

A TMG Administrator's Guide to Sophos UTM

If you have made (or are considering making) the switch from Microsoft's TMG and Sophos UTM, this migration guide highlights the key differences between the two products. Its goal is to help UTM administrators with a TMG background migrate to Sophos UTM more easily by highlighting major similarities and differences.

Audience

Technical administrators of TMG with a general networking and firewalling background.

Intended use

This guide serves only as a general starting point for UTM admins to become more comfortable with Sophos UTM and to encourage self-learning and exploration of its many features and functionalities.

This is not a TMG to UTM migration scenario guide. TMG setups vary widely, and it is virtually impossible to list all possible configurations one can build using TMG.

Topics covered

This guide covers comparisons on TMG Access Rules, Publishing Rules, Web Filtering, Email Protection and Network rules, along with the extraneous settings related to these functionalities.

Similarities and missing functionalities

Throughout the document, both similarities and missing functionalities are discussed. When reviewing similarities, the guide illustrates the general experience of using the products on a day-to-day basis.

While Sophos UTM aims to match TMG's functionalities, there are differences between the systems that cannot be addressed due to the general architecture of the systems and differences in development between both products. If a functionality is not available in Sophos UTM, an alternate solution or workaround is offered.

Contents

1. Access Rules

Similarities

- Interface
- Configuration

Differences

- IPv6 support
- Rule naming
- Rule enabling
- User filtering
- Malware filtering

Missing functionality

2. Network rules and VPN

Similarities

- Static routing
- ISP Redundancy
- IPSec Site-to-Site VPN
- L2TP and PPTP Client VPN

Differences

- NAT

Missing functionality

- Dynamic routing – RIPv2
- SSTP VPN
- Dynamic WPAD

3. URL filtering and malware inspection

Similarities

- General configuration
- URL filtering overrides

Differences

- User-based override
- Anti malware
- HTTPS inspection

Missing functionality

- Secondary categories

4. Publishing rules

Similarities

- General configuration
- Site path routing

Differences

- Web listeners
- Web application protection
- Authentication
- URL forwarding
- Link translation

Missing functionality

- Default domain name
- X.509 client certificate authentication
- Persistent cookies

5. Email protection

Similarities

- Mail flow configuration
- Anti-spam configuration
- Anti-malware configuration

Differences

- Mail manager
- User portal

Missing functionality

29

29

29

30

31

31

33

34

36

36

37

37

38

38

39

39

39

40

41

41

41

42

43

1. Access Rules

Access Rules are an integral part of TMG and form the backbone to its functionality. This is where network-level permissions in a TMG system are assigned, and is one of the most basic features of the product. These rules allow the blocking or permitting of traffic through the firewall, from single hosts to entire networks and from a single protocol to the entire array of layer 3 protocols as defined by the IEEE and IETF.

The Sophos UTM equivalents are called Firewall rules and they serve the exact same purpose: to allow traffic through the firewall.

Similarities

TMG and Sophos UTM perform similar functionalities, so the implementation is largely similar too. This section covers the major similarities and illustrates the general experience of using the products on a day-to-day basis.

Interface

When comparing the overall layout of the TMG access rule to the UTM firewall rule, the main similarities are clearly noticeable, as highlighted below.

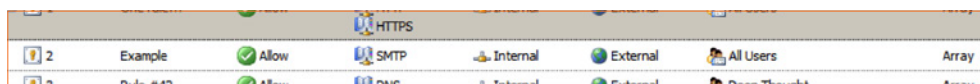


Figure 1 - TMG interface

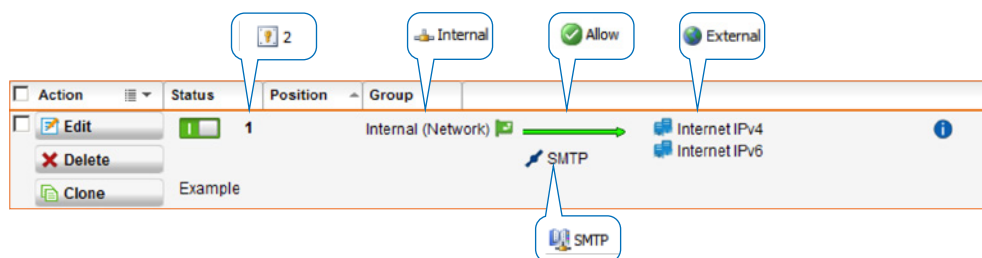


Figure 2 - UTM Interface

As noted above, the rule functionality and way of presenting are remarkably similar, except for some interface elements that are presented differently.

The overall information conveyed by the Sophos UTM and TMG is exactly the same (traffic from a network called "Internal" to the Internet using the protocol "SMTP" is allowed), and the expected outcome of the discussed rule is similar too.

Configuration

The same is true for the configuration of rules in Sophos UTM. While different in appearance from TMG, (configuration elements are all presented in a toolbox on the left side of the UTM interface, rather than using popups) the general mode of configuration is similar. You still need to select a source, destination and protocol from a list and then add them to the rule being configured. TMG does this through double-clicking, while UTM uses a drag-and-drop style.

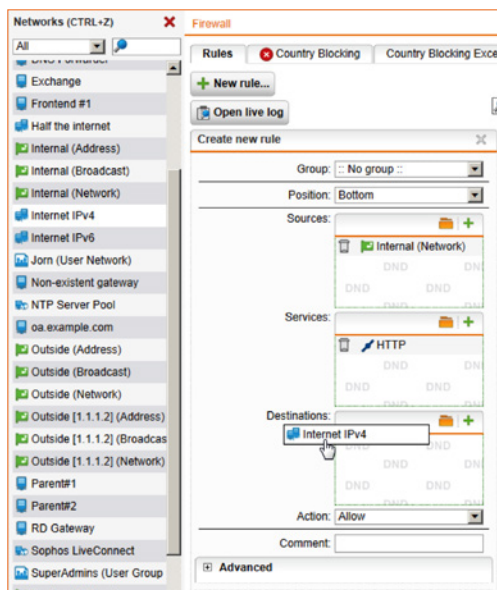


Figure 3 - UTM firewall rule

Creating or manipulating rules is also similar to TMG. To create a new rule, you click the "+ New Rule" button. To edit a rule, you double-click the rule or click the "Edit" button.

Even for some mode "hidden" or advanced features of TMG like the System Policy configuration, there are Sophos UTM equivalents.

An example is the System Policy Rule that allows Ping. Not only is it a separately configured item in UTM, it's hidden under its own menu: the "advanced" tab of the firewall configuration, just like the System Policy menu in TMG.

Differences

At first glance, it may seem just a matter of getting used to the new look and feel of Sophos UTM, rather than there being actual differences. While this is true to some extent, there are differences in functionality between TMG and UTM. This section will attempt to convey these differences with as much detail as possible, instead of the broader generalizations of the previous section.

IPv6 support

One of the major differences between UTM and TMG is IPv6 support. TMG is only IPv6 capable, which means that it can only forward or block all IPv6 traffic without any means of filtering. Sophos UTM on the other hand is fully IPv6 compatible so you can filter IPv6 traffic in the same manner as IPv4 traffic.

This translates into slightly different rules and objects that can be applied in Sophos UTM that cannot be configured in TMG, for example the TMG "External" object. It is used to indicate any IPv4 object that is not part of a reserved range, and therefore it's frequently used as the destination object of access rules allowing traffic to the internet. Sophos UTM does not have this object due to the distinction made between IPv4 and IPv6 internet.

- › **How to do this in UTM:** To allow the equivalent of "External" in Sophos UTM, use the "Internet IPv4" and "Internet IPv6" objects in tandem as seen in figure 2.

Rule naming

A minor difference is rule naming. In TMG you're explicitly obligated to configure a name for a rule in the "Name" field. Such functionality does not exist in Sophos UTM, nor is it mandatory. You can, however, add comments to firewall rules through the "Comment" field.

- › **How to do this in UTM:** If you need to name a rule in UTM, simply use the "Comment:" field for setting the name of the rule. This will prompt UTM to display the rule comment in the bottom left corner of the configured rule.

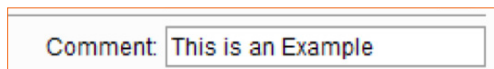


Figure 4 - Comment field in UTM firewall rule

Rule enabling

Rule enabling is another minor difference. In TMG, you either click a button in the toolbar or right-click a rule and select the "enable"/"disable" item from the popup. Neither of these options is available in the UTM interface, but Sophos does offer an elegant take on performing this action.

- › **How to do this in UTM:** Every rule object in UTM has a small slider in the top left corner, next to the "Edit" button. Clicking this slider enables/disables the rule, and the slider turns green as a visual cue to indicate which rules are enabled.

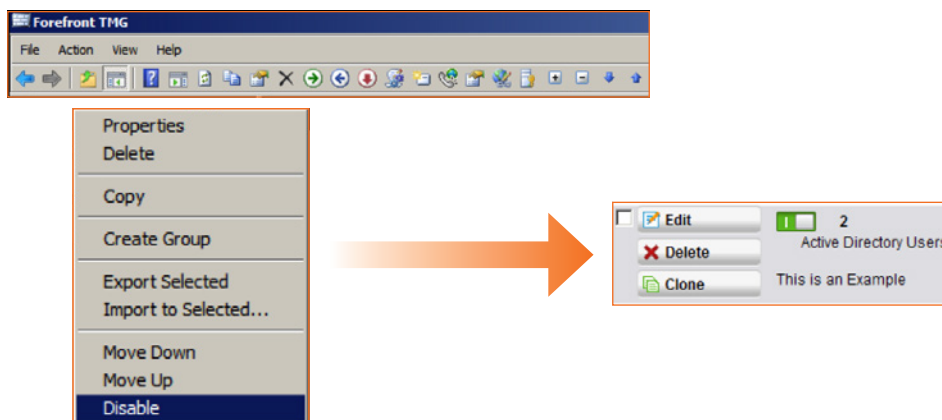


Figure 5 - Rule enabling TMG vs. UTM

User filtering

Both TMG and UTM offer user based filtering, but the exact implementation differs greatly. Getting authentication data to the respective systems is quite similar though.

In TMG one can apply user-level filtering on any access rule as long as the client workstations are configured to use the TMG as a proxy server (which works only for HTTP and HTTPS) or the client machines are running the optional firewall client to transmit the user's credentials. In Sophos UTM the options are nearly identical. One can either configure the UTM as a proxy server on the client workstation (for HTTP, HTTPS and FTP traffic), or you can use the Sophos Authentication Agent (SAA) to send the credentials to UTM.

But unlike TMG, Sophos UTM has additional methods of extracting information about the user. In addition to the aforementioned methods, you can configure the "browser" authentication model (which transparently redirects users to a website with a form where they need to log in) or perform transparent AD authentication, which works similarly but sends an NTLM request to the client instead of a logon form and thereby allows for transparent authentication in AD integrated environments.

The biggest difference between both products however is the method of assigning users to a rule. In TMG, you assign a user to a rule as an additional filtering component, thereby adding to the filtering criteria. We illustrate how this works in the example below:

2	Example	Allow	SMTP	Internal	External	All Users
3	Rule #42	Allow	DNS	Internal	External	Deep Thought

Figure 6 - TMG user filtering example

In this screenshot notice that "Rule #42" only allows traffic if **four** conditions are met 1) the source is "Internal" **AND** 2) the destination is "External" **AND** 3) the protocol is DNS **AND** 4) the user sending the traffic is "Deep Thought".

This type of user filtering can be applied to any type of Access Rule in TMG, regardless of whether it's used to filter web traffic (HTTP/HTTPS) or protocols that require the use of the Firewall Client for authentication (such as DNS in this example).

UTM takes quite a different approach, with a distinct split in functionality between a "user object" and a "user." While they sound similar or interchangeable, the difference between them is how they function: a "user object" is a straight user-to-IP mapping scheme which resolves a user to an IP address, while a "user" is used as a metadata in web protection rules.

This limits the use of "user objects" to firewall rules (where they can be used regardless of protocol) and requires that the user logged in to the UTM using either the SAA or through a VPN (similar to TMG). "Users" on the other hand are used in web protection profiles to limit or extend rights to specific users depending on their logon data.

Users in firewall rules

Another difference is that UTM allows the use of a "user object" as a source or destination to a firewall rule, unlike TMG which used it as an additional filtering criterion. This means that the effective filtering will filter on three instead of four conditions: 1) the user group "Active Directory Users" **AND** 2) the protocol "HTTP" **AND** 3) the destination "Internet IPv4". If the traffic matches this pattern, traffic is allowed. See illustration below.

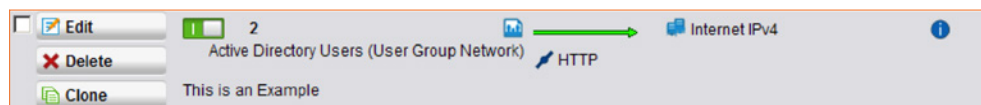


Figure 7 - User filtering UTM firewall rule

This works in many cases, but for some scenarios (such as allowing only users coming from a specific subnet) there is a need to filter on an additional parameter (source network in this case).

