

Task 1:

- VM A: 10.0.2.5
- VM B: 10.0.2.15

a. The left screenshot is VM A, and the right one is VM B

The image shows two side-by-side terminal windows. Both are titled 'Terminator' and show a bash shell. The left window (VM A) has a blue border and displays the following command outputs:
[04/09/22]seed@VM:~\$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:ed:cc:24
inet addr: 10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::8c83:eb90:adc8:48c4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:8 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1780 (1.7 KB) TX bytes:7552 (7.5 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:67 errors:0 dropped:0 overruns:0 frame:0
TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:21400 (21.4 KB) TX bytes:21400 (21.4 KB)

[04/09/22]seed@VM:~\$ telnet 10.0.2.15
Trying 10.0.2.15...
telnet: Unable to connect to remote host: No route to host
[04/09/22]seed@VM:~\$ telnet 10.0.2.15
Trying 10.0.2.15...
The right window (VM B) has a red border and displays:
[04/09/22]seed@VM:~\$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:5c:8d:cf
inet addr: 10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::4c0b:3971:5ce8:a329/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:5 errors:0 dropped:0 overruns:0 frame:0
TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1070 (1.0 KB) TX bytes:7110 (7.1 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:67 errors:0 dropped:0 overruns:0 frame:0
TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:21416 (21.4 KB) TX bytes:21416 (21.4 KB)

[04/09/22]seed@VM:~\$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.

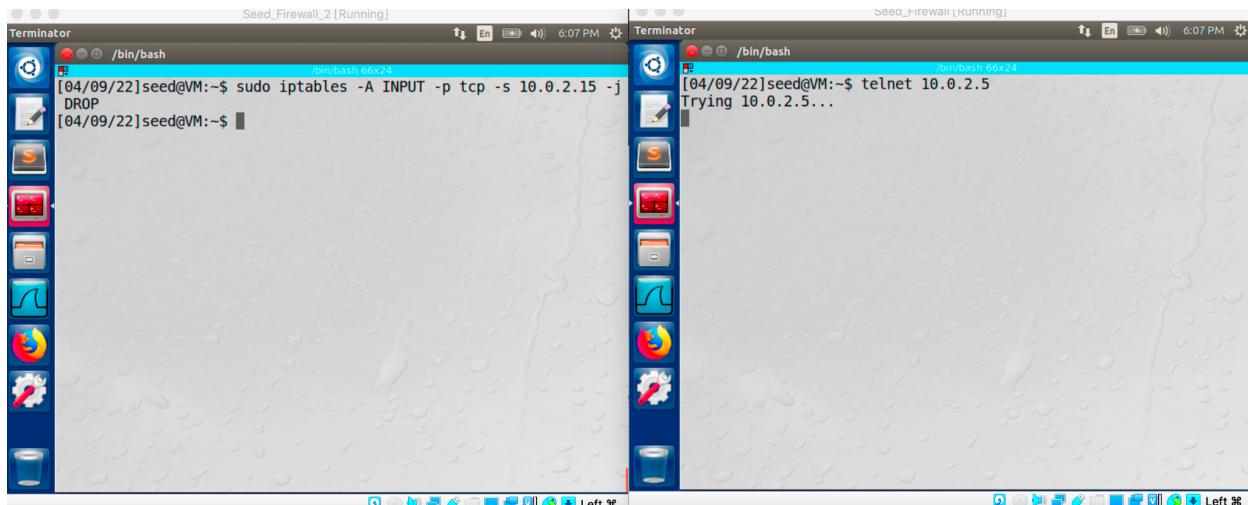
b. The below screenshot shows that both VM A(10.0.2.5) and VM B (10.0.2.15) do not configure firewall policy, and both of them can access each other via telnet and vice versa.

The image shows two side-by-side terminal windows. Both are titled 'Terminator' and show a bash shell. The left window (VM A) has a blue border and displays:
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: [REDACTED]
Login timed out after 60 seconds.
Connection closed by foreign host.
[04/09/22]seed@VM:~\$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Apr 9 17:22:07 EDT 2022 from 10.0.2.4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
1 package can be updated.
0 updates are security updates.
[04/09/22]seed@VM:~\$ |

The right window (VM B) has a red border and displays:
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: ^CConnection closed by foreign host.
[04/09/22]seed@VM:~\$ telnet 10.0.2.4
Trying 10.0.2.4...
telnet: Unable to connect to remote host: No route to host
[04/09/22]seed@VM:~\$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Sat Apr 9 17:22:07 EDT 2022 from 10.0.2.4 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
1 package can be updated.
0 updates are security updates.
[04/09/22]seed@VM:~\$ |

