Test Documentation

Ben Soer

A00843110

COMP 8006

BTECH Set 6D

Table of Contents

Test Chart

Below is a breakdown chart of all the tests executed and the appropriate tests. Note that the Rule/Test # correspond directly to the iptables rule in the fwall.sh file and the hping3 test in the hping-tests.sh file. Each rule is commented with these numbers in the source files if you would like to see how each rule corresponds.

Rule/Test #	Test Description	Tool Used	Expected Result	Pass / Fail
DNS_T1	Accept UDP DNS Lookup Requests	Hping3 + Accounting Tables	Packet Accepted	PASS – See Test Results Section For Details
DNS_T2	Accept UDP DNS Lookup Responses	hping3	Packet Accepted	PASS – See Test Results Section For Details
DNS_T3	Accept TCP DNS Lookup Responses	hping3	Packet Accepted	PASS – See Test Results Section For Details
DNS_T4	Accept TCP DNS Lookup Responses	Hping3 + Accounting Tables	Packet Accepts	PASS – See Test Results Section For Details
SSH_T1A	Drop SSH Responses that are SYN	Hping3 + Accounting Tables	Packet Dropped	PASS – See Test Results Section For Details
SSH_T1B	Accept SSH Responses that are not SYN	hping3	Packet Accepts	PASS – See Test Results Section For Details
SSH_T2	Accept SSH Connection Request	hping3	Packet Accepts	PASS – See Test Results Section For Details
SSH_T3	Accept SSH Outbound Connection Request	Hping3 + Accounting Tables	Packet Accepts	PASS – See Test Results Section For Details
SSH_T4	Accept SSH Outbound Connection Responses that are not SYN	Accounting Tables	Packet Accepts	PASS – See Test Results Section For Details
HTTP_T1	DROP HTTP Connections from ports 0:1024 to port 80	hping3	Packet Dropped	PASS – See Test Results Section For Details
HTTP_T2	DROP HTTP	hping3	Packet Dropped	PASS – See Test

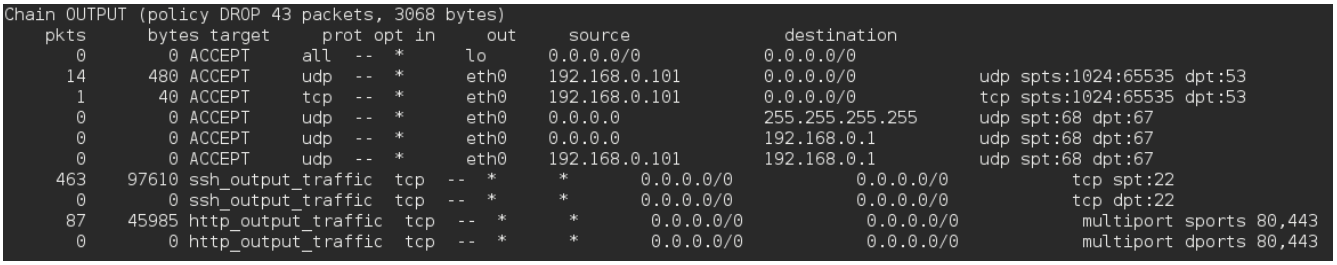
	Connections from 0:1024 to port 80			Results Section For Details
HTTP_T3	Accept HTTP Inbound Responses from port 80 that are not SYN	Hping3 + Accounting Tables	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T4	Accept HTTP Inbound Responses from port 443 that are not SYN	Hping3 + Accounting Tables	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T5	Accept HTTP Inbound Connections to port 80	Hping3	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T6	Accept HTTP Inbound Connections to port 443	Hping3	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T7	Accept HTTP Outbound Connections to port 80	Hping3	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T8	Accept HTTP Outbound Connections to port 443	Hping3	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T9	Accept HTTP Outbound Responses from port 80 that are not SYN	Hping3 + Accounting Tables	Packet Accepted	PASS – See Test Results Section For Details
HTTP_T10	Accept HTTP Outbound Responses from port 80 that are not SYN	Hping3 + Accounting Tables	Packet Accepted	PASS – See Test Results Section For Details
DHCP_T1	Do a full DHCP Renewal	dhclient	Renewal Succeeds	PASS – See Test Results Section For Details

