Lightspeed Blackbox Developers Kit (BDK)

How-To Use SSH

Version 1.01
September 30, 2010

1. Introduction

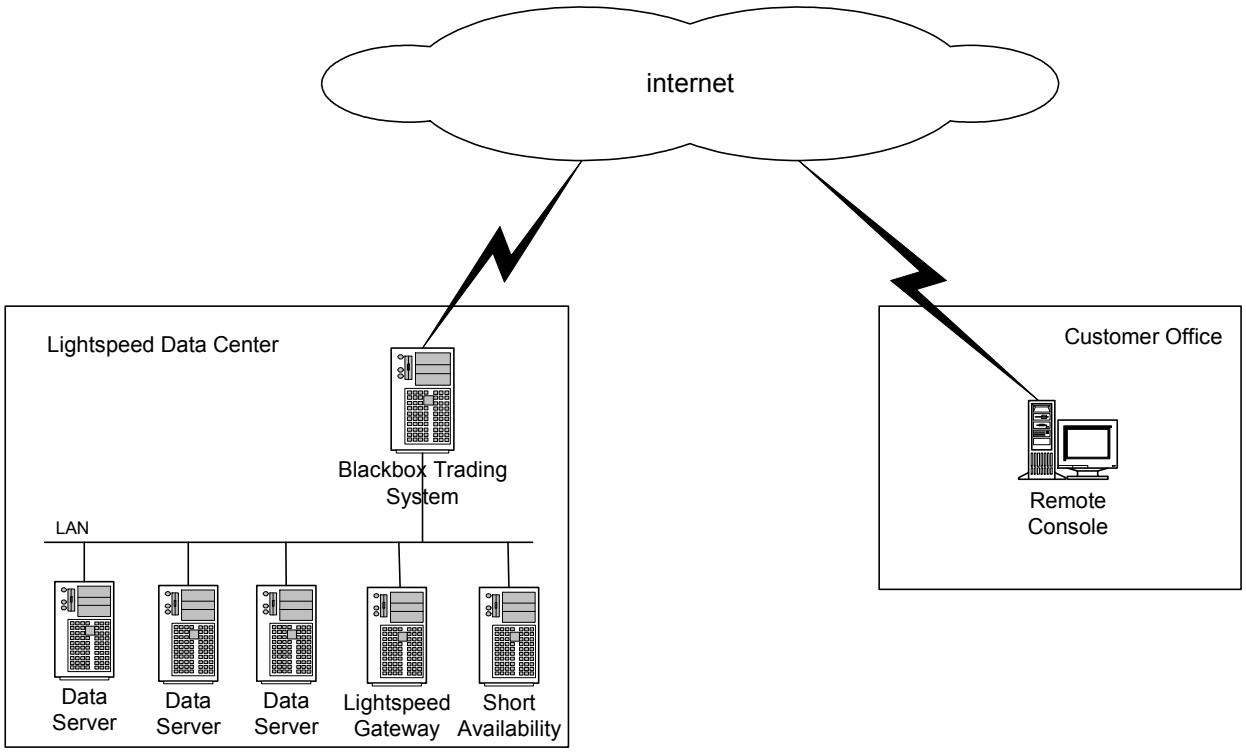
This document provides the following information:

- The recommended method for deploying a Blackbox Trading System.
- Using SSH to create a secure tunnel between a remote console and the Blackbox Trading System.
- Instructions for configuring the SSH server on the Linux system that runs the Blackbox Trading System.
- Instructions for obtaining PuTTY (SSH client software).
- Instructions for using PuTTY to set up a SSH Tunnel.

2. Connectivity Model

There are many ways to configure a Blackbox Trading System with regard to where the computers are located. However, a typical set up is to have one computer running the Blackbox Trading System application located in Lightspeed's data center, and a second computer running a remote console located at the customer's office. This model has the advantage that the Blackbox Trading System located in Lightspeed's data center will have access to the Data servers, Order server, and Short Availability Server over the local area network. A remote console can be located anywhere, at the customer's office or the customer's home, and can communicate with the Blackbox Trading System over the Internet.

The following figure illustrates this connectivity model.



