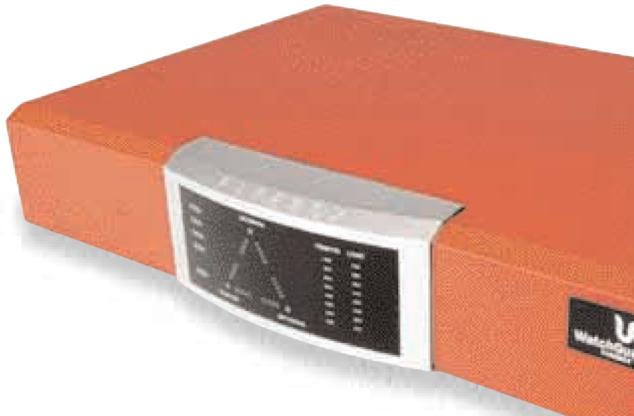
Hardware firewalls



Eight of the top vendors pitch their best defenders against Dave Mitchell's scrutiny

Firewalls have been in the domain of the enterprise network for many years, but with more and more small businesses switching to always-on Internet connections, the risks to their data are now great enough to warrant the same tough approach to intruders. No longer is an on-demand PSTN or ISDN connection sufficient for the communication needs of the majority of companies irrespective of their size. With many hosting their own Web and mail servers, a permanent connection is the only answer, and the price drop for many xDSL business packages means it's more cost-effective as well. However, the drawback of being online permanently is that the risk of having your data compromised by external attack has just gone up, making a firewall an essential purchase.

The consumer market is filled with personal firewalls, but these software utilities are of severely limited use to businesses. They simply don't have the features or the power to deal with the high levels of inbound and outbound Internet traffic being generated by multiple users and the various different internal services. Furthermore, they'd be useless against threats such as a DoS (Denial-of-Service) attack. The only answer is a dedicated business-level firewall, and in this month's group test we take a look at eight hardware solutions designed for small to medium businesses and remote or branch offices.

> Software utilities are of severely limited use to businesses, as they simply don't have the features or the power

All the firewalls in this test use stateful packet inspection, allowing them to detect and block attacks far more efficiently than other filtering methods. The most basic is packet filtering, which simply examines the information held in the IP address in the packet header and checks it against a list to see if it should be accepted or denied. This can be used for blocking access to specific Web sites, as the IP address of these sites will be contained in the header of the incoming packet. The advantage of packet filtering is high performance, but security is minimal, as the filtering mechanism is only examining packets at the network layer and can't therefore determine what application, if any, they're bound for, making it easier for hackers to break in. Connectionless protocols such as UDP (User Datagram Protocol) can be difficult to filter, since there's no distinction between the request and the response.

Invented by Check Point, stateful inspection still intercepts packets at the network layer for the best performance, but it looks at the contents as well as the header of each packet, allowing it to gather far more information than merely the source and destination addresses. The term is derived from the fact that this process examines the contents of the packet to see what the state of the communication is, so it can ensure that any inbound communication is as a result of being requested by the destination system. The firewall is now capable of ensuring that all communications are initiated by the recipient computer. A further advantage of the stateful inspection firewall is that it keeps ports closed until a connection request is received, increasing the protection against port-scanning activities.

Although these tools are mostly optional extras, the firewalls on review offer a wide range of possibilities for tightly controlling Internet access. Many can perform Web content filtering, allowing you to ensure access is denied to dubious Web sites, or you can use it to log the access behaviour of users. In the case of the firewalls from 3Com and SonicWALL, you can also apply filtering to email attachments and use lists of forbidden file extensions, so the firewalls can either delete them on receipt or disable them by altering the extension name. Along with firewall facilities, all the products offer support for VPNs (virtual private networks), allowing secure tunnels to be created between firewalls and remote users, where all data passing along these pipelines is encrypted for maximum security.

By their nature, firewalls can be complex, so ease of installation and configuration have to be key features. With the consequences all too obvious, no business can afford to make a mistake when configuring their firewall, so the user interface needs to be as intuitive as possible, and this should be backed up by good supporting documentation and online help. Alas, during testing, we found this generally wasn't the case, with even simple Web browser access proving either impossible or extremely difficult to achieve in the case of two products. Setting up rules to allow or deny traffic in or out of the firewall proved a problem with many of the firewalls and, in some cases, was frustrating due to the arcane methods required. Documentation was also found to be inadequate, particularly when it came to creating rules for specific protocols and port numbers.

