COMP8006 Assignment 1

Linux Firewalls

Kevin Lo, A00952922

2-3-2021

Table of Contents

1 Introduction

This assignment was test on how to use iptables rules to allow or drop packets depending on if they fulfill the conditions in the ruleset in the iptables. The rules used are made to the specifications of COMP 8006 Assignment 1 specifications. Instructions on how to setup the firewall and the internal host's routing

2 How to Use

The following section teaches how to use the Bash scripts provided with this report to apply the same iptables ruleset used in this report.

2.1 Physical Requirements

Two different machines are required to perform this test, one machine as the firewall, and the other machine as the internal host. One more machine may be used to test the traffic going from external to internal network.

My current setup is:

- **Firewall** (External 192.168.1.250[wlp2s0], Internal 192.168.2.1[enp0s20f0u1])
- **Internal Host** (192.168.2.2[eth0])

2.2 Operating System

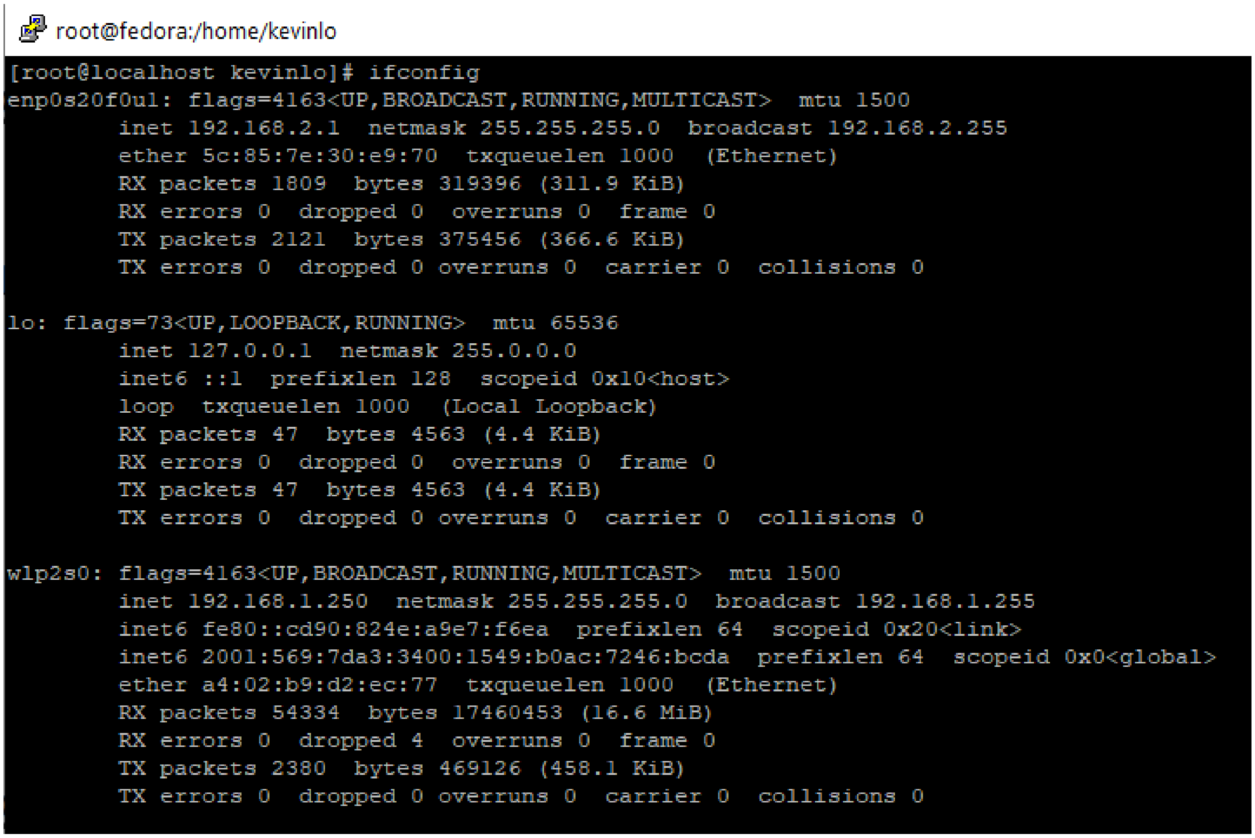
The two machines should be running a variant of Linux. In my case my firewall runs on Fedora and the internal host runs on Raspbian

2.3 Setting up the Routing Configurations

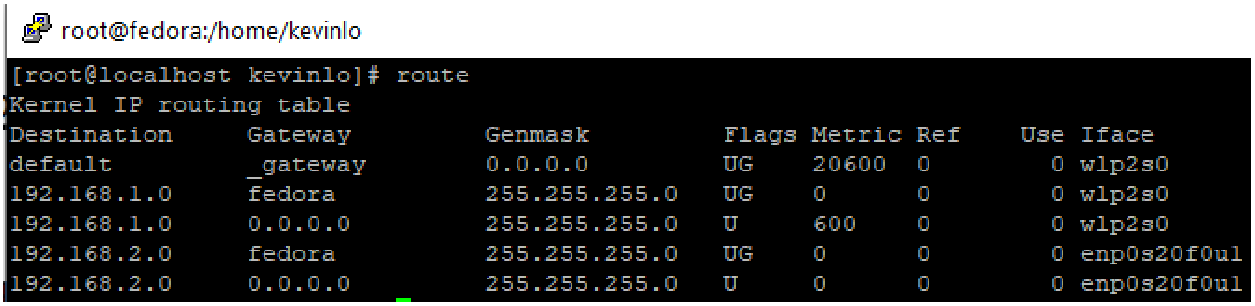
There are two scripts provided for setting up the basic routing configuration for both the firewall and internal host. Sometimes the routing configurations may reset by itself so you may need to run the script multiple times.

2.3.1 Firewall Routing

Run the **firewallsetup.sh** script on your firewall and the **ifconfig** and **route** command outputs should look like the following.



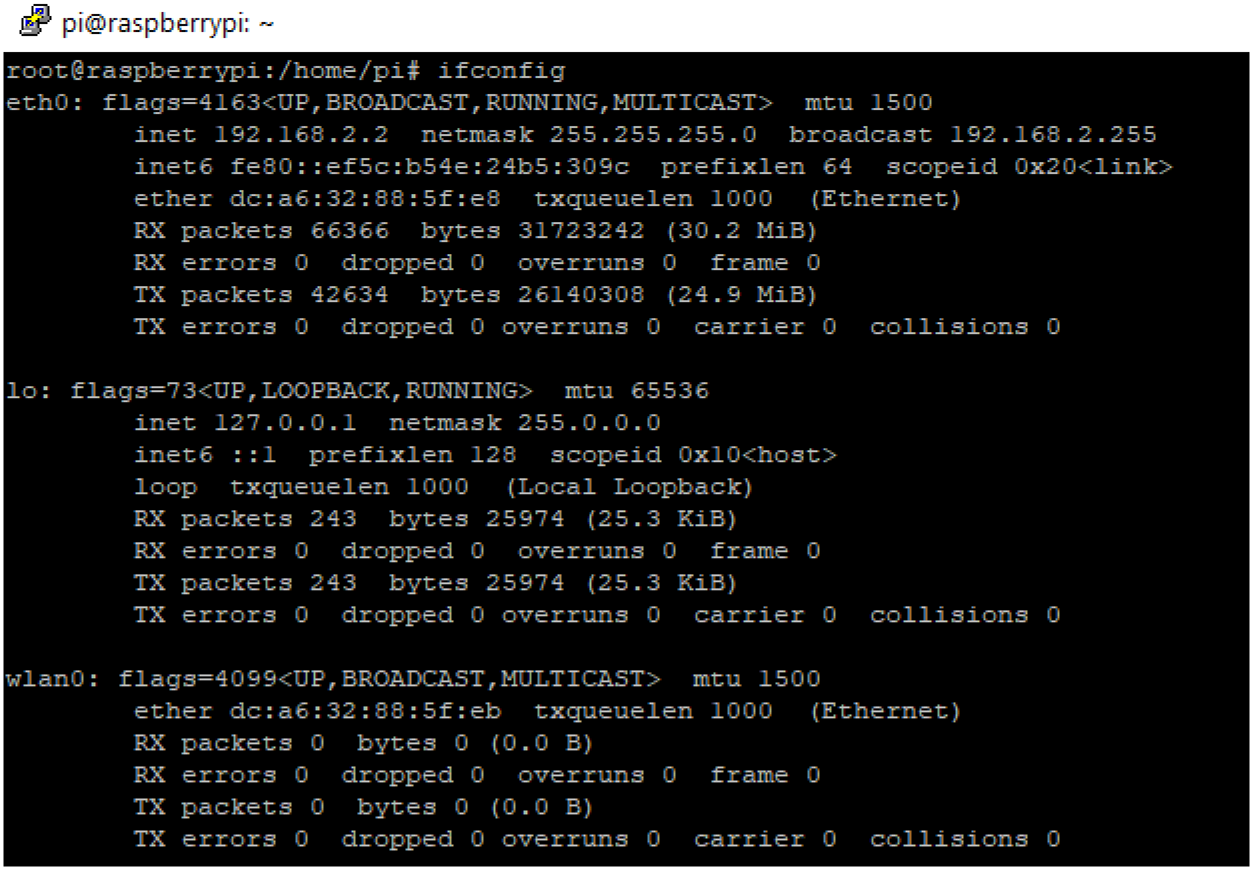
```
[root@localhost kevinlo]# ifconfig
enp0s20f0u1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.1  netmask 255.255.255.0  broadcast 192.168.2.255
        ether 5c:85:7e:30:e9:70  txqueuelen 1000  (Ethernet)
        RX packets 1809  bytes 319396 (311.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2121  bytes 375456 (366.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 47  bytes 4563 (4.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 4563 (4.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.250  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::cd90:824e:a9e7:f6ea  prefixlen 64  scopeid 0x20<link>
        inet6 2001:569:7da3:3400:1549:b0ac:7246:bcda  prefixlen 64  scopeid 0x0<global>
        ether a4:02:b9:d2:ec:77  txqueuelen 1000  (Ethernet)
        RX packets 54334  bytes 17460453 (16.6 MiB)
        RX errors 0  dropped 4  overruns 0  frame 0
        TX packets 2380  bytes 469126 (458.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
[root@localhost kevinlo]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    20600  0        0 wlp2s0
192.168.1.0     fedora          255.255.255.0   UG    0      0        0 wlp2s0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp2s0
192.168.2.0     fedora          255.255.255.0   UG    0      0        0 enp0s20f0u1
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s20f0u1
```

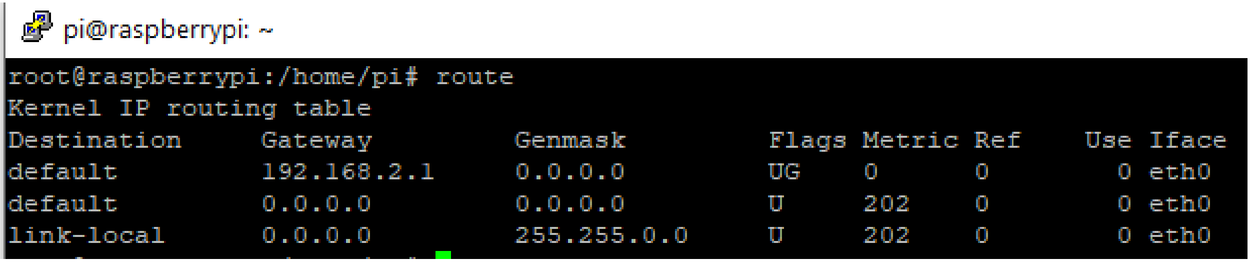
2.3.1 Internal Host Routing

Run the **internalhostsetup.sh** script on your firewall and the **ifconfig** and **route** command outputs should look like the following.



pi@raspberrypi: ~

```
root@raspberrypi:/home/pi# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.2  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::ef5c:b54e:24b5:309c  prefixlen 64  scopeid 0x20<link>
        ether dc:a6:32:88:5f:e8  txqueuelen 1000  (Ethernet)
        RX packets 66366  bytes 31723242 (30.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42634  bytes 26140308 (24.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 243  bytes 25974 (25.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 243  bytes 25974 (25.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether dc:a6:32:88:5f:eb  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



pi@raspberrypi: ~

```
root@raspberrypi:/home/pi# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.2.1     0.0.0.0         UG    0      0        0 eth0
default         0.0.0.0         0.0.0.0         U     202    0        0 eth0
link-local      0.0.0.0         255.255.0.0     U     202    0        0 eth0
```

2.4 Add iptables Rules using User Defined Variables

This section will detail what variable in the user defined variable section is.

2.4.1 Firewall Configuration File

The file used by the firewall for the user defined configuration is called **FWrules.sh**

- **NIC_INTERNAL_NAME:** The name of the network card connected to the internal network (ex. enp0s20f0u1)

- **IP_INTERNAL:** The IP address of the network card connected to the internal network (ex. 192.168.2.1)

- **IP_INTERNAL_HOST:** The IP address of the internal host to forward packets to from external network (ex. 192.168.2.2)

- **IP_INTERNAL_NETWORK:** The address space of the internal network (ex. 192.168.2.0/24)

- **NIC_EXTERNAL_NAME:** The name of the network card connected to the external network (ex. wlp2s0)

- **IP_EXTERNAL:** The IP address of the network card connected to the external network (ex. 192.168.1.250)

- **IP_EXTERNAL_NETWORK:** The address space of the external network (ex. 0.0.0.0/0)

- **ALLOWED_TCP_PORT_RANGE:** The user defined configuration for allowed TCP ports (ex. 53,21,20)

- **ALLOWED_UDP_PORT_RANGE:** The user defined configuration for allowed TCP ports (ex. 53,21)

- **ALLOWED_ICMP_TYPES:** The user defined configuration for allowed ICMP type numbers (ex. [8,0])

- **DEMO_SSH_FIREWALL**: Configuration that opens the INPUT and OUTPUT to allow SSH access into the firewall from the internal network, this will be used for recording the video of the network activity on the firewall, should normally be disabled when using it as a commercial firewall (ex. false)

2.4.2 Firewall Base Configuration

The firewall by default will allow inbound and outbound connections for SSH, HTTP, HTTPS and drop packets coming from wrong ports, spoofed outside IP addresses mimicking addresses from the internal network, SYN packets going to high ports, packets containing both SYN and FIN flags and, all telnet packets.

3 Testing Details

This section details the testing methods to meet the requirements of the assignment.

3.1 Computers

I use three different computers for the testing, all three machines are running a variant of Linux.

-**External Host** (Fedora) (IP: 192.168.1.251)

-**Internal Host** (Raspbian) (IP: 192.168.1.251)

-**Firewall** (Fedora) (external IP: 192.168.1.250[wlp2s0], internal IP: 192.168.2.1[enp0s20f0u1])

For this assignment, outbound connections are going from the internal network into the external network. Inbound connections are going from the external network into the internal network.

4 Tests

The following table details the tests used to verify the capabilities of my iptables configuration.

Outbound: Is internal network traffic going out the external network

Inbound: Is external network traffic going into the internal network

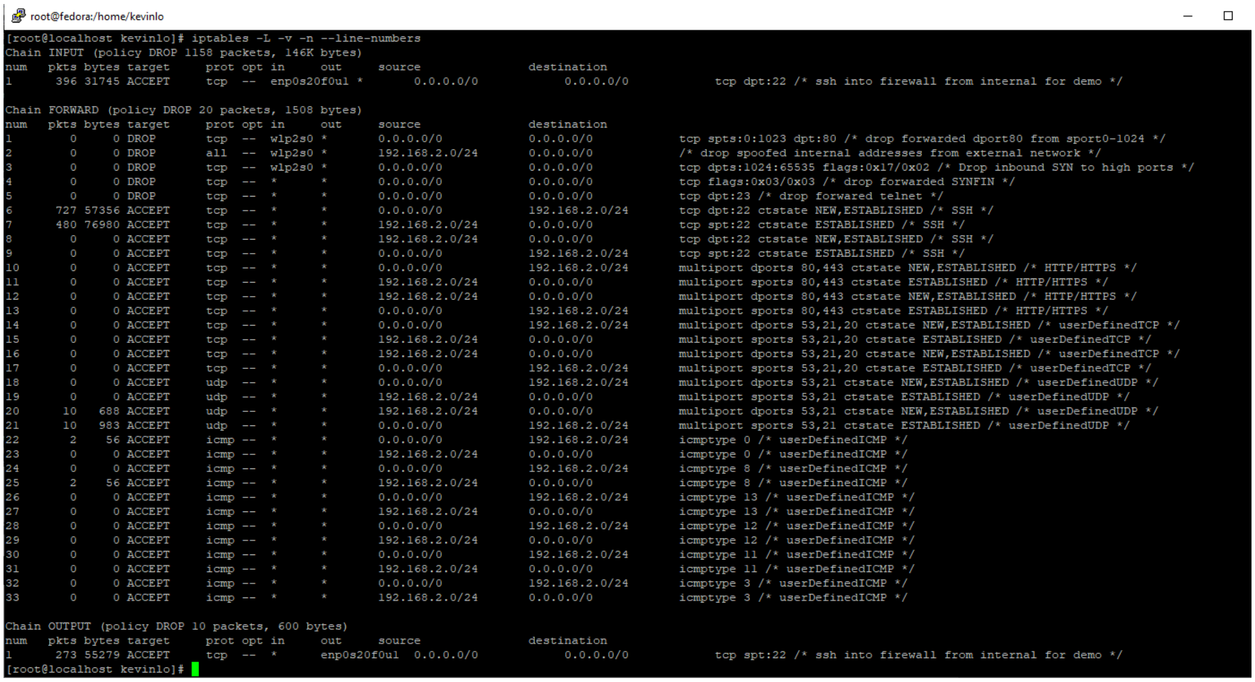
General: Generally, for rules that are one command and apply to both internal and external such as dropping all telnet

Rule #	Test Description	Tool Used	Expected Result	Pass/Fail
1 (Outbound)	Accept outbound TCP packets from dport 22	hping3	The firewall should allow TCP the packets from internal host to reach the external host on dport 22 as it is part of the default requirements.	Pass. Detailed results attached.
2 (Outbound)	Accept outbound TCP packets from dport 80	hping3	The firewall should allow TCP the packets from internal host to reach the external host on dport 80 as it is part of the default requirements.	Pass. Detailed results attached.
3 (Outbound)	Accept outbound TCP packets from dport 53	hping3	The firewall should allow the TCP packets from internal host to reach the external host on dport 53 as it is on the **ALLOWED_TCP_PORT_RANGE**	Pass. Detailed results attached.
4 (Outbound)	Accept outbound UDP packets from dport 53	hping3	The firewall should allow the UDP packets from internal host to reach the external host on dport 53 as it is on the **ALLOWED_UDP_PORT_RANGE**	Pass. Detailed results attached.
5 (Outbound)	Accept outbound ICMP packets type 0,8	hping3	The firewall should allow the ICMP packets from internal host to reach the external host as it is on the **ALLOWED_ ICMP_TYPES**	Pass. Detailed results attached.
1 (Inbound)	Accept outbound TCP packets from dport 22	hping3	The firewall should allow TCP the packets from external host to reach the internal host on dport 22 as it is part of the default requirements.	Pass. Detailed results attached.
2 (Inbound)	Accept outbound TCP packets from dport 80	hping3	The firewall should allow TCP the packets from external host to reach the internal host on dport 80 as it is part of the default requirements.	Pass. Detailed results attached.
3 (Inbound)	Accept outbound TCP packets from dport 53	hping3	The firewall should allow the TCP packets from external host to reach the internal host on dport 53 as it is on the **ALLOWED_TCP_PORT_RANGE**	Pass. Detailed results attached.
4 (Inbound)	Accept outbound UDP packets from dport 53	hping3	The firewall should allow the UDP packets from external host to reach the external host on dport 53 as it is on the **ALLOWED_UDP_PORT_RANGE**	Pass. Detailed results attached.
5 (Inbound)	Accept outbound ICMP packets type 0,8	hping3	The firewall should allow the ICMP packets from external host to reach the internal host as it is on the **ALLOWED_ICMP_TYPES**	Pass. Detailed results attached.
6 (Inbound)	Drop packets from sport 0 to 1023 going to dport 80	hping3	The firewall should drop the packets from external host as it is part of the default requirements to not allow wrong way traffic.	Pass. Detailed results attached.

7 (Inbound)	Drop packets with src address of internal network but coming from the external NIC	hping3	The firewall should drop the packets from external host as it is part of the default requirements to drop packets coming from spoofed outside addresses mimicking the internal network addresses.	Pass. Detailed results attached.
8 (Inbound)	Drop SYN packets going to dport 1024 to 65535 coming from the external NIC	hping3	The firewall should drop the packets from external host as it is part of the default requirements to drop packets going to dport 1024 to 65535 coming from the external NIC	Pass. Detailed results attached.
9 (General)	Drop TCP packets with the SYN,FIN TCP flags	hping3	The firewall should drop any packet containing the SYN,FIN TCP flags as it is part of the default requirements to prevent SYN,FIN flood	Pass. Detailed results attached.
10 (General)	Drop all TCP port 23 telnet packets	hping3	The firewall should drop all TCP port 23 used by telnet	Pass. Detailed results attached.
11 (General)	FTP and SSH to have “Minimum Delay” and FTP to have “Maximum Throughput” flags set	iptables -t mangle -L -v -n	There should be packet activity in the iptables -t mangle table to show that packets are being affected by the rule	Pass. Detailed results attached.
12 (General)	Verify the ports opened match up to the ports opened stated by the config	nmap	The result from nmap should match up with the TCP ports open on the firewall	Pass. Detailed results attached.

4.1 Test Results

Base iptables Table

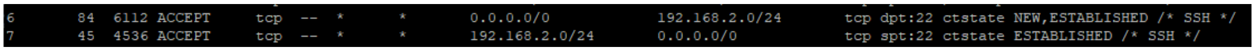


