Subject: APF on hardware node
Posted by ugob on Thu, 19 Jul 2007 20:52:10 GMT
View Forum Message <> Reply to Message

Hi,

I'm running APF (iptables frond-end) on all my VE's and some HN. One question... how do I manage connections from a VE to the HN?

I've tried simply add a rule so that it results in

```
0     0 ACCEPT     tcp  --  any    any     70.70.70.70  anywhere            tcp dpt:ssh
```

(IP address of the VE is 70.70.70.70. It doesn't work because it looks like the packets are not coming from 70.70.70.70 since it goes through the venet0 interface. Is there a way to manage this? The only I found for now is to add 'venet0' to the list of trusted interfaces in apf.conf, but this allow all traffic from the VEs, which is not perfect.

Thanks,
Ugo

Subject: Re: APF on hardware node
Posted by Vasily Tarasov on Fri, 20 Jul 2007 10:57:59 GMT
View Forum Message <> Reply to Message

What table have you added this rule in? It should be in FORWARD table, I guess...

Thank you,
Vasily

Subject: Re: APF on hardware node
Posted by ugob on Fri, 20 Jul 2007 11:10:52 GMT
View Forum Message <> Reply to Message

From what I can understand, APF doesn't manage the FORWARD table, so it was in the input table.

Subject: Re: APF on hardware node
Posted by Vasily Tarasov on Fri, 20 Jul 2007 11:25:56 GMT
View Forum Message <> Reply to Message

I can assume that APF can prohibit all FORWARD trafic by default.
Can you post here the output of the following command on HN:

iptables -L -nv

Thank you,
Vasily

Subject: Re: APF on hardware node
Posted by ugob on Fri, 20 Jul 2007 14:18:12 GMT
View Forum Message <> Reply to Message

These rules are working (I added venet0 to trusted interface)

```
Chain INPUT (policy ACCEPT 1 packets, 78 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
    0     0 ACCEPT     all  --  venet0 *       0.0.0.0/0           0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       69.63.144.19        0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       69.63.144.15        0.0.0.0/0           tcp dpt:22
  181 13802 ACCEPT     tcp  --  *      *       71.252.120.209      0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       74.59.221.180       0.0.0.0/0           tcp dpt:22
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpts:135:139
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpts:135:139
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:111
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:111
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:513
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:513
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:520
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:520
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:445
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:445
    2    96 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:1433
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:1433
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:1434
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:1434
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:1234
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:1234
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:1524
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:1524
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:3127
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:3127
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:0x03/0x03
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:0x06/0x06
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:0x05/0x05
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:0x11/0x01
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:0x30/0x20
```

```
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x18/0x08
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x29
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x37
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x3F
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x01
    0     0 FUDP       udp  -f  eth0   *      0.0.0.0/0           0.0.0.0/0
    0     0 PZ         udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:0
    0     0 PZ         tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:0
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:7778 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:7778 reject-with
icmp-port-unreachable
```

```
    0     0 TELNET_LOG  tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:23 state NEW
    0     0 SSH_LOG     tcp  --  *      *       0.0.0.0/0           0.0.0.0/0           tcp dpt:22 state NEW
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp dpt:5666
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 3 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 5 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 11 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 0 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 30 limit: avg
30/sec burst 5
   20  1220 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 8 limit: avg
30/sec burst 5
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:!0x16/0x02 state
NEW
   37  2404 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           state
RELATED,ESTABLISHED
   70  5531 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           state
RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       69.63.129.15        0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     tcp  --  eth0   *       69.63.129.15        0.0.0.0/0           tcp spt:53
dpts:1023:65535
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spt:53 dpts:1023:65535

    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     udp  --  eth0   *       69.63.129.16        0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     tcp  --  eth0   *       69.63.129.16        0.0.0.0/0           tcp spt:53
dpts:1023:65535
