

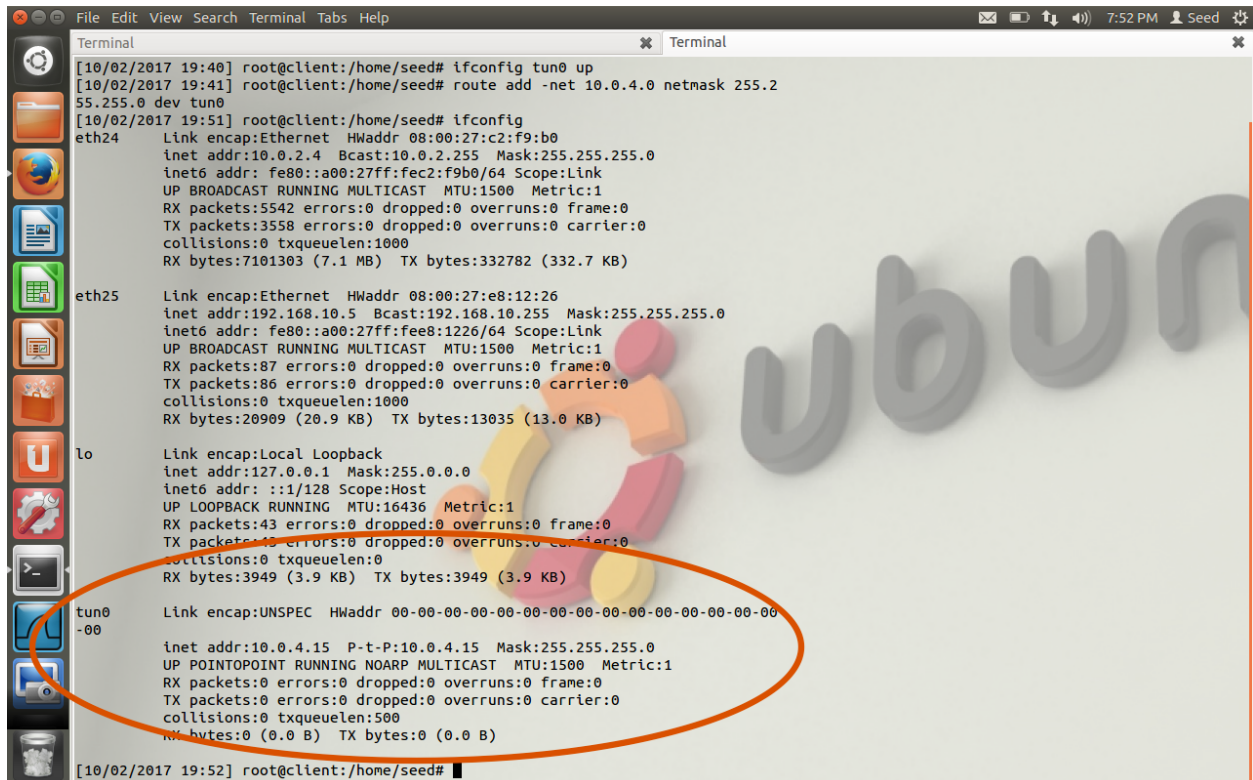
Ravee Khandagale

Lab 04

CS 266

Tunnel Setup

On VM1 show me you have tun0 interface using ifconfig.



```
File Edit View Search Terminal Tabs Help
Terminal
[10/02/2017 19:40] root@client:/home/seed# ifconfig tun0 up
[10/02/2017 19:41] root@client:/home/seed# route add -net 10.0.4.0 netmask 255.255.0 dev tun0
[10/02/2017 19:51] root@client:/home/seed# ifconfig
eth24      Link encap:Ethernet  HWaddr 08:00:27:c2:f9:b0
           inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:fec2:f9b0/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:5542 errors:0 dropped:0 overruns:0 frame:0
           TX packets:3558 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:7101303 (7.1 MB)  TX bytes:332782 (332.7 KB)

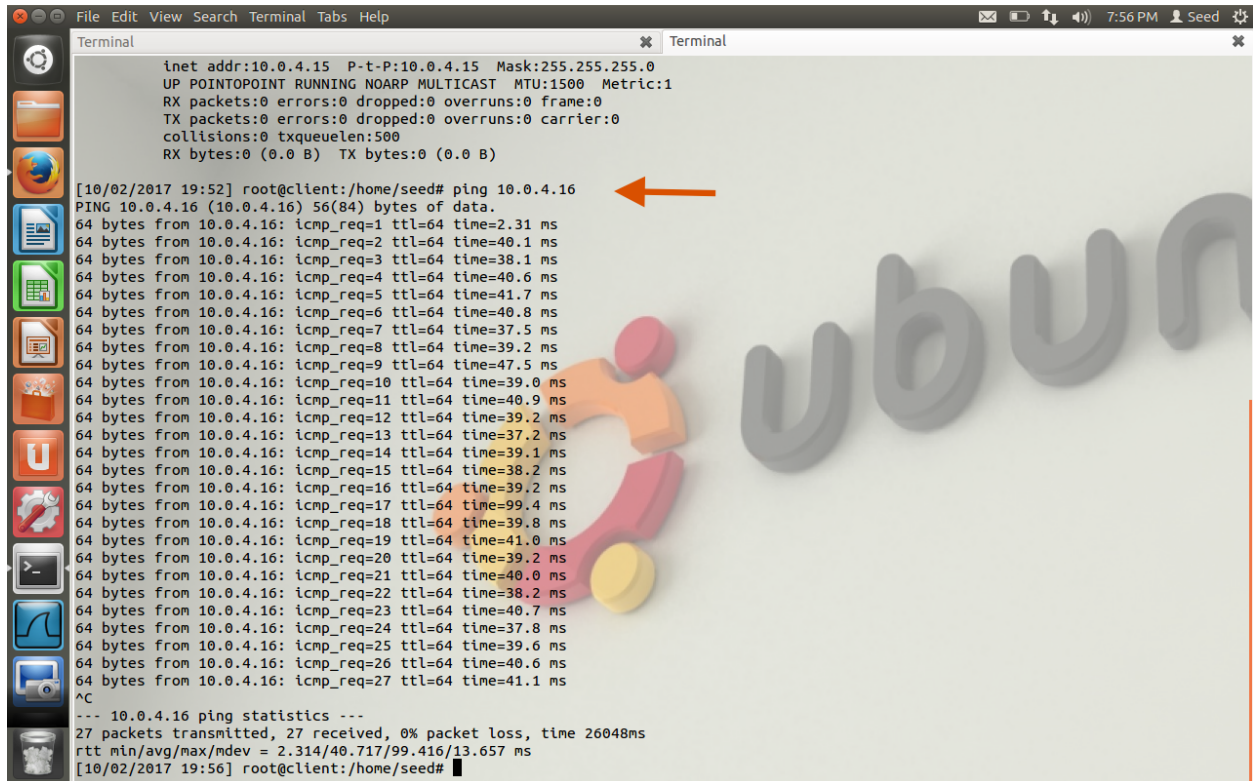
eth25      Link encap:Ethernet  HWaddr 08:00:27:e8:12:26
           inet addr:192.168.10.5  Bcast:192.168.10.255  Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:fee8:1226/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:87 errors:0 dropped:0 overruns:0 frame:0
           TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:20909 (20.9 KB)  TX bytes:13035 (13.0 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:16436  Metric:1
           RX packets:43 errors:0 dropped:0 overruns:0 frame:0
           TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:3949 (3.9 KB)  TX bytes:3949 (3.9 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
           inet addr:10.0.4.15  P-t-P:10.0.4.15  Mask:255.255.255.0
           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)

[10/02/2017 19:52] root@client:/home/seed#
```

Ping VM1 from VM2 using tunnel. Take a screenshot.

