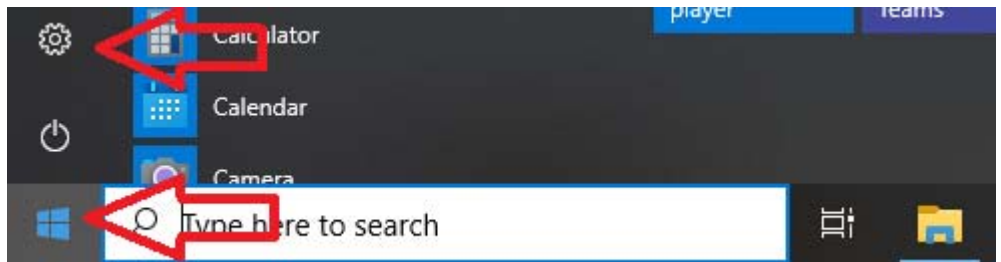
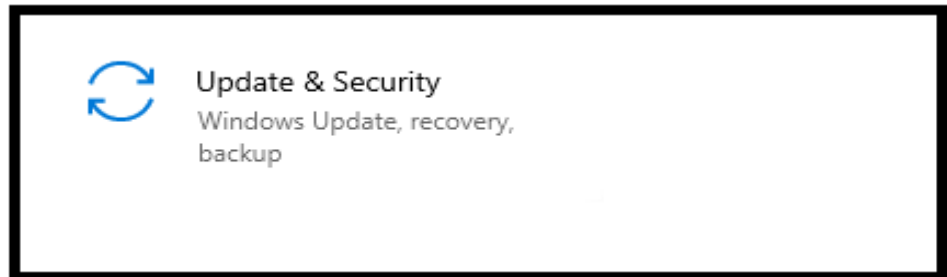


# Configuring Automatic Updates:

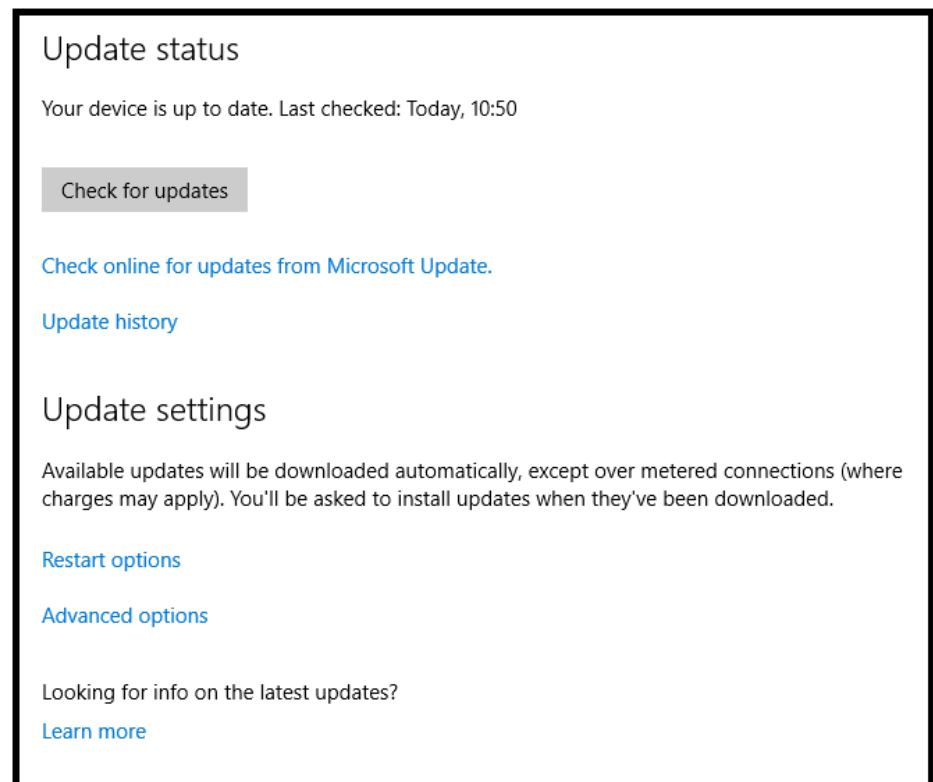
Press the Start button and choose the settings button.



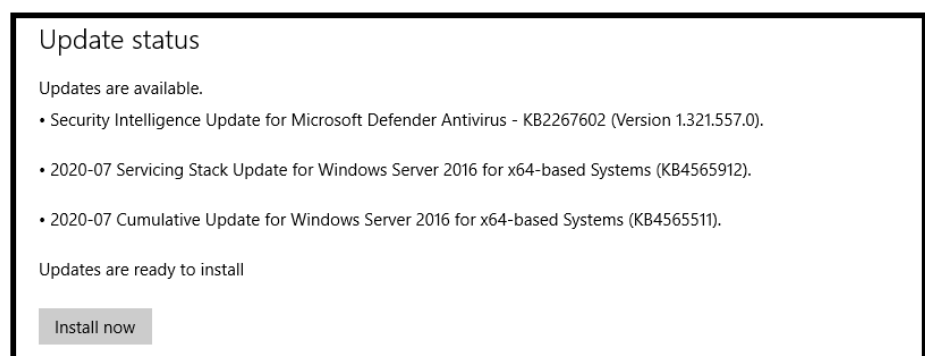
Click on Update & Security



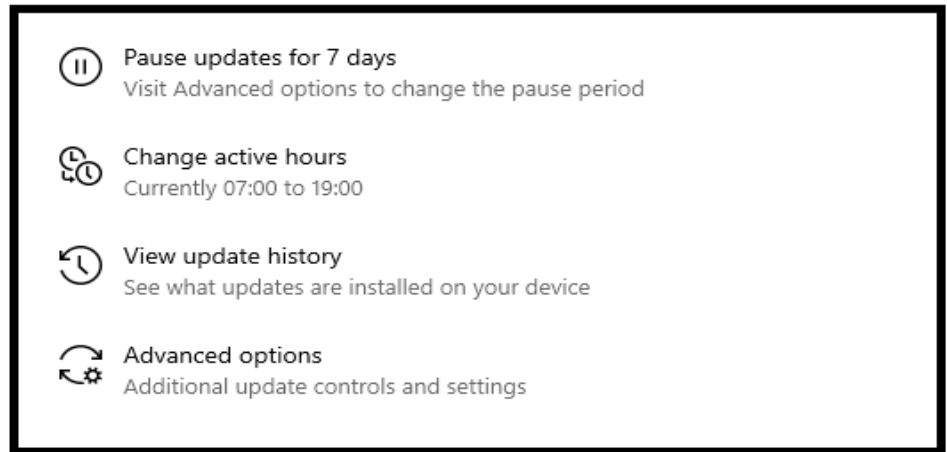
Click the Check for updates button and run update,



Install as required.



