

# OpenVPN over SSH tunneling

## Step 1: What you'll need before starting

You're going to need a couple of things in order to create an SSH tunnel that you can use as a SOCKS 5 proxy for tunneling OpenVPN or any application that supports Socks 5. This is useful when OpenVPN traffic is filtered by a your ISP firewall/proxy or double encryption is needed. Here's a short list of things you'll need:

1. A remote server you can connect to using SSH. You will be provided the SSH server IP after your signup
2. A remote OpenVPN server. You will need to signup for our OpenVPN service and OpenVPN client
3. By default our SSH runs on port 443 to enable our users bypass through any firewall/proxy
4. The Putty software, which you can download for free.

Once you have all those things in place we're ready to get started.

## Step 2: Downloading and installing Putty

This step is easy. Just browse to the official Putty website at:

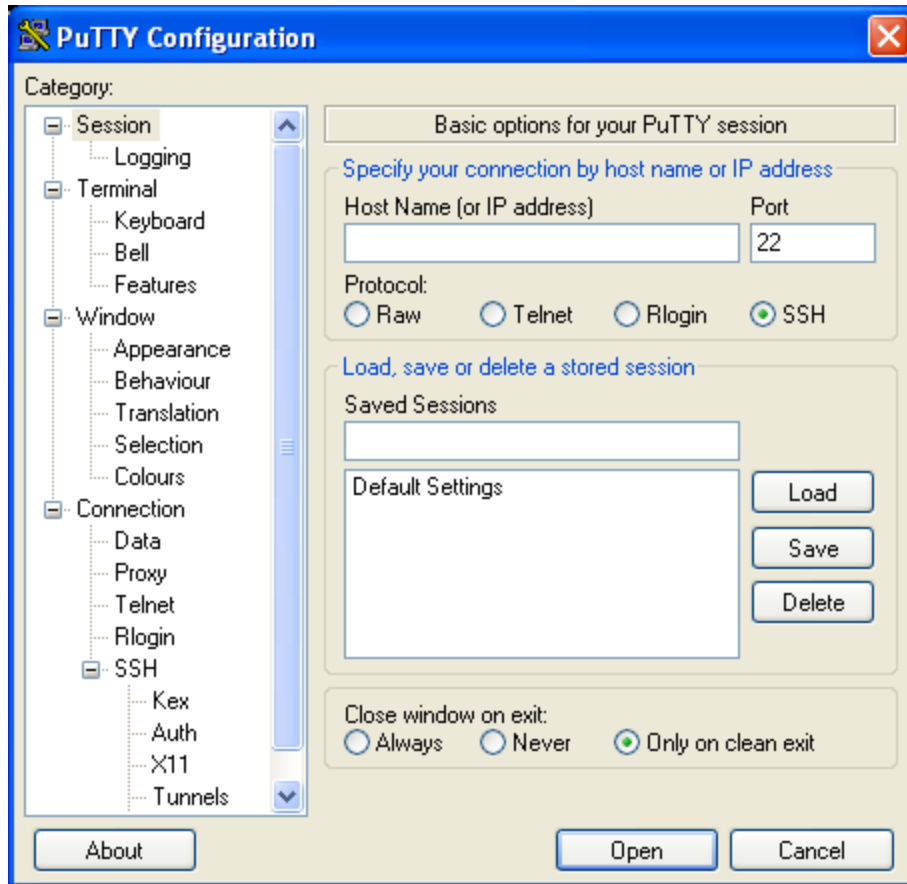
<http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe>,

Then download the putty.exe executable file. As of this writing there is no installation process -- just download it, drop it in a folder, and it's ready to be used.

## Step 3: Configuring a tunnel to your SSH server

Next, we'll use Putty to create an SSH tunnel and connect to your remote server. You will need the SSH server IP which was provided to you when you signed up.

