NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE = JANUARY 5, 2015

# Check Point, Watchguard earn top spots in UTM shootout

*UTM appliances for SMB security are getting smaller, more powerful and more feature rich.*

BY DAVID STROM, NETWORK WORLD

When it comes to unified threat management appliances aimed at the SMB market, vendors are finding a way to fit additional security features into smaller and more powerful appliances.

In 2013, we looked at nine UTMs. This time around we reviewed six products: the Calyptix AccessEnforcer AE800, Check Point Software's 620, Dell/Sonicwall's NSA 220 Wireless-N, Fortinet's FortiWiFi-92D, Sophos' UTM SG125 and Watchguard Technologies' Firebox T10-W. (Cisco, Juniper and Netgear declined to participate.)

We observed several megatrends across all the units that we tested:

- **Small is beautiful.** Boxes are getting smaller and more powerful. You don't need a 19-inch rack-sized unit any longer unless you have the need for connecting to a lot of cables or to buy something bigger that is designed to support a very large network. Throughput and features have gone up as the size of the box has diminished, too.
- **Big-ticket firewall features are entering the SMB UTM space.** Even these smallest UTM models offer features that are often found in the largest of enterprise firewalls. Today's typical UTM box includes application awareness, APT screening, and real-time threat visualization tools. While most small businesses don't have skilled IT staffs to handle all of these features, they are still nice to have.
- **Cloud management tools are more prevalent.** Several vendors work with various add-on features to scan files for potential malware, or to off-load management features into the cloud. For example, WatchGuard works with Lastline's cloud-based anti-malware tools, Sophos and Fortinet have cloud-based tools too.
- **Mobile VPN clients now available.** The VPN features on these boxes used to be more of an afterthought, but most of the vendors have beefed up their remote access features. Most products now have more of a selection of VPN types. They also offer the ability to support the built-in or open source mobile IPsec VPN clients of the latest phone and tablet operating systems. That is good news if you want to craft your own mobile device management alternative solution to at least protect data in transit with a smartphone. However, getting phones to work with these boxes is still somewhat of a chore. A few UTM vendors, such as WatchGuard and Calyptix, have added their own tools, clients, or configuration files to make establishing mobile connections easier, while others support the OpenVPN mobile clients.
- **Better botnet containment.** Fighting botnets is a cat-and-mouse war of attrition, but several vendors, including Check Point and Dell, have added specific policies to try to better contain these nasty forms of malware.
- **Better enterprise wireless management tools.** WatchGuard, Fortinet, Dell and Sophos all have beefed up their wireless management features so you can deploy multiple access points around your office and manage them centrally from a single set of screens.

## Winners

All six of these units will do fine for securing small offices of 25 people, but Check Point and WatchGuard stand out as the top vendors in this review. They have solid features, great user interfaces, and coverage across the multiple security technologies that form the basis of what UTM means today. Both also offer relatively inexpensive boxes for small offices with low annual subscription fees.

The others, though, aren't all that far behind. Dell and Fortinet have very tired Web-based interfaces that are in need of a complete overhaul. Sophos has great features but its interface has gotten a bit unwieldy too. And Calyptix shows a lot of promise and has a great way to price its box that the others should follow.

## SCORECARD

| Product | Calyptix | Check Point Software | Dell/ Sonicwall | Fortinet | Sophos | WatchGuard |
|---|---|---|---|---|---|---|
| Installation | 3.5 | 5 | 3.5 | 3 | 3 | 5 |
| Features | 3.5 | 4.5 | 4 | 4.5 | 4 | 4.5 |
| Value | 3.5 | 5 | 3 | 4 | 4 | 5 |
| **Total** | **3.5** | **4.8** | **3.5** | **3.8** | **3.7** | **4.8** |

**SCORING KEY > 5:** Exceptional, **4:** Very Good, **3:** Average, **2:** Below Average, **1:** Consistently Subpar

Here are the individual reviews (watch a slideshow version of this story):

## Calyptix

We tested the AE-800, which comes with four wired Ethernet ports that can be arranged in various VLANs or as a single flat network running version 3.1.15. None of the Calyptix boxes come with wireless access points. That could be a plus if you are worried that you will inadvertently leave your network open to wireless exploits or a minus if you have to deal with buying an additional wireless access points.

Calyptix has the simplest pricing: You get everything they offer without having to purchase individual subscriptions for particular features or for a certain number of users, and it also includes unlimited

business hour phone support. If you have relatively modest needs (meaning don't have a lot of exacting security requirements) and are on a budget, this might be the right box for you.