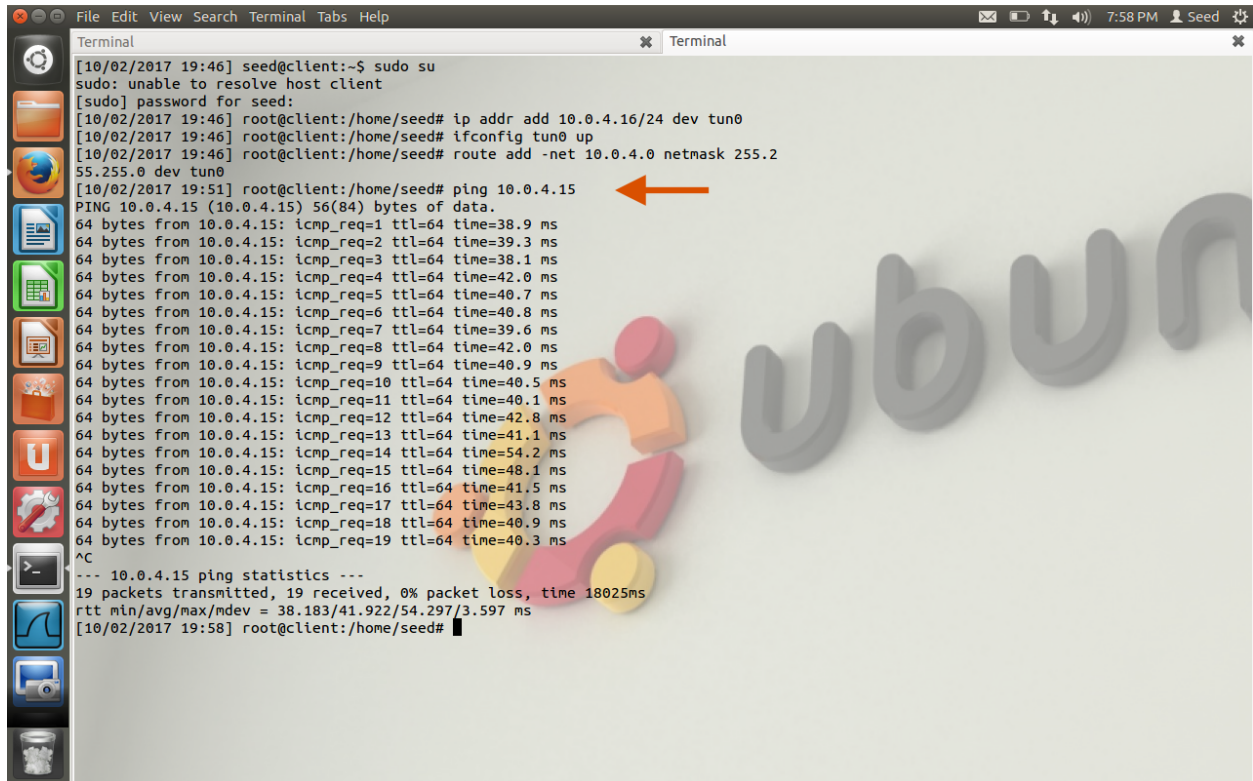


The screenshot shows a terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Tabs, Help) and a status bar (7:56 PM, Seed). The terminal output shows the configuration of the tunnel interface 'tun0' and a successful ping from VM2 to VM1. An orange arrow points to the first line of the ping output.

```
inet addr:10.0.4.15 P-t-P:10.0.4.15 Mask:255.255.255.0
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)

[10/02/2017 19:52] root@client:/home/seed# ping 10.0.4.16
PING 10.0.4.16 (10.0.4.16) 56(84) bytes of data.
64 bytes from 10.0.4.16: icmp_req=1 ttl=64 time=2.31 ms
64 bytes from 10.0.4.16: icmp_req=2 ttl=64 time=40.1 ms
64 bytes from 10.0.4.16: icmp_req=3 ttl=64 time=38.1 ms
64 bytes from 10.0.4.16: icmp_req=4 ttl=64 time=40.6 ms
64 bytes from 10.0.4.16: icmp_req=5 ttl=64 time=41.7 ms
64 bytes from 10.0.4.16: icmp_req=6 ttl=64 time=40.8 ms
64 bytes from 10.0.4.16: icmp_req=7 ttl=64 time=37.5 ms
64 bytes from 10.0.4.16: icmp_req=8 ttl=64 time=39.2 ms
64 bytes from 10.0.4.16: icmp_req=9 ttl=64 time=47.5 ms
64 bytes from 10.0.4.16: icmp_req=10 ttl=64 time=39.0 ms
64 bytes from 10.0.4.16: icmp_req=11 ttl=64 time=40.9 ms
64 bytes from 10.0.4.16: icmp_req=12 ttl=64 time=39.2 ms
64 bytes from 10.0.4.16: icmp_req=13 ttl=64 time=37.2 ms
64 bytes from 10.0.4.16: icmp_req=14 ttl=64 time=39.1 ms
64 bytes from 10.0.4.16: icmp_req=15 ttl=64 time=38.2 ms
64 bytes from 10.0.4.16: icmp_req=16 ttl=64 time=39.2 ms
64 bytes from 10.0.4.16: icmp_req=17 ttl=64 time=99.4 ms
64 bytes from 10.0.4.16: icmp_req=18 ttl=64 time=39.8 ms
64 bytes from 10.0.4.16: icmp_req=19 ttl=64 time=41.0 ms
64 bytes from 10.0.4.16: icmp_req=20 ttl=64 time=39.2 ms
64 bytes from 10.0.4.16: icmp_req=21 ttl=64 time=40.0 ms
64 bytes from 10.0.4.16: icmp_req=22 ttl=64 time=38.2 ms
64 bytes from 10.0.4.16: icmp_req=23 ttl=64 time=40.7 ms
64 bytes from 10.0.4.16: icmp_req=24 ttl=64 time=37.8 ms
64 bytes from 10.0.4.16: icmp_req=25 ttl=64 time=39.6 ms
64 bytes from 10.0.4.16: icmp_req=26 ttl=64 time=40.6 ms
64 bytes from 10.0.4.16: icmp_req=27 ttl=64 time=41.1 ms
^C
--- 10.0.4.16 ping statistics ---
27 packets transmitted, 0% packet loss, time 26048ms
rtt min/avg/max/mdev = 2.314/40.717/99.416/13.657 ms
[10/02/2017 19:56] root@client:/home/seed#
```

