TechTarget SearchSecurity

E-guide

TechTarget Research Peer Network

Unified Threat Management Buyer's Guide

Your expert guide to unified threat management

In this e-guide

Introduction to unified threat management appliances

Ed Tittel

Expert Ed Tittel describes unified threat management (UTM) appliances and features, and explains its advantages to organizations of all sizes.

A unified threat management (UTM) system is a type of network hardware appliance, virtual appliance or cloud service that combines and integrates several security technologies -- typically, a firewall, intrusion prevention system (IPS), antimalware, virtual private networking (VPN) and Web/content filtering.

UTM virtual appliances and cloud services are gaining in popularity. Both types of UTM eliminate the need for an on-premises appliance, but still offer centralized control and ease of use. However, this article focuses on UTM appliances.

Unified threat management appliances simplify management by granting network administrators use of an integrated interface to configure and maintain each component. Centralized control also reduces complexity and the likelihood of errors because the details of each component are clearly visible on a dashboard. An administrator can react quickly to performance issues as they arise, and can monitor how changes affect other components. Plus, organizations realize lower overall costs compared to acquiring each component separately, and they can produce cohesive compliance reports when required by regulations, such as Health Insurance Portability and Accountability Act, Sarbanes-Oxley Act and so on.

On the downside, UTM products also present a single point of failure should an event occur that cannot be handled proactively or remediated quickly.

The demographics of UTM customers

UTM vendors initially targeted the small to medium-sized business (SMB) market to help them reduce administrative overhead and control security costs. However, the reliability and scalability of UTM products makes them suitable for enterprise adoption as well.

Today, UTM appliances are found in small office/home offices (SOHOs), retail, banking and similar environments, branch offices, midsize organizations and large enterprises. Most UTM vendors offer a line of products to accommodate each type of customer.

In this e-guide

Characteristic features of UTM appliances

Nearly every unified threat management appliance includes the same core features, and each vendor may include additional components in various models to appeal to different customers. These core features may be described as follows:

- **Antivirus/antimalware**: This component scans for malicious programs and other types of malware, and either quarantines or removes it. Some UTM appliances include antispam features as well. If the antimalware scanner is appliance-based (meaning the software resides on the appliance), scans will affect the performance of the unit to some extent. Some vendors use antimalware scanners in the cloud, which minimizes the use of UTM appliance resources during scanning.

- **Firewall**: A next-generation firewall sits at the heart of a UTM appliance. Common throughput rates are 600 Mbps to 200 Gbps, with several ports that may include 10/100 Ethernet to 1, 10, 40 and 100 Gigabit Ethernet.

- **Intrusion prevention**: This component analyzes incoming network packets for attack signatures and evaluates results against a defined policy. Unsafe packets may be dropped or a connection terminated to protect the internal network.

- **Virtual private networking**: This component manages VPN connections for secure remote access to the internal network.
- **Web filtering**: This component prevents access to inappropriate Web content. An administrator may define URLs/domains that are not allowed (blacklisting), or the filter may communicate with a continuously updated reputation service. The filter may also intercept all HTTP requests in a TCP connection. Some vendors provide Web filtering as part of the core package, whereas other vendors require an additional Web filtering license.

Other features that are included in specific UTM models include application control, bandwidth management, data loss prevention, identity-based access control, load balancing and more. These more advanced features are generally found in higher-end systems aimed at midsize and larger organizations.

Pricing and support

How unified threat management appliances are packaged and sold varies by vendor. A customer may purchase or lease a unit from a vendor or reseller, which usually requires an annual subscription for software updates and upgrades. Such a subscription can add significantly to the total cost of purchase.

Appliances for SOHOs start at about $400, and small branch office units with subscriptions start at around $1,700, but are more typically in the $2,500 range. The next tier -- for midsize organizations -- jumps to about a $20,000 minimum. From there, the cost for a unit can climb to $200,000 or more for large enterprises.

For an additional fee, most vendors offer different tiers of support. At the low end, a support contract includes limited phone and email support, an online knowledge base and forums. Phone support at this level may be restricted to business hours only. Higher priced contracts may include 24/7 phone support, four-hour or next-day on-site engineer support, next-day parts delivery, and an assigned account representative. Annual support contracts cost in the range from $500 to over $25,000.

UTM training

Many vendors and resellers provide UTM training for administrators and support engineers for an additional fee. Costs vary widely, but typically range from $1,000 to $3,500, depending on whether sessions are Web-based or in-classroom.

Although it's usually not required, training can help an administrator get up to speed on new technology more quickly than self-learning, and training can be critical for an administrator that is migrating technology from one vendor's products to another.

Technical staff might also sign up for training while pursuing a certification from a particular vendor, which might or might not be paid for by the employer.

Are UTM appliances right for your organization?

Although many organizations install and manage firewalls, antimalware software, an IPS, Web filtering software and other security technologies from a variety of vendors, a UTM product can make the process much easier and more cost-effective. The best approach may be for an organization to document its current security appliances and purchase dates, when they will reach their end of life, the manufacturer/vendor of each appliance, and estimated replacement costs. Then find out more about UTM appliances and compare the hard and soft costs.

That is personnel time that could be freed up by standardizing many security components on a single system and vendor, with a centralized management console.

Organizations may very well find that UTM is the smart decision going forward.

Next article

In this e-guide

How UTM products can benefit your enterprise network environment

Ed Tittel

Expert Ed Tittel explains why unified threat management is the right holistic IT security approach for SMBs and how it can fit into the enterprise, as well.

With the number of network-connected devices increasing exponentially, threats to corporate networks and the data they contain pose an ever-increasing risk, as well. Attackers have proven their capability to find and exploit security holes, whether their target is perimeter defense measures, employees who receive phishing emails or the unsuspecting telecommuter without proper controls in place on a home computer.

Historically, organizations have used a patchwork collection of security devices, often from different vendors, to protect and defend their networks. Acquiring, configuring, managing and monitoring this assortment of devices takes considerable effort and expertise, which puts undue strain on the administrators and engineers tasked with the responsibility of network security.

Unified threat management (UTM) products are dedicated security systems with optimized hardware and software that can perform many security functions simultaneously, such as firewall, intrusion detection and prevention, antivirus, virtual private networking and more. The point of a UTM product is to provide layered, integrated protection all within a single appliance, which requires less administrative effort and generally comes at a lower cost.

Note: Cloud-based UTM services are also available, but haven't yet been widely adopted by organizations. According to Gartner's 2014 Magic Quadrant for Unified Threat Management, cloud-based UTM services are adopted in less than 5% of UTM implementations. Though UTM is edging toward the cloud, it hasn't really made that jump just yet -- no matter what vendors may proclaim.

This article explores the pros and cons of UTM products and examines how UTM can benefit different network environments.

Advantages and disadvantages of a UTM product

A UTM appliance offers many key advantages for managing data threats and protecting networks and sensitive information. Here are some of the advantages of deploying a UTM appliance:

- **Hardware consolidation**: An administrator can purchase, deploy and manage one appliance in an SMB, or a small number of appliances in larger environments, rather than multiple devices.

- **Simplified management and patching**: Blended threats and emerging threats may target different parts of a network simultaneously, causing an administrative nightmare if many security devices are involved. UTM offers centralized management, enabling administrators to manage a large range of threats to local and remote environments from a single console. Patch management is also simplified because only one or relatively few appliances need to be patched rather than many different devices.

- **One vendor, one license, one support contact**: Administrators can work with a single vendor and its support department, fostering a solid relationship that promotes continuity. Licensing of a single appliance is easy to manage, even as an organization's needs grow.

- **Lower expenses**: The consolidation of hardware offers a lower price point compared to acquiring multiple devices, and administrators can focus their knowledge and training on one appliance.

While UTM products resolve many administrative and operational security issues, they also pose a few drawbacks, as well:

- **Single point of failure**: Because UTM combines many security features into one appliance, it presents a single point of failure if the appliance stops working or if malware makes it to the internal network. To mitigate this situation, SMBs might implement a secondary failsafe service, such as a software-based firewall. However, more robust UTM appliances, such as enterprise-ready products, are designed with built-in redundancy to avoid the single-point-of-failure scenario.

- **Performance issues**: Until recently, performance was cited as a major drawback for UTM appliances. When all features were enabled -- especially the antivirus feature that checked all traffic and email -- network performance took an appreciable hit. UTM vendors have greatly improved the their appliances' performance to overcome most issues, but an organization looking to implement a UTM product needs to pay close attention to performance rates and perform thorough tests of any appliance that makes its acquisition shortlist.

Organizations that benefit from UTM products

Most UTM vendors offer a range of appliances in different capacities and capabilities. A high-capacity UTM appliance protects primary network connections to the Internet -- on the edge -- or may be implemented in the core network, providing fault tolerance and high availability. Smaller UTM appliances offer most of the same features as their larger counterparts, and are ideal for SMBs, as well as remote offices with connections to corporate networks. Due to the modular nature of a UTM appliance, an administrator can enable all or some of the features to suit the needs of the environment.

UTM scenario No. 1: SMB organizations

The UTM concept was originally aimed at the SMB market -- organizations with fewer than 100 employees to upwards of 1,000 -- as an all-in-one security box that was easy to install and administer. And SMBs still represent a significant percentage of the UTM customer base -- for good reason. UTM is an ideal security product for nearly every SMB infrastructure. All of the major vendors -- such as Fortinet, Dell, Cisco, WatchGuard, Check Point, Sophos and Barracuda -- offer a solid range of appliances for the SMB market. With the right unit in place, UTM provides comprehensive, yet flexible, network security, cost effectively.

UTM scenario No. 2: Branch office/home office environment

According to the 2014 National Study of Employers (NSE), 67% of employers with 50 or more employees allow them to occasionally work some of their regular paid hours at home. Although a virtual private network (VPN) is commonly used to secure communications between the home office and the corporate network, administrators have little control over the security of the home computer itself. If the home computer is infected with a virus, rootkit or other form of malware, the corporate network is at risk when the VPN connection is used.

Some UTM vendors, such as WatchGuard, offer relatively low-cost UTM appliances that protect data and communications between the branch or home office and corporate resources. For example, the WatchGuard Firebox T10 self-configures upon plugging in the appliance, immediately communicates with the administrator's central console at the corporate office and incorporates security intelligence from the cloud. The administrator can remotely manage the appliance, ensuring the remote office computer and connection is secure and complies with corporate security policy.

UTM scenario No. 3: Large enterprise environment

In the past, UTM products were designed primarily for hardware consolidation, ease of use and lower costs rather than performance and reliability, which are critical to enterprises. Today, some of the top-ranked UTM vendors offer truly enterprise-ready appliances that perform well at the network edge and the core, offering virtual local area network (VLAN) capabilities that support multiple security zones, load balancing, scalability and more.

The problem, however, is that most enterprises are committed to their current security infrastructure, and may be loath to replacing standalone units that are performing well with an all-in-one UTM appliance -- essentially putting their trust in a single appliance.

A large organization that is dealing with an acquisition or merger -- and needs to standardize on security -- or one that has consolidated its firewalls on a large network, should consider adding UTM functionality. Regardless of the situation, that organization will need to spend a good deal of time researching specifications and talking to salespeople. Testing units with all features enabled is also necessary. And to perform those tests, organizations should push traffic through the appliance that mimics real-time network traffic.

Next steps: How to select the right UTM product

SMBs continue to be the primary UTM product consumer. An SMB that plans to upgrade its current security infrastructure should look closely at the top-rated UTM vendors as part of its research. Large enterprises now have a fairly good range of UTM products to choose from that are truly enterprise-ready; they meet performance requirements and provide high availability and redundancy. Additionally, reasonably priced appliances are available for remote offices that provide critical protection beyond the VPN connection.

Once an organization has determined it is a good candidate for UTM, the next step is to select the product that provides the best fit for its needs. The next article in this series on UTM products will provide readers with the criteria to consider just that.

Next article

Six criteria for purchasing unified threat management appliances

Ed Tittel

Expert Ed Tittel explores key criteria for evaluating unified threat management (UTM) appliances to determine the best choice for your organization.

Unified threat management appliances -- devices that bundle all kinds of network infrastructure protection into one device -- are mighty popular in small to midsize environments -- and are gaining traction in larger infrastructures -- for many good reasons. In the right environment, relying on a single device to cover firewall, virtual private network (VPN) access, application control, intrusion protection and lots of other services saves money and administrative effort.

Determine your needs

Before diving deep into unified threat management (UTM) appliance comparisons and ordering trial units, the first step toward procuring a UTM is to determine an organization's security needs.

