WatchGuard Firebox T50-W

binary testing | LAB REVIEWS

WatchGuard delivers enterprise-class security to SMBs and remote offices at a sensible price

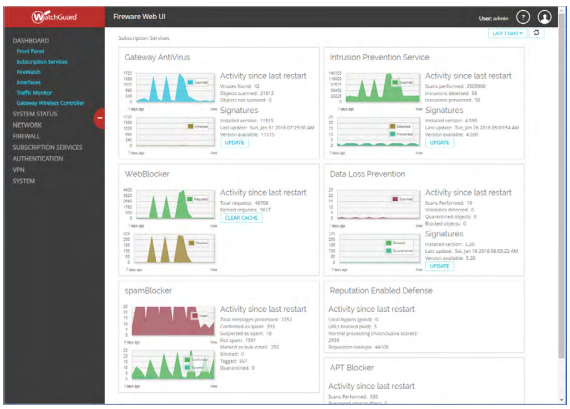
A perfect choice for SMBs, WatchGuard's Firebox T50-W offers a remarkable range of tough security measures at a very tempting price.

Deployment has been nicely streamlined, plenty of good reporting tools are provided as standard and it even includes fast 11ac wireless services.

WatchGuard's new Firebox T Series of UTM appliances

deliver enterprise performance and features at prices that will make SMBs and remote offices sit up and take notice.

There are no compromises in WatchGuard's search for value as these little desktop appliances run the same Fireware OS and security modules as its high-end appliances.



WatchGuard's security services are easily monitored from the well-designed web interface

In this review we look at the flagship Firebox T50-W which comes with seven Gigabit ports for LAN, WAN and DMZ duties. It claims industry-leading firewall and UTM throughputs of 1.2Gbits/sec and 165Mbits/sec respectively.

Its internal aerials don't give the game away, but it provides fast dual-band 802.11ac wireless services and can act as a wireless gateway for centrally managing WatchGuard's own access points. There's even a PoE port to connect one to - or you can use it to power an IP camera.

Many businesses have concerns about the hidden costs of additional services but WatchGuard's simplified subscription services should allay their fears. The appliance, NextGen firewall and 3-year support contract costs a very reasonable £1,130 ex VAT.

A standard 3-year UTM subscription increases the price to £2,240 ex VAT and enables anti-spam, gateway anti-virus, IPS, web content filtering, application controls, HTTPS inspection and WatchGuard's reputation enabled defence.

Adding WatchGuard optional data leak prevention (DLP) and advanced persistent threat (APT) blocker services pushes the total cost for 3 years to £3,148 ex VAT.

Simple deployment

Deployment in the lab was a swift process as the web console's wizard set up the first two network ports with Internet and LAN access and applied a base firewall security policy.

The appliance supports three operational modes including transparent drop-in but we find mixed routing the most flexible as it allows ports to be defined as separate interfaces, each with their own DHCP server.

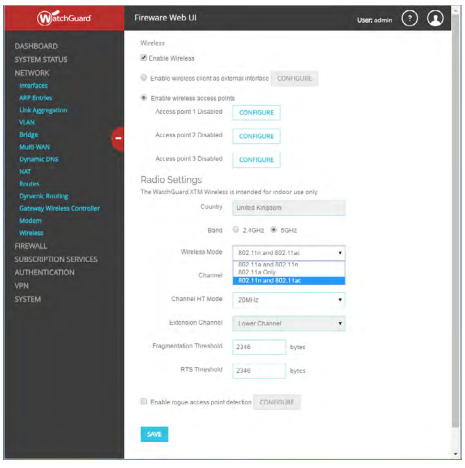
Wireless configuration is equally undemanding and very flexible. The T50-W can present wireless services as an external interface so it will be subjected to all security policies protecting the trusted LAN side.

Alternatively, you can choose from 2.4GHz or 5GHz wireless bands and create three APs each with their own SSIDs and encryption schemes. They can also be used to authenticate guest access and provide secure hotspot services.

We tested the wireless gateway feature using a WatchGuard AP200. It was automatically discovered by the T50-W and after pairing them from the web console, we pushed predefined SSIDs to the AP and used the console's heat map to view its wireless coverage.

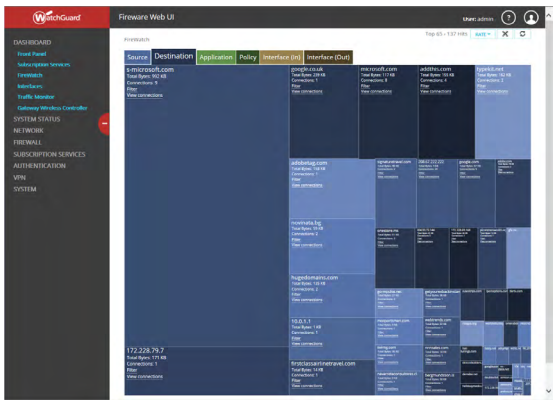
WatchGuard's RapidDeploy cloud service will appeal to businesses juggling multiple remote offices. Factory default appliances are registered with the RaidDeploy service and sent out to each office.