Ping VM2 from VM1 using tunnel. Take a screenshot.



The screenshot shows a terminal window with the following commands and output:

```
[10/02/2017 19:46] seed@client:~$ sudo su
sudo: unable to resolve host client
[sudo] password for seed:
[10/02/2017 19:46] root@client:/home/seed# ip addr add 10.0.4.16/24 dev tun0
[10/02/2017 19:46] root@client:/home/seed# ifconfig tun0 up
[10/02/2017 19:46] root@client:/home/seed# route add -net 10.0.4.0 netnask 255.2
55.255.0 dev tun0
[10/02/2017 19:51] root@client:/home/seed# ping 10.0.4.15
PING 10.0.4.15 (10.0.4.15) 56(84) bytes of data.
64 bytes from 10.0.4.15: icmp_req=1 ttl=64 time=38.9 ms
64 bytes from 10.0.4.15: icmp_req=2 ttl=64 time=39.3 ms
64 bytes from 10.0.4.15: icmp_req=3 ttl=64 time=38.1 ms
64 bytes from 10.0.4.15: icmp_req=4 ttl=64 time=42.0 ms
64 bytes from 10.0.4.15: icmp_req=5 ttl=64 time=40.7 ms
64 bytes from 10.0.4.15: icmp_req=6 ttl=64 time=40.8 ms
64 bytes from 10.0.4.15: icmp_req=7 ttl=64 time=39.6 ms
64 bytes from 10.0.4.15: icmp_req=8 ttl=64 time=42.0 ms
64 bytes from 10.0.4.15: icmp_req=9 ttl=64 time=40.9 ms
64 bytes from 10.0.4.15: icmp_req=10 ttl=64 time=40.5 ms
64 bytes from 10.0.4.15: icmp_req=11 ttl=64 time=40.1 ms
64 bytes from 10.0.4.15: icmp_req=12 ttl=64 time=42.8 ms
64 bytes from 10.0.4.15: icmp_req=13 ttl=64 time=41.1 ms
64 bytes from 10.0.4.15: icmp_req=14 ttl=64 time=54.2 ms
64 bytes from 10.0.4.15: icmp_req=15 ttl=64 time=48.1 ms
64 bytes from 10.0.4.15: icmp_req=16 ttl=64 time=41.5 ms
64 bytes from 10.0.4.15: icmp_req=17 ttl=64 time=43.8 ms
64 bytes from 10.0.4.15: icmp_req=18 ttl=64 time=40.9 ms
64 bytes from 10.0.4.15: icmp_req=19 ttl=64 time=40.3 ms
^C
--- 10.0.4.15 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18025ms
rtt min/avg/max/mdev = 38.183/41.922/54.297/3.597 ms
[10/02/2017 19:58] root@client:/home/seed#
```

