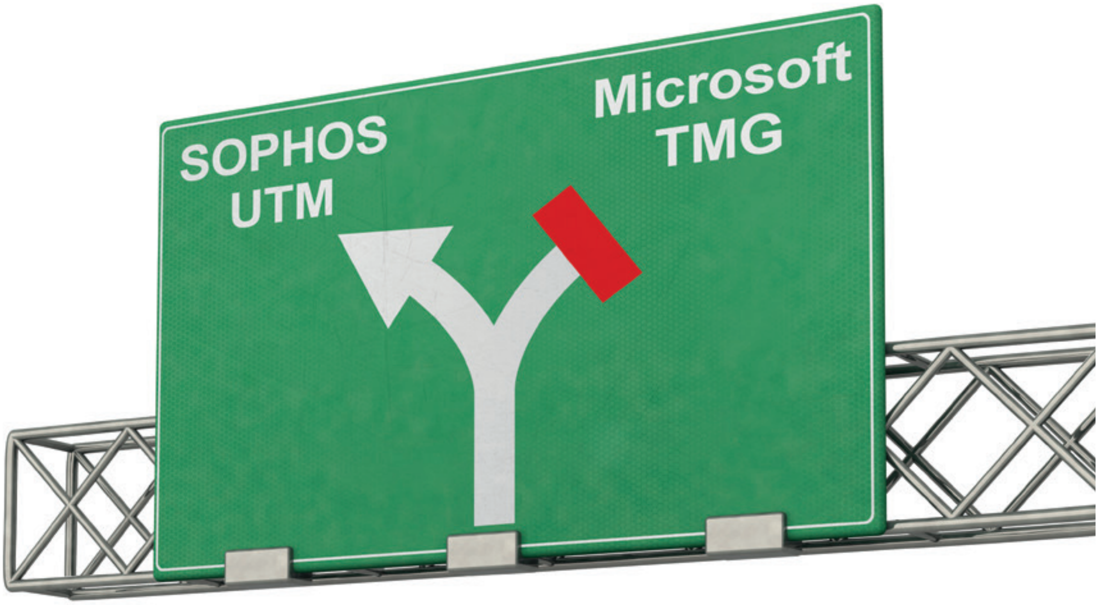
SOPHOS



TMG Replacement Guide

Your guide to replacing Microsoft Forefront Threat Management Gateway

By **Chris McCormack**, Senior Product Marketing Manager

and **Angelo Comazzetto**, UTM Product Manager

During one of the most active periods for hackers and cyber threats in IT history, Microsoft has quietly brought its Forefront Threat Management Gateway (TMG) to a dead-end. There are plenty of firewall solutions out there that claim to offer a reasonable alternative, but you need to cut through the marketing rhetoric from vendors to find a capable replacement for TMG. This TMG replacement guide covers some key areas of Microsoft's TMG—and explains how Sophos Unified Threat Management (UTM) can provide a clear path forward and improve your network protection.

A Sophos Whitepaper July 2013

Simplify Licensing and Deployment

Microsoft's 58-page licensing guide for Windows Server and Forefront products explains that TMG is licensed as part of at least 11 different programs. In terms of deployment, TMG is offered as a native 64-bit software product for Windows Server 2008, deployed on hardware or virtual machines—with an increasing trend towards virtualization.

> "Sophos UTM does not only replace the TMG but also brings a number of new benefits that will help improve your businesses security"[1]

You need to understand the various licensing models and feature deployment options to find a TMG replacement. Be careful to understand what products you need to achieve a TMG equivalent, their deployment options, and feature availability in various models. Some vendors try to upsell their high-end firewall products by only offering advanced features at premium prices. And, some vendors are exclusively hardware or software—or offer limited or no Hyper-V support. Be sure to find a solution that not only meets your needs today but can meet future needs as well.

Sophos has invested significantly in making things simple. From how you buy, to deployment and management; every feature is available on every model and for every form factor. You simply choose the model with the performance required for the size of your network, and add the FullGuard license to enable all the protection options you need, with a single license.

You'll find that Sophos UTM is unique in the security industry. It offers the broadest range of deployment options available. You can select from a range of purpose-built security appliances. Or you can deploy Sophos UTM on your own hardware—such as the server you were using for Microsoft TMG itself.

If you're not quite ready to repurpose your TMG hardware, you can start by running Sophos UTM on any virtual platform, like Microsoft Hyper-V, without losing any features or functionality at all. Sophos UTMs can also be easily deployed in Amazon's Virtual Private Cloud, allowing you to start moving to the cloud at your own pace, without having to fully invest all at once. Our interactive wizard closely resembles TMG's and makes initial setup easy.

