Subject: How to access private IPs from a container
Posted by tscargo on Wed, 26 Aug 2009 07:46:11 GMT
View Forum Message <> Reply to Message

I have been using openvz for quite a while and am very happy with it.
Recently I added a vps to monitor some devices on my local network in a 10.x range.
My hardware-node and all other VPSes run in my 'external' ip range.

Configuration on my HN (real ip changed to 1.2.3.4):

```
eth0      Link encap:Ethernet  HWaddr 00:30:48:91:3E:14
          inet addr:1.2.3.4  Bcast:1.2.3.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:755314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1039609 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:212586182 (202.7 MiB)  TX bytes:1382180633 (1.2 GiB)
          Base address:0x5000 Memory:e1000000-e1020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          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:1035141 errors:0 dropped:0 overruns:0 frame:0
          TX packets:680342 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1362997196 (1.2 GiB)  TX bytes:194411390 (185.4 MiB)
```

My VPS has the following configuration:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2075571777 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1631407695 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1140876388 (1.0 GiB)  TX bytes:1095784005 (1.0 GiB)

venet0    Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:127.0.0.1  P-t-P:127.0.0.1  Bcast:0.0.0.0  Mask:255.255.255.255
          UP BROADCAST POINTOPOINT RUNNING NOARP  MTU:1500  Metric:1
          RX packets:764 errors:0 dropped:0 overruns:0 frame:0
```

TX packets:1118 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:68840 (67.2 KiB) TX bytes:137911 (134.6 KiB)

venet0:0 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:1.2.3.5 P-t-P:1.2.3.5 Bcast:1.2.3.5 Mask:255.255.255.255
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1

venet0:1 Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
inet addr:10.1.1.27 P-t-P:10.1.1.27 Bcast:10.1.1.27 Mask:255.255.255.255
UP BROADCAST POINTOPOINT RUNNING NOARP MTU:1500 Metric:1

I can communicate fine with IPs in the 1.2.3.x range, any ip in the 10.1.1.x range is unpingable.

While doing a ping from the vps to a private ip, I can see (using tcpdump on HN)

tcpdump icmp -n -i any
tcpdump: WARNING: Promiscuous mode not supported on the "any" device
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
03:40:45.637296 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 1
03:40:45.637296 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 1
03:40:45.637309 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 1
03:40:46.637303 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 2
03:40:46.637303 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 2
03:40:46.637317 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 2
03:40:47.637076 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 3
03:40:47.637076 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 3
03:40:47.637088 IP 1.2.3.5 > 10.1.1.25: icmp 64: echo request seq 3

As you can see the ping packets originate from the IP from venet0:0 instead of from venet0:1

What am I doing wrong ?

Thanks for your help !

Subject: Re: How to access private IPs from a container
Posted by Paparaciz on Thu, 27 Aug 2009 18:52:47 GMT
View Forum Message <> Reply to Message

in HW node add iptables rule smth like:
iptables -A POSTROUTING -s 1.2.3.5 -d 10.1.1.0/255.255.255.0 -j SNAT --to-source 10.1.1.1

where 1.2.3.5 is vps ip
10.1.1.0 your private network (change subnet mask as needed)

10.1.1.1 is ip of HN interface to the 10.1.1.0 network
or if some how you don't need such interface (going through gateway?) you can put ip 1.2.3.4

Subject: Re: How to access private IPs from a container
Posted by tscargo on Thu, 27 Aug 2009 22:19:16 GMT
View Forum Message <> Reply to Message

Paparaciz wrote on Thu, 27 August 2009 14:52in HW node add iptables rule smth like:
iptables -A POSTROUTING -s 1.2.3.5 -d 10.1.1.0/255.255.255.0 -j SNAT --to-source 10.1.1.1

Unfortunately I don't have a POSTROUTING chain ....

iptables --list

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

Subject: Re: How to access private IPs from a container
Posted by tscargo on Thu, 27 Aug 2009 23:54:18 GMT
View Forum Message <> Reply to Message

Some additional information:

If I assign just the private address to the VPS, I can ping all private addresses on the network.

If I then add the address in the 1.2.3.x range, I am no longer able to ping the private addreses.

This really doesn''t make sense to me at all...

Subject: Re: How to access private IPs from a container
Posted by Paparaciz on Fri, 28 Aug 2009 04:00:43 GMT
View Forum Message <> Reply to Message

sorry

iptables -t nat -A POSTROUTING -s 1.2.3.5 -d 10.1.1.0/255.255.255.0 -j SNAT --to-source 10.1.1.1

can you ping private ip from HN?

Subject: Re: How to access private IPs from a container
Posted by tscargo on Fri, 28 Aug 2009 06:52:40 GMT
View Forum Message <> Reply to Message

That indeed worked out fine. Thank you very much.
I am just wondering why I need to do NAT to access a local private address....
The VPS should not send out the packets via the normal IP-address ....

I can't imagine that there is not a way this will work without NAT.

Regards,

Taco
