Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

Rule #	Test Description	Tool Used	Expected Result	Pass/Fail
1)	Drop all **outgoing** packets, that are not accept by the rule in the firewall, due to the default policy. In order to test the default policies, the test will attempt to make a ftp connection on port 21	Hping3 and Firefox's FireFTP client.	• Expected result for hping3 is a message saying **"Operation not Permitted"** • Expected result for FireFtp is that it will **Hang and keep trying to connect until it times out**	Pass. Detailed results are attached below.
2)	Drop all **incoming** packets, that are not accept by the rule in the firewall and are dropped due to the default policy. In order to test the default policies, the test will attempt to make a ftp connection on port 21	Hping3	• Firewall should drop the packets and the send should not receive any packets back • Default policy Drop count should increase by number of packets send by the client.	Pass. Detailed results are attached below
3)	Drop any **outgoing** packets from port 0 for TCP	Hping3	• Drop count for port 0 in traffic-out should increase	Pass. Detailed results are attached below
4)	Drop any **incoming** packets from port 0 for TCP	Hping3	• Drop count for port 0 in traffic-in should increase	Pass. Detailed results are attached below
5)	Drop any **outgoing** packets from port 0 for UDP	Hping3	• Drop count for port 0 in traffic-out should increase	Pass. Detailed results are attached below
6)	Drop any **incoming** packets from port 0 for UDP	Hping3	• Drop count for port 0 in traffic-in should increase	Pass. Detailed results are attached below
7)	Verify that SSH traffic inbound/outbound is allowed	Log on to the ssh server from and external ssh client	• User should be able to ssh to another machine and also ssh to this machine from another machine, results can be seen in the ACCEPT count in the iptables traffic-in and traffic-out	Pass. Detailed Results are attached below

Testing Document

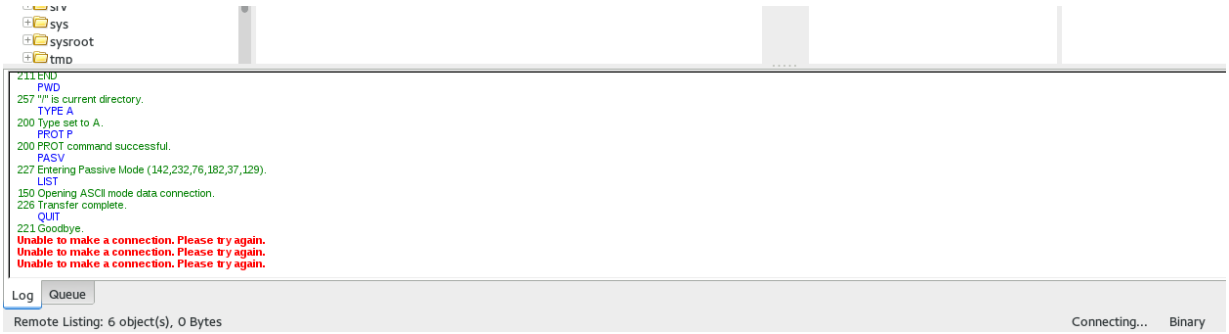
Jivanjot S. Brar A00774427 January 31, 2014

			chain	
8)	Verify that www(80, 443) traffic inbound/outbound is allowed	Browser, Hping3	• For outbound Browser should be able to access any http or https site. • For inbound hping3 should succeed in receiving packets	Pass. Detailed results are attached below
9)	Drop all packets with source port less than 1024 trying to connect to destination port 80	Hping3	• Hping3 should loose all the transmitted packets • iptables drop count should increase	Pass. Detailed results are attached below
10)	Drop all packets with source port less than 1024 trying to connect to destination port 443	Hping3	• Hping3 should loose all the transmitted packets • Iptables drop count should increase	Pass. Detailed results are attached below
11)	Drop all the **inbound** packets that come without a SYN for port 80, 443, ssh	Hping3	• Hping3 should loose all the transmitted packets • Iptables default policy drop count should increase	Pass. Detailed results are attached below
12)	Drop all the **inbound** packets that come with a syn packet unless there is a rule that permits inbound traffic	Hping3	• Hping3 should drop all packets with syn that come to any port except 80, 443, ssh (tested on port 53)	Pass. Detailed results are attached below
13)	Ip Accounting for www and ssh traffic	Open a browser and open any http or https site	• Iptables www-ssh-traffic counting increase with only incoming ssh or www packets (ports 80, 443)	Pass. Detailed results are attached below
14)	IP Accounting for rest of the traffic	Open a browser to any site	• Iptables noness-traffic counting should increase for any traffic except ssh and www	Pass. Detailed results are attached below