Choose how to deploy

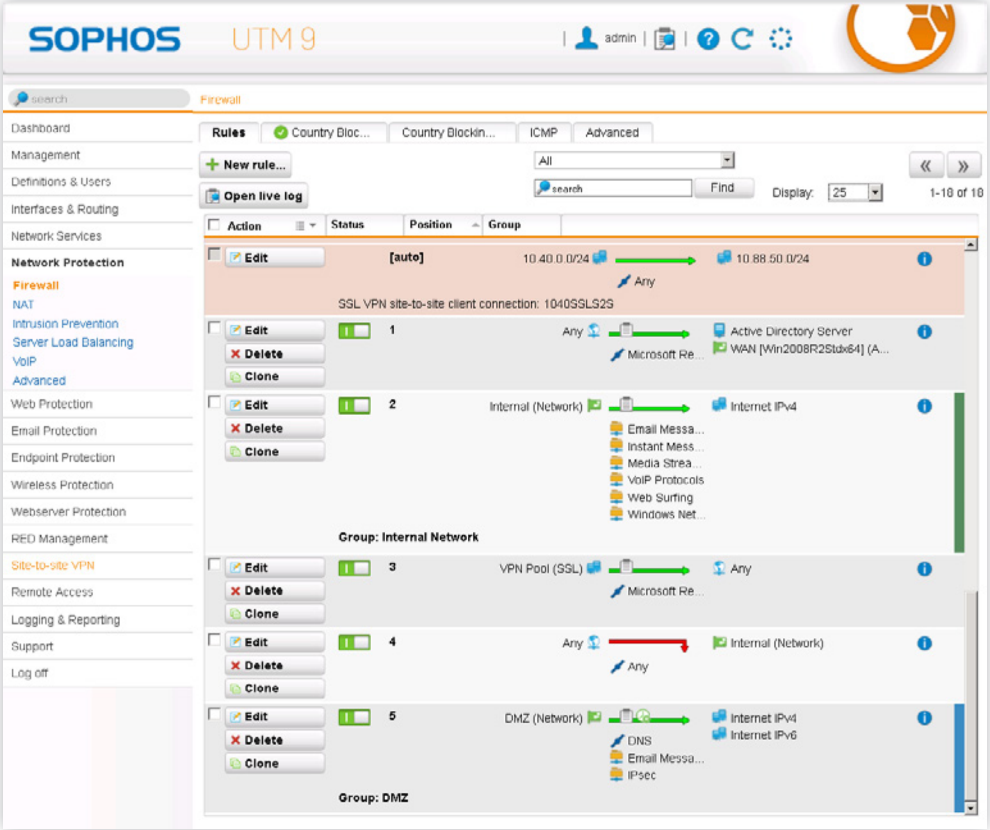
Hardware	Virtual	Software	Cloud-based Appliances
A full range of hardware appliance models are available to fit any business, with all features available in all models.	Sophos UTM's run in Microsoft Hyper-V, KVM, VMware and Citrix virtual environments allowing you to get the most out of your virtualization investment.	The Sophos UTM is also available as a software appliance that can easily install on the server you're using for TMG today, saving you from any additional hardware investment.	Using Amazon Virtual Private Cloud (VPC), you can run the appliance in the cloud. Or, you can use the Amazon VPC connector on the appliance at your office for secure and robust access to your Amazon-hosted resources.

Secure Firewall, Intuitive Management

The core of any secure gateway solution is the firewall, which was a key strength of TMG. Make sure the vendor you choose offers a proven and trusted solution backed by solid network security engineering. Also look for a solution that offers you similar, if not better ease-of-management than what you experienced with TMG. Don't settle for cryptic management consoles that have you reaching for the manual every time you need to make a change.

As you've probably discovered with TMG, over time you can easily end up with thousands of rules that make it difficult to audit your configuration and secure your system. Sophos UTM eliminates the clutter easily and elegantly. It takes advantage of a central object model that lets you make changes across the entire installation with simple edits. You can make groups of rules that have multiple sources and destinations, and even create rules that adapt to changing network conditions so you can be sure your connectivity continues. This cuts down the number of rules and makes them much easier to manage.

With our mantra of "security made simple," Sophos has a strict focus on making security simpler without compromising on features or flexibility. With Sophos, you're working with a vendor that has 25 years of experience securing businesses. The Sophos UTM firewall combines the best in performance with powerful configuration options and intuitive management.



Action	Status	Position	Group			
Edit		[auto]		10.40.0.0/24	Any	10.88.50.0/24
		SSL VPN site-to-site client connection: 1040SSLS2S				
Edit Delete Clone		1		Any	Microsoft Re...	Active Directory Server WAN [Win2008R2Stdx64] (A...
Edit Delete Clone		2		Internal (Network)	Email Messa... Instant Mess... Media Strea... VoIP Protocols Web Surfing Windows Net...	Internet IPv4
		Group: Internal Network				
Edit Delete Clone		3		VPN Pool (SSL)	Microsoft Re...	Any
Edit Delete Clone		4		Any	Any	Internal (Network)
Edit Delete Clone		5		DMZ (Network)	DNS Email Messa... IPsec	Internet IPv4 Internet IPv6
		Group: DMZ				

TMG Administrators will feel right at home with Sophos UTM's firewall rules. However, they can take advantage of the UTM's powerful object model to make management simpler and easier

High Performance, Advanced Protection

TMG offers a variety of IPS, web, and protocol filtering options. TMG's IPS options cover a variety of common attacks, while its web malware filtering evaluates web traffic against known virus and malware signatures, with occasional updates as needed. You'll find this is fairly common in the industry. Unfortunately, it's generally not adequate against threats that use obfuscation and polymorphism to change with each incident or request.

