

Re: Problem with IP Masquerade + routed internal network (pretty newbie question)

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2003-07/0971.html>

From: David Efflandt (efflandt_at_xnet.com)

Date: 07/15/03

Date: Tue, 15 Jul 2003 01:32:01 +0000 (UTC)

On Mon, 14 Jul 2003 17:11:23 +0200, Dragan <gekko@eunet.yu> wrote:

> I have a class C internal network divided into 3 sections (one central
> office and two branches) connected by 2 routers (DSL router). Routers are
> communicating through RIP2 protocol. Machines are Win98 and WinXP, servers
> are Linux servers (Samba and SQL used), Windows addresses are leased through
> DHCP. The network looks like this:
>
> 192.168.1.0/24 network (around 10 computers) – 192.168.1.1 server,
> 192.168.2.1 router
> /
> 192.168.1.2
> 192.168.0.3
> /
> 192.168.0/24 network (50 computers) – 192.168.0.1 server, 192.168.0.3 and
> 192.168.0.2 routers
> /
> 192.168.0.2
> 192.168.2.1
> /
> 192.168.2.0/24 network (20 computers) 192.168.2.3 server, 192.168.2.1 router
>
> It works fine, but now we want to connect central office (192.168.0.0/24) to
> the internet. We have one public IP address and we would like to use IP
> Masquerade. I have set up a Red Hat 9 Linux as a NAT server with address
> 192.168.0.10, IP Masquerade works fine, but now there is a problem with
> internal routed network. I had to set up 192.168.0.10 server as a default
> gateway but that breaks connection with other two subnetworks. If I define
> static routes to two subnetworks on each of the Windows machines then it
> works fine, but I can't set up static routing through DHCP, and I know of no
> other way to define routes other than typing route add... in command prompt.
> If static routes are not defined then everything that goes out of
> 192.168.0.0/24 network goes to 192.168.0.10 NAT server, where it gets lost.
> If it were only one internal network then it wouldn't be a problem but this
> way I don't know how to solve the problem. Tnx in advance.

If you have a proper router set up, each box on each subnet should only

comp.os.linux.networking: Re: Problem with IP Masquerade + routed internal network (pretty newbie question)

need a local network route (for its directly connected LAN) and default route to the local router. Then the local router should be properly configured to route anything else to the other subnets or default to internet gateway.

I do not know if you have a central router to coordinate things, or if you really do have one network chained to another network chained to another network, and a router in the middle gets confused which way it should send specific traffic. Perhaps you need a more sophisticated routing protocol than RIP, or failing that, maybe proper static routes on the routers would help.

A couple of examples: the Cisco in our office used to be the default route for our office subnet (and local dialin PPP proxy arp to our LAN), which would route everything to our factory WAN over frame relay. A Cisco router there would decide whether to route the traffic locally, to another office subnet, or to our RedHat masq box to the internet. I think the Cisco routers were using EGP routing protocol.

Now that changed and we use a SonicWall on sdsl, which is the default route for our office subnet, and the SonicWall decides what should go through VPN to our factory WAN, or what should NAT directly to the internet. Our local Cisco is now configured with a static default route to the SonicWall. So a dialin PPP has a default route to the Cisco it connects to, the Cisco has a default route to the SonicWall, and the SonicWall decides between factory VPN, or NAT to internet. And it is all done with just local LAN route and default route on local PCs, and static routes on our Cisco or SonicWall.

But our traffic is primarily between our remote offices/foreign factories, and our main factory. The remote offices do not really communicate directly between each other (just to our main factory mail/document retrieval, and HP3000 computer for order entry/inventory). So a star topography is all we really need for our factory WAN.

--

David Efflandt - All spam ignored <http://www.de-srv.com/>
<http://www.autox.chicago.il.us/> <http://www.berniesfloral.net/>
<http://cgi-help.virtualave.net/> <http://hammer.prohosting.com/~cgi-wiz/>