Virtual Loaner Program

Connecting to your VLP System
A User Guide

Total Pages: 22
Document Version 1.1

October 20, 2005

Table of Contents

Change History:

Version	Change Summary	Date
1.0	Initial release	10/10/05
1.1	Minor corrections to SSH section	10/20/05

Reserved System Login Information Form

There are two ways that you can connect to the VLP Network: either using the VPN Appliance or the SSH Gateway. Once you are connected to the VLP Network you must use an SSH client (for AIX and Linux) or a tn5250 client (for i5/OS) to access your VLP system.

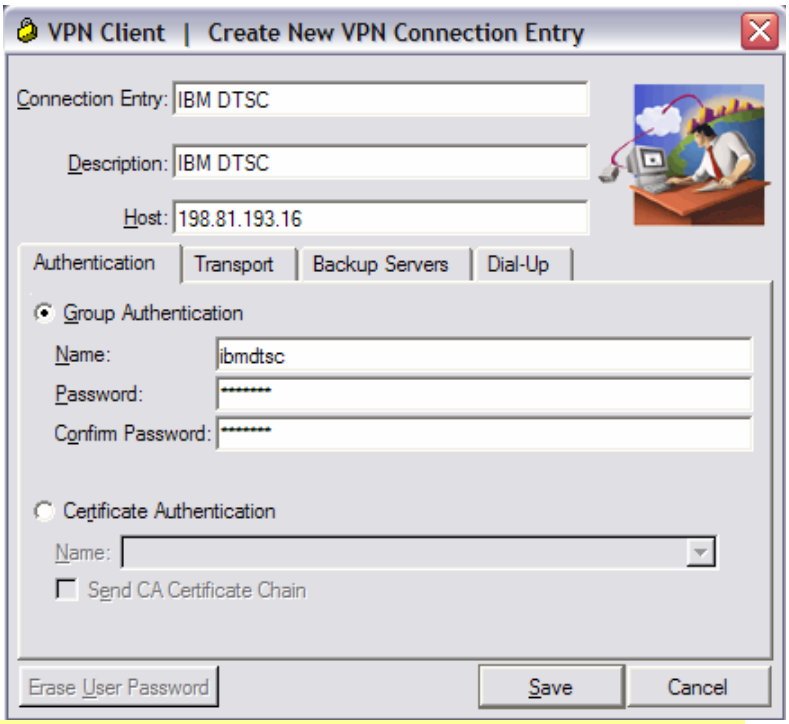
The following table is provided for you to record your reserved system login information:

	Initial	Changed	Changed
Date:			
User ID:			
VPN Appliance IP Address:	198.81.193.16		
SSH Gateway IP Address:	198.81.193.104		
VPN Password:			
SSH Password:			
VPN Client Group Name and Password:	ibmdtsc		
Project Name:			
Res ID:			
Operating System:			
IP Address:			
User Password:			
Root Password:			
Project Name:			
Res ID:			
Operating System:			
IP Address:			
User Password:			
Root Password:			
Project Name:			
Res ID:			
Operating System:			
IP Address:			
User Password:			
Root Password:			
Project Name:			
Res ID:			
Operating System:			
IP Address:			
User Password:			
Root Password:			
Project Name:			
Res ID:			
Operating System:			
IP Address:			
User Password:			
Root Password:			

Where to get your Reserved System Information: User id, Password, and IP Addresses

1. The VNP Client Group Authentication Name and Password are:

   Name: ibmdtsc
   Password: ibmdtsc
   Confirm Password: ibmdtsc

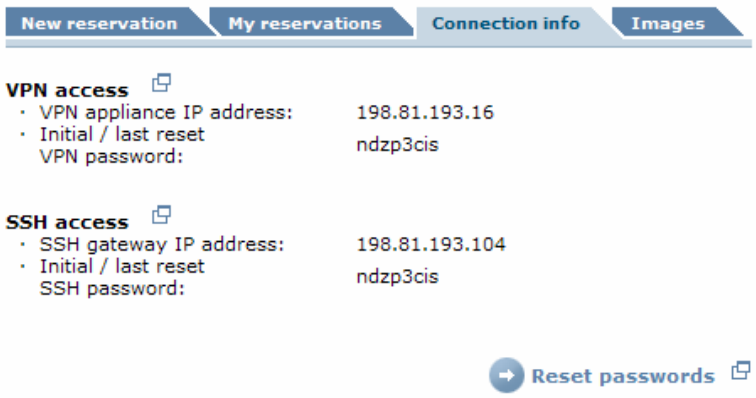


Note: You must use VPN Client Version 4.6.02 or greater

2. The VPN Appliance and SSH Gateway initial and last reset Passwords and IP Addresses are available on the Connection Info page at:

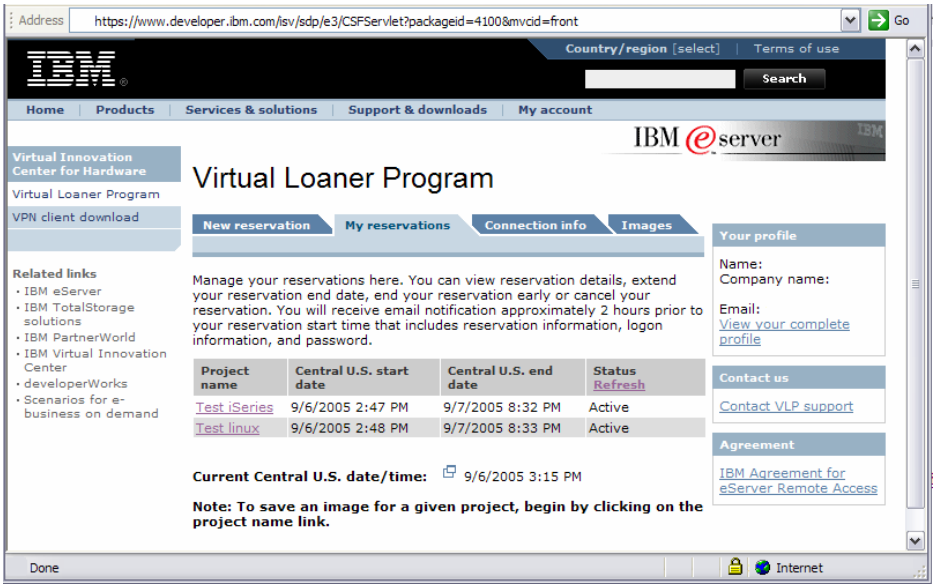
   https://www.developer.ibm.com/sdp/e3/CSFServlet?packageid=4100&mvcid=front

   a. Log in with your PartnerWorld User Id and Password.
   b. Click on the Connection info Tab.
   c. The VPN and SSH Gateway IP Address and your passwords will be displayed as follows:

