SOPHOS

Network protection and UTM Buyers Guide

Using a UTM solution for your network protection used to be a compromise—while you gained in resource savings and ease of use, there was a payoff in terms of protection capabilities. Now, network protection through a UTM solution gives you the best of both worlds. You can enjoy the highest standards of network security, plus the ability to integrate multiple security capabilities within a single platform. Add security capabilities as you need them, when you need them.

This buyers guide is designed to help you choose the right solution for your organization. It looks at the factors you should consider when evaluating solutions to ensure you have the protection and functionality you need, both now and as your business evolves.

How to use this guide

This guide details the capabilities to look for when evaluating security solutions. It's separated into individual protection areas—network, web, email, etc.—for ease of of use. It also includes suggested questions to ask your vendors to help you identify which solution best meets your requirements.

At the end of the document is a product comparison check list. Some of the data is already supplied and you can also add in additional requirements you may have to meet the needs of your organization.

What is UTM?

Unified threat management (UTM) is a suite of security software integrated into a single platform, upholding consistent security policies and protection across the organization. You choose which security elements you use, and manage them all through a single platform with a centralized management console.

According to Gartner*, UTM products need to provide the following functions as a minimum:

- Standard network stateful firewall functions
- Remote access and site-to-site virtual private network (VPN) support
- Web-security gateway functionality (anti-malware, URL and content filtering)
- Network intrusion prevention focused on blocking attacks against unpatched Windows PCs and servers

When reviewing UTM solutions, there are two things you should consider.
Think of the overall benefits offered by the UTM approach, as well as how the individual network security features meet your specific requirements.

Next-generation firewalls (NGFW)

Right now, next-generation firewalls are a hot topic. Many vendors vary in their description of exactly what constitutes a NGFW. However, there is widespread agreement that, in essence, a NGFW goes beyond a traditional firewall, protecting organizations in a world where everything is about the web.

The four core features of a NGFW are:

1. Application visibility and control
2. Optimizing the use of the internet connection(s)
3. Clear, understandable Intrusion Prevention Systems (IPS)
4. Seamless VPN for connecting to remote sites and allowing access for remote users

Many UTM solutions offer NGFW capabilities. It's important is to understand what you need to do, so you can evaluate solutions against your requirements.

* 2012 Gartner Magic Quadrant for Unified Threat Management

Evaluating solutions: security features

Network protection

Cyber-criminals are continually changing their attack methods to avoid detection. The best way to protect the network against these new and emerging threats is through multiple layers of defense.

A UTM product should provide a solid network security foundation even before you add network protection subscriptions or licenses. At a basic level UTM should include static routing, DNS proxy services, DHCP server options, NTP functionality, stateful firewall, network address translation, basic remote access VPN, local user authentication, local logging and daily reports and basic management functionality.

Capability to look for	Description	Questions to ask your vendor
IPS	Bolsters your firewall's security policy by inspecting approved traffic for malicious packets. Can drop packets that match a signature list of threat patterns.	‣ What kind of expertise is needed to properly use the system? ‣ How are rules delivered and configured?
Bandwidth control/ Quality of service	Prioritizes traffic based on the rules you set and allows you to control how a fixed resource is used during different conditions.	‣ How many WAN connections can you support on a single appliance? ‣ How easy is it to identify and control the bandwidth applications use?
Site-to-site VPN options	Links remote sites with the main office, allowing users to send and receive information via a secure connection. Also allows employees to use devices such as file servers and printers that are not in the same office.	‣ What protocols does your VPN support? ‣ How much experience or VPN knowledge is required to set up a VPN?
Remote access options	Allows users to securely connect to the UTM appliance from any location.	‣ Do you offer multiple remote access options including clientless VPN? ‣ Is remote access supported from any OS and/or device? ‣ Is the clientless VPN truly clientless or are applets required on end-user devices? ‣ Are additional licenses required?
Remote office support	Connects remote office networks to the UTM appliance to protect them with the same policies and capabilities.	‣ How easy is it to connect remote offices? ‣ technician required? ‣ Can remote offices be centrally managed? ‣ Are additional subscriptions or licenses needed?
Detailed reports	Provides detailed real-time and historical statistics and reports on network/bandwidth usage, network security, etc.	‣ Does the UTM contain a built-in hard drive? ‣ What kind of reports are available without a separate application?

