Subject: Re: Netfilter connection tracking not working in VE?
Posted by Frederik on Thu, 06 Mar 2008 11:43:27 GMT
View Forum Message <> Reply to Message

On Thu, 06 Mar 2008 12:21:03 +0100, MailingListe wrote:

>> 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.

> The available features of iptables depend on the kernel modules loaded.
> By default it is not possible to load additional kernel modules on
> demand inside the VE. Older kernels even need to enable firewall inside
> the VE to get it work but i don't know for which version this have
> changed. So double check if the necessary modules are loaded at startup

I think shorewall checks this at start-up, and AFAIK this looks good.

>From /var/log/shorewall-init.log on VE:
Shorewall has detected the following iptables/netfilter capabilities:
NAT: Not available
Packet Mangling: Available
Multi-port Match: Available
Extended Multi-port Match: Available
Connection Tracking Match: Available
Packet Type Match: Available
Policy Match: Available
Physdev Match: Available
Physdev-is-bridged Support: Available
Packet length Match: Available
IP range Match: Available
Recent Match: Available
Owner Match: Available
Ipset Match: Not available
CONNMARK Target: Available
Extended CONNMARK Target: Available
Connmark Match: Available
Extended Connmark Match: Available
Raw Table: Not available
IPP2P Match: Not available
CLASSIFY Target: Available
Extended REJECT: Available
Repeat match: Available
MARK Target: Available
Extended MARK Target: Available
Mangle FORWARD Chain: Available

Comments: Available
Address Type Match: Available
TCPMSS Match: Available
Hashlimit Match: Available
NFQUEUE Target: Available

> and if the kernel log /proc/kmesg is available inside the VE.

It exists:
ls -lh /proc/kmsg
-r-------- 1 root root 0 Mar 6 12:28 /proc/kmsg

klogd is started, but I cannot find anything in the logs when nmapping the host.

Actually now I found out why looking at the shorewall show output after nampping: when the firewall is enabled, all packets which are correctly dropped, are not dropped (and hence logged) because of my shorewall policy, but because they end up matching the state INVALID rule, which drops without logging. So this is actually exactly the same problem as above.

--
Frederik