Subject: shorewall + OpenVZ. What set in interfaces file for correct work?
Posted by sHaggY_caT on Fri, 31 Oct 2008 12:24:26 GMT
View Forum Message <> Reply to Message

Sorry for my bad English.

I have troubles for shorewall with OpenVZ.

Becouse I'm new shorewall user, I maked test configuration on Virtual Mashine (VirtualBOX) with bridge network.

Prodaction OVZ server work with iptables, and I'm afraid destroy work configuration.
Work, but not work fine. I want simple create new subnetworks, DMZ and overs.

Please help me for make work configuration.

Configuration

1. Host-system:

```
[shaggycat@desktop ~]$ cat /etc/redhat-release
Fedora release 8 (Werewolf)
[shaggycat@desktop ~]$ uname -a
Linux desktop.loc 2.6.26.5-28.fc8 #1 SMP Sat Sep 20 09:12:30 EDT 2008 x86_64 x86_64 x86_64
GNU/Linux
[shaggycat@desktop ~]$ ifconfig
br0       Link encap:Ethernet  HWaddr **************
          inet addr:10.0.5.2  Bcast:10.0.5.255  Mask:255.255.255.0
          inet6 addr: fe80::211:d8ff:fe91:a3da/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1246145 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1563590 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:975442995 (930.2 MiB)  TX bytes:1051074268 (1002.3 MiB)

eth0      Link encap:Ethernet  HWaddr ********
          inet6 addr: fe80::211:d8ff:fe91:a3da/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1246044 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1563463 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:998007741 (951.7 MiB)  TX bytes:1057556364 (1008.5 MiB)
          Interrupt:17

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
```

RX packets:1353 errors:0 dropped:0 overruns:0 frame:0
TX packets:1353 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2680004 (2.5 MiB) TX bytes:2680004 (2.5 MiB)

vbox0 Link encap:Ethernet HWaddr 00:FF:9E:34:22:E5
inet6 addr: fe80::2ff:9eff:fe34:22e5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:5161 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

vbox1 Link encap:Ethernet HWaddr 00:FF:EE:80:DA:5C
inet6 addr: fe80::2ff:eeff:fe80:da5c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:119 errors:0 dropped:0 overruns:0 frame:0
TX packets:142 errors:0 dropped:5142 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:15192 (14.8 KiB) TX bytes:12786 (12.4 KiB)

virbr0 Link encap:Ethernet HWaddr B2:12:B1:BF:97:CB
inet addr:192.168.122.1 Bcast:192.168.122.255 Mask:255.255.255.0
inet6 addr: fe80::b012:b1ff:febf:97cb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:4855 (4.7 KiB)

2. VirtualBOX with host system:

[shaggycat@desktop ~]$ rpm -qa | grep Virtual
VirtualBox-2.0.2_36488_fedora8-1

3. Guest system with ovz-kernel:

[root@localhost ~]# cat /etc/redhat-release
CentOS release 5.2 (Final)
[root@localhost ~]# uname -a
Linux localhost.localdomain 2.6.18-92.1.13.el5.028stab059.3 #1 SMP Wed Oct 15 17:48:55 MSD 2008 i686 athlon i386 GNU/Linux
[root@localhost ~]# ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:89:FF:82
inet addr:10.0.5.4 Bcast:10.0.5.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe89:ff82/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:47 errors:0 dropped:0 overruns:0 frame:0

```
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5274 (5.1 KiB)  TX bytes:5888 (5.7 KiB)
          Interrupt:11 Base address:0xc020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

venet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[root@localhost shorewall]# rpm -qa | grep vz
ovzkernel-2.6.18-92.1.13.el5.028stab059.3
vzrpm44-4.4.1-22.5
vztmpl-fedora-7-1.1-1
vzquota-3.0.11-1
vzctl-3.0.22-1
vzrpm44-python-4.4.1-22.5
vzpkg-2.7.0-18
vzctl-lib-3.0.22-1
vzyum-2.4.0-11
```