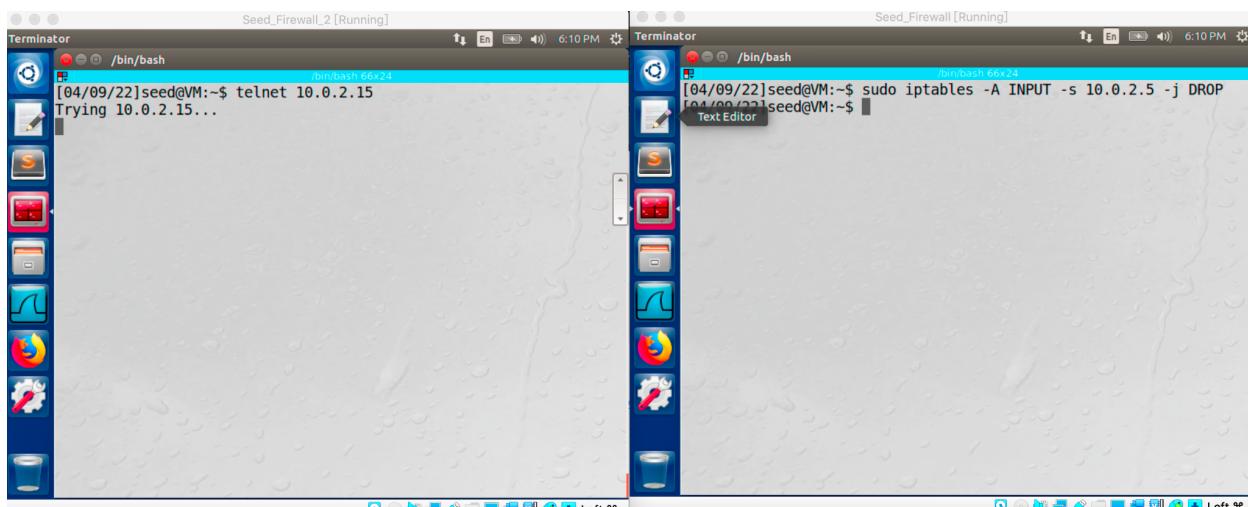
Prevent B from doing telnet to Machine A

- c. Based on the iptables firewall policy, it is used to prevent VM B (10.0.2.15) from doing telnet to VM A (10.0.2.5)



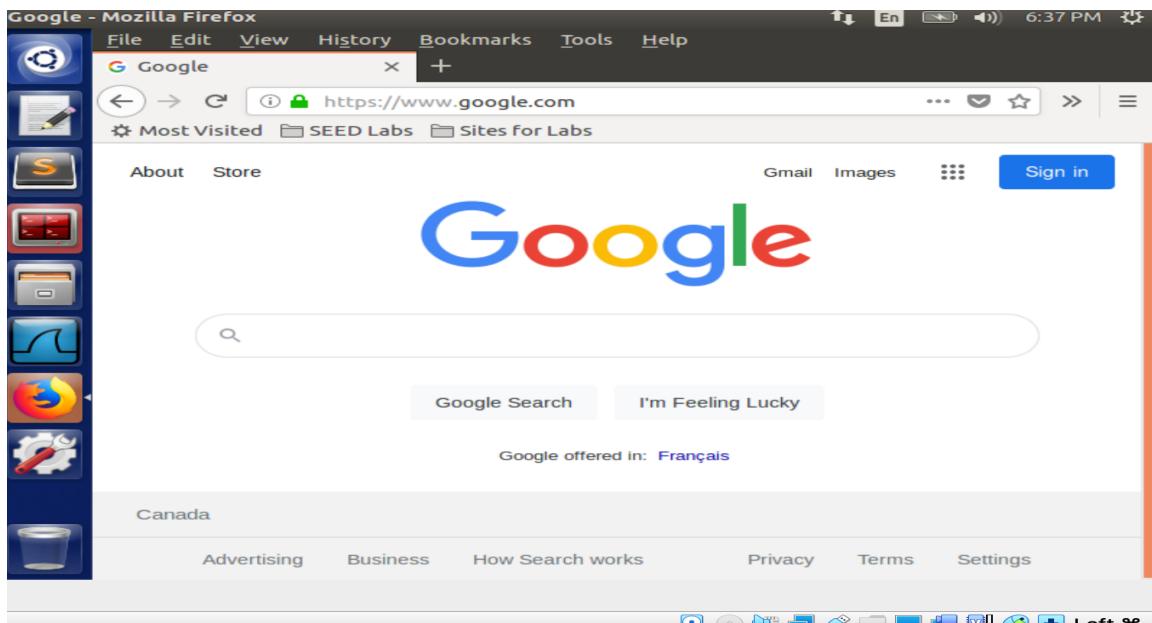
Prevent A from doing telnet to Machine B

- d. Based on the iptables firewall policy, it is used to prevent VM A (10.0.2.5) from doing telnet to VM B (10.0.2.15)

