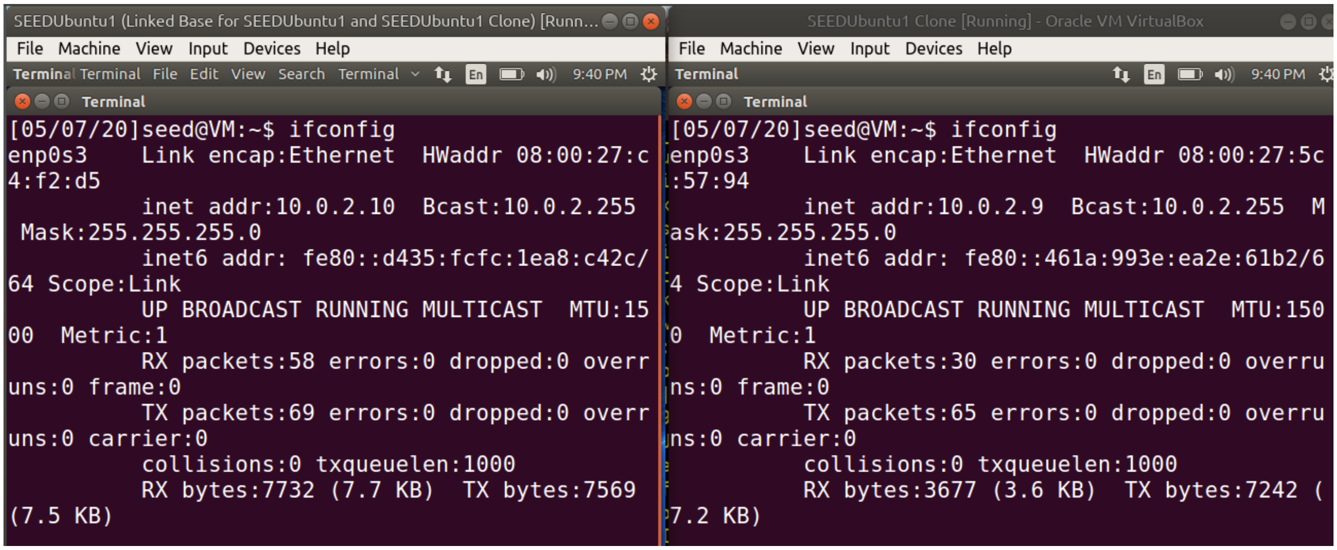
Lab18
Firewall Evasion Lab: Bypassing Firewalls using VPN
Varun Gunda

2.1 Task 1: VM Setup

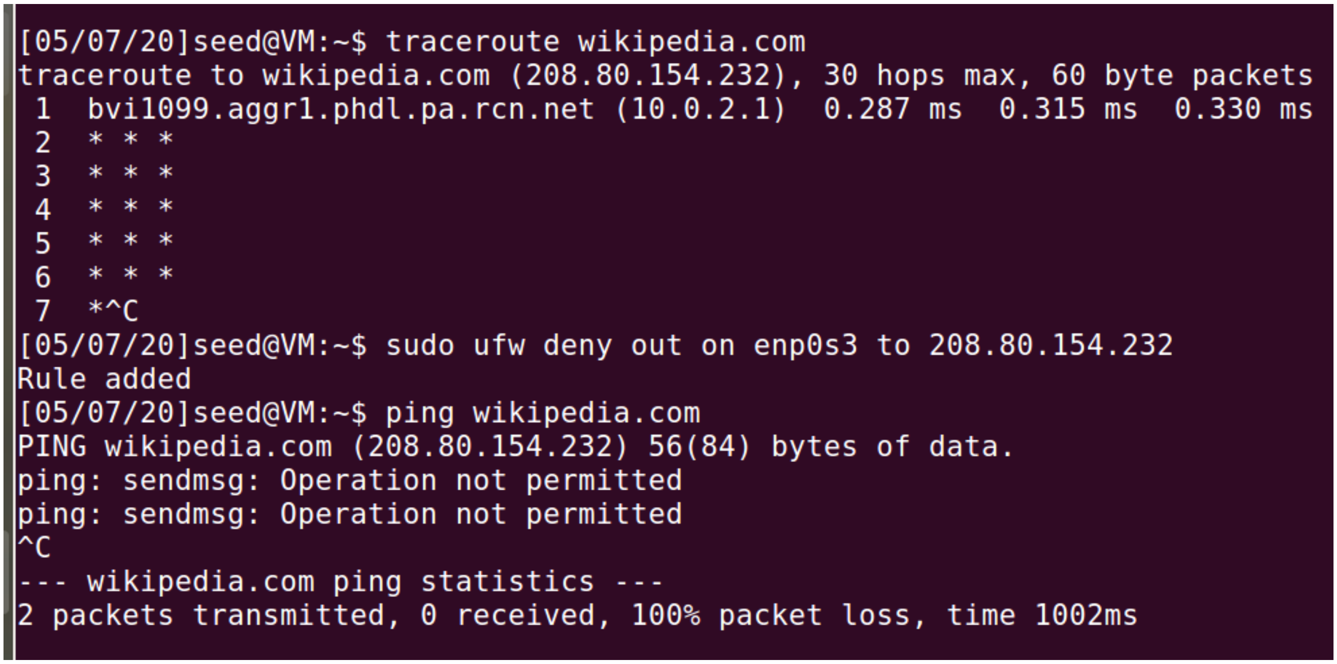
As seen below two vms 10.0.2.9(VM B) and 10.0.2.10(VM A) are connected to LAN using NAT Network adapter


