

SSL to SSH Tunneling Software Installation (Windows)

This guide explains how to install Anonyproz SSL to SSH tunneling application which is pre-configured and compiled from [Putty](#) and [stunnel](#) open source software packages. The program can be used to create a secure encrypted tunnel via SSH Socks proxy.

Note: This program is mainly intended for users who cannot connect directly to any SSH server listening on port 443 for SSH tunneling as a result of SSH traffic filtering and blocking by strong firewalls or Deep Packet Inspection devices using protocol handshake filtering. The aim of the program is to make your SSH traffic indistinguishable from real SSL traffic.

Below are the main benefits of using this program:

1. Bypass Deep Packet Inspection (DPI) or layer-7 protocol firewall filtering of SSH protocol
2. Ability to connect to SSH server on port 443 if direct outgoing connection to SSH server listening on port 443 is blocked on your network
3. SSH over SSL traffic is indistinguishable from real SSL traffic
4. All SSH traffic nicely hidden in SSL tunnel
5. Double encryption for paranoid users

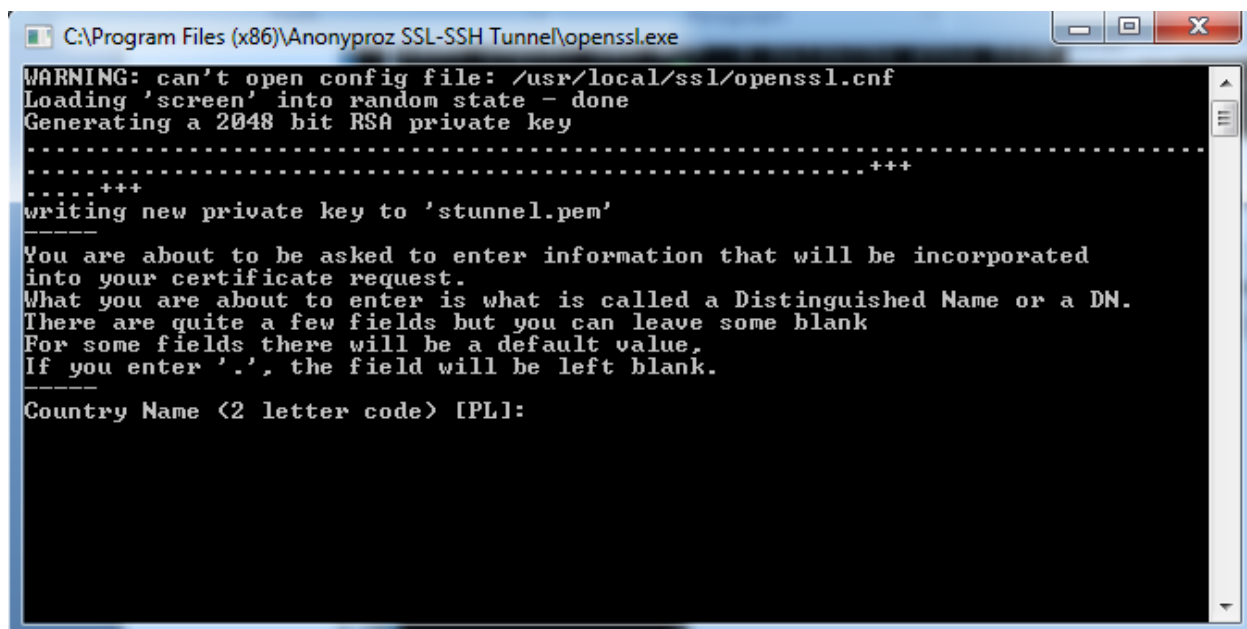
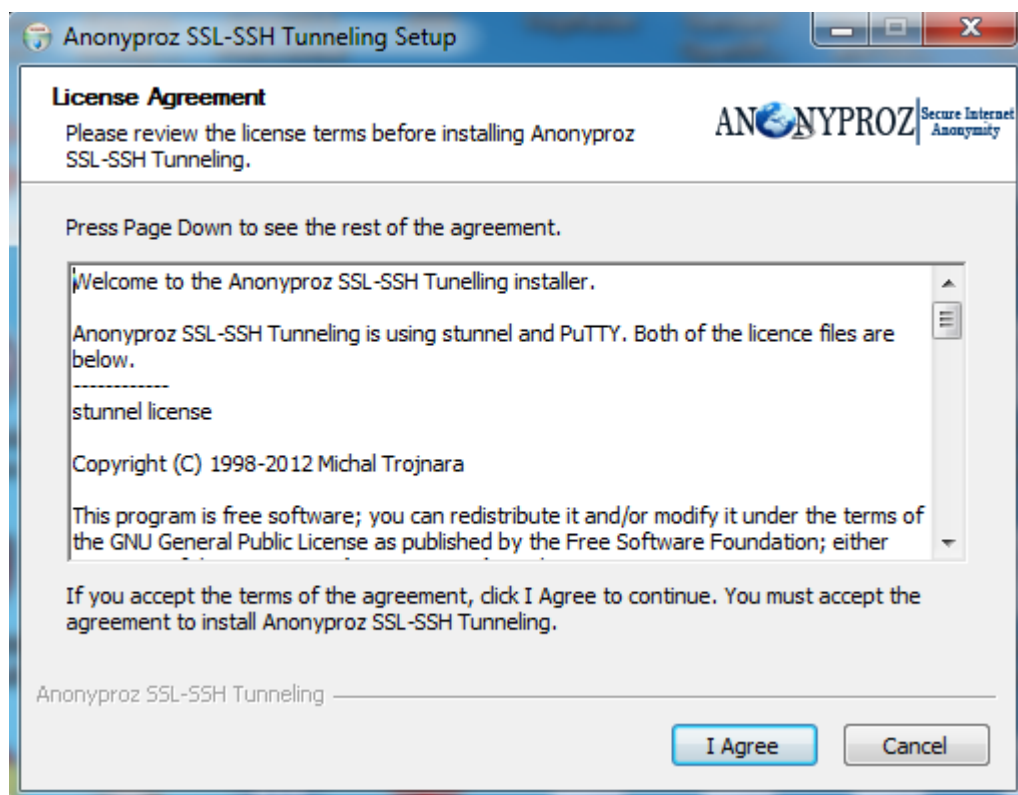
Installation Steps:

