Subject: Public IP via VETH seen as the bridge interface IP
Posted by johey on Mon, 17 Mar 2014 15:42:12 GMT
View Forum Message <> Reply to Message

HN running CentOS release 6.5 (Final), containers running Ubuntu 12.04.4 LTS. My ISP is giving me 10 public IP addresses via DHCP bound to MAC addresses. I can successfully create VETH interfaces for all my containers and I get a public IP address from the ISP. For example container "playground" has 79.136.52.217 and container "web" has 79.136.52.109. My HN has interface vzbr0 with ip 79.136.52.117. All these are assigned from my ISP.

So far so great, but now... If I from "playground" or "web" go to a service telling me my IP address, it shows 79.136.52.117. This is not right. This is my HN vzbr0 interface. It should show the IP from the container from which I am curling. It looks like I am connecting through a NAT, but as far as I know I am not.

For instance:

curl www.ipchicken.com | grep 79.136

shows 79.136.52.117 from any of "playground" or "web". What have I done and how can I solve it?

From HN:

```
[root@openvz ~]# iptables -t nat -L && iptables -t filter -L && iptables -t mangle -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source          destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source          destination
MASQUERADE  all  -- anywhere           anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
Chain INPUT (policy ACCEPT)
target     prot opt source          destination

Chain FORWARD (policy ACCEPT)
target     prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source          destination
Chain PREROUTING (policy ACCEPT)
target     prot opt source          destination

Chain INPUT (policy ACCEPT)
target     prot opt source          destination
```

Chain FORWARD (policy ACCEPT)
target   prot opt source   destination

Chain OUTPUT (policy ACCEPT)
target   prot opt source   destination

Chain POSTROUTING (policy ACCEPT)
target   prot opt source   destination

From container "web":

root@web:/# iptables -t nat -L && iptables -t filter -L && iptables -t mangle -L
iptables v1.4.12: can't initialize iptables table `nat': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.