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spt:53 dpts:1023:65535

    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spts:1023:65535
dpt:21 state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spt:22 dpts:513:65535
state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spts:1024:65535
dpt:22 flags:0x16/0x02 state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:22 state
```

```
ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           state NEW udp
dpts:33434:33534
   27  1288 LOG        tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** IN_TCP DROP ** '
    0     0 LOG        udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** IN_UDP DROP ** '
   27  1288 DROP       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT 11446 packets, 6864K bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 62 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
    0     0 ACCEPT     all  --  *      venet0  0.0.0.0/0           0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           69.63.144.15        tcp dpt:22
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:135:139
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:135:139
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:111
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:111
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:513
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:513
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:520
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:520
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:445
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:445
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1433
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1433
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1434
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1434
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1234
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1234
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1524
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1524
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:3127
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:3127
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x03/0x03
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x06/0x06
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x05/0x05
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x11/0x01
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x18/0x08
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x30/0x20
    0     0 FUDP       udp  -f  *      eth0    0.0.0.0/0           0.0.0.0/0
    0     0 PZ         udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:0
```

```
    0     0 PZ         tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:0
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:7778 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:7778 reject-with
icmp-port-unreachable
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:21
   24  7117 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:25
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:43
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:20
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:21
```

```
    6   528 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:53
   64  4864 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:123
   20  1220 ACCEPT     icmp --  *      eth0    0.0.0.0/0           0.0.0.0/0           limit: avg 30/sec burst
5
  113 38219 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:1024:65535
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:1024:65535
state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp spt:21
dpts:1023:65535 state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           state NEW udp
dpts:33434:33534
    0     0 LOG        tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** OUT_TCP DROP ** '
    0     0 LOG        udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** OUT_UDP DROP ** '
    0     0 DROP       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain FUDP (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5 LOG
flags 0 level 2 prefix `** UDP Frag ** '
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain GTA (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain GTD (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain IN_SANITY (11 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** SANITY ** '
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0

Chain LA (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0           LOG flags 0 level 2
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0           0.0.0.0/0
```

```
Chain LD (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 2
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain LMAC (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 30/min burst 5 LOG
flags 0 level 2 prefix ` ** DROP FORIGN MAC ** '
    0     0 REJECT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           reject-with
icmp-net-prohibited

Chain OUT_SANITY (7 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** SANITY ** '
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0

Chain PROHIBIT (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with
icmp-host-prohibited

Chain PZ (4 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 30/min burst 5 LOG
flags 0 level 2 prefix `** Port Zero ** '
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain RESET (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with tcp-reset

Chain SSH_LOG (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 2 prefix `**
SSH ** '

Chain TA (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain TD (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain TELNET_LOG (1 references)
```

```
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 2 prefix `** TELNET ** '
```

