Introduction to Firewalls

Introduction to Firewalls

In the real world a firewall is a solid barrier between a precious asset on one side and a hazard on the other. For example, we hope that there is a firewall between the passengers in a car and the petrol tank. A network firewall performs exactly the same role, protecting an asset inside the firewall from a hazard on the outside. Firewalls are often used to protect an organisation from hazards on the Internet but they can, and probably should, also be used within an organisation to separate different departments, working areas or networks. Locked offices and buildings cannot protect information if the computers holding it are open to everyone on the network.

Firewall controls

The simplest network 'firewall' is not to have a network connection at all. This gives good protection against hazards, but unfortunately it also prevents all legitimate use of the network. A practical firewall must therefore establish connection, but must also have rules to enable it to distinguish 'good' network traffic from 'bad'. Of course no computer can truly understand the intent of a traffic flow, so most make simple decisions based on where the traffic is coming from and going to, and what service it appears to be requesting. A firewall might be set up to allow nothing but e-mail traffic to pass from the outside in, but allow both e-mail and web requests by local users to pass out.

The rules that govern the firewall define what to do with some of the traffic, but this leaves the question of what to do with the rest. Firewalls can be set up either to let all undefined traffic through, a strategy known as default-permit, or block all undefined traffic, default-deny. If an event is unexpected it is clearly safer to assume that it is hazardous, at least until it has been investigated. Firewalls should therefore use defaultdeny to block all traffic that they are not explicitly told to permit. Inevitably this will occasionally stop new, legitimate, traffic but this inconvenience is much less painful to resolve than the alternative of allowing in new, unknown traffic that later proves to be hostile. An effective process for discovering and permitting new legitimate applications will help reduce the temptation for users to 'work-around' firewall rules.

Security policy

Before implementing a firewall, an organisation must have a defined security policy. The firewall may then be used to enforce some aspects of that security policy. By implementing an appropriate policy, vulnerable assets can be protected against attack from outside the

firewall. A default-deny firewall can also protect against forms of attack that are as yet unknown, since only predefined traffic is accepted. Without a policy, a firewall is unlikely to be effective since there is no agreed basis for making decisions about which traffic should be permitted.

Other considerations

It is not possible to keep all of an organisation's networks inside a firewall. Public servers, such as e-mail and web, must be exposed to the outside world in order to perform their function. Careful configuration and maintenance are vital, and a firewall useful, to minimise the risk in running such services.

Furthermore a firewall cannot protect against attackers who can place themselves, or their tools, inside the firewall. A common method of attack, which a firewall cannot prevent, is to persuade a local user to run a hostile program inside the firewall. This may be as simple as persuading the local user to click on an attractive e-mail attachment (viruses using this technique are still extremely successful) or to run a program that promises to be one thing (such as an attractive screen saver, or a new game) but conceals another, which has a hostile purpose.

Insecure dial-in modems and wireless networks can bypass firewalls, leaving the network nearly as vulnerable as if the firewall were not there. Official access points must be set up securely: unofficial ones should be prohibited and disconnected as a serious risk when they are found. see *Wireless Security* Factsheet at:
http://www.ja.net/documents/publications/factsheets/040-wireless-securit... [1]

Implementation

Firewalls come in many different guises. They can be bought off the shelf as dedicated devices or can be constructed from individual components by individuals with the necessary skills. simple firewall programs available for, or included in, modern operating systems can provide effective protection for workstations against some user mistakes. In addition many routers also provide basic, but useful, firewall facilities. A choice between these options should be based on convenience, flexibility, available skills and cost. A dedicated package is likely to be easiest to configure and support but may prove inflexible and expensive, while custom built firewalls require high levels of technical expertise but are infinitely flexible.

Conclusion

Firewalls can be a valuable component of an organisation's security plan. When implementing appropriate policies, both at the perimeter and within the organisation, they can protect against existing and new forms of attack. however, there are attacks that a firewall alone cannot prevent, in particular those performed or assisted by insiders. Indeed local users may deliberately circumvent a firewall, and thereby endanger the whole network, if they do not see it as beneficial. It is therefore important that local users understand and endorse the measures that are implemented and recognise that they are an important part of the

organisation's overall security policy.

Firewalls alone are not a solution to the problem of securing a network. Users need to be informed and educated to see security as a vital part of their computer use; systems need to be configured securely and maintained to address new security problems and requirements; policies and guidelines need to be introduced and supported so that secure working becomes easier and more acceptable than insecure. Any reliable system will have multiple layers of protection so the failure of any single component does not result in loss of control of the whole network.

Security is a culture, not a black box.

Further Information

Firewall Implementation at JANET-connected Organisations [2], M. Cook, Loughborough University