

## Re: XP Home: selective folder sharing

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network\\_web/2005-01/2130.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2005-01/2130.html)

---

**From:** Chuck (*none\_at\_example.net*)

**Date:** 01/20/05

Date: Wed, 19 Jan 2005 17:14:10 -0800

On Wed, 19 Jan 2005 12:17:03 -0800, DaddySchlich  
<DaddySchlich@discussions.microsoft.com> wrote:

>Chuck,

>

>Thanks. You've given me a lot to think about, which is as it should be. As  
>I mentioned earlier, we were using the wireless connection on and off –  
>largely because of the potential problems caused. I'm comfortable with the  
>network doing dial-up; not so with wireless. And you're telling me I've got  
>that right.

>

>A few nuts-and-bolts questions that reflect my level of knowledge/ignorance:

>

>1. can you explain further what you mean by "bridge" and by "NAT" early on,  
>or give me a references? I basically have a cabled Ethernet LAN with a 100  
>Mbps switch at the center, with printers plugged into PCs. As I mentioned  
>earlier, ICS was not a whole lot of fun (or successful or simple) the last  
>time I tried, which is why we've been using three separate dial-up  
>connections.

>

>2. I understand the idea of putting firewalls on all three machines and  
>putting only these three PCs in the Local Zone, and using manually assigned  
>IP addresses to make sure those are the only three PCs included.

>

>Alternatively, where I started this exercise was restricting access to all  
>but selected files on the XP machine to others on the wired LAN, figuring the  
>same would hold for any wireless connection. Even better would be disabling  
>SFS for those few files to limit access to specific selected Users. With  
>user-level access possible on the Win98 machines, limiting access to files on  
>those machines to specific selected Users would appear to be easier.

>

>I am bit fuzzy about the reasons for having to have both firewalls and  
>separate logons. If the wall around the PC prevents any non-trusted source  
>from getting inside the PC, why is it necessary to ask for a passworded  
>login? Alternatively, if files are limited to selected Users, why the wall?  
>Similarly, if I have a wall on the XP machine, the only one with wireless  
>access, why do I need separate walls on the other PCs?

>  
>Similarly, I am a bit unclear about your suggestion that, if I am logged on  
>as an Administrator, someone from outside can breach the wall and step into  
>my shoes to wreak havoc as an Administrator on the PC. There must be  
>something here I'm not understanding.  
>  
>In short, I have been aware that I need to worry these issues. If you can  
>help me directly by answering or giving references to read, that would be  
>most helpful. At the end of the day, I may decide to bag the wireless access  
>altogether.  
>  
>If I ultimately do set something up, I would be happy to share with the  
>group.  
>  
>Thanks for your help, and your willingness to answer my questions.

Explaining bridges vs NAT is not easy. Here are a couple mentions about NAT, to start:

<http://compnetworking.about.com/b/a/071937.htm>  
[http://www.internet-sharing.com/nat\\_faqs/what\\_is\\_nat.html](http://www.internet-sharing.com/nat_faqs/what_is_nat.html)

A bridge simply connects two or more physically separate networks (such as the Wireless LAN of your neighbor and your Ethernet LAN). All components on each network are visible to all other components on each network.

With a bridge (if Falcon-II is providing one), the ip addresses of Falcon (192.168.0.179) and Micron (192.168.0.43) are visible to any computer connected to Falcon-II at the other end of the wireless link (ie to the owner of the WLAN). Thus, Falcon, Falcon-II, and Micron are all open to hacking and other abuse by the WLAN operator (and possibly the internet, if the WLAN isn't properly secured).

If you setup ICS properly, it operates as a NAT router, and only the upstream side of Falcon-II (probably 192.168.1.104) is visible to the bad guys (rest of the WLAN etc). Falcon and Micron are accessible only to ICS on Falcon-II.

I, and various other paranoiacs, recommend a layered (redundant component) security strategy. All individual security components are subject to abuse, and potentially, to breach. The recommendation is for multiple layers to protect you.

NAT is a good protective outer layer. There is no known vulnerability of NAT in general, though there have been reported weaknesses in specific NAT hardware that causes some concern. But NAT operates at the network layer.

<http://networking.ringofsaturn.com/Protocols/sevenlayer.php>

If you were to import hostile code (such as spyware, trojan, or virus), it would enter your network as data, and would not be filtered by a NAT router. Once inside your network, it could attack any unprotected computer.

For protection inside the NAT router (assuming that you have one), I recommend protection of a firewall on each computer, and use of non-administrative accounts except when intentionally installing software. A software firewall protects each computer individually, similarly to a NAT router protecting the LAN as a whole, from network level threats.

Unfortunately, a software based firewall can be bypassed too, by data level threats. If you import spyware onto your computer, and you are logged in as an administrator, it is that much easier for spyware to install, and operate, on your system. By logging in as a non-administrator, you make it a little harder for malicious software to attack your system, and maybe interfere with your software firewall.

Since the Administrator and Guest accounts have well known names, they are frequently used in a network based attack. Deleting the Guest account, and renaming the Administrator account, are recommended so a bad guy (maybe the owner of the WLAN) can't access your system thru brute force password guessing.

None of this is to say that you WILL be attacked if you don't use every one of these protective strategies. But, recognising that none of these strategies are 100% invulnerable, I generally recommend using as many as possible. And, if you intend to connect your network to another, unknown network, I absolutely recommend as many layers as possible.

--

Cheers,  
Chuck

Paranoia comes from experience - and is not necessarily a bad thing.