How to make a VPN connection to our servers from Windows Vista

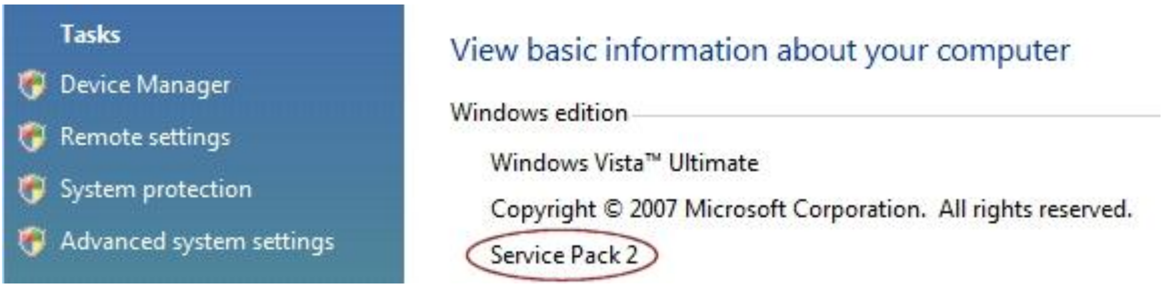
Windows Vista is able to make a new type of VPN connection called a Secure Socket Tunneling Protocol (SSTP) connection. This works just like a traditional Point-To-Point Tunneling Protocol (PPTP) VPN except that it uses the same TCP ports and protocol type as a secure website.
This has the advantage that almost all firewalls allow this type of connection to pass through, by default, and it's very difficult to block an SSTP VPN and still allow secure websites to function.

Vista only got the ability to make SSTP connections with Service Pack 1 so, before you begin, you should check that your Vista installation is up-to-date by clicking:-

Start – All Programs – Windows Update and selecting: **Check for updates**

Alternatively, you can just check that you have at least Service Pack 1 installed by clicking:-

Start then right-click on **Computer** and choose **Properties** to see which service pack that you have:-



View basic information about your computer

Windows edition

Windows Vista™ Ultimate

Copyright © 2007 Microsoft Corporation. All rights reserved.

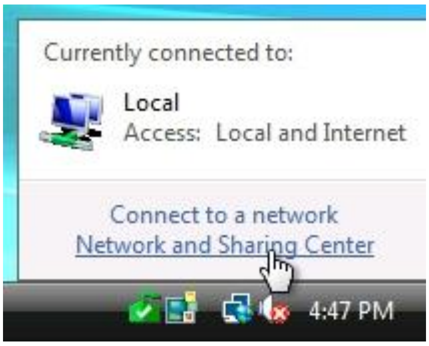
Service Pack 2

By default, Windows Vista tries to make a SSTP connection first and then falls back to a PPTP if SSTP fails. Our VPN servers support both types of VPN but, if you have Windows Vista, there no reason ***not*** to use SSTP. This means you will always be able to make an SSTP VPN connection to our servers, however and wherever you've connected to the Internet.

1 - How to Create a new VPN Connection

From the Windows Vista Desktop click on the Network icon in the Notification Area:

and click on **Network and Sharing Center**



Currently connected to:

Local
Access: Local and Internet

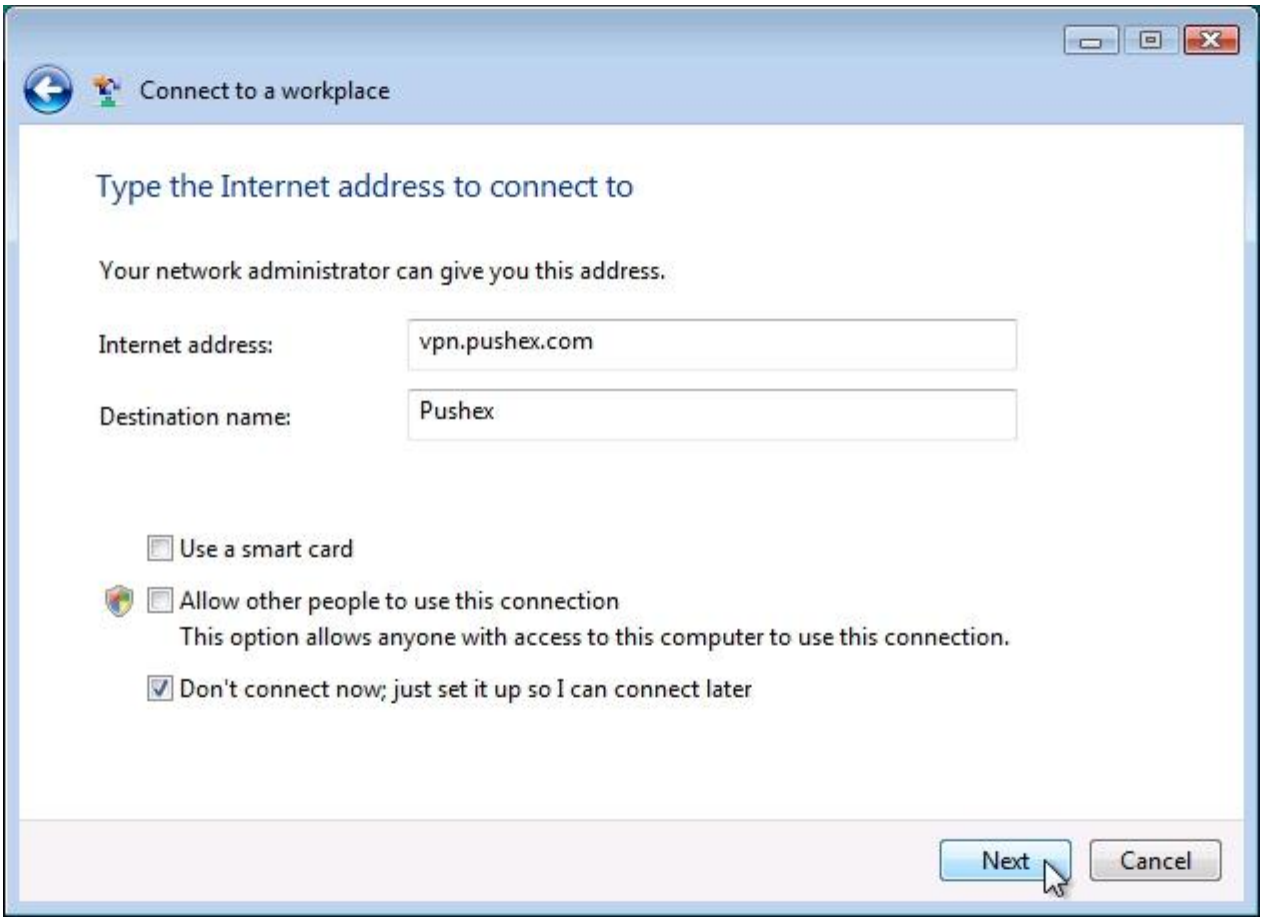
From the list of tasks in the left-hand column select: **Set up a connection or network**