We found that Calyptix has the least intuitive web UI, with a complex series of menu buttons across the top and left-hand sides, and the UI itself seems somewhat old-fashioned and a bit cryptic. They do get kudos for providing hotlinks to help texts for further explanations of their configuration settings though. Graphical elements are sparse: most menus are fairly text-heavy.

The Security menu is divided into four sections: Network, Web, Email and Instant Messaging. The latter is just a simple radio button to block traffic with each of the major IM protocols. Again, if you want more subtle controls, you will need to look elsewhere. Web filtering can white/black list particular URLs, and there is a place to test whether a domain will be blocked by your settings. You can also block particular file types from entering your network through users' web browsers, such as PDFs or Word files, with a few simple menu selections.

The AE-800 does support load balancing to multiple WAN connections, but getting that setup will require some effort at navigating several menus to prioritize outbound traffic and set up firewall rules accordingly. Recent updates to their firmware include more accurate and faster antivirus scanning. Another nice feature is its best practices analyzer: it will look over all your settings and suggest ways to improve them.

VPN support is somewhat limited, but has an interesting usability feature. Most other vendors have a long list of files that describe particular client software versions. Calyptix puts all of its VPN client tools and configuration settings into one ZIP file, and you generate this file for each specific user. This is done using the web UI.

Currently, their VPN supports only IPsec and passthrough PPTP connections using OpenVPN for Windows, OS X and iOS. It also uses FEAT VPN for Android v2.1 or later devices. You'll want to review carefully the setup instructions that are included as part of the ZIP file, because of the several steps involved. But at least they put all the information together in one place.

One downside is that only the administrator has rights to the entire box, meaning if you want to have someone else have partial rights you can't. Delegation of sub-admin rights is expected in an upcoming release. Another is that Web traffic doesn't go through the anti-virus scanner, but can be filtered by URL or content.

Reports can be scheduled on a daily, weekly or monthly basis, and can be sent via email or just collected in the unit's own archive. The first year's price for our unit was $999, with subsequent years costing $449. While not the least expensive, this is close to the bottom.

## Check Point

When we looked at UTM devices in 2013, Check Point was far and away the best product. While it still has strong features, the others, in particular WatchGuard, are catching up. We tested an early version of the 620, which comes with eight wired Ethernet ports that can be arranged in various VLANs or as a single flat network and running vR77 of firmware. It features support up to four different wireless SSIDs.

Check Point has been our favorite in terms of ease of initial setup and its user interface is still the best by far. Commands are intuitively laid out, there is ample use of graphical elements and just by clicking on a couple of buttons you can easily create protective policies. For example, adding a guest wireless network takes just a few mouse clicks and with an obvious link on the wireless settings screens. You can segregate wireless traffic for better protection with another mouse click.

Since we looked at its product in 2013, Check Point has added new security features such as anti-bot protection, which shares the same protective structure as anti-virus policies. They have also added mobile VPN clients to their mix of LL2P, SSL and IPsec VPNs. One nice feature is a link to the instructions on how to install and configure them from the Google Play or Apple iTunes Stores.

Check Point has beefed up its application controls, with more than 6,000 application policies, the most by far of any of the products we reviewed. You can quickly search through these and with a couple of clicks define a custom set of rules, such as 10 ways to regulate Facebook behavior across your network. Our only complaint is that they are tucked under the Users tab, making them initially hard to find. And with one click, you can place bandwidth limits on apps that can tend to hog it, like peer-to-peer networks and file sharing tools. This is one of the reasons why we continue to like what Check Point offers.

Check Point doesn't offer much in the way of reporting options, with overall summary reports for fixed time periods. But at least you can query its log files if you are trying to track down something suspicious.

One downside is that an administrator has full access rights to the entire box; you can only assign a secondary admin for read-only access. Check Point has added a more capable cloud-managed security service for more granular management. This is useful for ISPs who want to centrally manage and support security policy management, firmware upgrades and automatic backups across multiple boxes. We briefly tested this feature.

Pricing is $598 for the wireless version that we tested, with a very low annual subscription fee of $100. This provides great value for the money.

## Dell/Sonicwall

We tested the NSA 220 Wireless-N, which comes with seven wired Ethernet ports that can be arranged in various VLANs or as a single flat network and running v5.9 firmware. Dell continues to be in the middle of the pack: it isn't the most feature rich or have the most intuitive user interface, but it does deliver solid protection.