- **How to do this in UTM:** To enable filtering on another parameter, you need to nest firewall rules. For example, to only enable users in the Active Directory users group to access the internet when coming from a specific source network (the "Marketing" subnet in this case) you need to create two rules: One to first block access to the internet for any network but the allowed source network and a second rule that allows the configured group, as demonstrated below:



Figure 8 - Advanced user filtering in UTM

This firewall rule authentication scheme works for any type of action (allow, reject or drop) and any protocol, even for HTTP and HTTPS rules (provided that the users have logged in to UTM through the Sophos Authentication Agent or a dial-in client VPN).

Users in Web protection profiles

The use of the proxy-, browser or transparent authentication options is limited to the Web protection component of Sophos UTM. Web protection in UTM manages HTTP, HTTPS and FTP filtering and authentication for these protocols. Functionally, this is similar to the way user filtering works in TMG. But unlike TMG, these settings are not configured through the equivalent of Access Rules, but through a separate configuration menu altogether. This is because Sophos separates Firewalling and Web Filtering into different components and subsystems to cut down on configuration errors and unintended user privileges.

- **How to do this in UTM:** To configure proxy-based authentication, enable the Web protection feature and select to which users the main or auxiliary profile applies by dragging them to an object box (much like with the firewall rules) as part of the “Policies” configuration of the Web protection profile.

You also have to configure which authentication modes are allowed when connecting to the UTM. This setting is unique to the configured profile and limits the available methods on the network to which the profile applies. This means that you cannot mix standard and transparent authentication for the same network, for example.

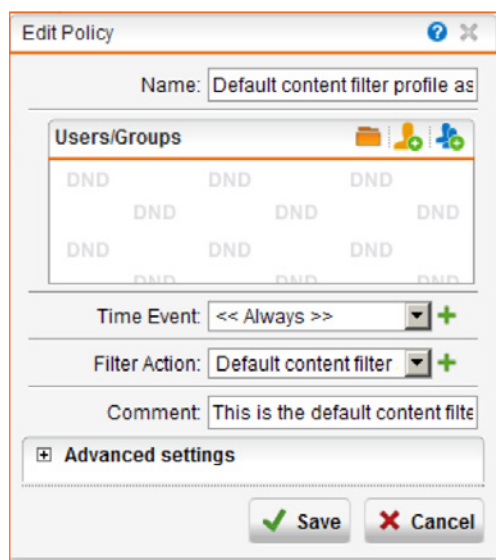


Figure 9 - User filtering in UTM Web Protection

Malware filtering

Malware filtering is related to Web protection settings, and represents another major difference between Sophos UTM and TMG. With TMG, each rule that allowed HTTP traffic displayed a configuration tab that where one could enable or disable malware filtering for said rule.

In UTM however, this is part of the Web Protection profile configuration and cannot be enabled on firewall rules.

- **How to do this in UTM:** To enable malware filtering, go into the Filter Actions configuration of the Filtering Profiles settings of the Sophos UTM Web Protection configuration. There you find all the Web Filtering related settings, such as URL and Content filtering, which is inspected in more detail later.

This is also where you configure advanced HTTP/HTTPS protocol filtering, such as MIME type inspection and extension filtering.

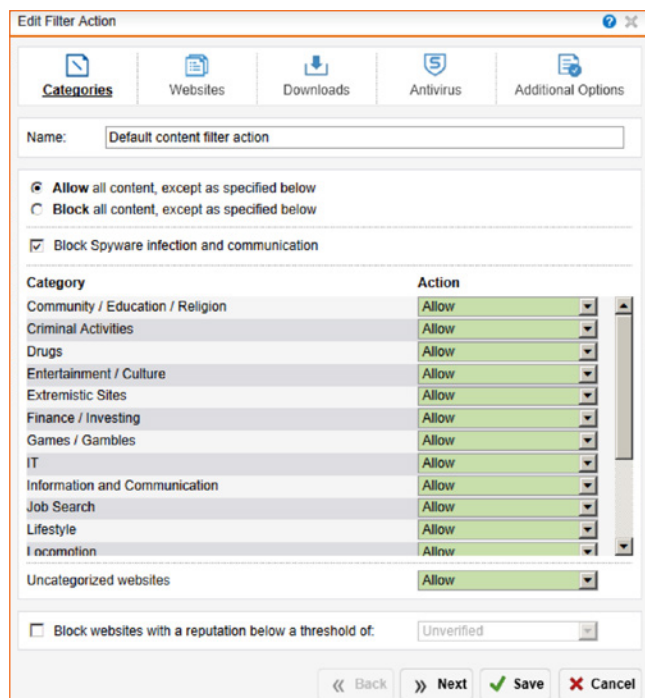


Figure 10 - UTM Web Protection Filter Actions

Missing functionality

There are some unique TMG features that cannot be replaced by Sophos UTM. Here, we discuss these functionalities and provide alternative solutions and workarounds wherever possible.

URL Redirection

URL redirection in Access Rules is configured as part of the "Deny" behavior for an Access rule. If traffic that applies to the configured rule arrives, an admin can choose to forward the traffic to another URL (for example if user lands on www.webserver.com/home, redirect to www.webserver.com/myhome). This functionality does not exist in this form in UTM, which only allows redirection of HTTP to HTTPS as part of the Web Server Protection settings (see chapter four).

- › **How to work around this:** Use the web server's built-in redirection features, such as the "HTTP Redirects" functionality in IIS (described [here](#)) or the "mod_rewrite" component in Apache (described [here](#)).

2. Network rules and VPN

Network rules are essential to TMG as they govern the network related settings of the firewall. Network rules range from routing and NAT-related settings to Web Proxy configuration settings and remote networking-related settings such as VPNs.

While a lot can be said for Microsoft's decision to group all these settings in one place, it tends to confuse novice TMG admins.

Sophos takes a different approach in UTM and groups only the settings relevant to each other. This setup feels more comfortable to anyone with a networking background, but will be a bit difficult for long-time ISA and TMG admins who may lose time finding the appropriate menu to configure these settings.

Similarities

Due to this radically different approach to configuring the networking, NAT, VPN and connectivity related settings, there appear to be a lot of differences at first. Upon closer inspection, quite a few are related to the interface. This chapter focuses on the similarities hidden behind the slightly different interfaces of TMG and Sophos UTM

Static routing

A major improvement in TMG was the incorporation of the "Enhanced Networking" features, which included a more centralized means of configuring routing. Previously this used to be configured on each ISA server locally instead of through the central management.

The routing settings are found under the "Routing" tab of the "Networking" menu and allow a route to be pushed to all nodes of the TMG array.

TMG only allows for "Gateway" type static routes, where one indicates the destination, destination netmask and the next-hop router or gateway the TMG can use to reach the configured destination.

For fine tuning purposes (such as fallback routing when using multiple network interfaces) a TMG admin has the option to set a static route metric for the configured route.

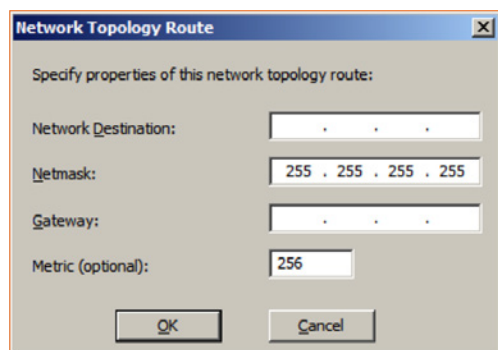


Figure 11 - Static routing in TMG

Sophos UTM has the ability to configure many routing options, including both dynamic (BGP and OSPF) and static routing. These are all configured through the "Interfaces & Routing" menu.

Configuration of static routes is done through the "Static Routing" submenu, and looks quite similar to the routing configuration in TMG, especially when using the "Gateway route" route type.

You have the option to select the network (which is configured through drag-and-drop from the toolbox, or by clicking the "+" sign and creating a new "Network" object by setting the network and netmask), selecting the gateway (again either through drag-and-drop or by creating a new host object) and setting a Metric for the route.

The main difference with TMG is the option to add a comment in the "Comment:" field, allowing for easier recognition and administrative notes (such as indicating that a particular route is a backup route).

Figure 12 - Static routing in UTM

The other static routing options available in Sophos UTM are "Interface" and "Blackhole," neither of which are found in the TMG interface, but expert TMG admins have configured through the Windows Server commandline interface for some time.

The "Interface" route type configures UTM to forward any traffic for a given destination to a specific interface and from there it is sent to the interface's default gateway. A similar configuration on TMG would be to use the following commands on the Windows server command line interface:

```
Route add -p <network> mask <netmask> <gateway> <interface>
```

The "Blackhole" type discards any traffic for the configured network, thereby effectively making the entire network unreachable. This can be used to offload the firewall and IPS engines of the UTM in case of a (perceived) DoS attack, or to render specific parts of the (inter)network unreachable for security purposes.

Neither TMG nor Windows Server offer the exact same behavior, but this functionality can be mimicked by sending traffic for a specific network to a nonexistent router. A sample configuration for such a setup would use the following command:

```
Route add -p <network> mask <netmask> 255.255.255.255
```

ISP Redundancy

Another welcomed TMG feature is the option to connect multiple upstream connections and either loadbalance the connections or configure them in a failover scheme called "ISP Redundancy."

Automatic failover in TMG takes place based on a dead link detection mechanism that polls a host (or the root DNS servers by default) to determine if a link is still viable. Additionally administrators can bind specific hosts, networks and users (or a combination) to a specific link for administrative purposes.

Both of these loadbalancing modes are also available in Sophos UTM, with some added traffic selection options when binding traffic to a specific interface and the option to loadbalance more than two uplinks.

The Sophos UTM equivalent of ISP Redundancy is configured as part of the interface configuration under the "Uplink balancing" tab.

To enable Sophos UTM to perform the equivalent to TMG's "Failover only" option, add the preferred primary uplink to the "Active Interfaces" dropdown, while adding the standby interface(s) to the "Standby Interfaces" dropdown.

To configure the equivalent of "Loadbalancing with failover," add all interfaces that should be used simultaneously to the "Active Interfaces" and then determine the priority (which interface should be checked for availability first) of the interfaces by clicking on the arrows behind the configured interfaces to adjust the hierarchy.

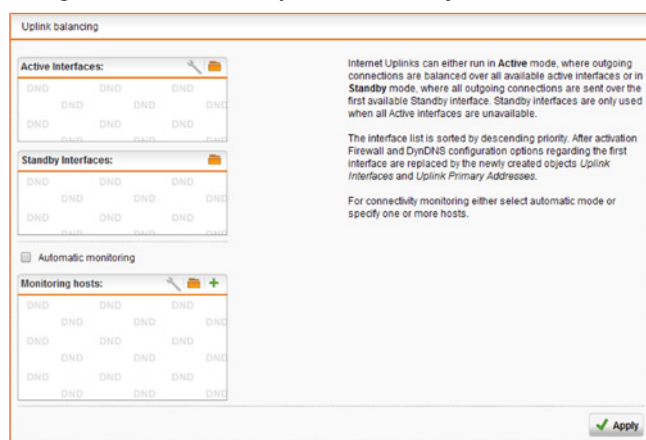


Figure 13 - Sophos UTM Uplink balancing

In both cases, you have the option to enable Automatic monitoring for the configured links (the default option) or to select the hosts to monitor by adding them to the "Monitoring hosts" dropdown.

IPSec Site-to-Site VPN

Configuring site to site tunnels using IKE/IPSec is one of the biggest similarities between both products.

TMG is known for the simplification of configuring these tunnels, but it also introduced troubleshooting issues for advanced admins due to the absence of tools to accurately troubleshoot IPSec issues (when compared to its predecessor ISA server 2006).

The configuration of IPSec tunnels in Sophos UTM doesn't feature TMG's excellent wizard, but to admins familiar with TMG's advanced configuration it will look quite similar.

Sophos UTM configures a tunnel in three steps: 1) set the remote gateway, 2) configure a (or select a predefined) IPSec policy and 3) combine the remote gateway and the policy in a new IPSec connection.

Each step has its own tab in the IPSec configuration menu (as shown in figure 13), reducing the chance of confusion or configuration misinterpretation.



Figure 14 - Sophos Site to Site IPSec VPN menu

Remote gateway

The Remote gateway configuration covers the settings at the remote end of the tunnel, where one configures the tunnel endpoint, authentication settings and the tunneled subnet(s), along with more advanced options such as Path MTU discovery. TMG doesn't have a separate menu for this, but these settings are covered in the "Addresses," "Connection" and "Authentication" tabs of TMG's configuration.

