UW-Madison College of Engineering

How to Tunnel Remote Desktop Through SSH on a Windows Computer

Why me and why now?

CAE has been charged to implement the College of Engineering Network Security Policy . As part of the security measures, the College has set up a firewall, which blocks access to the College's network on certain ports.

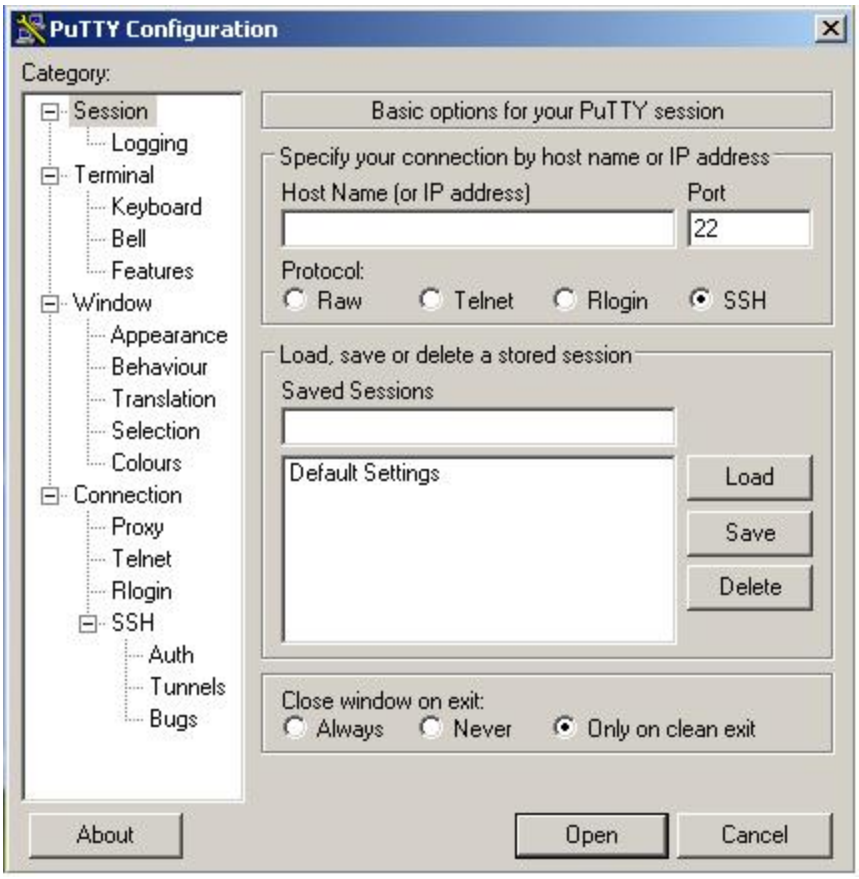
Those wishing to access their office (or lab) computer can do so via "Windows Remote Desktop", although not directly. The method described below provides a secure (encrypted via SSH) method to gain access to a remote desktop (computer) behind the College's firewall. This procedure is called tunneling. For details on how to remotely connect to a CAE Desktop, see the CAE Remote Desktop page on the CAE web site.