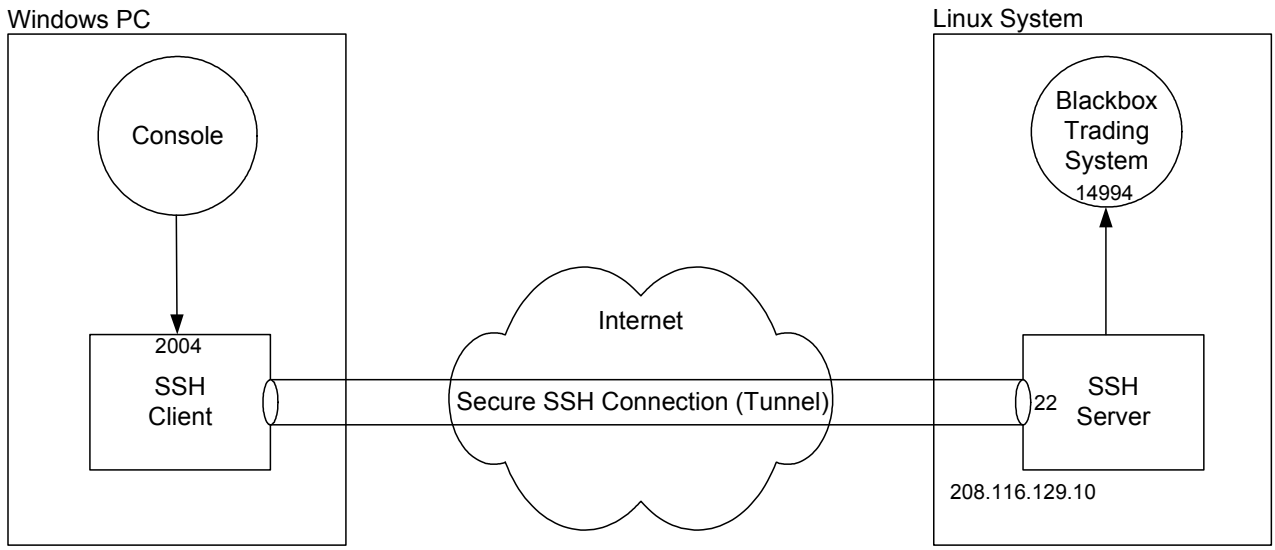
The console communicates with the Blackbox Trading System using a TCP connection over the Internet. To provide security, SSH is used. SSH is a popular, software-based approach to network security. Whenever data is sent by a computer to the network, SSH automatically encrypts it. When the data reaches the intended destination, SSH automatically decrypts it.

SSH uses a client/server architecture. An SSH Server is installed on the Linux system and will accept or reject incoming connections. Customers run an SSH Client programs on another computer and establishes a secure connection to the SSH Server. Once the secure connection is established, clients can make requests of the SSH server, such as, "Please log me in". All communications between the client and server are securely encrypted and protected from modification.

This description is simplified, but should give the reader a general idea of what SSH does. The basic idea is that SSH clients communicate with SSH servers over encrypted network connections.

2.1. SSH Tunneling

Tunneling means encapsulating another TCP-based service (like a console connection) within an SSH session. This brings the security benefits of SSH (privacy, integrity, authentication, authorization) to other TCP-based services (console connection). SSH uses a technique called Port Forwarding to allow the console application to make a connection to the Blackbox Trading System over a secure SSH tunnel. The following figure illustrates Port Forwarding.



The following example outlines the steps required to use SSH Port Forwarding to establish a secure connection between the console and Blackbox Trading System. The port numbers and IP address shown in the figure above are also used in the example below.

1) The SSH Server must be installed, configured and run on the Linux system (208.116.129.10).
2) The SSH Client must be installed on the Windows PC.
3) When the SSH Client is started, it is instructed to accept connections on port 2004 and forward them to port 14994 on system 208.116.129.10.
4) When the SSH Client is started it will connect to the SSH Server on 208.116.129.10, port 22 (SSH's assigned port number). All data transferred between the SSH Client and SSH Server is encrypted, thus creating a secure connection.
5) The console makes a local connection to the SSH Client on port 2004.
6) The SSH Client instructs the SSH Server to make a local connection to port 14994. In this example the Blackbox Trading System is accepting connections on port 14994.