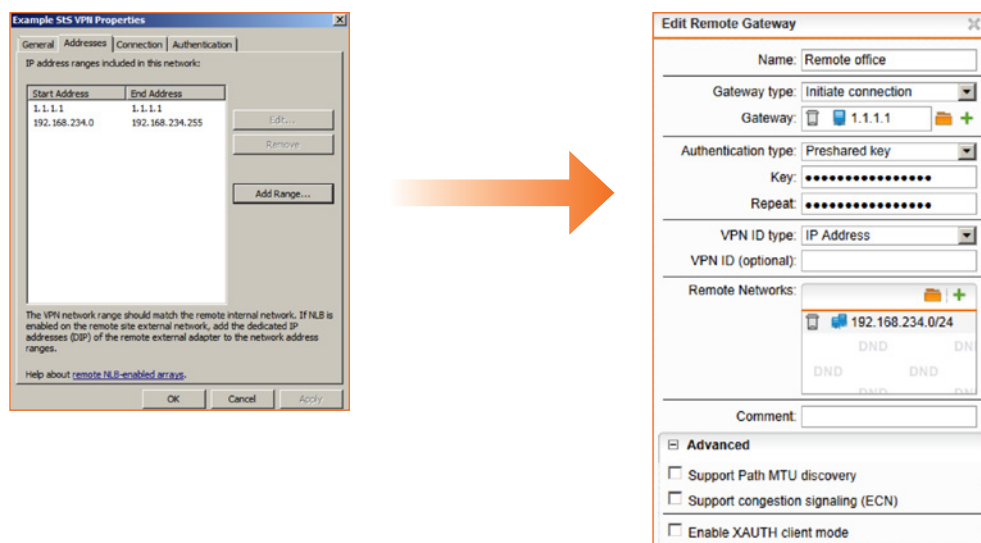


Figure 15 - TMG IPSec vs Sophos UTM

Policies

All settings covered under Policy in Sophos UTM apply to the phase 1 and 2 configurations of the IKE-IPSec tunnel and they function much like those found under the "IPSec settings" in TMG's "Connection" tab. There is little difference between UTM and TMG here, except that Sophos UTM labels the IKE settings "IKE <setting>" instead of "Phase 1" and the IPSec settings "IPSec <setting>" instead of "Phase 2" and the broader support for cryptography standards UTM offers (UTM adds Blowfish, Twofish and Serpent encryption algorithms, SHA2 384bit and SHA2 512bit authentication algorithms and Diffie-Helman Groups 14, 15 and 16 for IKE and AES CTR, Blowfish, Twofish and Serpent encryption algorithms, SHA 2 96bit mode for authentication algorithms, and Diffie-Helman groups 14 – 16 for IPSec).

Lastly, Sophos UTM gives administrators the option to enable "Strict Policy," which enforces the tunnel policy more strictly and will not allow negotiation if the tunnel settings do not exactly match on both ends of the tunnel. This is the default behavior in TMG (among many others, such as many Cisco routers), but many TMG admins find this helpful in troubleshooting VPN negotiation issues.

Connections

Needing to configure a VPN connection by combining the previously configured elements might seem foreign to a veteran TMG admin, as TMG essentially did this automatically.

The downside to TMG's approach however is that IPSec settings and gateways could not be reused in other rules, requiring a TMG admin to manually edit these settings for each new tunnel, which can become quite cumbersome when administering a large amount of tunnels (e.g., in a corporate branch network scheme).

Sophos UTM alleviates the manual labor by allowing administrators to reuse these settings for multiple tunnels, which enables simultaneous tunnel reconfiguration and faster deployment of new tunnels.

The settings stored in an "IPSec connection" combine the Remote gateway (to determine the tunnel endpoint, tunneled subnet and authentication) and a previously configured Policy (to determine the cryptographic and authentication algorithms used) with the local subnet(s) allowed in the tunnel, the interface UTM should use as the local tunnel endpoint and some advanced features (such as "Strict Routing", "Bind tunnel to Local Interface" and "Automatic Firewall Rules").

Strict Routing functions like the Strict Policy setting in that it more strictly enforces routing policy settings. Traffic is not allowed to enter the tunnel if it doesn't specifically match the configured networks. This is a default setting on TMG, but having the option to turn this off enables easier troubleshooting and improved compatibility with multiple vendors.

"Bind Tunnel to Local Interface" forces the Local Network traffic to reach UTM through a specific interface if it wishes to enter the tunnel. Any traffic reaching the UTM through another (internal) interface will be dropped. This allows for stricter filtering and multi-tenancy setups.

Add IPsec connection

Name: Remote office

Remote Gateway: Remote office

Local Interface: Outside

Policy: AES-128

Local Networks

Internal (Network)	DND	DND	DND
	DND	DND	DND
	DND	DND	DND
	DND	DND	DND

☒ Automatic Firewall Rules

☐ Strict Routing

☐ Bind Tunnel to Local Interface

Comment:

Save Cancel

Figure 16 - Sophos UTM IPSec connection

The "Automatic Firewall Rules" option automatically creates a firewall rule in the UTM firewall that allows traffic from and to the configured networks. This is similar to the access rule created in TMG's Site-to-Site connection wizard, but without the option to select the tunneled protocols (UTM enables all traffic by default). If such fine-tuning of firewall rules is required for your setup, refer to Chapter 1 on Firewall rules.

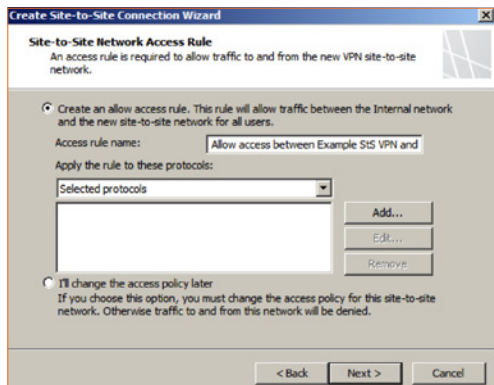


Figure 17 - TMG StS Wizard Access Rule

L2TP and PPTP Client VPN

Configuring client access VPNs in TMG requires admins to follow steps in the GUI and apply the configuration, which makes for a fairly simple deployment.

During these steps an administrator determines the interface the VPN users connect to, the number of – and which – users are allowed, the address assignment method, the desired VPN technology, EAP options and (in the case of L2TP over IPsec) the IPsec settings.

Afterwards the administrator configures both access rules and routing rules for the VPN users and enables the incoming VPN users to connect.



Figure 18 - TMG client VPN configuration

Sophos has further simplified this deployment process by condensing the entire task of configuring client VPNs to a single page per technology, supplying preconfigured IP pools for client assignment and automatically configuring routing for the remote users.

Configuring PPTP client VPNs is therefore as easy as enabling the technology, selecting the users and creating a firewall rule for them.

Configuring L2TP VPNs is almost as simple, though it requires administrators to additionally set IPSec related attributes such as the incoming interface, the authentication type and the preshared key or X509 certificate.

There is one important difference though: Both PPTP and L2TP VPN types can only use local or RADIUS based users, so you cannot use native AD users and groups as with TMG.

Differences

There are quite a few more differences to be found between Sophos UTM and TMG. Sophos UTM not only offers support for more networking settings, but also for many more networking technologies. This section describes the biggest discrepancies between both products.

NAT

ISA administrators rejoiced when Microsoft announced it would add NAT control as part of the Enhanced Networking features, as this finally allowed more flexibility in configuring which networks should be NATted, and which IP addresses should be used.

TMGs implementation is not without drawbacks though. Configuring IP addresses or IP pools that are not part of the interface that the traffic is traversing is impossible due to lack of Proxy ARP, for example. Another issue is the inability of TMG to NAT traffic inside a VPN tunnel making it virtually impossible to resolve overlapping subnet issues without a compromise.

Sophos UTM on the other hand has very advanced NAT controls, allowing for almost any kind of NATing scheme, including configuring non-interface IP addresses and pools, NATing entire networks and protocol manipulation during NAT translation.

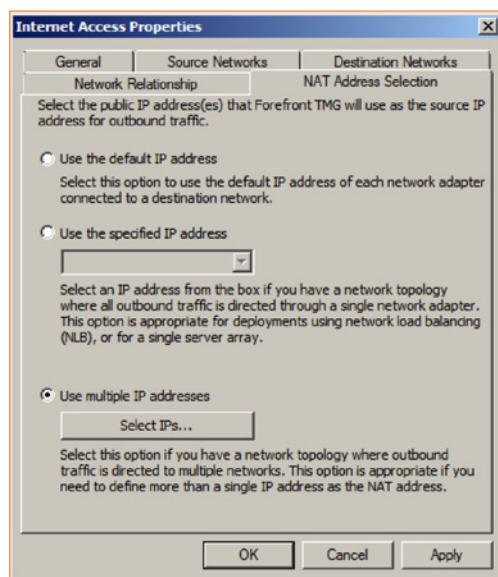


Figure 19 - TMG NAT settings

The implementation of advanced options is outside the scope of this guide, which focuses on mimicking TMG's functionalities and will therefore concentrate on just the configuration of Masquerade and Source NAT and rules using static IP addresses.

- › **How to do this in UTM:** To configure the Sophos UTM equivalent of the NAT address selection in TMG go to Network Protection -> NAT. Here you'll find two tabs: "Masquerade" and "NAT." Both tabs allow an administrator to configure a NAT rule, the difference is that Masquerade only allows for broad traffic selection and does not allow for protocol manipulation, whereas the Source NAT option under the NAT tab does.

Setting up Masquerade is fairly straightforward, and will NAT any matching traffic to a configured IP address on a specific interface. Just select the interface, the IP address you wish to use (or use the primary IP address, which is the default setting) and the network(s) that should be translated.

Source NAT changes the source of a data packet and alters some of the associated properties of said packet. Configuring a Source NAT rule is very similar to configuring Masquerade, but the latter requires you to configure the source, protocol and destination of the traffic instead of just setting the source. Furthermore, administrators have the option to select which IP address and interface to NAT the traffic to, along with to which protocol the traffic should be translated.

Figure 20 - Masquerade NAT in Sophos UTM

An interesting addition is the option to automatically create a firewall rule for the associated traffic, such as VPN traffic. The automatically-created firewall rule will match the exact settings in the firewall rule and thus allow only the configured source, protocol and destinations set in the NAT rule.

Figure 21 - Sophos UTM Source NAT

Missing functionality

There are some unique TMG features that cannot be replaced by Sophos UTM. Here, we discuss these functionalities and provide alternative solutions and workarounds wherever possible.

Dynamic routing – RIPv2

Neither TMG nor ISA server feature extensive support for dynamic routing protocols. Where ISA server support just the OSPF and RIPv2 protocols, Microsoft removed even more routing functionality in TMG, which only supports RIPv2.

But despite these limitations, the dynamic routing capabilities in both ISA and TMG were welcomed by administrators, as it allowed them to automate route distribution. Even if it meant they had to preform route redistribution or other workarounds later on to allow for interoperability with the rest of their network.

Sophos UTM has no support for the Routing Information Protocol (RIP), but instead offers the superior OSPF (Open Shortest Path) and iBGP and eBGP (interior/exterior Border Gateway Protocol) routing protocols as alternatives.

- **How to work around this:** Both OSPF and BGP are available on Sophos UTM and can be configured through the Interfaces & Routing configuration menu.

While the both protocols are beyond the scope of this guide, enabling them is quite simple to anyone familiar with these protocols.

OSPF configuration

In order to enable dynamic (OSPF) routing, first enable a forwarding interface in the "Interfaces" tab, along with the authentication type used on said interface (Plain-text or MD5). Next, configure a new area under the "Area" tab by setting a name, area-id, area type (normal, stub, nssa, stub no-summary or nssa no-summary), authentication type (off, plain-text or MD5) and cost associated to this area. This area is then associated with a forwarding interface and any virtual links that might be active in the area.

Lastly, set a router ID in the "Global" tab and click the slider to enable the routing protocol. If needed, route redistribution can be configured through the "Advanced" tab, by selecting which routes are to be redistributed and whether or not a static default route should be advertised.

BGP configuration

BGP routing configuration consists of configuring at least one neighbor (by setting a name, IP address, AS number and authentication type (along with any possible filters and route-maps if required)). Afterwards, you can then enable the routing process and set the AS number, router-ID and networks to advertise.

Route maps and filter lists can be configured under the tabs "Route Maps" and "Filter Lists" if required.

Redistribution

If RIPv2 interoperability is required, a popular workaround is to redistribute the routes from the internal network to Sophos UTM and vice versa through an external router.

SSTP VPN

With the introduction of Windows Vista, Microsoft introduced its own SSL-based VPN technology dubbed "SSTP" or Secure Sockets Tunneling Protocol, which enabled Windows users to securely connect to their work infrastructure over HTTPS without the need for a separate client. This technology has since been implemented in every Windows version released, but has been largely superseded by Microsoft's own DirectAccess tunneling protocol, which offers similar functionality with the added benefit of requiring no user interaction to establish.

Due to the proprietary nature of SSTP (Microsoft owns the source code and has been reluctant to license or share the technology with third parties), Sophos UTM cannot offer support of this protocol.

- **How to work around this:** Sophos UTM offers both our own SSL VPN solution (which works on Windows XP SP3 and up and requires its own client) and our clientless HTML5 VPN portal (which works completely OS independent and requires no client software) which can tunnel specific applications to the end user as workarounds.

SSL VPN

Setting up SSL Client access VPN is very simple and closely follows PPTP and L2TP configuration steps, complete with preconfigured IP address distribution configuration.

To configure a new connection, create a new "Remote Access Profile" consisting of a name, the appropriate users (AD is supported along with RADIUS and Local in contrast with the PPTP and L2TP options) for this connection and the networks these users should have access to.