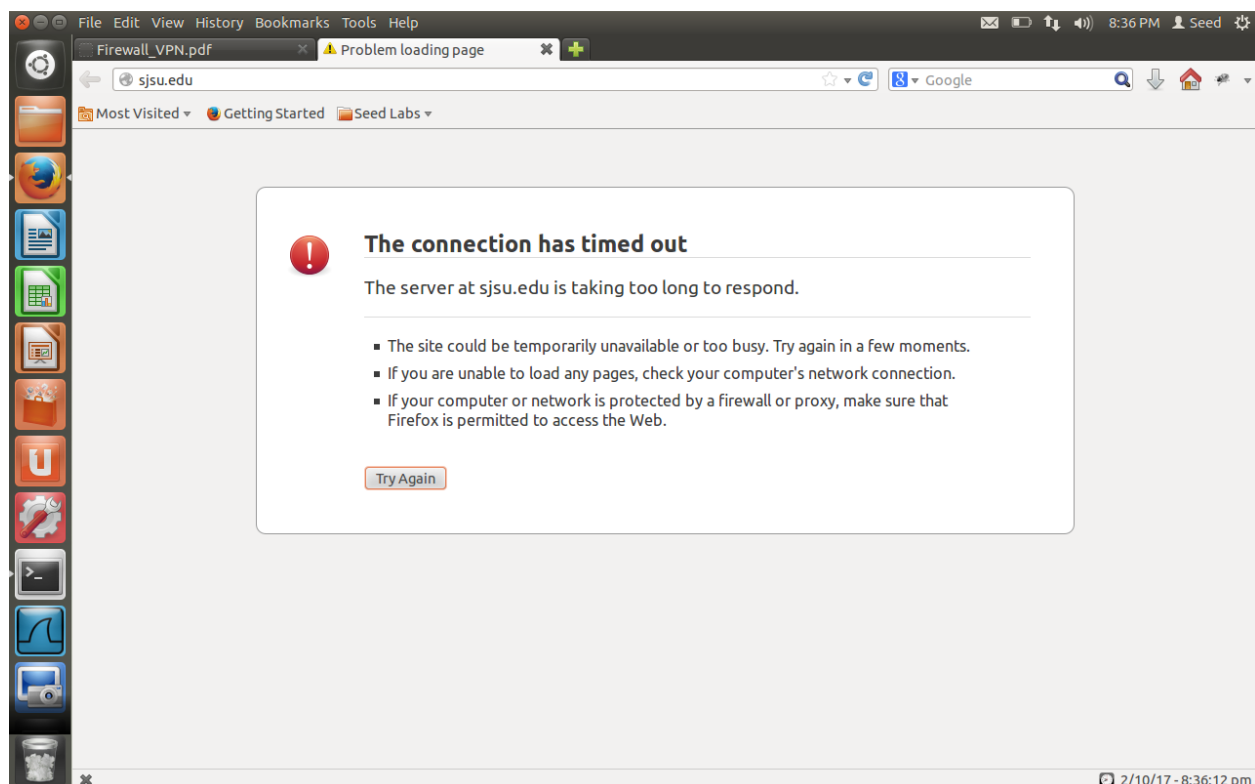
An orange arrow points to the command `ping 10.0.4.15`. The background of the terminal window features a large, stylized 'ubuntu' logo.

Firewall setup

Tell me what happens. What is the site you are trying to block?