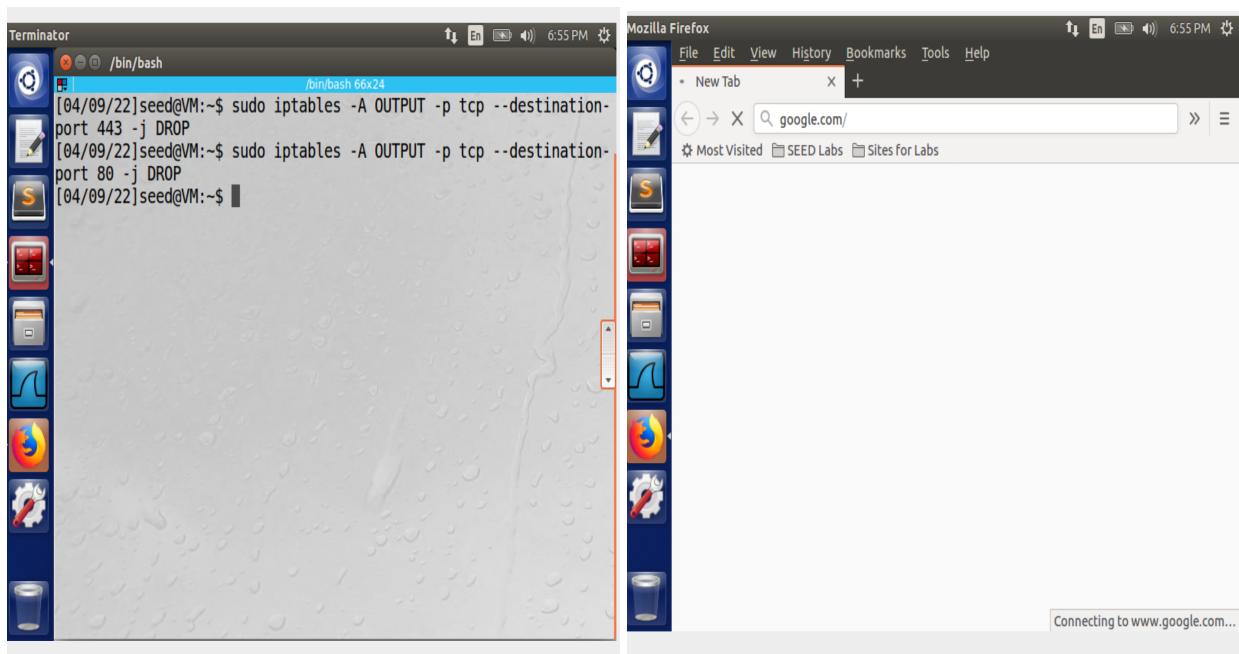


Prevent A from visiting an external website

e. On the VMA (10.0.2.15), it can access the google website without configuring the firewall policy.



f. If VM A (10.0.2.15) configures the iptables firewall policies in terms of the left screenshot, accessing the google website will be loading continually that means can not access.

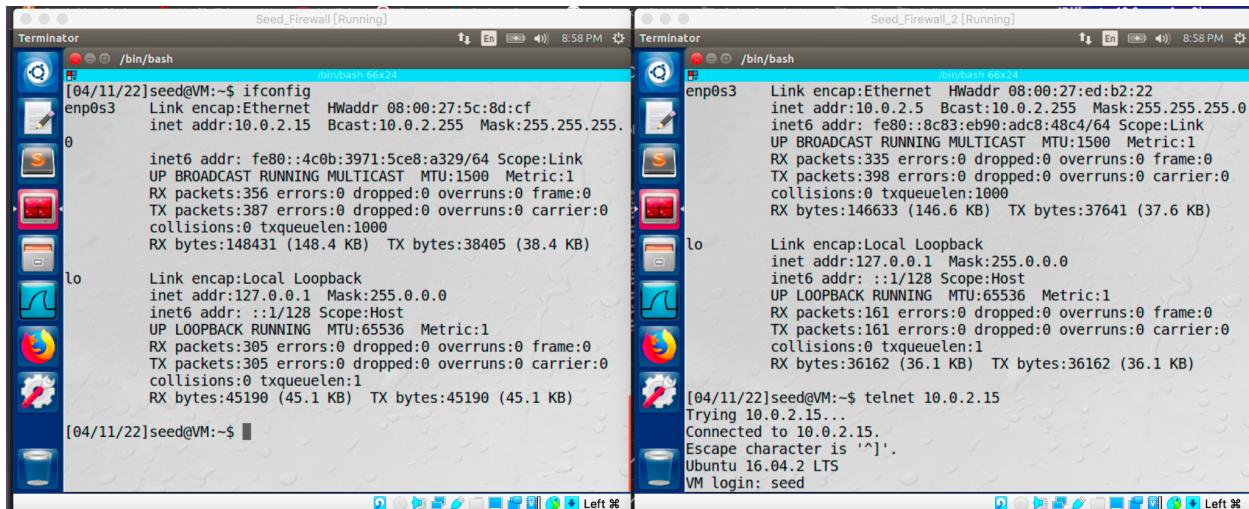


Task 3

Block all the outgoing traffic to external telnet servers

- VM A: 10.0.2.5
- VM B: 10.0.2.15

g. On the VM A (10.0.2.5) in the right screenshot, it can access VM B(10.0.2.15) via telnet without configuring the firewall policy.



The image shows two terminal windows side-by-side. Both are titled "Terminator" and have the command "/bin/bash" at the top. The left window is titled "Seed_Firewall [Running]" and the right one is "Seed_Firewall_2 [Running]". Both are running at 8:58 PM. The left window displays the output of the "ifconfig" command:

```
[04/11/22]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:5c:8d:cf
            inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
                        inet6 addr: fe80::4c0b:3971:5ce8:a329/64 Scope:Link
                        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                        RX packets:356 errors:0 dropped:0 overruns:0 frame:0
                        TX packets:387 errors:0 dropped:0 overruns:0 carrier:0
                        collisions:0 txqueuelen:1000
                        RX bytes:148431 (148.4 KB) TX bytes:38405 (38.4 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:305 errors:0 dropped:0 overruns:0 frame:0
            TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:45190 (45.1 KB) TX bytes:45190 (45.1 KB)

[04/11/22]seed@VM:~$
```

The right window displays the output of "ifconfig" and then a telnet session:

```
Link encap:Ethernet HWaddr 08:00:27:ed:b2:22
inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::8c83:eb90:adc8:48c4/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:335 errors:0 dropped:0 overruns:0 frame:0
TX packets:398 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:146633 (146.6 KB) TX bytes:37641 (37.6 KB)

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:161 errors:0 dropped:0 overruns:0 frame:0
TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:36162 (36.1 KB) TX bytes:36162 (36.1 KB)

[04/11/22]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^'.
Ubuntu 16.04.2 LTS
VM login: seed
```

h. After configuring the firewall policy which blocks outgoing packets to the external telnet, VM A (10.0.2.5) can not access VM B(10.0.2.15).

