THE PROTECTIVE ARM around your network

As private networks integrate with the Internet, ensure that your network stays safe by installing a firewall

Illustration: FARZANA COOPER

"Unknown and unauthorised individuals are increasingly attacking and gaining access to highly sensitive unclassified information on the Department of Defense's computer systems.... At a minimum, these attacks are a multimillion-dollar nuisance to Defense. At worst, they are a serious threat to national security."

You could not be more wrong if you dismiss this as an excerpt from a Tom Clancy novel. The above extract is from a report prepared by the United States General Accounting Office, on the vulnerability of the non-classified computer systems of the Department of Defense. The study revealed that out of the 250,000 attacks on the Department's computer systems, about 65 percent succeeded. Closer home, the country's premier nuclear research institute, the Bhabha Atomic Research Centre, suffered a similar fate when hackers from the MiLw0rm group broke into its systems.

Dangers such as ones mentioned above are frequently faced by the organisations that are accessible through the Net. To minimise such problems, the companies need to add a 'firewall' between the network and the Internet. A concept which is derived from the firewall used in vehicles—a barrier made of fire retardant material to offer protection in case of a fire—and is a system or a group of systems that guard a trusted network (yours) from an 'untrusted' network (say, the Internet), while allowing data exchange between the two.

However, this does not mean that a firewall is the answer to all your network security problems. There are a host of security issues that are not addressed by a firewall (*See 'Where firewalls are not hot enough*'). Also, like all computer systems, the effectiveness of any firewall depends on how it is implemented by the system administrator. And lastly, though a firewall may enhance your network's security, it may also hamper the efficient use of the network as a firewall is designed to deny and not enhance network access.

Is that a firewall?

Unlike the firewall in real life, the firewall in computers, in most cases, is an abstract concept. Physically, it may consist of hardware such as routers and host systems, software, or both hardware and software. In terms of functionality, a firewall is basically a data packet filter that selectively routes packets between trusted and untrusted networks. To understand this, let us first understand how computers communicate on the Internet with Transmission Control Protocol/ Internet Protocol or TCP/IP.

The data transmission process in a network begins with an application like an e-mail program presenting data to TCP, which then breaks the data into chunks called packets and hands them over to IP or Internet Protocol, which is responsible for host-to-host communication on the Internet. The IP attaches the source and destination address to the packet before transmitting it over the Net.

Once the packets reach their destination, they are handed back by IP to TCP for re-assembly. To further ensure that the data reaches the correct application, TCP also uses a port number that ranges between 1 and 65,535. E-mail applications, for example, typically use port number 25.

Any kind of network (Internet, intranet or extranet) that uses TCP/IP for data transmission depends on source address, destination address, and the port number. A Firewall uses these addresses and port numbers to control the flow of data packets between the trusted and untrusted network.

Depending on how they deal with the ports and addresses, firewalls are classified as packet filter, application proxy or application gateway and packet inspection firewall.