We invited ten companies to participate in this group test and only two declined. Nokia was unable to send in any firewall products, advising us that this was due to 'resource bandwidth issues'. No, we had no idea what this meant either and, after we queried it further, Nokia explained that it didn't have a suitable review machine available. NetScreen also declined, saying that it didn't sell its SME firewall products directly as standalone devices.

SPECIFICATIONS AND FEATURES

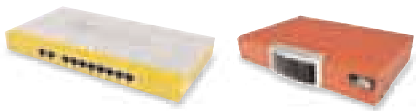
PC PRO LABS WINNER

	3Com SuperStack 3 Firewall	Cisco PIX 515E	GTA GB-1000	Intrusion PDS 2105	Lucent VPN Firewall Brick 80	SonicWALL PRO 300
Overall score	★★★★☆☆	★★★☆☆☆	★★★☆☆☆	★★★☆☆☆	★★★☆☆☆	★★★★★☆
Price (exc VAT)	£2,320	£2,330	£2,295	£2,770	£2,663	£3,400
Basic warranty	Lifetime	1yr	1yr	1yr	1yr	1yr
Manufacturer's Web site	www.3com.co.uk	www.cisco.com	www.gta.com	www.intrusion.com	www.lucent.com	www.sonicwall.com
Supplier	3Com 01442 438000	Cisco Systems 020 8824 1000	GTA 0870 458 1113	Intrusion 01252 812030	Lucent 020 7004 0000	SonicWALL 01344 668090
HARDWARE						
Processor	StrongARM RISC	Intel Celeron	Intel Celeron	Intel Celeron	AMD K6-2	StrongARM RISC
Speed (MHz)	233	433	800	600	350	233
Memory	16Mb	32Mb	64Mb	64Mb	32Mb	64Mb
Expansion slots	✖	✔ (2 PCI)	✔ (1 PCI)	✖	✖	✖
Power supply	Internal	Internal	Internal	External	External	Internal
NETWORK INTERFACES						
Number	3	2	4	3	4	3
Type	10/100BaseTX	10/100BaseTX	10/100BaseTX	10/100BaseTX	10/100BaseTX	10/100BaseTX
LAN	✔	✔	✔	✔	✔	✔
WAN	✔	✔	✔	✔	✔	✔
DMZ	✔	Optional	✔	✔	✔	✔
Other	✖	✖	1 (LAN/DMZ)	✖	1 (LAN/WAN/DMZ)	✖
FIREWALL TECHNOLOGY						
Stateful packet inspection	✔	✔	✔	✔	✔	✔
Static packet filtering	✖	✖	✖	✖	✖	✖
Max. concurrent connections	30,000	125,000	32,000	Not stated	25,000	128,000
NAT	✔	✔	✔	✔	✔	✔
DHCP	✔	✔	✔	✔	✔	✔
PPPoE	✔	✔	✔	✔	✔	✔
High availability	✔	Optional	✖	✖	✔	✔
Load balancing	✖	✖	✖	✖	✖	✖
Web content filtering	Optional	Optional	Optional	Requires Filtering Server	✖	Optional
Content database	CyberNOT	WebSENSE	CyberNOT	N/A	N/A	CyberNOT
Virus protection	✖	✖	✖	Requires AV Server	Optional	Optional
Email content filtering	✖	✖	✖	✖	Optional	Optional
Spam filtering	✖	✖	✖	✖	✖	✖
MANAGEMENT						
Out-of-band management port	✖	Serial	Serial	Serial	Serial	Serial
Telnet	✖	✔	✔	✔	✔	✔
Web browser	✔	See below	✔	✔	✖	✔
Other	Transcend Network Monitor	Cisco PDM	GBAdmin	✖	LSMS	✖
VPN SUPPORT						
IPsec	✔	✔	✔	Not supplied	✔	✔
IKE	✔	✔	✔	N/A	✔	✔
PPTP	✔	✔	✔	N/A	✔	✔
Tunnels supported	1,000	2,000	Not stated	N/A	400	1,000
User licence included	50	0	0	N/A	5	50
VPN client software	IRE SafeNet/Soft-PK	Cisco VPN Client	IRE SafeNet/Soft-PK	N/A	Lucent IPSec Client	IRE SafeNet/Soft-PK

