WatchGuard Firebox T30-W

binary testing | LAB REVIEWS

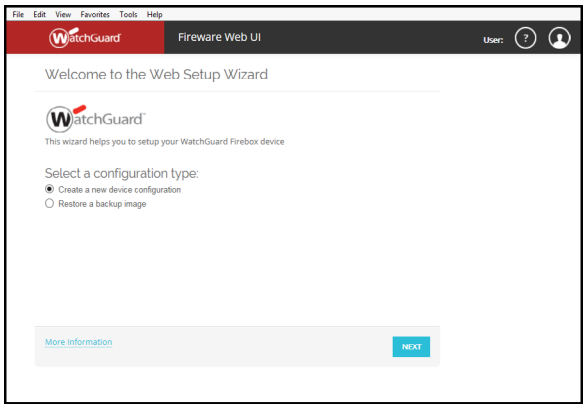
This little desktop appliance is big on security features and won't be beaten for value either

The Firebox T30-W offers a raft of enterprise level security features that SMBs will find very affordable.

Its integral 11ac wireless AP makes it even more versatile and new features include simplified installation and zero-touch deployment for remote offices.

Watchguard's new Firebox T30-W raises the bar for value

as this fire-engine red appliance delivers industrial-strength gateway security at an affordable price. Along with budget conscious SMBs, it also has a sharp focus on distributed enterprises as Watchguard's RapidDeploy service is designed to provide plug and play deployment in remote and branch offices.



Initial installation is streamlined with a wizard that helps set up protected Internet access

This little desktop appliance looks to have every security angle covered as Watchguard's UTM subscription activates a veritable wealth of features.

These include IPS, web content filtering, anti-spam, anti-virus, application controls, HTTPS inspection and Watchguard's own reputation enabled defence.

Prices look good as the appliance plus a one year UTM subscription costs £988 rising to only £1,575 for three years.

There's more as you can add WatchGuard's optional advanced persistent threat (APT) blocker service and data leak prevention (DLP) with a three year license for the full works costing only £2,229.

The T30-W has five Gigabit ports and offers high firewall and UTM throughputs of 620Mbits/sec and 135Mbits/sec respectively. We review the model with integral dual-band 802.11ac wireless services and both this and the non-wireless T30 present PoE on their fourth LAN port for connecting an access point (AP) or IP camera.

More wireless services are on the cards as both the T30 and T30-W can function as a wireless gateway controller for any of Watchguard's four current AP models. Once the appliance has discovered and paired with them, it will provision centrally managed SSIDs and protect wireless clients with all the same security measures enjoyed by LAN users.

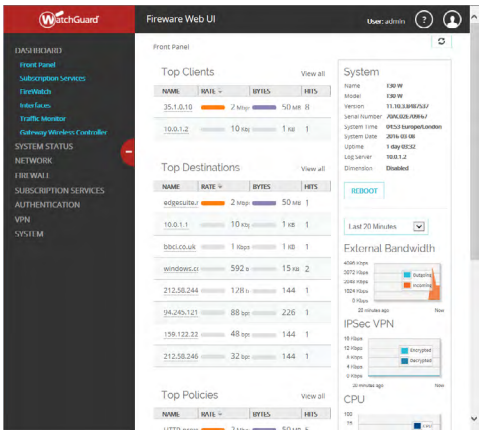
Easy installation

Small businesses with limited IT resources will find installation a very simple process. We pointed a web browser at the appliance's default management address and followed the quick-start wizard which steps through setting up the first two network ports for LAN and WAN duties and providing DHCP services on the LAN.

Protection starts immediately as the wizard applies a basic firewall policy to protect LAN users. It also configures the appliance to use the flexible mixed routing mode which defines all ports as separate interfaces allowing us to apply different security policies to network segments.

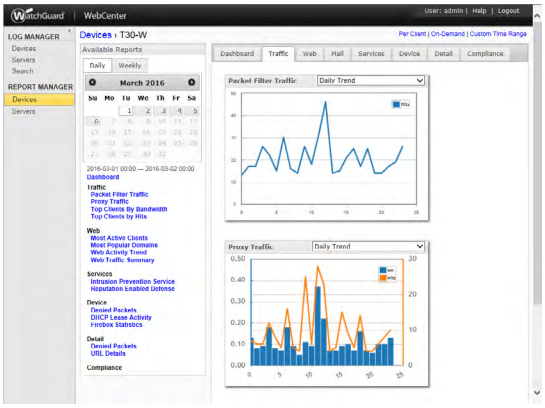
Big businesses with multiple remote or branch offices will approve of WatchGuard's RapidDeploy cloud service. They can use a local WatchGuard appliance to create a standard configuration file and upload it to their cloud account.