Results

Below is the various screenshots of the test being run. The original images can be found in the /tests folder

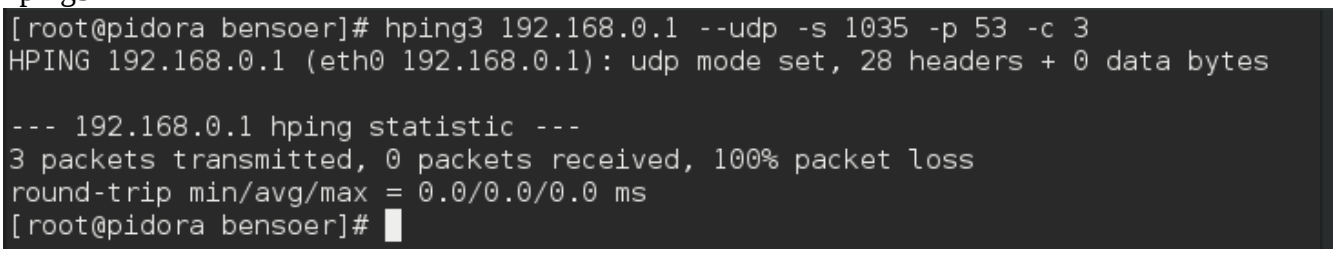
DNS_T1

Accounting Table Before



```
Chain OUTPUT (policy DROP 43 packets, 3068 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
      14      480 ACCEPT     udp  --  *      eth0    192.168.0.101        0.0.0.0/0           udp spts:1024:65535 dpt:53
       1       40 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:53
       0        0 ACCEPT     udp  --  *      eth0    0.0.0.0              255.255.255.255     udp spt:68 dpt:67
       0        0 ACCEPT     udp  --  *      eth0    0.0.0.0              192.168.0.1         udp spt:68 dpt:67
       0        0 ACCEPT     udp  --  *      eth0    192.168.0.101        192.168.0.1         udp spt:68 dpt:67
     463    97610 ssh_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
       0        0 ssh_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
      87    45985 http_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 80,443
       0        0 http_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
```

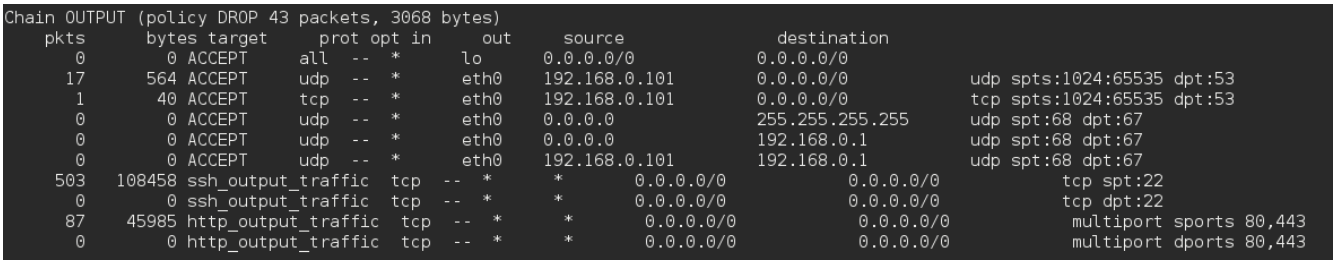
hping3



```
[root@pidora bensoer]# hping3 192.168.0.1 --udp -s 1035 -p 53 -c 3
HPING 192.168.0.1 (eth0 192.168.0.1): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.1 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@pidora bensoer]#
```

Accounting Table After



```
Chain OUTPUT (policy DROP 43 packets, 3068 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
      17      564 ACCEPT     udp  --  *      eth0    192.168.0.101        0.0.0.0/0           udp spts:1024:65535 dpt:53
       1       40 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:53
       0        0 ACCEPT     udp  --  *      eth0    0.0.0.0              255.255.255.255     udp spt:68 dpt:67
       0        0 ACCEPT     udp  --  *      eth0    0.0.0.0              192.168.0.1         udp spt:68 dpt:67
       0        0 ACCEPT     udp  --  *      eth0    192.168.0.101        192.168.0.1         udp spt:68 dpt:67
     503   108458 ssh_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
       0        0 ssh_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
      87    45985 http_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 80,443
       0        0 http_output_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
```

