



Devices deliver security to the edge

Smaller firms that need to securely connect remote workers to a centralised LAN have a wide range of VPN appliances to choose from. Alan Stevens puts six models to the test

> NETWORK SECURITY

Virtual private network (VPN) appliances provide branch offices, teleworkers and roaming users with secure access to resources located on the company LAN via the internet.

These devices are available at a variety of price points, and are no longer designed only with large corporates in mind. Small businesses and branch offices catering for tens or hundreds of users can purchase the necessary VPN server technology, typically built into a router and combined with a firewall and other security options. Moreover the technology involved – whereby data is encrypted and directed over the internet in secure VPN “tunnels” – is both mature and proven to provide high levels of security.

Point-to-point VPNs connecting two sites are easy to deploy. All that is required is a VPN appliance at each end, which once configured need very little day-to-day management. Providing the same make and, preferably, the same model of hardware is used, few problems are likely to arise.

Some VPNs can be fiendishly difficult to set up and manage, however, particularly where individual remote and roaming users are concerned. These still need VPN client software, but there is a wide choice of protocol standards and vendor implementations; not all of them can be made to work together.

The client included in Windows 2000 and XP, for example, can be used with VPN networks based on the Point-to-Point Tunnelling Protocol (PPTP) and Layer 2 Tunnelling Protocol (L2TP). Unfortunately, support for these protocols is waning. Most vendors now prefer to use IPSec which, combined with the Advanced Encryption Standard (AES) method of scrambling data, is reckoned to be about as secure as it is possible to get.

The trouble is that IPSec is far from



The OfficeConnect appliance from 3Com has a very compact design

easy to configure. There can be subtle differences when it comes to encryption standards and user authentication, requiring lots of experimentation and tinkering unless custom client software is provided. The more users there are on the network, the more work is involved, and setting up and managing even a small VPN can be very time consuming.

With so many potential pitfalls, it is important to buy the right hardware for the job. This group test concentrates not just on the functionality and performance of the appliances tested, but also on how easy they are to configure, the availability or other use of suitable client software, and the quality of documentation and assistance provided. We also examined user authentication policies and other security options provided to help network managers decide which, if any, of the VPN appliances featured here might be suitable for their organisation's remote networking needs.

3COM OFFICECONNECT

On paper the 3Com OfficeConnect VPN Firewall ought to be a very capable small business appliance, but appearances can be deceptive. In reality, this appliance falls some way short of the standard set by the other products reviewed in this test.

The hardware itself is very compact, with four 10/100Mbit/s LAN ports and a separate connector for WAN connectivity. There is no hardware demilitarised zone (DMZ) port, though, just

FINDINGS

3Com OfficeConnect VPN Firewall

Priced to appeal to the SME market, the OfficeConnect appliance is out-classed by others in this group test.

- ✓ Integrated encryption accelerator; AES encryption; support for PPTP, L2TP and IPSec
- ✗ No DMZ port, no VPN client software and little supporting help or documentation; no external user authentication; limited additional security options

Price £170 + VAT

Contact 3Com 01422 438000

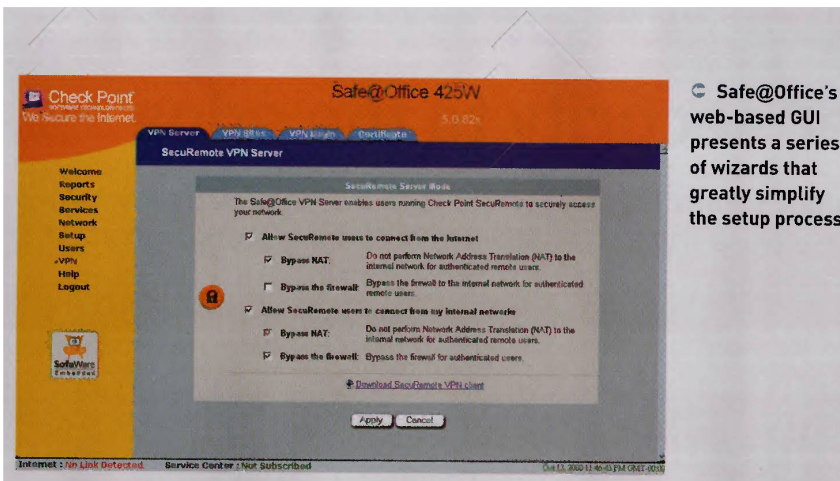
➔ www.tinyurl.com/8c622

NETWORK IT WEEK LABS

a basic virtual server option implemented through the firewall.