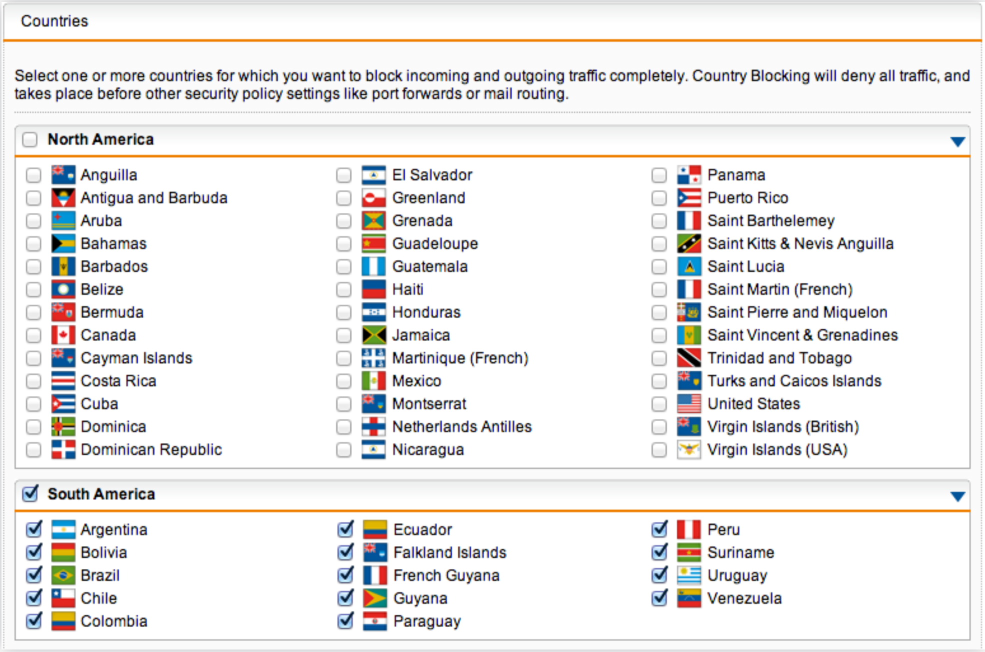
When evaluating alternatives, look beyond each vendor's simple checklist of filtering options and focus more on the performance and scope of the scanning taking place. Find a solution that improves on TMG with real-time traffic scanning against thousands of patterns. What's even more important is where the threat intelligence is coming from, and how often it's updated.

With Sophos, the SophosLabs Live Protection Network provides around-the-clock threat analysis to continuously monitor IPS, malicious websites, web malware, spam, app control and more. Live Protection tracks global issue patterns and updates your UTM in real time through the cloud. So you know you have the latest in network defense—automatically.

With Sophos UTM, you can also shield your network in ways just not possible with TMG. For example, you can stop traffic to and from countries you have no interest in communicating with, significantly reducing your attack surface.

TMG's web protection is easily improved upon with Sophos UTM. Sophos UTM ties right into your existing Active Directory server, and lets you apply policies to your existing users and groups without a conversion processor or configuration changes. With full support for single sign-on (SSO), your users can be protected effortlessly in minutes.

> "... the (Sophos UTM) interface just works, plain and simple. In fact, I think this interface might even surpass TMG's when it comes to usability."[2]



Countries

Select one or more countries for which you want to block incoming and outgoing traffic completely. Country Blocking will deny all traffic, and takes place before other security policy settings like port forwards or mail routing.

□ North America

□ Anguilla
□ Antigua and Barbuda
□ Aruba
□ Bahamas
□ Barbados
□ Belize
□ Bermuda
□ Canada
□ Cayman Islands
□ Costa Rica
□ Cuba
□ Dominica
□ Dominican Republic
□ El Salvador
□ Greenland
□ Grenada
□ Guadeloupe
□ Guatemala
□ Haiti
□ Honduras
□ Jamaica
□ Martinique (French)
□ Mexico
□ Montserrat
□ Netherlands Antilles
□ Nicaragua
□ Panama
□ Puerto Rico
□ Saint Barthelemey
□ Saint Kitts & Nevis Anguilla
□ Saint Lucia
□ Saint Martin (French)
□ Saint Pierre and Miquelon
□ Saint Vincent & Grenadines
□ Trinidad and Tobago
□ Turks and Caicos Islands
□ United States
□ Virgin Islands (British)
□ Virgin Islands (USA)

