

IPTables with Virtual Interfaces and Multiple Public IPs

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2007-08/msg00089.html>

- *From:* martin.fowler@xxxxxxxxxx
 - *Date:* Mon, 06 Aug 2007 16:04:40 -0000
-

Hello everyone, I am not new to linux, but I am by no stretch an expert. I have looked at all the other forums for my solution but I cant seem to get it to work. Here is my situation.

Multiple Public IP addresses feed into a single ubuntu 7.04 server linux box runing an iptables firewall. The server has 2 nics, 1 external 207.xxx.xxx.xxx and the other nic is for the internal network 192.168.yyy.yyy with multiple servers that need all the same ports. For instance, there is a windows media server (among the ports is 80), a server for web hosting (again port 80), and a development web server (another on port 80) so you can see the need for the multiple public ips. I want 207.xxx.xxx.42 to point to one, .43 to point to another, and .44 to point to the last.

```
..42 -----| |-----| | server 1 .50
..43 -----|-----| gateway |-----| server 2 .51
..44 -----| |-----| | server 3 .52
```

The external interface on the gateway is set up for eth0, and I have setup virtual interfaces to handle the different ip addresses

```
auto lo
iface lo inet loopback
```

```
auto eth0
iface eth0 inet static
address 207.xxx.xxx.42
netmask 255.255.nnn.nnn
gateway 207.xxx.xxx.41
```

```
auto eth0:0
iface eth0:0 inet static
address 207.xxx.xxx.43
netmask 255.255.nnn.nnn
```

```
auto eth0:1
iface eth0:1 inet static
address 207.xxx.xxx.44
```

IPTables with Virtual Interfaces and Multiple Public IPs

```
netmask 255.255.nnn.nnn
```

```
auto eth1
iface eth1 inet static
address 192.168.yyy.yyy
netmask 255.255.255.0
```

The virtual interfaces work, i can connect to the ip address, ping them, and so forth.

But when I try to access port 80, only the .42 address works correctly. Here is how I have iptables set up.

```
#!/bin/sh

EXTIF1="eth0"
INTIF="eth1"
INTR="192.168.yyy.yyy/24"
IPT="/sbin/iptables"

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

modprobe ip_conntrack
#modprobe ip_conntrack_pptp
#modprobe ip_nat_pptp

# Clear the iptables configuration
$IPT -F FORWARD DROP
$IPT -F INPUT DROP
$IPT --flush
$IPT -t nat --flush
$IPT -X
$IPT -t nat -X

# Setup the default IPTABLES config for internet access
$IPT -t nat -A POSTROUTING -s $INTR -j MASQUERADE
$IPT -A FORWARD -s $INTR -o $EXTIF1 -j ACCEPT
$IPT -A FORWARD -d $INTR -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# PORT FORWARDING

#### MEDIA ####
EXTIP1="207.xxx.xxx.42"
MEDIA="554,1755,80,3389,8080"
MEDIAUDP="5004,5005,1755,1024:5000"
$IPT -t nat -A PREROUTING -p tcp -m multiport -i $EXTIF1 -d 207.xxx.xxx.42 --dport $MEDIA -j DNAT --to 192.168.yyy.50
$IPT -t nat -A POSTROUTING -p tcp -m multiport --sport $MEDIA -o $EXTIF1 -s 192.168.yyy.50 -j SNAT --to-source 207.xxx.xxx.42
```

IPTables with Virtual Interfaces and Multiple Public IPs

```
$IPT -A FORWARD -p tcp -m multiport -d 192.168.yyy.50 -o $INTIF --  
dport $MEDIA -j ACCEPT
```

..... same lines only for udp instead of tcp. Then I have a definition for all the other hosts with their respective ip addresses for external and internal. Then at the end of the script I have

```
# Enable Traffic Logging on everything except ssh or web  
IGNORE="22,80"  
$IPT -A INPUT -p TCP -m multiport --dport ! $IGNORE -j LOG --log-  
prefix "[IN][dst]: " --log-level 4  
$IPT -A INPUT -j ACCEPT  
  
$IPT -A OUTPUT -j ACCEPT  
  
$IPT -A FORWARD -p TCP -m multiport --dport ! $IGNORE -j LOG --log-  
prefix "[FORWARD][dst]: " --log-level 4  
$IPT -A FORWARD -j ACCEPT
```

so that is basically what I have. Yet only web on the .42 address works. When I hit .43 or .44 all I get is a page not found error. Can someone debug the script and tell me what I am doing wrong? Its basically cobbled together from other scripts that I have found on the internet. If you dont know whats wrong with my script, could you provide an example script of what should work with my configuration?

Thank you in advanced to all who reply

Regards
Martin Fowler

.