The option to automatically create firewall rules is present here as well and works completely similar to PPTP and L2TP options.

The major difference between SSL VPN and the other client VPN options is that SSL VPN offers additional configuration through the "Settings" and "Advanced" tabs, which are used to set the incoming interface, signing certificate, tunnel cryptography, IP Pool and content compression characteristics of the connection.

To further simplify the distribution of the SSL VPN software, Sophos adds a preconfigured SSL VPN client installation package to the user portal, so each user authorized to use the tunnel can download and install the package (complete with required settings) in just a few clicks.

HTML 5 VPN Portal

The HTML 5 VPN Portal is a revolutionary new approach to remote access that allows the streaming of certain applications (RDP, Telnet, SSH, VNC, HTTP and HTTPS) to a webpage, requiring no specific components on the client machine. This portal is available as a part of the user portal to further simplify the deployment.

To configure the HTML 5 VPN Portal, select an application to publish and then set the appropriate configuration parameters such as name, connection type, destination system and allowed users. For applications and/or websites requiring authentication, Sophos UTM adds the option to automatically log in to the published resource using the credentials entered by the administrator.

Figure 22 - Sophos UTM SSL client VPN

Dynamic WPAD

WPAD (Web Proxy AutoDetection) is an IEEE-standardized technology used to automatically distribute proxy settings to WPAD-capable web browsers.

TMG supports the dynamic generation and distribution of the required settings by enabling the option "Publish automatic discovery information for this network" option in the "Auto Discovery" tab of each (local) interface, which creates a custom wpad.dat file with settings specifically tailored for the users in said network. These settings are also automatically updated every time any significant (proxy-related) setting is change on TMG.

This functionality is not available in Sophos UTM, but the option to manually create a WPAD or Proxy.pac file and have UTM distribute it exists.

- How to work around this:** To configure a manual proxy WPAD or PAC file, enable the option under the "Misc" tab of the Web Protection -> Filtering Options submenu. In the dropdown below, an administrator can copy and paste the desired configuration of the file. This is outside the scope of this document, but for syntax, functionality and content information, visit <http://findproxyforurl.com>.

Figure 23 - Sophos UTM WPAD configuration

3. URL filtering and malware inspection

URL filtering and malware inspection was added to TMG mainly due to the popularity of third party addons for ISA, such as GFI's Webmonitor, that provide these services on a subscription basis.

Microsoft copied this model for its own Forefront Protection functionalities, charging a recurring fee on a per-user basis as part of the Enterprise Agreement contract. Sophos uses a similar subscription model for its Web Protection component.

Similarities

Due to the similar goals and functionalities, the URL filtering features in TMG and those found in Sophos UTM share are quite similar but some might be difficult to grasp due to interface differences. This section highlights the similarities between the products for day-to-day operations.

General configuration

While the configuration in TMG and Sophos UTM might appear to have little in common at first glance, due to Sophos' approach to firewall rules, the actual URL filtering rules have quite a bit in common. By comparing them side-by-side the similarities between both products become apparent.

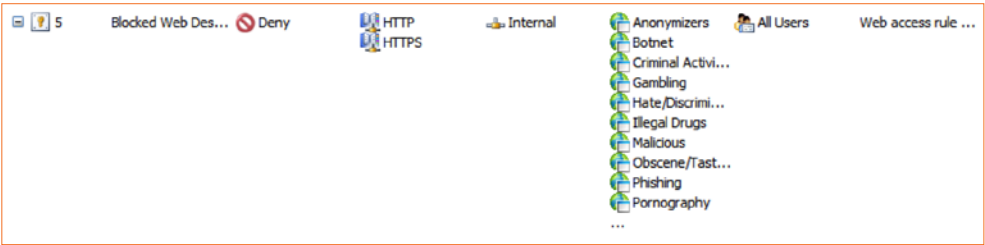


Figure 24 - Microsoft TMG URL Filtering

While Sophos UTM does not feature a similar summary overview, the "Policies" tab of the Web Filtering configuration does offer some "at a glance" information.

Active	Name	Users/Groups	Time	Filter Action	
1	Default content filter profile assign...	Any	Anytime	Default content filter action	

Figure 25 - Sophos UTM Web Filtering policies

As with the firewall rules, the configuration might seem foreign at first, but when the familiar TMG elements are overlaid, the picture becomes clear, as demonstrated below.

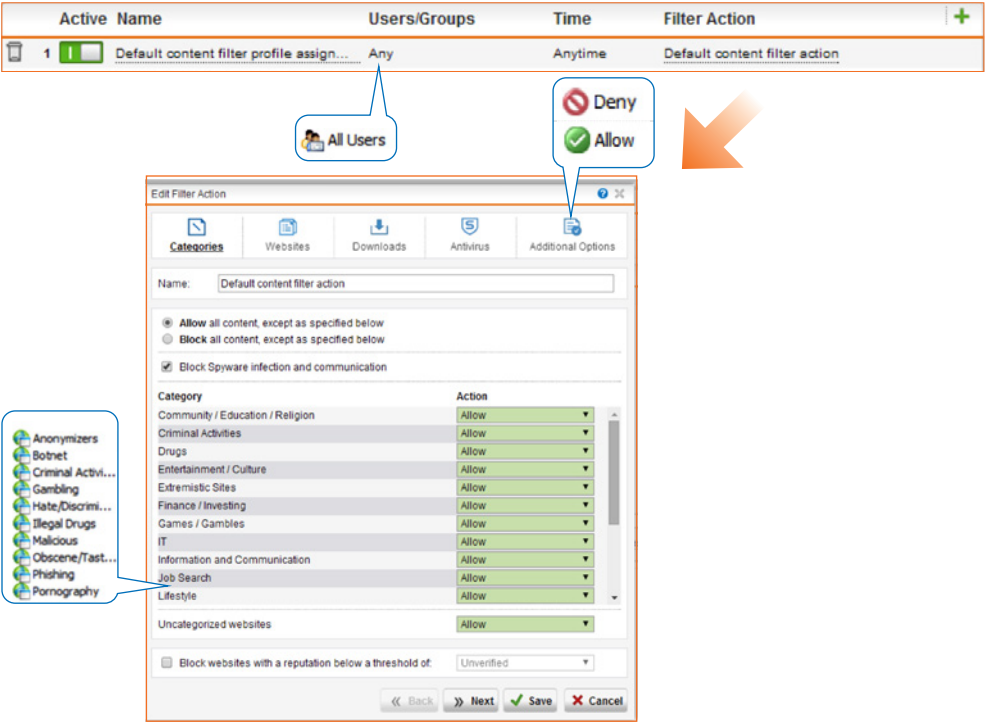


Figure 26 - Sophos UTM Web Filtering Filter actions

The rest of the settings from the displayed TMG URL filtering rule are found on the "Web Filter Profile" tab (or the "Global" tab if you are configuring the default profile):

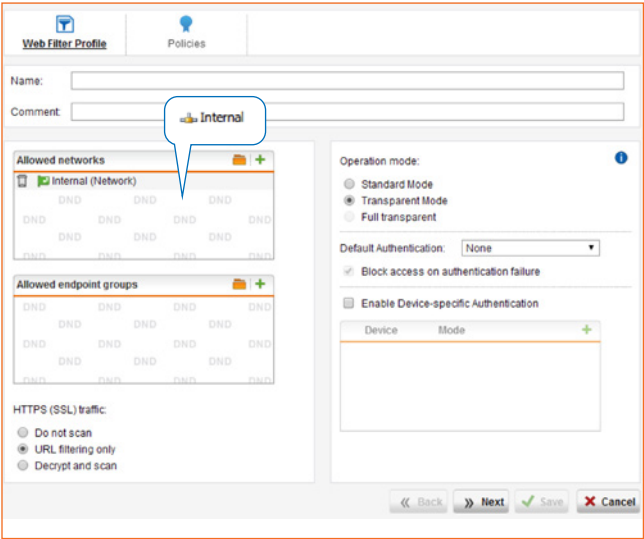


Figure 27 - Sophos UTM Web Filtering Profile settings

So while the interface is vastly different, configuring URL filtering still consists of setting a source network for the traffic, selecting the users the filter should apply to and determining the filter action (allow or block) and the categories of websites to be filtered.

This is true for other parts of the filtering configuration as well, such as creating URL Category Sets in TMG. Category sets create a summary of different categories in TMG to allow for easier configuration and management.

Sophos uses a similar approach to URL Filtering Categories, which consist of many sub-categories. Creating your own URL Filtering Category works exactly the same as it did in TMG. First, create a new Category and then select the applicable subcategories from a list. These settings are found under Web Protection -> Filtering Options -> Categories by clicking "+New filter category."

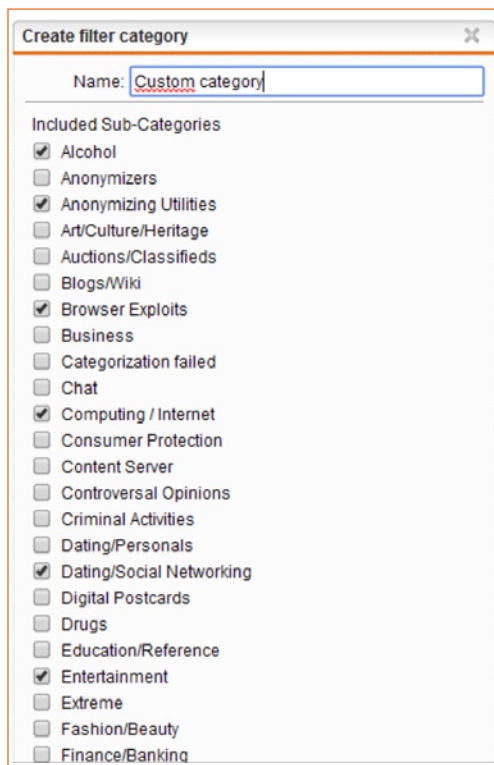


Figure 28 - Creating custom URL filtering categories in Sophos UTM

URL filtering overrides

Another area where the similarities between both products really shine is in the configuration or URL filtering exceptions.

Creating URL filtering exceptions in TMG was done by going to the "Web Access Policy" view and opening the "Create URL category override" tool in the toolbox. Any exception configured here was applied on a system-wide level, every user or source network would use the configured exception.

Sophos UTM features a similar URL categorization override functionality, which can be accessed through Web Protection -> Filtering Options -> Websites. A new category or reputation override can be configured by clicking "+New Website" which prompts a popup where the URL, domain, IP address or IP range to override can be entered. The new appropriate category can then be selected from the drop-down menu directly below the textbox.

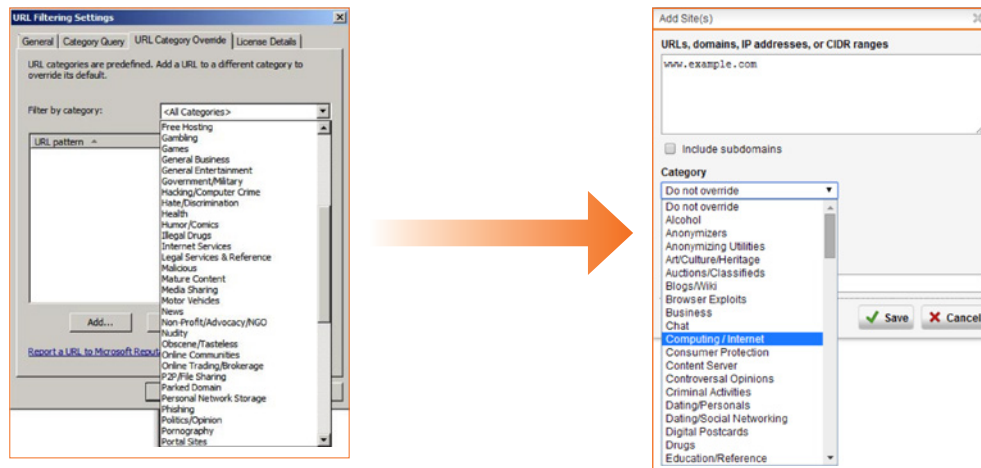


Figure 29 - TMG – UTM URL override comparison

Another way to override a URL filter in TMG is to add a rule-specific exception based on the URL or domain name of the object (HTTP rules allow for URLs and domains, whereas HTTPS rules allow only for exceptions based on domain name). These exceptions function as a whitelist or blacklist based on the rule action; a rule that allows traffic would make any exception a blacklist item, a rule that denies specific traffic would work as a whitelist.

Sophos UTM includes this exact same mechanism, but instead of configuring exceptions, administrators can directly configure whitelisted and blacklisted websites based on domain (including subdomains) or a regular expression, as part of any filter action as a part of the "Websites" configuration item.

Differences

As a result of the different underpinnings of the systems, there are bound to be some differences in functionality between TMG and Sophos UTM. This section covers some of the biggest differences between the systems, and how they affect configuration.

User-based override

Microsoft first introduced user-based overrides in TMG for web filtering rules to minimize the workload on IT staff by allowing users to self-service false positives and incorrectly blocked resources on a rule-by-rule basis. This freedom to override can be time-based and limited, and comes with additional logging options to track abuse. Administrators even have the option to inform the users about the consequences of the override through a configurable message on the "Website blocked" page.

