Introduction

SSL Tunnel vs Traditional VPN

Traditional VPN:

PPTP: TCP 1723, GRE (IP Protocol 47)

L2TP: UDP 1701.

IPSec: UDP 500, ESP (IP Protocol 50), AH (IP Protocol 51).

SSL Tunnel:

TCP 443, uses HTTPS to establish a secure connection.

Common Problems of Traditional VPN

1. Firewall Problem: There are many blocking issues involving connections in relation to GRE port blocking or ESP/AH port blocking.
2. NAT Problem: There are many IPSec NAT incompatibility problems. (RFC 3715)
3. User clients are a must have. Each time when you use a new computer, you have to install the VPN tool and enter the settings.

Advantages of SSL Tunnel

1. Typical port blocking is decreased. Generally no firewall will block TCP 443.
2. No NAT incompatibility problem.
3. No static IPs are required, and a client is unnecessary in most cases.

Note:

SSL VPN is not designed for site to site VPN connections but is intended to be used for **client to site** VPN connections.

How to connect SSL tunnel

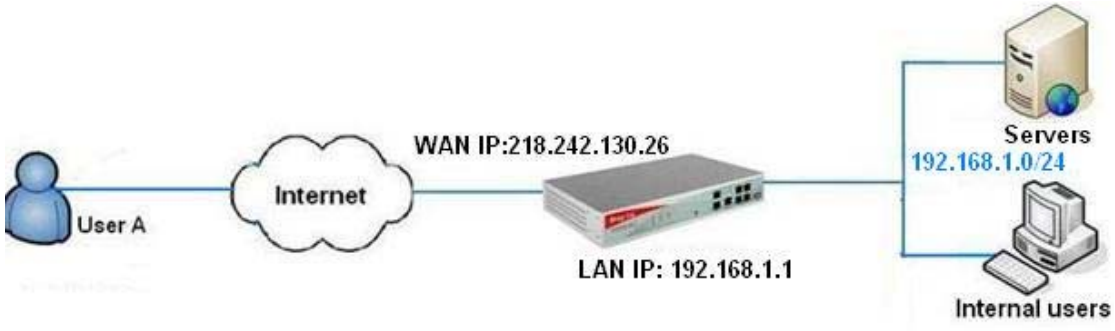


Figure 1

User A connects a SSL Tunnel VPN to Vigor2950. After the connection is established, he is able to access the whole network behind Vigor2950.

Configurations on the Router :

1. Go to **SSL VPN >> User Account** page and an account for User A.

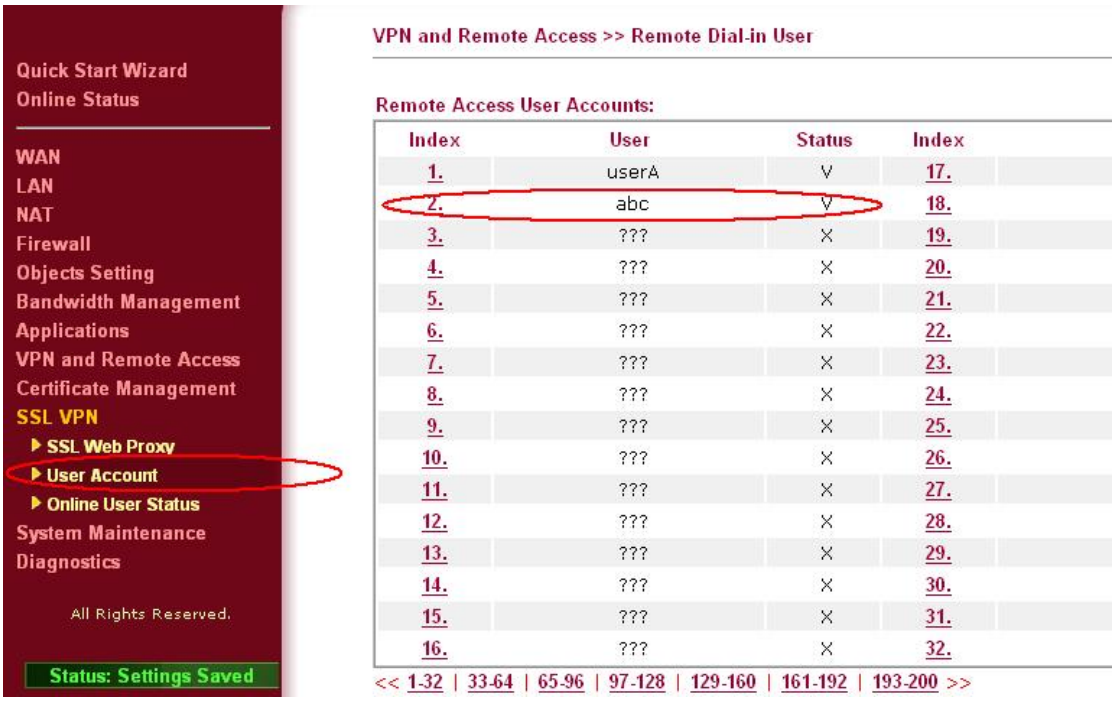


Figure 2

2. Enter the following:

- Enable the account.
- Setup the username/password for User A.
- Enable **SSL Tunnel**.