then select: **Connect to a workplace** and click: **Next**

Click: **Use my Internet connection (VPN)**

When the window below appears, enter: **vpn.pushex.com** as the Internet address.

The **Destination name:** is just what you want to call this connection.
It can be anything, but **Pushex** is good:-



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: vpn.pushex.com

Destination name: Pushex

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

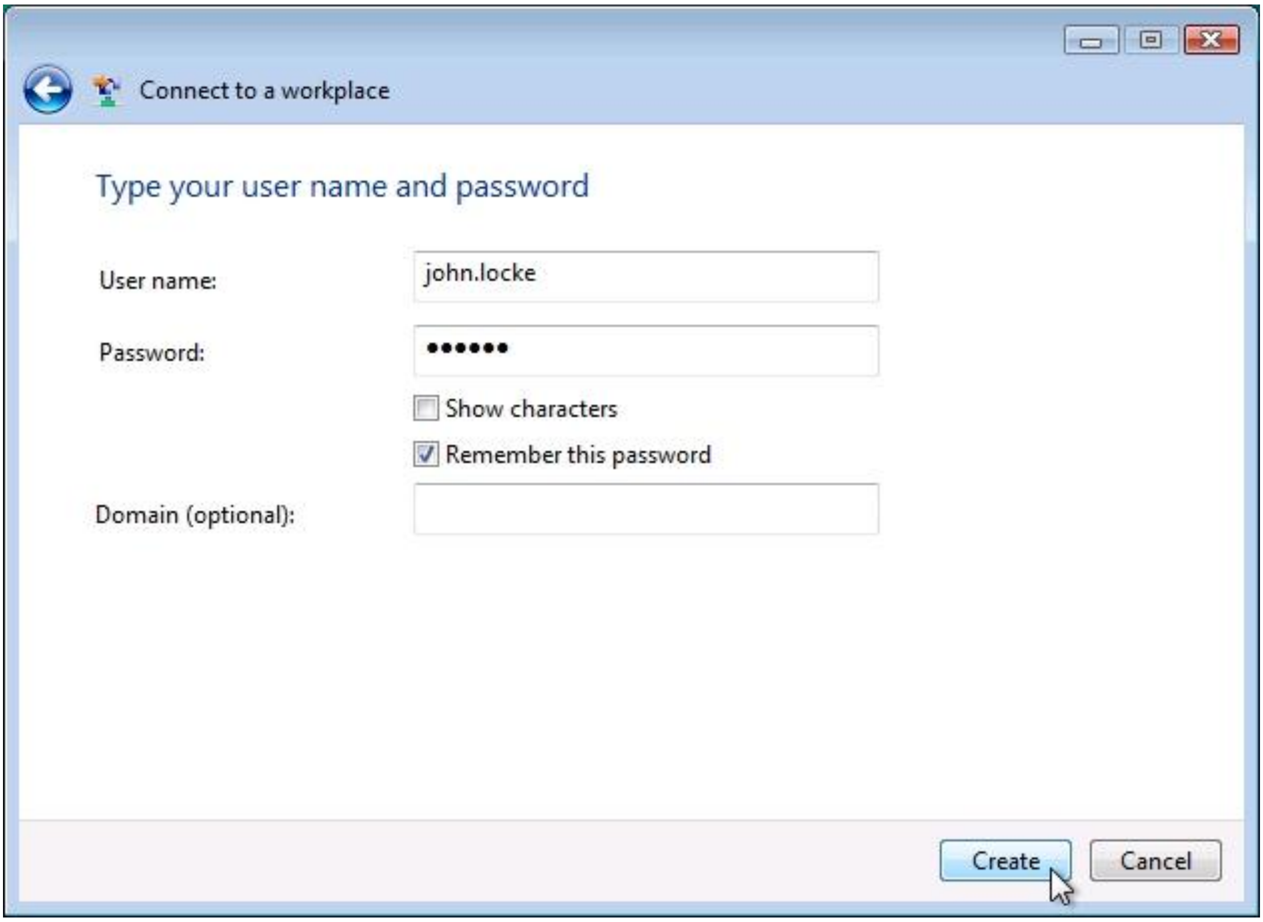
Select: **Don’t connect now…**

then click: **Next >**

Enter the same username and password as you use for the Pushex Exchange server.

Select: **Remember this password** if you wish.

Leave the **Domain (optional):** box blank.