Web protection

You may already block access to potentially dangerous URLs with a web filter. But many filters inspect traffic from the sidelines, providing little if any malware scanning.

You need web protection that allows you to apply terms and conditions to where and how users spend their time online, and stops spyware and viruses before they can enter the network. Detailed reports should show you how effective your policy is so you can make adjustments.

Capability to look for	Description	Questions to ask your vendor
URL filtering	Controls employee web usage to prevent casual surfing and to keep inappropriate content and malware off the network.	‣ Are live updates available? ‣ How many web surfing profiles can be created and used?
Spyware protection	Prevents malicious software from installing on employees' computers, consuming bandwidth and sending sensitive data out of the network.	‣ Are live updates available?
Antivirus scanning	Scans content before it enters the network to prevent viruses, worms and other malware from infecting computers on the network.	‣ Are live updates available?
HTTPS scanning	Provides visibility into encrypted web traffic to protect the network against threats that can be transmitted via HTTPS.	‣ Can HTTPS traffic be inspected and checked against policies?
Application control	Provides visibility into how employees are using the web and controls which applications they can use and how.	‣ Are live updates available?
Interactive web reporting	Provides flexible reporting capabilities to allow administrators to build their own reports.	‣ Are real-time and historical usage reports available? ‣ Can reports be scheduled for delivery? ‣ Is a third-party reporting application required?

Next-generation firewall protection

NGFW is an evolution of the traditional port-based protections used in most network security approaches. Rather than simply allowing traffic through on ports like HTTP or HTTPS, NGFWs have application signatures that can identify traffic on a much more granular level. For example, administrators can choose to block Facebook Messaging while still allowing access to Facebook.

NGFWs also do deep packet inspection at a high speed, identifying and blocking exploits, malware and other threats with high levels of precision. Because many attacks are now web-based, traditional firewalls filtering only by port are of limited effectiveness in defending you against these threats.

A NGFW also allows organizations to be more strategic by prioritizing their network usage with powerful shaping rules. For example, you can choose to allow VOIP phone calls or prioritize Salesforce.com traffic while the throughput or blocking outright applications like Bittorrent.

Capability to look for	Description	Questions to ask your vendor
Application visibility and control	Having visibility of the applications being used enables you to make educated decisions about what to allow, what to prioritize and what to block. So your bandwidth is used to best effect and you don't waste time blocking applications that aren't a problem.	‣ Can you prioritize and control access to applications and see in real-time how your Internet connection is being used, and by whom? ‣ How easy is it to set a policy from a live view of your current activity?
Optimizing the use of the internet connection(s)	Bandwidth is a limited commodity and you need to make sure that you make best use of it, like ensuring business-critical applications like salesforce.com have priority.	‣ How easy is it to shape bandwidth? ‣ Do you have a Quality-of-Service (QoS) toolkit?
Clear, understandable IPS	Many web-based attacks are now able to masquerade as legitimate traffic. Effective IPS enables you to see what web traffic actually does, rather than just what it is.	‣ How easy it is to manage IPS? ‣ What level of expertise is required – for example, do you need to understand different types of threats?
Seamless VPN for remote connections	Remote and mobile working are becoming increasingly common. Organizations need quick, easy and secure VPN so users can connect to the network and be productive from any location.	‣ How easy is it to set up client VPNs for your remote workers? ‣ Which devices can you use to connect to the network? ‣ Do you offer a clientless HTML5 solution?

Email protection

Protecting email against spam and viruses isn't a new problem. But, email security threats continually evolve, making email protection a full-time job that never ends. You need email protection so that common email problems like spam, viruses and the leaking of confidential information don't affect your business.