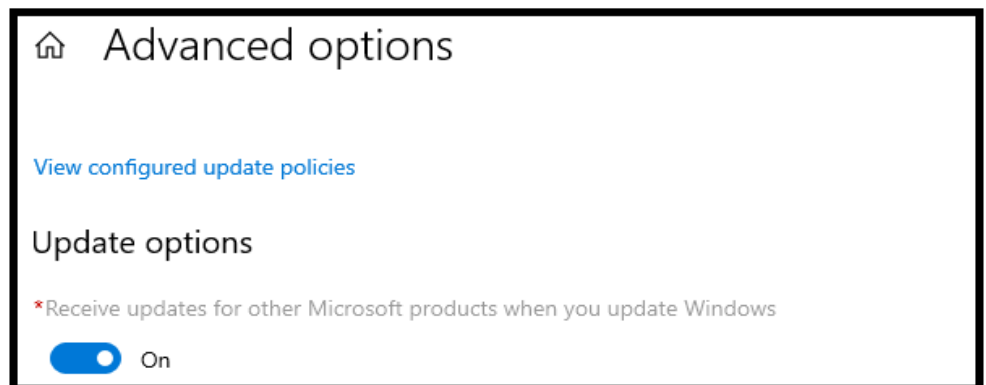
Click on the Advanced options button



A screenshot of the Windows Update 'Advanced options' menu. It contains four items, each with an icon and a description:

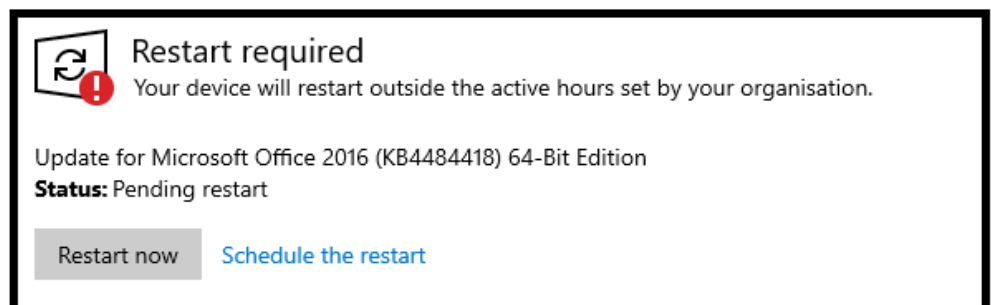
- Pause updates for 7 days**: Visit Advanced options to change the pause period
- Change active hours**: Currently 07:00 to 19:00
- View update history**: See what updates are installed on your device
- Advanced options**: Additional update controls and settings

Make sure that 'Receive updates for other Microsoft products' is turned on to receive Microsoft Office updates



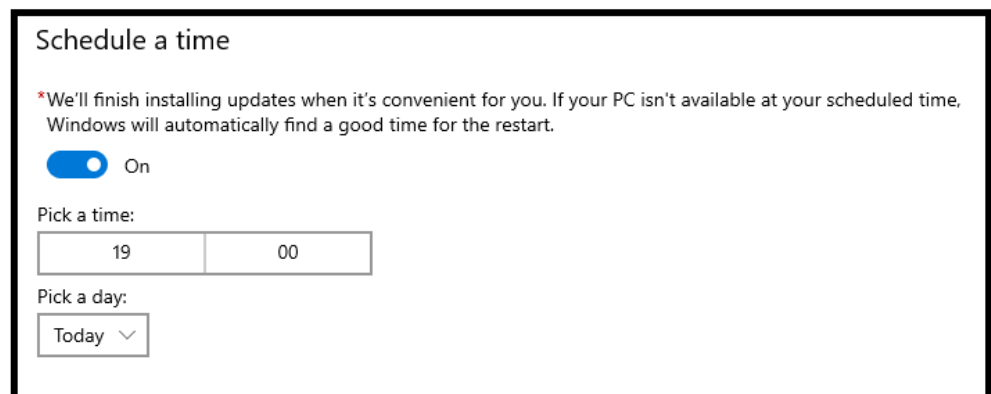
A screenshot of the Windows Update 'Advanced options' page. It features a home icon and the title 'Advanced options'. Below the title is a link: 'View configured update policies'. Underneath is the section 'Update options' with a sub-header: '\*Receive updates for other Microsoft products when you update Windows'. At the bottom, there is a blue toggle switch labeled 'On'.

You can either restart immediately if updates are ready or schedule a restart time.



A screenshot of a Windows Update notification titled 'Restart required'. It includes a circular icon with a refresh symbol and a red exclamation mark. The text reads: 'Your device will restart outside the active hours set by your organisation.' Below this, it specifies: 'Update for Microsoft Office 2016 (KB4484418) 64-Bit Edition' and 'Status: Pending restart'. At the bottom, there are two buttons: 'Restart now' (grey) and 'Schedule the restart' (blue).

Click Schedule the restart to choose a convenient time. Click the on button and choose the time and day.



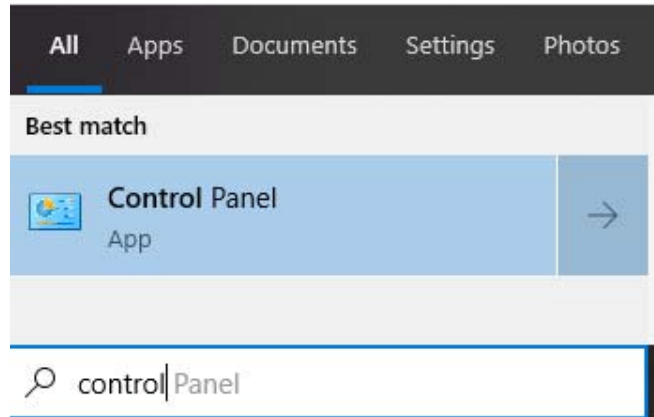
A screenshot of the 'Schedule a time' dialog box. It starts with a sub-header 'Schedule a time' and a note: '\*We'll finish installing updates when it's convenient for you. If your PC isn't available at your scheduled time, Windows will automatically find a good time for the restart.' Below the note is a blue toggle switch labeled 'On'. There are two input fields for 'Pick a time:'. The first field contains '19' and the second contains '00'. Below these is a 'Pick a day:' label and a dropdown menu showing 'Today' with a downward arrow.