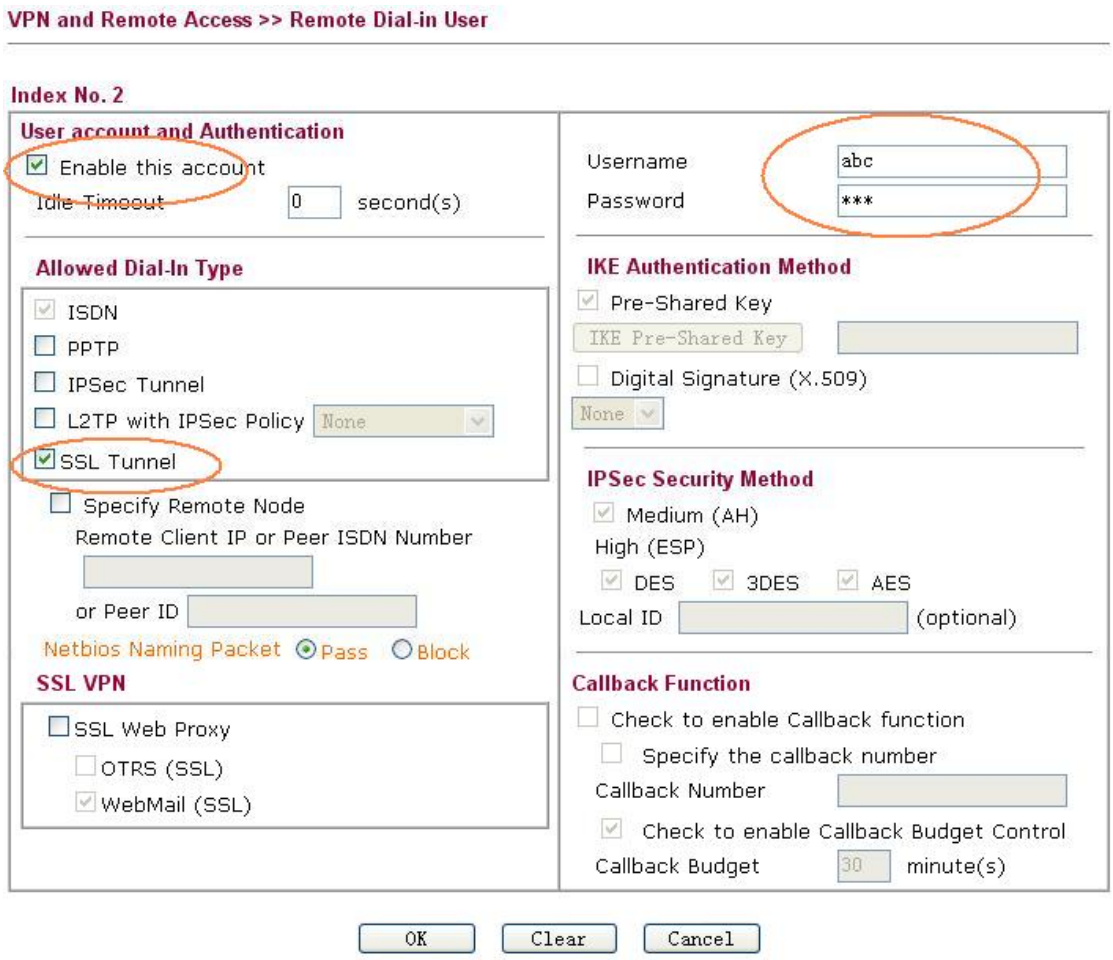


Figure 3

3. Go to **System Maintenance >> Management** page and make sure **HTTPS Server** is enabled. If you don't want to use the standard TCP 443 port, change the port as follows.

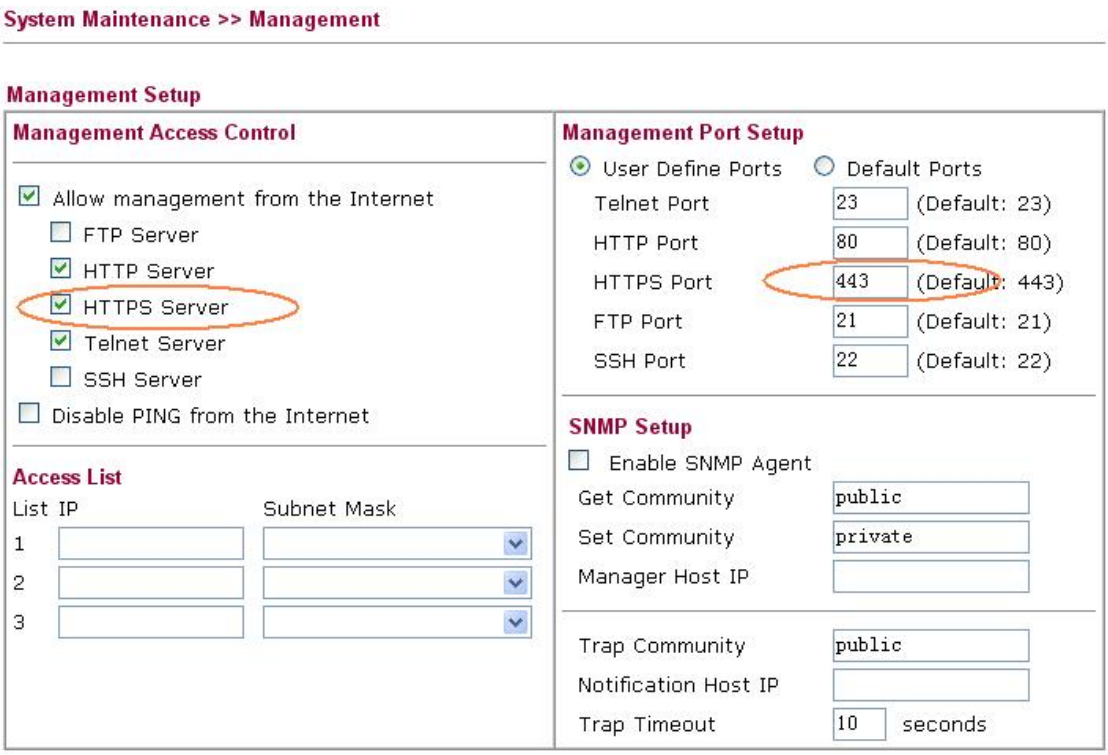


Figure 4

Steps for User A to connect SSL Tunnel (First Time)

1. Open a web browser(I.E or Firefox), and go to the following URL :

   https://218.242.130.26

2. Internet Explorer 6 will display the below security alert stating that the security certificate is valid but is not from a known source. Please accept the certificate with confidence by pressing the **Yes** button.

Figure 5

Internet Explorer 7 will display the below security alert stating that the security certificate is valid but is not from a known source. Please select the ***Continue to this website (not recommended)*** choice.

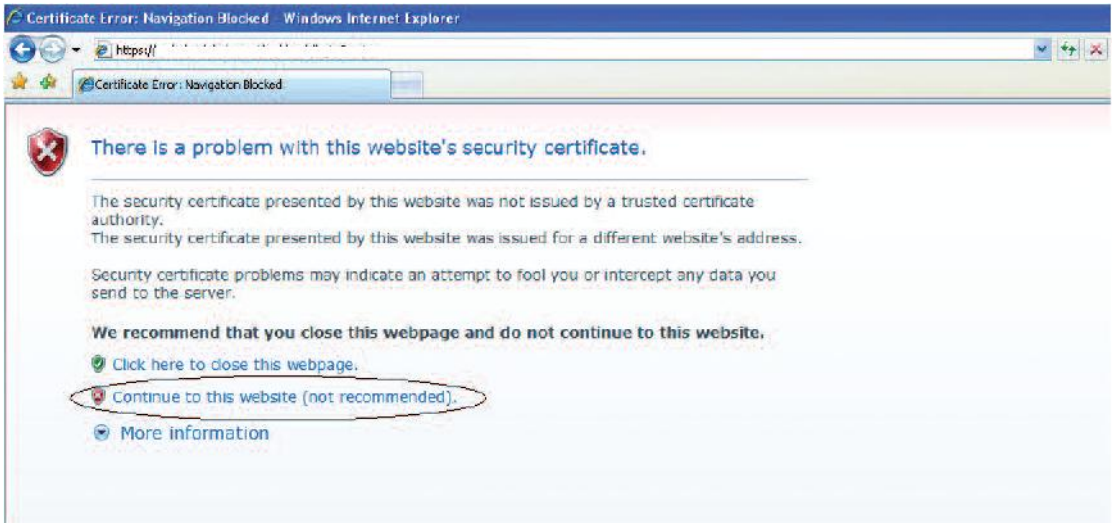


Figure 6

3. A login window pops up. Input the username and password for User A.

Figure 7

4. If login successfully, you will see a window like the one shown below.

Press **SSL Tunnel** .