```
[root@localhost kevinlo]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 1158 packets, 146K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      396 31745 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 20 packets, 1508 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6      727 57356 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      480 76980 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20      10   688 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21      10   983 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       2    56 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       2    56 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 10 packets, 600 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      273 55279 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost kevinlo]#
```

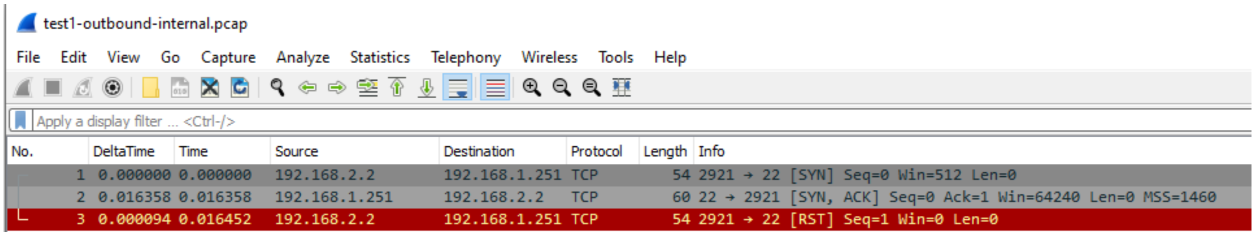
This is the configuration of the iptables output with the default settings and provided **FWconf.sh** configuration.

4.1.1 Test 1 – Outbound TCP dport 22 (SSH)

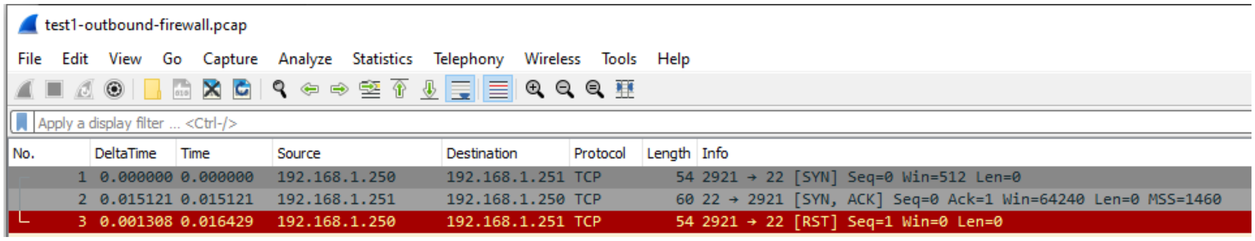
Firewall Lines (FORWARD chain)



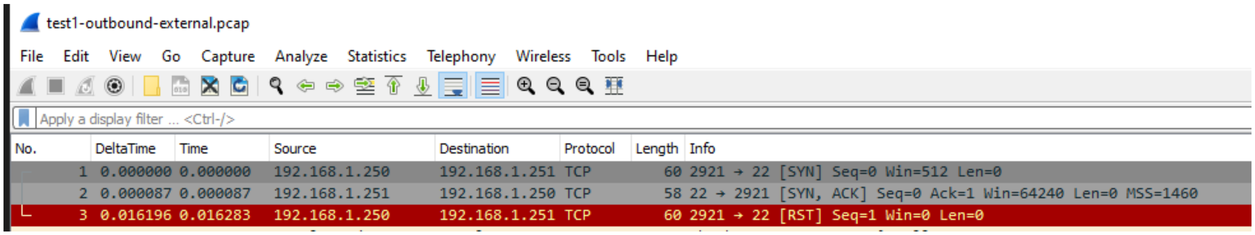
```
6       84  6112 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       45  4536 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
```



No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.2.2	192.168.1.251	TCP	54	2921 → 22 [SYN] Seq=0 Win=512 Len=0
2	0.016358	0.016358	192.168.1.251	192.168.2.2	TCP	60	22 → 2921 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000094	0.016452	192.168.2.2	192.168.1.251	TCP	54	2921 → 22 [RST] Seq=1 Win=0 Len=0



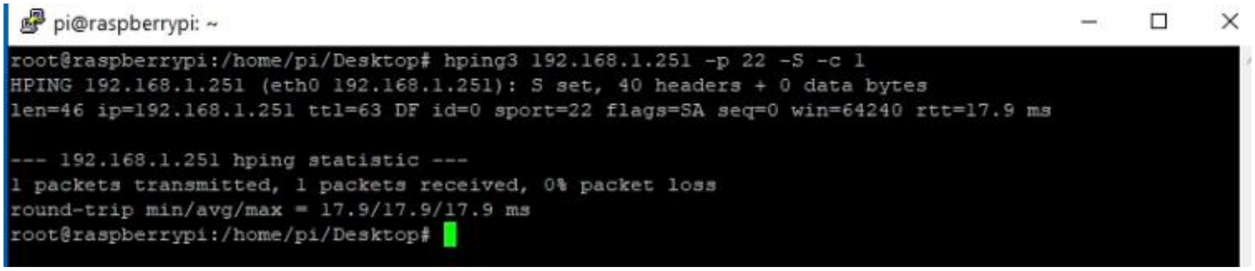
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.250	192.168.1.251	TCP	54	2921 → 22 [SYN] Seq=0 Win=512 Len=0
2	0.015121	0.015121	192.168.1.251	192.168.1.250	TCP	60	22 → 2921 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.001308	0.016429	192.168.1.250	192.168.1.251	TCP	54	2921 → 22 [RST] Seq=1 Win=0 Len=0



test1-outbound-external.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time      Source         Destination    Protocol Length Info
   1 0.000000 0.000000  192.168.1.250  192.168.1.251  TCP      60 2921 → 22 [SYN] Seq=0 Win=512 Len=0
   2 0.000087 0.000087  192.168.1.251  192.168.1.250  TCP      58 22 → 2921 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   3 0.016196 0.016283  192.168.1.250  192.168.1.251  TCP      60 2921 → 22 [RST] Seq=1 Win=0 Len=0
```



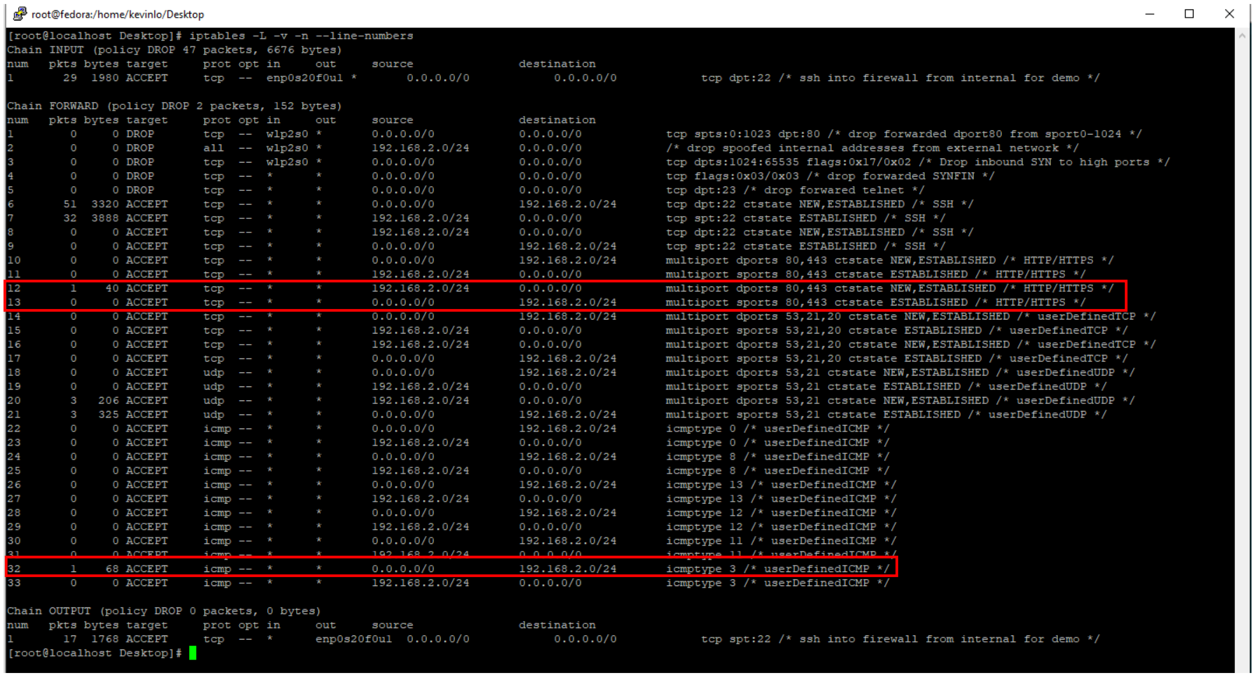
pi@raspberrypi: ~

```
root@raspberrypi:/home/pi/Desktop# hping3 192.168.1.251 -p 22 -S -c 1
HPING 192.168.1.251 (eth0 192.168.1.251): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.251 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=17.9 ms

--- 192.168.1.251 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 17.9/17.9/17.9 ms
root@raspberrypi:/home/pi/Desktop#
```

The following packet captures shows that the packet from internal network TCP dport 22 was able to successfully reach the external network and receive a response back.

4.1.2 Test 2 – Outbound TCP dport 80 (HTTP)

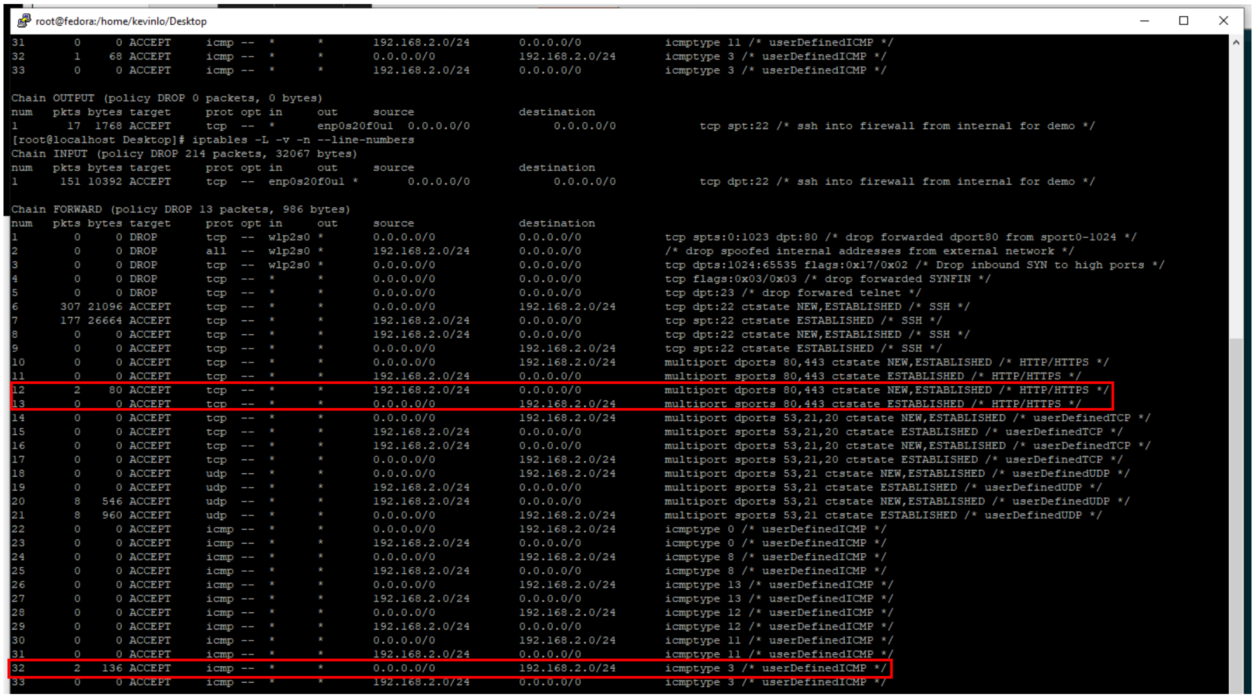
Firewall Lines (FORWARD chain)



root@fedora:/home/kevinlo/Desktop

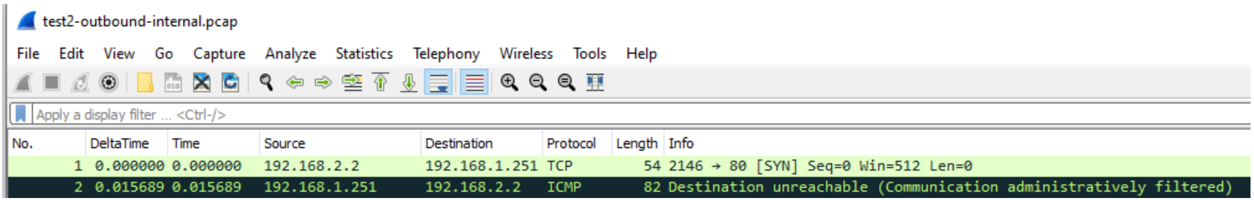
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 47 packets, 6676 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       29  1980 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 2 packets, 152 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6       51  3320 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       32  3888 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       1    40 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       3   206 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       3   325 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       1    68 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       17  1768 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After



root@fedora:/home/kevinlo/Desktop

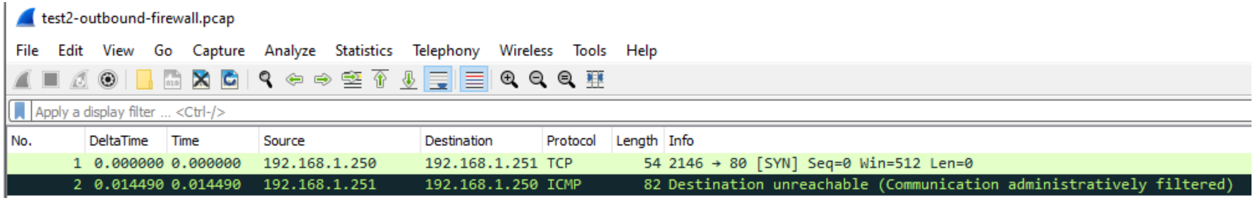
```
31      0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32      1    68 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33      0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       17  1768 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 214 packets, 32067 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      151 10392 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 13 packets, 986 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6      307 21096 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      177 26664 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       2    80 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       8   546 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       8   960 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       2   136 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */
```



test2-outbound-internal.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

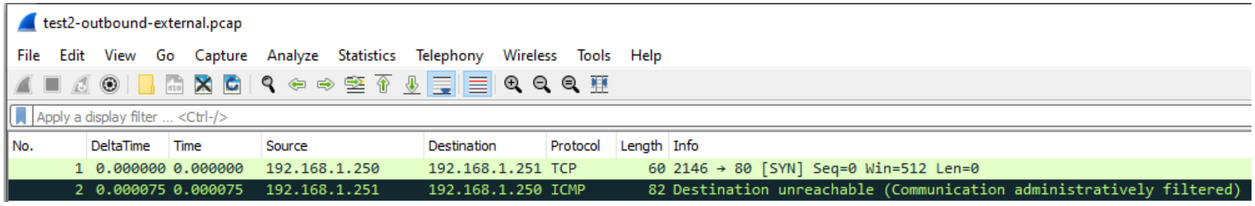
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.2.2	192.168.1.251	TCP	54	2146 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.015689	0.015689	192.168.1.251	192.168.2.2	ICMP	82	Destination unreachable (Communication administratively filtered)



test2-outbound-firewall.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

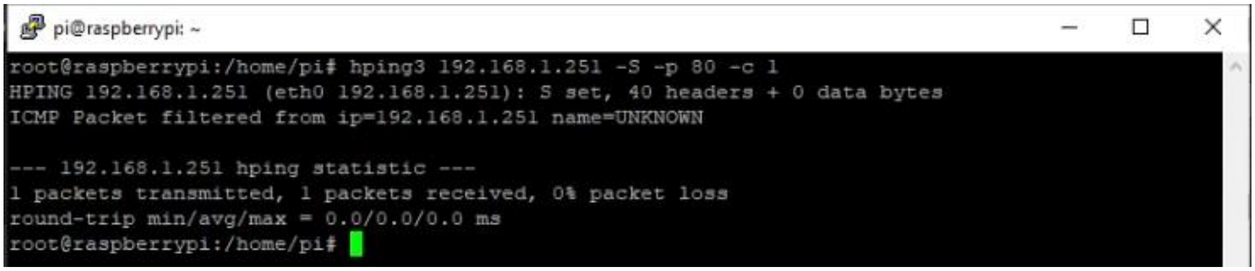
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.250	192.168.1.251	TCP	54	2146 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.014490	0.014490	192.168.1.251	192.168.1.250	ICMP	82	Destination unreachable (Communication administratively filtered)



test2-outbound-external.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.250	192.168.1.251	TCP	60	2146 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.000075	0.000075	192.168.1.251	192.168.1.250	ICMP	82	Destination unreachable (Communication administratively filtered)



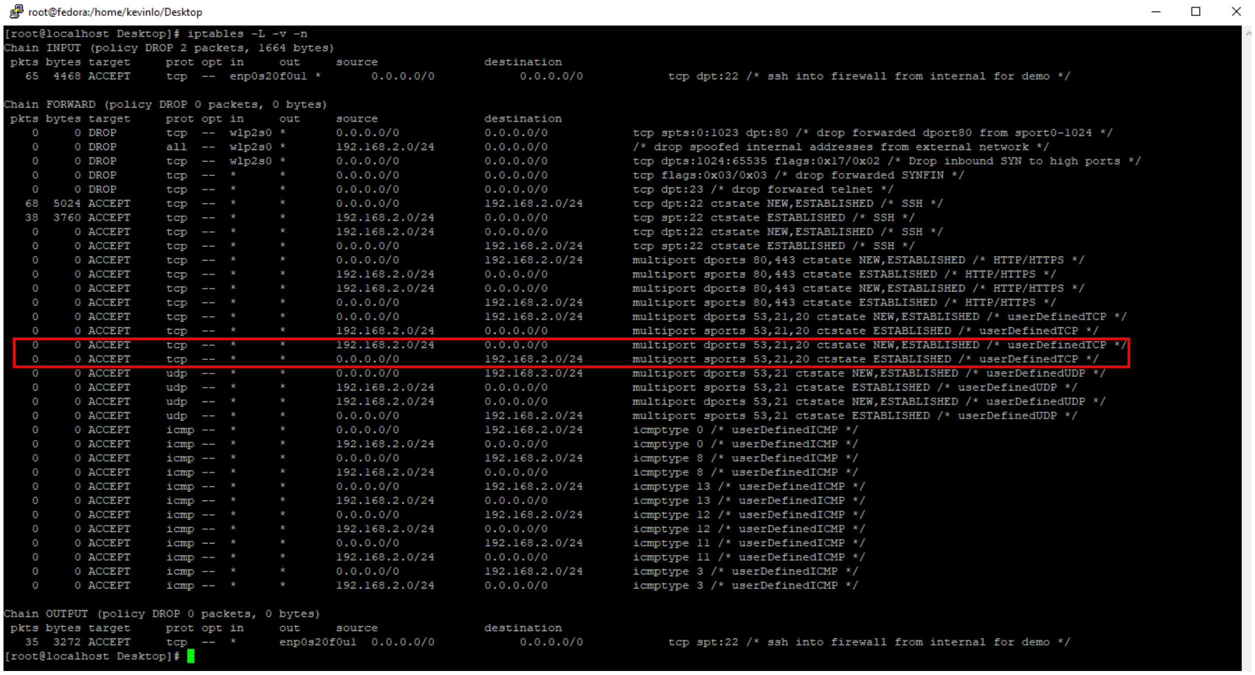
pi@raspberrypi: ~

```
root@raspberrypi:/home/pi# hping3 192.168.1.251 -S -p 80 -c 1
HPING 192.168.1.251 (eth0 192.168.1.251): S set, 40 headers + 0 data bytes
ICMP Packet filtered from ip=192.168.1.251 name=UNKNOWN

--- 192.168.1.251 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@raspberrypi:/home/pi#
```

The following packet captures shows that the packet from internal network TCP dport 80 was able to successfully reach the external network and receive a response back however the response came back from ICMP type 3.

