
Subject: *RESOLVED* APF firewall problem!
Posted by [omega36](#) on Wed, 06 Jun 2007 15:12:43 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hello.

I am running two VPS's. They are both from the same VPS provider.
They are both the same OS with the same kernel.

I have rebuilt both from scratch and then run yum update on both.
I installed apf firewall on VPS A and VPS B after modifying
conf.apf with the following changes on both VPS's:

changed interfaces to 'venet0', opened necessary ingress ports
(outgoing filtering is set to 0), and then set monokern to 1

When I run apf on VPS A, it starts fine with no errors, when I
run the same on VPS B, it starts, but I get a bunch of errors.
Here is the total output of the startup sequence on the VPS
with errors:

```
[root@vpsB ~]# apf -s
apf(29931): {glob} activating firewall
apf(29988): {glob} determined (IFACE_IN) venet0 has address 127.0.0.1
apf(29988): {glob} determined (IFACE_OUT) venet0 has address 127.0.0.1
apf(29988): {glob} loading preroute.rules
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
apf(29988): {resnet} downloading http://r-fx.ca/downloads/reserved.networks
apf(29988): {resnet} parsing reserved.networks into /etc/apf/internals/reserved.networks
apf(29988): {glob} loading reserved.networks
apf(29988): {glob} loading bt.rules
apf(29988): {dshield} downloading http://feeds.dshield.org/top10-2.txt
apf(29988): {dshield} parsing top10-2.txt into /etc/apf/ds_hosts.rules
apf(29988): {dshield} loading ds_hosts.rules
apf(29988): {sdrop} downloading http://www.spamhaus.org/drop/drop.lasso
apf(29988): {sdrop} parsing drop.lasso into /etc/apf/sdrop_hosts.rules
apf(29988): {sdrop} loading sdrop_hosts.rules
apf(29988): {glob} loading common drop ports
apf(29988): {blk_ports} deny all to/from tcp port 135:139
```

```
apf(29988): {blk_ports} deny all to/from udp port 135:139
apf(29988): {blk_ports} deny all to/from tcp port 111
apf(29988): {blk_ports} deny all to/from udp port 111
apf(29988): {blk_ports} deny all to/from tcp port 513
apf(29988): {blk_ports} deny all to/from udp port 513
apf(29988): {blk_ports} deny all to/from tcp port 520
apf(29988): {blk_ports} deny all to/from udp port 520
apf(29988): {blk_ports} deny all to/from tcp port 445
apf(29988): {blk_ports} deny all to/from udp port 445
apf(29988): {blk_ports} deny all to/from tcp port 1433
apf(29988): {blk_ports} deny all to/from udp port 1433
apf(29988): {blk_ports} deny all to/from tcp port 1434
apf(29988): {blk_ports} deny all to/from udp port 1434
apf(29988): {blk_ports} deny all to/from tcp port 1234
apf(29988): {blk_ports} deny all to/from udp port 1234
apf(29988): {blk_ports} deny all to/from tcp port 1524
apf(29988): {blk_ports} deny all to/from udp port 1524
apf(29988): {blk_ports} deny all to/from tcp port 3127
apf(29988): {blk_ports} deny all to/from udp port 3127
apf(29988): {pkt_sanitiy} set active PKT_SANITY
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ALL NONE
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs SYN,FIN SYN,FIN
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs SYN,RST SYN,RST
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs FIN,RST FIN,RST
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ACK,FIN FIN
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ACK,URG URG
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ACK,PSH PSH
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ALL FIN,URG,PSH
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ALL SYN,RST,ACK,FIN,URG
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ALL ALL
apf(29988): {pkt_sanitiy} deny inbound tcp-flag pairs ALL FIN
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs ALL NONE
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs SYN,FIN SYN,FIN
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs SYN,RST SYN,RST
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs FIN,RST FIN,RST
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs ACK,FIN FIN
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs ACK,PSH PSH
apf(29988): {pkt_sanitiy} deny outbound tcp-flag pairs ACK,URG URG
apf(29988): {pkt_sanitiy} deny all to/from 255.255.255.255
apf(29988): {pkt_sanitiy} deny all to/from 0.0.0.255/0.0.0.255
apf(29988): {pkt_sanitiy} deny all fragmented udp
apf(29988): {pkt_sanitiy} deny inbound tcp port 0
apf(29988): {pkt_sanitiy} deny outbound tcp port 0
apf(29988): {blk_p2p} set active BLK_P2P
apf(29988): {blk_p2p} deny all to/from tcp port 1214
apf(29988): {blk_p2p} deny all to/from udp port 1214
apf(29988): {blk_p2p} deny all to/from tcp port 2323
apf(29988): {blk_p2p} deny all to/from udp port 2323
```

```
apf(29988): {blk_p2p} deny all to/from tcp port 4660:4678