7) Data received by the SSH Client from the console will be encrypted and sent to the SSH Server. The SSH Server will decrypt the data and forward it to the Blackbox Trading System.

8) Data received by the SSH Server from the Blackbox Trading System will be encrypted and sent to the SSH Client. The SSH Client will decrypt the data and forward it to the console.

3. SSH Server

Installing and configuring the SSH Server only needs to be done once. The easiest way to install the SSH Server is to include it when installing Linux. The procedure for installing the SSH Sever may vary for different Linux distributions. Refer to your Linux documentation for instructions.

Once the SSH Server is installed, it needs to be configured to perform Port Forwarding. When using Redhat Linux, the following step can be performed to enable Port Forwarding.

1) Edit the sshd_config file
    a. cd /etc/ssh
    b. vi sshd_config
2) Ensure the AllowTcpForwarding parameter is set to yes. If the AllowTcpForwarding parameter is not found in sshd_config, then add it (AllowTcpForwarding yes).

Before the SSH Server can be used, an encryption key must be created. When using Redhat Linux, the following step can be performed to create the encryption key.

1) cd /etc/ssh
2) Run the following command:
    a. ssh-kengen –t rsal -N ‘‘ –b 768 –f /etc/ssh/ssh_host_key

The above command creates a 768 bit encryption key. The number of bits to be used is specified in the sshd_config file. To determine the number of bits, edit the sshd_config file and locate the ServerKeyBits parameter. If the ServerKeyBits parameter is set to something other than 768, then there are two options to resolve the issue.

1) Change the ServerKeyBits parameter in sshd_config to be 768.
2) Create the encryption key with the number of bits specified by the ServerKeyBits parameter. For example, if the ServerKeyBits parameter is set to 1024, then run the following command to create a 1024 bit encryption key.
    b. ssh-kengen –t rsal -N ‘‘ –b 1024 –f /etc/ssh/ssh_host_key

4. SSH Client

4.1. Installing SSH Client

Installing the SSH Client on the Windows PC that will run the console application only needs to be done once.

There are several free SSH Clients available. PuTTY is a free SSH Client that can be downloaded from www.putty.org.

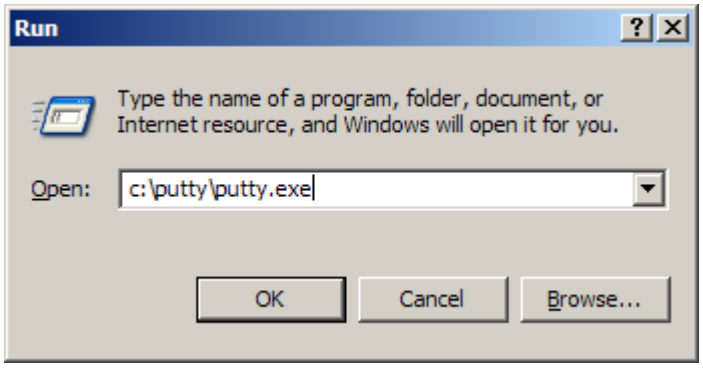
The following steps can be performed to install PuTTY.

1) Create a folder (directory) on the Windows PC to store the PuTTY application (putty.exe). For example, create the folder putty under the C drive (c:\putty).
2) Download putty.exe from www.putty.org and save it in the directory c:\putty

