Source based routing / policy routing

02.05.24

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

Source based routing / policy routing

How to make persistent policy routing with iproute2

This is very simple but still every time I do this I need to look it up. Maybe getting old?

So this is a quick set of instructions to get you (and me) quickly through source based routing with Linux using sysv init files which should be pretty standard on any distro. I am doing this document as I am doing it for real so this will be tested to be working :)

I use example tables called “internal” and “public”. I've done internal / public sites before without policy routing but I think this may be the preferred way since you don't have to lower your security settings with this one.

Remove NetworkManager

NetworkManager is always full of surprises. Some day when you update your box remotely you may find yourself cut out from your server. And policy routing does not work when your interfaces are NetworkManager controlled.

Firstly make your interfaces free from NetworkManager by adding a line

```
NM_CONTROLLED=no
```

to your /etc/sysconfig/network-scripts/ifcfg-* files.

Then erase NetworkManager with command

```
yum erase NetworkManager
```

Create route tables in rt_tables

Edit /etc/iproute2/rt_tables and add the following (note example table names)

```
1       internal
2       public
```

Create routes

We use networks 1.2.3.0/24 and 172.16.10.0/24 with devices eth0 and eth1.

Set /etc/sysconfig/network-scripts/route-eth0 to

```
1.2.3.0/24 dev eth0 src 1.2.3.123 table public
default via 1.2.3.1 dev eth0 table public
```

Set /etc/sysconfig/network-scripts/route-eth1 to

```
172.16.10.0/24 dev eth1 src 172.16.10.123 table internal
default via 172.16.10.1 dev eth1 table internal
```

Create rules

Set /etc/sysconfig/network-scripts/rule-eth0 to

```
from 1.2.3.123 table public
```

Set /etc/sysconfig/network-scripts/rule-eth1 to

```
from 172.16.10.123 table internal
```

Test

You can reboot or try ifdown + ifup ethN but better be sure you have console access locally or via virtual console.

```
ip rule show
ip route show table internal
ip route show table public
```

Also don't forget to update your iptables and other stuff.