Subject: Ability to use VE as firewall? Recommended security pattern?
Posted by jbwiv on Thu, 10 Aug 2006 17:53:52 GMT
View Forum Message <> Reply to Message

Guys,

First of all, thanks for this project. It has really been a great experience so far!

I'm building an OpenVZ box that will host two types of VEs, hopefully. One set of VEs will have private IP addresses and will be NAT'd and PAT'd through a firewall. The other set of VEs will have public IP addresses, and will either live outside the firewall or will be set up as a bidirectional NAT.

What I'd like to know....can I run a VE and use it as THE firewall to do the above? I'm very concerned with using the Hardware host as a firewall in this regard, as I believe it makes it a target for compromise, and if successful ALL VEs are compromised as well.

So, is it possible?

Also, one thing that may complicate this is that VEs cannot see eachother over IP, and in the above possible configuration they would need to (at the very least, the Firewall VE would need to be able to see each VE it was NAT'ing, and vice versa. Is it possible to do this? Is this what veth is for? If so, can I run some VEs with veth and others with venet (i.e., veth only for those that I want to NAT). What are the implications here?

Finally, any other security concerns you would recommend I consider? I want to lock down as much as possible.

I appreciate the help and look forward to using (and contributing to) OpenVZ!

jbwiv

Subject: Re: Ability to use VE as firewall? Recommended security pattern?
Posted by jbwiv on Thu, 10 Aug 2006 23:26:54 GMT
View Forum Message <> Reply to Message

Is it better to post questions like this to the mailing list? Anyone?

Thanks,
jbwiv

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