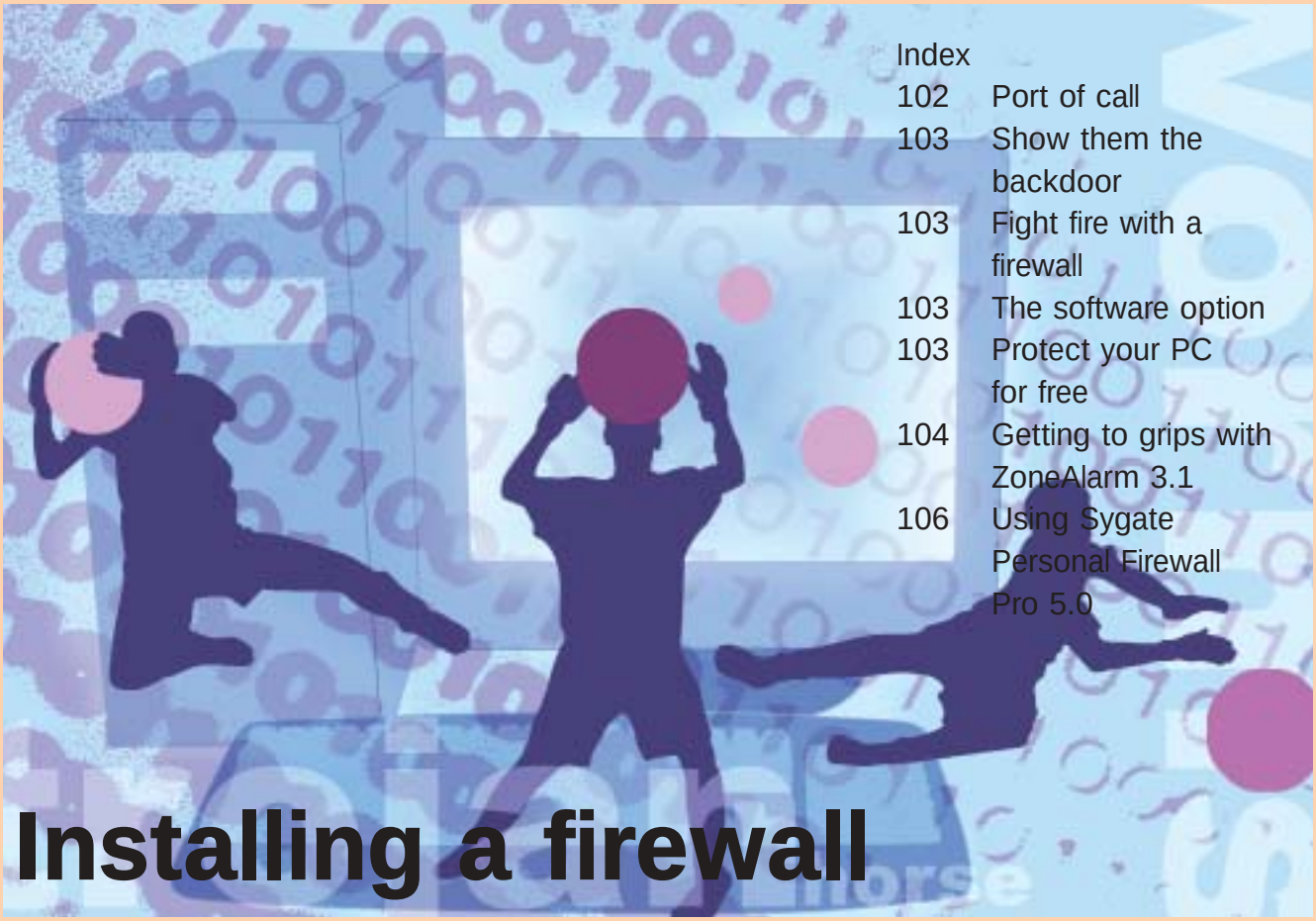
workshop



Index

102 Port of call
103 Show them the backdoor
103 Fight fire with a firewall
103 The software option
103 Protect your PC for free
104 Getting to grips with ZoneAlarm 3.1
106 Using Sygate Personal Firewall Pro 5.0

Installing a firewall

With always-on internet connections like broadband, it's more important than ever that you secure your PC from external attack. Robin Morris reviews the packages designed to do just that and helps you bolster your defences with a firewall

Riding a wave of publicity reminiscent of the worst excesses of the dotcom era, broadband suppliers are luring customers with the promise of high-speed transfer rates, smooth full-screen video and a direct connection to the web that never has to be turned off.

