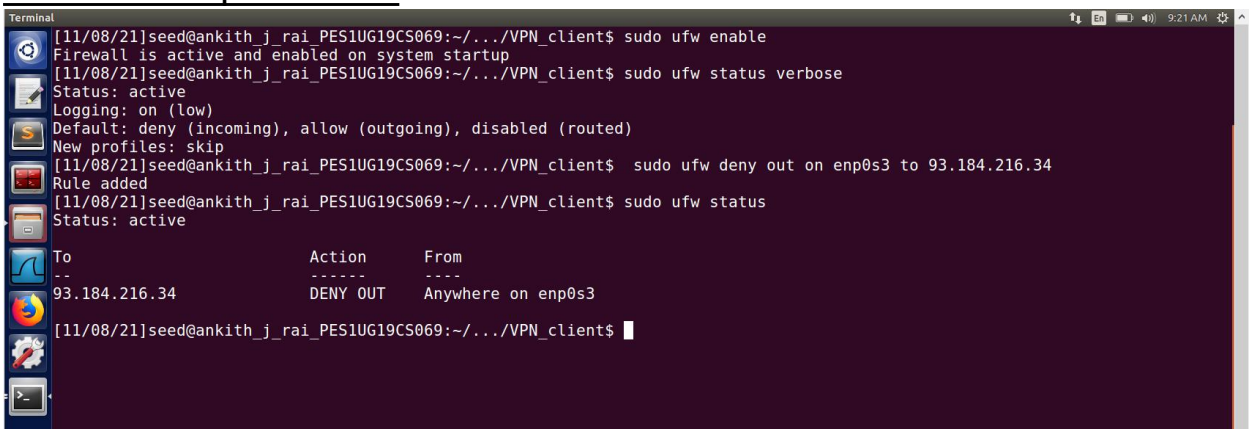
Firewall Evasion Lab: Bypassing Firewalls using VPN

Name : Ankith J Rai
SRN : PES1UG19CS069
SEC : B

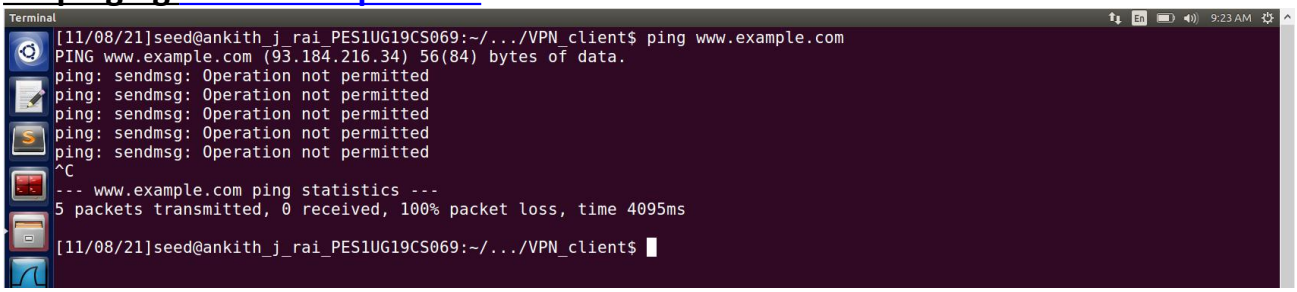
Machine	IP address
VPN Client(VM 1)	10.0.2.12
VPN Server(VM 2)	10.0.2.13

Task 2: Set up Firewall:



From the above screenshot we can see that the firewall has been enabled on the VM 1(VPN client) and a rule denying packets to go from VM 1 to www.example.com (whose ip address is 93.184.216.34) has been added to the firewall.

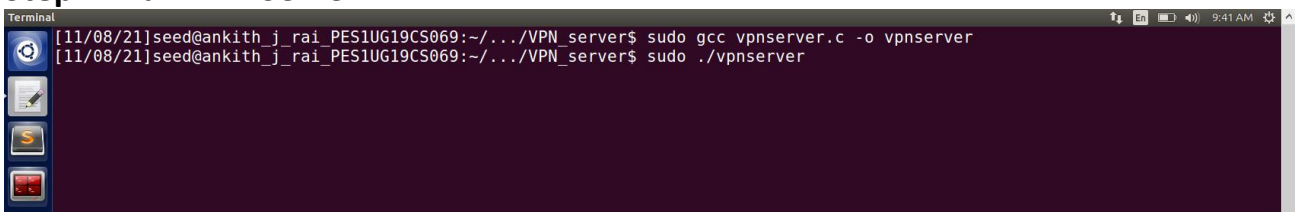
On pinging www.example.com :