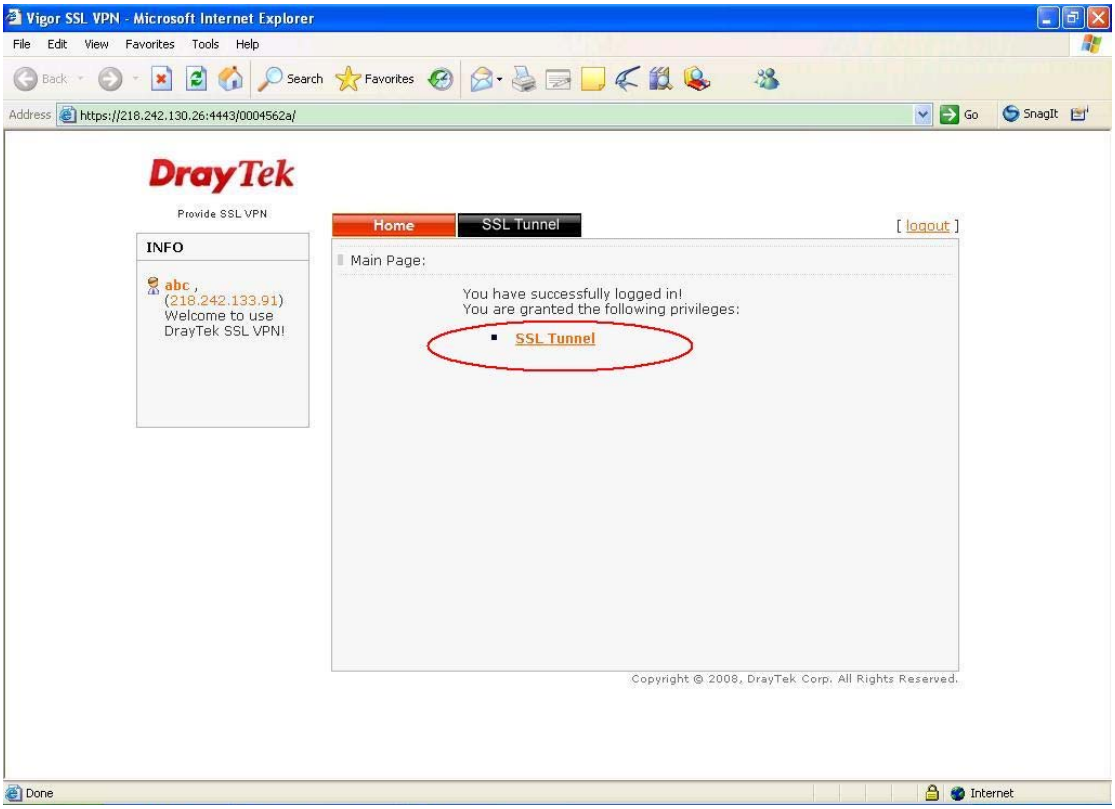


Figure 8

5. In this page if the button is "**Install**", it means you haven't installed relevant components on that PC. Press the button **Install** to download the cpmponents from the router.

   Note: Verify your browser's security settings allow ActiveX controls. And you must turn off the protected mode in Vista IE7.