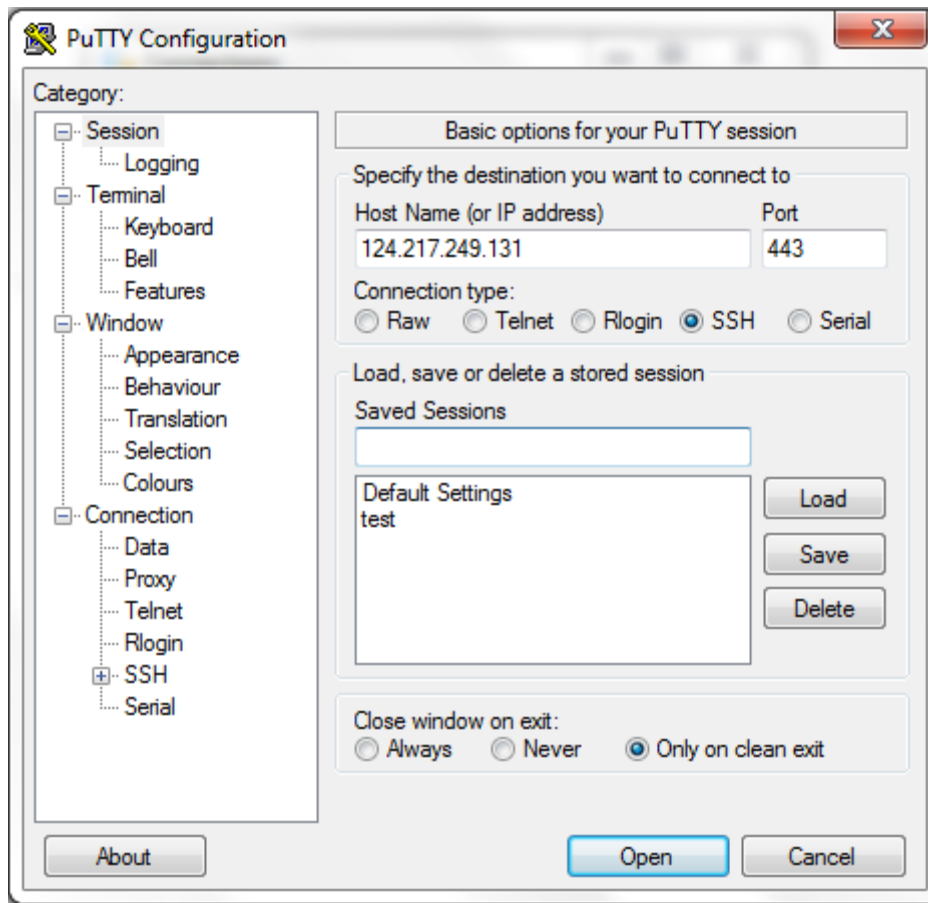
When you start Putty you should see a window that looks like the next figure:



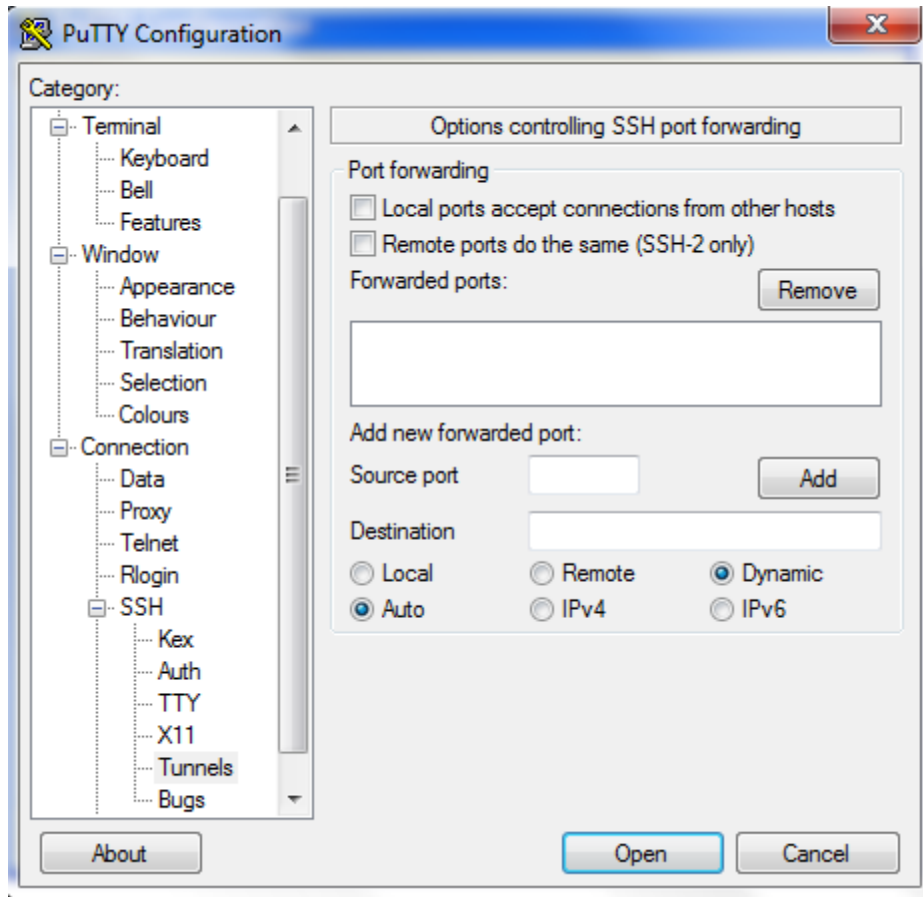
Start Putty, and we'll create a new session configuration that will serve as your tunnel. In the field labeled "Host Name (or IP address)", enter the hostname or TCP/IP address of our remote server.