What you need

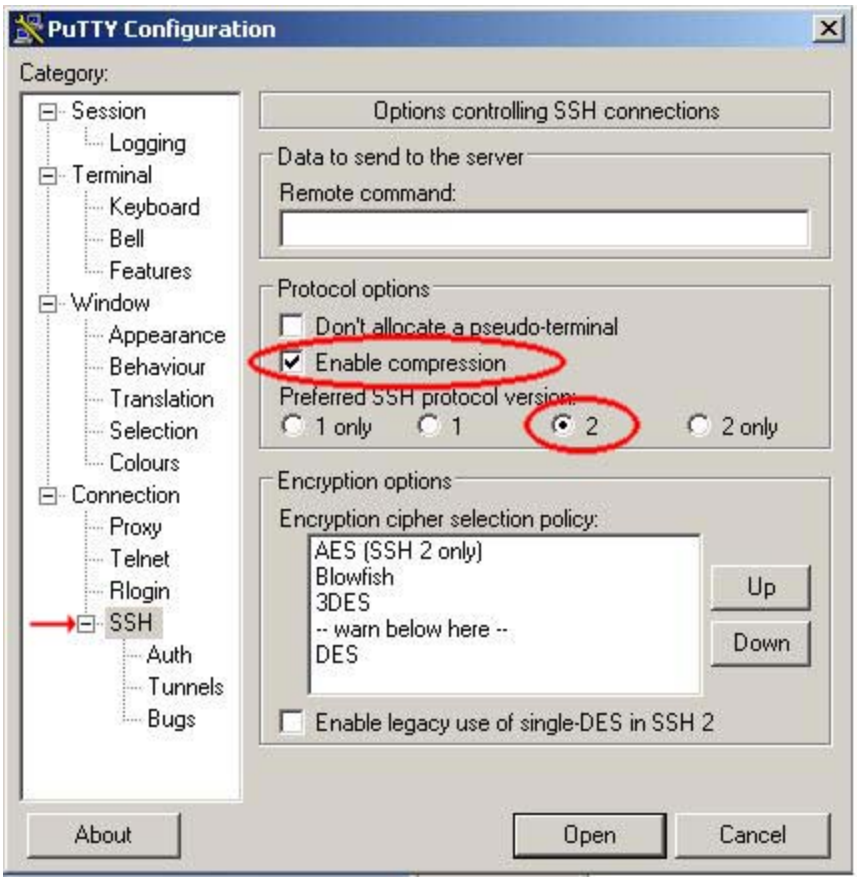
- The SSH client called PuTTY which can be downloaded from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html . There is no installation routine for PuTTY as the entire program consists of the file "putty.exe"
- A CAE account to log into any CAE Unix computer