But what these companies fail to mention is that your newly wired PC could also play host to a variety of uninvited guests, from viruses and worms to Trojan horses and spyware. Theoretically, any PC attached to the internet is open to attack. But whereas your humble 56K modem isn't likely to be connected for more than an hour or two at most, broadband is designed to be always on, offering a potential 24-hour one-stop shop for malicious internet surfers.

Port of call

The majority of disturbances are the result of port scanning. Ports are like doors leading in and out of your PC – if your system wants to receive or send information to the outside world (the internet), it has to open a port before it can transfer a packet of data.

Certain ports are identified with particular activities. For example, TCP port 80 is used to access the worldwide web, while TCP port 21 is used for FTP (file transfer protocol) services. Hackers (or, to use the more accurate term, crackers) will run port scanning programs across large numbers of PCs connected to the internet, looking for any computers with open ports that they might be able to hijack. Once inside your PC, the cracker can write and delete files, look for passwords and credit card details or infect your machine with a virus or worm. Alternatively, he could install a backdoor program – a piece of code that sits undetected in your PC, waiting for instructions from its originator.

In theory, a backdoor program can make your PC do almost anything the cracker wishes. In a DOS (denial of service) attack, a targeted internet server is flooded by packets of data and rendered temporarily unusable.

Far more harmful and destructive is the DDOS (distributed denial of service) attack, where huge numbers of internet-connected PCs are ordered to flood the targeted server. These PCs are often 'innocent' systems being controlled through backdoor programs.

Show them the backdoor

Backdoor programs can also be installed through worms, viruses and Trojan horses. The latter comes disguised as a new game, application or utility but its real purpose is to smuggle a backdoor program on to your PC. Because Trojan horses often arrive as email attachments, there's a strong chance you may unknowingly invite the intruder on to your system.

Spyware works in a similar way to a backdoor program and sits on your hard drive relaying your personal information – ranging from what keys you've been pressing to which emails you've sent out and which websites you've been visiting – to an anonymous third party.

You probably won't even know when spyware appears on your system since it'll be installed as part of another software package. File transfer programs such as Kazaa are regular offenders.

The bottom line is that you need to exercise control over who is allowed access to your PC. The best way to do this is to install a software firewall which, in effect, surrounds your PC with high-security fencing. The firewall will investigate all data entering and, ideally, leaving your computer.

Fight fire with a firewall

A PC linked to the web can be identified through its IP (internet protocol) address and, by keeping a list of 'trusted' IP addresses, the firewall can choose to allow or block other computers trying to access your system.

If it has suspicions about a request, it can ask you whether you wish to authorise the visit. If you've just asked for a Windows update, for instance, and an IP address connected to Microsoft tries to send you data, you're probably in safe hands. But if a system located in Estonia contacts you out of the blue, you might want to exercise caution.

Alternatively if a program on your PC tries to access the internet, the firewall can check that it's supposed to be there. Most firewalls, particularly older versions, are less than competent at stopping data (such as your passwords) from getting out. There are basic firewall facilities built into Windows XP – for details on enabling them, click Start, Help and Support and type 'internet connection firewall overview' into the search box. But while these do a solid job of keeping intruders out, they make little attempt to confine rogue programs to your PC.

Instead you need a dedicated firewall package, preferably one that uses 'stateful inspection'. This increases the detection rate by thoroughly filtering the data and uses past experience of internet traffic on your computer to try and catch out intruders. The web is full of tools for testing the security of your firewall connection – www.grc.com/default.htm is a particularly good starting point.

The software option

If all of this sounds expensive you can rest easy. It's true that, for large networks, hardware firewall solutions can cost anything from a couple of hundred to several thousand pounds. But for the average small business or home user, a software firewall should do the job.

