



Firewalls & Routers	What are the Cyber Essentials controls?
	<p>There must be a firewall at the boundary between your devices/network and the wider internet</p> <p>All inbound ports must be closed unless you have a documented business need to have them open</p> <p>All controls need to be applied to physical and software firewalls</p>
<p>www.ncsc.gov.uk/cyberessentials </p>	

Create a security filter between the internet and your network

Throughout history, when building homes, villages and towns, people have sought to create a layer of defence or security to maintain their safety and keep threats out. Means of doing this have included locating oneself on a high hill, building boundary walls, moats, strong front doors and deploying armed guards and dogs.

In the cyber world, rather than your physical safety and material possessions, the commodity here is your data, and there are numerous people trying to get hold of that. On computers, there are some key layers of defence you can activate to keep your information safe.

The main methods are:

- using strong passwords - like having a unique front door key
- enabling your firewall - like having a secure front gate
- securing your router - having a front door at all

Protecting networks with a firewall

What is a network?

A network is a collection of devices such as computers, laptops, smart phones and tablets that can communicate with each other. It could describe your 'home network', which is all the devices you have connected to your Wi-Fi at home, your 'company network' which is all the devices connected together that can access your company systems and data, or something as big as 'the internet' which connects lots of these smaller networks across the world.

Boundary devices

Boundary devices are the devices found on the edge of the network you control and want to keep private. Examples of boundary devices include a hardware firewall or a broadband router.

When you sign up for an internet service plan, your internet service provider (e.g., Sky, BT, or Virgin Media) sends you a small box to plug in. This device is your 'router' and is the key part of your network, as the router's job is to move data between your private network and the internet.

Routers

The router plays a very important role, as it sits at the gateway between your private network and the internet and allows devices and networks to connect together. If not secured correctly, this gateway could potentially allow cyber criminals access into to your private network and anything within it. For this reason, it is vital that your router's security settings are configured correctly.

Some routers arrive from the manufacturer with a default password such as 'ADMIN', and even if your router has a more complicated default password, it is not difficult to find it out with a quick search on the internet.

Note that the router password isn't the same as the Wi-Fi password which is necessary to access the network; that is a separate passcode.

The router password protects the router's settings and configuration. It is vital that you change this so that anyone cannot log onto your network and intercept your data or lock you out of your own network. You will find information about both the router password and the WIFI passcode with the information booklet that came with the

router, or most likely written onto the router. You will also be able to get information about your router on your internet provider's website.

Please note that **home routers** provided by an internet service provider are not in scope for Cyber Essentials and do not need to meet this requirement.

Networks must be protected by either a physical or virtual firewall

Firewalls

The term firewall comes from the name of a physical boundary or fireproof 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.

Different types of firewall

Boundary firewall

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.

Another type of boundary firewall is found at the entrance to your network within the router.

For small business networks and home networks, the internet router is usually the boundary firewall. It acts as a protective buffer zone between your devices and the internet. The inbuilt firewall within the router checks the connections to and from your devices to make sure that they are not likely to be harmful. It is important to check that your router firewall is turned on and configured in a way that is most beneficial.

If your router firewall is not enabled, a bit like not changing your router's default password, it is the equivalent to leaving your front door wide open. Some devices come from the manufacturer with the firewall switched off.

Software firewall

A software firewall provides added internal protection within a network. The software firewall 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.

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.

All devices must have a software firewall configured, where it is installed as part of the operating system.

Virtual firewalls

Another type of software firewall is the one built into the **hypervisor**; it is also known as a virtual firewall. A hypervisor is a piece of software that is installed over the hardware of a server to divide up the power of the server for use in different functions. The hypervisor turns the divided sections of the server into **virtual machines (VM)** and the server as a whole into a **virtual server (VS)**. Like a traditional network firewall, a virtual firewall inspects packets and uses security policy rules to block unapproved communication between virtual machines. A virtual firewall can be a boundary firewall.

For best practice cyber security, use two types of firewall for ideal levels of protection in the workplace. A software firewall on each computer within a private network and another one (physical or virtual) at the entrance or boundary to the organisation's network.

For Cyber Essentials, applicants must understand how to access their firewalls and be able to change the administrator password when it has been compromised.

Exceptions:

If employees work from home, their home router is not in scope for Cyber Essentials unless the organisation has supplied it. It is vital that home workers have their software firewalls configured securely on their devices that access organisational data and/or services.

Smartphones do not come with firewalls as default. A firewall is not necessary on your mobile phone as long as you only download trusted apps from reputable sources.

Virtual Private Networks (VPNs)

If an organisation uses a virtual private network, Cyber Essentials requires the use of a single tunnel VPN. A corporate or single tunnel VPN is a secure solution that connects remote workers back to their organisation's firewall and provides access to the organisation's private network. The use of a split tunnel VPN does not transfer the internet boundary solely to the company firewall and is therefore not an acceptable option.

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.

A secure firewall will only allow traffic from trusted sources listed in an allow-list, denying anything that is not listed.

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

Your organisation's devices will connect to the outside, wider internet through the gateway of your boundary device; this is the hardware firewall, the router or a virtual firewall. The gateway in a network has the same job as a gateway in a field. It is there to keep some things in, keep some things out and allow specific things to pass through. The firewall protects this gateway.

At times, your firewall may be configured to open a hole and allow a system on the inside of your network to become accessible from the wider internet. 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. There are many reasons why you would want to do this, for example to allow access to a **Virtual Private Network** server, a mail server or a service such as a database that is accessed by your

customers. It is possible to open a port in a secure way, however, there needs to be a valid business requirement to do so. If this has not been a considered and deliberate decision, it could present a risk to your organisation and the safety of its information.

A 'bot' is a software application that runs automated tasks over the internet. Criminals use this tool to scan the internet for open ports and services that are available for use and could be exploited. If there was a vulnerability or misconfiguration, they would know before you.

Can you configure your internet routers or hardware firewalls over the internet? This might be in place if you have a third-party IT company managing those devices on your behalf. Always review what services from within your network you expose to the outside world, and how many people you are allowing to use that service. It is a good idea to have mechanisms in place to permit only the people who need to access your configuration. For example, the firewall or router might be configured to allow access to an external IP address or range that only your supplier uses, or it might be configured to require two factor authentication. Where inbound ports are required, they must be documented and then turned off when no longer required.

Make sure that you can continually update those services exposed to the outside world. Do not leave any port open that does not have a legitimate reason for being open. **All inbound ports must be blocked by default.** If you are unsure about this, seek guidance from a professional who can perform a security scan against your network.

The five controls of Cyber Essentials are:

- User Access Control
- Security Updates
- Secure Configuration
- Malware Protection
- **Firewall and Routers**

Help and support

There are over 300 specially trained cyber security companies around the UK who are licensed to certify against the Government's Cyber Essentials Scheme. They can offer help and support in preparation for the assessment. [Find one near you.](#)

For questions and feedback about the Cyber Essentials scheme, contact IASME at info@iasme.co.uk or Tel: 03300 882 752