Step1: Download the application from the links below:

<http://www.bpsocks.com/ssl-ssh-usa.exe> (USA Server)

<http://www.bpsocks.com/ssl-ssh-nl.exe> (Netherlands Server)

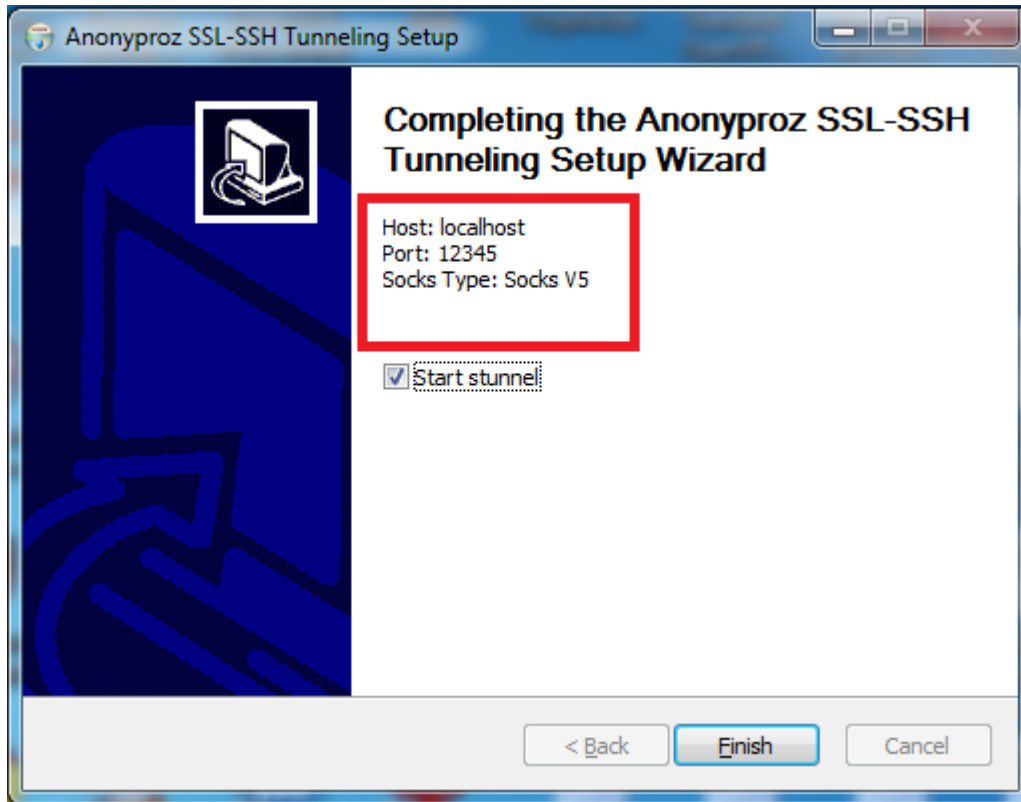
Step2: Install the application. Run the downloaded file and accept all defaults. During the installation, a command line window will pop up for the certificate installation. Then when prompted for the information to be incorporated into the certificate request, press enter for all to choose the defaults or enter your desired values.