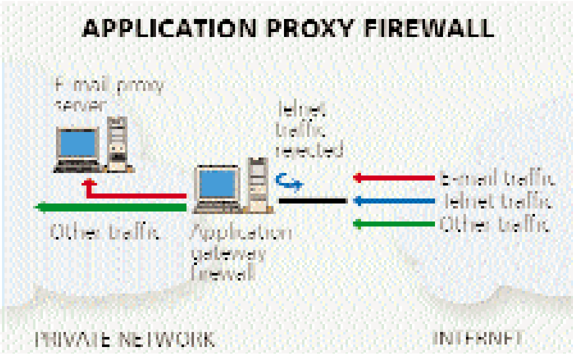
Brothers in firewalls

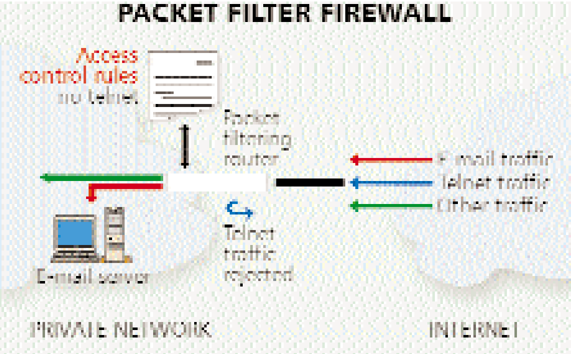
The fastest and the simplest of the three, the packet filter firewall, is also one of the earliest firewalls and made its debut about ten years ago. Usually router (hardware)-based, in this system a packet filter compares the header information–source and destination address, and port number–of each incoming or outgoing packet against a table of access control rules. The packet having the right address and port is allowed to pass through, else it is dropped. Packet filter firewalls are however, criticised for allowing a direct connection between the untrusted source and trusted computer, which exposes the network to an attack.

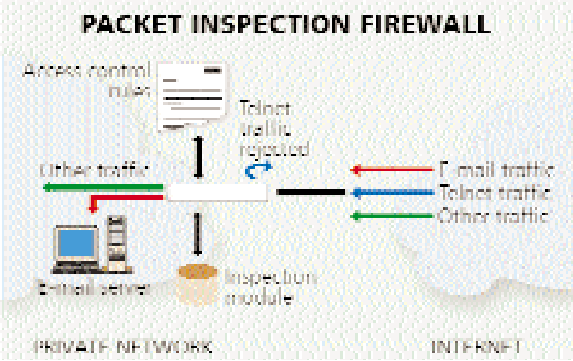
In real terms it is just like the stern receptionist in your office, who allows only people on your appointment list to meet or call you, and politely tells the others that you are unavailable. But convince the receptionist that you have been expecting him (or her), and the person is allowed to enter the office.

This problem is addressed by the application proxy firewalls. Developed by USA's Trusted Information Systems for the Defense Advanced Research Projects Agency (DARPA), proxy firewalls are built on the principle that security can be reliable if there is no direct connection between the trusted and untrusted network. This segregation is achieved through software applications, called proxy servers, running on host computers. Proxy servers designed to work as firewalls are called application proxy firewalls and the computers running them are called application gateway firewalls.

An application proxy firewall works by examining what application or service (such as e-mail or file transfer) a data packet is directed to. If no service is available, the packet is discarded at the firewall. If the service exists and is available to that packet, the packet is allowed to pass through. Once verified, the data is extracted from the incoming packets and then delivered by the application proxy. The original packets are terminated at the firewall.







The most common way networks are broken in is not by brute-force password guessing but by social engineering

Keeping with our receptionist analogy, it would mean that he or she would only allow a visitor to deliver a package to you if you are available in the office. After checking if you are in the office, the receptionist will hand the package to the office boy who takes it to your table, rather than send the person in with the package. Which brings us to the advantage of using a proxy firewall: addresses of individual computers in the trusted

GLOSSARY

Gateway: A gateway is a system that sits between two networks and provides access and control from one to the other.

Port: Ports are virtual pipes that allow services such as file transfer and e-mail to share a single physical connection or an Internet address.

Protocols: Protocols are standard or language rules that define how devices on a network can communicate with each other.

Router: A router is a network device that links two or more networks together. A router selectively channels packet transmissions from one network to another rather than broadcasting it to all networks.

Where firewalls are not hot enough

Computer security is not just about keeping hackers and industrial spies at bay. It is also about safeguarding the organisation s information assets.

This is where firewalls fail.

Contrary to popular belief, the most common way networks are broken in is not by brute-force password guessing but by social engineering. This involves tricking trusted network users into revealing some information (like passwords) which can then be used for breaking into the system. Firewalls cannot prevent this.