TEST RESULTS

TEST TYPE	3Com SuperStack 3 Firewall	Cisco PIX 515E	GTA GB-1000	Intrusion PDS 2105	Lucent VPN Firewall Brick 80
NMAP Stealth Scan	⚫	⚫	🔴	🔴	🔴
NMAP OS ID	🟠	🟢	🟢	🟢	🟢
SYN Flood	🟢	⚫	⚫	🔴	⚫
Smurf	🟢	⚫	🟢	🟠	🟢
UDP Traceroute	🟠	🟢	⚫	🟢	🟢
PING	🟠	🟢	⚫	🟢	🟢

Key: 🟢 Attack failed and logged 🟠 Attack failed but not logged 🔴 Attack succeeds but logged ⚫ Attack succeeds and not logged



Symantec Firewall/VPN 200R	WatchGuard Firebox 1000
★★★☆☆	★★★★☆
£850	£3,326
1yr	1yr
www.symantec.com	www.watchguard.com
Symantec 0800 389 7030	WatchGuard 01737 735491
Not stated	AMD K6-2E
N/A	300
Not stated	64Mb
✖	✖
External	Internal
10	3
10/100BaseTX	10/100BaseTX
✔	✔
✔	✔
✔ (One system only)	✔
Eight-port 10/100BaseTX switch	✖
✔	✔
✖	✖
Not stated	Not stated
✔	✔
✔	✔
✔	✔
✖	Optional
✔	✖
✖	✔
N/A	SurfControl
✖	Optional
✖	✔
✖	Optional
✖	Serial
✖	✖
✔	✖
✖	Control Centre
✔	✔
✔	✔
✔	✔
Not stated	1,000
Unlimited	5
Enterprise VPN Client	Mobile User VPN

SonicWALL PRO 300	Symantec Firewall/ VPN 200R	WatchGuard Firebox 1000
⚫	🔴	🟢
🟢	🟢	🟢
🟢	⚫	⚫
🟢	Test not applicable	🟠
🟠	🟢	⚫
🟠	⚫	🟢

How we test

Instead of running basic performance and throughput tests, we decided it would be more applicable to see how each firewall coped with a range of common Internet-borne attacks, and our thanks go to I-SEC (**www.i-sec.biz**) for creating a test scenario that involved running basic penetration tests on each firewall. Based in Brighton, I-SEC offers a range of risk-assessment services, which includes penetration testing, vulnerability assessment and secure configuration of firewalls and Web sites.

Each firewall was connected into a test network (*see below*) that represented a typical small business setup, with local users behind a protected LAN port, Web and mail servers on a DMZ port and a WAN port connected to a router providing Internet access. Configuration was kept to a minimum to simulate the typical small business that's going to use the default settings on the firewall and then open up basic access to the Internet and servers on the DMZ.

Five tests were conducted:

1. NMAP – This is the leading open-source network audit tool that enables rapid scanning of systems to identify available services. An NMAP Stealth Scan was used to identify open ports and verify that only the correct services were visible to the Internet, while an NMAP OS ID scan was used to attempt to identify the operating system in use on the servers in the DMZ.

2. SYN Flood – This creates a DoS attack by taking advantage of the way connections are set up over TCP/IP and should be detected and blocked by the firewall.

3. Smurf – Takes advantage of the broadcast address on TCP/IP networks. If you send a PING to the broadcast address of a network, all the systems in it should respond. A hacker spoofs the source address of the PING to that of the system to be attacked and attempts to get large networks to send PING responses to this spoofed address.

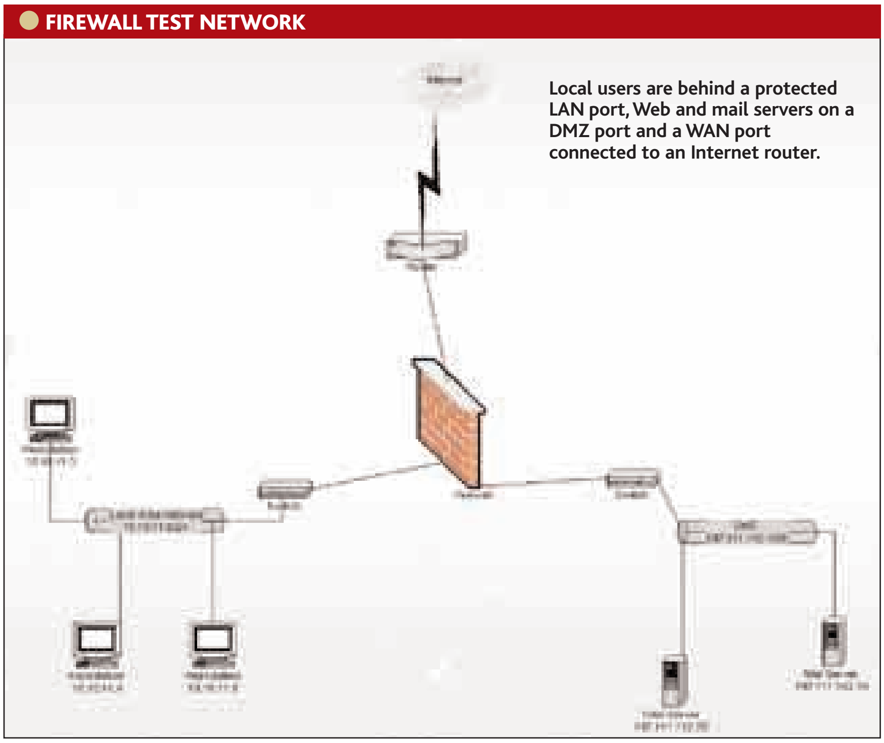
4. UDP Traceroute – As the name suggests, this traces a route from one system to another on the Internet and lists the name of each router it encounters, which could include the firewall. Traceroute packets should be dropped by the firewall so that no response is sent back to the client.