Connect to a workplace

Type your user name and password

User name: john.locke

Password: ••••••

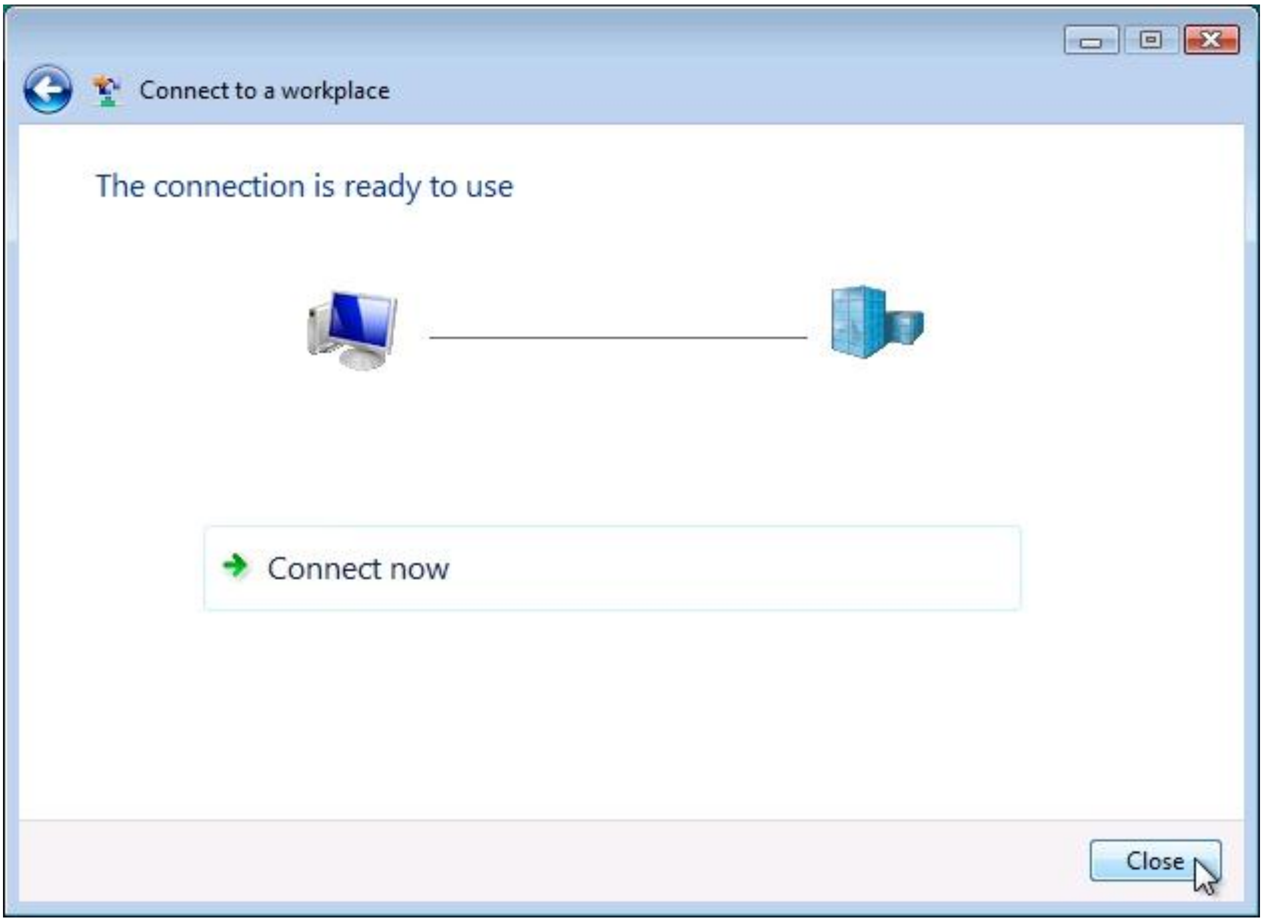
□ Show characters

☑ Remember this password

Domain (optional):

Click: **Create**

The VPN connection is now setup.