DNS_T2

Although 3 packets were sent, only 1 was accepted

Accounting Table Before

```
[root@pidora bensoer]# iptables -L -v -n -x
Chain INPUT (policy DROP 1497 packets, 247799 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       6      252 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
       6      374 ACCEPT     udp  --  eth0   *       0.0.0.0/0            192.168.0.101       udp spt:53 dpts:1024:65535
       1       40 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            192.168.0.101       tcp spt:53 dpts:1024:65535
       0        0 ACCEPT     udp  --  eth0   *       0.0.0.0              255.255.255.255     udp spt:67 dpt:68
       3     1023 ACCEPT     udp  --  eth0   *       192.168.0.1          255.255.255.255     udp spt:67 dpt:68
       0        0 ACCEPT     udp  --  eth0   *       192.168.0.1          0.0.0.0/0           udp spt:67 dpt:68
       0        0 ACCEPT     udp  --  eth0   *       192.168.0.1          192.168.0.101       udp spt:67 dpt:68
       0        0 ssh_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
    1063    70674 ssh_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
       0        0 http_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 80,443
      95    11198 http_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
```

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 --udp -s 53 -p 1035 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): udp mode set, 28 headers + 0 data bytes

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@ironhide bensoer]#
```

Accounting Table After

```
[root@pidora bensoer]# iptables -L -v -n -x
Chain INPUT (policy DROP 1512 packets, 249980 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       6      252 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
       7      402 ACCEPT     udp  --  eth0   *       0.0.0.0/0            192.168.0.101       udp spt:53 dpts:1024:65535
       1       40 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            192.168.0.101       tcp spt:53 dpts:1024:65535
       0        0 ACCEPT     udp  --  eth0   *       0.0.0.0              255.255.255.255     udp spt:67 dpt:68
       3     1023 ACCEPT     udp  --  eth0   *       192.168.0.1          255.255.255.255     udp spt:67 dpt:68
       0        0 ACCEPT     udp  --  eth0   *       192.168.0.1          0.0.0.0/0           udp spt:67 dpt:68
       0        0 ACCEPT     udp  --  eth0   *       192.168.0.1          192.168.0.101       udp spt:67 dpt:68
       0        0 ssh_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spt:22
    1098    72566 ssh_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
       0        0 http_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport sports 80,443
      95    11198 http_input_traffic  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 80,443
```

DNS_T3

hping3

```
[root@pidora bensoer]# hping3 192.168.0.1 -p 53 -c 3
HPING 192.168.0.1 (eth0 192.168.0.1): NO FLAGS are set, 40 headers + 0 data byte
s
len=46 ip=192.168.0.1 ttl=64 id=9708 sport=53 flags=RA seq=0 win=0 rtt=6.9 ms
len=46 ip=192.168.0.1 ttl=64 id=9709 sport=53 flags=RA seq=1 win=0 rtt=5.9 ms
len=46 ip=192.168.0.1 ttl=64 id=9710 sport=53 flags=RA seq=2 win=0 rtt=4.8 ms

--- 192.168.0.1 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.8/5.8/6.9 ms
[root@pidora bensoer]#
```

DNS_T4

Although 3 packets were sent, only 1 was accepted

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -s 53 -p 1035 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.0.101 ttl=64 DF id=43380 sport=1035 flags=RA seq=0 win=0 rtt=0.9 ms

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 1 packets received, 67% packet loss
round-trip min/avg/max = 0.9/0.9/0.9 ms
[root@ironhide bensoer]#
```

SSH_T1A

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -S -s 22 -p 1035 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): S set, 40 headers + 0 data bytes

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@ironhide bensoer]#
```

SSH_T1B

Although 3 packets were sent only 1 was accepted, returning a reset request

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -SA -s 22 -p 1035 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): SA set, 40 headers + 0 data bytes
len=46 ip=192.168.0.101 ttl=64 DF id=43381 sport=1035 flags=R seq=0 win=0 rtt=0.7 ms

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 1 packets received, 67% packet loss
round-trip min/avg/max = 0.7/0.7/0.7 ms
[root@ironhide bensoer]#
```

