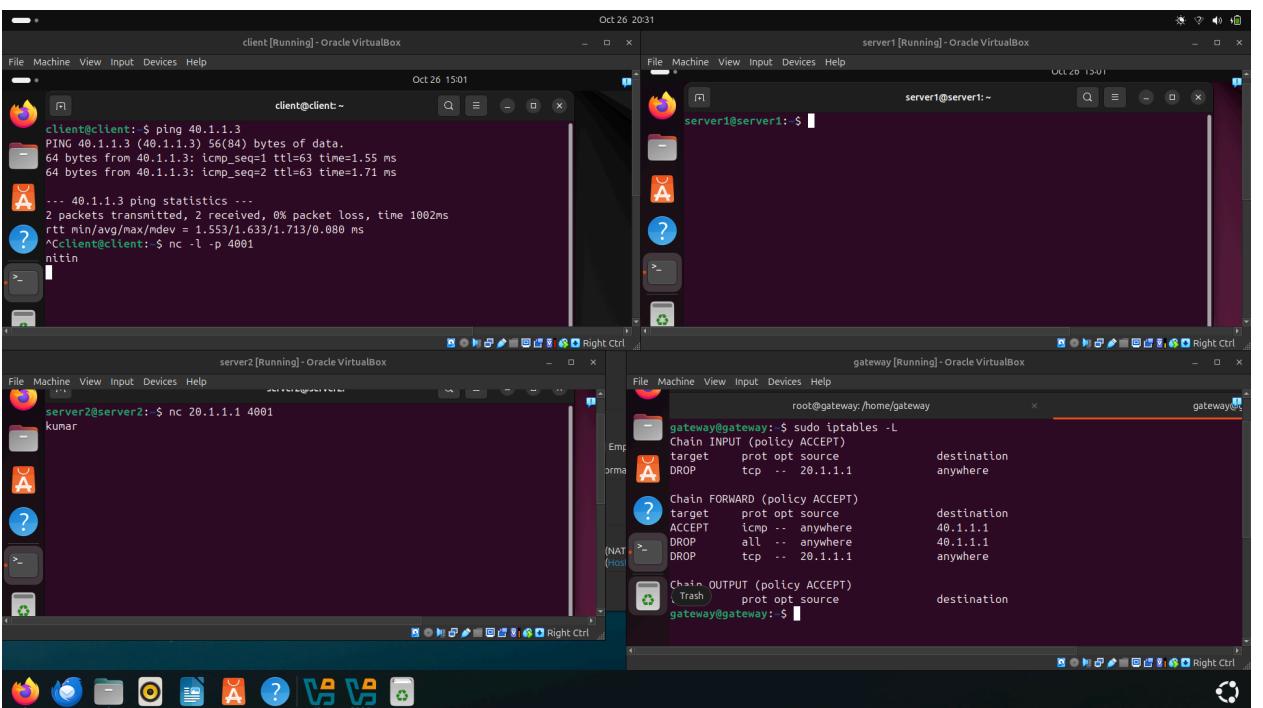
target      prot opt source          destination
gateway@gateway:/$ sudo iptables -A INPUT -p tcp -s 20.1.1.1 -j DROP
gateway@gateway:/$ sudo iptables -A FORWARD -p tcp -s 20.1.1.1 -j DROP
gateway@gateway:/$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target      prot opt source          destination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

Chain FORWARD (policy ACCEPT)
target      prot opt source          destination
ACCEPT    icmp  --  anywhere        40.1.1.1
DROP      all   --  anywhere        40.1.1.1
DROP      tcp   --  20.1.1.1
                                         anywhere

