

Re: Internet sharing in Windows 2000

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2003-03/0622.html>

From: Karl Levinson [x y] mvp (levinson_k@despammed.com)

Date: 03/01/03

From: "Karl Levinson [x y] mvp" <levinson_k@despammed.com>

Date: Sat, 1 Mar 2003 16:42:48 -0500

"Q" <Q@nospam.net> wrote in message
news:O2muuYB4CHA.2416@TK2MSFTNGP11.phx.gbl...

- > *The NAT functionality of w2k server is more than adequate for small networks*
- > *in terms of functionality. However, NAT (or Internet Sharing) should be*
- > *treated as a "routing" function rather than a security one.*
- > *W2K has built in packet filtering at several layers (either via IPSEC*
- > *policies or via the RRAS administrative interface).*
- > *Correctly configured, the packet filtering should offer the necessary*
- > *security for a) the w2k NAT box and b) the network behind it. (although the*
- > *flexibility of the w2k pf is rather limited and there are no log*
- > *facilities). This "necessary security" refers to protecting the fw box and*
- > *the network behind it from direct external attacks. All other aspects of*
- > *your network security should be dealt with using third party applications:*
- > *IDS, AV, Distributed Firewalls, sound policies and user education, etc.*

I agree... If you use Windows 2000 in this manner, there's nothing protecting your gateway machine. Unless you configure Windows very carefully, a windows computer on the internet with no firewall is very easy to hack and will be hacked sooner or later.

Note that NAT makes it difficult for people to get into your network, but does nothing to stop outbound traffic, so that if someone got a worm or trojan on their computer, that computer could be remotely controlled completely using an "outbound" connection established by the internal computer, and that computer could be used to reach any other computer on the network.

Also note that if someone on the internet was able to use a simple hack to compromise your gateway computer, NAT wouldn't stop them from getting to your internal network. They could do anything remotely that you can do while logged into the gateway computer, and that includes sending and receiving data to and from your internal network, because NAT would not be used when your gateway computer talks to your internal network.

I would really suggest using a firewall in addition to or instead of your Windows gateway computer. There are even free firewalls out there, so price should not be a big issue:

<http://securityadmin.info/faq.htm#firewall>

You could just install a software firewall on your gateway computer to just protect that one computer. Or, you could set up a Linux firewall on a boot CD and an old 486 computer. Or, you could buy a www.netgear.com or www.linksys.com firewall or NAT router starting around \$70 US. If you had more money, the www.netscreen.com 5XP has a lot of professional features starting around \$500 US.

Windows is also not the fastest way to share an internet connection. Depending on the speed of the connection, you might or might not notice. AFAIK you can't use DHCP with Windows internet sharing feature, and I'm not sure if static IP addresses are supported either. I've used static IP addresses on a shared network of two computers, but if the internet sharing feature passes out IP addresses and it passes out an IP address that is already taken by a computer, I'm not sure you wouldn't have problems.

If you still use your Windows gateway computer, you'd want to harden that machine and maybe your other computers as below:

<http://securityadmin.info/faq.htm#harden>

IMHO IPsec filtering and native windows tools are not the best tools for protecting Windows, as they don't have any logging. If you were hacked, you'd have no idea who hacked you or when.

If you do want to use IPsec filtering, here are more articles on it:

<http://securityadmin.info/faq.htm#ipsec>

Outgoing mail is certified Virus Free.
Checked by AVG anti-virus system (<http://www.grisoft.com>).
Version: 6.0.449 / Virus Database: 251 - Release Date: 1/27/2003