

VPN Access using SSH and VNC - HOWTO

Don Davies, Prosig Ltd (don.davies@prosig.com)
January 2003

Describes the configuration and setup of a simple VPN for graphical remote access using the Open Source tools SSH and VNC.

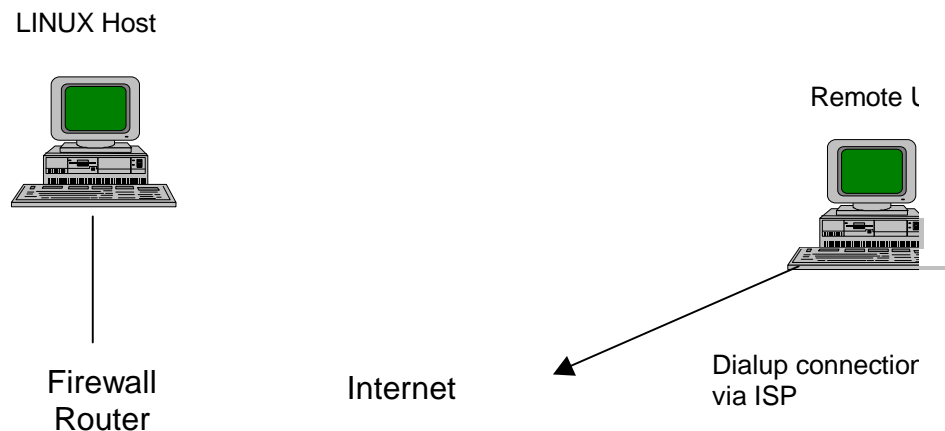
1. Introduction

This note describes the setup and configuration of a simple VPN for graphical access to a Linux system from a remote PC. Previously, remote access to a Linux box has been possible via dialup modem using dialup networking (PPP) and VNC. This presents a number of security issues especially if the Linux system is connected to a corporate network. The aim of this note is to describe how secure remote access may be achieved by creating a simple VPN using standard the Open Source Secure Shell (SSH) utilities. Most Linux distributions include the OpenSSH¹ package, if not download a copy from the web site shown in the reference and install the package.

Graphical access to a Linux system is readily provided by the Virtual Network Computing (VNC²) package. The VNC server (Xvnc) is generally installed and configured on the PROTOR host as standard on most Linux distributions.

A Linux system may be configured for VPN access provided that Internet access and suitable firewall hardware or software is available. Linux can either provide this Internet access and firewall protection itself or, more commonly, can take advantage of existing high-speed internet access and firewalling. It is assumed for this description that remote access is required from a stand-alone PC running Windows. This PC has Internet access either via an analogue dialup or ISDN via an ISP.

This method uses the simplest form of VPN which is a host-host topology illustrated below.



The remote PC must be loaded with a suitable SSH client program³ for Windows and also the VNC client or viewer program. Access from a correctly authenticated SSH client creates an "Internet Tunnel". Information passing through this tunnel is encrypted for security and is also compressed for efficiency. In order to make full advantage of the PROTOS User Interface it is also possible to pass direct graphical information through this tunnel using the VNC package.

Details are given below on a typical VPN configuration. The Linux host system is connected via a dedicated network to an Internet server providing broadband access and firewall protection. Remote access is provided from a Windows PC running MS-Windows for which a SSH client and VNC distribution are provided.

2. Configuration Details

This VPN demonstrator has been configured using in-house broadband internet server and firewall. The only configuration needed on this firewall is to enable SSH port (port 22) and to forward this port via the specific network route to the Linux host. An SSH client request for connection to this server results in the request being routed directly to the Linux Host.

The VNC package allows X-window type graphics information from a server to be presented on a client screen. This package also uses specific port numbers on the system based on a requested display number. Requesting a display number 0 for a specific server uses port 5900, display number 1 port 5901 and so on. In order to route VNC through our SSH tunnel then we use a facility within SSH called "local port forwarding". We can use this facility to forward port 5910 on the Windows PC system such that it appears at the other end of the tunnel (the Linux host) as if it is a connection from itself (localhost) on port 5900.

Therefore specifying a connection within VNCVIEWER to localhost on display 0 causes a connection to be established to local port 5910 which is local forwarded through the SSH tunnel to port 5900 on the Linux Host. This connection is then seen by the VNC server as a connection request for its display number 0 and a VNC session is established.