Subject: Re: APF on hardware node
Posted by ugob on Fri, 20 Jul 2007 14:19:57 GMT
View Forum Message <> Reply to Message

These rules are not working (IFACE_TRUSTED="")

```
Chain INPUT (policy ACCEPT 1 packets, 78 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
    6   528 ACCEPT     tcp  --  *      *       69.63.144.19         0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       69.63.144.15         0.0.0.0/0           tcp dpt:22
    3   216 ACCEPT     tcp  --  *      *       71.252.120.209       0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       74.59.221.180        0.0.0.0/0           tcp dpt:22
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpts:135:139
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpts:135:139
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:111
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:111
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:513
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:513
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:520
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:520
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:445
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:445
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:1433
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1433
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:1434
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1434
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:1234
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1234
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:1524
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:1524
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp dpt:3127
    0     0 DROP       udp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           udp dpt:3127
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x03/0x03
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x06/0x06
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x05/0x05
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x11/0x01
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x30/0x20
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x18/0x08
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x29
    0     0 IN_SANITY  tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x3F/0x37
```

```
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x3F
    0     0 IN_SANITY  tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x01
    0     0 FUDP       udp  -f  eth0   *      0.0.0.0/0           0.0.0.0/0
    0     0 PZ         udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:0
    0     0 PZ         tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:0
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:7778 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           udp dpt:7778 reject-with
icmp-port-unreachable
    0     0 TELNET_LOG  tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp dpt:23 state NEW
    0     0 SSH_LOG    tcp  --  *      *      0.0.0.0/0           0.0.0.0/0           tcp dpt:22 state NEW
    0     0 ACCEPT     tcp  --  eth0   *      0.0.0.0/0           0.0.0.0/0           tcp dpt:5666
```

```
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 3 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 5 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 11 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 0 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 30 limit: avg
30/sec burst 5
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0           0.0.0.0/0           icmp type 8 limit: avg
30/sec burst 5
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp flags:!0x16/0x02 state
NEW
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           state
RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           state
RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       69.63.129.15        0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     tcp  --  eth0   *       69.63.129.15        0.0.0.0/0           tcp spt:53
dpts:1023:65535
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spt:53 dpts:1023:65535

    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     udp  --  eth0   *       69.63.129.16        0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     tcp  --  eth0   *       69.63.129.16        0.0.0.0/0           tcp spt:53
dpts:1023:65535
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spt:53 dpts:1023:65535

    0     0 DROP       udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp spt:53
dpts:1023:65535
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spts:1023:65535
dpt:21 state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spt:22 dpts:513:65535
state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           tcp spts:1024:65535
dpt:22 flags:0x16/0x02 state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           udp dpt:22 state
ESTABLISHED
    0     0 ACCEPT     udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           state NEW udp
dpts:33434:33534
```

```
    0     0 LOG        tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** IN_TCP DROP ** '
    0     0 LOG        udp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** IN_UDP DROP ** '
    0     0 DROP       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain FORWARD (policy ACCEPT 2 packets, 132 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 62 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
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0           69.63.144.15        tcp dpt:22
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:135:139
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:135:139
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:111
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:111
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:513
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:513
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:520
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:520
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:445
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:445
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1433
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1433
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1434
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1434
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1234
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1234
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1524
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1524
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:3127
    0     0 DROP       udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:3127
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x3F/0x00
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x03/0x03
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x06/0x06
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x05/0x05
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x11/0x01
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x18/0x08
    0     0 OUT_SANITY  tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp flags:0x30/0x20
    0     0 FUDP       udp  -f  *      eth0    0.0.0.0/0           0.0.0.0/0
    0     0 PZ         udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:0
    0     0 PZ         tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:0
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:1214 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:1214 reject-with
```

```
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:2323 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:4660:4678
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6257 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6699 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6347 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:6881:6889
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:6346 reject-with
icmp-port-unreachable
    0     0 REJECT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:7778 reject-with
icmp-port-unreachable
    0     0 REJECT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:7778 reject-with
icmp-port-unreachable
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:21
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:25
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:443
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpt:43
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:20
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:21
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:53
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpt:123
    0     0 ACCEPT     icmp --  *      eth0    0.0.0.0/0           0.0.0.0/0           limit: avg 30/sec burst 5
    2   208 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp dpts:1024:65535
```

```
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           udp dpts:1024:65535
state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           tcp spt:21
dpts:1023:65535 state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           multiport dports 21,20
state RELATED,ESTABLISHED
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           state NEW udp
dpts:33434:33534
    0     0 LOG        tcp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** OUT_TCP DROP ** '
    0     0 LOG        udp  --  *      eth0    0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** OUT_UDP DROP ** '
   25  6824 DROP       tcp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       udp  --  *      *       0.0.0.0/0           0.0.0.0/0
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain FUDP (2 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5 LOG
flags 0 level 2 prefix `** UDP Frag ** '
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain GTA (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain GTD (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain IN_SANITY (11 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** SANITY ** '
    0     0 DROP       tcp  --  eth0   *       0.0.0.0/0           0.0.0.0/0

Chain LA (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0           LOG flags 0 level 2
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain LD (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0           0.0.0.0/0           LOG flags 0 level 2
    0     0 DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0
```

```
Chain LMAC (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 30/min burst 5 LOG
flags 0 level 2 prefix ` ** DROP FORIGN MAC ** '
    0     0 REJECT     all  --  eth0   *       0.0.0.0/0            0.0.0.0/0           reject-with
icmp-net-prohibited

Chain OUT_SANITY (7 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0           limit: avg 30/min burst 5
LOG flags 0 level 2 prefix `** SANITY ** '
    0     0 DROP       tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0

Chain PROHIBIT (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with
icmp-host-prohibited

Chain PZ (4 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           limit: avg 30/min burst 5 LOG
flags 0 level 2 prefix `** Port Zero ** '
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain RESET (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with tcp-reset

Chain SSH_LOG (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 2 prefix `**
SSH ** '

Chain TA (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain TD (0 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain TELNET_LOG (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 2 prefix `**
TELNET ** '
```