Subject: (NAT Internet for containers) in a container
Posted by alevchuk on Fri, 05 Mar 2010 05:39:26 GMT
View Forum Message <> Reply to Message

Dear OpenVZ support,

How can I setting-up a container that provides the service of a NAT Internet access for other containers?

Specifically:

I have Container N, Container C1, Container C2.

1. N is talking to the Internet through anything (veth, venet, a "moved" --netdev_add device).

2. N, C1, and C2 all have a venet0:0 IP which they all use to talk to each other.

3. N has ip_forwading enabled

4. N is running something like:

```
iptables -A POSTROUTING -s 192.168.16.0/24 -o vzbr0 -j SNAT --to-source PUBLIC_IP
```

5. C1 and C2 have N as their default gateway.

Problem:

I attempted this setup 2 times in two completely different places, and tested. Each of the 5 above steps work individually.

The packets of C1 and C2 going to Internet never reach N.

My Best Explanation:

I read (don't remember where) that OpenVZ drops all traffic on the Venet if the packet's destination does not match any of the IPs on the private network.

Thank you for reading.

Sincerely,
Alex

Subject: Re: (NAT Internet for containers) in a container
Posted by TheStig on Fri, 05 Mar 2010 11:37:35 GMT
View Forum Message <> Reply to Message

i haven't tried anything like that, but i guess you will have to bind a NIC to N or at least use veth instead of venet in order to make a VPS route traffic.

Why don't you use the HN for NAT?

Subject: Re: (NAT Internet for containers) in a container
Posted by alevchuk on Fri, 05 Mar 2010 21:55:34 GMT
View Forum Message <> Reply to Message

Dear Stig,

Thank you for your feedback.

My N is already using a binded NIC to access the Internet, but that does not help. And it would really suck if I have to switch all containers to veth.

My reasoning for moving the NAT service away from using the Hardware Node (HN) is two fold:
1. The sysadmin work becomes much cleaner when I separate the various services into dedicated containers.
2. I want to move away from having Internet on the HN. I'm running a local approx container, so Internet access is not needed to do the OS updates on the HN.

Alex

Subject: Re: (NAT Internet for containers) in a container
Posted by SeaX on Tue, 04 May 2010 16:28:38 GMT
View Forum Message <> Reply to Message

Hi,

I'm looking to setup exactly the same thing. Have you solved it ? And could you tell me how please ?

I'm quite new using openvz, and looking for this solution for my school project.

Thanks in advance

Subject: Re: (NAT Internet for containers) in a container
Posted by maratrus on Fri, 07 May 2010 13:54:14 GMT
View Forum Message <> Reply to Message

Hello,

I suppose tcpdump would be helpful in your case.

Suppose a C1 is pinging some host in the Internet.
Are you sure that a packet that is going out of C1
reaches HN? Where does it go afterwards? Make sure
that it goes inside N! There has to be an appropriate
routing record on the HN.

Then make sure that this packet passing N's
iptables rules and leaving the HN. Look whether
reply is reaching HN and going to N.