

## Installing SSH for managing FreeNAS

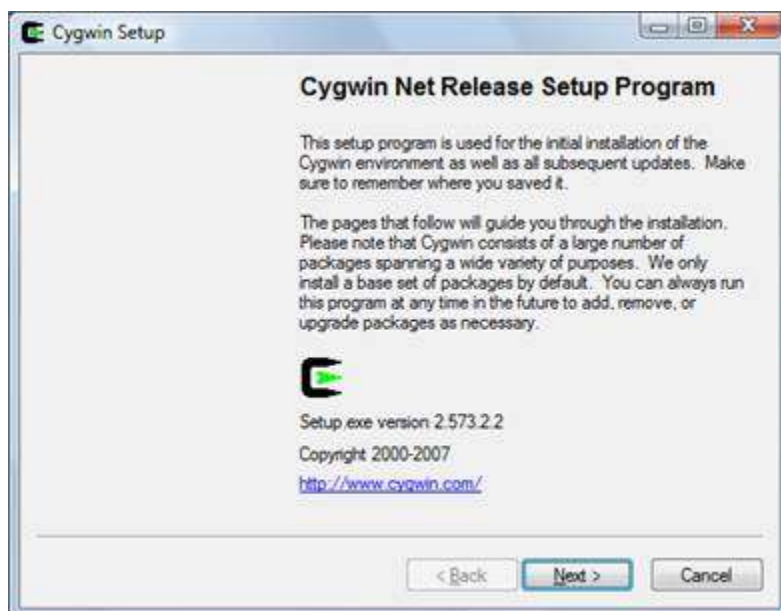
Despite the rather complete and very professional web interface that FreeNAS uses for management, there are still some tasks that require access to the underlying command line. One example that comes to mind is making directories for mount points and setting the necessary permissions. Granted, this could be done from the GUI's "run" command, but entering commands one at a time into a GUI prompt gets a bit tedious.

One option you have is to go to the FreeNAS console and choose option 6 - this launches a shell where you can enter any commands you wish. of course, the console has to be enabled, and you have to actually walk over to the FreeNAS box. Hey! Where's the technology when you need it?

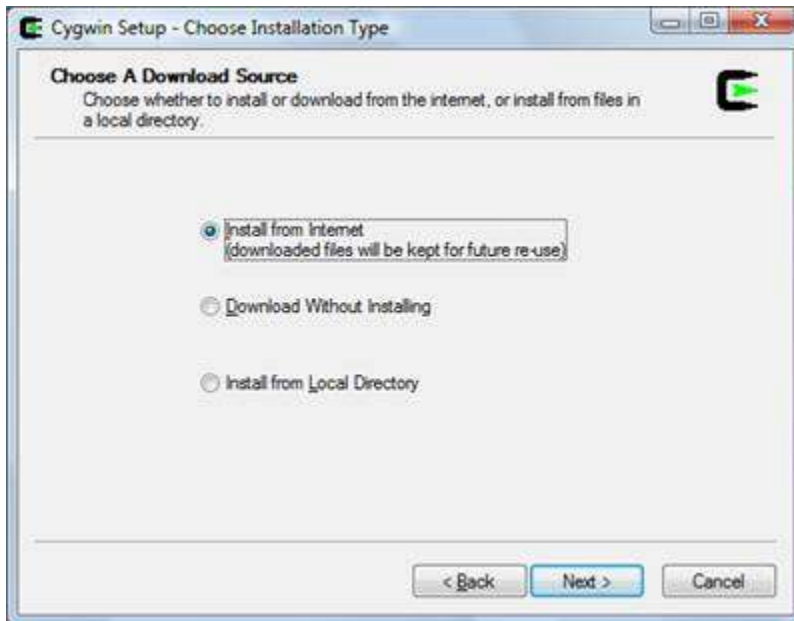
It's here, actually, and comes in the form of SSH - the Secure SHell. SSH works very much like telnet (a common terminal emulator for the network) except that it encrypts the traffic. SSH also has some interesting capabilities beyond remote shell access. You can use it for secure file transfer (via SFTP) and even remotely run a command, returning the output back to your computer.