# Configuring Windows Firewall:

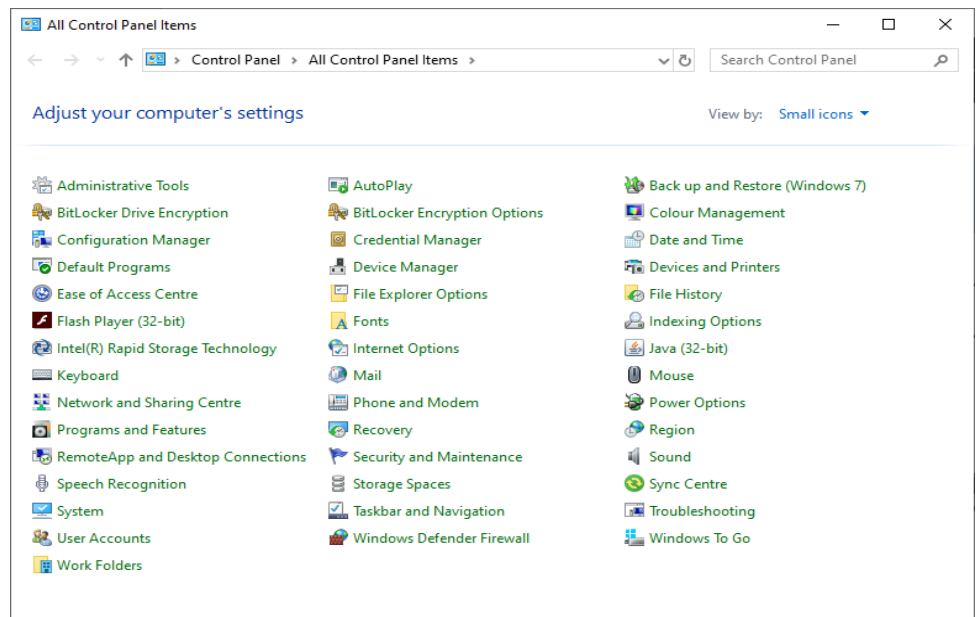
It monitors Inbound and can monitor outbound traffic, and has two ways of accessing it.

**The simple way**, you are only able to turn the **firewall on and off**, and **enable or disable** any exceptions already recorded by Windows.

Open the Control Panel by typing Control in the Search box and clicking on it.  
(For convenience, a number of Apps have been removed between Best match and the search bar).



In the Control Panel, click Windows Defender Firewall



Click **Change Notification Settings** or **Turn Windows Firewall on or off**

Go on to the next picture.



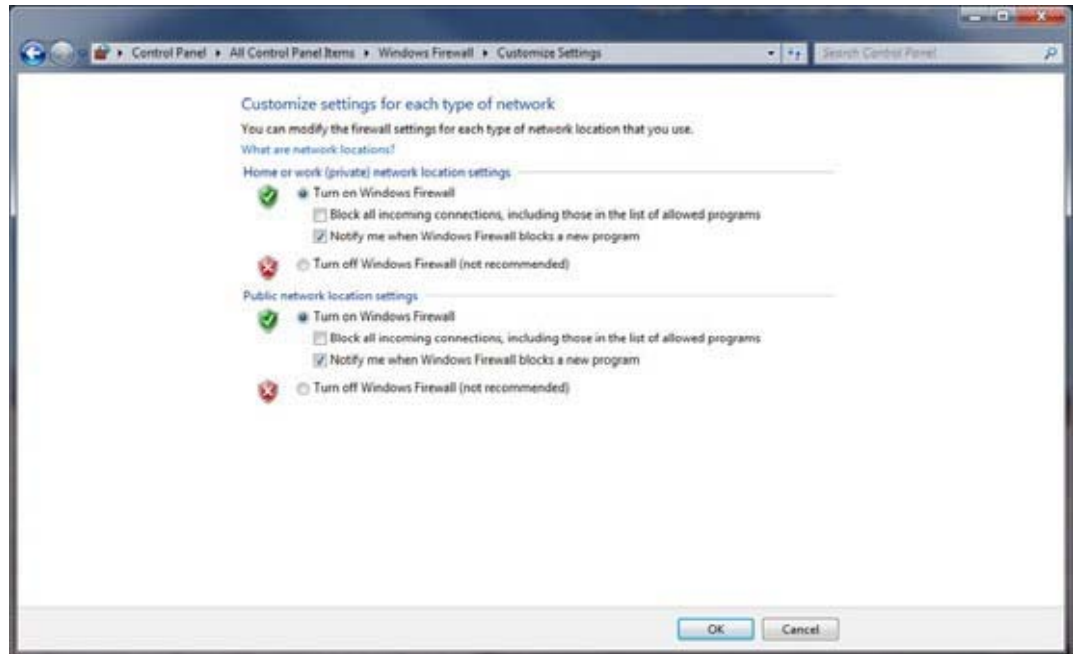
## Firewall Settings

Here, you can turn the Firewall On and Off, make sure it is **ON** for both the **Home or Work** and **Public network location settings** and that **Block all incoming connections** is not checked.

Tick the box, **Notify me when Windows Firewall blocks a new program** on both the **Home or Work** and **Public network location settings**