For example, others have more capable VPNs or offer more wireless options. If you used Sonicwalls before the Dell acquisition, you will find your way around their menu structure just fine. But if you are new to the brand, you will wish for a new interface that is more usable, graphical, and simpler.

A case in point: Dell offers more than six different dashboards and at least as many setup wizards. These dashboards will show you in real time what is going on across your network, both from a bandwidth consumption as well as a threat analysis perspective. The wizards handle common tasks, such as setting up a switch port group or your wireless access. Navigating among all these choices can be daunting and take some time, which sort of defeats their purpose. On the other hand, once you run through the wizard, you probably don't need to ever see it again.

Another example: Dell doesn't offer the best support for VPNs, but they have widened their IPsec coverage somewhat and include mobile VPN clients for Android and iOS.

All Dell UTMs have integrated wireless access points, which exhibit this odd dichotomy. For example, you can schedule the times you want your wireless coverage to be active and you can manage an entire distributed network of wireless access points across your entire enterprise (which are both things just a few competitors have in their products), but configuring the wireless connection is somewhat cumbersome, requiring you to step through a series of several menus. You can set up multiple SSIDs with different security and access profiles though.

Dell has had the ability to set up specialized sub-admin accounts for some time, so you can delegate particular management tasks or have administrators view configuration settings in read-only mode. This is also missing in a few competitors' products.

Dell has made several functional improvements in its UTM code in the past year, and most of them are under the covers: adding distributed DoS flood and botnet protection, improving IPv6 support, allowing deep packet inspection with no limits on file sizes and adding bandwidth management on a per user or per IP address basis to identify and eliminate network hogs.

Another new feature is the ability to detect rogue access points so you can get a

| Vendor/ Product | Price: 1st year (HARDWARE/SUPPORT) 2ND YEAR (SUPPORT, LICENSE FEES) | Wired GigE LAN Ports | VPN Support/ Clients Available | Additional Modules | Throughput (BASED ON VENDOR-SUPPLIED DATA) |
|---|---|---|---|---|---|
| Calyptix AccessEnforcer AE800 | $999/$449 | 4 | Fair/Excellent | N/A | 100 Mbps |
| Check Point Software 620 | $598/$100 | 8 | Excellent/ Excellent | Anti-botnet | 1.5 Gbps (FW) 220 Mbps (VPN) |
| Dell/Sonicwall NSA 220 Wireless-N | $1,860/$615 | 7 | Good/Good | Cloud AV | 110 Mbps |
| Fortinet FortiWiFi-92D | $1,745/$584 | 14 | Good/Good | Sandbox AV, DLP | 700 Mbps |
| Sophos SG 125 | $1,280/$364 | 7 | Good/ Excellent | 3 boxes, including Sandbox | 165 Mbps |
| WatchGuard Technologies Firebox T10-W | $630/$135 | 3 | Excellent/ Excellent | APT, DLP, Sandbox | 55 Mbps |

handle on who might be leaking data. They have included this as part of its intrusion detection screens. Several others have this feature, including Fortinet and Watchguard. Dell has also enhanced the cloud-based antivirus scanner to get the latest updates via an online repository. Finally, they have beefed up their real-time network traffic analysis so you can see which applications are active across your network and then add firewall rules to manage their use.

Pricing for the Dell is high, at an initial cost of $1,860, but a more reasonable recurring cost of $615 after the first year.

## Fortinet

We tested the 92-D, which comes with 14 wired Ethernet ports that can be arranged in various VLANs or as a single flat network and includes four PoE ports and running v5.2.2 firmware.

Fortinet has always had a broad range of impressive features, they just aren't packaged very well. They are trying to make their Web user interface easier to navigate, but it still seems somewhat behind the times. There is only one setup wizard, and this can be run from the Web interface or via a special Windows or Mac configuration client with a USB connection to the box.

There is also a very meek attempt at a graphical interface for the feature selection, and they have reorganized where particular control menus are located. This will confuse existing Fortinet users and newbies alike. As an example, their DOS and Instant Messaging screening options used to be part of the Web interface; now you have to use the command line for setting up both activities. Like Dell, it is time for a major interface overhaul.

However, they have added a few new things to their latest firmware release, including having the second broadest range of application signatures, at more than 3,400 separate rules. As an example, there are at least 60 of them concerning Facebook alone. Check Point has nearly double the total rule set but still what Fortinet has is impressive and both vendors are on par with application firewall specialty vendors such as Palo Alto Networks. You can add a signature to any firewall policy with just a few screens.