The image shows two terminal windows side-by-side. The left window, titled 'Seed_Firewall [Running]', displays the output of the 'ifconfig' command. It lists two interfaces: 'enp0s3' (Link encap:Ethernet, HWaddr 08:00:27:5c:8d:cf) and 'lo' (Link encap:Local Loopback). The right window, titled 'Seed_Firewall_2 [Running]', shows the results of running 'sudo iptables -A OUTPUT -d 10.0.2.15 -j DROP'. It includes error messages about bad arguments for 'save' and 'iptables -h' or '--help' for more information. It also shows the generated iptables-save command and its output.

```
[04/11/22]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:5c:8d:cf
            inet  addr:10.0.2.15   Bcast:10.0.2.255  Mask:255.255.255.
              brd 0
            inet6 addr: fe80::4c0b:3971:5ce8:a329/64  Scope:Link
                           UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
                           RX packets:356 errors:0 dropped:0 overruns:0 frame:0
                           TX packets:387 errors:0 dropped:0 overruns:0 carrier:0
                           collisions:0 txqueuelen:1000
                           RX bytes:148431 (148.4 KB)  TX bytes:38405 (38.4 KB)

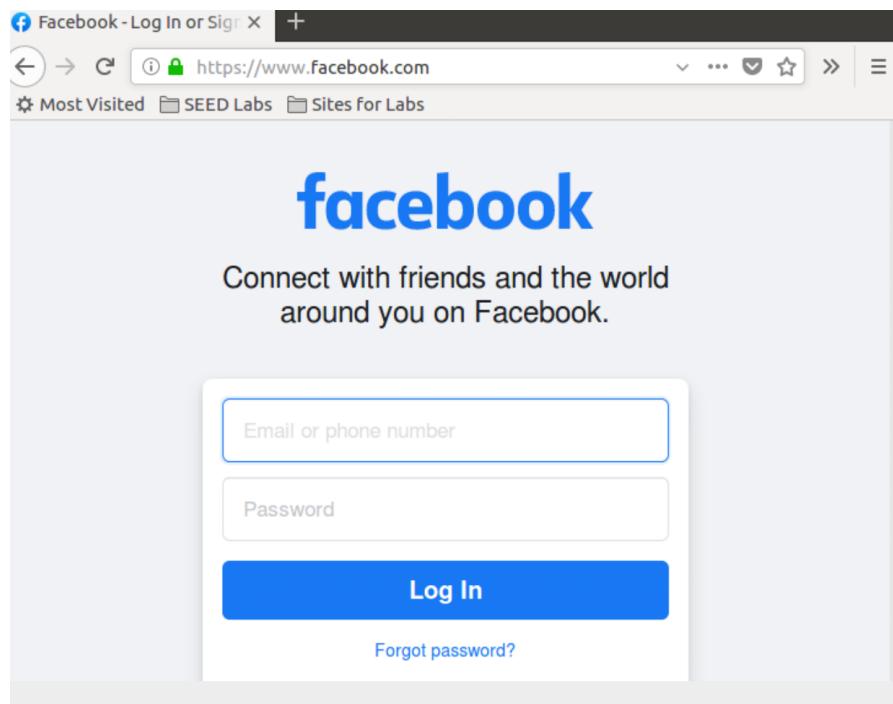
lo          Link encap:Local Loopback
            inet  addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
                           UP LOOPBACK RUNNING  MTU:65536 Metric:1
                           RX packets:305 errors:0 dropped:0 overruns:0 frame:0
                           TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
                           collisions:0 txqueuelen:1
                           RX bytes:45190 (45.1 KB)  TX bytes:45190 (45.1 KB)

[04/11/22]seed@VM:~$ 

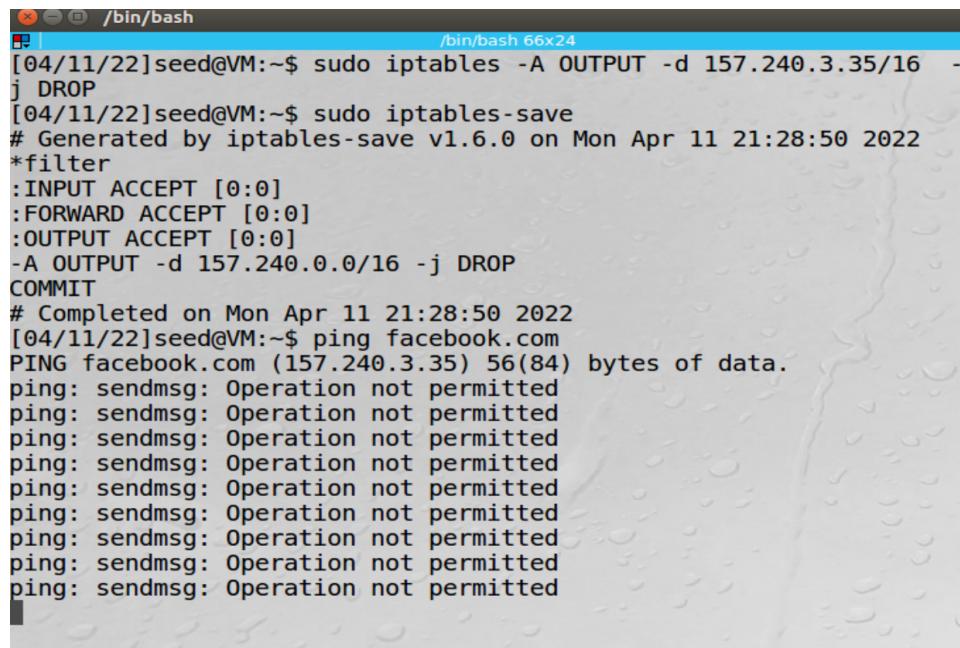
[04/11/22]seed@VM:~$ sudo iptables -A OUTPUT -d 10.0.2.15 -j DROP
[04/11/22]seed@VM:~$ sudo iptables save
Bad argument 'save'
Try 'iptables -h' or 'iptables --help' for more information.
[04/11/22]seed@VM:~$ sudo iptables-save
# Generated by iptables-save v1.6.0 on Mon Apr 11 21:02:31 2022
*filter
:INPUT ACCEPT [1:576]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1:328]
-A OUTPUT -d 10.0.2.15/32 -j DROP
COMMIT
# Completed on Mon Apr 11 21:02:31 2022
[04/11/22]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
```

