



Windows XP Service Pack 2 Cisco Software Client VPN

EbisExchange Confidential and Proprietary

This document and the information contained therein are confidential to and the property of EbixExchange Australia Pty Ltd. This information is made available to Sunrise customers for the sole purpose of conducting the company's business and is not to be disclosed without prior written consent. All rights reserved.

Windows XP Service Pack 2 Cisco Software Client VPN

© EbixExchange Australia Pty Ltd 2008

Disclaimer:

Every effort has been made to provide accurate and complete information. However, EbixExchange Australia Pty Ltd assumes no responsibility for any direct, indirect, incidental or consequential damages arising from the use of the information in this document. Data and case-study examples are intended to be fictional.

Copyright:

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means electronic, mechanical photocopying, recording, or otherwise without written permission from EbixExchange Australia Pty Ltd.

This manual was produced using Windows XP Professional and Microsoft Word 2003

Last Updated: 18/03/08

1	Introduction	1
2	Deactivating Windows Firewall	1
3	Configuring the VPN and Windows Firewall	2
3.1	Before You Begin	2
3.2	Configure the VPN Client to use UDP.....	3
3.3	Adding an Exception to Windows Firewall.....	5
	Adding a Program Exception.....	5
	Adding Port Exceptions	8

1 Introduction

Microsoft has released a major security update for Windows XP called Service Pack 2. This update contains many fixes and enhancements to increase security on Windows XP. For more information on the features added in Service Pack 2, please refer to the Microsoft website <http://www.microsoft.com/windowsxp/sp2/features.mspx>.

As a result of installing Windows XP Service Pack 2, the Windows Firewall is switched on by default. This firewall automatically blocks certain incoming and outgoing connections from establishing, including the Cisco Software Client VPN used by Sunrise™ Exchange.

EbixExchange has conducted internal testing to establish a solution to the blocking of the Cisco Software Client VPN by the Windows Firewall. From the results of our internal testing, we are able to offer the following options to help overcome this issue.

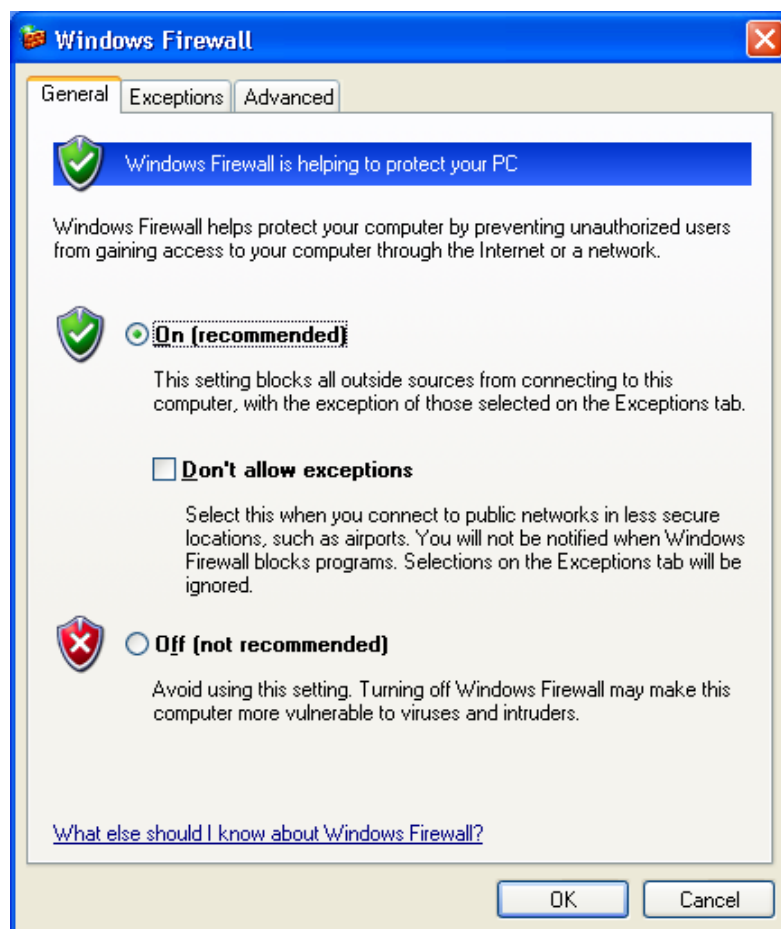
2 Deactivating Windows Firewall

You may already have existing firewalls in place on individual PC's, your network, or your router. At your computer technician's discretion, you may decide that you do not wish to use the firewall that comes with Windows XP.

