FIREWALL - DEFINITION

A firewall is a system or group of systems that enforces an access or deny policy. That is all. The firewall filters all the packets of data that go in and out of a *network* and blocks them or allows them to continue to their destination. For example, you can configure a *firewall* to allow only email to enter your network, thus shielding you from any attacks except for ones via email.
A firewall is typically a separate computer or device on your network that sits between your private network and your *Internet* connection. This way a successful break-in to your network must still go through a separate level of security to get to your files.
A firewall often includes or works alongside a proxy server. A proxy server is a computer that also sits between computers on an organisation's network and the Internet. It allows an organisation to ensure security and administrative control (amongst other things). This way information on your organisation's network can be hidden from the outside world. A firewall also acts as the concentrator for your Internet access. Since all of your traffic goes through one place, you can produce great logs of who tried to access your network, what traffic went where, and much, much more.

Does your organisation need a firewall?

The only computer that does not need a firewall is one with no connection to the Internet. In that case, all you need to protect your information from outsiders is a door with a good lock. However, since many organisations have an always-on "broadband" Internet connection such as ADSL, a firewall is a necessity. For more information on Internet Security see the Knowledgebase article How secure is the Internet? A firewall is **not** a substitute for good *Antivirus software*, regularly updated. Antivirus software should be used in conjunction with a suitable firewall to give additional protection your computers.

Types of Firewall

Firewalls can come in many different types, but they will always have one or two of the following items.

Packet Filter

This technique looks at each packet entering or leaving a network, accepting or rejecting it based on established rules. Packet filtering is fairly effective and transparent to users, however it is often difficult to configure. It is also vulnerable to Denial of Service attacks, featured prominently with the attacks on Ebay, Yahoo, Microsoft and friends (during which these websites were forced to temporarily close due to deliberate malicious activity from an external source via the Internet).

Application Gateway

This method is used for specific applications, such as *FTP* and *Telnet*. This can allow for a secure connection to these relatively insecure services but the performance typically suffers.

Circuit-Level Gateway

This is also used for specific applications, such as *TCP*. Once a connection has been established, packets can flow between the hosts without further checking.

Proxy Server

This method intercepts all messages entering and leaving a network. The proxy server hides the network's true address giving out a phoney one to anyone who might want to know.

What you need to think about first!

A firewall is only your first line of defence. If the rest of your network is insecure, a firewall breach will be disastrous. Network security is a tricky business, and you need to be diligent in keeping your entire network secure. No network is safe if the entire system isn't safe. Your security policy needs to take into consideration employees, physical systems (doors) and waste paper, amongst many other things. A locked door means nothing if the window is wide open. The first thing you need to think about is your overall security policy. This may sound suspiciously like planning, but if you don't have a strong security policy, your firewall will be an interesting experiment, but not much more.

A security policy will take into account your entire system causing you to think about how long your passwords are in place before they must be changed, who has the keys to the server, and your own paranoia level. Pay special attention to the level of security and the effect on usability. The more secure a system is, the more often the users are required to remember multiple passwords or to change their passwords, making the system more cumbersome to use. After you have worked that out, you want to think specifically about the firewall. A Firewall Policy will answer the questions:

- What type of traffic do you want to allow? (e.g. do you want to restrict access to certain websites? Do you want to allow only email and web access or do you need services such as FTP for example to upload web pages to your website or to download software?)
- Is your firewall just there for queuing traffic and monitoring or do you want to restrict everything but Web traffic?
- What are the risks associated with these things?
- Is security more important than usability or vice-versa?

Usually it is best to deny first and ask questions later. Deny all services not crucial to your needs. Discuss these issues with your network support provider if you do not have appropriate IT support in house.Once you have figured out what you want and need, it is time to talk about the budget. Costs for firewalls can

literally range from free to £35,000. How much you are willing to spend on security can often drastically reshape peoples' paranoia levels. None of these devices should be seen as the final solution either. All of them will need to be configured to your level of need and will need to be updated regularly to keep track of new security holes.

Firewall Options

For most voluntary sector organisations, the way to start is to look for a product to buy. If someone has told you about how you can build a firewall to meet your needs with existing routers, please think twice or thrice about embarking on this endeavour. In theory this approach is good if you have a full-time IT staff member who really understands wide area networking. In practice this approach often costs much more in staff time and energy than comparable out-of-the-box firewalls.

Currently you can buy firewall systems in any shape or size that your heart desires. You can buy software, hardware devices, and hardware bundled with an operating system like Unix or Windows NT/2000 and firewall software. Software firewalls usually cost between £1500 and £7000. There are popular free software firewalls such as ZoneAlarm but these are generally best used for *standalone*machines **not** computers on an organisational network.
Hardware solutions are often much easier to install and require lower system resources. In the end, the only one who can tell you which is the right product is you, based on your needs and budget and advice from your network support provider or other appropriate source. There are a few things to consider when deciding though:

1. Will the firewall implement **your** security system or are you dependent on the firewall's in built security?
2. Is the firewall, flexible, user-friendly easy to program and able to filter on a wide variety of attributes, including source and destination *IP address*?
3. Does it contain mechanisms for logging traffic and suspicious activity, as well as mechanisms for log reduction to keep logs readable and understandable?
4. The firewall and any corresponding *operating system* should be updateable with patches and other bug fixes in a timely manner.

Now you need to define your network (with appropriate help if needed). List out your network protocols, main systems such as email, file server version and*patch* level, list out your Internet connection, speed, IP addresses and services.
Defining where a firewall will go and what its purpose will be can help you determine what device will work best for your organisation. For small offices and homes with an ADSL connection to the Internet, ADSL Modems with built-in firewalls are a good bet. If you are getting ADSL anyway you might as well get a decent modem that has a firewall. Check with your Internet Service Provider as to which modem

they are giving you, or to make sure that the one you buy is compliant with their system. Often these devices also include:

- VPN
- NAT
- DHCP

For stand-alone firewalls, products like the WatchGuard Firebox SOHO device costs around £350-£500 + VAT, are relatively easy to install and configure and are suitable for up to 50 users.

Source : http://www.ictknowledgebase.org.uk/firewalls