There are many forms of SSH - its built into most versions of Unix/Linux, and several incarnations are available for the Windows world. One common version for Windows is called "putty", and provides a GUI interface. VanDyke Technologies offers VShell, a commercial implementation. I've used both, and for general terminal connections they are fine, but I prefer a traditional command-line based version because I can take advantage of automation more easily. I'll explain how to install a minimal CygWin environment with SSH. One advantage of this is that you will be able to sharpen your \*nix command line skills without ever leaving your PC.

Installing CygWin is easy, and is done directly over the Internet. Simply point your browser to <http://cygwin.com>. In the upper right-hand corner of the page is a link to "install CygWin now". Click that and choose "Run" when prompted. This will download and run the installer. (you might have to click Run twice, depending on your local security settings.



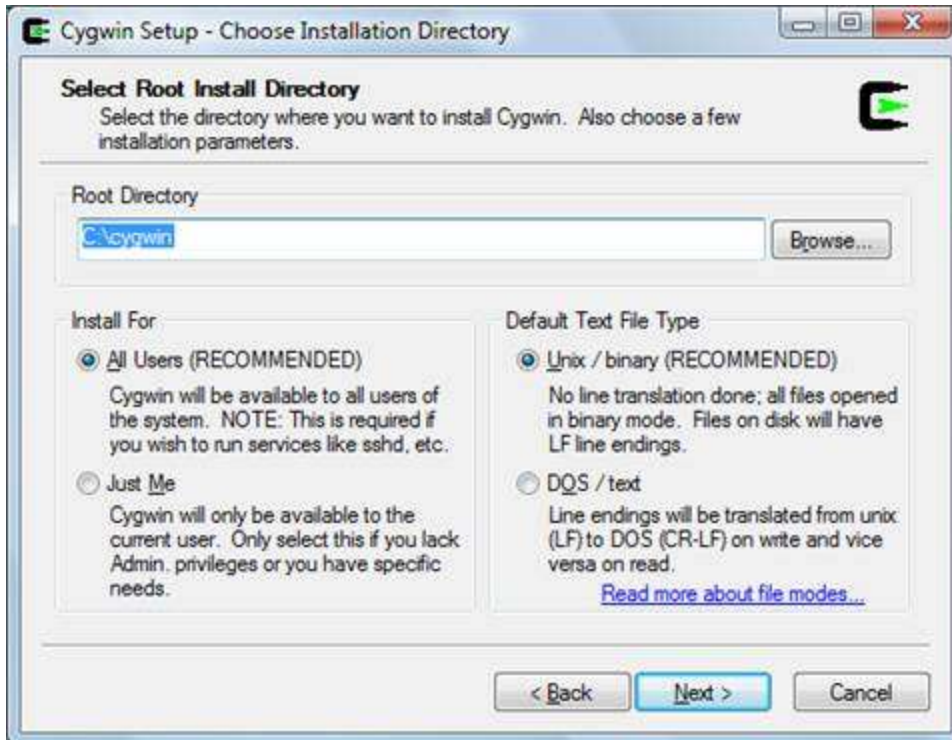
Continue by clicking Next. Choose “Install from Internet and click Next.



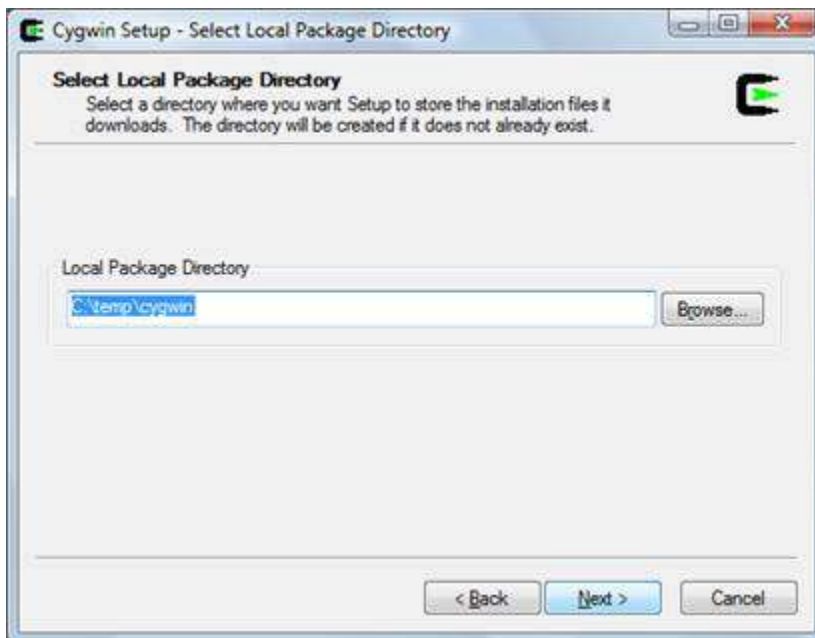
Choose the default C:\Cygwin. Resist the urge to place this in C:\Program Files\Cygwin for several reasons!