SEEDUbuntu1 (Linked Base for SEEDUbuntu1 and SEEDUbuntu1 Clone) [Runn...
File Machine View Input Devices Help
Terminal Terminal File Edit View Search Terminal
En 9:40 PM
Terminal
SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En 9:40 PM
Terminal

```
[05/07/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:c
4:f2:d5
          inet addr:10.0.2.10  Bcast:10.0.2.255
 Mask:255.255.255.0
          inet6 addr: fe80::d435:fcfc:1ea8:c42c/
64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:15
00  Metric:1
          RX packets:58 errors:0 dropped:0 overr
uns:0 frame:0
          TX packets:69 errors:0 dropped:0 overr
uns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7732 (7.7 KB)  TX bytes:7569
(7.5 KB)
```

```
[05/07/20]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5c
:57:94
          inet addr:10.0.2.9  Bcast:10.0.2.255  M
ask:255.255.255.0
          inet6 addr: fe80::461a:993e:ea2e:61b2/6
4 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:150
0  Metric:1
          RX packets:30 errors:0 dropped:0 overru
ns:0 frame:0
          TX packets:65 errors:0 dropped:0 overru
ns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3677 (3.6 KB)  TX bytes:7242 (
7.2 KB)
```

2.2 Task 2: Set up Firewall

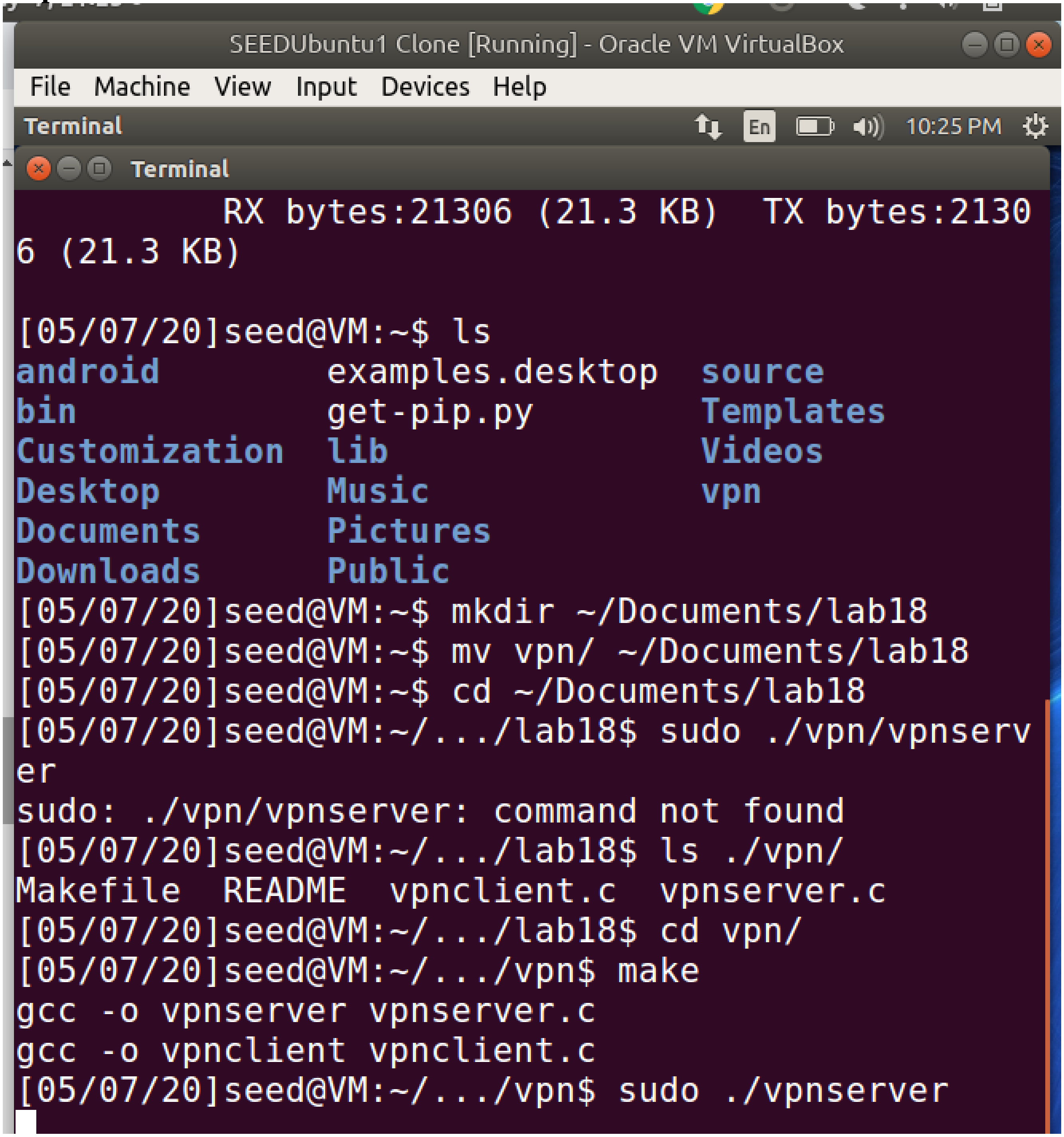


```
[05/07/20]seed@VM:~$ traceroute wikipedia.com
traceroute to wikipedia.com (208.80.154.232), 30 hops max, 60 byte packets
 1  bvi1099.aggr1.phdl.pa.rcn.net (10.0.2.1)  0.287 ms  0.315 ms  0.330 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *^C
[05/07/20]seed@VM:~$ sudo ufw deny out on enp0s3 to 208.80.154.232
Rule added
[05/07/20]seed@VM:~$ ping wikipedia.com
PING wikipedia.com (208.80.154.232) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- wikipedia.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1002ms
```

As seen in the image above, chose wikipedia.com website to block on VM A. Once we add the rule, the ip address 208.80.154.232 is no longer reachable.