4. VE containers with venet network (Fedora 7 distribution):

```
[root@localhost shorewall]# vzlist
      VEID      NPROC STATUS  IP_ADDR         HOSTNAME
       201          5 running 10.0.2.1        test_vps1.loc
       202          3 running 10.0.2.2        test_vps2.loc
[root@localhost shorewall]#
```

If service shorewall stoped, and, all iptables policy set for ACCEPT, all connections successfully:

VPS<-->lan
VPS<-->HN
HN<-->lan

For example, with host computer(from LAN):

```
[shaggycat@desktop ~]$ ssh root@10.0.2.1
root@10.0.2.1's password:
Last login: Sun Oct 26 20:13:56 2008 from 10.0.5.2
[root@test_vps1 ~]#
```

But, from this test policy of shorewall:

```
[root@localhost shorewall]# ls
backup backup2 hosts hosts~ interfaces interfaces~ policy policy~ shorewall.conf
shorewall.conf~ zones zones~

[root@localhost shorewall]# cat hosts
##################### hosts#####################
#ZONE           HOST(S)                                 OPTIONS
web1            venet0:10.0.2.1
desk1           eth0:10.0.5.2
serv2           venet0:10.0.2.2

#inet           0.0.0.0/24

[root@localhost shorewall]# cat interfaces
#ZONE   INTERFACE       BROADCAST       OPTIONSnet     eth0
loc     eth0            detect
net     venet0          detect          routeback
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE

[root@localhost shorewall]# cat policy
################### policy
#############################################################################
#SOURCE         DEST            POLICY          LOG             LIMIT:BURST
#
$FW             all         ACCEPT

#Remove this string!
all             $FW         ACCEPT

#net            $FW         ACCEPT
#loc            $FW         ACCEPT

loc             net         ACCEPT
net             loc         ACCEPT

#net            dmz         ACCEPT
#dmz            all         DROP

all             all         REJECT
#LAST LINE -- DO NOT REMOVE
```

[root@localhost shorewall]# cat zones
#########################zones###
######
#ZONE   TYPE   OPTIONS   IN   OUT
OPTIONS   OPTIONS
fw   firewall

Remove?
#dmz   ipv4
#hn   ipv4
#inet

#local Network
loc   ipv4

#Virtual Network
net   ipv4

#
web1:net
desk1:loc
serv2:net

#LAST LINE - ADD YOUR ENTRIES ABOVE THIS ONE - DO NOT REMOVE

I get trouble

All connections VE <--> Virtual HN accept, becouse:

##########policy#########
<skip>
$FW   all   ACCEPT
all $FW   ACCEPT
<skip>

[root@test_vps1 /]# ping -c 1 10.0.5.4
PING 10.0.5.4 (10.0.5.4) 56(84) bytes of data.
64 bytes from 10.0.5.4: icmp_seq=1 ttl=64 time=0.096 ms

--- 10.0.5.4 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.096/0.096/0.096/0.000 ms
[root@test_vps1 /]#

(I enter for container for "vzctl enter")

```
[root@localhost ~]# ping -c 1 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_seq=1 ttl=64 time=0.100 ms

--- 10.0.2.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.100/0.100/0.100/0.000 ms
```

(from Virtual HN)

But, from external network, connection not work:

```
[shaggycat@desktop bin]$ ssh 10.0.2.1
ssh: connect to host 10.0.2.1 port 22: Connection refused
[shaggycat@desktop bin]$
```

But! If is establishing connection, befor shorewall start, it's work. For example, work ssh connection in lan for VPS.

I think, trouble in this line:

```
[root@localhost shorewall]# cat interfaces | grep venet0
net     venet0          detect          routeback
```

I set this, when i use search for forum:

* http://forum.openvz.org/index.php?t=msg&goto=16406&& amp;amp;srch=shorewall#msg_16406

I don't understand, what I need set from interfaces file?

If is simple and true method, and i'm idiot, please say me)

Thank's for all answers!