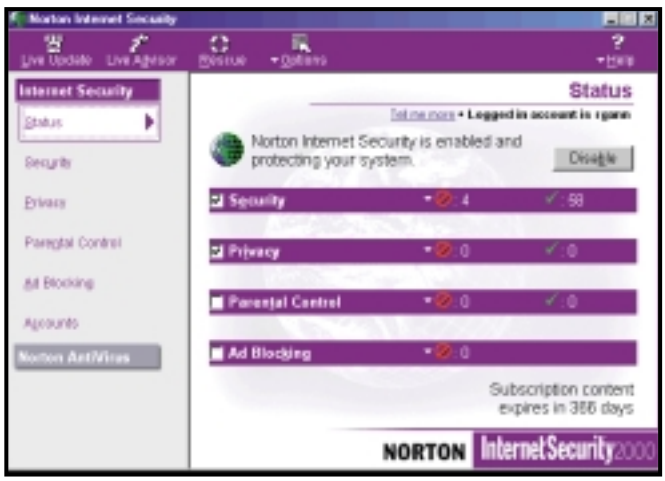
Block those trespassers

Firewalls are a necessary part of a network, however large or small explains Roger Gann.

Over the past couple of columns I've been banging on about the importance of security if your network is connected to the Internet. I've looked at simple security measures you can take that'll cost you nothing and last month I talked about the protection that all proxy servers offer, that of Network Address Translation (NAT). This month, it's time to get hardcore about network security – I'm going to look at firewalls.

A firewall is a system designed to prevent unauthorised access to or from a private network. It protects a trusted network from an untrusted network. The most important aspect of a firewall is that it is located at the entry point of the networked system it protects. Essentially this means that the firewall is the first program or process that receives and handles incoming network traffic and it is the last program to handle outgoing traffic.

Firewalls can be implemented in both hardware and software or a combination of both. They're frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.



Personal firewall packages include Norton's Internet Security 2000

Firewalls can use a variety of security techniques:

● **Packet filtering**

All Internet traffic travels in the form of packets – all file downloads, web page retrievals, emails – and these Internet communications always occur in packets. This technique examines every packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packets can be allowed or disallowed on the basis of the source IP address, on the basis of the destination port or on the basis of protocol used. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing. This is where a host sends out packets which claim to be from another host. Since packet filtering makes decisions based on this source address, IP spoofing is used to fool packet filters. It is also used to hide the identity of attackers using attacks such as SYN, Teardrop, Ping of Death and the like.

A firewall is not a 'fit and forget' device: it needs to be managed and monitored

● **Application gateway**

This applies security mechanisms to specific applications, such as FTP and Telnet servers. It acts as a proxy for applications, performing all data exchanges with the remote system on their behalf. It can allow or disallow traffic according to very specific rules, for instance permitting some commands to a server but not others, limiting file access to certain types, varying rules according to authenticated users and so forth. Application-level gateways are generally regarded as the most secure type of firewall. They are, however, complicated to set up and maintain. They can also degrade performance of the network.

● **Circuit-level gateway**

This validates connections before allowing data to be exchanged. As well as scrutinising packets, it also determines whether the connection between both ends is valid according to configurable rules, then opens a session and permits traffic only from the allowed source and possibly only for a limited period of time. Once the connection has been made, packets can flow between the hosts without further checking.

● **Proxy server**

Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses. Some routers also feature NAT, which hides the IP addresses of the workstations behind the IP address of the router.

In practice, many firewalls use two or more of these techniques in concert. Remember, a firewall is not a 'fit and forget' device: it needs to be managed and monitored regularly, and action taken if there is an attack. If the attackers do get inside, security measures at each domain and server need to be implemented to prevent them looting systems.

Don't forget, either, that firewalls offer no protection against attacks that don't pass through the firewall. Sensitive data can be stolen from a company simply by copying it on to a floppy disk and walking out of the building with it. Uncontrolled remote access via modems and a constant stream of laptops in and out of a building are other examples of security weaknesses. For a firewall to work, it must be part of a consistent overall security architecture.

Firewall products

As a breed, firewalls are being downsized and becoming more affordable to small and medium-sized businesses. However, setting up a firewall still requires a good technical understanding of the principles of TCP/IP and other networking protocols and technologies. Despite their initial complexity, most of the simpler firewall packages have preset security policies, but allow you to develop your own network security policies, as you grow more familiar with them.

Most firewall products have, until recently, been too expensive for smaller networks and for personal use. However, a new breed of affordable personal firewall software and hardware-based firewalls has emerged. The additional challenge at this end of the market is making what is fairly complicated technology easy enough to configure and use by a non-expert end user. This requires many things to be done automatically, and for large amounts of detail to be hidden.