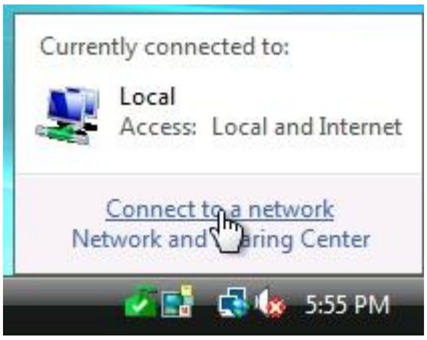
Connect to a workplace

The connection is ready to use

Click: **Close**

2 – Connecting to the VPN

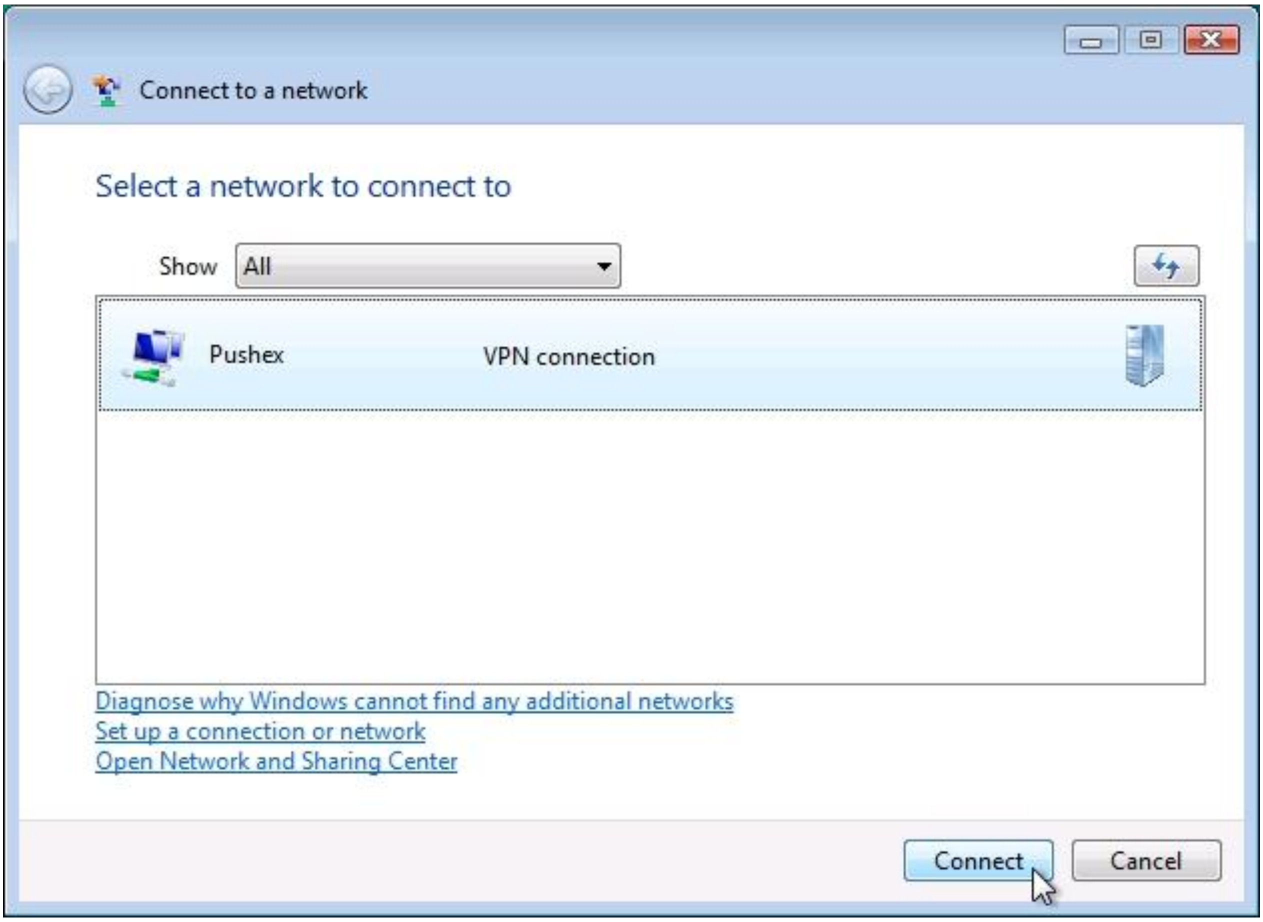
Click on the Network icon in the Notification Area, then click: **Connect to a network**



Currently connected to:

Local
Access: Local and Internet

Select **Pushex** and then click **Connect**



Select a network to connect to

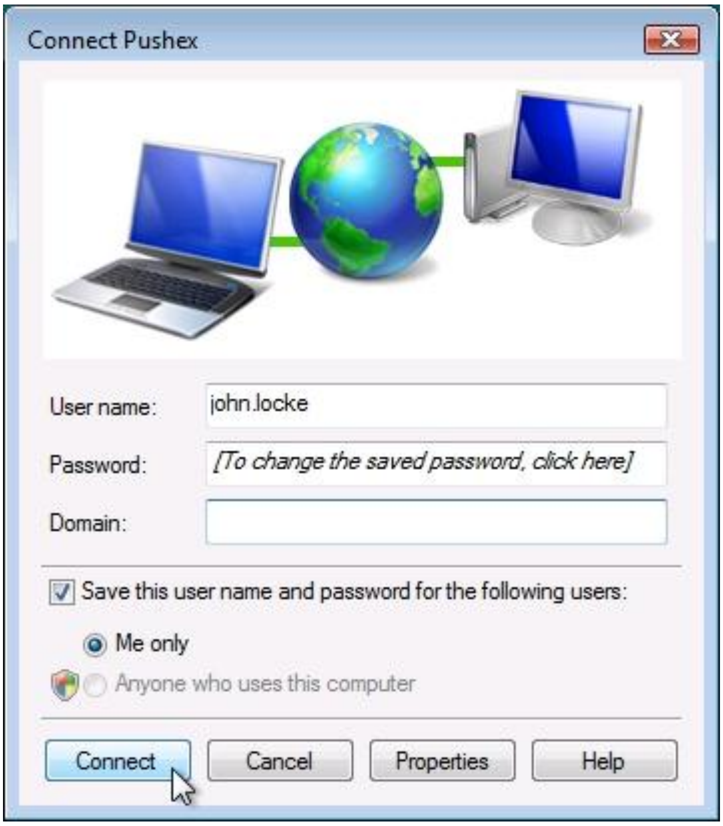
Show: All

Pushex	VPN connection

Diagnose why Windows cannot find any additional networks
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

This is where you can access all the VPN connection properties, by clicking **Properties**, but usually all the default settings work fine, so just:-

