Subject: Re: Ability to use VE as firewall? Recommended security pattern?
Posted by scythe on Fri, 11 Aug 2006 13:30:42 GMT
View Forum Message <> Reply to Message

Hi,

I think it is possible.

It's just a theory, but I made up an example like this:

You got the HN with an Incoming eth. You don't give this eth an IP, instead You bridge it to the Firewall VE's veth interface, which gets the real IP.
The firewall VE got another interface, like a real firewall with 2 eths. The other interface (It can be veth or venet, doesn't matter I think) got an IP of your internal network. On the host node, only this other interface got an own IP address (the host node will only get internal IP addresses this way). The host node does routing between the firewall VE and the other VEs on this second interface, while all incoming/outgoing communications goes trough the first interface, which is just bridged trough the host node. Poor performance can be a result, I think the whole thing can be done using only the quicker venet interfaces, while that possibly limits the firewall rules You use.

Some drawing for this:
(Sorry for the dots, html doesn't like more than one spaces)

INTERNET <-> eth0_on_host_node, NO REAL IP ADDRESS
.... | Bridged |
.... veth0_on_host_node <-> veth0_firewall_VE, REAL IP
 ....| iptables,etc |
.... veth1_on_host_node <-> veth1_firewall_VE, 10.x.x.x
.... | routing |
.... venetX/vethX_on_host <-> corresponding_internal_VE

I think this should work, altough I didn't try it (but I will, this interests me aswell).

Scythe