5. PING – A TCP/IP diagnostic tool that tries to get a response from the target address specified. Information returned such as the TTL (time to live) value is different for each operating system – a TTL value of 128 shows the target is probably a Windows system.

The results in the attack table show the type of test conducted and the firewall's response. Black indicates the worst response – that with the basic settings the attack succeeded and wasn't logged. Green indicates the opposite, with the attack both repulsed and logged. See the key for the steps in between. For example, the Lucent Brick 80 failed to stop the NMAP Stealth Scan, but did actually provide logging information about the attack.

Contact: I-SEC 01273 704477

FIREWALL TEST NETWORK



Local users are behind a protected LAN port, Web and mail servers on a DMZ port and a WAN port connected to an Internet router.

3Com SuperStack 3 Firewall

PRICE £2,320 (exc VAT) SUPPLIER 3Com 01442 438000
INTERNET www.3com.co.uk BASIC WARRANTY Lifetime

VERDICT **As easy to install and configure as the SonicWALL PRO 300, with good performance and plenty of optional extras, although logging detail is minimal.**

The SuperStack 3 Firewall is at the top of 3Com's modest firewall product range and bears more than a passing resemblance to SonicWALL's PRO 300. You get the same 233MHz RISC processor accompanied by 16Mb of memory and identical LAN, WAN and DMZ ports. However, each port on the SuperStack has an MDI/MDI-X switch for connection using straight- through or crossover cables, and an extra socket at the rear accepts 3Com's redundant power supply for improved fault tolerance.

Installation follows the SonicWALL path – a Wizard asks some simple questions and then sets up basic protection. The same tidy Web browser interface is provided, making general configuration reasonably straightforward. The home page of the device is well designed, with a full status report of all available features, so you can see at a glance whether these are activated. Filters are used to control access to the Internet from the LAN and ActiveX controls; Java applets and cookies can be either allowed or denied. 3Com offers the same optional Web Site Filter as SonicWALL, but you'll need to look elsewhere for virus protection.

3Com also provides its Transcend Network Monitor utility, which builds a map of SNMP-compliant devices for quick access, although there's little firewall-related information this can provide. Overall performance in the tests was particularly good – the SuperStack successfully blocked all attacks except the Stealth Scan. The levels of logging details were more limited than other offerings, although basic reports can be generated, showing the top 25 Web sites or bandwidth usage by IP address or service.

For remote VPN connections, 3Com bundles IRE's SafeNet/Soft-PK VPN Windows client software and the price includes a 50-user licence. Installation is a complex affair as, although creating a secure tunnel between two firewalls is straightforward, setting up remote clients is overly complex.

The differences in memory between the PRO 300 and the SuperStack mean the former will perform better under heavy load, but it's unlikely most SMEs will generate sufficient stress levels. The other significant feature of the SuperStack is that 3Com offers a lifetime warranty, making it a good long-term investment.