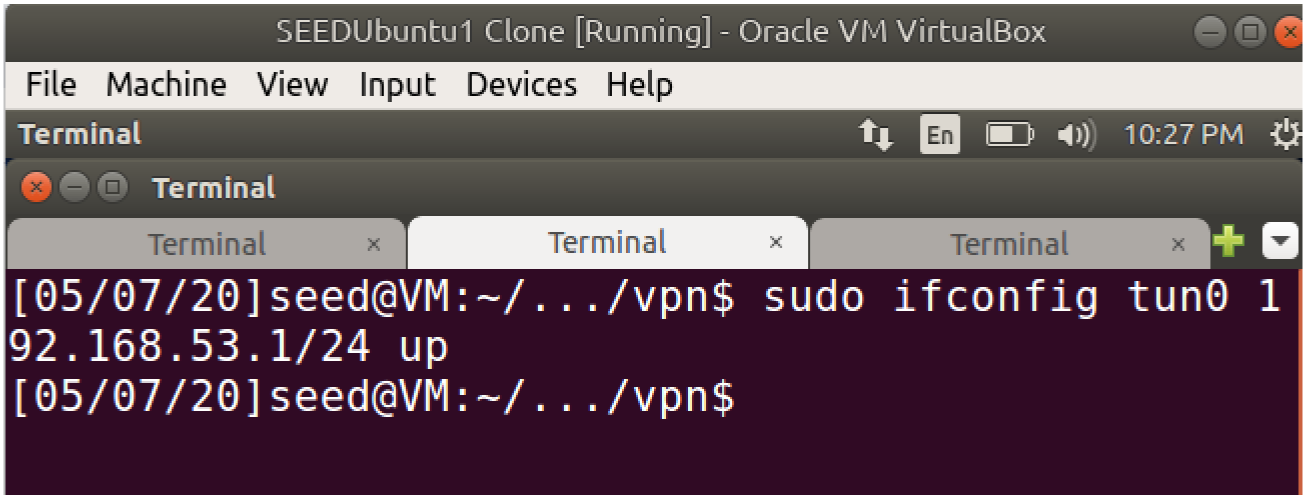
2.3 Task 3: Bypassing Firewall using VPN:

Step 1: Run VPN Server


SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
10:25 PM
Terminal

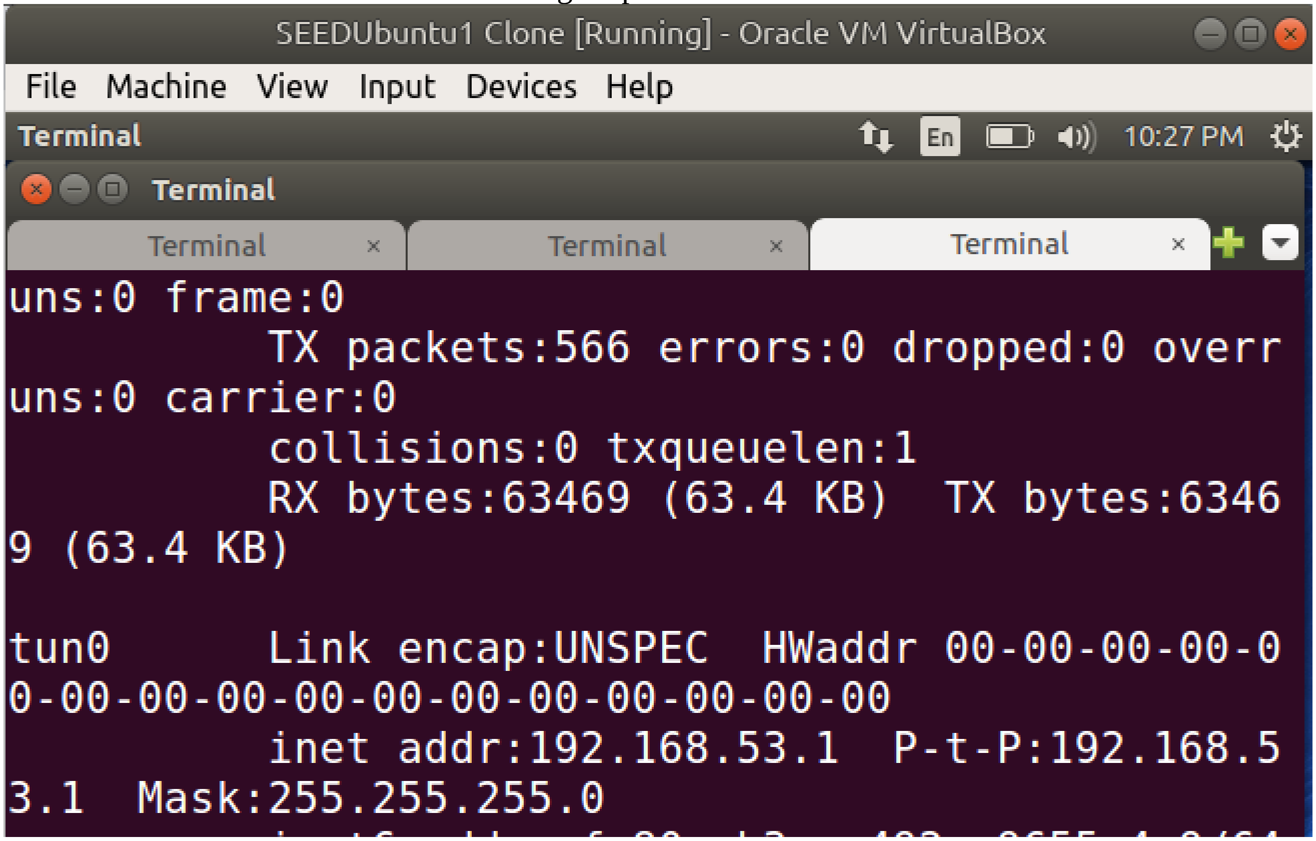
```
          RX bytes:21306 (21.3 KB)  TX bytes:21306 (21.3 KB)

[05/07/20]seed@VM:~$ ls
android          examples.desktop  source
bin              get-pip.py        Templates
Customization    lib               Videos
Desktop          Music             vpn
Documents        Pictures
Downloads        Public
[05/07/20]seed@VM:~$ mkdir ~/Documents/lab18
[05/07/20]seed@VM:~$ mv vpn/ ~/Documents/lab18
[05/07/20]seed@VM:~$ cd ~/Documents/lab18
[05/07/20]seed@VM:~/.../lab18$ sudo ./vpn/vpnserver
sudo: ./vpn/vpnserver: command not found
[05/07/20]seed@VM:~/.../lab18$ ls ./vpn/
Makefile  README  vpnclient.c  vpnserver.c
[05/07/20]seed@VM:~/.../lab18$ cd vpn/
[05/07/20]seed@VM:~/.../vpn$ make
gcc -o vpnserver vpnserver.c
gcc -o vpnclient vpnclient.c
[05/07/20]seed@VM:~/.../vpn$ sudo ./vpnserver
```