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

Detailed Results

Rule #	Results
1)	**HPING3** [root@BossLinux ~]# `iptables -Z` | hping3 -S 127.0.0.1 -p 21 -c 5 HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes [send_ip] sendto: Operation not permitted **FIREFTP** 
2)	**Before Testing Default Policy Drop Count** Chain INPUT (policy DROP 0 packets, 0 bytes) **After Testing Default Policy Drop Count for hping 192.168.0.22 -p 21 -c 5** Chain INPUT (policy DROP 5 packets, 200 bytes) **Status on the client machine** [root@DataComm ~]# hping3 -S 192.168.0.22 -p 21 -c 5 HPING 192.168.0.22 (em1 192.168.0.22): S set, 40 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 5 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
3)	**Before Testing Port 0 Drop Count** Chain traffic-out (1 references) pkts bytes target prot opt in out source destination 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0 0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:0 0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:0 **After Testing Port 0 Drop Count** Chain traffic-out (1 references) pkts bytes target prot opt in out source destination 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0 1 40 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

	0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:0 0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:0 **HPING3 MESSAGE** [root@DataComm ~]# hping3 192.168.0.23 -p 22 -s 0 -c 1 HPING 192.168.0.23 (em1 192.168.0.23): NO FLAGS are set, 40 headers + 0 data bytes [send_ip] sendto: Operation not permitted
4)	**Before Testing Port 0 Drop Count** Chain traffic-in (1 references) pkts bytes target prot opt in out source destination 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 Testing Port 0 Drop Count** Chain traffic-in (1 references) pkts bytes target prot opt in out source destination 1 40 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 **HPING3 MESSAGE** [root@DataComm ~]# hping3 -S 192.168.0.22 -p 22 -s 0 -c 1 HPING 192.168.0.22 (em1 192.168.0.22): S set, 40 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 1 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
5)	**Before Testing Port 0 Drop Count** Chain traffic-out (1 references) pkts bytes target prot opt in out source destination 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0 0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:0 0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:0 **After Testing Port 0 Drop Count** Chain traffic-out (1 references) pkts bytes target prot opt in out source destination 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:0 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:0 0 0 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:0

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

	1 28 DROP udp -- * * 0.0.0.0/0 0.0.0.0/0 udp spt:0 **HPING3 MESSAGE** [root@DataComm ~]# hping3 --udp 192.168.0.23 -p 22 -s 0 -c 1 HPING 192.168.0.23 (em1 192.168.0.23): udp mode set, 28 headers + 0 data bytes [send_ip] sendto: Operation not permitted
6)	**Before Testing Port 0 Drop Count** Chain traffic-in (1 references) pkts bytes target prot opt in out source destination 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 Testing Port 0 Drop Count** Chain traffic-in (1 references) pkts bytes target prot opt in out source destination 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 1 28 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 **HPING3 MESSAGE** [root@DataComm ~]# hping3 --udp 192.168.0.22 -p 22 -s 0 -c 1 HPING 192.168.0.22 (em1 192.168.0.22): udp mode set, 28 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 1 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
7)	**Before Testing** Chain traffic-in (1 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW,ESTABLISHED 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 state ESTABLISHED Chain traffic-out (1 references) pkts bytes target prot opt in out source destination 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 state ESTABLISHED 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW,ESTABLISHED **After Testing** Chain traffic-in (1 references) pkts bytes target prot opt in out source destination 2 80 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW,ESTABLISHED 1 44 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 state ESTABLISHED Chain traffic-out (1 references) pkts bytes target prot opt in out source destination 1 44 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spt:22 state ESTABLISHED