In its favour, a hardware accelerator is built in to offload encryption processing and enable the OfficeConnect to handle up to 50 encrypted VPN tunnels. Plus there is a choice of data encryption standard (DES), 3DES or advanced encryption standard (AES) encryption algorithms and support for PPTP, L2TP and IPSec tunnelling protocols.

There is also a reasonable web-based GUI, with a wizard to ease the initial setup phase. Unfortunately that doesn't include VPN configuration, and the documentation does not add much value either. Neither is there any VPN client software or, really, any help at all when it comes to



Safe@Office's web-based GUI presents a series of wizards that greatly simplify the setup process

Network managers can even opt for a managed installation and have a specialist reseller install and maintain the Safe@Office appliance for them.

D-LINK DFL-700

Though it is touted primarily as a small business firewall device, the D-Link DFL-700 can also be used to support VPN tunnelling to create both secure distributed networks, and to support teleworkers and mobile users.

The appliance is easy to deploy, at least in terms of the initial setup. There are just three 10/100Mbit/s Ethernet connectors at the back, one for LAN attachment, another for the WAN link, and a DMZ port for public-facing web and email servers. SNMP management is an option too but, as per usual, a web-based GUI is presented as the starting point.

A wizard is on hand to guide new users through the first few steps required, after which a fairly basic but effective interface takes over. Moreover, VPN connectivity is very well catered for, with facilities to configure site-to-site and remote user tunnels using PPTP, L2TP and IPSec tunnelling. Likewise there is a choice of encryption protocols, shared key and PKI support, plus user authentication against either an internal database or an external Radius server.

Unfortunately there is not a great deal of help on hand when it comes to explaining what can be a very complex setup procedure. The accompanying documentation includes examples, and there are a couple of configuration guides on the D-Link web site. However, the emphasis is on site-to-site tunnelling with very little about what is required at the remote end when connecting individual users. The lack of any client software is another big concern and it took several attempts to get the IPSec facilities to work.

Beyond the VPN capabilities there is a stateful inspection firewall plus tools to filter traffic.

FORTINET FORTIGATE-60

The FortiGate 60 is an impressive integrated security appliance. In addition to the firewall and VPN server, it scans

FINDINGS

Check Point Safe@Office

Accomplished Check Point technology and ease of installation make this a capable security appliance well worth investigating.

- ✓ Fast setup and bundled VPN client; excellent supporting documentation; local VPN option particularly useful for wireless security
- ✗ Relatively expensive; no support for PPTP or L2TP tunnelling

Price £811 + VAT for model 425W

Contact Check Point 01223 713600

www.checkpoint.com

NETWORKITWEEK LABS

software it runs comes from Check Point, the market leader in enterprise firewall and VPN technology.

Physically the device appears much like the others reviewed here with four 10/100Mbit/s LAN ports plus separate WAN and a dedicated DMZ interface. The 425W also features an integrated 802.11g wireless access point, as well as two USB ports to facilitate printer sharing.

Support for the secure socket shell (SSH) remote access protocol and simple network management protocol (SNMP) is available, though most users will start with the easy-to-use web-based setup interface. This is simple to follow with lots of wizard help and good supporting documentation.

The VPN facilities were particularly easy to employ, with a custom client (VPN-1 SecuRemote) to make life easy for teleworkers and roaming users. Site-to-site tunnels can also be established and it is possible to configure internal VPN tunnels to fully secure wireless user connections.

The lack of support for anything other than IPSec with 3DES/AES encryption could be seen as a drawback, but this security combination is as good as it gets.

We had no problems using the Check Point device, which was one of the easiest of those reviewed to get up and running. Of course, we were mainly interested in the VPN facilities but that is not all the product has to offer.

There is also Check Point's excellent stateful inspection firewall, and administrators can subscribe to additional services that provide email, anti-virus, anti-spam and content filtering.

setting things up at the remote end to establish a VPN connection.

A lack of support for anything other than shared keys is another drawback. Nor is there any external authentication option and, apart from an optional subscription-based content filtering service, no other security options.

The OfficeConnect VPN Firewall's remote access facilities are clearly aimed at the SME market, but most businesses in this bracket will find it difficult to get to grips with. The device could alternatively be used by larger organisations for branch office and teleworker support where the lack of client software and documentation will not be such an issue.

