

Firewalls for peace of mind

When I first heard about firewalls I imagined a wall of fire surrounding my computer, protecting it from all the nastiness that permeates the web. It has since been brought to my attention that the obvious comparison is with a fire break, a sort of demilitarised zone that stops fires from spreading.

Firewalls act as a permeable space between your computer and the rest of the net. They deny undesirable items entry while allowing network friendly ones to pass unhindered. I think that I prefer my vision of evil transmissions going up in flames while the righteous enter unharmed.

Firewalls function according to rule sets that can be specified and customised according your business's needs. Rule sets can be either inclusive or exclusive. Exclusive firewalls block only the traffic that has been specified in the rule set; all other traffic is allowed through. Inclusive firewalls on the other hand, only allow through the traffic that matches the rule sets and block all other transmissions. Inclusive firewalls offer more security than the exclusive kind.

Firewall controls traffic through the use of one of three methods:

- **Packet filtering:** filters analyse chunks of data to see if they match the rule sets. If the packets of data meet the set specifications they are forwarded to a requesting system. Packets that fail to make the grade are summarily discarded.
- **Proxy service:** In this method, the firewall retrieves information directly from the Internet before it's forwarded to the requesting system.
- **Stateful inspection:** A relatively new method that singles out key aspects of data packets and compares them to information that is stored in a database. The method is based on an analysis of information sent from the business. If incoming information matches the type of content going out, it's allowed in.

You can customise firewalls by adding or removing filters according to criteria that's relevant to your business. Some examples of features that can be customised include:

- **IP addresses:** filters can block traffic transfers to and from certain IP addresses if they suspect them of foul play or malicious intentions.
- **Domain names:** Access to and from certain domain names can be blocked by the same process that blocks IP addresses.
- **Protocols:** According to howstuffworks.com, protocols are the pre-defined ways in which people or computer programmes talk to services that they want to use. Firewalls can be set for the following protocols:

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

Hyper Text Transfer Protocol (HTTP)

Simple Network Management Protocol (SNMP)

Transmission Control Protocol TCP)

It's possible for businesses to set up protocols on only a few of their computers while blocking them on the rest. In this way it's possible for the business to retain complete control of information entering and leaving their networks. They can also restrict their employees' access to certain kinds of network sites and capabilities.

However you imagine them, be it as fiery walls consuming Internet evil, or as the more traditional protective permeable space between your computer and the rest of the net, there is no denying their extreme importance. With hackers and e-vandals using the net as their personal playgrounds, it's more essential than ever to protect your assests, particularly valuable data. It's no longer a qestion of should you get a firewall, but which firewall is best for you?

Recommended sites:

<http://www.howstuffworks.com/firewall.htm>

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html

About the Author

Sandra wrote this article for the online marketers Star Business Internet [internet service provider and website hosting](#) one of the leading Internet service companies specialising in business website hosting in the UK

Source: <http://www.articletrader.com>