Important: Before installing the application, please turn off any firewalls and anti-virus software for the duration of the install. If this is not done, there could be a failure in the software install.

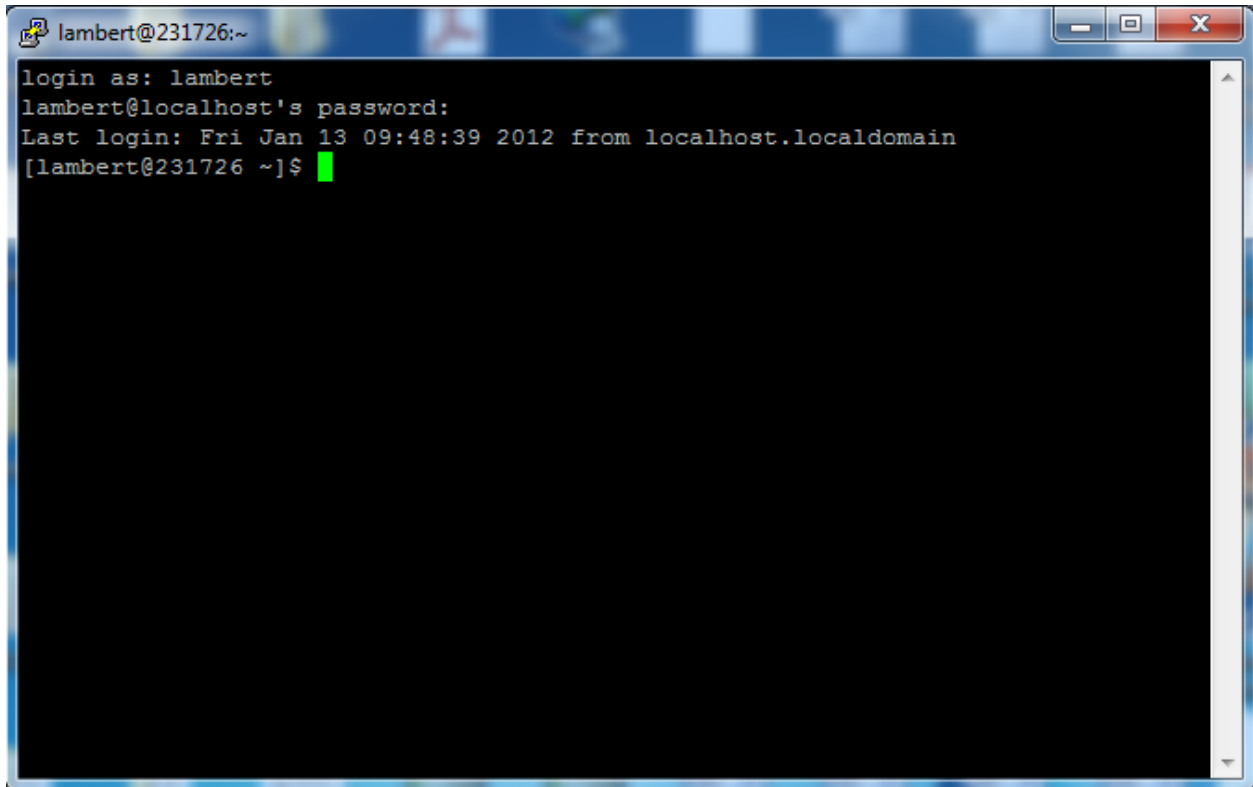
Step3: On the final screen of the installer, you will see the Socks proxy information created and you will find stunnel and Putty icons placed on your desktop with Putty icon name "Anonymprox

