Subject: Recommended iptables / ip6tables configuration?
Posted by HHawk on Thu, 15 Aug 2019 09:29:29 GMT
View Forum Message <> Reply to Message

Hi all,

With OpenVZ 7 we are redoing also our iptables / ip6tables configurations (on the hardware node).
However I am experiencing some issues with it.

So first off; does anyone have or can share good iptables / ip6tables configurations?

I have the following two configurations, however these give out errors.

Configuration iptables:

```
# DEFAULT IPTABLES (IPv4) CONFIGURATION [08.2019]
*filter
:INPUT ACCEPT [906:8314795]
:FORWARD ACCEPT [11341:732007]
:OUTPUT ACCEPT [939:67434]
-A INPUT -p tcp -m tcp --dport 1622 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 1621 -j ACCEPT
-A INPUT -s 95.170.131.46/32 -j ACCEPT
-A INPUT -s 81.184.0.141/32 -j ACCEPT
-A INPUT -s 80.237.178.180/32 -j ACCEPT
-A INPUT -s 91.204.24.0/22 -j ACCEPT
-A INPUT -s 91.204.24.0/22 -j ACCEPT
-A INPUT -s 195.214.233.0/24 -j ACCEPT
-A INPUT -i virbr0 -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -i virbr0 -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -i virbr0 -p udp -m udp --dport 67 -j ACCEPT
-A INPUT -i virbr0 -p tcp -m tcp --dport 67 -j ACCEPT
-A FORWARD -i virbr0 -o virbr0 -j ACCEPT
-A FORWARD -o virbr0 -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -i virbr0 -j REJECT --reject-with icmp-port-unreachable
-A OUTPUT -p tcp -m tcp --dport 1622 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 1621 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 21 -j ACCEPT
-A OUTPUT -o virbr0 -p udp -m udp --dport 68 -j ACCEPT
COMMIT
*raw
:PREROUTING ACCEPT [12250:9046982]
:OUTPUT ACCEPT [939:67434]
:OUTPUT_direct - [0:0]
:PREROUTING_ZONES - [0:0]
:PREROUTING_ZONES_SOURCE - [0:0]
:PREROUTING_direct - [0:0]
```

```
:PRE_public - [0:0]
:PRE_public_allow - [0:0]
:PRE_public_deny - [0:0]
:PRE_public_log - [0:0]
-A PREROUTING -j PREROUTING_direct
-A PREROUTING -j PREROUTING_ZONES_SOURCE
-A PREROUTING -j PREROUTING_ZONES
-A OUTPUT -j OUTPUT_direct
-A PREROUTING_ZONES -i venet0 -g PRE_public
-A PREROUTING_ZONES -i eth0 -g PRE_public
-A PREROUTING_ZONES -g PRE_public
-A PRE_public -j PRE_public_log
-A PRE_public -j PRE_public_deny
-A PRE_public -j PRE_public_allow
COMMIT
*security
:INPUT ACCEPT [909:8314975]
:FORWARD ACCEPT [11341:732007]
:OUTPUT ACCEPT [939:67434]
:FORWARD_direct - [0:0]
:INPUT_direct - [0:0]
:OUTPUT_direct - [0:0]
-A INPUT -j INPUT_direct
-A FORWARD -j FORWARD_direct
-A OUTPUT -j OUTPUT_direct
COMMIT
*security
:INPUT ACCEPT [909:8314975]
:FORWARD ACCEPT [11341:732007]
:OUTPUT ACCEPT [939:67434]
:FORWARD_direct - [0:0]
:INPUT_direct - [0:0]
:OUTPUT_direct - [0:0]
-A INPUT -j INPUT_direct
-A FORWARD -j FORWARD_direct
-A OUTPUT -j OUTPUT_direct
COMMIT
*mangle
:PREROUTING ACCEPT [12250:9046982]
:INPUT ACCEPT [909:8314975]
:FORWARD ACCEPT [11341:732007]
:OUTPUT ACCEPT [939:67434]
:POSTROUTING ACCEPT [12280:799441]
:FORWARD_direct - [0:0]
:INPUT_direct - [0:0]
:OUTPUT_direct - [0:0]
:POSTROUTING_direct - [0:0]
:PREROUTING_ZONES - [0:0]
```

```
:PREROUTING_ZONES_SOURCE - [0:0]
:PREROUTING_direct - [0:0]
:PRE_public - [0:0]
:PRE_public_allow - [0:0]
:PRE_public_deny - [0:0]
:PRE_public_log - [0:0]
-A PREROUTING -j PREROUTING_direct
-A PREROUTING -j PREROUTING_ZONES_SOURCE
-A PREROUTING -j PREROUTING_ZONES
-A INPUT -j INPUT_direct
-A FORWARD -j FORWARD_direct
-A OUTPUT -j OUTPUT_direct
-A POSTROUTING -o virbr0 -p udp -m udp --dport 68 -j CHECKSUM --checksum-fill
-A POSTROUTING -o virbr0 -p udp -m udp --dport 68 -j CHECKSUM --checksum-fill
-A POSTROUTING -j POSTROUTING_direct
-A PREROUTING_ZONES -i venet0 -g PRE_public
-A PREROUTING_ZONES -i eth0 -g PRE_public
-A PREROUTING_ZONES -g PRE_public
-A PRE_public -j PRE_public_log
-A PRE_public -j PRE_public_deny
-A PRE_public -j PRE_public_allow
COMMIT
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT_direct - [0:0]
:POSTROUTING_ZONES - [0:0]
:POSTROUTING_ZONES_SOURCE - [0:0]
:POSTROUTING_direct - [0:0]
:POST_public - [0:0]
:POST_public_allow - [0:0]
:POST_public_deny - [0:0]
:POST_public_log - [0:0]
:PREROUTING_ZONES - [0:0]
:PREROUTING_ZONES_SOURCE - [0:0]
:PREROUTING_direct - [0:0]
:PRE_public - [0:0]
:PRE_public_allow - [0:0]
:PRE_public_deny - [0:0]
:PRE_public_log - [0:0]
-A PREROUTING -j PREROUTING_direct
-A PREROUTING -j PREROUTING_ZONES_SOURCE
-A PREROUTING -j PREROUTING_ZONES
-A OUTPUT -j OUTPUT_direct
-A POSTROUTING -j POSTROUTING_direct
-A POSTROUTING -j POSTROUTING_ZONES_SOURCE
```

```
-A POSTROUTING -j POSTROUTING_ZONES
-A POSTROUTING_ZONES -o venet0 -g POST_public
-A POSTROUTING_ZONES -o eth0 -g POST_public
-A POSTROUTING_ZONES -g POST_public
-A POST_public -j POST_public_log
-A POST_public -j POST_public_deny
-A POST_public -j POST_public_allow
-A PREROUTING_ZONES -i venet0 -g PRE_public
-A PREROUTING_ZONES -i eth0 -g PRE_public
-A PREROUTING_ZONES -g PRE_public
-A PRE_public -j PRE_public_log
-A PRE_public -j PRE_public_deny
-A PRE_public -j PRE_public_allow
COMMIT
```

