Cyber Security Guide

What are Firewalls?

A firewall is a network security device that monitors and controls incoming and outgoing network traffic (data) based on predetermined security rules. A firewall establishes a barrier between trusted and untrusted networks, such as the Internet.

Software firewalls are installed on individual computers or devices, while physical firewalls are hardware devices installed between a network and the Internet.

Software firewalls are typically less expensive than physical firewalls, but they may not be as powerful or effective at blocking malicious traffic. Physical firewalls are more expensive than software firewalls but usually offer higher security. Most modern operating systems (e.g. Windows 10/11 contain software firewalls that are turned on by default.

Here are some of the key differences between software firewalls and physical firewalls:

- **Cost:** Software firewalls are typically less expensive than physical firewalls.
- **Power:** Physical firewalls are typically more potent than software firewalls.
- **Effectiveness:** Physical firewalls are typically more effective at blocking malicious traffic than software firewalls. This is especially true for outgoing traffic, as most software firewalls work on an "allow everything out" model and only block unauthorised incoming data.
- **Ease of use:** Software firewalls are typically more straightforward than physical firewalls.
- **Location:** Software firewalls are installed on individual computers or devices, while physical firewalls are installed between a network and the Internet.

Even physical firewalls run software inside; the primary difference is that this software is often "security hardened" to make it far less likely to compromise. Unnecessary components found in standard software-on-computer-based firewalls are therefore not running, reducing the risk. Due to the complexity of a hardware firewall, it is possible to misconfigure it and render your protection reduced or even negate it entirely. Expert advice is therefore recommended if choosing to protect a physical network with a physical firewall.

Simple firewall configurations only block incoming data that is unauthorised/unexpected, and even when that data is expected, they pass it through to the computer that requested that data.

Modern firewalls, especially hardware models with security subscriptions, will examine even allowed data for potential threats. Because these types of firewalls can also monitor outgoing traffic, they can also protect users on the network by scanning outbound requests for threats, such as attempting to visit a compromised website.

We would always recommend that a hardware firewall protects a network, but that is still no reason not to run a software firewall on each device. That's because a network firewall usually only protects the network's boundary with the Internet; it will not protect a computer inside the network from being compromised by another computer on the same network.