Many of these firewalls come with modest pricing policies – some won't even cost you a penny. Most of the packages will have to be downloaded over the internet, but you may find titles such as Norton's and BlackICE's available through high street retailers or reputable online suppliers such as Amazon.co.uk.

If you're new to firewalls look for a package that's user-friendly. Most of the US-based firewall companies have little or no presence in the UK, so aftersales support may be severely lacking. Luckily, most of the companies offer a wealth of information through their websites.

Online knowledgebases and FAQ (frequently asked question) pages offer solutions to most of the problems you're likely to have, while with the ZoneAlarm and Sygate packages you can access online forums and discuss your queries with fellow users.

Email enquiries are supported in most cases, although direct telephone enquiries aren't generally among the options. The big exception to the latter is Norton Personal Firewall 2003 where, if you've exhausted the other possibilities, you can ring the UK helpline. Unfortunately, at a cost of £18 (inc VAT) per incident, this won't be an appealing prospect.

Firewalls will keep data from getting in and out, but there's not much they can do about programs already installed on your PC. For maximum protection you should also install an antivirus package. At £43 ex VAT, Norton Internet Security 2003 is a bargain. This comprehensive virus package is combined with Personal Firewall 2003, so you get the best of both worlds.

Protect your PC for free

There's no need to shell out for a firewall if your budget's tight as the web has plenty of freebie downloads that will do the job admirably, particularly for home users. Here are a few suggestions to get you started.

- Agnitum Outpost **The free version of Agnitum's Oupost firewall comes with basic security functions – network monitoring, web privacy and packet/application filtering. www.agnitum.com**
- Sygate Personal Firewall **A gratis download for personal and home use, Sygate's Personal Firewall is a 'lite' version of its Pro software. The package will protect your system against Trojans, spyware, worms and other threats as well as prevent unauthorised or malicious applications bypassing its defences. Inexperienced users will find it easy to get to grips with. http://smb.sygate.com**
- Zone Labs ZoneAlarm **As well as offering a no-cost and painless introduction to the world of firewalls, ZoneAlarm is also incredibly effective. From the bright and intuitive interface to its comprehensive wizards, the firewall is constantly on hand to guide the user through the maze that is internet security.**

Behind this plain exterior lurk inner workings as complex as those of any package on the market. But because it's so simple to use, it won't be hard to set up the right level of protection. www.zonelabs.com

Getting to grips with ZoneAlarm 3.1

ZoneAlarm enjoys a reputation as one of the most intuitive firewall packages on the market – even the free version, used here, will make a great job of protecting your PC. Choosing the default settings should be enough to secure your PC against intruders, although the tutorials and extensive help resources will prove handy if you want to maximise security.

1 ZoneAlarm's colourful menu system offers helpful advice and clear choices at every step. From this screen we can set the level of security. ZoneAlarm's Internet Zone Security is currently set to High, so we're protected from outside influences. Turning it down to Low will switch off the firewall function.

Note the red Stop button at the top of the screen. This is always present. Any time you feel your machine is vulnerable to attack, a single click on the Stop button will temporarily close off all contact with the outside world

3 This ZoneAlarm Alert is more worrying – another computer on the internet has tried to access our PC using port 1434. We don't recognise the IP address or the port, so click on the More Info button under AlertAdvisor. Thanks to ZoneAlarm's online database we can be reasonably certain that this was an attempt to copy a worm to our PC. This probably wouldn't have damaged our machine but it might have slowed things down. Luckily, ZoneAlarm refused access and protected us from danger

2 ZoneAlarm has just warned us that an installed program is trying to access the internet. The information bubble clearly tells us that 'nlnotes.exe' is the application in question. Since we've just opened our Lotus Notes email client, we can rest safe in the knowledge that there's nothing sinister afoot.