Chain OUTPUT (policy ACCEPT)
target      prot opt source          destination
gateway@gateway:/$

```

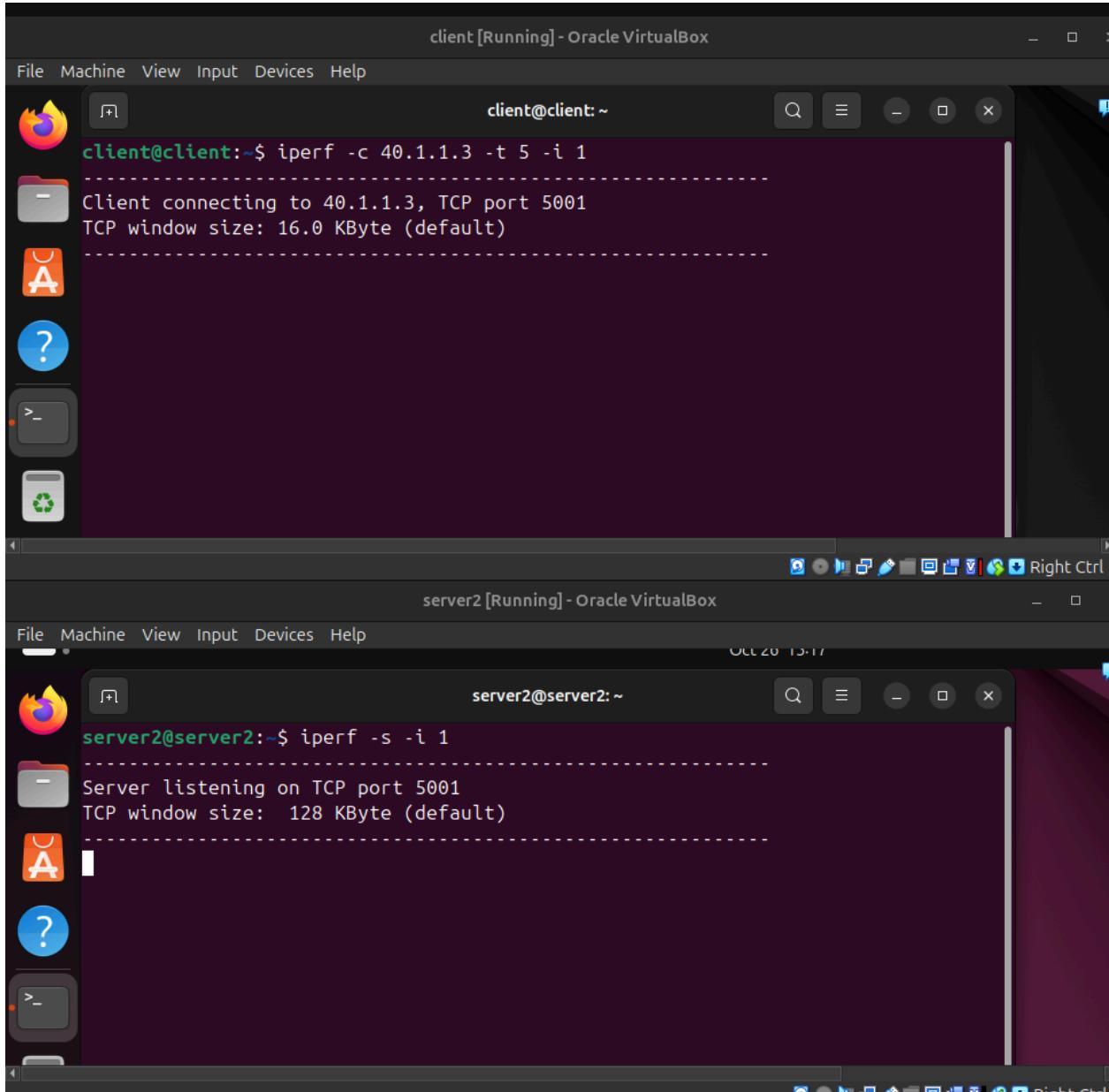
## Proof:



### Ans 3

(a) Using iperf tools to test the tcp and udp bandwidth between 20.1.1.1/24 and 40.1.1.3/24

because tcp packets from client machine is blocked therefore the connection not established



The image shows two Oracle VirtualBox windows side-by-side. The top window is titled "client [Running] - Oracle VirtualBox" and the bottom window is titled "server2 [Running] - Oracle VirtualBox". Both windows have a dark theme and show terminal sessions.

In the "client" window, the terminal command is:

```
client@client:~$ iperf -c 40.1.1.3 -t 5 -i 1
```

The output shows the client connecting to the server:

```
Client connecting to 40.1.1.3, TCP port 5001
TCP window size: 16.0 KByte (default)
```

In the "server2" window, the terminal command is:

```
server2@server2:~$ iperf -s -i 1
```

The output shows the server listening on port 5001:

```
Server listening on TCP port 5001
TCP window size: 128 KByte (default)
```

as there is no restriction on udp packets from client therefore connection is established

client@client:~\$ iperf -c 40.1.1.3 -u -t 30 -i 1

```
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 39367 connected with 40.1.1.3 port 5001
ID] Interval      Transfer     Bandwidth
  1] 0.0000-1.0000 sec   131 KBytes  1.07 Mbits/sec
  1] 1.0000-2.0000 sec   128 KBytes  1.05 Mbits/sec
  1] 2.0000-3.0000 sec   128 KBytes  1.05 Mbits/sec
  1] 3.0000-4.0000 sec   128 KBytes  1.05 Mbits/sec
  1] 4.0000-5.0000 sec   128 KBytes  1.05 Mbits/sec
  1] 5.0000-6.0000 sec   128 KBytes  1.05 Mbits/sec
  1] 6.0000-7.0000 sec   129 KBytes  1.06 Mbits/sec
  1] 7.0000-8.0000 sec   128 KBytes  1.05 Mbits/sec
```

server2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help Oct 25 15:43

srever2@srever2:~\$ iperf -s -u -i 1

```
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 39367
ID] Interval      Transfer     Bandwidth      Jitter    Lost/Total Datagrams
  1] 0.0000-1.0000 sec   131 KBytes  1.07 Mbits/sec  0.124 ms 0/91 (0%)
  1] 1.0000-2.0000 sec   128 KBytes  1.05 Mbits/sec  0.139 ms 0/89 (0%)
  1] 2.0000-3.0000 sec   128 KBytes  1.05 Mbits/sec  0.102 ms 0/89 (0%)
  1] 3.0000-4.0000 sec   128 KBytes  1.05 Mbits/sec  0.129 ms 0/89 (0%)
  1] 4.0000-5.0000 sec   128 KBytes  1.05 Mbits/sec  0.256 ms 0/89 (0%)
  1] 5.0000-6.0000 sec   128 KBytes  1.05 Mbits/sec  0.141 ms 0/89 (0%)
  1] 6.0000-7.0000 sec   129 KBytes  1.06 Mbits/sec  0.139 ms 0/90 (0%)
  1] 7.0000-8.0000 sec   128 KBytes  1.05 Mbits/sec  0.127 ms 0/89 (0%)
```

(b)