Here's a list of questions to consider:

- Does it need a full protection solution or a solution that supplements current technologies?
- What types of protection does the UTM appliance need to implement? This includes firewall, VPN, application control and so on.
- Does it want an access point included in the appliance? Only certain UTM appliances have integrated wireless access points, and those are usually found in entry-level or small office products.
- What is the infrastructure's bandwidth? This involves gathering statistics from the infrastructure, such as average incoming and outgoing bandwidth usage, the average number of users accessing the Internet, and the number of daily email messages (sent and received). Also record spikes and determine if they occur regularly. These statistics help with right-sizing a UTM appliance to its environment and in determining if a network upgrade is necessary.
- How many users and devices does the organization need to support today? How many two years from now? This answer helps it right-size an appliance with an eye on growth. Higher-end UTM appliances are fully scalable, but come with bigger price tags.

- Does it have a solid antivirus product in place that's working well? Many unified threat management appliances come with antivirus, but not every organization wants to replace its current solution.

During needs analysis, be sure to keep notes (perhaps in a spreadsheet) to enable mapping the organization's needs to UTM features on a per-vendor basis.

Shopping 101: The big picture

Today's leading UTM vendors, such as Fortinet, Check Point, Dell, Sophos and others, make the shopping and purchasing process pretty easy (with the exception of licensing and subscriptions, which you'll learn about soon). The vendor websites typically list appliances for small, midsize and large environments -- clearly stating performance details, like firewall throughput, VPN throughput, number of users, and number and type of ports.

Note: Be careful of nomenclature when perusing vendor products. Not every company calls its products "unified threat management" or "UTM." In fact, UTMs are often simply referred to as "security appliances," and many companies still call them "next-generation firewalls." However, a next-generation firewall typically includes intrusion protection and perhaps application control, where a UTM appliance includes a firewall, IPS and a whole lot more.

Each website also lists the features and controls that are either integrated into the appliance by default or that can be integrated by purchasing a license or subscription. It's important for an organization to understand which features they will actually use, because appliance performance can be affected (sometimes greatly) when all available features are enabled.

Evaluation criteria for UTM appliance

When researching unified threat management appliances, use the following list of criteria to make a proper comparison:

- **Vendor**: It's usually best to pick a market leader, the assumption being that the vendor has a good track record, adequate or excellent support, and has produced a well-honed line of products. Also consider that top vendors typically have the resources to perform ongoing research into emerging threats and can roll that knowledge and captured data into their products. Continuity and compatibility are also factors when looking at vendors. If an organization's security staff already uses products from a specific vendor, the learning curve can be much shorter by sticking with a UTM appliance from that same vendor.

- **Features**: Not every unified threat management appliance has the same features. Data loss prevention and deep packet inspection over SSL connections aren't usually part of the standard feature set. Models from the same vendor can include different features, too, although many vendors' appliances do include a common feature set across all models. An organization's needs analysis should help whittle down which features are must-haves versus nice-to-haves.

Regarding antivirus, find out if the vendor has its own antivirus solution or is partnered with another company that provides it. Some vendors use Kaspersky or Sophos, for example. The vendor's choice of antivirus product might not be the organization's first choice.

- **Performance**: As mentioned, vendors publish firewall and VPN throughput rates for their appliances. Those ratings are not necessarily the same rates that will be experienced in different environments. When researching products, also check UTM ratings or reviews from independent sources such as NSS Labs and Miercom.

Tip: Time allowing, it's a good idea to reach out to other organizations that already use UTM appliances and get their feedback on performance in a live environment, as well as ease of deployment, compatibility with other network protection equipment, and tech support responsiveness.

- **Cost**: The cost of UTM appliances varies greatly, from those geared toward small environments (usually in the range of $400 to $1,200) to the highly scalable, highly available appliances for enterprises (tens of thousands of dollars). This is where a needs analysis pays off -- that data should point to the appliance with the best fit and tell the organization which features it truly needs.

- **Licensing and subscriptions**: With very few exceptions, UTM vendors require licenses or subscriptions to turn on UTM features, such as application control, antivirus and so on, and/or cloud-based management control. In some cases, it's possible to configure those features, but they won't be active until a valid license key is supplied.

Those licenses or subscriptions are offered with term limits -- one year, two years and up to 10-year increments -- and may or may not include support, such as 24/7 assistance and replacement hardware. This is one area of research where it takes time to comb through each vendor's requirements and offerings, and to find a bundle at the best price. Licensing and subscriptions can easily run 50% or more than the cost of the appliance. Dig into upgrade pricing as well, in case the number of devices or users changes or additional features are needed following initial purchase.

Another issue with licensing is to understand if the vendor licenses its product per user, per device or per IP address. If the vendor follows the IP address model, do only those IP addresses behind the firewall count toward the total? If an organization has a high-availability cluster, does each device in the cluster need a separate license?

- **Support**: Find out what's included in the standard support package, and the price of a premium package if standard isn't adequate. Remember, some vendors roll support into their licensing packages, which needs to be taken into account when examining overall costs.

Other considerations

UTM vendors want customers to be satisfied with their products -- a happy customer doesn't need as much support, right? Vendors often allow organizations to request a unit of their choice and run it in their own environment, taking time to thoroughly test performance and compatibility with other equipment. Some vendors even offer free support during the evaluation period, and online demos may be available to help customers tinker with the interface and to safely reconfigure a virtual appliance to mimic their own network.

During the evaluation stage, be sure to assess ease of deployment, configuration interfaces (GUI, command line or both) and usability of the management console. Can staff easily maneuver around the screens? Are settings easy to find, and is the documentation clear enough to avoid a support call? Ease of use is especially important to smaller organizations that may not have dedicated security staff.

Finally, if an organization must follow compliance regulations and laws, find out if the UTM appliance offers functionality and reporting tools needed for a compliance audit. Most appliances do, but double-checking this important feature before purchase will prevent headaches down the road.

Conclusions

Even though the UTM appliance buying experience has been simplified thanks to fairly consistent comparison points and a highly competitive market with vendors who want your business, there are still a lot of factors to consider carefully before making a decision.

Every decision should start with a thorough needs analysis of an organization's particular environment and a map from those needs to vendor offerings. Then, find out what experts think are the best products for environments similar to yours.

The next article in this series will match the evaluation criteria outlined in this feature to products from some of the top unified threat management appliance makers on the market today.

↘ Next article

In this e-guide

Comparing the best UTM products in the industry

Ed Tittel

Expert Ed Tittel examines the top unified threat management appliances to determine which one could be the best for your organization.

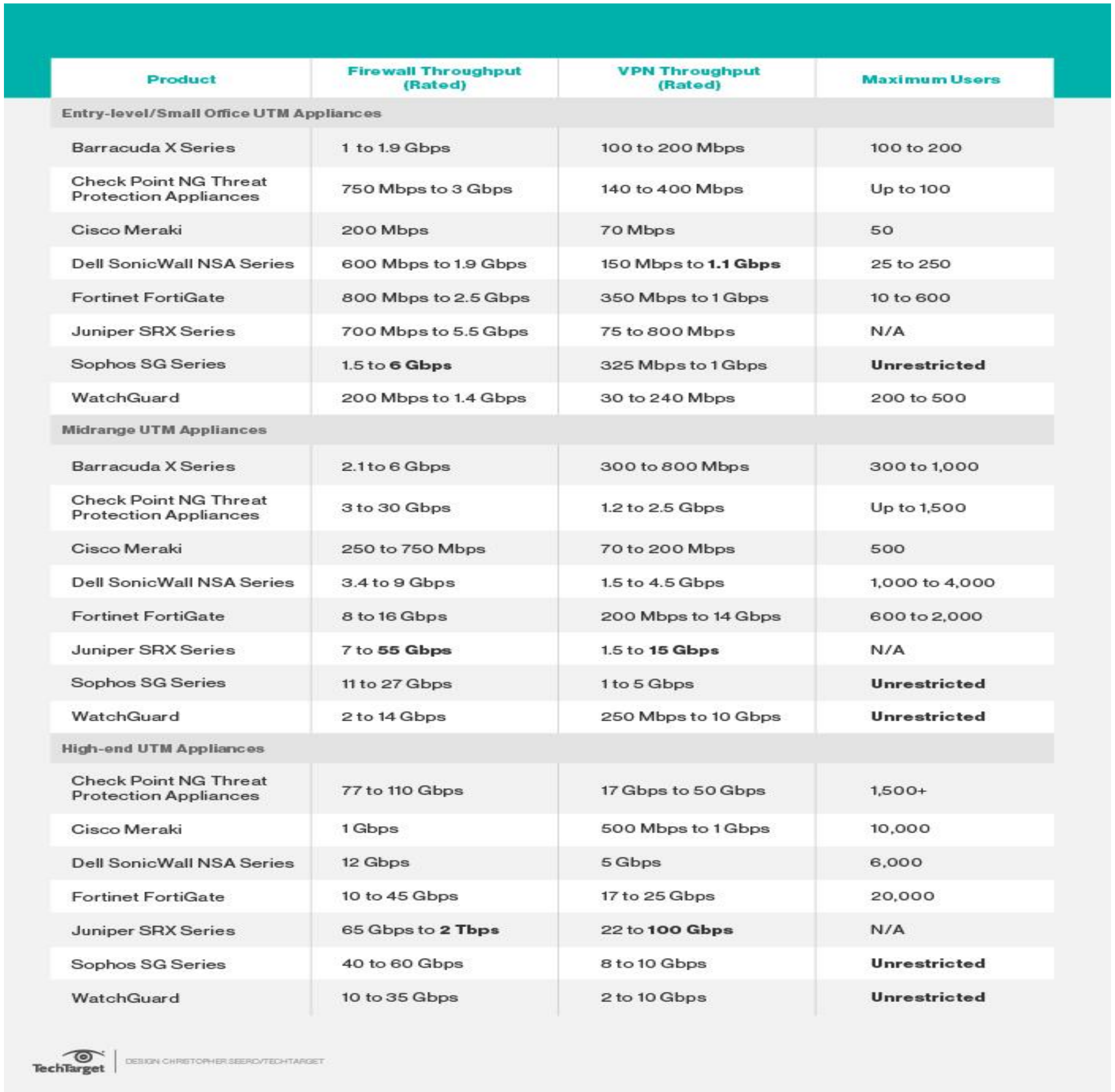
Unified threat management (UTM) can provide significant equipment cost savings and reduce administrative efforts by combining several security features into one appliance.

This article examines how to choose the best UTM appliance by comparing product series from eight of the leading vendors: Barracuda X Series, Check Point Next Generation Threat Prevention Appliances, Cisco Meraki, Dell SonicWALL NSA Series, Fortinet FortiGate, Juniper Networks SRX Series, Sophos UTM SG and WatchGuard XTM and Firebox. UTM appliances share a set of basic features, such as firewall, virtual private network (VPN) and application control, and the vendors require the purchase of a license or subscription for those modules. All of the companies have entry-level units for small offices and remote locations, as well as mid-level units for small and midsize environments. Six of the eight vendors offer high-end appliances suitable for enterprise data centers.

Performance: Throughput and number of users

Performance specifications vary greatly from vendor to vendor, and some vendors have many UTM products in a series (over 40 in the case of Fortinet). The following table summarizes firewall and VPN throughput rates, as well as the maximum number of users for the featured vendors' UTM appliance series. UTM models and specifications change frequently, so consider the numbers a snapshot in time. The highest advertised firewall and VPN rates, and number of users, are indicated in bold.