- A. It's a separate form of an O/S environment
- B. \*nix is sensitive to spaces – “Program Files” has spaces!

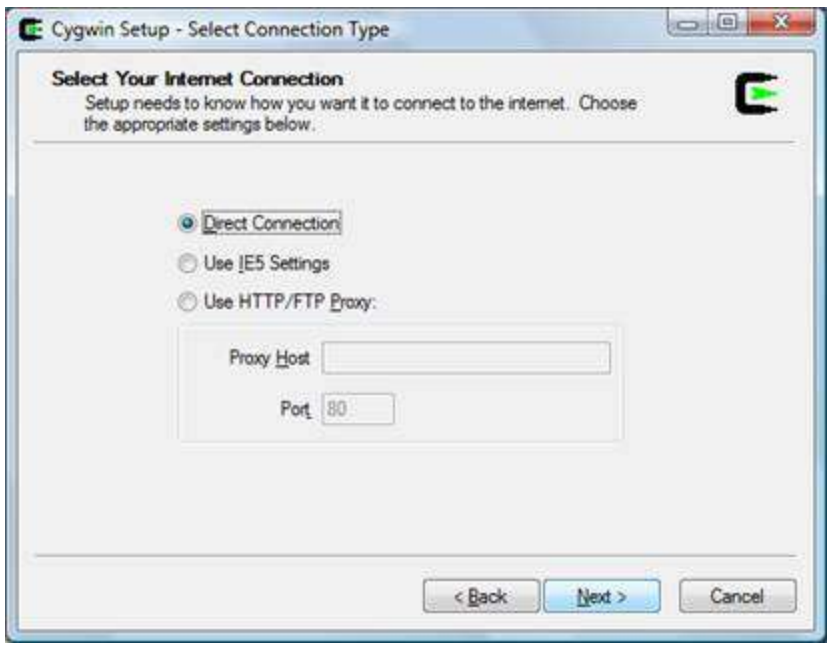
The other default settings are also recommended.



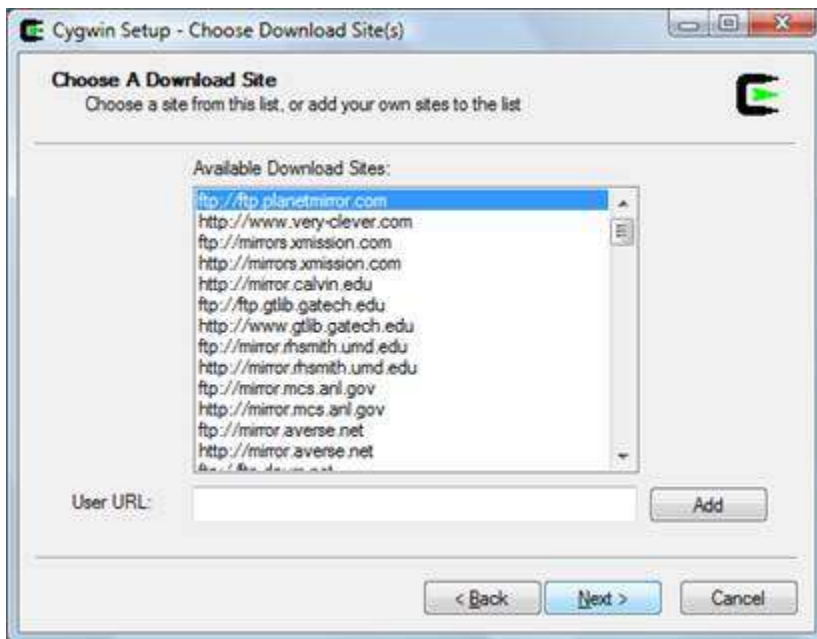
Select a path where the installation files can be maintained. You can do future CygWin installs from this location, so choose wisely.