This VPN demonstrator is described in the following diagram.

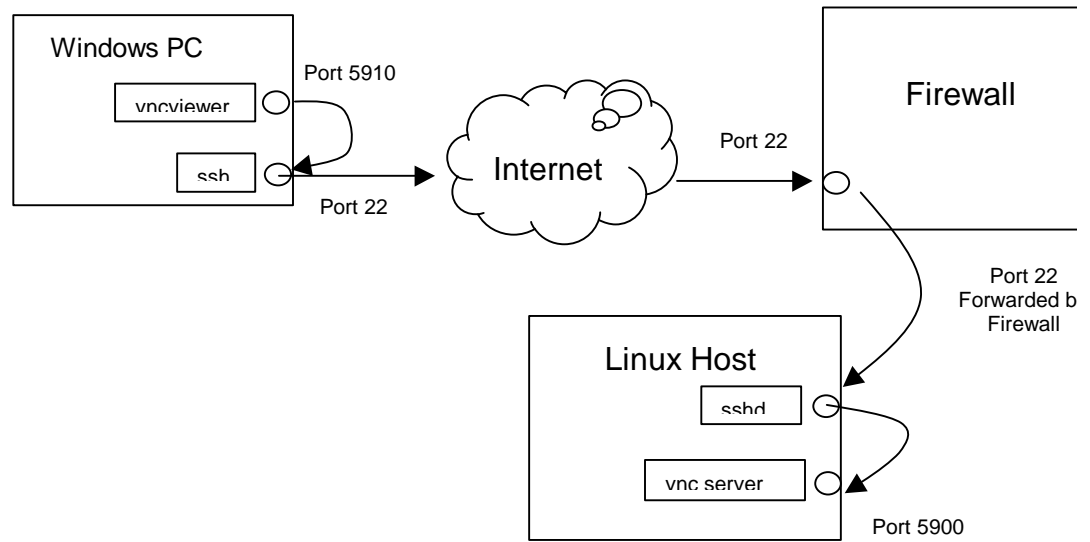


Figure 1. VPN Demonstrator Configuration

3. *Installation Details*

Included in the references is a suitable SSH client program for Windows. The program is distributed in the form of a ZIP file. To install the package simply extract all files from the archive to a suitable location on your system.

Also included in the references is an address for the VNC web site. The Windows download for this package includes the VNC client program (vncviewer).

It is beyond the scope of this note to describe the installation and setup of SSH under Linux. Essentially you will need the ssh-server package installed and generation of the authentication keys. Ensure that the ssh-server is running on the Linux host system. You can check this on the Linux system by command

```
service sshd status
```

If the server is not running then start it by the command

```
service sshd start
```

4. Configuration and Testing

Make and verify a connection to the Internet using an appropriate connect from your remote Windows PC.

Check that you can resolve the name of your server. Note you should be able check that the your server address using the "ping" command. Note that server may not respond to the pings but the name should be resolved into an address.

On the Windows PC Start the program SSH.EXE which may be found in "Program Files/ssh" directory from where the SSH package was extracted and follow these configuration steps.

1. Create a New connection Profile by clicking on the New Button. Any existing entries will be cleared. Give the Profile a suitable name. Setup the main entries for the profile as follows (all other values may remain as their default setting).

```
Hostname :your-server.co.uk
Port :22
User ID :protor
CipherType:Blowfish
Authentication
    Type : RSA and Password
X11 Forward:On
```

SSH options

Profile Name:

Delete Save New OK Cancel

Host Name: Port:

User ID: ddd Cipher Type:

Identities

Command:

Authentication Type

RSA Password Challenge/Response

Remote Forwards X11 Forward Close on exit

Local Forwards Strict host key checking Hide window

Connection Attempts:

Receive LF as CR/LF Copy EOL CR+LF LF

Send BS as DEL Paste EOL as CR+LF LF

2. Enable the Tunnel for the VNC viewer task by clicking on the Local Forwards Button. On this menu set the following :

```
Local Port : 5910
Host : localhost
Remote port : 5900
```

When set click on New to add the Local Forwarded Ports and Click on OK.