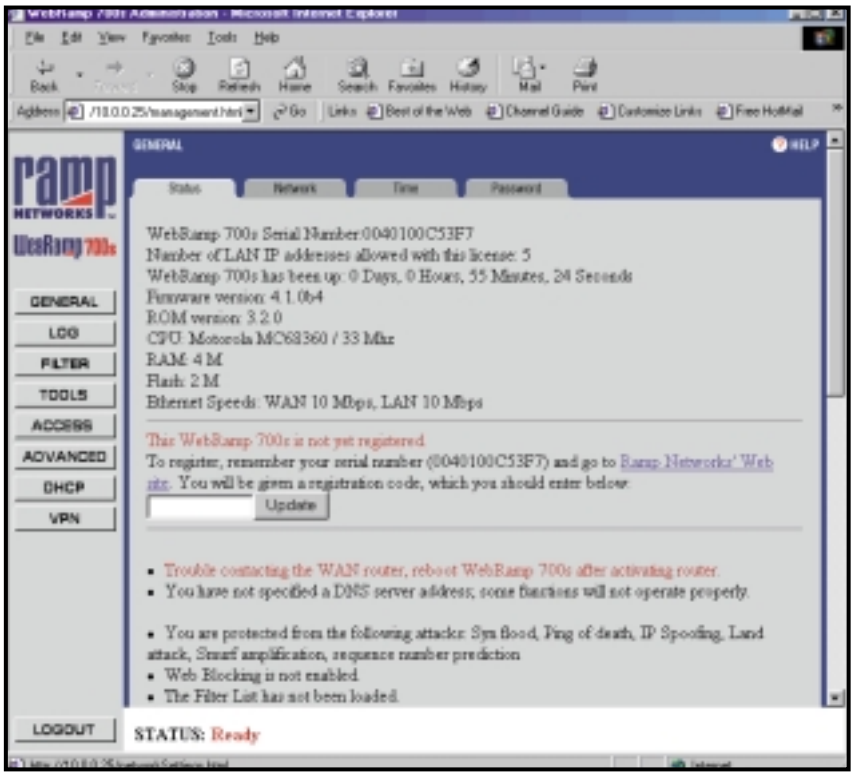
On the software side, the undoubted market leader is Network Ice's BlackICE Defender, which costs £24.21 from www.networkice.com.

Other personal firewall packages for Windows 9x include:

- ConSeal PC Firewall: £30.27 from www.signal9.com
- Norton Internet Security 2000: £32.70 from www.symantec.co.uk
- Sybergen Secure Desktop: £18.15 from www.sybergen.com.

There are one or two free firewall products available as well. The best known is ZoneAlarm 2.0 from Zone Labs, which is free for personal or non-profit use and can be downloaded from the company's site at www.zonelabs.com. The main difference between ZoneAlarm and all other firewalls, is that its primary focus is the prevention of the escape of information from inside our machines. By continuously monitoring the actions of every Internet-connected program running inside our machine, the ZoneAlarm firewall completely blocks unknown programs from connecting to the Internet. But ZoneAlarm's firewall goes further than this. Since it always knows exactly which programs are allowed to communicate, it also knows exactly which inbound traffic to expect and permit.

Thus, ZoneAlarm functions as a much smarter firewall than any traditional rule-based system ever could. It doesn't need low-level port, protocol, and IP address rules since it is able to operate at the higher trust-based application level. Zone Alarm is a bit flakey at present but it is free for most users – so you should beat a path to its door. Highly recommended.



WebRamp 700s is easy to configure and can restrict or block access to certain web sites

Steve Gibson also has a freebie firewall in the pipeline – check out his website http://grc.com for the latest news on this.

On the hardware side, two uncannily similar products have been released by Ramp Networks and Sonic Systems. The former is the WebRamp 700s, (see www.rampnetworks.com/products/700s/index.html) and the latter is the SonicWALL SOHO (www.sonicwall.com/products.html). Designed for small to medium-sized networks, these modem-sized devices sit between your network and the connection to your ISP. They offer very similar protection to that offered by full-blown firewalls, but at prices that start below £400. With one installed, you can restrict or block access to certain web sites, filter web content, monitor user access, protect your network from unauthorised access and so on.

These devices are also easy to configure, using a Java-enabled web browser interface. Both devices also offer detailed activity logs, which are essential if you're to trace persistent attacks on your network. You can also opt to be emailed when an 'attack' is detected.

I've had the WebRamp 700s for a couple of months now. It operates either in screening mode, where your users all have Internet-routable IP addresses, or in NAT mode, where your users all get private addresses. By default, it blocks all incoming connections to computers on your LAN but permits all outgoing connections, giving your users transparent network access without direct Internet exposure: the 700s uses a 'Stateful' inspection model, which is found in most high-end firewalls. The unit also protects your LAN from known denial-of-service attacks.

You can even optionally open holes in the firewall for individual FTP, SMTP, POP3, DNS, and HTTP servers on your LAN. By the same token, it's easy to block various types of activity, too, including RealAudio, Java and ActiveX applets and cookies.

CONTACTS

Roger Gann welcomes your comments on the Networks column. Contact him via the *PCW* editorial office or email:
networks@pcw.co.uk