In this e-guide



Product	Firewall Throughput (Rated)	VPN Throughput (Rated)	Maximum Users
Entry-level/Small Office UTM Appliances			
Barracuda X Series	1 to 1.9 Gbps	100 to 200 Mbps	100 to 200
Check Point NG Threat Protection Appliances	750 Mbps to 3 Gbps	140 to 400 Mbps	Up to 100
Cisco Meraki	200 Mbps	70 Mbps	50
Dell SonicWall NSA Series	600 Mbps to 1.9 Gbps	150 Mbps to **1.1 Gbps**	25 to 250
Fortinet FortiGate	800 Mbps to 2.5 Gbps	350 Mbps to 1 Gbps	10 to 600
Juniper SRX Series	700 Mbps to 5.5 Gbps	75 to 800 Mbps	N/A
Sophos SG Series	1.5 to **6 Gbps**	325 Mbps to 1 Gbps	**Unrestricted**
WatchGuard	200 Mbps to 1.4 Gbps	30 to 240 Mbps	200 to 500
Midrange UTM Appliances			
Barracuda X Series	2.1 to 6 Gbps	300 to 800 Mbps	300 to 1,000
Check Point NG Threat Protection Appliances	3 to 30 Gbps	1.2 to 2.5 Gbps	Up to 1,500
Cisco Meraki	250 to 750 Mbps	70 to 200 Mbps	500
Dell SonicWall NSA Series	3.4 to 9 Gbps	1.5 to 4.5 Gbps	1,000 to 4,000
Fortinet FortiGate	8 to 16 Gbps	200 Mbps to 14 Gbps	600 to 2,000
Juniper SRX Series	7 to **55 Gbps**	1.5 to **15 Gbps**	N/A
Sophos SG Series	11 to 27 Gbps	1 to 5 Gbps	**Unrestricted**
WatchGuard	2 to 14 Gbps	250 Mbps to 10 Gbps	**Unrestricted**
High-end UTM Appliances			
Check Point NG Threat Protection Appliances	77 to 110 Gbps	17 Gbps to 50 Gbps	1,500+
Cisco Meraki	1 Gbps	500 Mbps to 1 Gbps	10,000
Dell SonicWall NSA Series	12 Gbps	5 Gbps	6,000
Fortinet FortiGate	10 to 45 Gbps	17 to 25 Gbps	20,000
Juniper SRX Series	65 Gbps to **2 Tbps**	22 to **100 Gbps**	N/A
Sophos SG Series	40 to 60 Gbps	8 to 10 Gbps	**Unrestricted**
WatchGuard	10 to 35 Gbps	2 to 10 Gbps	**Unrestricted**

DESIGN: CHRISTOPHER SEERO/TECHTARGET

Barracuda and Dell SonicWALL cater mainly to small to midsize businesses (SMBs), although Dell's high-end NSA 6600 is advertised for "emerging large businesses" and is included in the "high-end" category. No Barracuda products are considered high end at this time. (If you view TechTarget's Barracuda UTM product description, you will see products listed as "high-end." However, when compared to other vendors' offerings, the high-end Barracuda products are more accurately categorized as midrange.)

It's also questionable whether the "high-end" Cisco Meraki product (there is only one in that range) should be considered enterprise-class, given the lower firewall and VPN throughput rates compared to the competition -- even though the product claims to support up to 10,000 users.

Related to performance, Barracuda, Check Point, Dell SonicWALL, Sophos and WatchGuard products are known for their ease of implementation and use, which is particularly important in an SMB environment.

Features

Every UTM appliance has a firewall, VPN and intrusion prevention system, and supports application control, content filtering, malware and spam protection, as well as network- or cloud-based centralized management. Most vendors also include Web filtering, although it's an optional feature of Barracuda appliances.

Check Point UTMs include advanced networking and clustering, identity awareness, network policy management and logging and status features. The company's Next Generation Threat Extraction software package also includes threat emulation (sandboxing) and threat extraction for protecting documents from exploitable content.

Cisco Meraki appliances provide identity-based security policies, multiple WAN uplinks and 4G failover, but they do not include email scanning or SSL decryption for HTTP.

Every UTM appliance has a firewall, VPN and intrusion prevention system, and supports application control, content filtering, malware and spam protection, as well as network- or cloud-based centralized management.

Dell SonicWALL NSA Series products examine all traffic, regardless of port or protocol, unlike many competitors.

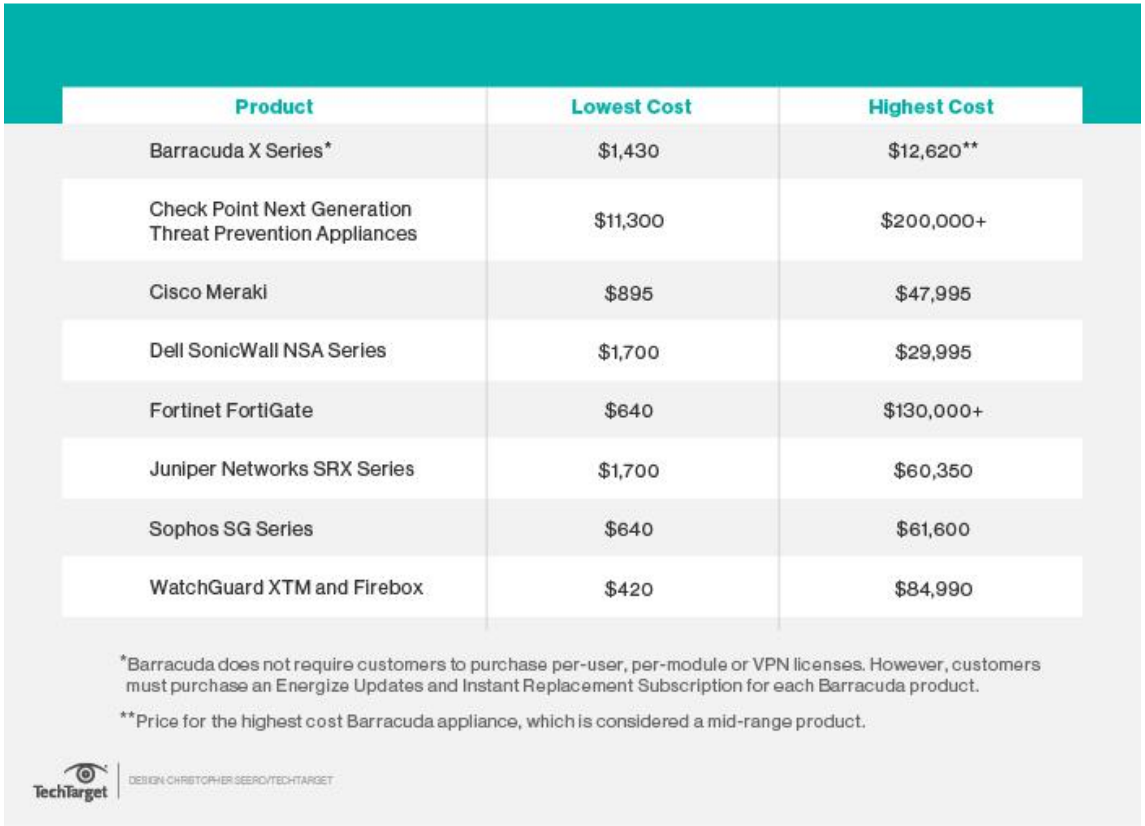
Check Point, Fortinet, Juniper and WatchGuard support advanced persistent threat protection (which is optional for WatchGuard). Fortinet, Sophos and WatchGuard also provide data loss prevention.

Customers who need detailed compliance reporting should take a close look at the Sophos products. Sophos offers iView, a separate appliance that gathers information across multiple UTMs and provides reporting to meet compliance requirements.

Pricing, licensing or subscriptions support

One of the most complex aspects of selecting the best UTM appliance for your organization is to understand software feature licenses (also referred to as "subscriptions" by some vendors). All of the featured vendors except Barracuda license UTM features, such as application control and antivirus, as separate licenses and/or in bundles. Customers choose the license term, which is usually one or three years, but can go up to 10 years in some cases.

The following table shows the lowest and highest retail costs for each vendor's appliances, along with required software licensing or subscriptions (one year). The vendors with the largest range of prices typically offer the most individual products.



Product	Lowest Cost	Highest Cost
Barracuda X Series*	$1,430	$12,620**
Check Point Next Generation Threat Prevention Appliances	$11,300	$200,000+
Cisco Meraki	$895	$47,995
Dell SonicWall NSA Series	$1,700	$29,995
Fortinet FortiGate	$640	$130,000+
Juniper Networks SRX Series	$1,700	$60,350
Sophos SG Series	$640	$61,600
WatchGuard XTM and Firebox	$420	$84,990

*Barracuda does not require customers to purchase per-user, per-module or VPN licenses. However, customers must purchase an Energize Updates and Instant Replacement Subscription for each Barracuda product.

**Price for the highest cost Barracuda appliance, which is considered a mid-range product.

TechTarget | DESIGN: CHRISTOPHER SEERO/TECHTARGET

Cisco Meraki appliances use a cloud-based management tool that requires customers to purchase a license for the cloud on a per-device basis. Other vendors, such as Barracuda and Sophos, provide centralized management for free.

All of the companies offer similar standard support packages, along with the opportunity to purchase premium support at an additional cost.

Choosing the best UTM product for you

Organizations that are in the market for UTM products and are already running networking equipment from a particular vendor should stick with the same vendor, assuming they are satisfied with quality, ease of use and support. Standardizing on similar equipment reduces compatibility issues and lowers the learning curve for administrators. SMBs that are looking for a change should consider Barracuda, Dell SonicWALL, Sophos and WatchGuard. For the enterprise, Check Point, Fortinet, Sophos and WatchGuard stand out among the competition.

About the author

Ed Tittel is a 30-plus year IT veteran who's worked as a developer, networking consultant, technical trainer, writer and expert witness. Perhaps best known for creating the Exam Cram series, Ed has contributed to more than 100 books on many computing topics, including titles on information security, Windows OSes and HTML. Ed also blogs regularly for TechTarget (Windows Enterprise Desktop), Tom's IT Pro, GoCertify and PearsonITCertification.com.

↘ Next article

In this e-guide

Check Point UTM Threat Prevention Appliances: Product review

David Strom

Check Point UTM Threat Prevention Appliances are recognized by our reviewer as consistent software architectures that are easy to configure.

The Check Point Software Next Generation Threat Prevention Appliances are the latest in a long line of security products from the vendor, whose brand is synonymous with firewalls. Check Point has one of the best united threat management, or UTM, approaches, providing solid products -- both for the high and low ends of the market -- with the essential features enterprises look for.

Product specs

Check Point Software Technologies Ltd. sells 17 different models of its rather oddly named Next Generation Threat Prevention Appliances. They have a range of 10 1 Gigabit Ethernet (GbE) ports on the smallest unit to 37 1 GbE and 13 10 GbE ports on the largest unit.

The rated firewall throughput of the devices ranges from 750 Mbps to 110 Gbps, which covers a lot of ground. Check Point also sells acceleration modules to push the higher-end rates to faster-rated throughputs.

Additionally, Check Point has a smaller model, called the UTM-1 Edge N Industrial Appliance, which runs the same software, but is designed for industrial Ethernet and SCADA environments. This is the latest version of a long line of Check Point UTM appliances that use the company's "software blade" architecture, which is a fancy way of saying it packages and bundles various features for network protection or Web-filtering appliances.

Understand Check Point software blades

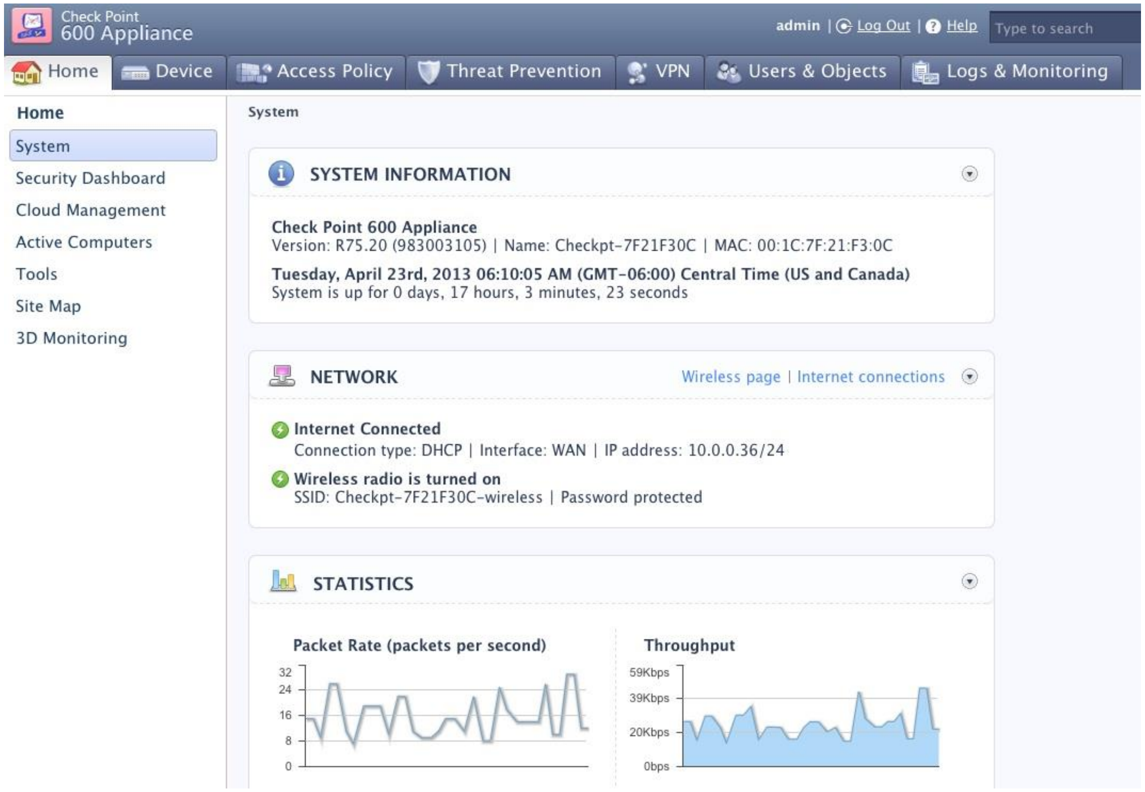
Check Point UTM appliances are offered with two different software packages -- Next Generation Threat Prevention and Next Generation Threat Extraction (NGTX).