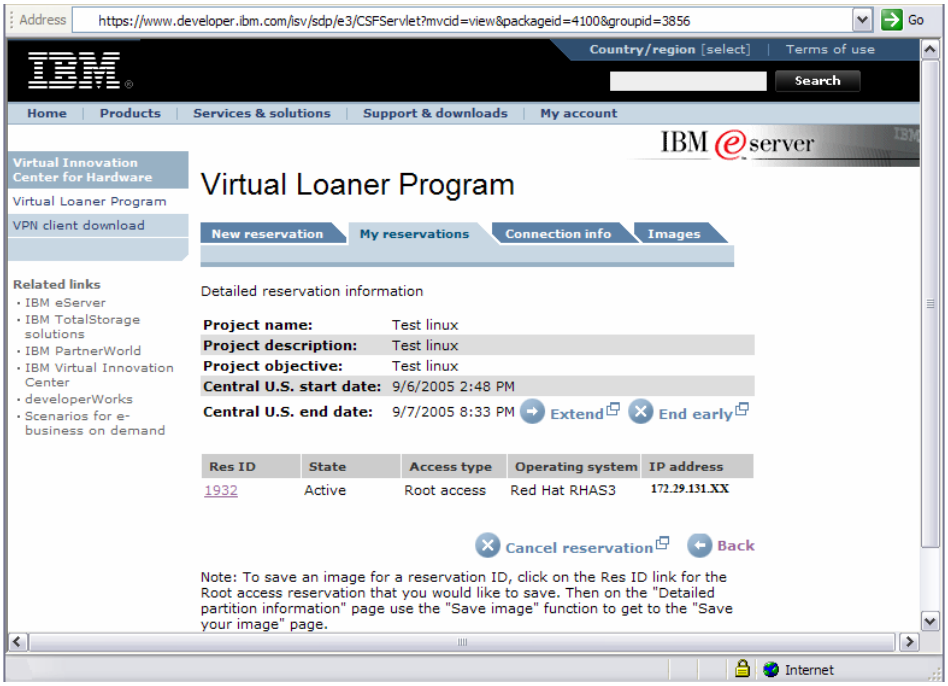


   Note: a button is provided should you need to reset your VPN or SSH passwords.

3. To obtain your Reserved VLP Server's IP Address click the "My reservations" tab and click on the Project Name that you would like to work with.



4. Click the "Res ID" number for each reservation within the project.



5. Your IP Address, User id, and Initial password (user, and root (if applicable)) are displayed. Record your information on the **Reserved System Login Information Form.**

New reservation | My reservations | Connection info | Images

Detailed partition information

Res ID:	1074	Reset partition
State:	Active	
Access type:	Root access	
Operating system:	AIX 5.3	Reset OS
Architecture:	POWER 5 on pSeries	
CPUs:	1	
Memory(GB):	2	
Disk space(GB):	20	
Saved image info:	Image not saved	Save image
IP address:	172.29.136.8	
User id:	u0000203	
Initial / last reset passwords:		Reset passwords
User password:	fmpi2zol	
Root password:	rczw3gja	

Note, you may reset your system password(s) or reset your partition or OS from this screen should this become necessary. Additionally you can initiate a Save Image beginning from this page.

Connecting to the VLP Network Using the VPN Appliance.

There are two ways that you can connect to the VLP Network: either using the VPN Appliance or the SSH Gateway. Once you are connected to the VLP Network you must use an SSH client (for AIX and Linux) or a tn5250 client (for i5/OS) to access your VLP system.
The following instructions explain how to connect to the VLP Network through the VPN Appliance.

How to get the VPN Client – you must use v4.6.02 or higher

1. The VPN client is available at (Note: you will be required to enter your PartnerWorld ID and Password):

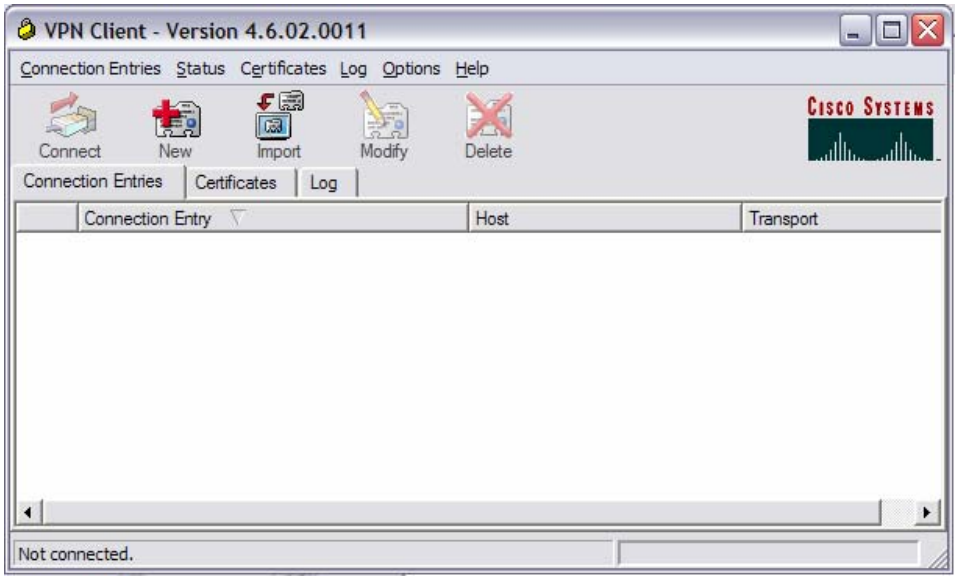
   https://www.developer.ibm.com/isv/sdp/e3/CSFServlet?mvcid=front&packageid=4110

   It also may be found on the left hand side of the reservation management pages by clicking on "VPN client download".