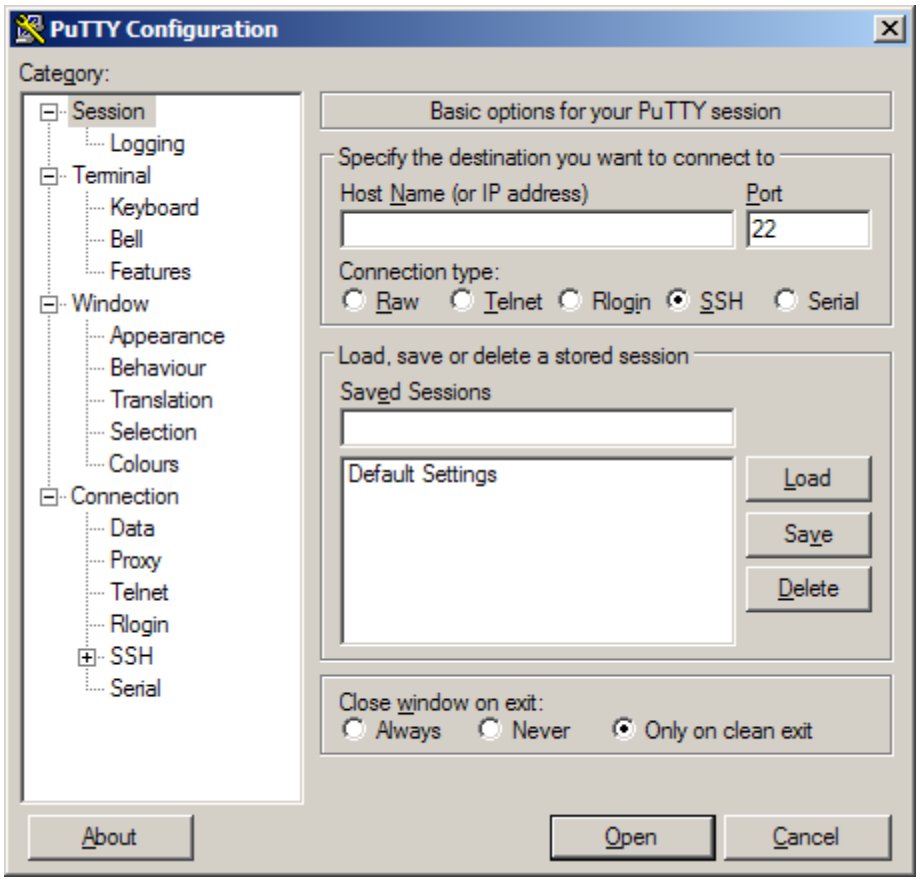
4.2. Running SSH Client (PuTTY)

The following instructions are used to run the SSH Client. Port Forwarding is used to create a secure tunnel to allow the console to connect to the Blackbox Trading System.

1) Runthe putty.exe application. There are several ways to run an application. One way is to use the "Run" command. Click the Windows Start button (lower left corner of screen) and select Run. The following window appears. Enter the application to be run: c:\putty\putty.exe

