REVSYS | revolution systems

▼ MENU ▼

Quick-Tip: Linux NAT in Four Steps using iptables

— *By Frank Wiles*

In everyone's life a little rain must fall. My main Linux workstation at home suffered a hard drive failure the day after Christmas. I can only guess I was bad last year and Santa turned my hard drive into a lump of coal as punishment.

Unfortunately, at some point over the year I introduced a typo in a script I used to backup my personal website and some other data on that particular computer. Along with some data that wasn't very important, I lost my handy little script I used to setup iptables to NAT my internal network to the Internet at large.

After an hour of not being able to find a quick and easy tutorial on how to do this seemingly basic task on Google, I promised myself I would write this Quick-Tip.

If you are running a recent 2.6 Linux Kernel this four step process should work for you. This has been specifically tested on Fedora Core 3, 4, 5, and 6, but should work on any modern Linux distribution. All of these commands must be executed as the root user. First you need to tell your kernel that you want to allow IP forwarding.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Then you'll need to configure iptables to forward the packets from your internal network, on /dev/eth1, to your external network on /dev/eth0. You do this will the following commands:

```
# /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# /sbin/iptables -A FORWARD -i eth0 -o eth1 -m state
    --state RELATED,ESTABLISHED -j ACCEPT
# /sbin/iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

You should now be NATing. You can test this by pinging an external address from one of your internal hosts. The last step is to ensure that this setup survives over a reboot. Obviously you should only do these last two steps if your test is a success.

You will need to edit `/etc/sysctl.conf` and change the line that says `net.ipv4.ip_forward = 0` to `net.ipv4.ip_forward = 1`. Notice how this is similar to step number one? This essentially tells your kernel to do step one on boot.

Ok last step for Fedora/RHEL users. In order for your system to save the iptables rules we setup in step two you have to configure iptables correctly. You will need to edit `/etc/sysconfig/iptables-config` and make sure `IPTABLES_MODULES_UNLOAD` , `IPTABLES_SAVE_ON_STOP` , and `IPTABLES_SAVE_ON_RESTART` are all set to 'yes'.

For non-Fedora/RHEL users you can simply setup an init script for this or simply append these commands to the existing rc.local script so they are executed on boot. Or if you want to get even more fancy, you can use the commands iptables-save and iptables-restore to save/restore the current state of your iptables rules.

After all that is done, you should probably do a test reboot to ensure that you've done everything correctly. If you find any errors on this page or this does not work for you please feel free to E-mail me directly at frank@revsys.com(mailto:frank@revsys.com).

Common Problems

The most common problem or question I receive about this is related to DNS. The instructions above setup the network to route the packets for you, but if your DNS isn't setup correctly (or at all) you won't be able to reference sites by their domain or hostnames. If at first you think this isn't working for you, please try to ping an external IP address. If you can do this, then your problem is with DNS and not iptables.

Additional Information

A nice article on setting up NAT in both directions NAT with IPTables(http://debianclusters.org/index.php /NAT_with_IPTables). For example if you need to route traffic from your NAT/firewall's port 80 to an internal webserver.

Related Books

- Linux iptables Pocket Reference(http://www.amazon.com/gp/product/0596005695/ref=as_li_ss_tl?ie=UTF8&tag=linux-nat-20& linkCode=as2&camp=217145&creative=399349&creativeASIN=0596005695)
- Linux Networking Cookbook(http://www.amazon.com/gp/product/0596102488/ref=as_li_ss_tl?ie=UTF8&tag=linux-nat-20&linkCode=as2& camp=217145&creative=399349&creativeASIN=0596102488)
- Linux Network Administrator's Guide(http://www.amazon.com/gp/product/0596005482/ref=as_li_ss_tl?ie=UTF8&tag=linux-nat-20& linkCode=as2&camp=217145&creative=399349&creativeASIN=0596005482)

RECENT TWEETS

RT @webology: Nice @djangobirthday 🎍 write-up by @gmcconnaughey http://t.co/l3TILRzmXY

– *Wednesday Aug 12th 2015 at 7:11 p.m.*

Emoji Mosaic for fun! http://t.co/MLliKQGKEI

– *Tuesday Aug 11th 2015 at 9:03 p.m.*

We're working on a cool dev/debugg tool for local logs. @devspectrum Want to be a beta tester? Signup up! http://t.co/XC3JcPAiVb

– *Monday Aug 10th 2015 at 7 p.m.*

TALKS »

All of our recent technical talks are also online. Watch them here »

RECENT BLOG ENTRIES »

- Django Birthday: Recap
- Django Birthday Party
- Improved Django Tests

TECHNICAL ARTICLES »

- Recommended Django Project Layout
- Ultimate Front End Development Setup
- PostgreSQL Performance Tuning
- Centralized Logging with Syslog

FEATURED PRODUCT

HOME

SERVICES

Django

PostgreSQL

Infrastructure / Ops

Open Source Software Support

Software Development

Systems Administration

PRODUCTS

Grove

Open-Source Projects

WRITING

Technical Articles

Talks

Quick Tips

12 Days of Performance Series

Blog

Featured Posts

ABOUT

Team Members

Featured Clients

Testimonials

Press

Contact

Have a comment or suggestion? Please send it to us! Follow us on Twitter or signup for our newsletter for tips and tricks.