2. Select and download the appropriate client for the operating system that you are running on your local machine.
3. Install the client (Note: this may require that your system be rebooted).

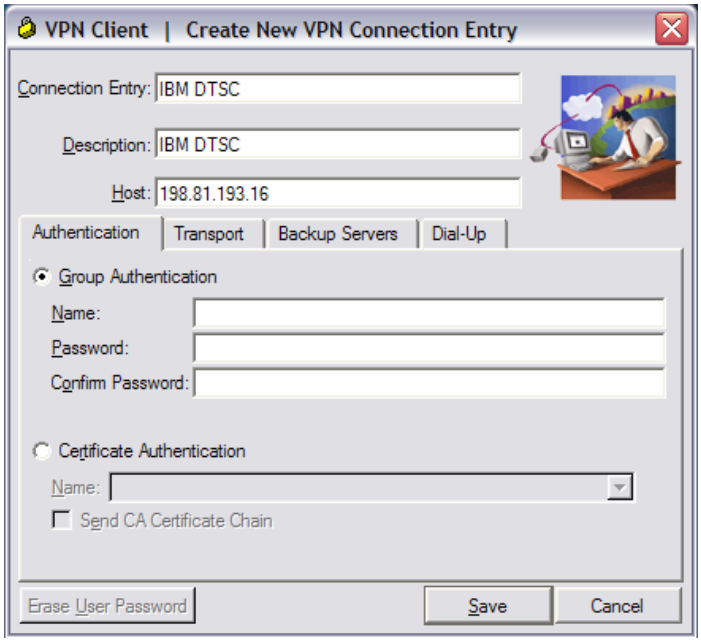
How to Configure the VPN Client

1. After the VPN Client has been installed and the System is rebooted, go to the Windows taskbar, Click on the Start button, Go to Programs, CISCO Systems VPN Client, and select VPN Client.
2. The VPN Client program will start and you will see this window pop up.

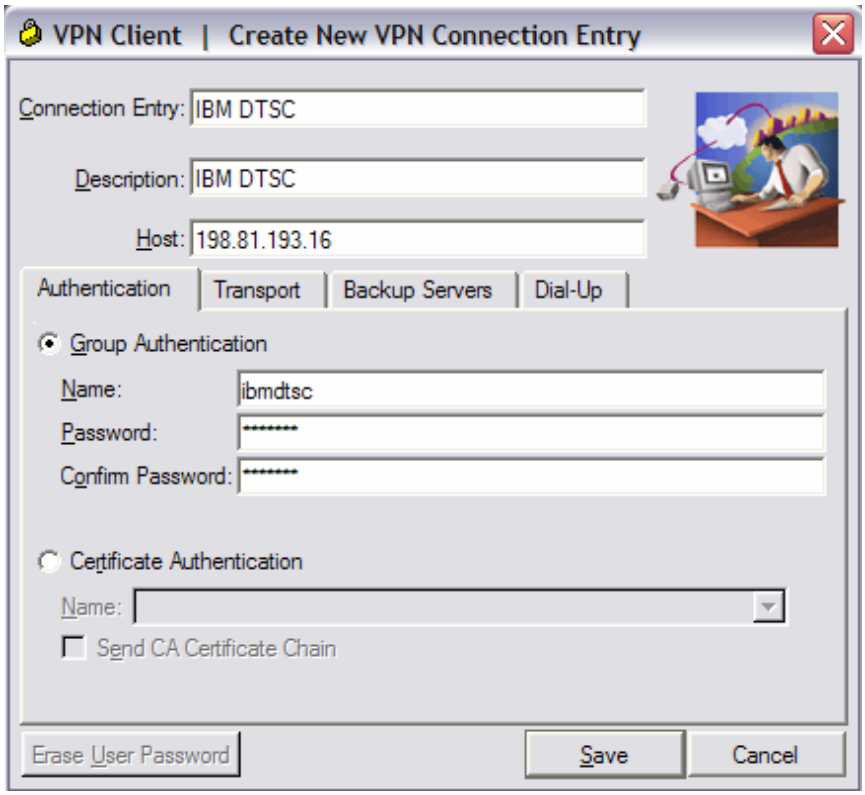


3. Click on the New icon

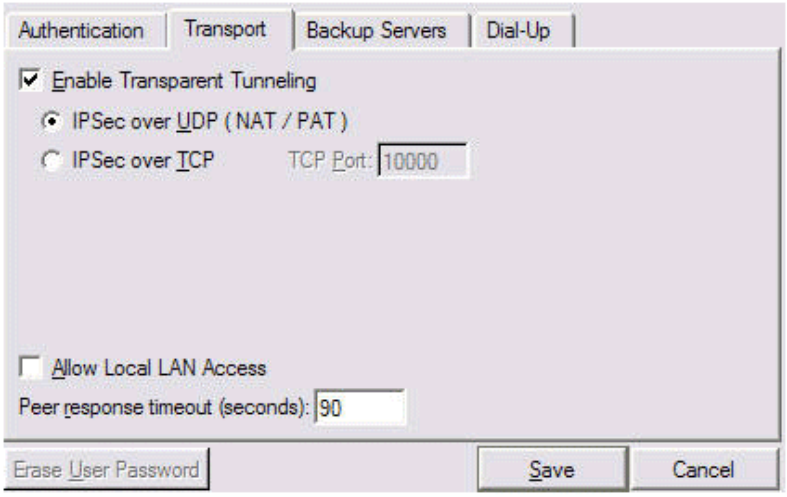
4. Now enter IBM DTSC in the Connection Entry box. This is a name for the connection you are creating. Enter IBM DTSC in the Description box. This is a description for your connection. In the Host box, enter the IP address of 198.81.193.16.



5. Next configure the Authentication for your client. Go to the Group Authentication Section under the Authentication Tab. Type in the GROUP Name and Password EXACTLY as shown below:
   Name: ibmdtsc
   Password: ibmdtsc
   Confirm Password: ibmdtsc



9. Click on the Transport tab. Select the "Enable Transparent Tunneling" AND "IPSec over UDP (NAT/PAT)". Troubleshooting: If IPSec over UDP (NAT/PAT) doesn't work for you, try the IPSec over TCP option. (Both are supported by the VLP.)



