COMP 8006 Assignment 1 Testing Doc

Alex Zielinski – A00803488

02/01/2018

Table of Contents

Test Cases

Test Case	Test Description	Tool Used	Expected Results	Pass/Fails
1	Accept inbound/ outbound HTTP (port 80) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this up	Pass
2	Drop inbound HTTP (port 80) traffic with source port lower than port 1024	hping3	Hping3 results should be 100% packet loss with iptables logs backing this up	Pass
3	Accept inbound/ outbound HTTPS (port 443) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass
4	Accept inbound/ outbound SSH (port 22) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass
5	Accept inbound/outbound DNS (port 53) traffic	hping3	Hping3 results should be 0% packet loss with iptables logs backing this	Pass
6	Drop all port 0 traffic	hping3	Hping3 results should be 100% packet loss with iptables logs backing this	Pass
7	Test if web traffic via web browser works	Web browser	Web page should be visible. HTTP, HTTPS and DNS traffic should be visible in iptables logs	Pass

Note: Two lab computers were used for these tests. ***Computer A*** (192.168.0.19) was running the firewall and ***Computer B*** (192.168.0.18) was running hping3. The following iptables command was used to view logs of chains: ***iptables -L -n -v -x*** .

There are three user defined chains (UDC): WWW_ACCT, SSH_ACCT, and OTHER_ACCT. The first UDC contains rules for HTTP and HTTPS traffic. The second UDC contains rules for SHH traffic and the third UDC contains rules for other traffic. The UDC's also implemented IP accounting.

Please refer to the design doc located in the project folder's top directory for a detailed description of how the firewall script works.

Test Case 1.

- To ensure that inbound and outbound HTTP (port 80) traffic is permitted. Hping3 was used to send 4 packets from computer A to computer B with a source port of 7000 and a destination port of 80. Hping3 results state 0% packet loss with the 4 transmitted packets.

```
19:34:27(-)root@datacomm-18:~$ hping3 192.168.0.19 -s 7000 -k -p 80
HPING 192.168.0.19 (eno1 192.168.0.19): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.0.19 ttl=64 DF id=50182 sport=80 flags=RA seq=0 win=0 rtt=1.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=50733 sport=80 flags=RA seq=0 win=0 rtt=1001.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=51180 sport=80 flags=RA seq=0 win=0 rtt=2001.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=52069 sport=80 flags=RA seq=0 win=0 rtt=3002.9 ms
^C
--- 192.168.0.19 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

- Before the test the iptables logs for INPUT chain and OUTPUT chain show:

INPUT CHAIN

```
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

OUTPUT CHAIN

```
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   0     0            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

- After the test the iptables log show:

INPUT CHAIN

```
4   160 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

OUTPUT CHAIN

```
4   160 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   8   320            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
   4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

- Notice the INPUT chain took the 4 inbound packets and forwarded them to the WWW_ACCT chain where they were accepted. The same can be seen happening within the OUTPUT chain where the packets were forwarded to the WWW_ACCT chain and the outbound traffic was accepted.

Test Case 2.

- To ensure that inbound http packets with a source port lower than 1024 are being dropped. Hping3 was used to send 5 packets from computer A to computer B with a source port of 10 and a destination port of 80. Hping3 results state 100% packet loss (note: in test case 1 the source port was 7000 and the traffic was accepted).

```
19:48:17(-)root@datacomm-18:~$ hping3 192.168.0.19 -s 10 -k -p 80
HPING 192.168.0.19 (eno1 192.168.0.19): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.19 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
```

- Before the test the iptables logs for INPUT chain and OUTPUT chain show:

INPUT CHAIN

```
0    0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0    0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

OUTPUT CHAIN

```
0    0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0    0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   0     0            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

- After the test the iptables log show:

INPUT CHAIN

```
5   200 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

OUTPUT CHAIN

```
0    0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0    0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   5   200            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   5   200 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
```

- Notice that the INPUT chain took the 5 inbound packets and forwarded them to the WWW_ACCT chain where the packets were dropped. As a result, 0 packets went through the OUTPUT chain.

Test Case 3.