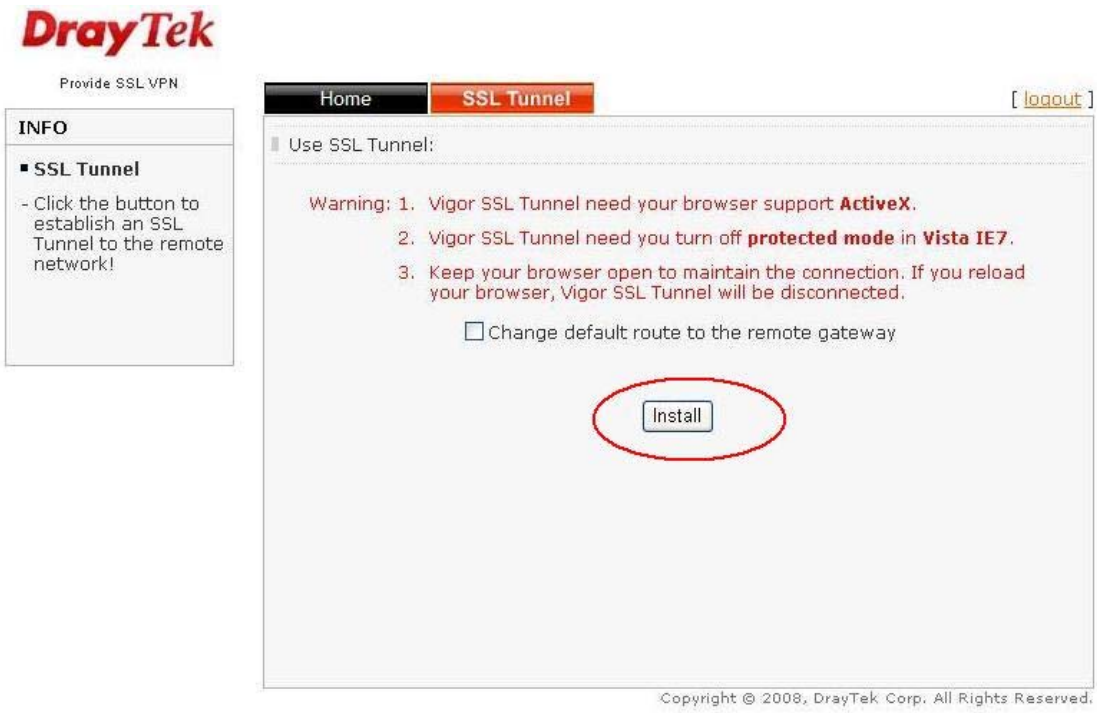


Figure 9

6. Wait for some minutes. Your browser is downloading the components.

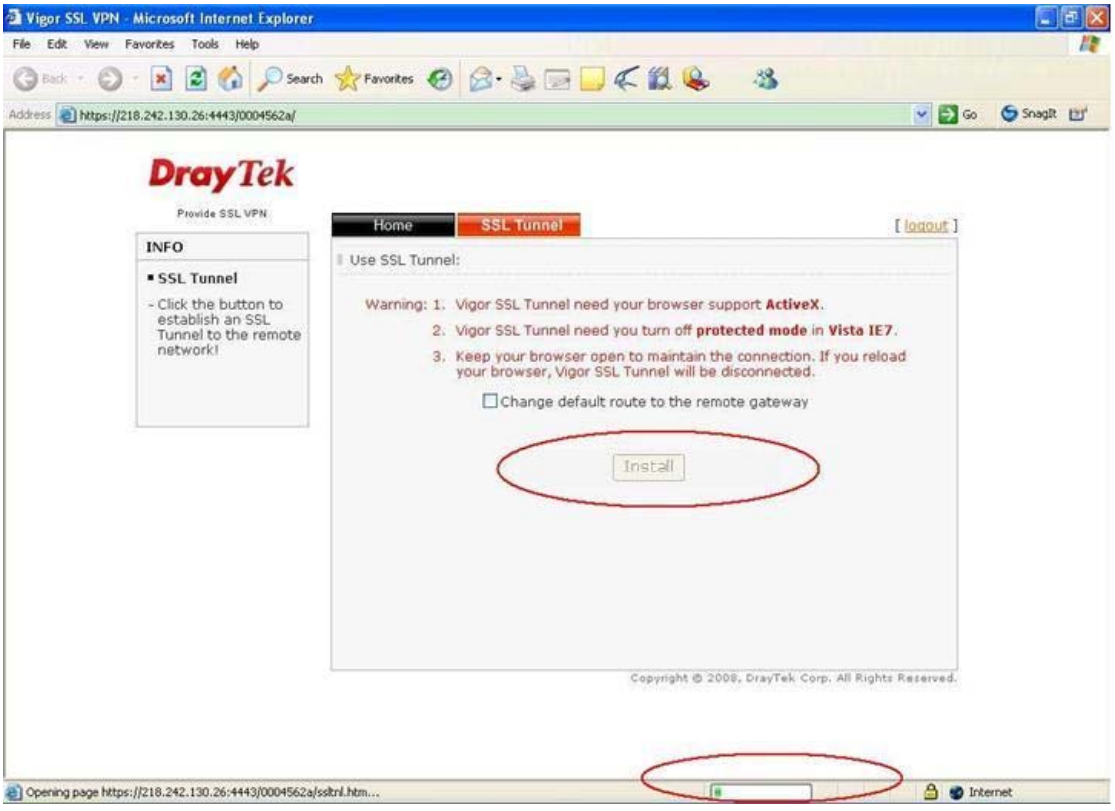


Figure 10

7. After the components are downloaded on your PC, you will get the following message.

“Vigor SSL Tunnel could not be installed. Verify your browser security settings allow ActiveX controls. And you must have administrative rights.” Please press **OK**.

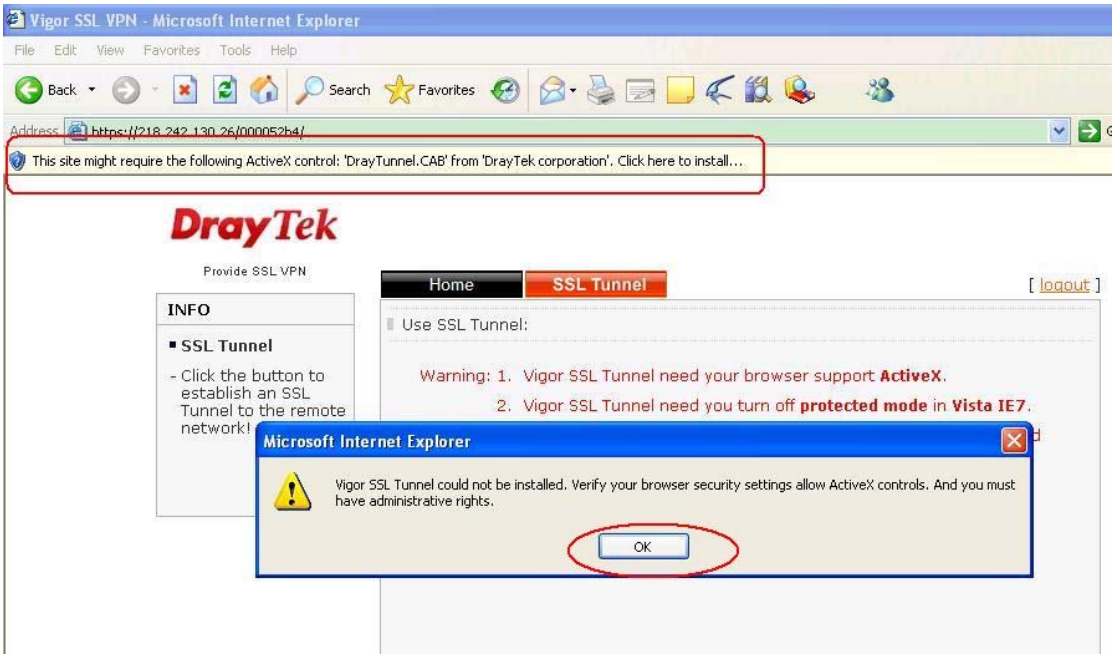


Figure 11

Then right click the mouse and select “Install ActiveX Control…”

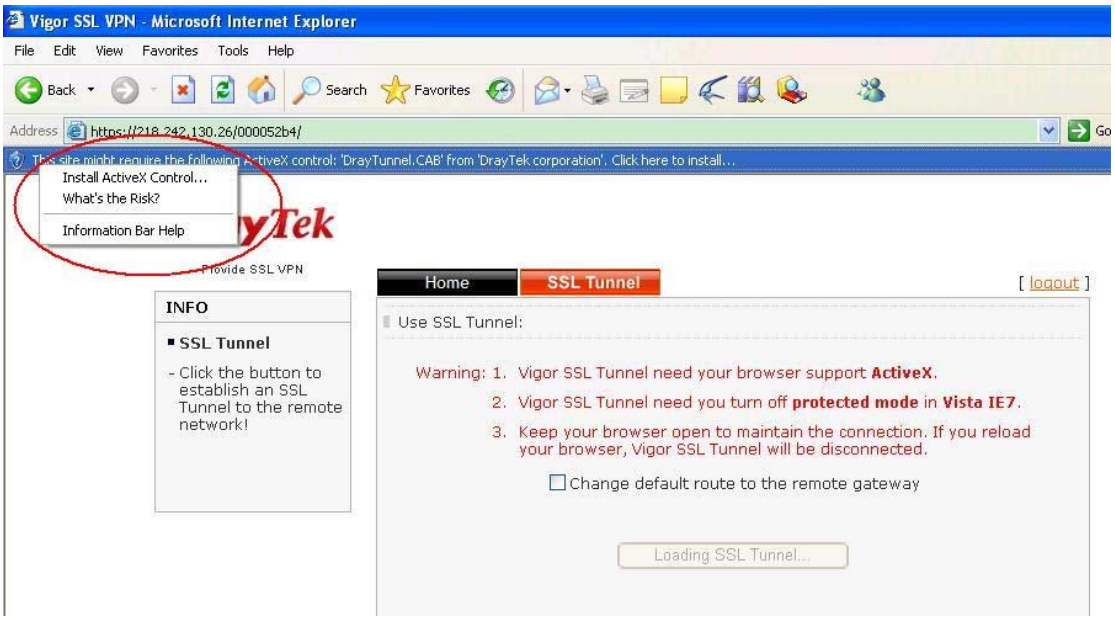


Figure 12

It will go to the Home page again.