CHECK POINT SAFE@OFFICE

The little orange Safe@Office 425W box doesn't look like much, but don't be fooled. The VPN-1 Embedded NG



D-Link's DFL-700 features just three 10/100Mbit/s Ethernet connectors

for viruses, blocks spam, filters content and identifies possible network intrusions. Automatic updates are another useful feature along with extensive documentation and support.

The hardware itself is very compact, although there is still room for a four-port 10/100Mbit/s switch for LAN connectivity plus two WAN connectors (for load-balancing and failover) and a separate DMZ port.

A comprehensive web-based GUI is provided for management, with an optional command line interface and SNMP support if required.

We were particularly impressed by the VPN facilities. Site-to-site and client tunnels can both be defined with support, too, for so-called hub-and-spoke deployment where tunnels between remote sites can be managed via a central unit. IPSec is the preferred tunneling protocol, although PPTP and L2TP tunnels can also be configured and there is support for DES, 3DES and AES encryption, pre-shared keys and digital certificates. User authentication using external LDAP or Radius servers is also supported.

If we had any complaints it was the sheer number of options and customisation facilities available, which can make VPN setup very daunting. However, the comprehensive documentation provided helps enormously, particularly the 168-page FortiGate VPN Guide that includes detailed examples of different deployment scenarios. Optional FortiClient software (around £14 per user) is also available to simplify the setup of remote IPSec clients complete with anti-virus and personal firewall facilities.

The firewall and other security options are equally programmable, and again there is lots of documentation to help with setup. Plus, it is possible to buy the FortiGate as part of a managed service and have all the hard work done by experts.

NETGEAR PROSAFE FVS328

The FVS328, which can support 50 VPN tunnels, is an affordable small business security appliance with a built-in stateful inspection firewall

FINDINGS

D-Link DFL-700

D-Link's Network Security Firewall DFL-700 is an easy-to-deploy and affordable solution that is let down by a lack of VPN client software, poor documentation and limited additional security options.

- ✓ Dedicated DMZ port; external Radius authentication
- ✗ Single LAN port; no client VPN software; flimsy documentation

Price £210 + VAT

Contact D-Link 01753 555000

www.dlink.co.uk

NETWORK IT WEEK LABS

and URL filtering facilities as well as VPN support. That said, it does lack some of the more advanced options found on other products.

The Netgear hardware itself is very robust and features eight 10/100Mbit/s ports for LAN connections and a serial connector for dial up backup. But there is only one Ethernet WAN connector and no DMZ port.

The story is much the same on the software front. The familiar Netgear browser GUI makes the unit relatively easy to configure, while a wizard is included specifically to help with VPN deployment in the latest firmware. This can configure site-to-site and site-to-client tunnels, and is supported by useful documentation. Although not shipped with the unit, this can also be downloaded from the Netgear web site.

However, there is no support at all for the latest AES encryption standard

FINDINGS

Fortinet FortiGate-60

Fortinet's FortiGate-60 is a comprehensive VPN appliance that can be configured with a range of add-on services to build a complete business security solution.

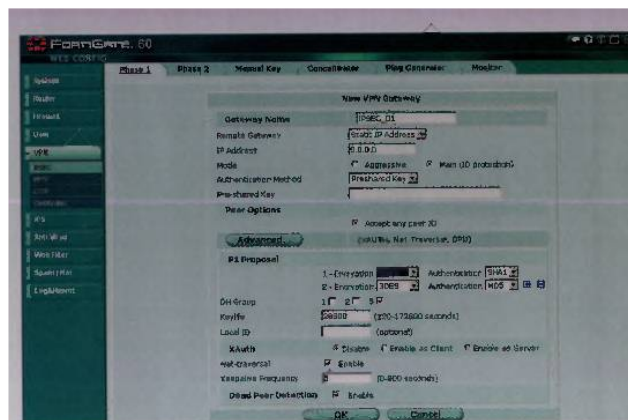
- ✓ Excellent management interface with comprehensive supporting documentation; optional VPN client software; anti-virus, anti-spam, content filtering and intrusion detection options
- ✗ Range of VPN options can make initial setup a little daunting

Price £620 + VAT

Contact Fortinet 08707 353666

www.fortinet.com

NETWORK IT WEEK LABS



As well as a VPN firewall, the Fortinet-60 also boasts anti-virus, anti-spam and content-filtering capabilities



Netgear's FVS328 is an affordable security appliance with an integrated eight-port switch, but software is limited

FINDINGS

Netgear ProSafe FVS328

Netgear's ProSafe VPN Firewall gets the VPN job done at a great price, but it lacks sophistication and some of the extras that are available on competitive products.