Compiling vpnserver and running it on VM B as seen above
Assigning an IP address to the tun0 interface and activating it as seen below


SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
10:27 PM
Terminal
Terminal
Terminal
Terminal

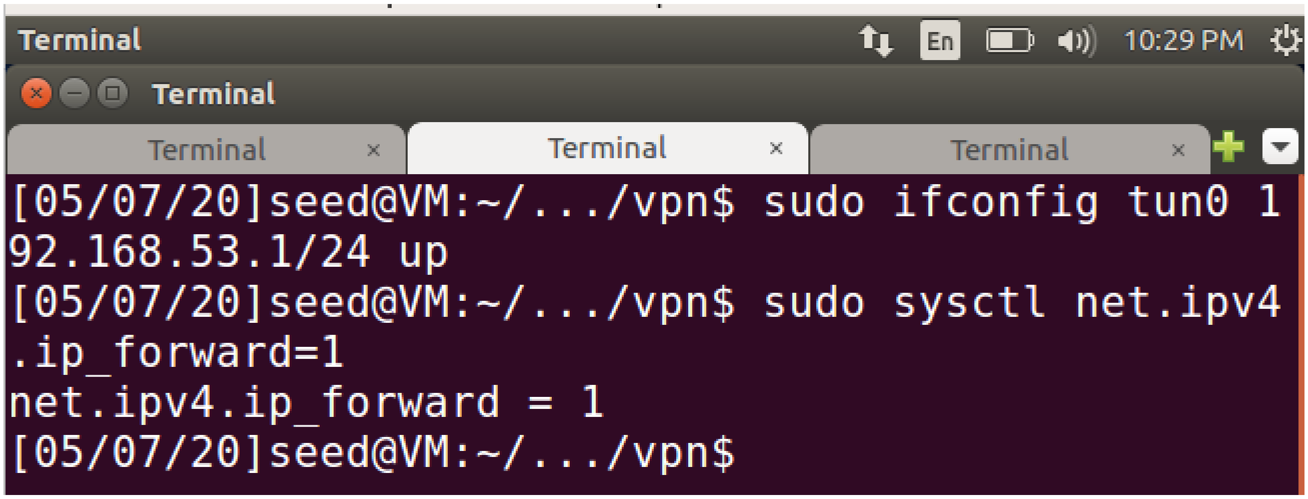
```
[05/07/20]seed@VM:~/.../vpn$ sudo ifconfig tun0 1
92.168.53.1/24 up
[05/07/20]seed@VM:~/.../vpn$
```