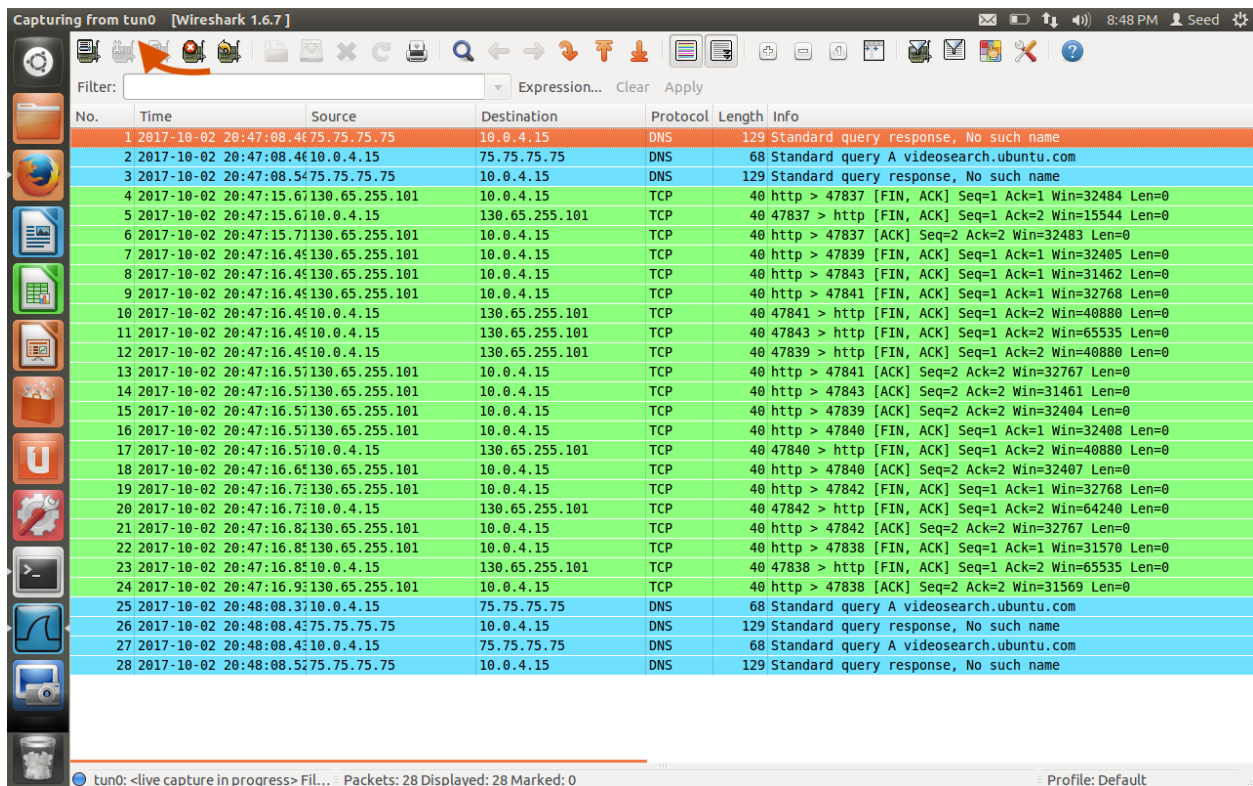
Answer: We are setting up a firewall on VM1 to block the access of a target website.

- I am trying to block the **sjsu.edu website (130.65.255.0/24)**.
- When I run the command, `sudo iptables -t mangle -A POSTROUTING -d 130.65.255.0/24 -o eth24 -j DROP` All the packets to sjsu.edu on eth24 (which is the interface for natnetwork) are dropped.
- As a result, the sjsu.edu website is not accessible.
- We are using iptables command to achieve this due to which the packets at eth24 are getting dropped.
- We are setting up the firewall to block packets.
- We are setting the rule on VM1's network interface (non virtual). This way we make sure that packets going to the virtual interfaces are still received.
- The following screenshot shows the blocked site



Bypassing Firewall

Open a browser and visit <http://www.sjsu.edu/> or site of your choice Take a screenshot of wireshark trace to show the traffic is going through the tunnel (tun0). Make your screenshot shows you are capturing data on tun0.



Capturing from tun0 [Wireshark 1.6.7]