- To ensure that inbound and outbound HTTPS (port 443) traffic is permitted. Hping3 was used to send 4 packets from computer A to computer B with a source port of 7000 and a destination port of 443. Hping3 results state 0% packet loss.

```
19:55:52(-)root@datacomm-18:~$ hping3 192.168.0.19 -s 7000 -k -p 443
HPING 192.168.0.19 (eno1 192.168.0.19): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.0.19 ttl=64 DF id=41441 sport=443 flags=RA seq=0 win=0 rtt=1.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=42432 sport=443 flags=RA seq=0 win=0 rtt=1001.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=43054 sport=443 flags=RA seq=0 win=0 rtt=2000.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=43115 sport=443 flags=RA seq=0 win=0 rtt=3000.8 ms
^C
--- 192.168.0.19 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

- Before the test the iptables chain logs show:

INPUT CHAIN

```
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

OUTPUT CHAIN

```
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   0     0            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

- After the test the iptables chain logs show:

INPUT CHAIN

```
4   160 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

OUTPUT CHAIN

```
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
4   160 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   8   320            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
   4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
   4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

- Notice the INPUT chain took the 4 inbound packets and forwarded them to the WWW_ACCT chain where they were accepted. The same can be seen happening within the OUTPUT chain where the packets were forwarded to the WWW_ACCT chain and the outbound HTTPS traffic was accepted.

Test Case 4.

- To ensure that inbound and outbound SSH (port 22) traffic is permitted. Hping3 was used to send 4 packets from computer A to computer B with a source port of 7000 and a destination port of 22. Hping3 results state 0% packet loss.

```
20:05:13(-)root@datacomm-18:~$ hping3 192.168.0.19 -s 7000 -k -p 22 -S
HPING 192.168.0.19 (eno1 192.168.0.19): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.19 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1.8 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=1001.8 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=2001.8 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=3001.8 ms
^C
--- 192.168.0.19 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

- Before the test the iptables chain logs show:

INPUT CHAIN

```
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

OUTPUT CHAIN

```
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

SSH_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   0     0            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:22
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:22
```

- After the test the iptables chain logs show:

INPUT CHAIN

```
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
8   320 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

OUTPUT CHAIN

```
4   176 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

SSH_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
  12   496            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   4   176 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
   8   320 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:22
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:22
```

- Notice the INPUT chain took the 4 inbound SSH packets and forwarded them to the SSH_ACCT chain where they were accepted. The same can be seen happening within the OUTPUT chain where the packets were forwarded to the SSH_ACCT chain and the outbound SSH traffic was accepted.

Test Case 5.

- To ensure that inbound and outbound DNS (port 53) traffic is permitted. Hping3 was used to send 4 packets from computer A to computer B with a source port of 7000 and a destination port of 53. Hping3 results state 0% packet loss.

```
20:13:22(-)root@datacomm-18:~$ hping3 192.168.0.19 -s 7000 -k -p 53
HPING 192.168.0.19 (eno1 192.168.0.19): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.0.19 ttl=64 DF id=8243 sport=53 flags=RA seq=0 win=0 rtt=1.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=8383 sport=53 flags=RA seq=0 win=0 rtt=1001.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=8968 sport=53 flags=RA seq=0 win=0 rtt=2001.9 ms
DUP! len=46 ip=192.168.0.19 ttl=64 DF id=9896 sport=53 flags=RA seq=0 win=0 rtt=3001.9 ms
^C
--- 192.168.0.19 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
```

- Before the test the iptables chain logs show:

INPUT CHAIN

```
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

OUTPUT CHAIN

```
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

OTHER_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   0     0            all  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

- After the test the iptables chain logs show:

INPUT CHAIN

```
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
8   320 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

OUTPUT CHAIN

```
4   176 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
```

OTHER_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
  13  1416            all  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
   4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   4   160 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

- Notice the INPUT chain took the inbound DNS packets and forwarded them to the OTHER_ACCT chain where they were accepted. The same can be seen happening within the OUTPUT chain where the packets were forwarded to the OTHER_ACCT chain and the outbound DNS traffic was accepted.

Test Case 6.

- To ensure that all port 0 traffic is dropped. Hping3 was used to send 4 packets from computer A to computer B with a source port of 7000 and a destination port of 0. Hping3 results state 100% packet loss.

