Subject: IPTables Issue
Posted by rcraig114 on Sun, 02 Mar 2014 23:18:24 GMT
View Forum Message <> Reply to Message

I am attempting to lock down a VoIP box that is an OpenVZ container in a colo. The goal is to only allow TCP 80 to certain IPs, but with the below rules, it's open period. Anyone see what I am missing? Thanks for your help.

```
# reset
iptables -F
iptables -X

# default policy
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# openvz policy
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i venet0 -j ACCEPT
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#SERVER_IP="63.141.X.X"
iptables -A INPUT -p icmp --icmp-type 0 -s 0/0 -d 63.141.X.X -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -d 63.141.X.X -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 0 -s 63.141.X.X -d 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 8 -s 63.141.X.X -d 0/0 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# gre tunnel
iptables -A INPUT -p gre -j ACCEPT


# open ports

# ssh
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# web
iptables -A INPUT -s 192.168.4.0/24 -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 70.122.X.X -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 192.168.0.16/28 -m state --state NEW -p tcp --dport 80 -j ACCEPT

# ssl
#iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

TFTP
iptables -A INPUT -p udp --dport 69 -j ACCEPT

SIP Ports
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 5060:5080 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 10000:20000 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 16384:32767 -j ACCEPT

Subject: Re: IPTables Issue
Posted by marcin4 on Mon, 03 Mar 2014 14:02:45 GMT
View Forum Message <> Reply to Message

I am no expert, but after you allow ip's to access your port 80:
iptables -A INPUT -s 192.168.4.0/24 -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 70.122.X.X -m state --state NEW -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 192.168.0.16/28 -m state --state NEW -p tcp --dport 80 -j ACCEPT

You need to block every other host from it:

/sbin/iptables -A INPUT -i eth0 -p tcp --dport 80 -j DROP

Adjust your eth to your server.

Subject: Re: IPTables Issue
Posted by Paparaciz on Tue, 04 Mar 2014 19:15:45 GMT
View Forum Message <> Reply to Message

at the very beginning you have added rule:

iptables -A INPUT -i venet0 -j ACCEPT

you start to accept everything even your default policy is to drop. please adjust your firewall without that line

---