If this is the case, your technician may switch the Windows Firewall off by completing the following:

Click **Start** and select **Control Panel**.

Double Click on **Windows Firewall**. The following window will appear:



Select **Off** and click **OK**.

You should now find the VPN Client will be able to connect.

3 Configuring the VPN and Windows Firewall

If you wish to have Windows Firewall activated, it is possible to configure the Cisco Software Client VPN and Windows Firewall to allow the VPN to connect.

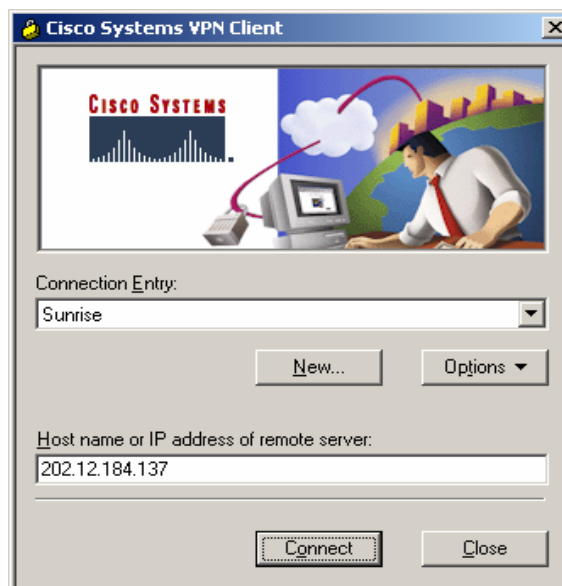
3.1 Before You Begin

Before you can begin, you will need to know which version of the Cisco Software Client VPN you are running.

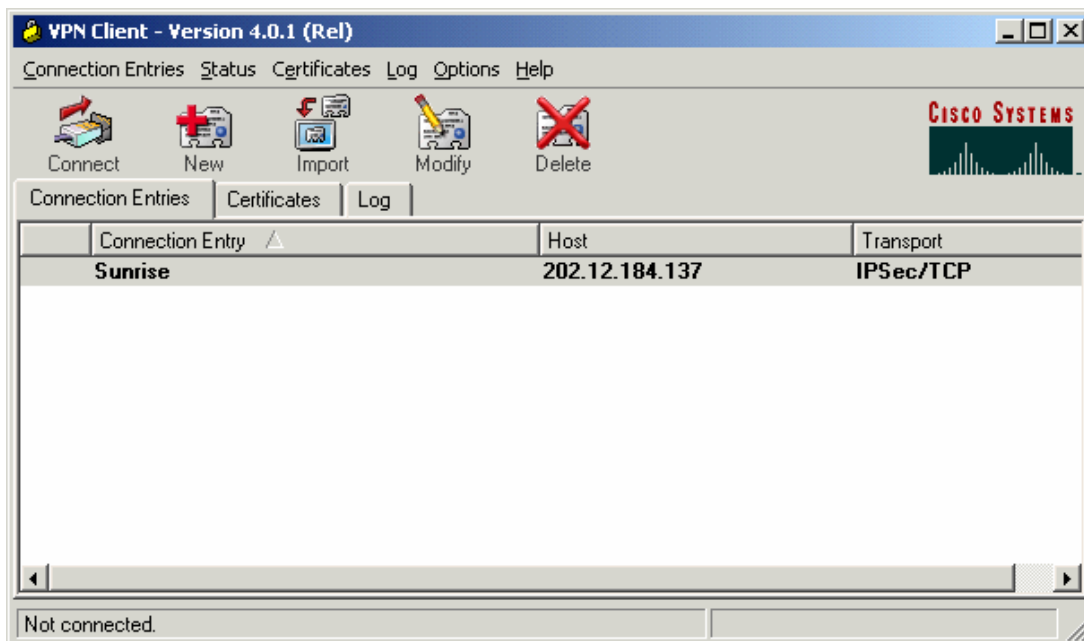
To check your Cisco VPN client version, double click on your VPN icon.