Fortinet also offers a primitive data loss prevention monitor, with checks on Social Security and credit card numbers only, although you can add a custom fingerprint to their process. The unit's Wi-Fi comes with two radios that can be set separately with different access rules. If you want more you'll have to purchase a separate wireless access point. This isn't as capable as some of the other vendors. It comes with built-in two-factor authentication using hardware tokens, email or SMS. And like Dell, it has support for a wide variety of sub-admin profiles. There are now more than a dozen configurations, and all can be set at read only or read/write access.

It also augments its anti-malware scanning by using a cloud-based sandbox. If you enable this option, files can be tested there as part of your protection policies. This is similar to how both WatchGuard and Sophos handle this. Speaking of the cloud, you can also store configurations there to provision multiple boxes, which is similar to how Check Point uses its cloud management tool.

Fortinet's support for both SSL and IPsec VPNs is also middle of the pack. If you make use of their FortiClient software, you get both endpoint antivirus protection and a VPN included in the package.

Pricing is $1,745 for the initial purchase with $584 a year for subscription renewals.

## Sophos

We tested three boxes from Sophos: the SG125 that provides the basic UTM functionality, a wireless access point (AP15) and a Remote Ethernet Device (RED 10) that has some unique remote access features. Sophos actually has two UTM lines: the SG line that it originally acquired from Astaro (and which we tested using a slightly earlier firmware version last year) and another line that they recently acquired from Cyberroam. Sophos is in the process of integrating some of Cyberroam's features into a subsequent release in 2015. Since they sent us the SG125, they now offer models with integrated wireless access points in them that carry a "w" suffix, such as the SG125w.

We tested version 9.3 of the UTM firmware. It includes some advanced features that distinguish the unit, including web server reverse proxy protection and the beginnings of APT protection. Also new is the ability to enforce web traffic policies on encrypted connections without the need to decrypt the actual traffic.

Both the general and wireless Sophos configuration took a bit longer to understand. We actually got our unit into some unworkable state and had to reinstall its firmware. Like most of these units, wireless connections can be segregated into their own VLAN, or combined with the general wired traffic. Multiple SSIDs can be created on the same access point for a separate guest network for example. Understanding the menus that provide this flexibility took some careful study, more so than the other units.

One nice default is that Sophos will send any file to be first analyzed with its cloud-based sandbox. There is nothing for the user to do; it is part of their scanning engine. Another advanced feature is the ability to support two-factor user authentication, there are a number of ways to set this up. Finally, it offers a nice change log that shows you all the various configuration options you have done as an administrator: we wish other boxes would offer this feature.

Sophos has improved its applications control, and while it is not as capable as Fortinet's, it can be easily accessed through the network flow monitor or by setting up an explicit policy on one of more than 1,200 behavior rules. For example, for Facebook there are 10 different rules.

Sophos VPN clients include support for both OpenVPN (include the iOS and Android clients) and Cisco VPN clients. One nice feature is being able to quickly access your Amazon-based virtual private cloud by either downloading the configuration file from Amazon or uploading this information from the UTM box. And for the easiest VPN access, there is the Remote

Ethernet Device, a separate box that attaches to your remote network. You set up its identity on the UTM and it makes the connection easily.

Like Fortinet, Sophos has its own endpoint protection client called Live. It only works to protect Windows endpoints.

There are lots of reports that can be archived and accessed from Web UI, including a daily "executive report" that contains network usage, top destinations and clients, The reports failed to disclose our BitTorrent activity, but that may be due to our error in setting up the correct policy.

Pricing was $1,280 for the initial purchase, with second and subsequent years costing $364 for annual subscriptions.

## WatchGuard

We tested the T-10-W, which comes with three wired Ethernet ports that can be arranged in various VLANs or as a single flat network. WatchGuard has always had a mixture of Web, Windows and command line management interfaces. What is changing in the past year is which features are available under each interface, with the Web receiving some much-needed attention.

In October 2013 the company announced an upgraded tool called Dimension that carries several new features and is available with any UTM appliance running at least version 11.8 (we tested v 11.9.3). Dimension is a new real-time visualization tool that can be used to quickly identify emerging threats and network usage trends. Dimension is packaged as a virtual machine and is downloaded for free from the WatchGuard support website. It replaces the log servers that were difficult to interpret and search. Setting up Dimension is easy: you just point the log server from your UTM box to the appropriate IP address of your Dimension server, and it begins collecting information automatically. The company is in the process of taking some of the features from Dimension and moving them over to the web interface for several of their UTM appliances, including the T-10-W.