Both packages include a firewall, VPN, intrusion prevention system (IPS), application control, antivirus, antibot, URL filtering, antispam and email security, advanced networking and clustering, identity awareness, mobile access, network policy management, and logging and status features. NGTX also includes threat emulation, or sandboxing, and threat extraction. Using threat extraction, exploitable content such as some embedded objects and active

In this e-guide

content is removed from infected documents, leaving a safe -- yet somewhat altered -- document.

Special features



Check Point 600 Appliance
Version: R75.20 (983003105) | Name: Checkpt-7F21F30C | MAC: 00:1C:7F:21:F3:0C

Tuesday, April 23rd, 2013 06:10:05 AM (GMT-06:00) Central Time (US and Canada)
System is up for 0 days, 17 hours, 3 minutes, 23 seconds

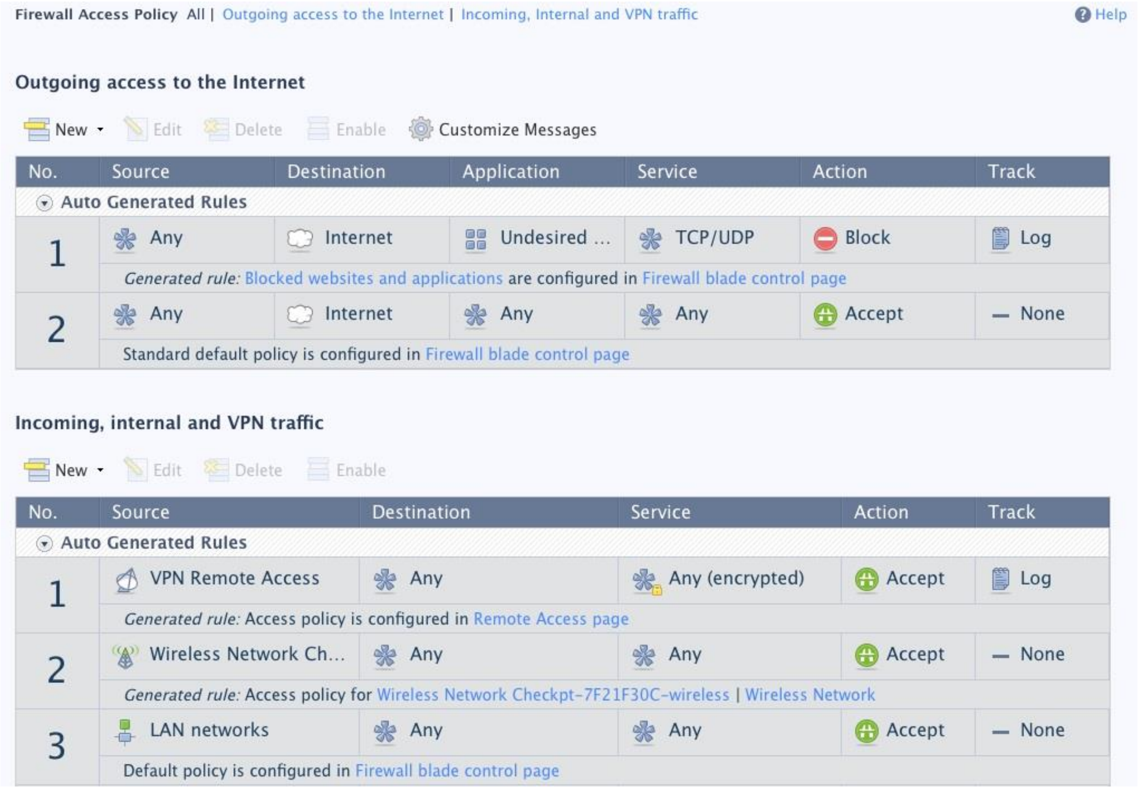
Internet Connected
Connection type: DHCP | Interface: WAN | IP address: 10.0.0.36/24

Wireless radio is turned on
SSID: Checkpt-7F21F30C-wireless | Password protected

One of the things I like about Check Point UTM products is that the software architecture is the same whether an organization buys a high-end box or a small office box. That consistency not only eases management, but also allows an organization to put more faith in the product as a whole. It also offers a leading-edge user interface that is clean, easy to understand, and has the best-looking and clearest menus of any of the boxes I have used. Its policy-creation tools are also straightforward, and it's easy to understand the inherent workflow -- unlike the tools on Juniper's SRX or Dell's SonicWALL. It also works well with mixed Mac and Windows networks.

By default, Check Point's appliance enables all of its ports on a single LAN switch, and you can define any port to be part of any network via its configuration software; so, it is quite flexible. For the smaller boxes that have an integrated wireless access port, organizations can set up multiple SSIDs for the wireless interface with just a single policy selection. This is the easiest wireless configuration of any of the boxes I have tested. Check Point seems to have tried to cover all of the bases in terms of features and functionality for a wide range of network sizes and use cases.

In this e-guide



Firewall Access Policy All | Outgoing access to the Internet | Incoming, Internal and VPN traffic
Help

Outgoing access to the Internet

New
Edit
Delete
Enable
Customize Messages

No.	Source	Destination	Application	Service	Action	Track
Auto Generated Rules						
1	Any	Internet	Undesired ...	TCP/UDP	Block	Log
	Generated rule: Blocked websites and applications are configured in Firewall blade control page					
2	Any	Internet	Any	Any	Accept	None
	Standard default policy is configured in Firewall blade control page					

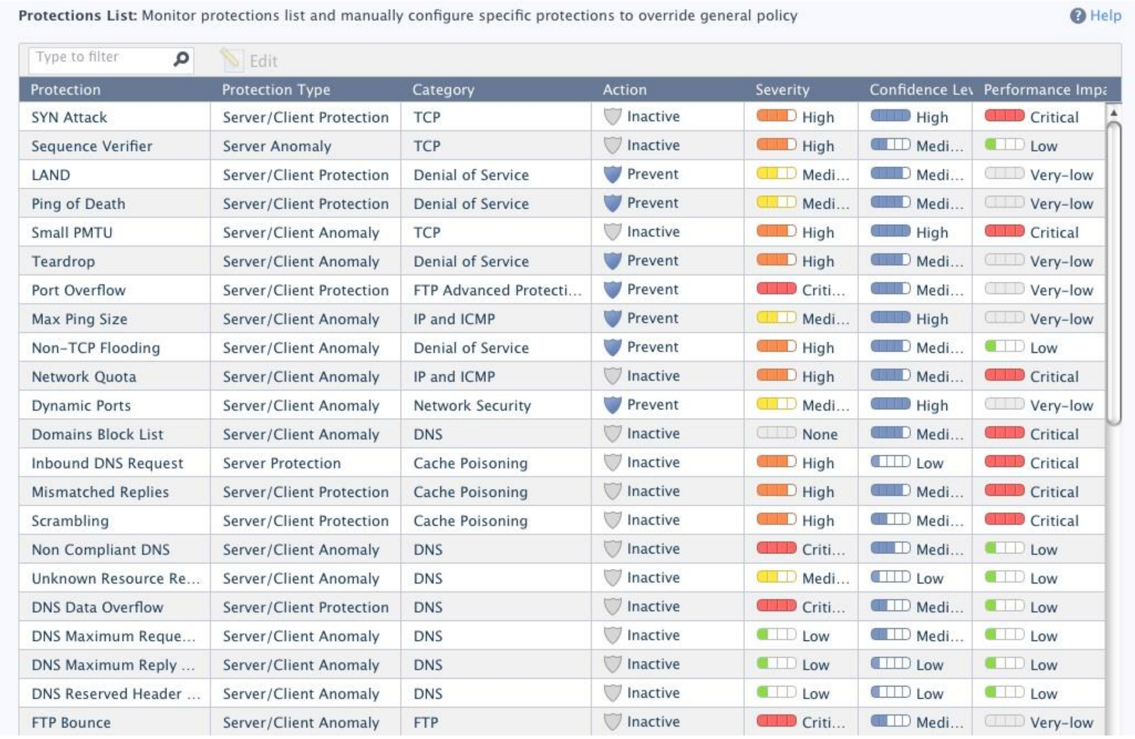
Incoming, internal and VPN traffic

No.	Source	Destination	Service	Action	Track
Auto Generated Rules					
1	VPN Remote Access	Any	Any (encrypted)	Accept	Log
	Generated rule: Access policy is configured in Remote Access page				
2	Wireless Network Ch...	Any	Any	Accept	None
	Generated rule: Access policy for Wireless Network Checkpt-7F21F30C-wireless | Wireless Network				
3	LAN networks	Any	Any	Accept	None
	Default policy is configured in Firewall blade control page				

Unlike Juniper, Check Point doesn't hide its advanced settings in a command-line interface. Instead, everything is accessible from its Web interface. If an enterprise needs extra features, such as setting up a failover link or changing the priority of a particular security policy, it isn't too hard to find the right menu option to accomplish the task.

Check Point also includes a connection to its Threat Cloud online reputation service-monitoring tool, allowing organizations to screen traffic for near real-time malware detection.

Performance



Protections List: Monitor protections list and manually configure specific protections to override general policy

Protection	Protection Type	Category	Action	Severity	Confidence Lev	Performance Impa
SYN Attack	Server/Client Protection	TCP	Inactive	High	High	Critical
Sequence Verifier	Server Anomaly	TCP	Inactive	High	Medi...	Low
LAND	Server/Client Protection	Denial of Service	Prevent	Medi...	Medi...	Very-low
Ping of Death	Server/Client Protection	Denial of Service	Prevent	Medi...	Medi...	Very-low
Small PMTU	Server/Client Anomaly	TCP	Inactive	High	High	Critical
Teardrop	Server/Client Anomaly	Denial of Service	Prevent	High	Medi...	Very-low
Port Overflow	Server/Client Protection	FTP Advanced Protecti...	Prevent	Criti...	Medi...	Very-low
Max Ping Size	Server/Client Anomaly	IP and ICMP	Prevent	Medi...	High	Very-low
Non-TCP Flooding	Server/Client Anomaly	Denial of Service	Prevent	High	Medi...	Low
Network Quota	Server/Client Anomaly	IP and ICMP	Inactive	High	Medi...	Critical
Dynamic Ports	Server/Client Anomaly	Network Security	Prevent	Medi...	High	Very-low
Domains Block List	Server/Client Anomaly	DNS	Inactive	None	Medi...	Critical
Inbound DNS Request	Server Protection	Cache Poisoning	Inactive	High	Low	Critical
Mismatched Replies	Server/Client Protection	Cache Poisoning	Inactive	High	Medi...	Critical
Scrambling	Server/Client Protection	Cache Poisoning	Inactive	High	Medi...	Critical
Non Compliant DNS	Server/Client Anomaly	DNS	Inactive	Criti...	Medi...	Low
Unknown Resource Re...	Server/Client Anomaly	DNS	Inactive	Medi...	Low	Low
DNS Data Overflow	Server/Client Protection	DNS	Inactive	Criti...	Medi...	Low
DNS Maximum Reque...	Server/Client Anomaly	DNS	Inactive	Low	Medi...	Low
DNS Maximum Reply ...	Server/Client Anomaly	DNS	Inactive	Low	Low	Low
DNS Reserved Header ...	Server/Client Anomaly	DNS	Inactive	Low	Low	Low
FTP Bounce	Server/Client Anomaly	FTP	Inactive	Criti...	Medi...	Very-low

Based on my previous testing of various Check Point UTM appliances, they deliver both the protection features, as well as the ease of configuration and use that enterprises would expect from a leading-edge UTM vendor.

But also note

The biggest issue for Check Point is its sheer number of different products. If you don't need every UTM security feature under the sun, you might be better off purchasing a more focused product that has fewer key features, such as a combination firewall and IPS. Equally complex is its support pricing. While its menus are clearly presented, there are some context changes on the left-hand menu when choosing top menu tabs that can be somewhat annoying at first.

