



UTM SECURITY APPLIANCE

PRICE

Inc 1yr subscriptions and support, £4,477 exc VAT

SUPPLIER

Fortinet
08707 353666

INTERNET

www.fortinet.com

WARRANTY

1yr RTB

SPECIFICATIONS

1U rack chassis • 512MB RAM • 24 x 10/100 Ethernet • 2 x Gigabit • 2 x 10/100 WAN • 2 x USB • RJ-45 serial • web management. Options: 2yr bundle subscription, £1,381 exc VAT

PERFORMANCE



FEATURES & DESIGN



VALUE FOR MONEY



OVERALL



Fortinet FortiGate-224B

A feature-packed switch and security appliance that's remarkably easy to configure yet highly versatile

Coming in at the entry point of Fortinet's higher-end UTM appliances, the FortiGate-224B aims to offer a complete network security solution augmented with more than a few unusual features. You get firewalling, antivirus, antispam, web-content filtering, traffic management and IDS/IPS, but this 1U rack-mount appliance combines them into a 24-port Layer 2 switch, allowing security policies and quarantining to be deployed right down to individual ports.

We found installation a swift affair, aided admirably by the well-designed web interface. The status page provides plenty of information on general system activity, subscription services plus alert messages, and provides a statistics table showing URLs visited and blocked, incoming and outgoing mail, spam and virus counts, and much more.

Security policies are applied at the VLAN, or zone, level and the appliance starts with all its LAN ports grouped together under one zone. By default, you get a base security policy, which uses the default zone and primary WAN port as source and destination, and blocks all unsolicited inbound traffic. We connected an intelligent ADSL



Security policies can be assigned to individual ports on the FortiGate.

broadband router to one of the pair of WAN ports, and after configuring DHCP services we were up and running.

Policies use source and destination zones, so it's possible to apply them to intrazone traffic as well as LAN and WAN traffic. You can also assign a protection profile that contains all details on measures such as antivirus, antispam and content filtering. For the latter, you can use the FortiGate filtering service, which offers eight main headings containing around 80 categories that can be individually blocked or allowed. Spam checks can be applied to IMAP, POP3 and SMTP traffic, so you don't need to add details of internal mail servers, and for SMTP you can tag or discard suspect messages.

IM apps don't get off lightly, as you can block logins or file transfers and audio. Using the MSN option, we could easily stop Windows Messenger clients

from logging in. For P2P, you have six main culprits including BitTorrent, and you can block them or apply bandwidth restrictions. Clients can be checked for local third-party AV and firewall software and permitted Windows OSes, although Symantec and McAfee aren't on the list and neither is Vista. On first contact, the switch downloads an ActiveX control that scans the system and clears it for network access if it passes. Both IPsec and SSL VPNs are on the menu and, although more

basic than point solutions, the latter does allow you to control what types of applications mobile clients can access on the LAN and scan the client for required local AV and firewall apps.

For testing, we ran the 224B in a live environment for a week and were impressed with its capabilities. The FortiGate content filtering was very accurate with few websites slipping through the net, while antispam measures were found to be 80% effective out of the box. We did have a 3% false-positive rate at first, but it was easy enough just to tag rather than discard emails, allowing us to customise the filters.

As a good-value UTM appliance, the FortiGate-224B takes some beating. It offers a wide range of features that are particularly easy to deploy and the switch adds some very interesting possibilities to security policies. **DAVE MITCHELL**