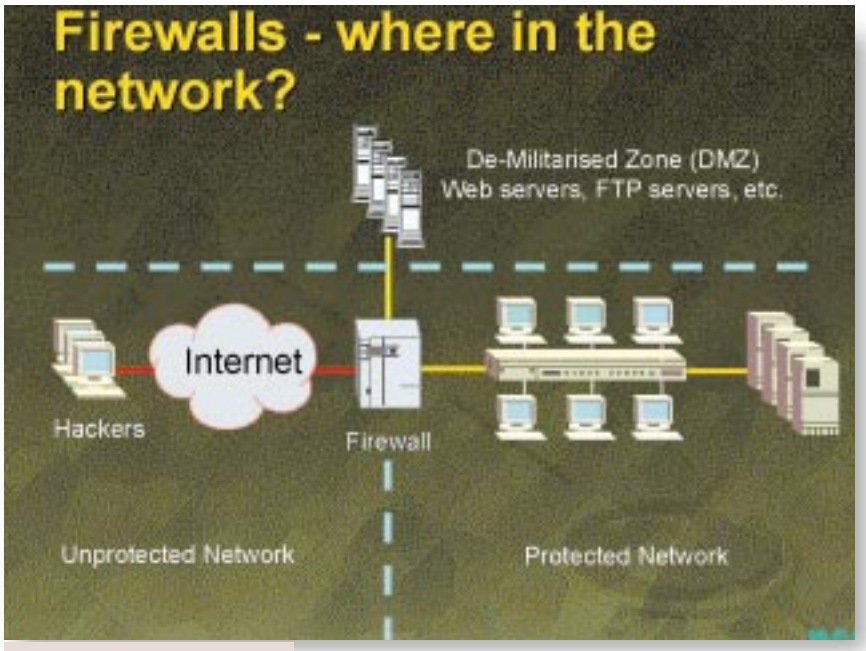
The heat is on

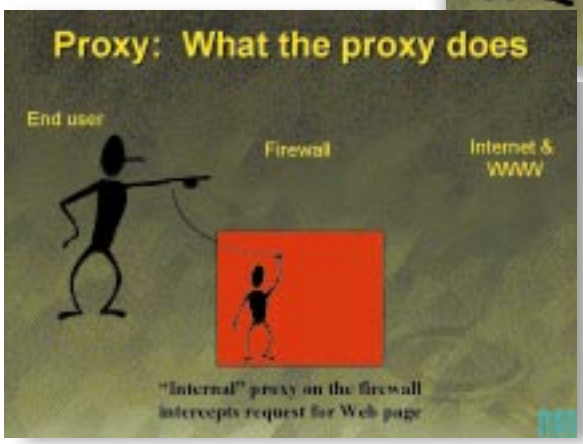
Bob Walder tackles firewalls, a crucial weapon in the war against corporate hacking.

In previous columns I have covered the mystic world of IP addressing, WINS, DNS, routing and internet connectivity. Anyone who has followed this little lot and actually got as far as connecting their network (big or small) to the internet will no doubt be worried sick about all those nasty little hackers out there just waiting to break in, rifle their server's disks for juicy data, and wipe everything clean or install terrible viruses, before disappearing back into whatever adolescent world they inhabit. What do you mean, you hadn't even considered it?

One in five respondents to a recent survey admitted that intruders had broken into, or had tried to break into, their corporate networks, via the internet, during the preceding 12 months. This is even more worrying than it sounds, since most experts agree that the majority of break-ins go undetected. For example, attacks by the Defence Information Systems Agency (DISA) on 9,000 U.S. Department of Defence computer systems had an 88 percent success rate but were detected by less that one in 20 of the target organisations. Of those, only five percent actually reacted to the attack, says the National Centre of Supercomputing Applications (NCSA).



▲ KEEPING THE BAD GUYS OUT: A FIREWALL IS A NETWORK'S MEANS OF PROTECTION AGAINST DANGEROUS NET ELEMENTS
▶ ALL NET TRAFFIC CAN BE CONSTANTLY MONITORED USING A STATEFUL INSPECTION FIREWALL
▼ PROXY SERVERS ACT AS INTERMEDIARIES IN CLIENT/SERVER OPERATIONS



Mind the gap

So, is there anything you can do about it? Plenty, as it happens, so I thought I would set you on your way by covering the subject of firewalls: how they work, and how you use them.

Essentially, a firewall should be thought of as a gap between two networks — in our case, an internal network and the internet — occupied by a mechanism that lets only a few selected forms of traffic through. The important thing to remember is that there are three main firewall architectures currently in use.