Pricing

The price of the CheckPoint UTM-1 unit ranges from $1,175 to $3,150, depending on the number of users, and is sold as a bundle -- appliance and software, plus a one-year support contract. Pricing on all other units starts at $11,300 for the appliance and basic software modules, and can top $200,000 for the larger units. There are five different support packages, which include next business day or four-hour on-site response, along with next-day air shipments of replacement parts and other options. If an organization has a customer account with Check Point already, it can configure its appliance with the right collection of software and support services. Adding high-availability service will up the price tag significantly, too.

About the author

David Strom is a freelance writer and former editor in chief of several information technology publications. He has written for many TechTarget properties since 2000. His blog can be found at strominator.com and is @dstrom on Twitter.

Next article

Cisco Meraki MX appliances: UTM product overview

Ed Tittel

Expert Ed Tittel examines Cisco's Meraki MX UTM Appliances, a series of UTM products that combines various network security and protection features into a single device.

Cisco is the largest provider of network infrastructure products and services, catering to small and medium-sized businesses, as well as the largest of enterprises. Cisco's ISA500 series of integrated UTM products for small businesses reached its end of life in 2013, and is no longer sold. The company's current unified threat management offerings are Cisco Meraki security appliances, which are cloud-managed devices designed for SMBs, and are integrated with Sourcefire intrusion protection -- or contextual feeds.

Gartner's 2014 Magic Quadrant for Unified Threat Management lists Cisco as a challenger, along with Juniper Networks, to the UTM market leaders -- Fortinet, Check Point, Dell, Sophos and WatchGuard.

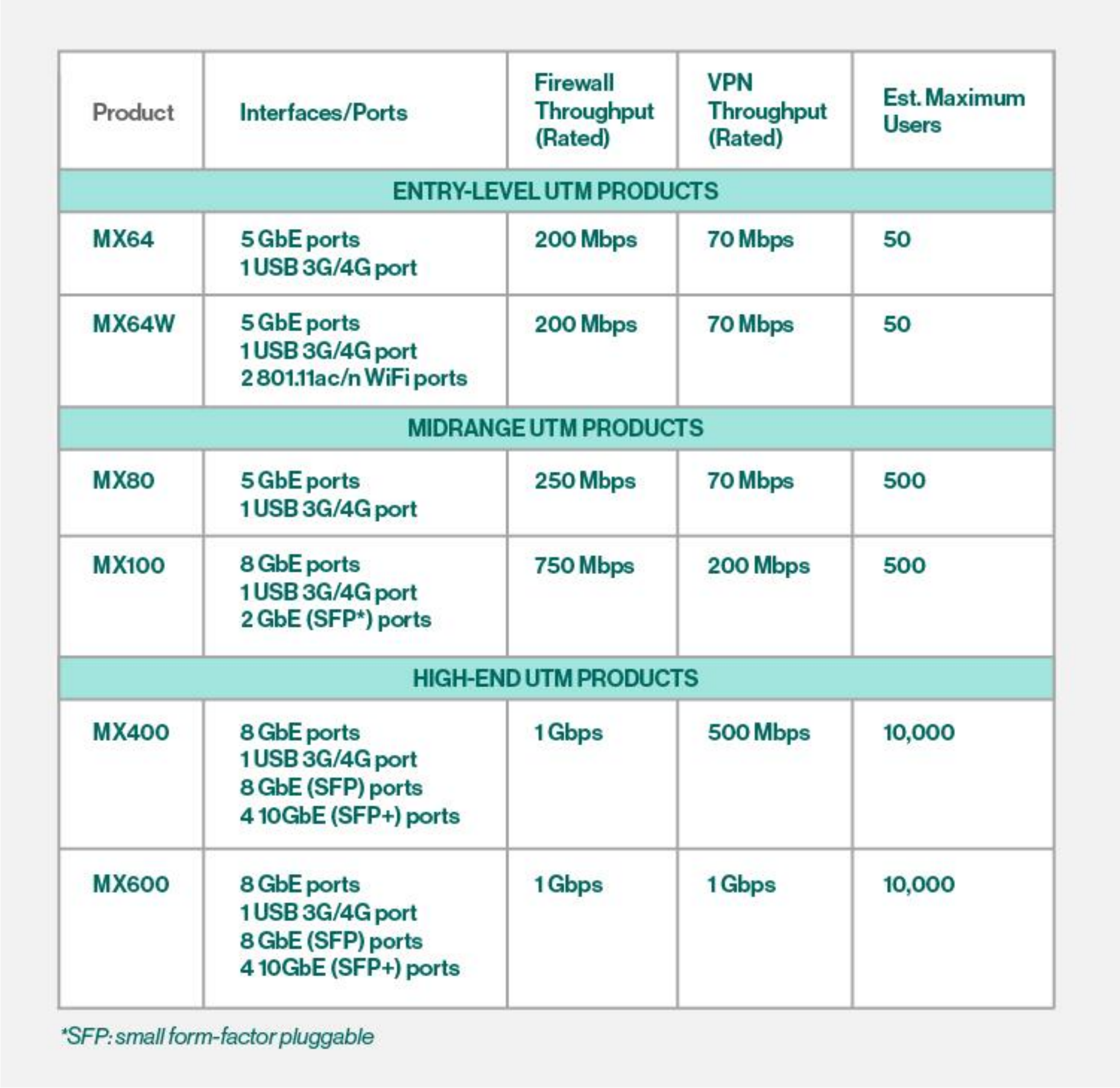
Product specs and performance

Six Cisco Meraki MX models are available as of this writing.

- Cisco recommends the MX64 models for small offices, the MX80 and MX100 for medium-sized offices, the MX400 for larger offices and the MX600 for campus environments.
- Cisco also sells the Meraki Z1 Teleworker Gateway, which includes a firewall, VPN client and 802.11n wireless access point for folks who work from home.

The number and type of interfaces, firewall and VPN throughput rates, and estimated maximum number of users are shown in the following table.

In this e-guide



Product	Interfaces/Ports	Firewall Throughput (Rated)	VPN Throughput (Rated)	Est. Maximum Users
ENTRY-LEVEL UTM PRODUCTS				
MX64	5 GbE ports 1 USB 3G/4G port	200 Mbps	70 Mbps	50
MX64W	5 GbE ports 1 USB 3G/4G port 2 801.11ac/n WiFi ports	200 Mbps	70 Mbps	50
MIDRANGE UTM PRODUCTS				
MX80	5 GbE ports 1 USB 3G/4G port	250 Mbps	70 Mbps	500
MX100	8 GbE ports 1 USB 3G/4G port 2 GbE (SFP*) ports	750 Mbps	200 Mbps	500
HIGH-END UTM PRODUCTS				
MX400	8 GbE ports 1 USB 3G/4G port 8 GbE (SFP) ports 4 10GbE (SFP+) ports	1 Gbps	500 Mbps	10,000
MX600	8 GbE ports 1 USB 3G/4G port 8 GbE (SFP) ports 4 10GbE (SFP+) ports	1 Gbps	1 Gbps	10,000

**SFP: small form-factor pluggable*

Product features

Cisco Meraki MX appliances include an application firewall, Web search and content filtering, intrusion prevention (SNORT) and Web caching, with integrated Kaspersky antivirus and antiphishing services.

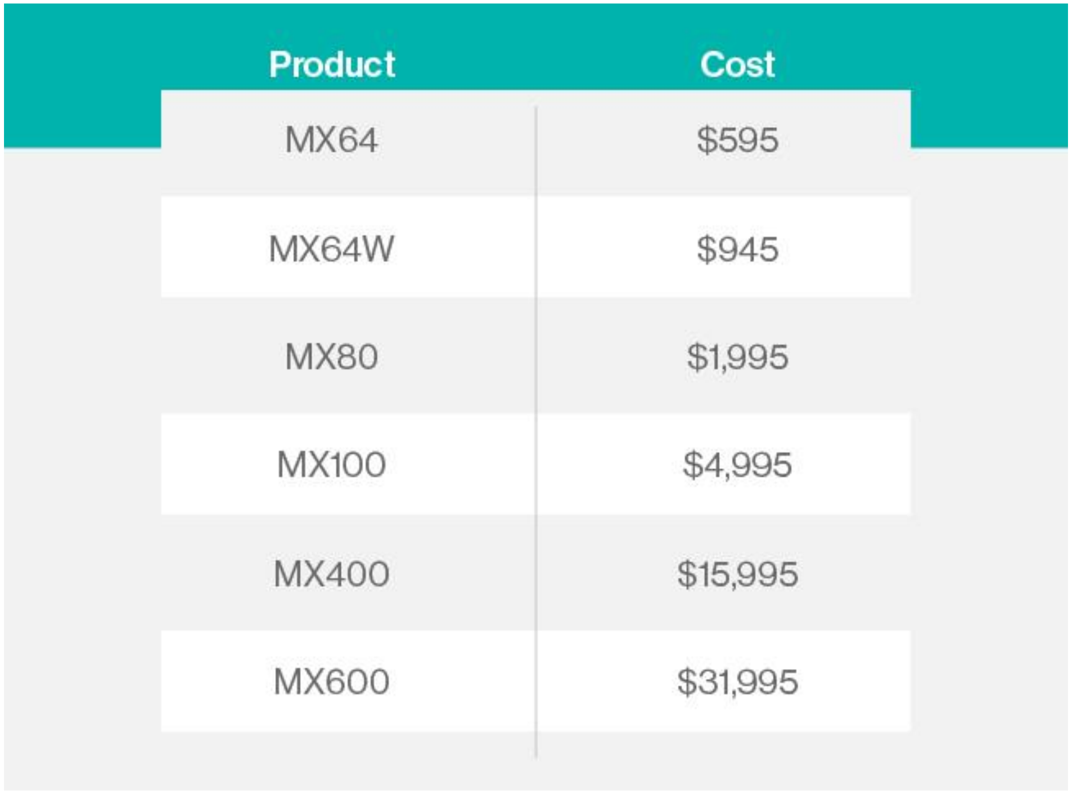
The site-to-site IPSec VPN supports Windows, Mac OS X, iOS and Android clients, but there is no SSL VPN available. Each model also provides identity-based security policies and application management, as well as "intelligent WAN" that has multiple WAN uplinks and 4G failover. The cloud-based centralized management console gives administrators a view of Meraki appliances, wireless access points and switches.

Unlike many competitors, Cisco Meraki MX appliances do not include email scanning or SSL decryption for HTTP.

Cisco lets customers and prospects try Cisco Meraki MX units on their own networks for free. Other testing options include free webinars by Meraki experts, which include live demonstrations, question and answer sessions, and a simulated demonstration of the Cisco Meraki cloud management platform via a Web browser.

Pricing and licensing

Cisco list prices are shown in the following table.



Product	Cost
MX64	$595
MX64W	$945
MX80	$1,995
MX100	$4,995
MX400	$15,995
MX600	$31,995

The Cisco Meraki MX UTM products use cloud-based management, and Cisco requires customers to purchase a license for the cloud on a per-device basis. The licensing tiers are Enterprise Edition and Advanced Security Edition, and each license is limited to a term of one to 10 years, depending on the selected license.

Licensing covers specific features and services used by the appliances; note that the Enterprise Edition license does not cover geography-based firewall rules, intrusion protection, content filtering, antivirus and antiphishing, or Web search filtering.

License prices vary by MX appliance. For example, a one-year Enterprise license lists for $300 for the MX64, and $16,000 for the MX600. An Advanced Security license is $600 and $32,000, respectively.

Support

Cisco provides full online documentation for installing and configuring Meraki security appliances. Enterprise-class support is included in both types of Meraki MX cloud licenses.

Organizations may very well find that UTM is the smart decision going forward.

In this e-guide

About the author

Ed Tittel is a 30-plus year IT veteran who's worked as a developer, networking consultant, technical trainer, writer and expert witness. Perhaps best known for creating the Exam Cram series, Ed has contributed to more than 100 books on many computing topics, including titles on information security, Windows OSes and HTML. Ed also blogs regularly for TechTarget (Windows Enterprise Desktop), Tom's IT Pro, GoCertify and PearsonITCertification.com.

➘ Next article

In this e-guide

Dell SonicWALL NSA UTM: Product overview

David Strom

Expert David Strom explains why the feature-rich Dell SonicWALL NSA Series of enterprise unified threat management devices may take some getting used to.

The Dell SonicWALL Network Security Appliance (NSA) Series could be considered one of the creators of the unified threat management (UTM) industry. Even though the market has evolved considerably since those early days, Dell still offers a very robust UTM product set, many of which are appropriate for enterprises.

