Secure Access to Remote Computers from Windows

John Ogren, NOAA/ESRL, Boulder, USA

September 2, 2009

The aerosol group at NOAA/ESRL/GMD uses Linux-based software for data acquisition and instrument control, as well as for subsequent data processing. The data acquisition and processing computers can either be stand-alone systems, or they can be running as virtual machines (VM) on a host computer. Both systems run a server that allows connections from remote clients over a secure, encrypted connection. This document describes the software required to remotely access either of these systems from a Windows computer.

Secure connection to the remote computer is achieved using a combination of the *SSH* (Secure Shell) and *VNC* (Virtual Network Computing) client software for Windows. The *SSH* software provides secure, compressed and encrypted connections over the public internet, while the *VNC* software allows graphical display of the remote computer's screen and control of the remote computer's keyboard and mouse.

a. Links for downloading software.
   - http://www.realvnc.com has client and server software for *VNC* connections for both Windows and Linux. The free "VNC Free Edition Viewer for Windows" software is all that is needed for remote access to the remote Linux system.
   - http://www.chiark.greenend.org.uk/~sgtatham/putty/ has the free *SSH* client software for SSH connections for Windows computers. The putty.exe client is a graphical *SSH* client, and plink.exe is a command-line, text-mode *SSH* client.
   - ftp://ftp.cmdl.noaa.gov/aerosol/etc/cpd/svnc has custom software written by NOAA/ESRL, called "svnc.exe", that facilitates using *SSH* to establish secure *VNC* connections from Windows clients. For convenience, this directory also contains the free VNC viewer and the SSH client program from the above sources. (Note that plink.exe must be renamed to ssh.exe for compatibility with svnc.exe.) The three programs in ftp://ftp.cmdl.noaa.gov/aerosol/etc/cpd/svnc must be placed in a directory in the Windows PATH, e.g., C:\windows\system32.

b. Router configuration.
   The router at the remote site must be configured to forward incoming *SSH* connections to the appropriate computer. Alternatively, the operator at the remote site can click on the "Make Tunnel" icon on the remote desktop, which will enable remote access via a server at NOAA/ESRL, aerolab6.cmdl.noaa.gov.

c. Linux server configuration.
   The CMDL Linux-based aerosol data acquisition computer, and the VM-based data processing system "AER_VM", come pre-configured for secure graphical access using *VNC* over an *SSH* connection. The normal (insecure) port used by the *VNC* server is blocked by the firewall on the Linux server, so that the only access is through an encrypted connection via the *SSH* server. These systems both also allow remote, text-only access using an *SSH* client.

d. Windows client operation.
   Both SSH and VNC client software are needed for remote Windows clients to connect to the Linux server. NOAA/ESRL has written the *svnc.exe* program to make it easy to make a connection. The SSH client *ssh.exe* (Putty's 'plink.exe' program, renamed to 'ssh.exe') and VNC client *vncviewer.exe* programs must be available in a directory in the Windows path on the client computer. The syntax

for running *svnc* to connect to the remote Linux server is

svnc -C -P port -l user servername

where *port* is the port number used for the connection, *user* is the username on the server (normally, this is "cpd"), and *servername* is the name or IP address of the remote system. The value of *port* depends on whether a connection is being made directly to the remote Linux server or via a tunnel connection.

For example, if the remote server is named aerosol.dyndns.org, a direct connection would be made with the command

svnc -C -P 22 -l cpd aerosol.dyndns.org

If a tunnel connection is used, the command normally would be

svnc -C -P 10220 -l cpd aerolab6.cmdl.noaa.gov

In exceptional cases, another tunnel might be in use when the "Make Tunnel" icon is clicked. In this case, the tunnel ID will not be the default value of "0" assumed in the above example. If this happens, the operator of the remote computer must be asked to look at the screen and find the actual tunnel ID, which will be displayed in the window that is opened by the "Make Tunnel" icon. The actual tunnel ID will be a value in the range 0-9. The last digit of the argument after "-P" should be replaced with the actual tunnel ID. For example, if the remote screen displays "Opening tunnel for NIL on port index: 1", the actual tunnel ID is 1, and the command to use on the Windows client would be

svnc -C -P 10221 -l cpd aerolab6.cmdl.noaa.gov

The *svnc* command can be associated with an icon on the Windows client's desktop, so that the remote computer can be accessed by simply double-clicking on an icon.

Revision Notes

original September 2, 2009