

Name: Adarsh Kumar

SRN No: PES2UG20CS016

Assignment No: Optional

Section: B

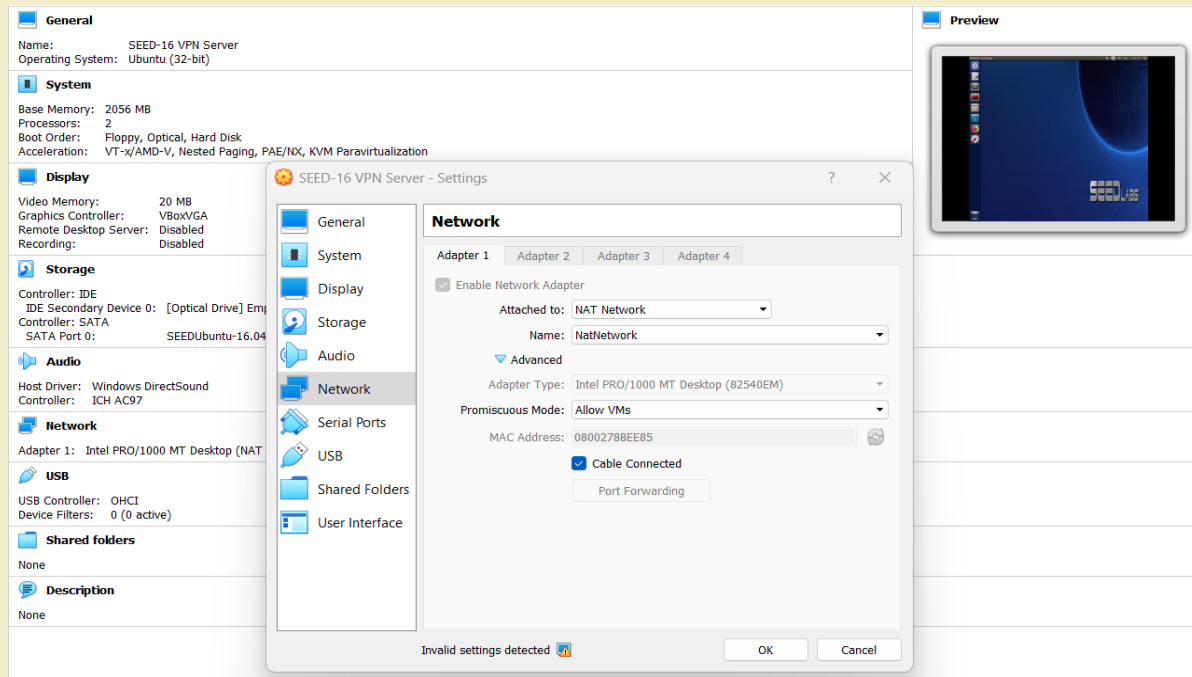
Date: 8/11/2022

Task 1:

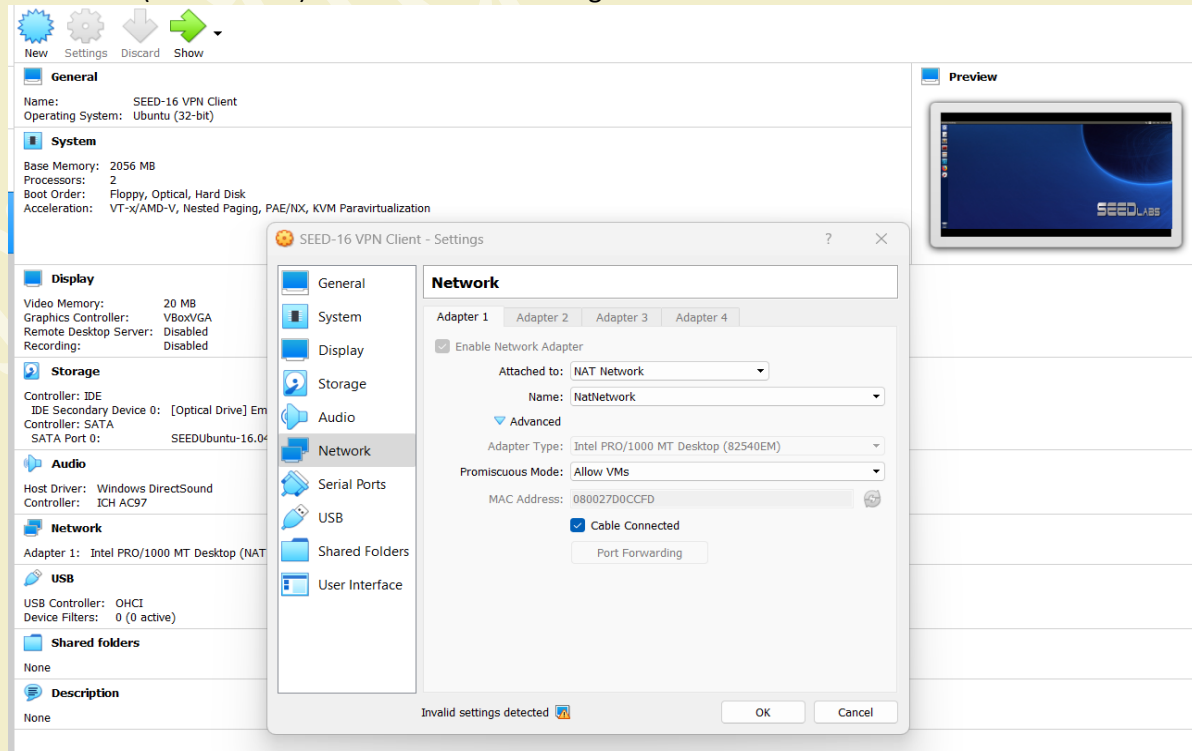
VM Setup

Screenshots of basics setups.

Both the VMs need to have the "NAT Network" Adapter enabled on them:
VPN Server (IP: 10.0.2.6) machine network configuration



VPN Client (IP: 10.0.2.15) machine network configuration



We have configured both VM at NAT network settings.