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

2 80 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 state NEW,ESTABLISHED

SSH MESSAGES

```
[root@DataComm ~]# ssh 192.168.0.23
root@192.168.0.23's password:
Last login: Fri Jan 31 14:30:38 2014 from 192.168.0.22

[root@DataComm ~]# ssh 192.168.0.22 The authenticity of host '192.168.0.22
(192.168.0.22)' can't be established. ECDSA key fingerprint is
0b:cb:0c:ff:6d:de:f5:ee:92:57:1a:f9:97:23:6b:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.22' (ECDSA) to the list of known hosts.
root@192.168.0.22's password:
Last login: Fri Jan 31 14:29:37 2014
```

8)

HTTPS

HTTP

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

INBOUND PORT 80

```
Chain traffic-in (7 references)
  pkts  bytes target  prot opt in  out  source        destination
    0     0 DROP    tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spts:0:1023 dpt:80
    0     0 DROP    tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spts:0:1023 dpt:443
   10   400 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:80 state NEW,ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:80 state ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:443 state NEW,ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:443 state ESTABLISHED
Chain traffic-out (7 references)
  pkts  bytes target  prot opt in  out  source        destination
    5   220 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:80 state ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:80 state NEW,ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:443 state ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:443 state NEW,ESTABLISHED
```

HPING3 MESSAGES

```
[root@DataComm ~]# hping3 -S 192.168.0.17 -p 80 -c 5 HPING 192.168.0.17 (em1 192.168.0.17): S
set, 40 headers + 0 data bytes len=46 ip=192.168.0.17 ttl=64 DF id=0 sport=80 flags=SA seq=0
win=29200 rtt=0.3 ms len=46 ip=192.168.0.17 ttl=64 DF id=0 sport=80 flags=SA seq=1
win=29200 rtt=0.4 ms len=46 ip=192.168.0.17 ttl=64 DF id=0 sport=80 flags=SA seq=2
win=29200 rtt=0.3 ms len=46 ip=192.168.0.17 ttl=64 DF id=0 sport=80 flags=SA seq=3
win=29200 rtt=0.3 ms len=46 ip=192.168.0.17 ttl=64 DF id=0 sport=80 flags=SA seq=4
win=29200 rtt=0.3 ms

--- 192.168.0.17 hping statistic --- 5 packets transmitted, 5 packets received, 0% packet loss round-
trip min/avg/max = 0.3/0.4/0.4 ms
```

INBOUND PORT 443

```
Chain traffic-in (7 references)
  pkts  bytes target  prot opt in  out  source        destination
    0     0 DROP    tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spts:0:1023 dpt:80
    0     0 DROP    tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spts:0:1023 dpt:443
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:80 state NEW,ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:80 state ESTABLISHED
    5   200 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:443 state NEW,ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:443 state ESTABLISHED
Chain traffic-out (7 references)
  pkts  bytes target  prot opt in  out  source        destination
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:80 state ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:80 state NEW,ESTABLISHED
    5   200 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp spt:443 state ESTABLISHED
    0     0 ACCEPT  tcp  --  *   *   0.0.0.0/0     0.0.0.0/0     tcp dpt:443 state NEW,ESTABLISHED
```

HPING3 MESSAGES

```
[root@DataComm ~]# hping3 -S 192.168.0.17 -p 443 -c 5 HPING 192.168.0.17 (em1 192.168.0.17):
S set, 40 headers + 0 data bytes len=46 ip=192.168.0.17 ttl=64 DF id=9388 sport=443 flags=RA
seq=0 win=0 rtt=0.3 ms len=46 ip=192.168.0.17 ttl=64 DF id=9389 sport=443 flags=RA seq=1
win=0 rtt=0.4 ms len=46 ip=192.168.0.17 ttl=64 DF id=9390 sport=443 flags=RA seq=2 win=0
rtt=0.3 ms len=46 ip=192.168.0.17 ttl=64 DF id=9391 sport=443 flags=RA seq=3 win=0 rtt=0.3
ms len=46 ip=192.168.0.17 ttl=64 DF id=9392 sport=443 flags=RA seq=4 win=0 rtt=0.3 ms

--- 192.168.0.17 hping statistic --- 5 packets transmitted, 5 packets received, 0% packet loss round-
trip min/avg/max = 0.3/0.3/0.4 ms
```