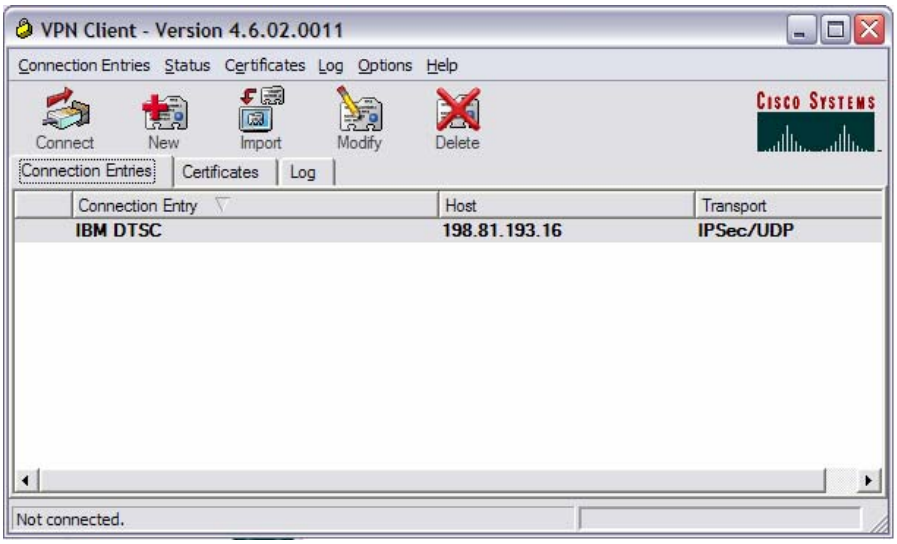
11. Click on the Save button.

Connecting with the VPN Client

Note: this example is specific to the Windows Client
(this will be similar for Linux, Macintosh, and Solaris clients)

1. From the Windows taskbar, go to Start, Programs, CISCO System VPN Client, and select VPN Client or alternatively locate the VPN client on your desktop.

2. Select the IBM DTSC line and click on the Connect icon:



3. A window should pop up that says VPN Client | User Authentication for "IBM DTSC".

Enter your user name and password.

4. Once you have entered your username and password, you will see a small lock in the bottom right corner of your task bar indicating you now have a VPN connection. 

5. Depending upon which operating system you have selected for your reservation, you may now connect to your system's IP Address.

How to Connect to your System once connected to the VLP Network through the VPN Appliance:

Once Connected to the VLP Network through VPN, Access AIX Systems as follows:

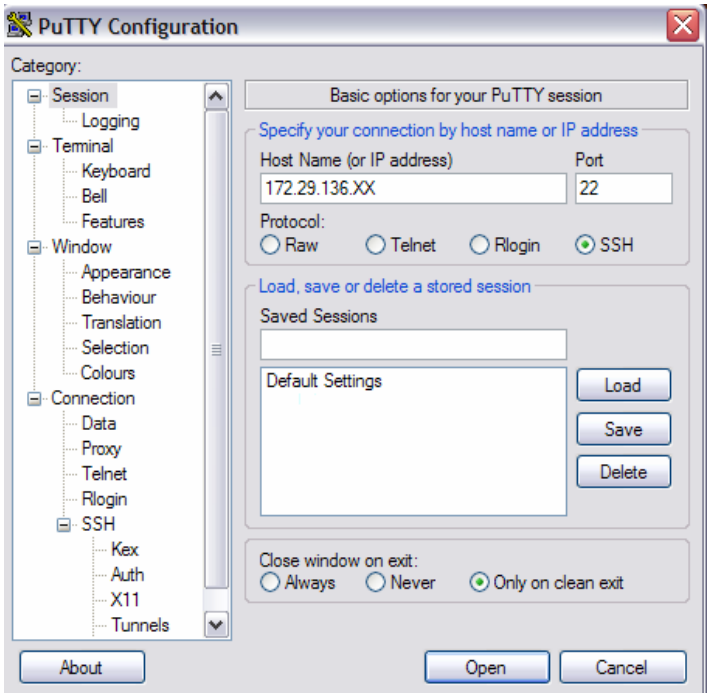
The following instructions explain how to connect to your VLP AIX system after you are connected to the VLP Network. Most Linux distributions include an SSH client. AIX has a SSH client on the "bonus" CD. Windows systems can use the PUTTY client, available at:

http://www.chiark.greenend.org.uk/~sgtatham/putty/

See Appendix B for information on the installation and usage of PuTTY.

IBM does not make any recommendations about the use of this client. Please read the documentation and disclaimers that come with it.

1. Use PuTTY or another SSH client to connect to your system (Telnet is not enabled on VLP systems).
2. Start PuTTY or another SSH Client (this example illustrates using PuTTY). Enter the IP address of your machine in the Host Name (or IP address) and select SSH under Protocol.



Press the Open button and a new SSH session will open up. Log in with your User id and password.

You may be prompted to change your password. Enter your OLD password first, then enter your NEW password twice. Record your new password in the **Reserved System Login Information Form.**.

You have now successfully completed connection to your reserved VLP server.

Once Connected to the VLP Network through VPN, Access iSeries i5/OS Systems as follows:

There are two ways that you can connect to the VLP Network: either using the VPN Appliance or the SSH Gateway. Once you are connected to the VLP Network you must use a tn5250 client or an SSH client to access your VLP system.

Once logged into the VPN you can connect to your i5/OS system by using the 5250 emulator (recommended) or an SSH client. The following describes how to use the tn5250 emulator.