Block all the outgoing traffic to www.facebook.com or Static IP like www.syr.edu

- VM A: 10.0.2.5
- VM B: 10.0.2.15
 - On VM A(10.0.2.5), it can access the normal Facebook page without blocking outgoing packets.*

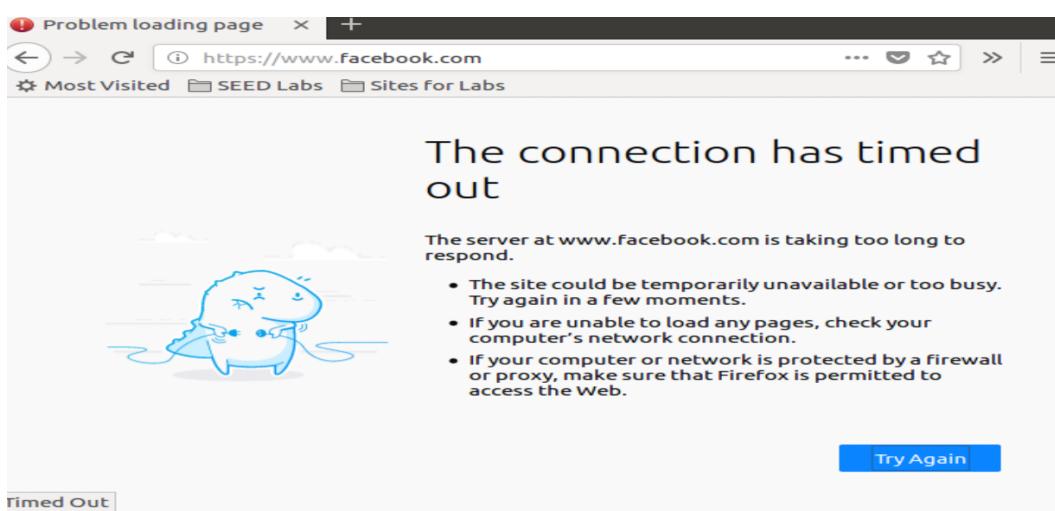


j. Find the Facebook IP via “dig” command, and then block the Facebook IP(157.240.3.35). Considering Facebook has many IP addresses, it can block with submask 16 (255.255.0.0) to ensure this can block all Facebook IP. After configuring the firewall policy, use “ping” to check the connection with facebook.com.

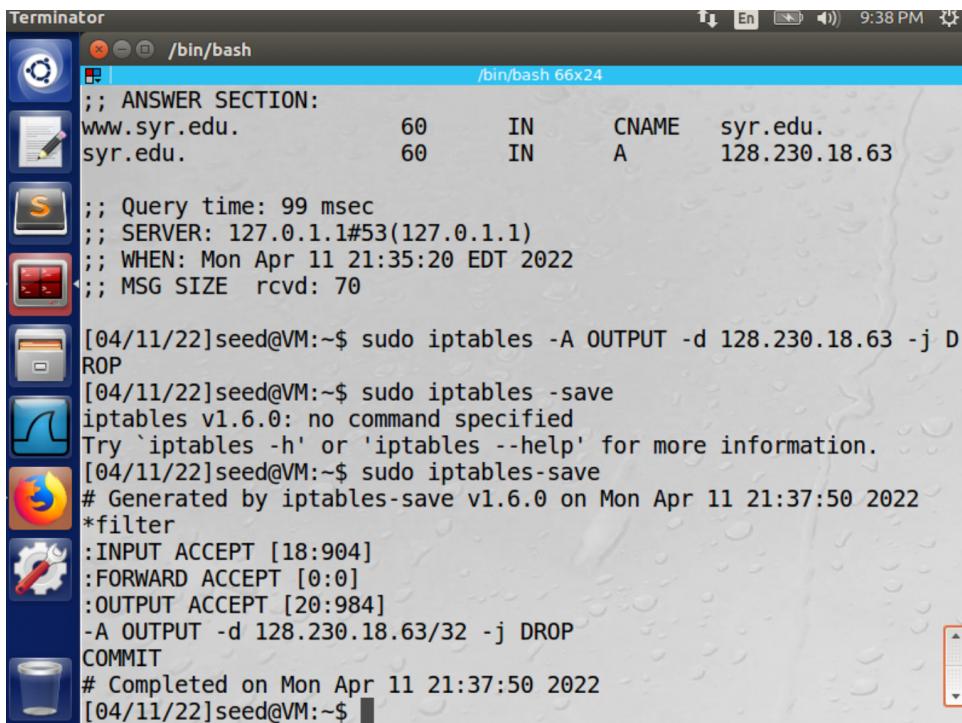


```
/bin/bash
[04/11/22]seed@VM:~$ sudo iptables -A OUTPUT -d 157.240.3.35/16 -j DROP
[04/11/22]seed@VM:~$ sudo iptables-save
# Generated by iptables-save v1.6.0 on Mon Apr 11 21:28:50 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A OUTPUT -d 157.240.0.0/16 -j DROP
COMMIT
# Completed on Mon Apr 11 21:28:50 2022
[04/11/22]seed@VM:~$ ping facebook.com
PING facebook.com (157.240.3.35) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
```

k. This below screenshot shows the firewall policy is configuring properly and VM can not access Facebook.



