

# Re: Help with Iptables on with RH linux

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-07/msg00229.html>

---

- *From:* Stuart Sears <[stuart@xxxxxxxxxxxx](mailto:stuart@xxxxxxxxxxxx)>
  - *Date:* Sat, 22 Jul 2006 11:03:35 +0100
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

James Marcinek wrote:

[other stuff snipped]

/me wrote this:

iptables -A FORWARD -i eth0 -d 192.168.0.2 -j ACCEPT does it suddenly start working?

James wrote this:

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).

okay, let's see if I can make this clearer. Apologies if I am telling you stuff you already know.

The -i and -d switches refer to physical NICs. Not IP addresses. eth0:0 is merely a way of adding a second IP to the same physical interface and being able to bring that 2nd IP up/down at will. So packets hitting the virtual IP on eth0:0 really pass through the physical interface eth0, which is what netfilter will see. You can see a similar view of this using 'ip addr show'. which will have no reference to eth0:X at all. Just 2 IPs on eth0.

- -i and -d are used for `_directional_` filtering/natting.

If you are dropping packets in the FORWARD chain, there are two rules needed to ensure that permitted traffic flows through your firewall:

Re: Help with Iptables on with RH linux

1. The DNAT rule in PREROUTING.

without this in place the packets you wish to redirect to 192.168.0.2 will *\*never\** end up in the FORWARD chain.

2. A rule in FORWARD that allows specific traffic through your system if it is destined for 192.168.0.2.

\* The eth0 bit was just to ensure that the rule I wrote only applies to packets flowing from out to in. -o eth1 would also do this. In fact you can use both.

\* You can adjust these rules to allow only certain protocols and ports. I would. In fact, I would do this in the NAT rule as well.

does this make more sense?

#### contrived example #####

assume I am running a webserver on 192.168.0.2:80  
one of my external IPs (on eth0:X) is 172.16.32.64  
so:

1) redirect *\*only\** http traffic aimed at eth0:X to 192.168.0.2:

```
iptables -t nat -A PREROUTING -d 172.16.32.64  
-p tcp --dport 80 -i eth0 -j DNAT --to-dest 192.168.0.2
```

2) permit http traffic to 192.168.0.2 to pass through from out to in:

```
iptables -A FORWARD -i eth0 -d 192.168.0.2 -p tcp --dport 80 -j ACCEPT
```

#####

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.

good. Just checking. I come across *\*far\** too many people who set their rules using a shell script called from rc.local, *\*after\** their network has already come up. doh.

Regards

Stuart

ps would you mind setting your MUA (thundervird, I believe) to wrap lines at a fixed length? your diagram in the original mail was way over to the right and the long lines are sometimes very hard to read...  
thx. :)

Re: Help with Iptables on with RH linux

-- --

Stuart Sears RHCA RHCX

Quit worrying about your health. It'll go away.

-- Robert Orben

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

Version: GnuPG v1.4.4 (GNU/Linux)

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

iD8DBQFEwff3amPtx1brPQ4RAgwVAJwMuHFEaO/gdeSXiKP9AhF1JO+bwgCfVeYC  
ulNJCCE2RETwUes4c/aHV4c=  
=NEYW

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

--

This message has been scanned for viruses and  
dangerous content by MailScanner, and is  
believed to be clean.

--

redhat-list mailing list

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

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