1. **How to obtain a tn5250 emulator client**.

   a. You can use the 5250 emulator from iSeries Access or IBM Personal Communications.

   b. An additional site for the tn5250 client is:

      http://sourceforge.net/project/showfiles.php?group_id=27533

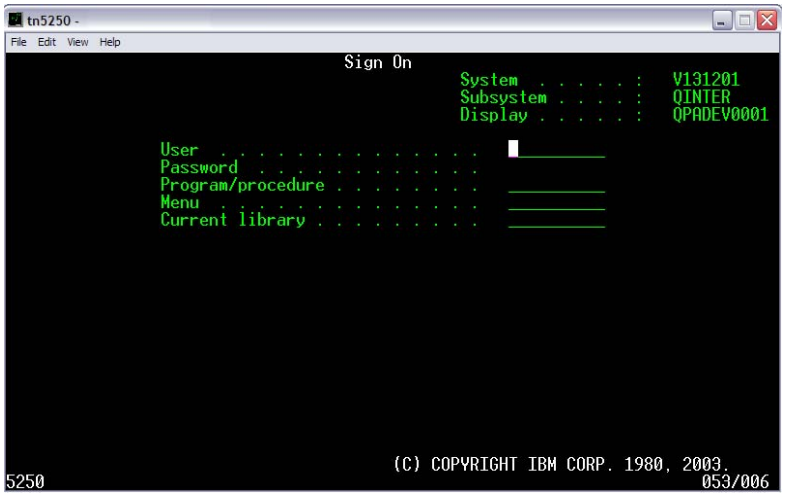
      IBM does not make any recommendations about the use of this client. Please read the documentation and disclaimers that come with it.

2. **How to Connect to your system with the tn5250 emulator client.**

   a. First, connect to the VPN as described in earlier steps.

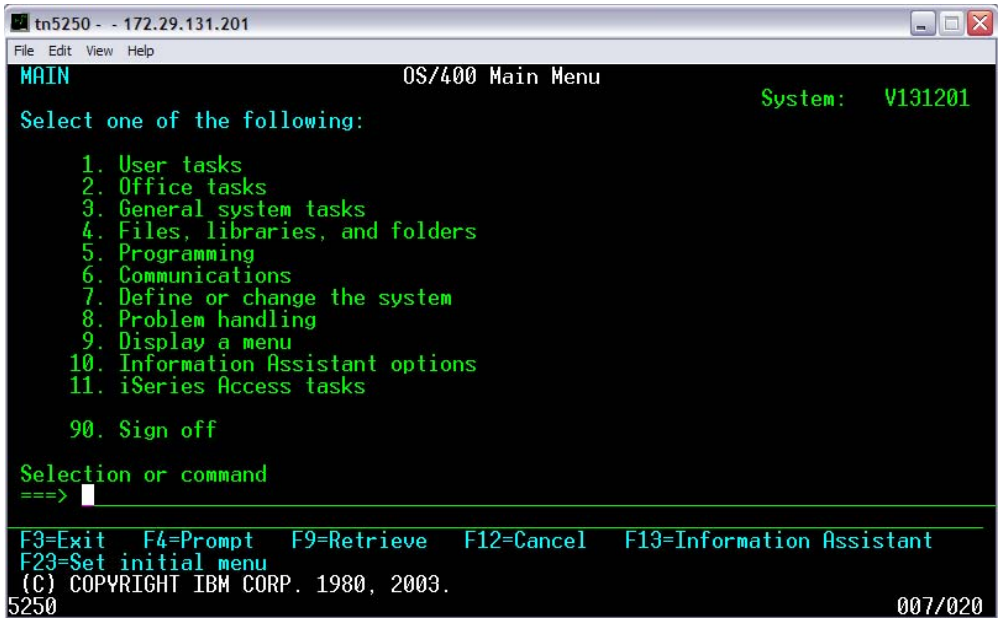
   b. Now, start your 5250 emulator client and enter the IP address of the reserved VLP server

   c. Enter your User id and log in with the reserved VLP server User id or QSECOFR..



d. You may be prompted to change your password. Enter your OLD password first, then enter your NEW password twice. Record your new password in the **Reserved System Information Login Form.**.

e. You are now logged into your reserved VLP server and can proceed with exploring the server.

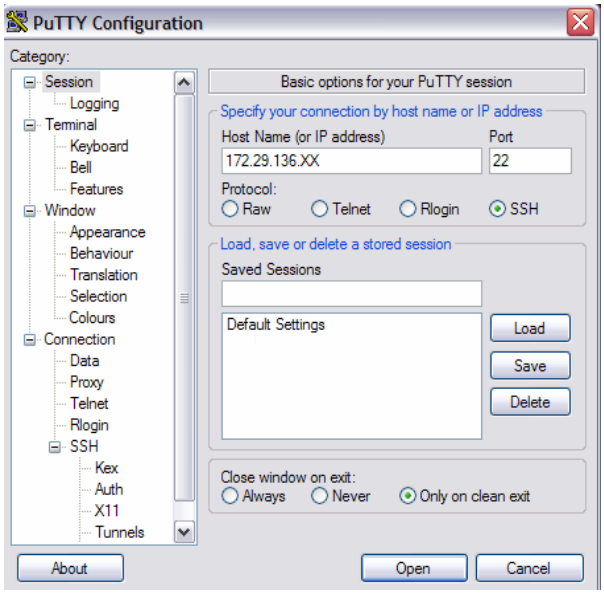


You have now successfully completed connection to your reserved VLP server.

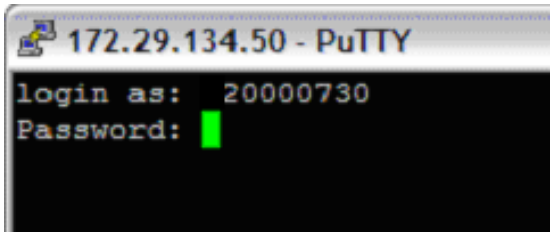
Once Connected to the VLP Network through VPN, Access Linux Systems ONLY as follows:

Once logged into the VPN appliance you can connect to your Linux system by using an SSH client. The following describes how to use the PuTTY SSH client.

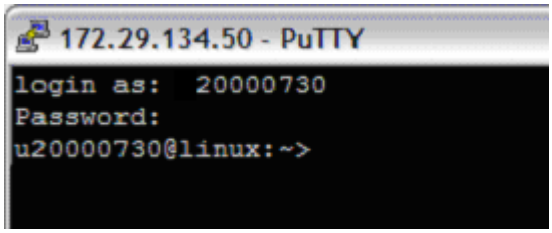
1. Once connected to the VPN appliance you may log into your LPAR**.**
2. Now that you have your Reserved VLP Server User id and password, you can use PuTTY or another SSH client to connect to your system. Telnet is not enabled on VLP systems. See Appendix B for information on the installation and usage of PuTTY.
3. Start PuTTY or another SSH Client. Enter the IP address of your machine in the Host Name (or IP address) box and select SSH under Protocol.