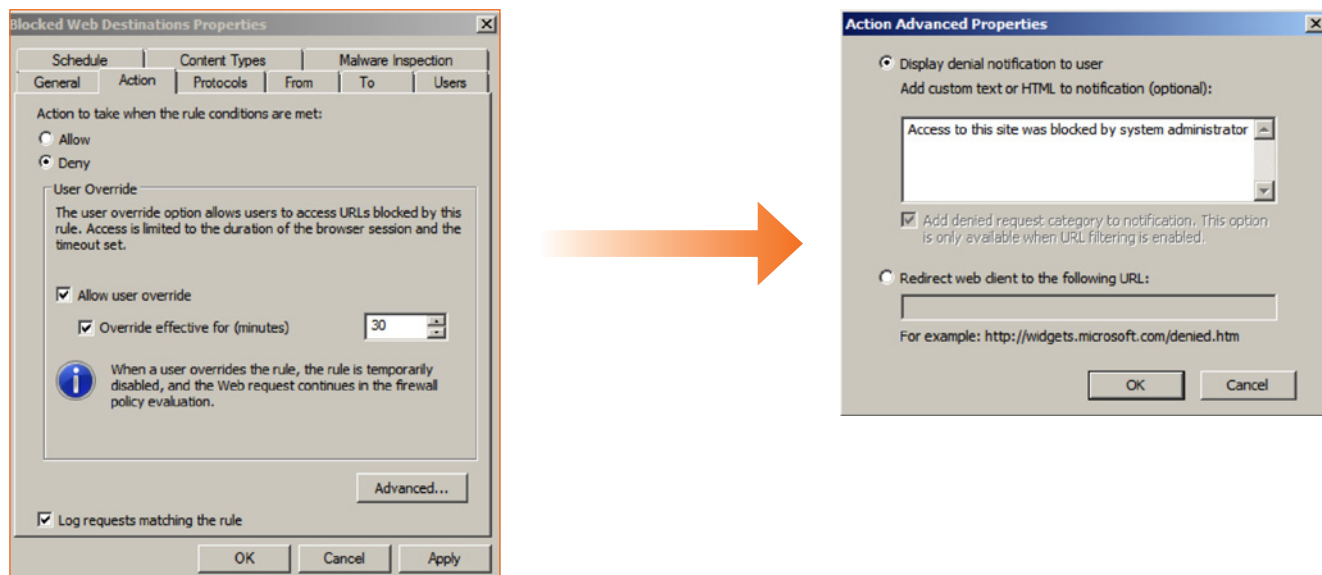


Figure 31 - TMG user-based override for web filtering

- How to do this in UTM:** Sophos UTM features a similar functionality called "Bypass users," complete with extended logging, but lacks the functionality to configure this on a per-rule basis. This means that any users allowed to perform overrides will be able to do so, regardless of the Filtering Actions configured for their network. UTM also lacks the ability to restrict this behavior on a time-of-day basis like TMG can.

To configure user-based overrides, an administrator enables the functionality under Web Protection -> Filtering Options -> Bypass Users by adding a user or group of users to the dropdown.

Modification of the notification users receive is also possible by going to Management -> Customization -> Web Messages. Here, select the message you wish to edit from a dropdown menu and enter new or revised text in the textbox below.

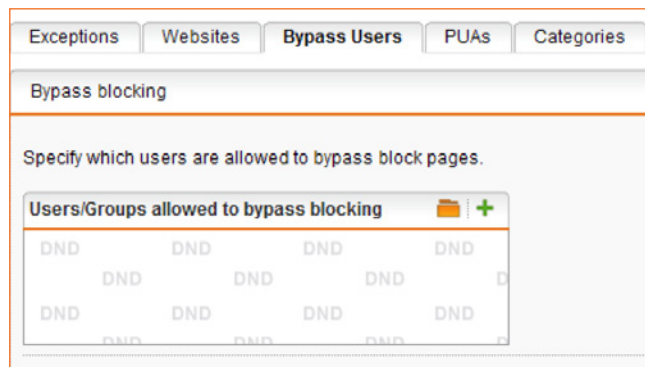


Figure 32 - Sophos UTM bypass users configuration

Anti malware

The Anti Malware component in TMG is based on the Forefront antivirus solution and uses Microsoft's own engine (during the TMG beta admins could choose between 5 different malware engines, but the functionality of these engines has since been concatenated into a single entity).

- › **How to do this in UTM:** Sophos UTM uses two engines for malware filtering: its own engine and Avira. You can enable scanning on one or two engines, a tradeoff between speed and scanning thoroughness. These settings can be altered on a per profile basis, under the "Antivirus" items.

A noteworthy difference in the malware scanning applications of TMG and Sophos UTM is the customization of TMG's "trickling" system. Both TMG and Sophos UTM have a mechanism that intercepts large downloads and places them in a cache on the firewall instead of streaming them to the client directly. This speeds up the download process from an end-user perspective, as they will not need to wait until the entire file is scanned in order to see progress in their browser.

Microsoft allows admins to pick which filetypes / contenttypes should be delivered via the "standard trickling" system, which downloads the file to TMG using the mechanism discussed above, and which should be delivered through the "fast trickling" system, which only scans the first 1% of the file before sending the rest of the file directly to the client without any interruptions like the standard system.

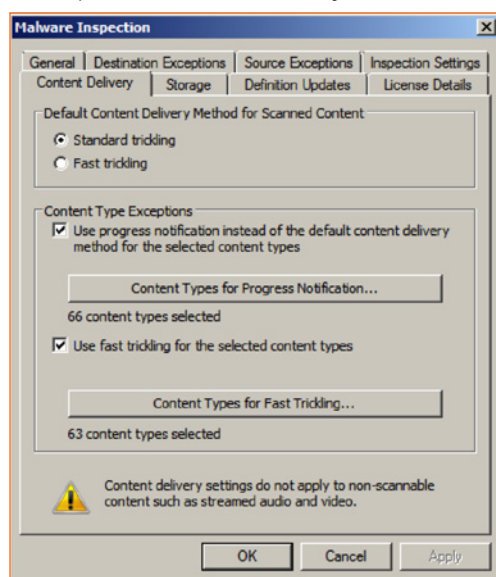


Figure 33 - Trickling configuration in TMG

- › **How to do this in UTM:** Sophos UTM does not have these configuration options and instead determines which files should be delivered directly based on a predetermined list of file and content types. These are engineered to not interfere with real-time applications such as streaming video and audio.

Also, TMG has an option to fine-tune the inspection settings by determining parameters such as the maximum allowed archive level depth and what to do with broken or encrypted files. Administrators can also select whether TMG should attempt to clean infected files (or drop them), how long scanning is allowed to take and predefined size limits for downloads in both archived and unarchived state.

- › **How to do this in UTM:** Sophos UTM also features customization for malware filtering parameters, but only allows administrators to set a maximum scannable file size limit and a maximum download filesize limit. One advantage UTM has over TMG is the option to use our reputation engine to recognize PUA (Potentially Unwanted Applications) downloads and filter them according to company policy.

As already mentioned, Sophos UTM is fully capable of filetype and MIME filtering of HTTP-based access rules like TMG and even enables administrators to configure this type of scanning for HTTPS traffic as well.

- › **How to do this in UTM:** To configure which files are blocked, open the "Downloads" menu of a Web Protection profile.

Here, administrators can not just block downloads based on extension or MIME type, but also can define which filetypes will trigger Sophos UTM to generate a warning for the endusers when they attempt to download such a file.

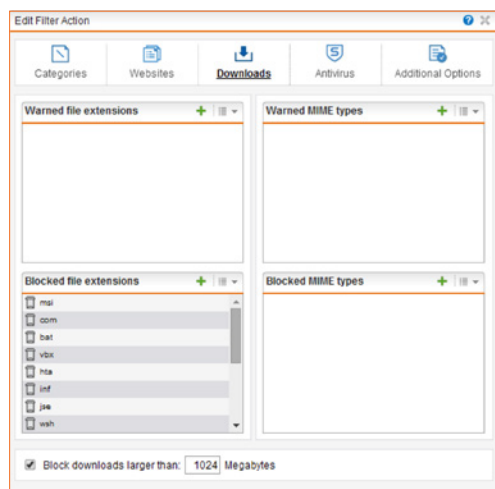


Figure 34 - Sophos UTM download settings

The last aspect of malware inspection in TMG to be examined is the ability to create malware exceptions based on a source or destination basis. These exceptions can be created on a URL, domain or IP address basis by adding network objects to the exception list.

- › **How to do this in UTM:** This functionality is configured under the "Exceptions" tab of Web Protection -> Filtering Options. These exceptions allow for the skipping of any part of Web Protection in UTM, ranging from download size blocking to content filtering.

Filters can be applied based on source network, source endpoint group, source user (group), a specific URL destination or on a URL category. Administrators even have the option to perform logical AND and OR operations between these criteria, allowing for very precise filtering.

HTTPS inspection

HTTPS inspection has always been a weak point of TMG due to a lack of wildcard support. That is, any website using a wildcard certificate would be dropped by TMG due to having non-matching SSL certificates. As a result, this feature went mainly unused due to the enormous number of false positives.

A redeeming quality of this feature is that Microsoft went out of its way to make the general process of HTTPS Inspection as simple as possible by allowing administrators to push the signing certificate to the clients who use Active Directory with a single click.

- › **How to do this in UTM:** Sophos UTM has support for wildcard certificates and allows HTTPS inspection through two modes: "URL Filtering Only" and "Decrypt and Scan," which are configured either as part of the "General" configuration in Web Protection or as part of the "Web filtering Profile" settings in a web filtering profile.

"Decrypt and Scan" will appeal to many TMG administrators, as it allows Sophos UTM to function as simply as the setup in TMG. This mode does not require any reconfiguration by the client (not even pushing a signing certificate) because Sophos UTM will not actively decrypt the traffic. Instead it uses the SNI (Server Name Indicator) field of the data packets to determine the destination of the web traffic and apply URL filtering rules based on this.

The limitation of this option is the inability to inspect traffic for malware, as UTM cannot read the (still encrypted) datapackets.

If your organization requires full malware inspection on all traffic, including HTTPS, enable the "Decrypt and Scan" option. This will perform a regular man-in-the-middle-attack and intercept all traffic from the client to the internet by impersonating the requested resource. This will require distribution of the signing certificate or importing an already trusted certificate from an internal Certification Authority.

In both cases the administrator has to open the Certificate Management item under Web Protection -> Filtering Options -> HTTPS CAs. Here, either click "Upload" to upload a new signing certificate from an internal CA, or click "Download" to download the UTM's current signing certificate to redistribute manually.

Missing functionality

There are some unique TMG features that cannot be replaced by Sophos UTM. Here, we discuss these functionalities and provide alternative solutions and workarounds wherever possible.

Secondary categories

Microsoft's URL filtering is based on the Microsoft Reputation Services webservice, which contains filtering information from a large number of participating companies. Websites are ranked based on their reputation, and filed on a primary and secondary category basis. This means that a website that sells shoes and hosts fashion news will have a high rank in the "Online shopping" category and a moderate ranking in the "Fashion" category.

By default TMG will only filter on the primary category, but when needed, administrators can enable filtering on secondary categories on a rule-by-rule basis.

This allows for an unprecedented level of control by which TMG admins can block only the parts of a website that fit the offending category and make sure that other parts are available due to belonging to another category.

Or, alternatively, it can be used to block URLs that would otherwise slip detection due to being allowed on the primary category (so in the previous example, if the configured policy called for blocking all fashion websites but allowing web shopping, the website would have been allowed). Filtering on secondary categories allows administrators to still block this site based on the secondary category assigned to it.

Sophos UTM does not use secondary filtering categories and can therefore not function as TMG would.

- › **How to work around this:** If a website slips through the filtering criteria configured, an administrator has two options: add the website to a category as an override (as detailed in "URL Filtering Overrides" above) or add the website to a whitelist or blacklist as part of the filter actions of the offending profile (detailed in the same section).

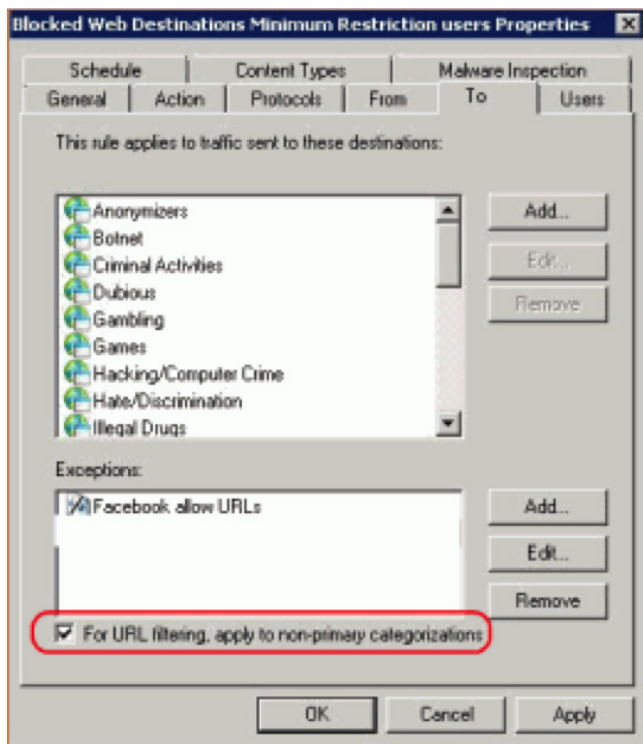


Figure 35 - TMG non-primary category filtering

4. Publishing rules

Publishing rules are one of TMG's strongest features, and a major reason for the product's popularity. Publishing rules allow internal resources to be securely exposed to the public internet by having TMG function as both a filtering platform and web application security engine.