Setting up PuTTY

1. Start PuTTY (double-click on putty.exe). You will see a window similar to this one:

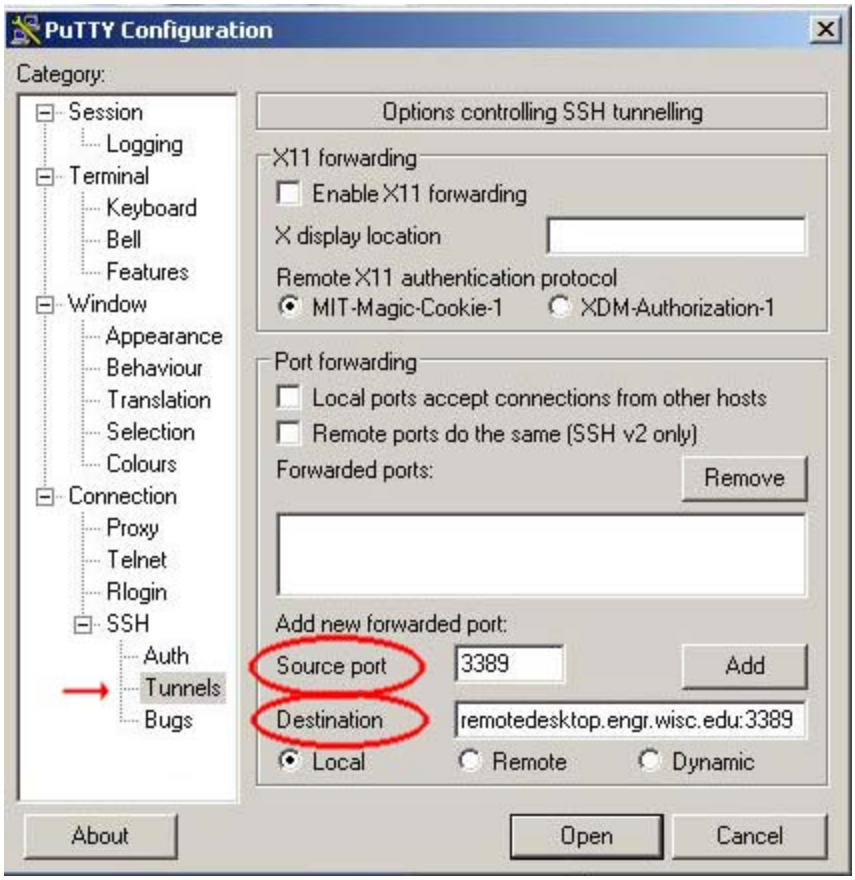


2. Next, enable compression. Select SSH protocol level 2 as the default in the **SSH** subcategory for better security:

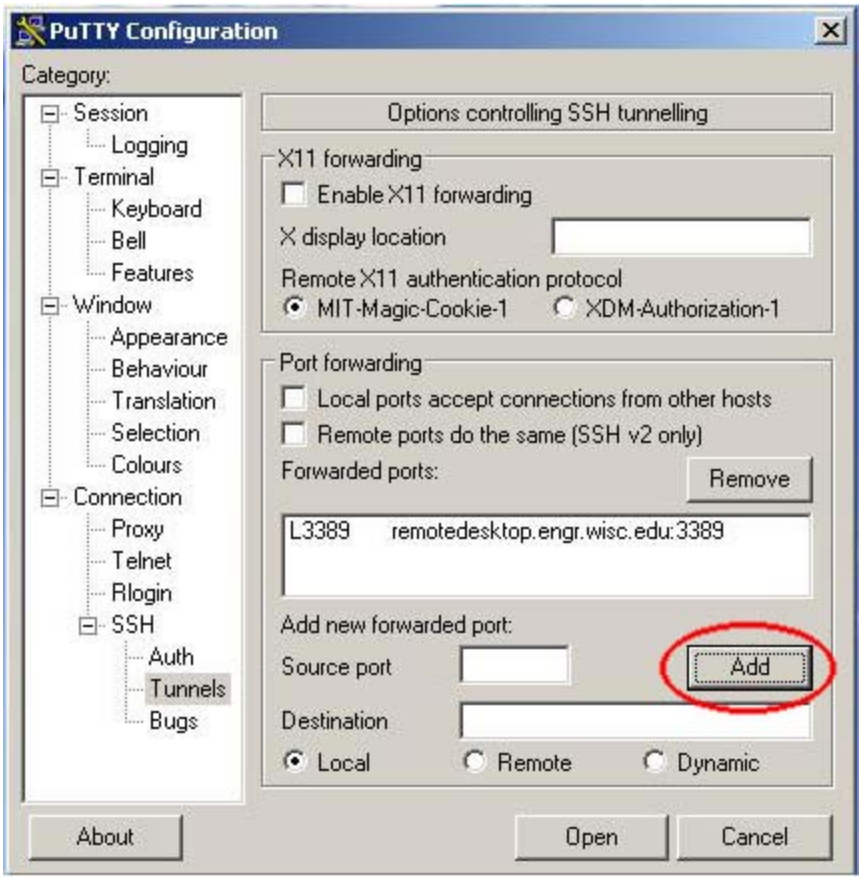


3. To configure the "tunneling". In the example below, we are tunneling the remote desktop port on the local machine, through the gateway to the Remote Desktop port on the fictitious remote server "remotedesktop.engr.wisc.edu" (enter the name or IP address of your computer in place of this name). The name is resolved from the remote gateway machine, so it can be a hostname not visible to the user machine. Depending on your operating system, what you enter into "Source Port" may be different from the example shown:
    - Windows XP **127.0.0.2:3389**
    - Other Windows Platforms: **3389**