Click: **Connect**



Connect Pushex

User name: john.locke

Password: *[To change the saved password, click here]*

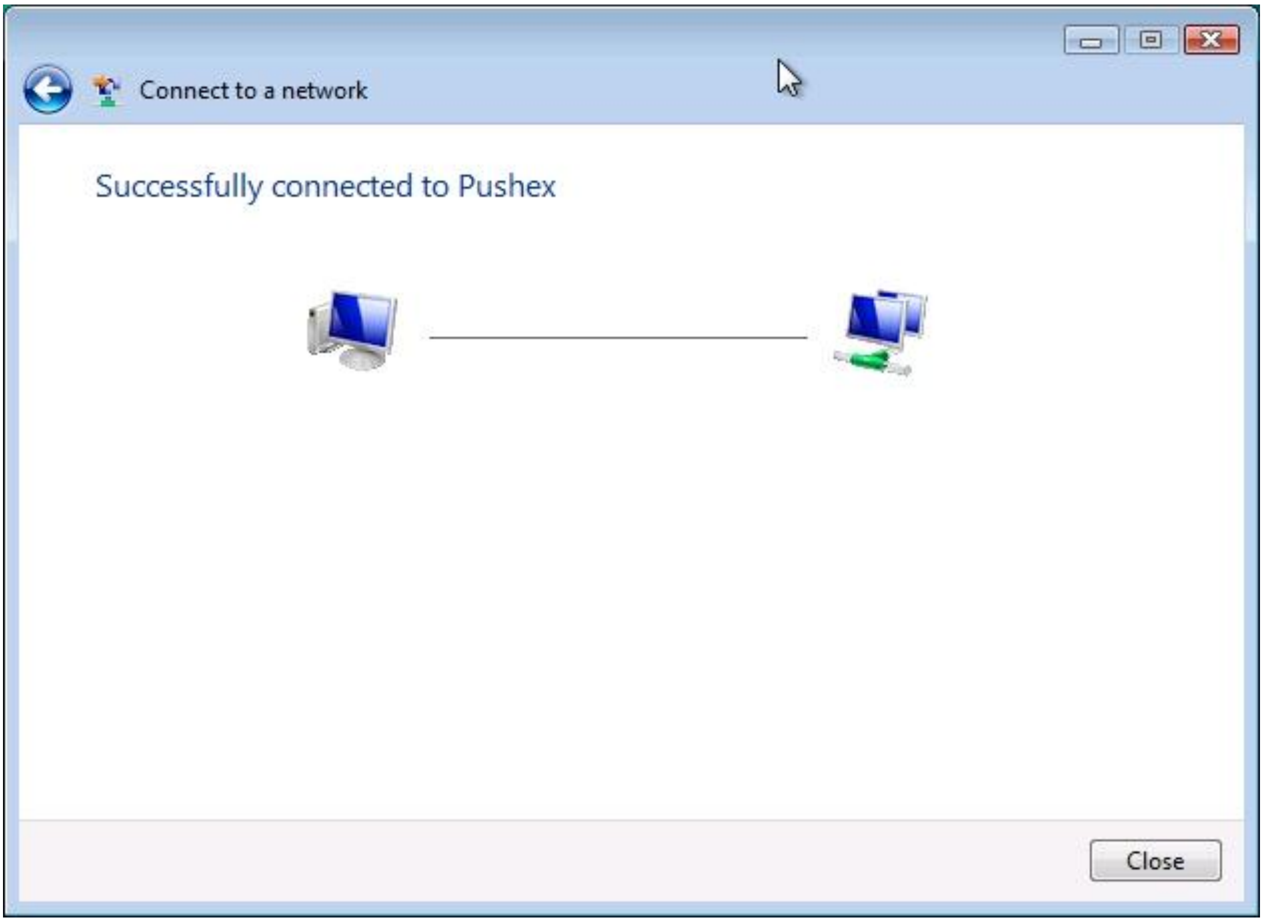
Domain:

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

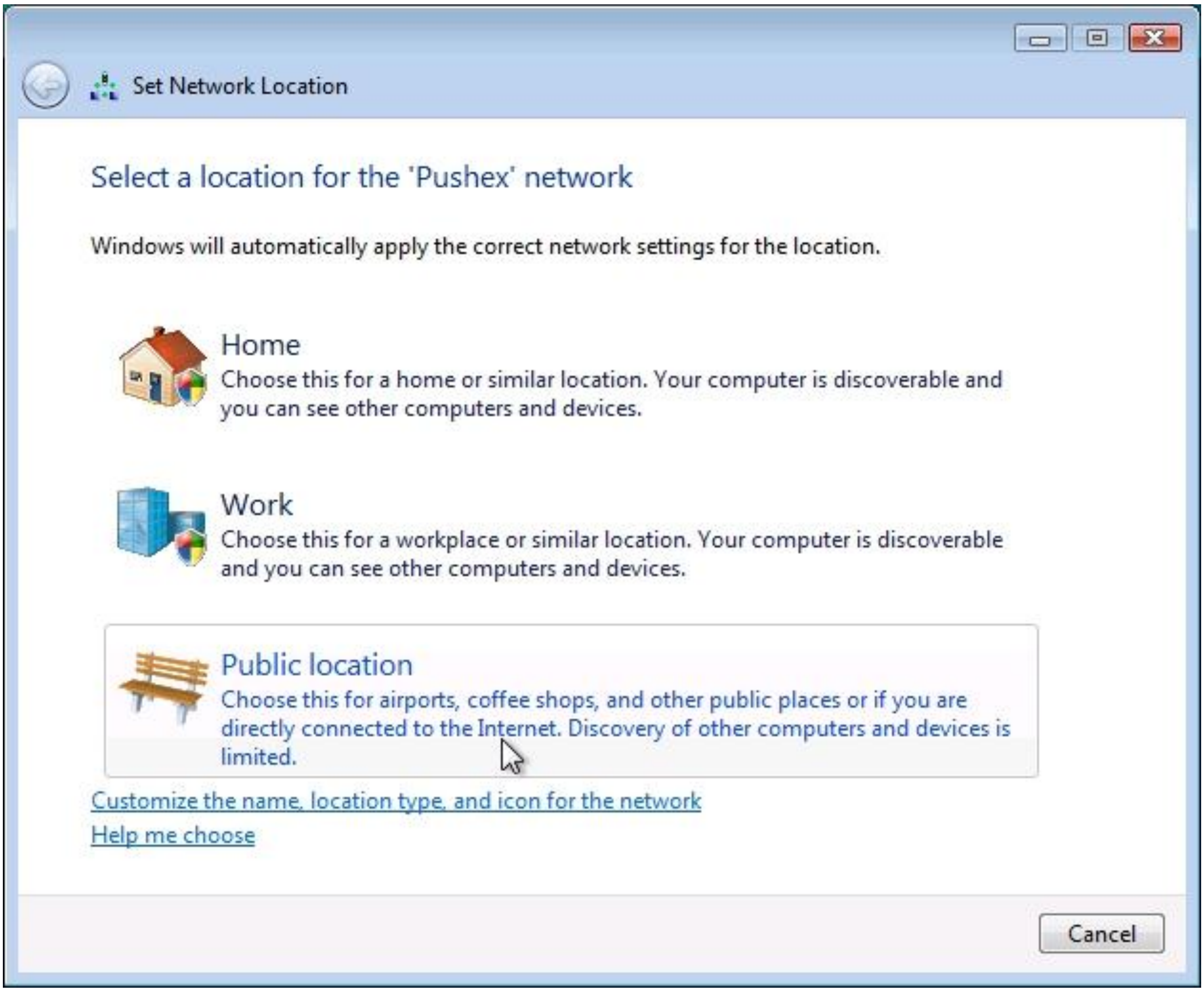
After a few seconds you should get the screen shown below, click: **Close**:-



Connect to a network

Successfully connected to Pushex

The first time you connect, Windows Firewall will popup this message asking you to classify this network connection:-



Set Network Location

Select a location for the 'Pushex' network

Windows will automatically apply the correct network settings for the location.