PC PRO RATINGS

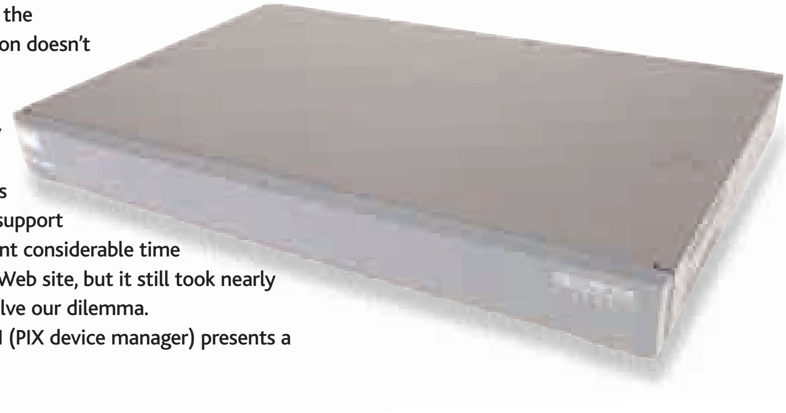
PERFORMANCE	★★★★☆☆
FEATURES	★★★★☆☆
VALUE FOR MONEY	★★★★★☆
OVERALL	★★★★☆☆

Cisco PIX 515E

PRICE £2,330 (exc VAT) SUPPLIER Cisco Systems 020 8824 1000
INTERNET www.cisco.com BASIC WARRANTY One year

VERDICT **Good value with a fine specification for the price. Cisco's new PDM is well designed, but even basic configuration is unnecessarily complex.**

Cisco's new PIX 515E proved to be one of the most awkward to set up for Web browser access. It can be configured using the CLI (command-line interface) over a serial port connection, but this is so complex Cisco can't seriously expect the average small business to use it. The 515E only supports secure browser access and needs encryption enabled, which wasn't the case with the review system. An activation key is supplied, but the documentation doesn't provide any insight into how to apply this. We discussed this with Cisco's support staff and spent considerable time browsing its Web site, but it still took nearly a day to resolve our dilemma.



The PDM (PIX device manager) presents a Wizard for setting up basic options such as secure access to internal Web and mail servers and NAT configuration. The main interface presents a tidy row of five tabbed folders for easy access to each main function. Access rules need to be defined to permit or deny specific protocols and services between the internal and external interfaces.

The 515E supports both NAT and PAT (port address translation), so rules also need to be created here as well, while hosts and networks need to be declared and have routing and NAT parameters applied. The PDM interface is well designed with plenty of online help to hand, but the procedures required for declaring our simple test network were overly complex.

Results from the penetration tests showed that the 515E configured with basic parameters provides insufficient protection. The firewall didn't log the Stealth Scan and it was the only unit that allowed a Smurf attack. However, we're under no illusions that the 515E is clearly capable of dealing with all these types of attacks, but the convoluted configuration process will be beyond the capabilities of most small businesses unless they have access to a CCE (Cisco-certified engineer).

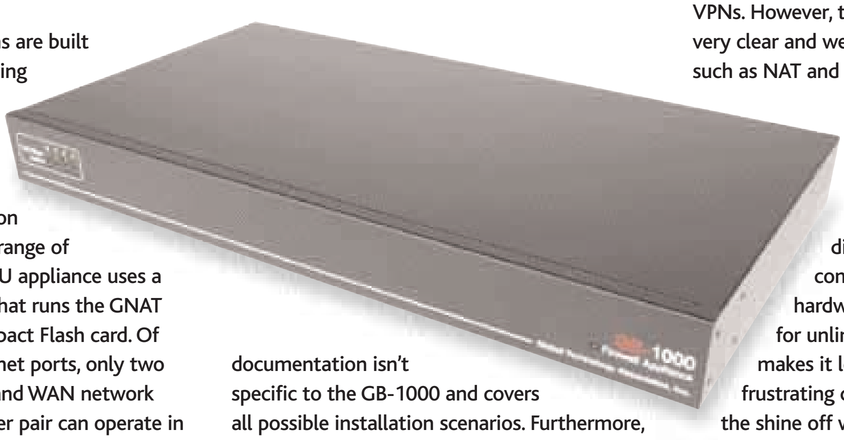
Overall build quality is particularly good, although the basic 515E only offers LAN and WAN Ethernet ports. However, the controller board does have two spare PCI slots, which can accept either two single-port or one four-port dual-speed Ethernet adaptors.

PC PRO RATINGS

PERFORMANCE	★★☆☆☆☆
FEATURES	★★★★☆☆
VALUE FOR MONEY	★★★☆☆☆
OVERALL	★★★☆☆☆

GTA GB-1000

PRICE £2,295 (exc VAT) SUPPLIER GTA 0870 458 1113
INTERNET www.gta.com BASIC WARRANTY One year
VERDICT **Good performance under attack, but the confusing documentation and awkward configuration routines mark this firewall down.**



GTA's firewall solutions are built around its space-saving GNAT Box software – the Pro version, which can be purchased separately, still fits on a floppy disk. Running version 3.2, the GB-1000 offers a range of useful features, and this 1U appliance uses a custom controller board that runs the GNAT Box software from a Compact Flash card. Of the four dual-speed Ethernet ports, only two are required for the LAN and WAN network connection, while the other pair can operate in either protected, external or PSN (private services network) mode. An extra PCI slot provides a range of upgrade possibilities, and GTA offers Gigabit, Token Ring and fibre network cards.