- l. From the lab description, the website www.syr.edu has a static IP (128.230.18.63), so we can also block this IP.*

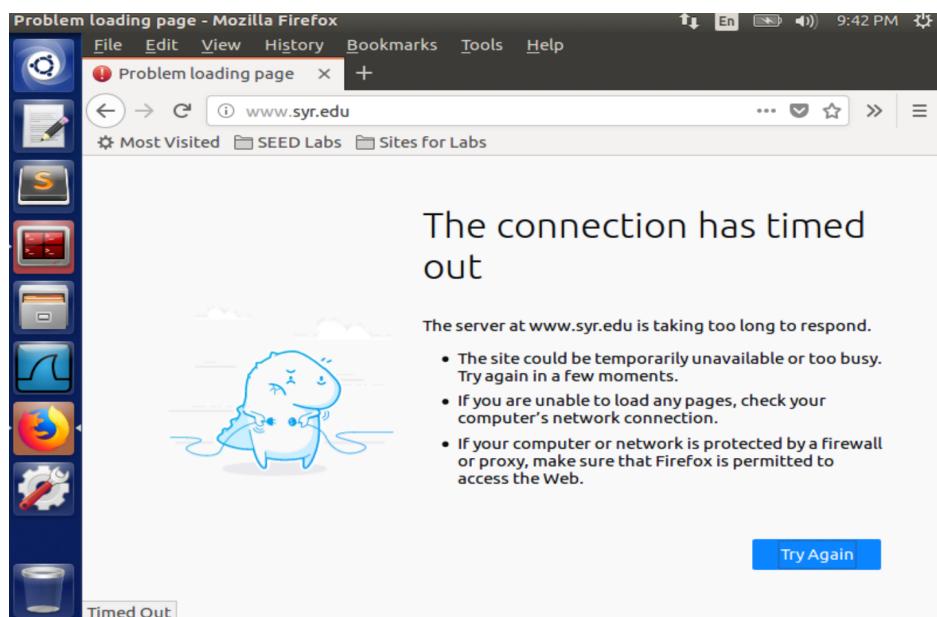


```
;; ANSWER SECTION:
www.syr.edu.          60      IN      CNAME   syr.edu.
syr.edu.              60      IN      A       128.230.18.63

;; Query time: 99 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Apr 11 21:35:20 EDT 2022
;; MSG SIZE  rcvd: 70

[04/11/22]seed@VM:~$ sudo iptables -A OUTPUT -d 128.230.18.63 -j DROP
[04/11/22]seed@VM:~$ sudo iptables -save
iptables v1.6.0: no command specified
Try `iptables -h' or `iptables --help' for more information.
[04/11/22]seed@VM:~$ sudo iptables-save
# Generated by iptables-save v1.6.0 on Mon Apr 11 21:37:50 2022
*filter
:INPUT ACCEPT [18:904]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [20:984]
-A OUTPUT -d 128.230.18.63/32 -j DROP
COMMIT
# Completed on Mon Apr 11 21:37:50 2022
[04/11/22]seed@VM:~$
```

- m. The below screenshot shows the firewall policy works successfully.*



Task 3a. Telnet to Machine B through the firewall

- VM A: 10.0.2.5
- VM B: 10.0.2.15

n. Considering it only has two virtual machines, VM B is used for the telnet and ssh server, and VM A is used to be a remote client.

The image shows two terminal windows side-by-side. The left window is titled '/bin/bash' and shows the command: [04/13/22]seed@VMA:~\$ ssh -L 7000:10.0.2.15:23 -f -N seed@10.0.2.15. It also displays the password entry and the telnet session starting at port 7000. The right window is titled 'ifconfig' and shows the network interface configuration for VM B. It lists 'enp0s3' (Link encap:Ethernet) and 'lo' (Link encap:Local Loopback). Both interfaces show their respective IP addresses (10.0.2.15 and 127.0.0.1).

o. After establishing an ssh tunnel, VM A(10.0.2.5) telnet VM B(10.0.2.15).

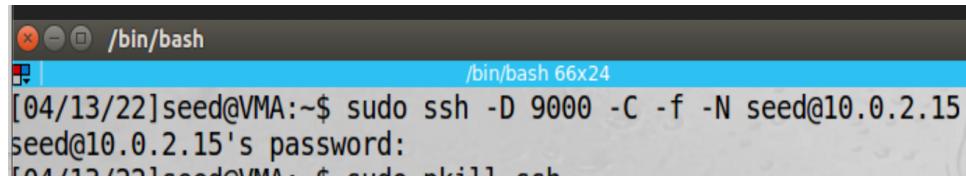
Using Wireshark captures the packet which can see the communication is use SSH protocol.