Home
Choose this for a home or similar location. Your computer is discoverable and you can see other computers and devices.

Work
Choose this for a workplace or similar location. Your computer is discoverable and you can see other computers and devices.

Public location
Choose this for airports, coffee shops, and other public places or if you are directly connected to the Internet. Discovery of other computers and devices is limited.

Customize the name, location type, and icon for the network

Help me choose

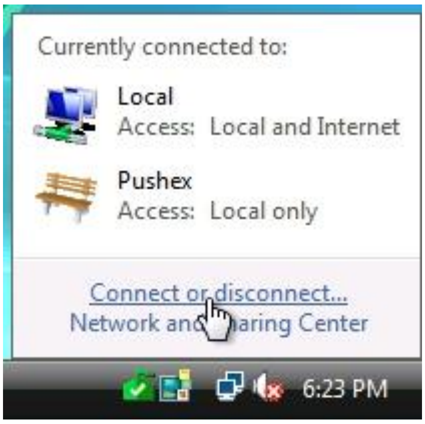
Public location is probably the best choice.

When connected, to check that your PC is sending all its Internet traffic over the VPN, go to the website:-

http://www.whatismyipaddress.com

and it should show your computer as being located in the UK.

To disconnect from the VPN, click the Network icon in the Notification Area, and then click **Connect or disconnect…**



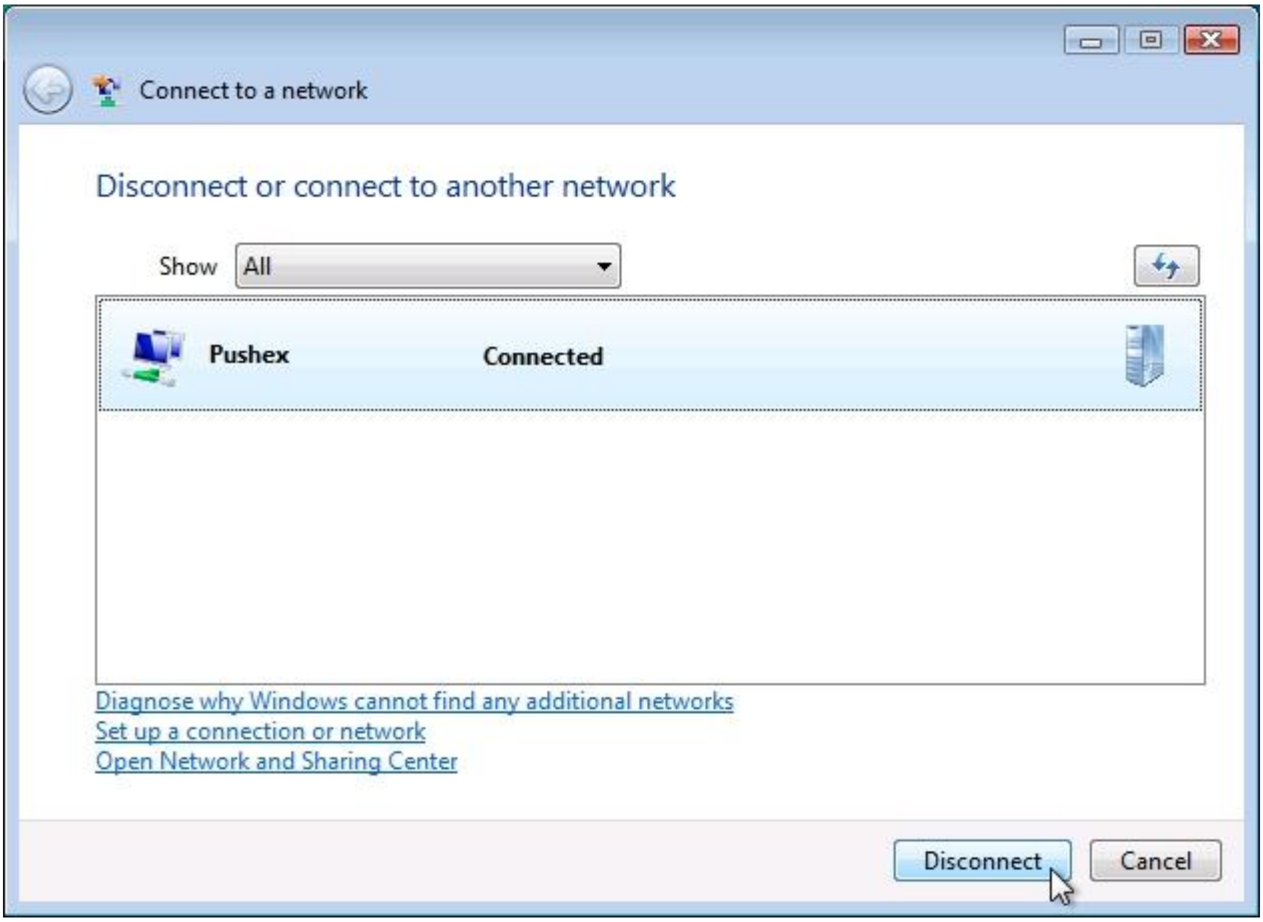
Currently connected to:

