Subject: iptables help please
Posted by Light Speed on Fri, 11 Jul 2008 00:02:48 GMT
View Forum Message <> Reply to Message

Since upgrading my VE from CentOS 5.1 to 5.2 I am getting some errors in messages that look like they are iptables related.

If anybody could help comment on my iptables rules to let me know if I have them set up incorrectly I would appreciate it

This is on a VPS at a remote data center and not a box on my lan.

The xx.xx.xx.xx is my static IP for my home office.

The chain banished is IPs of crackers that were repeatedly trying to get in my system and their source IPs are set to deny.

Run chain banished Always
Accept If input interface is lo
Accept If protocol is TCP and TCP flags ACK (of ACK) are set
Accept If state of connection is ESTABLISHED
Accept If state of connection is RELATED
Accept If protocol is TCP and source port is 53
Accept If protocol is UDP and source port is 53
Accept If protocol is ICMP and ICMP type is echo-reply
Accept If protocol is ICMP and ICMP type is destination-unreachable
Accept If protocol is ICMP and ICMP type is source-quench
Accept If protocol is ICMP and ICMP type is time-exceeded
Accept If protocol is ICMP and ICMP type is parameter-problem
Accept If protocol is ICMP and ICMP type is echo-request
Drop If protocol is TCP and destination port is ftp
Accept If protocol is TCP and source is xx.xx.xx.xx and destination port is ssh
Drop If protocol is TCP and destination port is ssh
Accept If protocol is TCP and destination port is 25
Accept If protocol is TCP and destination port is 80
Accept If protocol is TCP and source is xx.xx.xx.xx and destination port is 110
Drop If protocol is TCP and destination port is 110
Accept If protocol is TCP and destination port is 113
Accept If protocol is TCP and source is xx.xx.xx.xx and destination port is 143
Drop If protocol is TCP and destination port is 143
Accept If protocol is TCP and destination port is 443
Drop If protocol is TCP and destination port is 465
Accept If protocol is TCP and source is xx.xx.xx.xx and destination port is 10000:10010
Drop If protocol is TCP and destination port is 10000:10010
Accept If protocol is TCP and source is xx.xx.xx.xx and destination port is 20000
Drop If protocol is TCP and destination port is 20000
Accept If source is 127.0.0.1
Accept If input interface is venet0

The type of error I am seeing is:
Jul 10 16:42:12 vps kernel: IN= OUT=venet0 SRC=IP.IP.IP.IP DST=xx.xx.xx.xx LEN=1452 TOS=0x08 PREC=0x00 TTL=64 ID=4361 DF PROTO=TCP SPT=22 DPT=63628 WINDOW=644 RES=0x00 ACK URGP=0

xx.xx.xx.xx=any ip accessing the server
IP.IP.IP.IP=IP of the server