SSL-SSH Tunneling". To start the tunnel, simply double click on this Putty icon to begin the authentication process.

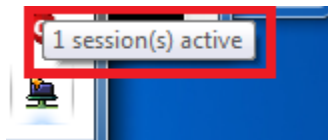


Step 4: Authenticate to the server. You will be prompted to enter your member username and password which you have received from us or chosen during your signup.

Note: You must leave the Putty window open. Do not close it or attempt to enter any command. You must leave the window open throughout your tunnel session.



After successful authentication, the stunnel icon on your taskbar should now display an active session as shown below:



That's all you need to do to open the tunnel. Now you're ready to configure your application such as web browser, VOIP, messengers, OpenVPN etc with the Socks 5 proxy as displayed above:

Host: localhost

Port: 12345

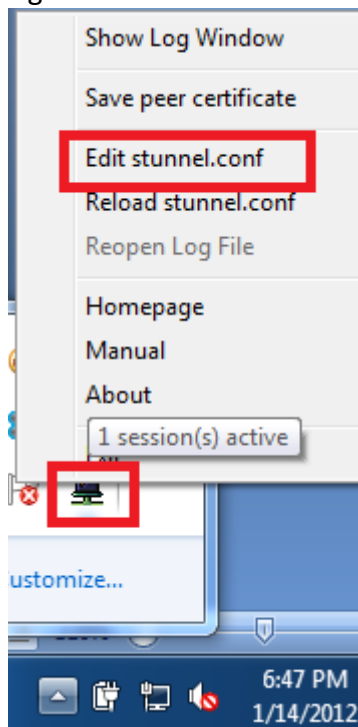
Proxy Type: Socks 5 (Requires no authentication)