	Source	Destination	Protocol	Length
!-04-13 18:10:30.0734319...	10.0.2.5	10.0.2.15	SSH	158
!-04-13 18:10:30.0740350...	10.0.2.15	10.0.2.5	TCP	66
!-04-13 18:10:30.0742109...	10.0.2.15	10.0.2.5	SSH	110

Task 3b. Connect to Facebook using SSH Tunnel

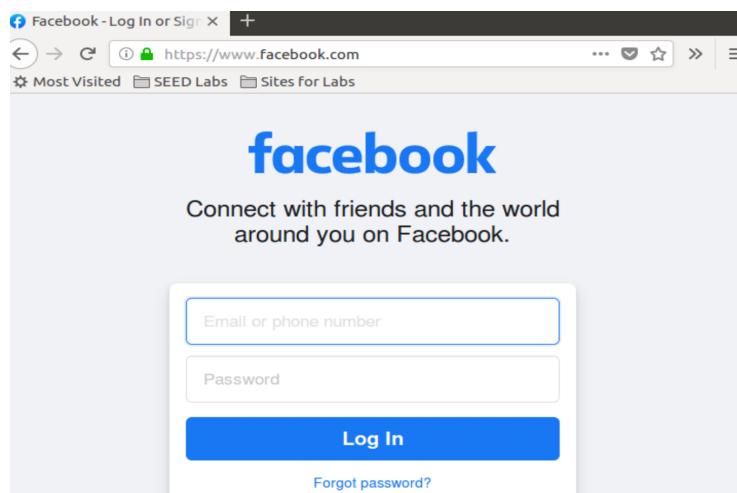
- VM A: 10.0.2.5
- VM B: 10.0.2.15
- Configure ssh dynamic port forwarding and socks proxy in the browser

- p. Establish an ssh tunnel between VMA and VMB, which can use this tunnel to forward packets.*

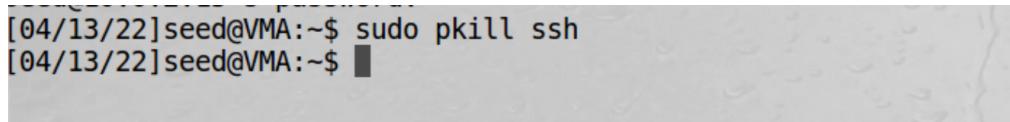


A screenshot of a terminal window titled '/bin/bash'. The window shows a command being run: 'sudo ssh -D 9000 -C -f -N seed@10.0.2.15'. Below the command, it asks for 'seed@10.0.2.15's password:'. The terminal window has a dark background with light-colored text.

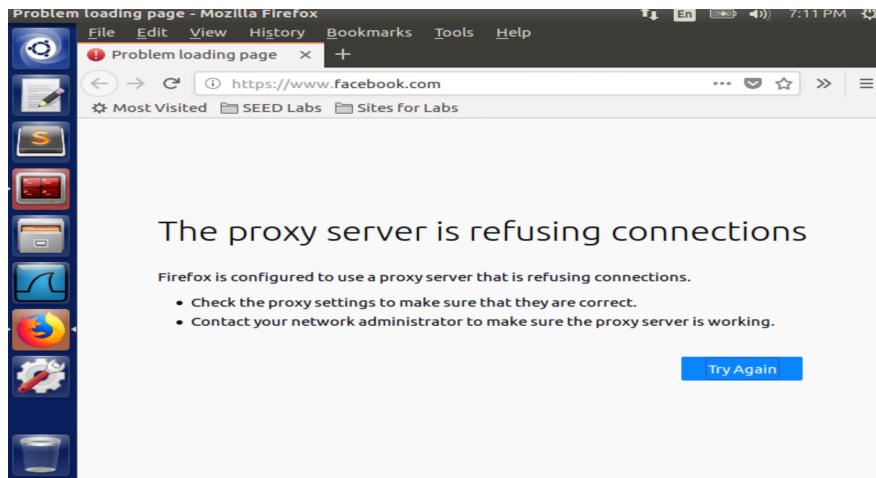
- Run Firefox and go visit the Facebook page
- q. Access successfully*



- Break the SSH tunnel, clear the Firefox cache, and try the connection again
- r. Using "pkill" command to kill all ssh sessions, and then accessing the Facebook page will be refused by the proxy server (127.0.0.1:9000).*



A screenshot of a terminal window showing the command 'sudo pkill ssh' being run. The terminal window has a dark background with light-colored text.