If the following screen appears, your VPN version is **3.6**.



Alternatively, if your screen looks similar to the one below, your VPN version is **4.0.1** or higher.

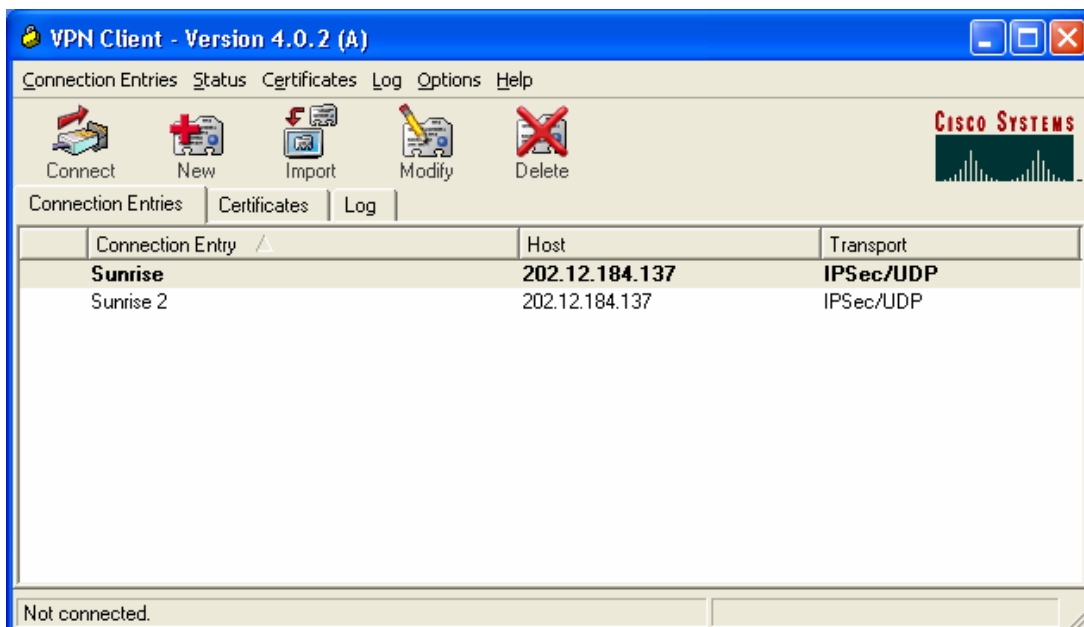


3.2 Configure the VPN Client to use UDP

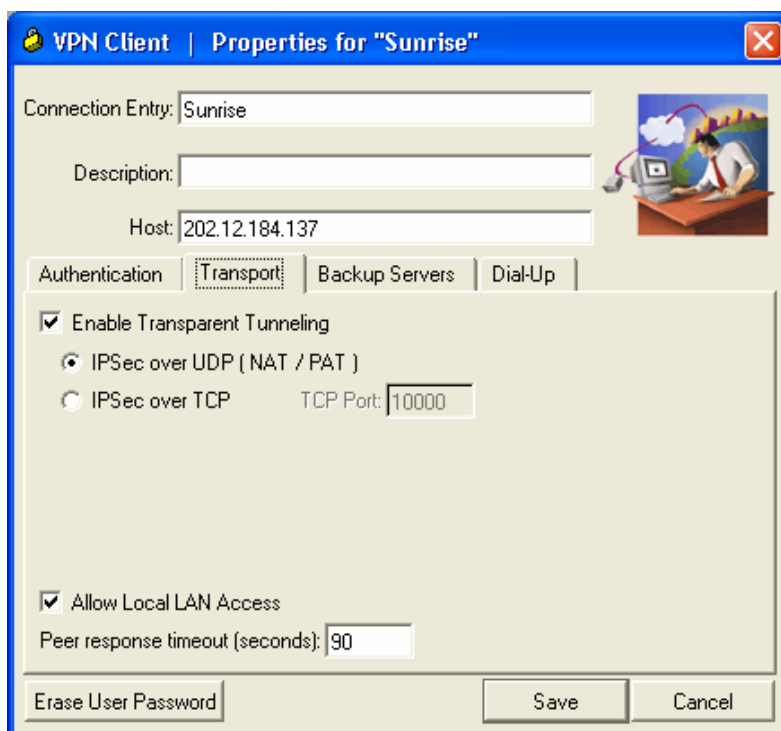
In order to use the Cisco Software Client VPN in conjunction with the Windows firewall, the Cisco Software Client VPN must be configured to use the UDP protocol.

