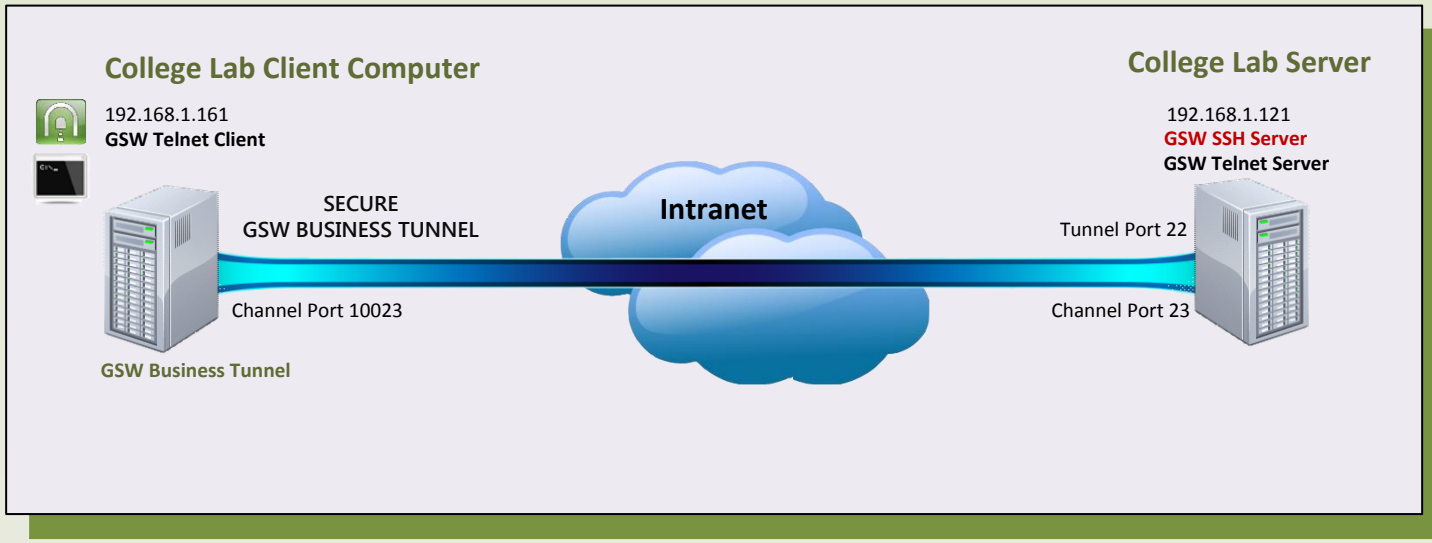
GSW Business Tunnel

Example L01

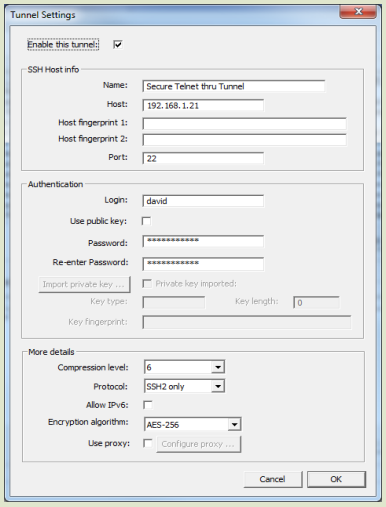
Make a Telnet Connection Secure using the GSW Business Tunnel



Case:

A local technical college wants to demonstrate how you can secure telnet with an SSH Tunnel. In the technical lab they set up a telnet connection and use a network monitoring tool to observe the data. Then as shown in this example they set up the GSW Business Tunnel and then create the Telnet connection. Now when they monitor the line the data is encrypted

Lab Client Computer – GSW Business Tunnel Configuration

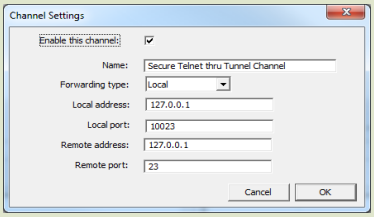


SSH Host and Authentication Settings

1. Set Address of SSH Server Host.

2. Set Authentication Requirements. In this case, Authentication consisted of: Logon name and a password.

Lab Client Computer – Channel Configuration



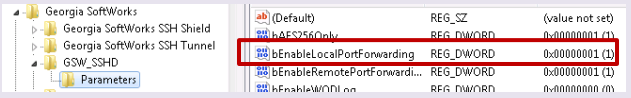
1. Select Local forwarding type.
2. Set the loopback address (127.0.0.1) as the local address.
3. Choose available port number to assign for local port. We selected 10023.
4. For the remote address, use the loopback address 127.0.0.1
5. For the remote port, use Port 23, the common Telnet Server port.

College Lab Server – GSW SSH Server Configuration

Make sure local port forwarding is enabled on the SSH Server. With the GSW SSH Server, the setting is in the registry, as shown below.

x64 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Georgia SoftWorks\GSW_SSHD\Parameters

x86 system:
HKEY_LOCAL_MACHINE\SOFTWARE\Georgia SoftWorks\GSW_SSHD\Parameters



Lab Client Computer – Telnet Client Shortcut

Using the local address and port configured in the channel configuration, modify the Telnet Client Shortcut
@gs_clnt.exe -h127.0.0.1 -P10023 -udavid -phidden -d.