4. Press the Open button and a new SSH session will open up. Log in with your User id and password.



5. You are now able to log into your LPAR and perform testing or installation of software that you wish using the User Id and Password obtained in **Step 3** and **Step 4**.



You have now successfully completed connection to your reserved VLP server.

Connecting with the SSH Client to the SSH Gateway rather than using the VPN Appliance:

It is recommended that you use the VPN Appliance to connect to the VLP Network, however, if this is not an option for you then you may connect via the SSH Gateway. The following instructions explain how to connect to the VLP Network via the SSH Gateway rather than using the VPN Appliance.

SSH Gateway Connection Instructions:

1. Obtain the SSH client. Most Linux distributions include an SSH client. AIX has a SSH client on the "bonus" CD. Windows systems can use the PUTTY client, available at:

   http://www.chiark.greenend.org.uk/~sgtatham/putty/

   IBM does not make any recommendations about the use of this client. Please read the documentation and disclaimers that come with it.

2. Start the SSH client session and connect to the SSH gateway IP address by entering 198.81.193.104 as the Server Address.

3. Enter your user id and SSH Gateway password at the Login as: prompt.

   - The first time you connect through the SSH gateway on a new reservation, you will be asked to change your password. PLEASE MAKE NOTE OF YOUR NEW PASSWORD, VLP DOES NOT KEEP TRACK OF THIS NEW PASSWORD.
   - When prompted, re-enter the ORIGINAL password
   - Now enter the NEW password, and then confirm the NEW password by entering it again.

4. You are now logged into the VLP Network via the SSH gateway and should see the "$" prompt. You are not yet logged into your VLP System, just the VLP Network.

5. Now that you are in the VLP Network you will connect to your VLP System. Using the SSH gateway, you can login to your reserved VLP server by either direct access to the server from the gateway, or by creating and using an SSH tunnel for your server. An SSH tunnel enables you to secure copy (scp) and secure ftp (sftp) to your reserved VLP server. You only need to create a tunnel at the start of each session with a server.

Creating an SSH tunnel to access your reserved VLP server (you need to do this at the start of each session with your VLP server):

1. Choose a port number between 20000-20099. If the port chosen is already in use, please select a different port number and try again. REMEMBER THIS PORT NUMBER, IT WILL BE USED AGAIN. Type the following command in the existing SSH session.

   ssh -gL <tunnel_port>:<reserved_server_ip_address>:22 <reserved_server_user_id>@<reserved_server_ip_address>

   example:

   ssh -gL 20099:172.29.131.99:22 20000999@172.29.131.99

2. You will be prompted for your USER password (not your Root password).
3. You have now created an SSH tunnel to your reserved VLP server.
4. Leave this session open. Note: You will start or restart this tunnel session (using the same port) each time you want to access your reserved VLP server via the SSH Tunnel.
5. Proceed to, "Accessing your Reserved VLP server via the SSH Tunnel".

Accessing your Reserved VLP Server via the SSH Tunnel – Do this only after you have created an SSH tunnel:

1. If the session from the previous step has timed out or is closed, use the command in step 1, above to open the tunnel.
2. Start a NEW SSH session.
3. Access your reserved VLP server using the tunnel created earlier, by typing:

   ssh -p <port> <reserved_server_user_id>@<SSH_gateway_IP_Address>

   where <port> is the port number you chose earlier(20099).

   Note: If you are using an SSH client that gives you a Windows type interface, enter the SSH gateway IP address and change the port from the default of 22 to the port you used when creating the tunnel which was (20099).

   Example:

   ssh -p 20099 20000999@198.81.193.104

4. You now have an SSH session to your reserved VLP server. Use this session to perform the functions on your reserved VLP server.

Accessing your Reserved VLP Server with Direct SSH without using a Tunnel:

Note: secure copy (scp) and secure ftp (sftp) are not supported without a Tunnel. If you need to transfer any files then do not use "Direct SSH without using a Tunnel".

1. You should already have a connection to the VLP SSH gateway server. If your connection is inactive or has been closed, connect to the gateway using the information in "SSH Gateway Connection Instructions", above.

2. You will use that SSH session to connect to your reserved VLP server.

3. From your VLP SSH gateway connection, SSH to the VLP reserved server address:

   ssh <reserved_server_user_id>@<reserved_server_IP_Adress>

   example (use the original user id provided by VLP):