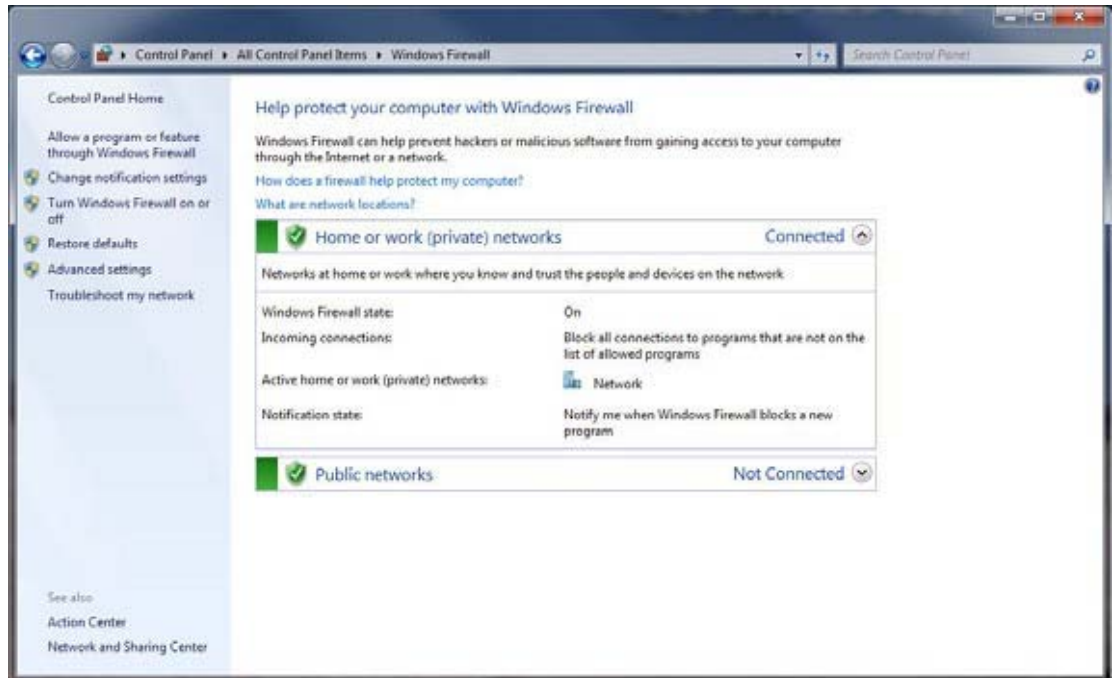
*Click ok*

*Go on to the next picture.*



Now click **Allow a program or feature through the Windows Firewall.**

*Go on to the next picture.*



## Firewall Settings – Allowed Programs

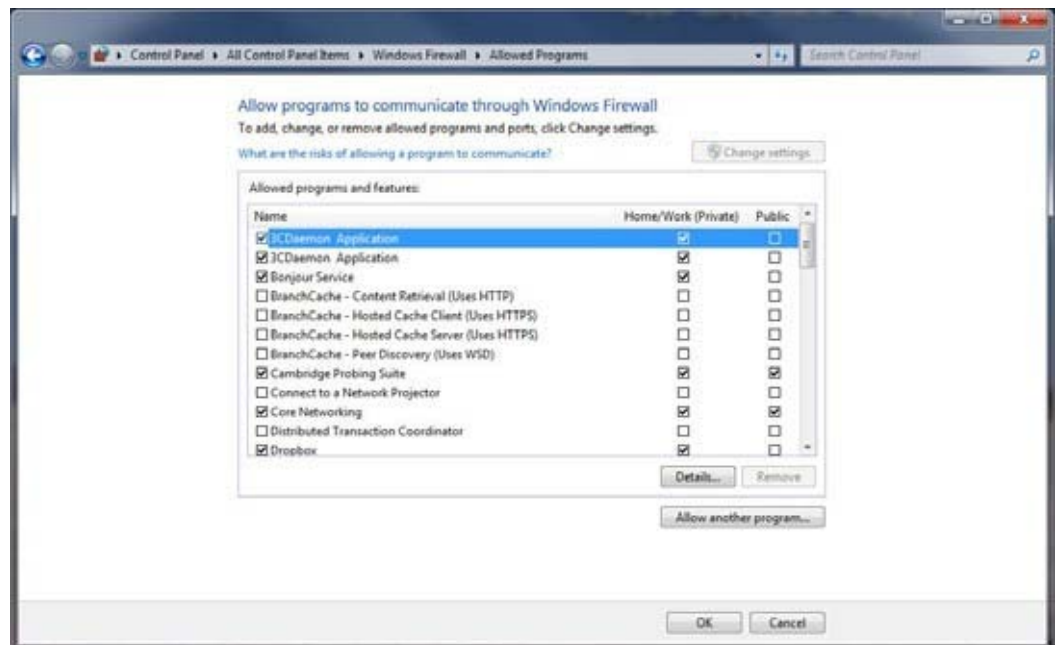
The list of Programs shown in this picture might differ from the ones you see.

If you chose to enable **File and Printer Sharing**, then you must ensure that **File and Printer Sharing** is checked here. Otherwise, for greater security, it should be unchecked.

Other entries in this list will be added automatically by Windows as you use the PC, or you may add them manually.

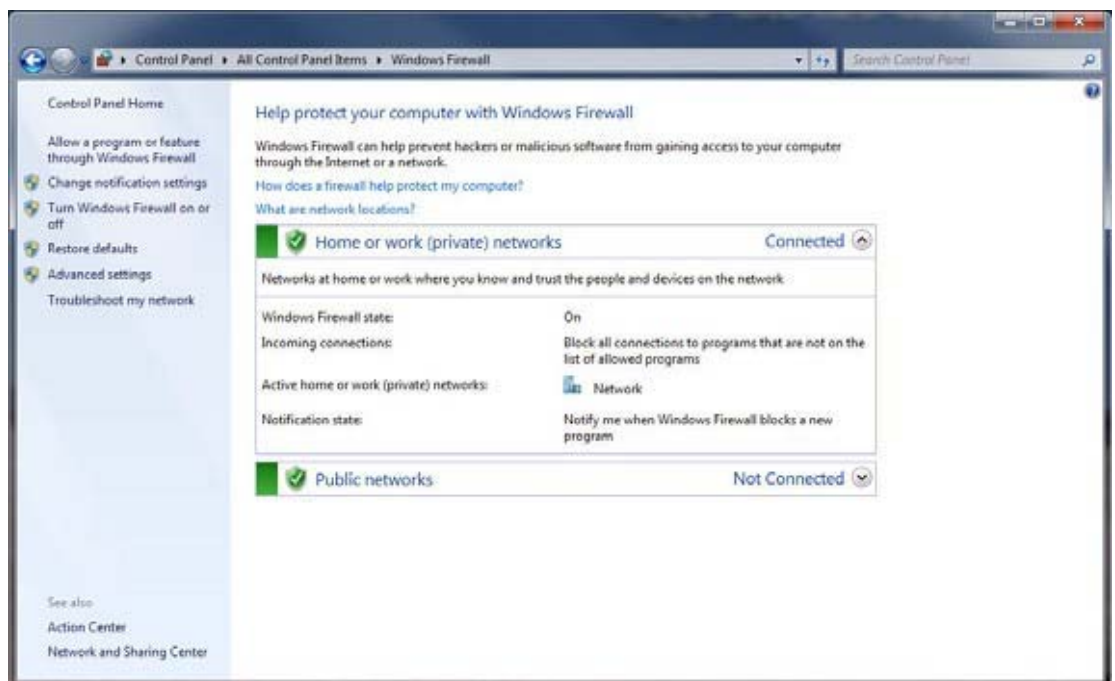
*Click ok*

*Go on to the next picture.*



Now click **Advanced settings**. This will take you to the next section to enable ICMP Echo request

*Go on to the next page.*



The **Windows Firewall** used to be configured **per User**, and only an **Administrator** could change the settings, now it has three types of possible profiles;

- **Domain**
- **Public**
- **Private**

The Firewall's behavior depends on which profile it chooses. The profile depends upon the type of network connection, which is why Microsoft recommends that you enable any rule for all three profiles.