Local
Access: Local and Internet

Pushex
Access: Local only

Connect or disconnect...
Network and Sharing Center

Select **Pushex** and then click: **Disconnect**



Connect to a network

Disconnect or connect to another network

Show: All

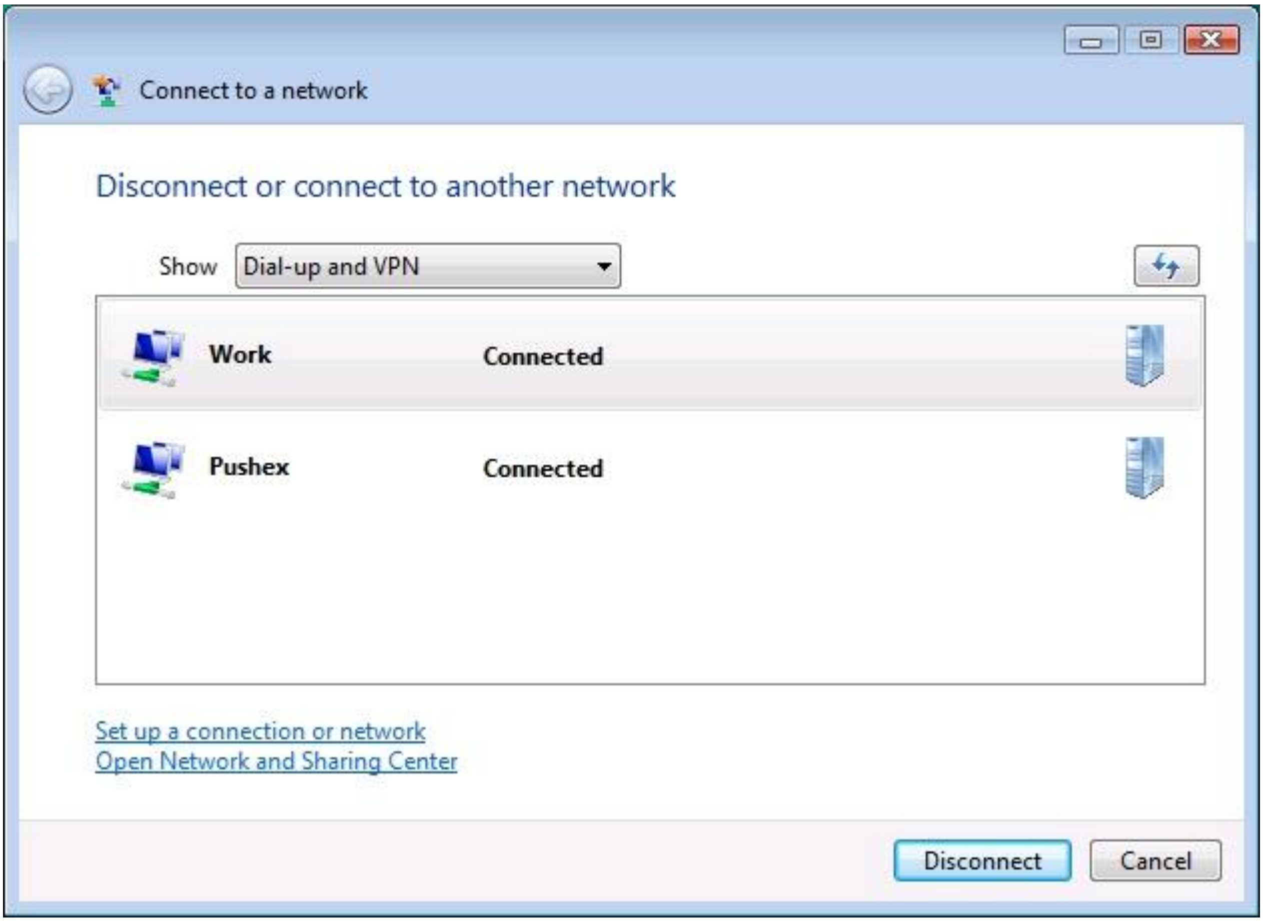
Pushex	Connected

Diagnose why Windows cannot find any additional networks
Set up a connection or network
Open Network and Sharing Center

3 – The VPN over VPN trick

It’s so amazing that this actually works we’ve given it a section of its own.

If your work has a VPN setup for you to access company files when you’re away from the office, you may find that it can’t always connect. This is because most VPNs need specific ports to be open on any firewalls they pass through and these ports can sometimes be blocked, either on purpose or through ignorance.
An SSTP VPN uses Port 443 which is almost certain to be open on all firewalls.
What you can do, therefore, is to first make an SSTP VPN to our servers and then make a second VPN connection to your office, over our SSTP VPN, which has all the ports open that your VPN requires.
The picture below shows two VPNs connected simultaneously:-



Connect to a network

Disconnect or connect to another network

Show: Dial-up and VPN

Work	Connected
Pushex	Connected

Set up a connection or network
Open Network and Sharing Center
Disconnect
Cancel

This also works on a Mac running Windows Vista using Parallels. You first make an SSTP connection with Windows Vista and then make a PPTP connection from the Mac OS.

We haven’t tested all types of VPN to see if they will connect over an SSTP VPN connection.

4 - Troubleshooting Tips

Certificate Revocation List problem

A valid commercial digital certificate is required on our VPN server to make an SSTP connection, which, of course, we have in place.
Valid means the certificate was issued by an authority Windows trusts, the name on the certificate is **vpn.pushex.com** and the certificate hasn't expired.
It could be possible that someone's stolen our certificate from us and is using it to ***pretend*** to be our company.
When a certificate is stolen or compromised in some way, it can be reported to the issuer who will then revoke the certificate and, until it expires, add it to its list of invalid certificates on the Certificate Revocation List or CRL.

So, before Windows will allow an SSTP connection to connect, it goes out onto the Internet to check the CRL to see if our certificate is on it. It isn't, of course, but it's possible that there could be a problem downloading the CRL from your location.

If Windows can't access the CRL then it will refuse to make the VPN connection – simple as that.

The CRL checking process usually works without a hitch but, if you ever get an error message about a CRL problem, or you just want to save a few seconds during the connection process, you can tell Windows not to bother checking the CRL.

