

Re: Windows client – internet connection sharing

Source: <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2003-12/1541.html>

From: Matthew Seaman (*m.seaman_at_infracaninophile.co.uk*)

Date: 12/16/03

Date: Tue, 16 Dec 2003 15:18:08 +0000
To: Gareth Bailey <blygar1@webmail.co.za>

On Mon, Dec 15, 2003 at 07:40:14PM +0200, Gareth Bailey wrote:

> *Is it possible to set up a freebsd server connected to an*
> *ADSL line to provide internet access via LAN to a number of*
> *Windows clients. I don't know where to start. Any*
> *information in this regard will be greatly appreciated.*

Yes, absolutely. However, there are such a huge number of variations on possible ways of doing that that it's impossible to describe everything you'd need to know in a simple e-mail.

Lets look at a few questions you'd need to answer:

1) ADSL router or modem?

This is all about how you interface your FreeBSD system to ADSL — the basic choice is between a router: a standalone unit which you plug the phone line into one side of, and an ethernet cable into the other — or a modem: this is a device that plugs into a serial or USB port on your FreeBSD box.

Routers will work entirely independently of your FreeBSD machine. Since your connection to them is via ethernet, there's practically no compatibility problems. Depending on how much money you spend, you can get routers which provide packet filtering, network and port address translation, DNS, DHCP and various other capabilities — although if you go to the expense of buying a really capable router there's not much left to do for your FreeBSD box.

Modems are the other end of this scale: you need to find a device for which appropriate drivers are available under FreeBSD. Once you've got the modem connected up, you'll need to use the attached FreeBSD box to provide appropriate functionality to make a practicable ADSL connection. This includes running PPPoA or PPPoE (A = ATM, E = Ethernet: all ADSL in the UK is PPPoA, other countries do things differently) to establish networking into your service provider. You would use the standard FreeBSD stuff to do

NAT and firewall packet filtering, and you can install DHCP servers and so forth. Effectively the FreeBSD box + modem takes the place of the standalone router above.

2) What sort of address space do you want to have assigned to you from your ISP? The cheapest ADSL accounts give you a single Internet-routable IP number, usually assigned via DHCP. There can be an implicit assumption that you've basically got just one machine you want to have net access, although this is becoming less common nowadays. Lots of ISPs will give you two addresses: this is intended to give you an address for the router box, plus an address for a real PC. Next step up is to get that one or two addresses permanently assigned to you. Beyond that, you can get a routed connection — you get a small net block permanently assigned to you, as well as the single IP used for the WAN side of your router. This enables you to set up a 'DMZ' network, and for instance have several servers visible on the Internet. Many ISPs will have local policies forbidding you from running servers of various sorts, mostly as a way of protecting the ISP from the awful consequences of allowing Windoze machines out on the open Internet in the hands of the clueless.

3) A consequential decision related to the above: do you want some or all of your Windows (or other) LAN machines to have Internet routable addresses or to run Internet visible services? There's several ways of doing this:

DMZ network — classic firewall design. Here the Internet accessible machines are kept on a separate small sub-net, and you have a second packet-filtering router (generally a machine with a couple of network cards, running natd and ipfw or similar) between that and your private internal network.

Packet filtering bridge — similar to the above, except that the DMZ is and the internal private stuff are now technically on the same subnet, and your packet filter serves to separate public and private parts of the subnet. This is a much harder setup to get working effectively and securely than either of the other two, so use only as a last resort.

NAT address proxying — your NAT gateway has one or more IP addresses assigned and the NAT gateway knows how to forward incoming connections to an internal server. Or you run proxy servers on the Internet visible addresses which will accept incoming connections and relay them to the real servers on the internal network. Taken to the extreme, you could use this sort of setup to do load balancing and other fancy networking tricks, but you'd probably have to spend \$\$\$ to by the right sort of hardware load balancing kit needed.

4) From the point of view of the private side of your network, the FreeBSD box should minimally appear as the default gateway to the Internet. You can assign IP addresses and other configuration parameters to each machine manually or you can run various network servers to provide a level of autoconfiguration and subnet wide resources. Generally these do not need to be run on the gateway machine, and in many ways it's better to keep them on separate servers. However, not being made of money, that may not be entirely practical: if you're going to run DNS, DHCP, Samba, Kerberos, LDAP, Sendmail, Apache etc. on the gateway machine you will a) make the firewall rule set you need on that box significantly more complicated, b) have to take extra care when configuring those servers that you don't unintentionally expose them on the Internet side of the box and c) give potential attackers a lot more scope for finding an exploitable flaw. Most server software on Unix machines can be configured to bind to a subset of the available network interfaces.

Cheers,

Matthew

--

Dr Matthew J Seaman MA, D.Phil.

PGP: <http://www.infracaninophile.co.uk/pgpkey>

Tel: +44 1628 476614

26 The Paddocks

Savill Way

Marlow

Bucks., SL7 1TH UK

-
- application/pgp-signature attachment: [stored](#)