

# FW: DNAT SSH

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/RedHat/2008-01/msg00285.html>

---

- *From:* "Geoffrey Rainey" <[Geoffrey.Rainey@xxxxxxxxxxx](mailto:Geoffrey.Rainey@xxxxxxxxxxx)>
  - *Date:* Thu, 31 Jan 2008 14:18:19 +1300
- 

Hi,

Perhaps there is someone in the ether au fait with IPtables...?

Cheers,  
Geoff.

---

From: Geoffrey Rainey  
Sent: Thursday, 31 January 2008 1:13 p.m.  
To: 'netfilter@xxxxxxxxxxxxxxxxxxx'  
Subject: DNAT SSH

Hello,

I would like to obscure the SSHD listening port from 22 to another, but allow 22 access from the local subnet.

Described succinctly, this is what I think I need:

NAT PREROUTING chain:

1. `-s anywhere --dport 5000 -j DNAT --to-destination :22`

FILTER INPUT chain:

2. `-s subnet --dport 22 -j ACCEPT`

3. `all others -j REJECT`

The problem is the packet arrives on 5000 and is natted to 22 correctly (1. - all good so far), but because its source IP is not the local subnet (defined in 2.), it is rejected in the filter INPUT chain (3).

So I'm think something like the following:

- a. can the packet bypass the INPUT filter chain?
- b. how can I identify my natted packet within the INPUT filter chain and thus ACCEPT it?

Regards,  
Geoffrey Rainey.

=====  
For more information on the Television New Zealand Group, visit us  
online at [tvnz.co.nz](http://tvnz.co.nz)  
=====

CAUTION: This e-mail and any attachment(s) contain information that  
is intended to be read only by the named recipient(s). This information  
is not to be used or stored by any other person and/or organisation.

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