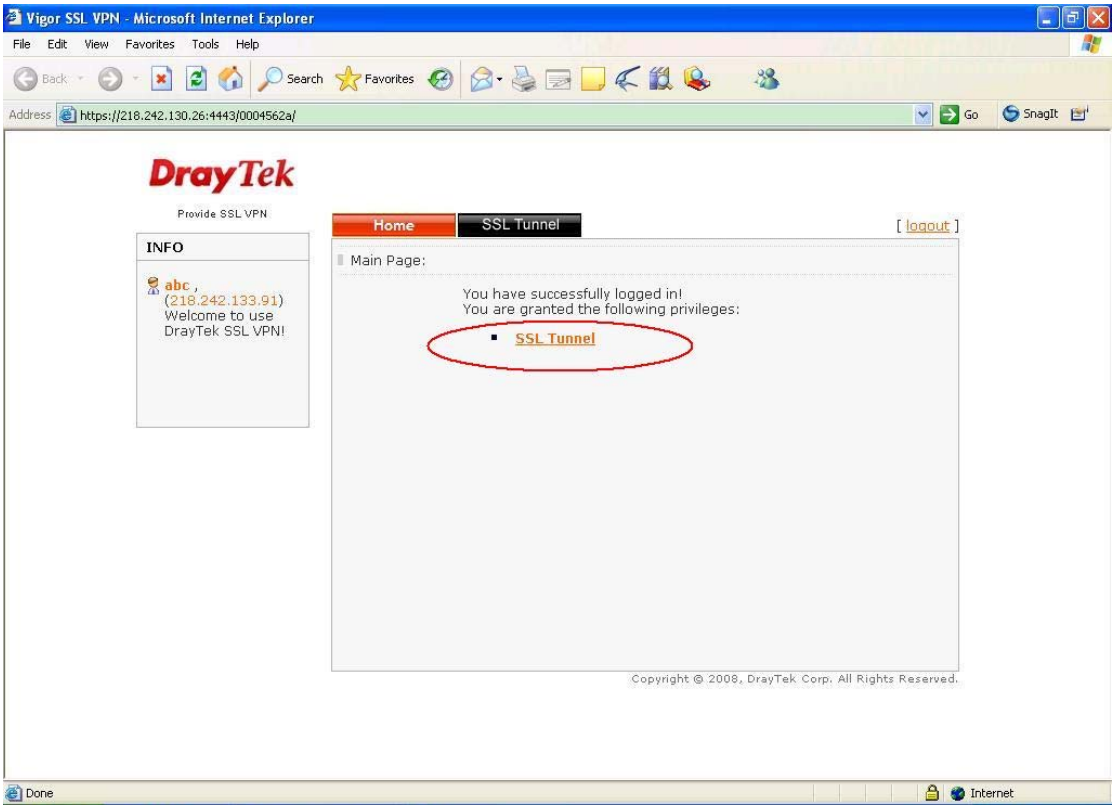


Figure 13

Press the **Install** button again.

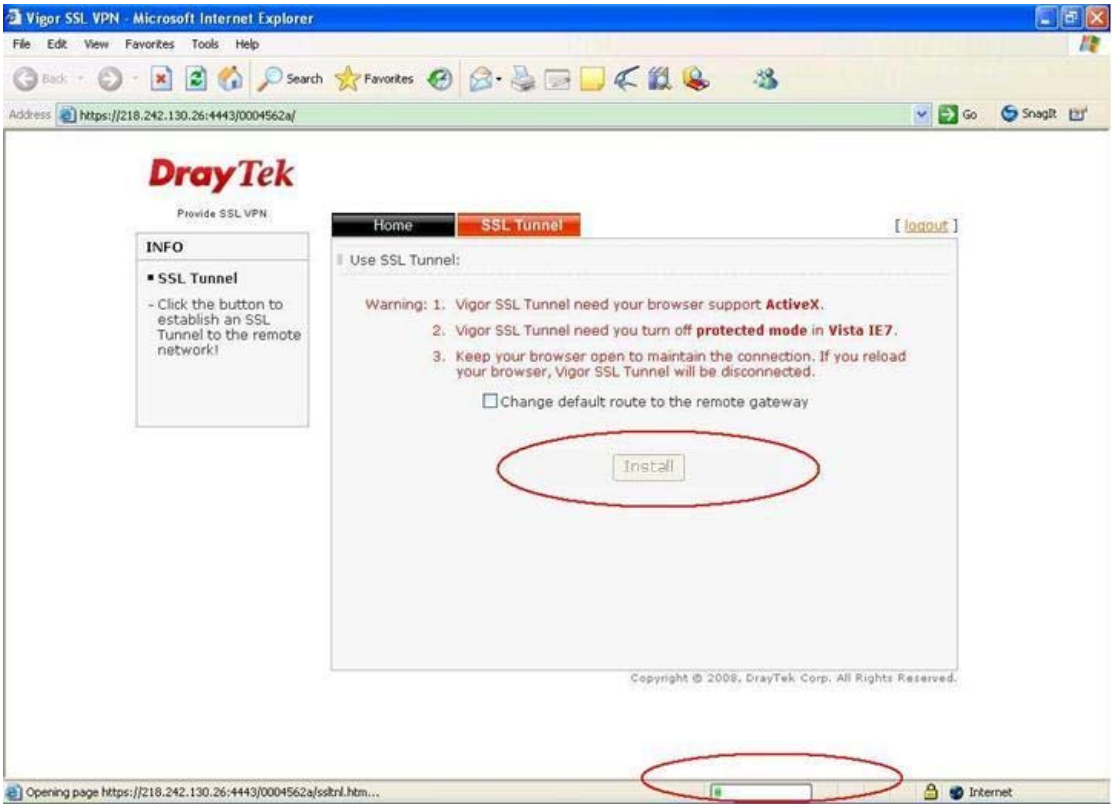


Figure 14

8. A window pops up. Press the button **Install**.

Figure 15

9. Wait for some minutes. The driver is installed first, then the DraySSL Tunnel Client tool will pop up and dial the connection automatically.

Figure 16

10. If the tunnel is connected successfully, the status will show **Connected**.

Figure 17

You may use ping to check the connection.

```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
```

Figure 18

11. If you want to drop the SSL tunnel, please press the **Disconnect** button (Figure 17). The DraySSL Tunnel Client will be turned off automatically. And you may find the button in SSL Tunnel page changes to **Connect**.