Product specs

In this security product review, we look at all seven of the Dell SonicWALL NSA series models -- NSA 6600, NSA 5600, NSA 4600, NSA 3600, NSA 2600, NSA 250M and NSA 220 -- to fulfill the needs of various-sized businesses. Some models have 10 Gigabit Ethernet connectors, while others just have a single gigabit port. The rated firewall inspection throughput ranges from 600 Mbps to 12 Gbps, which may not be sufficient for larger network configurations.

The range of supported site-to-site VPN tunnels varies from 25 on the smallest unit to 6,000 on the largest box. While some models are relatively new, know that SonicWALL has been in the UTM business from the earliest days, practically creating the category before it was acquired by Dell.

Standard features

Each unit features a multi-core architecture that includes a firewall, virtual private network (VPN), intrusion prevention system (IPS), application control, network-based antimalware, gateway anti-spam, secure remote access and wireless, URL filtering and centralized management.

Market position

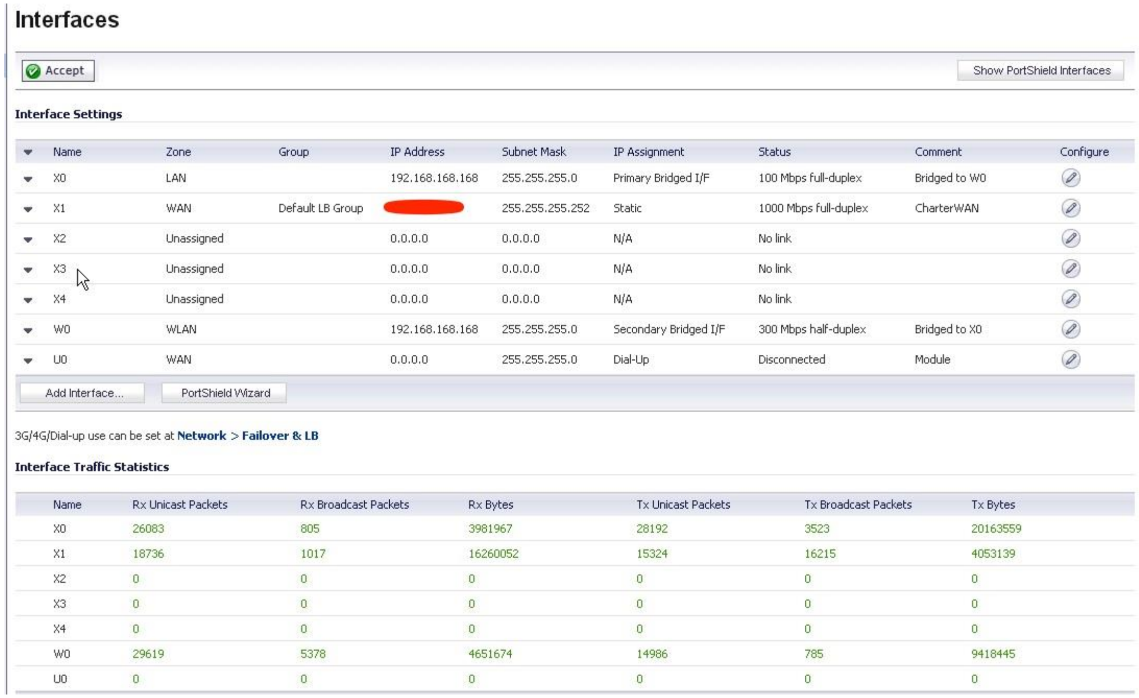
Dell was a UTM market leader in the early days, when it only sold small and midsize business units. However, as it grew to offer larger and more capable boxes, Dell has had a harder time adjusting its features and functions to the enterprise market. For example, it offers a confusing series of menu choices on enterprise-class devices that will take some work to sort out. There are also separate menus for protecting against SYN floods and distributed denial-of-service attacks that require adjusting a series of timeout and threshold parameters.

Special features

One nice feature of the Dell SonicWALL NSA series is there is no maximum file attachment size for the antimalware scanner since it looks at the entire packet as it streams by the box. Some of its competitors place email file attachments in memory before they are scanned.

The Dell SonicWALL NSA products come with each port set up independently, but enterprises can add what are called "PortShield groups" to turn a box into a single network switch. Organizations can also set up the box to automatically forward NetBIOS protocols across subnets (to make it easier to build a flat network to handle Windows file and printer sharing, for example).

In this e-guide



Interfaces

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Primary Bridged I/F	100 Mbps full-duplex	Bridged to W0	✎
X1	WAN	Default LB Group	[redacted]	255.255.255.252	Static	1000 Mbps full-duplex	CharterWAN	✎
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		✎
X3	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		✎
X4	Unassigned		0.0.0.0	0.0.0.0	N/A	No link		✎
W0	WLAN		192.168.168.168	255.255.255.0	Secondary Bridged I/F	300 Mbps half-duplex	Bridged to X0	✎
U0	WAN		0.0.0.0	255.255.255.0	Dial-Up	Disconnected	Module	✎

3G/4G/Dial-up use can be set at **Network** > **Failover & LB**

Interface Traffic Statistics

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Bytes
X0	26083	805	3981967	28192	3523	20163559
X1	18736	1017	16260052	15324	16215	4053139
X2	0	0	0	0	0	0
X3	0	0	0	0	0	0
X4	0	0	0	0	0	0
W0	29619	5378	4651674	14986	785	9418445
U0	0	0	0	0	0	0

Another great feature Dell offers is online demos of all of its products, so you can experience the product's user interface first-hand without going to the trouble of putting a test box in your environment. Additionally, setting up its high-availability feature is simple, with just a few checkboxes to select. Finally, SonicWALL supports deep packet inspection over SSL connections, something not every UTM offers.

But also note…

The two smallest Dell SonicWALL NSA units come with integrated wireless controllers; the larger units do not. Until recently, Dell supported only Windows SSL VPN connections, but has added Mac, IOS and Android clients, making it more in line with what competitors offer. Another potential issue is that unlike several of its competitors, some SonicWALL ports are tied to particular network zones and can't be changed via software configurations. This limits the cabling flexibility if you don’t have a switch in front of the UTM box.

Pricing

The smallest unit, SonicWALL NSA 220, is suitable for branch and small offices and starts at $1,095 for the basic software configuration, but can quickly rise beyond $1,700 when you add in the first year's subscriptions. The largest unit, NSA 6600, starts at $19,995, and subscriptions can add another $10,000 to the first year cost.

Dell also offers two categories of support available for an annual subscriptions: The Gold-level support is available on the larger units that provides 24x7 telephone access, and Silver-level support for the smaller units provides only daytime access. Both add about a third of the initial purchase price without any other options.

About the author

David Strom is a freelance writer and former editor in chief of several information technology publications. He has written for many TechTarget properties since 2000. His blog can be found at strominator.com and is @dstrom on Twitter.

Next article

In this e-guide

Fortinet FortiGate UTM: Product overview

Ed Tittel

Expert Ed Tittel looks at Fortinet FortiGate UTM appliances, which combine different network infrastructure protection features into a single device.

Fortinet has been in the network security appliance business since 2000 and is well known for its firewalls, network security access products and UTM offerings. Fortinet has been recognized as a market leader for UTM by Gartner since 2008, and IDC's Worldwide Quarterly Security Appliance Tracker report, released in March 2015, indicates Fortinet is the largest security appliance vendor in terms of total units shipped globally.

Product specs and performance

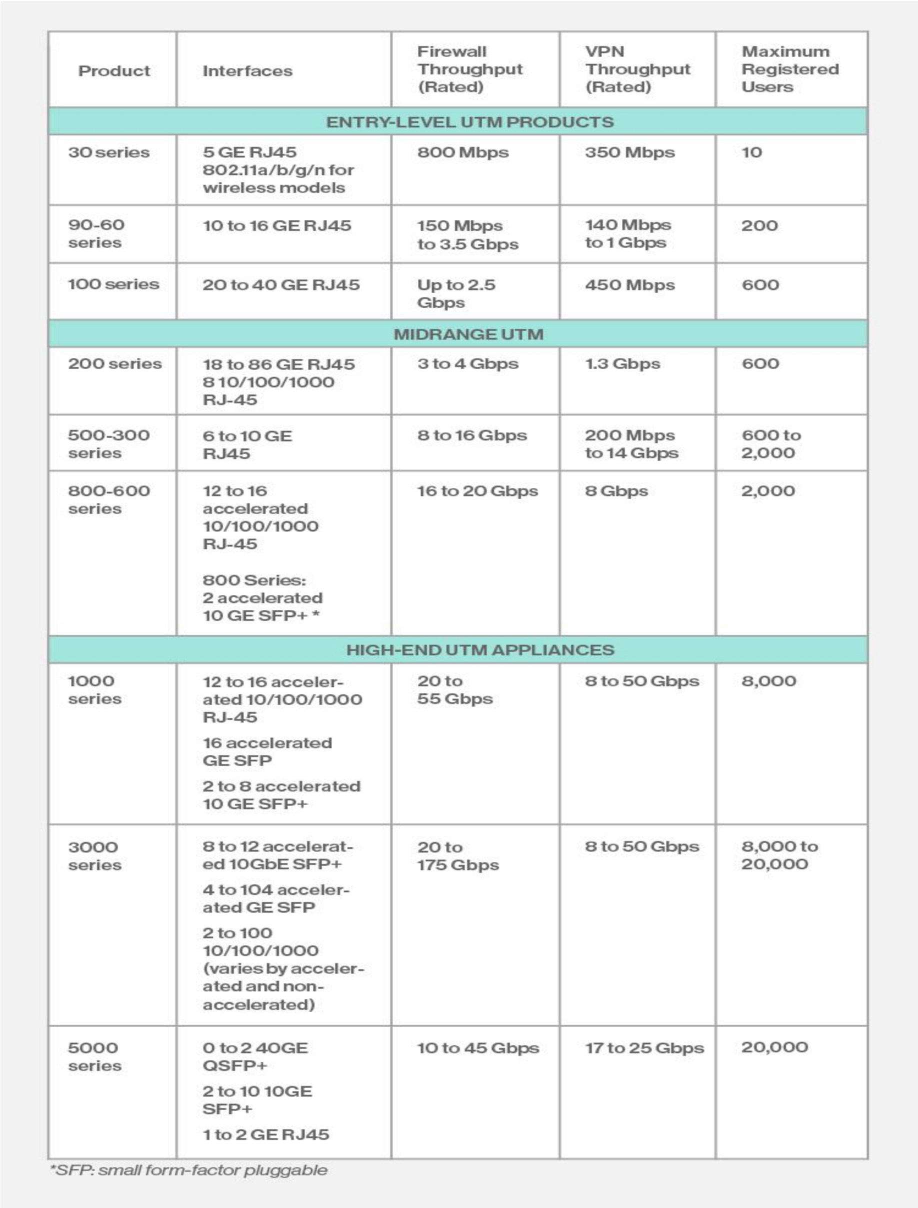
Fortinet sells over 40 FortiGate products, which include high-end and mid-range next-generation firewalls and entry-level unified threat management (UTM) appliances.

- Entry-level Fortinet FortiGate UTM appliances are designed for small offices and remote locations; the product line includes the 30 Series, 90-60 Series and the 100 Series.
- Fortinet's mid-range products include the 200 Series for branch offices, the 500-300 Series for branch offices and midsize organizations, and the 800-600 Series that supports enterprise campuses.
- The high-end FortiGate products are geared for data centers and multi-tenant cloud environments, and include the Fortinet FortiGate 1000, 3000 and 5000 Series appliances.

The following table lists the number and type of interfaces, firewall and VPN throughput, and maximum number of users per appliance.

* SFP stands for small form-factor pluggable.

