Subject: Netfilter connection tracking not working in VE?
Posted by Frederik on Thu, 06 Mar 2008 09:44:20 GMT
View Forum Message <> Reply to Message

Hi,

I am using Shorewall to set up a firewall in a VE. Now the problem is that outgoing connections do not work, although I accept traffic from the firewall to the network zone. I contacted the shorewall developer, and he took a look at my configuration and he thinks that something is going wrong in the kernel's connection tracking system. It seems indeed the incoming packets responding to the outgoing packets, do not match the state RELATED,ESTABLISHED rules which should accept them. Disabling the firewall in the VE, or creating rules which accept the incoming packets, makes it work, but of course this should not be necessary with the RELATED,ESTABLISHED rule.

Some information on the hardware host (running Debian Lenny):
http://artipc10.vub.ac.be/openvz/hnode.txt

And on the VE (running Debian Etch):
http://artipc10.vub.ac.be/openvz/ve.txt

As you can see in the shorewall show output, no packets matched the RELATED,ESTABLISHED rule in the net2fw rule, but instead packets are matched by the fallback rule forwarding them to the Drop chain, and they eventually seem to be dropped in the DropInvalid chain because of state INVALID.

There's a Shorewall firewall on the hardware host too, but that one accepts all relevant traffic: everything works with the firewall on the hardware node enabled and the firewall in the VE disabled.

A related question, where can I find the logs of the firewall in the VE? dmesg in the VE is empty and nothing is logged in /var/log, while the logs in the hardware node only seem to reflect the firewall on the hardware node.

--
Frederik