Subject: iptables do not append rules
Posted by andrex on Sun, 14 Jun 2015 01:14:33 GMT
View Forum Message <> Reply to Message

I want to make a set of rules on iptables inside of a node, but it seems that the iptables isn't appending all the rules or somehow and kick me out everytime I run the script:

```
# Allow connections that are already connected to your server
iptables -A INPUT -i venet0 -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow connections to SSH
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT

# Allowing connections to HTTP/HTTPS
iptables -A INPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW -j ACCEPT

# Allow icmp input but limit it to 10/sec
iptables -A INPUT -p icmp -m limit --limit 10/second -j ACCEPT
iptables -A INPUT -p icmp -j ACCEPT

# Allow all incoming traffic from local
iptables -A INPUT -i lo -j ACCEPT

# Changing the default policy for INPUT chain
iptables -A INPUT -j DROP
```

I already change the conf for vz:
IPTABLES_MODULES="ipt_REJECT ipt_tos ipt_limit ipt_multiport iptable_filter iptable_mangle ipt_TCPMSS ipt_tcpmss ipt_ttl ipt_length ipt_state xt_state ip_conntrack"

Any help with this is aprecciated.

Thanks.

Subject: Re: iptables do not append rules
Posted by andrex on Mon, 07 Sep 2015 17:31:44 GMT
View Forum Message <> Reply to Message

Nobody? *bump*

Subject: Re: iptables do not append rules
Posted by curx on Sat, 12 Sep 2015 08:08:08 GMT

more info please:

- vzctl version
- ouput $ grep NETFILTER /etc/vz/con/<ctid>.conf # ctid=container id
- can you enter ct via vzctl enter and apply the iptables rules