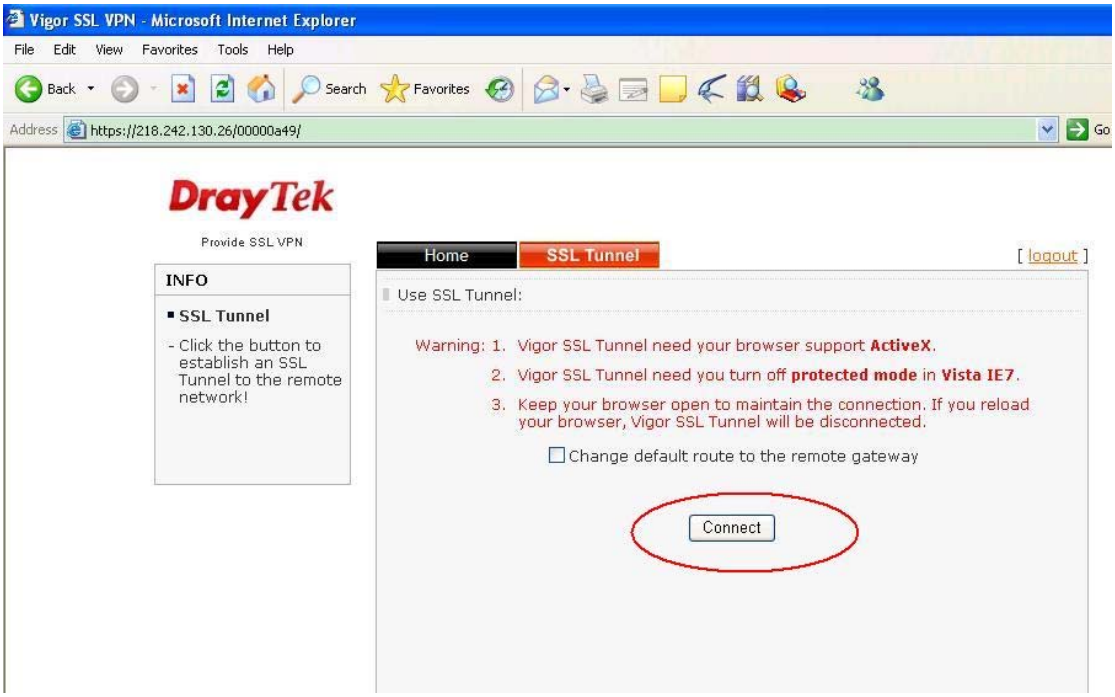


Figure 19

Note:

1. If you don't tick "**Remove Virtual Driver on disconnecting**" (Figure 17) when pressing the **Disconnect** button, next time when you connect the SSL Tunnel from the same PC, you needn't install the driver again. Press the **Connect** button in SSL Tunnel page (Figure 19), the DraySSL Tunnel Client will be loaded directly to connect the VPN.

2. If you tick "**Remove Virtual Driver on disconnecting**" (Figure 17) when pressing the **Disconnect** button, next time when you connect the SSL Tunnel from the same PC, you still need install the driver again. Press the **Connect** button in SSL Tunnel page (Figure 19). During installing the driver, you may get the following warning message. Please press **Continue Anyway**.

Figure 20

3. Do not close the SSL Tunnel page before you drop the VPN connection.

4. If you don't enable ActiveX controls, you will get the following error message:

   "Your security settings do not allow Web sites to use ActiveX controls installed on your computer…"

Q&A

1. If the button in the SSL Tunnel page shows Update, what does it mean?

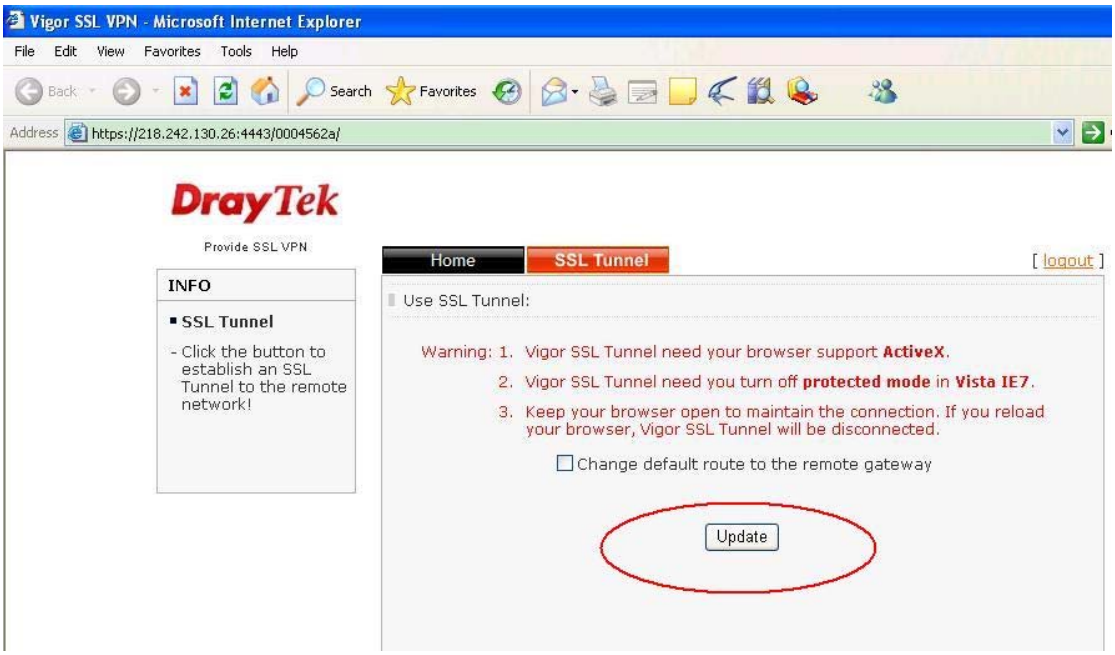


Figure 21

We may update the version of the components in new firmware. So if you see the button Update, it means the components installed on your PC is old. Please press Update to download and install the new components.

2. What will be installed on your PC after connecting the SSL Tunnel?

a. Draytek Virtual PPP Adapter. You may find it from *Control Panel* > *System* > *Hardware* > *Device Manager*.

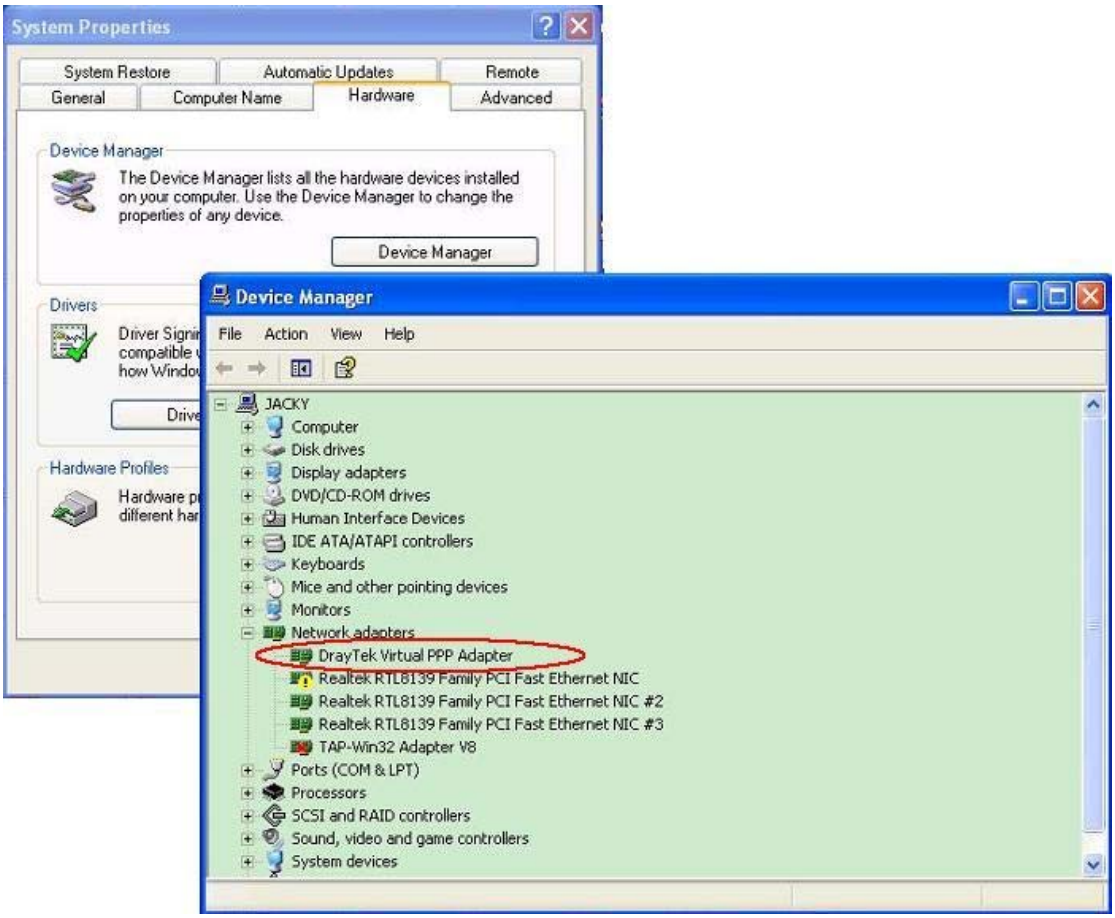


Figure 22

b. The file “DraySSL TunnelCtrl Class” in *C:\Windows\Downloaded Program Files*.

