COMPUTER NETWORK SECURITY OPTIONAL LAB 02

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

BYPASSING FIREWALLS USING VPN

Task 1: VM Setup

In this task, we create two VMs, one that will lie inside the firewall (10.0.2.5) and one that'll be present outside the firewall (10.0.2.4).

The host/site for which the firewall will block access to, is www.example.net (93.184.216.34).

Before setting up the firewall, Host 2.5 is able to ping www.example.net.

```
PES1UG20CS280(10.0.2.5) -$ping www.example.net
PING www.example.net (93.184.216.34) 56(84) bytes of data.
64 bytes from www.example.net (93.184.216.34): icmp_seq=1 ttl=53 time=241 ms
64 bytes from www.example.net (93.184.216.34): icmp_seq=2 ttl=53 time=231 ms
64 bytes from www.example.net (93.184.216.34): icmp_seq=3 ttl=53 time=237 ms
64 bytes from www.example.net (93.184.216.34): icmp_seq=4 ttl=53 time=232 ms
64 bytes from www.example.net (93.184.216.34): icmp_seq=5 ttl=53 time=245 ms
^X64 bytes from www.example.net (93.184.216.34): icmp_seq=6 ttl=53 time=232 ms
64 bytes from www.example.net (93.184.216.34): icmp_seq=7 ttl=53 time=232 ms
^Z
[1]+  Stopped                 ping www.example.net
```

Task 2: Set up Firewall

The firewall is enabled using the first command. The second command is used to specify the rule—deny any packets directed to 93.184.216.0/24 network (outgoing traffic from the host/host's enp0s3 network in our case).

The status of these rules can be seen using the third command.

We see that now when the host pings www.example.net , the firewall drops all packets directed to it. Therefore, ping is not successful and the output is as shown below-

```
PES1UG20CS280(10.0.2.5) -$sudo ufw enable
Firewall is active and enabled on system startup
PES1UG20CS280(10.0.2.5) -$sudo ufw deny out on enp0s3 to 93.184.216.0/24
Rule added
PES1UG20CS280(10.0.2.5) -$sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
93.184.216.0/24            DENY OUT    Anywhere on enp0s3

PES1UG20CS280(10.0.2.5) -$ping www.example.net
PING www.example.net (93.184.216.34) 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
^Z
[2]+  Stopped                 ping www.example.net
```

COMPUTER NETWORK SECURITY OPTIONAL LAB 02

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Task 3: Bypassing Firewall using VPN

Step 1: Run VPN Server:

The server code is executed on the host outside of the firewall (10.0.2.4). Once the server is up, a tun0 interface is created for the VPN_server. An IP address must be bound to the tun0 interface of the server and we do that with the below command.

```
PES1UG20CS280(10.0.2.4) -$sudo ifconfig tun0 192.168.53.1/24 up
PES1UG20CS280(10.0.2.4) -$ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:c6:fa:69
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::2966:fab7:f473:7dbc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21347 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13015 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23433375 (23.4 MB)  TX bytes:7192771 (7.1 MB)

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:3439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3439 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:320258 (320.2 KB)  TX bytes:320258 (320.2 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::dbc7:d297:5f3c:c66b/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)

PES1UG20CS280(10.0.2.4) -$sudo sysctl net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

IP forwarding is enabled at the server end, as the server must be able to route packet requests received at the VPN tunnel to appropriate destination hosts.

Initially, no details are displayed when the server starts running as there is no VPN tunnel established yet. The server part of the tunnel is brought up. The next task is to bring the client part of the tunnel up.

```
PES1UG20CS280(10.0.2.4) -$gcc vpnserver.c -o vpnserver
PES1UG20CS280(10.0.2.4) -$sudo ./vpnserver
```

COMPUTER NETWORK SECURITY OPTIONAL LAB 02

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

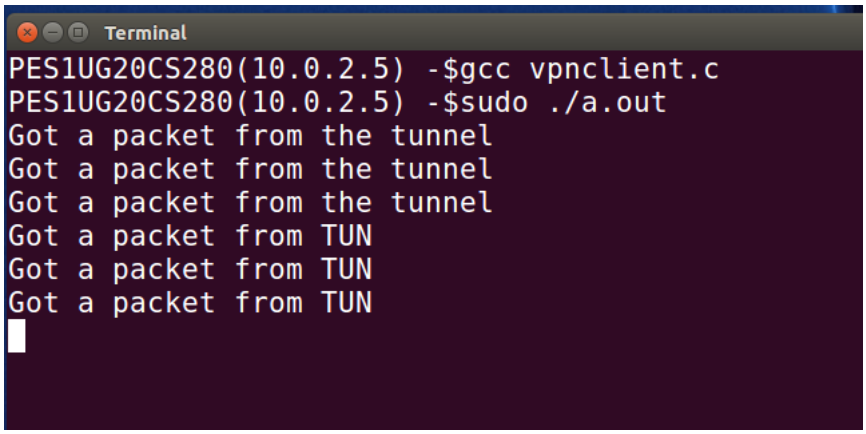
Step 2: Run VPN Client:

In this task, the client part of the VPN tunnel is brought up. The tun0 interface of the client must also be bound to an IP address. The same is done with the command below-