SSH_T2

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -S -s 1035 -p 22 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.101 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=29200 rtt=0.9 ms
len=46 ip=192.168.0.101 ttl=64 DF id=0 sport=22 flags=SA seq=1 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.101 ttl=64 DF id=0 sport=22 flags=SA seq=2 win=29200 rtt=1.0 ms

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.0/1.0 ms
[root@ironhide bensoer]#
```

SSH_T3

The return messages are coming as RA because there is no SSH daemon running at the destination host

hping3

```
[root@pidora bensoer]# hping3 192.168.0.186 -S -s 1035 -p 22 -c 3
HPING 192.168.0.186 (eth0 192.168.0.186): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.186 ttl=64 DF id=1458 sport=22 flags=RA seq=0 win=0 rtt=6.7
ms
len=46 ip=192.168.0.186 ttl=64 DF id=1734 sport=22 flags=RA seq=1 win=0 rtt=6.0
ms
len=46 ip=192.168.0.186 ttl=64 DF id=2245 sport=22 flags=RA seq=2 win=0 rtt=5.4
ms

--- 192.168.0.186 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 5.4/6.0/6.7 ms
[root@pidora bensoer]#
```

SSH_T4

Note that the two accounting reads don't accuratly match in how much they have incremented. That is because for this experiement SSH was being used to connect to the device that this test was being executed on.

Accounting Table Before

```
Chain ssh_output_traffic (2 references)
    pkts      bytes target     prot opt in     out     source               destination
      11      440              tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1020:65535 dpt:22
      11      440 ACCEPT       tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1020:65535 dpt:22
    1300   303478              tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:22 dpts:1020:65535 flags:!0x17/0x02
    1300   303478 ACCEPT       tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:22 dpts:1020:65535 flags:!0x17/0x02
```

Accounting Table After

```
Chain ssh_output_traffic (2 references)
    pkts      bytes target     prot opt in     out     source               destination
      11      440              tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1020:65535 dpt:22
      11      440 ACCEPT       tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1020:65535 dpt:22
    1444   344606              tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:22 dpts:1020:65535 flags:!0x17/0x02
    1444   344606 ACCEPT       tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:22 dpts:1020:65535 flags:!0x17/0x02
```

HTTP_T3

Although 3 packets were sent. Only one was received

hping3

```
[root@ironhide bensoer]# hping3  192.168.0.101 -S -s 80 -p 80 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): S set, 40 headers + 0 data bytes

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@ironhide bensoer]#
```

HTTP_T4

Although 3 packets were sent. Only one was received

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -S -s 443 -p 443 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): S set, 40 headers + 0 data bytes

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@ironhide bensoer]#
```

HTTP_T5

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -S -s 1035 -p 80 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.101 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=29200 rtt=1.0 ms
len=46 ip=192.168.0.101 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=29200 rtt=1.1 ms
len=46 ip=192.168.0.101 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=29200 rtt=1.0 ms

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.0/1.0/1.1 ms
[root@ironhide bensoer]#
```

HTTP_T6

hping3

```
[root@ironhide bensoer]# hping3 192.168.0.101 -S -s 1035 -p 443 -c 3
HPING 192.168.0.101 (enp4s0f2 192.168.0.101): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.101 ttl=64 DF id=43391 sport=443 flags=RA seq=0 win=0 rtt=1.0 ms
len=46 ip=192.168.0.101 ttl=64 DF id=43392 sport=443 flags=RA seq=1 win=0 rtt=1.1 ms
len=46 ip=192.168.0.101 ttl=64 DF id=43393 sport=443 flags=RA seq=2 win=0 rtt=0.9 ms

--- 192.168.0.101 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.0/1.1 ms
[root@ironhide bensoer]#
```

HTTP_T7

hping3

```
[root@pidora bensoer]# hping3 google.com -S -s 1035 -p 80 -c 3
HPING google.com (eth0 216.58.216.174): S set, 40 headers + 0 data bytes
len=46 ip=216.58.216.174 ttl=58 id=22556 sport=80 flags=SA seq=0 win=42900 rtt=1
6.1 ms
len=46 ip=216.58.216.174 ttl=58 id=34058 sport=80 flags=SA seq=1 win=42900 rtt=2
5.4 ms
len=46 ip=216.58.216.174 ttl=58 id=39055 sport=80 flags=SA seq=2 win=42900 rtt=1
5.0 ms