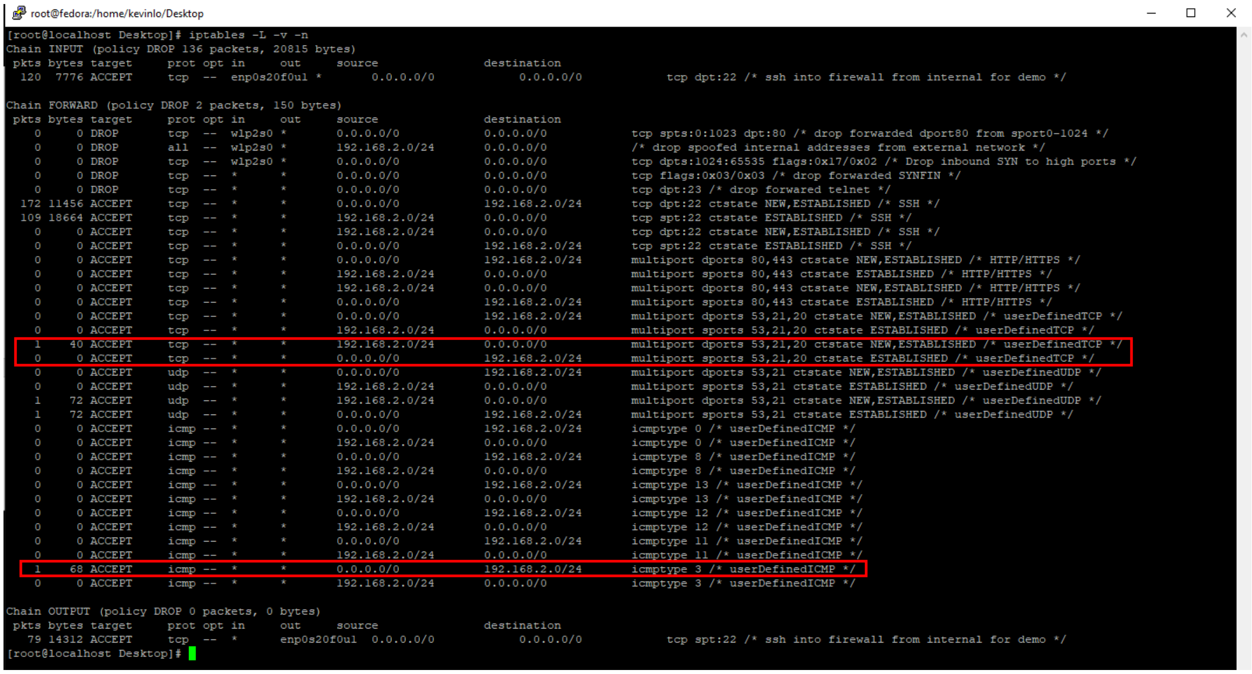
4.1.3 Test 3 – Outbound TCP dport 53 (DNS)

Firewall Lines (FORWARD chain)

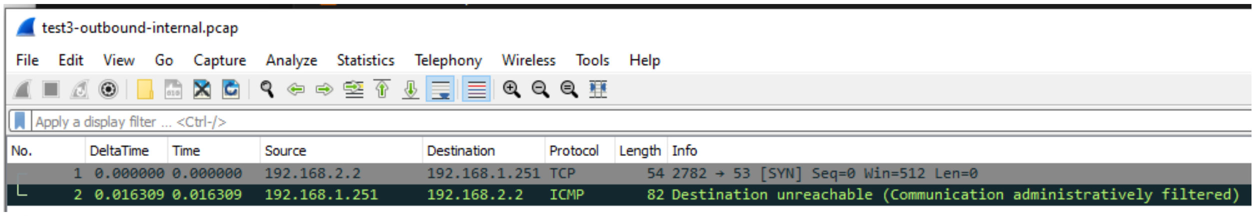


```
[root@localhost Desktop]# iptables -L -v -n
Chain INPUT (policy DROP 2 packets, 1664 bytes)
 pkts bytes target     prot opt in     out     source               destination
   65  4468 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
    0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
   68  5024 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
   38  3760 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   35  3272 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

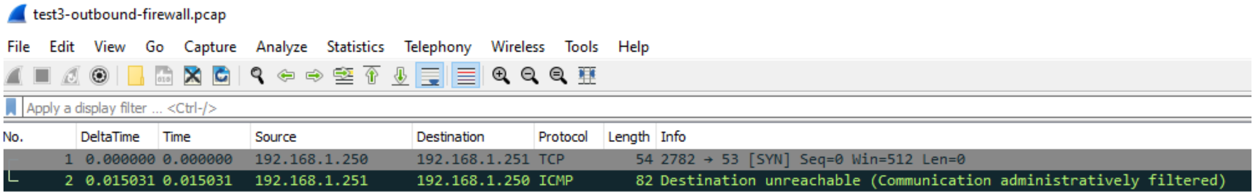
After



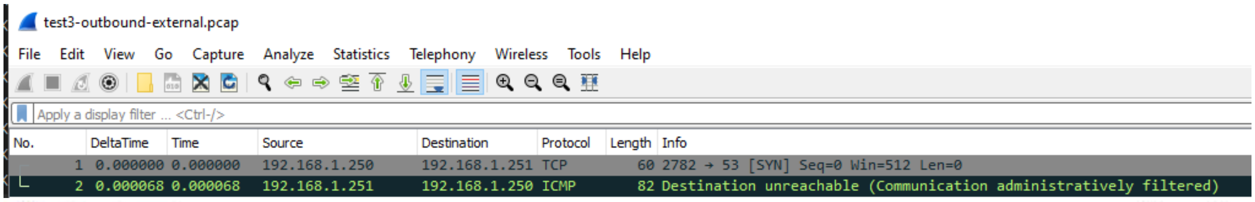
```
[root@localhost Desktop]# iptables -L -v -n
Chain INPUT (policy DROP 136 packets, 20815 bytes)
 pkts bytes target     prot opt in     out     source               destination
  120  7776 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 2 packets, 150 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
    0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
  172 11456 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
  109 18664 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    1    40 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    1    72 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    1    72 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
    1    68 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   79 14312 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```


test3-outbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

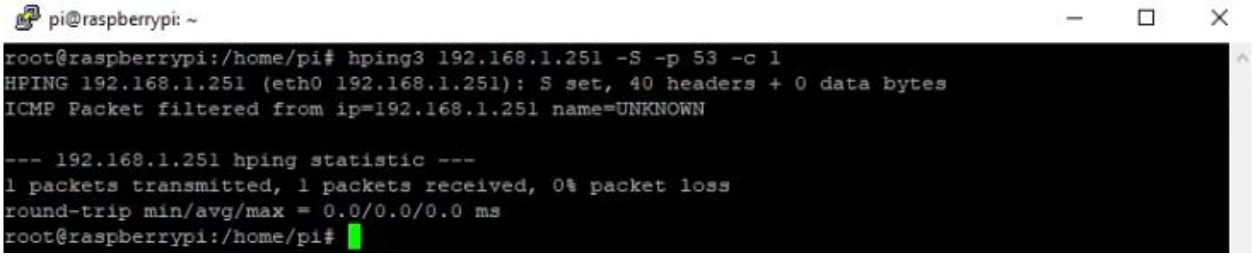
```
No.  DeltaTime Time      Source         Destination    Protocol Length Info
   1 0.000000 0.000000   192.168.2.2    192.168.1.251  TCP        54 2782 → 53 [SYN] Seq=0 Win=512 Len=0
   2 0.016309 0.016309   192.168.1.251  192.168.2.2    ICMP       82 Destination unreachable (Communication administratively filtered)
```


test3-outbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time      Source         Destination    Protocol Length Info
   1 0.000000 0.000000   192.168.1.250  192.168.1.251  TCP        54 2782 → 53 [SYN] Seq=0 Win=512 Len=0
   2 0.015031 0.015031   192.168.1.251  192.168.1.250  ICMP       82 Destination unreachable (Communication administratively filtered)
```


test3-outbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time      Source         Destination    Protocol Length Info
   1 0.000000 0.000000   192.168.1.250  192.168.1.251  TCP        60 2782 → 53 [SYN] Seq=0 Win=512 Len=0
   2 0.000068 0.000068   192.168.1.251  192.168.1.250  ICMP       82 Destination unreachable (Communication administratively filtered)
```

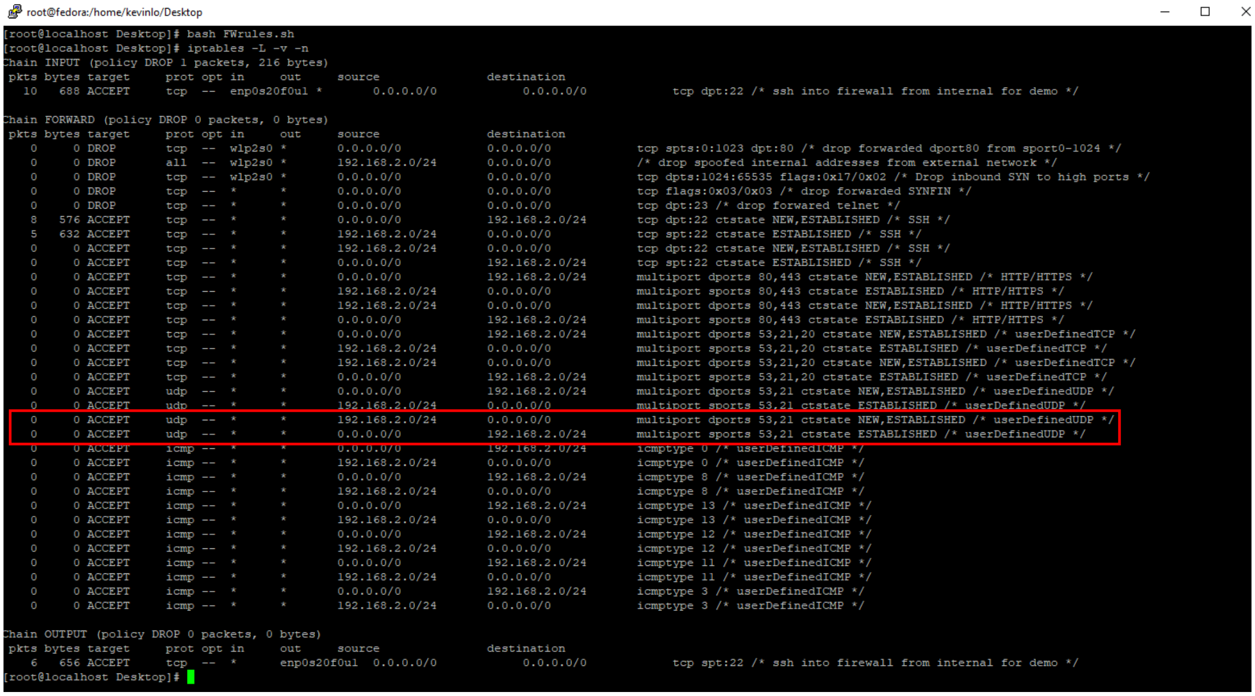


```
root@raspberrypi:/home/pi# hping3 192.168.1.251 -S -p 53 -c 1
HPING 192.168.1.251 (eth0 192.168.1.251): S set, 40 headers + 0 data bytes
ICMP Packet filtered from ip=192.168.1.251 name=UNKNOWN

--- 192.168.1.251 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@raspberrypi:/home/pi#
```

The following packet captures shows that the packet from internal network TCP dport 53 was able to successfully reach the external network and receive a response back however the response came back from ICMP type 3.

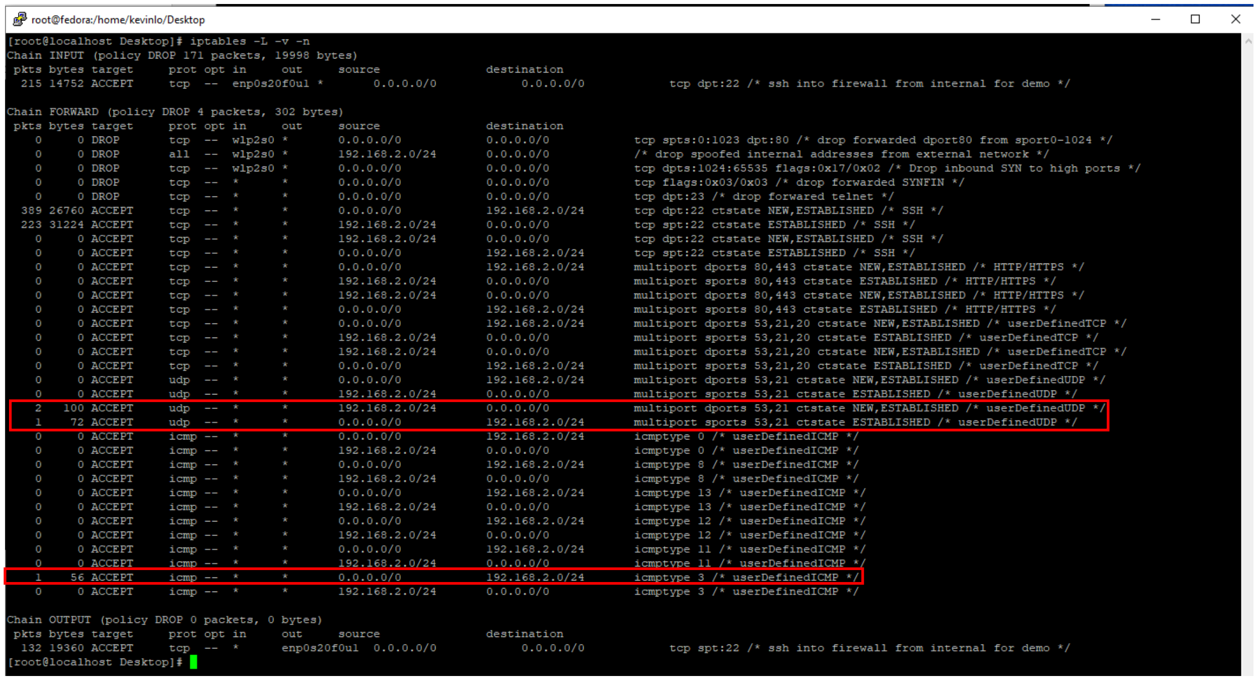
4.1.4 Test 4 – Outbound UDP dport 53 (DNS)

Firewall Lines (FORWARD chain)

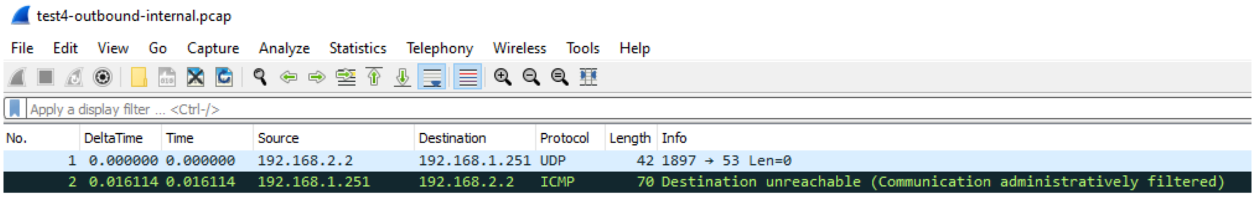


```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n
hain INPUT (policy DROP 1 packets, 216 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10   688 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

hain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
    0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
    8   576 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    5   632 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

hain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    6   656 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

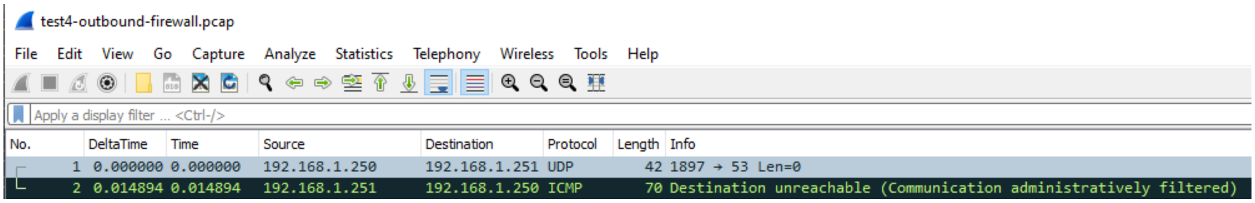
After



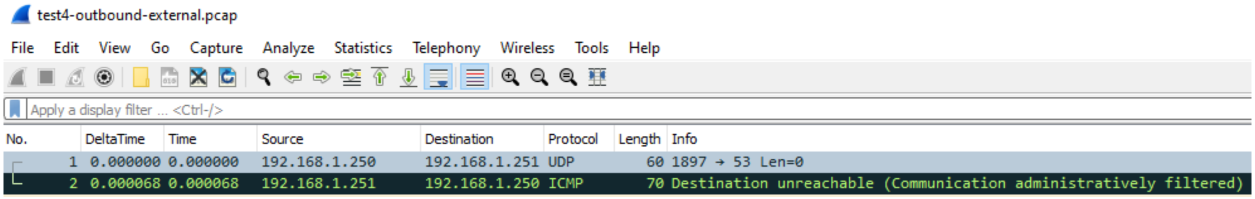
```
[root@localhost Desktop]# iptables -L -v -n
Chain INPUT (policy DROP 171 packets, 19998 bytes)
 pkts bytes target     prot opt in     out     source               destination
  215 14752 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 4 packets, 302 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
    0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
  389 26760 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
  223 31224 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    2   100 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    1    72 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
    1    56 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  132 19360 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```


test4-outbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

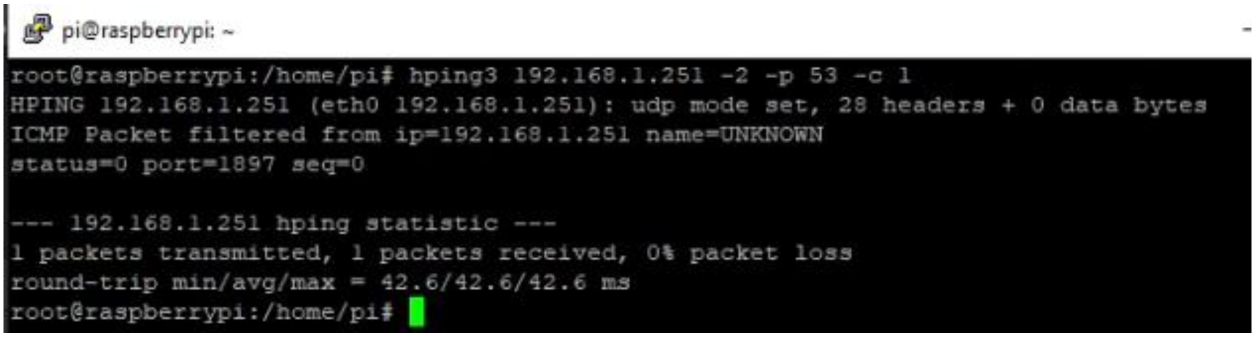
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.2.2	192.168.1.251	UDP	42	1897 → 53 Len=0
2	0.016114	0.016114	192.168.1.251	192.168.2.2	ICMP	70	Destination unreachable (Communication administratively filtered)


test4-outbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.250	192.168.1.251	UDP	42	1897 → 53 Len=0
2	0.014894	0.014894	192.168.1.251	192.168.1.250	ICMP	70	Destination unreachable (Communication administratively filtered)


test4-outbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.250	192.168.1.251	UDP	60	1897 → 53 Len=0
2	0.000068	0.000068	192.168.1.251	192.168.1.250	ICMP	70	Destination unreachable (Communication administratively filtered)

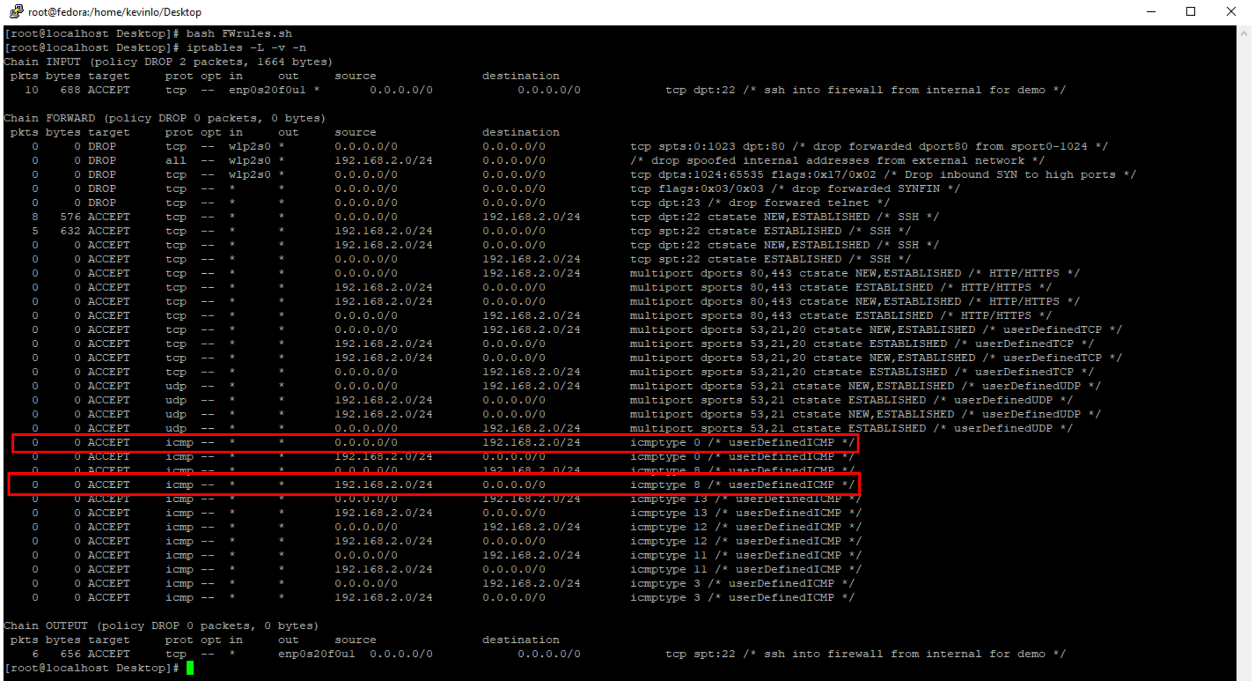


```
root@raspberrypi:/home/pi# hping3 192.168.1.251 -2 -p 53 -c 1
HPING 192.168.1.251 (eth0 192.168.1.251): udp mode set, 28 headers + 0 data bytes
ICMP Packet filtered from ip=192.168.1.251 name=UNKNOWN
status=0 port=1897 seq=0

--- 192.168.1.251 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 42.6/42.6/42.6 ms
root@raspberrypi:/home/pi#
```

The following packet captures shows that the packet from internal network UDP dport 53 was able to successfully reach the external network and receive a response back however the response came back from ICMP type 3.