In the text field labeled "Saved Sessions", enter a name that you want to use to identify this configuration. This is typically the hostname or IP address of the remote server, but it can also be something like "SSH tunnel".

At this point your Putty window should look like the following figure:

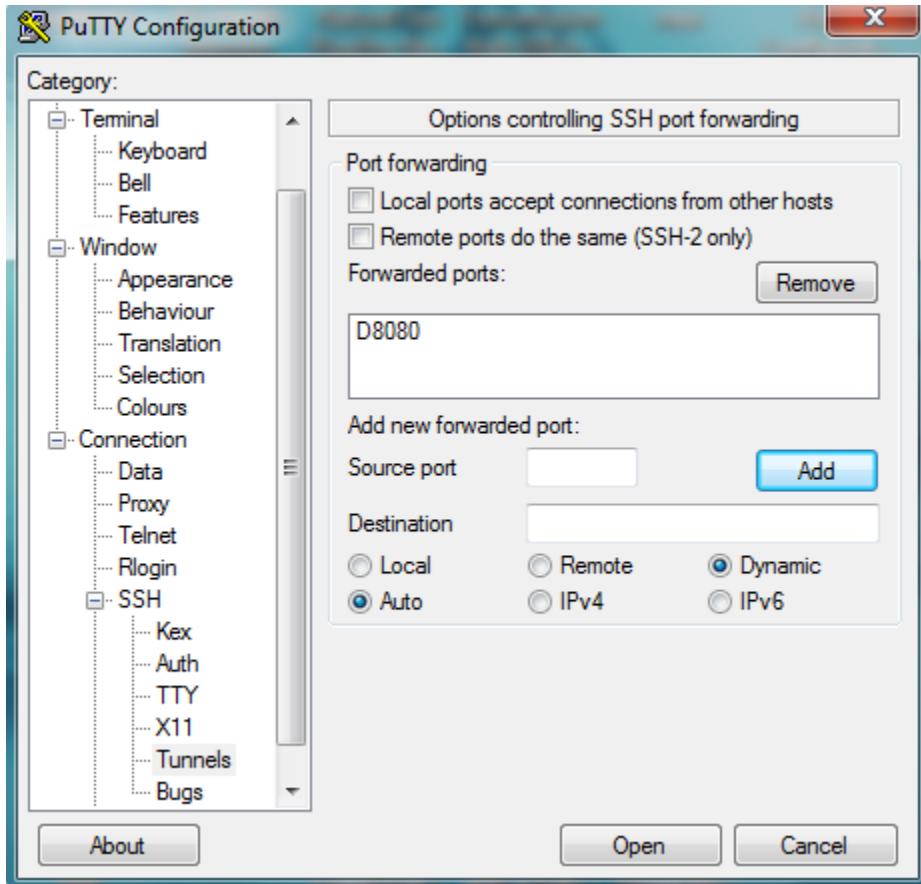


Next, on the left side of the putty window there is a navigation tree. In that tree you want to select the Tunnels item. If this item isn't already visible, you can find it by clicking the Connection node in the tree, then SSH, and then Tunnels. This is shown in the next figure:



Under the section labeled "Add a new forwarded port" type in a port such as 8080 for the source port. Leave the Destination field blank, and then select the Dynamic and Auto radio buttons. Then click the Add button, and you should see the text D8080 show up in the text area just above the "Add a new forwarded port".

