
Subject: configure iptables on VZ7 host
Posted by [mangust](#) on Sun, 03 Sep 2017 10:04:47 GMT
[View Forum Message](#) <> [Reply to Message](#)

Hi,

I have some interfaces on external network with other machines plugged in there. I want to give some containers public IPs

Interfaces got automatic local IPv6 and able to communicate with any neighbours and maybe beyond.

```
17: bond0.798@bond0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
master vzbr798 state UP qlen 1000
    link/ether b8:ca:3a:6a:0f:d4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::baca:3aff:fe6a:fd4/64 scope link
        valid_lft forever preferred_lft forever
18: vzbr798: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
qlen 1000
    link/ether b8:ca:3a:6a:0f:d4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::baca:3aff:fe6a:fd4/64 scope link
        valid_lft forever preferred_lft forever
```

I want to protect my node with firewall and disable all IPv6 traffic:

```
ip6tables -F
ip6tables -t nat -F
ip6tables -t mangle -F
ip6tables -t raw -F
ip6tables -t nat -F

ip6tables -X
ip6tables -t nat -X
ip6tables -t mangle -X
ip6tables -t raw -X
ip6tables -t nat -X

ip6tables -P FORWARD DROP
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
```

/usr/libexec/iptables/ip6tables.init save

It help till next reboot. But some default rules appears again. Especially I like:

```
-A INPUT -j INPUT_ZONES
-A INPUT_ZONES -i vzbr799 -g IN_public
-A INPUT_ZONES -i vzbr798 -g IN_public
```

```
-A IN_public -j IN_public_allow  
-A IN_public_allow -d fe80::/64 -p udp -m udp --dport 546 -m conntrack --ctstate NEW -j ACCEPT  
-A IN_public_allow -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
```

How can I protect hardware nodes?

Maybe configure ip6tables from crontab every minute? Funny isn't it?

Subject: Re: configure iptables on VZ7 host
Posted by [mangust](#) on Sun, 03 Sep 2017 10:48:19 GMT

[View Forum Message](#) <> [Reply to Message](#)

We did barbarian way this time

```
cat <<EOT > /root/closeip6.sh  
#!/bin/sh  
  
/usr/sbin/ip6tables -P FORWARD DROP  
/usr/sbin/ip6tables -P INPUT DROP  
/usr/sbin/ip6tables -P OUTPUT DROP
```

```
/usr/sbin/ip6tables -F  
/usr/sbin/ip6tables -t nat -F  
/usr/sbin/ip6tables -t mangle -F  
/usr/sbin/ip6tables -t raw -F  
/usr/sbin/ip6tables -t nat -F
```

```
/usr/sbin/ip6tables -X  
/usr/sbin/ip6tables -t nat -X  
/usr/sbin/ip6tables -t mangle -X  
/usr/sbin/ip6tables -t raw -X  
/usr/sbin/ip6tables -t nat -X
```

EOT

```
chmod +x /root/closeip6.sh
```

```
cat <<EOT > /etc/cron.d/closeip6  
@reboot root /root/closeip6.sh  
* * * * * root /root/closeip6.sh
```

EOT

```
systemctl restart crond
```

It works, remember last MadMax movie? "Witness me!!!" This is what I feel by controlling firewall

this way

Any better way?

Subject: Re: configure iptables on VZ7 host

Posted by [mangust](#) **on** Mon, 11 Sep 2017 09:13:14 GMT

[View Forum Message](#) <> [Reply to Message](#)

Looks like it was firewalld related. Need just remove it. Not OVZ related. It was Centos 7 new features related.
