

Configure PuTTY To Create SSH SOCKS Proxy For Secure Browsing

Thursday, 01 May 2008

You need to have a SSH (Secure SHell) account for this to work. If you have not yet done so, Download PuTTY for free.

- Open PuTTY.
- Where it says 'Host Name (or IP address)' and has a box underneath it, enter the name of your SSH host into the box.
- Under 'Saved Sessions' enter a name for this connection that will help you remember it later. For example, you could call it 'SSH Proxy' so you know this will be the proxy connection.
- In the 'Category:' menu on the left, expand the 'Connection' menu list if it is not expanded already. Expand the 'SSH' menu list if that one is not expanded already. Click 'Tunnels' (underneath 'SSH'). This opens the options where you will enter the settings for PuTTY to create the tunnel.
- Under 'Add new forwarded port:' enter 9853
- Where it says 'Destination' leave that field blank but be sure to select the 'Dynamic' option underneath it.
- Click the 'Add' button to add this port.
- In the 'Category:' menu on the left, click the click 'Connection'.
- Where it says 'Seconds between keepalives (0 to turn off)' enter 5 in the box. This will keep your connection alive and prevent it from timing out even when you walk away from the computer for a while.
- In the 'Category:' menu on the left, click 'Session' at the very top to go back to the first screen.
- Click the 'Save' button to save all of the settings you just entered. Later you will not have to enter these settings again in the future, you will only need to load up your saved profile (by double-clicking it after you open PuTTY) every time you wish to connect to the proxy.
- Click the 'Open' button to open the connection to the proxy.
- When connected you will be asked for your username and password. Enter the username and password for your account. Once connected the tunnel is open. After you are finished using the tunnel, type logout and press Enter. Finished. Now you can connect using any SOCKS compatible software by configuring it to use localhost as the proxy server and use port 9853. The reason why you connect to localhost and not the address of the server is because PuTTY has forwarded that port from the server to your computer. Once you connect to localhost, it sends the data right back up through the encrypted tunnel to the server. Keep in mind data that leaves the server and goes out to the Internet is not encrypted unless you are connecting to a secure web site that uses SSL encryption (https://).

Alternative method: If you use PuTTY from the command line, here is a faster way to establish the secure tunnel without having to use any of the steps above:

```
putty.exe -D 9853 username@sshhost and press Enter
```

Just replace username with your actual username and ssh.host with the address of the SSH server. When it logs in you will automatically be asked for your password. Once that is accepted the encrypted tunnel is automatically created on port 9853 on your computer.

Another neat trick for command line users: Rename PuTTY.exe to ssh.exe. Move the newly renamed file to c:\windows\. From then on, all you have to do to establish the tunnel from Windows is click 'Start --> Run...' to open the 'Run' dialogue box and then type ssh -D 9853 username@sshhost and press Enter. Replace username with your real username and ssh.host with the address of the SSH host.

[Click here for instructions on configuring Firefox to use the secure tunnel.](#) You will also find out how to download it if you do not have it already.

[Click here for instructions on hiding the PuTTY window while you are logged on.](#) This can be convenient since you do not need to use it while it is open.

[Click here to sign up for VectroProxy SSH tunnel and go online anonymously.](#) Works just as described above.