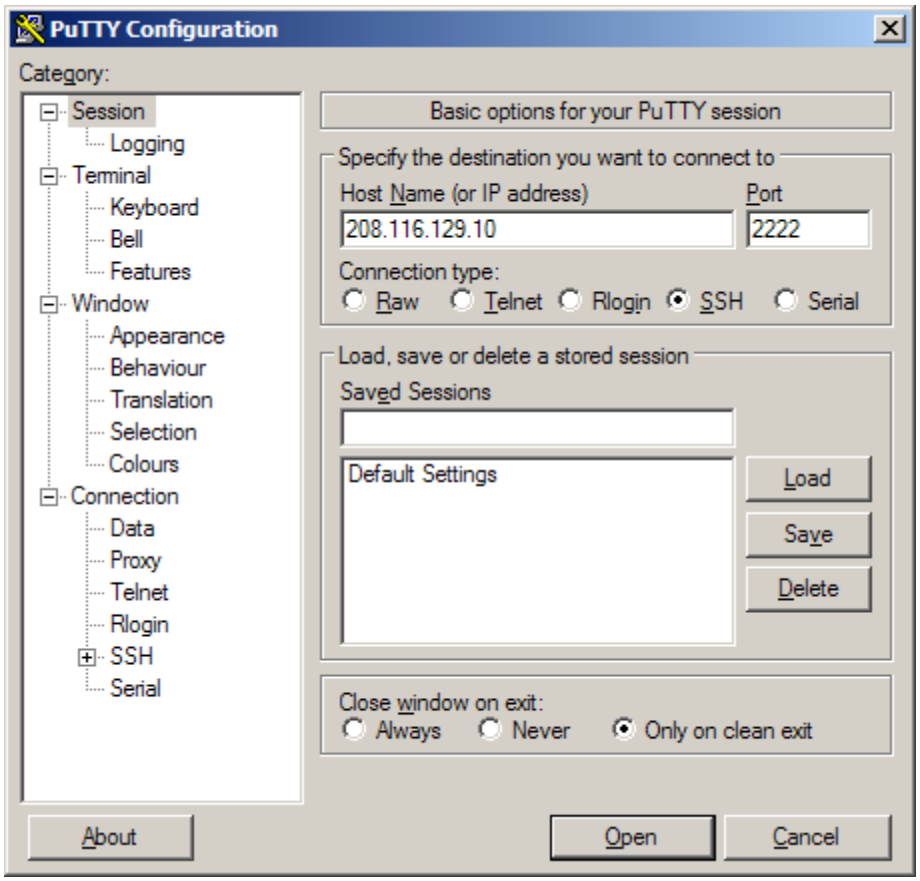


2) When putty is run the following window appears

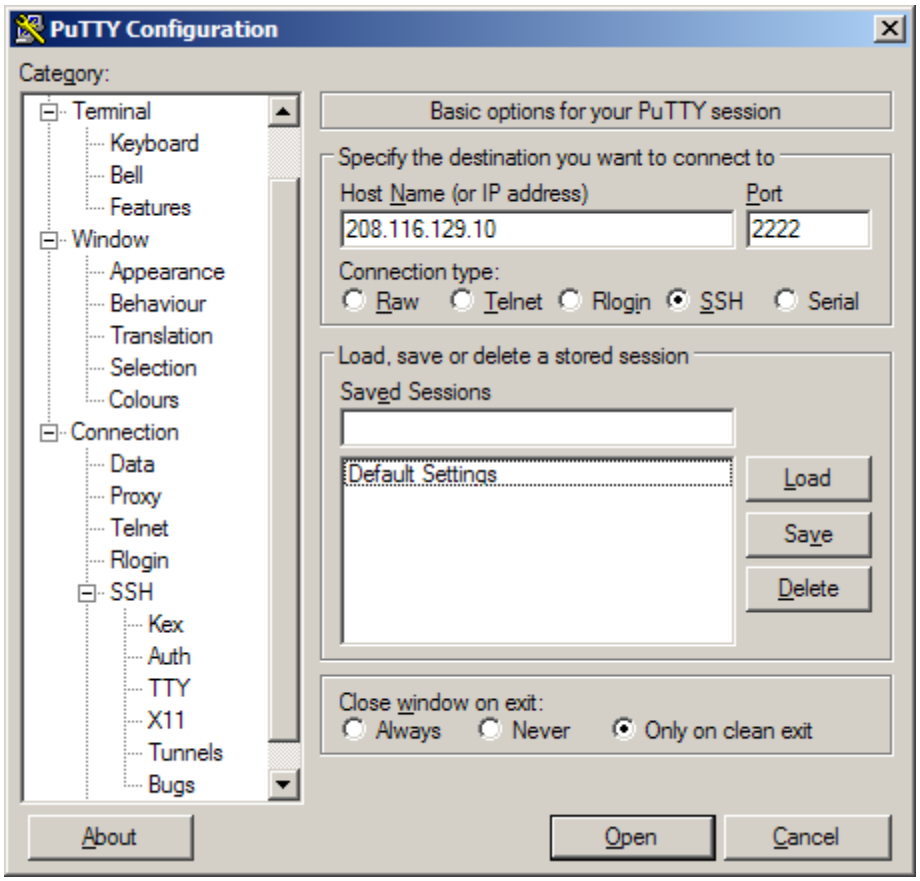


3) Enter the IP address and port number of the Linux system the Blackbox Trading System runs on. If the Linux system the Blackbox Trading System runs on is located in the Lightspeed data center, then the Lightspeed Operations Team will provide the IP address and port number when the system is installed in the Lightspeed data center. Enter the IP address in the Host Name (or IP address) box (208.116.129.10). Enter thb

