

**About firewalls**

**Firewalls**

The term firewall comes from the name of a physical boundary or fire proof wall that is built between parts of buildings and between each home in a row of terraced houses to prevent fire spreading. A computer firewall is also a safety barrier, but unlike the one in buildings, a computer firewall is more of a filter than a total block and works both ways to check, then accept or deny data that is moving through a network.

**The two firewalls to protect your information**

**A boundary firewall** can be a hardware device like a small computer that is installed between your computer network and the internet. It will monitor the packets of data as they move in and out of your network and can block or permit data according to its predefined rules. Hardware firewalls are usually used by large companies so not everyone will use one. However, there is another type of boundary firewall and it is found at the entrance to your network within your router.

Your router is the small box with lights on it that you were sent by your service provider when you signed up for broadband. Most routers have a firewall build into them, click here to see [about routers](https://getreadyforcyberessentials.iasme.co.uk/guidance/about-routers/) guidance to find out how to check your router firewall and make sure it is turned on. A boundary firewall can protect other network devices that don’t have built-in firewalls, such as printers and other smart devices.

**A personal firewall** provides added internal protection within a network. This is a software firewall which is installed on an individual computer and protects that single device. If multiple computers need protection, the software firewall must be installed and configured on each device. Most modern operating systems include a free software firewall already installed. We will be showing you how to check your operating system firewall and ensure that it is switched on.

A software firewall controls the behaviour of specific applications (e.g. blocking access to certain websites) and can be set up differently for each computer depending on the required levels of access and permissions. Software firewalls are useful if a threat does manage to infect a computer, as it can prevent the malware spreading to the other computers connected to the same network. (see guidance [about malware](https://getreadyforcyberessentials.iasme.co.uk/guidance/about-malware/))

**Best practice cyber security requires two types of firewall are used for ideal levels of protection. One on each computer within a private network and another one at the entrance or boundary to the network.**

**Firewall rules**

A firewall works by filtering the incoming network data and determining if something is allowed to enter a network. The firewall uses a set of rules known as an access control list to determine what is allowed in and what is denied, it also decides what can leave a network and what is denied. These rules are customisable and can be determined by the network administrator.

If you are working from home or in a small business, the chances are, you are the network administrator and therefore responsible for setting up the firewalls. Firewalls can be set up or configured in several different ways. For example, a basic firewall may allow traffic from all locations on the internet except those flagged in a block-list.

A more secure firewall might only allow traffic from selected web locations listed in a safe-list. Most firewalls use a combination of rules to filter traffic, such as blocking known threats while allowing incoming traffic from trusted sources. A firewall can also restrict outgoing traffic to prevent spam or hacking attempts.

Network administrators often custom configure the network boundary firewall and the firewalls located within the operating system software of each computer. While custom settings may be important for a company network, the firewalls on personal computers and on most routers typically include basic default settings that are sufficient for most users. Anti-virus software often comes with firewall software that overrides the one from the operating system.

**Open ports**

In networking the term ‘open port’ indicates a port number has been configured to accept data packets. Different software and services will require different numbers of ports to be open on firewalls, in order to establish connections. Do not leave any port open that does not have a legitimate reason for being open. Close all unnecessary ports.

**How to check the firewall on your computer’s operating system**

Most computers come with firewalls already installed into their operating system. The following is an easy guide to checking and configuring your computer’s software firewall.

**Microsoft Windows**

To turn on and configure the Windows firewall in Windows 10, go to the Settings option, click on Update & Security, then select Windows Security and click on Firewall Network Protection. Once the window is open, you have the choice to enable the firewall for whichever mode you are in, Domain, being a business, Private being your home and Public, being when you are out and about in public spaces.

You may find that your firewall is so good at blocking potential threats that a program you are wanting to access gets stopped. It is possible to manually configure the firewall to allow a program through or to communicate with another machine or the internet. Click on the option ‘Allow an app through firewall’

Click to the Change settings button, to allow changes and the select the application you want to add and then select the profile you want to add it to (Private, Public or Domain).

Microsoft Windows can also automatically notify you if an application is trying to gain access to a resource it doesn’t have, for example if you’ve installed a new application and it tries to access the internet, Windows will ask if you want to add a rule. It will notify you by displaying a pop-up windows asking you to make a choice to allow or deny. Check to make sure its correct and take appropriate action.

**Mac OS**

Enabling the firewall on an Apple Mac OS device is a fairly simple process. Open up System Preferences, then go to Security & Privacy, then select the Firewall tab and click on the Turn On Firewall button.

To configure the firewall, you can click on the Firewall Options button and configure the settings based on your preferences.

**Linux**

Like Microsoft Windows and Apple Mac OS, Linux supports the use of software firewalls, Linux supports several different versions of firewall depending upon the distribution you are using. This could be iptables or firewalld. Its recommended that you check your Linux version website for more information on setting up and configuring your firewall, however below are a few links to get you started: