Subject: Re: 2 interfaces local network routing issue possible bug?
Posted by QuantumNet on Mon, 30 Jul 2007 23:11:22 GMT
View Forum Message <> Reply to Message

Quote: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.

I dont agree with this one bit, it is not default behavior to make the public IP space communicate with the private IP space unless otherwise specified in NAT redirection or the system routing rules but it is not a default behavior it has to be later implimented.

Anyways I curbed this issue as stated with iptables:

iptables -A FORWARD -i venet0 -s 75.21.221.23 -d 10.21.1.3/24 -j DROP
iptables -A INPUT -i venet0 -s 75.21.221.23 -d 10.21.1.3/24 -j DROP

then in each VE that I wanted to be able to communicate with the backend network I assigned a local IP to it and set a corrusponding routing rule:
ip route add 10.0.0.0/8 dev venet0 src 10.21.1.32