```
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=2.51 ms
64 bytes from 40.1.1.1: icmp_seq=2 ttl=63 time=1.74 ms
64 bytes from 40.1.1.1: icmp_seq=3 ttl=63 time=1.69 ms
64 bytes from 40.1.1.1: icmp_seq=4 ttl=63 time=1.81 ms
64 bytes from 40.1.1.1: icmp_seq=5 ttl=63 time=1.86 ms
64 bytes from 40.1.1.1: icmp_seq=6 ttl=63 time=1.55 ms
^C
--- 40.1.1.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.546/1.857/2.506/0.306 ms
[...]
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=1.31 ms
64 bytes from 40.1.1.3: icmp_seq=2 ttl=63 time=1.20 ms
64 bytes from 40.1.1.3: icmp_seq=3 ttl=63 time=1.20 ms
64 bytes from 40.1.1.3: icmp_seq=4 ttl=63 time=1.03 ms
64 bytes from 40.1.1.3: icmp_seq=5 ttl=63 time=1.67 ms
^C
--- 40.1.1.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.030/1.281/1.668/0.212 ms
client@client:~$
```

There is a clear difference between rtt in 40.1.1.1 and 40.1.1.3 because on the gateway there are processings going on for the 40.1.1.1 destination packets. Hence rtt for 40.1.1.3 is lower than 40.1.1.1.

#### Q.4. Network address translation at the gateway VM [4]

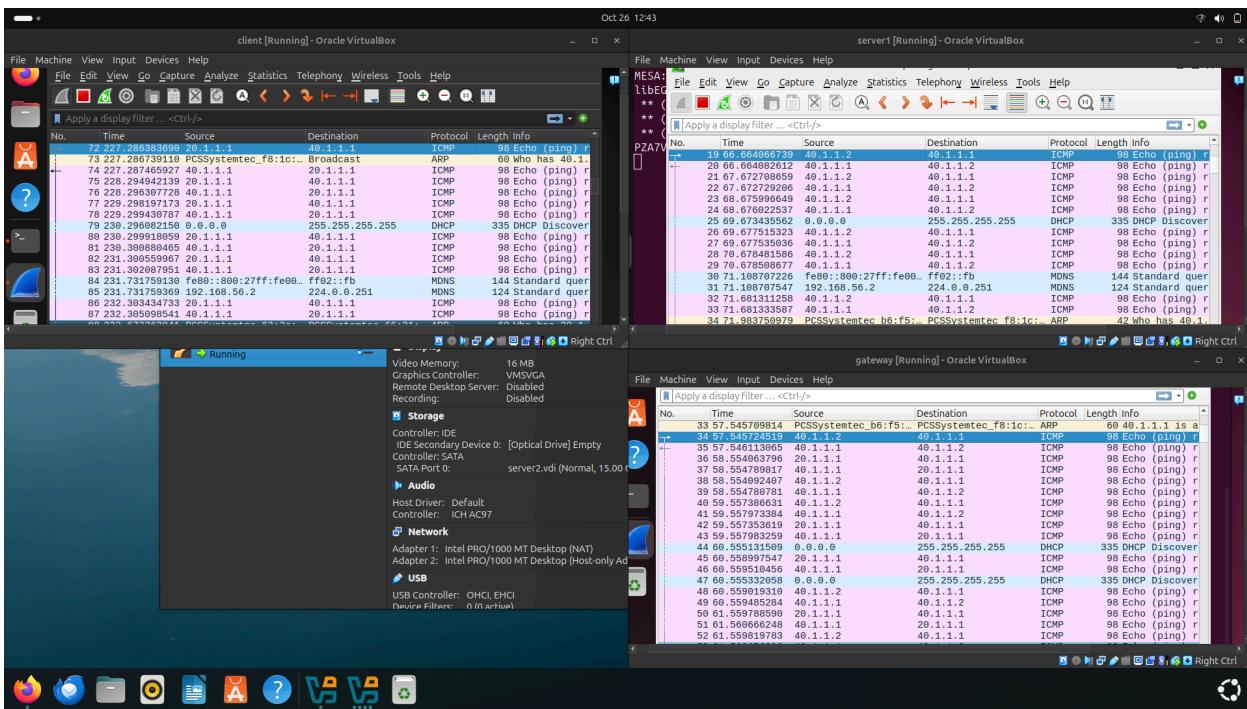
(a) & (b) adding the DNAT and SNAT rules in iptables rules.

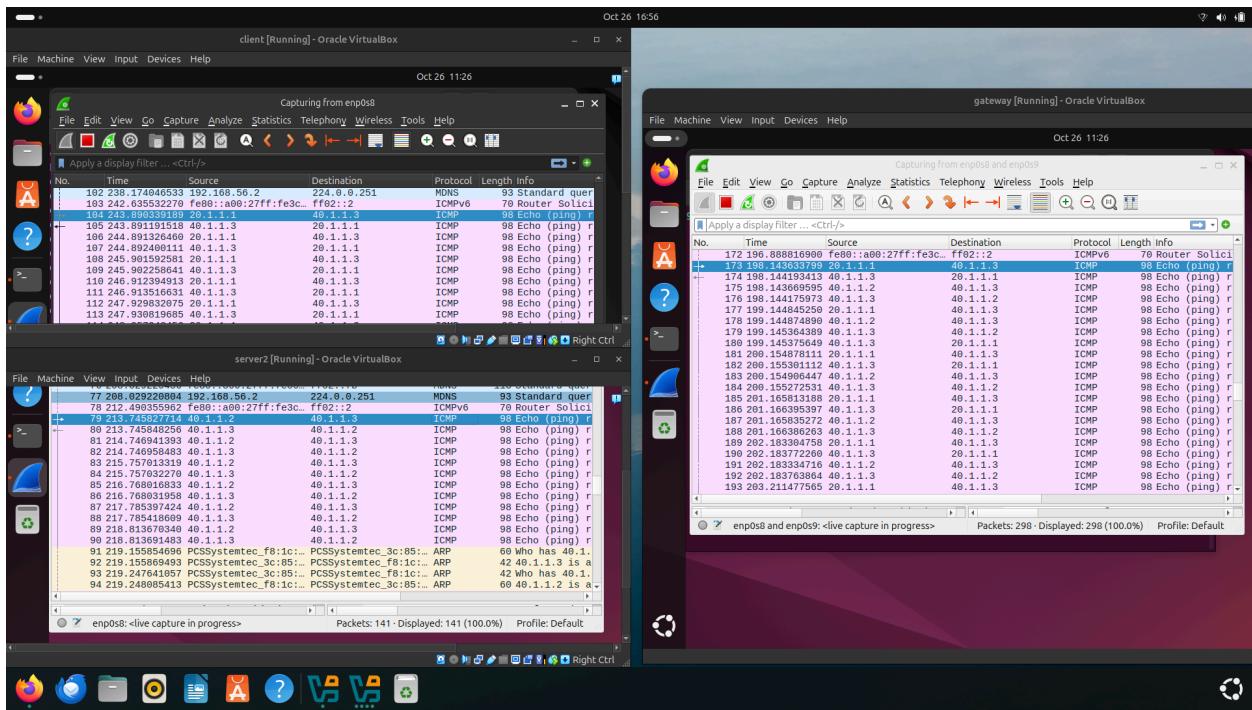
```

