Subject: Re: 2 interfaces local network routing issue possible bug?
Posted by khorenko on Mon, 30 Jul 2007 11:12:48 GMT
View Forum Message <> Reply to Message

QuantumNet wrote on Fri, 27 July 2007 17:36So IPtables is the only way to curb this behavior huh? I figured there would have been a proper way to disable it in the kernel routing or some config file.

Let's imagine you have 2 physical nodes A (public IP) and B (private IP) in the same segment.
Can you ping the node B from A?
If you set the correct routing on the A (dev eth0) the answer will be YES if node B has a route back to A and no iptables rules on B prevent this.
In your case node A - the VE, node B - the Hardware Node. Node B already has a route to node A (or no packets at all will reach node A (VE)). Thus the only way to deny the ping from VE to HN is iptables.

Well, not exactly. You can completely change the network scheme: you can set up a bridge on the HN and use veth interface for VE instead of venet. Create and configure a bridge on the HN and add physical eth0 and corresponding veth interface to it. In this case you can remove route to the VE's IP on the HN and set up the exact default gateway (not just "dev" but also "via") on HN. Thus if that default gateway won't know about the VE's IP, the packets from HN won't reach VE.

But IMHO, iptables variant is much simpler if you definitely want to deny the connections.