Click Yes to allow email access, ensuring that the checkbox for 'Remember this answer the next time I use this program' is ticked, otherwise ZoneAlarm will ask you for confirmation every single time the email package tries to connect to the web

4 From the Alerts & Logs screen we can see names and IP addresses for all of the machines and programs that have tried to transfer data in or out of our PC. We've told ZoneAlarm not to inform us when another computer tries to access our PC but, should we be curious, all the details are logged here. We can also see which connections and programs were allowed and which ones were blocked. If an innocent IP address is being turned away, select its entry and click on the Add to Zone button to put it on the Trusted list

Using Sygate Personal Firewall Pro 5.0

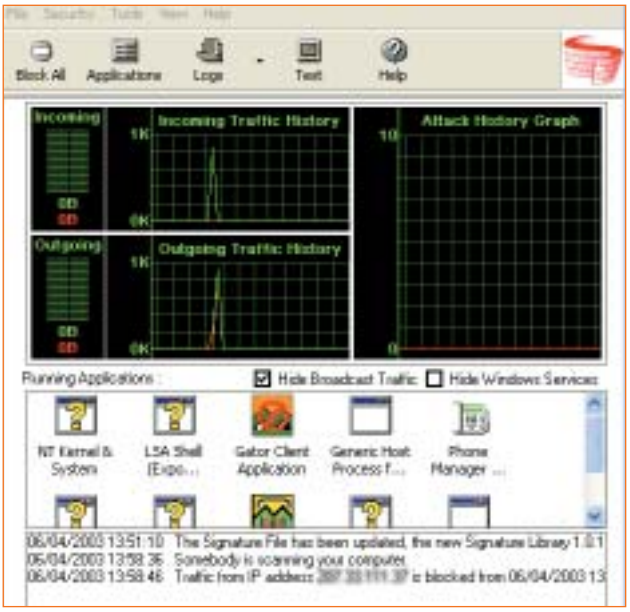
While ZoneAlarm is perfect for newcomers, Sygate's Personal Firewall Pro 5.0 is the choice for those who want something to sink their teeth into. The problem is that the average user won't be able to find, much less understand or operate, most of the functions.

There's no doubting the power of the software, however. Sygate uses some excellent techniques, including fingerprinting of files, to ensure the integrity of applications and programs bouncing around in your system, while most Trojan horses are swiftly dealt with. The detailed rules system Firewall Pro applies gives you almost complete control over how ports, protocols and applications are handled.

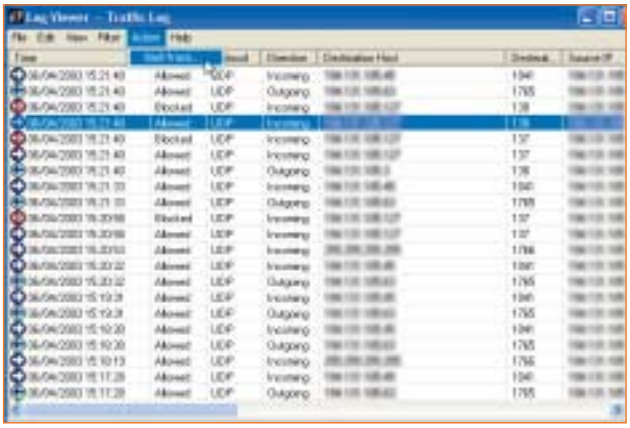
When another system does try to access your PC, the Action menu's illuminating BackTrace / Whois command is effective at identifying the sender. You can even get the program to run a battery of security tests on your system to identify potential loopholes.

It's a shame Sygate's obscure interface makes it difficult to harness the power of Personal Firewall. Be prepared to spend many hours trying to master even basic functions. Still, the online help forums and knowledgebase will give you plenty of ideas, while the vastly cut-down Personal Firewall 5.0 is a free download from http: / / smb.sygate.com, as is a trial of the Pro version for any home users who want to try it for size.

1 When it first loads, Sygate Personal Firewall Pro will alert you when any program tries to access the internet from your PC or your PC from the internet. You must tell the software whether to allow the traffic or not then, as with ZoneAlarm, a pop-up notification box appears above the System Tray to tell you that your chosen action has been performed. Tick the 'Do not show this window again' option and Sygate won't bother you the next time it blocks the same application



2 Firewall Pro has a graphical status monitor which looks not unlike Windows System Resources Manager. It monitors incoming and outgoing traffic and gives updates on current activity in the Message Console



3 Choose View, Traffic Log to see all the comings and goings on your PC. Click on any of the log entries and choose Action, BackTrace to reveal the source of the traffic, and hit the Whois button for further information