Your Putty window should now look like the next figure:

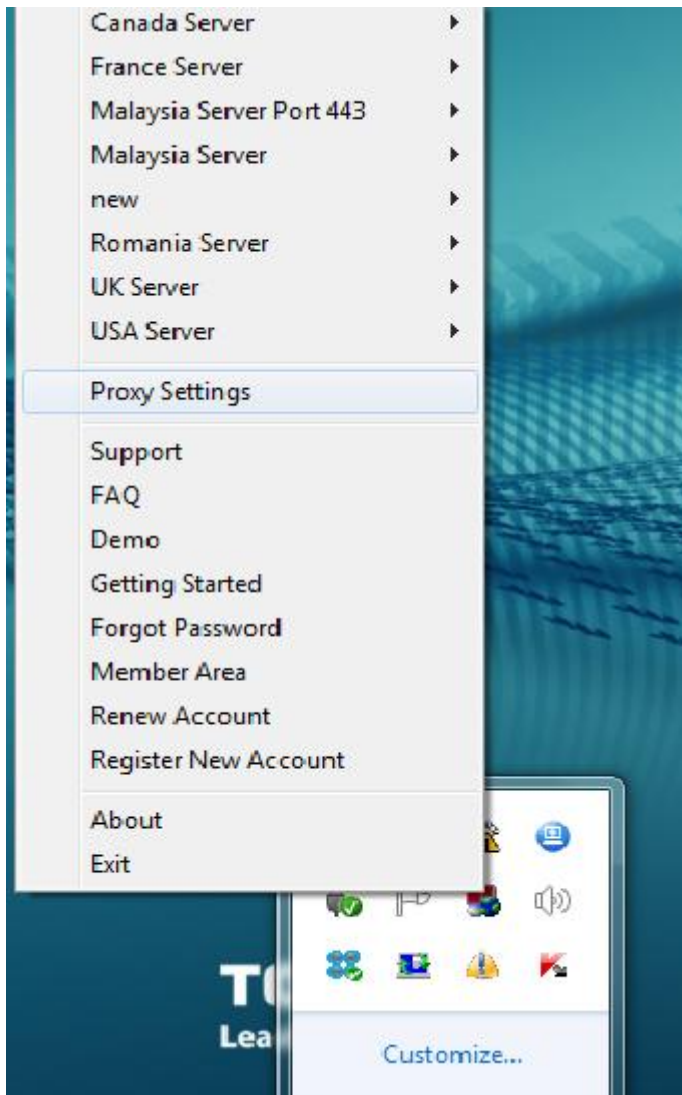


That's all you have to do on this screen. In the Putty navigation tree on the left click on the Session node (at the top of the tree), and then click the Save button on the right side of the screen to save this configuration.

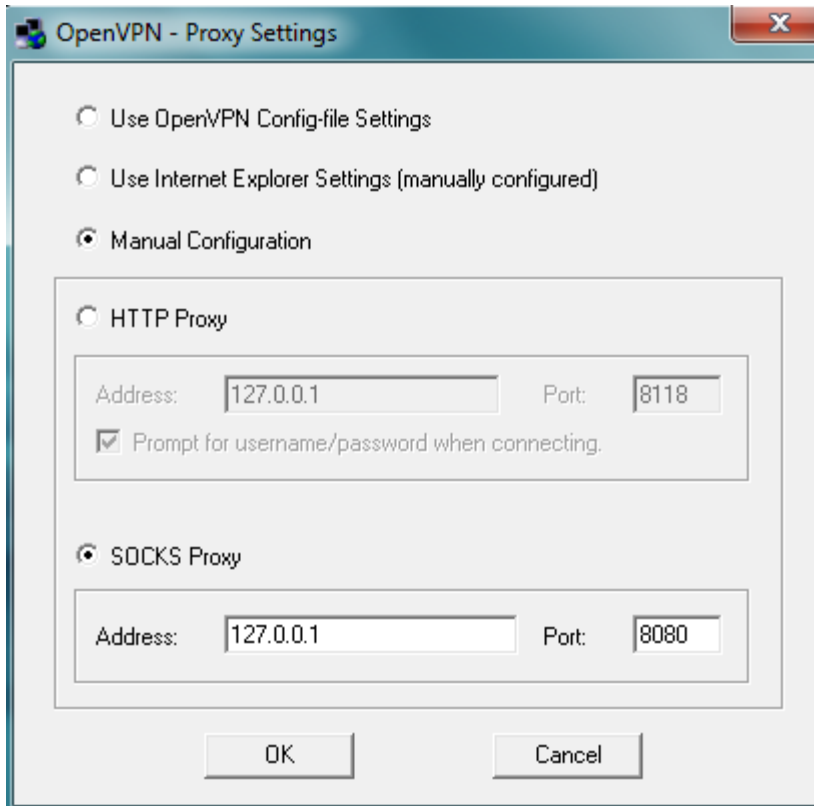
Congratulations -- that's all you had to do to configure Putty. Now all you have to do is login to your remote server. To do this, just click the Open button at the bottom of this window. You should see a Putty login shell open up to your remote server. Just login to your remote server with your username and password, and you're done. That's all you need to do to open the tunnel. Now you're ready to configure OpenVPN.

