Setting Up Gateway Using iptables and route on Linux

By Eric Zhiqiang Ma on July 13th, 2013

Sharing the networking is important. Setting up a gateway is a good solution to it. Building up the gateway on a Linux box is easy and cost efficient, but reliable. With a Linux box, you can share the internet connection or the only cable connected to the network.

The Linux box

The Linux box that we use has this configuration:

OS: Fedora 12

NIC1: *eth0* with ip 192.168.0.1 connected to our small local area network.

NIC2: *eth1* with ip 143.89.111.111 connected to the internet.

Now we want to share this Linux box's connection with the other computers in the local area network with ip in 192.168.0.0/16.

Setting up the gateway

All the operations in this part is done under root on the Linux gateway.

Manipulate the IP route table

```
# ip route add 192.168.0.0/16 dev eth0
```

or

```
# route add -net 192.168.0.0/16 dev eth0
```

Enable Linux IP forwarding

```
# sysctl -w net.ipv4.ipforward=1
```

or

```
# echo 1 > /proc/sys/net/ipv4/ipforward
```

You can also make the setting permanent in "/etc/sysctl.conf` by adding a line below to */etc/sysctl.conf*:

```
net.ipv4.ip_forward = 1
```

Set up SNAT by *iptables*

Change the source IP of out packets to gateway's IP. Don't worry since iptables will automatically change the replied packet's destination IP to the original source IP.

```
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j SNAT --to-source
143.89.111.111
```

And then make sure that the other *iptables* tables do not deny these connections.

If you have problem in this step, you can try

```
# iptables -F
# iptables -t nat -F
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j SNAT --to-source
143.89.111.111
```

to allow all connections in. But there may be security problems after open all ports to the public. Firewall should be carefully configured.

By now, the we have set up the Linux gateway.

Client side configuration

On client such as Linux or Windows with IP 192.168.0.4, set the network connection to use this profile:

The configuration profile:

Gateway: *192.168.0.1.*

DNS Server: your ISP's DNS server IP addresses.

The method to configure the network maybe different from using NetworkManager and network and Windows.

You can try this command on Linux:

```
ip route add default via 192.168.0.1 dev eth0
```

or

```
# route add default gw 192.168.0.1 eth0
```

You can use this GUI/TUI tool on Fedora / RedHat / CentOS systems:

```
# system-config-network
```

or

```
# system-config-network-tui
```

About Eric Zhiqiang Ma

289 articles and counting.

Eric Zhiqiang Ma is interested in operating systems and distributed computing and processing systems. Find Eric on Facebook, Twitter, LinkedIn and Google+. The views or opinions expressed here are solely Eric's own and do not necessarily represent those of any third parties.

All posts by Eric Zhiqiang

4 comments:

Zhiqiang Ma says:
Sep 20, 2012 at 8:52 pm

Remember to enable forwarding in the FORWARD chain:

iptables -I FORWARD -j ACCEPT

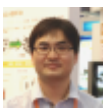
more strict rules are also suggested.

Zhiqiang Ma says:
Sep 20, 2012 at 8:53 pm

Another option for configuring iptables:

iptables -I FORWARD -j ACCEPT
iptables -t nat -I POSTROUTING –out-interface eth1 -j MASQUERADE

Pingback: Port Forwarding Using iptables - Linux Tutorials - Fclose



Zhiqiang Ma says:
Oct 4, 2013 at 1:43 pm

Instead of using SNAT, another way is to use MASQUERADE:

```
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j MASQUERADE
```

However, for static IPs, SNAT is suggested as from the iptables man page (http://www.pkill.info/linux/man/8-iptables/):

> This target is only valid in the nat table, in the POSTROUTING chain. It should only be used with dynamically assigned IP (dialup) connections: if you have a static IP address, you should use the SNAT target. Masquerading is equivalent to specifying a mapping to the IP address of the interface the packet is going out, but also has the effect that connections are forgotten when the interface goes down. This is the correct behavior when the next dialup is unlikely to have the same interface address (and hence any established connections are lost anyway).

Some other discussion on the Web:

http://lists.debian.org/debian-firewall/2002/02/msg00020.html

Comments are closed.