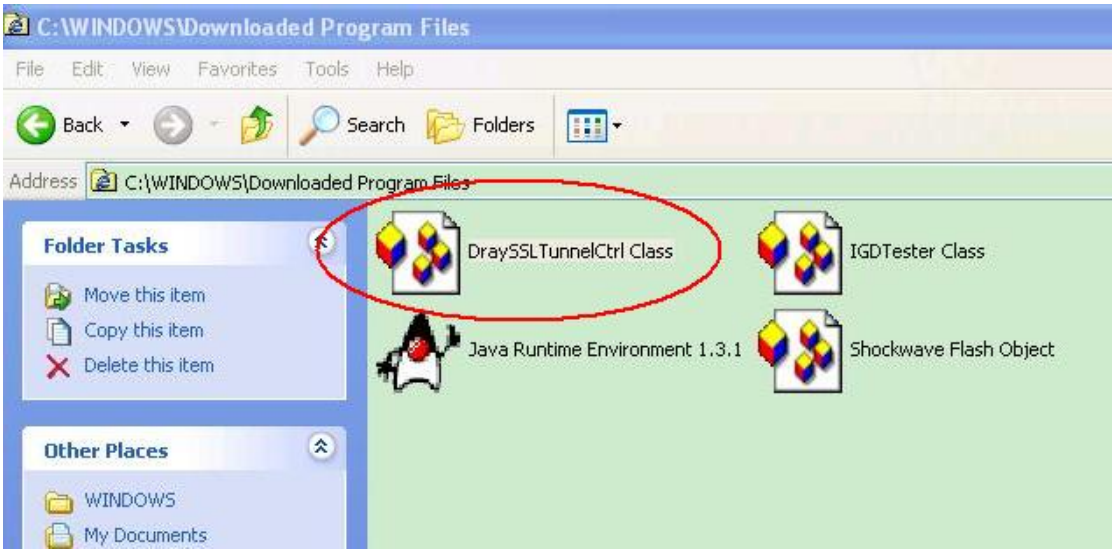


Figure 23

3. How to uninstall the components and the files?

a. To uninstall the driver you have the following two methods:

1. When disconnecting the SSL tunnel, please tick “**Remove Virtual Driver on**

disconnecting.”

Figure 24

2. Go to *Control Panel* > *System* > *Hardware* > *Device Manager* and manually uninstall Draytek Virtual PPP Adapter

b. To uninstall the file “DraySSL TunnelCtrl Class”, please go to *C:\Windows\Downloaded Program Files*, right click the mouse on the file “DraySSL TunnelCtrl Class”, and select “Remove”.

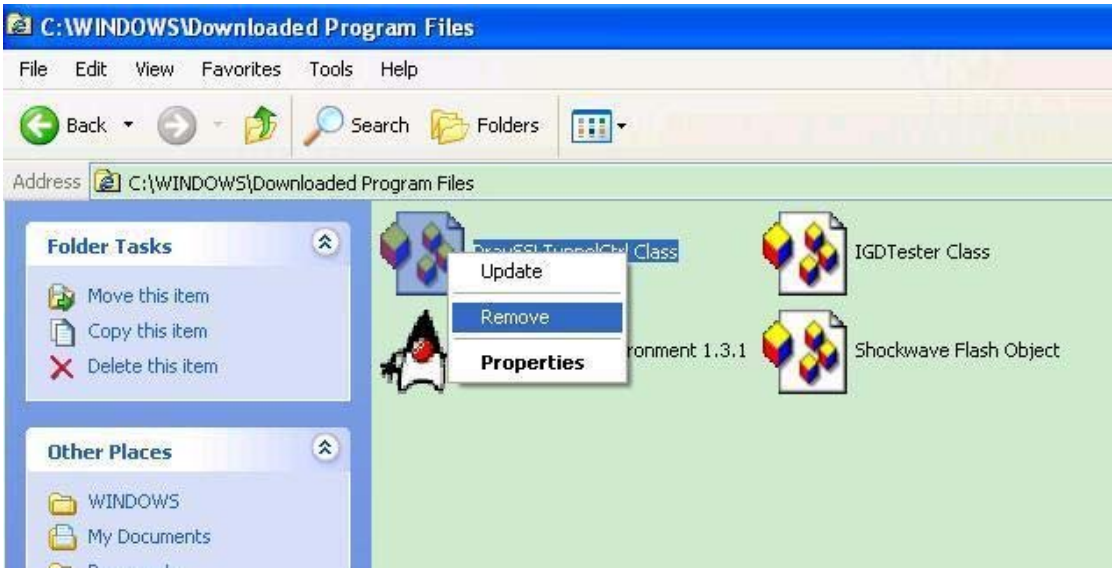


Figure 25

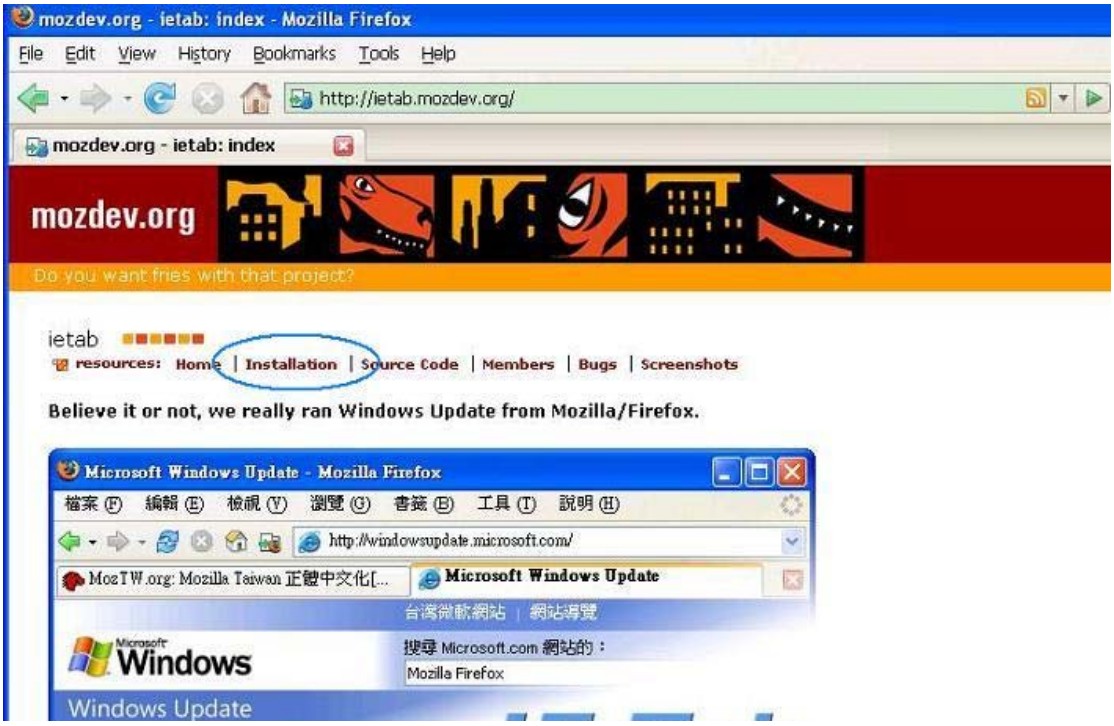
If you get the following error message, please close all the IE windows you have open.