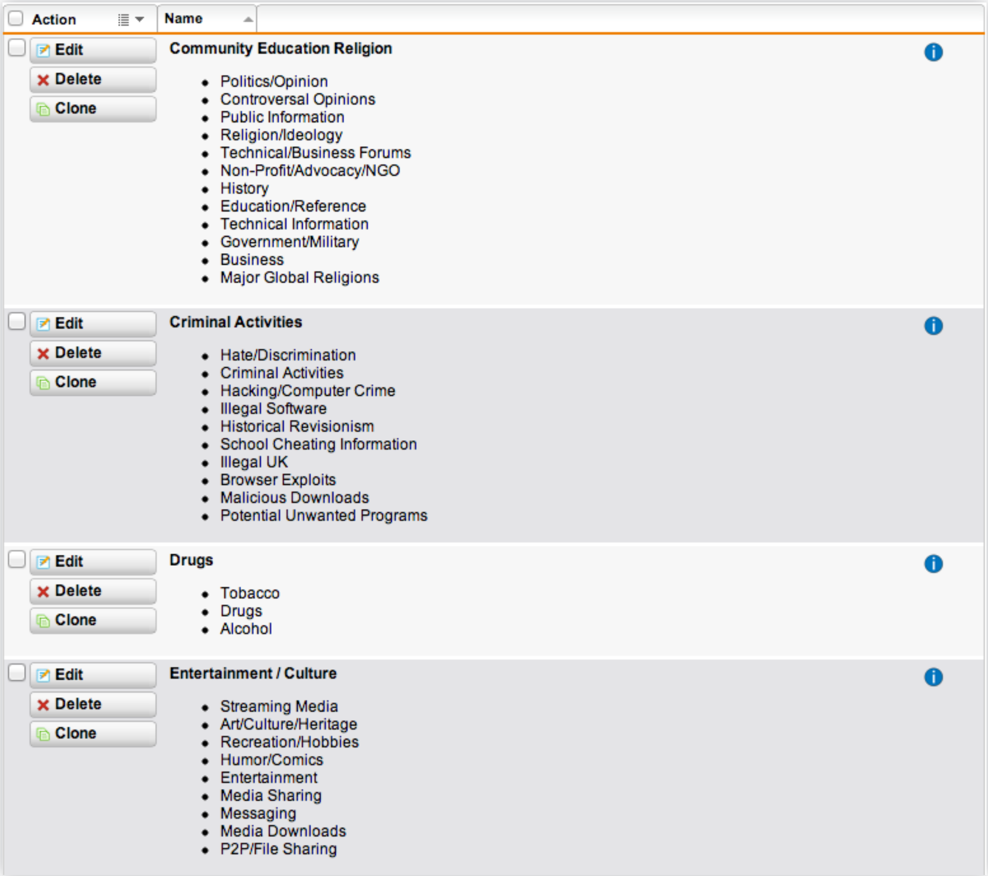
☑ South America

☑ Argentina
☑ Bolivia
☑ Brazil
☑ Chile
☑ Colombia
☑ Ecuador
☑ Falkland Islands
☑ French Guyana
☑ Guyana
☑ Paraguay
☑ Peru
☑ Suriname
☑ Uruguay
☑ Venezuela

Sophos UTM allows you select countries for which you want to block all traffic, significantly reducing your attack surface area

Sophos UTM lets you apply much more granular permissions than TMG ever could. For instance, you can:

- Monitor and control web applications in real time. Making configuration changes and blocking or shaping traffic on the fly, using detailed patterns. For example, deny Facebook chat while still allowing Facebook wall posts, or limit all YouTube traffic.
- Manage access to websites. With over 100 categories to choose from, maximize productivity and control access to inappropriate websites.
- Enforce the safe-search features of major search engines. Without changing anything on your client browsers.



□ Action	Name
□ Edit ✕ Delete Clone	**Community Education Religion** • Politics/Opinion • Controversal Opinions • Public Information • Religion/Ideology • Technical/Business Forums • Non-Profit/Advocacy/NGO • History • Education/Reference • Technical Information • Government/Military • Business • Major Global Religions
□ Edit ✕ Delete Clone	**Criminal Activities** • Hate/Discrimination • Criminal Activities • Hacking/Computer Crime • Illegal Software • Historical Revisionism • School Cheating Information • Illegal UK • Browser Exploits • Malicious Downloads • Potential Unwanted Programs
□ Edit ✕ Delete Clone	**Drugs** • Tobacco • Drugs • Alcohol
□ Edit ✕ Delete Clone	**Entertainment / Culture** • Streaming Media • Art/Culture/Heritage • Recreation/Hobbies • Humor/Comics • Entertainment • Media Sharing • Messaging • Media Downloads • P2P/File Sharing