```
PES1UG20CS280(10.0.2.5) -$sudo ifconfig tun0 192.168.53.5/24
PES1UG20CS280(10.0.2.5) -$ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:ec:31:3a:8a
          inet addr:172.17.0.1  Bcast:0.0.0.0  Mask:255.255.0.0
          UP BROADCAST 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:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

enp0s3    Link encap:Ethernet  HWaddr 08:00:27:94:43:70
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::7cf3:ab06:1a80:e10b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:298 errors:0 dropped:0 overruns:0 frame:0
          TX packets:406 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:119741 (119.7 KB)  TX bytes:44387 (44.3 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:319 errors:0 dropped:0 overruns:0 frame:0
          TX packets:319 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:45950 (45.9 KB)  TX bytes:45950 (45.9 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::4afe:2d60:ef68:5f69/64 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
```

When the client is brought up, the VPN tunnel is established. The server sends three packets to the client and the client does the same too, to verify each other's presence.

The client receives three packets from the server (via the VPN tunnel). The client sends three packets to the server (via its TUN interface). Because the server is brought up first, the server first sends the packets, followed by the client.



At the server's end, the exact opposite is observed. The first line output indicates that a connection is established with the client i.e a VPN tunnel is established. The server sends out 3 packets via its TUN interface to the client. Three packets sent by the client arrive at the server via the tunnel.

```
PES1UG20CS280(10.0.2.4) -$sudo ./a.out
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
```

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

Once the VPN tunnel is established, the client's routing path must be updated so that any packet requests pertaining to the 93.184.216.0/24 network or www.example.net (93.184.216.34) is redirected to its tun interface (and eventually the VPN tunnel).

```
PES1UG20CS280(10.0.2.5) -$sudo route add 93.184.216.34 tun0
```

Step 4: Set Up NAT on Server VM

The current rules in the NAT table must be flushed before new rules can be added. The first two commands are used to do the same.

The next rule is used to route the packet requests arriving at the VPN tunnel to the destined host by masquerading them (as though the VPN server is sending those packet requests).

The network interface name is enp0s3.

```
PES1UG20CS280(10.0.2.4) -$sudo iptables -F
PES1UG20CS280(10.0.2.4) -$sudo iptables -t nat -F
PES1UG20CS280(10.0.2.4) -$sudo iptables -t nat -A POSTROUTING -j MASQUERADE -o enp0s3
PES1UG20CS280(10.0.2.4) -$
```

COMPUTER NETWORK SECURITY OPTIONAL LAB 02

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Task 4: Demonstration

Now, when the client/host inside the firewall tries to ping www.example.net , we see that the ping is successful even when the firewall blocks packet requests directed to that site.

However, one important observation is that the time taken is much greater (when compared to a regular ping). This is because the ICMP requests must first pass through the VPN tunnel and get directed to the intended host. ICMP response packets must also follow the same path to reach the host.

```
PES1UG20CS280(10.0.2.5) -$sudo route add 93.184.216.34 tun0
PES1UG20CS280(10.0.2.5) -$ping www.example.net
PING www.example.net (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34: icmp_seq=1 ttl=51 time=237 ms
64 bytes from 93.184.216.34: icmp_seq=2 ttl=51 time=232 ms
64 bytes from 93.184.216.34: icmp_seq=3 ttl=51 time=233 ms
64 bytes from 93.184.216.34: icmp_seq=4 ttl=51 time=235 ms
^Z
[1]+  Stopped                 ping www.example.net
PES1UG20CS280(10.0.2.5) -$sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
93.184.216.0/24            DENY OUT    Anywhere on enp0s3

PES1UG20CS280(10.0.2.5) -$
```

ICMP requests pass through the TUN interface of Host2.5 and get sent into the VPN tunnel. ICMP responses pass through the VPN tunnel and reach Host2.5. The same is shown below -

```
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
^C
PES1UG20CS280(10.0.2.5) -$
```

COMPUTER NETWORK SECURITY OPTIONAL LAB 02

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

ICMP request packets arrive at the VPN server via the VPN tunnel. The VPN server routes these packets to the intended host (example.net) in this case. ICMP response packets sent by the intended host are sent back to the VPN server. The VPN server sends those packets back via its TUN interface into the VPN tunnel. The same is shown below -

