What is a firewall and what does it do?

So far, while you have been pooing (or weeing, whatever your preference), we have been learning about the fundamental bits of kit that keep us all networked, namely routers and switches. Switches help switch packets quickly between PCs and other devices on a network, while routers plot and guide routes between different switched networks.

So what does a firewall do? A firewall is probably the next most important piece of the networking puzzle. Exactly as it says on the tin, put simply it acts as a wall that protects you against potential threats. Deployed as either a stand-alone box or as software on an already existing piece of kit, a firewall is used to control access between two networks using pre-configured rules and filters. These two networks are commonly referred to as a trusted network and an untrusted network.

In a simple example, the trusted network portion would be you, your network, a network that you trust! The untrusted network would be the outside world, potentially every single hacker in the world, an untrusted source of network traffic. The firewall sits in the middle and runs checks against the traffic flowing between those two networks and based on the rules you have programed it with, will either allow it through or not. The firewall will only do exactly as it is told so those filters you put in place are incredibly important.

Now you may be thinking, well hang on, surely you can't configure the firewall filters with every single possible permutation of traffic that it is supposed to block or allow?! The internet and everything on it is changing by the second, how would you keep up? Well firstly it is important to understand that firewalls generally only worry about inbound traffic. This isn't always the case but most of the time, if you need to go outbound from your trusted network to the untrusted network, the firewall will just assume that traffic originating from the trusted side is safe, allow it to pass out, and then the responses are automatically allowed back in along the same path.

Traffic that originates from the untrusted network i.e. the outside, and is trying to get into your trusted network, this is where the firewall really does its job and is considered its main function. A firewall looks at that inbound traffic and decides whether to allow it based on the rules you have given it. The list of filters you give a firewall are based on the premise that everything from the untrusted zone is blocked unless otherwise specified, so if you want to allow someone from the untrusted side into your safe trusted zone, you have to tell the firewall their specifics, usually an IP address and/or the port that they will be coming from.

Modern firewalls do tend to have a plethora of other functions, which some may consider secondary but they are becoming more and more common. Network managers may wish to introduce things like content and service filtering, so for instance if you wanted to block your employees from being able to reach Facebook or Youtube, a modern firewall will be able to achieve this easily. They may also wish to grant access to certain services based on user control, so managers and directors are able to visit any website they like, where as everyone else is restricted. Again this user based policy system can be implemented on newer firewalls and is becoming the norm.