--- google.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 15.0/18.8/25.4 ms
[root@pidora bensoer]#
```

HTTP_T8

hping3

```
[root@pidora bensoer]# hping3 google.com -S -s 1035 -p 443 -c 3
HPING google.com (eth0 216.58.216.174): S set, 40 headers + 0 data bytes
len=46 ip=216.58.216.174 ttl=58 id=3408 sport=443 flags=SA seq=0 win=42900 rtt=1
6.9 ms
len=46 ip=216.58.216.174 ttl=57 id=1126 sport=443 flags=SA seq=1 win=42900 rtt=1
6.4 ms
len=46 ip=216.58.216.174 ttl=57 id=62426 sport=443 flags=SA seq=2 win=42900 rtt=
14.8 ms

--- google.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 14.8/15.7/16.9 ms
[root@pidora bensoer]#
```

HTTP_T9

Accounting Table Before

```
Chain http_output_traffic (2 references)
    pkts      bytes target     prot opt in     out     source               destination
      24      960            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
      24      960 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
       7      280            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
       7      280 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
      12     5513            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
      12     5513 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
       3      120            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
       3      120 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
```

hping3

```
[root@pidora bensoer]# hping3 192.168.0.186 -SA -s 80 -p 1035 -c 3
HPING 192.168.0.186 (eth0 192.168.0.186): SA set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
[root@pidora bensoer]#
```

Accounting Table After

```
Chain http_output_traffic (2 references)
    pkts      bytes target     prot opt in     out     source               destination
      24      960            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
      24      960 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
       7      280            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
       7      280 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
      13     5553            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
      13     5553 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
       3      120            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
       3      120 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
```

HTTP_T10

Accounting Table Before

```
Chain http_output_traffic (2 references)
    pkts      bytes target     prot opt in     out     source               destination
      24      960            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
      24      960 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
       7      280            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
       7      280 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
      13     5553            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
      13     5553 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
       3      120            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
       3      120 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
```

hping3

```
[root@pidora bensoer]# hping3 192.168.0.186 -SA -s 443 -p 1035 -c 3
HPING 192.168.0.186 (eth0 192.168.0.186): SA set, 40 headers + 0 data bytes
[send_ip] sendto: Operation not permitted
[root@pidora bensoer]#
```

Accounting Table After

```
Chain http_output_traffic (2 references)
    pkts      bytes target     prot opt in     out     source               destination
      24      960            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
      24      960 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:80
       7      280            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
       7      280 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spts:1024:65535 dpt:443
      13     5553            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
      13     5553 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:80 dpts:1024:65535 flags:!0x17/0x02
       4      160            tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
       4      160 ACCEPT     tcp  --  *      eth0    192.168.0.101        0.0.0.0/0           tcp spt:443 dpts:1024:65535 flags:!0x17/0x02
```

DHCP_T1

This test shows the firewall is allowing the correct data through as DHCP is able to renew the ip address on the firewall device. You can view details in the release.txt and renew.txt files.

Release.txt – Releasing of IP through the firewall

Internet Systems Consortium DHCP Client 4.2.6
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/b8:27:eb:75:d6:99
Sending on LPF/eth0/b8:27:eb:75:d6:99
Sending on Socket/fallback
DHCPRELEASE on eth0 to 192.168.0.1 port 67 (xid=0x357d175c)

Renewal.txt – Renewal of IP through the firewall

Internet Systems Consortium DHCP Client 4.2.6
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/b8:27:eb:75:d6:99
Sending on LPF/eth0/b8:27:eb:75:d6:99
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 8 (xid=0x1848e1ee)
DHCPREQUEST on eth0 to 255.255.255.255 port 67 (xid=0x1848e1ee)
DHCPOFFER from 192.168.0.1
DHCPACK from 192.168.0.1 (xid=0x1848e1ee)
bound to 192.168.0.101 -- renewal in 42606 seconds.