Figure 26

4. How can I connect with the Firefox browser?

Firefox doesn't support ActiveX control, so you must install a plugin for it. For example **IE Tab**, an extension which embeds **Internet Explorer** in a **Mozilla/Firefox tab**. Please follow the steps below to install IE Tab.

1. Go to http://ietab.mozdev.org and open the **Installation** page.

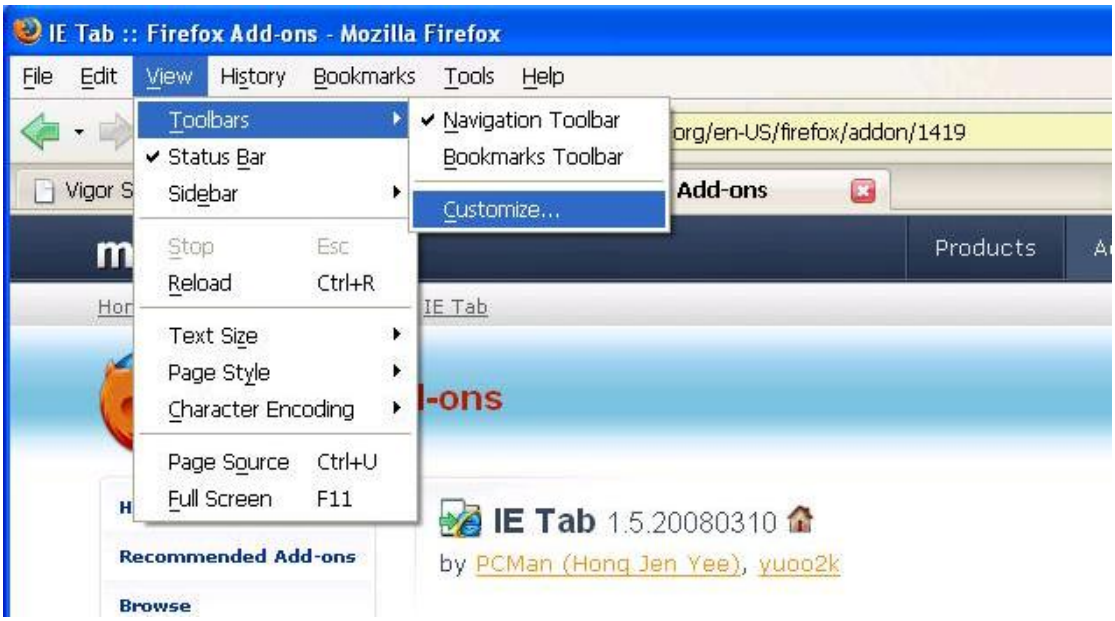


Select a compatible version, download and install it.

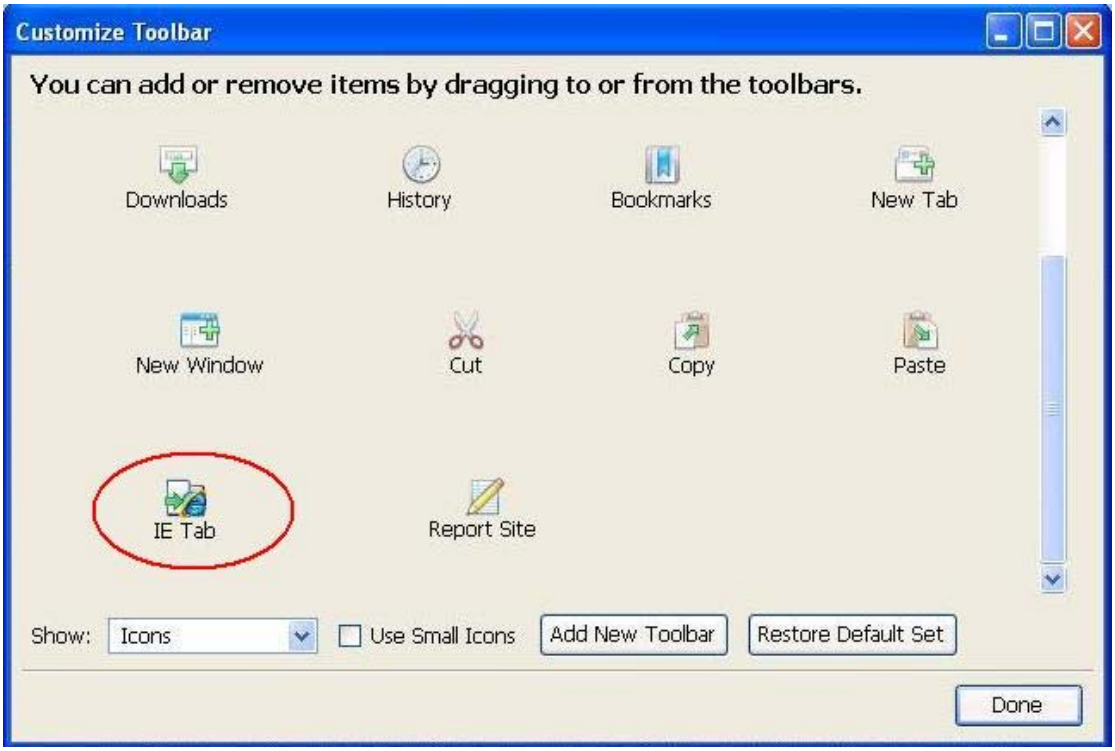
2. After installation, you will find a new icon like the figure shown below.

3. If the icon doesn't exist, please manually add it as follows:

Select **View >> Toolbars >> Customize…**



Find the IE Tab icon in the pop-up window. Left click the mouse on it, hold it and pull it onto the Toolbar.



4. Click the icon first. Then type the address, such as https://218.242.130.26


IE Tab :: Firefox Add-ons - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Vigor SSL VPN
IE Tab :: Firefox Add-ons
mozilla
Products
Home » Add-ons » Extensions » IE Tab