- ✓ Optional VPN client software; integrated eight-port switch
- ✗ No DMZ port; no user authentication facilities; PPTP/L2TP support limited to forwarding

Price £104 + VAT

Contact Netgear 01344 397021

www.netgear.co.uk

NETWORK IT WEEK LABS

170/25 model we looked at had just five fixed 10/100Mbit/s Ethernet ports plus a separate Ethernet interface to connect these to the WAN. There is also a DMZ port although, usefully, this can also double up as another LAN connector or as a second WAN port for extra bandwidth and redundancy. Additionally, it can be used to provide wireless connectivity.

Installation is very straightforward. The web-based management interface is a delight, with simple navigation and numerous wizards to help with setup. We were particularly impressed by the VPN wizard, which can be used to configure both site-to-site and site-to-client tunnels, backed up by good on-screen help and supporting documentation.

IPSec is the preferred protocol here, although L2TP is also available, plus there's a choice of DES - 3DES or AES encryption - and both shared secret and public key infrastructure (PKI) keys. Additionally it is possible to enforce IPSec as well as Wi-Fi protected access (WPA) encryption on wireless connections and authenticate remote users, either against an internally maintained user store or external LDAP/Radius servers.

(just DES and 68-bit 3DES) and no user authentication options, either local or via an external Radius/LDAP server. On top of that, and despite references to PPTP/L2TP support in the documentation, the Netgear ProSafe can only forward these tunnels onto other servers, not terminate them itself.

Lastly, Netgear now offers its own ProSafe VPN client software. Based on the popular SafeNet technology, this costs £35 + VAT per user and can also be used with IPSec servers from other vendors. It is not strictly necessary, as the Windows XP VPN client can be used, but it does make life simpler in practice and can be used with other versions of Windows as well.

SONICWALL TZ 170

The TZ 170 is a very capable and well specified branch office solution. Several models of the extended family of SonicWall security appliances are available with a choice of 10, 25 or unlimited supported LAN users.

There is also a wireless implementation available, although the TZ

At the client end the L2TP support makes it possible to connect remote Windows systems directly without any special software. A copy of SonicWall's own Global VPN Client software is also included though, which can be used on a variety of operating systems and greatly simplifies deployment.

A firewall, of course, is included as standard, and it is possible to add optional antivirus, anti-spyware and intrusion-protection services. SNMP management is another option, along with integration into the SonicWall Global management System (SMS) on larger distributed networks.

FINDINGS

SonicWall TZ 170

A well-specified and implemented security appliance with easy-to-deploy VPN tunnelling capabilities tailored to the needs of the small to medium business.

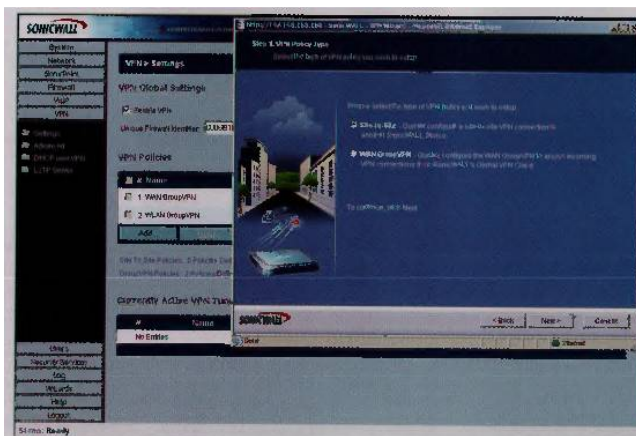
- ✓ DMZ port; flexible "optional" port for LAN, WAN or wireless connectivity; VPN client software included; simple wizard setup of VPN tunnels; optional add-on antivirus, anti-spyware and IDS services
- ✗ No PPTP support

Price £340 + VAT for the TZ170/25

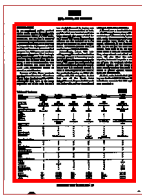
Contact SonicWall 01628 640140

www.sonicwall.com

NETWORK IT WEEK LABS



SonicWall's TZ 170 had the most intuitive web-based management console of all the devices we tested



EDITOR'S CHOICE

As we mentioned earlier, product choice can be a major determinant in the success or failure of a VPN implementation, and not just in terms of functionality or performance. Indeed, while some vendors go out of their way to help with the deployment of their products, others seem to assume that everyone is a VPN guru and needs no assistance whatsoever. That is simply not the case and even for those administrators that do know what they are doing, a lack of documentation, VPN client software, and other tools to assist with installation should be viewed as a deal breaker.