The installation routine proved to be more difficult than expected and wasn't helped by the fact that the GNAT Box software documentation isn't specific to the GB-1000 and covers all possible installation scenarios. Furthermore, although the GB-1000 supports secure Web browser access, we were unable to connect to the firewall using either IE5 or IE6. We sent a log file to GTA for its attention and the only solution it could offer was to switch off remote access encryption via the GBAdmin utility so we could access the firewall over an unsecured Web browser link.

The GBAdmin utility provides a simple interface with a colour-coded system for each category, so you can easily locate any problems at a glance. Filters allow or deny access to internal and external traffic, and can be linked to time groups so that they can be activated during specific periods each day. The manual provides a few basic examples of filters along with some samples to help set up VPNs. However, the documentation wasn't very clear and we found it confusing on areas such as NAT and DMZ setup.

The GB-1000 delivered a reasonable performance, handling all the tests relatively well, although logging information can be difficult to interpret. The combination of a powerful hardware specification and support for unlimited users as standard makes it look good value, but the frustrating configuration routines took the shine off what could have been an impressive firewall.

PC PRO RATINGS

PERFORMANCE	★★☆☆☆☆
FEATURES	★★★☆☆☆
VALUE FOR MONEY	★★★☆☆☆
OVERALL	★★★☆☆☆

Intrusion PDS 2105

PRICE £2,770 (exc VAT) SUPPLIER Intrusion 01252 812030
INTERNET www.intrusion.com BASIC WARRANTY One year
VERDICT **A desktop firewall that's easy to set up and configure, but the modest feature set doesn't justify the comparatively high price.**

The PDS Series of firewalls is designed specifically to be powered by Check Point's Firewall-1 SmallOffice NG software, and the PDS 2105 can also be upgraded with Check Point's VPN-1 software, although this wasn't provided with the review sample.

Aimed at small, remote and branch offices with up to 50 staff, this compact firewall is designed to be simple to install and use, and a brief glance at Check Point's well-designed Web browser interface shows that it has largely achieved its goal. However, it's worth noting that the Firewall-1 software gives absolutely no indication of which firewall appliance it's actually running on, which could be problematic if the appliance is being remotely managed.

All Web access is over an encrypted link, and Check Point provides a step-by-step guide to help get the firewall up and running. Four simple security modes are available – wide open, all incoming traffic blocked, locked down tight or a custom mode, which allows you to choose which inbound and outbound traffic is allowed to pass through. Outbound services such as HTTP, FTP and SMTP are blocked by default, but these can be opened to the internal network as required, while five rules can be used to specify protocol as well as port numbers and which interfaces they're allowed through.

Anti-virus measures and URL filtering are supported, but only if another local server or an ISP provides these services. The status of the firewall and all three network interfaces can be checked from a single screen, and the PDS 2105 provides a logging facility that displays the last 50 entries but can't save this information to a file for future use.

The PDS 2105 performed well enough in the penetration tests, apart from the Stealth Scan, where we were able to see additional ports other than those expected. The supplied documentation was dated and the correct manuals weren't available on the Web site, making it difficult to configure the firewall as required. With the correct information to hand, we believe that the firewall could have been configured correctly and would have performed better than most others.

PC PRO RATINGS

PERFORMANCE	★★★☆☆☆
FEATURES	★★★☆☆☆
VALUE FOR MONEY	★★☆☆☆☆
OVERALL	★★★☆☆☆

Lucent VPN Firewall Brick 80

PRICE £2,663 (exc VAT) | SUPPLIER Lucent 020 7004 0000

INTERNET www.lucent.com | BASIC WARRANTY One year

VERDICT **A wealth of security features, but the additional management software puts the price beyond the budget of the average small business.**

Brick by name, brick by nature, Lucent's Brick 80 firewall certainly looks solid enough to survive most office environments. However, it's not such a cost-effective choice for small offices, as it's aimed primarily at companies looking to deploy firewalls across remote and branch offices but still be able to manage them all from a central location.