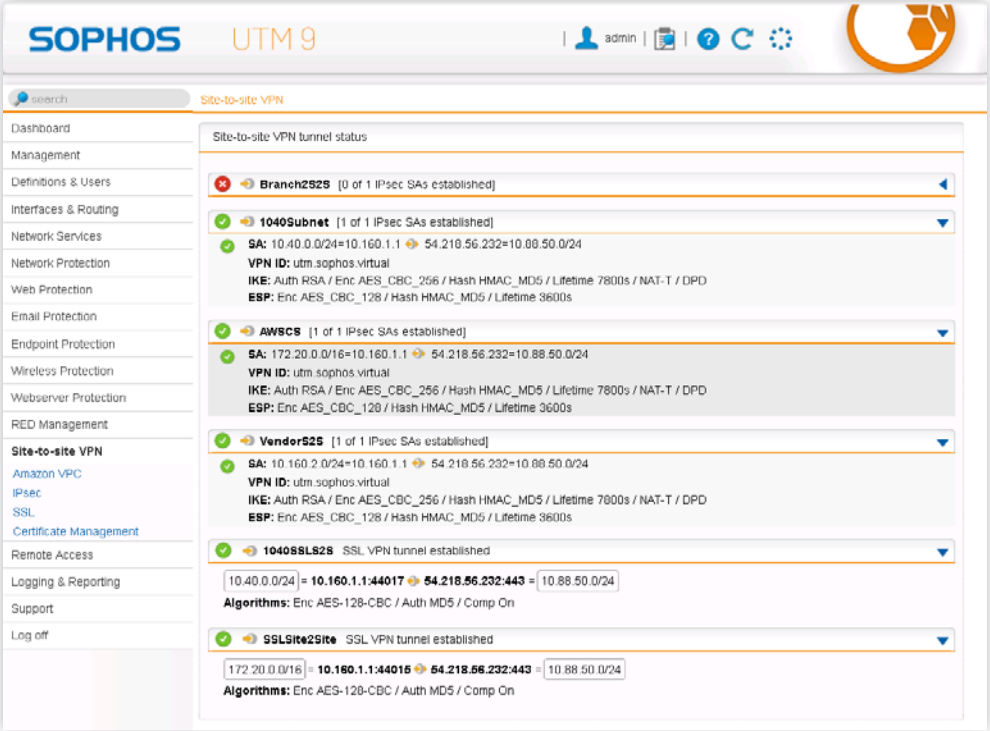
Sophos UTM uses more than 100 categories for controlling access to inappropriate websites

Advanced VPN for Easy Remote Access

TMG allows you to build basic site-to-site VPN tunnels using IPSec, and connect remote users with two kinds of legacy technologies (PPTP and IPSEC). You should take this opportunity to consider the much easier and more flexible VPN solutions available today.

Sophos UTM gives you an entire suite of options to meet your needs, and connect the latest devices to your network from anywhere in the world. You can easily set up site-to-site connections using traditional IPSec, or with an SSL-based tunnel engine that works in environments which block IPSec. Going further, our unique Layer-2 VPN tightly binds your offices together and allows for communication of services like DHCP—which is simply not possible with TMG.

Remote users can log in with integrated clients on their mobile devices, and choose from five different technologies to connect their Windows, Mac and Linux laptops—including a full browser-based HTML5 VPN that requires no client at all! Sophos has gone above and beyond in providing a rich set of powerful VPN tools that are simple to manage.



Site-to-site VPN tunnel status

```
Branch2S2S  [0 of 1 IPsec SAs established]

1040Subnet  [1 of 1 IPsec SAs established]
SA: 10.40.0.0/24=10.160.1.1 54.218.56.232=10.88.50.0/24
VPN ID: utm.sophos.virtual
IKE: Auth RSA / Enc AES_CBC_256 / Hash HMAC_MD5 / Lifetime 7800s / NAT-T / DPD
ESP: Enc AES_CBC_128 / Hash HMAC_MD5 / Lifetime 3600s

AWSCS  [1 of 1 IPsec SAs established]
SA: 172.20.0.0/16=10.160.1.1 54.218.56.232=10.88.50.0/24
VPN ID: utm.sophos.virtual
IKE: Auth RSA / Enc AES_CBC_256 / Hash HMAC_MD5 / Lifetime 7800s / NAT-T / DPD
ESP: Enc AES_CBC_128 / Hash HMAC_MD5 / Lifetime 3600s

VendorS2S  [1 of 1 IPsec SAs established]
SA: 10.160.2.0/24=10.160.1.1 54.218.56.232=10.88.50.0/24
VPN ID: utm.sophos.virtual
IKE: Auth RSA / Enc AES_CBC_256 / Hash HMAC_MD5 / Lifetime 7800s / NAT-T / DPD
ESP: Enc AES_CBC_128 / Hash HMAC_MD5 / Lifetime 3600s

1040SSLS2S  SSL VPN tunnel established
10.40.0.0/24 = 10.160.1.1:44017 54.218.56.232:443 = 10.88.50.0/24
Algorithms: Enc AES-128-CBC / Auth MD5 / Comp On

SSLSite2Site  SSL VPN tunnel established
172.20.0.0/16 = 10.160.1.1:44015 54.218.56.232:443 = 10.88.50.0/24
Algorithms: Enc AES-128-CBC / Auth MD5 / Comp On
```

