

Help with Iptables on with RH linux

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-07/msg00222.html>

- *From:* James Marcinek <jmarc1@xxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 21 Jul 2006 10:48:14 -0400
-

Hello Everyone,

I've been running my Red Hat box as a router for my small network for the past couple of years with no problems (if it works don't fix it). I have another live IP address that I would like use. I would like any traffic destined for this 'new' address to forward (DNAT) traffic to a system in my intranet. I don't want to blindly allow all traffic, just certain ones based off of rules. I have attempted to do this a couple of time but without success. Below is my current topology (real IP's have been substituted for 172.10.10.x addresses:

Internet

|
|
|

| 172.10.10.1 eth0 |

||
||

192.168.0.1 eth1

|
|
|

Intranet (private network)

Here's what I would like to have:

Internet

|
|
|

| 172.10.10.1 eth0 |

| 172.10.10.2 eth0:0 |

||
||

192.168.0.1 eth1

|

Help with Iptables on with RH linux

|
|
Intranet (private network)
|

----->172.10.10.2 traffic to 192.168.0.2

I have already setup the 'outside' interface for both IP addresses but I have had no success. Below is the firewall script I have modified and no longer works properly! (Thank god I didn't save it!):

```
# First drop everything (lets you open what you want)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP

# PREROUTING chain rules
iptables -t nat -A PREROUTING -d 68.238.170.99 -j DNAT --to-dest 192.168.0.2

# User-defined chain for ACCEPTed TCP packets
iptables -N okay
iptables -A okay -p TCP --syn -j ACCEPT
iptables -A okay -p TCP -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A okay -p TCP -j DROP

# INPUT chain rules
iptables -A INPUT -p ALL -i eth1 -s 192.168.0.0/24 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 127.0.0.1 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 192.168.0.1 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 172.10.10.1 -j ACCEPT
iptables -A INPUT -p ALL -i lo -s 172.10.10.2 -j ACCEPT
iptables -A INPUT -p ALL -i eth1 -d 192.168.0.255 -j ACCEPT

# Rules for incoming packets from the Internet

# Packets for established connections
iptables -A INPUT -p ALL -d 172.10.10.1 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p ALL -d 172.10.10.2 -m state --state ESTABLISHED,RELATED -j ACCEPT

# TCP rules
iptables -A INPUT -p TCP -d 172.10.10.2 -s 0/0 --destination-port 21 -j okay
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 21 -j okay
iptables -A INPUT -p TCP -d 172.10.10.2 -s 0/0 --destination-port 22 -j okay
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 22 -j okay
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 25 -j okay
iptables -A INPUT -p TCP -d 172.10.10.2 -s 0/0 --destination-port 80 -j okay
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 80 -j okay
iptables -A INPUT -p TCP -d 172.10.10.2 -s 0/0 --destination-port 443 -j okay
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 443 -j okay
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 953 -j okay
```

Help with Iptables on with RH linux

```
iptables -A INPUT -p TCP -i eth0 -s 0/0 --destination-port 993 -j okay

# UDP rules
iptables -A INPUT -p UDP -d 172.10.10.2 -s 0/0 --destination-port 53 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 -s 0/0 --destination-port 53 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 -s 0/0 --destination-port 2074 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 -s 0/0 --destination-port 4000 -j ACCEPT
iptables -A INPUT -p UDP -i eth0 -s 0/0 --destination-port 953 -j ACCEPT

# ICMP rules

# FORWARD chain rules
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# OUTPUT chain rules
iptables -A OUTPUT -p ALL -s 127.0.0.1 -j ACCEPT
iptables -A OUTPUT -p ALL -s 192.168.0.1 -j ACCEPT
iptables -A OUTPUT -p ALL -s 172.10.10.1 -j ACCEPT
iptables -A OUTPUT -p ALL -s 172.10.10.2 -j ACCEPT

# POSTROUTING
iptables -t nat -A POSTROUTING -s 192.168.0.2 -j SNAT --to-source 172.10.10.2
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 172.10.10.1
```

The last time I attempted to load this I could no longer ssh into my router once the rules were applied (I needed to do an service iptables restart). Each time I would do iptables -F to flush the rules. Can anyone tell me how to go about this?

Thanks,

James

--
redhat-list mailing list
unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>
<https://www.redhat.com/mailman/listinfo/redhat-list>