To this end, you'll need to purchase LSMS (Lucent security management software) to configure and manage the firewall, which, at £3,666 for a five-unit management licence, puts it beyond the reach of the average small business. This also only includes a five-user licence for Lucent's IPSec VPN client software.

The Brick 80 performed well in the penetration tests, only missing the SYN Flood attack, indicating this is yet another firewall that needs to have defences against DoS attacks as a default setting, such as those included in the PRO 300 and SuperStack 3.

Initial installation is unusual, as along with a monitor port the Brick 80 comes with a floppy disk port designed to allow an initial configuration to be entered simply by booting the firewall from a floppy disk prepared at the LSMS console. Once this has been carried out, the firewall can be remotely managed, although it was annoying to find that we needed to connect a keyboard and monitor to the firewall as the boot sequence required user input.

Zone rule sets are used to determine how the Brick 80 functions as a firewall, and these settings can be saved and applied to multiple Brick devices. Different rule sets can be implemented on each port on the firewall and, although the documentation makes a valiant effort in explaining how to create them, we found these to be overly complex.

The LSMS Navigator provides an Explorer-style interface, offering easy access to all Bricks, policies and VPNs, plus quick access to a Brick monitoring utility, which keeps you in touch with utilisation, sessions and general traffic. Lucent also bundles a wealth of tools and utilities, including a log viewer, plus monitors and configuration assistants for LSMS itself.

PC PRO RATINGS

PERFORMANCE	★★★☆☆☆
FEATURES	★★★★★☆
VALUE FOR MONEY	★★☆☆☆☆
OVERALL	★★★☆☆☆

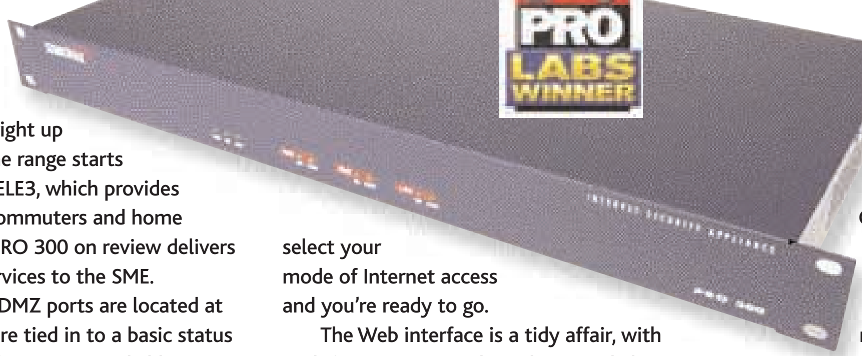
SonicWALL PRO 300

PRICE £3,400 (exc VAT) | SUPPLIER SonicWALL 01344 668090

INTERNET www.sonicwall.com | BASIC WARRANTY One year

VERDICT **Simple Web browser management, remarkably easy configuration and top performance in the penetration tests outweigh the higher than average cost.**

PC PRO LABS WINNER



Formed in 1991, US-based SonicWALL has always concentrated solely on Internet security solutions and offers a wide choice of products aimed at the smallest office right up to the enterprise. The range starts with the compact TELE3, which provides protection for telecommuters and home workers, while the PRO 300 on review delivers firewall and VPN services to the SME.

LAN, WAN and DMZ ports are located at the rear and these are tied in to a basic status display panel. Installation is remarkably simple – you just connect the LAN port to the network and point a Web browser at its default IP address. On first contact, the PRO 300 automatically loads a Wizard to help with initial configuration – provide IP addresses for the unit, the WAN gateway and DNS servers, select your mode of Internet access and you're ready to go.

The Web interface is a tidy affair, with each function grouped neatly in a side bar for easy selection. Online help is provided and the accompanying manual covers all areas of configuration in detail. Basic protection is implemented after initial configuration and can be customised by adding new services and rules, but you need to know your port numbers and protocols to use this. Overall, we found the PRO 300 a pleasure to use, as it was the easiest to configure by a wide margin.

It also delivered the best overall performance in the penetration tests. The detail provided by its logging facilities was extensive, and it was the only product that not only blocked the NMAP OS identification scan but also correctly identified it; the other firewalls merely logged the fact that packets were being blocked.

The firewall comes with a 100 VPN client licence, but while the manual makes a valiant effort, we found these difficult to set up. Access to specific Web sites can be denied by URL, and optional Web content filtering is based on the CyberNOT database. The content filter can be left active at all times or you can select specific time periods when you want to restrict access.