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	2017-10-02 20:47:08.46	75.75.75.75	10.0.4.15	DNS	129	Standard query response, No such name
2	2017-10-02 20:47:08.46	10.0.4.15	75.75.75.75	DNS	68	Standard query A videosearch.ubuntu.com
3	2017-10-02 20:47:08.54	75.75.75.75	10.0.4.15	DNS	129	Standard query response, No such name
4	2017-10-02 20:47:15.67	130.65.255.101	10.0.4.15	TCP	40	http > 47837 [FIN, ACK] Seq=1 Ack=1 Win=32484 Len=0
5	2017-10-02 20:47:15.67	10.0.4.15	130.65.255.101	TCP	40	47837 > http [FIN, ACK] Seq=1 Ack=2 Win=15544 Len=0
6	2017-10-02 20:47:15.71	130.65.255.101	10.0.4.15	TCP	40	http > 47837 [ACK] Seq=2 Ack=2 Win=32483 Len=0
7	2017-10-02 20:47:16.45	130.65.255.101	10.0.4.15	TCP	40	http > 47839 [FIN, ACK] Seq=1 Ack=1 Win=32405 Len=0
8	2017-10-02 20:47:16.45	130.65.255.101	10.0.4.15	TCP	40	http > 47843 [FIN, ACK] Seq=1 Ack=1 Win=31462 Len=0
9	2017-10-02 20:47:16.45	130.65.255.101	10.0.4.15	TCP	40	http > 47841 [FIN, ACK] Seq=1 Ack=1 Win=32768 Len=0
10	2017-10-02 20:47:16.45	10.0.4.15	130.65.255.101	TCP	40	47841 > http [FIN, ACK] Seq=1 Ack=2 Win=40880 Len=0
11	2017-10-02 20:47:16.45	10.0.4.15	130.65.255.101	TCP	40	47843 > http [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
12	2017-10-02 20:47:16.45	10.0.4.15	130.65.255.101	TCP	40	47839 > http [FIN, ACK] Seq=1 Ack=2 Win=40880 Len=0
13	2017-10-02 20:47:16.57	130.65.255.101	10.0.4.15	TCP	40	http > 47841 [ACK] Seq=2 Ack=2 Win=32767 Len=0
14	2017-10-02 20:47:16.57	130.65.255.101	10.0.4.15	TCP	40	http > 47843 [ACK] Seq=2 Ack=2 Win=31461 Len=0
15	2017-10-02 20:47:16.57	130.65.255.101	10.0.4.15	TCP	40	http > 47839 [ACK] Seq=2 Ack=2 Win=32404 Len=0
16	2017-10-02 20:47:16.57	130.65.255.101	10.0.4.15	TCP	40	http > 47840 [FIN, ACK] Seq=1 Ack=1 Win=32408 Len=0
17	2017-10-02 20:47:16.57	10.0.4.15	130.65.255.101	TCP	40	47840 > http [FIN, ACK] Seq=1 Ack=2 Win=40880 Len=0
18	2017-10-02 20:47:16.65	130.65.255.101	10.0.4.15	TCP	40	http > 47840 [ACK] Seq=2 Ack=2 Win=32407 Len=0
19	2017-10-02 20:47:16.73	130.65.255.101	10.0.4.15	TCP	40	http > 47842 [FIN, ACK] Seq=1 Ack=1 Win=32768 Len=0
20	2017-10-02 20:47:16.73	10.0.4.15	130.65.255.101	TCP	40	47842 > http [FIN, ACK] Seq=1 Ack=2 Win=64240 Len=0
21	2017-10-02 20:47:16.82	130.65.255.101	10.0.4.15	TCP	40	http > 47842 [ACK] Seq=2 Ack=2 Win=32767 Len=0
22	2017-10-02 20:47:16.85	130.65.255.101	10.0.4.15	TCP	40	http > 47838 [FIN, ACK] Seq=1 Ack=1 Win=31570 Len=0
23	2017-10-02 20:47:16.85	10.0.4.15	130.65.255.101	TCP	40	47838 > http [FIN, ACK] Seq=1 Ack=2 Win=65535 Len=0
24	2017-10-02 20:47:16.93	130.65.255.101	10.0.4.15	TCP	40	http > 47838 [ACK] Seq=2 Ack=2 Win=31569 Len=0
25	2017-10-02 20:48:08.37	10.0.4.15	75.75.75.75	DNS	68	Standard query A videosearch.ubuntu.com
26	2017-10-02 20:48:08.43	75.75.75.75	10.0.4.15	DNS	129	Standard query response, No such name
27	2017-10-02 20:48:08.43	10.0.4.15	75.75.75.75	DNS	68	Standard query A videosearch.ubuntu.com
28	2017-10-02 20:48:08.52	75.75.75.75	10.0.4.15	DNS	129	Standard query response, No such name

tun0: <live capture in progress> Fil... Packets: 28 Displayed: 28 Marked: 0 Profile: Default