VPN Client v4.0.1 (or above):

Start the VPN Client.



Click Modify.



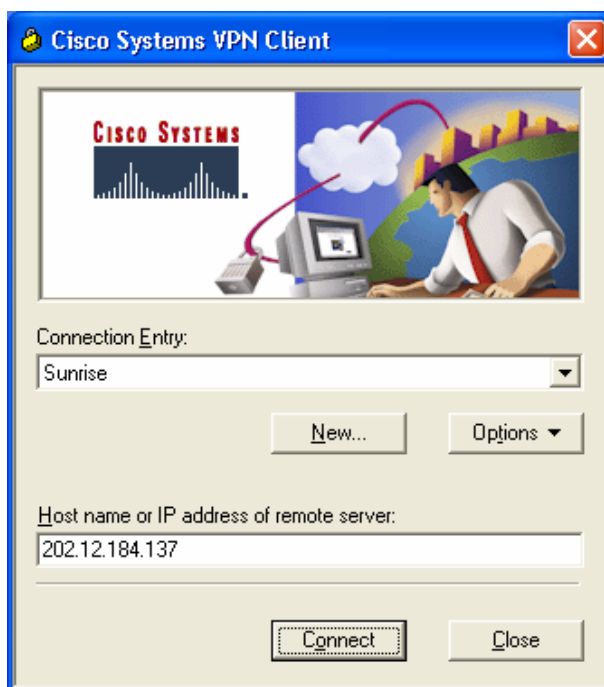
Click Transport.

Ensure that IPSec over UDP (NAT / PAT) is selected.

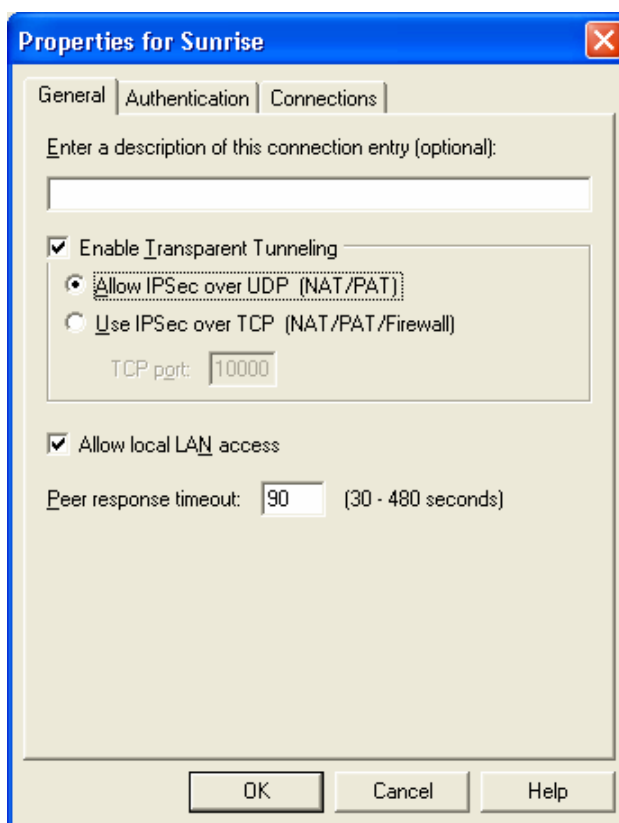
Click Save.

VPN Client v3.6 users:

Start the VPN Client.



Click on **Options**, and select **Properties**.



Select the **Authentication** tab.

Ensure that **Allow IPsec over UDP (NAT / PAT)** is selected.

Click **OK**.

3.3 Adding an Exception to Windows Firewall

Note:

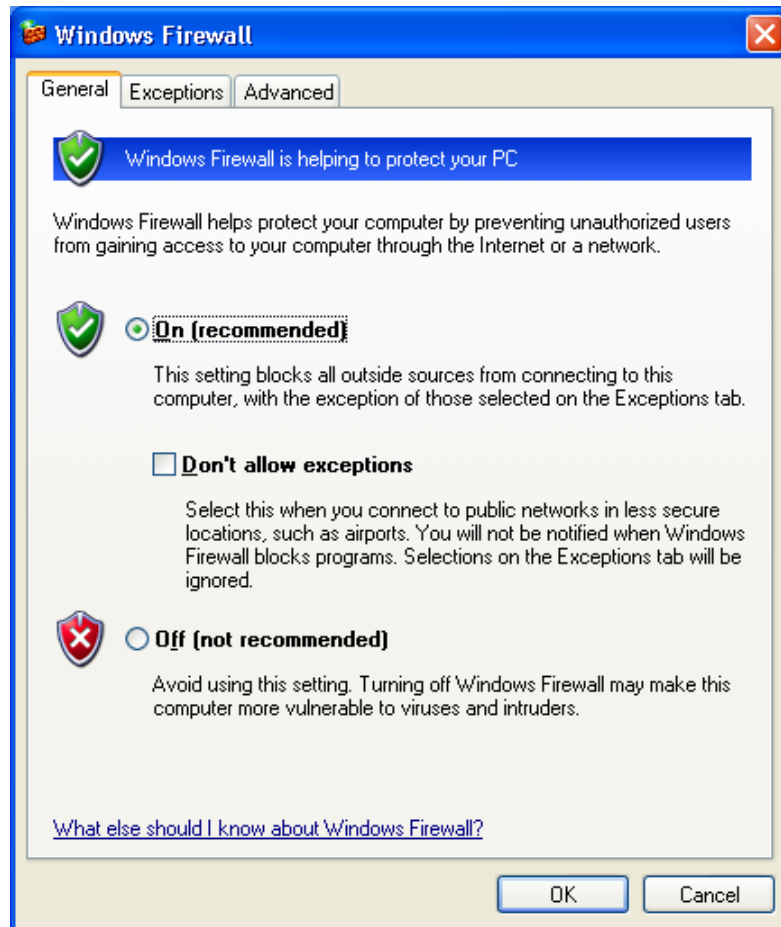
If you are using **Cisco VPN Client 4.0.2(a)**, you do not need to perform the following steps. You should find that the VPN Client should now connect successfully.

For all other versions of the Cisco VPN Client, the Windows Firewall must be configured to allow the VPN Client to pass through. You will need to try one (or both) of the following methods.