In this e-guide



Product	Interfaces	Firewall Throughput (Rated)	VPN Throughput (Rated)	Maximum Registered Users
ENTRY-LEVEL UTM PRODUCTS				
30 series	5 GE RJ45 802.11a/b/g/n for wireless models	800 Mbps	350 Mbps	10
90-60 series	10 to 16 GE RJ45	150 Mbps to 3.5 Gbps	140 Mbps to 1 Gbps	200
100 series	20 to 40 GE RJ45	Up to 2.5 Gbps	450 Mbps	600
MIDRANGE UTM				
200 series	18 to 86 GE RJ45 8 10/100/1000 RJ-45	3 to 4 Gbps	1.3 Gbps	600
500-300 series	6 to 10 GE RJ45	8 to 16 Gbps	200 Mbps to 14 Gbps	600 to 2,000
800-600 series	12 to 16 accelerated 10/100/1000 RJ-45 800 Series: 2 accelerated 10 GE SFP+ *	16 to 20 Gbps	8 Gbps	2,000
HIGH-END UTM APPLIANCES				
1000 series	12 to 16 accelerated 10/100/1000 RJ-45 16 accelerated GE SFP 2 to 8 accelerated 10 GE SFP+	20 to 55 Gbps	8 to 50 Gbps	8,000
3000 series	8 to 12 accelerated 10GbE SFP+ 4 to 104 accelerated GE SFP 2 to 100 10/100/1000 (varies by accelerated and non-accelerated)	20 to 175 Gbps	8 to 50 Gbps	8,000 to 20,000
5000 series	0 to 2 40GE QSFP+ 2 to 10 10GE SFP+ 1 to 2 GE RJ45	10 to 45 Gbps	17 to 25 Gbps	20,000

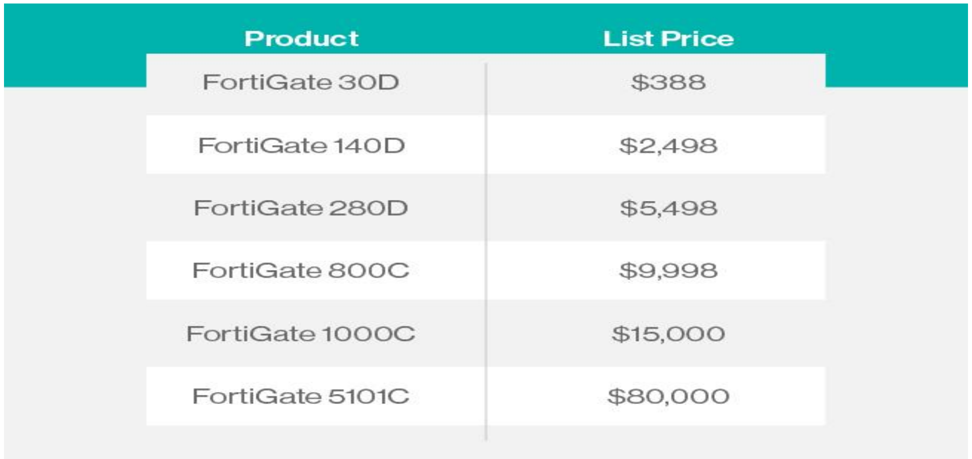
**SFP: small form-factor pluggable*

Product features

Every Fortinet FortiGate UTM appliance supports the same network security features: application control, advanced persistent threat protection, Web and content filtering, IP reputation, integrated WLAN controller, intrusion prevention system, data loss prevention and antimalware -- antivirus and antispam

Pricing and licensing

List prices for a sampling of Fortinet FortiGate UTM appliances are shown in the following table.



Product	List Price
FortiGate 30D	$388
FortiGate 140D	$2,498
FortiGate 280D	$5,498
FortiGate 800C	$9,998
FortiGate 1000C	$15,000
FortiGate 5101C	$80,000

Fortinet licenses UTM network security features, called FortiGuard, on a per-device basis; customers do not incur additional license costs if they add modules or users. UTM appliances are typically purchased with a FortiGuard bundle, which includes a standard FortiCare support plan.

At the low end, a Fortinet FortiGate 30D appliance and one-year FortiGuard bundle lists for $640, but jumps to about $3,300 for the FortiGate 100D.

For a mid-range environment, the cost of a FortiGate 800C appliance and one-year FortiGuard bundle license is about $16,500.

The cost of the Fortinet FortiGate 5101C appliance and the full FortiGuard UTM bundle costs approximately $130,000.

Support

Beyond the standard FortiCare support plan, customers can purchase FortiCare Premium Gold and Premium Global Gold support contracts. Key Gold-level services include a designated technical account manager (TAM), quarterly onsite visits, extended software support and enhanced service-level agreements -- priority service. The Global Gold plan includes the same services as the Gold plan, along with additional site visits and global TAM availability.

↘ Next article

Sophos SG Series UTM: Product overview

Ed Tittel

Expert Ed Tittel looks at the Sophos SG Series of unified threat management appliances, which bundle various kinds of network infrastructure protection into a single device.

While many people associate Sophos with antivirus software, the company also offers a bevy of UTM and next-gen firewall appliances, wireless access points and Web and email gateways.

The Sophos SG Series unified threat management (UTM) products are so good, in fact, that Gartner categorizes Sophos as a leader in the UTM market, at much the same level as WatchGuard, and trailing only behind UTM heavy-hitters Fortinet, Check Point and Dell.

Product specs and performance

The Sophos SG Series offers over 10 UTM models, covering small, midsize and large environments.

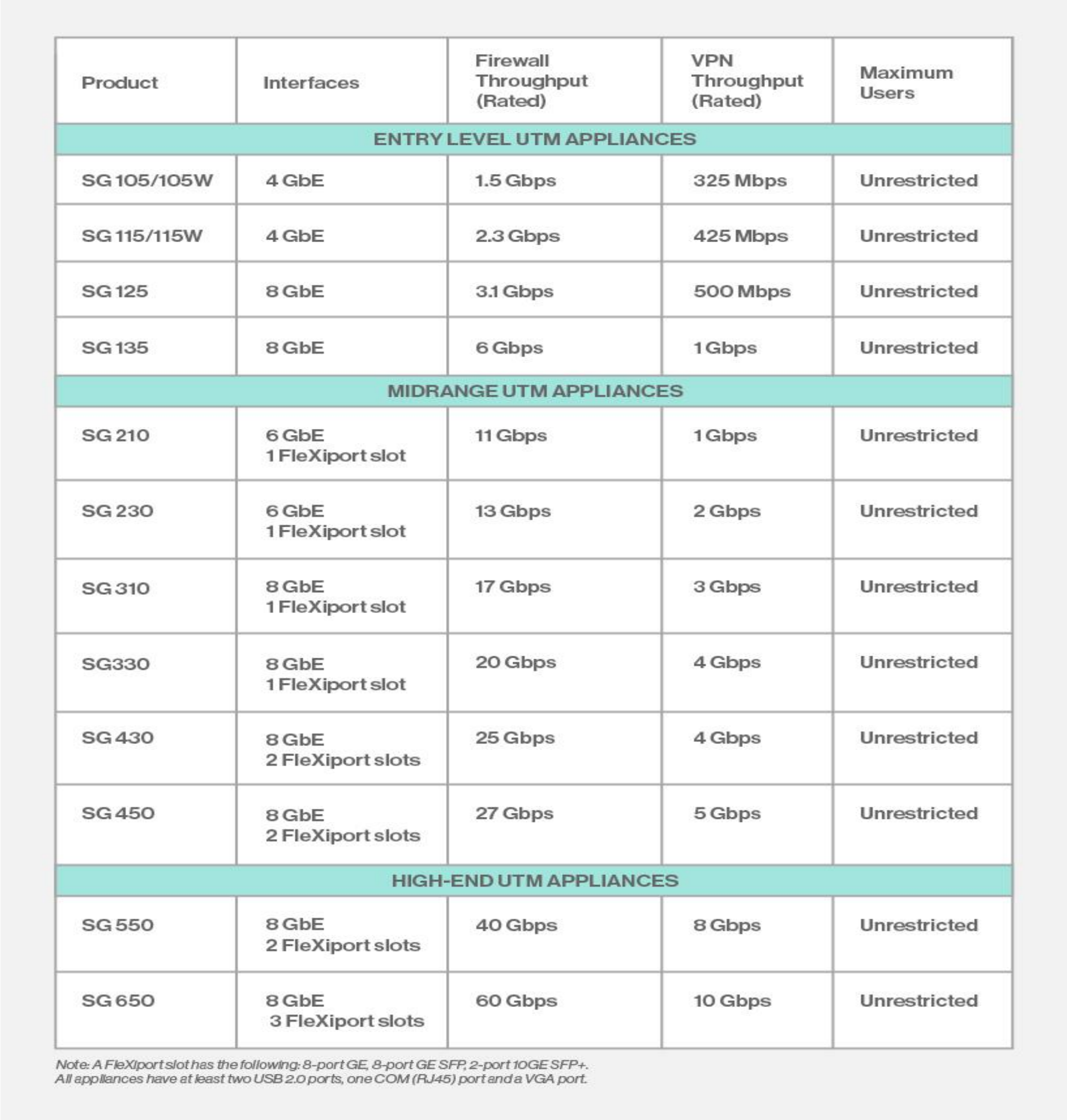
At the entry-level range are four models -- the SG 105W, SG 115W, SG 125 and SG 135 -- which are ideal for small offices, retail locations and the like. Only the "W" models include 802.11b/g/n 2.4 GHz wireless ports.

Midrange models include the SG 210, SG 230, SG 310, SG 330, SG 430 and SG 450, aimed at branch offices and similar environments.

At the high end of the series line are two models: the SG 550 and SG 650. These scalable appliances are suitable for midsize and distributed environments.

The following table lists the number and type of interfaces, firewall and VPN throughput rates, and number of users for each Sophos SG Series model.

In this e-guide



Product	Interfaces	Firewall Throughput (Rated)	VPN Throughput (Rated)	Maximum Users
ENTRY LEVEL UTM APPLIANCES				
SG 105/105W	4 GbE	1.5 Gbps	325 Mbps	Unrestricted
SG 115/115W	4 GbE	2.3 Gbps	425 Mbps	Unrestricted
SG 125	8 GbE	3.1 Gbps	500 Mbps	Unrestricted
SG 135	8 GbE	6 Gbps	1 Gbps	Unrestricted
MIDRANGE UTM APPLIANCES				
SG 210	6 GbE 1 FleXiport slot	11 Gbps	1 Gbps	Unrestricted
SG 230	6 GbE 1 FleXiport slot	13 Gbps	2 Gbps	Unrestricted
SG 310	8 GbE 1 FleXiport slot	17 Gbps	3 Gbps	Unrestricted
SG330	8 GbE 1 FleXiport slot	20 Gbps	4 Gbps	Unrestricted
SG 430	8 GbE 2 FleXiport slots	25 Gbps	4 Gbps	Unrestricted
SG 450	8 GbE 2 FleXiport slots	27 Gbps	5 Gbps	Unrestricted
HIGH-END UTM APPLIANCES				
SG 550	8 GbE 2 FleXiport slots	40 Gbps	8 Gbps	Unrestricted
SG 650	8 GbE 3 FleXiport slots	60 Gbps	10 Gbps	Unrestricted

Note: A FleXiport slot has the following: 8-port GE, 8-port GE SFP, 2-port 10GE SFP+.
All appliances have at least two USB 2.0 ports, one COM (RJ45) port and a VGA port.

Product features

Every Sophos SG Series UTM appliance has a high-speed hard disk or SSD to speed up access to reports and logs, and to store quarantined spam data. In larger environments, customers can create a dynamic cluster of appliances -- maximum of 10 -- without the need for load balancers.

- In addition, every appliance supports the same security modules:
- Network protection -- firewall, intrusion protection, other;
- Email protection -- antispam, data loss protection;
- Web protection -- filtering;
- Web server protection -- Web app firewall, reverse proxy, antivirus;
- Wireless protection -- wireless controller; and
- An optional endpoint protection module that covers Windows desktops and laptops.

Sophos provides its Sophos UTM Manager for managing appliances for free -- no licensing or subscription is required.

Each unit has built-in reporting functionality, which displays usage trends, daily summaries and log reports. Customers who need more detailed reports to meet compliance requirements can purchase Sophos iView, a separate appliance.

Pricing and licensing

The SG 105 appliance lists for $440.00; at the high end, the SG 650 lists for $18,995.

Customers must license each protection module they want to use. Modules are licensed individually or in a package, either FullGuard or TotalProtect. FullGuard and TotalProtect licenses cover all protection modules -- with the exception of endpoint protection, which is optional. TotalProtect also includes a Sophos support plan and the SG series appliance.

Individual license costs for protection modules vary by appliance. For example, a one-year Email Protection license for the SG 105 is $62, but jumps to $7,600 for the SG 650. A Network Protection license costs $42 for the SG 105 and $5,262 for the SG 650.

Prepackaged licenses offer a better deal. For example, a one-year FullGuard license for the SG 105 costs just under $200; the TotalProtect license is $638 -- SG appliance, all protection modules and 24/7 support.

A one-year FullGuard license for the SG 650 is about $23,600, and the TotalProtect license is $42,608.

Support

Sophos offers a free online knowledge base, documentation and community forums, as well as webinars and classroom training for a fee.