GNU nano 7.2                               iptablesrules.v4
:INPUT ACCEPT [666:130938]
:FORWARD ACCEPT [231:19086]
:OUTPUT ACCEPT [162:14595]
-A INPUT -s 20.1.1.1/32 -p tcp -j DROP
-A FORWARD -d 40.1.1.1/32 -p icmp -j ACCEPT
-A FORWARD -d 40.1.1.1/32 -j DROP
-A FORWARD -s 20.1.1.1/32 -p tcp -j DROP
COMMIT
# Completed on Sat Oct 26 14:47:45 2024
# Generated by iptables-save v1.8.10 (nf_tables) on Sat Oct 26 14:47:45 2024
*nat
:PREROUTING ACCEPT [38:3768]
:INPUT ACCEPT [37:3695]
:OUTPUT ACCEPT [75:5648]
:POSTROUTING ACCEPT [74:5575]
-A PREROUTING -d 40.1.1.0/24 -j DNAT --to-destination 20.1.1.1
#-A PREROUTING -d 20.1.1.2/32 -j DNAT --to-destination 40.1.1.3
#-A PREROUTING -d 20.1.1.2/32 -m statistic --mode random --probability 0.79999999
-A POSTROUTING -s 20.1.1.0/24 -j SNAT --to-source 40.1.1.2
COMMIT

```

(c)





## Q.5. Load balancing at the gateway VM. Attach screenshots [4]

**Ans**

```
root@gateway:/home/gateway# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DNAT      all  --  anywhere       40.1.0/24      to:20.1.1.1
DNAT      all  --  anywhere       gateway        to:40.1.1.3
DNAT      all  --  anywhere       gateway        statistic mode random probability 0.79999999981 to:40.1.1.1
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  --  20.1.1.0/24   anywhere        to:40.1.1.2
root@gateway:/home/gateway#
```

(a)