Capability to look for	Description	Questions to ask your vendor
Anti-spam	Stops spam and other unwanted email from being delivered to employees' inboxes.	‣ What are your spam detection and false positive rates? ‣ What techniques do you use to identify spam?
Antivirus scanning	Scans and blocks malicious content at the gateway to stop viruses and other malware from infecting computers.	‣ How many antivirus engines does your solution use? ‣ How often does your solution scan content?
Email encryption	Renders email illegible to prevent eavesdroppers and other unintended recipients from obtaining sensitive and confidential information.	‣ What does a user have to do to encrypt and decrypt email? ‣ How is encryption managed?
User portal	Gives employees control over their email, including spam quarantine and message activity.	‣ Can end users handle their own email quarantine?

Webserver protection

Every weakness in your web application is exposed when you connect a server to the Internet. And securing each and every configuration and line of code is probably out of the question.

Webserver protection stops hackers from using attacks like SQL injection and cross-site scripting from stealing sensitive information like credit card data and personal health information. And it should help you achieve regulatory compliance when a web application firewall is required.

A web application firewall scans activity and identifies attempts to exploit web applications, preventing network probes and attacks.

Capability to look for	Description	Questions to ask your vendor
Form hardening	Inspects and validates the information submitted by visitors via forms on your websites. Prevents invalid data from damaging or exploiting your server as it is processed.	‣ Is a complete form analysis performed? ‣ Can the system detect tampered forms?
Antivirus scanning	Scans and blocks malicious content at the gateway to stop viruses and other malware from infecting computers.	‣ How many antivirus engines does your solution use? ‣ How often does your solution scan content?
URL hardening	Prevents your website visitors from accessing content they aren't allowed to see.	‣ Do I have to enter the structure of my website manually, or can it be done automatically with dynamic updates?
Cookie protection	Protects from tampering the cookies given to your website visitors.	‣ Does the system protect my ecommerce site against manipulation of product prices?

Wireless protection

Wireless networks require the same security policies and protection as the main corporate network. Unfortunately, they are often operated by network administrators as two separate networks. Wireless protection from your UTM vendor should reduce if not eliminate the problem of enforcing consistent security policies across your organization.

Make sure your wireless protection extends UTM security features to your wireless networks. And it should provide a way for you to centrally manage the wireless network. Protect your network and data equally, regardless of whether your employees are plugged in or accessing the network over the air.

Capability to look for	Description	Questions to ask your vendor
Plug-and-play deployment	Provides fast and simple set-up because access points are configuration-less.	‣ How long does it take to set up and deploy access points and policies?
Central management	Simplifies management of the wireless network by centralizing configuration, logging and troubleshooting within a single console.	‣ Do I have to configure the access points one-by-one in the local GUI or command line?
Integrated security	Offers instant protection to all wireless clients through complete UTM security.	‣ Can all wireless traffic be forwarded directly to the security gateway?
WPA/WPA 2 encryption options	Enterprise-level encryption that prevents data loss and theft by rendering data illegible to unauthorized recipients.	‣ Are multiple encryption and authentication methods supported? ‣ Is an interface to my RADIUS server available?
Guest Internet access	Protects multiple wireless zones, each with different authentication and privacy settings. Enables and supports wireless hot spots.	‣ How many different wireless network zones are supported? ‣ What type of hot spots are supported? ☐ terms-of-use acceptance ☐ password of the day ☐ voucher-based
Detailed reporting	Provides information about connected wireless clients and network usage.	‣ Is there built-in reporting? ‣ Is a separate tool required for reports?

Endpoint protection

Your corporate network grows and changes every time a laptop or mobile device connects to it. To maintain a secure network, you need endpoint protection that checks connecting devices for current updates and security policies.

Your endpoint protection also needs to protect company-owned devices on and off the network. Reduce your management effort and save money by integrating your endpoints directly into your UTM appliance. This also helps to achieve regulatory compliance when different antivirus engines are running at the gateway and on the endpoint.