You can easily set up site-to-site connections using traditional IPSec, or with an SSL-based tunnel engine

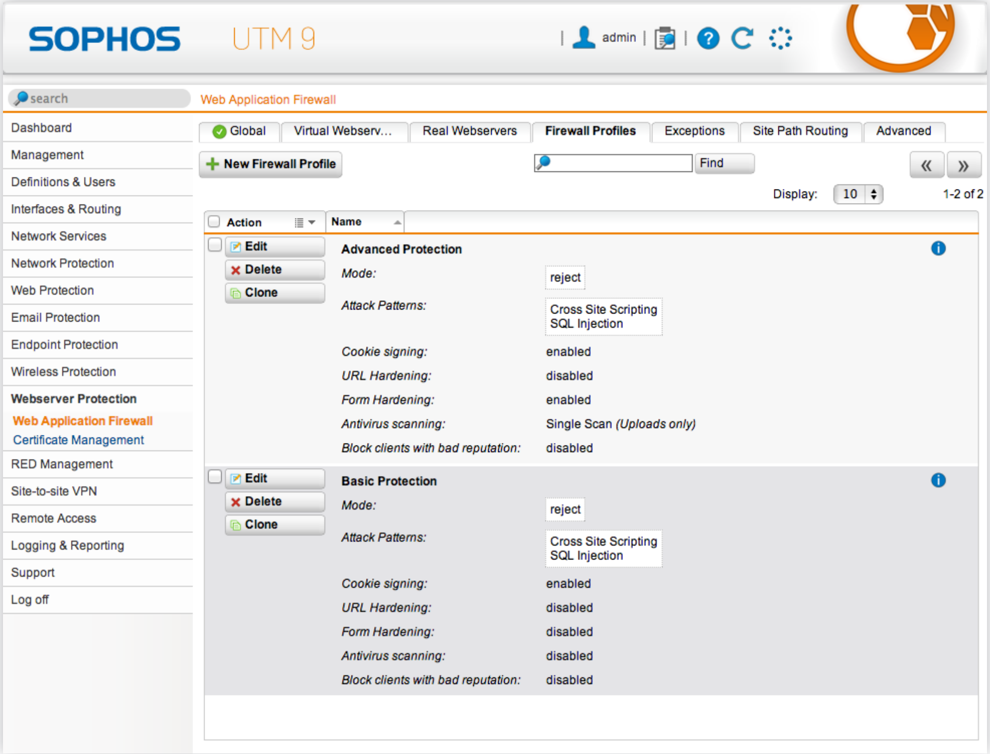
> "Sophos UTM supports pretty much any VPN technology out on the market today… I have yet to see a less complicated way of configuring site-to-site connections, my hat's off to Sophos for this one."[2]

Web Application Firewall and Robust Reverse-Proxy

A key component of TMG that you need to have is reverse proxy and web application firewall capabilities that protect your outward facing servers and resources from attack. Replacement solutions must allow your offsite users to communicate with essential corporate resources like Exchange or SharePoint. And it must provide features like SSL offloading and security features for database fields, forms and cookies.

Sophos UTM is a replacement for TMG's reverse proxy, allowing you to wrap your web server applications in layers of security to protect them against hackers and threats. Our Web Server Security provides antivirus scanning and stops SQL injection and cross-site scripting attacks, so you don't have to be an expert in database and server hardening.

Of course, your clients can communicate with servers over Outlook Anywhere and you can make your Outlook Web Access login page available only to securely connected clients with ease. The reverse proxy is further outfitted with SSL offloading abilities, a dynamic whitelisting path system called URL hardening, as well as security features for cookies and forms.



Advanced Protection

Mode:	reject
Attack Patterns:	Cross Site Scripting SQL Injection
Cookie signing:	enabled
URL Hardening:	disabled
Form Hardening:	enabled
Antivirus scanning:	Single Scan *(Uploads only)*
Block clients with bad reputation:	disabled

Basic Protection

Mode:	reject
Attack Patterns:	Cross Site Scripting SQL Injection
Cookie signing:	enabled
URL Hardening:	disabled
Form Hardening:	disabled
Antivirus scanning:	disabled
Block clients with bad reputation:	disabled

Sophos UTM includes a robust reverse-proxy to protect your servers from attacks and malicious behavior