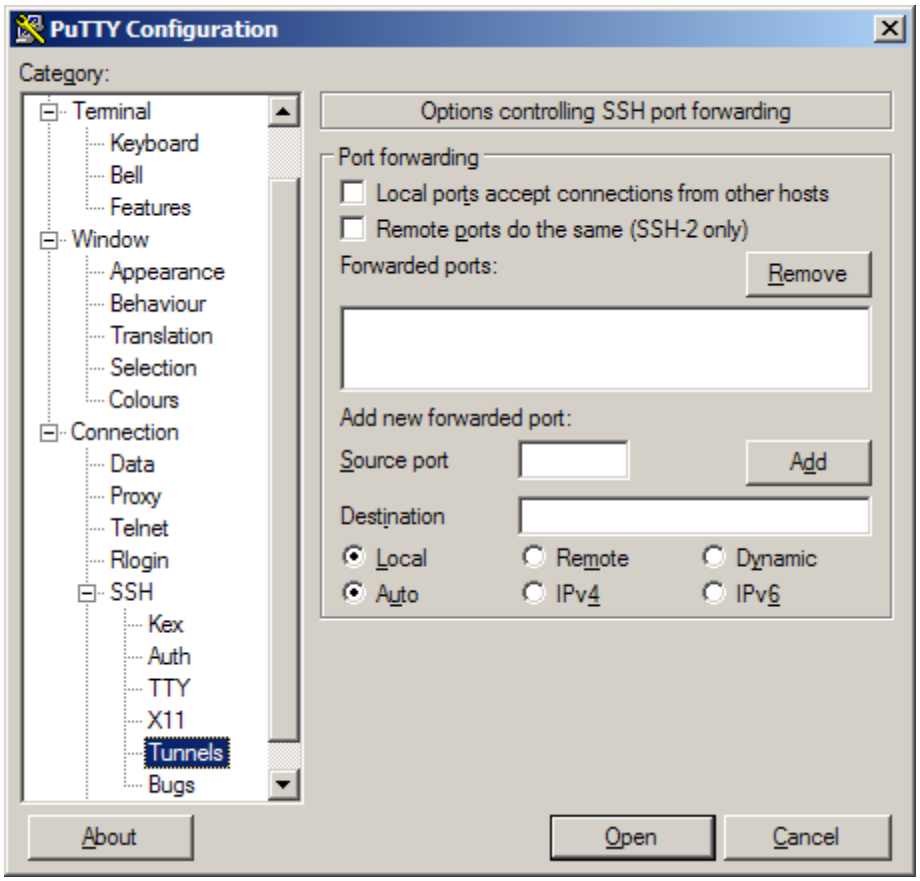
4) e port number in the Port box (2222). See the figure below.



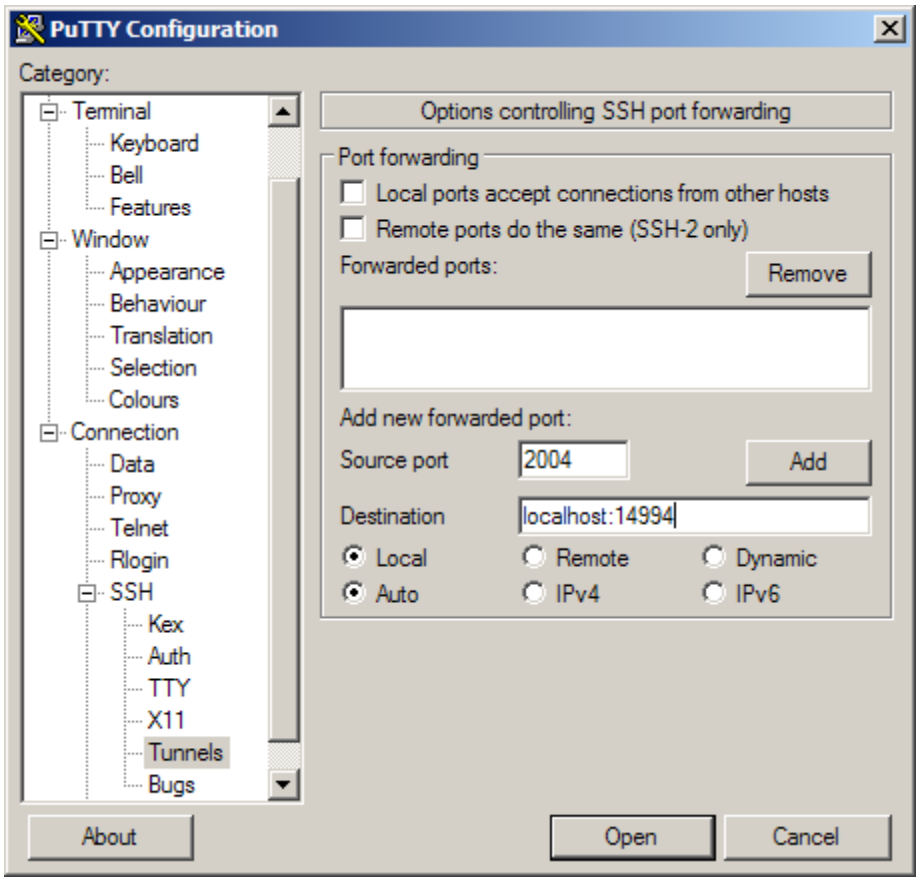
5) Next expand the SSH item in the Category Tree on the left side of the window. See the figure below.