apf(29988): {blk_p2p} deny all to/from udp port 4660:4678
apf(29988): {blk_p2p} deny all to/from tcp port 6257
apf(29988): {blk_p2p} deny all to/from udp port 6257
apf(29988): {blk_p2p} deny all to/from tcp port 6699
apf(29988): {blk_p2p} deny all to/from udp port 6699
apf(29988): {blk_p2p} deny all to/from tcp port 6346
apf(29988): {blk_p2p} deny all to/from udp port 6346
apf(29988): {blk_p2p} deny all to/from tcp port 6347
apf(29988): {blk_p2p} deny all to/from udp port 6347
apf(29988): {blk_p2p} deny all to/from tcp port 6881:6889
apf(29988): {blk_p2p} deny all to/from udp port 6881:6889
apf(29988): {blk_p2p} deny all to/from tcp port 6346
apf(29988): {blk_p2p} deny all to/from udp port 6346
apf(29988): {glob} loading log.rules
apf(29988): {glob} virtual network enabled, loading vnet rules.
apf(29988): {glob} loading 206.71.150.203.rules
apf(29988): {glob} opening inbound tcp port 20 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 21 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 22 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 25 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 80 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 110 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 143 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 443 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 3306 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 7776 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 7777 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 7778 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 7779 on 206.71.150.203
apf(29988): {glob} opening inbound tcp port 8089 on 206.71.150.203
apf(29988): {glob} opening inbound udp port 20 on 206.71.150.203
apf(29988): {glob} opening inbound udp port 21 on 206.71.150.203
apf(29988): {glob} opening inbound udp port 53 on 206.71.150.203
apf(29988): {glob} opening inbound icmp type 3 on 206.71.150.203
apf(29988): {glob} opening inbound icmp type 5 on 206.71.150.203
apf(29988): {glob} opening inbound icmp type 11 on 206.71.150.203
apf(29988): {glob} opening inbound icmp type 0 on 206.71.150.203
apf(29988): {glob} opening inbound icmp type 30 on 206.71.150.203
apf(29988): {glob} opening inbound icmp type 8 on 206.71.150.203
apf(29988): {glob} loading main.rules
apf(29988): {glob} opening inbound tcp port 20 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 21 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 22 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 25 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 80 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 110 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 143 on 127.0.0.1
```

```
apf(29988): {glob} opening inbound tcp port 443 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 3306 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 7776 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 7777 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 7778 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 7779 on 127.0.0.1
apf(29988): {glob} opening inbound tcp port 8089 on 127.0.0.1
apf(29988): {glob} opening inbound udp port 20 on 127.0.0.1
apf(29988): {glob} opening inbound udp port 21 on 127.0.0.1
apf(29988): {glob} opening inbound udp port 53 on 127.0.0.1
apf(29988): {glob} opening inbound icmp type 3 on 127.0.0.1
apf(29988): {glob} opening inbound icmp type 5 on 127.0.0.1
apf(29988): {glob} opening inbound icmp type 11 on 127.0.0.1
apf(29988): {glob} opening inbound icmp type 0 on 127.0.0.1
apf(29988): {glob} opening inbound icmp type 30 on 127.0.0.1
apf(29988): {glob} opening inbound icmp type 8 on 127.0.0.1
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
apf(29988): {glob} resolv dns discovery for 206.71.148.231
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
apf(29988): {glob} loading postroute.rules
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
iptables: No chain/target/match by that name
apf(29988): {glob} default (egress) output accept
apf(29988): {glob} default (ingress) input drop
apf(29931): {glob} firewall initialized
apf(29931): {glob} fast load snapshot saved
```

It seems to run okay, but I am unable to use wget or yum and FTP does not work correctly on VPS B. On VPS A, everything works fine.

I have searched endlessly and I have found no fix for this yet, I have also tried adding

```
IPTABLES_MODULES="ipt_REJECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport
iptables_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state iptable_nat
```

ip_nat_ftp"

to /etc/sysconfig/iptables-config but to no avail.

Could somebody help me please