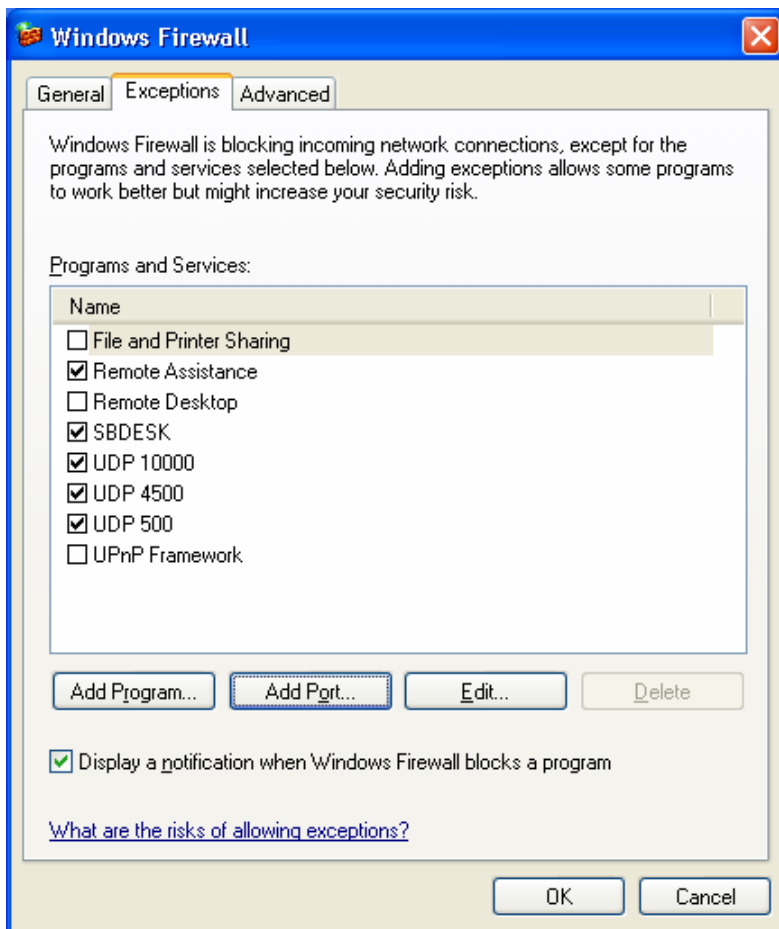
Adding a Program Exception

Click **Start** and select **Control Panel**.

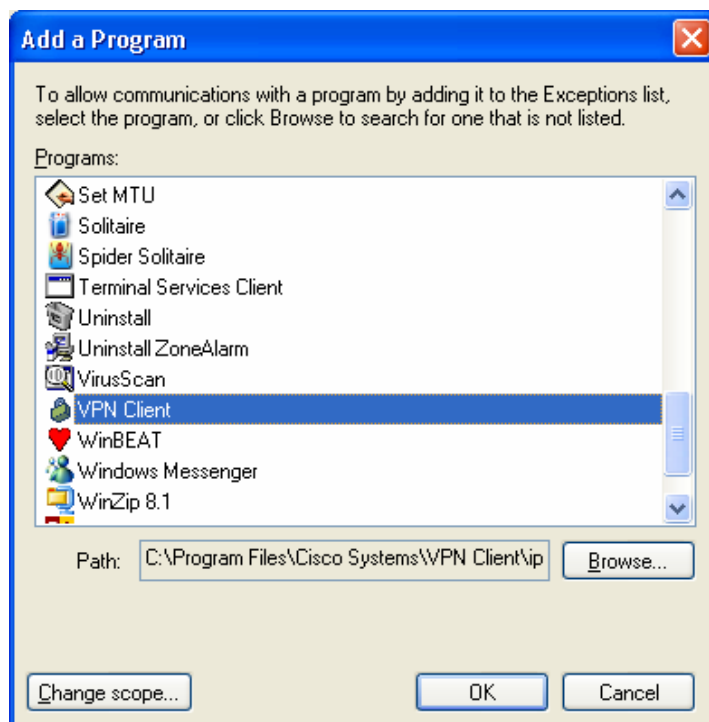
Double Click on **Windows Firewall**. The following window will appear:



Select the Exceptions Tab.



Click Add Program.



Look for **VPN Client** in the list of installed programs. If it exists, select it, and click **OK**. Proceed to the next step.

If **VPN Client** does not appear in the list, click Cancel. Proceed to *Adding Port Exceptions* section for further instruction.

You should now see **VPN Client** (with a tick beside it) listed under the **Programs and Services** section of the Exceptions window.