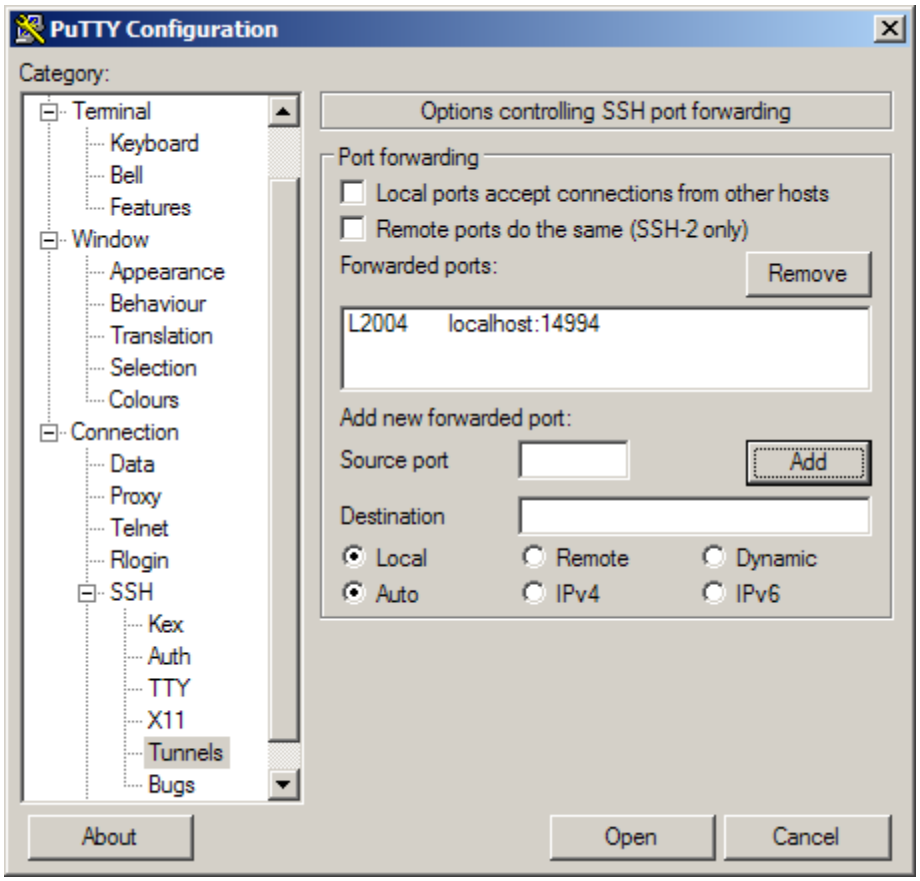
6) Select Tunnels under the SSH item and the following window appears.