The biggest benefit of the publishing feature is TMG's ability to function as a reverse proxy for the internal resources. This means TMG can impersonate the actual resource, which allows for detailed scrutiny of any command sent to the backend server and negates any attacks that might target the vulnerabilities in the protected resources. TMG will request content from a resource on behalf of a client, never allowing the original traffic to reach the published resource directly. So even if an attacker succeeds to exploit a vulnerability in a published resource, the result is that TMG now has unintended privileges on the published resource, but never the attacker's machine.

These impressive functionalities have been expanded by Microsoft to also include offloading and delegation of authentication, allowing TMG to function as a complete black box for any traffic sent to the published resource. The added benefit is that TMG knows the credentials of the users trying to access the published resources, and can perform Single Sign On for any published resource by delegating the already known user credentials to any backend system requiring authentication.

Similarities

Sophos UTM has had a strong reverse proxy and web application filtering engine for quite some time (aptly named "Web Application Firewall"), but with the 9.2 release these features now include TMG-like reverse authentication functionalities. This allows Sophos UTM to closely match most TMG functionalities. This section documents these functional matches and the general TMG similarities in Sophos UTM.

General configuration

To configure a publishing rule in TMG you must set both the internal configuration (server hostname or IP address, ports, virtual directories and hostheader values) which determines how TMG should communicate with the server and external configuration (through the Web Listener, which contains settings related to public IP, SSL and authentication) which determines how the end users reach the server.

Sophos UTM uses a similar scheme, whereby administrators configure a "Real Web Server" (which defines the internal hostname or IP, protocol and port of an internal server) with internal reachability settings and then use these settings in a "Virtual Web Server" where the settings get appended with settings related to external IP addresses, ports and SSL settings.

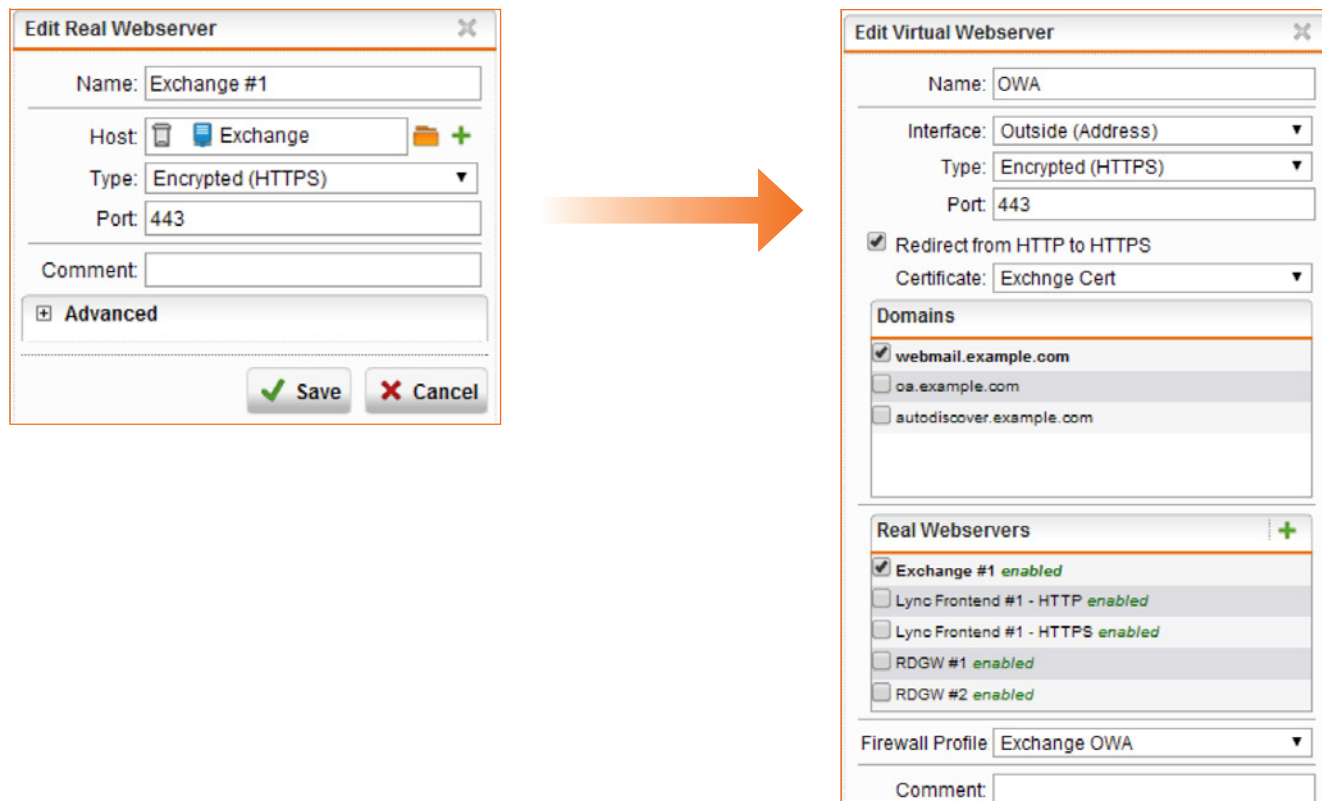


Figure 36 - Sophos UTM Real and Virtual server concept

Site path routing

Another resemblance between TMG and Sophos UTM is that both allow traffic for different paths on the same hostname to be routed to different backend systems. For example, you can send `www.example.com/public` to server A, while sending `www.example.com/private` to server B.

TMG administrators can configure separate publishing rules to determine which traffic should end up at which server, by defining the appropriate paths for each server in the "Paths" tab of the configuration.

Sophos UTM lets administrators configure which paths should be sent to which “Real Web Server” by editing or adding paths to the “Site Path Routing” tab and determining the source for this traffic from a list of servers.

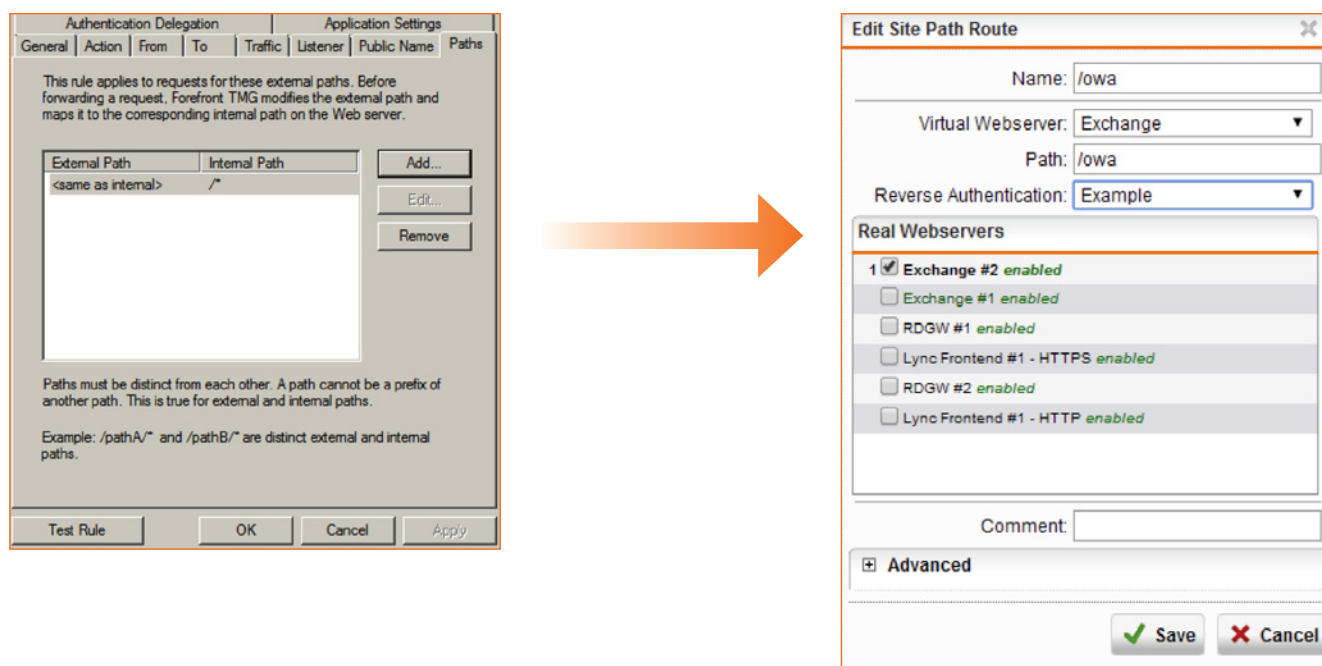


Figure 37 - Site path routing in TMG and UTM

Differences

This section discusses the differences between TMG and Sophos UTM and how they affect administration.

Web listeners

Microsoft ISA server 2004 introduced the concept of the Web Listener: a reusable component that tied one or multiple (public) IP addresses to an authentication scheme and an SSL certificate. This component could be used by publishing rules to instantly configure the appropriate security and addressing settings. This component also enabled Single Sign On by allowing all publishing rules sharing the same listener to share authentication credentials (as long as they were within the same domain name).

Sophos UTM does not use a concept like Web Listeners. Instead each published resource (called a “Real Server”) is associated with its own unique “Virtual Webserver,” which basically serves the same purpose as the Web Listener, but on a per-resource level.

- **How to do this in UTM:** To create a new Virtual Webserver, click the “+New Virtual Webserver” in Web Server Protection -> Web Application Firewall -> Virtual Webservers.

Here, set a name for the Virtual Webserver, select the IP address it should listen on, determine the protocol (“Plaintext” for HTTP, “Encrypted” for HTTPS) and set the port used by the Virtual Webserver.

Depending on the protocol selected, the next configuration steps are to enter the hostname(s) for the webserver in the "Domains" field (for HTTP) or enable HTTP to HTTPS redirection, select an applicable SSL certificate and then select the appropriate hostnames in the "Domains" field (for HTTPS).

The screenshot shows the 'Create Virtual Webserver' dialog box with the following configuration:

- Name:** (empty text field)
- Interface:** :: Please select :: (dropdown menu)
- Type:** Plaintext (HTTP) (dropdown menu)
- Port:** 80 (text field)
- Domains:** A list containing 'www.example.com' with a '+' button to add more domains.

Figure 38 - Sophos UTM HTTP Virtual Webserver

The screenshot shows the 'Create Virtual Webserver' dialog box with the following configuration:

- Name:** (empty text field)
- Interface:** :: Please select :: (dropdown menu)
- Type:** Encrypted (HTTPS) (dropdown menu)
- Port:** 443 (text field)
- ☒ **Redirect from HTTP to HTTPS**
- Certificate:** Exchnge Cert (dropdown menu)
- Domains:** A list containing 'webmail.example.com', 'oa.example.com', and 'autodiscover.example.com'.

Figure 39 - Sophos UTM HTTPS Virtual Webserver

The rest of the configuration is similar, as both require selecting a previously configured server from the "Real Webservers" field, or adding a new one by clicking the "+" button in the upper left corner of the field. The next step in setting up a Virtual Webserver is selecting a Firewall Profile (explained in the "Web Application protection" section below) and adding a comment in the "Comment" field if needed.

The advanced settings allow administrators to configure Compression support, HTML rewriting and Host Header Passthrough. With the exception of HTML rewriting (see "Link Translation" section), these work similar to TMG's option to remove a Web Listener from the "Return Compressed Data" list (found in the HTTP Compression settings) and the "Forward the original hostheader instead of the actual one" option of a publishing rule, respectively.

Web application protection

As mentioned in the previous section, Sophos UTM lets administrators configure specific protection parameters of a virtual webserver, unlike TMG. These settings are configured through what UTM calls the "Firewall Profile" which can be found under Web Server Protection -> Web Application Firewall -> Firewall Profiles.