Once connected to the Internet, they'll download and apply a configuration file from the cloud with no user intervention required.



The 50-W includes an integral dual-band 802.11ac AP for secure wireless services and guest access

WatchGuard Firebox T50-W



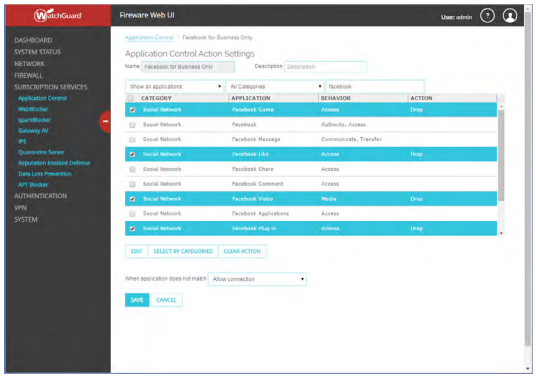
We could keep a close eye on network activity using WatchGuard's smart FireWatch feature

Proxy perfection

The T50-W controls all network traffic using proxies and WatchGuard includes ones for HTTP, HTTPS, FTP, DNS, SIP, H.323, POP3 and SMTP. Proxy configuration used to be unintuitive but WatchGuard has remedied this as the latest Fireware OS includes wizards for each one.

We enforced web content filtering in a few minutes as the wizard requested a name for the proxy blocking action, presented us with 130 Websense URL categories to choose from and asked whether to apply them to HTTP and HTTPS traffic.

On completion, the wizard created a new firewall rule for the web filter and activated it for us.



Application controls can be used to allow or deny access to specific Facebook activities

The new rules could be tweaked to suit by modifying the interface types they applied to and enabling the IPS service as required. We could include traffic management actions to guarantee or limit inbound and outbound rates.

During testing, we also found WatchGuard's web filtering to be highly effective with very few web sites slipping through its net.

Anti-spam measures were equally simple to apply as the wizard helped create actions for the spamBlocker service and set it to tag the subject line of spam, suspect and bulk messages.

It's a top performer too, as we left the POP3 proxy scanning inbound live mail for two weeks and recorded an impressive spam detection rate of 98.5 per cent.

Cloud app control

Many business have a solid case for using a wide range of cloud apps and so require a far more granular approach to controlling their usage. WatchGuard's application controls make the T50-W stand out as it is capable of managing access to over 1,800 predefined apps.

The list is fully searchable and WatchGuard includes options to manage access to social networking sites such as Twitter and Facebook. The latter has twelve entries covering most activities so you could easily allow users to access the company Facebook account but stop them from playing games, transferring files or uploading video.

Best of the rest

Gateway anti-virus measures can be enabled on any or all proxies. It's very simple to configure and global settings include the depth you want nested archives to be scanned to and how often automatic signature updates are conducted.

The APT blocker service needs gateway AV running and can be enabled on the HTTP, FTP and SMTP proxies.

There's nothing else to do as the service scans all inbound files, computes an MD5 hash for each one and compares it with the LastLine cloud service to see if it's known malware.

The DLP module is well worth considering if you want to keep sensitive information where it belongs.

Applied to the HTTP, FTP and SMTP proxies, it checks for keywords such as credit card or bank account numbers being transmitted and carries out actions such as blocking or dropping the connections.

Along with the predefined HIPAA and PCI sensors, you can easily create your own and also use them to check emails and remove keywords from messages.

Reporting

We could keep a close eye on the action in real-time as the appliance's web console offers a comprehensive dashboard. Along with bar charts showing the top users, destinations and policies, it provides activity and status graphs for each subscription service

The dashboard includes WatchGuard's slick FireWatch feature which uses coloured squares of differing sizes to represent inbound, outbound, app and policy activity.

Select the full-screen option for FireWatch and you have a ready-made security status monitor that automatically scrolls through each graph.

View From The Lab

Binary Testing has extensive experience with many UTM appliance vendors and has consistently found WatchGuard's products to be amongst the easiest to deploy and manage. The Firebox T50-W is no exception and the new features and wizards in the latest Fireware OS simplify this process even further.

It may be a small but the T50-W packs in a remarkable range of security features, including sophisticated wireless network provisioning. It offers everything an SMB could possibly want in a security appliance and all at a very affordable price.

Binary Testing Ltd

Newhaven Enterprise Centre
Denton Island
Newhaven
BN9 9BA
UK
t +44 (0)1273 615270
e info@binarytesting.com
i www.binarytesting.com