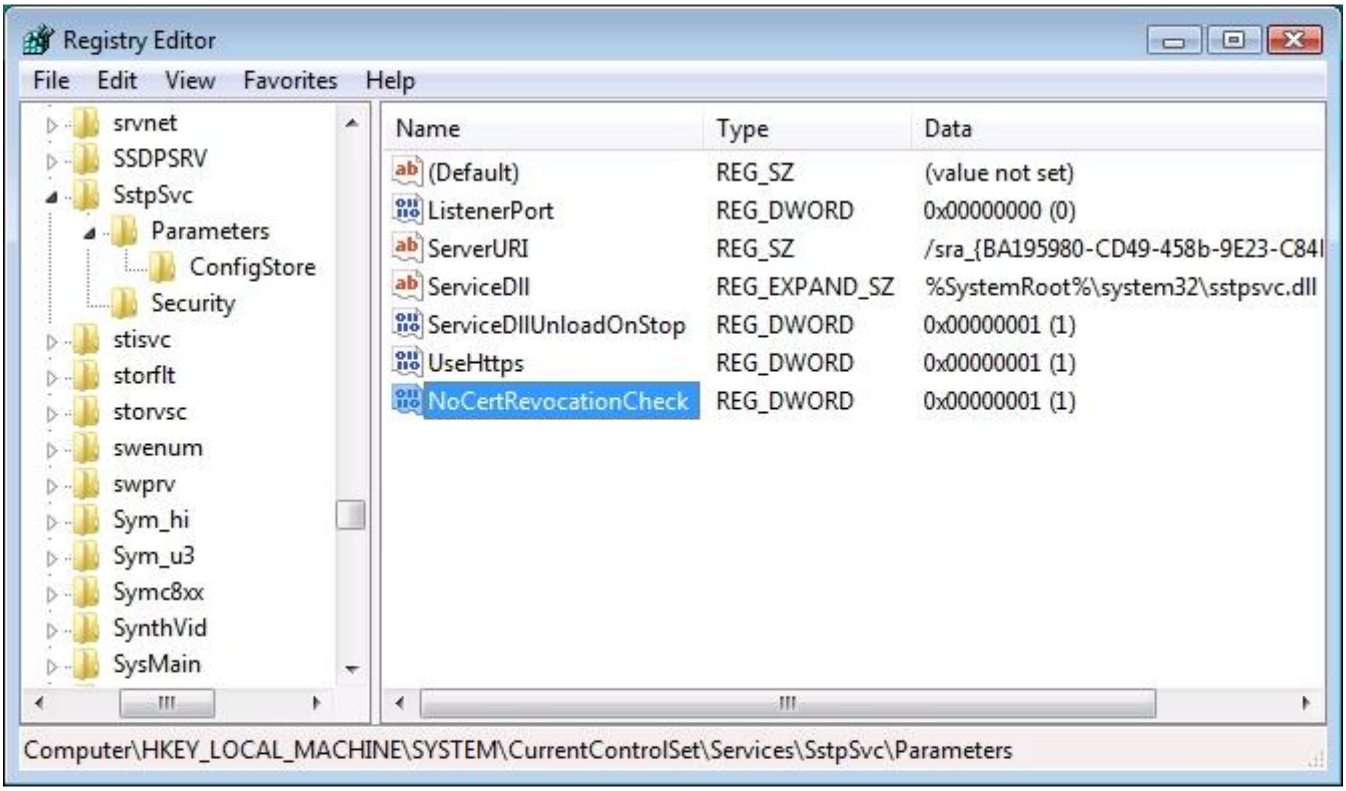
To disable CRL checking you need to edit the Windows registry.
The Registry contains settings which, if changed or deleted, can stop your PC functioning.
Don't be put off by this warning, just make the changes carefully.

To run the Registry Editor click: **Start** and type **regedit** into the Search box, then press **Enter**

Navigate to the key:-

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Sstpsvc\Parameters

Create a new REG_DWORD value called **NoCertRevocationCheck** and set its value to **1**



Name	Type	Data
(Default)	REG_SZ	(value not set)
ListenerPort	REG_DWORD	0x00000000 (0)
ServerURI	REG_SZ	/sra_{BA195980-CD49-458b-9E23-C84I
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\system32\sstpsvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)
UseHttps	REG_DWORD	0x00000001 (1)
NoCertRevocationCheck	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SstpSvc\Parameters

Click: **OK** and then **File – Exit** to quit the Registry Editor.

To save you having to edit the Windows Registry, we have a file you can download to create the required registry value automatically.

Download this file:-

http://support.pushex.com/files/NoCertRevocationCheck.reg

Save it to your Desktop and then double-click on it.
Click: **Yes** to the warnings and the required value will be added to your registry.

DNS Server Problems

DNS servers convert website names, such as **www.google.com**, into numeric IP addresses, such as **209.85.229.104**

There are several reasons why you want to use the DNS servers on our VPN servers, rather than your local DNS servers, when the VPN is connected:-

1. Your ISP might be giving you the wrong answers to DNS lookup requests, ***on purpose***, as an easy way to block access to particular sites.
2. Your ISP could be logging all your DNS requests to check what you are doing.
3. Your ISP could, quite legitimately, be sending you to, for example, your nearest Hotmail server when what you ***actually*** want, to get the speediest response, is the Hotmail server located nearest to our VPN servers.

Unlike Windows XP, there's usually ***no problem*** with Windows Vista using the VPN server's DNS servers when connected, and then your local DNS servers when not connected.
All this section is doing, therefore, is to show you a simple way to check which DNS servers your computer is using.

When you're connected to the VPN, you can check that you're using the DNS servers on the VPN server by typing the following into your browser:-

http://www.dns.test

The top-level domain **test** doesn't exist and so no DNS servers on the Internet will be able to find the required IP address, which means the webpage will fail to load.
We've added a dummy record to the DNS servers on our VPN servers so, if your PC is using our DNS servers, the webpage ***will*** load correctly.