- **How to do this in UTM:** Creating a firewall profile consists of naming the profile and setting the following parameters:
 - Pass Outlook Anywhere: used to allow RPC over HTTPS traffic
 - Mode (Reject/Monitor): the Mode setting refers to how UTM should treat detected threats. In Monitor mode UTM will allow the traffic even if it violates the configured protection settings, in Reject mode UTM will discard the traffic and reject the session.
 - Common Threats Filter: enables configuration of the following options:
 - Rigid Filtering -decreases tolerance on filtering rules
 - Skip Filter Rules -set the signature IDs that should be skipped
 - Protocol Violations -blocks any traffic not adhering to protocol definitions
 - Protocol Anomalies -blocks any content not normally associated with a specific protocol)
 - Request Limits -limits request length to prevent protocol abuse
 - HTTP Policy -blocks attempted HTTP attacks
 - Bad Robots -blocks known malicious web crawling engines and automated attacks
 - Generic Attacks -blocks attacks not associated to the other categories
 - SQL Injection Attacks -blocks attempted SQL Injection attacks
 - XSS Attacks -blocks cross site scripting attempts
 - Tight Security -reduce tolerance for the filter, increasing the likeliness of catching suspicious traffic by combining other filter elements
 - Trojans -blocks traffic and attacks from known Trojans and infected machines
 - Outbound -prevents leaking server-side information (such as session tables) back to the client
 - Cookie Signing
 - Intercepts and signs cookies generated by the real webserver, preventing cookie tampering
 - URL Hardening
 - Filters traffic by only allowing a specific set of URLs. These can be supplied by means of Google sitemap file, Google sitemap URL or manually
 - Form Hardening
 - Intercepts HTML forms sent by the backend application and makes sure the forms are only used as intended (blocking things such as entering URLs in a password field and such)

- Antivirus
 - Filters traffic sent to (Upload Only direction), sent from (Download Only direction) or bidirectional (Uploads and Downloads direction) for viruses and malware
 - This scan can be performed by either one (Single Scan mode) or both (Dual Scan mode) antivirus engines of Sophos UTM
- Block Unscannable Content
 - Blocks any content sent from or to the webserver that cannot be read due to encryption, archiving or corruption
- Block Clients with Bad Reputation
 - Blocks client IP addresses with a known bad reputation in Sophos Labs' database or in the Maxmind GeoIP database due to being involved in such activities as malware or spyware proliferation
 - Skip remote lookups for clients with bad reputation
 - Skips the database lookups in favor of GeoIP based filtering only, speeding up detection and processing

These settings can then be applied to the aforementioned Virtual Web Servers in the "Firewall Profile" dropdown menu.

Authentication

Authentication settings for Publishing Rules were set in two different places in TMG, on Web Listeners and on the publishing rules themselves. The first (Web Listeners) determines the applicable authentication backend system (Active Directory, RADIUS, TACACS, RSA), the second determines which users are actually allowed to access the resource (based on the user(s) or group(s) configured in the "Users" tab and the mode of delegation to be used on the backend).

The Web Listener also dictates the methods the users can use to provide their credentials (HTML Forms login page, HTTP 401 with Kerberos, NTLM or Basic authentication).

Sophos UTM combines these settings in the Reverse Authentication profile, which can be applied to Virtual Web Server(s) on a virtual directory basis, much like how TMG publishing rules work on a per-host, per-virtual directory/directories basis.

- › **How to do this in UTM:** Reverse authentication profiles are configured through Web Server Protection -> Reverse Authentication.

To create a new reverse authentication profile:

- set a name for the profile;
- select a frontend mode (the logon scheme presented to the end user(s) – "Basic" or "Form"), a frontend realm (this is either the title of the HTTP 401 logon popup [when using "Basic" frontend mode] or the URL of the page UTM uses for the "Form" logon prompt – this has to be a unique page that does not exist on the backend server), a form template (when using the "Form" frontend mode)

- set the backend mode ("None" delegates nothing to the backend, whereas "Basic" delegates the credentials received by the client to the real server using Basic authentication)

Figure 40 - Sophos UTM reverse authentication profile

After setting the general mode of operation, determine the user (groups) allowed to authenticate to the resource by adding user(s) and groups to the "Users / Groups" dropbox.

Figure 41 - Sophos UTM site path routing

To apply the settings configured in the reverse authentication profile navigate to Web Server Protection -> Web Application Firewall -> Site Path Routing tab. By editing an existing site path or when creating a new one, authentication can be appended to a certain path by selecting the previously configured reverse authentication profile from the "Reverse Authentication" dropdown menu.

URL forwarding

URL forwarding allows TMG to redirect incoming requests to another path using HTTP 302 messages. This can be used to redirect incoming HTTP traffic to HTTPS, as part of a Web Listener configuration, or to redirect incoming requests to an administrator-defined location when traffic is denied by TMG.

- **How to do this in UTM:** While there is no support for customer redirection in Sophos UTM, the 9.2 release introduced automatic HTTP to HTTPS redirection.

This is configured on a per Virtual Web Server basis, and automatically enabled when creating a new profile, but can be enabled on existing HTTPS-based Virtual Web Servers by ticking the "Redirect from HTTP to HTTPS" checkbox.

This will prompt any incoming traffic on port 80 to be redirected to the configured HTTPS port on the Interface/IP address associated to the Virtual Web Server.

The image shows a configuration window for a Virtual Web Server. It contains several fields: 'Interface' with a dropdown menu showing 'Please select'; 'Type' with a dropdown menu showing 'Encrypted (HTTPS)'; 'Port' with a text box containing '443'; a checked checkbox labeled 'Redirect from HTTP to HTTPS'; and 'Certificate' with a dropdown menu showing 'Please select'. The entire configuration area is enclosed in a light gray border.

Figure 42 - Sophos UTM HTTP-HTTPS redirection

Link translation

Link Translation is a powerful component of TMG that allows for the rewriting (on the fly altering) of any hostname that passes through the system. This can be used to translate hyperlinks using hard paths to the appropriate relative path, or to completely rewrite all content on a website to appear as if coming from www.example.com while actually being sourced from www.source.net.

Another popular way to deploy this technique is to alter any hyperlink on websites for which TMG provides SSL offloading from <http://> to <https://>, preserving the scheme of the website (and preventing unnecessary redirection).

While Sophos UTM does not support the former behavior, the latter has been incorporated into the Virtual Web Server configuration.

- **How to do this in UTM:** When creating or editing a Virtual Web Server under Web Server Protection -> Web Application Firewall -> Virtual Web Servers, open the "Advanced" settings by clicking the "+" sign.

To prompt UTM to translate all HTTP links to HTTPS in offloaded resources, tick the "Rewrite HTML" checkbox.

Please note that this will only be applied to translated resources, so any Virtual Web Server set to HTTPS that uses a Real Server listening on HTTP.

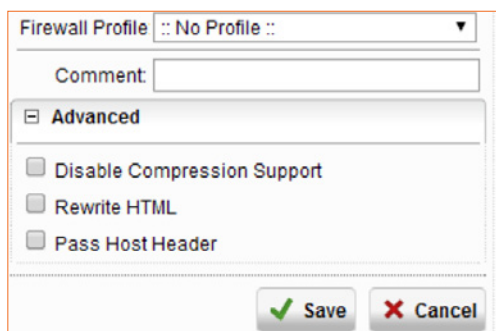


Figure 43 - Sophos UTM Virtual Web Server advanced settings

Missing functionality

There are some unique TMG features that cannot be replaced by Sophos UTM. Here, we discuss these functionalities and provide alternative solutions and workarounds wherever possible.

NTLM and Kerberos delegation

Sophos UTM does not support NTLM or Kerberos Constrained Delegation modes of authentication.

- **How to work around this:** Most applications that are configured to use Kerberos or NTLM authentication by default (such as Exchange and SharePoint) can be reconfigured to use basic authentication instead. Check the vendor's documentation and support information to determine if your application can be reconfigured for Basic authentication.

If the backend application requires the use of NTLM to properly function, there are third party programs that can be used to translate basic authentication to NTLM, such as APS (<http://ntlmmaps.sourceforge.net/>).

Please note that any third party applications used to perform these tasks are not supported by Sophos outside of the delegation of Basic authentication credentials to this backend. Any further troubleshooting or technical assistance should be acquired through the provider of the third party solution.

Default domain name

TMG allows administrators to configure a default domain name in the advanced settings of a Web Listener. This domain name would then be appended to any authentication credentials supplied to this Web Listener by the end user. This saves users the inconvenience of entering their credentials in the "domain\username" or "user@domain" UPN format.

Sophos UTM, by contrast, filters any authentication supplied through the reverse authentication from domain names. This can cause some issues for web applications that require a "domain\user" or UPN format.

- **How to work around this:** Most Microsoft-based products use the Windows IIS (Internet Information Server) component as a web server for their services, including the offloading of web-based authentication to this platform.

IIS allows for default domains to be appended to credentials received using Basic authentication, as explained in this Microsoft TechNet article: [http://technet.microsoft.com/en-us/library/cc772009\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc772009(v=ws.10).aspx)

X.509 client certificate authentication

Microsoft UTM has the ability to add X.509 client certificate checks to any Web Listener, allowing only those users that have a valid certificate to access the resource or post their authentication details to TMG.

Sophos UTM does not currently have this functionality.

- **How to work around this:** Depending on the intended functionality of the client certificates, a viable alternative would be to configure OTP (One Time Password) login using soft- or hardware tokens on UTM at no extra cost. For more information on this feature, refer to your user manual or <http://blogs.sophos.com/2014/02/21/whats-coming-in-sophos-utm-accelerated-9-2-4-safer-two-factor-authentication/>

Persistent cookies

TMG administrators can configure persistent cookies by editing the "Forms" settings on a Web Listener. These settings allow you to select which computers ("Public", "Private" or All) are eligible for a persistent cookie, and to determine the length of the cookie's validity.

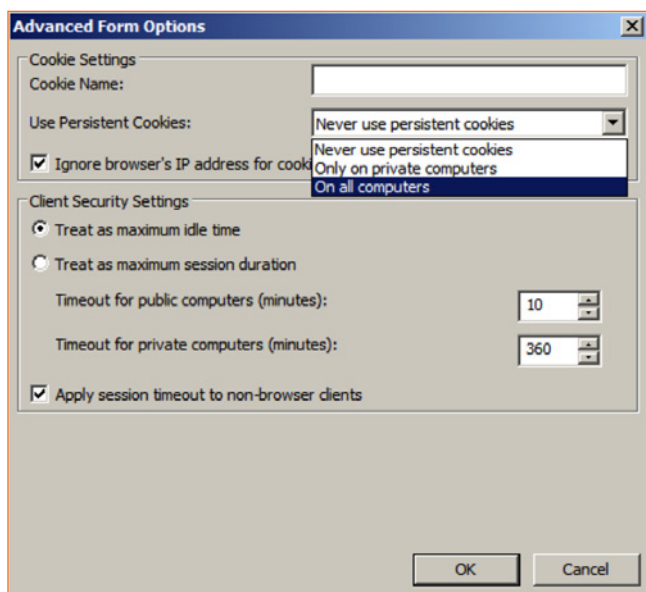


Figure 44 - TMG Web Listener Advanced Forms settings

These persistent cookies can then be used to enable cross-client authentication, such as between Internet Explorer and the Office suite when working with web services such as Microsoft's SharePoint.

Sophos UTM does not support this type of client authentication persistency.

- **How to work around this:** There are currently no workarounds for this feature, other than manually logging in for each application accessing the UTM-protected resource.

5. Email protection

Email protection is a feature Microsoft touted at the release of TMG but has fallen into disuse due to lack of support in recent years (most notably the lack of Exchange 2013 support). But the idea of integrating email filtering with a firewall is absolutely appealing and because of that, it is one of the most popular components in Sophos UTM.

Similarities

Since both Sophos UTM and TMG are basically protecting against the same threats (spam and malicious content), there are obvious similarities between the products. These similarities might be slightly obfuscated by the differences in user interface, but are quite obvious upon closer inspection.

Mail flow configuration

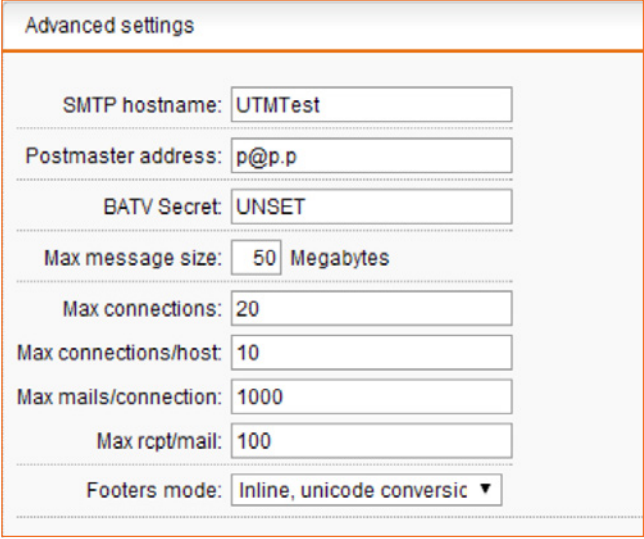
After enabling the Email Protection features in TMG, administrators have to configure the flow of mail by selecting the accepted domains, set the internal email server's IP address or hostname, select the interface to use for mail coming from the internet (for reverse ARP purposes) and determine the server response to HELO/EHLO messages.

Configuration in Sophos UTM is similar, apart from the selection of running the configuration in "Simple" or "Profile" mode which is used by UTM to enable running multiple email configurations simultaneously. The Profile feature will not be discussed in this guide, as TMG is unable to run multiple mail server configurations.