Capability to look for	Description	Questions to ask your vendor
Ease of deployment	Gives the organization the ability to easily deploy and manage endpoint clients to prevent malware and data loss.	‣ How is the endpoint client deployed?
Antivirus scanning	Scans the endpoint for viruses and other malware to prevent it from entering the network.	‣ How many different antivirus engines are used? ‣ Does the solution provide live updates via the cloud?
Device control	Allows the organization to prevent the use of modems, Bluetooth, USB ports, CD/DVD drives, etc.	‣ What devices can be controlled through your solution? ‣ Does endpoint protection only work if endpoints are in the domain or connected through a VPN tunnel?
Real-time reporting	Provides visibility into endpoints with up-to-date statistics.	‣ Is real-time reporting built in?

Comparing UTM solutions

When comparing UTM solutions there are a number of factors you should consider alongside individual security features.

Specific needs of your organization

At a minimum, a UTM product should provide stateful firewall functionality, VPN support (both site-to-site and remote user), web security (content filtering and malware protection) and network intrusion protection (IPS).

You should also consider any specific security requirements for your organization. Do you have remote offices? If so, consider how you can securely connect them. If performance and fail-over are important, you should look into the ability to have Active/Active clusters.

Ease-of-use

UTM solutions by their nature help reduce day-to-day IT administrative time and effort. However, the level of resource savings will vary depending on how easy the solution is to use. Consider both the initial start-up period, and also regular activities that your IT teams and your staff perform.

Future-proofing your security

When reviewing solutions you should also consider how your business needs may change in the future. Even if you don't want to use all the protection options available at the start, you may need to add additional features as your business and security requirements evolve. If you don't know what features you'll need in the future it's wise to choose a UTM with a consistent feature set across all models.

Also consider deployment models. A hardware appliance may be a good fit for your organization today. But it may not be the best option as you extend to the cloud. Don't forget to also consider your current and future plans to use virtualization and cloud technologies.

Side-by-side comparision

Use our Product Comparison checklist on the next page to see which solution best meets your specific needs.

Conclusion

By focusing on the checklists in this buyers guide and working closely with your vendor, you can find a UTM product that provides the protection you need now and in the future. So you get network threat protection with less effort, less complexity and for less money.

United Kingdom and Worldwide Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

bg.04.13V2

SOPHOS

Product comparison checklist

Use this table to evaluate different solutions. Some of the data is already supplied. You can also add any additional requirements you may have to meet the specific needs of your organization. Then use the questions earlier on in the guide to help you identify the right solution for you.

Feature	SOPHOS UTM	SONICWALL NSA	WATCH GUARD XTM	FORTINET Fortigate	CHECK POINT UTM-1
CORE SECURITY					
Firewall	✓	✓	✓	✓	✓
Concurrent, independent AV Engines	2	1	1	1	1
Integrated Endpoint Protection	✓	Limited	Limited	✓	Limited
NEXT-GENERATION PROTECTION TECHNOLOGIES					
Web Application Firewall	✓				✓
Web Application Control	✓	✓	Larger models	✓	✓
Intrusion Protection System	✓	✓	✓	✓	✓
Filtering of HTTPS data	✓	Limited	Larger models	Limited	
CONNECTING USERS/ REMOTE OFFICES					
IPSec & SSL VPN	✓	✓	Limited	Limited	✓
HTML5 VPN portal	✓				
Wireless mesh networks	✓			✓	✓
Enduser self service portal	✓				
Plug and Protect Remote Office security (RED)	✓				
EASE OF DEPLOYMENT AND USE					
Choice of Hardware, Software Virtual or Cloud deployment	✓				✓
Default Reporting – for day-to-day performance review	1000s	Few	Few	Few	Few
Software version runs on standard Intel hardware	✓				✓
Zero-configuration high availability hardware appliance	✓				
Free central UTM manager (for managing multiple appliances centrally)	✓				
Active/Active Cluster with integrated load balancing	✓	✓	Limited	Larger models	✓
Gartner Magic Quadrant for UTM	Leader	Leader	Leader	Leader	Leader
LICENSING AND SUPPORT					
Consistent feature set on all models	✓				
Ability to add additional license modules as and when required	✓	✓	✓	Larger models	Larger models
Multiple technical support options	✓	✓	✓	✓	✓
ADDITIONAL REQUIREMENTS					