We can see tun0 interface in VM B’s ifconfig output:


SEEDUbuntu1 Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
10:27 PM
Terminal
Terminal
Terminal
Terminal

```
uns:0 frame:0
          TX packets:566 errors:0 dropped:0 overr
uns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:63469 (63.4 KB)  TX bytes:6346
9 (63.4 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-0
0-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.53.1  P-t-P:192.168.5
3.1  Mask:255.255.255.0
```

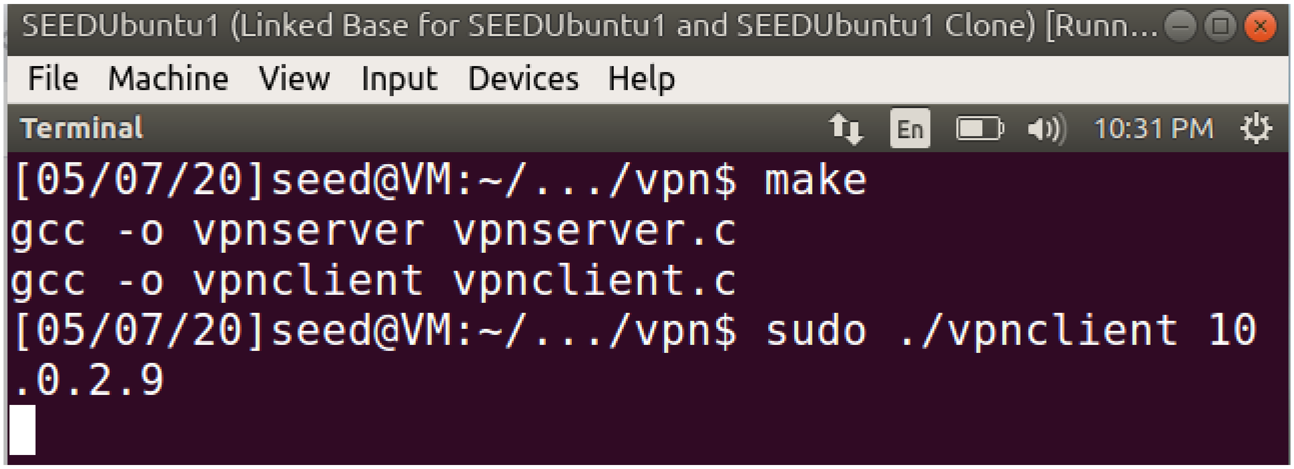
Enabling IP Forwarding as seen below:



```
[05/07/20]seed@VM:~/.../vpn$ sudo ifconfig tun0 1
92.168.53.1/24 up
[05/07/20]seed@VM:~/.../vpn$ sudo sysctl net.ipv4
.ip_forward=1
net.ipv4.ip_forward = 1
[05/07/20]seed@VM:~/.../vpn$
```

