

Re: RH9, NAT and routing

Source: <http://linux.derkeiler.com/Mailing-Lists/RedHat/2004-06/0197.html>

From: Pete Nesbitt (pete_at_linux1.ca)

Date: 06/08/04

To: General Red Hat Linux discussion list <redhat-list@redhat.com>

Date: Mon, 7 Jun 2004 18:12:10 -0700

On June 7, 2004 02:26 pm, Bob Smith wrote:

> *I'm trying to set up my local network so that my RH9 box acts as a router
> between my LAN and the Internet via a DSL connection. The DSL connection
> is solid and working, and I have no problems accessing the Web. I think
> that I set the operation up correctly, but it's not working, hence my yelp
> for help...*

>

> *The DSL modem is accessed via eth0, the LAN via eth1. Traffic on either
> side works well, and I have DNS working such that I can access DNS values
> for sites not in my local DNS configuration throughout my LAN. The
> exterior network values are correct for the DSL connection and the
> network connection values for the ISP.*

>

> *I used the RHCE study manual as a guide, and did the following:*

>

> *In IP tables, created a forwarding rule, as it appears in this excerpt
> from the file:*

>

> **nat*

> *-A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE*

>

> *In /etc/sysctl.conf, I turned on forwarding:*

> *net.ipv4.ip_forward = 1*

>

> *After reboot, the /proc/sys/net/ipv4/ip_forward file has a value of 1.*

>

> *I set up ftp as recommended in the manual:*

>

> */sbin/modprobe -a ip_conntrack_ftp ip_nat_ftp*

>

> *At this point, I can get any DNS query vi nslookup that I want, and get a
> return value. However, I cannot FTP out, I can't get out via web browser,
> and ping returns "Request timed out." Traffic within the LAN is fine, and
> traffic up to the Internet is fine.*

>

> *So, I'm thinking that I need some kind of either forwarding or routing
> rule to be configured for one of the ethernet card interfaces to allow*

RedHat: Re: RH9, NAT and routing

> forwarding. I checked with Evi's Linux Sys Admin book, and I think the
> routing rules are correct, but I'm not sure.
>
> Any help would be appreciated.
>
> Thanks,
>
> -Bob

Hi,

I have a similar fw (but 3 nics).

here is the basic sequence of the pertinent rules from my fw to let LAN traffic out. Depending on your comfort level, using firestarter may be preferred. These are only a few of a complete set.

```
# Default deny all inbound & forwards.
# probably just allow all out, your discretion, but if you deny all outbound
# you won't contribute to DDOS, just make last one DENY as well then
# allow the desired services out.
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD DROP
$IPTABLES -P OUTPUT ACCEPT

# outbound LAN connections are all masquaraded
$IPTABLES -A POSTROUTING -t nat -o $EXT_IF -s $LAN_RANGE -j MASQUERADE

# allow existing communications to continue
$IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# forward
$IPTABLES -A FORWARD -i $LAN_IF -s $LAN_RANGE -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# I end each section (input, forward, output) with log and drop, here the
# forward set
$IPTABLES -A FORWARD -m limit -j LOG --log-prefix "NetF FORWARD CHAIN: "
$IPTABLES -A FORWARD -j DROP
```

Of course, there should be other rules in place, but this should allow successful outbound connections from your LAN.

Hope that helps.

```
--
Pete Nesbitt, rhce
--
redhat-list mailing list
unsubscribe mailto:redhat-list-request@redhat.com?subject=unsubscribe
https://www.redhat.com/mailman/listinfo/redhat-list
```