Static Packet Filtering Working at the Network Layer (i.e. very low down) in the OSI stack, packet filters make simple deny or permit choices depending on the network address of the packet and a number of rules defined by the administrator. Packet filtering is fast, transparent (no changes are required at the client), flexible and cheap: most routers will provide packet filtering capabilities, and pure packet filter firewalls do not require powerful hardware.

Dynamic Packet Filtering/Stateful Inspection Some vendors are touting this as the "third generation" of firewall architectures, but it's really just an extension of the basic packet filtering architecture employed by most routers. Stateful Inspection occurs low down in

BEHIND THE MASQUE

Another important feature of today's firewall is Network Address Translation (NAT). This is also occasionally referred to as "IP Masquerading". Here's how NAT works. When one of the machines on your internal LAN wants to communicate with one elsewhere on the internet, it sends a packet to the firewall using its normal IP address. On its way through the firewall, the packet is altered — its return address is replaced by the IP address belonging to the firewall itself. All responses to those packets therefore come back to the firewall. The firewall then reverses the address-swapping process and passes the reply straight back to the target computer .

Why is this useful? First, the outside world never gets a glimpse of the addressing structure of your protected network. Everything looks as though it is coming from a single address — that of the firewall. This then gives rise to a useful side effect. If the internal address is never seen by the outside world, there is no need for any of the computers behind the firewall to have legitimate IP addresses. This provides complete freedom for your internal IP numbering system. There are several groups of IP addresses which are considered to be "reserved" and are never actually used on the internet, making them ideal for use in an internal numbering system protected by NAT. They are: 10.0.0.0 to 10.255.255.255; 172.16.0.0 to 172.31.255.2551; and 192.168.0.0 to 192.168.255.255

The use of NAT also means that the firewall will allow any number of machines on the LAN to share a single, legitimate IP address, thus making your internet connectivity costs that much lower.

the network stack, at the MAC or Network Layer, thus making it fast and preventing suspect packets from travelling up the protocol stack to the operating system above (never a good thing!). Unlike static packet filtering, however, Stateful Inspection makes its decisions based on all the data in the packet, corresponding to all the levels of the OSI stack.

The state of the connection is monitored at all times (hence Stateful Inspection), allowing the actions of the firewall to vary based on the administrator-defined rules and the state of previous conversations. In effect, the firewall is capable of remembering the state of each ongoing conversation across it, thus allowing it to screen all packets for unauthorised access while maintaining high security, even with connectionless protocols such as UDP.

Inevitably there are penalties to be paid for this level of security

Proxy Servers Working very high up at the Application Layer of the OSI stack, a Proxy Server firewall acts as an intermediary for user requests, setting up a second connection to the desired resource either at the application layer (an application level gateway) or at the session or transport layer (a circuit-level gateway).

Proxy code is effectively split into two halves, and actually "stands in" for both client and server operations, relaying valid requests between the trusted and untrusted networks via the proxies. For a simple client request to retrieve a web page, the proxy server fools the client into thinking that it (the proxy) is the required web server. It then passes the request to its "external half", which pretends to be the client making the request. As far as the outside world is concerned, the protected internal network does not exist — all that is visible is the external portion of the proxy. The web server passes the page back to the proxy, which transfers it to the internal proxy, which finally passes it on to the user's web browser. Unlike Packet Filter and Stateful Inspection firewalls, a direct connection is never allowed between the two networks. The penalties paid for this level of security, however, are performance — Proxy Server firewalls have large processor and memory requirements in order to support many simultaneous users, and flexibility — the introduction of new internet apps and protocols can often involve significant delays while new proxies are developed to support them.

While static packet filtering alone is usually confined to the router these days and not considered strong enough for enterprise-class firewall devices, the differences between the remaining two architectures are negligible. True proxy servers are the safest, but impose a severe overhead in heavily loaded networks. Dynamic packet filtering is definitely faster, though most high-end firewalls are hybrids these days, using elements from all three architectures.

Most of the currently available products are available as dual or tri-homed gateways: they have two or three separate network interfaces for the internal, external and "De-Militarised Zone" (DMZ) networks. The DMZ adds extra protection for the internal network, providing a secure subnet which allows internal web, FTP and mail servers to be accessed from both the trusted and untrusted sides of the firewall without compromising security. Even if an attacker on the external segment manages to compromise machines on the DMZ, everything on the inside remains guarded by the firewall.

A DMZ is the only safe way of allowing external users access to some of the servers on your site.

PCW CONTACTS

Bob Walder *can be contacted via the usual PCW editorial office (address, p10) or email* networks@pcw.vnu.co.uk.