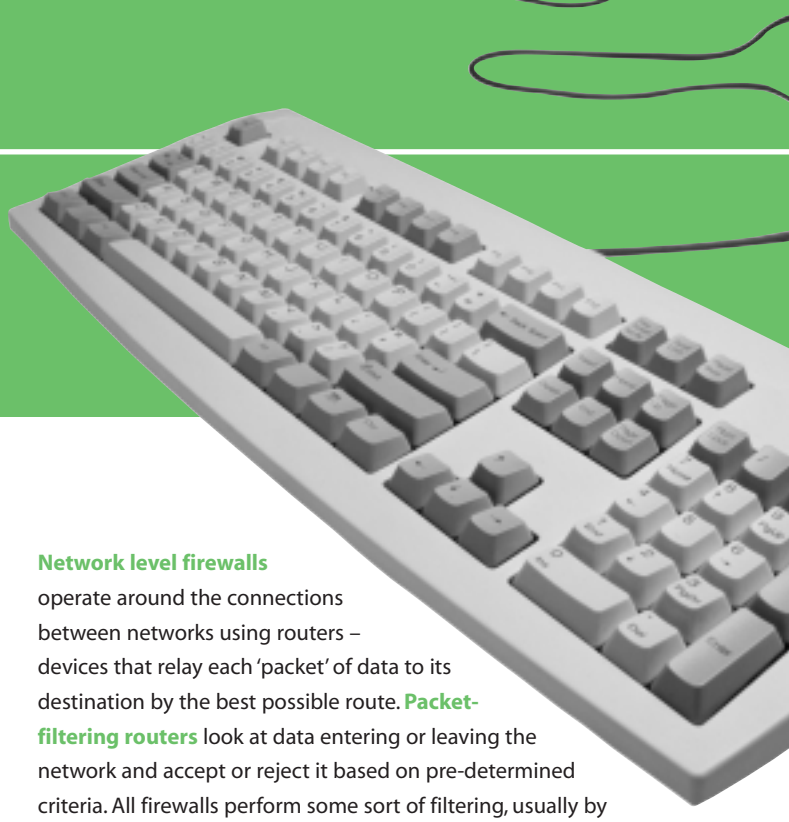

Firewalls

What are they?

Firewalls are security systems that are designed to prevent unauthorised access to or from a private network and provide a security control point that enables sites to connect safely to other networks. The network connections could be between one organisation and another or between one part of an organisation and another, such as could exist in a school that has separate administrative and curriculum networks. Firewalls can take the form of hardware or software, or a combination of both, and are configured to an organisation's own requirements.

What do they do?

Firewalls protect computer networks and their contents from malicious users ('attackers') and accidental damage, caused either by users from within or outside an organisation. For example, a firewall could prevent confidential information about pupils being corrupted or seen by unauthorised users. They can also be set up to prevent users from within the organisation from carrying out specific transactions. In a school, for example, a firewall could block access to unsuitable websites.

Most firewalls log the electronic traffic passing through them, which allows the administrator to see what has been attempted and, possibly, identify who had carried out the action.

How do they work?

Broadly speaking, firewalls work by checking all the traffic passing through them, blocking data which does not conform to pre-determined security criteria and allowing everything else through. Firewalls can be set up to block specific sites or type of sites or entire parts of the Internet. For example, some schools use their firewall to block all e-mail and newsgroups. Some firewalls place a greater emphasis on blocking traffic, while others emphasise permitting traffic.

Firewall development is split into two main types: network level and application level.

Network level firewalls operate around the connections between networks using routers – devices that relay each 'packet' of data to its destination by the best possible route. **Packet-filtering routers** look at data entering or leaving the network and accept or reject it based on pre-determined criteria. All firewalls perform some sort of filtering, usually by means of a router. Network level firewalls are fairly effective but difficult to set up and some routers do not provide any logging capability. They are generally very fast and transparent to network users.

Application level firewalls, also known as **application gateways** or **proxy servers**, are applications that sit between a client application (such as a Web browser) and a real server (such as a Web server). They prevent traffic from passing directly between networks by acting as an intermediary between the client and the server. This means that the server never knows the whereabouts of the client and vice versa. Application level firewalls provide a high level of security and logging capability but can be slow and lack the transparency of packet-filtering firewalls.

Firewall technology is one of the fastest developing areas in computing. Increasingly, **hybrid firewalls** are being developed that combine existing mechanisms.

What can't firewalls protect against?

Firewalls should form only part of an overall security system. They are generally unable to protect against damage caused by users within the network (whether deliberate or accidental) and computer viruses. Viruses can be introduced into a computer in many ways, via floppy disk, e-mail, network or other hardware, such as when uploading files directly from a laptop computer, for example.




Some firewalls can check incoming code for signs of viruses and bar access when detected. However, a firewall can only address malicious code coming from another network. It would not be able to detect a virus entering a system via, for example, floppy disks or e-mail attachments. Firewalls therefore need to be run alongside other security measures, such as virus detection software.

Note to parents and home users

It is highly unlikely that a home user would need a firewall. Consequently, home users need to think about the alternatives. Parents might consider subscribing to an ISP who offers some form of filtering service, or install filtering software on their own machine (see the 'Internet Filtering Systems' information sheet). To prevent virus infections, virus detection software (which should be updated regularly) would be required.

Further information

There is a great deal of information about firewalls available on the World Wide Web. The following selection offers listings of firewall products and resellers, explanatory information about firewalls and a mailing list concerned solely with firewalls:

Dmoz – Open Directory Project
The Open Directory Project's goal is to produce the most comprehensive directory of the Web, by relying on a vast army of volunteer editors. Among other things, this site provides a comprehensive directory of sites offering access to sites on firewall products and security.
http://dmoz.org/Computers/Security/Firewalls/

Firewalls Mailing List
Internet firewall mailing list for discussions of Internet firewall security systems and related issues.
http://spike.rwc.gnac.net/firewalls

Firewall Product Overview
Directory of commercial firewall products, firewall resellers, public domain and shareware firewall products.
http://www.thegild.com/firewall/

ICSA.net
Leading membership organisation for information security, including information about firewalls, ethics, defence against viruses, Trojan horses and other malicious code attacks.
Includes listing of certified products together with laboratory reports of products.
http://www.icsa.net/

ICSA.net Firewall Buyer's Guide
Guide can be viewed on line or downloaded as a PDF file.
http://www.icsa.net/html/communities/firewalls/buyers_guide/index.shtml

Information Security Standards
The EC's Open Information Exchange Service provides information on standards and specifications that can be used to ensure the security of data interchanged between two open systems.
http://www.cordis.lu/saferinternet/

Network Security Buyer's Guide
Information about network security, utilities and virus protection. Offers a searchable database of products, links to vendor sites and a library of white papers, press releases and product presentations.
http://www.netsecurityguide.com/