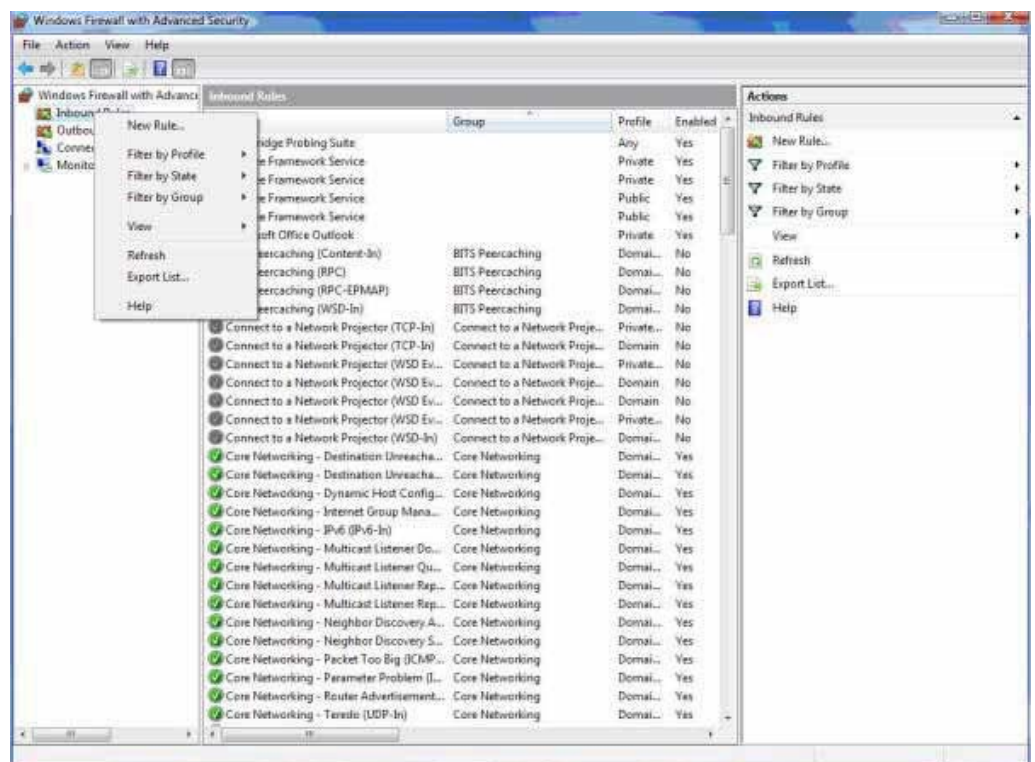
## Adding a New Rule to allow ICMP Echo Request (inbound ping) *REQUIRED for College use.*

After clicking **Advanced settings**, you will see this screen.



Highlight the **Inbound Rules** and **right click on it** and click **New Rule**

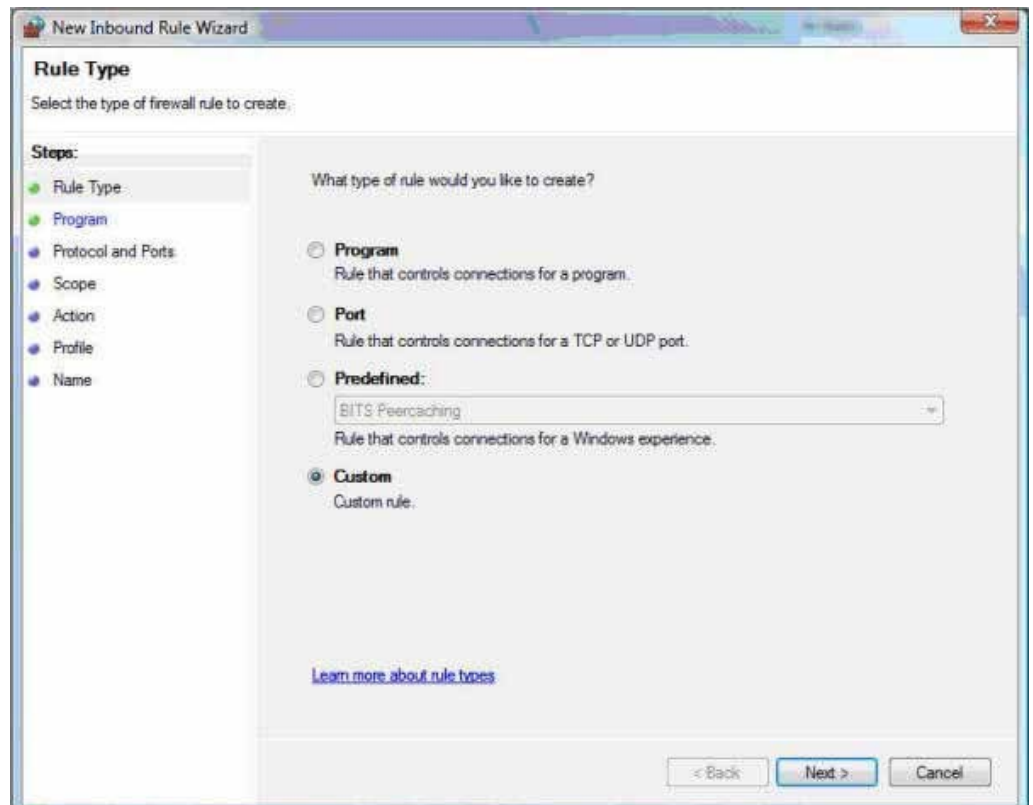
*Go on to the next picture.*



Click on the 'Custom' radio button.