```
20:13:33(-)root@datacomm-18:~$ hping3 192.168.0.19 -s 7000 -k -p 0
HPING 192.168.0.19 (eno1 192.168.0.19): NO FLAGS are set, 40 headers + 0 data bytes
^C
--- 192.168.0.19 hping statistic ---
4 packets transmitted, 0 packets received, 100% packet loss
```

- Before the test the iptables chain logs show:

INPUT CHAIN

```
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
```

OUTPUT CHAIN

```
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
```

OTHER_ACCT CHAIN

```
 pkts bytes target     prot opt in     out     source               destination
    0     0            all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
```

- After the test the iptables chain logs show:

INPUT CHAIN

```
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
 4   160 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
```

OUTPUT CHAIN

```
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
 0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
 0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
```

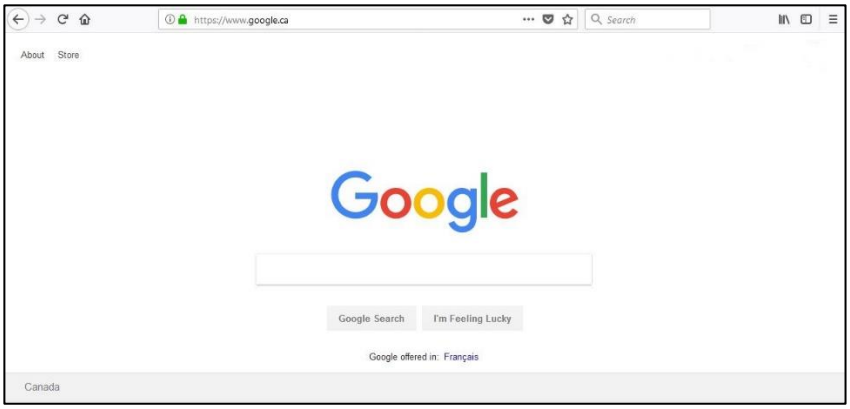
OTHER_ACCT CHAIN

```
 pkts bytes target     prot opt in     out     source               destination
   16  2806            all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
    4   160 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
    0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
```

- Notice the INPUT chain took the inbound packets and forwarded them to the OTHER_ACCT chain where they were dropped. As a result, no port 0 outbound traffic is created.

Test Case 7.

- To ensure that the web browser can be accessed while the firewall is running. On computer B where the firewall was running a web browser (Firefox) was opened to where the home page of Google was displayed.



- Before the test the iptables chain logs show:

INPUT CHAIN

```
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
0     0 SSH_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:22
0     0 SSH_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:22
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:443
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:443
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

OUTPUT CHAIN

```
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
0     0 SSH_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
0     0 SSH_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:22
0     0 SSH_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:22
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:443
0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:443
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

OTHER_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
   0     0            all  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

- After the test the iptables chain logs show:

INPUT CHAIN

```
  0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
 25  6854 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
  0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
221  433K WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:443
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:443
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
  0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
  0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
  0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
 36  4484 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

OUTPUT CHAIN

```
 33  5129 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
  0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
231 22243 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
  0     0 WWW_ACCT   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:443
  0     0 WWW_ACCT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:443
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
  0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
  0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  0     0 OTHER_ACCT  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
 36  2320 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
  0     0 OTHER_ACCT  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

OTHER_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
  72  6804            all  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:0
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:0
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
   0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:53
  36  2320 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
  36  4484 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:53
```

WWW_ACCT CHAIN

```
pkts bytes target     prot opt in     out     source               destination
 510  467K            tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0            udp  --  *      *       0.0.0.0/0            0.0.0.0/0
   0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:0:1023 dpt:80
   0     0 DROP       udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spts:0:1023 dpt:80
  33  5129 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
  25  6854 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:80
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:80
   0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp spt:80
 231 22243 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
 221  433K ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:443
```

- Inbound and outbound HTTP, HTTPS and DNS traffic can be seen being forwarded to the OTHER_ACCT chain (for DNS) and the WWW_ACCT chain (for HTTP and HTTPS) and accepted.