Forum: CentOS 6 - General Support
Topic: iptables blocks dns
Subject: Re: iptables blocks dns
Posted by: agriz
Posted on: 2011/12/8 21:52:03

I had the output policy to deny. But i was having problems with wget, curl and yum
Temporarily i have changed the deny to accept. Before finding a solution, i got problem with name server.

When i turn on iptables, site is not loading.

This is the output of iptables-save

:INPUT DROP [0:0] :FORWARD DROP [0:0] :OUTPUT ACCEPT [26:2884] -A INPUT -i lo -j ACCEPT -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p tcp -m tcp --dport 1234 -m state --state NEW,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p icmp -m icmp --icmp-type 8 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p icmp -m icmp --icmp-type 0 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p tcp -m tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p tcp -m tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p tcp -m tcp --dport 10000 -m state --state NEW,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p tcp -m tcp --dport 21 -m state --state NEW,ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p tcp -m tcp --sport 1234 -m state --state ESTABLISHED -j ACCEPT -A INPUT -i eth0 -p udp -m udp --sport 53 --dport 1024:65535 -j ACCEPT -A INPUT -p tcp -m state --state NEW -m tcp --dport 25 -j ACCEPT -A OUTPUT -o lo -j ACCEPT -A OUTPUT -o eth0 -p tcp -m tcp --sport 1234 -m state --state ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p icmp -m icmp --icmp-type 0 -m state --state RELATED,ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p icmp -m icmp --icmp-type 8 -m state --state RELATED,ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p tcp -m tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p tcp -m tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p tcp -m tcp --sport 10000 -m state --state ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p tcp -m tcp --sport 21 -m state --state ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p tcp -m tcp --dport 1234 -m state --state NEW,ESTABLISHED -j ACCEPT -A OUTPUT -o eth0 -p udp -m udp --sport 1024:65535 --dport 53 -j ACCEPT COMMIT # Completed on Fri Dec 9 03:18:50 2011 # Generated by iptables-save v1.4.7 on Fri Dec 9 03:18:50 2011 *mangle :PREROUTING ACCEPT [40:22161] :INPUT ACCEPT [40:22161] :FORWARD ACCEPT [0:0] :OUTPUT ACCEPT [40:3964] :POSTROUTING ACCEPT [40:3964] COMMIT # Completed on Fri Dec 9 03:18:50 2011 # Generated by iptables-save v1.4.7 on Fri Dec 9 03:18:50 2011 *nat :PREROUTING ACCEPT [6:265] :POSTROUTING ACCEPT [5:356] :OUTPUT ACCEPT [5:356] COMMIT # Completed on Fri Dec 9 03:18:50 2011

1234 is my ssh
10000 is webmin control panel