Task 2:	Set up Firewall									
Screenshot	<p>I have identified 'www.wikipedia.org' as a website to be blocked on the client machine. The client machine is inside the firewall.</p> <p>The website is able to be pinged from the client machine initially:</p> <pre>Client/AdarshKumar/PES2UG20CS016/>>\$ping www.wikipedia.org PING dyna.wikimedia.org (103.102.166.224) 56(84) bytes of data. 64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=1 ttl=50 time=41.6 ms 64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=2 ttl=50 time=42.6 ms 64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=3 ttl=50 time=44.5 ms 64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=4 ttl=50 time=44.4 ms 64 bytes from text-lb.eqsin.wikimedia.org (103.102.166.224): icmp_seq=5 ttl=50 time=43.7 ms ^C --- dyna.wikimedia.org ping statistics --- 5 packets transmitted, 5 received, 0% packet loss, time 4008ms rtt min/avg/max/mdev = 41.666/43.410/44.556/1.125 ms</pre> <p>Therefore, we can see that Wikipedia.org has a fixed IP address: 103.102.166.224</p> <p>Now, we will set up a firewall to block this website from being accessed</p> <pre>rtt min/avg/max/mdev = 41.666/43.410/44.556/1.125 ms Client/AdarshKumar/PES2UG20CS016/>>\$sudo ufw enable Firewall is active and enabled on system startup Client/AdarshKumar/PES2UG20CS016/>>\$sudo ufw deny out on enp0s3 to 103.102.166.224 Rule added Client/AdarshKumar/PES2UG20CS016/>>\$sudo ufw status Status: active</pre> <table><tr><th>To</th><th>Action</th><th>From</th></tr><tr><td>--</td><td>----</td><td>----</td></tr><tr><td>103.102.166.224</td><td>DENY OUT</td><td>Anywhere on enp0s3</td></tr></table> <p>Now we can see that www.wikipedia.org is blocked. The rule is added into our firewall table.</p> <pre>Client/AdarshKumar/PES2UG20CS016/>>\$ping www.wikipedia.org PING dyna.wikimedia.org (103.102.166.224) 56(84) bytes of data. ping: sendmsg: Operation not permitted ping: sendmsg: Operation not permitted ping: sendmsg: Operation not permitted ping: sendmsg: Operation not permitted ping: sendmsg: Operation not permitted ^C --- dyna.wikimedia.org ping statistics --- 5 packets transmitted, 0 received, 100% packet loss, time 4080ms</pre> <p>Client/AdarshKumar/PES2UG20CS016/>>\$</p> <p>Now it can be observed that we are not able to ping to www.wikipedia.org website. It is because we blocked the request message which was going outside to (103.102.166.224) from client machine.</p>	To	Action	From	--	----	----	103.102.166.224	DENY OUT	Anywhere on enp0s3
To	Action	From								
--	----	----								
103.102.166.224	DENY OUT	Anywhere on enp0s3								
Task 3:	Bypassing Firewall using VP									
Step 1:	<p>Run VPN Server:</p> <pre>Server/AdarshKumar/PES2UG20C016/>>\$ifconfig -a enp0s3 Link encap:Ethernet HWaddr 08:00:27:8b:ee:85 inet addr:10.0.2.7 Bcast:10.0.2.255 Mask:255.255.255.0 inet6 addr: fe80::297e:9f1a:5de:c230/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:13240 errors:0 dropped:0 overruns:0 frame:0 TX packets:4884 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:17055159 (17.0 MB) TX bytes:673043 (673.0 KB) lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:1427 errors:0 dropped:0 overruns:0 frame:0 TX packets:1427 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1 RX bytes:163249 (163.2 KB) TX bytes:163249 (163.2 KB) Server/AdarshKumar/PES2UG20C016/>>\$</pre> <p>Initially only two interfaces were present. There is no mention of tun0 interface, so it is inactive.</p>									

VPN server code run on the server to establish the tunnel.

```
VPN Server/AdarshKumar/PES2UG20CS016/>$gcc -o vpn_server vpnserver.c
VPN Server/AdarshKumar/PES2UG20CS016/>$sudo ./vpn_server
```

Now we are assigning an IP address to the tun0 interface and activate it. IP Address assigned: 192.168.53.1/25

Upon checking ifconfig -a: we have an established tunnel

```
Server/AdarshKumar/PES2UG20CS016/>$sudo ifconfig tun0 192.168.53.1/24 up
Server/AdarshKumar/PES2UG20CS016/>$ifconfig -a
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:8b:ee:85
            inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::297e:9f1a:5de:c230/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:7169 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4771 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:7316095 (7.3 MB)  TX bytes:657276 (657.2 KB)

lo          Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:1298 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1298 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:151343 (151.3 KB)  TX bytes:151343 (151.3 KB)

tun0        Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
            inet addr:192.168.53.1  P-t-P:192.168.53.1  Mask:255.255.255.0
            inet6 addr: fe80::27d8:88f3:a4f3:35b0/64 Scope:Link
            UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:500
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

```
Server/AdarshKumar/PES2UG20CS016/>$
```

Here we can see that Tun0 interface got the IP address of 192.168.53.1

Now the VPN Server needs to forward packets to other destinations, so it needs to function as a gateway. We need to enable the IP forwarding for a computer to behave like a gateway.

```
Server/AdarshKumar/PES2UG20CS016/>$sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
Server/AdarshKumar/PES2UG20CS016/>$
```

Step 2:

Run VPN Client:

```
Client/AdarshKumar/PES2UG20CS016/>$ifconfig -a
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:d0:cc:fd
        inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::f9f4:e76c:bcfa:2c29/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:17553 errors:0 dropped:0 overruns:0 frame:0
        TX packets:4882 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:23219017 (23.2 MB)  TX bytes:678220 (678.2 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:2017 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2017 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:242112 (242.1 KB)  TX bytes:242112 (242.1 KB)

Client/AdarshKumar/PES2UG20CS016/>$
```

On the client machine we are checking that we got only 2 interface there is no tun0 interface now.

VPN client code run on the client to establish the tunnel.