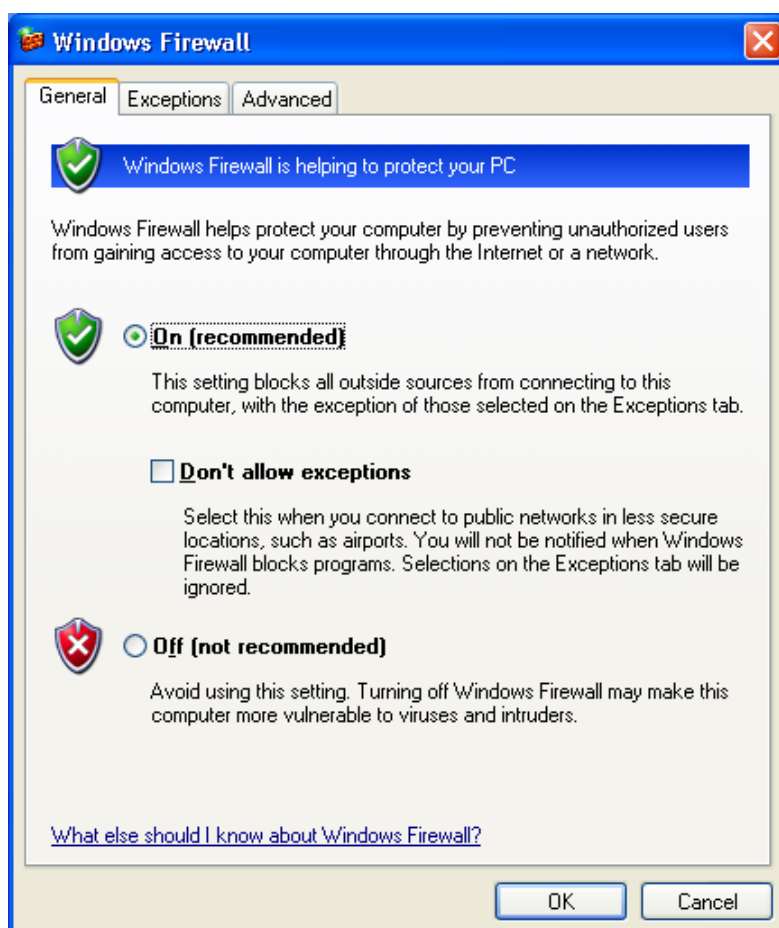
Click OK.

Attempt to connect to the VPN again. If you are still having difficulties connecting, proceed to *Adding Port Exceptions* section for further instruction.

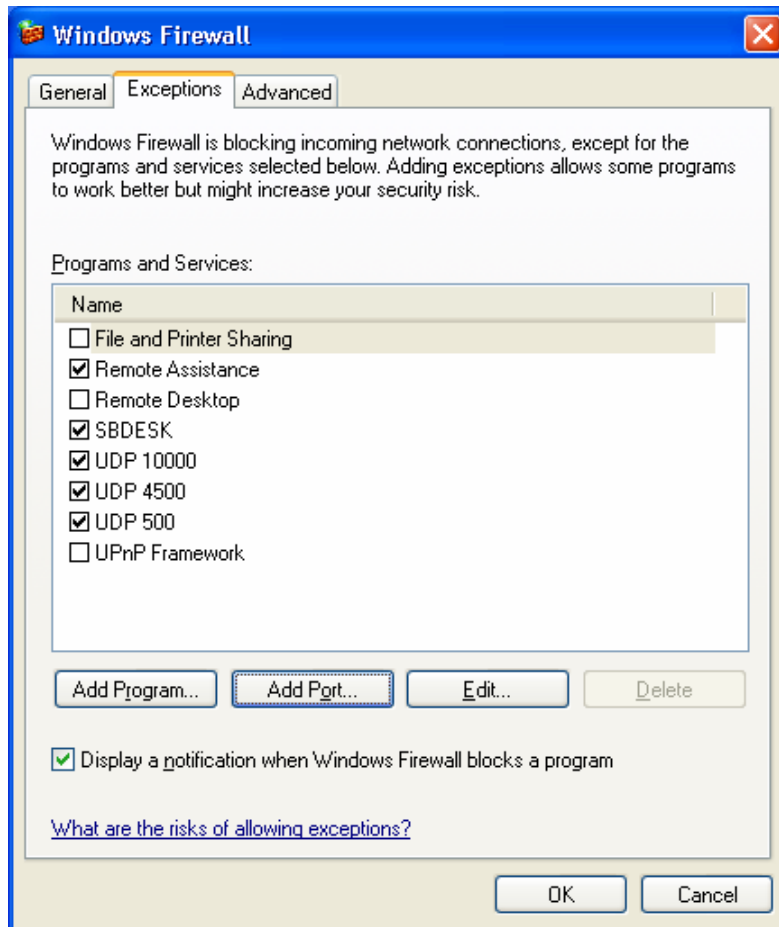
Adding Port Exceptions

Click **Start** and select **Control Panel**.

