

Re: Help with Iptables on with RH linux

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-07/msg00226.html>

- *From:* James Marcinek <jmarc1@xxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 21 Jul 2006 16:56:20 -0400
-

Stuart,

First – thanks for responding

Stuart Sears wrote:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

James Marcinek wrote:

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:

[huge diagram snipped]

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!):

okay, I have edited this to show the rules that will (mostly) be relevant here.

```
# First drop everything (lets you open what you want)
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Re: Help with Iptables on with RH linux

This may be what is causing ssh to fail.

```
iptables -P FORWARD DROP
```

I'm not sure. This was part of my original script and caused no problems before. Basically I drop everything and allow the rules/tables to specify what comes through.

this may be your problem. See below

```
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP

# PREROUTING chain rules
iptables -t nat -A PREROUTING -d some_ip_address* -j DNAT
--to-dest
192.168.0.2
```

* perhaps you meant to change that destination IP to 172.x.x.x as well?
other than that the rule looks okay.

My attempt (I say attempt) here is to say anything destined for -d 172.x.x.2, forward this to my internal IP of 192.168.0.2. - yes you were correct.

```
# FORWARD chain rules
```

this is where I think your problem lies.

```
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT
```

you are only accepting traffic in the FORWARD chain if

- a) it comes from inside your network
- b) it is part of an existing connection.

with a policy of DROP here, any traffic attempting to flow from eth0:0 through eth1 to 192.168.0.2 is being dropped.

to follow this you need to understand iptables packet flow.

```
|-> FORWARD ->|
packet in -> PREROUTING ->| |--> POSTROUTING ---> out.
|-> INPUT ->|
```

INPUT only when packets have a destination IP of your firewall.
FORWARD when they don't and are just passing through.

Re: Help with Iptables on with RH linux

the FORWARD chain contains rules that affect packets passing through your system (in either direction).

It looks like you were correctly changing the destination of packets hitting your new IP but were then DROPPing them in the FORWARD chain.

if you add this:

```
iptables -A FORWARD -i eth0 -d 192.168.0.2 -j ACCEPT
```

does it suddenly start working?

Ok, now this is where I'm losing you a little. My server has several ports that it listens... Any internal established connections from my traffic from my internal NIC (eth1), as well as any established connections are OK. The IP address eth0:0 is what is listening to the IP address. Shouldn't it be from that? Also when I tried using the eth0:0 I recieved an error indicating that 'aliases' could not be used so I have to specify -d versus the -i (eth0:0). then how would this work. I'm trying to interpret the command... Will this substitute the IP address of 172.x.x.2 for the IP or will it use the IP address assigned to 172.x.x.1 (eth0).

The last time I attempted to load this I could no longer ssh into my router once the rules were applied

then add a rule to permit specific incoming traffic from your box to tcp port 22. and out again. (OUTPUT).

These worked previously (with the new IP ommitted)... Will give it another shot.

(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?

n.b. you should realise (if you didn't already know). that the iptables -F command only clears your rules (and only rules in the 'filter' table for that matter). It will not put the chain policies back to ACCEPT.

Yes I flushed the rules before calling the script..

incidentally, are you applying these rules every boot using this shell script? Or is it only for testing purposes?
if your set them this way at boot, when/how is the script run?

I originally wrote the script to build my initial rules and use it when I want to implement changes... I flush the tables, execute the firewall script then save the rules.

Re: Help with Iptables on with RH linux

Regards

Stuart

--

Stuart Sears RHCA RHCX

To err is human, to forgive is Not Company Policy.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.4 (GNU/Linux)

Comment: Using GnuPG with Fedora - <http://enigmail.mozdev.org>

iD8DBQFEwPDvamPtx1brPQ4RAqiTAJ9KZBrPbHg2MnbljT6NlvGpaMiTGQCdHJVt
yrdFhT7KpZvliRSAdhDFey8=

=Pk+y

-----END PGP SIGNATURE-----

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>

<https://www.redhat.com/mailman/listinfo/redhat-list>