Subject: Firewalls and security patterns
Posted by John Wells on Fri, 11 Aug 2006 01:19:14 GMT
View Forum Message <> Reply to Message

Guys,

First of all, thanks to all involved for this project. It has really been a great experience so far! I have been working with Xen before OpenVZ, and really like the ease of use and documented features OpenVZ offers.

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