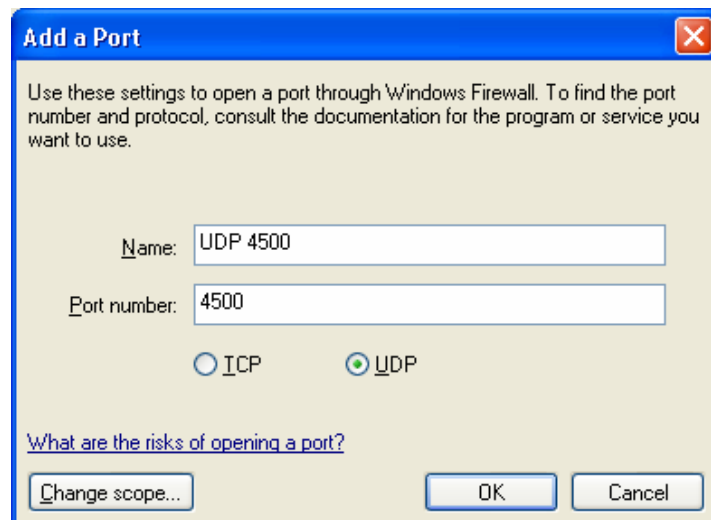
Double Click on **Windows Firewall**. The following window will appear:



Select the Exceptions Tab.



Click **A**dd **P**ort.



Enter **UDP 4500** in the **N**ame field.

Enter **4500** in the **P**ort number field.

Select **U**DP.

Click **O**K.

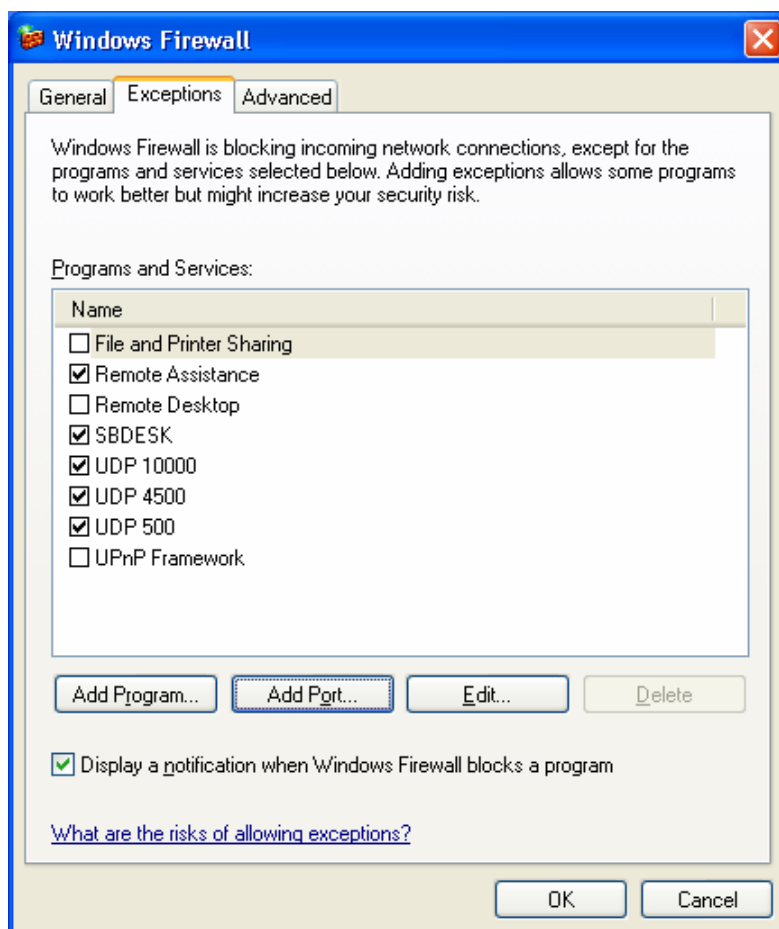
Repeat above, until all three of the following ports have been added:

UDP 4500

UDP 500

UDP 10000

When complete, all three ports should now appear under the **P**rograms and Services window with a tick beside them.



Click OK.

Attempt to connect to the VPN again.