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

9)	**BEFORE TESTING** Chain traffic-in (7 references) pkts bytes target prot opt in out source destination 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:0:1023 dpt:80 **AFTER TESTING** Chain traffic-in (7 references) pkts bytes target prot opt in out source destination 7 280 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:0:1023 dpt:80 **HPING MESSAGES** [root@DataComm ~]# hping3 -S 192.168.0.22 -p 80 -s 1000 -c 7 HPING 192.168.0.22 (em1 192.168.0.22): S set, 40 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 7 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
10)	**BEFORE TESTING** Chain traffic-in (7 references) pkts bytes target prot opt in out source destination 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:0:1023 dpt:443 **AFTER TESTING** Chain traffic-in (7 references) pkts bytes target prot opt in out source destination 7 280 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp spts:0:1023 dpt:443 **HPING MESSAGES** [root@DataComm ~]# hping3 -S 192.168.0.22 -p 443 -s 1000 -c 7 HPING 192.168.0.22 (em1 192.168.0.22): S set, 40 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 7 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
11)	**BEFORE TESTING** Chain INPUT (policy DROP 0 packets, 0 bytes) Chain OUTPUT (policy DROP 0 packets, 0 bytes) **AFTER TESTING** Chain INPUT (policy DROP 7 packets, 280 bytes) Chain OUTPUT (policy DROP 0 packets, 0 bytes) **HPING MESSAGES** [root@DataComm ~]# hping3 192.168.0.22 -p 80 -c 7 HPING 192.168.0.22 (em1 192.168.0.22): NO FLAGS are set, 40 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 7 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
12)	**HPING MESSAGES** [root@DataComm ~]# hping3 -S 192.168.0.22 -p 53 -c 7 HPING 192.168.0.22 (em1 192.168.0.22): S set, 40 headers + 0 data bytes --- 192.168.0.22 hping statistic --- 7 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

13)

BEFORE TESTING

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts  bytes target     prot opt in     out     source           destination
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:22 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:22 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:80 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:80 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:443 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:443 state ESTABLISHED

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts  bytes target     prot opt in     out     source           destination
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:22 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:22 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:80 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:80 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:443 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:443 state NEW,ESTABLISHED

Chain www-ssh-traffic (12 references)
  pkts  bytes target     prot opt in     out     source           destination
     0     0          all  --  *      *       0.0.0.0/0          0.0.0.0/0
```

AFTER TESTING

```
Chain INPUT (policy DROP 2 packets, 152 bytes)
  pkts  bytes target     prot opt in     out     source           destination
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:22 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:22 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:80 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:80 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:443 state NEW,ESTABLISHED
    41 10538 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:443 state ESTABLISHED

Chain OUTPUT (policy DROP 2 packets, 152 bytes)
  pkts  bytes target     prot opt in     out     source           destination
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:22 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:22 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:80 state ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:80 state NEW,ESTABLISHED
     0     0 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp spt:443 state ESTABLISHED
    38 15154 www-ssh-traffic  tcp  --  *      *       0.0.0.0/0          0.0.0.0/0          tcp dpt:443 state NEW,ESTABLISHED

Chain www-ssh-traffic (12 references)
  pkts  bytes target     prot opt in     out     source           destination
    79 25692          all  --  *      *       0.0.0.0/0          0.0.0.0/0
```

14)

BEFORE TESTING

```
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts  bytes target     prot opt in     out     source           destination
     0     0 noness-traffic  all  --  *      *       0.0.0.0/0          0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts  bytes target     prot opt in     out     source           destination
     0     0 noness-traffic  all  --  *      *       0.0.0.0/0          0.0.0.0/0

Chain noness-traffic (12 references)
```

Testing Document

Jivanjot S. Brar A00774427 January 31, 2014

```
  pkts     bytes target    prot opt in     out    source           destination
    0       0          all  --  *      *      0.0.0.0/0          0.0.0.0/0
```

AFTER TESTING

```
Chain INPUT (policy DROP 2 packets, 152 bytes)
  pkts     bytes target    prot opt in     out    source           destination
    3     480 noness-traffic  all  --  *      *      0.0.0.0/0          0.0.0.0/0

Chain OUTPUT (policy DROP 2 packets, 152 bytes)
  pkts     bytes target    prot opt in     out    source           destination
    3     480 noness-traffic  all  --  *      *      0.0.0.0/0          0.0.0.0/0

Chain noness-traffic (2 references)
  pkts     bytes target    prot opt in     out    source           destination
    6     960          all  --  *      *      0.0.0.0/0          0.0.0.0/0
```