Forwards

Forwarded port(s) Local Port:

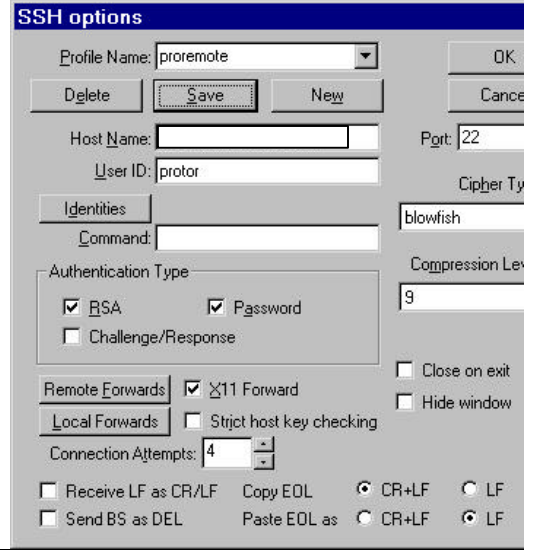
5910 localhost:5900 New 5910

Delete Host: localhost

Reset Remote Port: 5900

OK Cancel Help

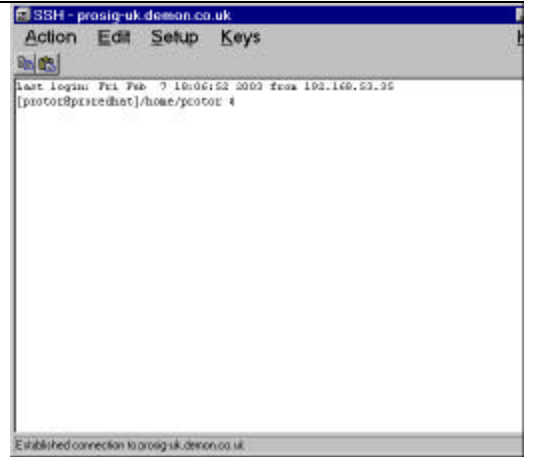
3. Ensure you save the Profile by clicking on the Save button. You should now be ready to make the connection by clicking on the OK button.



4. The SSH program will now attempt to connect to the Linux server your-server.co.uk. If a connection attempt is successful then you will be prompted to authenticate the connection by providing an authentication password.



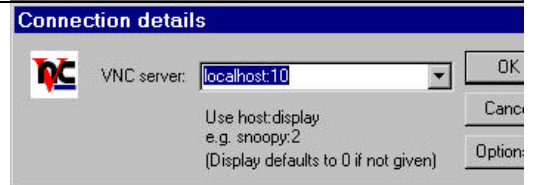
5. If the connection is authenticated then you will see a simple text-based login screen.



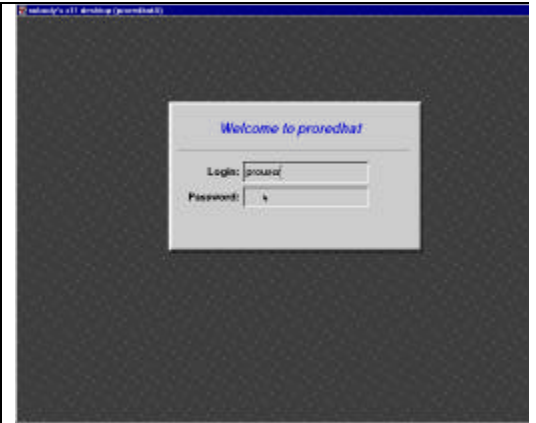
6. Now Startup the VNC viewer tasks. On the resultant menu set the connection node as :

localhost:10

When you click on OK the viewer will attempt to connect to the VNC server on the PROTOR host system through the SSH tunnel.



7. If the connection is made then you will be presented with a login screen to the Linux Host. Enter the Login name and password as necessary.



References.

1. OpenSSH. Version of SSH protocol suite from OpenBSD. (<http://www.openssh.com>).
2. VNC Virtual Network Computing. AT&T Labs Cambridge. (<http://www.uk.research.att.com/vnc>)
3. SSH32. A free SSH client for Windows by C. Igaly (<http://linuxmafia.com/pub/ms-windows/igaly-ssh>)