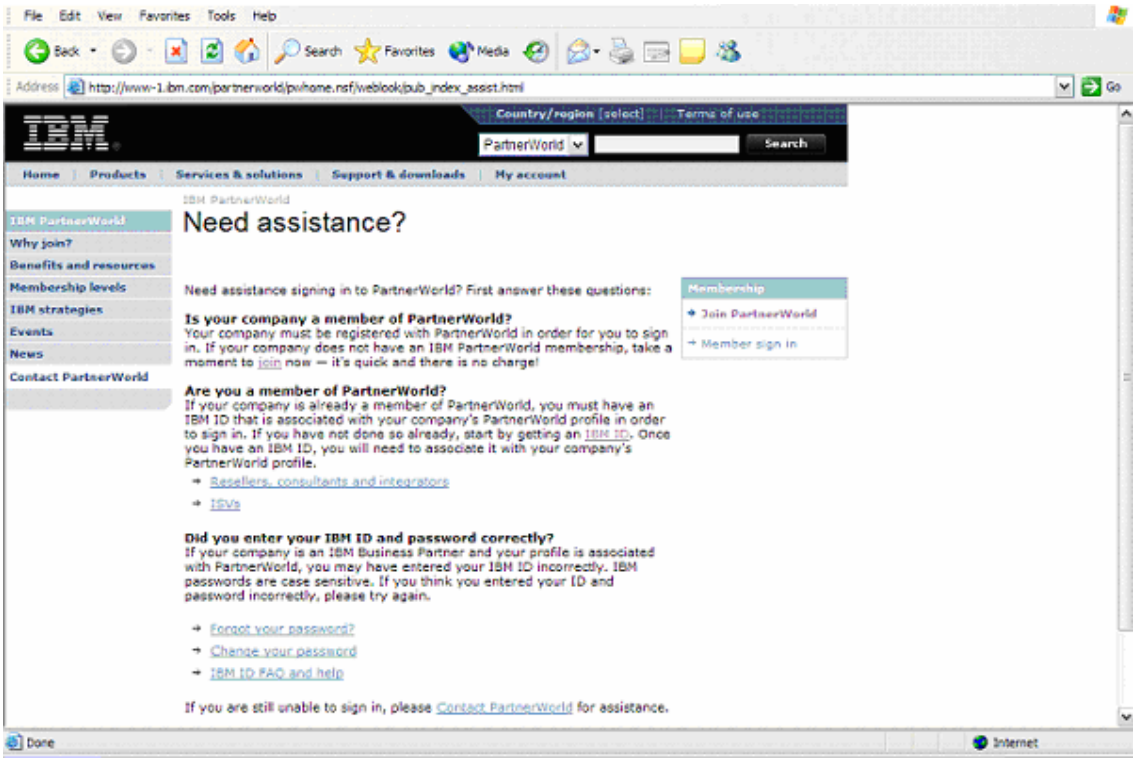
   ssh 20000999@172.29.133.99

Note: The first time you connect to an AIX reserved VLP server, you will be asked to change your password. PLEASE MAKE NOTE OF YOUR NEW PASSWORD. If you lose your password you may reset it from the VLP Reservation management pages.

Appendix A: How to get a PartnerWorld ID & Password

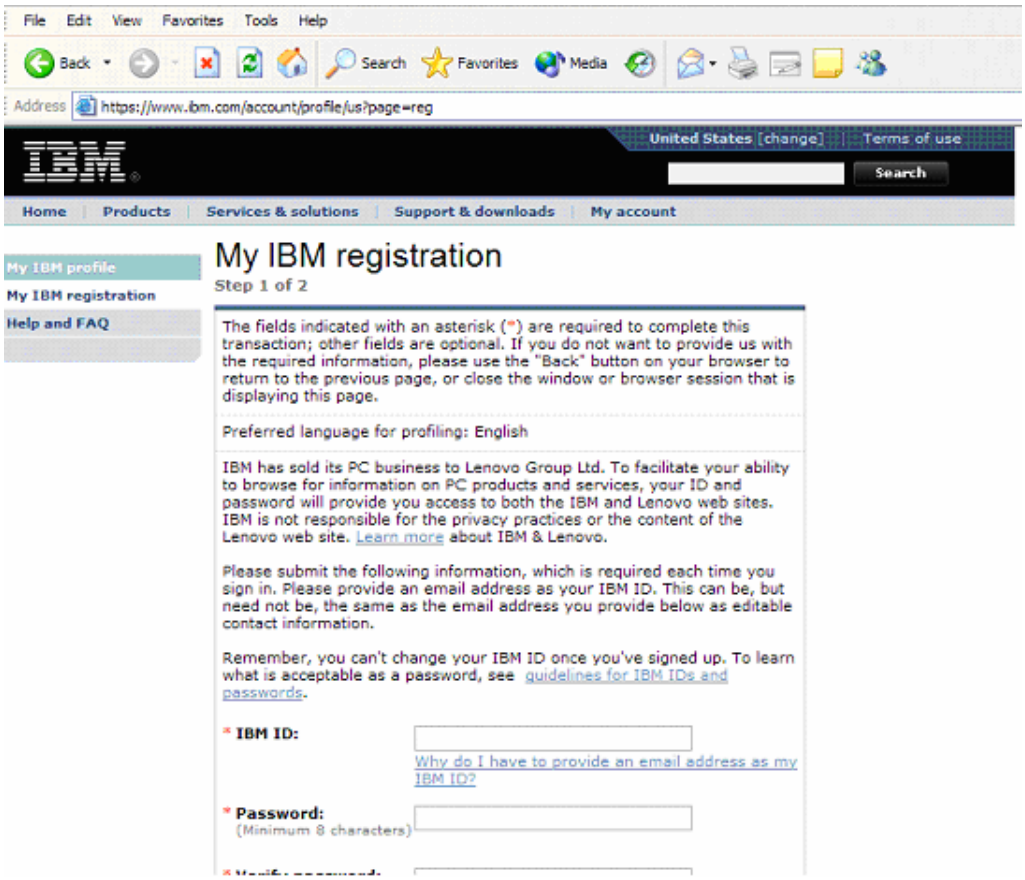
Existing PartnerWorld ID & Password

1. You will need to go to this website to register for an Partnerworld ID: http://www-1.ibm.com/partnerworld/pwhome.nsf/weblook/pub_index_assist.html



2. You must register as a company member of PartnerWorld or become a new member of PartnerWorld.

   https://www.ibm.com/account/profile/us?page=reg



Why do I need an IBM ID?

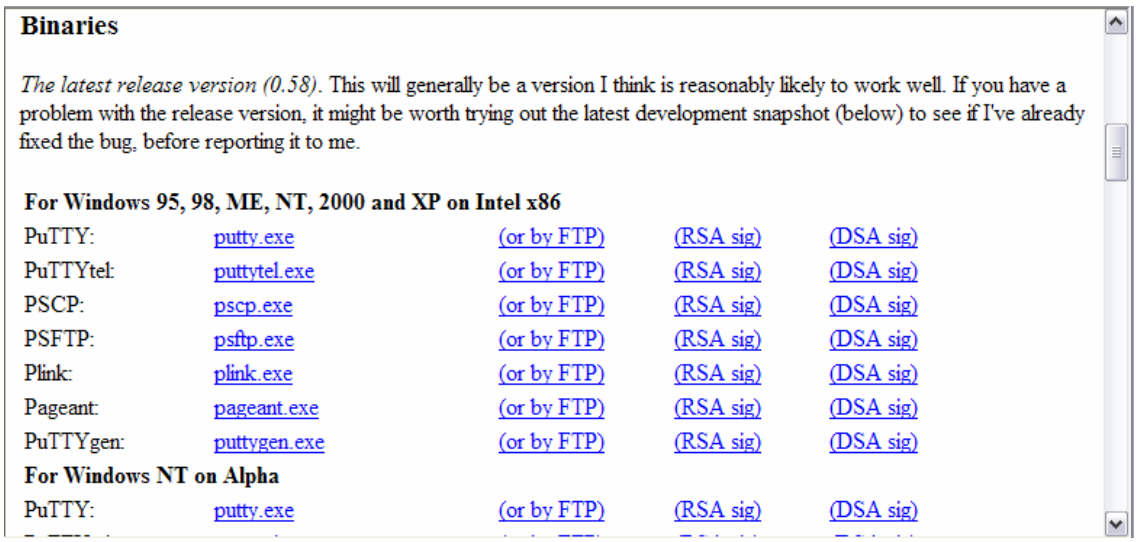
Your IBM Registration ID is your single point of access to IBM web applications that use IBM Registration. You need just one IBM ID and one password to access any IBM Registration based application. Furthermore, your information is centralized so you can update it in a convenient and secure location. The benefits of having an IBM Registration ID will increase over time as more and more IBM applications migrate to IBM Registration

