Subject: certain iptables filter rules not working ?
Posted by geejay on Tue, 27 May 2008 14:42:05 GMT
View Forum Message <> Reply to Message

Further to my problem below.

It appears that certain filter directives in iptables are causing the error and not the COMMIT, when I comment out these directives then my firewall inside the container works:

Accept traffic with the ACK flag set
-A INPUT -p tcp -m tcp --tcp-flags ACK ACK -j ACCEPT

Accept responses to DNS queries
-A INPUT -p udp -m udp --dport 1024:65535 --sport 53 -j ACCEPT

Allow SSH
-A INPUT -p tcp -m tcp -s 34.158.176.17 --dport 22 -j ACCEPT

Anyone any idea what is "wrong" with these iptable rules ?

TIA

Geejay

Hello,

I am trying to set up iptables inside a container. I see that iptables-restore fails always on the line with the last COMMIT command after the *filter rules.

My parameters in vz.conf are

IPTABLES="iptable_filter iptable_mangle ipt_limit ipt_multiport ipt_tos ipt_TOS ipt_REJECT ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_LOG ipt_length ip_conntrack ip_conn track_ftp ip_conntrack_irc ipt_conntrack ipt_state ipt_helper iptable_nat ip_nat_ftp ip_nat_irc ipt_REDIRECT"

I cant see any descriptive error message other than the "line XX failed", which contains the last COMMIT command.

Any help would be greatly appreciated. I am running openvz on Debian Etch, self-compiled kernel 2.6.18 with openvz patch.

BTW: Iptables on the host itself does not complain and works.

Thanks

Geejay