Subject: Routing problem
Posted by pennywize on Fri, 19 Jan 2007 21:35:50 GMT

Hello all,

I have a massive routing problem. My system is running with Debian Etch. VZCTL Version: 3.0.11
It is running on a root server with 1 static IP. A VM is able to ping its host (via public IP) but unable
to go to internet.
My iptables seems to be incomplete or I did something wrong else. Am in hope one of you is able
to enlight me regarding this.

Here are my configy

HOSTSYSTEM

/etc/network/interfaces
iface lo inet loopback
auto lo

auto eth0
iface eth0 inet static
        address 85.xx.yy.112
        netmask 255.255.255.0
        broadcast 85.xx.yy.255
        network 85.xx.xx.0
        gateway 85.xx.xx.254

        up sysctl -w net.ipv4.conf.eth0.proxy_arp=1
        pre-down sysctl -w net.ipv4.conf.eth0.proxy_arp=0

VM have following config:

/etc/network/interfaces

auto venet0 lo
iface venet0 inet static
        address 127.0.0.1
        netmask 255.255.255.255
        broadcast 0.0.0.0
        up route add -net 191.255.255.1 netmask 255.255.255.255 dev venet0
        up route add default gw 191.255.255.1
iface lo inet loopback

auto venet0:0
iface venet0:0 inet static
        address 192.168.0.196
        netmask 255.255.255.255

broadcast 0.0.0.0

/etc/resolv.conf

nameserver 127.0.0.1
nameserver 85.xx.yy.112

It is possible to ping external IP from inside VM

ping 85.xx.yy.112
PING 85.xx.yy.112 (85.xx.yy.112) 56(84) bytes of data.
64 bytes from 85.xx.yy.112: icmp_seq=1 ttl=64 time=0.159 ms
64 bytes from 85.xx.yy.112: icmp_seq=2 ttl=64 time=0.092 ms
64 bytes from 85.xx.yy.112: icmp_seq=3 ttl=64 time=0.094 ms

I have choosen an http source for apt

My iptables rules look like this

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A FORWARDING -p tcp -d 85.xx.yy.112 --dport 53 -j DNAT --to-destination
192.168.0.196
iptables -t nat -A PREROUTING -i eth0 -p udp -d 85.xx.yy.112 --dport 53 -j DNAT --to-destination
192.168.0.196

iptables -t nat -A PREROUTING -p tcp -d 85.xx.yy.112 --dport 80 -j DNAT --to-destination
192.168.0.196
iptables -t nat -A PREROUTING -i eth0 -p tcp -d  85.xx.yy.112 --dport 80 -j DNAT --to-destination
192.168.0.196
```

And of course not to mention this, its hosts is able to ping that VM as well:

ping 192.168.0.196
PING 192.168.0.196 (192.168.0.196) 56(84) bytes of data.
64 bytes from 192.168.0.196: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 192.168.0.196: icmp_seq=2 ttl=64 time=0.093 ms

Guess the mistake could be either in /etc/resolv.conf (VM) or to find iptables rules.

I really hope you can tell me where the mistake is.

Kind regards
Pennywize