Subject: Iptables inside VE only works for a few minutes
Posted by Tobi2WO on Wed, 22 Jul 2009 14:11:05 GMT
View Forum Message <> Reply to Message

I use iptables inside a VE (10.0.0.103) with an OUTPUT rule to re-route outgoing traffic with destination of hardware node to another VE on the same machine (specific tcp port).

This is the rule:
iptables -t nat -A OUTPUT -d *public_ip*/32 -p tcp -m tcp --dport 51234 -j DNAT --to-destination 10.0.0.106:51234

The problem is, that connections does not work until i trigger the rule with something like "telnet 10.0.0.106 51234". After that, it is working for a few minutes before it stops again.

Heres a detailed log of my actions:

1) telnet *public_ip* 51234
- no reaction
2) grep 51234 /proc/net/ip_conntrack
- no output

3) telnet 10.0.0.106 51234
- connection successful
4) grep 51234 /proc/net/ip_conntrack
- tcp 6 118 TIME_WAIT src=10.0.0.103 dst=10.0.0.106 sport=54398 dport=51234 packets=5 bytes=274 src=10.0.0.106 dst=10.0.0.103 sport=51234 dport=54398 packets=5 bytes=274 [ASSURED] mark=0 secmark=0 use=1

5) telnet *public_ip* 51234
- now it works!
6) grep 51234 /proc/net/ip_conntrack
- in addition to upper output:
tcp 6 118 TIME_WAIT src=10.0.0.103 dst=*public_ip* sport=40356 dport=51234 packets=5 bytes=274 src=10.0.0.106 dst=10.0.0.103 sport=51234 dport=40356 packets=5 bytes=274 [ASSURED] mark=0 secmark=0 use=1

My system:
64bit Debian Lenny with Kernel 2.6.26-2-openvz-amd64
Problem occurs in 32 and 64 bit VEs (all Debian Lenny)

Before that, I had a 32 bit Debian Lenny Hardware Node with exactly the same VEs and a vanilla 2.6.18 kernel with OpenVZ Patch. There, my iptables rules worked correctly.
Either its a problem with 64bit hardware node or with the 2.6.26 kernel.