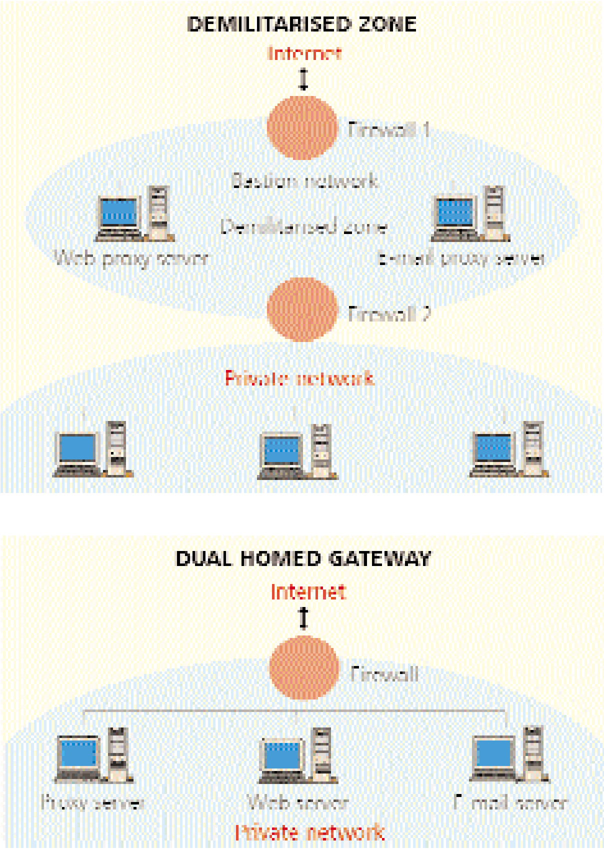
Neither can they prevent hackers from snooping when they wiretap telephone lines intended for remote network maintenance.

Firewalls fail when the systems encounter viruses and Trojans that users download from the Net or get through e-mail. They cannot fight the new areas of infection such as ActiveX, Java and HTML-based viruses. True, some firewalls offer virus protection by scanning incoming e-mail, but the only effective solution in such cases is a strong network access policy.

Firewalls also fail when it comes to the physical security of data and hardware failure. After all, what good is a reliable firewall when someone can walk into your office premises and walk out with your data? Or if it is destroyed by an accident like fire?

Trusted users with access to the network could play havoc with the data too. Perhaps this is why many organisations are establishing firewalls internally to secure, say, the finance or personnel department, from the rest of the organisation. Nor are they of much help if the network system with which your network has a trust relationship, like your supplier or customer, is broken into through which your network can be compromised.

In short, don t place all your bets on your firewall.



Two basic configurations of a Firewall

network are 'hidden' from the untrusted source and provides authentication services to registered users from the untrusted network. Perhaps the only problem with application proxy firewalls is that they are slow.

In the packet inspection firewall (an extension of the packet filter firewall), besides data packet-addresses and ports, the content of the packets is also considered before accepting or rejecting the data packet. This 'inspection' of the packet can be either based on its 'state' or 'session'.

Some network services are more open to misuse, so the firewall must be configured to restrict access to these services

In case of state inspection, the firewall only allows an incoming packet if it can be matched with an outbound request (or 'invitation') for that packet. If there is no corresponding request, the packet is rejected.

In case of the session filtering, rather than inspecting the packet's content, the network session is tracked. Once the trusted network user terminates the session, all incoming packets with identity pertaining to that session are rejected.

An analogy would be the 'open to public' days held by the Armed Services. Here the general public is 'invited' to wander about selected restricted areas and inspect military hardware. However, once the 'open to public' days are over, no one is allowed to visit the restricted area.

Establishing the foundation

Real-life firewalls are almost always a hybrid of the different types of firewall. It is how you organise the different components together that will determine how effective your firewall is.

There are two ways in which firewalls can be set-up: dual-homed gateway and demilitarised zone (DMZ). In a dual-homed gateway setup, a single firewall with two connections is used, one for the trusted network and the other for the untrusted one. A DMZ setup uses two firewalls. As before, both firewalls have two connections, but with a difference.

The first firewall has one connection leading to the untrusted network and the second leading to host systems that can be accessed through the untrusted network. The host systems—usually e-mail or Web servers—in turn are connected to another firewall, which links them to the trusted network. The area between the firewalls is called the 'demilitarised zone'. The host systems populating this region are known as bastion servers and the network so created is called a bastion network.

Of the two, DMZ is inherently more secure: Should an unauthorised user from the untrusted network get through, he only gets to the bastion network, while the trusted network remains safe within the second firewall.

A look at the standards

While how effective a firewall is eventually depends upon how you configure your firewall, it helps if you know that the product that you are purchasing meets certain standards. In firewalls, this internationally accepted 'standard' is provided by the ICSA, the International Computer Security Association.