Because of this, three products stood out from the crowd – those from Check Point, Fortinet and SonicWall. Admittedly they were at the more expensive end of the scale but each

was straightforward to deploy and came with documentation to both explain what was involved and take users through the steps needed for each type of VPN setup. Custom client software was also included or, in the case of the FortiGate-60, could be purchased, as was also possible with the much cheaper Netgear solution.

Interestingly, actual VPN tunnelling, encryption and authentication protocol support is becoming much less of an issue. Most customers simply want a VPN server that works and that provides a high level of security regardless of how it is achieved; as such it came as little surprise to find most of the products focusing on IPSec tunnelling with AES encryption. In fact that was all the Check Point Safe@Office and Netgear ProSafe products had to offer, and was the preferred

setting on most of the others too.

A firewall was a standard feature on all of the appliances, along with a smattering of other security options with, again, the more expensive products scoring most highly in this regard. Ultimately, it was the SonicWall TZ 170 that got the most votes overall, with ticks in all the right boxes when it came to documentation, setup wizards and client software. We also liked the extra interface that could be put to a variety of uses, the optional wireless-enabled version and the range of extra security services that could be added to protect against viruses, spam and other nasties.

All that, and a modest £340 price tag won the SonicWall TZ 170 our Editor's Choice award for this VPN appliance groupset. ■

Table of features

NETWORK WEEK
EDITOR'S CHOICE

Vendor	3Com	Check Point	D-Link	Fortinet	Netgear	SonicWall
Product name	OfficeConnect	Safe@Office	Network Security Firewall	FortiGate	ProSafe VPN Firewall	TZ 170
Model tested	VPN Firewall 3CR870-95	425VV	DFL-700	FG-60	FVS328	TZ170/25
Price (+ VAT)	£170	£811	£210	£520	£104	£340
Phone number	01442 438000	01223 713600	01753 555000	08707 353666	01344 397021	01628 640140
URL	www.3com.co.uk	www.checkpoint.com	www.dlink.co.uk	www.fortinet.com	www.netgear.co.uk	www.sonicwall.com
Warranty (years)	3	1	2	1	3	1
Max concurrent VPN tunnels	50	25	200	40	50	50 (set by licence)
Claimed throughput using 3DES	Not specified	20Mbit/s	20Mbit/s	20Mbit/s	20Mbit/s	30Mbit/s
Physical						
LAN ports	4	4	1	4	8	5
WAN ports	1	1	1	2	1	1
DMZ ports	-	1	1	1	-	1
Other ports	-	2 USB (print server) + console port	Serial console port	2 USB + console port	Serial modem port for dial backup	console port, DMZ port can be used for LAN/WAN connectivity option
Wireless interfaces	-	802.11g	-	-	-	-
VPN tunneling						
PPTP	✓	X	✓	✓	X	X
L2TP	✓	X	✓	X	X	✓
IPSec	✓	✓	✓	✓	✓	✓
Site-to-site tunnels	✓	✓	✓	✓	✓	✓
Site-to-client client	✓	✓	✓	✓	✓	✓
Client software	X	VPN-I SecuRemote	X	optional (FortiClient)	optional (ProSafe VPN client)	Global VPN client
Encryption algorithms						
DES	✓	✓	✓	✓	✓	✓
3DES	✓	✓	✓	✓	✓	✓
AES	✓	✓	✓	✓	X	✓
Encryption keys						
Shared keys	✓	✓	✓	✓	✓	✓
PKI/digital certificates	X	✓	✓	✓	✓	✓
User authentication						
Internal database	✓	✓	✓	✓	X	✓
LDAP	X	X	X	✓	X	✓
RADIUS	X	✓	✓	✓	X	✓
Other security features						
Firewall	✓	✓	✓	✓	✓	✓
Anti-virus	X	✓	X	✓	X	option
Anti-spam	X	optional	X	✓	X	X
Anti-spyware	X	X	X	X	X	option
Intrusion detection	X	X	✓	✓	✓	option
URL/content filtering	X	✓	X	✓	X	option
Scores						
Features	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Performance	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Value for money	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
Overall	★★★★	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★