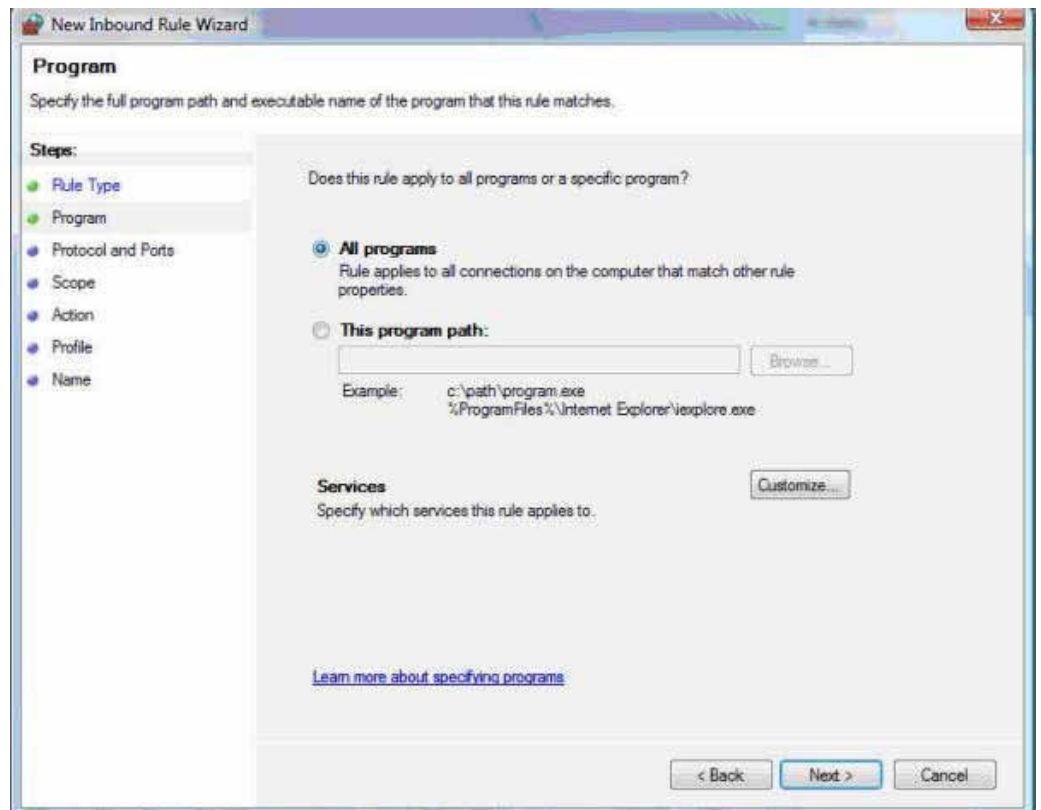
Click Next

Go on to the next picture.



Click on All Programs then click Next.

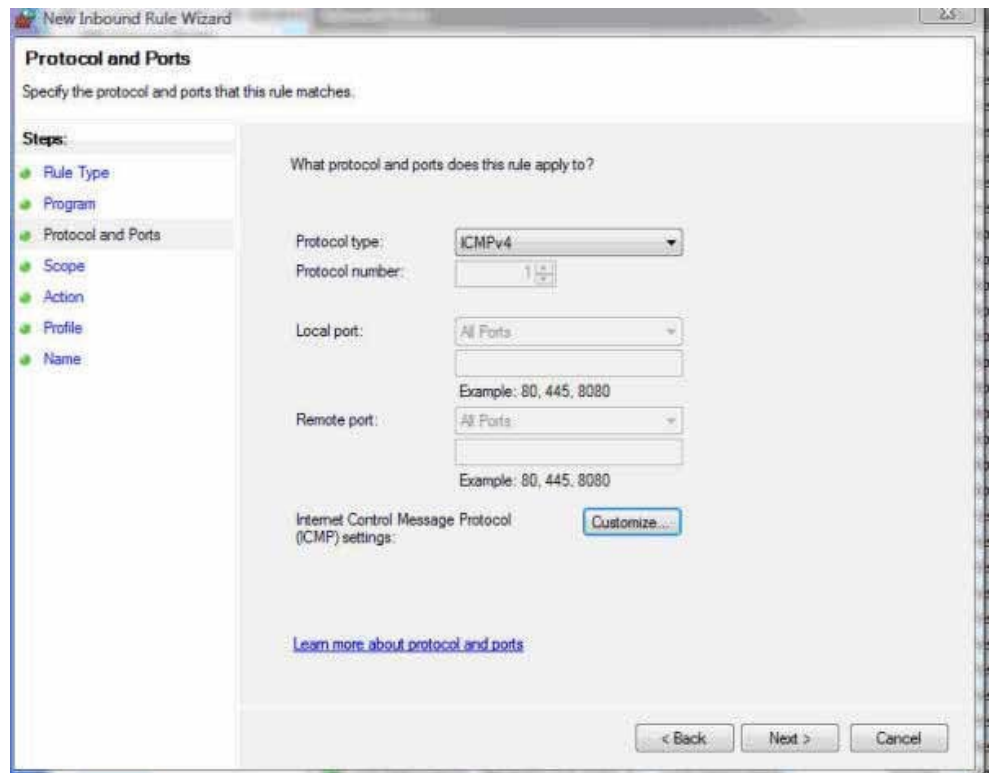
Go on to the next picture.



Set the **Protocol Type** to **ICMPv4**.

Click the **Customise** button next to **Internet Control Message Protocol (ICMP)** settings:

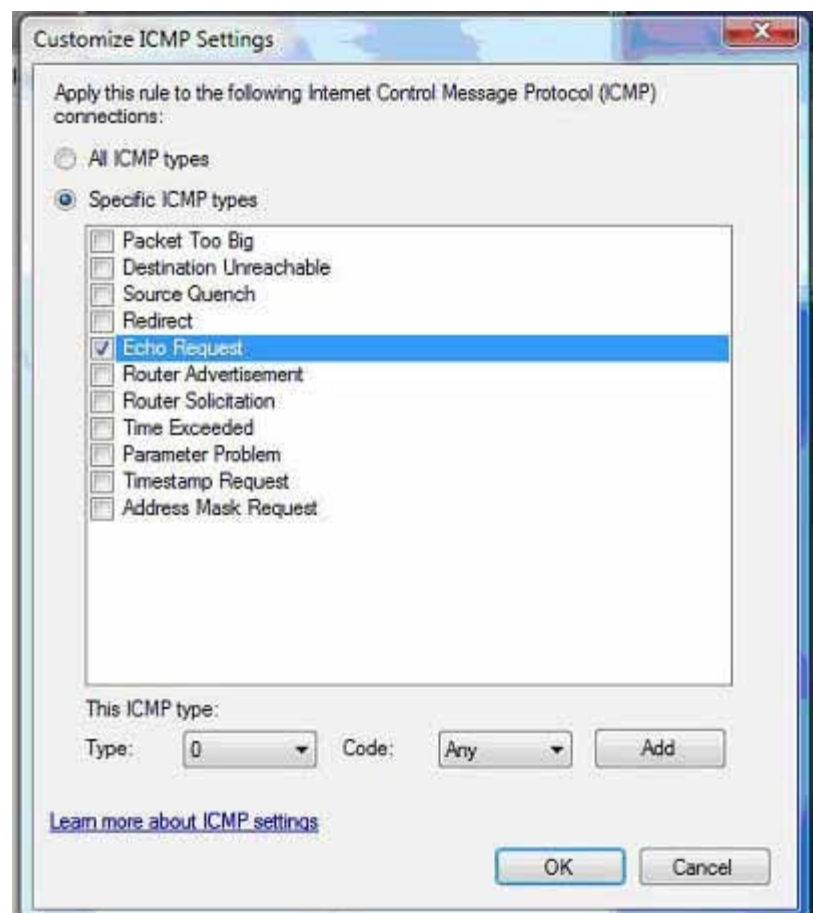
*Go on to the next picture.*



Click **Specific ICMP types**.

Tick **Echo Request** then click **OK** to return to the **Protocol and Ports** window, then click **Next**.

*Go on to the next picture.*



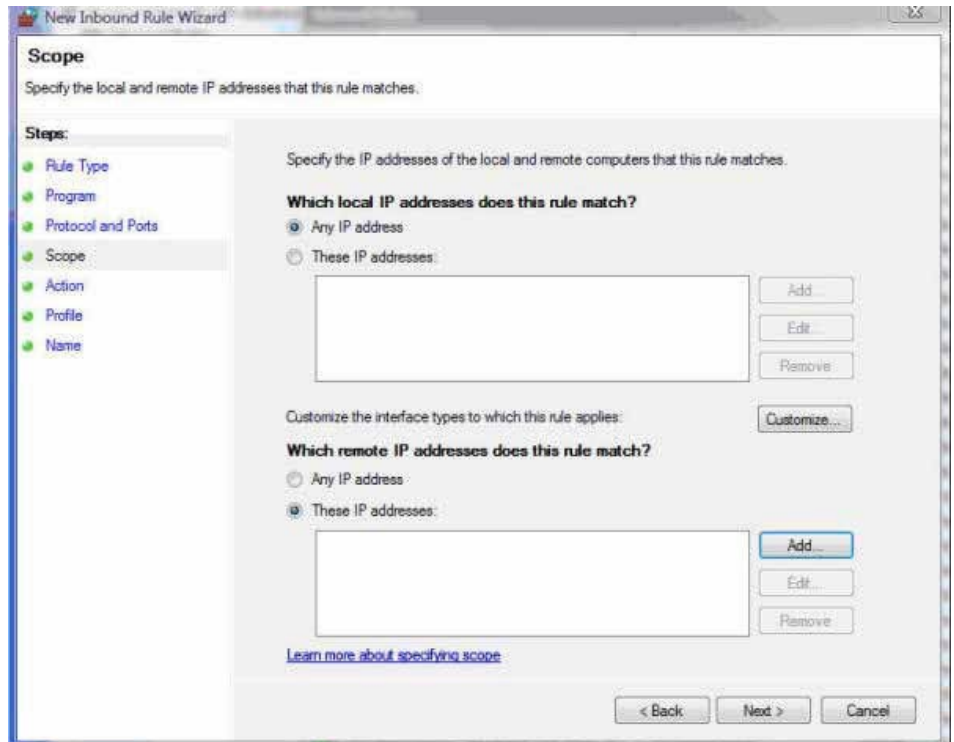


You will now be asked to **Specify the local and remote IP Addresses to which this rule applies.**

Under the Local IP addresses, select **Any IP Address.**

Under the Remote IP Address, select **These IP Addresses** and then click **Add.**

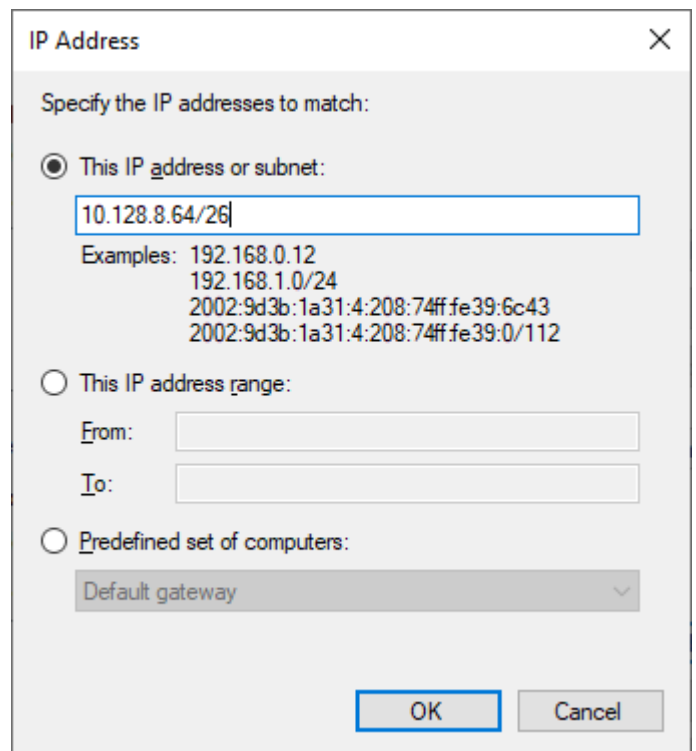
*Go on to the next picture.*



In the box, **This IP or Subnet**, enter the Friendly Probing address range of **10.128.8.64/26**

Then click **OK** to return to the **Scope window**, and then click **Next**.