4.1.5 Test 5 – Outbound ICMP 0,8 (Ping)

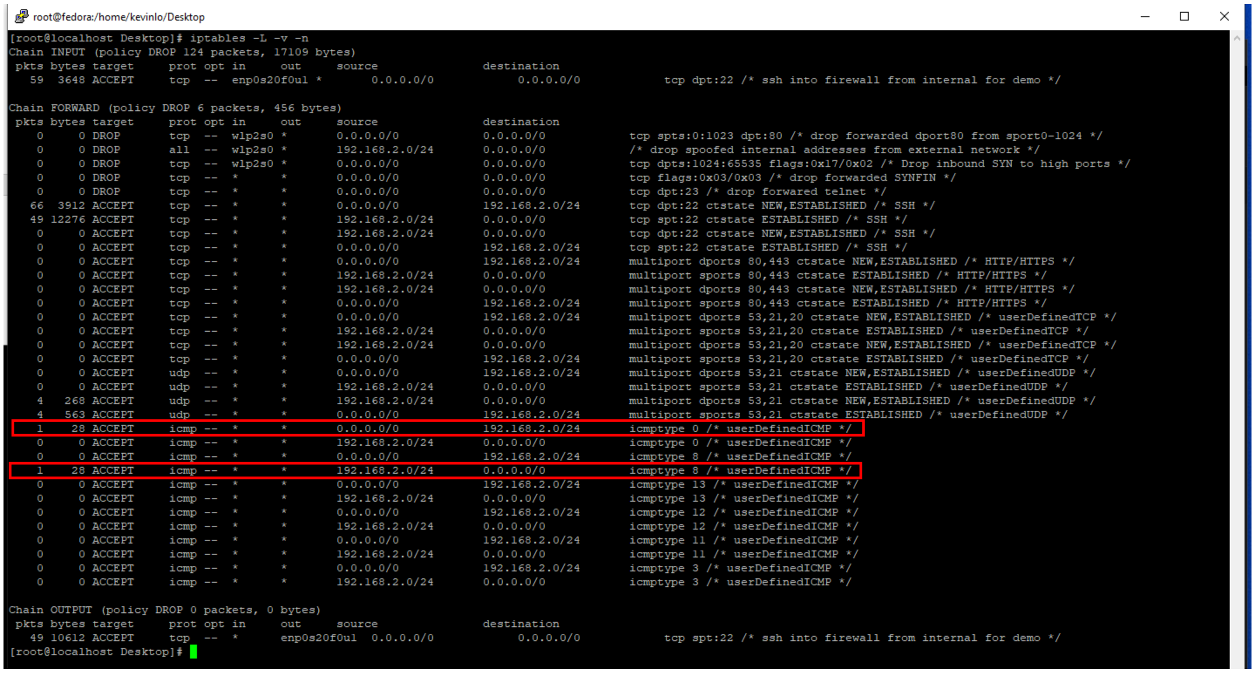
Firewall Lines (FORWARD chain)



root@fedora:/home/kevinlo/Desktop

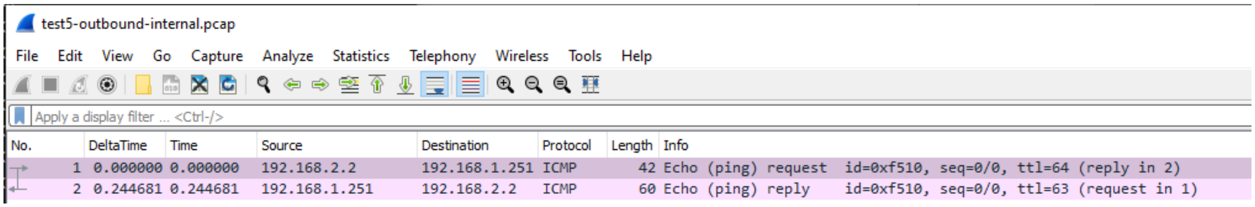
```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n
Chain INPUT (policy DROP 2 packets, 1664 bytes)
 pkts bytes target     prot opt in     out     source               destination
   10   688 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
    0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
    8   576 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    5   632 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    6   656 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After

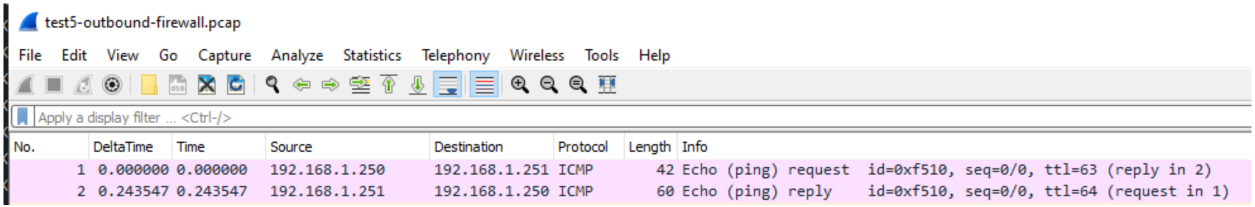


root@fedora:/home/kevinlo/Desktop

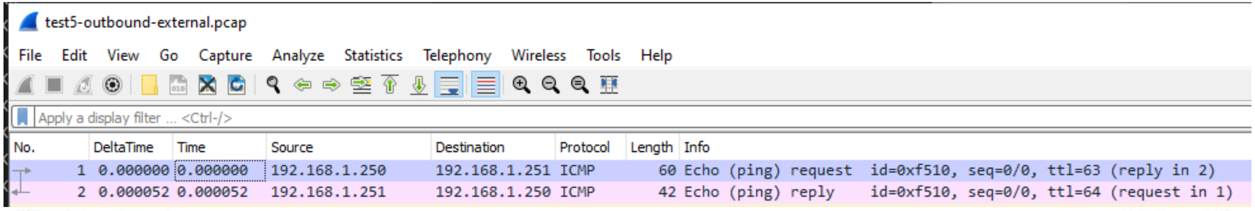
```
[root@localhost Desktop]# iptables -L -v -n
Chain INPUT (policy DROP 124 packets, 17109 bytes)
 pkts bytes target     prot opt in     out     source               destination
   59  3648 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 6 packets, 456 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
    0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
    0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
   66  3912 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
   49 12276 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    4   268 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
    4   563 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
    1    28 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
    1    28 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
    0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   49 10612 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```


test5-outbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

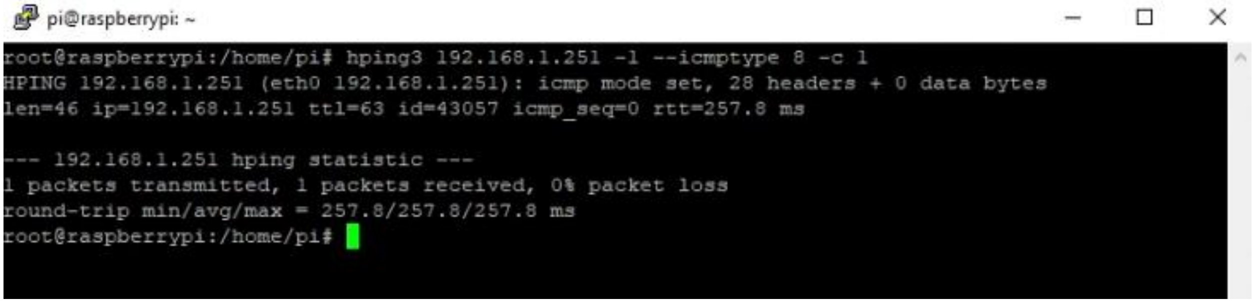
```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
   1 0.000000 0.000000  192.168.2.2   192.168.1.251 ICMP      42 Echo (ping) request  id=0xf510, seq=0/0, ttl=64 (reply in 2)
   2 0.244681 0.244681  192.168.1.251 192.168.2.2   ICMP      60 Echo (ping) reply    id=0xf510, seq=0/0, ttl=63 (request in 1)
```


test5-outbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
   1 0.000000 0.000000  192.168.1.250 192.168.1.251 ICMP      42 Echo (ping) request  id=0xf510, seq=0/0, ttl=63 (reply in 2)
   2 0.243547 0.243547  192.168.1.251 192.168.1.250 ICMP      60 Echo (ping) reply    id=0xf510, seq=0/0, ttl=64 (request in 1)
```


test5-outbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
   1 0.000000 0.000000  192.168.1.250 192.168.1.251 ICMP      60 Echo (ping) request  id=0xf510, seq=0/0, ttl=63 (reply in 2)
   2 0.000052 0.000052  192.168.1.251 192.168.1.250 ICMP      42 Echo (ping) reply    id=0xf510, seq=0/0, ttl=64 (request in 1)
```

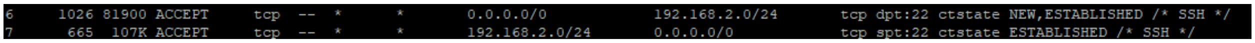


```
root@raspberrypi:/home/pi# hping3 192.168.1.251 -1 --icmptype 8 -c 1
HPING 192.168.1.251 (eth0 192.168.1.251): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.251 ttl=63 id=43057 icmp_seq=0 rtt=257.8 ms

--- 192.168.1.251 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 257.8/257.8/257.8 ms
root@raspberrypi:/home/pi#
```

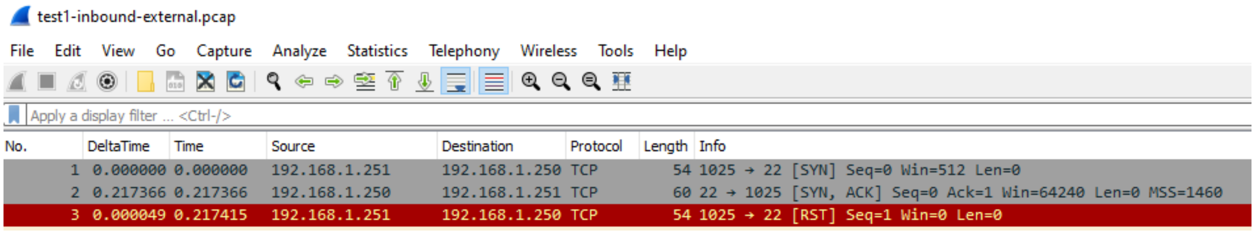
The following packet capture shows that the ping was able to successfully go through, it needed both ICMP type 0 and type 8 to have the regular ping functional.

4.1.6 Test 1 – Inbound TCP dport 22 (SSH)

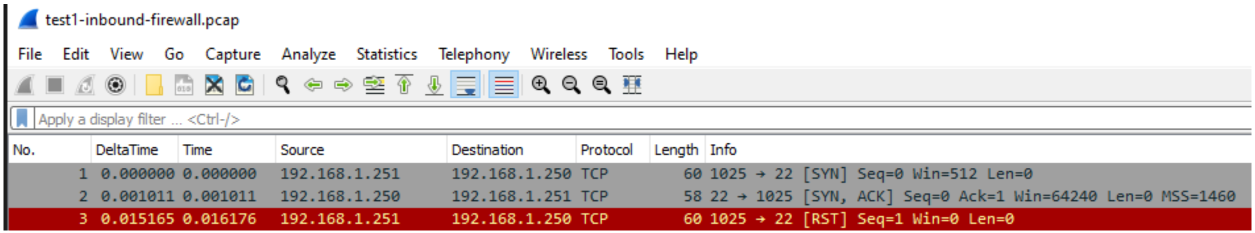
Firewall Lines (FORWARD chain)



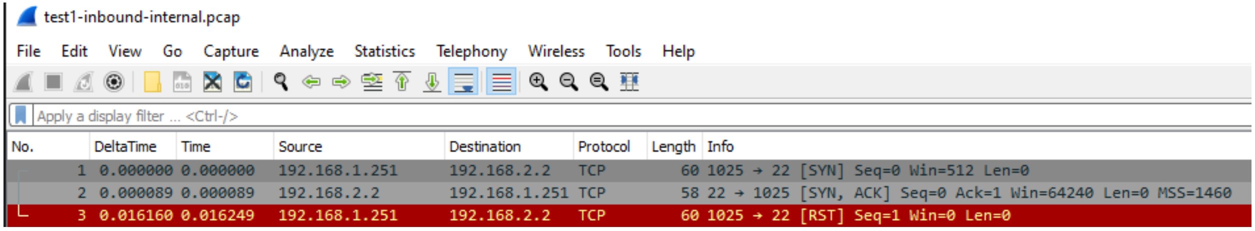
```
6     1026 81900 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      665  107K ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
```


test1-inbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

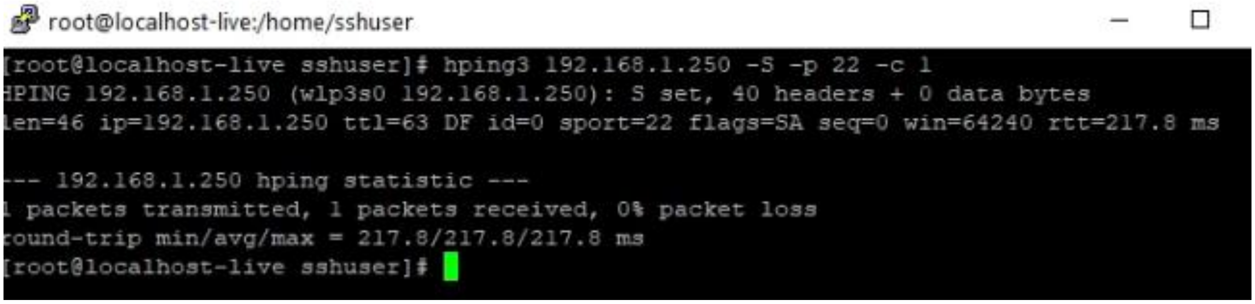
```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
   1 0.000000 0.000000  192.168.1.251 192.168.1.250 TCP       54 1025 → 22 [SYN] Seq=0 Win=512 Len=0
   2 0.217366 0.217366  192.168.1.250 192.168.1.251 TCP       60 22 → 1025 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   3 0.000049 0.217415  192.168.1.251 192.168.1.250 TCP       54 1025 → 22 [RST] Seq=1 Win=0 Len=0
```


test1-inbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time      Source         Destination    Protocol Length Info
    1 0.000000 0.000000   192.168.1.251  192.168.1.250  TCP        60 1025 → 22 [SYN] Seq=0 Win=512 Len=0
    2 0.001011 0.001011   192.168.1.250  192.168.1.251  TCP        58 22 → 1025 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
    3 0.015165 0.016176   192.168.1.251  192.168.1.250  TCP        60 1025 → 22 [RST] Seq=1 Win=0 Len=0
```


test1-inbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time      Source         Destination    Protocol Length Info
    1 0.000000 0.000000   192.168.1.251  192.168.2.2    TCP        60 1025 → 22 [SYN] Seq=0 Win=512 Len=0
    2 0.000089 0.000089   192.168.2.2    192.168.1.251  TCP        58 22 → 1025 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
    3 0.016160 0.016249   192.168.1.251  192.168.2.2    TCP        60 1025 → 22 [RST] Seq=1 Win=0 Len=0
```

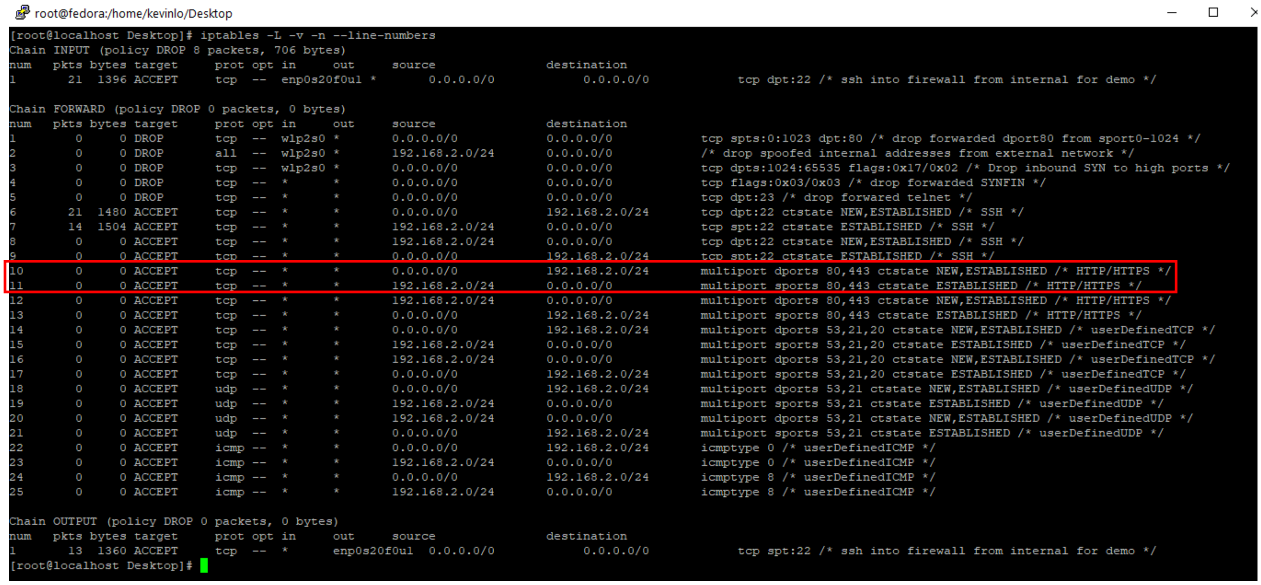


```
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -p 22 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.250 ttl=63 DF id=0 sport=22 flags=SA seq=0 win=64240 rtt=217.8 ms

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
ound-trip min/avg/max = 217.8/217.8/217.8 ms
[root@localhost-live sshuser]#
```

The following packet captures along with hping3 shows that the packet from internal network TCP dport 22 was able to successfully reach the external network and receive a response back.

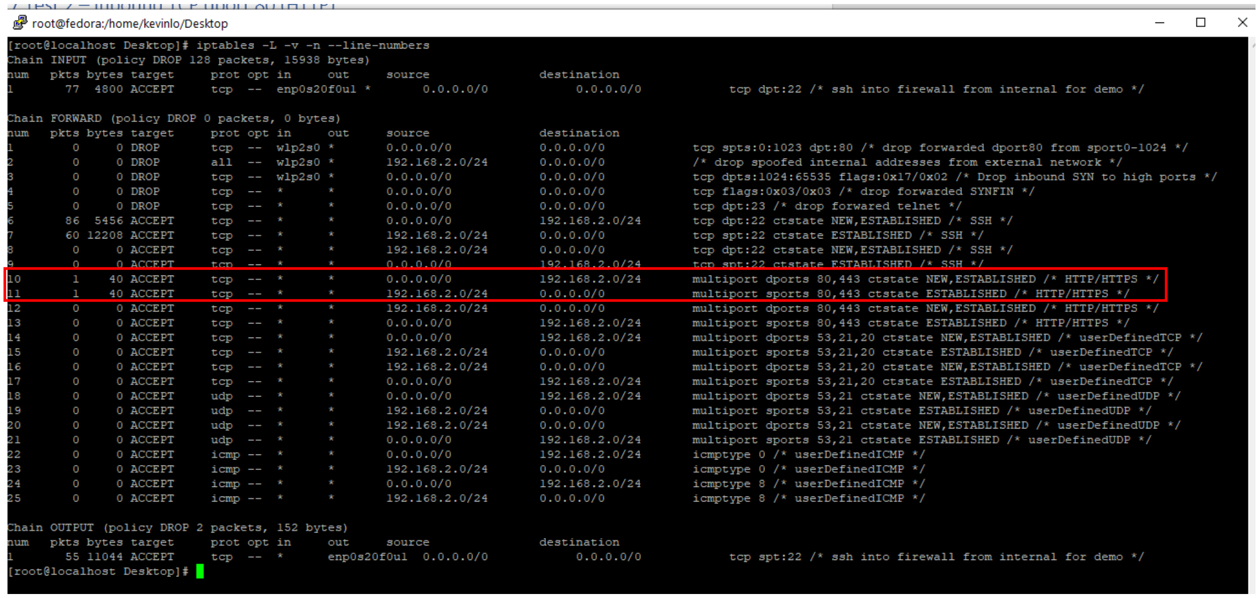
4.1.7 Test 2 – Inbound TCP dport 80 (HTTP)

Firewall Lines (FORWARD chain)

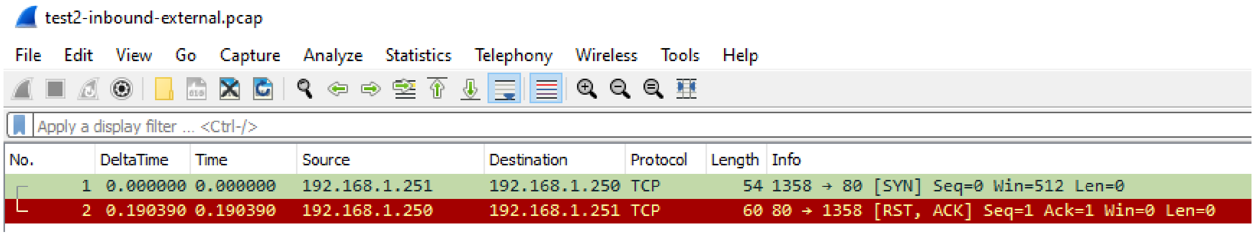


```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 8 packets, 706 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       21  1396 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6       21  1480 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       14  1504 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       13  1360 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After

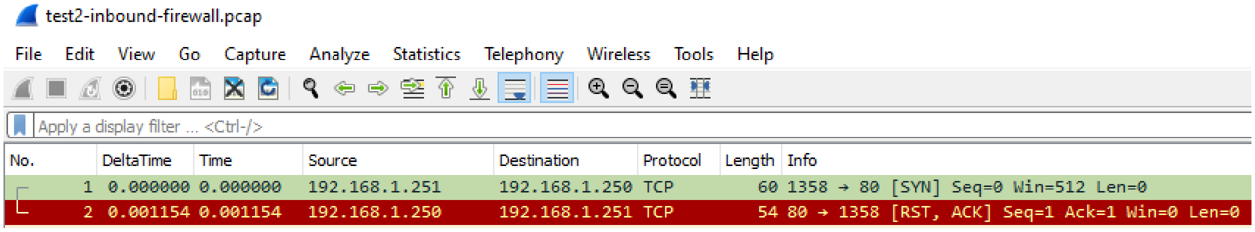


```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 128 packets, 15938 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       77  4800 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6       86  5456 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       60 12208 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       1    40 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       1    40 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 2 packets, 152 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       55 11044 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```



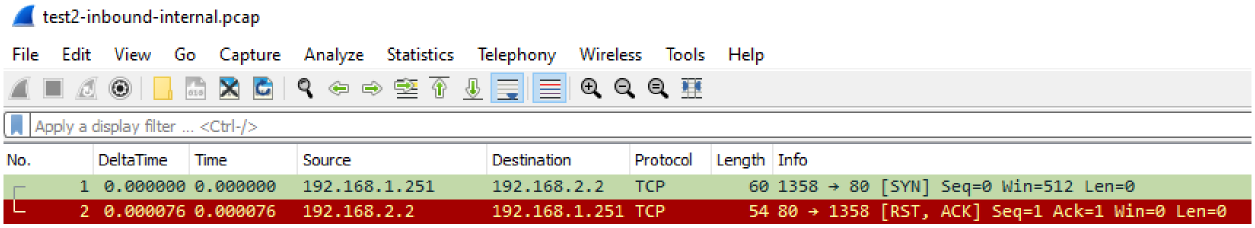
test2-inbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	54	1358 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.190390	0.190390	192.168.1.250	192.168.1.251	TCP	60	80 → 1358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



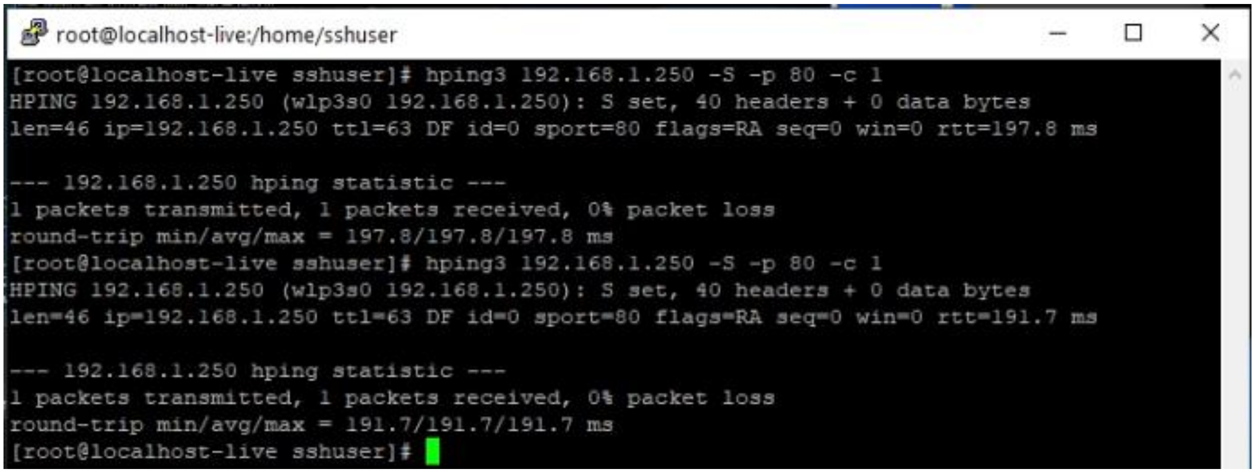
test2-inbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	60	1358 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.001154	0.001154	192.168.1.250	192.168.1.251	TCP	54	80 → 1358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



test2-inbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.2.2	TCP	60	1358 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.000076	0.000076	192.168.2.2	192.168.1.251	TCP	54	80 → 1358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