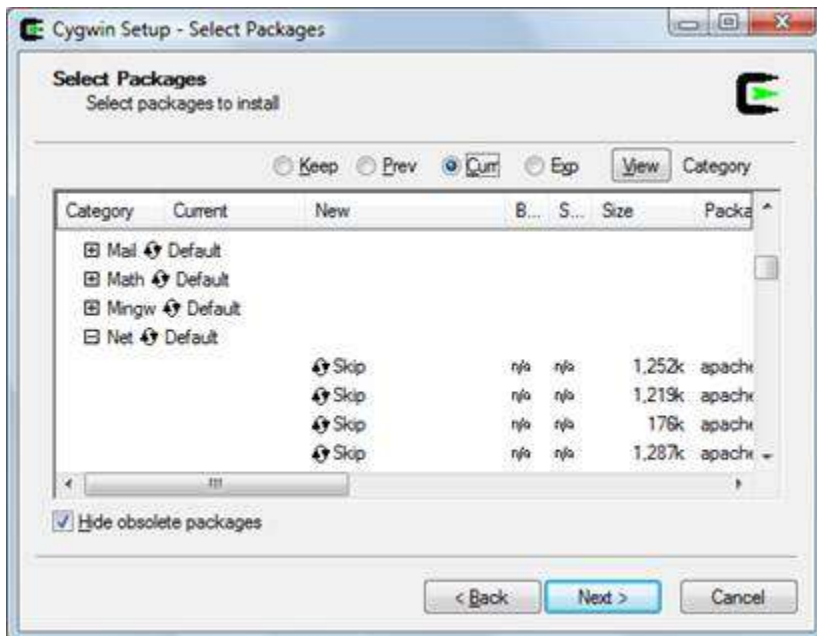
Set the connection parameters as necessary for your environment.



Choose a download site based on your geographic area:



When the Select Packages page appears, scroll down to the Net section and expand it. Locate the OpenSSH and OpenSSL components and make sure that they are selected for install. The version number will appear if it will be installed.