Configuration of the accepted domains and the internal server IP addresses/hostnames is configured under the "Routing" tab similar to TMG. Sophos UTM offers extended options by allowing mail to also be routed to a server based on MX records, enabling it to function as a relay for a public mail scenario (such as a hosting provider).

Settings related to the system's HELO/EHLO response are found under the "Advanced" tab of the SMTP configuration, where you can set settings such as the SMTP hostname, postmaster address, message size and other advanced configuration items in the "Advanced settings" section.

This is also where connection limits for the UTM email system are configured, along with size restrictions for SMTP messages, recipient limits and the BATV secret for the email system.



The screenshot shows the 'Advanced settings' tab for SMTP configuration in Sophos UTM. The settings are as follows:

Advanced settings	
SMTP hostname:	UTMTest
Postmaster address:	p@p.p
BATV Secret:	UNSET
Max message size:	50 Megabytes
Max connections:	20
Max connections/host:	10
Max mails/connection:	1000
Max rcpt/mail:	100
Footers mode:	Inline, unicode conversic ▼

Figure 45 - Sophos UTM advanced email settings

Anti-spam configuration

Anti-spam configuration in TMG consists out of several components found in most anti-spam products such as a whitelist (IP Allow List), blacklist (IP Block List), content filtering (keywords), Recipient and Sender filters, Sender ID and a Sender Reputation framework.

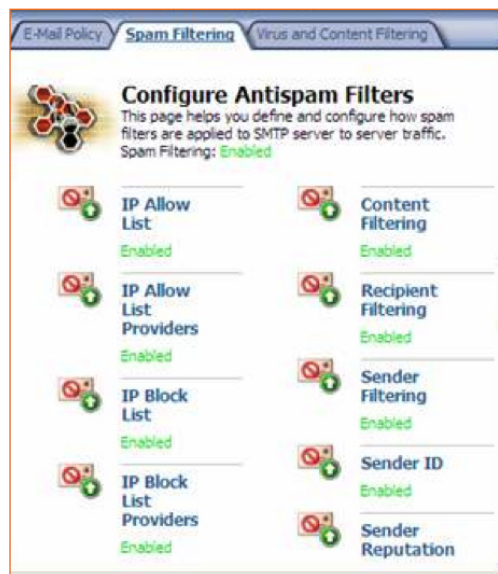


Figure 46 - TMG Email Protection antispam

All of these features are available in Sophos UTM and are configured in roughly the same manner as TMG. The only difference is that Sophos combines some of the configuration items in TMG.

All configuration related to spam filtering is located under the "AntiSpam" tab of Sophos UTM, which is part of the Email Protection configuration.

Blacklisting is found in the "Sender blacklist" section, which allows blacklisting IP addresses, email addresses and domains similar to TMG's configuration, including wildcard support. This feature combines both the Sender Filtering and IP Blocklist features of TMG.

Realtime Blackhole Lists combines the "-List provider" features in a single item. Realtime Blackhole Lists are configured in the "RBLs (Realtime Blackhole Lists)" and allow similar configuration as TMG's setup. You can only enable the service and configure any additional RBL providers if required.

Content filtering is also available in the "Expression filter" configuration section, which allows you to set a list of keyword with regular expressions, which will trigger UTM to drop the incoming email.

Other features such as RDNS checks, Greylisting, BATV (Bounce Address Tag Validation) and SPF (Sender Policy Framework) checking are also included in the antispam configuration of UTM.

The only feature not listed here is whitelisting, which is implemented in Sophos UTM as part of the "Exceptions" tab. Here you can determine, based on a multitude of characteristics (IP address, sender address and recipient address), if a packet should skip certain antispam checks or all of them, depending on the actual message.

Anti-malware configuration

The anti-malware component of TMG ("Virus and content filtering") has three filters for incoming malware: File filtering, content filtering and antivirus filtering.



Figure 47 - TMG Virus and Content Filtering

This is similar to Sophos UTM, which features content filtering, filetype filtering and antivirus filtering as part of the "Antivirus" configuration tab.

Content filtering takes place based on MIME type, and features a blacklist and whitelist approach, allowing administrators to specifically block the content they wish to target.

The File Extension filter in UTM takes care of filetype filtering by letting you submit the filetypes deemed unsuitable for your corporate environment.

Lastly, the antivirus component in the "Antivirus" section can be configured to use either one or two engines to scan emails, and you have the option to either block emails with confirmed malware or to quarantine them for later review.

Of interest in both the anti-malware and anti-spam configurations is that you have the option to reject confirmed bad email messages during transfer, reducing the load on the system and reducing the bandwidth waste generated by downloading all messages before scanning them. This is very effective against emails containing attacks specifically designed to overload a mail filtering system such as Sophos UTM (for example emailed archive bombs and such).

Differences

Apart from the interface differences, there aren't many real differences between TMG and Sophos UTM in terms of email protection. Sophos UTM does however add some functionalities not available in TMG. Some of these are discussed in this section and we will obviously omit the "→How to do this in UTM:" feature seen in previous chapters.

Mail manager

TMG has no built-in functionality to monitor and administer the flow of emails through the system, and relies on the Exchange Management Console for these tasks. This makes troubleshooting filtering-related issues a disjointed experience where two separate consoles (usually running on two separate systems) are required to determine the cause of a reported issue.

Sophos addresses this with the Mail Manager, a built-in mail flow analyzer tool that can be used for everything from troubleshooting to green lighting blocked emails.

The Mail Manager is found in the Email Protection menu and starts with a summary of email activity, giving you an at-a-glance view of the general health and operation of your email traffic. By clicking the "Open Mail Manager in a new window" button, the GUI will pop up the Manager, as shown in the figure below.

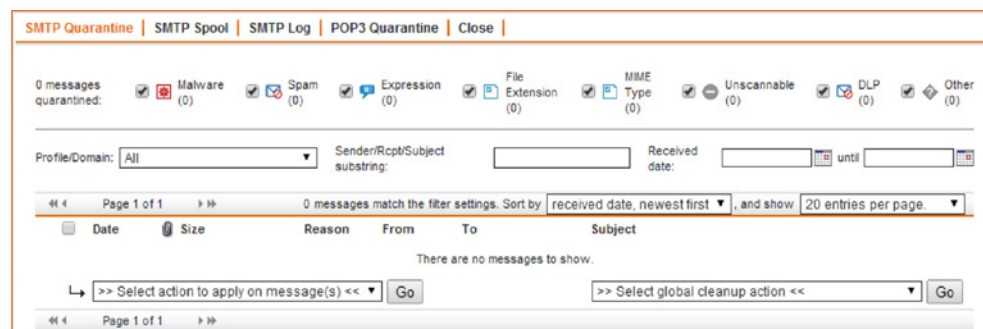


Figure 48 - Sophos UTM Mail Manager

Quarantined mail can be retrieved, released and reviewed from the SMTP and POP3 Quarantine tabs. The SMTP Spool tab shows all mail currently stuck in delivery on the UTM, and the SMTP Log shows any action performed by the subsystems, providing valuable data on the detailed processing of mail and any errors that might have occurred in the transactions witnessed by Sophos UTM.

User portal

The user portal is one of Sophos UTM's main strengths when it comes to end user usability. It allows users to set parameters such as whitelists and blacklists without administrative intervention, and to release their own quarantined items, delivering on our promise to simplify security.

To enable the user portal, go to Management -> User Portal and select which networks are allowed to reach the portal and which users are allowed access (or allow any user). This will prompt UTM to start the User Portal on port TCP 443 on the default IP address of the configured interface.

The items shown in the user portal are dynamically generated based on the user's profile (administrators see different items than regular users) and the features enabled on the UTM. Administrators can however choose to influence which parts of the user portal should not be available by selecting them from the "Disable Portal Items" menu in the "Advanced" tab.

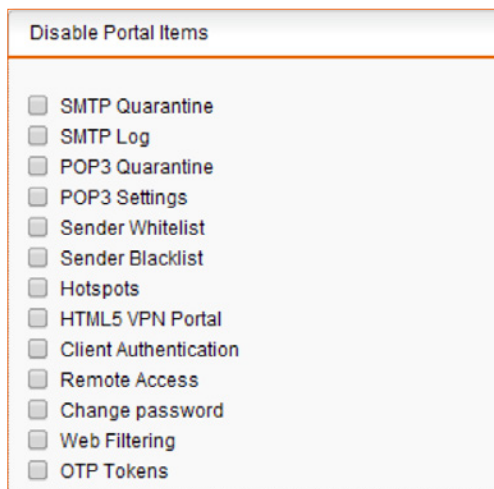


Figure 49 - Sophos UTM User Portal items

This tab also houses configuration items related to the IP address and port the User Portal utilizes, allowing administrators to pick a port and address more suitable to their environment.

Missing functionality

There are some unique TMG features that cannot be replaced by Sophos UTM. Here, we discuss these functionalities and provide alternative solutions and workarounds wherever possible.

EdgeSync support

Microsoft first introduced the Edge server with the release of Exchange 2007. This server role was designed to be at the edge or in the DMZ of a network and was therefore hardened quite thoroughly. Microsoft immediately realized that enabling RPC traffic to and from such a potentially vulnerable host would be detrimental to the security effort, and set out to find a way to integrate a server into Exchange's infrastructure without requiring the server to be part of Active Directory or to use RPC for communication with the other Exchange components.

The solution they came up with is EdgeSync, a service that uses secure LDAP connections to communicate and only work in a one direction: from internal to external. An Edge server can never initiate a connection to other Exchange services, and any traffic without a previously established connection coming from this host will be dropped.

Creating a new EdgeSync connection is done through the EdgeSubscription protocol, in which the Edge Server generates a hashed configuration file which is exported as an XML.

When the XML is imported to Exchange, it will automatically configure the new Edge server and use the hashed credentials used in the EdgeSubscription file to authenticate when communicating with the Edge service. This negates any potential man-in-the-middle and impersonation attacks from both sides of the communication.

Due to its proprietary nature, Sophos UTM cannot support this protocol.

- › **How to work around this:** While Sophos UTM supports multiple methods of intercepting and filtering incoming and outgoing email, the most widely used workaround for EdgeSync is to configure authenticated relaying on UTM and configure the appropriate smarthost settings in Exchange's Send Connector.

Authenticated Relaying is configured on Sophos UTM by navigating to the "Relaying" tab of the SMTP configuration settings. The feature requires a user or group to be configured (these can be selected from any source, ranging from local to AD and RADIUS) and can be enabled by ticking the "Allow authenticated relaying" checkbox. Best practice is to configure a single "service" user (either local or on a remote authentication system) with a very strong password for this exact purpose.

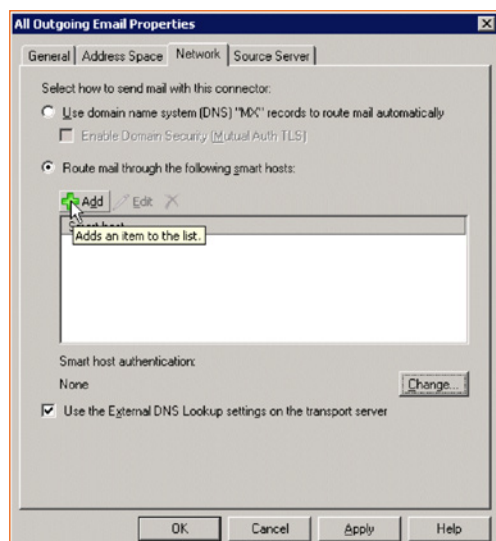


Figure 50 - Exchange smart host configuration

On Exchange, you need to configure a smart host for outgoing email as part of the send connector. Click the default send connector (or create a new one) and edit its settings by double clicking it.

In the next menu, simply configure the required smart host settings by selecting the radio button "Route mail through the following smart hosts" and clicking "+Add."

Add the IP address associate to Sophos UTM's internal (or nearest, network-wise) interface or the FQDN of the UTM in the next menu and click "OK."

To enable authentication for the smart host, click the "Change" button. Select the radio button called "Basic Authentication" and fill in the authentication details in the fields below. This will prompt Exchange to use these authentication settings when connecting to Sophos UTM.

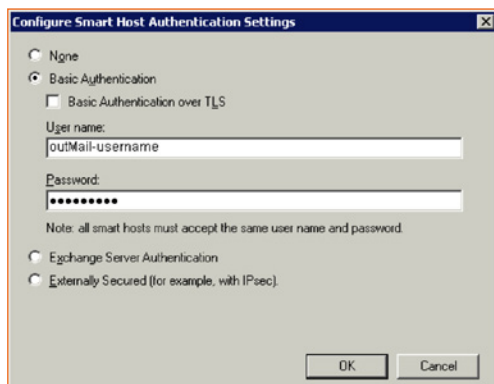


Figure 51 - Exchange smart host authentication

As this migration guide highlights, Sophos UTM not only replaces your aging Microsoft TMG with all the features and capabilities you need, but it can also expand your protection with more capabilities. If you haven't already made the switch from TMG to Sophos UTM, [get a free trial of the best TMG replacement today](#).

Sophos UTM

Get a free trial at sophos.com/utm

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

Oxford, UK | Boston, USA
© Copyright 2014, Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

1166-05.14DD.gna.simple

SOPHOS