Subject: Problem with IPTABLES OpenVZ kernel
Posted by linux_342 on Fri, 19 May 2017 19:01:38 GMT
View Forum Message <> Reply to Message

I was trying to lock down iptables on a new OpenVZ node and noticed a big issue.
While setting my input chains to only allow connections from a list of trusted IP addresses I noticed that all the statements in the input chains are being ignored.
I have the same iptables running on a kvm node without a problem.
I went to my other OpenVZ node to check and see if the same issue can be found there also and to my surprise, the same issue is on both OpenVZ nodes.
That is a big problem as I always had my list of trusted IPs to allow SSH connections from.
I only have this problem running on my OpenVZ slaves with uname "2.6.32-042stab123.3" and "2.6.32-042stab117.14".
My other servers with kernel uname "696.1.1.el6.x86_64" works fine as it should.

Here are the condensed version of the rules...
If it works like it should, the following will drop any ssh connection from source IPs that is not listed in the "whitelisted_ip" chain. But the problem I am having, is it ignoring all the statements except for statement 10. The result is it blocks all traffic period!
If I append statement "-A whitelisted_ip -j DROP to the end of the "whitelisted_ip" chain" and remove statement 10, it does nothing as the chain is ignored completely.

01 -P INPUT ACCEPT
02 -P FORWARD ACCEPT
03 -P OUTPUT ACCEPT
04 -N whitelisted_ip
05 -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
06 -A INPUT -p icmp -j ACCEPT
07 -A INPUT -i lo -j ACCEPT
08 -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j whitelisted_ip
09 -A INPUT -j REJECT --reject-with icmp-host-prohibited
10 -A INPUT -j DROP
11 -A FORWARD -j REJECT --reject-with icmp-host-prohibited
12 -A whitelisted_ip -s xxx.xxx.xxx.xxx/26 -j ACCEPT
13 -A whitelisted_ip -s xxx.xxx.xxx.xxx/32 -j ACCEPT
14 -A whitelisted_ip -s xxx.xxx.xxx.xxx/32 -j ACCEPT

I checked iptables-config and verified the statement:
IPTABLES_MODULES="ipt_REJECT ipt_tos ipt_TOS ipt_LOG ip_conntrack ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state iptable_nat ip_nat_ftp ipt_owner ipt_REDIRECT"

Please shine some light if you know that there is an issue with the kernel mentioned or f there needs to be another tweak I am unaware of.