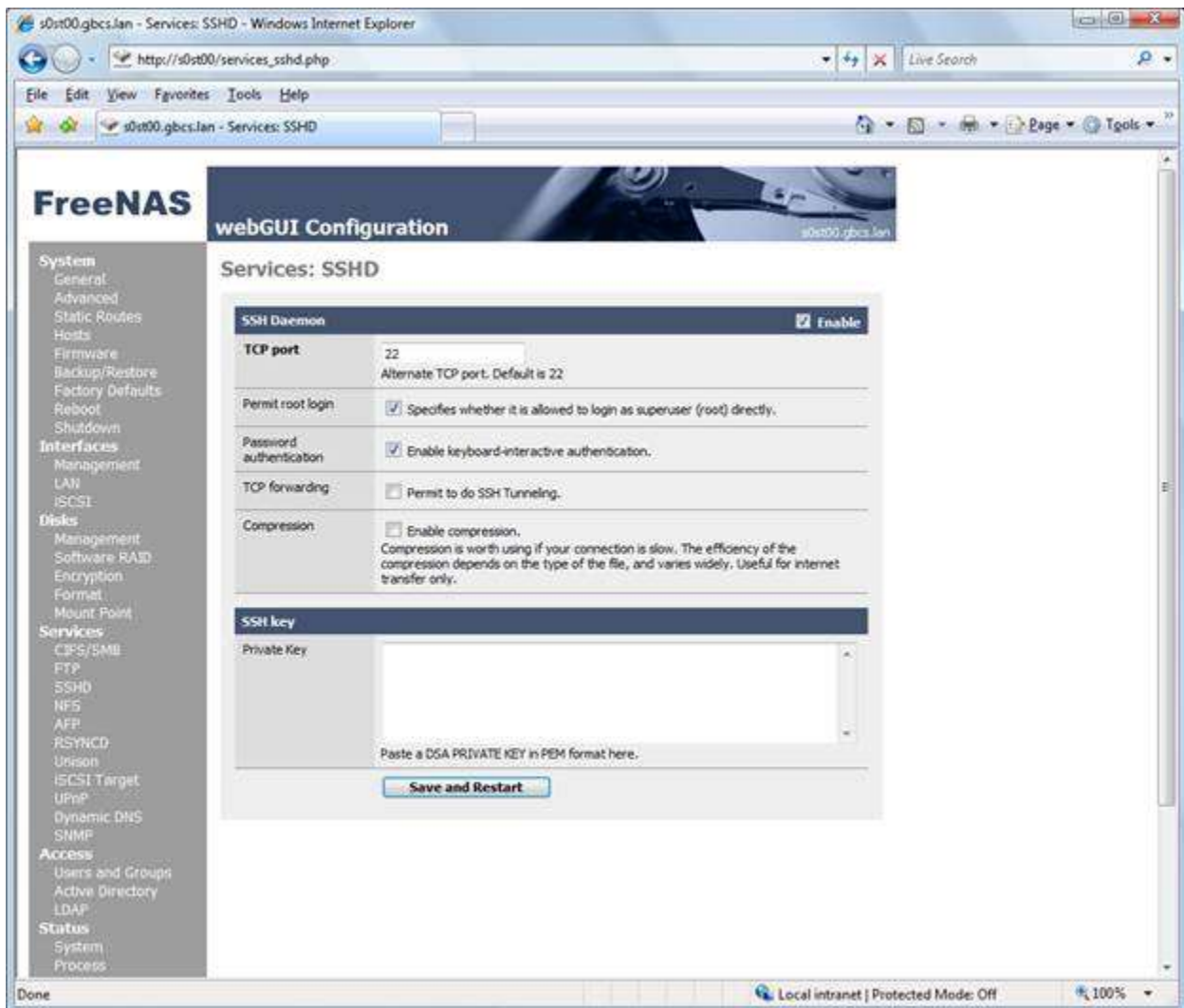
Click Next to begin the download and installation.

The first time you open a CygWin console window, you will be asked to run two commands. These update the password and group files from the Windows (and Active Directory) environments. This could take a LONG time if you have more than a few-hundred users in AD!

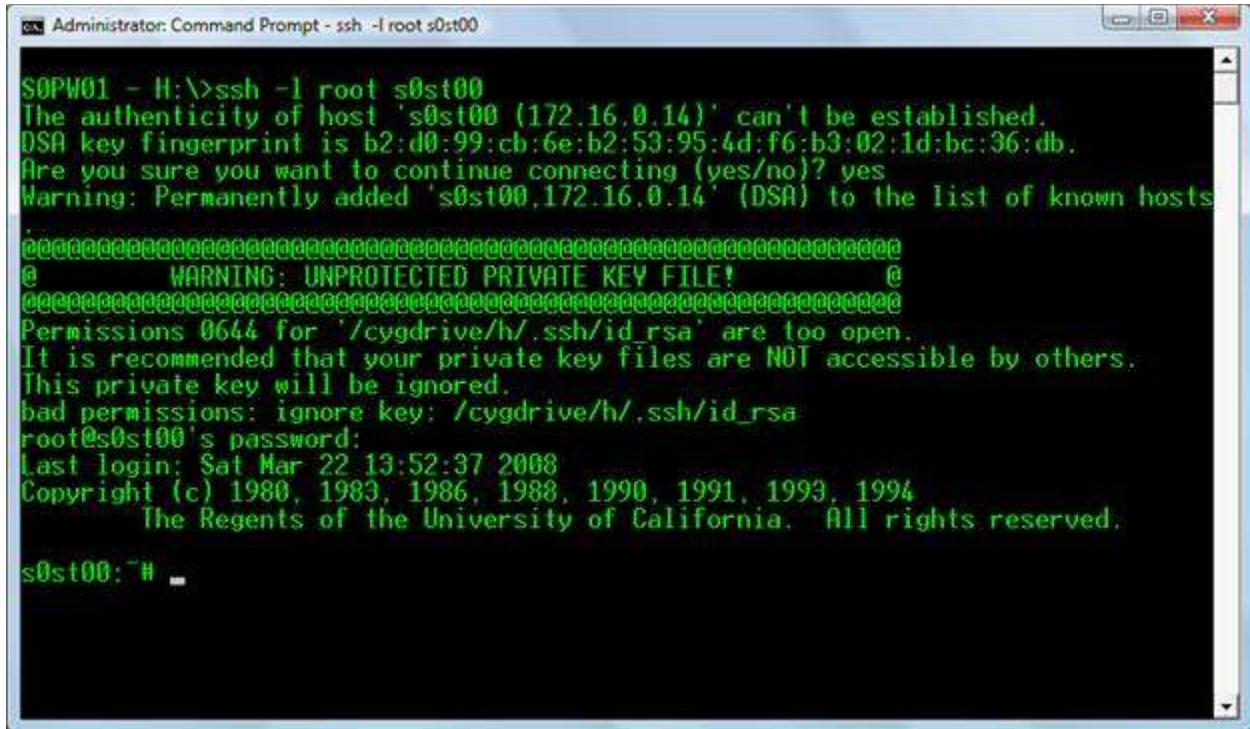
This isn't required just to use SSH, so don't worry if you don't run the commands. One thing you should do, however, is to add C:\Cygwin\bin to the Windows system PATH. This will let you run the CygWin commands directly from any command prompt (and even mix & match DOS and CygWin commands!).