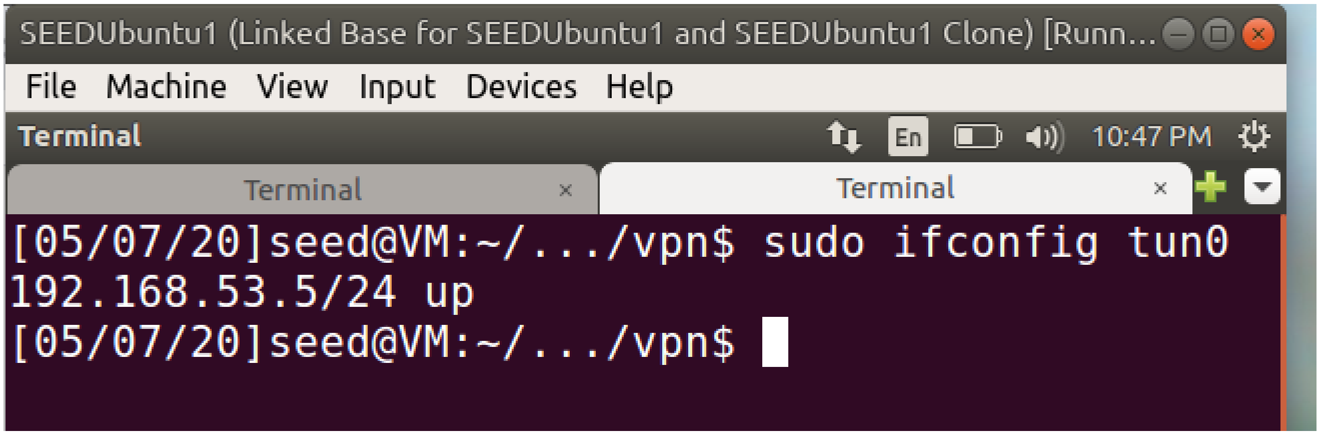
Step 2: Run VPN Client.

Compiling and running vpnclient program on VM A and connecting it to VPN server running on VM B as seen below:


SEEDUbuntu1 (Linked Base for SEEDUbuntu1 and SEEDUbuntu1 Clone) [Runn...
File
Machine
View
Input
Devices
Help
Terminal
10:31 PM

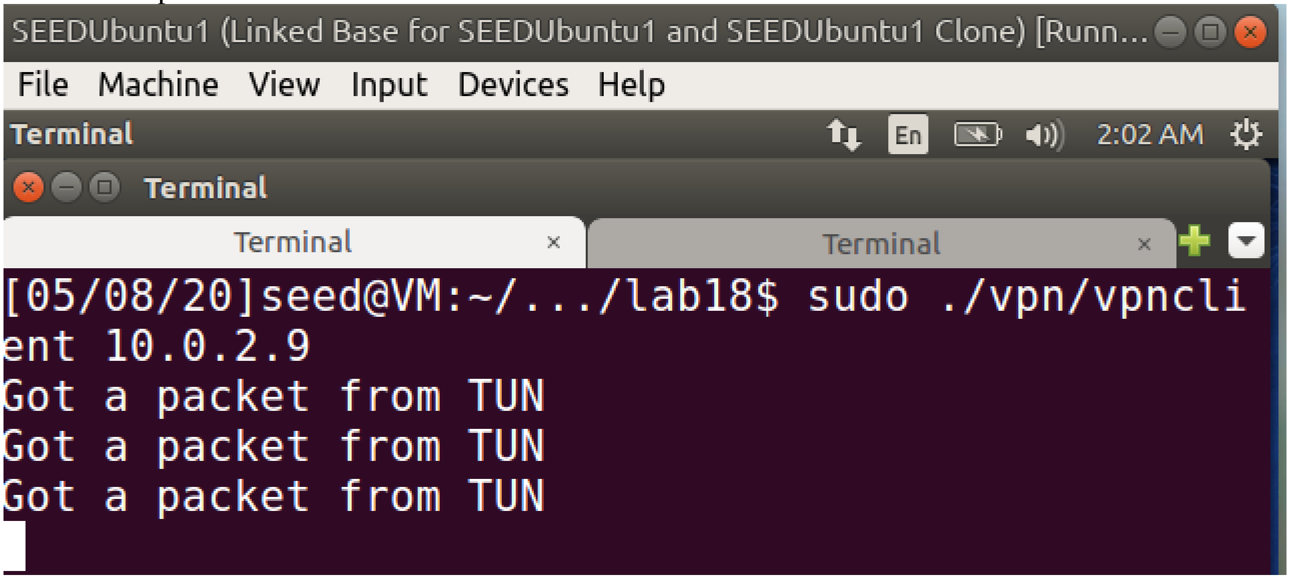
```
[05/07/20]seed@VM:~/.../vpn$ make
gcc -o vpnserver vpnserver.c
gcc -o vpnclient vpnclient.c
[05/07/20]seed@VM:~/.../vpn$ sudo ./vpnclient 10
.0.2.9
```