Prior to sending out the new appliances to each office, they are registered with the RapidDeploy service. On receipt at the remote site, the appliance is simply plugged in and connected to the Internet whereupon it downloads and applies the relevant configuration file.



The web console's dashboard provides plenty of useful information on traffic and user activity

WatchGuard Firebox T30-W

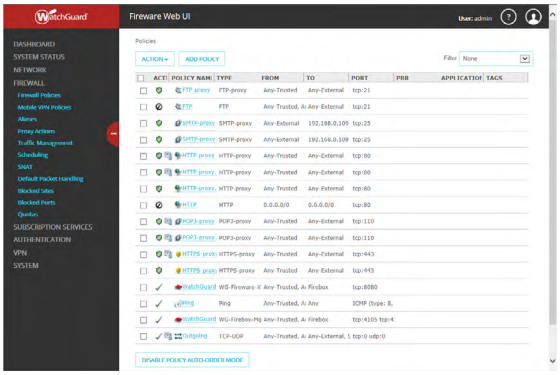


Unlike most other vendors, Watchguard provides all reporting tools as standard

Improved policy configuration

All traffic is controlled using proxies and Watchguard includes ones for HTTP, HTTPS, FTP, SIP, H.323, POP3 and SMTP. Previously, we've found these can be complex to configure and were pleased to see Watchguard's latest Fireware OS includes additional wizards for every proxy.

These streamline security policy creation with web filtering, for example, reduced to a simple three-step process. The WebBlocker service offers over 120 URL categories and the wizard asked us to name the policy action, select the categories we wanted blocked and apply it to HTTP and HTTPS traffic.



Firewall policies control all proxies and are automatically placed in the correct order

Once the proxy had been configured, the wizard created a new firewall rule for us. This was automatically applied to traffic between all trusted and external interfaces but could easily be modified to use specific interfaces on the appliance.

There's a lot more to security policies as they can enforce bandwidth controls for inbound and outbound traffic and be linked up with WatchGuard's Application Control feature. This provides a searchable list of over 1,800 apps with eleven just for Facebook, allowing you to easily block or control access to unproductive and non-business apps.

Top anti-spam performance

To test the spamBlocker service, we used the wizard to swiftly configure the appliance's POP3 proxy to tag messages classed as spam, suspect and bulk. Performance is very impressive as after running it for a month against live email, we saw a very high spam detection rate of 98.8 per cent with only a smattering of false positives.

This process transparently scans inbound email at the gateway but as it doesn't provide quarantining, we needed to create email client rules to decide how to handle tagged messages. Businesses with an internal mail server can also use spamBlocker to filter incoming messages simply by creating an SMTP proxy action and entering their server's email address.

Gateway AV scanning is enabled on a per policy basis and you'll need it running if you want to apply APT protection. As files come in to the network, it scans them, creates an MD5 hash and checks this using the LastLine cloud-based sandbox to see if they're known malware.

Businesses handling confidential information will like Watchguard's DLP module. Along with predefined policies for HIPPA and PCI, you can create your own which run in the HTTP, FTP and SMTP proxies and check for keywords such as social security and credit card numbers or bank account details.

If it spots them being transmitted, the proxy action can be set to drop or block connections. For email, you have seven possibilities including stripping matched keywords from the message body or dropping the connection.

Free reporting

Watchguard also scores over most of the competition as it includes all reporting tools for free as opposed to expensive options. The appliance's web interface provides real-time graphs of proxy activity and includes WatchGuard's FireWatch which clearly shows inbound, outbound, app and policy activity using clever graphs comprising coloured squares where their size indicates the level of activity.

Part of Watchguard's free System Manager suite, the Log and Report servers use a separate Windows host. We ran them on a basic Windows 7 desktop and were able to view graphs on web, user and proxy activity, create regular reports and email them to selected users.

And then there's Watchguard's free Dimension cloud reporting software which is deployed as a VMware VM. Dimension collects, analyses and presents security information from multiple appliances regardless of their physical location and provides a wealth of reporting tools along with the slick Security Dashboard and Threat Map.

View From The Lab

The Firebox T30-W is an impressive little UTM appliance that teams up a wealth of security features with excellent performance.

Its wireless capabilities allow the T30-W to extend its security umbrella over employees and guest users alike and the comprehensive range of free reporting tools adds even more to its value score.

We highly recommend it for SMBs that want the best security at the most affordable prices and enterprises looking for hassle-free deployment to remote and branch offices.

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