Subject: Re: Do yo firewall your HN and VE
Posted by marcel.chastain on Tue, 17 Jun 2008 16:05:00 GMT
View Forum Message <> Reply to Message

There are 3 main ways that a packet can be filtered in iptables -
INPUT
OUTPUT
FORWARD

The INPUT chain is traffic from the external internet to the Hardware Node
The OUTPUT chain is traffic from the Hardware Node to the external internet
The FORWARD chain is all traffic TO and FROM the jails, and is the only way to filter stuff.

Your APF is probably misconfigured to DROP EVERYTHING on the FORWARD chain, which is common for normal servers (because they aren't forwarding network traffic).

run this to see your currently active rules
iptables-save | less

It should print out your current rules, and check for the default policy at the top, something like this:

:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0] # <---- Right there
:OUTPUT ACCEPT [0:0]

You can change it to 'ACCEPT', or create rules on the FORWARD chain to allow/disallow all the traffic you want. Might be difficult with APF.

Hope this helps.