POLICY ROUTING - IPTABLES

Policy routing is one of those cool tricks system administrators can do with network traffic. What it means is that we can send all of a certain type of traffic out of a certain line we choose. For example, if you have leased line for mail and other traffic requiring that type of connection, but you want to move all web traffic to a less expensive setup, like a broadband connection. You would have to use policy routing, because you are wanting to route based on traffic type not traffic destination. Now you can do this using the *iproute2* utility in linux, but now we can do it through iptables.

Iptables Routing

First off, you will need an iptables firewall, in fact you will need one where you can add the *patch-o-matic* modules (see here), and then add the *ROUTE* target. Once you have the *ROUTE* target working you can use this to do policy routing, I think this is very nice because all your setup sits in your firewall configuration script, plus you can use all the other firewall settings to add more granular control to your policy routing setup. Here is an example of routing out web traffic over a modem..

```
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter

LANIP=<your internal network addresses>
LAN=<your internal network interface>
SRCPPP=`ifconfig ppp0 | grep inet | gawk '{ print $2 }' | cut -f 2 -d ":"`
GWPPP=`ifconfig ppp0 | grep inet | gawk '{ print $3 }' | cut -f 2 -d ":"`

for x in 80 443
 do
  $IPT -t nat -A PREROUTING -s $LANIP -i $LAN -p tcp -m tcp --dport $x -j ACCEPT
  $IPT -A FORWARD -s $LANIP -i $LAN -p tcp -m tcp --dport $x -j ACCEPT
  $IPT -t nat -A POSTROUTING -s $LANIP -p tcp --dport $x -j SNAT --to-source $SRCPPP
  $IPT -t mangle -A POSTROUTING -p tcp --dport $x -j ROUTE --gw $GWPPP --continue
 done
```

Simple. Two important gotchas to remember

1. Always make sure the *rp_filter* is set to *0*
2. Always make sure you use the --*continue* option in your *mangle* rule

Final Words

That is fairly short and sweet is it not. But do not underestimate how much this little trick can help you. Policy routing is a very handy for traffic segregation and very useful for dynamically growing bandwidth as needed. As always, learn and have fun.