#### **Step 4: Configure OpenVPN to use the Putty SSH tunnel as a SOCKS proxy**

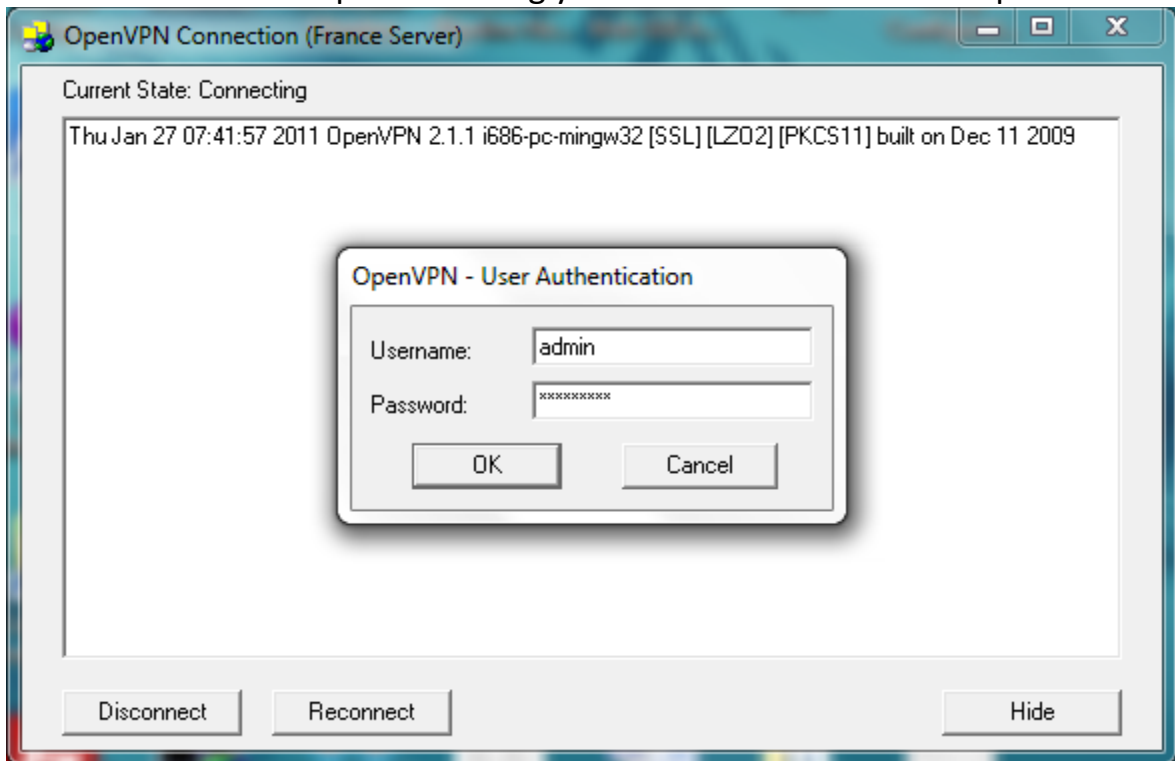
1. Configuring OpenVPN to use this new SSH tunnel is simple. To start OpenVPN, first run the OpenVPN GUI client by double clicking on the desktop icon or start menu icon. The OpenVPN GUI is a system-tray applet, so a red icon for the GUI will appear in the lower-right corner of the screen as shown below:



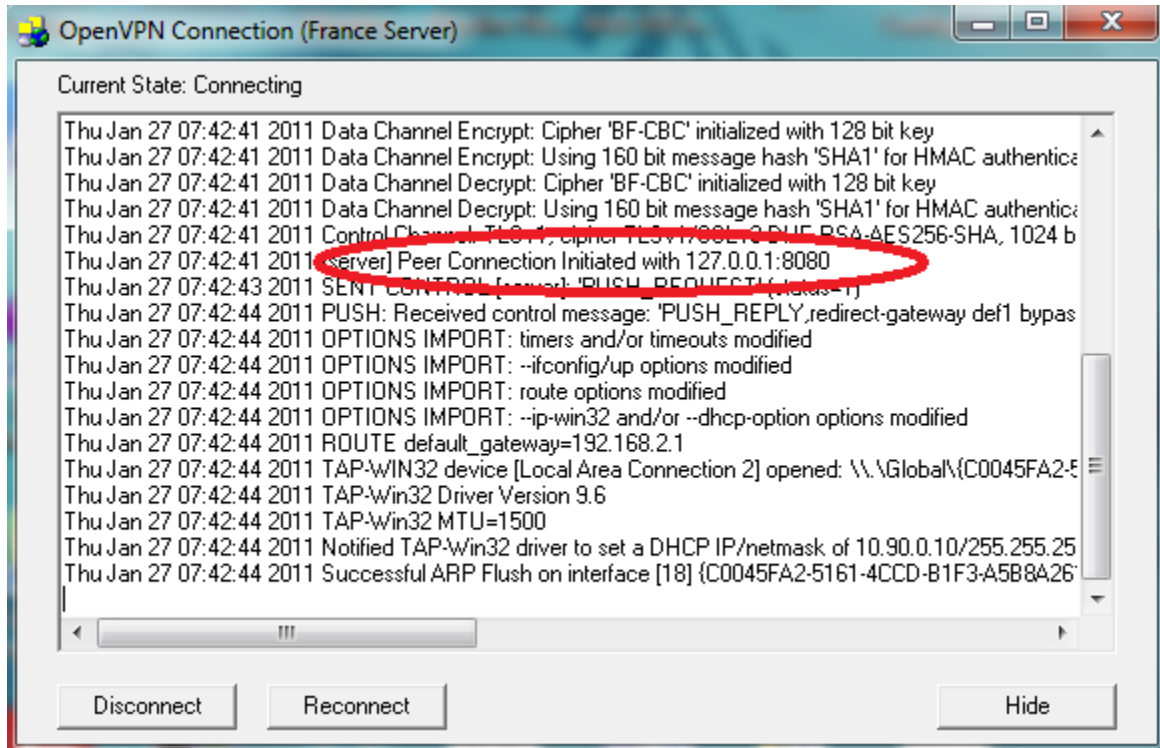
2. Right click on the system tray icon, and a menu should appear showing Anonyproz OpenVPN servers, and giving you the option to connect.
3. Then click on " Proxy Settings". You will be presented a window to select "Manual Configuration" and choose the proxy type. Select "Socks Proxy" and input 127.0.0.1 in the address field and the Port you choose for the SSH tunnel. (8080 according to this manual) and then click OK



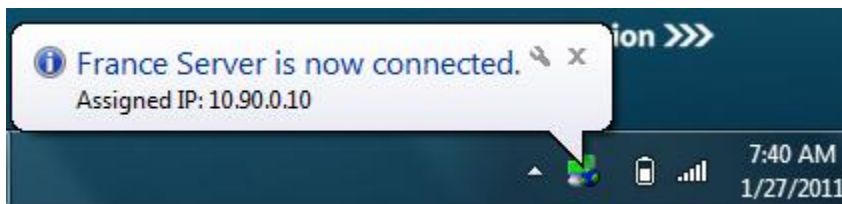
4. Now connect to the OpenVPN using your member username and password



5. If successful you will see a connection window as shown below. The circled text in Red confirms that the connection to the SSH Socks proxy was successful.



6. After successful authentication, you will see a window as shown below:



Congratulations!

### Testing your connection

To test and confirm your connection, you can do a tracert on the windows command prompt as follow:

```
Administrator: C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>tracert google.com\
Unable to resolve target system name google.com\.

C:\Users\>tracert google.com

Tracing route to google.com [72.14.204.104]
over a maximum of 30 hops:

  0  270 ms  270 ms  607 ms  10.90.0.1
  1  371 ms  474 ms  542 ms  vss-3-6k.fr.eu [188.165.196.252]
  2  271 ms  274 ms  271 ms  rdx-3-29.fr.eu [213.251.130.50]
  3  *      *      *      Request timed out.
  4  276 ms  285 ms  457 ms  th2-1-6k.fr.eu [213.186.32.166]
  5  281 ms  275 ms  275 ms  google.as15169.fr.eu [91.121.131.2]
  6  275 ms  279 ms  275 ms  72.14.238.234
  7  354 ms  360 ms  352 ms  216.239.43.90
  8  362 ms  356 ms  358 ms  66.249.94.46
  9  354 ms  356 ms  355 ms  iad04s01-in-f104.1e100.net [72.14.204.104]

Trace complete.

C:\Users\>
```

The output shows and confirms that your traffic to Google.com was routed through the OpenVPN server.

Note: If you check <http://www.myiptest.com>, your IP will show the SSH server.