Configuring tun0 intergace on VPN client as seen below:


SEEDUbuntu1 (Linked Base for SEEDUbuntu1 and SEEDUbuntu1 Clone) [Runn...
File
Machine
View
Input
Devices
Help
Terminal
10:47 PM
Terminal
Terminal

```
[05/07/20]seed@VM:~/.../vpn$ sudo ifconfig tun0
192.168.53.5/24 up
[05/07/20]seed@VM:~/.../vpn$
```

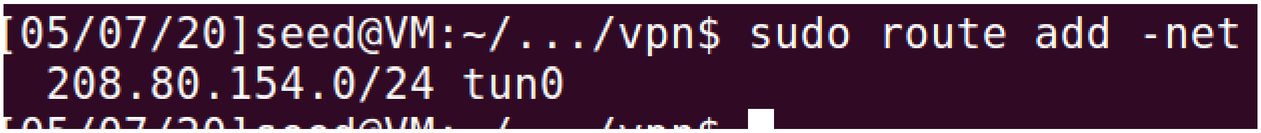
The above steps established a VPN tunnel as seen below:


SEEDUbuntu1 (Linked Base for SEEDUbuntu1 and SEEDUbuntu1 Clone) [Runn...
File
Machine
View
Input
Devices
Help
Terminal
En
2:02 AM
Terminal
Terminal
Terminal

```
[05/08/20]seed@VM:~/.../lab18$ sudo ./vpn/vpncli
ent 10.0.2.9
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
```

Step 3: Set Up Routing on Client and Server Vms.

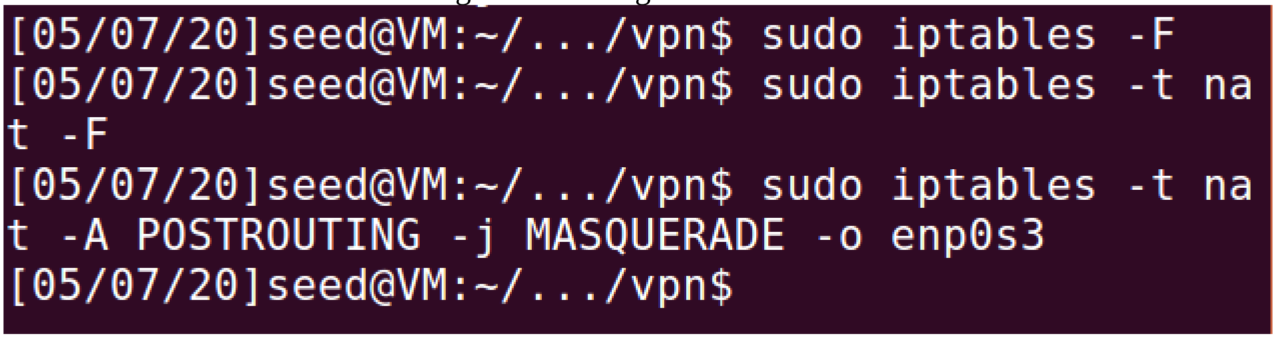
Added folowing command on both client and server vms to direct traffic related to wikipedia.com to tun0 interface.



```
[05/07/20]seed@VM:~/.../vpn$ sudo route add -net
 208.80.154.0/24 tun0
[05/07/20]seed@VM:~/.../vpn$
```

Step 4: Set Up NAT on Server VM

Executed NAT on the server VM using the following commands:



```
[05/07/20]seed@VM:~/.../vpn$ sudo iptables -F
[05/07/20]seed@VM:~/.../vpn$ sudo iptables -t na
t -F
[05/07/20]seed@VM:~/.../vpn$ sudo iptables -t na
t -A POSTROUTING -j MASQUERADE -o enp0s3
[05/07/20]seed@VM:~/.../vpn$
```

Now, although I am able to see in wireshark that the packets are sent from vpn client to vpn server through tun0 interface (I couldn’t attach the image as vm crashed), there are no packets sent by server to client. I tried to debug this but couldn’t find the solution.