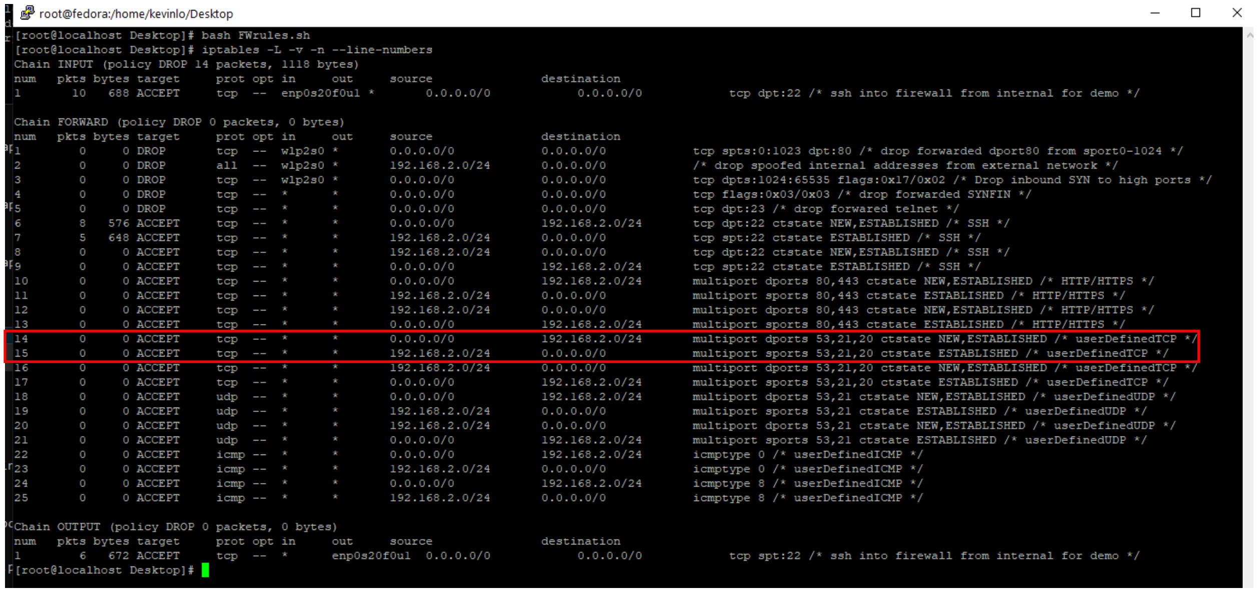
root@localhost-live:/home/sshuser

```
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -p 80 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.250 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=197.8 ms

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 197.8/197.8/197.8 ms
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -p 80 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.250 ttl=63 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=191.7 ms

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 191.7/191.7/191.7 ms
[root@localhost-live sshuser]#
```

The following packet captures and hping3 show that dport 80 is accessible from the external network to the internal network by being able to send the packet and receive a response back.

4.1.8 Test 3 – Inbound TCP dport 53 (DNS)

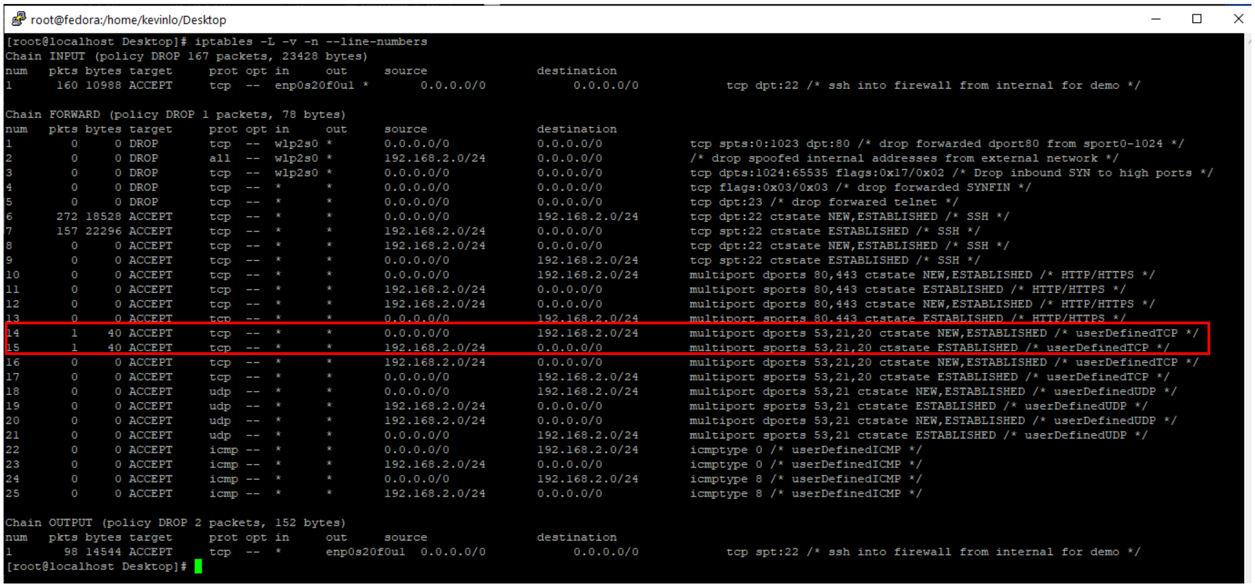
Firewall Lines (FORWARD chain)



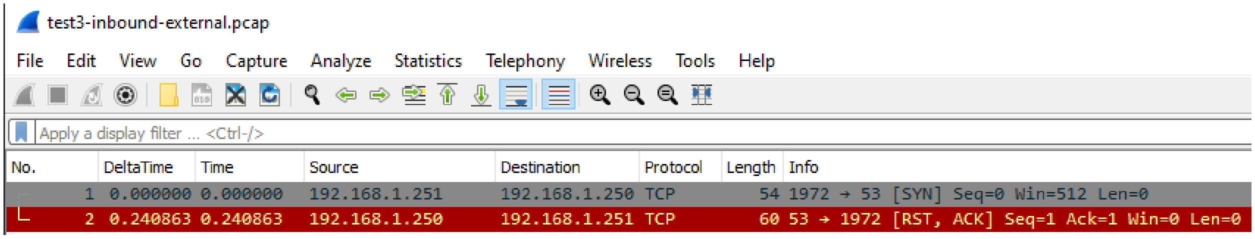
root@fedora:/home/kevinlo/Desktop

```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 14 packets, 1118 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       10   688 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6        8   576 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7        5   648 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        6   672 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

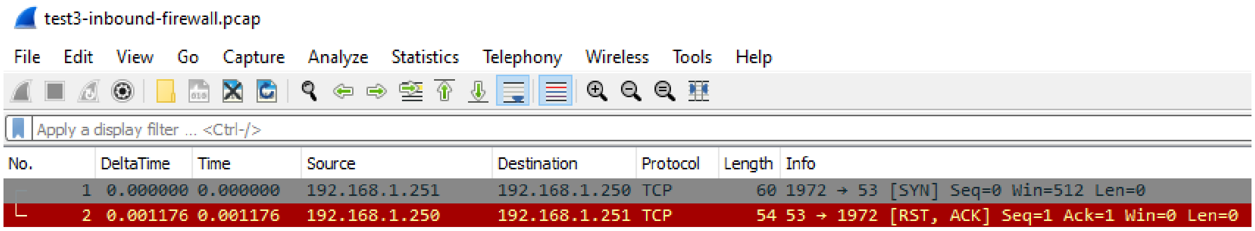
After



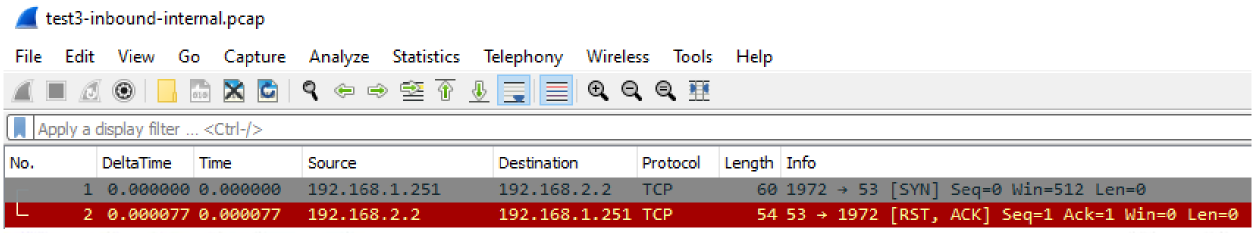
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 167 packets, 23428 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      160 10988 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 1 packets, 78 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forward telnet */
6      272 18528 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      157 22296 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       1    40 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       1    40 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 2 packets, 152 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       98 14544 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```



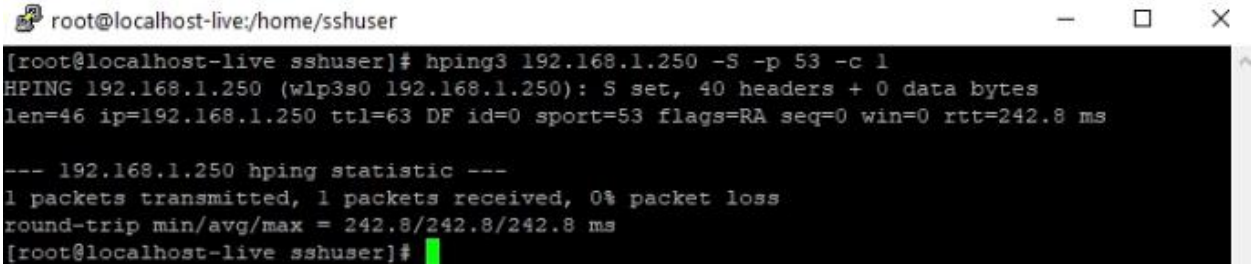
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	54	1972 → 53 [SYN] Seq=0 Win=512 Len=0
2	0.240863	0.240863	192.168.1.250	192.168.1.251	TCP	60	53 → 1972 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	60	1972 → 53 [SYN] Seq=0 Win=512 Len=0
2	0.001176	0.001176	192.168.1.250	192.168.1.251	TCP	54	53 → 1972 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.2.2	TCP	60	1972 → 53 [SYN] Seq=0 Win=512 Len=0
2	0.000077	0.000077	192.168.2.2	192.168.1.251	TCP	54	53 → 1972 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

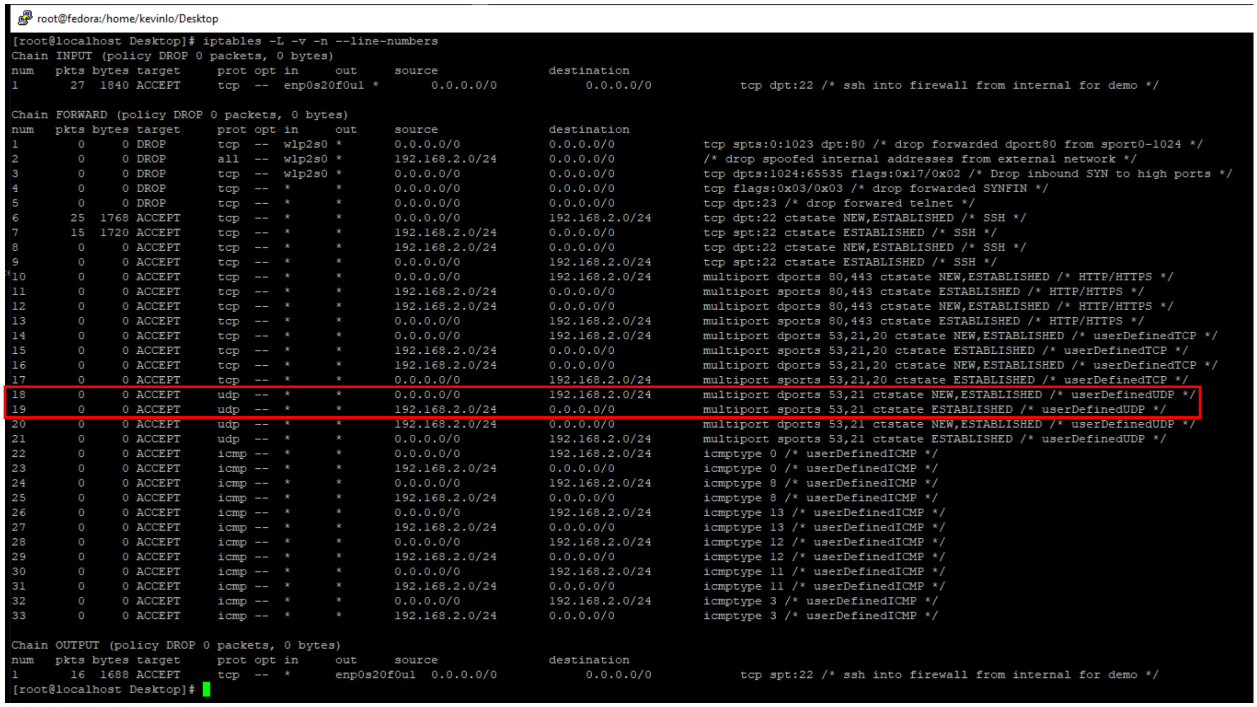


```
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -p 53 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.250 ttl=63 DF id=0 sport=53 flags=RA seq=0 win=0 rtt=242.8 ms

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 242.8/242.8/242.8 ms
[root@localhost-live sshuser]#
```

The following packet captures and hping3 show that TCP dport 53 is accessible from the external network to the internal network by being able to send the packet and receive a response back.

4.1.9 Test 4 – Inbound UDP dport 53 (DNS)

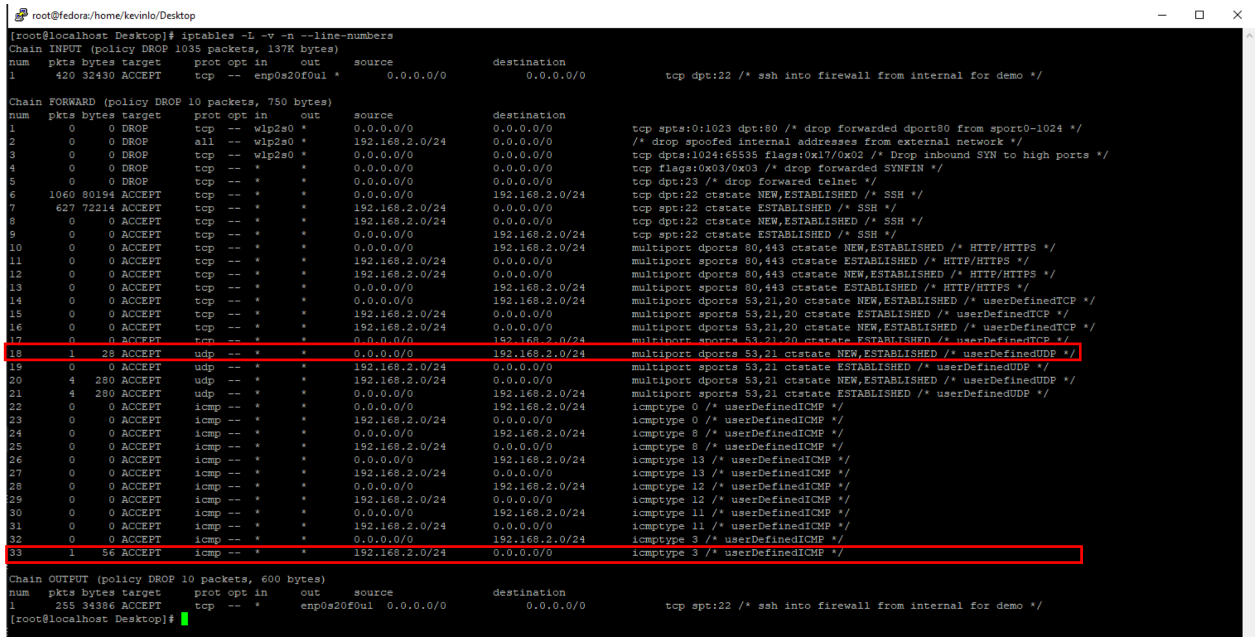
Firewall Lines (FORWARD chain)



root@fedora:/home/kevinlo/Desktop

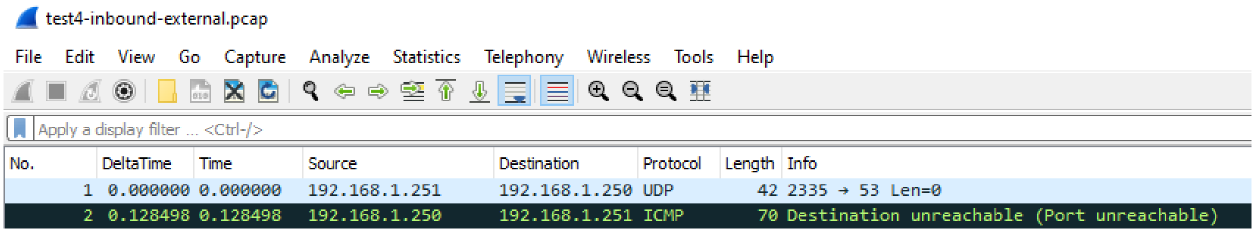
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       27  1840 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6       25  1768 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       15  1720 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       16  1688 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After

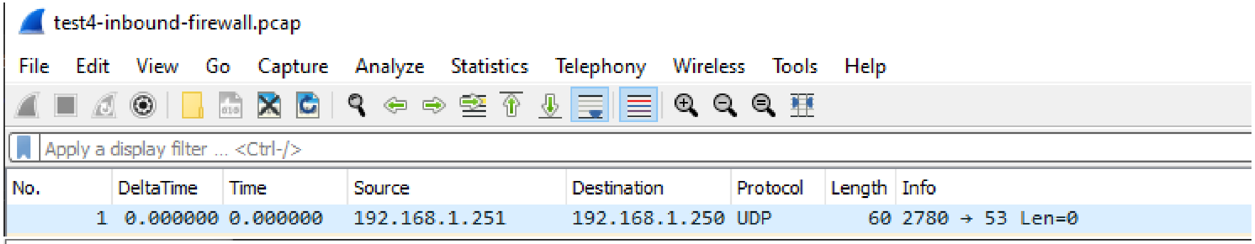


root@fedora:/home/kevinlo/Desktop

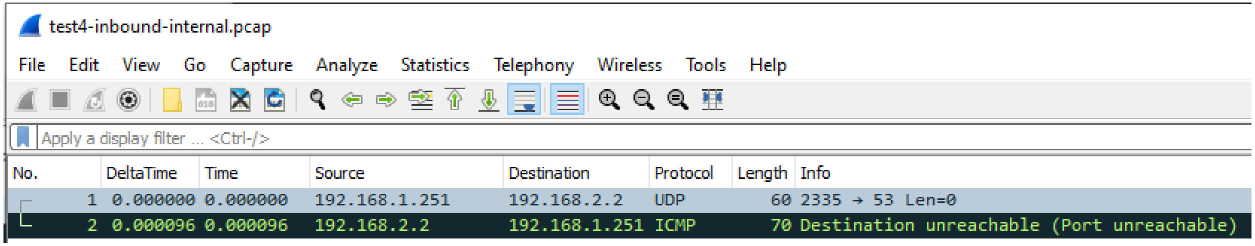
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 1035 packets, 137K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      420 32430 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 10 packets, 750 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6     1060 80194 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      627 72214 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       1    28 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       4   280 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       4   280 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       1    56 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 10 packets, 600 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      255 34386 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```


test4-inbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

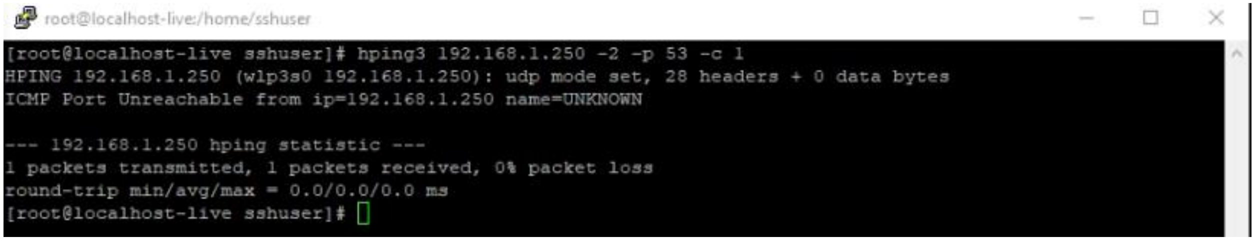
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	UDP	42	2335 → 53 Len=0
2	0.128498	0.128498	192.168.1.250	192.168.1.251	ICMP	70	Destination unreachable (Port unreachable)


test4-inbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	UDP	60	2780 → 53 Len=0


test4-inbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.2.2	UDP	60	2335 → 53 Len=0
2	0.000096	0.000096	192.168.2.2	192.168.1.251	ICMP	70	Destination unreachable (Port unreachable)

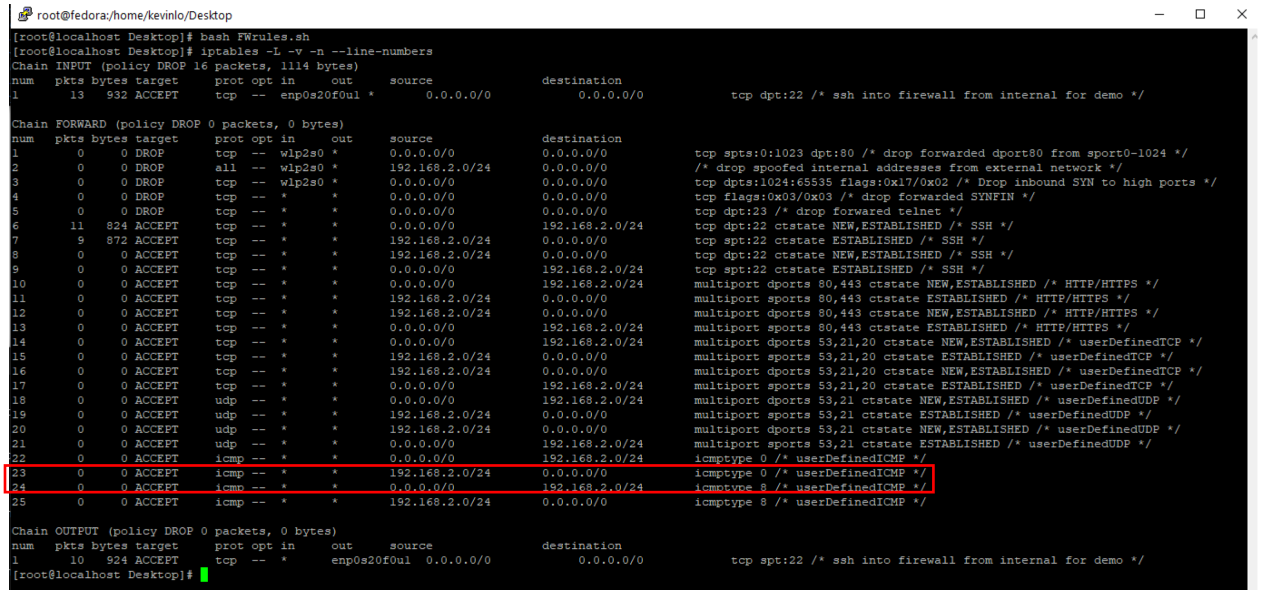


