Firewall for free

Roger Gann shows how network address translation can increase security on your network.

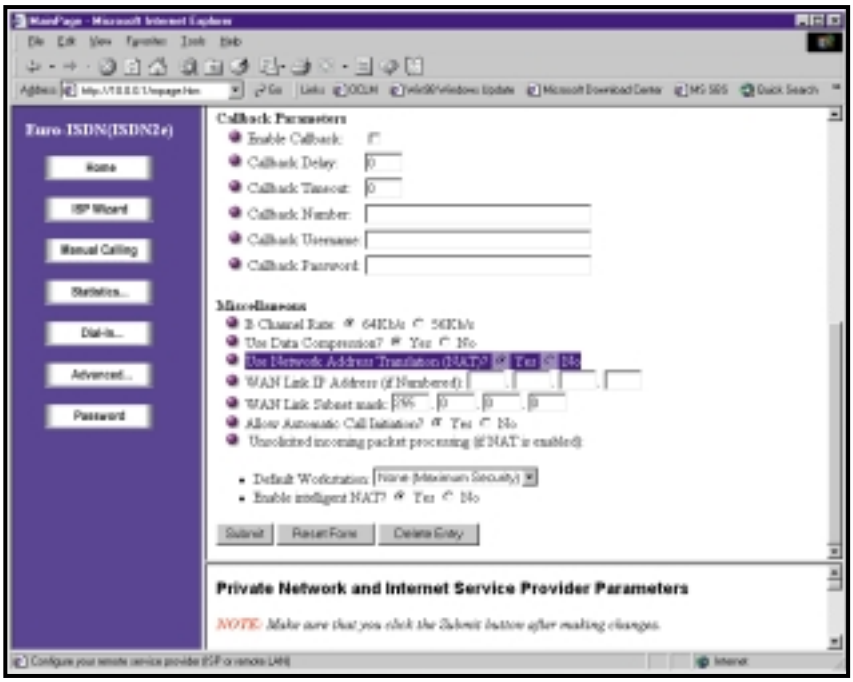
Last month I looked at the basics of Internet security – those simple, no-cost steps you can take to reduce the risk of exposure to hacking when you're connected to the Internet. This month, I'm going to up the ante and look at some of the low-cost security options available for the home and small-business user. A pretty good line of defence is offered by network address translation (NAT), a feature found in many low-cost routers and proxy servers. These products are designed to share a single connection to the Internet between several users, and the way this is achieved is via a process that involves NAT. In fact, the security and other benefits NAT affords are almost an incidental bonus.

NAT has three attractive features:

- It allows you to connect many more machines to the Internet than you have IP addresses for.
- Increased security. When you use reserved addresses behind the NAT router, the addresses are not globally routable. It is more difficult to attack hosts when you can't reach them directly.
- Additional security, because no inbound connections are allowed through the NAT translator unless it is specifically configured to allow them.

This dropping of inbound connections, while allowing outbound connections, turns NAT routers into cheap, low-end firewalls.

NAT can be provided either by hardware (ie a router) or by software (ie a proxy server). Either way, NAT hides your internal IP addresses from the outside world and it's this feature that makes it so secure. Under NAT, you use a range of 'private' IP addresses on your LAN. These are private in the sense that there are no computers connected to the Internet with an IP address in that range – so long as they are not connected to the Internet or each other, many thousands of computers around the world can have identical IP addresses.



NAT is an inexpensive way to provide good security from a dial-up connection

Only the router has a single 'public' IP address and so the router or proxy server has the job of working out which incoming packet belongs to which workstation. As a result, the only IP address that intruders see is the port on the NAT device which connects you to the Internet. A by-product of using private IP addresses on your network, is that it lets you use a common or garden dial-up ISP account. This is a cost-effective solution for small businesses that don't want to fork out to an ISP for a group of Internet-compliant addresses.

I use NAT on my small office network. It comes courtesy of a 3Com OfficeConnect ISDN LAN Modem (OCLM), which is a combined 10Base-T hub and ISDN router. All my PCs use IP addresses in the private range, 192.168.nnn.nnn. Like most of its rivals, the OfficeConnect LAN Modem is also a mini DHCP server, which means I can specify a range of IP addresses, say 192.168.0.1 to 192.168.0.10. Providing each workstation is configured to collect an IP address from the DHCP server when it first boots, I can forget about the tedious chore of allocating static IP addresses to all my workstations.

FIG 1

A NAT translation table

Workstation	Private IP address	Public IP address
WS1	192.168.16.12	204.116.73.1
WS2	192.168.16.26	204.116.73.2
WS3	192.168.16.27	204.116.73.3
WS4	192.168.16.59	204.116.73.4

How NAT works

NAT substitutes a globally-registered IP address into the source IP address part of a message leaving the private network. It then restores the private IP address into the destination part of a reply message entering the private network.

The best way to explain this is using an example. Figure 1 shows a NAT translation table. A message originating at WS1 has 192.168.16.12 in the Source IP Address part of the message header. As it passes through the NAT to the 'public' Internet, the NAT substitutes 204.116.73.1 into that part of the header and recalculates the

various message checksums. The message is then sent to the addressed host on the 'outside' as though it originated from the public address. When a message arrives at the NAT from the public Internet addressed to 204.116.73.1, the private IP Address of 12 is substituted into the destination part of the message header, the checksums are recalculated, and the message is delivered to WS1.