Appendix B: How to Install and Run the PuTTY Client

1. To obtain Putty, you can go to several sites. A suggestion to get Putty is to go to this site:

   http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

2. Scroll down the page and find your operating system. Double click the putty.exe file so you can download the program.



Binaries

The latest release version (0.58). This will generally be a version I think is reasonably likely to work well. If you have a problem with the release version, it might be worth trying out the latest development snapshot (below) to see if I've already fixed the bug, before reporting it to me.

For Windows 95, 98, ME, NT, 2000 and XP on Intel x86

PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel:	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP:	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP:	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)
Plink:	plink.exe	(or by FTP)	(RSA sig)	(DSA sig)
Pageant:	pageant.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYgen:	puttygen.exe	(or by FTP)	(RSA sig)	(DSA sig)

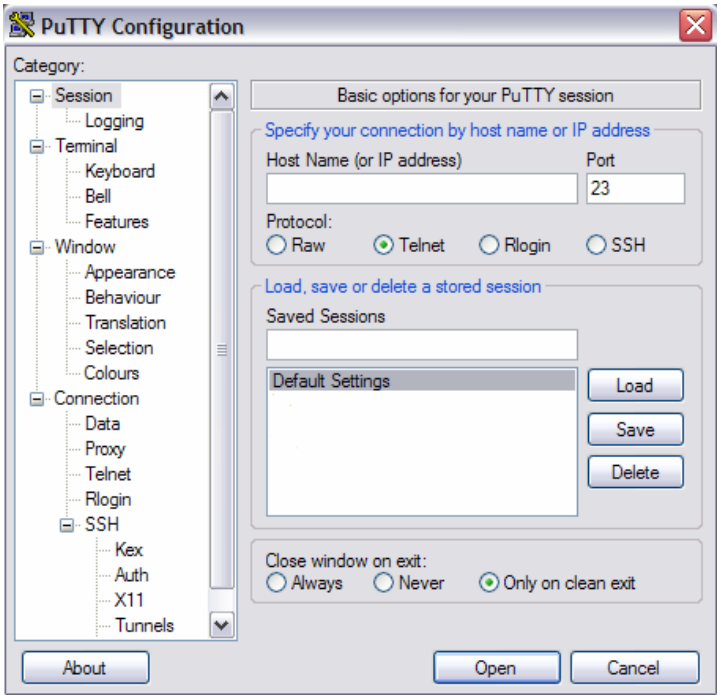
For Windows NT on Alpha

PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)

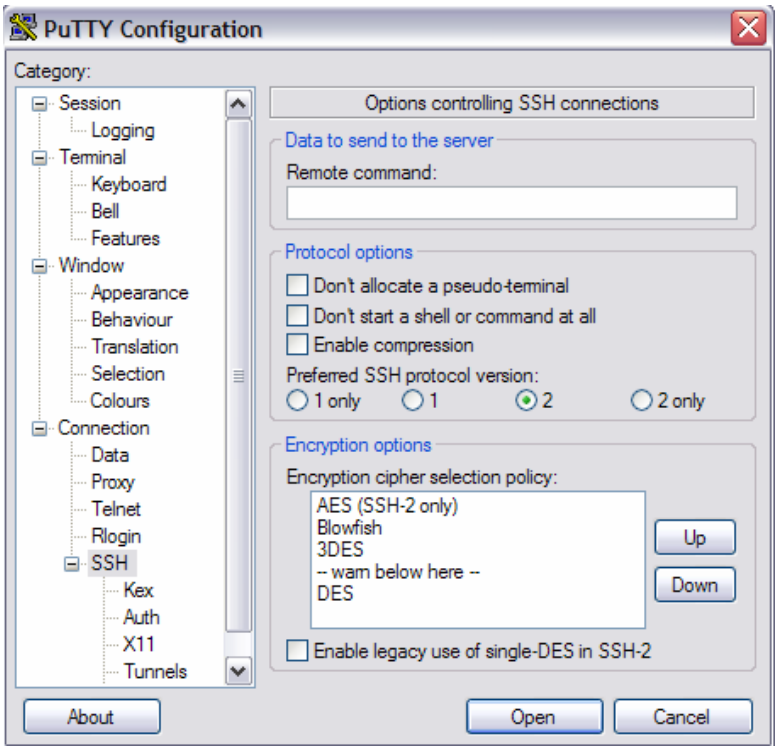
3. A Save File Dialog will pop up. Choose the Option to Save the File. Pick a location to save your file, such as C:\temp.

4. Run Putty by first locating the putty.exe file and double clicking on the putty.exe file to run the program.

5. The Putty Dialog box will pop up.



6. Under Saved Sessions, Select Default Settings, then click on the Load button.
7. Now Under the Category list on the Left hand side, select SSH.
8. You will see this dialog box, under Preferred SSH Protocol Version, Select 2.



9. Under the Category Dialog box on the left hand side, Select Session. Now Select SSH under the Protocol Session.
10. Select Default Setting under Saved Sessions and click the Save button. You now have saved the settings that you have just configured so by default you will use SSH Protocol 2 when you use PuTTY.

Appendix C: What is a Virtual Private Network (VPN)?

A virtual private network (VPN) is private network that uses a public network, such as the Internet, to create a secure private connection through a private tunnel. A VPN uses a virtual connection that is routed from a company's private network through the internet to a remote system or site. The VPN connection creates a secure connection between the user's machine and the remote network giving that user local access to the remote site. The user can then have access to the remote company's network as if they were locally connected to that company's network.