Subject: ipsec in openvz - cannot ping containers on the same host
Posted by sikp on Fri, 12 Sep 2014 14:32:50 GMT
View Forum Message <> Reply to Message

Hi,

I have ipsec in openvz container. Seemingly all is running and connection is sucessfully established.
But I have weird problem - I cannot ping containers which are on the same host as the ipsec gw. Other containers - on different hosts - are ok. Better exaplained by the "image" I hope :-):

ipsec - other location - can ping host2 and container2-1 but I cannot ping host1 and container1-2 from here

|
INTERNET
|

host 1 - 10.8.1.1
container1-1 10.8.200.1 - ipsec+firewall
container1-2 10.8.200.2

|
LAN
|
host 2 - 10.8.1.2
container2-1 10.8.200.3

I can ping host2 and container2-1
but I cannot ping host1 and container1-2

When I ping container1-2,
I see packets in container1-1(ipsec) on external iface eth1
root@container1-1:/# tcpdump -i eth1 host 10.2.1.159
11:55:20.599632 IP 10.2.1.159 > 10.8.200.2: ICMP echo request, id 12765, seq 366, length 64

I see them also in container1-1 LAN iface eth0
root@container1-1:/# tcpdump -i eth0 host 10.2.1.159
11:55:20.599632 IP 10.2.1.159 > 10.8.200.2: ICMP echo request, id 12765, seq 366, length 64

And I see them in host1 in bridge vmbr0 (bridged as eth0 in container1:1)

root@host1:~# tcpdump host 10.2.1.159 -i vmbr0
11:55:20.599632 IP 10.2.1.159 > 10.8.200.2: ICMP echo request, id 12765, seq 366, length 64

But I cannot see them in container1-2
root@container1-2:/# tcpdump -i venet0 host 10.2.1.159

When I try ping host1, it's similar - I see ICMP requests packets in host1 but there is no reply to them.

My config:

My kernel
root@host1:~# uname -a
Linux host1 2.6.32-29-pve #1 SMP Thu Apr 24 10:03:02 CEST 2014 x86_64 GNU/Linux

There are no iptables rules - all acccept

My host network configuration:
iface vmbr0 inet static
    address 10.8.1.1
    netmask 255.255.0.0
    gateway 10.8.200.1
    bridge_ports eth0
    bridge_stp off
    bridge_fd 0

auto vmbr1
iface vmbr1 inet static
    bridge_ports eth1
    bridge_stp off
    bridge_fd 0

My ipsec container configuration (only part of..):
..
NETIF=" ifname=eth0,bridge=vmbr0,mac=5E:A0:6E:9F:45:1F,host_ifname=v
eth103.0,host_mac=6A:55:55:AE:74:BF;ifname=eth1,bridge=vmbr1
,mac=1E:E7:AA:7A:1B:95,host_ifname=veth103.1,host_mac=DA:58: B6:B2:5B:E5 "
IPTABLES="ip_tables iptable_filter iptable_mangle ipt_limit ipt_multiport ipt_tos ipt_TOS
ipt_REJECT ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_LOG ipt_length ip_conntrack ip_conntrack_ftp
ipt_state iptable_nat ip_nat_ftp ipt_recent"
CAPABILITY=" NET_ADMIN:on"
DEVNODES="net/tun:rw "
DEVICES="c:10:200:rw "

I have found I think very similar problem here
  forum.openvz.org/index.php?t=msg&goto=45326&&rch =ipsec#msg_45326
I have tried
 net.ipv4.conf.all.disable_xfrm = 1
 net.ipv4.conf.all.disable_policy = 1
but without success..

But my config is a little bit different - I have bridged interfaces in my container.

If you have any idea, please help..

Thanks, Petr