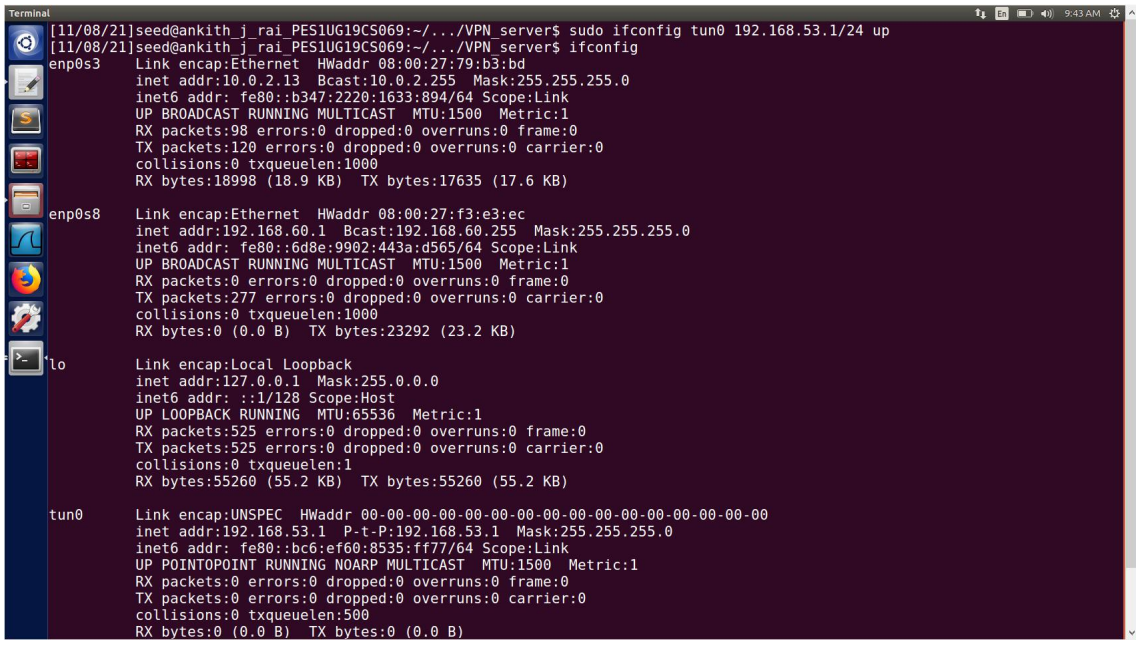
We can see that we get operation not permitted on pinging www.example.com as the firewall is blocking the flow of packets from VM 1 to www.example.com .

Task 3: Bypassing Firewall using VPN:

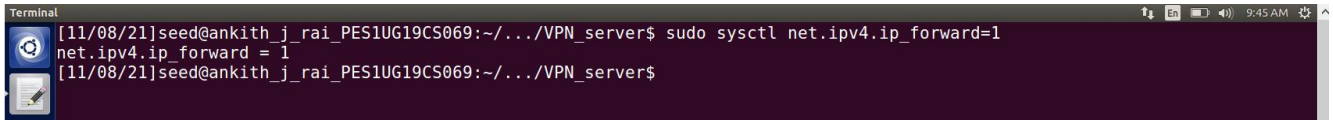
Step 1: Run VPN Server:



From the above screenshot we can see that vpnserver.c program is running on VM 2.



From the above screenshot we can see that the new interface tun0 which got created during running the vpnserver.c program is now configured by giving it ip address 192.168.53.1 .



As VPN Server needs to forward the packets it receives further to respective destination hence the ipv4.ip_forward is set to 1.

Step 2: Run VPN Client:

```
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo gcc vpnclient.c -o vpnclient
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo ./vpnclient 10.0.2.13
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from the tunnel
Got a packet from TUN
Got a packet from TUN
Got a packet from TUN
```

From above screenshot we can see that vpnclient.c program is running on VPN client machine.

```
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo ifconfig tun0 192.168.53.5/24 up
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:86:13:83
          inet addr:10.0.2.12  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::33d:a775:37d5:a1e9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18224 (18.2 KB)  TX bytes:15718 (15.7 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:191 errors:0 dropped:0 overruns:0 frame:0
          TX packets:191 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:31842 (31.8 KB)  TX bytes:31842 (31.8 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::1ee1:afc9:e342:458f/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)

[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$
```

From the above screenshot we can see that the interface tun0 on VPN client machine has been configured and has been given the ip address 192.168.53.5 .

Step 3: Set Up Routing on Client and Server VMs:

```
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ 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
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
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$
```

After using sudo route add 93.184.216.34 tun0

```
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ sudo route add 93.184.216.34 tun0
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ 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
93.184.216.34   0.0.0.0         255.255.255.255 UH    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
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$
```

From the above screenshot we can see that the route has been added.

Step 4: Set Up NAT on Server VM:

```
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ sudo iptables -F
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ sudo iptables -t nat -F
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$ sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o enp0s3
[11/08/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_server$
```

Now server will capture and forward all the packets to it's respective destination.

Task 4: Demonstration

Screenshot of terminal of VPN client:

```
Terminal
[11/09/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$ ping www.example.com
PING www.example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34: icmp_seq=1 ttl=56 time=367 ms
64 bytes from 93.184.216.34: icmp_seq=2 ttl=56 time=235 ms
64 bytes from 93.184.216.34: icmp_seq=3 ttl=56 time=231 ms
64 bytes from 93.184.216.34: icmp_seq=4 ttl=56 time=283 ms
64 bytes from 93.184.216.34: icmp_seq=5 ttl=56 time=231 ms
64 bytes from 93.184.216.34: icmp_seq=6 ttl=56 time=234 ms
64 bytes from 93.184.216.34: icmp_seq=7 ttl=56 time=250 ms
^C
--- www.example.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 231.063/261.826/367.102/46.267 ms
[11/09/21]seed@ankith_j_rai_PES1UG19CS069:~/.../VPN_client$
```

Screenshot of terminal of VPN client where the vpnclient.c program is running:

```
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
```

We can see that the packets have been sent through the tunnel successfully.

Screenshot of terminal of VPN client where the vpnclient.c program is running:

```
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
Got a packet from TUN
Got a packet from the tunnel
```

We can see that the packets have been sent through the tunnel successfully.

From the wireshark of both VPN client and VPN server I have seen that the packets are sent from the VPN client to VPN server through the tunnel and VPN server sends packet to ip address of www.example.com and the reply from www.example.com goes first to VM server and VM

server forwards these reply packets to VM client. Hence VM client is able to ping www.example.com