Once you have updated the PATH, you can open a command prompt and type "ssh -l root host", where "host" is the hostname or IP address of your FreeNAS host. The "-l root" tells ssh that you want to log into the remote system with a different logon ID – "root" in this case. If you created other accounts on your FreeNAS system, you could use those instead. If you don't specify a logon name, it will default to the UserID you used to log onto your workstation, which likely will not work (unless you've integrated FreeNAS with AD).

Before you connect with SSH, be sure you have enabled it on the FreeNAS GUI. Click the "Enable" checkbox in the upper-right corner, and also (at least for now) select the "Permit root login". If you defined other FreeNAS accounts, or have A-D integration enabled, turning this off will enhance security, and is recommended. Make the changes and click "Save and Restart".



The ssh command will connect and validate the host hash value. Since none exists, it will warn you that it has changed, and ask if you want to update the list with this host's hash. Respond with "yes" (spelled out, case sensitive!), otherwise it will ask each time you connect. You'll be prompted to supply the password for the account you defined. If you are using "root", enter the same password that you use for "admin" in the GUI. See the example session below:



```
Administrator: Command Prompt - ssh -l root s0st00
S0PW01 - H:\>ssh -l root s0st00
The authenticity of host 's0st00 (172.16.0.14)' can't be established.
DSA key fingerprint is b2:d0:99:cb:6e:b2:53:95:4d:f6:b3:02:1d:bc:36:db.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 's0st00,172.16.0.14' (DSA) to the list of known hosts
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for '/cygdrive/h/.ssh/id_rsa' are too open.
It is recommended that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: /cygdrive/h/.ssh/id_rsa
root@s0st00's password:
Last login: Sat Mar 22 13:52:37 2008
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California.  All rights reserved.

s0st00:~#
```

You should now be connected to your FreeNAS system. You have administrative rights, so be careful! Run whatever commands you need to and log off by typing "exit", or simply "^D" (control-D). Notice the prompt has a "#" – this indicates "superuser" or admin level access. Normal accounts use a "\$" on the prompt. Also notice the warning about an unprotected key file. That is because my CygWin home folder is also my Windows home folder and not on the local drive's CygWin\home path. I have not set the permissions on my network folder using the CygWin tools, and would suggest either doing so or changing the /etc/passwd file to point to the local CygWin home path. Until this change is made, ssh will not update the trusted hosts file, and will prompt the user to accept the connection each time.

Glenn Barnas  
Innovative Technology Consulting Group  
<http://www.innotechcg.com>