

RE: FW: DNAT SSH

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2008-01/msg00288.html>

- *From:* "Geoffrey Rainey" <Geoffrey.Rainey@xxxxxxxxxxx>
 - *Date:* Thu, 31 Jan 2008 21:11:31 +1300
-

I think this won't work because I am wanting to allow the world to talk to 5000 then NAT to 22, while also disallowing the world to talk to 22 – only the local subnet can talk to 22.

So I want:

```
subnet only -> :22
world (REJECT) -> :22
world -> :5000
world:5000 -> (NAT) subnet:22
```

make sense?

Regards,
Geoff.

-----Original Message-----

From: redhat-list-bounces@xxxxxxxxxxx on behalf of Nilesh Vaghela
Sent: Thu 1/31/2008 8:38 PM
To: General Red Hat Linux discussion list
Subject: Re: FW: DNAT SSH

I think the following can work.

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

```
-s subnet --dport 5000 -j DNAT --to-destination 22
```

This will do NATing only on the subnet.

Thanx.

```
FILTER INPUT chain:
```

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

RE: FW: DNAT SSH

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,
Geofrey Rainey.

=====
For more information on the Television New Zealand Group, visit us
online at 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>

--
Nilesh Vaghela
ElectroMech
Redhat Channel Partner and Training Partner
74, Nalanda Complex, Satellite Rd, Ahmedabad
25, The Emperor, Fatehgunj, Baroda.
www.electromech.info

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

=====
For more information on the Television New Zealand Group, visit us
online at tvnz.co.nz
=====

CAUTION: This e-mail and any attachment(s) contain information that

RE: FW: DNAT SSH

RE: FW: DNAT SSH

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>