```
Client/AdarshKumar/PES2UG20CS016/>$gcc -o vpn_client vpnclient.c
Client/AdarshKumar/PES2UG20CS016/>$sudo ./vpn_client 10.0.2.8
```

Now we are assigning an IP address to the tun0 interface and activate it. IP Address assigned: 192.168.53.1/25 Upon checking ifconfig -a: we have an established tunnel:

```
Client/AdarshKumar/PES2UG20CS016/>$sudo ifconfig tun0 192.168.53.5/24 up
Client/AdarshKumar/PES2UG20CS016/>$ifconfig -a
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:d0:cc:fd
        inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::f9f4:e76c:bcfa:2c29/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:17561 errors:0 dropped:0 overruns:0 frame:0
        TX packets:4891 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:23220717 (23.2 MB)  TX bytes:679339 (679.3 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:2089 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2089 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:247469 (247.4 KB)  TX bytes:247469 (247.4 KB)

tun0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
        inet addr:192.168.53.5  P-t-P:192.168.53.5  Mask:255.255.255.0
        inet6 addr: fe80::b419:ecbb:87bc:cecf/64 Scope:Link
        UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:500
        RX bytes:0 (0.0 B)  TX bytes:144 (144.0 B)

Client/AdarshKumar/PES2UG20CS016/>$
```

We can see that tun0 interface got IP address of 192.168.53.5

Step 3:

Set Up Routing on Client and Server VMs:

We can now see that the tunnel is established because of the messages displayed like 'Connected with client: Hello'

Server

```

VPNserver:~$ sudo ./
vpnserv 10.0.2.8
Connected with the client: Hello
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from the tunnel

```

Client

```

Client/AdarshKumar/PES2UG20CS016/>$gcc -o vpn_client vpnclient.c
Client/AdarshKumar/PES2UG20CS016/>$sudo ./vpn_client 10.0.2.8
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN

```

We need to set up routing paths on both client and server machines to direct the intended traffic through the tunnel. This is done on the client machine as follows:

```

Client/AdarshKumar/PES2UG20CS016/>$sudo route add -net 103.102.166.0/24 tun0
Client/AdarshKumar/PES2UG20CS016/>$route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.0.2.1       0.0.0.0         UG    100    0      0 enp0s3
10.0.2.0         0.0.0.0        255.255.255.0   U     100    0      0 enp0s3
103.102.166.0    0.0.0.0        255.255.255.0   U     0      0      0 tun0
169.254.0.0      0.0.0.0        255.255.0.0     U    1000    0      0 enp0s3
192.168.53.0     0.0.0.0        255.255.255.0   U     0      0      0 tun0
Client/AdarshKumar/PES2UG20CS016/>$

```

This ensures that all the packets from the IP address 103.102.166.0/24 (Wikipedia's IP) will be routed to tun0 interface.

Step 4:

Set Up NAT on Server VM:

We make NAT to believe that the MAC address of 192.168.53.5 is the VPN server's MAC address. The following commands can enable the NAT on the Server VM

