Subject: private ip for host-to-ve communication only
Posted by nikb on Fri, 13 Oct 2006 12:51:10 GMT
View Forum Message <> Reply to Message

When I setup a VE with a private, non-routeable ip number (192.168.xxx.xxx) the ip turns up on my hosts external interface, and is noticed by my provider.

Actually I only need a purely private point-to-pont connection between my host node and the VE, without any arp packets or anything else escapeing to the outside world...

Is this doable? Any comments would be appreciated.
Cheers!

Subject: Re: private ip for host-to-ve communication only
Posted by John Kelly on Fri, 13 Oct 2006 16:02:31 GMT
View Forum Message <> Reply to Message

See http://wiki.openvz.org/Using_NAT_for_VE_with_private_IPs

Subject: Re: private ip for host-to-ve communication only
Posted by nikb on Fri, 13 Oct 2006 16:31:30 GMT
View Forum Message <> Reply to Message

Hi,

thanks for the pointer to the docs, but my problem was not to get NAT
working - in fact it worked excellently with very little effort - but to keep
packets with a private ip as return address from going out into the internet. (or at least from reaching my providers`s router/gateway, which is where they get logged, and then I get a phone call).

In fact I have no idea what exactly my provider notices, but something makes him uneasy. He says that my external IF is configured with a private ip when in fact it isnt. Or shouldnt be. Could that be arp packets?

Seemingly with venet my external interface is somehow showing up configured with the private ip (192.168.XXX.XXX) in my provider`s logs.

Everything looks normal here:

```
hardwarenode:/home/username# ip a
2: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
```

inet 127.0.0.1/8 scope host lo
4: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:e0:83:41:f7:4e brd ff:ff:ff:ff:ff:ff
inet 213.XXX.XXX.hardwarenodeip/24 brd 213.XXX.XXX.255 scope global eth0
1: venet0: <BROADCAST,POINTOPOINT,NOARP,UP> mtu 1500 qdisc noqueue
link/void

and here:

hardwarenode:/home/username# ip r
192.168.0.1 dev venet0 scope link src 213.XXX.XXX.hardwarenodeip
192.168.0.0/24 dev eth0 proto kernel scope link src 213.XXX.XXX.hardwarenodeip
default via 213.XXX.XXX.gateway dev eth0

Subject: Re: private ip for host-to-ve communication only
Posted by John Kelly on Fri, 13 Oct 2006 16:55:42 GMT
View Forum Message <> Reply to Message

nikb wrote on Fri, 13 October 2006 12:31He says that my external IF is configured with a private ip when in fact it isnt. Or shouldnt be. Could that be arp packets?

Yes, that's what OpenVZ does for you, automatically. Try "arp -an" on the HN node, and you will see that your HN is publishing an arp entry for your private IP address.

Although your provider can easily suppress routing of any private address packets, and prevent them from reaching the Internet, apparently he considers it poor management on your part, and expects you to fix it, in order to be considered a good citizen on his network.

That may seem like needless trouble from your POV, but I am impressed with a provider who is strict about keeping his local network clean. If you will reveal who the provider is, I may consider using them myself!

So it seems the challenge is to find a solution that makes your provider happy. Are you saying that packets from the VE are never routed to the outside Internet? And that *only* the HN needs to talk to the VE? If that is true, what is the purpose of the VE? IOW, what application is running on the VE, and why does the HN need to talk to it? Maybe understanding that can help us recommend a solution.

Subject: Re: private ip for host-to-ve communication only
Posted by nikb on Fri, 13 Oct 2006 22:10:06 GMT
View Forum Message <> Reply to Message

Thanks for your answer. Glad to hear I wasnt all wrong;)

My provider, which I will gladly recommend, is internet24.de
from Dresden/Germany. Its a good ISP and I am a customer for several years now.
Never got a phone call before either.

Actually I am in the process of setting up a LAMP-Environment on the ve, and of course it needs contact to the outside world in order to make it easier for me to set it up.

But apart from that its going to run a LAMP configuration behind a SQUID cacheing/accelerating proxy that will run on the host machine. So everyone from outside will talk to the proxy on the HN, and ideally only the proxy will talk to the Webserver on the ve(s).

Subject: Re: private ip for host-to-ve communication only
Posted by Vasily Tarasov on Sat, 14 Oct 2006 07:00:41 GMT
View Forum Message <> Reply to Message

I suppose you installed openvz using rpm. During installation the following changes to sysctl.conf file introduced:

```
# On Hardware Node we generally need
# packet forwarding enabled and proxy arp disabled
net.ipv4.ip_forward = 1
net.ipv4.conf.default.proxy_arp = 0
# Enables source route verification
net.ipv4.conf.all.rp_filter = 1
# Enables the magic-sysrq key
kernel.sysrq = 1
# TCP Explict Congestion Notification
#net.ipv4.tcp_ecn = 0
# we do not want all our interfaces to send redirects
net.ipv4.conf.default.send_redirects = 1
net.ipv4.conf.all.send_redirects = 0
```

I suppose, changing net.ipv4.ip_forward to 0 should help in your situation.

HTH,
vass.

Subject: Re: private ip for host-to-ve communication only
Posted by nikb on Sat, 14 Oct 2006 07:28:55 GMT
View Forum Message <> Reply to Message

That was helpful, thanks.

My servers (both HN and VEs) are debian setups, so you can configure

ipv4 forwarding both in sysctl.conf and in /etc/network/options.

I had it turned off in the options-file but turned on (by the openvz-installation) in sysctl.conf. Turns out sysctl.conf prevailed, and it was thus turned on:

hardwarenode:~# cat /proc/sys/net/ipv4/ip_forward
1

OK, but now lets make things a little more difficult: My HN is also hosting a
regular ve with a regular, routeable external ip that, of course, should remain
reacheable from outside. So I really cannot turn off ip forwarding altogether.
Any idea how I could disable forwarding for one specific subnet or maybe just for interface venetXXX?

On top of that - I dont even think that regular data got routed out of my eth0 - I think my provider really just picked up arp packets.

But right now, I`m even lacking a proper way to find out what exactly is leaving my HN. Probably should look into it with tcpdump.

Subject: Re: private ip for host-to-ve communication only
Posted by Vasily Tarasov on Sun, 15 Oct 2006 16:14:59 GMT
View Forum Message <> Reply to Message

Hello,

and what about setting routing in VE/on HN in the way that this VE can see only HN?

HTH,
vass.

Subject: Re: private ip for host-to-ve communication only
Posted by John Kelly on Mon, 16 Oct 2006 16:07:23 GMT
View Forum Message <> Reply to Message

You said:

Quote:My HN is also hosting a regular ve with a regular, routeable external ip that, of course, should remain reacheable from outside

And:

Quote:I am in the process of setting up a LAMP-Environment on the ve, and of course it needs contact to the outside world in order to make it easier for me to set it up

Then the LAMP VE needs a routeable IP, just like the other VE. Otherwise, how will you login for management purposes, from the outside? If you insist on using a private IP for the LAMP VE, then you must do a two-stage login (which will soon become tiresome and annoying), or set up some kind of tunnel.

If that is the case, consider using a veth device for the private IP, because AFAIK, there is no way to prevent OpenVZ from publishing an ARP entry for the IP address of a venet interface.

I'm not sure how that will work with a veth interface, because I have not tried it. You can read about veth devices in the wiki. Please let us know how it goes.