```
[root@localhost-live sshuser]# hping3 192.168.1.250 -2 -p 53 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.1.250 name=UNKNOWN

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost-live sshuser]#
```

The following packet captures and hping3 show that UDP dport 53 is accessible from the external network to the internal network by being able to send the packet and receive a response back.

4.1.10 Test 5 – Inbound ICMP 0,8 (Ping)

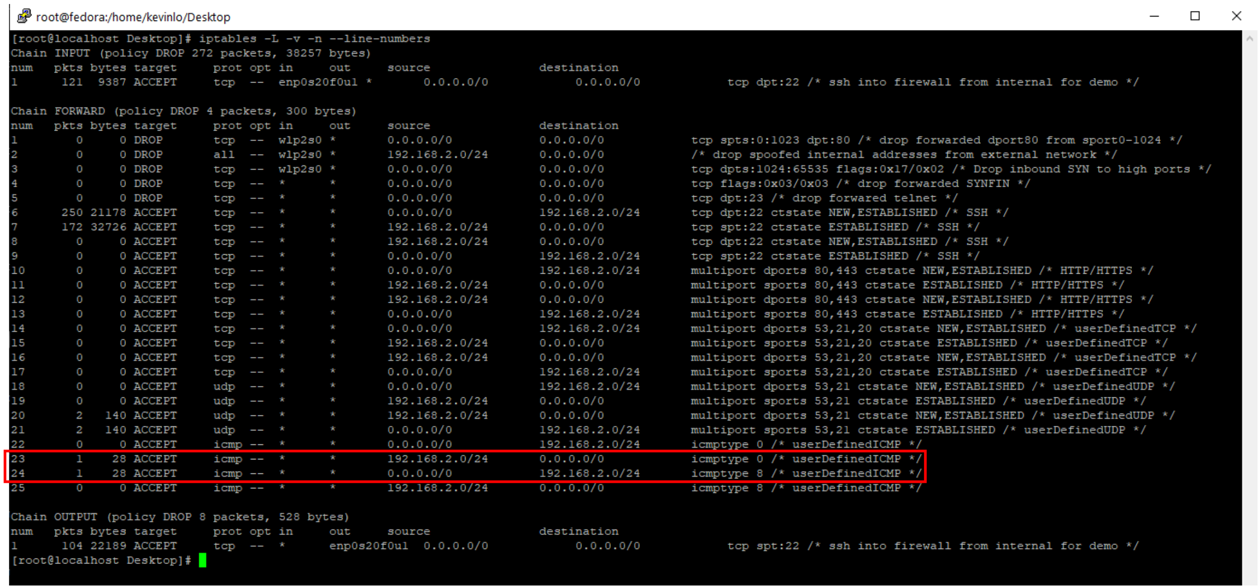
Firewall Lines (FORWARD chain)



root@fedora:/home/kevinlo/Desktop

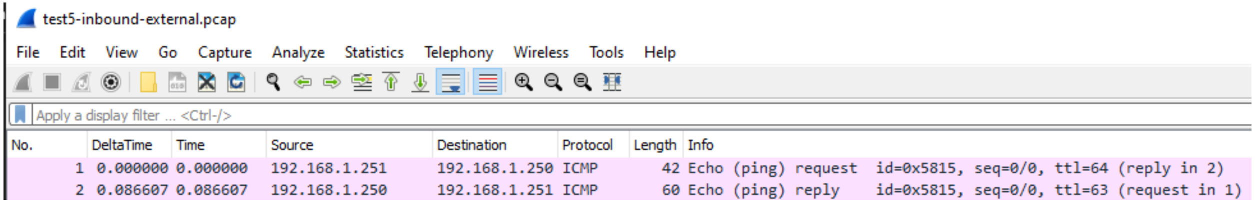
```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 16 packets, 1114 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       13   932 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6       11   824 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7        9   872 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       10   924 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After



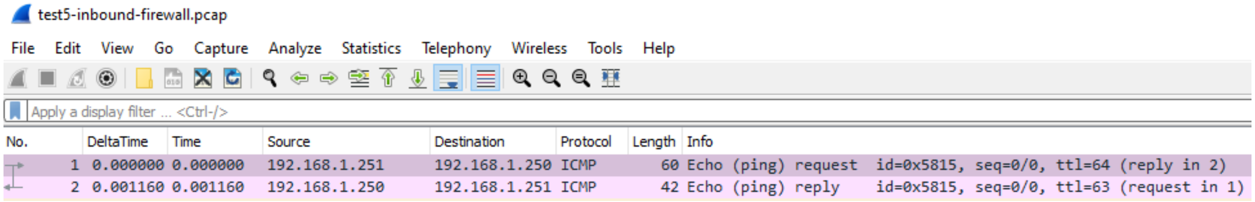
root@fedora:/home/kevinlo/Desktop

```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 272 packets, 38257 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      121  9387 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 4 packets, 300 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6      250 21178 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      172 32726 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       2   140 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       2   140 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       1    28 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       1    28 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 8 packets, 528 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      104 22189 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

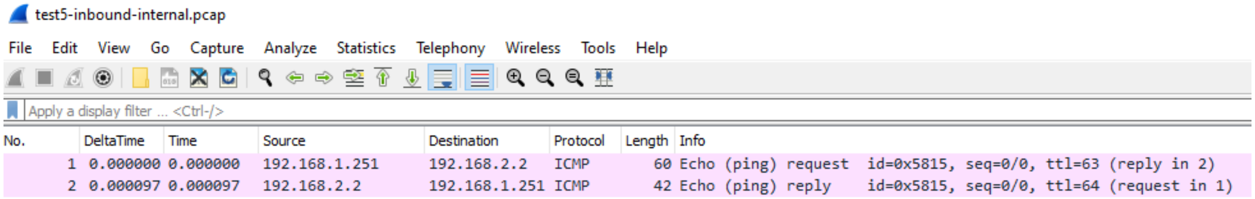


test5-inbound-external.pcap

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	ICMP	42	Echo (ping) request id=0x5815, seq=0/0, ttl=64 (reply in 2)
2	0.086607	0.086607	192.168.1.250	192.168.1.251	ICMP	60	Echo (ping) reply id=0x5815, seq=0/0, ttl=63 (request in 1)


test5-inbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
   1 0.000000 0.000000  192.168.1.251 192.168.1.250 ICMP       60 Echo (ping) request  id=0x5815, seq=0/0, ttl=64 (reply in 2)
   2 0.001160 0.001160  192.168.1.250 192.168.1.251 ICMP       42 Echo (ping) reply    id=0x5815, seq=0/0, ttl=63 (request in 1)
```

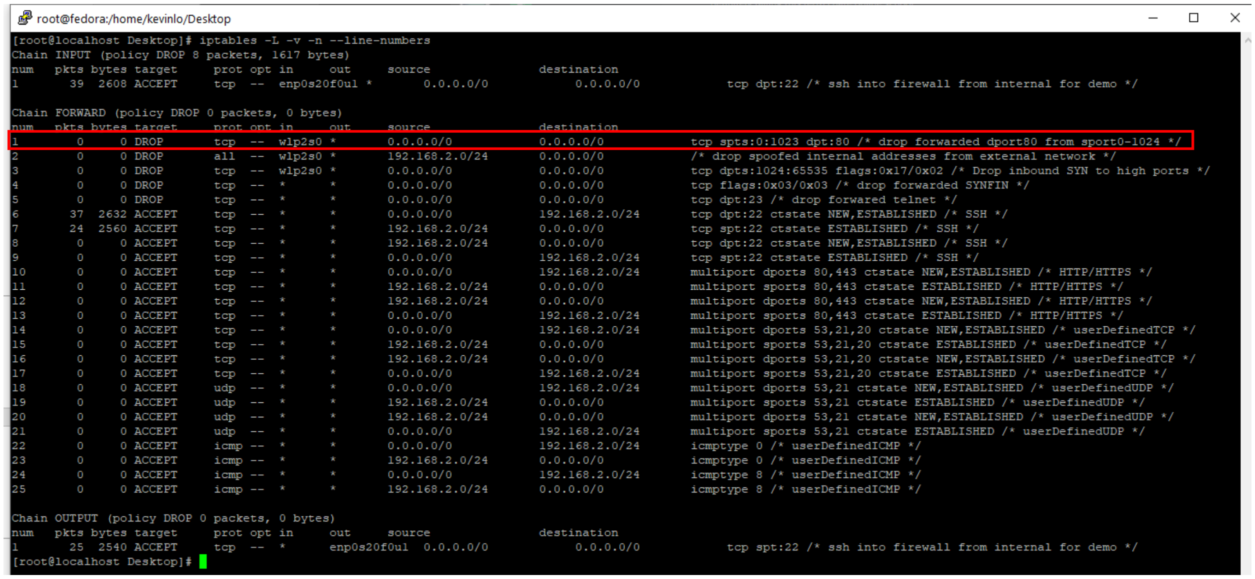

test5-inbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time     Source        Destination   Protocol Length Info
   1 0.000000 0.000000  192.168.1.251 192.168.2.2   ICMP       60 Echo (ping) request  id=0x5815, seq=0/0, ttl=63 (reply in 2)
   2 0.000097 0.000097  192.168.2.2   192.168.1.251 ICMP       42 Echo (ping) reply    id=0x5815, seq=0/0, ttl=64 (request in 1)
```

The following packet capture shows that the ping was able to successfully go through, it needed both ICMP type 0 and type 8 to have the regular ping functional.

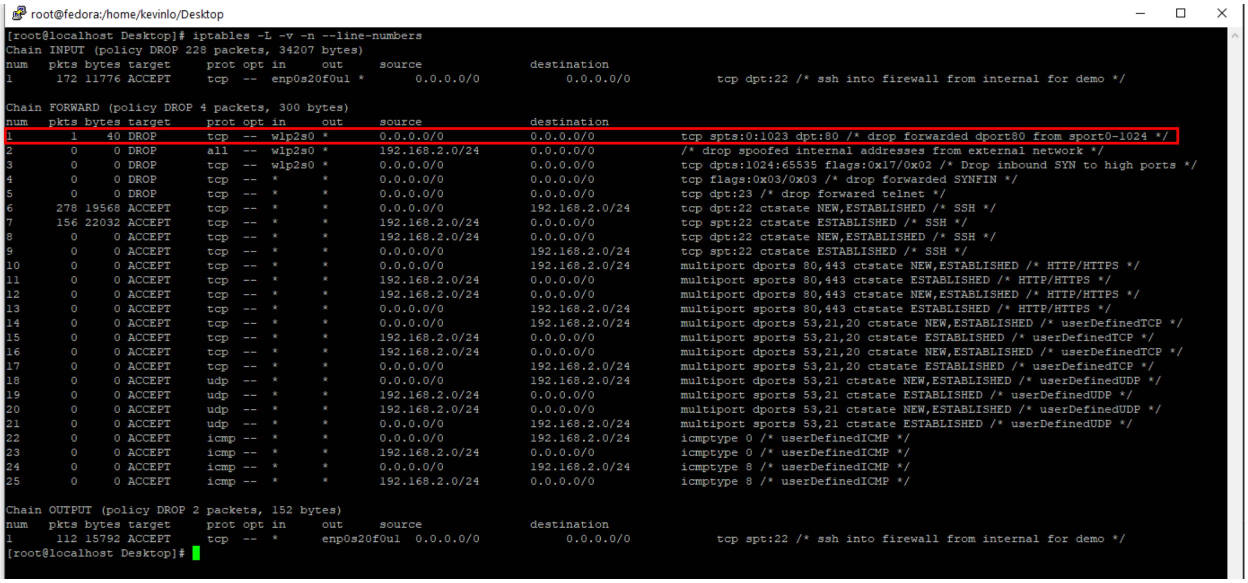
4.1.11 Test 6 – Inbound sport 0-1023 to dport 80 DROP

Firewall Lines (FORWARD chain)

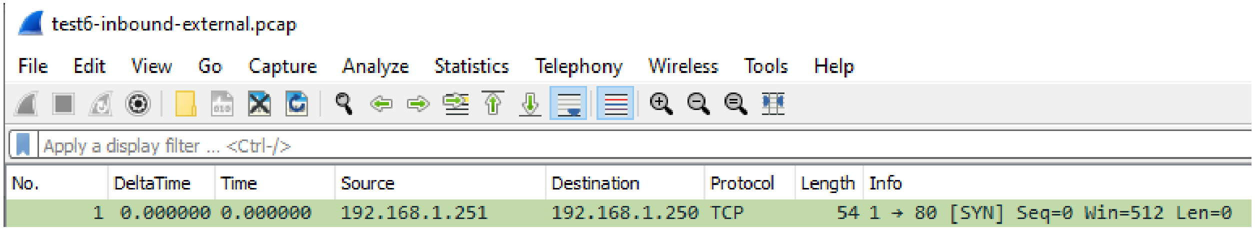


```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 8 packets, 1617 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       39  2608 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6       37  2632 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       24  2560 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       25  2540 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

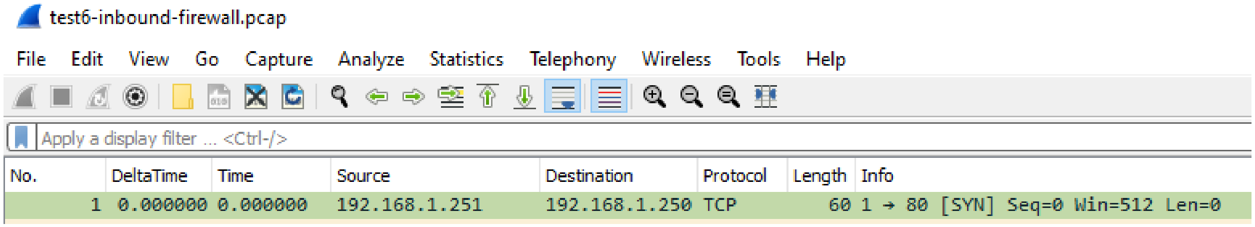
After



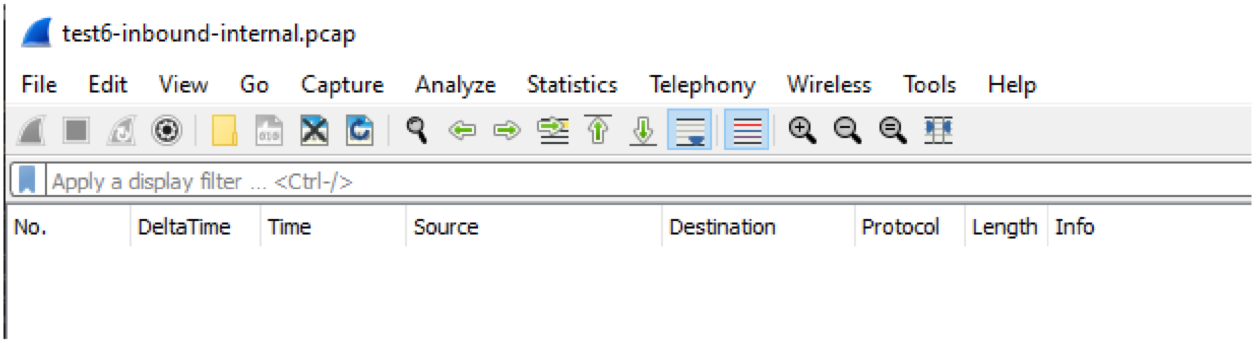
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 228 packets, 34207 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      172 11776 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 4 packets, 300 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        1    40 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6      278 19568 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      156 22032 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 2 packets, 152 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      112 15792 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```


test6-inbound-external.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

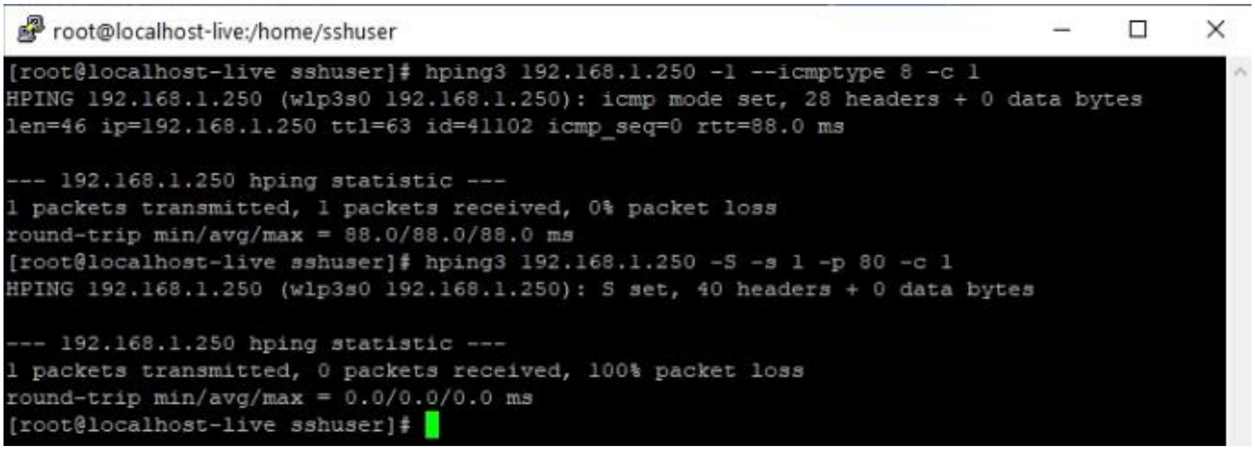
```
No.  DeltaTime Time     Source         Destination    Protocol Length Info
   1 0.000000 0.000000  192.168.1.251  192.168.1.250  TCP          54 1 → 80 [SYN] Seq=0 Win=512 Len=0
```


test6-inbound-firewall.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime Time     Source         Destination    Protocol Length Info
   1 0.000000 0.000000  192.168.1.251  192.168.1.250  TCP          60 1 → 80 [SYN] Seq=0 Win=512 Len=0
```


test6-inbound-internal.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  DeltaTime  Time  Source  Destination  Protocol  Length  Info
```

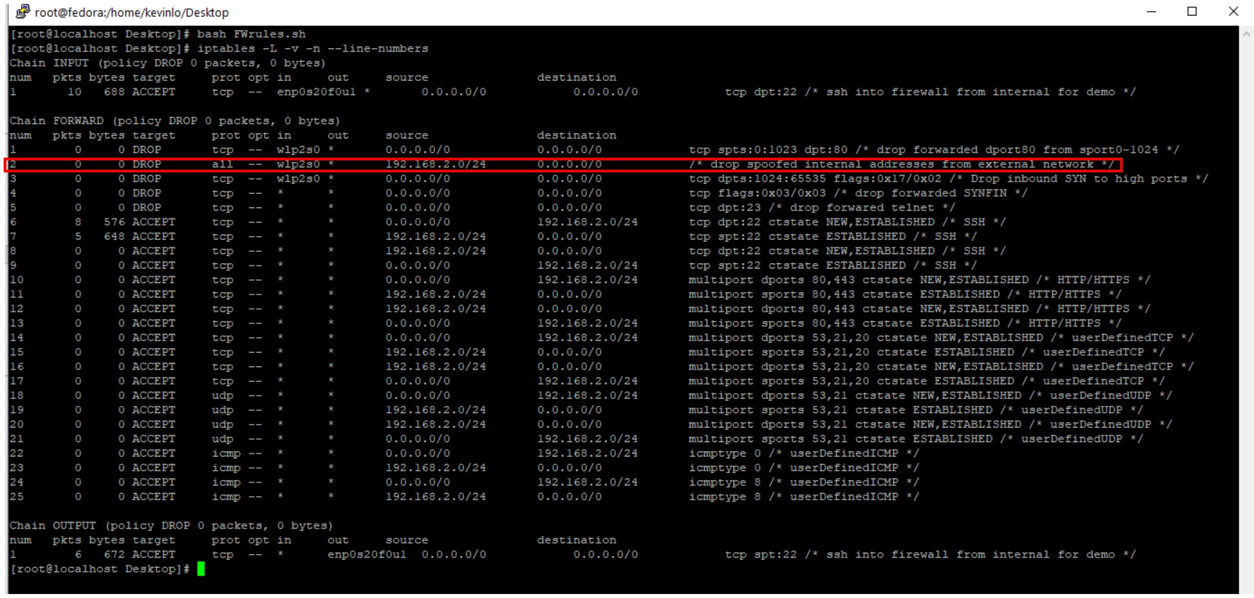


```
[root@localhost-live sshuser]# hping3 192.168.1.250 -1 --icmptype 8 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.250 ttl=63 id=41102 icmp_seq=0 rtt=88.0 ms

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 88.0/88.0/88.0 ms
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -s 1 -p 80 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost-live sshuser]#
```

There is no packets at the internal network because the firewall stopped the packet from going any futher because it successfully matched the drop rule of being to dport 80 from sport 0-1023