Founded in 1989 as the NCSA and focussing on virus threat, the ICSA is an independent corporation that certifies security products and establishes security practices. An ICSA-certified firewall means that you can rest assured that the product meets a certain minimum standard of security. What this means is that when the product is configured according to the manufacturer's instructions, it will provide protection from known attacks while providing operational access to the Net and vice versa.

However, please note that it is how well you fine-tune a firewall that makes it effective. And this can only happen if you have a security policy set in stone that defines what approach to take while setting up firewalls.

Dangerous connections
A look at some vulnerable network services

NETWORK SERVICES	PORT	DESCRIPTION
DNS	53	Contains information on host computers, useful to crackers
FTP	20, 21	Poorly configured, it can be used to download password files
Remote procedure calls	111	Password and system files can be stolen
Remote services	512 to 514	Includes rlogin, rsh and rexec services. Permits unauthorised access to accounts and commands
RIP	520	Can be spoofed to redirect data packets
SMTP	25	Transports e-mail. Can be used to gain access to the system
Telnet	23	Can provide access to the system if improperly configured
Trivial FTP	69	Can be used to read any file on the system
UUCP	540	Poorly configured, it can be used to gain access to the system
X- & Open Windows	6000+ & 2000	Can leak data from display, including keystrokes. Intruders can even control the X-server

Honing the edge

Keening the firewall's edge begins with establishing what network service access policy to adopt when setting up a firewall and this can be done in two ways—the open access to all services except selected ones; and the restrictive no-access-to-any services except selected ones.

In most cases the latter policy is the better option. The restrictive, no-access-to-any-services policy only allows access to e-mail services to enable communication. Most system administrators usually also disable services such as Telnet, which allows remote users or 'guest' users from the Internet to log into the network. (*See box 'Dangerous connections'*)

However, making a network secure does not end at the installation of a firewall and through a network policy. Once the firewall is installed, a regular 'firewall health check' has to be done because a network organically grows and changes with user needs (especially when users establish their own network services).

You can even check if all the measures that you have taken are good enough by opting for ICSA's TruSecure security assurance services. This service tests your network's vulnerability to attacks from the Net.

However, do remember that there is no such thing as a perfectly secure network. A growing network also increases the possibility of intrusion and the possibility of detection. According to another survey conducted on 38,000 computer systems belonging to the US Department of Defense, 33,440 systems were broken into. Less than one in twenty were detected.

And your network could be next, unless you have a firewall.

ARJUN S RANA

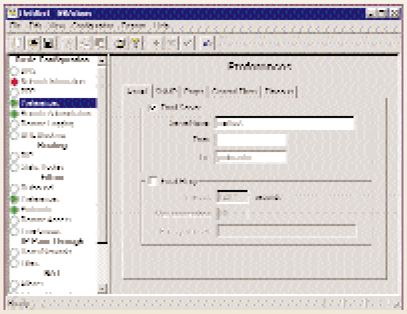
SECURITY TOOLKIT

FIND IT ON THE CHIP CD

GNAT Box Light 2.1.1

A light version of the commercial GNAT Box firewall, GNAT Box Light supports a maximum of 100 concurrent connections from within the trusted network. External connections from the untrusted network are, however, more restrictive a maximum of four unique incoming source addresses are allowed by this application proxy firewall. But hey, what more can you ask from something that is free?

The interesting part about GNAT is that it fits in a single floppy disk and is a totally self-contained system. It does not run on top of any operating systems, just boot your PC from the disk and you are in business. The advantage of having an operating system-independent firewall is that it is not vulnerable to viruses that normally plague popular operating systems like Windows. The GNAT also comes with both Web and console-based administration tools to configure the firewall and has to be installed on a separate machine.



NukeNabber 2.0b

Designed to monitor hacker attacks, the NukeNabber is another free tool for network administrators. Running on Windows 9x/NT operating system, the program can be configured to listen to up to 50 ports for possible hacker activity. The program also includes an option to block port scanners and offers multiple pre-defined intrusion logging options from low to high or custom security logging.