More typically, a range of private IP addresses map to the single IP address of the router (see Figure 2).

In this instance, the private network, 192.168.1.0, is 'hiding' behind the public address, 130.102.1.1 – the NAT router having the addresses 130.102.1.1 and 192.168.1.1.

All requests originating from the private network (192.168.1.0) have their source IP address replaced with the NAT router's public IP address, 130.102.1.1. Only one IP address is visible from the public network.

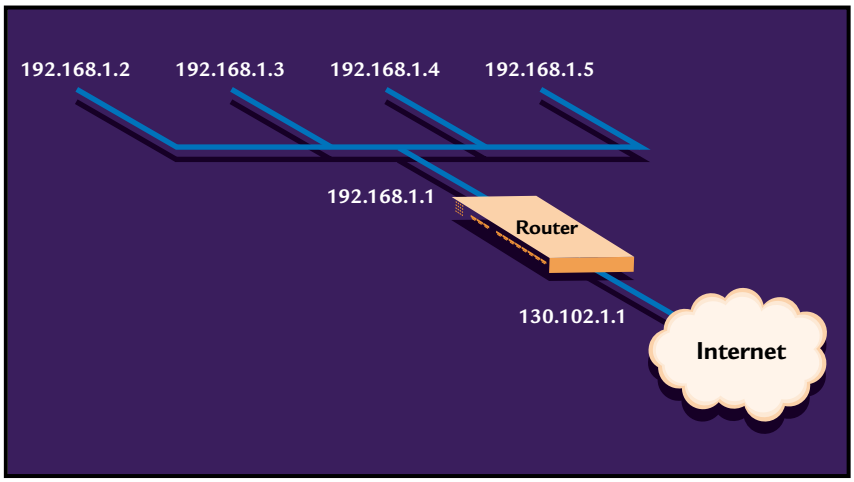


Fig 2: A range of IP addresses map to a router's single IP address

NAT protection

Thanks to NAT, instead of using an expensive 'business' ISP account, I can use a common or garden free ISP account, such as Freeserve or MSN FreeWeb. Whenever the OCLM spots IP traffic that is destined for addresses outside my network it connects to my ISP, where it collects a 'dynamic' IP address. It then translates the network addresses between the Internet and the private IP addresses, effectively buffering the private addresses from the Internet – as far as the rest of the Internet is concerned, there is only one IP address at the end of that connection. And what's attached to that address is a simple router and not a PC, which makes it just that little bit harder to hack. Note that, if the router does have password protection, it's essential to use it, to deter casual intruders.

NAT automatically provides firewall-style protection without any special set-up. That is because it only allows connections that are originated on the inside network. This means, for example, that an internal client can connect to an outside FTP server, but an outside client will not be able to connect to an internal FTP server because it would have to originate the connection, and NAT will not allow that. It is possible to make some internal servers available to the outside world via inbound mapping, which maps certain well-known TCP ports (eg 21 for FTP) to specific internal addresses, thus making services, such as FTP or the web, available in a controlled way.

NAT automatically provides firewall-style protection without any special setup

Many TCP/IP stacks are susceptible to low-level protocol attacks such as the recently publicised 'SYN flood' or 'Ping of Death'. These attacks do not compromise the security of the computer, but can cause the servers to crash, resulting in potentially damaging 'denials of service'. Such attacks can cause abnormal network events that can be used as a precursor or cloak for further security breaches. Routers with NAT do not use the host machine protocol stack, eg the Microsoft TCP/IP stack, but supply their own and this can provide additional protection from such attacks.

Most low-cost routers offer NAT, such as those from Nortel Networks (formerly Bay), Ramp Networks and Zyxel. But you don't have to invest in new hardware to get the benefits of NAT. For example, a couple of months ago I described Internet Connection Sharing (ICS), a new feature of Windows 98 Second Edition. ICS is, in effect, a software-based NAT server.

Other proxy servers – such as Deerfield.com's WinGate and Ositis Software's WinProxy 3.0 perform a similar job – although not for free. They're also a bit slower than hardware-based NAT. This is because, unlike proxy gateways, NAT gateways operate within the routing layer and are inherently much faster than their proxy counterparts. Since NAT routers do hide many machines behind a single IP address, putting a server behind a NAT router becomes a problem, since the NAT software has no way of determining for itself what IP address to forward the inbound connection requests to.

Of course, NAT routers do nothing to prevent users from downloading viruses or trojan horse programs (like the well-publicised trojan horse Back Orifice) but they do go a long way towards blocking attempts to connect inbound to the running trojan horse, if accidentally or maliciously installed.

NAT is not totally impervious to external attack either: there are several tools, called IP spoofers, that can deduce internal 'private' IP addresses and present themselves as being local users. Fortunately, these tools are not widely used, and only fairly sophisticated hackers would try to use them in breaking into your system. NAT, combined with a dial-up account and a dynamic IP address, is probably enough protection for most small businesses that aren't involved in ecommerce.

CONTACTS

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