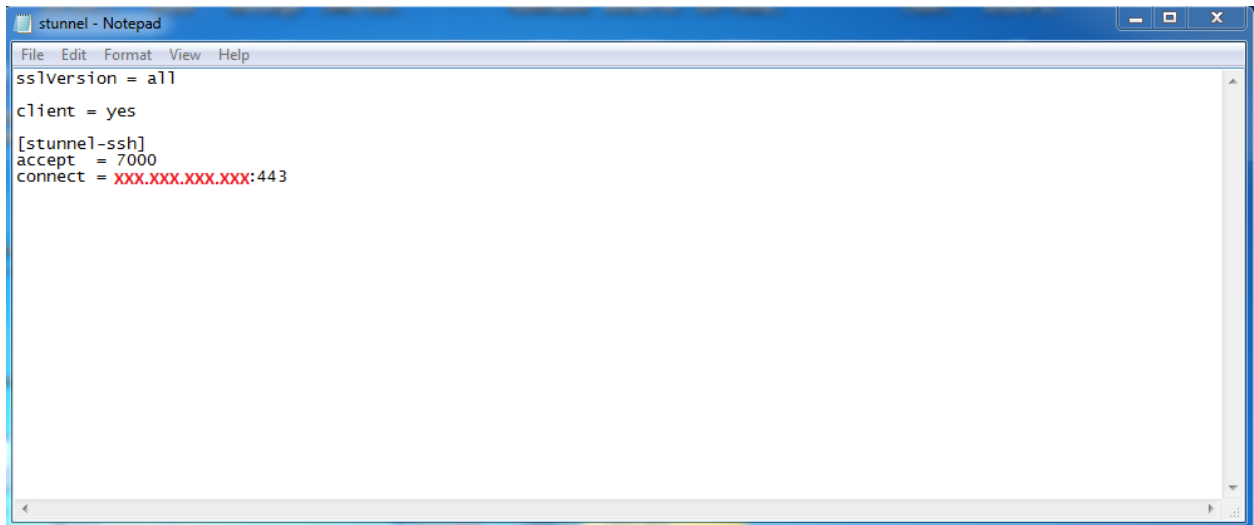
Switching Servers

Our SSL-SSH servers are currently located in USA and Netherlands. Unlike OpenVPN, stunnel can only accommodate one client config file at a time on the GUI. This means that if you want to switch from one server to another, you must terminate your current connection, and edit the remote SSH server IP on client config file in the stunnel program folder on your computer. This should be at : C:\Program Files (x86)\stunnel (For windows 7)

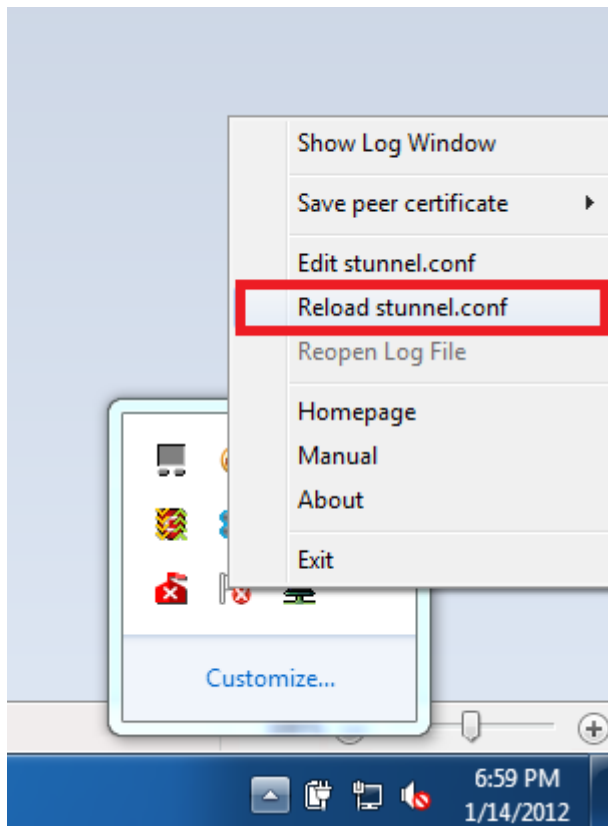
You will receive the SSL-SSH servers IP in your welcome email. To edit the IP take the following steps:

1. Terminate your current connection by closing the Putty window
2. Right click on the stunnel icon on the taskbar and click on "Edit stunnel.conf"