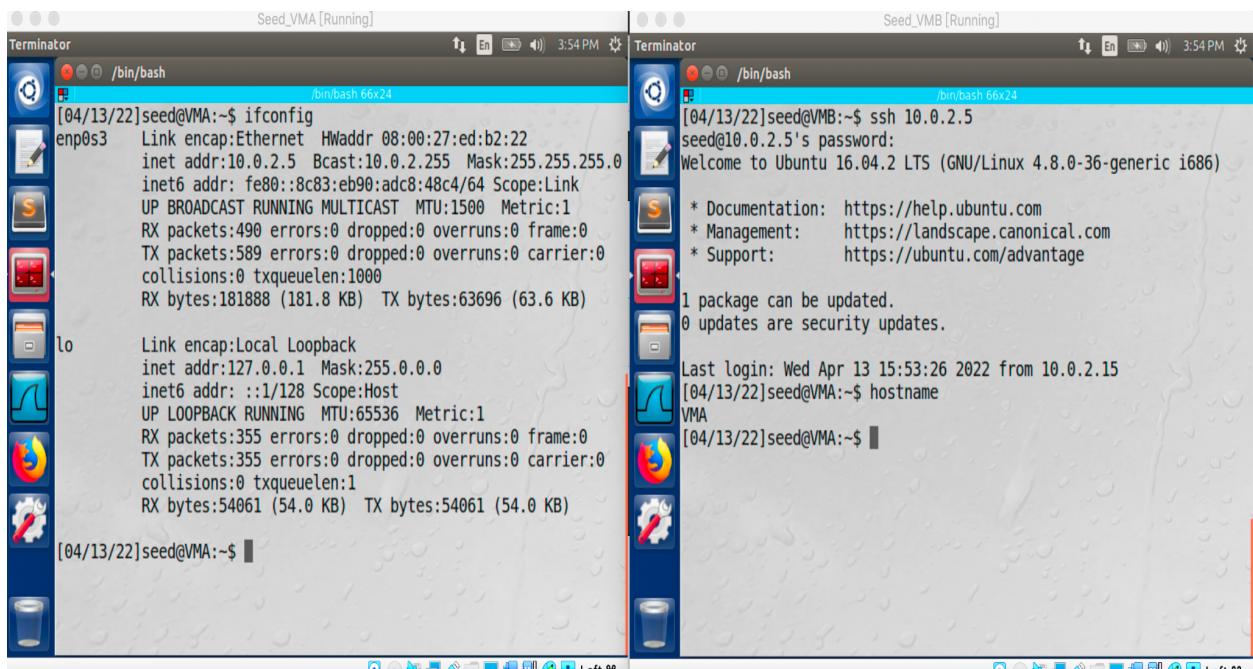
- Establish the SSH tunnel again and connect to Facebook
 - s. Reconnect the ssh session to VM B(10.0.2.15); facebook.com can be accessed.
- Explain why the SSH tunnel can help bypass the egress filtering and capture the packets with Wireshark.
 - t. Facebook Public IP (157.240.22.35).
 - u. Remote side: VM A (10.0.2.5) firstly connect to VM B (10.0.2.15) via an ssh tunnel, and then VM B will forward the packet to the Facebook page establishing TCP 3 ways handshake.

10.0.2.5	10.0.2.15	SSH	110 Client: Encrypted packet (le
10.0.2.15	157.240.22.35	TCP	74 58628 → 443 [SYN] Seq=275391
10.0.2.15	10.0.2.5	TCP	66 22 → 41288 [ACK] Seq=1450762
157.240.22.35	10.0.2.15	TCP	60 443 → 58628 [SYN, ACK] Seq=1
10.0.2.15	157.240.22.35	TCP	60 58628 → 443 [ACK] Seq=275391
10.0.2.15	10.0.2.5	SSH	102 Server: Encrypted packet (le
10.0.2.5	10.0.2.15	TCP	66 41288 → 22 [ACK] Seq=1030764
10.0.2.5	10.0.2.15	SSH	286 Client: Encrypted packet (le
10.0.2.15	10.0.2.5	TCP	66 22 → 41288 [ACK] Seq=1450762

Task 4:

Reverse SSH tunnel

- The goal of this task is to set up a reverse SSH tunnel on VM A that is protected by the firewall. VM A configures firewall policy with blocking ports 22 and 80. And, this VM A is accessible from the outside VM B.
 - VM A: 10.0.2.5
 - VM B: 10.0.2.15
- v. *Without configuring blocking ports 80,22 and establishing an ssh reverse tunnel, VM B can ssh to VM A.*



- w. *Blocking ports 80,22 and establishing an ssh reverse tunnel on VMA, which allows VMB ssh to VMA.*

The image shows two terminal windows side-by-side. The left window, titled 'Seed_VMA [Running]', displays network interface statistics for 'enp0s3' and 'lo'. The right window, also titled 'Seed_VMA [Running]', shows an SSH session from 'VMB' to 'VMA' on port 8000, with a warning about host authenticity.

```

Terminal /bin/bash /bin/bash 73x27
enp0s3 Link encap:Ethernet HWaddr 08:00:27:ed:b2:22
          inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::8c83:eb90:adcb:48c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1878 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2090 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:398166 (398.1 KB) TX bytes:269924 (269.9 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:687 errors:0 dropped:0 overruns:0 frame:0
      TX packets:687 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1
      RX bytes:78571 (78.5 KB) TX bytes:78571 (78.5 KB)

[04/13/22]seed@VMA:~$ sudo iptables -A INPUT -p tcp -s 10.0.2.15 --dport 22 -j DROP
[04/13/22]seed@VMA:~$ sudo iptables -A INPUT -p tcp -s 10.0.2.15 --dport 80 -j DROP
[04/13/22]seed@VMA:~$ sudo ssh -R 8000:10.0.2.5:22 -f -N seed@10.0.2.15
seed@10.0.2.15's password:
[04/13/22]seed@VMA:~$ Warning: remote port forwarding failed for listen port 8000

Terminal /bin/bash /bin/bash 66x24
[04/13/22]seed@VMB:~$ ssh 10.0.2.5
^C
[04/13/22]seed@VMB:~$ ssh localhost -p 8000
The authenticity of host '[localhost]:8000 ([127.0.0.1]:8000)' can't be established.
ECDSA key fingerprint is SHA256:p1zAio6c1bI+8HDp5xa+eKRi561aFDaPE1/xqleYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:8000' (ECDSA) to the list of known hosts.
seed@localhost's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

Last login: Wed Apr 13 16:53:56 2022 from 10.0.2.5
[04/13/22]seed@VMA:~$ hostname
VMA
[04/13/22]seed@VMA:~$ 

```

Based on the configuration, the below architecture shows how does the ssh reverse tunnel work.