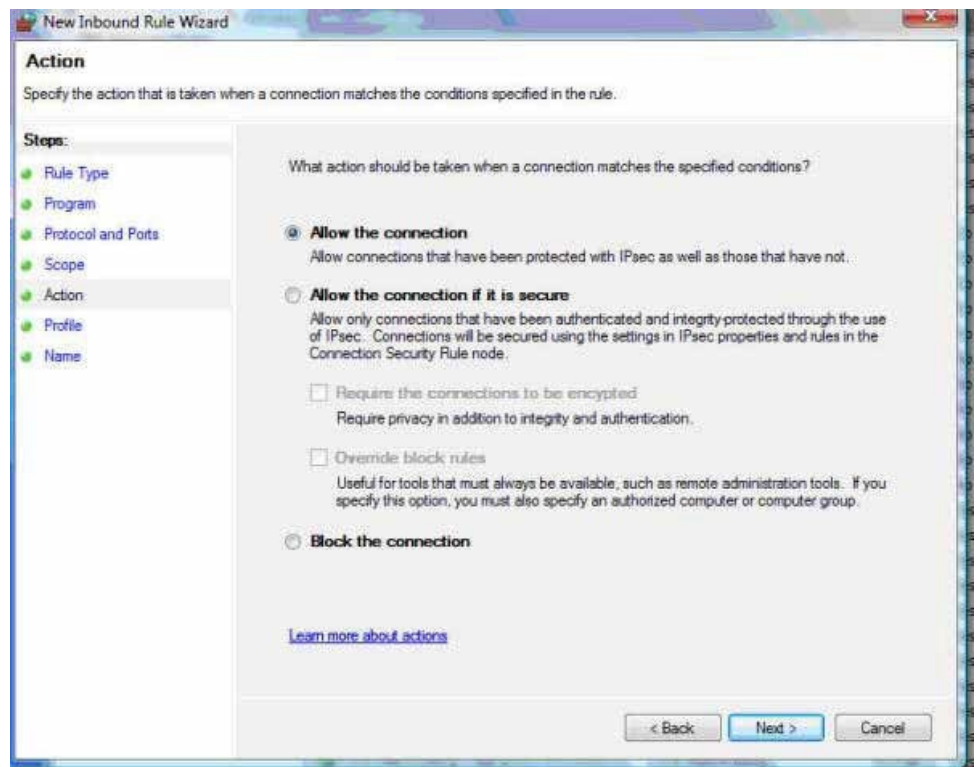
*Go on to the next picture.*



Check the **Allow the Connection** radio button.

Click **Next**.

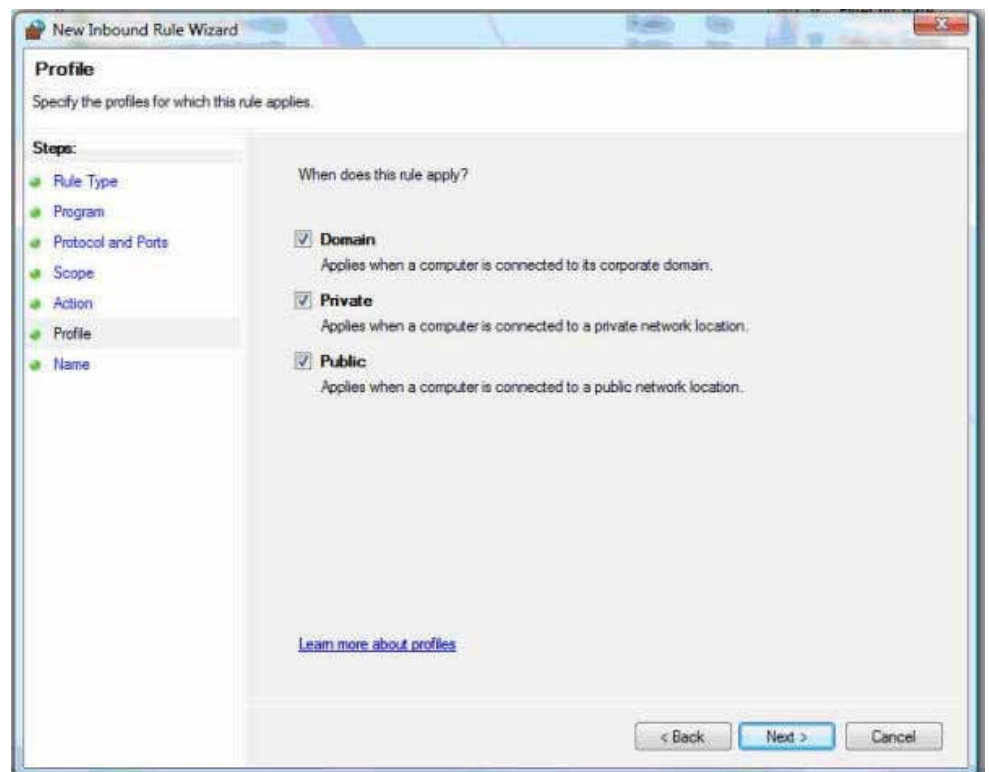
Go on to the next picture.



When asked "Which profiles does this rule apply", make sure that all three types (**Domain**, **Private** and **Public**) are ticked.

Click **Next**.

Go on to the next picture.

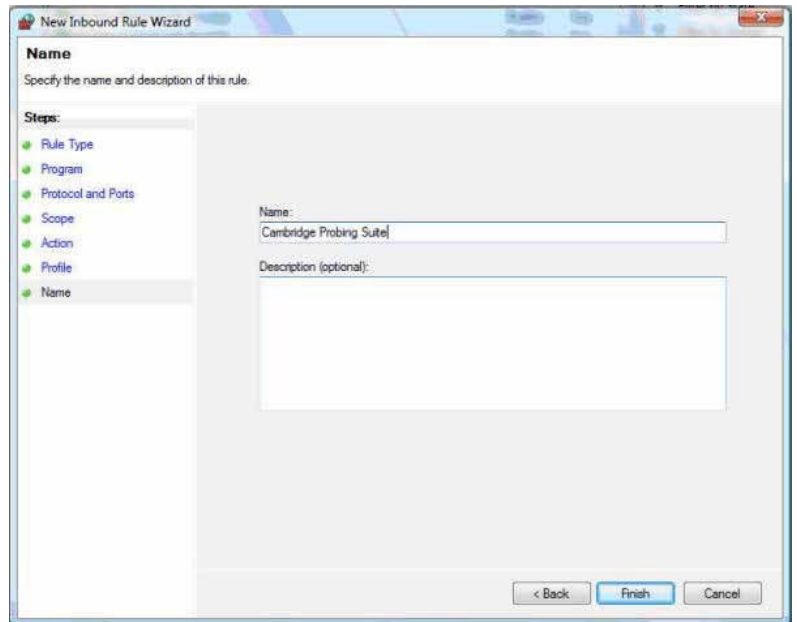


Now choose a sensible name to apply to the rule e.g. Cambridge Probing Suite.

Click **Finish**.

Close the **Windows Firewall with Advanced Security** window.

Close the **Administrative Tools** window.



**ICMP Echo Request has now set up**