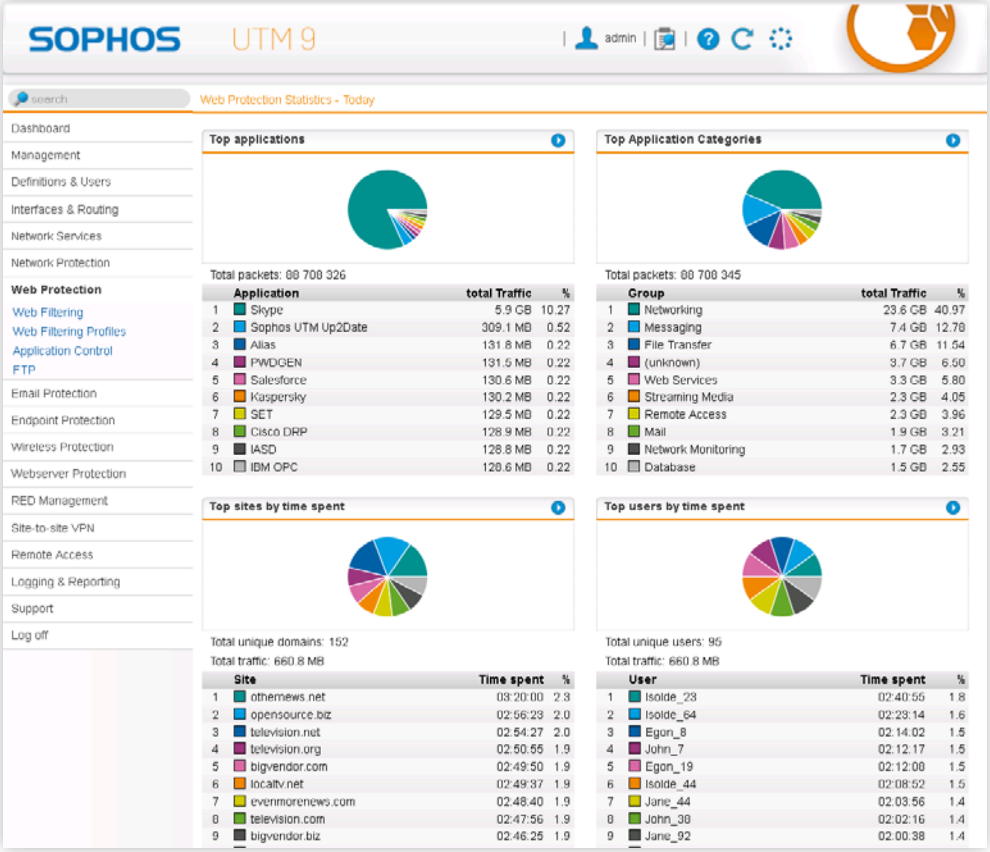
Complete On-Box Reporting and Dynamic Monitoring

TMG reports lack helpful features like drill-downs, filtering and customization, and TMG uses a variety of third party add-ons to address these shortcomings. When considering prospective replacements, make sure they don't suffer from some of the same weaknesses. You don't want to have to buy additional hardware, software, or both to do reporting. Many vendors sell reporting as an extra cost add-on that requires a separate server or appliance.

Sophos' integrated on-box reporting and dynamic monitoring is a key strength. Our UTM's built-in reporting means you'll know exactly what's happening on the network. It enables you to identify problems quickly and shape policies to get the best protection, performance and productivity. Detailed informational reports with deep drill-down capabilities are standard, and stored locally, with no separate tools required.

In addition, at-a-glance flow monitors show usage trends—providing real-time insights into network activity. Report anonymization hides user names, requiring the four-eyes principle to unhide them.

> "This level of detail and customization means that UTM can run just about any possible report imaginable, thus making it one of its greatest strong points in my opinion."[2]



Top applications

Total packets: 88 708 326

	Application	total Traffic	%
1	■ Skype	5.9 GB	10.27
2	■ Sophos UTM Up2Date	309.1 MB	0.52
3	■ Alias	131.8 MB	0.22
4	■ PWDGEN	131.5 MB	0.22
5	■ Salesforce	130.6 MB	0.22
6	■ Kaspersky	130.2 MB	0.22
7	■ SET	129.5 MB	0.22
8	■ Cisco DRP	128.9 MB	0.22
9	■ IASD	128.8 MB	0.22
10	□ IBM OPC	128.6 MB	0.22

Top Application Categories

Total packets: 88 708 345

	Group	total Traffic	%
1	■ Networking	23.6 GB	40.97
2	■ Messaging	7.4 GB	12.78
3	■ File Transfer	6.7 GB	11.54
4	■ (unknown)	3.7 GB	6.50
5	■ Web Services	3.3 GB	5.80
6	■ Streaming Media	2.3 GB	4.05
7	■ Remote Access	2.3 GB	3.96
8	■ Mail	1.9 GB	3.21
9	■ Network Monitoring	1.7 GB	2.93
10	□ Database	1.5 GB	2.55