Sophos Standard support, which is included with Email, Network, Web, Wireless and Web Application Security licenses, includes phone support during normal business hours and 24-hour bring-in hardware replacement -- customer must ship the defective unit to Sophos at their own expense.

Premium support can be purchased separately, is part of the TotalGuard package and includes 24/7 support, software updates and 24-hour upfront hardware replacement --customer ships defective unit to Sophos; Sophos pays shipping costs.

Next article

WatchGuard UTM appliances: Product overview

Ed Tittel

Expert Ed Tittel examines WatchGuard UTM appliances that bundle different kinds of network infrastructure protection into a single device for small, midsize and large businesses.

WatchGuard Technologies provides UTM products, as well as next-generation firewalls, wireless access points with security modules, and a variety of virtual solutions. WatchGuard is a Gartner market leader for UTM, along with Fortinet, Check Point, Dell and Sophos.

Product specs and performance

There are more than 30 WatchGuard unified threat management (UTM) appliances aimed at organizations across the market spectrum, from home offices to large enterprises.

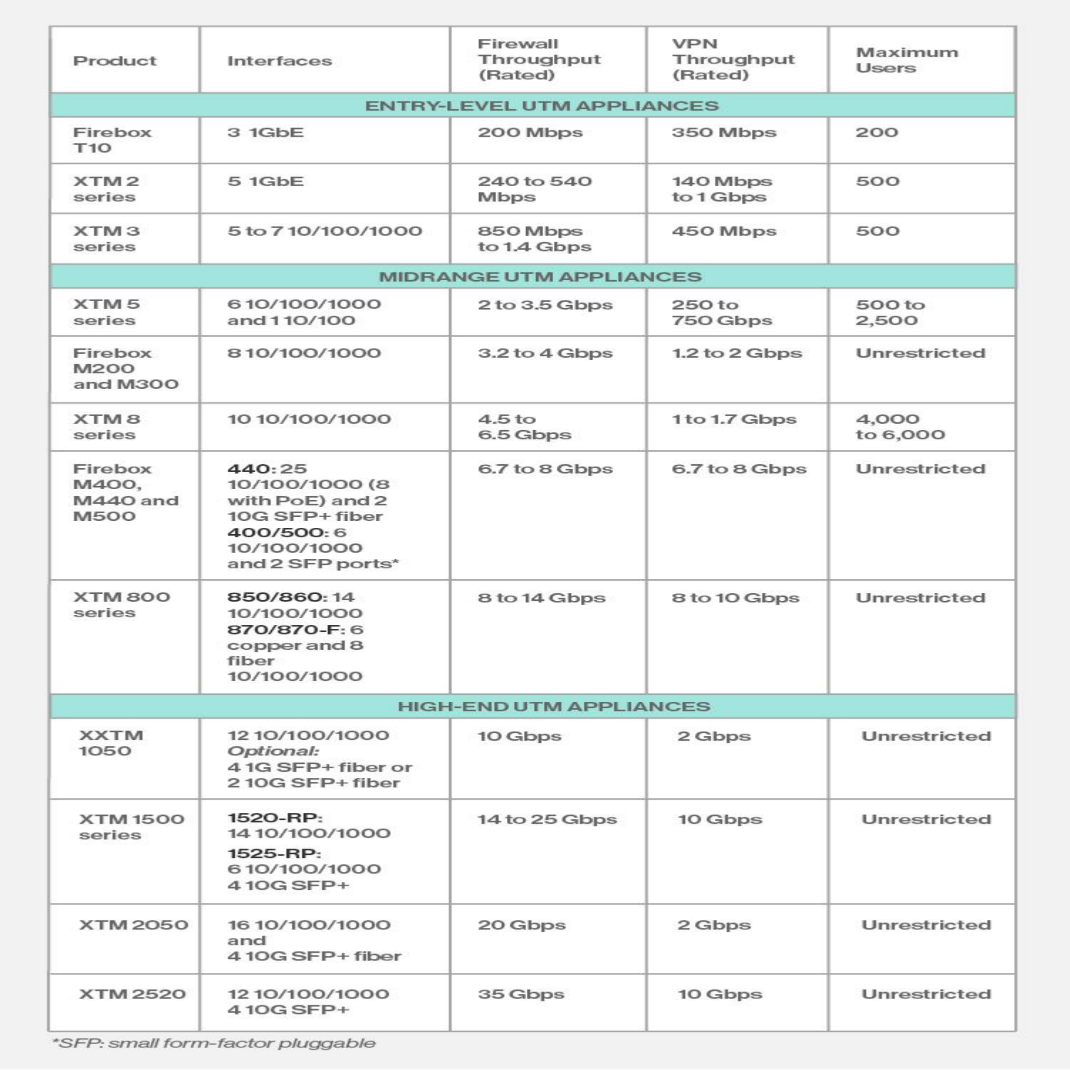
- At the entry level, there are three appliances/series: the WatchGuard Firebox T10, XTM 2 Series and XTM 3 Series. The Firebox T10 is geared

In this e-guide

toward small office/home office environments. The XTM 2 and XTM 3 are designed for small offices -- including branch and remote -- retail locations and wireless hotspots.

- Midrange WatchGuard UTM appliances, ideal for midsize to large organizations, include the XTM 5 Series, XTM 8 Series and the XTM 800 Series, as well as the Firebox M Series.
- At the high end are several appliances for the enterprise: the XTM 1050, XTM 1500 Series, XTM 2050 and XTM 2520.

The following table lists the number and type of interfaces, firewall and VPN throughput, and maximum number of users per appliance.



Product	Interfaces	Firewall Throughput (Rated)	VPN Throughput (Rated)	Maximum Users
ENTRY-LEVEL UTM APPLIANCES				
Firebox T10	3 1GbE	200 Mbps	350 Mbps	200
XTM 2 series	5 1GbE	240 to 540 Mbps	140 Mbps to 1 Gbps	500
XTM 3 series	5 to 7 10/100/1000	850 Mbps to 1.4 Gbps	450 Mbps	500
MIDRANGE UTM APPLIANCES				
XTM 5 series	6 10/100/1000 and 1 10/100	2 to 3.5 Gbps	250 to 750 Gbps	500 to 2,500
Firebox M200 and M300	8 10/100/1000	3.2 to 4 Gbps	1.2 to 2 Gbps	Unrestricted
XTM 8 series	10 10/100/1000	4.5 to 6.5 Gbps	1 to 1.7 Gbps	4,000 to 6,000
Firebox M400, M440 and M500	**440:** 25 10/100/1000 (8 with PoE) and 2 10G SFP+ fiber **400/500:** 6 10/100/1000 and 2 SFP ports*	6.7 to 8 Gbps	6.7 to 8 Gbps	Unrestricted
XTM 800 series	**850/860:** 14 10/100/1000 **870/870-F:** 6 copper and 8 fiber 10/100/1000	8 to 14 Gbps	8 to 10 Gbps	Unrestricted
HIGH-END UTM APPLIANCES				
XXTM 1050	12 10/100/1000 *Optional:* 4 1G SFP+ fiber or 2 10G SFP+ fiber	10 Gbps	2 Gbps	Unrestricted
XTM 1500 series	**1520-RP:** 14 10/100/1000 **1525-RP:** 6 10/100/1000 4 10G SFP+	14 to 25 Gbps	10 Gbps	Unrestricted
XTM 2050	16 10/100/1000 and 4 10G SFP+ fiber	20 Gbps	2 Gbps	Unrestricted
XTM 2520	12 10/100/1000 4 10G SFP+	35 Gbps	10 Gbps	Unrestricted

**SFP: small form-factor pluggable*

WatchGuard also offers four XTM virtual appliances for small, medium and large offices, and a model designed for data centers. These virtual appliances include a firewall, application proxies, intrusion prevention, Voice over Internet Protocol and security subscriptions for application control, antivirus and so on -- see the Product features section below.

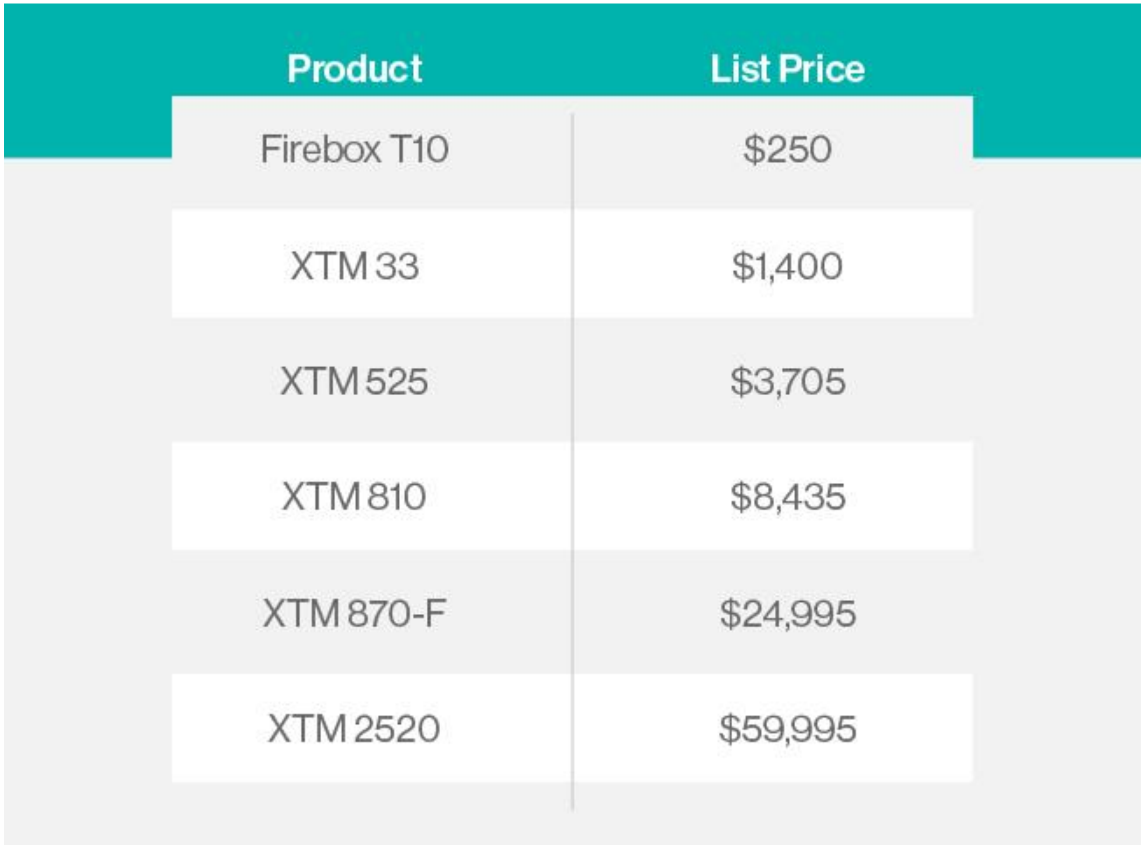
Product features

Each appliance supports a standard set of software security modules: packet filtering, intrusion prevention service, application control, WebBlocker -- content and URL filtering -- gateway antivirus, spam blocker and reputation-enabled defense. Customers can also get data loss prevention and advanced persistent threat blocker modules, which are optional.

Pricing and licensing

List prices for a sampling of WatchGuard UTM appliances are shown in the following table.

In this e-guide



Product	List Price
Firebox T10	$250
XTM 33	$1,400
XTM 525	$3,705
XTM 810	$8,435
XTM 870-F	$24,995
XTM 2520	$59,995

In addition, WatchGuard sells subscriptions for the security software modules for UTM appliances, either individually or as a suite. For example, a one-year subscription for the standard security suite costs $170 for the Firebox T10 and

$24,995 for the XTM 870-F. Bundles are also available, in which the appliance and security suite can be purchased at a cost savings.

Support

Every WatchGuard UTM appliance includes a 90-day LiveSecurity subscription, which includes software updates, alerts and hardware replacement, among other services. Customers can purchase a subscription to Standard, Plus (24/7), Gold or Premium for ongoing support.

Support subscriptions are based on one- and three-year terms, and vary by UTM appliance. For example, the list price for a one-year subscription to WatchGuard LiveSecurity with 24/7 support for the Firebox T10 is $55, but jumps to $4,445 for the XTM 870-F.

About the author

Ed Tittel is a 30-plus year IT veteran who's worked as a developer, networking consultant, technical trainer, writer and expert witness. Perhaps best known for creating the Exam Cram series, Ed has contributed to more than 100 books on many computing topics, including titles on information security, Windows OSes and HTML. Ed also blogs regularly for TechTarget (Windows Enterprise Desktop), Tom's IT Pro, GoCertify and PearsonITCertification.com.