Q: How do I set up active mode with a Linux based firewall/router?

A:

How do I set up active mode with a Linux based firewall/router?

It depends on what kernel version you are using. With 2.4 you can choose between doing postrouting or the easier prerouting. The difference is if you do a postrouting, all clients withing your internal network (LAN) can connect and download/upload between eachother. Postrouting is not nessesary if you are the only client wich uses DC behind the router/firewall. Examples below uses the following settings: External ethernet card: eth1, external IP 213.112.8.55, firewall (router) IP: 192.168.0.1, client IP: 192.168.0.2, external and internal port: 555

Linux 2.4, postrouting example

```
iptables -t nat -A POSTROUTING -d 192.168.0.2 -s 192.168.0.0/24 -p tcp --dport 555 -j SNAT --to
192.168.10.1

iptables -t nat -A POSTROUTING -d 192.168.0.2 -s 192.168.0.0/24 -p udp --dport 555 -j SNAT --to
192.168.10.1

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 555 -j DNAT --to 192.168.10.2:555

iptables -t nat -A PREROUTING -i eth1 -p udp --dport 555 -j DNAT --to 192.168.10.2:555

iptables -t nat -A PREROUTING -d 213.112.8.55 -p tcp --dport 555 -j DNAT --to 192.168.10.2:555

iptables -t nat -A PREROUTING -d 213.112.8.55 -p udp --dport 555 -j DNAT --to 192.168.10.2:555
```

Linux 2.4, prerouting example

```
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 555 -j DNAT --to 192.168.0.2:555

iptables -t nat -A PREROUTING -i eth1 -p udp --dport 555 -j DNAT --to 192.168.0.2:555
```

Linux 2.2, example

```
ipmasqadm portfw -a -P tcp -L 213.112.8.55 555 -R 192.168.0.2 555

ipmasqadm portfw -a -P udp -L 213.112.8.55 555 -R 192.168.0.2 555
```

*Submitted by **tajisen***

How to use Shorewall to configure your iptables

Here's what you have to add to rules (assuming loc is the zone where your computer is located, 192.168.0.7 is your computer's IP, 666 is the port you wish to use and 123.45.67.89 is your external IP):

#ACTION	SOURCE	DEST	PROTO	DEST PORT	SOURCE PORT(S)	ORIGINAL DEST
DNAT	net	loc:192.168.0.7	tcp	666	-	123.45.67.89
DNAT	net	loc:192.168.0.7	udp	666	-	123.45.67.89