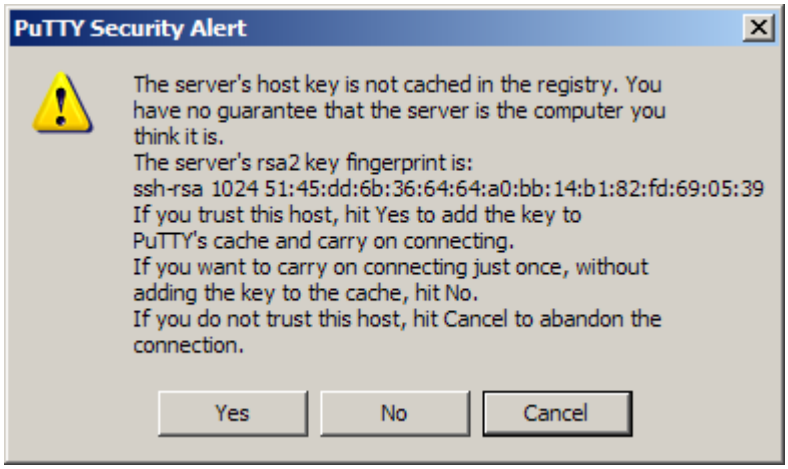
7) Enter the port number (2004) that the SSH Client will accept local connection on in the Source port box. Enter localhost:14994 in the Destination box. 14994 is the port number the Blackbox Trading System will accept connections on. See the figure below.



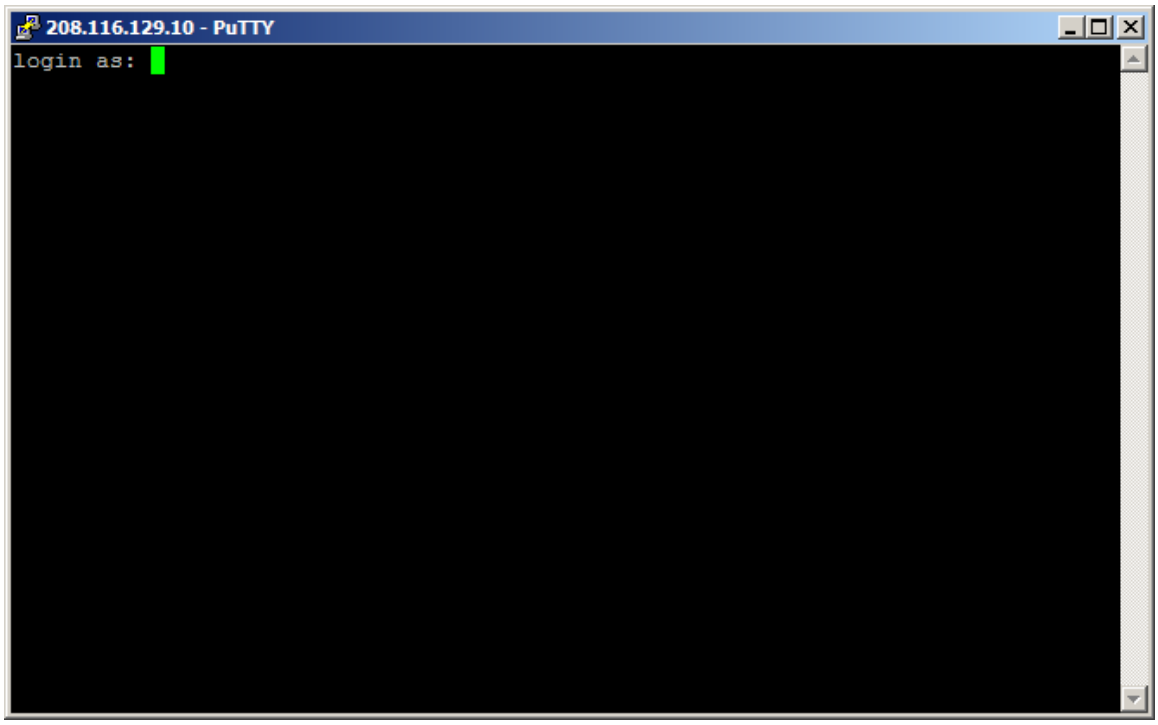
7) Click the Add button. This will cause L2004 localhost:14994 to be displayed in the Forwarded ports box. See the figure below.



8) Click the Open button. The following window appears.



9) Click the Yes button. The following window appears.



10) The user is being prompted to log into the Linux system that the Blackbox Trading System runs on. Enter the account and password when prompted.

At this point, a secure tunnel has been created. The console can be started. When making a console connection to the Blackbox Trading System enter the following IP address and port number.

IP ddress: 127.0.0.1 (Local IP address)
Port number: 2004

The following figure is the dialog box the console displays to allow the operator to enter the IP address and port number to connect to the Blackbox Trading System.