Top sites by time spent

Total unique domains: 152

Total traffic: 660.8 MB

	Site	Time spent	%
1	■ othernews.net	03:20:00	2.3
2	■ opensource.biz	02:56:23	2.0
3	■ television.net	02:54:27	2.0
4	■ television.org	02:50:55	1.9
5	■ bigvendor.com	02:49:50	1.9
6	■ localtv.net	02:49:37	1.9
7	■ evenmorenews.com	02:48:40	1.9
8	■ television.com	02:47:56	1.9
9	■ bigvendor.biz	02:46:25	1.9

Top users by time spent

Total unique users: 95

Total traffic: 660.8 MB

	User	Time spent	%
1	■ Isolde_23	02:40:55	1.8
2	■ Isolde_64	02:23:14	1.6
3	■ Egon_8	02:14:02	1.5
4	■ John_7	02:12:17	1.5
5	■ Egon_19	02:12:08	1.5
6	■ Isolde_44	02:08:52	1.5
7	■ Jane_44	02:03:56	1.4
8	■ John_38	02:02:16	1.4
9	■ Jane_92	02:00:38	1.4

Sophos UTM provides a complete set of pre-defined reports with deep drill-down and customization options

Key Capabilities Compared

TMG	UTM	Adds even more...
Hyper-V Support	✓	More deployment choices (HW, SW, VM, Cloud)
Firewall (stateful packet filtering)	✓	Advanced Routing, Country Blocking
IPS	✓	11,000 IPS attack patterns – Live Protection
Exchange anti-spam, anti-malware	✓	User Portal Quarantine, Email encryption
Redundancy	✓	WAN redundancy & load balancing
Logging/Reporting	✓	Customizable reports, Drill-down, and more
Client VPNs (PPTP/L2TP)	✓	Added flexibility (SSL, HTML5)
Site-to-Site VPNs (IPSEC)	✓	Broader VPN Support, Amazon VPC, RED
URL Filtering	✓	Reputation filtering, Customizable categories
Content Scanning	✓	Real-time App Control
Malware Scanning	✓	Dual Engine, Backed by Sophos Labs
HTTPS Scanning	✓	HTTPS Scanning in Transparent Mode
User Authentication	✓	Added flexibility, Transparent Mode
Reverse Proxy	✓	WAF with server hardening
Reverse Proxy SSL Offloading	✓	Included feature of WAF
Reverse Proxy Authentication	✓	Coming in UTM v9.2

Sophos UTM: Your Best Alternative

TMG has provided a broad set of features widely adopted by many Microsoft partners and might otherwise be sorely missed without an adequate replacement. Sophos UTM lets you easily replace TMG, providing a simple way to keep your network and users secure. Sophos UTM's technologies are tightly integrated—working better together. And, most importantly, it's easier to manage than any other UTM product on the market.

You don't have to take our word for it—industry experts who have looked at the alternatives give us high marks. West Coast Labs' April 2013 Threat Assessment Journal concludes:

> "The combination of security technologies included, along with extended functionality and central management, should appeal to companies who are considering rationalizing their protection into a single solution from a single, well-respected vendor. Sophos UTM has shown and continues to show itself to be a worthy candidate for inclusion on any shortlist of consolidated protection devices."[3]

Sophos UTM not only replaces your aging Microsoft TMG with all the features and capabilities you need, but can also expand your protection to add even more capabilities than TMG could ever offer. And you can add them whenever you want. For example, you can add an integrated wireless controller with a full range of plug-and-play wireless access points. Or add a unique, low-cost plug-and-protect RED device for easy secure branch-office VPN extensions to your network, and much more.

Take it from industry experts who have compared multiple candidates and thoroughly tested their features: Sophos UTM is the best TMG replacement solution and the easy choice to replace your TMG solution.

Get Started Today

Visit www.sophos.com/TMG to learn more and sign up for a free trial of Sophos UTM. Or, contact your Sophos UTM authorized reseller or Sophos Representative for more information and to take advantage of a special limited time TMG replacement offer.

Sources

1. Bytes Technology Group (2013, July) Goodbye Microsoft Forefront TMG - Hello Sophos UTM http://www.bytes.co.uk/info/technology-updates/goodbye-microsoft-forefront-threat-management-gateway-hello/

2. Lutters, Jorn. (2013, January 16). Securing the edge in a post-TMG world. [Web Log Post]. Retrieved from https://www.winsec.nl/2013/01/16/securing-edge-post-tmg-world/. This blog series reviewed replacements for Microsoft's Forefront Threat Management Gateway 2010 that had multiple parts and spanned several weeks. Technical details on what they thought of Sophos UTM here: https://www.winsec.nl/2013/03/29/securing-edge-post-tmg-world-part-5/.

3. "Technology Performance: Real Time performance for Sophos UTM." Threat Assessment Journal 1 (April 2013): 12-15. Web.

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

Asia Sales
Tel : +65 62244168
Email : salesasia@sophos.com

Boston, USA | Oxford, UK

SOPHOS