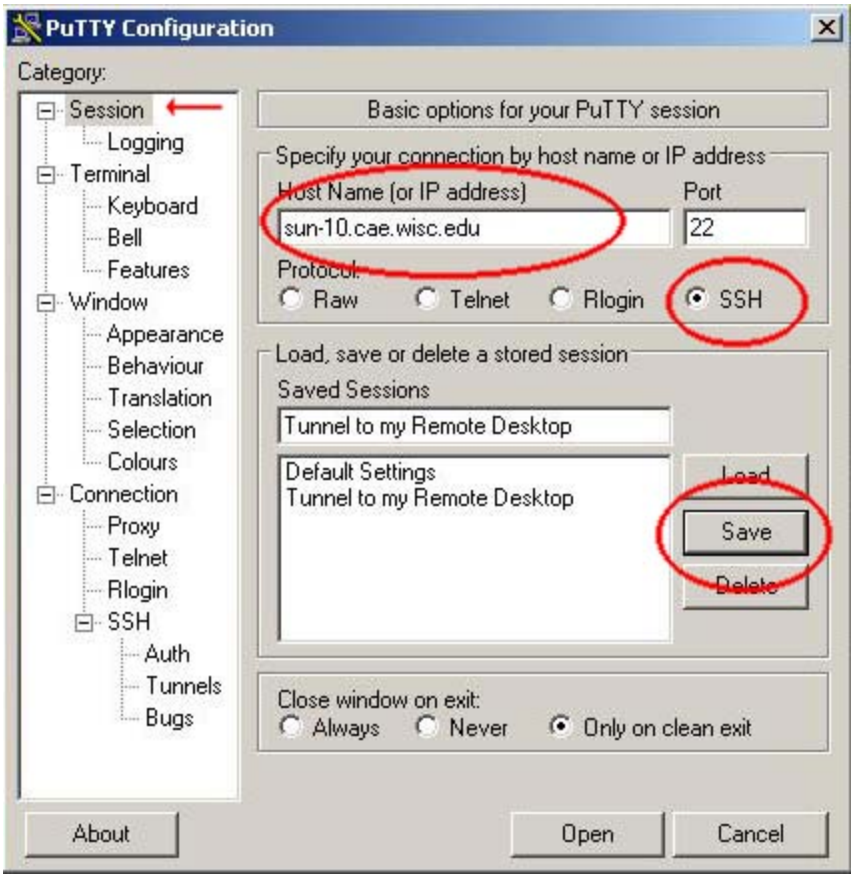
    For more information on why this is necessary, see this page



- The source port is the port on the user machine to which you will address connections that you intend to have tunneled.
- The destination defines a host and a port to which the remote gateway's sshd will connect incoming traffic from the user machine. When you click on
- Add, the results are displayed like this:



4. Go back to the **Session** subcategory, identify the gateway host's IP address or name (in the example below we used sun-10.cae.wisc.edu as the gateway, although it could be any computer with ssh allowed through the firewall), make sure that the SSH button is filled, name your session (in this case "Tunnel to my Remote Desktop") and save it:



Whenever you need the tunnel to appear, you can start PuTTY and double-click that session.

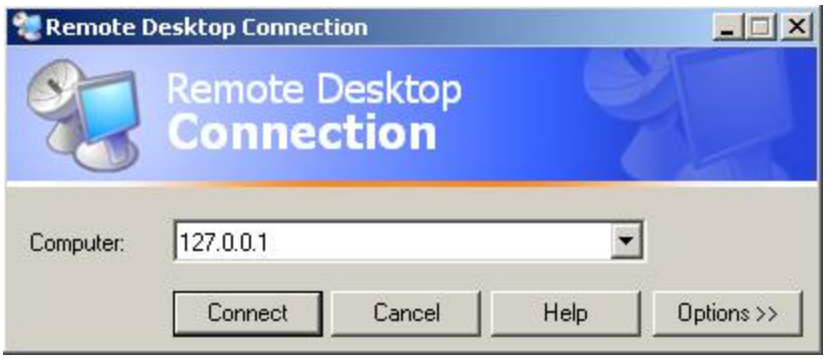
Starting Remote Desktop

1. Start PuTTY and then click on the session that you saved earlier; this will start the SSH connection.

2. Login to the gateway computer when prompted (in this case, the gateway computer is 'sun-10.cae.wisc.edu') and when the login process is done, you can minimze the active PuTTY session (you don't need to type anything more, but you need to keep the program running).

3. Start your Remote Desktop program as usual. Instead of entering the name of the computer that you want to connect to, you must type in the address and port that Putty is forwarding to. Depending on your operating system, this may be different from what is shown in the example:
   - Windows XP: **127.0.0.2**
   - Other Windows Platforms: **127.0.0.1**

   This will connect you to the computer that was specified in PuTTY (in this case, the fictional computer **remotedesktop.engr.wisc.edu**).



4. Voila! You are now connected to your Remote Desktop computer through an SSH tunnel!

5. After you are done using Remote Desktop, exit from the program as normal and then you may close the PuTTY program.

Date last modified: Wednesday, 10-Mar-2005 14:42:24 CDT
Date created: Tuesday, 22-Jun-2004
Content by: decoster@engr.wisc.edu