Configuration ip6tables:

```
# DEFAULT IP6TABLES (IPv6) CONFIGURATION [08.2019]
*filter
:INPUT ACCEPT [5130:369136]
:FORWARD ACCEPT [16926:9952446]
:OUTPUT ACCEPT [282:18936]
-A INPUT -s 2a00:1730:fff9::/48 -j ACCEPT
-A INPUT -i virbr0 -p udp -m udp --dport 547 -j ACCEPT
-A INPUT -i virbr0 -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -i virbr0 -p tcp -m tcp --dport 53 -j ACCEPT
-A FORWARD -i virbr0 -o virbr0 -j ACCEPT
-A FORWARD -o virbr0 -j REJECT --reject-with icmp6-port-unreachable
-A FORWARD -i virbr0 -j REJECT --reject-with icmp6-port-unreachable
COMMIT
*mangle
:PREROUTING ACCEPT [22875:10436248]
:INPUT ACCEPT [5490:395224]
:FORWARD ACCEPT [17384:10040952]
:OUTPUT ACCEPT [362:26100]
:POSTROUTING ACCEPT [17756:10068092]
COMMIT
```

Both give errors when I restore them. No clue though what is wrong, as there is no detailed feedback about the error in any of the logs unfortunately.

Also I have a few questions. Maybe someone can answer that as well, so I am able to understand it better.

We still use containers on our new hardware nodes with OpenVZ 7. Containers use venet0 and our hardware nodes are always setup with eth0 (or ethX in general).

I don't see either back in the config? Is this normal? Or am I doing everything completely wrong.

The weird thing is, is that I noticed issues recently with a kickstarted hardware node with OpenVZ 7. When we created a container on that hardware node, it was not able to ping outside (for example Google). It started working *after* I ran iptables -F and ip6tables -F.

The only kickstart configuration's I apply to iptables/ip6tables are the following:

```
#PLESK SUPPORT IPS
iptables -I INPUT -s
195.214.233.0/24,91.204.24.0/22,91.204.25.0/22,80.237.178.180,81.184.0.141,95.170.131.46 -j
ACCEPT
ip6tables -I INPUT -s 2A00:1730:FFF9::/48 -j ACCEPT

#ENABLING PORTS
iptables -I INPUT -p tcp --dport 64000 -j ACCEPT
iptables -I INPUT -p tcp --dport 50398 -j ACCEPT
iptables -I INPUT -p tcp --dport 1621 -j ACCEPT
iptables -I INPUT -p tcp --dport 1622 -j ACCEPT
iptables -I INPUT -p tcp --dport 5666 -j ACCEPT
iptables-save > /etc/sysconfig/iptables
service iptables save

ip6tables -I INPUT -p tcp --dport 64000 -j ACCEPT
ip6tables -I INPUT -p tcp --dport 50398 -j ACCEPT
ip6tables -I INPUT -p tcp --dport 1621 -j ACCEPT
ip6tables -I INPUT -p tcp --dport 1622 -j ACCEPT
ip6tables -I INPUT -p tcp --dport 5666 -j ACCEPT
ip6tables-save > /etc/sysconfig/ip6tables
service ip6tables save

sed -i'' -e 's/IPTABLES_SAVE_ON_STOP="no"/IPTABLES_SAVE_ON_STOP="yes"/'
/etc/sysconfig/iptables-config
sed -i'' -e 's/IPTABLES_SAVE_ON_RESTART="no"/IPTABLES_SAVE_ON_RESTART="yes"/'
/etc/sysconfig/iptables-config
sed -i'' -e 's/IP6TABLES_SAVE_ON_STOP="no"/IP6TABLES_SAVE_ON_STOP="yes"/'
/etc/sysconfig/ip6tables-config
sed -i'' -e 's/IP6TABLES_SAVE_ON_RESTART="no"/IP6TABLES_SAVE_ON_RESTART="yes"/'
/etc/sysconfig/ip6tables-config

systemctl restart iptables
systemctl restart ip6tables
```

So I am hoping someone (experienced) can share some light on the above. And maybe have good configurations for iptables/ip6tables I can use?

Thanks in advance.

Regards