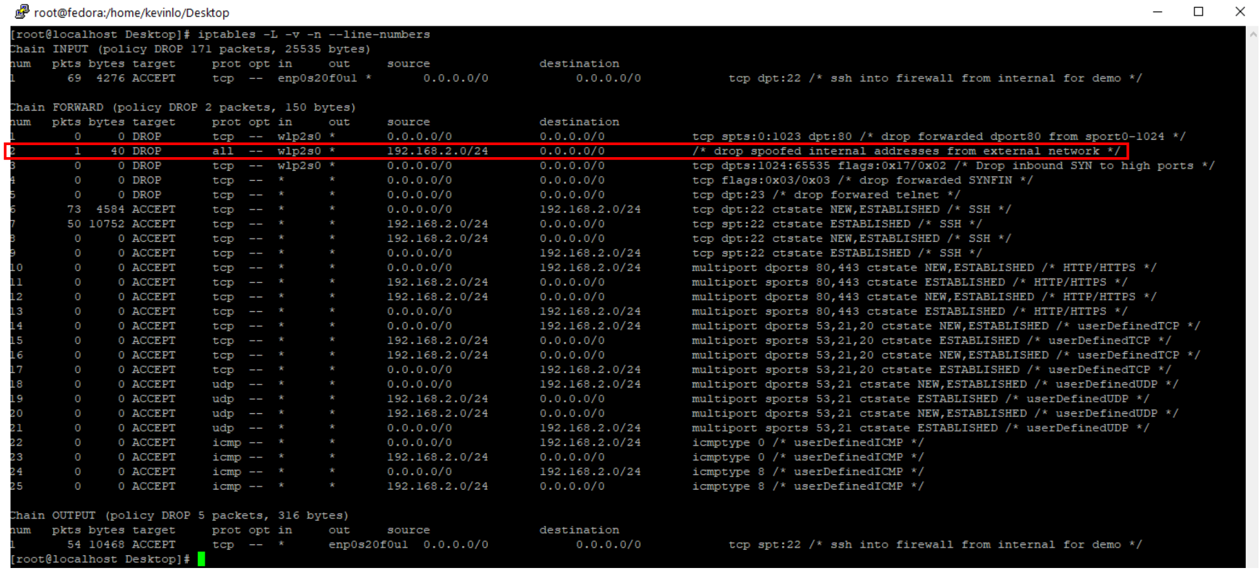
4.1.12 Test 7 – Inbound spoofed internal address from external NIC DROP

Firewall Lines (FORWARD chain)



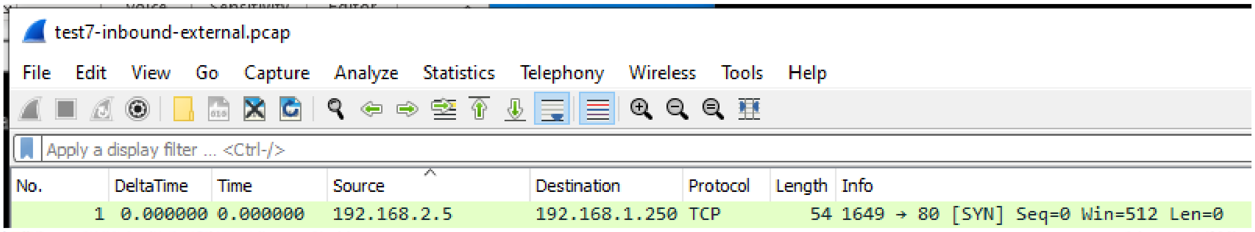
```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       10   688 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forward telnet */
6        8   576 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7        5   648 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        6   672 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After



root@fedora:/home/kevinlo/Desktop

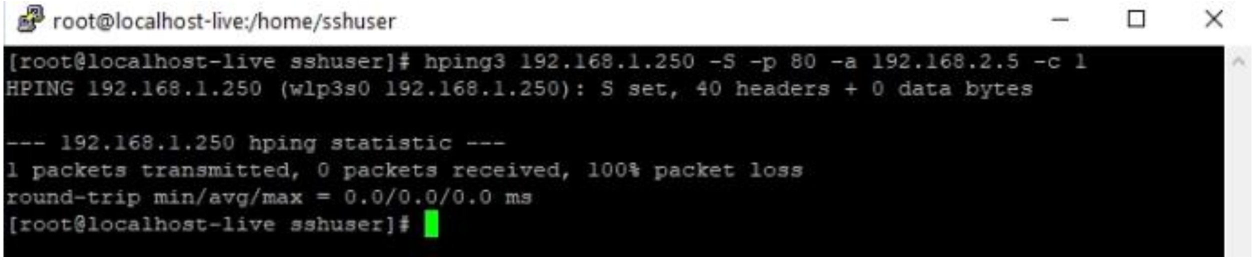
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 171 packets, 25535 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       69  4276 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 2 packets, 150 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        1    40 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6       73  4584 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7       50 10752 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 5 packets, 316 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       54 10468 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```



test7-inbound-external.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime Time      Source        Destination    Protocol Length Info
    1 0.000000  0.000000  192.168.2.5   192.168.1.250  TCP          54 1649 → 80 [SYN] Seq=0 Win=512 Len=0
```



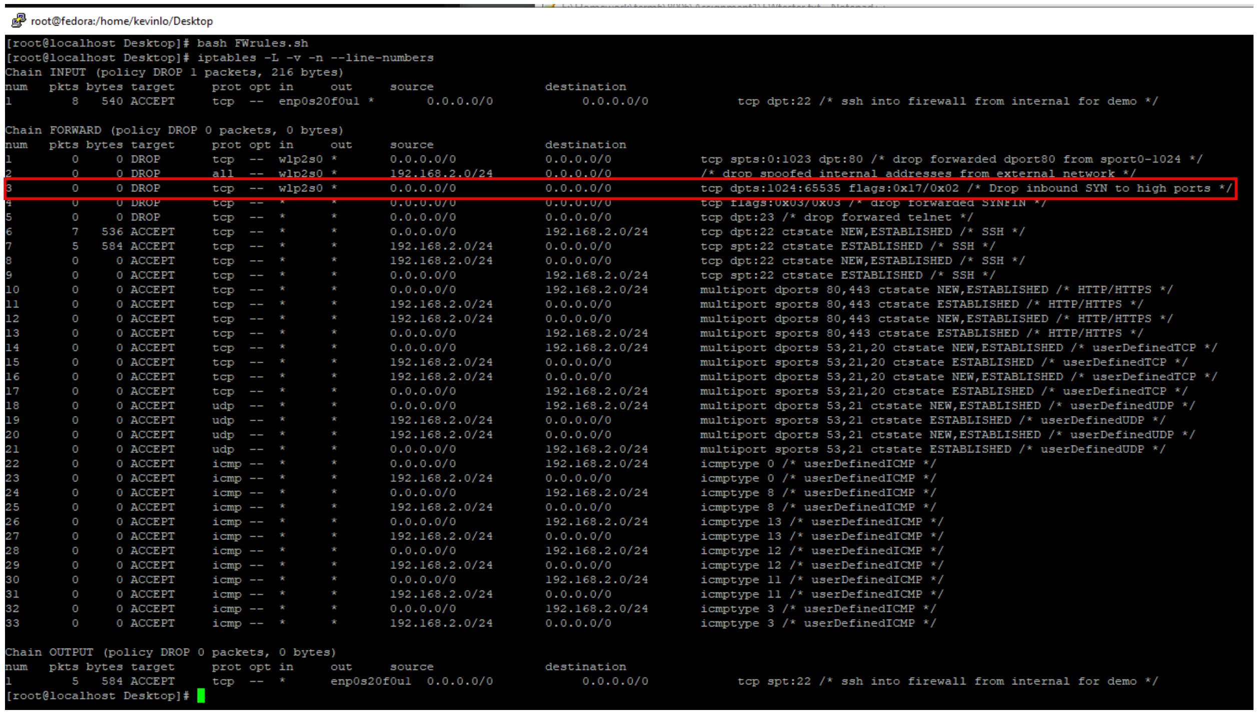
root@localhost-live:/home/sshuser

```
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -p 80 -a 192.168.2.5 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost-live sshuser]#
```

Both the internal and firewall did not have the packet with the spoofed address show up in the packet capture, external host spoofed an address in the 192.168.2.0/24 range which falls under the spoof drop rule which matched and successfully dropped the packet.

4.1.13 Test 8 – Inbound to high ports 1024-65535 DROP

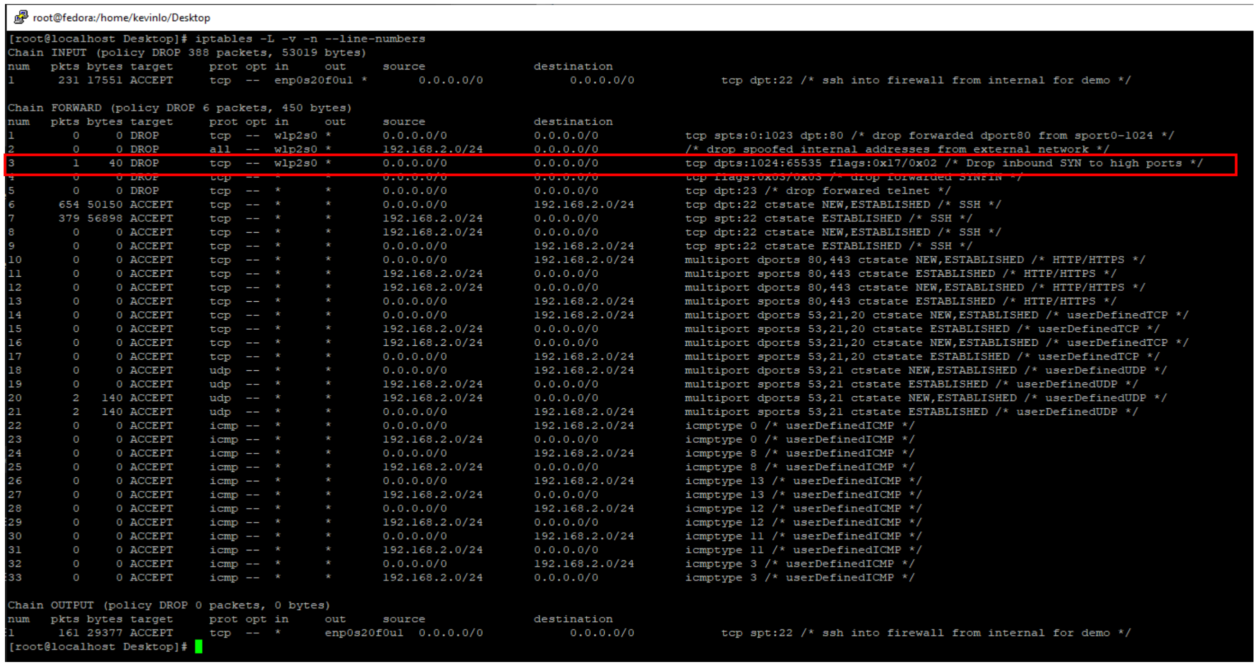
Firewall Lines (FORWARD chain)



root@fedora:/home/kevinlo/Desktop

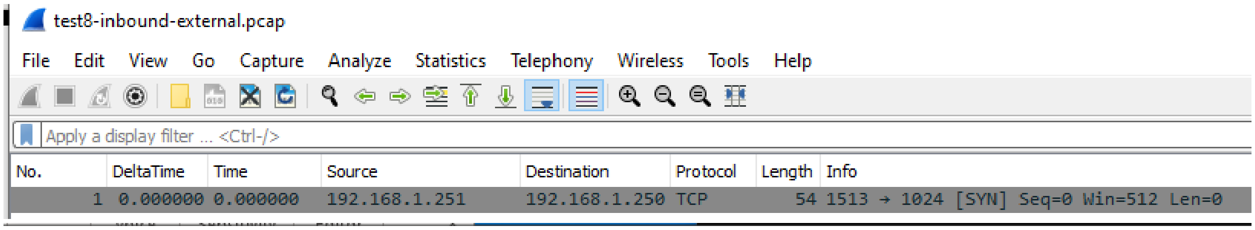
```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 1 packets, 216 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        8   540 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6        7   536 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7        5   584 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        5   584 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After



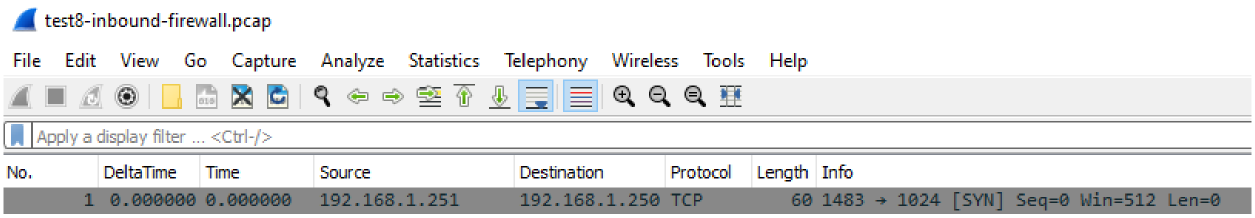
root@fedora:/home/kevinlo/Desktop

```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 388 packets, 53019 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      231 17551 ACCEPT     tcp  --  enp0s20f0ul *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 6 packets, 450 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        1    40 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6      654 50150 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      379 56898 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       2   140 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       2   140 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */
26       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 13 /* userDefinedICMP */
27       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 13 /* userDefinedICMP */
28       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 12 /* userDefinedICMP */
29       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 12 /* userDefinedICMP */
30       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 11 /* userDefinedICMP */
31       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 11 /* userDefinedICMP */
32       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 3 /* userDefinedICMP */
33       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 3 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      161 29377 ACCEPT     tcp  --  *      enp0s20f0ul  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```



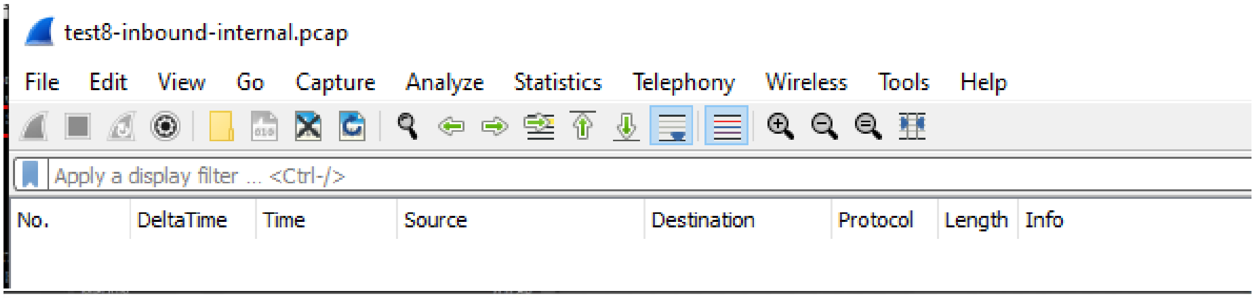
test8-inbound-external.pcap

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	54	1513 → 1024 [SYN] Seq=0 Win=512 Len=0



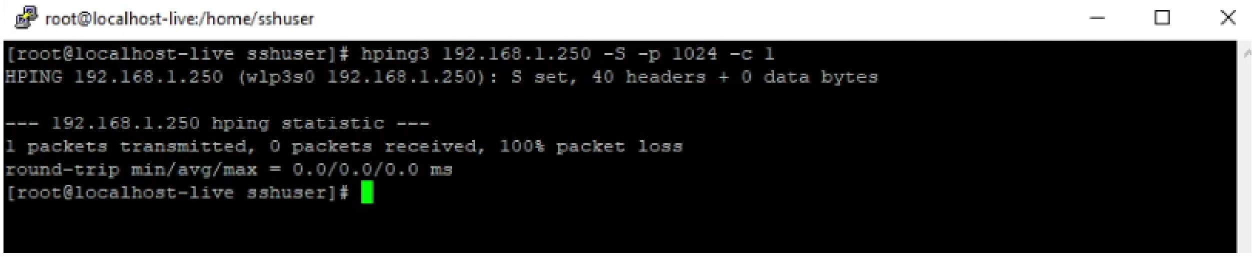
test8-inbound-firewall.pcap

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	60	1483 → 1024 [SYN] Seq=0 Win=512 Len=0



test8-inbound-internal.pcap

No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info

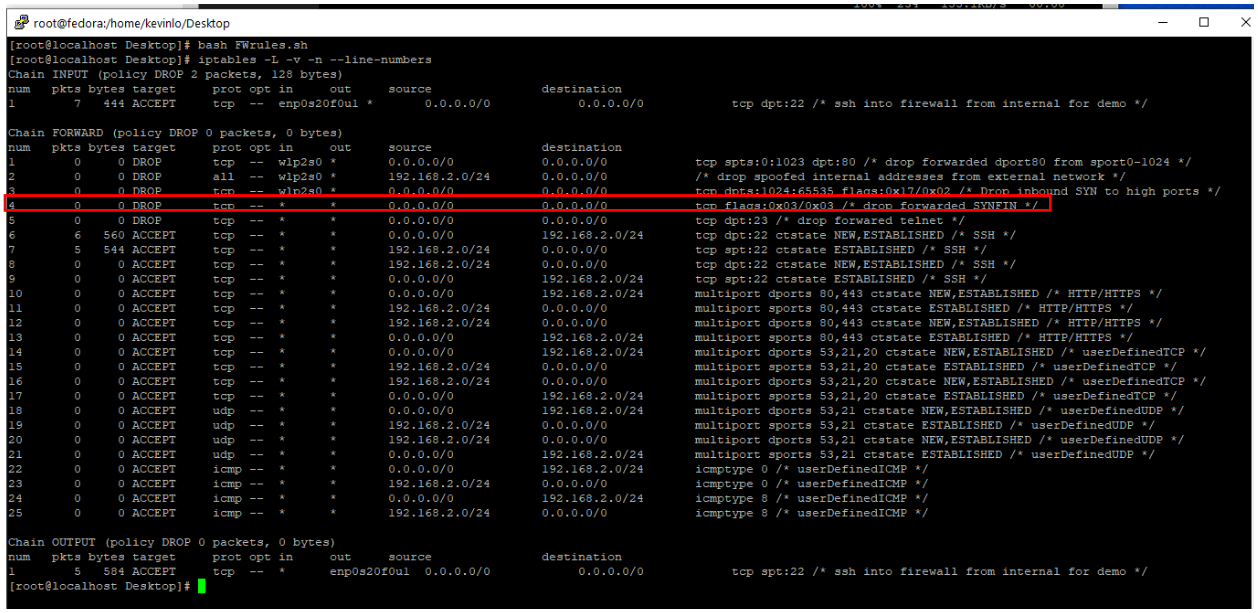

root@localhost-live:/home/sshuser

```
[root@localhost-live sshuser]# hping3 192.168.1.250 -S -p 1024 -c 1
HPING 192.168.1.250 (wlp3s0 192.168.1.250): S set, 40 headers + 0 data bytes

--- 192.168.1.250 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@localhost-live sshuser]# 
```

The packet going to high port dport 1024 was dropped at the firewall and successfully prevented it from reaching the internal network.

4.1.13 Test 9 – SYNFIN Packets DROP

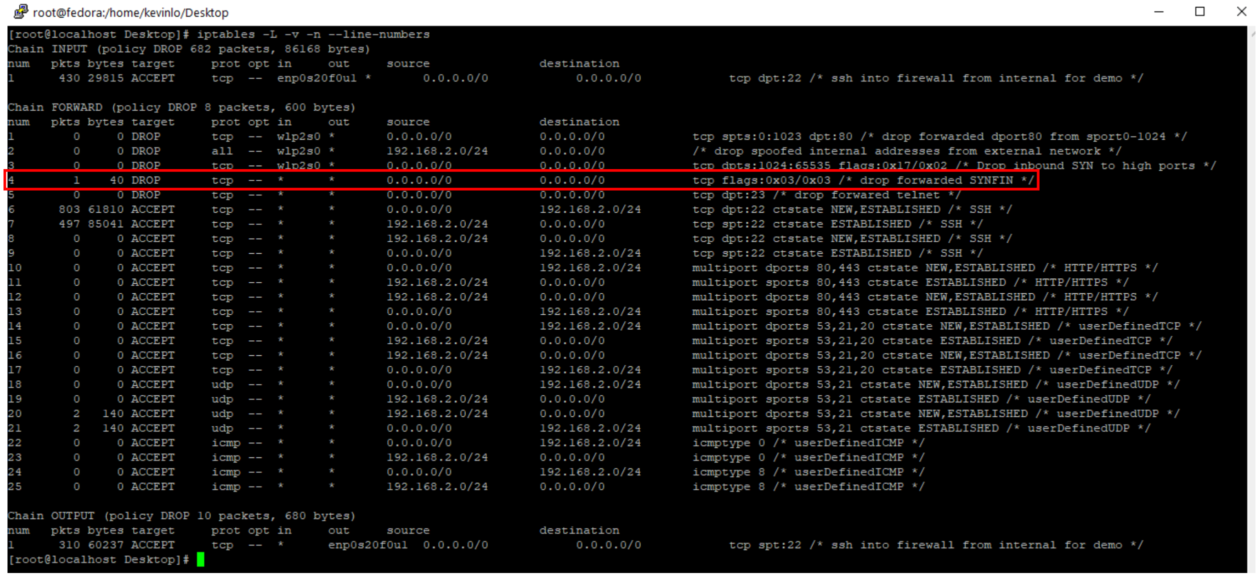
Firewall Lines (FORWARD chain)



root@fedora:/home/kevinlo/Desktop

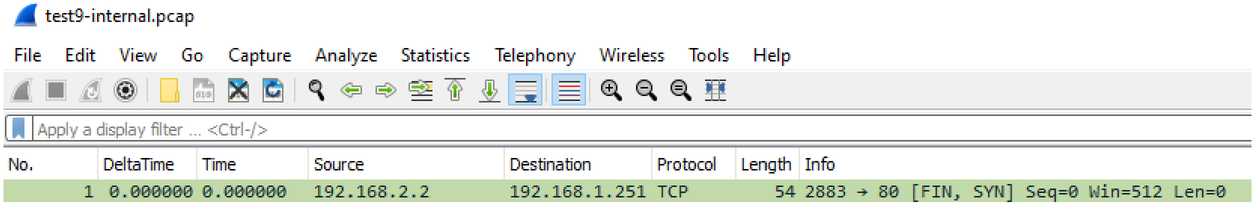
```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 2 packets, 128 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        7   444 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6        6   560 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7        5   544 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        5   584 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

After



root@fedora:/home/kevinlo/Desktop

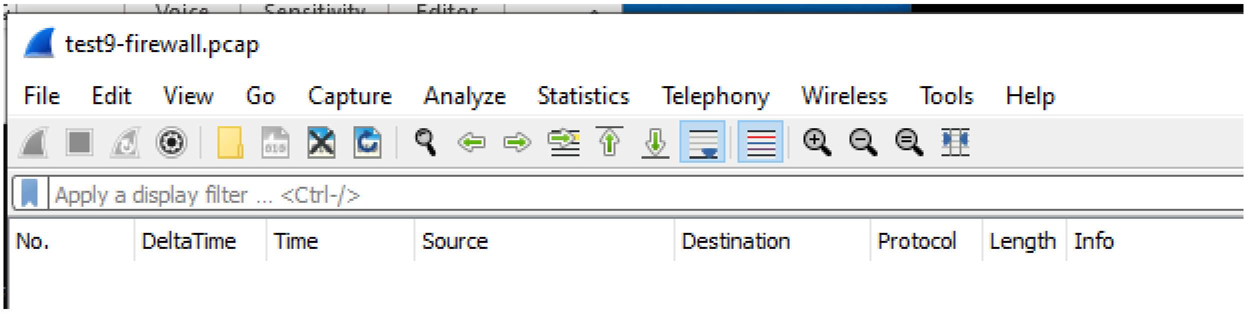
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 682 packets, 86168 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      430 29815 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 8 packets, 600 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        1    40 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6      803 61810 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      497 85041 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       2   140 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       2   140 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 10 packets, 680 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      310 60237 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```



test9-internal.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

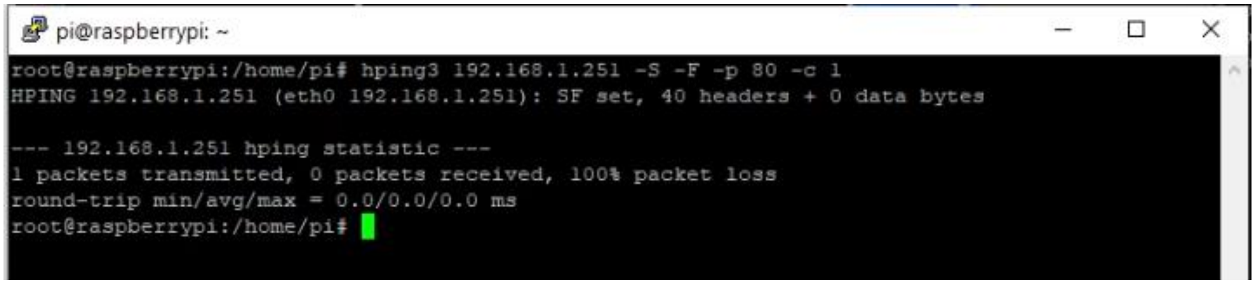
```
No.   DeltaTime  Time      Source       Destination    Protocol Length Info
    1 0.000000   0.000000  192.168.2.2  192.168.1.251  TCP      54 2883 → 80 [FIN, SYN] Seq=0 Win=512 Len=0
```



test9-firewall.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   DeltaTime  Time  Source  Destination  Protocol  Length  Info
```