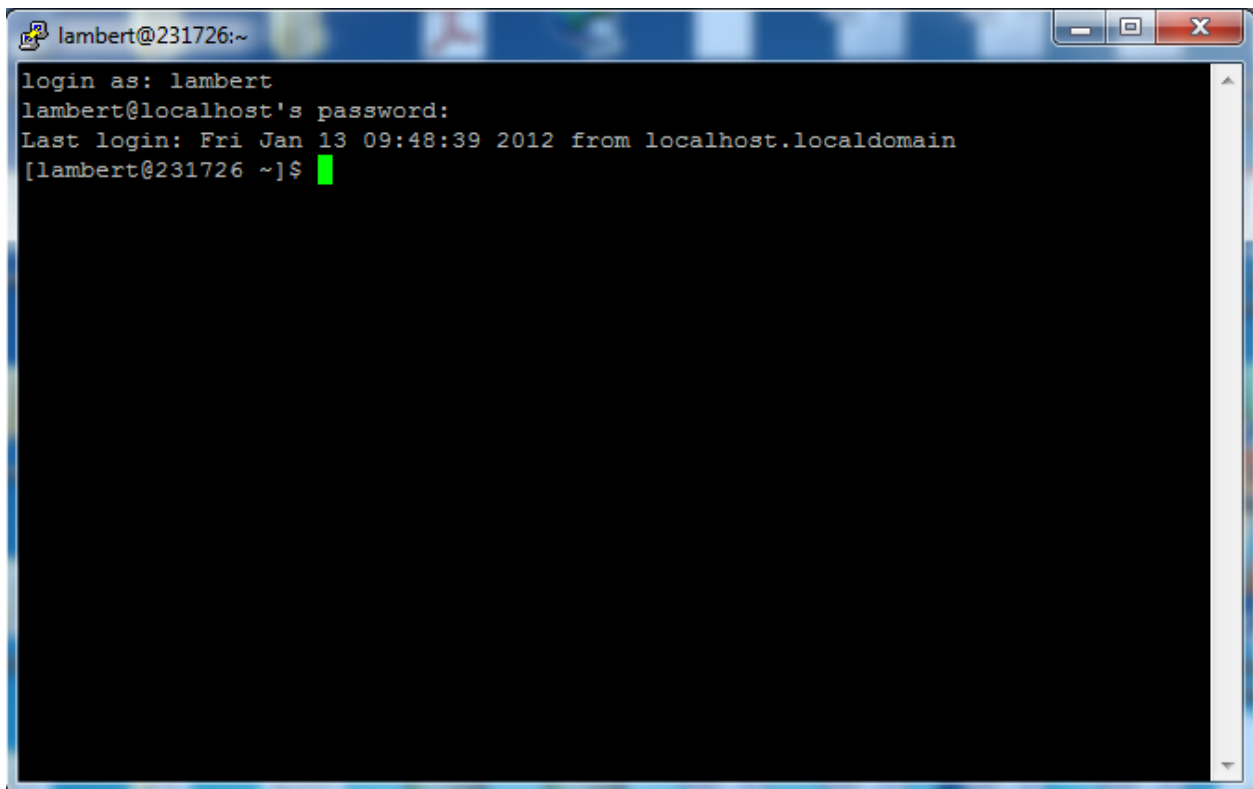


3. Edit the IP marked xxx.xxx.xxx.xxx to the new IP and save the changes. Leave the other parameters unchanged! Do not edit the other lines. The Port must remain as 443.
4. Reload the config file- Right click on the stunnel icon on the taskbar and click on "Reload stunnel.conf"



5. Finally click on the Putty icon on your desktop and authenticate to the new server using your login credentials. Then confirm if your IP has changed by visiting <http://www.myiptest.com>

Important: This SSL-SSH tunneling application do not currently support automatic re-connection when disconnected due to shaky ISP connections, outage or server disconnections. Whenever you lose your tunnel, you must always re-start the tunnel by clicking on the Putty icon and then authenticate to the server.

A screenshot of a terminal window titled 'lambert@231726:~'. The terminal shows the following text: 'login as: lambert', 'lambert@localhost's password:', 'Last login: Fri Jan 13 09:48:39 2012 from localhost.localdomain', and '[lambert@231726 ~]\$' with a green cursor. The window has standard Windows-style title bar buttons (minimize, maximize, close) in the top right corner.

```
lambert@231726:~  
login as: lambert  
lambert@localhost's password:  
Last login: Fri Jan 13 09:48:39 2012 from localhost.localdomain  
[lambert@231726 ~]$
```

Legal Disclaimer: Use of VPN and tunneling services is perfectly legal in most countries and jurisdictions. As long as you are not performing illegal activities, then it is perfectly legal to use a VPN service. By subscribing for our VPN services, you agree not to violate any laws of your jurisdiction and the laws of the specific VPN server location (country) which you are connected to and tunneling your traffic through. It is your responsibility to know and understand any relevant laws pertaining to the use of encryption products such as OpenVPN in your jurisdiction. Anonyproz cannot be held liable for using our services.