```

Server/AdarshKumar/PES2UG20CS016/>$sudo iptables -F
Server/AdarshKumar/PES2UG20CS016/>$sudo iptables -t nat -F
Server/AdarshKumar/PES2UG20CS016/>$sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o enp0s3
Server/AdarshKumar/PES2UG20CS016/>$

```

Task 4:

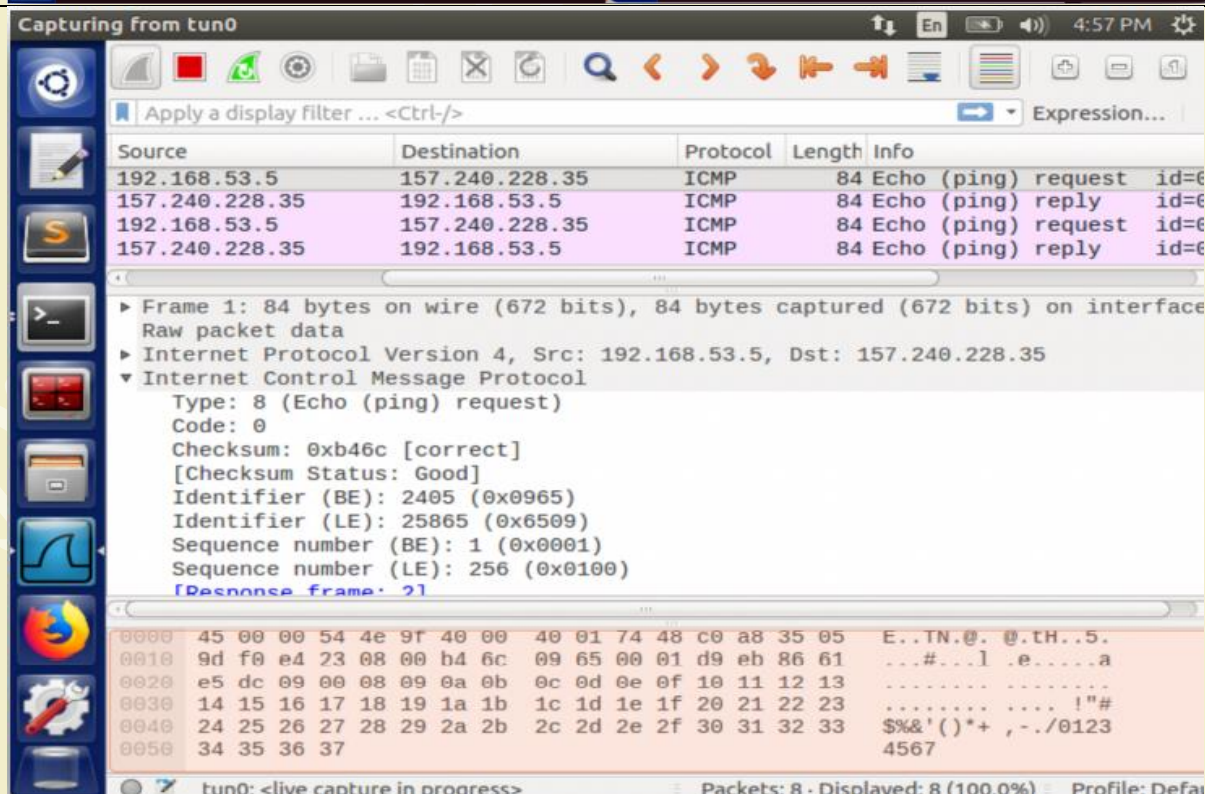
Demonstration


```
Client/AdarshKumar/PES2UG20CS016/>$ping wikipedia.com
PING wikipedia.com (103.102.166.226) 56(84) bytes of data.
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=1 ttl=56 time=169 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=2 ttl=56 time=58.9 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=3 ttl=56 time=82.9 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=4 ttl=56 time=75.2 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=5 ttl=56 time=78.4 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=6 ttl=56 time=75.8 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=7 ttl=56 time=82.9 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=8 ttl=56 time=88.3 ms
^C
--- wikipedia.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7015ms
rtt min/avg/max/mdev = 58.920/89.052/169.806/31.588 ms
Client/AdarshKumar/PES2UG20CS016/>$
```

Client machine can now access W through the tunnel established. We can try ping command. Therefore, the task has been completed successfully



Screenshot



We can observe that the ICMP request packet from tunnel interface (192.168.53.5) is created to IP (157.240.228.35), the tunnel writes the packet to the UDP socket which sends the packet to server machine. (10.0.2.5). The ping reply is received back on tun0 interface. Hence, ping works bypassing firewall through the created tunnel.