Subject: Re: Routing blues
Posted by laotse on Mon, 22 Dec 2008 11:43:26 GMT
View Forum Message <> Reply to Message

Quote:venet driver drops all packets with destination addresses which are not assigned to venet0 interface inside VE.
In your case (172.16.2.1 is belong to eth3 not venet0).

Ah, this explains it. I guess that this is a feature and probably has no configuration option.

Quote:Why don't you use veth interface

If I understand correctly this produces an additional internal interface.

The container is expected to be the endpoint of subnets of medium and no trust. So, if someone should manage breaking e.g. OpenVPN and inject code, he'll end up in a container, which does not even have a root user. Dead End!

The rest of the machine - both node and containers - do not have to be aware of these physical interfaces. In security language: eth3 shall not be accessible except for this one container.

So the second best solution will probably be to add another venet and NAT eth3 to it. Or would it drop the post routed packets?

Setting up a veth bridged to eth3 adds another level of configuration and therefore errors. Is there anything, which I am missing in this picture?

Regards,
- lars.