UW-Madison College of Engineering

College of Engineering > Computing Resources > Computing Best Practices > Windows Remote Desktop

How to Tunnel Remote Desktop

Through SSH on a Windows Computer

Why me and why now?

CAE has been charged to implement the <u>College of Engineering Network Security Policy</u>. 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 <u>CAE Remote Desktop</u> page on the CAE web site.

What you need

- The SSH client called <u>PuTTY</u> which can be downloaded from <u>http://www.chiark.greenend.org.uk/~sgtatham</u> /<u>putty/download.html</u>. 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:

Session	Basic options for your PuTTY s	ession
Terminal Keyboard Bell	Specify your connection by host name or Host Name (or IP address)	IP address Port 22
 Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Auth Tunnels Bugs 	Protocol: C Raw C Telnet C Rlogin	 SSH
	Saved Sessions Default Settings	Load Save Delete
	Close window on exit: C Always C Never ⓒ Only on	clean exit

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

Consistent	Orticus controlling CCU comparisons
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Connection Proxy Telnet Rlogin SSH Auth Tunnels Bugs 	Data to send to the server Remote command:
	Protocol options □ Don't allocate a pseudo-terminal □ Enable compression Preferred SSH protocol version: □ 1 only □ 1 • 2 □ 2 only Encryption options Encryption cipher selection policy: AES (SSH 2 only) Blowfish 3DES - warn below here DES Down
	Enable legacy use of single-DES in SSH 2

- 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

ategory:	
🖃 Session	Options controlling SSH tunnelling
Logging Logging Logging Logging Keyboard Sell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet	X11 forwarding Enable X11 forwarding X display location Remote X11 authentication protocol MIT-Magic-Cookie-1 C XDM-Authorization-1 Port forwarding Local ports accept connections from other hosts Remote ports do the same (SSH v2 only) Forwarded ports: Remove
- Rlogin ⊡ SSH	Add new forwarded port: Source port 3389 Add

- 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:

 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Auth Tunnels 	Options controlling 9	SSH tunnelling
	X11 forwarding Enable X11 forwarding X display location Remote X11 authentication pro MIT-Magic-Cookie-1 Port forwarding Local ports accept connect Remote ports do the same (Forwarded ports:	tocol XDM-Authorization-1 tions from other hosts (SSH v2 only) Remove
	L3389 remotedesktop.eng Add new forwarded port: Source port Destination	r.wisc.edu:3389

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:

🛛 Session 🛛 🔶	Basic options for your PuTTY session
 Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin SSH Auth Tunnels Bugs 	Specify your connection by host name or IP address Host Name (or IP address) Port [sun-10.cae.wisc.edu 22 Protocol: C Raw C Telnet C Rlogin • SSH Load, save or delete a stored session Saved Sessions
	Tunnel to my Remote Desktop
	Default Settings Tunnel to my Remote Desktop Save Delete
	Close window on exit: C Always C Never © Only on clean exit

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**).

🐮 Remote I	Desktop Connection				
E.	Remote Desktop Connection				
Computer:	127.0.0.1	•]		
	Connect Cancel	Help	Options >>		

- 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.

Copyright 2004 The Board of Regents of the University of Wisconsin System Date last modified: Wednesday, 10-Mar-2005 14:42:24 CDT Date created: Tuesday, 22-Jun-2004 Content by: <u>decoster@engr.wisc.edu</u>