Here are some of the more interesting newer features:

- **Active threat map,** shows by location where identified threats originate by geo-locating their IP addresses. IT managers can use this information to block particular geographic access to their networks, or investigate potential oddities such as users from outside a particular state or city.
- **FireWatch** (which is also available through the web interface) shows you the most popular destination domains and most active users, along with other information in near-real time in a nice graphical area plot diagram. IT managers can use this information to tune their firewall rules and policies.
- **A variety of reports can be now emailed** to recipients from within the Dimension interface.
- **Executive dashboards** that summarize network activity and threats experienced in graphical form. Some of this information is available from the Web UI as well.

Even though the T-10-W is a small box, it has some solid management features that are found in larger UTMs and corporate firewalls. For example, you can set up to three different SSIDs using the built-in wireless access point and manage other access points that are external to the box. You can also segment the wireless traffic by specific firewall policies, so you could for example set up a guest network for visitors to your office.

There are some solid firewall features too: it comes with the ability to handle advanced persistent threats (APT) and data loss prevention situations. To get APT, you have to pass traffic through a proxy, then through the antivirus engine, and then to the APT routine. That takes some effort to setup. One benefit is that it works in conjunction with Lastline's cloud-based sandbox routine to determine if any malware has infected your system. Like Sophos, there isn't much to set this up, it is just part of the malware scanning process.

One other noteworthy item is the number of custom application behavior controls has been significantly beefed up: there are more than 2,000 behavior profiles that you can incorporate into protection policies. For example, there are 10 different Facebook profiles, so like Sophos and Fortinet, you can restrict traffic based on whether it is a Facebook game, or message, or Wall update. While not as numerous as Fortinet or Check Point, it is still impressive.

WatchGuard has excellent VPN support for L2TP, SSL (using OpenVPN) and IPsec VPN types. For IPsec you can use its own mobile VPN clients, the Cisco VPN clients that are built into Mac OS X or those from Shrew Soft. You set up a configuration using the Web or Windows management interface and then send that configuration file to the particular mobile device that you want to grant access. The mobile VPN clients support iOS v5 and higher, and Android v4 or higher.

Pricing was $630 for the initial purchase, with second and subsequent year subscriptions at $135 annually. This represents great value for the money.

## How we tested UTM appliances

We connected each box to our small office DSL router and tried out the various Web and (in some cases) Windows-based management interfaces. We set up clients on various Windows 7 and 8 and Mac OS X machines as well as several iPhones of varying vintages. We assumed these devices will be placed on networks without any central Active Directory or RADIUS servers and added user accounts and set up security groups manually.

Once a box was connected, we updated the firmware and licensed individual software modules on each box, and then set up each UTM with WAN and LAN interfaces to operate with DHCP addresses whenever possible to remove the headache of managing IP subnets. We looked at what it would take to create a more restrictive policy for guest workers, as one example, and to see how to automatically block incoming threats. We added particular policies for sample users and performed other common tasks.

We examined packet captures across each box to see if firewall rules and other security policies were operating correctly. We also tried out various VPN and remote access connections from outside our office network to verify these features.

We evaluated the units based on these three criteria: installation, features, and overall value.

For installation, we reviewed the basic setup of the various network interfaces, users, and licenses. These products should be geared towards smaller networks, with limited IT expertise and time to administer them. We looked at how much time was needed to set them up and configure properly.

When it came to examining features, we looked at the ability to manage and monitor the box remotely, set up new security policies, and review reports. We also looked at how well the basic five security modules integrate with each other, and what kind of workflow is needed to implement its protective features.

Finally, to assess value, we accounted for the overall first year purchase price plus the cost of any support and software licenses.

## A note on throughput

We didn't measure throughput – instead we reported in the comparison table the data that we got from the various vendors. Since we didn't independently verify these claims, we suggest that you take the throughput numbers with several helpings of salt. All UTM boxes will bog down as you turn on more of their features, particularly the VPNs and the IDS that take more processing horsepower. The good news is that the ASICs inside even the lower-end boxes that we tested are getting better all the time, and that combined with offloading tasks to the cloud means that these products can handle more packet processing than ever before.

*Strom is the founding editor-in-chief of Network Computing magazine and has written thousands of magazine articles and two books on various IT and networking topics. His blog can be found at strominator.com and you can follow him on Twitter @dstrom. He lives in St. Louis.*