```
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
^C
PES1UG20CS280(10.0.2.4) -$
```

Wireshark capture on HOST (10.0.2.5)

22	2022-11-22 22:50:29.8369239…	202.138.96.2	10.0.2.5	DNS	226 Standard query response 0x71c7 A www.example.net A 93.184.216.34 NS a.iana-servers.ne
23	2022-11-22 22:50:29.8369866…	10.0.2.5	202.138.96.2	ICMP	254 Destination unreachable (Port unreachable)
24	2022-11-22 22:50:30.5675601…	192.168.53.5	93.184.216.34	ICMP	100 Echo (ping) request id=0x0c0f, seq=2/512, ttl=64 (reply in 27)
25	2022-11-22 22:50:30.5676746…	10.0.2.5	10.0.2.4	UDP	128 46352 → 55555 Len=84
26	2022-11-22 22:50:30.7998201…	10.0.2.4	10.0.2.5	UDP	128 55555 → 46352 Len=84
27	2022-11-22 22:50:30.7999240…	93.184.216.34	192.168.53.5	ICMP	100 Echo (ping) reply id=0x0c0f, seq=2/512, ttl=51 (request in 24)
28	2022-11-22 22:50:31.5694952…	192.168.53.5	93.184.216.34	ICMP	100 Echo (ping) request id=0x0c0f, seq=3/768, ttl=64 (reply in 31)
29	2022-11-22 22:50:31.5696641…	10.0.2.5	10.0.2.4	UDP	128 46352 → 55555 Len=84
30	2022-11-22 22:50:31.8023212…	10.0.2.4	10.0.2.5	UDP	128 55555 → 46352 Len=84
31	2022-11-22 22:50:31.8025634…	93.184.216.34	192.168.53.5	ICMP	100 Echo (ping) reply id=0x0c0f, seq=3/768, ttl=51 (request in 28)
32	2022-11-22 22:50:32.5709348…	192.168.53.5	93.184.216.34	ICMP	100 Echo (ping) request id=0x0c0f, seq=4/1024, ttl=64 (reply in 35)
33	2022-11-22 22:50:32.5711511…	10.0.2.5	10.0.2.4	UDP	128 46352 → 55555 Len=84
34	2022-11-22 22:50:32.8064590…	10.0.2.4	10.0.2.5	UDP	128 55555 → 46352 Len=84
35	2022-11-22 22:50:32.8066462…	93.184.216.34	192.168.53.5	ICMP	100 Echo (ping) reply id=0x0c0f, seq=4/1024, ttl=51 (request in 32)
36	2022-11-22 22:50:32.9305591…	192.168.3.5	10.0.2.5	DNS	93 Standard query response 0x71c7 A www.example.net A 93.184.216.34
37	2022-11-22 22:50:32.9306387…	10.0.2.5	192.168.3.5	ICMP	121 Destination unreachable (Port unreachable)
38	2022-11-22 22:50:33.5736407…	192.168.53.5	93.184.216.34	ICMP	100 Echo (ping) request id=0x0c0f, seq=5/1280, ttl=64 (reply in 41)
39	2022-11-22 22:50:33.5738859…	10.0.2.5	10.0.2.4	UDP	128 46352 → 55555 Len=84
40	2022-11-22 22:50:33.8068045…	10.0.2.4	10.0.2.5	UDP	128 55555 → 46352 Len=84
41	2022-11-22 22:50:33.8069489…	93.184.216.34	192.168.53.5	ICMP	100 Echo (ping) reply id=0x0c0f, seq=5/1280, ttl=51 (request in 38)
42	2022-11-22 22:50:34.5901077…	PcsCompu_94:43:70		ARP	44 Who has 10.0.2.4? Tell 10.0.2.5
43	2022-11-22 22:50:34.5901673…	PcsCompu_94:43:70		ARP	44 Who has 10.0.2.1? Tell 10.0.2.5

As seen above, the initial ICMP request packet has a source IP of 192.168.53.5 (IP of the client tun0 interface). The destination IP is that of example.net (where the packets are destined to).

The ICMP packet is encompassed by a UDP packet whose source IP is the client's IP (10.0.2.5) and destination IP is the server's (10.0.2.4). This encompassed packet passes through the VPN tunnel that has been established between VPN-Client and VPN-Server.

On reaching the VPN-Server, the ICMP request packets are directed to the intended host. The corresponding response packet is redirected back to the VPN Server. The ICMP response packet has source IP (93.184.216.34) and destination IP as the tun interface. The corresponding IP response packet is encompassed by a UDP packet and redirected back to the VPN-client. The source IP of this UDP packet is 10.0.2.4 and destination IP is 10.0.2.5.