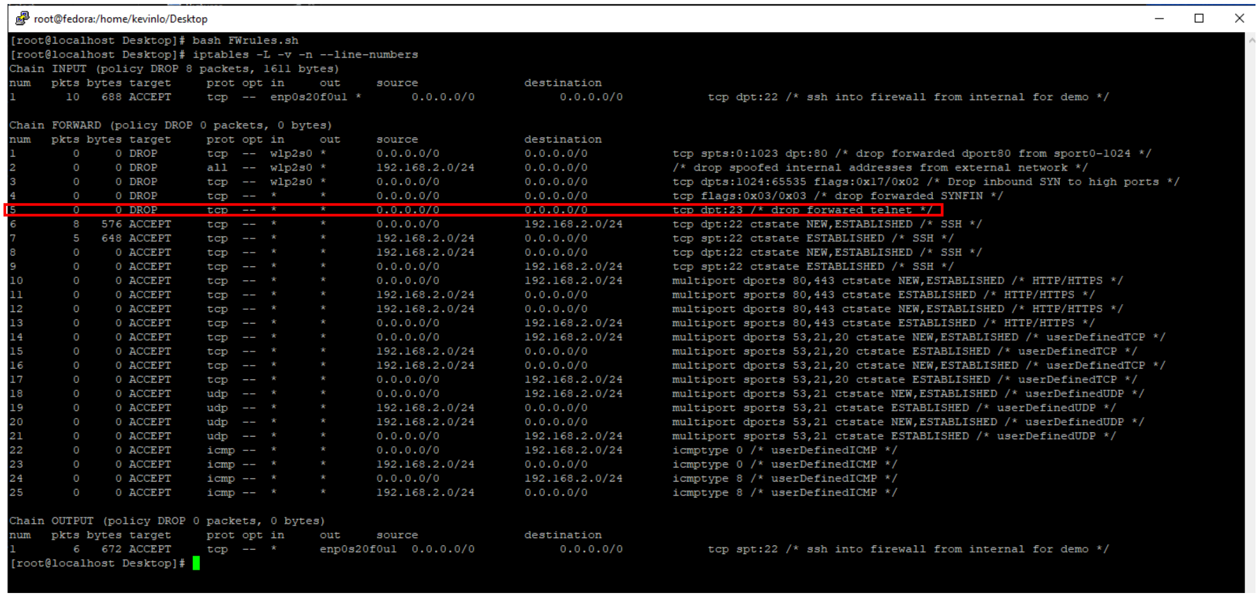
pi@raspberrypi: ~

```
root@raspberrypi:/home/pi# hping3 192.168.1.251 -S -F -p 80 -c 1
HPING 192.168.1.251 (eth0 192.168.1.251): SF set, 40 headers + 0 data bytes

--- 192.168.1.251 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@raspberrypi:/home/pi#
```

The SYN,FIN packet was successfully dropped at the firewall

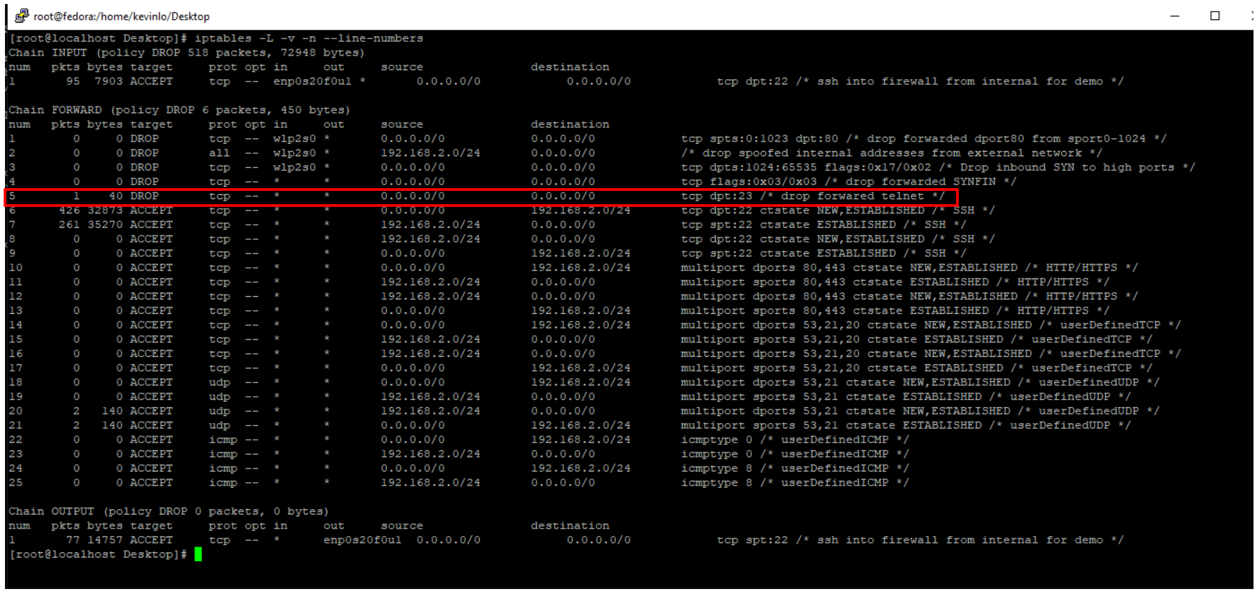
4.1.13 Test 10 – Telnet dport 23 DROP

Firewall Lines (FORWARD chain)

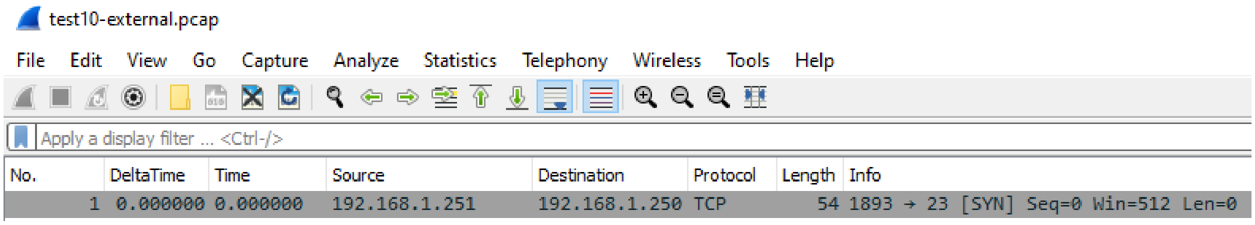


```
[root@localhost Desktop]# bash FWrules.sh
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 8 packets, 1611 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       10   688 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6        8   576 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7        5   648 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        6   672 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```

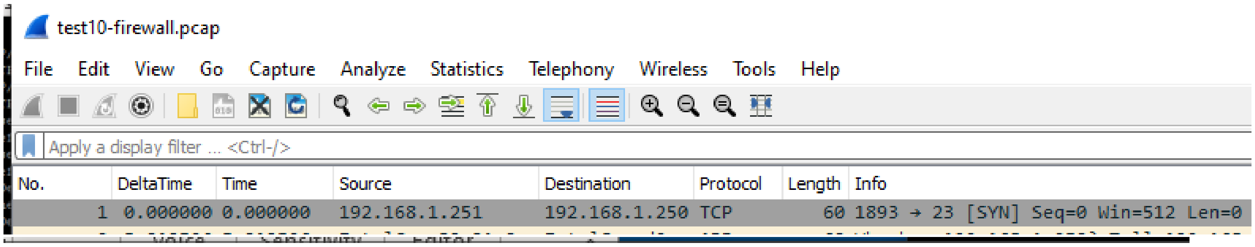
After



```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 518 packets, 72948 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       95  7903 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 6 packets, 450 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        1    40 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwarded telnet */
6      426 32873 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      261 35270 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       2   140 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       2   140 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       77 14757 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
[root@localhost Desktop]#
```



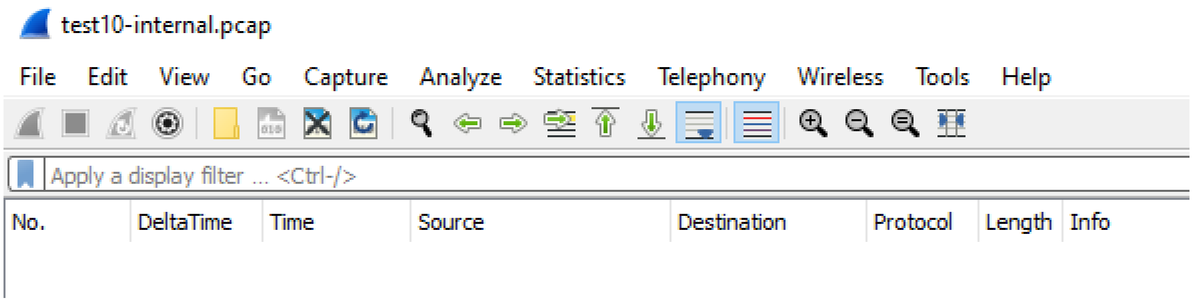
No.	DeltaTime	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.000000	192.168.1.251	192.168.1.250	TCP	54	1893 → 23 [SYN] Seq=0 Win=512 Len=0



test10-firewall.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   DeltaTime Time     Source         Destination    Protocol Length Info
    1 0.000000  0.000000 192.168.1.251  192.168.1.250  TCP          60 1893 → 23 [SYN] Seq=0 Win=512 Len=0
```



test10-internal.pcap

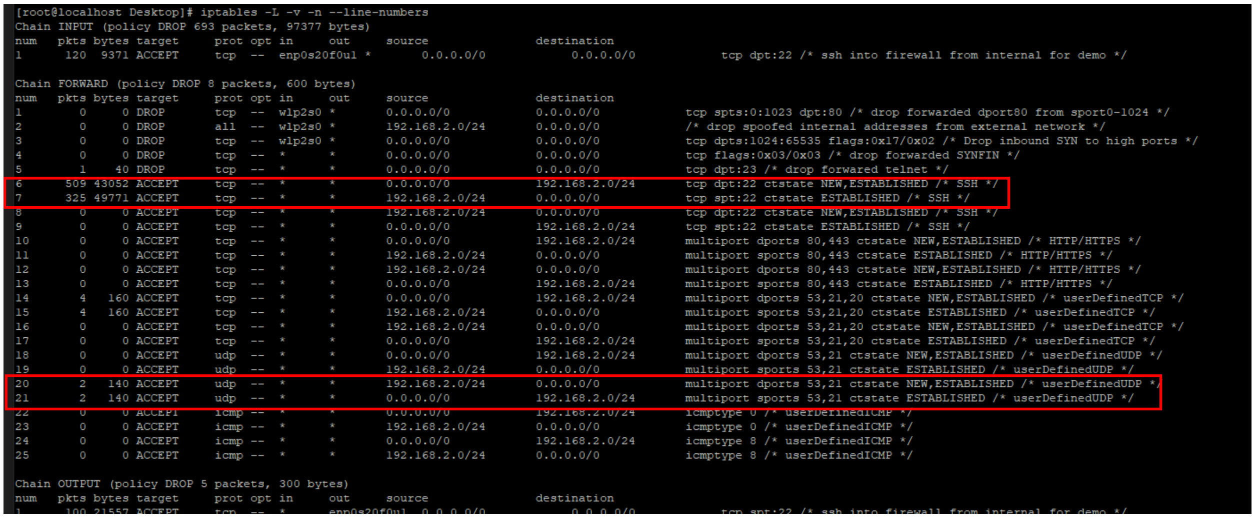
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   DeltaTime   Time   Source   Destination   Protocol   Length   Info
```

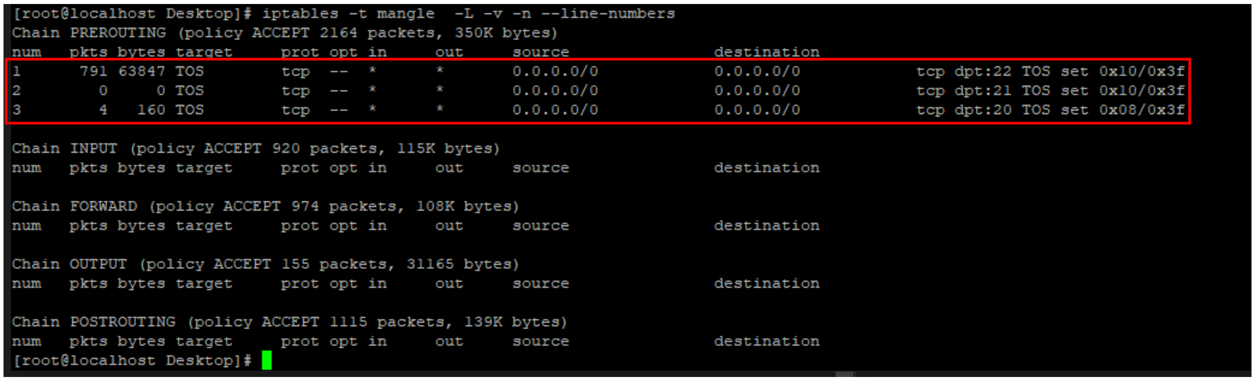
The firewall successfully dropped the dport 23 telnet packet coming from the external network into the internal network and prevented it from reaching the internal host.

4.1.13 Test 11 – FTP and SSH having their TOS set with Minimum Delay & Maximum Throughput

Firewall Lines (FORWARD chain)



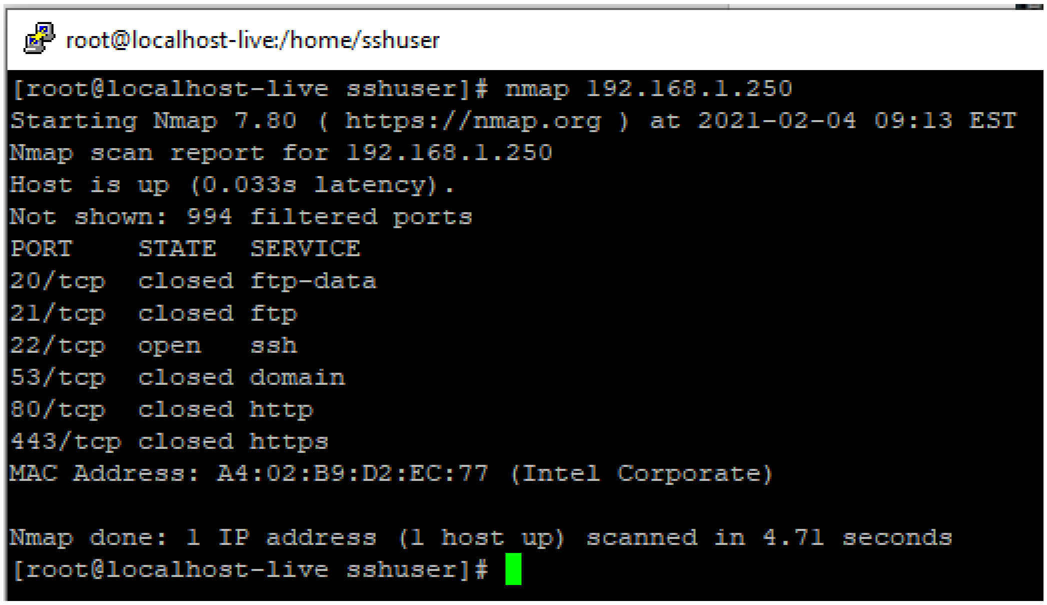
```
[root@localhost Desktop]# iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 693 packets, 97377 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      120  9371 ACCEPT     tcp  --  enp0s20f0u1 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 /* ssh into firewall from internal for demo */

Chain FORWARD (policy DROP 8 packets, 600 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp spts:0:1023 dpt:80 /* drop forwarded dport80 from sport0-1024 */
2        0     0 DROP       all  --  wlp2s0 *       192.168.2.0/24       0.0.0.0/0            /* drop spoofed internal addresses from external network */
3        0     0 DROP       tcp  --  wlp2s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpts:1024:65535 flags:0x17/0x02 /* Drop inbound SYN to high ports */
4        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x03/0x03 /* drop forwarded SYNFIN */
5        1    40 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:23 /* drop forwared telnet */
6      509 43052 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
7      325 49771 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp spt:22 ctstate ESTABLISHED /* SSH */
8        0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED /* SSH */
9        0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       tcp spt:22 ctstate ESTABLISHED /* SSH */
10       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
11       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
12       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 80,443 ctstate NEW,ESTABLISHED /* HTTP/HTTPS */
13       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 80,443 ctstate ESTABLISHED /* HTTP/HTTPS */
14       4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
15       4   160 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
16       0     0 ACCEPT     tcp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21,20 ctstate NEW,ESTABLISHED /* userDefinedTCP */
17       0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21,20 ctstate ESTABLISHED /* userDefinedTCP */
18       0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
19       0     0 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
20       2   140 ACCEPT     udp  --  *      *       192.168.2.0/24       0.0.0.0/0            multiport dports 53,21 ctstate NEW,ESTABLISHED /* userDefinedUDP */
21       2   140 ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.2.0/24       multiport sports 53,21 ctstate ESTABLISHED /* userDefinedUDP */
22       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 0 /* userDefinedICMP */
23       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 0 /* userDefinedICMP */
24       0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            192.168.2.0/24       icmptype 8 /* userDefinedICMP */
25       0     0 ACCEPT     icmp --  *      *       192.168.2.0/24       0.0.0.0/0            icmptype 8 /* userDefinedICMP */

Chain OUTPUT (policy DROP 5 packets, 300 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      100 21557 ACCEPT     tcp  --  *      enp0s20f0u1  0.0.0.0/0            0.0.0.0/0            tcp spt:22 /* ssh into firewall from internal for demo */
```



```
[root@localhost Desktop]# iptables -t mangle  -L -v -n --line-numbers
Chain PREROUTING (policy ACCEPT 2164 packets, 350K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      791 63847 TOS        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:22 TOS set 0x10/0x3f
2        0     0 TOS        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:21 TOS set 0x10/0x3f
3        4   160 TOS        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp dpt:20 TOS set 0x08/0x3f

Chain INPUT (policy ACCEPT 920 packets, 115K bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 974 packets, 108K bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 155 packets, 31165 bytes)
num   pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 1115 packets, 139K bytes)
num   pkts bytes target     prot opt in     out     source               destination
[root@localhost Desktop]#
```

SSH and FTP successfully have Minimum Delay and Maximum Throughput TOS bits set because it shows that some packets have been modified according to the iptables -t mangle table

4.1.13 Test 12 – nmap



```
[root@localhost-live sshuser]# nmap 192.168.1.250
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-04 09:13 EST
Nmap scan report for 192.168.1.250
Host is up (0.033s latency).
Not shown: 994 filtered ports
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  closed ftp
22/tcp  open   ssh
53/tcp  closed domain
80/tcp  closed http
443/tcp closed https
MAC Address: A4:02:B9:D2:EC:77 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 4.71 seconds
[root@localhost-live sshuser]#
```

The nmap scan shows that the TCP ports I opened are there and available.

4.2 Verdict

17 out of 17 tests were successful.

5 Conclusion

This report tests out the features of iptables rules to make sure it can satisfy the requirements of the COMP 8006 assignment 1. The response back from certain ports is not always from the same ports or protocol. This report also demonstrates how to set up the scripts to replicate the iptables rules to perform this test and setup the firewall and internal host. All my tests passed successfully which shows that my iptables rules are made to specification.