PC PRO RATINGS

PERFORMANCE	★★★★★☆
FEATURES	★★★★★☆
VALUE FOR MONEY	★★★★☆☆
OVERALL	★★★★★☆

Symantec Firewall/VPN 200R

PRICE £850 (exc VAT)	SUPPLIER Symantec 0800 389 7030
INTERNET www.symantec.com	BASIC WARRANTY One year

VERDICT **Worthy of consideration by small offices with cable or DSL modem links, but the comparatively low price still doesn't justify the limited feature set.**

Symantec's Firewall/VPN range consists of three products offering budget-priced intrusion protection for small office networks of up to 30 users. The 200R on review combines a pair of WAN ports with an eight-port, dual-speed switch. Aimed at DSL or cable modem connections, both WAN ports can be simultaneously active across two ISPs, where they'll perform load balancing and fail-over should one link die.

A serial port at the rear provides even more fault tolerance by using a PSTN or ISDN modem for a dial-up Internet connection, which is activated if the main WAN links become unavailable. A virtual DMZ port can be created, but the firewall only allows one IP address to be associated with this.

Access via a Web browser is the only method of configuration, but you'll find the interface is well designed and easy to use. Traffic filtering options are more limited, but the target market will find plenty to play with here. Different sets of filters can be applied to specific systems on the LAN by placing them in one of five groups, although their MAC and IP addresses must be entered manually. Basic packet filters can be created quickly and simply by selecting services such as FTP and HTTP from the list provided, and custom filters can also be applied, but it was disappointing to find no help provided on the subjects of protocols and associated port numbers.

You can run services such as Web, FTP or mail from behind the firewall by creating virtual servers. Any external traffic bound for these services is automatically routed through to the designated IP address of the server. There was nothing unusual to report back in the performance tests, although logging could have been more detailed.

Secure tunnels to Symantec's Enterprise VPN Server are supported, and the 200R adds VPN support for remote clients with Symantec's Enterprise VPN Client 7 software. Configuration at both client and firewall is lengthy, but not as complicated as the 3Com or SonicWALL routines. Fortunately, plenty of supporting documentation is provided, making the task of creating secure tunnels to the firewall that much easier.

PC PRO RATINGS

PERFORMANCE	★★★★☆☆
FEATURES	★★☆☆☆☆
VALUE FOR MONEY	★★★★☆☆
OVERALL	★★★☆☆☆

WatchGuard Firebox 1000

PRICE £3,326 (exc VAT)	SUPPLIER WatchGuard 01737 735491
INTERNET www.watchguard.com	BASIC WARRANTY One year

VERDICT **A wide range of features for the price, backed up by good performance and comparatively straightforward installation.**

Aimed squarely at mid-sized businesses and branch offices, the Firebox 1000 offers a complete firewall and VPN solution and backs this up with a range of optional features such as anti-virus protection and anti-spam filtering. This distinctive red box provides a comprehensive display on the raised front panel, with LED bars for general activity and system load along with a unique triangular display showing allowed traffic passing between the firewall's three network ports.

Initial installation requires a serial or network port connection to a designated management station. This is a simple affair: a Wizard notes down your chosen IP addresses, plus details of any SMTP mail servers on the trusted or optional ports, after which it asks you to switch the firewall on and then downloads this information into its internal flash disk. The LiveSecurity service could prove useful, because it provides regular software updates, plus warnings and advice on new security threats and virus alerts.

Overall performance was impressive, since this was the only firewall that fully blocked the Stealth Scan, which is simply because its default settings are set to block all suspicious traffic. However, it is possible that this capability could be used against it to create a DoS attack.

Further configuration is carried out from the Watchguard Control Centre. This mirrors the firewall's display panel and provides status details on each network port and VPN. A Policy Manager utility looks after your security settings and allows you to create services and store them in multiple configuration files, so you can download different policies to the firewall. Each policy contains a number of services that can contain proxies, packet filters and custom filters which determine how the firewall deals with inbound and outbound traffic.

Web site filtering tools are provided by WebBlocker. This works alongside the Proxied-HTTP service and allows you to block access to sites that contain dubious material. It relies on a database maintained by SurfControl, which can be downloaded at regular intervals. Content filtering can also be applied to email via the SMTP Proxy. This can block or allow access dependent on header, attachment type and address categories.

PC PRO RATINGS

PERFORMANCE	★★★★☆☆
FEATURES	★★★★★☆
VALUE FOR MONEY	★★★☆☆☆
OVERALL	★★★★☆☆