Firewalls

A firewall is a system that implements and enforces an access control (or security) policy between two networks, for example between an internal private network and an external public network. Essentially, a firewall connects two or more networks but only allows specified forms of traffic to flow between them.

Firewalls are used to restrict traffic between different parts of the network, thereby providing protection against some types of attack. This kind of system is often used at the entrance point of an organisation's network, where the LAN joins the WAN, to protect an organisation from hazards on the Internet. However, controls within an organisation can also be useful, for example to separate different departments, working areas or networks.

Sites that do not have a firewall may be subject to attack from hackers. If the hackers gain control of the network then the organisation may suffer:

- financial loss, such as loss of income or possibly fines/compensation imposed by a court
- loss of reputation, if embarrassing material is revealed or forged e-mails are sent
- denial of access to resources, if a key piece of network or server equipment has been rendered unserviceable.

Before implementing a firewall, an organisation must have a defined security policy. The firewall may then be used to enforce some aspects of that policy and vulnerable assets can be protected against attack from outside. A default deny firewall can also protect against unexpected forms of attack, since only predefined traffic is accepted. Without a policy, a firewall is unlikely to be effective since there is no defined basis for making decisions about which traffic should be permitted and which denied.

It is not possible to keep all of an organisation's networks entirely inside a firewall. Public servers, such as e-mail and web, must be exposed to the outside world in order to perform their functions. There is always a risk in running such services, but with careful configuration and maintenance, as well as a suitable firewall, that risk can be minimised.

Firewalls can be bought 'off the shelf' as dedicated devices or can be constructed from individual components by those with the necessary skills. A choice between these options should be based on convenience, flexibility and cost. A dedicated package is likely to be easier to configure and support but may prove inflexible and expensive, while custom-built firewalls require high levels of technical expertise but are infinitely flexible. Many routers also provide basic, but useful firewall facilities.

Further details about the process of choosing and implementing a firewall can be found in the JANET Technical Guide Firewall Implementation at JANET-connected Organisations [1] and the report The Use of Firewalls in an Academic Environment [2].

Links
[1] http://community.ja.net/library/advisory-services/firewall-implementation-janet-connected-organisations
[2] http://www.jisc.ac.uk/uploaded_documents/jtap-049.doc